ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ασφάλεια και Ιδιωτικότητα σε Περιβάλλοντα Ναυτιλίας** **(Αγγλικά)** **Security and Privacy in Maritime Environment.**
Ονοματεπώνυμο Φοιτητή	**Παναγιώτης Σχοινάς**
Πατρώνυμο	**Λεωνίδας**
Αριθμός Μητρώου	**ΜΠΚΣΑ20011**
Επιβλέπων	**Καθηγητής Χρήστος Δουληγέρης**

Δεκέμβριος 2024

Τριμελής Εξεταστική Επιτροπή

Όνομα Επώνυμο **Βαθμίδα**	**Όνομα Επώνυμο** **Βαθμίδα**	**Όνομα Επώνυμο** **Βαθμίδα**
Χρήστος Δουληγέρης Καθηγητής	Παναγιώτης Κοτζανικολάου Καθηγητής	Δέσποινα Πολέμη Καθηγήτρια

Περίληψη

Οι κυβερνο-επιθεσεις αποτελούν μία σύγχρονη μορφή απειλής και κινδύνου για τα πληροφοριακά ICT συστήματα. Η ένταση καθώς και η συχνότητα τους διαρκώς εντείνεται στα τελευταία χρόνια, δεδομένης της απρόσκοπτης και παγκόσμιας συνδεσιμότητας που προσφέρεται για όλα τα πληροφοριακά συστήματα, μέσω του παγκόσμιου ιστού του διαδικτύου (Internet). Επομένως, τα πληροφοριακά συστήματα έχουν αποκτήσει μία ανεξάρτητη και διαρκώς επεκτεινόμενη παρουσία στον κυβερνοχώρο, υποστηριζόμενα από τις μελλοντικές και τρέχουσες τάσεις της τεχνολογίας του Internet των Πραγμάτων.

Στα πλαίσια της παρούσας εργασίας, εξετάζεται ο κίνδυνος και οι επισφάλειες που εισάγονται μέσω των κυβερνο-επιθέσεων ειδικότερα στο χώρο της ναυτιλίας. Η σύγχρονη ναυτιλία μέσω της αυτοματοποίησης και της ικανότητας διασύνδεσης πλοίου - ακτής μέσω επίγειων και δορυφορικών συνδέσεων, έχει μετατραπεί σε ένα κινούμενο πληροφοριακό σύστημα. Οι μελλοντικές τάσεις για την μετεξέλιξη της ναυτιλίας σε αυτοματοποιημένη ή αυτόνομη, επιτείνει αυτούς τους κινδύνους.

Η παρούσα εργασία εστιάζει στην Ασφάλεια και περιλαμβάνει την ακόλουθη δομή. Αρχικά γίνεται μια αναφορά στα καταγεγραμμένα συμβάντα της προηγούμενης δεκαετίας στη Ναυτιλία καθώς και κατηγοριοποίησή τους.Ακολούθως παρουσιάζονται οι τεχνικές επιθέσεων και τα τρωτά σημεία της ναυτιλίας σε όλες τις υποδομές της.Ιδιαίτερη μνεία γίνεται σε επιθέσεις και ευπάθειες στις δορυφορικές επικοινωνίες καθώς και στα αυτόνομα πλοία. Τέλος, αποτυπώνονται οι τρόποι αντιμετώπισης των κυβερνο-επιθέσεων σε όλόκληρη την υποδομή της ναυτιλίας. Η αντιμετώπιση περιλαμβάνει τις ρυθμιστικές αρχές – φορείς και οργανισμούς που ασχολούνται με τα θέματα των κανονισμών και της κυβερνο-ασφάλειας,καθώς και τις τεχνολογικές προτάσεις, οι οποίες μπορούν να υιοθετηθούν από τη σύγχρονη ναυτιλία. Οι προτάσεις αυτές αντιμετωπίζουν και θωρακίζουν από τις τρέχουσες και μελλοντικές τάσεις των κυβερνο-απειλών στο χώρο της ναυτιλίας, βάσει των υποστηριζόμενων δυνατοτήτων από την σύγχρονη τεχνολογία.

Abstract

Cyber-attacks are a modern form of threat and risk for information ICT systems. Their intensity and frequency have been constantly increasing in recent years, given the seamless and global connectivity offered to all information systems, through the World Wide Web (Internet). Therefore, information systems have acquired an independent and constantly expanding presence in cyberspace, supported by future and current trends in Internet of Things technology.

In this thesis, the risk and uncertainties introduced by cyber-attacks are examined, in Maritime Sector. Modern shipping, through automation and the ability to interconnect between ship and shore via terrestrial and satellite connections, has been transformed into a mobile information system. Future trends for the evolution of shipping to automated or autonomous, exacerbate these risks.

This paper focuses on Security and includes the following structure. Initially, a reference is made to the recorded incidents of the previous decade in the Maritime Environment as well as their categorization. Then, the attack techniques and vulnerabilities in maritime infrastructures are presented. Attacks and vulnerabilities in satellite communications as well as in autonomous ships are thoroughly analyzed. Finally, the ways of dealing with cyber-attacks in the entire maritime Industry are depicted. The measurements include the authorities – bodies and organizations that deal with the regulations and guidance, as well as the technological proposals, which can be adopted by modern maritime industry. These proposals address and protect against current and future trends in cyber threats in the maritime sector, based on the capabilities supported by modern technology.

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον Καθηγητή μου Κο. Χρήστο Δουληγέρη τόσο για την εμπιστοσύνη που μου έδειξε αναθέτοντας μου την διεκπεραίωση της παρούσας εργασίας, όσο και για την άριστη συνεργασία μας για την επιτυχημένη ολοκλήρωσή της.

Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου και τα κοντινά μου πρόσωπα, για την αμέριστη υποστήριξη που μου έδειξαν καθόλη τη διάρκεια του μεταπτυχιακού μου.

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Συντμήσεων

3DES	**Triple Data Encryption Standard**
ABS	**American Bureau of Shipping**
AEMC	**Autonomous Engine Monitoring and Control**
AES	**Advanced Encryption Standard**
AI	**Artificial Intelligence**
AIS	**Automatic Identification System**
ALE	**Annualized Loss Expectancy**
AMSC	**Area Maritime Security Committees**
ARO	**Annual Rate of Occurrence**
ASC	**Autonomous Ship Controller**
ASM	**Advanced Sensor Module**
ATON	**Aids to Navigation**
ATT	**Average Turnaround Time**
BiMCO	**Baltic and International Maritime Council**
BNS	**Bridge Navigation Systems**
BPA	**British Ports Association**
CA	**Certificate Authority**
CAN	**Controller Area Network**
CBC	**Cipher block chaining**
CCTV system	**Closed Circuit Television**
CEV	**Crewed Electric Vessels**
CI	**Critical Infrastructure**
CII	**Critical Information Infrastructure**
CISA	**Cybersecurity and Infrastructure Security Agency**
CISO	**Chief Information Security Officer**
COP	**Code of Practice**
COSCO	**China Ocean Shipping Company**
COTS	**Commercial-of-the-Shelf**
CPA	**Closest Point-of-Approach**
CPS	**Cyber-physical Systems**
CSA	**Cyber Security Assessment**
CSI	**Container Security Initiative**
CSIRT	**Computer Security Incident Response Team**
CSO	**Company Security Officer**
CSP	**Cyber Security Plan**
CSR	**Certificate Signing Request**
CySiMS	**Cyber Security in Merchant Shipping**
CYSO	**Cyber Security Officer**

DA	**Designated Authorities**
DCS	**Distributed Control System**
DHS	**Department of Homeland Security**
DoS	**Denial of Service**
DDoS	**(Distributed) Denial of Service**
DSP	**Digital Service Providers**
DWT	**Dead Weight Tonnage**
EAS	**Engine Automation Systems**
ECC	**Elliptic Curves Codes**
ECDIS	**Electronic Chart Display and Information System**
EDIFACT	**Electronic Data Interchange for Administration, Commerce and Transport**
EEAS	**European External Action Service**
EMSA	**European Maritime Safety Agency**
ENISA	**European Union Agency for Cyber Security**
EUMSS	**European Maritime Security Strategy**
FAL	**Facilitation Commitee**
FAS	**Fully Autonomous SHips**
FBB	**Intellian Fleet Broadband**
GDPR	**General Data Protection Regulation**
GEO	**Geosynchronous Equatorial Orbit**
GLONASS	**GLObalnaya NAvigatsionnaya**
GMDSS	**Global Maritime Distress and Safety System**
GMN	**Global MTCC Network**
GNSS	**Global Navigation Satellite System**
GPS	**Global Positioning System**
GSM	**Global System for Mobile tele-communications**
HTS	**High Throughput Satellite**
HTTP	**HyperText Transport Protocol**
IACS	**International Association of Classification Societies**
IAPH	**International Association of Ports and Harbors**
IBC code	**International Code for the Construction and Equipment of Ships carrying Dangerous Chemicals in Bulk**
IBMS	**Integrated Building Management Systems**
IBS	**Integrated Bridge System**
ICS	**Industrial Control System**
ICT	**Information Communication Technology**
IDS	**Intrusion Detection Systems**
IEEE	**Institute of Electrical and Electronics Engineers**
IET	**Institution of Engineering and Technology**
IFTFCC	**International transport freight costs and other charges**

ILO	**International Labour Organization**
IMDG Code	**International Maritime Dangerous Goods code**
IMO	**International Maritime Organization**
IMSBC code	**International Maritime Solid Bulk Cargoes code**
INS	**Integrated Navigation System**
IoT	**Internet of Things**
IPSec	**Internet Protocol Security**
IRNSS	**Indian Regional Navigation Satellite System**
ISAC	**Information Sharing and Analysis Centre**
ISM	**International Safety Management**
ISMS	**Information Security Management System**
ISPS	**International Ship and Port Facility Security**
IT	**Information Technology**
ITU-R	**International Telecommunication Union RadioCommunication**
LDAP	**Lightweight Directory Access Protocol**
LEO	**Low Earth Orbit**
LiDAR	**Light Detection and Ranging**
LNG	**Liquified Natural Gas**
LRIT	**Long Range Identification and Tracking**
MARAD	**Maritime Administration**
MARPOL	**International Convention for the Prevention of Pollution from Ships**
MASS	**Maritime Autonomous Surface Ships**
MCS	**Machinery Control System**
MEMS	**Micro - Electromechanical Systems**
MEO	**Medium Earth Orbit**
ML	**Machine Learning**
MMSI	**Mobile Maritime Service Identity**
MRCC	**Maritime Rescue Coordination Centres**
MSA	**Maritime Safety Administration**
MSC	**Mediterranean Shipping Company**
MTCC	**Maritime Technology Cooperation Centre**
MTS	**Maritime Transportation System**
MUNIN	**Maritime Unmanned Navigation through Intelligence in Networks**
NavIC	**Navigation with Indian Constellation**
NAVTEX	**Navigational telex**
NFAS	**Norwegian Forum for Autonomous Ships**
NIS	**Network and Information Systems**
NIST	**National Institute of Standards and Technology**

NLF	**New Legislative Framework**
NTP	**Network Time Protocol**
OCT	**On-board Control Team**
OES	**Operators providing Essential Services**
OT	**Operational Technology**
PCS	**Port Community System**
PGP	**Pretty Good Privacy**
PKI	**Public Key Infrastructures**
PLC	**Programmable Logic Controller**
PNT	**Positioning, navigation, and timing**
PPS	**Precise Positioning Service**
PFSO – PSO	**Port (Facility) Security Officer**
PSA – PFSA	**Port (Facility) Security Assessment**
PSC	**Port State Control**
PSO - PFSO	**Port (Facility) Security Officer**
PSP – PFSP	**Port (Facility) Security Plan**
QZSS	**Quasi-Zenith Satellite System**
QKD	**Quantum key distribution**
RA	**Risk Assessment**
RADAR	**Radio Detection and Ranging**
RADIUS	**Remote authentication dial-in user service**
RCS	**Remote Controlled Ships**
RCU	**Rendezvous Control Unit**
RDP	**Remote Desktop Protocol**
RF	**Radio-Frequency**
RIB	**Rigid Inflatable Boat**
RM	**Risk Management**
RMA	**Risk Managment Analysis**
RMF	**Risk Management Framework**
RSA	**Rivest-Shamir-Adleman**
RSE	**Regulatory Scoping Exercise**
SAE	**Society of Automotive Engineers**
SAML	**Security assertion markup language**
SAR	**Situational Awareness**
SAS	**Semi-Autonomous Ships**
SCADA	**Supervisory Control and Data Acquisition**
SCC	**Shore Control Center**
SCSO	**Ship Cyber Security Officer**
SeMS	**Security Management System**
SLE	**Single Loss Expectancy**
SMS	**Safety Management System**

SOC	**Security Operations Centre**
SOLAS	**Safety Of Life at Sea**
SOP	**Standard Operating Procedures**
SPS	**Standard Positioning System**
SSAS	**Ship Security Alert System**
SSH	**Secure Shell**
SSM fh	**Spread spectrum modulations and frequency hopping**
SSO	**Ship Security Officer**
SSP	**Ship Security Plan**
SSS	**Share-Store-Sale markets**
STCW	**Seafarers' Training, Certification and Watchkeeping**
TLS/SSL	**Transport Layer Security/Secure Sockets Layer**
TOS	**Terminal Operating System**
UAV	**Unmanned Air Vehicles**
USCG	**U.S. Coast Guard**
VDES	**VHF Data Exchange System**
VDR	**Voyage Data Recorder**
VHF	**Very High Frequency Radio Band**
VMS	**Vessel Monitoring Systems**
VoIP	**Voice over IP**
VPN	**Virtual Private Networks**
VSAT	**Very Small Aperture Terminals**
VTMIS	**Vessel Traffic Monitoring and Information System**
VTS	**Vessel Traffic Services**
XML	**eXtensible markup language**

1.Εισαγωγή

Η κυβερνοασφάλεια αποτελεί έναν από τους πιο κρίσιμους τομείς για τη ναυτιλιακή βιομηχανία, καθώς οι σύγχρονες τεχνολογίες και οι ψηφιακές υποδομές έχουν γίνει αναπόσπαστο κομμάτι της λειτουργίας των πλοίων και των λιμανιών. Έως και πριν λίγα χρόνια ωστόσο, οι φορείς της Ναυτιλίας δεν δίναν την απαραίτητη βαρύτητα στην κυβερνοασφάλεια και σε διοικητικό επίπεδο δεν γινόταν δαπάνη πόρων για λήψη μέτρων αποφυγής κυβενοπεριστατικών. Μολαταύτα, η αυξανόμενη εξάρτηση από αυτές τις τεχνολογίες έχει οδηγήσει σε μια σειρά από προκλήσεις και κινδύνους, όπως οι κυβερνοεπιθέσεις, οι οποίες μπορούν να προκαλέσουν σοβαρές ζημιές τόσο σε οικονομικό όσο και σε λειτουργικό επίπεδο. Στην παρούσα διπλωματική εργασία, αναλύονται παλαιότερα συμβάντα κυβερνοεπίθεσης, οι κατηγορίες τους, καθώς και οι επιπτώσεις τους στο ναυτιλιακό περιβάλλον. Ειδικότερα, εξετάζονται φαινόμενα όπως το GPS και GNSS jamming και spoofing, οι επιθέσεις στο σύστημα AIS, οι κυβερνοεπιθέσεις σε δορυφορικές επικοινωνίες και οι προκλήσεις που αντιμετωπίζουν τα αυτόνομα πλοία, καθώς και προτεινόμενα μέτρα περιορισμού και αποφυγής των κυβερνοπεριστατικών.

1.1 Κυβερνοεπιθέσεις στο Ναυτιλιακό τομέα

Ως Κυβερνο-επίθεση (cyber-attack) οριζεται κάθε είδος επιθετικής ενέργειας που προκαλείται από άτομα ή ολόκληρες οργανώσεις (ομάδες)και έχει ως στόχο τις πληροφοριακές υποδομές, τα συστήματα υπολογιστών, τις υποδομές επικοινωνιών, τα δίκτυα υπολογιστών ή/και συσκευές προσωπικών υπολογιστών. Η επίθεση εκδηλώνεται με διάφορα μέσα (υλικό - λογισμικό ή/και κακόβουλη χρήση και των δύο), που συνήθως προέρχονται από μια ανώνυμη πηγή. Σκοπός αυτής της κακόβουλης ομάδας, είναι η κλοπή, η αλλοίωση ή/και η καταστροφή μίας υποδομής - οργανισμού - εταιρείας - κυβέρνησης ή άλλου φορέα, μέσω εισβολής (Intrusion) στα συστήματα ζωτικών λειτουργιών της υποδομής.Άλλος ένας πιο συνοπτικός ορισμός, σύμφωνα με τον NIST, είναι ότι αποτελεί μια επίθεση, μέσω του Κυβερνοχώρου, που στοχεύει στη χρηση του κυβερνοχώρου ενός οργανισμού/επιχείρησης με σκοπό τη διατάραξη, την απενεργοποίηση, την καταστροφή ή τον κακόβουλο έλεγχο ενός υπολογιστικού συστήματος/υποδομής ή καταστροφή της ακεραιότητας των δεδομένων ή κλοπή ελεγχόμενων πληροφοριών.

Από κυβερνο-επιθέσεις κινδυνεύουν σχεδόν όλοι οι τομείς που κάνουν χρήση πληροφοριακών συστημάτων (Information Technology - IT ή Operational Technology - OT) [4] και υποστηρίζουν διασύνδεση των υπολογιστικών τους συστημάτων μέσω του παγκόσμιου ιστού του διαδικτύου (Internet). Από τις κυβερνο-επιθέσεις επίσης κινδυνεύουν, και οι υποδομές καθώς και οι δραστηριότητες των ναυτιλιακών εταιρειών και οργανισμών, εφόσον ο εκσυγχρονισμός τους, έχει οδηγήσει τις υποδομές τους σε χρήση δικτύων ΗΥ και του παγκόσμιου ιστού. Οπότε σε αυτήν την περίπτωση, οι ειδικού τύπου επιθέσεις χαρακτηρίζονται ως "ναυτιλιακές κυβερνο-επιθεσεις" (Maritime Cyber-attacks).

Ειδικότερα για τις ναυτιλιακές δραστηριότητες, η συνδεσιμότητα μέσω συστημάτων πλοήγησης και ηλεκτρονικής ταυτοποίησης, όπως το Automatic Identification System (AIS), το Global Navigation Satellite System (GNSS Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης), Το Global Positioning System (GPS - Παγκόσμιο Σύστημα Εντοπισμού) και η χρήση των εφαρμογών RADAR, αποτελούν ζωτικές τεχνολογίες γαι την ασφαλή πλοήγηση των σύγχρονων πλοίων (μερικώς ή ολικώς αυτόνομα σκάφη). Τα παραπάνω συστήματα υποστηρίζονται από τεχνολογίες, οι οποίες λόγω της διασυνδεσιμότητας τους σε παγκόσμιο επίπεδο, αποτελούν στόχους κυβερνο-επιθέσεων. Επιπλέον, οι ναυτιλιακές εταιρείες έχουν υποβληθεί σε εξαιρετικά περίπλοκες και νέες κατηγορίες κυβερνο-επιθέσεων, που στοχεύουν στα συστήματα πληροφοριών των υποδομών τους. Στόχος των επιθέσεων είναι να προκαλέσουν ζημιά στον εξοπλισμό του πλοίου [11], να λάβουν πληροφορίες ναυσιπλοΐας, πελατών, φορτίων ή/και δρομολογίων. Λόγοι που ευννούν την επιτυχία των κυβερνο-επιθέσεων στις ναυτιλιακές υποδομές, είναι:

- Η εξάρτηση λειτουργίας των εταιρειών, των λιμανιών, και των πλοίων από το Διαδίκτυο (Internet) και τις εφαρμογές του
- Η λειτουργία των συστημάτων υποδομών των πλοίων - εταιρειών - οργανισμών - λιμένων, με μη προστατευμένους υπολογιστές
- Η μη επαρκής εκπαίδευση των πληρωμάτων, του προσωπικού και των εργαζομένων στις υποδομές αυτές

Οι ανωτέρω λόγοι αυξάνουν περαιτέρω την πιθανότητα μίας επιτυχούς επίθεσης στον κυβερνοχώρο, ως προς την εκδήλωση και έκβαση τους. Υπάρχουν σαφείς ενδείξεις, ότι η απουσία εκπαίδευσης σχετιζόμενης με την ασφάλεια των δικτύων καθώς και των εργαζομένων σε ολόκληρη την αλυσίδα εφοδιασμού και λειτουργίας, είναι μια σημαντική πηγή για τα κενά ασφαλείας που εμφανίζονται στα πληροφοριακά συστήματα κάθε ναυτιλιακής εταιρείας - οργανισμού. Ως αποτέλεσμα, αυτοί που εκτελούν μία κυβερνο-επίθεση (hackers) μπορούν να χρησιμοποιούν "κλασικές προσεγγίσεις", όπως: ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου τύπου ψαρέματος (phishing), μολύνσεις με συνημμένα αρχεία, χρήση ιών και ransomware, ή επιθέσεις τύπου άρνησης παροχής υπηρεσίας (Denial-of-Service-DoS), για την επίτευξη επιτυχημένων παραβιάσεων των δικτύων [11]. Ένα σχέδιο ασφαλείας για την αποτροπή και αντιμετώπιση αυτών των επιθέσεων, πρέπει να παρέχει διαδικασίες για την προστασία της θαλάσσιας αλυσίδας εφοδιασμού και συντονισμένη στρατηγική δράσης με διεθνείς ναυτιλιακούς οργανισμούς [32], [33]. Η ενημέρωση του λογισμικού στα τερματικά των ΗΥ μέσω αφαιρούμενων μέσων (portable devices), αυξάνει τον κίνδυνο κλοπής ταυτοτήτων και προσωπικών δεδομένων των χειριστών των συστημάτων ναυτιλίας, και η ανταλλαγή πληροφοριών σε πραγματικό χρόνο με τη χρήση νέων τεχνολογιών όπως π.χ το Internet-of-Things - IoT, το οποίο επιτείνει τον κίνδυνο λόγω μη ασφαλών υπηρεσιών δικτύου ή αδύναμου ελέγχου ταυτότητας (weak authentication), είναι λόγοι που συντελούν σε επιτυχείς εκβάσεις των κυβερνο-επιθέσεων από πλευράς των επιτιθέμενων.

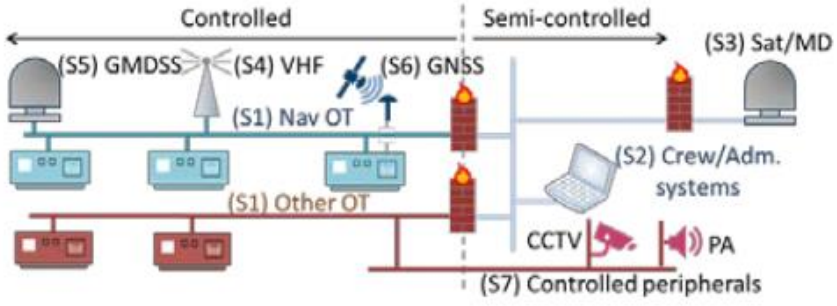
Στη συνέχεια, αν και η εκδήλωση των κυβερνο-επιθέσεων αποτελεί ένα χρονικά πρόσφατο φαινόμενο άρρηκτα συνδεδεμένο με την διάχυση των υπηρεσιών διασύνδεσης του διαδικτύου, παρουσιάζεται μία ιστορική αναδρομή κυβερνο-επιθέσεων στη ναυτιλία, με πρόσφατες αναφορές στο χρονικό διάστημα, το μέρος καθώς και τον στόχο αυτών των επιθέσεων.

1.2 Σημεία κυβερνο-επίθεσεις στη Ναυτιλία

Για την διευκόλυνση στην περιγραφή και τον εντοπισμό των συστημάτων που υπόκεινται σε μία κυβερνο-επίθεση, διακρίνουμε δύο κατηγορίες για τα ναυτιλιακά συστήματα και τον εξοπλισμό:

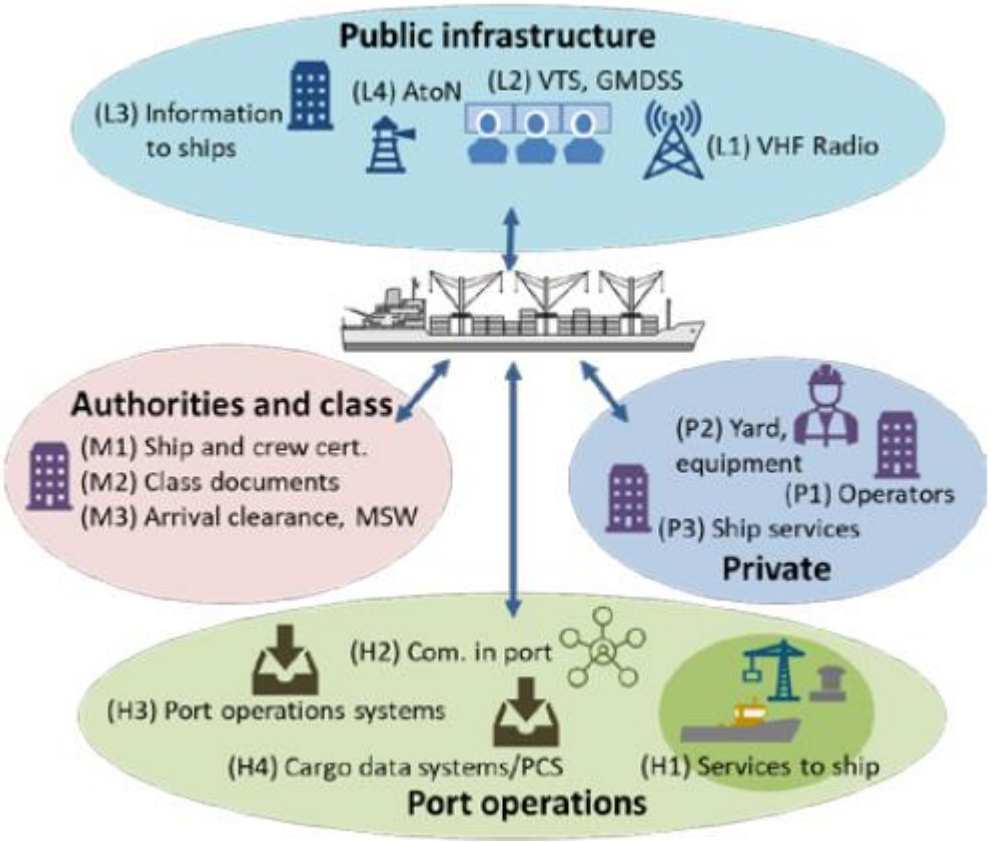
Συστήματα που είναι εγκατεστημένα επί του πλοίου
Συστήματα που είναι εγκατεστημένα εκτός του πλοίου (ακτή)

Το σχήμα που ακολουθεί δείχνει μια γενικευμένη αναπαράσταση των συστημάτων επί του σκάφους, με σημεία επίθεσης ταξινομημένα με κωδικούς από S1 έως S7. Το σημείο S1 αντιπροσωπεύει επιθέσεις σε ναυτιλιακά ή άλλα συστήματα επιχειρησιακής τεχνολογίας (Operational Technology - OT) [2], [5], που συνήθως εντοπίζονται σε ελεγχόμενο περιβάλλον εντός του σκάφους. Αυτό μπορεί επίσης να περιλαμβάνει επιθέσεις μέσω φορητών εξωτερικών δίσκων τύπου "usb", που μερικές φορές χρησιμοποιούνται για μεταφορά αρχείων ή/και ενημερώσεις λογισμικού στα τερματικά των ΗΥ του σκάφους. Το σημείο S2 αντιπροσωπεύει επιθέσεις σε διοικητικά συστήματα επί του σκάφους. Τα σημεία S3 και S4, ορίζονται για επιθέσεις σε δεδομένα κινητής - δορυφορικής επικοινωνίας ή ψηφιακή επικοινωνία ραδιοφάσματος (Very High Frequency Radio Band - VHF) αντίστοιχα. Το σημείο S5 αντιπροσωπεύει επιθέσεις σε παγκόσμια συστήματα εντοπισμού θαλάσσιου κινδύνου και ασφάλειας (Global Maritime Distress and Safety System - GMDSS). Το σημείο S6 αναφέρεται σε παγκόσμια δορυφορικά συστήματα πλοήγησης (Global Navigation Satellite Systems - GNSS) ενώ το σημείο S7 σε περιφερειακές συσκευές σε συστήματα ελέγχου. Το σημείο S0 χρησιμοποιείται για οποιαδήποτε άλλη επίθεση επί του πλοίου που δεν εντάσσεται στις ανωτέρω κατηγορίες.



Σχήμα 1: Σημεία εκδήλωσης κυβερνο-επιθέσεων επί του πλοίου [6]

Η άλλη ομάδα σημείων επίθεσης, εστιάζει στην επικοινωνία μεταξύ του πλοίου και της ακτής/λιμένα (shore) και περιλαμβάνει τα αντίστοιχα συστήματα ακτής/λιμένα. Αυτά τα σημεία παρουσιάζονται στο σχήμα που ακολουθεί:



Σχήμα 2: Σημεία εκδήλωσης κυβερνο-επιθέσεων στις συνδέσεις του πλοίου με την ακτή/λιμένα [6]

Η πρώτη ομάδα σημείων διεπαφής, ανήκει στις δημόσιες υποδομές. Οι πιο σχετικές είναι η υποδομή μετάδοσης φωνής και δεδομένων, που χρησιμοποιεί τον ραδιοδίαυλο VHF, συμπεριλαμβανομένων των υπηρεσιών συστήματος αυτόματης αναγνώρισης (AIS) (L1) [2]. Επιπλέον συμπεριλαμβάνει τις υπηρεσίες ρύθμισης κυκλοφορίας σκαφών, τις υπηρεσίες θαλάσσιας διάσωσης και GMDSS (L2), διάφορες υπηρεσίες πληροφοριών για τα πλοία, συμπεριλαμβανομένων μετεωρολογικών δεδομένων, συνιστώμενων δρομολογίων και ειδοποιήσεων προς τους ναυτικούς (L3), και ψηφιοποιημένα βοηθήματα πλοήγησης (L4). Άλλα σημεία επίθεσης που δεν εντάσσονται στις ανωτέρω κατηγορίες της εν λόγω ομάδας επισημαίνονται ως σημείο L0.

Η επόμενη ομάδα σημείων διεπαφής, για την εκδήλωση κυβερνο-επιθέσεων, είναι οι Αρχές, οι νηογνώμονες καθώς και τυχόν εταιρείες οι οποίες σχετίζονται με διαπίστευση/ελέγχους του πλοίου και των ναυτιλιακών εταιρειών. Η ομάδα αυτή περιλαμβάνει όλες τις διαδικασίες υποδομής που απαιτούνται για την ανταλλαγή πληροφοριών και την αρχειοθέτηση των πληροφοριών στα συστήματα. Το σημείο M1 σχετίζεται με τα πιστοποιητικά πλοίου και πληρώματος (π.χ. αυτά που εκδίδονται για επίδειξη νομιμότητας του σκάφους από το κράτος σημαίας του). Το σημείο M2 αφορά σε υπηρεσίες και έγγραφα που εκδίδονται από νηογνώμονες/εταιρείες διαπίστευσης. Το σημείο M3 αφορά σε Αρχές και τις αντίστοιχες υπηρεσίες τους που σχετίζονται με την διαπίστευση/εξουσιοδότηση της άφιξης και αναχώρησης του σκάφους από έναν λιμένα (π.χ., θαλάσσια μεμονωμένα χρονικά παράθυρα διέλευσης εντός των ορίων του λιμένα, πληροφοριακό σύστημα στο οποίο υποβάλλονται πληροφορίες πριν τον κατάπλου πλοίων σε λιμένες ή κατά τον απόπλου από αυτούς (Ενιαία Ναυτιλιακή Θυρίδα - MSW), διαπίστευση επιβατών, υγειονομικές υπηρεσίες κ.λπ). Το σημείο M0 χρησιμοποιείται για άλλα σημεία επίθεσης που δεν έχουν περιγραφεί σε αυτήν την ομάδα.

Η επόμενη ομάδα σημείων διεπαφής αφορά τις υπηρεσίες λιμένων.Το πρώτο σημείο επαφής H1 αφορά τις υπηρεσίες που παρέχονται προς τα πλοία,όπως για παράδειγμα διαδικασίες που σχετίζονται με την παροχή λιμενεργατών και ρυμουλκών. Το σημείο H2 επισημαίνει επιθέσεις σε εσωτερική επικοινωνία και ανταλλαγή δεδομένων εντός θυρών και τερματικών του σκάφους. Επιθέσεις στο σημείο H3 σε συστήματα δεδομένων λειτουργίας λιμένων, όπως τα συστήματα διαχείρισης κίνησης λιμένος, προϊστάμενου λιμενικού σώματος,OT συστήματα κ.λπ. Επίθεση στο σημείο H4 αφορά σε συστήματα δεδομένων που σχετίζονται με το φορτίο(cargo) για διαδικασίες φορτο-εκφόρτωσης στο λιμάνι. Αυτό μπορεί επίσης να περιλαμβάνει συστήματα κοινότητας λιμένων (Port Community Systems - PCS) που χρησιμοποιούνται για να διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ των διαφόρων φορέων που δραστηριοποιούνται σε ένα λιμάνι, όπως είναι οι λιμενικές αρχές, οι μεταφορείς, οι τελωνειακές υπηρεσίες και άλλοι εμπλεκόμενοι φορείς.Το σημείο H0 χρησιμοποιείται για άλλα σημεία επίθεσης στις λιμενικές υπηρεσίες, που δεν έχουν περιγραφεί στην προηγούμενη ομάδα.

Στην τελευταία ομάδα ανήκουν οι ιδιωτικές υπηρεσίες.Στο πρώτο σημείο (P1) ανήκουν οι εταιρείες εκμετάλλευσης (operators)πλοίων . Αυτό το σημείο περιλαμβάνει τον ιδιοκτήτη, τον διαχειριστή, και τις εντολές που αποστέλλονται από/προς το πλοίο κ.λπ. Το σημείο P2 χρησιμοποιείται για τις τεχνικές υπηρεσίες στα ναυπηγεία, τα ανταλλακτικά ή τους προμηθευτές αναλώσιμων ειδών. Το σημείο P3 αφορά σε άλλες υπηρεσίες, όπως η δρομολόγηση καιρού, η βελτιστοποίηση διαδρομής κ.λπ. Το σημείο P0 αντιπροσωπεύει άλλες υπηρεσίες που δεν περιγράφηκαν στην προηγούμενη ομάδα

Στη συνέχεια η παραπάνω κατηγοριοποίηση των τύπων των κυβερνο-επιθέσεων ως προς τα σημεία εκδήλωσης τους, χρησιμοποιείται ως βάση αναφοράς για τα ιστορικά γεγονότα και την περιγραφή τους, που παρατίθενται στην επόμενη ενότητα.

1.3 Ιστορική αναδρομή Κυβερνο-επιθέσεων στη Ναυτιλία

Διαχρονικά οι μεγαλύτεροι φόβοι της ναυτιλιακής κοινότητας καθώς και οι έρευνες προσδιορισμού των απειλών στην Ναυτιλιά που γίνονταν αφορούσαν την φυσική ασφάλεια και επικεντρώνονταν κυρίως στην παγκόσμια (διεθνή) τρομοκρατία [34], [35]. Το 2011, ο Ευρωπαικός Οργανισμός για την Κυβερνοασφάλεια (European Union Agency for Cyber security – ENISA), δημοσίευσε την έκθεση "Analysis of Cyber Security Aspects in the Maritime Sector" [36]. Η έκθεση αναγνώριζε τον ναυτιλιακό τομέα, ως "κρίσιμηυποδομή" για την εκδήλωση κυβερνο-επιθέσεων. Η έκθεση προσδιόρισε ότι, "η πολύ χαμηλή ευαισθητοποίηση σχετικά με την ασφάλεια στον κυβερνοχώρο, αποτελεί μείζονα πρόκληση" [36]. Επιπλέον η έκθεση πρότεινε ότι, "ο χαμηλός αριθμός δημοσίως γνωστών - κοινοποιούμενων, περιστατικών ασφάλειας στον κυβερνοχώρο, θα μπορούσε να είναι ο λόγος για την υποβάθμιση των κυβερνο-επιθέσεων" [36].Ένας πιθανός λόγος είναι ότι οι ναυτιλιακές δεν ήθελαν να κοινοποιήσουν τα κυβερνο-περιστατικά για να μην πληγεί το κύρος τους και η εμπιστοσύνη των πελατών, με απώτερο σκοπό την μείωση αποφυγής εσόδων. Μια αντίστοιχη νορβηγική έκθεση[52],κυκλοφόρησε το 2015και αφορούσε τα ψηφιακά "τρωτά σημεία" στον ναυτιλιακό τομέα. Με την έκθεση αυτή προσδιόριστηκαν οι 10 κορυφαίες προκλήσεις στον τομέα της ναυτιλίας, σχετικά με κυβερνο-επιθέσεις [52]. Επιπλέον παρείχε παραδείγματα τόσο επιθέσεων, όσο και ατυχημάτων που ήταν δυνατά ως "παράγωγα" εξαιτίας αυτών των κενών ασφαλείας. Ταυτόχρονα ένα Ευρωπαϊκό project με όνομα MUNIN (Maritime Unmanned Navigation through Intelligence in Networks) [28], πραγματοποίησε αξιολόγηση κινδύνου, για την ασφάλεια και τις απειλές στον κυβερνοχώρο, σχετίζοντας αυτές με την "μη επανδρωμένη-αυτόνομη πλοήγηση των σκαφών" [108]. Στους κινδύνους που αναγνώρισε, αναφέρει την παρεμβολή, την παραπλάνηση(spoofing) και την παραβίαση των συστημάτων AIS, GPS και του εξοπλισμού επικοινωνίας των πλοίων. Αυτοί θεωρήθηκαν ως οι "υψηλότεροι κίνδυνοι" για κυβερνο-επιθέσεις. Στο νορβηγικό ερευνητικό έργο CySiMS (Cyber Security in Merchant Shipping), εντοπίστηκαν επίσης απειλές που είναι ειδικού τύπου για τη θαλάσσια ψηφιακή επικοινωνία [37]. Επίσης ερευνητές από το Πανεπιστήμιο του Πλύμουθ έχουν δημοσιεύσει εδώ και αρκετά χρόνια, εργασίες που σχετίζονται με τα "τρωτά σημεία", τις απειλές και τις επιθέσεις στον ναυτιλιακό τομέα [38], [39], [40]. Στην παγκόσμια βιβλιογραφία υπάρχουν περαιτέρω παραδείγματα έρευνας των κενών ασφάλειας σε συγκεκριμένα υποσυστήματα ή λειτουργίες των πλοίων. Οι λειτουργίες αυτές αφορούν στην αυτόνομη ναυτιλία (Autonomous Shipping) [41], στους λιμένες και τα συστήματα πληροφοριών που χρησιμοποιούν [42], καθώς και στα συστήματα IT/OT που είναι ήδη εγκατεστημένα σε πλοία [43].

Σε μια προσπάθεια ανάλυσης των κυβερνοεπιθέσεων στα συστήματα των πλοίων το 2017, το Βρετανικό Υπουργείο Μεταφορών, δημοσίευσε μια επισκόπηση(η οποία αναθεωρήθηκε το 2021) των κινήτρων και συμπεριελάμβανε μεθόδους αξιολόγησης επιπέδου κυβερνοασφάλειας, δημιουργία πλάνου κυβερνοασφάλειας καθώς και κατηγοριοποίηση πιθανών κακόβουλων δρώντων (threat actors) [44] Ο ENISA το 2018 στην ετήσια έκθεσή του για "το τοπίο απειλών στον κυβερνοχώρο", όπου αναλύονται και όλες οι τάσεις των κακόβουλων δρώντων, υποστηρίξε ότι η "αποκόμιση εσόδων από τους εγκληματίες του κυβερνοχώρου, οι οποίοι μπορεί να ήταν και κρατικά υποστηριζόμενοι", γινόταν ένας από τους κύριους μοχλούς για επιθέσεις στον κυβερνοχώρο [45]. Η ανάλυση τους επιβεβαιώθηκε πρόσφατα από τη Νορβηγική Αστυνομική Υπηρεσία Ασφαλείας, η οποία προσδιορίζει τις κρατικές υπηρεσίες πληροφοριών (μυστικές υπηρεσίες) που δρουν κατά της ναυτιλιακής βιομηχανίας, ως "ένα σημαντικό κίνδυνο για τη Νορβηγία" [46]. Περαιτέρω, η Νορβηγική Αρχή Εθνικής Ασφάλειας (NSM), παρέχει ετήσιες αναφορές σχετικά με την εικόνα απειλών στον κυβερνοχώρο κατά της Νορβηγίας [47], [48]. Οι αναφορές αυτές περιλαμβάνουν περιστατικά επιθέσεων μέσω ransomware, επιχειρήσεις ψηφιακών πληροφοριών και διαταραχές στις υπηρεσίες εντοπισμού θέσης των πλοίων.Αντίστοιχες ετήσιες αναφορές αποτύπωσης και αξιολόγησης απειλών καθώς και επικείμενων τάσεων των κακόβουλων δρώντων εκδίδονται από τον ENISA και αφορούν συνολικά των Ευρωπαικό χώρο.

Στη συνέχεια περιγράφονται πραγματικά περιστατικά που αφορούν σε κυβερνο-επιθέσεις στον χώρο της ναυτιλίας, για το χρονικό διάστημα 2010 έως 2020. Τα συμβάντα έχουν κωδικοποιηθεί με αναφορές από A1 - A46 για την περαιτέρω επεξεργασία και εξαγωγή συμπερασμάτων.

Συμβάν A1

Χρονολογία: 2010

Σημείο επίθεσης: S1

Στο περιστατικό αυτό, ένα πλωτό γεωτρύπανο "μολύνθηκε" από κακόβουλο λογισμικό. Η επιμόλυνση του έγινε καθ'οδόν από το ναυπηγείο όπου κατασκευάστηκε στη Νότια Κορέα, προς τη Νότια Αμερική. Για να αποκατασταθούν τα κρίσιμα συστήματα ελέγχου του, απαιτήθηκαν 19 ημέρες διακοπής της λειτουργίας του, για την επίλυση του προβλήματος και τον "¨καθαρισμό" τους. Τέτοιες διακοπές λειτουργίας υπολογίζεται ότι κόστισαν περίπου 700,000 USD ανά ημέρα στην εταιρεία ιδιοκτησίας του γεωτρύπανου [49], [50].

Συμβάν A2

Χρονολογία: 2010 – 2011

Σημείο επίθεσης: P1

Μια ελληνική ναυτιλιακή εταιρεία γίνεται θύμα hackers μέσω του δικτύου WiFi των κεντρικών της γραφείων. Για τα επόμενα δύο χρόνια, οι πληροφορίες σχετικά με τα πλοία της και τις διαδρομές τους, διαρρέουν προς τους hackers. Τα δεδομένα αυτά χρησιμοποιούνται από τους επιτιθέμενους για να σχεδιάσουν επιθέσεις φυσικής πειρατείας στον Κόλπο του Άντεν. Στόχος ήταν η κατάληψη των πλοίων, η κλοπή των εμπορευμάτων τους, καθώς και πιθανή πίεση λύτρων για τα αιχμαλωτισμένα πληρώματα τους [51].

Συμβάν A3

Χρονολογία: 2011 - 2013

Σημείο επίθεσης: H4

Το σύστημα παρακολούθησης φορτίου στο λιμάνι της Αμβέρσας "μολύνθηκε" από ιό. Μια συμμορία διακίνησης ναρκωτικών προσέλαβε μια βελγική ομάδα Χάκερ, οι οποίοι έσπασαν τα συστήματα διαχείρισης δύο προβλητών στο λιμάνι. Το σύστημα αυτό διαχειριζόταν τη μεταφορά, την αποθήκευση και αποστολή χιλιάδων εμπορευματοκιβωτίων που διέρχονταν καθημερινά από το λιμάνι. Η επιμόλυνση είχε ως στόχο να επιτρέψει το λαθρεμπόριο ναρκωτικών και όπλων (αναφέροντας πλαστά μέσω του συστήματος ότι πρόκειται για φορτία μπανάνας από τη Νότια

Αμερική). Η επιχείρηση λαθρεμπορίας εκτιμάται ότι διήρκησε τουλάχιστον δύο χρόνια μέχρι να εντοπιστεί. Το ίδιο λιμάνι δέχτηκε ξανά ίδιου τύπου επίθεση το 2018 [51], [52], [53], [54].

Συμβάν Α4

Χρονολογία: 2011 - 2013

Σημείο επίθεσης: P2

Ένας κακόβουλως δρων (threat actor) που έγινε γνωστός από την Kaspersky [55] ως "Icefog", διεξήγαγε στοχευμένες επιθέσεις κατασκοπείας στον κυβερνοχώρο εναντίον διαφόρων ευαίσθητων οργανισμών στη Νότια Κορέα και την Ιαπωνία. Στους οργανισμούς αυτούς συμπεριλαμβάνονταν ναυτιλιακές και ναυπηγικές εταιρείες. Οι επιθέσεις βασίζονταν στο στοχευμένο ψάρεμα μέσω ηλεκτρονικού ταχυδρομείου (spear-phishing) και στην εκμετάλλευση γνωστών "κενών ασφαλείας" [55].

Συμβάν Α5

Χρονολογία: 2011

Σημείο επίθεσης: P1

Μια κυβερνο-επίθεση εναντίον της ιρανικής ναυτιλιακής εταιρείας IRISL (Ναυτιλιακές Γραμμές Ισλαμικής Δημοκρατίας του Ιράν), κατέστρεψε όλα τα δεδομένα που σχετίζονται με τις τιμές, τη φόρτωση, τον όγκο φορτίου, την ημερομηνία και τον τόπο προέλευσης/κατεύθυνσης των εμπορευμάτων. Η επίθεση δημιούργησε πρόβλημα λειτουργίας επίσης στο εσωτερικό δίκτυο επικοινωνίας της εταιρείας. Συνολικά η επίθεση προκάλεσε σοβαρές οικονομικές απώλειες και απώλεια φορτίου [56], [57].

Συμβάν Α6

Χρονολογία: 2012

Σημείο επίθεσης: S3

Μια άλλη κυβερνο-επίθεση εναντίον του Ιράν τον επόμενο χρόνο είχε ως στόχο τα δίκτυα επικοινωνίας σε υπεράκτια πλατφόρμα στον Περσικό Κόλπο. Η προέλευση της επίθεσης δεν καθορίστηκε [58].

Συμβάν Α7

Χρονολογία: 2012

Σημείο επίθεσης: H4

Μια παραλλαγή του συμβάντος στο λιμένα Αμβέρσας έλαβε χώρα στο σύστημα διακίνησης φορτίου που χρησιμοποιούσε η Υπηρεσία Τελωνείων και Προστασίας των Συνόρων της Αυστραλίας.Το σύστημα μολύνθηκε , επιτρέποντας στους εισβολείς να γνωρίζουν κατά πόσον οι αποστολές τους είχαν επισημανθεί ως "ύποπτες" από τις Αρχές. Σε τέτοιες περιπτώσεις, τα λαθραία εμπορεύματα δεν παραλαμβάνονταν ποτέ [49].

Συμβάν Α8

Χρονολογία: 2012

Σημείο επίθεσης: M1

Τον ίδιο χρόνο η Δανέζικη Ναυτιλιακή Αρχή έπεσε θύμα στοχευμένης επίθεσης από Κινέζους χάκερΣτην επίθεση αυτή κλάπηκαν έγγραφα και πληροφορίες σχετικά με την τοπολογία του δικτύου της ναυτιλιακής αρχής. Η επίθεση ξεκίνησε μέσω μηνύματος ηλεκτρονικού ταχυδρομείου(email), με χρήση ενός συνημμένου PDF που ήταν επιμολυσμένο από ιούς [49], [59].

Συμβάν Α9
Χρονολογία: 2013
Σημείο επίθεσης: S1

Σε ένα πλωτό γεωτρύπανο στον Κόλπο του Μεξικού το πλήρωμα συνέδεσε κατά λάθος μολυσμένους (από ιούς) υπολογιστές και εξωτερικές usb μνήμες ένα τοπικό δίκτυο της εξέδρας. Αυτό έδωσε τη δυνατότητα στον ιό να μολύνει το δίκτυο, και να διαταράξει την επικοινωνία μεταξύ του συστήματος δυναμικής θέσης της πλατφόρμας και των προωθητών(συστήματα υπεύθυνα για διατήρηση της σταθερής θέσης της πλατφόρμας). Ως αποτέλεσμα, η λειτουργία της γεώτρησης διακόπηκε μέχρι την αποκατάσταση της δυσλειτουργίας [53], [60], [61].

Συμβάν Α10
Χρονολογία: 2014
Σημείο επίθεσης: P1

Αφού κατάφεραν να υποκλέψουν email ναυτιλιακής εταιρείας οι κακόβουλοι/χάκερ άλλαξαν αριθμούς λογαριασμού τραπεζών για μεταφορές χρημάτων, προκαλώντας σοβαρές οικονομικές απώλειες για την εταιρεία. Οι επιθέσεις στοχεύουν στις συναλλαγές μεταξύ ναυτιλιακών εταιρειών και προμηθευτών καυσίμων, καθώς και ναυτιλιακές εταιρείες και ναυπηγεία [59].

Συμβάν Α11
Χρονολογία: 2012-2014
Σημείο επίθεσης: S4

Ένα φαινόμενο το οποίο χρησιμοποιείται κυρίως στις πολεμικές επιχειρήσεις αλλά και για απόκρυψη παράνομων δραστηριοτήτων (λαθρεμπόριο,λαθρομετανάστευση, τρομοκρατία, διακίνηση ναρκωτικών, κλπ) [62] αποτυπώθηκε σε μια αναφορά από την Windward [62]. Σύμφωνα με την έρευναμεταξύ 2012 και 2014, το 1% όλων των πλοίων παρείχαν πλαστές πληροφορίες αναγνώρισης (αριθμούς International Maritime Organization - IMO) στις εκπομπές AIS τους. Επιπλέον, περισσότερο από το 25% των σκαφών, απενεργοποιεί σκόπιμα το AIS τους (κάνοντας το μη ορατό στα υπόλοιπα πλοία/ναυτιλιακές αρχές), τουλάχιστον στο 10% των περιπτώσεων που ισχυρίζονται ότι πρόκειται για βλάβη του συστήματος τους.

Συμβάν Α12
Χρονολογία: 2016
Σημείο επίθεσης: S6

Η Νότια Κορέα κατηγόρησε την Βόρεια Κορέα για παρεμβολή (jamming)GPS με αποτέλεσμα 280 πλοία να επιστρέψουν στο λιμάνι αφού αντιμετώπισαν προβλήματα με τα συστήματα πλοήγησής τους. [51]. Για αυτό τον λόγο η Νότιο Κορέα ξεκίνησε ένα πρόγραμμα για την κατασκευή ενός εφεδρικού επίγειου ραδιοσυστήματος πλοήγησης πλοίων που θα ήταν δύσκολο να χακάριστεί (βελτιωμένη πλοήγηση μεγάλης απόστασης (eLoran)) προκειμένου να παρέχει αξιόπιστα εναλλακτικά σήματα θέσης και χρονισμού για την πλοήγηση.

Συμβάν Α13
Χρονολογία: 2014-2017
Σημείο επίθεσης: S4

Μια ανάλυση από τη Νορβηγική Ακτοφυλακή σχετικά με ιστορικά δεδομένα AIS από το 2014 έως το 2017, δείχνει ότι πολιτικά ρωσικά σκάφη πραγματοποιούν τακτικές στάσεις κατά μήκος της νορβηγικής ακτής. Αυτό δεν ήταν φυσιολογικό με βάση τα σχέδια πλεύσεως τους. Αυτές οι παρατυπίες τείνουν να συμπίπτουν, χρονικά και χωρικά, με τις επιχειρήσεις, την εκπαίδευση ή τις ασκήσεις του ΝΑΤΟ στην περιοχή. Υπάρχει υποψία ότι η συμπεριφορά αυτών των σκαφών

συνδέεται με ηλεκτρονική κατασκοπεία. Παρόμοια δραστηριότητα έχει παρατηρηθεί και στη Θάλασσα της Νότιας Κίνας καθώς και στη Μαύρη Θάλασσα [63], [64].

Συμβάν A14

Χρονολογία: 2017

Σημείο επίθεσης: P3

Ο βρετανικός όμιλος/ναυτιλιακός μεσίτης(broker) Clarksons "πέφτει" θύμα παραβίασης των πληροφοριακών συστημάτων του. Οι εισβολείς απαιτούν λύτρα για κλεμμένα δεδομένα από το δίκτυο ΗΥ του. Αποτέλεσμα της απώλειας των "ευαίσθητων πληροφοριών" που κλάπηκαν, ήταν η πληγή του κύρους της εταιρείας και η πτώση της αξίας της μετοχής της εταιρείας του κατά 5% αμέσως μετά το συμβάν [51], [53], [65], [66].

Συμβαν A15

Χρονολογία: 2017

Σημείο επίθεσης: P1

Μια από τις πιο γνωστές κυβερνοεπιθέσεις είναι η επίθεση με το ransomware NotPetya εναντίον του ναυτιλιακού γίγαντα Maersk Το ransomware διαδόθηκε μέσω μιας ενημέρωσης κώδικα για το λογισμικό φορολογικής λογιστικής MeDoc (το λογισμικό αυτό χρησιμοποιείται ευρέως στους φορολογικούς λογιστές στην Ουκρανία). Ο ιός εκμεταλλεύεται ευπάθειες στα Microsoft Windows και βασίζεται στο EternalBlue, ένα λογισμικό κυβερνο-επιθέσεων που αναπτύχθηκε από την αμερικανική NSA. Το περιστατικό θεωρείται ως η "πιο καταστροφική κυβερνο-επίθεση στην ιστορία", επηρρεάζοντας σχεδόν το ένα πέμπτο των παγκόσμιων ναυτιλιακών επιχειρήσεων, συμπεριλαμβανομένων και 76 λιμένων. Η Maersk έχει υπολογίσει τις οικονομικές της ζημίες σε σχεδόν 300 εκατομμύρια δολάρια USD από το συμβάν.Περισσότεροι από 4,000 διακομιστές, 45,000 υπολογιστές και 2,500 εφαρμογές χρειάστηκε να επαναεγκατασταθούν εξαρχής για την αποκατάσταση των λειτουργιών τους [53], [58], [67], [68], [69].

Συμβάν A16

Χρονολογία: 2017

Σημείο επίθεσης: S6

Άλλο ένα περιστατικό κυβερνοεπίθεσης, πιθανότατα στο σύστημα GNSS, συνέβη στη Μαύρη Θάλασσα κοντά στο Νοβοροσίσκ.Τουλάχιστον 20 πλοία ανέφεραν ότι τα συστήματα πλοήγησής τους, έδειχναν μια θέση που απείχε 32 χιλιόμετρα από τις πραγματικές τους συντεταγμένες. [51].

Συμβάν A17

Χρονολογία: 2018

Σημείο επίθεσης: S6

Ένα πλοίο εκτίθεται σε κυβερνο-επίθεση στο σύστημα GPS του, στη Μαύρη Θάλασσα (στην ίδια περιοχή με το προηγούμενο περιστατικό). Το πλοίο βρίσκεται στη θάλασσα, αλλά το σύστημα γεωγραφικού εντοπισμού του πλοίου δείχνει ότι το στίγμα του πλοίουβρίσκεται στη στεριά. Κατά τη διάρκεια των 3 ημερών αυτό συμβαίνει 4 φορές, με διάρκεια έως και 30 λεπτά [70].

Συμβάν A18

Χρονολογία: 2018

Σημείο επίθεσης: P3

Τον ίδιο χρόνο Κινέζοι χάκερ, που συνδέονται με την κινεζική κυβέρνηση, φέρεται να έκλεψαν εκατοντάδες gigabytes εξαιρετικά ευαίσθητων δεδομένων από υπεργολάβους του Πολεμικού Ναυτικού των ΗΠΑ συμπεριλαμβανομένων σχεδίων που σχετίζονται με έναν υπερηχητικό αντιπλοϊκό πύραυλο που πρόκειται να χρησιμοποιηθεί έως το 2020.Επιπλέον, εικάζεται ότι 27 αμερικανικά πανεπιστήμια έχουν δεχθεί παράλληλα με το συμβάν κυβερνο-επίθεση, σε μια προσπάθεια κλοπής ερευνητικών δεδομένων που σχετίζονται με τη ναυτιλιακή - ναυπηγική τεχνολογία [71], [72].

Συμβάν A19

Χρονολογία: 2018

Σημείο επίθεσης: H4

Το λιμάνι της Βαρκελώνης (Port of Barcelona) αναφέρει μια κυβερνο-επίθεση, η οποία αποδεικνύεται ότι είναι μόλυνση από το ransomware Ryuk. Η μόλυνση επηρέασε μόνο τα εσωτερικά συστήματα πληροφορικής του λιμένα και όχι την διαχείριση κυκλοφορίας των πλοίων [73], [74].

Συμβάν A20

Χρονολογία: 2018

Σημείο επίθεσης: H4

Από το ίδιο ransomware μολύνθηκε και το λιμάνι του Σαν Ντιέγκο (Port of San Diego) το οποίο ανέφερε σοβαρές διακοπές στα συστήματα πληροφορικής του. Ευτυχώς ο συνέπειες του περιορίζονται στις τοπικές λειτουργίες στο λιμάνι (OT). Το περιστατικό συνέβη μόλις 5 ημέρες μετά το προηγούμενο συμβάν στη Βαρκελώνη, αλλά δεν είναι σαφές εάν αυτά τα δύο γεγονότα σχετίζονται μεταξύ τους [73], [74].

Συμβάν A21

Χρονολογία: 2018

Σημείο επίθεσης: P2

Ιρανοί hackers κατηγορούνται για την κλοπή σχεδίων πλοίων και πληροφοριών σχετικά με το προσωπικό από την αυστραλιανή ναυπηγική εταιρεία Austal. Η Austal ναυπηγεί πλοία, τόσο για την Αυστραλία, όσο και για τις ΗΠΑ. Οι κλεμμένες πληροφορίες προσφέρθηκαν αργότερα προς πώληση στο dark web. Οι hackers προσπάθησαν επίσης να εκβιάσουν για τη λήψη χρημάτων από την Austal [75].

Συμβάν A22

Χρονολογία: 2017-2018

Σημείο επίθεσης: P1

Μια ομάδα Νιγηριανών hackers με το ψευδώνυμο "Gold Galleon", φέρεται να έκλεψε εκατοντάδες χιλιάδες δολάρια USD, μέσω παραβίασης και πλαστογράφησης επαγγελματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από ναυτιλιακές επιχειρήσεις. Οι hackers στόχευσαν κυρίως ιαπωνικές και νοτιο-κορεατικές εταιρείες. Επίσης όμως εταιρείες από άλλες χώρες έχουν δεχθεί ανάλογη επίθεση [75], [76].

Συμβάν A23

Χρονολογία: 2018

Σημείο επίθεσης: P1

Ένα άλλο επίσης ευρέως γνωστό συβάν αφορά την COSCO Shipping Lines.Η εταιρεία επλήγη από κυβερνο-επίθεση η οποία πιθανολογείται ότι οφείλεται σε μόλυνση από ransomware και προκάλεσε

σοβαρές διακοπές στα δίκτυα των γραφείων της, στις ΗΠΑ. Η επικοινωνία μέσω email και διαδικτύου δεν ήταν διαθέσιμη για 5 ημέρες. [77], [78].

Συμβάν A24

Χρονολογία: 2018

Σημείο επίθεσης: P3

Μια κυβερνοεπίθεση εναντίον περίπου 400 διακομιστών της στη Μέση Ανατολή ανίχνευσε η ιταλική εταιρεία πετρελαιοειδών Saipem. Ειδικότερα, οι διακομιστές στη Σαουδική Αραβία και στα Ηνωμένα Αραβικά Εμιράτα επλήγησαν ιδιαίτερα σοβαρά. Η εταιρεία είχε αντίγραφα ασφαλείας των επηρεαζόμενων δεδομένων, αποφεύγοντας έτσι τη μόνιμη απώλεια τους. Η κυβερνο-επίθεση δεν πιστεύεται ότι είχε υποκλέψει δεδομένα [79].

Συμβάν A25

Χρονολογία: 2019

Σημείο επίθεσης: S1

Ένα μεγάλο πλοίο καθ'οδόν προς τη Νέα Υόρκη, "μολύνεται" από κακόβουλο λογισμικό στο δίκτυο του συστήματος ελέγχου του. Αυτό έχει ως αποτέλεσμα την περιορισμένη λειτουργικότητα του [80].

Συμβάν A26

Χρονολογία: 2018 - 2019

Σημείο επίθεσης: S6

Παρεμβολή (jamming) των GPS συστημάτων παρατηρείται πολλές φορές κατά το διάστημα 2018 - 2019 στη βόρεια Νορβηγία. Η εμπλοκή εμποδίζει τη θαλάσσια κυκλοφορία σε κάποιο βαθμό, αλλά ευτυχώς αποφεύχθηκαν σοβαρές συνέπειες από ατυχήματα [48].

Συμβάν A27

Χρονολογία: 2019

Σημείο επίθεσης: H3

Από την Αμερικανική ακτοφυλακή ανακοινώθηκε (χωρίς να κατονομαστεί) ότι έναςναυτιλιακός οργανισμός/οντότητα, έχει "μολυνθεί" από το λογισμικό Ryuk τύπου ransomware. Η μόλυνση προήλθε μέσω ενός συνημμένου ηλεκτρονικού "ψαρέματος" (phishing),προκάλεσε διακοπή λειτουργίας όλου του δικτύου και έκανε τις κάμερες CCTV, τα συστήματα ελέγχου πρόσβασης και την παρακολούθηση κρίσιμων διαδικασιών να μην είναι διαθέσιμα. Η ναυτιλιακή οντότητα διέκοψε ολοκληρωτικά την λειτουργία της για πάνω από 30 ώρες[73].

Συμβάν A28

Χρονολογία: 2019

Σημείο επίθεσης: P3

Ο βρετανικός πάροχος θαλάσσιων υπηρεσιών James Fisher and Sons, "μολύνθηκε" από ransomware και αναγκάζεται να κλείσει τα ψηφιακά του συστήματα με άμεσο οικονομικό αντίκτυπο την άμεση πτώση της μετοχής του κατά 7% μετά τη γνωστοποίηση του συμβάντος [81].

Συμβάν A29

Χρονολογία: 2019

Σημείο επίθεσης: S1

Μια εγκατάσταση συμπίεσης φυσικού αερίου σε έναν διαχειριστή αγωγών των ΗΠΑ(που δεν κατονομάστηκε), έχει μολυνθεί με ransomware (πιθανώς Ryuk). Για το λόγο αυτό πρέπει να διακόψει τη λειτουργία της εγκατάστασης για δύο ημέρες. Η επίθεση ήρθε μέσω ηλεκτρονικού "ψαρέματος" και επηρέασε τόσο τα συστήματα IT όσο και τα συστήματα OT [82], [83].

Συμβάν A30

Χρονολογία: 2019

Σημείο επίθεσης: S2

Ο κεντρικός διακομιστής(server) ενός δεξαμενόπλοιου κοντά στο λιμάνι Naantali στη Φινλανδία, μολύνθηκε με ransomware. Ο δίσκος αντιγράφων ασφαλείας επίσης διαγράφηκε από τον ιό. Πιθανότερες αιτίες της επίθεσης είναι το πρωτόκολλο απομακρυσμένης πρόσβασης (Remote Desktop Protocol - RDP), κάποια συσκευή USB ή κάποιο συνημμένο email. Το ίδιο σκάφος μολύνεται ξανά 4 μήνες αργότερα, κοντά στο ίδιο λιμάνι [80].

Συμβάν A31

Χρονολογία: 2019

Σημείο επίθεσης: S2

Δύο πλοία ίδιας ιδιοκτησίας, μολύνθηκαν από το ransomware Hermes 2.1. Η μόλυνση προήλθε από ενεργοποίηση (από τους χρήστες) μακρο-εντολών σε έγγραφο του Word το οποίο ήταν επισυναπτόμενο σε ένα email. Από την μόλυνση επηρεάστηκαν πολλοί σταθμοί εργασίας στα δίκτυα διαχείρισης της εταιρείας [80].

Συμβάν A32

Χρονολογία: 2020

Σημείο επίθεσης: S2

Ο διακομιστής καθώς και πολλοί τερματικοί ΗΥ ενός σκάφους αγκυροβολημένο κοντά στο Tynemouth UK, μολύνθηκαν με το Ryuk ransomware με αποτέλεσμα όλα τα δεδομένα να κρυπτογραφηθούν και να είναι και μη ανακτήσιμα. Χρειάστηκε πλήρης επαναεγκατάσταση για την επαναφορά των συστημάτων [80].

Συμβάν A33

Χρονολογία: 2020

Σημείο επίθεσης: S2

Τρία πλοία αμερικανικής σημαίας, έχουν "μόλυνση" στα διοικητικά τους συστήματα από το ransomware Sodinokibi. Αυτός ο ιός απειλεί επίσης με διαρροή πληροφοριών ("ransomtheft"), εκτός από την κρυπτογράφηση δεδομένων που προκαλεί στα συστήματα που έχει μολύνει [80].

Συμβάν A34

Χρονολογία: 2020

Σημείο επίθεσης: P1

Η ναυτιλιακή εταιρεία MSC, πέφτει θύμα ενός ιού ransomware και η έδρα της στη Γενεύη κλείνει για πέντε ημέρες [69], [84].

Συμβάν A35

Χρονολογία: 2020

Σημείο επίθεσης: H3

Το Ισραήλ κατηγορείται για την παραβίαση του ιρανικού λιμανιού Shahid Rajaee, προκαλώντας διακοπή όλων των μεταφορών και της ροής εμπορευμάτων για μεγάλο χρονικό διάστημα. [84], [85].

Συμβάν A36
Χρονολογία: 2020
Σημείο επίθεσης: P2

Η νορβηγική ναυπηγική εταιρεία Vard, πλήττεται από επίθεση ransomware που προκαλεί σοβαρή λειτουργική διακοπή. Πολλοί από τους εργαζόμενους ενημερώνονται ότι οι διακοπή λειτουργίας της εταιρείας μπορεί να οδηγήσει σε προσωρινή απώλεια θέσεων εργασίας (λόγω της διακοπής της ναυπηγικής δραστηριότητας της εταιρείας) [86], [87].

Συμβάν A37
Χρονολογία: 2019 - 2020
Σημείο επίθεσης: P1

Η εταιρεία Cruise Carnival Corporation & plc, προσβλήθηκε από ιό ransomware δύο φορές σε δύο χρόνια και πιθανότατα εκλάπησαν προσωπικά δεδομένα και στοιχεία πιστωτικών καρτών πελατών και υπαλλήλων της εταιρείας. Δεν έγιναν γνωστές στο κοινό περαιτέρω λεπτομέρειες σχετικά με τον τύπο του ιού και τον φορέα επίθεσης. [88].

Συμβάν A38
Χρονολογία: 2020
Σημείο επίθεσης: M1

Η Αρχή Μεταφορών της Μάλτας(Transport Malta), υφίσταται κυβερνο-επίθεση με αποτέλεσμα την διακοπή λειτουργίας των συστήματων της για πέντε ημέρες [89], [90].

Συμβάν A39
Χρονολογία: 2020
Σημείο επίθεσης: P1

Η ελληνική ναυτιλιακή εταιρεία Diana Shipping, πέφτει θύμα του ransomware Egregor. Λίγες πληροφορίες είναι γνωστές για αυτό το περιστατικό [91], [92].

Συμβάν A40
Χρονολογία: 2020
Σημείο επίθεσης: P1

Η γαλλική εταιρεία μεταφοράς εμπορευματοκιβωτίων CMA CGM, χτυπήθηκε από το ransomware Ragnar Locker. Πολλά από τα κινεζικά γραφεία της επηρεάστηκαν και ορισμένες από τις διαδικτυακές της υπηρεσίες χρειάστηκε να κλείσουν, συμπεριλαμβανομένης της ηλεκτρονικής κράτησης [93], [94].

Συμβάν A41
Χρονολογία: 2020
Σημείο επίθεσης: M1

Θύμα στοχευμένης και υψηλού επιπέδου κυβερνοεπίθεσης έπεσε όμως και ο Διεθνής Ναυτιλιακός Οργανισμός των Ηνωμένων Εθνών IMO,με αποτέλεσμα να απενεργοποιήσει τον ιστότοπο και το εσωτερικό δίκτυό του (intranet Για την αποφυγή περαιτέρω ζημιών, απενεργοποιοήθηκαν και πολλά άλλα βασικά συστήματα χωρίς ωστόσο να έχουν δοθεί περισσότερες λεπτομέρειες για την επίθεση [95], [96].

Συμβάν A42

Χρονολογία: 2020

Σημείο επίθεσης: P1

Η βρετανική ναυτιλιακή εταιρεία Red Funnel, πλήττεται από κυβερνο-επίθεση, προκαλώντας σοβαρή αναστάτωση στα συστήματα πληροφορικής της. Κυριότερη απώλεια αποτελεί η διακοπή λειτουργίας του συστήματος κρατήσεων για αρκετές ημέρες, αναγκάζοντας τους πελάτες να φτάσουν πολύ πριν από τα δρομολόγια τους για να αγοράσουν εισιτήρια επί τόπου [97], [98].

Συμβάν A43

Χρονολογία: 2020

Σημείο επίθεσης: P1

Η εταιρεία μεταφορών και ναυτιλίας των ΗΠΑ Matson, αναφέρει ότι δέχτηκε παραβίαση των δικτύων της η οποία επηρρέασε κάποιους διακομιστές της και υφίσταται πιθανότητα διαρροής προσωπικών δεδομένων.. Η κυβερνο-επίθεση δεν σταμάτησε τις διαδικασίες μεταφοράς φορτίου, αλλά ορισμένες συναλλαγές καθυστερούν, καθώς οι επηρεαζόμενες λειτουργίες πρέπει να εκτελεσθούν χειροκίνητα (με μη αυτόματες διαδικασίες) [99].

Συμβάν A44

Χρονολογία: 2020

Σημείο επίθεσης: H4

Το Port of Kennewick, έχει απωλέσει τα συστήματα πληροφορικής του από ransomware. Οι hackers ζήτησαν λύτρα 200,000 δολλάρια USD, τα οποία δεν καταβλήθηκαν. Τα συστήματα δεν ήταν διαθέσιμα για αρκετές ημέρες, καθώς έπρεπε να αποκατασταθούν από τα εφεδρικά αντίγραφα ασφαλείας [100], [101].

Συμβάν A45

Χρονολογία: 2020

Σημείο επίθεσης: P1

Ένα επίσης θύμα κυβερνοεπίθεσης με ransomware ήταν και η νορβηγική εταιρεία κρουαζιέρας Hurtigruten. Τα πιο σημαντικά συστήματα της δεν είναι διαθέσιμα για αρκετές ημέρες και παράλληλα υφίσταται κλοπή και διαρροή προσωπικών δεδομένων επιβατών [102], [103], [104].

Συμβάν A46

Χρονολογία: 2020

Σημείο επίθεσης: P1

Η γερμανική εταιρεία κρουαζιέρας AIDA, με έδρα στο Ρόστοκ, χτυπήθηκε από το ransomware DoppelPaymer. Η επίθεση προκάλεσε διακοπή λειτουργίας τηλεφωνικών γραμμών και ίντερνετ τόσο στα γραφεία της εταιρείας στην ξηρά όσο και στα πλοία της εταιρείας, καθώς και διακοπή επικοινωνίας μεταξύ τους, αναγκάζοντας την AIDA να ακυρώσει αρκετές προγραμματισμένες κρουαζιέρες [105].

1.4 Κατηγοριοποίηση των Κυβερνο-επιθέσεων

Μια απειλή (threat) είναι η πιθανή αιτία ενός ανεπιθύμητου περιστατικού, το οποίο μπορεί να οδηγήσει σε σημαντική βλάβη ή/και δυσλειτουργία ενός πληροφοριακού συστήματος. Αυτό με τη σειρά του μπορεί να οδηγήσει σε δυσλειτουργία ή διακοπή της λειτουργίας όποιου φορέα κάνει χρήση των παρεχόμενων υπηρεσιών [106]. Ειδικότερα με βάση τα γνωστά περιστατικά και τις σχετικές εργασίες, προκύπτει μια λίστα (Top-10) των 10 κορυφαίων θαλάσσιων απειλών στον κυβερνοχώρο. Οι κατηγορίες ορίζονται από παρόμοια χαρακτηριστικά μεταξύ των περιστατικών, και ταξινομούνται με βάση τη συχνότητα και τη σοβαρότητα των περιστατικών και των επιδράσεων τους στα συστήματα πληροφοριών. Για κάθε κατηγορία έχουν περιγραφεί οι τυπικοί φορείς της κυβερνο-επίθεσης και οι στόχοι της. Ορισμένα περιστατικά έχουν συσχετιστεί με περισσότερες από μία κατηγορίες, κάτι που είναι φυσικό για επιθέσεις που αποτελούνται από πολλά στάδια και επίπεδα και μπορούν να επηρεάσουν περισσότερους από έναν στόχους. Ως εκ τούτου, οι κατηγορίες δεν αλληλοαποκλείονται και μπορούν να επικαλύπτονται για ένα μεμονωμένο περιστατικό.

1.4.1 Έκθεση των IT συστημάτων των ναυτιλιακών εταιρειών - οργανισμών (KE_1)

Τα συστήματα πληροφορικής IT των ναυτιλιακών εταιρειών και μεταφορέων είχαν μια έκρηξη σχετικών περιστατικών στον κυβερνοχώρο τα τελευταία χρόνια. Μπορούν να συνδεθούν με το 25% των συνολικών περιστατικών την τελευταία δεκαετία. Θα πρέπει να σημειωθεί ότι, ο πιο συνηθισμένος φορέας κυβερνο-επίθεσης είναι το ransomware, συνήθως με τη μορφή συνημμένων σε email ή συνδέσμων (hyperlinks). Όπως και σε πολλούς άλλους τομείς, υπάρχει μια αυξανόμενη τάση των ιών τύπου ransomtheft. Αυτοί συνδυάζουν διακοπές λειτουργίας, κρυπτογράφηση και κλοπή πληροφοριών. Υπάρχουν επίσης πολλά παραδείγματα οικονομικής απάτης (fraud) από κυβερνο-επιθέσεις κοινωνικής μηχανικής. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A2, A5, A10, A15, A22, A23, A34, A37, A39, A40, A42, A43, A45, A46.

1.4.2 Εκτιθέμενα IT συστήματα πληροφορικής που ανήκουν σε υπεργολάβους, ναυπηγεία, εγκαταστάσεις στην ξηρά, παρόχους υπηρεσιών, ρυθμιστικές αρχές και ερευνητικές εγκαταστάσεις (KE_2)

Τα περιστατικά αυτά συνήθως περιλαμβάνουν κλοπή κρίσιμων πληροφοριών για την επιχείρηση, καθώς και πιο κοινές περιπτώσεις εκβιασμού. Από τα περιστατικά αυτής της κατηγορίας, παρατηρούμε ότι η κοινωνική χειραγώγηση, το hacking και το ransomware είναι συνήθως τα εργαλεία (μέσα) της κυβερνο-επίθεσης. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A8, A14, A18, A21, A24, A28, A29, A36, A38, A41.

1.4.3 Έκθεση των IT συστημάτων λιμένων (KE_3)

Τα λιμάνια είναι δημοφιλείς στόχοι και έχουν τη φήμη ότι δεν προστατεύονται επαρκώς από κυβερνο-επιθέσεις στον κυβερνοχώρο. Οι διακοπές λειτουργίας που αυτές προκαλούν είναι ακριβές και προβλέψιμες. Το γεγονός αυτά καθιστά τα λιμάνια ως ελκυστικούς στόχους για τους εκβιαστές. Επιπλέον, η κλοπή πληροφοριών και ο χειρισμός των δεδομένων των λιμένων έχουν χρησιμοποιηθεί για λαθρεμπόριο. Ορισμένα περιστατικά αναφέρουν μόνο ότι το λιμάνι έχει τύχει αντικείμενο κυβερνο-επίθεσης (hacked), χωρίς να προσδιορίζουν ακριβώς τον επιτιθέμενο. Ειδικότερα σε περιοχές όπου διεξάγονται πολεμικές συγκρούσεις ή επιχειρήσεις είναι λογικό αυτές οι επιθέσεις να υλοποιούνται από κυβερνητικά υποστηριζόμενες ομάδες. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A3, A7, A15, A19, A20, A27, A35, A44.

1.4.4 Κατασκοπεία των Ναυτιλιακών Λειτουργιών (KE_4)

Σε αυτή την κατηγορία βρίσκουμε περιστατικά που χαρακτηρίζονται από εκτεταμένες και στοχευμένες κυβερνο-επιθέσεις που σχετίζονται με κατασκοπεία, υποκλοπές και επιτήρηση θαλάσσιων επιχειρήσεων. Οι αναφερόμενοι φορείς επίθεσης τείνουν να είναι το spear-phishing ή το γενικό hacking, καθώς και το tapping (παρακολούθηση και συνακρόαση) των επικοινωνιών. Οι επιτιθέμενοι μπορεί να είναι ομάδες από ανταγωνιστικές εταιρείες ή ακόμη και κράτη, με στόχο την παρεμπόδιση των λειτουργιών μίας εταιρείας ή ακόμη και την αποκόμιση τεχνογνωσίας. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A4, A7, A8, A13, A18, A21.

1.4.5 Έκθεση των IT συστημάτων πλοίου - ξηράς (KE_5)

Υπήρξαν πολλά περιστατικά όπου τα συστήματα πληροφορικής επί των πλοίων "μολύνθηκαν" από ransomware. Είναι κοινή υποψία ότι αυτά ήταν περισσότερο τυχαία παρά στοχευμένα περιστατικά. Τυπικοί φορείς επίθεσης ήταν συνημμένα σε email και σύνδεσμοι. Οι διακομιστές πλοίων και οι ΗΥ (πελάτες - clients) τους, καθίσταντο μη λειτουργικοί μέσω αυτών των κυβερνο-επιθέσεων. Από τις επιθέσεις αυτές συνήθως απομένουν περιορισμένα στοιχεία, καθώς όλα τα δεδομένα συνήθως σβήνονται. Στους γενικότερους στόχους αυτών των κυβερνο-επιθέσεων συγκαταλέγονται η παρακολούθηση διελεύσεων πλοίων, εμπορευμάτων, προγράμματα πλεύσης - διέλευσης, [2] κ.λπ. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A30, A31, A32, A33.

1.4.6 Χειρισμός των σημάτων του GNSS (KE_6)

Μια πολλή κρίσιμης σημασίας κατηγορία για την ασφαλή ναυσιπλοία που σχετίζεται κυρίως με παρεμβολές (jamming) ή πλαστογράφηση (spoofing) σημάτων των συστημάτων GPS/GNSS που χρησιμοποιούν τα πλοία για σκοπούς πλοήγησης, προσέγγισης και εντοπισμού θέσης. Οι φορείς (μυστικές υπηρεσίες) που χρηματοδοτούνται από τα κράτη, τείνουν να κρίνονται ως "οι πρώτοι ύποπτοι" για αυτά τα γεγονότα. Αυτό το είδος απειλής εκδηλώνεται συνήθως σε περιοχές γεωπολιτικών συγκρούσεων ή/και πολεμικών επιχειρήσεων/ασκήσεων και σε περιοχές αμφισβήτισης κυριαρχικών δικαιωμάτων. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A12, A16, A17, A26.

1.4.7 Έκθεση των OT συστημάτων πλοίου - ξηράς (KE_7)

Η σωστή κοινή πρακτική επιβάλει τον διαχωρισμό IT και OT συστημάτων. Ως εκ τούτου, τα OT συστήματα έχουν εκτεθεί λιγότερο σε κυβερνο-επιθέσεις. Ωστόσο, υπάρχουν παραδείγματα τέτοιων περιστατικών και οι συνέπειες τους είναι κρίσιμες. Οι επιτιθέμενοι συνήθως έχουν εισέλθει στο σύστημα μέσω μολυσμένων μονάδων USB ή ΗΥ που συνδέονται ακούσια σε λάθος δίκτυο. Παραδείγματα τέτοιων συστημάτων είναι το Electronic Chart Display and Information System - ECDIS (κατά τις ενημερώσεις χάρτη) και τα συστήματα ελέγχου πρόωσης. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A1, A9, A25, A29.

1.4.8 Έκθεση των συστημάτων επικοινωνιών (KE_8)

Υπήρξαν μερικά παραδείγματα κυβερνο-επιθέσεων εναντίον συστημάτων επικοινωνιών για χερσαίες επιχειρήσεις/λειτουργίες και υπεράκτιες εγκαταστάσεις. Οι επικοινωνίες των πλοίων δεν επηρεάζονται τόσο πολύ, ωστόσο, με πολλά διαφορετικά και απαραίτητα συστήματα επικοινωνίας επί του σκάφους, τα πλοία εξακολουθούν να είναι πιθανά θύματα τέτοιων επιθέσεων. Τα περιστατικά δείχνουν ότι οι συνέπειες τείνουν να είναι η απώλεια διαθεσιμότητας επικοινωνίας που προκαλείται από hacking ή ransomware. Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A5, A6, A13, A23.

1.4.9 Οικονομικές απάτες (KE_9)

Αυτά τα περιστατικά τείνουν να προκαλούνται από στοχευμένες και εξειδικευμένες κυβερνο-επιθέσεις, όπου πλαστά email ή παραβιασμένοι (Hacked) λογαριασμοί χρηστών χρησιμοποιούνται ως φορείς επίθεσης για την έναρξη ή τη χειραγώγηση οικονομικών συναλλαγών. Για παράδειγμα, τα στοιχεία λογαριασμού αλλάζουν ή αποστέλλονται πλαστά τιμολόγια για χρέωση προς τις ναυτιλιακές εταιρείες. Ο απώτερος σκοπός αυτών των κυβερνο-επιθέσεων είναι η αποκόμιση χρηματικών ποσών (απάτη). Στην κατηγορία αυτή περιλαμβάνονται τα συμβάντα: A10, A22.

1.4.10 Παρεμβολή στα συστήματα AIS και GPS (KE_{10})

Υπάρχουν πολλά γνωστά συμβάντα όπου τα συστήματα AIS επί των πλοίων είχαν παραποιηθεί ή απενεργοποιηθεί παράνομα. Αυτά συνήθως σχετίζονται με παράνομες διελεύσεις, λαθρεμπόριο,

παράνομη αλιεία ή στρατιωτικές συγκρούσεις. Πιθανές συνέπειες θα μπορούσαν, στη χειρότερη περίπτωση, να καταλήξουν σε συγκρούσεις σκαφών, αλλά το πιθανότερο είναι ότι άλλα πλοία θα αναγκαστούν να αλλάξουν την πορεία πλεύσης τους χωρίς λόγο, εφόσον τα συστήματα εντοπισμού τους δέχονται λάθος στίγμα και πορεία από τα άλλα διερχόμενα σκάφη. Στην κατηγορία αυτή περιλαμβάνεται το συμβάν Α11.

1.5 Συμπεράσματα

Στον πίνακα που ακολουθεί συγκεντρώνονται όλοι οι τύποι των κυβερνο-επιθέσεων με βάση την κωδικοποίηση και κατηγοριοποίηση των συμβάντων από τις προηγούμενες ενότητες:

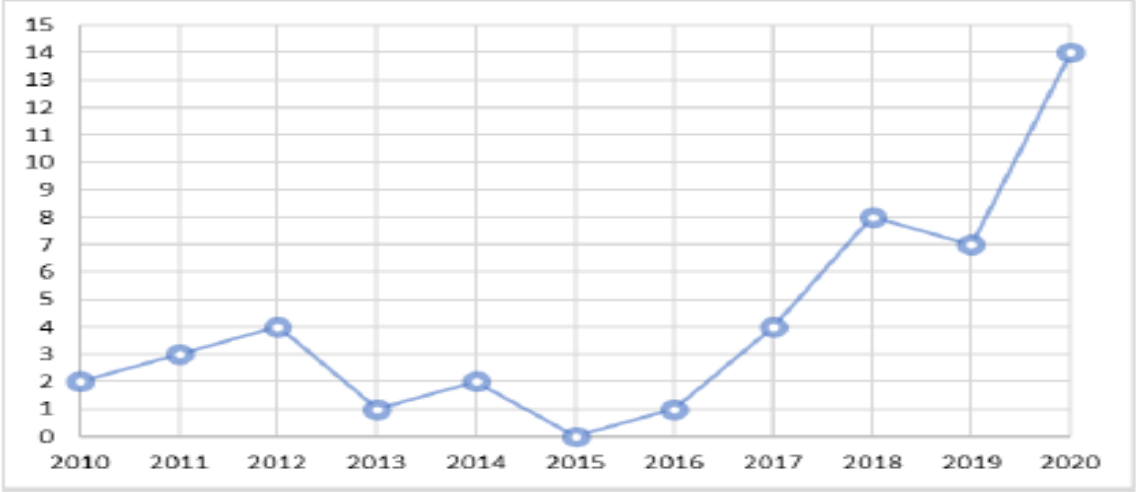
Πίνακας 1: Τύποι Κυβερνο-επιθέσεων και αντιστοίχηση συμβάντων σε κατηγορίες

Τύπος Κυβερνο-επίθεσης	Συμβάντα	Συνολικός Αριθμός
KE_1	A2, A5, A10, A15, A22, A23, A34, A37, A39, A40, A42, A43, A45, A46	14
KE_2	A8, A14, A18, A21, A24, A28, A29, A36, A38, A41	10
KE_3	A3, A7, A15, A19, A20, A27, A35, A44	8
KE_4	A4, A7, A8, A13, A18, A21	6
KE_5	A30, A31, A32, A33	4
KE_6	A12, A16, A17, A26	4
KE_7	A1, A9, A25, A29	4
KE_8	A5, A6, A13, A23	4
KE_9	A10, A22	2
KE_{10}	A11	1

Όπως αναφέρθηκε και κατά την διαδικασία κατηγοριοποίησης, οι κυβερνο-επιθέσεις αφορούν σε διαφορετικά σημεία διεπαφών από την αλληλεπίδραση των IT/OT πληροφοριακών συστημάτων καθώς και των συστημάτων επικοινωνίας και πλοήγησης των σκαφών. Ορισμένες από τις κυβερνο-επιθέσεις μπορεί να ανήκουν σε πλέον της μίας κατηγορίας, δεδομένης της αλληλεπίδρασης και των πολλαπλών επιπέδων δράσης της εφαρμογής της επίθεσης. Στη συνέχεια οι κυβερνο-επιθέσεις αναλύονται με χρήση των διαφορετικών χαρακτηριστικών που αυτές εμφανίζουν.

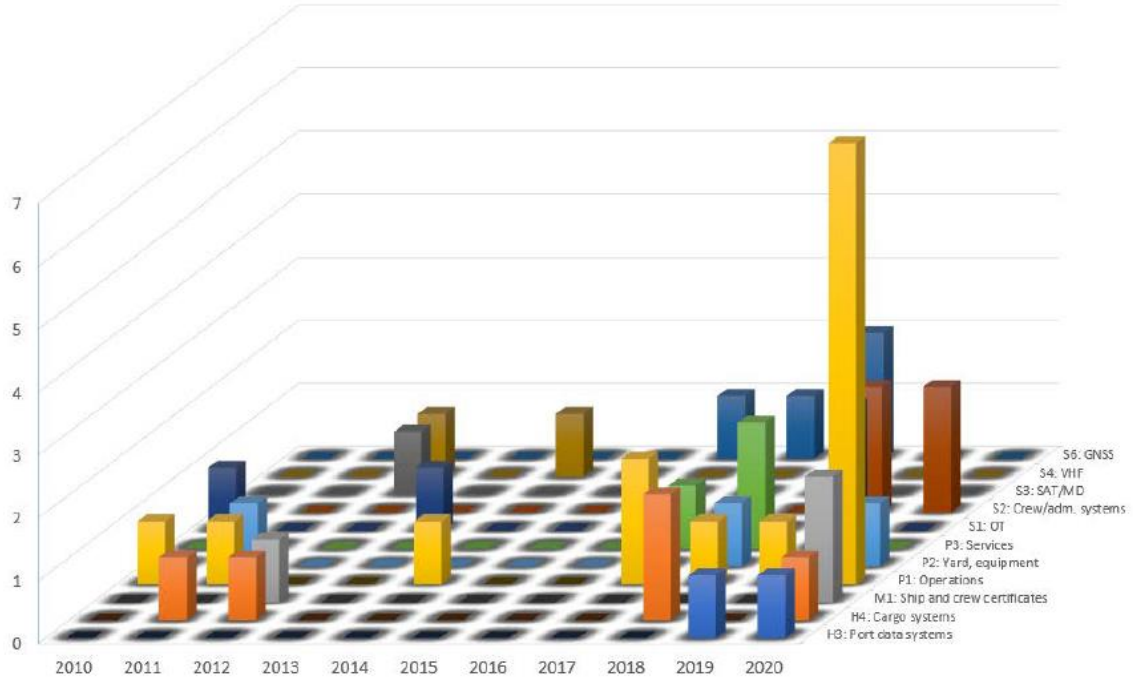
Λαμβάνοντας υπόψη τα περιστατικά ανά έτος, όπως παρουσιάζεται στο σχήμα που ακολουθεί, μπορούμε να δούμε ότι ο αριθμός των συμβάντων έχει επταπλασιαστεί από το 2010 έως το 2020. Η αύξηση αυτή προφανώς δεν είναι γραμμική, καθώς υπήρξε αισθητή πτώση κατά τα έτη

2013 - 2016. Αυτή η περίοδος μπορεί να έδωσε μια "ψευδαίσθηση ασφάλειας" του ναυτιλιακού χώρου από κυβερνο-επιθέσεις, καθώς ορισμένα από τα περιστατικά το 2017 (ειδικά τα A14 και A15) φάνηκαν να αιφνιδιάζουν τους επηρεαζόμενους οργανισμούς - φορείς και είχαν πολύ σοβαρές συνέπειες. Η αύξηση των συμβάντων αναμένεται να γίνει εντονότερη με την περαιτέρω διείσδυση των τεχνολογιών παγκόσμιου διαδικτύου σε όλες τις εφαρμογές στην ναυτιλία, στο άμεσο μέλον.



Σχήμα 3: Συμβάντα κυβερνο-επιθέσεων ανά έτος [6]

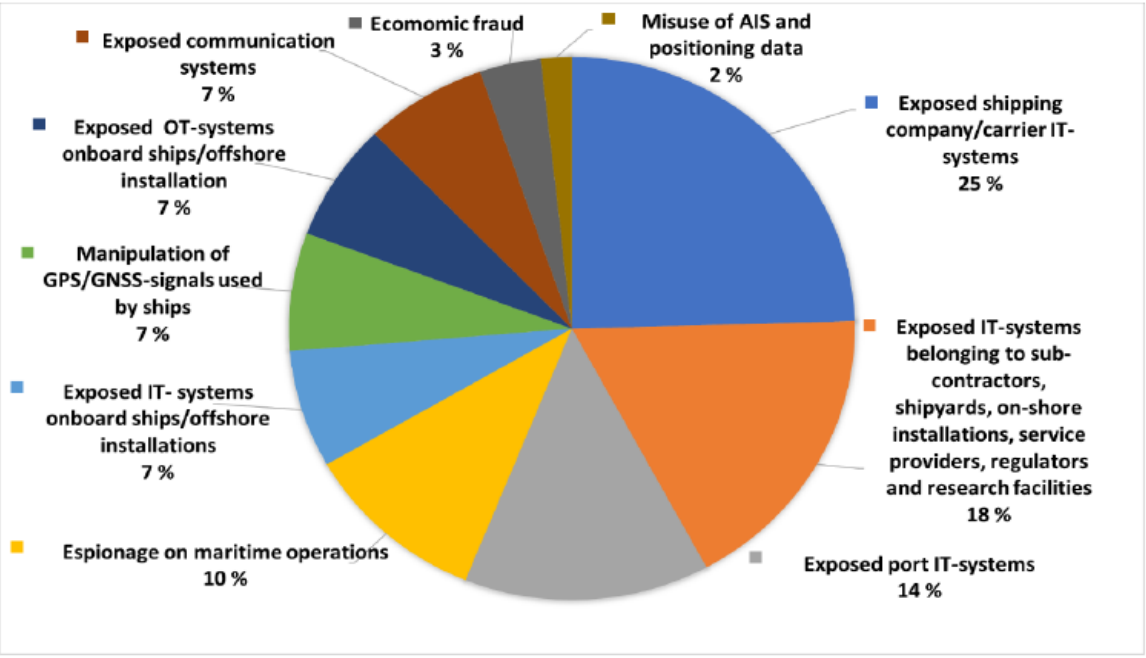
Εξετάζοντας πιο προσεκτικά τα σημεία επίθεσης που έχουν χρησιμοποιηθεί για το εν λόγω χρονικό διάστημα, μπορούμε να παρατηρήσουμε ότι αυτά είναι αρκετά διεσπαρμένα στον άξονα του χρόνου και στα σημεία επίθεσης, όπως παρουσιάζεται και στο τρισδιάστατο διάγραμμα που ακολουθεί. Υπάρχει μια προφανής κορυφή για το σημείο επίθεσης P1 το 2020, που προκαλείται από πολλά συστήματα πληροφορικής για ιδιωτικές επιχειρήσεις στην ξηρά. Εκτός από αυτό, δεν υπάρχουν ιδιαίτερες συγκεντρώσεις σε συγκεκριμένα σημεία διεπαφών και τύπους κυβερνο-επίθεσης. Μπορούμε να παρατηρήσουμε ότι με έναν αυξανόμενο αριθμό περιστατικών, υπάρχει επίσης μια ευρύτερη εκμετάλλευση της "επιφάνειας επίθεσης". Αυτό σημαίνει ότι δεν υπάρχει πιθανώς καμία ενιαία αιτία για τα περιστατικά που μπορεί να εξαλειφθεί,υπάρχει μεγάλη διασπορά αιτιών, και υπάρχει ανάγκη να εφαρμοστεί μια ποικιλία "εκτιμητών κινδύνου" από αυτές τις επιθέσεις, για όλα τα σημεία επίθεσης.



Σχήμα 4: Συμβάντα κυβερνο-επιθέσεων ανά έτος ανά σημείο επίθεσης [6]

Εκτός από τους περιορισμούς που αναφέρθηκαν ήδη στην προηγούμενη ενότητα, θα πρέπει να αναγνωριστεί ότι υπάρχουν αρκετές αδυναμίες στα δεδομένα των κυβερνοπεριστατικών. Πρώτα απ'όλα, υπάρχει μια μεροληψία αναφοράς από τον ίδιο τον "παθόντα", καθώς υπήρξαν ελάχιστα κίνητρα για την αποκάλυψη (δημοσιοποίηση) των περιστατικών στο ευρύ κοινό, από κυβερνο-επιθέσεις στο πεδίο της ναυτιλίας. Οι λόγοι για αυτές τις "αποκρύψεις" μπορούν να συμπεριλάβουν, την οικονομική ζημία μίας εταιρείας, την επισφάλεια μίας εταιρείας/οργανισμού από την κοινοποίηση, την δημιουργία "κακής φήμης" η οποία μπορεί να πλήξει τις μελλοντικές περαιτέρω οικονομικές δραστηριότητες, την αξίωση αποζημιώσεων από πιθανούς πελάτες της εταιρείας, κ.λπ. Ειδικότερα όταν οι κυβερνο-επιθέσεις διεξάγονται υπό την "επιμέλεια" κρατικών φορέων/μυστικών υπηρεσιών με στόχο κράτη ή οργανισμούς, είναι λογικό ότι προφανώς τα πλήγματα που αυτές παράγουν δεν είναι κοινοποιήσιμα, και πολύ περισσότερο μπορεί να μην είναι εύκολα εντοπίσιμα και ανιχνεύσιμα. Για τους παραπάνω λόγους είναι λογικό να θεωρηθεί ότι οι κυβερνο-επιθέσεις που έχουν διεξαχθεί κατά το χρονικό διάστημα που εξετάζεται (2010 - 2020), είναι σαφώς πολύ περισσότερες από αυτές που παρουσιάστηκαν. Ωστόσο, πολλά από τα περιστατικά που καταγράφηκαν ήταν αφενός πολύ μεγάλα για να αποκρυβούν, και αφετέρου δεν υπάρχουν πολλά άλλα του ίδιου μεγέθους που δεν έχουν αναφερθεί. Δεύτερον, υπάρχει πλέον μεγαλύτερη προσοχή στα περιστατικά στον κυβερνοχώρο από ό,τι στο παρελθόν, γεγονός που αυξάνει την πιθανότητα ένα περιστατικό να λάβει ειδησεογραφική κάλυψη και αναφορά. Αυτό μπορεί να οδηγήσει σε μεγαλύτερο αριθμό αναφερόμενων περιστατικών στα επόμενα χρόνια. Από την άλλη πλευρά, ο εύκολος χαρακτηρισμός μίας επίθεσης ως "κυβερνο-επίθεση", μπορεί να εξαλείψει άλλα χαρακτηριστικά μίας προσβολής που ενδεχόμενα στοχεύει σε συγκάλυψη μυστικών υπηρεσιών ή άλλων ομάδων.

Το σχήμα που ακολουθεί δείχνει πώς ταξινομούνται τα περιστατικά σύμφωνα με τις κορυφαίες 10 κυβερνο-απειλές. Τα τρία μεγαλύτερα τμήματα σχετίζονται όλα με εκτιθέμενες χερσαίες υποδομές πληροφορικών συστημάτων, από τις οποίες εξαρτάται η ναυτιλιακή βιομηχανία. Αυτό είναι λογικό αφού η λειτουργία της ναυτιλίας στηρίζεται σε πολύ μεγάλο βαθμό σε αυτά τα συστήματα και σε μεγάλο βαθμό υποφέρουν από τις "συνηθισμένες" ευπάθειες που μοιράζονται μεταξύ όλων των τομέων ανάλογα με την ψηφιακή τεχνολογία Commercial-of-the-Shelf - COTS που χρησιμοποιούν. Αυτό αποτύπωσε και ο ENISA [42] όταν περιέγραψε μια σειρά από "προκλήσεις ασφάλειας" στον κυβερνοχώρο που σχετίζονται ειδικά με τους λιμένες, όπως η έλλειψη ψηφιακής κουλτούρας, έλλειψη ευαισθητοποίησης, έλλειψη κατάρτισης, προϋπολογισμού και ειδικευμένων ατόμων (προσωπικού) που ενισχύονται για τον ναυτιλιακό τομέα. Η άποψη αυτή επιβεβαιώθηκε και σε νεότερη έρευνα[107] δείχνοντας ότι έμπειροι επαγγελματίες της ναυτιλίας πιστεύουν ότι υπάρχει "έλλειψη γενικών γνώσεων στον τομέα της θαλάσσιας ασφάλειας στον κυβερνοχώρο".



Σχήμα 5: Συμβάντα κυβερνο-επιθέσεων με βάση τους 10 επικρατέστερους Τύπους απειλών σε μορφή διαγράμματος πίτας [6]

Η εισαγωγή κακόβουλου λογισμικού, ιδίως ransomware και ransomtheft, ήταν η διαδεδομένη μέθοδος επίθεσης, όπως σε κάθε άλλο τομέα. Υπάρχουν επίσης πολλά παραδείγματα οικονομικής απάτης, χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής,παραπλανητικών email (phishing), πλαστά τιμολόγια και κλοπή λογαριασμών χρηστών. Αυτές οι επιθέσεις προέρχονται από φορείς του κοινού εγκλήματος στον κυβερνοχώρο με "καθαρά" οικονομικά κίνητρα. Ο εντοπισμός της αλυσίδας πίσω από αυτές τις επιθέσεις, μπορεί να είναι η καλύτερη μέθοδος για προστασία, από την ίδια την προσπάθεια προστασίας κάθε σημείου διεπαφής (Interface) που μπορεί να δεχθεί επίθεση ανά πάσα στιγμή. Αυτό απαιτεί διεθνή συνεργασία μεταξύ των υπηρεσιών επιβολής του νόμου (εθνικό επίπεδο,EUROPOL,INTERPOL), των ομάδων απόκρισης σε συμβάντα (CERT),εθνικών και μή καθώς και συντονισμός με διεθνείς οργανισμούς (ENISA,NIST,κλπ.), , υπηρεσιών πληροφοριών και της ίδιας της βιομηχανίας.

Απειλές που σχετίζονται με κατασκοπεία σε θαλάσσιες επιχειρήσεις, επιθέσεις σε υπεργολάβους, ναυπηγεία και ερευνητικές εγκαταστάσεις, καθώς και επιθέσεις σε συστήματα GNSS, μπορεί να συνδέονται με άλλους παράγοντες, ιδιαίτερα με κρατικούς φορείς ή ομάδες προγραμματιστών που σκόπιμα προσλαμβάνονται από κυβερνητικούς φορείς για την εκδήλωση κυβερνο-επιθέσεων. Αυτοί χρηματοδοτούνται αρκετά καλά, υποκινούνται από πολιτικούς παράγοντες ή αποκτούν ξένη τεχνολογία μέσω των κλοπών σε θέματα τεχνολογίας, και μπορεί να είναι εξαιρετικά δύσκολο, για αυτόν τον φορέα/οργανισμό που δέχεται την επίθεση, έτσι ώστε να αμυνθεί και να τους εντοπίσει. Σε αυτήν την περίπτωση οι επιτιθέμενοι διατηρούν προβάδισμα τόσο σε τεχνολογικές γνώσεις (κατάρτιση) καθώς και σε χρήματα (budget) εφόσον χρηματοδοτούνται ως ειδικοί για το σκοπό αυτό από κρατικούς φορείς ή μυστικές υπηρεσίες. Είναι απαραίτητη η ενεργός συμμετοχή των εθνικών αρχών ασφαλείας - γραφείων πληροφοριών - μυστικών υπηρεσιών, για την υποστήριξη της ναυτιλιακής βιομηχανίας που αντιμετωπίζει απειλές αυτού του επιπέδου.

2 Κυβερνο-Επιθέσεις, Απειλές στις υποδομές και τα συστήματα της Ναυτιλίας. Δράσεις Αντιμετώπισης τους

Οι σημερινές διεθνείς απειλές έχουν τη δυνατότητα να προκαλέσουν σημαντικές ζημιές και ανασφάλειες, οι οποίες ξεπερνούν τα εθνικά - διακρατικά όρια. Έτσι, η ασφάλεια του θαλάσσιου τομέα, απαιτεί ολοκληρωμένες και συνεκτικές προσπάθειες μεταξύ των κρατών και πολλών συνεργαζόμενων χωρών, για την προστασία του κοινού συμφέροντος στην παγκόσμια θαλάσσια ασφάλεια [3]. Η απαίτηση για την ανάπτυξη μίας τέτοιας στρατηγικής, θα πρέπει να περιγράφει πώς οι κυβερνήσεις των κρατών θα προωθήσουν μια διεθνή προσπάθεια θαλάσσιας ασφάλειας μέσω κανονισμών. Στόχος της προσπάθειας είναι να ενισχύσει αποτελεσματικά και αποδοτικά την ασφάλεια του θαλάσσιου τομέα, διατηρώντας παράλληλα την ελευθερία του τομέα ανάπτυξης, δραστηριοτήτων και εμπορίας της ναυτιλίας.

Σύμφωνα με αυτές τις κατευθυντήριες αρχές, τις βαθιές αξίες που κατοχυρώνονται στο ναυτιλιακό εμπόριο και το εφαρμοστέο εσωτερικό και διεθνές δίκαιο [5], οι ακόλουθοι στόχοι θα πρέπει να καθοδηγήσουν τις δραστηριότητες στον τομέα της θαλάσσιας ασφάλειας:

- Αποτροπή τρομοκρατικών επιθέσεων και εγκληματικών ή εχθρικών πράξεων μέσω της ναυτιλίας
- Προστασία Πληθυσμιακών Ομάδων και Υποδομών Ζωτικής σημασίας που σχετίζονται με τη Ναυτιλία
- Ελαχιστοποιήση της ζημιάς που προκαλούν οι κυβερνο-επιθέσεις και επιτάχυνση στις διαδικασίες αποκατάστασης των παραγομένων ζημιών
- Γενικότερη προστασία των ναυτιλιακών επιχειρήσεων και του οικοσυστήματος

Στα πλαίσια αυτά, οι δράσεις για την αντιμετώπιση των κυβερνο-επιθέσεων και των απειλών που έχουν εισαχθεί τα τελευταία χρόνια στο ναυτιλιακό χώρο, θα πρέπει να αντιμετωπίσουν με καθορισμένες διαδικασίες, την δυναμική του προβλήματος. Προφανώς για να καθοριστούν οι απαιτούμενες δράσεις που επικεντρώνονται στο ναυτιλιακό χώρο, θα πρέπει να διασαφηνιστούν τα εργαλεία των κυβερνο-επιθέσεων καθώς και τα συστήματα της ναυτιλίας που πλήττονται από αυτές. Στη συνέχεια παρουσιάζονται αναλυτικά οι τεχνικές κυβερνο-επιθέσεων και τα εργαλεία που αυτές χρησιμοποιούν, ασχέτως των πληττόμενων IT/OT συστημάτων. Δεδομένου ότι οι επιθέσεις εκδηλώνονται σε υπολογιστικά συστήματα που χρησιμοποιούνται για τις σκοπούς και τις λειτουργίες της ναυτιλίας, τα εργαλεία αυτά δεν απέχουν από τα συνήθη εργαλεία λογισμικού που αναπτύσσουν επιθέσεις γενικότερα σε υπολογιστικά συστήματα.

2.1 Εργαλεία εκδήλωσης επιθέσεων στα συστήματα ναυτιλίας

Για την επίτευξη των παραπάνω αντικειμενικών στόχων (objectives), είναι σημαντική η αναγνώριση των απειλών από τις κυβερνο-επιθέσεις και η χρήση των μέσων που αυτές χρησιμοποιούν για την εκδήλωση τους. Στις επόμενες ενότητες παρουσιάζονται οι τεχνολογικές βάσεις και τεχνικές (υλικού, λογισμικού ή χρήσης των υπαρχόντων συστημάτων με παράνομο τρόπο) που οι κυβερνο-επιθέσεις χρησιμοποιούν ως "εργαλεία ανάπτυξης" για την πραγμάτωση τους.

2.1.1 Οι τεχνικές Hacking ως εργαλείο κυβερνο-επίθεσης

Ως Hacking ορίζεται οποιαδήποτε διαδικασία παρέμβασης, που καθιστά ένα σύστημα (υλικό πλατφόρμας - λογισμικό), να λειτουργεί εκτός των προκαθορισμένων προδιαγραφών του (λειτουργίας - νομιμότητας). Στόχος του hacking, είναι η απόκτηση πρόσβασης σε συστήματα πληροφοριών με χρήση παράνομων τεχνικών, από μη εξουσιοδοτημένους - διαβαθμισμένους χρήστες των συστημάτων, με στόχο την αποκόμιση ίδιου ωφέλους (οικονομικού και μη), εκτός των συμφερόντων και λειτουργιών για τις οποίες εξ'ορισμού χρησιμοποιείται η συγκεκριμένη οργάνωση πληροφορίας. Οι διαδικασίες hacking βασίζονται είτε σε ανάπτυξη υλικού πλατφόρμας - λογισμικού (hw/sw) απο εξειδικευμένους γνώστες/μηχανικούς τεχνολογίας υπολογιστικών συστημάτων, είτε

στην χρήση έτοιμων συστημάτων/ρουτινών (sw) που προορίζονται για παράνομες τεχνικές διεργασίες. Η ανάπτυξη των τελευταίων μπορεί να έχει βασιστεί σε ήδη άλλες έτοιμες τεχνολογικές αναπτύξεις λογισμικού, που προορίζονται για επέκταση ή συμπληρωματικές λειτουργίες στα υφιστάμενα συστήματα. Ορισμένες φορές αυτά τα εργαλεία μπορεί να έχουν αναπτυχθεί για ερευνητικούς σκοπούς για την ανάδειξη ατελειών και εσφαλμένης λειτουργίας των υπολογιστικών συστημάτων. Επομένως η χρήση αυτής της τεχνολογίας είναι αυτή που χαρακτηρίζει την ίδια την έννοια του hacking [2].

Ειδικότερα, με τη χρήση των τεχνικών hacking για κυβερνο-επιθέσεις στον ναυτιλιακό χώρο, μπορεί να αποκτηθεί σημαντική πληροφορία από τα IT/OT συστήματα των εταιρειών - οργανισμών, η οποία να χρησιμοποιηθεί για αποκόμιση ωφέλους από τα επιτιθέμενα άτομα/ομάδες. Επιπλέον, οι διαδικασίες hacking μπορεί να καταστρέψουν τα υπολογιστικά συστήματα θέτοντας τα εκτός λειτουργίας, με παράλληλη καταστροφή και των βάσεων δεδομένων των υφιστάμενων πληροφοριών, οδηγώντας σε δυσλειτουργία ή ακόμη και οικονομική καταστροφή την εταιρεία - οργανισμό - φορέα που υφίσταται την κυβερνο-επίθεση. Οι επιτιθέμενοι [1] μπορούν να δώσουν ψευδείς πληροφορίες, να προβούν σε δημιουργία ψευδών δηλώσεων, σε πληροφόρηση τιμών, σε ημερομηνίες και τοποθεσίες παράδοσης κ.λπ. Οι πληροφορίες μεταξύ πελατών και προμηθευτών μπορούν να αλλοιωθούν, ή/και να κοινοποιηθούν, διαρρέοντας την παραπάνω πληροφορία στον παγκόσμιο ιστό του Διαδικτύου. Επιπλέον, οι παρακολουθήσεις των πλοίων μπορούν να χαθούν για μεγάλα χρονικά διαστήματα, κατά, αλλά και μετά την εκδήλωση των κυβερνο-επιθέσεων. Εκτός από τις τεράστιες οικονομικές απώλειες για τις εταιρείες (απώλεια φορτίων, κόστος αποκατάστασης), μπορεί να ανακύψουν και ζημιές από νομικές αξιώσεις των πελατών των εταιρειών και την πληγείσα φήμη τους.

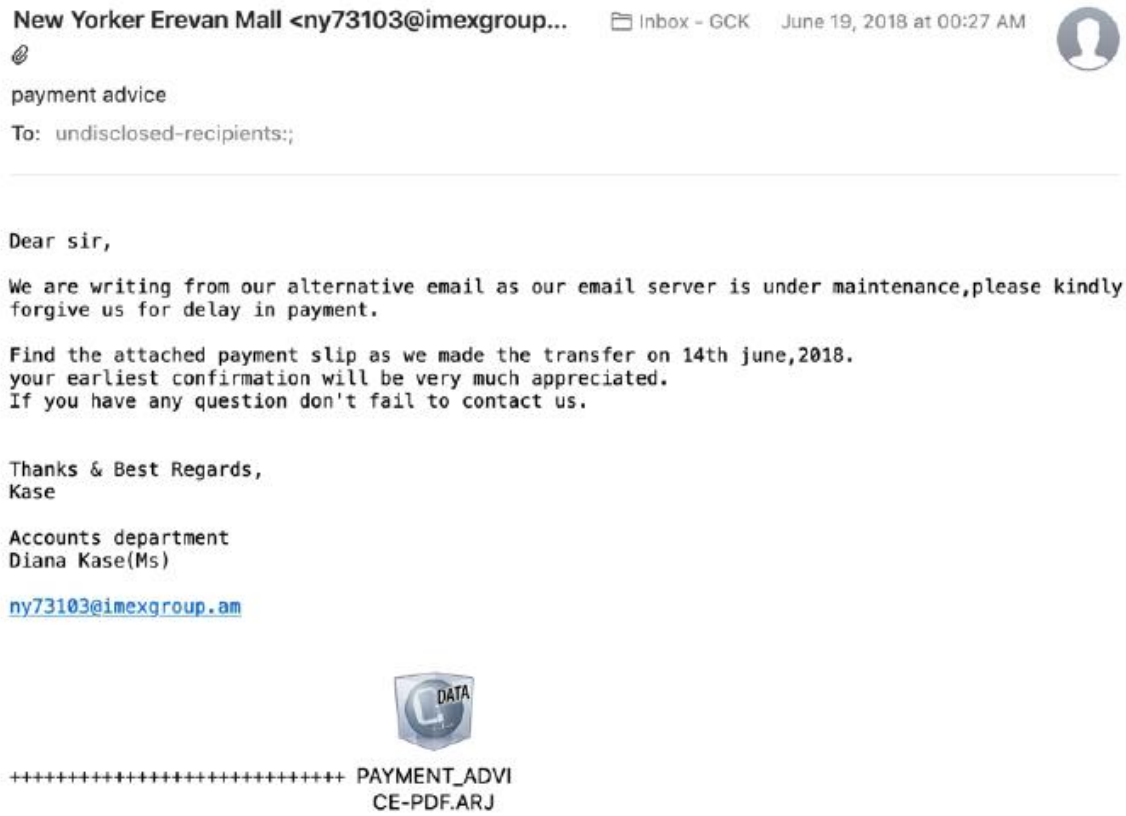
Η ναυτιλιακή βιομηχανία έχει υποστεί πολλές παραβιάσεις δεδομένων στις οποίες οι επιτιθέμενοι κατευθύνονται σε στοχευμένες εταιρικές πληροφορίες ή πληροφορίες εργαζομένων. Σε αυτήν την περίπτωση, οι διαδικασίες hacking απευθύνονται με χρήση "μολυσμένου λογισμικού" στους διακομιστές των υπολογιστικών δικτύων. Πολλές φορές μέσα στην ομάδα των επιτιθέμενων, δυστυχώς, μπορεί να συμπεριλαμβάνονται και εργαζόμενοι της ίδιας της ναυτιλιακής εταιρείας, οι οποίοι εργάζονται σε τομείς με "ευαίσθητα προσωπικά δεδομένα" (π.χ. λογιστήριο), οι οποίοι εν γνώσει ή εν αγνοία τους εγκαθιστούν το μολυσμένο λογισμικό. Το επιμολυσμένο λογισμικό συνήθως αφορά σε εμπορικά προϊόντα, πάνω στα οποία οι ιοί εκμεταλλεύονται γνωστά "κενά ασφαλείας" τους (π.χ. κενά ασφαλείας στα Windows, στο Office 365, κ.α.).

Οι ναυτιλιακές εφαρμογές τύπου smartphone/tablets, υπόκεινται επίσης σε κυβερνο-επιθέσεις. Σε αυτήν την περίπτωση, οι διαδικασίες hacking και επιμόλυνσης των διακομιστών των ναυτιλιακών φορέων, γίνονται μέσω αυτών των κινητών συσκευών, όταν δεν τηρούνται αυστηρές διαδικασίες ταυτοποίησης και διαχείρισης των χρηστών τους. Το hacking σε αυτές τις περιπτώσεις, μπορεί να ανακτήσει κωδικούς πρόσβασης των συστημάτων, κάνοντας ανοιχτή και προσβάσιμη ολόκληρη τη βάση δεδομένων του φορέα που δέχεται την επίθεση. Οι βάσεις δεδομένων των εταιρείων μπορεί να περιέχουν ευαίσθητα στοιχεία πελατών συμπεριλαμβανομένων ονομάτων, διευθύνσεων ηλεκτρονικού ταχυδρομείου, φυσικών διευθύνσεων, αποθηκών, προϊόντων και αναγνωριστικών χρήστη και πληροφορίες σκαφών (π.χ. γεωγραφικό πλάτος, γεωγραφικό μήκος, πορεία, ταχύτητα πλεύσης, κ.λπ.).

2.1.2 Η Αλίευση Δεδομένων (Phishing) ως εργαλείο κυβερνο-επίθεσης

Ως αλίευση δεδομένων (Phishing) [2], ορίζεται η διαδικασία με την οποία ο κακόβουλος αποκτά πρόσβαση σε ευαίσθητα πληροφοριακά δεδομένα, χωρίς απαραίτητα την χρήση επιμολυσμένου λογισμικού, αλλά με τεχνικές κοινωνικής ή άλλης δικτύωσης. Αυτός που δέχεται την "επίθεση" δεν αντιλαμβάνεται ότι πρόκειται για εκδήλωση επίθεσης, και με δική του βούληση ή αμέλεια, κοινοποιεί δεδομένα του, θεωρώντας ότι πρόκειται για άλλον πιστοποιημένο χρήστη, της μεταξύ τους επικοινωνίας. Οι τεχνικές αλίευσης μπορεί να εκκινήσουν από απλή ανταλλαγή emails και μηνυμάτων που ψευδώς θεωρούνται ότι αποστέλλονται από κάποιον πιστοποιημένο (επίσημο) φορέα μίας υπηρεσίας προς έναν χρήστη αυτής. Ο χρήστης που συνήθως δέχεται τέτοιο μήνυμα, δεν αντιλαμβάνεται ότι πρόκειται περί απάτης, διότι οι επιτιθέμενοι συνήθως "μιμούνται" τα χαρακτηριστικά και τα ειδικά αναγνωριστικά της επικοινωνίας του επίσημου φορέα. Έτσι εξαπατούν τον χρήστη, ο οποίος θεωρώντας ότι πρόκειται για επικοινωνία με τον νόμιμο φορέα προχωρεί σε περαιτέρω αποκαλύψεις δεδομένων του, τα οποία στη συνέχεια μπορούν να χρησιμοποιηθούν από τον επιτιθέμενο, έτσι ώστε να αποκομίσει πρόσβαση σε νόμιμες υπηρεσίες του κατόχου (π.χ. τραπεζικοί λογαριασμοί, IBAN και κωδικοί πρόσβασης τραπεζών για συναλλαγές WEB/e/Mobile-banking).

Πολλές ναυτιλιακές εταιρείες είναι ευάλωτες σε απάτες phishing και άλλες απάτες αναλογης μορφής, λόγω του μεγάλου όγκου επικοινωνίας, παραγγελιών και οικονομικών συναλλαγών που πραγματοποιούνται από αυτές στο διαδίκτυο. Ορισμένες από αυτές τις απάτες συμβαίνουν μέσω της χρήσης ψεύτικης ταυτότητας μέσω e-mail, μερικές μέσω phishing από πλευράς εργαζομένων και άλλες με χειραγώγηση των πρότυπων ηλεκτρονικών εγγράφων (standard electronic formats) τιμολόγησης, όπως η διεθνής αποστολή και το Μήνυμα μεταφοράς - Κόστους φορτίου και άλλες χρεώσεις (IFTFCC). Σε αυτές τις περιπτώσεις οι επιτιθέμενοι έχουν ως άμεσο στόχο την εκρροή σημαντικού χρηματικού ποσού από τις ναυτιλιακές εταιρείες για την πληρωμή ψεύτικων τιμολογίων παροχής υπηρεσιών/αγαθών προς αυτές. Τα ψεύτικα τιμολόγια μπορούν να αφορούν σε υπηρεσίες συνήθεις για τις ναυτιλιακές εταιρείες όπως, η φορτο-εκφόρτωση εμπορευμάτων, έξοδα ελλιμενισμού πλοίων, διελεύσεις από πορθμεία, αγορά καυσίμων, κ.λπ. Τα ποσά που μπορούν να εκταμιευτούν σε αυτήν την περίπτωση μπορεί να είναι αρκετά μεγάλα, στην περίπτωση όπου οι επιτιθέμενοι γνωρίζουν από τις εταιρείες ενδεχόμενες ναυπηγήσεις ή συντηρήσεις πλοίων, οπότε αξιώνουν σημαντικά μέρη του ποσού των υφιστάμενων συμβολαίων για να προχωρήσουν υποθετικά "με την συνέχιση των εργασιών". Ενδεικτικά παρατίθεται ένα τέτοιο email από ανάλογη περίπτωση εξαπάτησης, στο σχήμα που ακολουθεί. Στην προκειμένη περίπτωση οι επιτιθέμενοι διακαιολογούνται για τη μη χρήση του επίσημου email από τον γνωστό server της εταιρείας τους, λόγω συντήρησης και αποστέλλουν συνημμένο τιμολόγοιο αμοιβών μέσω άλλου λογαριασμού email (Invoice) [1].



Σχήμα 6: Ψευδές email για την αξίωση πληρωμής υπηρεσιών σε ναυτιλιακή εταιρεία [1]

Τα ποσά από αυτές τις συναλλαγές καταλήγουν σε τραπεζικούς λογαριασμούς σε χώρες που δεν υπόκεινται σε άμεσο τραπεζικό έλεγχο ή διατηρούν τραπεζικούς λογαριασμούς με ειδικά καθεστώτα. Πολλές φορές τα μεταβιβαζόμενα ποσά καταλήγουν σε κρυπτονομίσματα, τα οποία διασφαλίζουν την ανωνυμία και το ακαταδίωκτο των παραληπτών τους.

Οι τεχνικές phishing λειτουργούν επίσης πολλές φορές με χρήση στοχευμένων emails (targeted), τα οποία απυθύνονται σε υψηλά στελέχη των ναυτιλιακών εταιρειών, δεδομένου ότι αυτοί έχουν πρόσβαση σε μεγαλύτερα χρηματικά ποσά χωρίς να απαιτείται διαδικασία ελέγχου και εγκρίσεων των πληρωμών από τα συστήματα της ναυτιλιακής εταιρείας.

2.1.3 Το ransomware ως εργαλείο κυβερνο-επίθεσης

Τα ransomware αποτελούν εφαρμογές ειδικού λογισμικού, οι οποίες εγκαθίστανται στα υπολογιστικά συστήματα ως "περιτυλίγματα κώδικα" (malicious code). Ο κώδικας αυτός φαινομενικά προσφέρει άλλη λειτουργικότητα από αυτήν την οποία πραγματικά εκτελεί. Μετά την εγκατάσταση τους αποκτούν σταδιακή πρόσβαση στα πληροφοριακά συστήματα, και στη συνέχεια μπορούν να προβούν σε μία πληθώρα ενεργειών, εν αγνοία των χειριστών των πληροφοριακών συστημάτων, όπως, κοινοποίηση και διαρροή εγγράφων, ευαίσθητων δεδομένων, λήψη κωδικών πρόσβασης, παρακολούθηση των διενεργούμενων διαδικασίων του συστήματος, ή/και κρυπτογράφηση των δεδομένων των πληροφοριακών βάσεων των συστημάτων [1], [2]. Στην τελευταία περίπτωση, συνήθως οι επιτιθέμενοι αποκαλύπτονται στην εταιρεία-θύμα όταν αυτή ανιχνεύσει την διείσδυση του ransomware, αξιώνοντας υπερβολικά χρηματικά ποσά για την αποκρυπτογράφηση και αποκατάσταση των δεδομένων των πληροφοριακών συστημάτων της εταιρείας. Προφανώς, η λειτουργία του ναυτιλιακού φορέα μετά τις διαδικασίες κρυπτογράφησης που τα δεδομένα τους έχουν υποστεί από το ransomware, δεν μπορεί να συνεχιστεί. Αυτό αποτελεί και το κύριο διαπραγματευτικό θέμα με τους επιτιθέμενους. Στις περισσότερες των περιπτώσεων η πληρωμή των λύτρων [3] δεν αποτελεί λύση ή εγγύηση αποκατάστασης, δεδομένου ότι η εταιρεία που έχει δεχθεί την επίθεση προφανώς και δεν εμπιστεύεται τους hackers για την αποκατάσταση των πληροφοριακών συστημάτων της. Επομένως, η μόνη ενδεικνυόμενη λύση στην περίπτωση αυτή είναι η αποκατάσταση των πληροφοριακών συστημάτων και των βάσεων δεδομένων που αυτά κάνουν χρήση, από αντίγραφα ασφαλείας (εφόσον και αν υπάρχουν). Τα αντίγραφα ασφαλείας πρέπει να είναι όσο το δυνατόν πιο πρόσφατα για να περιορίσουν τον κίνδυνο απώλειας πληροφορίας - οικονομικής ζημίας για την εταιρεία. Επίσης θα πρέπει να σημειωθεί, ότι η διαδικασία αποκατάστασης των λειτουργιών της ναυτιλιακής εταιρείας μπορεί να είναι χρονοβόρα, δεδομένου ότι όλα τα τερματικά που έχουν επιμολυνθεί από το ransomware, θα πρέπει να εντοπισθούν και να αποκατασταθούν με απομάκρυνση/απομόνωση των επιμολυσμένων χαρακτηριστικών τους. Αυτό μπορεί να απαιτεί επαναεγκατάσταση ακόμη και των λειτουργικών συστημάτων των τερματικών και επανεγκατάσταση των εφαρμογών που απαιτούνται για τη λειτουργία. Όσο μεγαλύτερη η κλίμακα μίας ναυτιλιακής εταιρείας, τόσο μεγαλύτερος και ο απαιτούμενος χρόνος αποκατάστασης των ζημιών που επιφέρει η επίδραση των ransomwares. Επιπλέον, η διαδικασία αποκατάστασης συνεπάγεται επιπλέον κόστη για την εταιρεία, αφενώς για το εξειδικευμένο προσωπικό που θα προβεί στην αποκατάσταση, και αφετέρου από κόστη που προκύπτουν από τα διαφυγόντα κέρδη καθώς η εταιρεία δεν μπορεί να λειτουργήσει. Οι απώλειες σε μεγάλης κλίμακας εταιρείες αποτιμώνται σε πολλά εκατομμύρια δολλάρια από την εκδήλωση τέτοιας μορφής επιθέσεων.

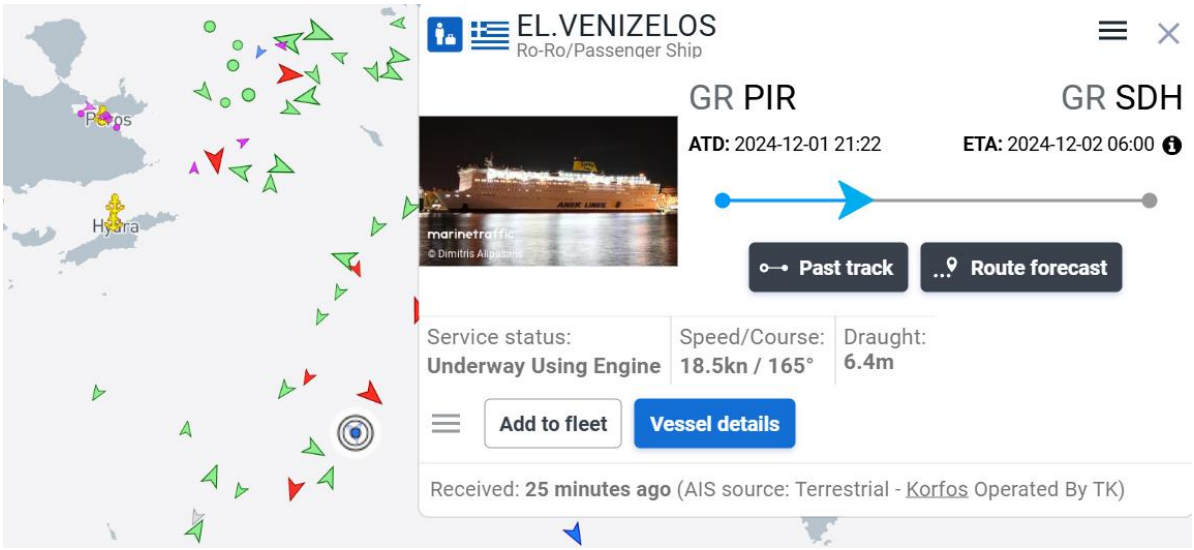
Τα ransomwares αποτελούν μία από τις χειρότερες μορφές επιθέσεων, δεδομένου ότι οι επιτιθέμενοι είναι απόλυτα καταρτισμένοι και γνώστες του επιχειρησιακού τοπίου και των τεχνικών προγραμματισμού. Εκμεταλλεύονται παθογένειες ή "τρύπες ασφαλείας" κυρίως λειτουργικών συστημάτων και εφαρμογών, μέσω της ύπαρξης των οποίων η επιτυχία μίας τέτοιας επίθεσης θεωρείται σχεδόν βέβαιη. Η μόνη τεχνική άμυνας των ναυτιλιακών εταιρειών είναι η χρήση ενημερωμένου λογισμικού και η αμεσότητα επικοινωνίας των μεγάλων ναυτιλιακών εταιρειών - οργανισμών με τις κατασκευάστριες εταιρείες των εφαρμογών, για την έγκαιρη λήψη νεώτερων εκδόσεων του λογισμικού (updates), που επιλύουν τα διαπιστωμένα κενά ασφαλείας τους. Επιπλέον η ευαισθητοποίηση των χρηστών-υπαλλήλων των ναυτιλιακών εταιρειών/φορέων είναι πολύ κρίσιμη καθώς η επίθεση είναι δυνατή ακόμη και με μια απλή επιλογή (κλικ) ενός υπερσυνδέμου (link) ή λήψη ενός συνημμένου αρχείο από ένα απλό email.

Η χρήση πλατφορμών πληροφοριακών συστημάτων ανοικτού κώδικα (open sourse) μπορεί να μην παρέχει τα απαιτούμενα επίπεδα ασφαλείας για τη λειτουργία των ναυτιλιακών εταιρειών, δεδομένου ότι ο κώδικας των συγκεκριμένων λειτουργικών συστημάτων/εφαρμογών είναι ανοικτός και προσβάσιμος στην διεθνή προγραμματιστική κοινότητα. Από την άλλη πλευρά, αυτό αποτελεί και μία επιτυχία των κοινοτήτων "ανοικτού κώδικα" εφόσον πρόκειται για λογισμικό το οποίο έχει εξετασθεί και έχει εμπλουτιστεί, από μεγάλο πλήθος προγραμματιστών της κοινότητας. Οι ναυτιλιακές εταιρείες όμως σε αυτήν την περίπτωση δεν μπορούν να λάβουν τα ωφέλη των "κοινοτήτων ανοικτού κώδικα", εφόσον οι άδειες κυκλοφορίας των λειτουργικών και των προγραμμάτων αυτού του τύπου δεν επιτρέπουν ενδεχόμενη εμπορική χρήση τους. Ακόμη όμως και στην περίπτωση που αυτός ο περιορισμός αρθεί, και πάλι οι ναυτιλιακές εταιρείες δύσκολα μπορούν να πεισθούν να κάνουν χρήση αυτών, δεδομένου ότι δεν υπάρχει μία άμεσα συμβαλλόμενη εταιρεία απέναντι τους για την υποστήριξη και εξέλιξη αυτών των πηγών κώδικα στην πορεία του χρόνου.

2.1.4 Η Διαρροή Πληροφοριών ως εργαλείο κυβερνο-επίθεσης

Η διαρροή πληροφοριών δεν είναι μια κυβερνο-επίθεση, αυτή καθεαυτή, αλλά αναφέρεται σε τρόπους με τους οποίους η βιομηχανία μέσω της τεχνολογίας εκρρέει "ακούσια" πληροφορίες που μπορεί να χρησιμοποιήσει μία κακόβουλη ομάδα για την εκδήλωση μιας επίθεσης σε ναυτιλιακό φορέα. Ο "ανοικτός κώδικας", μπορεί να περιλαμβάνει διαρροή πληροφοριών, όταν αναφέρεται στη χρήση βάσεων δεδομένων δημόσιων πληροφοριών για μια εταιρεία, πρόσωπο ή οργανισμό. Αυτός συνιστά και τον κύριο λόγο όπου η χρήση εφαρμογών "ανοιχτού κώδικα" δεν αποτελούν επιλογές εφαρμογών για τις εταιρείες. Η διαρροή πληροφοριών μπορεί να συντελεστεί επίσης και από τους ίδιους τους εργαζόμενους σε μία ναυτιλιακή ή άλλη εταιρεία, οι οποίοι είτε από αμέλεια κοινοποιούν είτε δεν λαμβάνουν τα απαιτούμενα μέτρα ασφαλείας για την προστασία των πληροφοριών από τρίτους (π.χ. μεταφορά εγγράφων και αρχείων μέσω φορητών συσκευών USB, αποθήκευση στο cloud, κ.λπ.) [2].

Ένα τέτοιο παράδειγμα δημόσιων βάσεων δεδομένων και εφαρμογών "ανοιχτού κώδικα", είναι οι πάρα πολλοί ιστότοποι που τα τελευταία χρόνια κατακλύζουν το Διαδίκτυο, που παρακολουθούν την τοποθεσία εμπορικών, κρουαζιερόπολοιων, και άλλων πλοίων σε όλο τον κόσμο, σε πραγματικό χρόνο. Αυτές οι πληροφορίες συλλέγονται από τα ίδια τα πλοία, τα οποία μεταδίδουν τις πληροφορίες θέσης του συστήματος αυτόματης αναγνώρισης (AIS), με βάση τους διεθνείς κανονισμούς ασφαλείας. Υπάρχει μια σειρά από ιστοτόπους παρακολούθησης σκαφών στο Διαδίκτυο, συμπεριλαμβανομένων των CruiseMapper, MarineTraffic, Shiptracker και Vesseltracker [1]. Ένας μεγάλος όγκος πληροφοριών για ένα σκάφους είναι άμεσα διαθέσιμος σε οποιονδήποτε έχει πρόσβαση στο Διαδίκτυο. Για παράδειγμα, το σχήμα που ακολουθεί δείχνει την τοποθεσία, ώρα αναχώρησης και άφιξης από λιμένες καθώς και άλλες πληροφορίες για το επιβατηγό πλοίο Ελευθέριος Βενιζέλος που μπορούν να ανευρεθούν μέσω του Marine Traffic. Ο ιστότοπος που διακινεί αυτήν την πληροφορία έχει τουλάχιστον εγγεγραμμένα 1.5 εκατομμύρια πλοία.



Σχήμα 7: Πληροφορίες διακίνησης επιβατηγού πλοίου Ελ. Βενιζέλος μέσω ιστοτόπου Marine Traffic

Στον παγκόσμιο ιστότοπο μπορούν να βρεθούν ένα μεγάλο πλήθος από διαθέσιμες σελίδες (WEB pages) οι οποίες προσφέρουν ανάλογες πληροφορίες για τη ναυτιλία. Προφανώς, η διακίνηση της πληροφορίας σε πραγματικό χρόνο μπορεί να διευκολύνει μία κακόβουλη ομάδα για την ανάπτυξη τόσο φυσικής όσο και κυβερνο-επίθεσης σε πλοία, με στόχο το φυσικό τους φορτίο ή άλλους σκοπούς.

Μερικές φορές, οι πληροφορίες διαρρέουν οικειοθελώς, έστω και ακούσια. Για παράδειγμα, πολλά πλοία θα απαγορεύσουν στους πειρατές την πρόσβαση σε αξιόπιστες πληροφορίες με απενεργοποίηση του AIS ή στέλνοντας πλαστά δεδομένα AIS ή μπορεί να κοινοποιήσουν αυτήν την πληροφορία σε μέσα κοινωνικής δικτύωσης. Αυτές οι προσπάθειες ενδέχεται να υπονομευθούν από τα μέλη του πληρώματος που ανεβάζουν πληροφορίες ακόμη και στις προσωπικές τους σελίδες, στα μέσα κοινωνικής δικτύωσης, μερικές φορές θέτοντας σε κίνδυνο την ασφάλεια του σκάφους. Δεν είναι μυστικό ότι οι ίδιοι οι άνθρωποι που χειρίζονται τα πληροφοριακά συστήματα, είναι συχνά ο πιο "αδύναμος κρίκος" στην αλυσίδα της κυβερνο-ασφάλειας.

Άλλες πληροφορίες που μπορεί να χρησιμοποιηθούν σε εκδηλώσεις κυβερνο-επιθέσεων αφορούν σε:

- Εικόνες και χάρτες (π.χ. Google Earth, εικόνες Google, IntelliEarth)
- Μηχανές αναζήτησης και ιστότοποι ειδήσεων
- Βάσεις δεδομένων επιχειρήσεων και κυβερνητικών οργανισμών
- Ιστότοποι απεικόνισης AIS
- Βάσεις δεδομένων λιμένων (π.χ. FleetMon)
- Ιστότοποι συμβάσεων (π.χ. GovTribe, GovWin)
- Ιστότοποι για Πλοία, λιμάνια και ναυτιλιακές γραμμές
- Ιστότοποι μέσων κοινωνικής δικτύωσης
- Google Dorking για εύρεση προσωπικού και διευθύνσεων ηλεκτρονικού ταχυδρομείου

2.2 Ναυτιλιακές Υποδομές και Κυβερνο-επιθέσεις

Στην προηγούμενη ενότητα παρουσιάστηκαν τα εργαλεία για την εκδήλωση των κυβερνο-επιθέσεων στην ναυτιλία. Στην συνέχεια παρουσιάζονται οι υποδομές της ναυτιλίας, οι οποίες συνιστούν και τα φυσικά σημεία επαφής για την εκδήλωση αυτών των επιθέσεων. Οι υποδομές προφανώς αφορούν σε όλα τα τμήματα της ναυτιλιακής αλυσίδας, εμπλέκοντας υλικο-τεχνικό καθώς και έμψυχο δυναμικό.

2.2.1 Τα Λιμάνια ως υποδομή κυβερνο-επίθεσης

Τα λιμάνια είναι μια μικρογραφία ολόκληρου του Maritime Transportation System - MTS. Οποιοδήποτε λιμάνι μπορεί να περιλαμβάνει διαφορετικούς συνδυασμούς πολλών στοιχείων, συμπεριλαμβανομένων των:

- στρατιωτικά, κυβερνητικά, εμπορικά, ή σκάφη κρουαζιέρας
- πλοιοκτήτες και φορείς εκμετάλλευσης
- ναυτιλιακούς πράκτορες
- διαχειριστές φορτίου
- μεταφορείς
- φορείς εκμετάλλευσης λιμένα
- μάρκετινγκ και επικοινωνίες
- διαχείριση τεχνολογίας υποδομής και λειτουργιών
- λιμενικές αρχές
- λιμενάρχες, πιλότους βοηθητικών σκαφών και διαχείριση κυκλοφορίας
- στρατιωτική ασφάλεια και αρχές επιβολής νόμου (αστυνομία,λιμενικό)
- υπηρεσίες τελωνείων και μετανάστευσης
- εγκαταστάσεις επισκευής και συντήρησης πλοίων
- τερματικά, επιθεωρητές ασφάλειας και περιβάλλοντος
- πλοηγοί και άλλοι λιμενεργάτες
- εταιρείες υλικοτεχνικής υποστήριξης και υποστηρικτικό προσωπικό

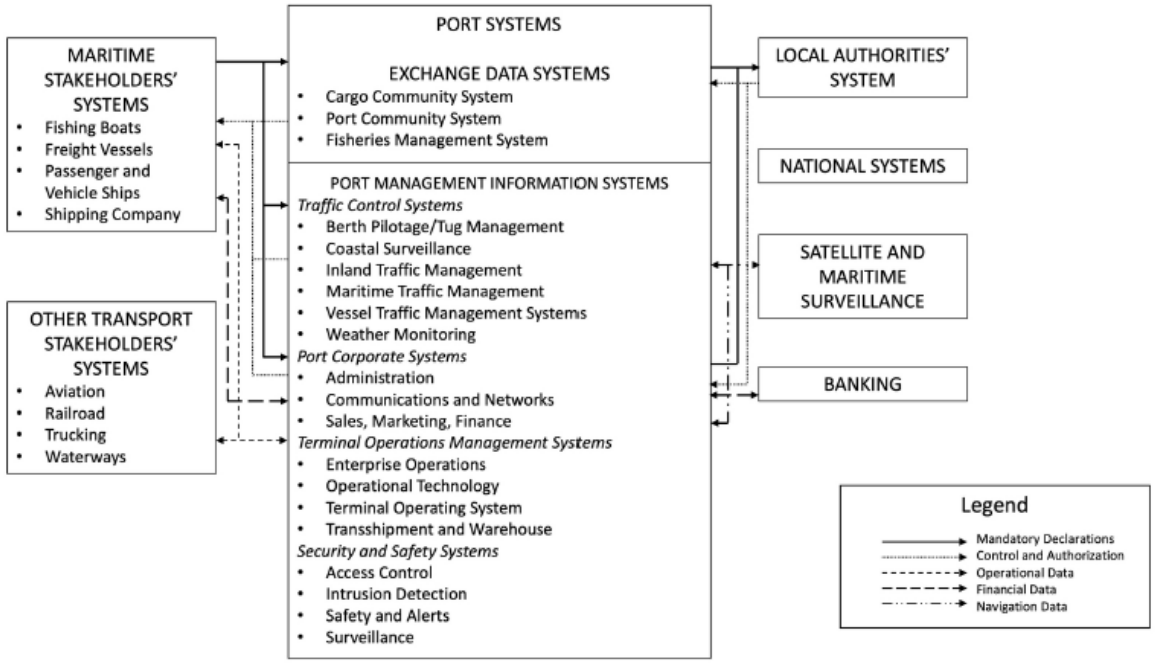
Τα λιμάνια δεν είναι μόνο αναπόσπαστα μέρη του θαλάσσιου περιβάλλοντος, αλλά είναι αυτόνομες οντότητες που λειτουργούν τόσο ως πάροχοι όσο και ως καταναλωτές ναυτιλιακών

υπηρεσιών. Εν ολίγοις, κάθε τύπος κυβερνο-επίθεσης που μπορεί να επηρεάσει οποιοδήποτε τμήμα του MTS, μπορεί να είναι παρόν και να εκδηλωθεί σε ένα λιμάνι. Δεν είναι καθόλου παράξενο, που τα λιμάνια αποτελούν στόχους "υψηλού επιπέδου" για επίδοξους εισβολείς του κυβερνοχώρου, διότι συνδυάζουν πολλά πληροφοριακά δεδομένα με πολλές ναυτιλιακές υπηρεσίες [1], [4].

Τα δομικά στοιχεία και οι ροές επικοινωνίας που συνιστούν το σύνολο των υπηρεσιών ενός λιμανιού είναι:

- Πύλη εισόδου (terminal gate)
- Οι ICT τεχνολογίες της πύλης εισόδου (ICT Gate technologies)
- Διοικητικά πληροφοριακά συστήματα της πύλης εισόδου (terminal headquarters)
- Βιομηχανικά Συστήματα Ελέγχου (Industrial Control Systems)
- Εγκαταστάσεις θέσεως, οδηγήσεως και πρόσδεσης πλοίων (Position, Navigation and Tiring)
- Βοηθητικά οχήματα (vessels)

Στο σχήμα που ακολουθεί παρουσιάζονται οι ροές δεδομένων (data flows) που αφορούν στις δραστηριότητες ενός λιμανιού:



Σχήμα 8: Πληροφορίες και ροές δεδομένων από τις διασυνδεόμενες δραστηριότητες ενός λιμανιού [1]

Προφανώς όλες οι δομικές οντότητες που συνιστούν ένα λιμάνι, σε συνδυασμό με τα πληροφοριακά συστήματα και τις ροές πληροφορίας, συνιστούν ένα ευρύ πεδίο για προστασία και κυβερνο-ασφάλεια από την εκδήλωση επιθέσεων. Οι μηχανισμοί αυτών των επιθέσεων, με βάση την εμπειρία που έχει αποκομιστεί από τέτοια παραδείγματα, αποδεικνύει ότι το πεδίο για την προστασία είναι ευρύ και εξαιρετικά αλληλοεπιδραστικό. Για παράδειγμα, οι λειτουργίες ενός λιμανιού μπορεί να επηρεαστούν σημαντικά με οποιονδήποτε τύπο επίθεσης, ο οποίος ενδεχόμενα θα αλλοιώσει την τοποθέτηση ενός εισερχόμενου πλοίου, την απαιτούμενη διαδικασία φορτο-εκφορτώσεως του, τα έγγραφα πλεύσης, κ.λπ.

Οι κανονιστικές οδηγίες που σχετίζονται με την κυβερνο-ασφάλεια στο παγκόσμιο MTS περιλαμβάνουν πολλά θέματα [1], [4], [32], τα οποία θα πρέπει να εξετασθούν λεπτομερώς. Δεδομένης της μοναδικής φύσης των λιμένων, αυτή η ενότητα εισάγει κανονισμούς που σχετίζονται ειδικά με την κυβερνο-ασφάλεια των λιμένων. Αρκετοί οργανισμοί παρέχουν καθοδήγηση (guidelines) για την κυβερνο-άμυνα που σχετίζεται με τα λιμάνια, συμπεριλαμβανομένων του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), του ιδρύματος Μηχανικής

και Τεχνολογίας (Institution of Engineering and Technology - IET) και της Διεθνούς Ένωσης Λιμένων και Προβλητών (International Association of Ports and Harbors - IAPH). Θα πρέπει να σημειωθεί ότι η κυβερνο-ασφάλεια των λιμένων αποτελεί αντικείμενο σημαντικών κανονιστικών ρυθμίσεων και εντολών.

Τα λιμάνια ως σημαντικές υποδομές της ναυτιλίας έχουν δεχθεί ένα σημαντικό πλήθος από κυβερνο-επιθέσεις. Ενδεικτικά στη συνέχεια, αναφέρονται περιστατικά τέτοιων κυβερνο-επιθέσεων [30].

Το 2013, το λιμάνι της Αμβέρσας ανακάλυψε ότι ένα καρτέλ ναρκωτικών είχε ελέγξει το σύστημα διαχείρισης εμπορευματοκιβωτίων. Στην πραγματικότητα, το δίκτυο υπολογιστών του λιμανιού είχε κατασκοπευθεί ήδη από τον Ιούνιο του 2011, όταν στο δίκτυο έγινε διείσδυση κακόβουλου λογισμικού. Συγκεκριμένα εγκαταστάθηκε ένας keylogger. Ο keylogger επέτρεπε στους hackers να καταγράφουν τα πλήκτρα των χειριστών φόρτωσης/εκφόρτωσης και έτσι να αποκτήσουν ονόματα χρήστη και κωδικούς πρόσβασης. Το λιμάνι της Αμβέρσας αποκατέστησε τελικά το σύστημά του επενδύοντας σχεδόν 200.000 ευρώ για τη δημιουργία αντιμέτρων, συμπεριλαμβανομένου ενός νέου συστήματος διαχείρισης κωδικών πρόσβασης (για την παροχή πρόσβασης σε εμπορευματοκιβώτια) και νέων καναλιών επικοινωνίας μεταξύ των φορέων εκμετάλλευσης λιμένων και των υπηρεσιών πελατών.

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. Το λιμάνι του Ρότερνταμ είναι ένα από τα λιμάνια που έχει επενδύσει στην πλήρη αυτοματοποίηση των λειτουργικών του διαδικασιών (ως μέρος μιας στρατηγικής Έξυπνου Λιμένα(Smart Port), η οποία ενσωματώνει το Internet of Things - IoT και την τεχνητή νοημοσύνη), γεγονός που το καθιστά ακόμη πιο εξαρτημένο από τη σταθερότητα των υπηρεσιών πληροφορικής. Σε απάντηση, ο Δήμος του Ρότερνταμ, η αστυνομία και οι λιμενικές αρχές διόρισαν από κοινού έναν Υπεύθυνο Port Cyber Resilience για τη βελτίωση της κυβερνο-αντοχής του λιμανιού, την εκπαίδευση των εμπλεκομένων μερών σε θέματα κυβερνο-ασφάλειας, τη βελτίωση της οργανωτικής εκπαίδευσης και τη εξασφάλιση καλύτερης διαχείρισης ρίσκου.

Ένα χρόνο μετά την κυβερνο-επίθεση του Ρότερνταμ, μια σειρά κυβερνο-επιθέσεων διέκοψε τις δραστηριότητες πολλών διεθνών λιμανιών. 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, διαπίστωσε ότι το σύστημα πληροφοριών της έχει μολυνθεί από ransomware.

Στις 20 Σεπτεμβρίου 2018, το λιμάνι της Βαρκελώνης ήταν το επόμενο που χτυπήθηκε. Από τις ελάχιστες πληροφορίες που χουν διαρρεύσει φαίνεται ότι τα εσωτερικά συστήματα πληροφορικής δέχθηκαν επίθεση, γεγονός που επηρέασε τις διαδικασίες φόρτωσης/εκφόρτωσης. Οι διαχειριστές (operators), ωστόσο, τόνισαν ότι η θαλάσσια δραστηριότητα δεν επηρεάστηκε, καθώς τα πλοία μπόρεσαν να κυκλοφορήσουν και να εισέλθουν στο λιμάνι.

Μια εβδομάδα αργότερα, το λιμάνι του Σαν Ντιέγκο διαταράχθηκε επίσης από μια "πολύ εξελιγμένη" κυβερνοεπίθεση, χωρίς περαιτέρω πληροφορίες για την τεχνική που χρησιμοποιήθηκε. Οι λιμενικές αρχές επιβεβαίωσαν ότι επρόκειτο για επίθεση ransomware που περιόριζε σοβαρά τις δυνατότητες των υπαλλήλων τους, κάτι που θα είχεπροσωρινές επιπτώσεις στην εξυπηρέτηση του κοινού, ειδικά στους τομείς των αιτημάτων δημόσιων αρχείων και των επιχειρηματικών υπηρεσιών.

Τέλος την ίδια χρονιά, το λιμάνι του Βανκούβερ υπέστη επίθεση brute-force τον Οκτώβριο, λίγους μήνες μετά από μία άλλη επίθεση του ίδιου τύπου. Σύμφωνα με γαλλικά δημοσιεύματα έγινε προσπάθεια παραβίασης σε σχεδόν 225,000 λογαριασμοί χρηστών εκείνη την ημέρα,(σε σχέση με 6000 λογαριασμούς συνήθους δραστηριότητας καθημερινά) αν και δεν δόθηκαν περισσότερες πληροφορίες σχετικά με τις συνέπειες αυτής της επίθεσης.

Τον Μάρτιο του 2020, το λιμάνι της Μασσαλίας χτυπήθηκε με το ransomware Mespinoza/Pysa. Στην περίπτωση αυτή, οι θαλάσσιες υποδομές δεν άμεσος στόχος της επίθεσης, αλλά επηρεάστηκαν λόγω της διασύνδεσής τους με τα πληροφοριακά συστήματα στην Aix-Marseille-Provence, που ήταν ο κύριος στόχος της επίθεσης. Σύμφωνα με πληροφορίες, τα αποτελέσματα της επίθεσης μειώθηκαν σημαντικά χάρη στην κοινή δράση των Chief Information Security Officers - CISOs των διαφόρων οργανισμών που επηρεάστηκαν. Αυτό το περιστατικό καταγράφηκε δημόσια από τη γαλλική ANSSI, η οποία συμμετείχε στην ανάλυση κινδύνου και βοήθησε στην ανάπτυξη των αντιμέτρων που ισχύουν μέχρι σήμερα. Κατά τη διεξαγωγή αυτού του ελέγχου, η ANSSI φέρεται να εντόπισε πολλά αρχεία ιού στα στοχευμένα τμήματα πληροφορικής, τα οποία έδειξαν ότι άλλο κακόβουλο λογισμικό είχε διεισδύσει τους προηγούμενους μήνες ή χρόνια

πριν. Σε κάθε περίπτωση, οι τεχνικές εισβολής που χρησιμοποιήθηκαν φέρεται να μην ήταν τόσο πολύ προηγμένες.

Τον Μάιο του 2020, το λιμάνι του Shahid Rajaee, στο Ιράν, είδε όλες τις επιχειρησιακές του διαδικασίες να διακόπτονται σχεδόν πλήρως. Εσωτερικές πηγές είπαν σε δημοσιογράφους αμερικανικής εφημαερίδας, ότι οι υπολογιστές που ρυθμίζουν τη ροή πλοίων, φορτηγών και εμπορευμάτων διέκοψαν την λειτουργία τους όλοι ταυτόχρονα. Ενώ ο τρόπος λειτουργίας ήταν άγνωστος, αξιωματούχοι των ΗΠΑ αναφέρθηκαν σε έναν κυβερνο-πόλεμο μεταξύ του Ιράν και του Ισραήλ. Αυτή η κυβερνο-επίθεση ήταν πιθανώς μια απάντηση σε μια επίθεση στο δίκτυο ύδρευσης του Ισραήλ που είχε προηγηθεί.

Τον Ιούνιο του 2020, ένα ναυπηγείο στο Λάνγκστεν της Νορβηγίας, που ανήκει στην εταιρεία Vard, έπεσε θύμα επίθεσης ransomware. Ενώ η εταιρεία δεν αποκάλυψε ποτέ τις ακριβείς συνέπειες και τις τεχνικές λεπτομέρειες της επίθεσης, ο εκπρόσωπός της, παραδέχτηκε ότι οι επιχειρήσεις έκτοτε ήταν υποτονικές. Εκτός από την κρυπτογράφηση αρχείων ransomware, η εταιρεία παραδέχτηκε επίσης παραβίαση της βάσης δεδομένων, χωρίς να παρέχει περισσότερες λεπτομέρειες σχετικά με την ποσότητα ή τη σημαντικότητα των δεδομένων που έχουν κλαπεί.

Τον Νοέμβριο του 2020, 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. Αλλά το μέγεθος του δεν εμπόδισε τους εγκληματίες του κυβερνοχώρου να επιτίθενται σε αυτούς τους στόχους, οι οποίοι συχνά προστατεύονται λιγότερο καλά. Οι λιμενικές αρχές χρειάστηκαν σχεδόν μια εβδομάδα για να ανακτήσουν τον έλεγχο των δεδομένων τους ανακατασκευάζοντας το σύστημα πληροφοριών τους με χρήση αντιγράφων ασφαλείας.

Τον Ιούλιο του 2021, τέσσερα μεγάλα λιμάνια στη Νότια Αφρική (Κέιπ Τάουν, Βασίλισσα Ελισάβετ, Ngqura και Durban), παρέλυσαν μετά από μια μαζική επίθεση στην Εθνική Λιμενική Αρχή Transnet, τον κύριο διαχειριστή εμπορευμάτων της χώρας. Το επίσημο δελτίο τύπου (αναφέρεται στο Reuters), χαρακτήρισε την επίθεση ως περίπτωση "ανωτέρας βίας" που κατέστησε το σύστημα υπολογιστή του άχρηστο, παρόμοια με τα αποτελέσματα μιας επίθεσης ransomware. 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.

Σύμφωνα με επίσημη δήλωση, το λιμάνι του Χιούστον δέχθηκε επίθεση το 2021 που εκμεταλλευόταν μια κρίσιμη ευπάθεια σε ένα πρόγραμμα διαχείρισης κωδικών πρόσβασης. Η ευπάθεια αυτή που ήταν κρίσιμη (CVSS 9.8 στα 10) επέτρεπε εύκολα στους κακόβουλους να εμφυτεύουν κελύφη κώδικα (web shell) στο σύστημα πληροφοριών ενός οργανισμού. Αυτό τους έδινε πρόσβαση/δυνατότητα εκτέλεσης διαφόρων ενεργειών, από την εξαγωγή κρίσιμων δεδομένων έως την εγκατάσταση κακόβουλου λογισμικού. Οι λιμενικές αρχές ισχυρίστηκαν ότι η ισχύουσα κυβερνο-άμυνα και το σχέδιο ασφαλείας της εγκατάστασης (το οποίο πρέπει να υποβληθεί σύμφωνα με τον Νόμο για την Ασφάλεια στη Θαλάσσια Μεταφορά - MTSA στις Ηνωμένες Πολιτείες) τους επέτρεψαν να αντιμετωπίσουν την απειλή.

2.2.2 Τα Δίκτυα του Πλοίου και τα Συστήματα Επικοινωνιών ως υποδομές κυβερνο-επίθεσης

Ένα πλοίο είναι μια πλωτή πόλη, και ως εκ τούτου, είναι μια "πλωτή πληροφορία και πλατφόρμα τεχνολογίας επικοινωνιών". Τα πλοία σήμερα, βασίζονται όλο και περισσότερο σε δίκτυα επικοινωνίας μεταξύ ανθρώπων, μεταξύ συστημάτων επί των εσωτερικών δικτύων του πλοίου, και άλλων επικοινωνιακών συστημάτων εκτός του πλοίου. Τα εξωτερικά δίκτυα χρησιμοποιούνται για επίσημες και ανεπίσημες επικοινωνίες, ρυθμιστικές και διοικητικές λειτουργίες, και συνομιλίες είτε από πλοίο σε πλοίο, είτε από πλοίο προς την ακτή. Στη συνέχεια παρουσιάζονται μερικά από τα δίκτυα επικοινωνιών του πλοίου και περιγράφονται ορισμένες από τις ευπάθειές τους στον κυβερνοχώρο.

Υπάρχει μια ποικιλία δικτύων επικοινωνιών, στα οποία ένα πλοίο πρέπει να είναι εγγεγραμμένο, για συνήθεις ή εξειδικευμένες λειτουργίες. Κάποια εξωτερικά δίκτυα είναι ιδιωτικά (private) οπότε και σχετικά ασφαλή, και μπορεί να λειτουργήσουν με ή χωρίς κρυπτογράφηση. Τα δημόσια δίκτυα (public networks) είναι συνήθως ανοιχτά σε οποιονδήποτε διαθέτει δέκτη

επικοινωνίας. Το σχήμα που ακολουθεί παρουσιάζει τα τυπικά δίκτυα επικοινωνιών επί ενός πλοίου. Τα εξωτερικά δίκτυα επικοινωνιών περιλαμβάνουν:

- Ναυτικός ραδιό-ασύρματος πολύ υψηλής συχνότητας (VHF). Οι ασύρματοι επικοινωνίας αυτής της τεχνολογίας αποτελούν ένα συνηθισμένο εξοπλισμό επικοινωνίας σε κάθε σκάφος οποιουδήποτε μεγέθους. Το Κανάλι 16 (156.8 MHz) είναι η διεθνής συχνότητα καταιγισμού/έκτακτης ανάγκης και κινδύνου.
- Τα συστήματα παρακολούθησης σκαφών (Vessel Monitoring Systems - VMS), τα οποία επιτρέπουν σε διάφορους ρυθμιστικούς/ελεγκτικούς οργανισμούς να παρακολουθούν την δραστηριότητα των αλιευτικών σκαφών.
- Αναγνώριση και παρακολούθηση μεγάλης εμβέλειας (Long Range Identification and Tracking - LRIT), για τη διασφάλιση επικοινωνίας σε όλα τα επιβατηγά και φορτηγά πλοία, κινητές υπεράκτιες μονάδες γεώτρησης, για να μπορούν να αναφέρουν τη θέση τους κάθε έξι ώρες. Οι αναφορές LRIT γενικά γίνονται πάνω από το δορυφορικό δίκτυο επικοινωνιών του πλοίου, τα οποία είναι ιδιωτικά και ασφαλή.
- Τα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks - VPNs), τα οποία επιτρέπουν ιδιωτικές, ασφαλείς επικοινωνίες μεταξύ του πλοίου και άλλου μέρους, χρησιμοποιώντας το Διαδίκτυο και άλλα δίκτυα δεδομένων, ή φωνής με χρήση Πρωτοκόλλου φωνής μέσω του Διαδικτύου (Voice over IP - VoIP). Οι λύσεις VoIP επιτρέπουν τη χρήση VPN είτε για φωνή είτε για δεδομένα.
- Τα συστήματα πολύ μικρού τερματικού διαφράγματος (Very Small Aperture Terminals - VSATs) επιτρέπουν αμφίδρομη επικοινωνία με δορυφορικούς επίγειους σταθμούς μέσω παρόχου δορυφόρου, για επικοινωνίες δεδομένων.
- Το Intellian/Inmarsat Fleet Broadband - FBB που δύναται να παρέχουν φωνητικές υπηρεσίες,βιντεοκλήσεις, κλήσεις GSM, δεδομένα, μηνύματα (SMS), και υπηρεσία φαξ μέσω δορυφόρου.
- Οι ναυτιλιακές υπηρεσίες κινητής τηλεφωνίας, όπως η Cellular at Sea, γίνονται ολοένα και πιο κοινά συστήματα επικοινωνίας επί των πλοίων, παρέχοντας απρόσκοπτες υπηρεσίες κινητών τηλεφώνων, δεδομένων και γραπτών μηνυμάτων με χρήση τυπικών κινητών τηλέφωνων και δυνατότητα περιαγωγής.
- Το GNSS και το AIS είναι σχεδιασμένα για θέση, πλοήγηση, ακριβούς χρονισμού και επίγνωση της κατάστασης πλεύσης του σκάφους.

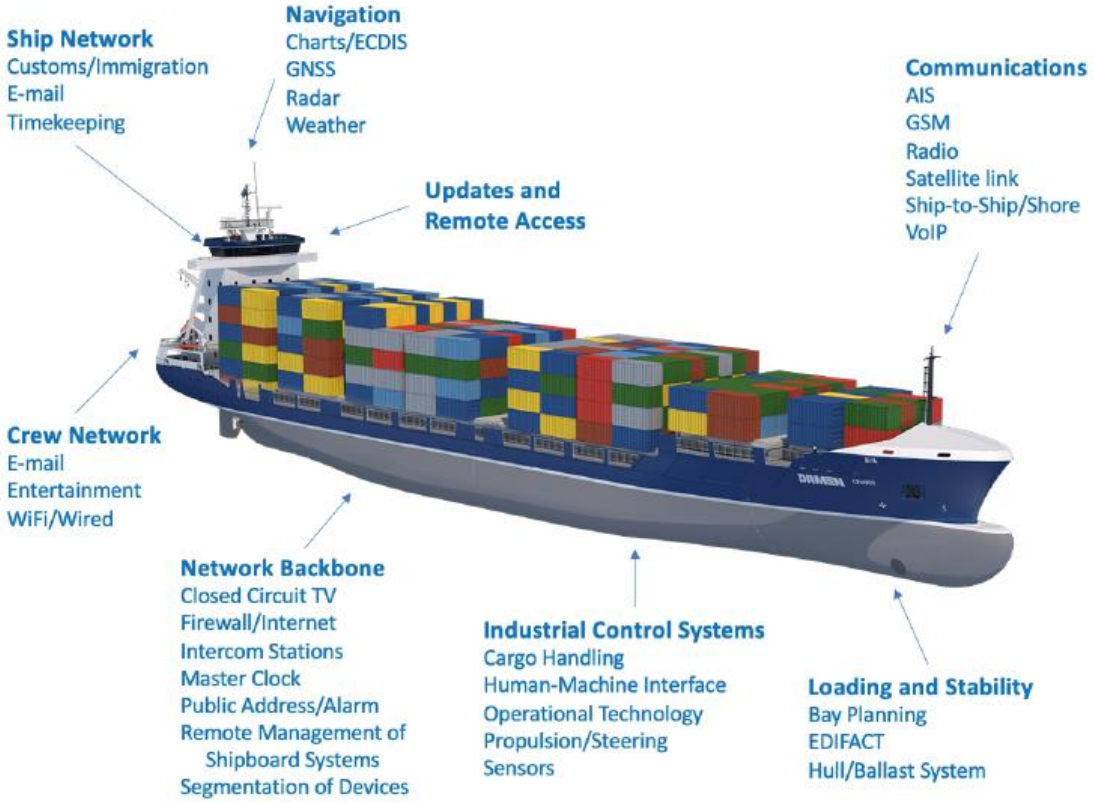
Παγκόσμιοι πάροχοι δορυφορικών επικοινωνιών, όπως η Globalstar, το Inmarsat και το Iridium λειτουργούν ως αστερισμοί (constellations,δηλ συνεργάζονται σαν ένα σύστημα) για κινητά και υπηρεσίες σταθερής τηλεφωνίας και επικοινωνιών δεδομένων για τη ναυτιλία, την αεροπορία και για άλλους κλάδους της κινητής τηλεφωνίας. Η εκκολαπτόμενη υπηρεσία StarLink του SpaceX, εισέρχεται στο διαδίκτυο σε αυτόν τον χώρο, όπου σε πλήρη ανάπτυξη αυτό το σύστημα θα μπορούσε να διαθέτει έως και 42,000 μικρούς δορυφόρους χαμηλής τροχιάς (Low Earth Orbit - LEOS), με τους οποίους θα προσφέρει υψηλή ταχύτητα και ευρυζωνικότητα για υπηρεσίες φωνής και δεδομένων.

Τα ίδια τα πλοία έχουν πολλά συστήματα [2] που διασυνδέονται μεταξύ τους σε μία μορφή δικτύου επικοινωνιών, όπως:

- Συστήματα πλοήγησης γέφυρας (Bridge Navigation Systems - BNS), συμπεριλαμβανομένου του AIS, του συστήματος Οθόνης Ηλεκτρονικού χάρτη και συστήματος πληροφοριών (Electronic Chart Display and Information System - ECDIS), του GNSS, του LRIT και του ραντάρ.
- Εξωτερικά συστήματα δεδομένων και τηλεπικοινωνιών, όπως το FBB, το Διαδίκτυο, το σύστημα VHF και το VSAT.
- Μηχανικά συστήματα, όπως ο κύριος κινητήρας, ο βοηθητικός κινητήρας, ο έλεγχος διεύθυνσης, ο έλεγχος πυρκαγιάς και η διαχείριση έρματος
- Συστήματα παρακολούθησης και ασφάλειας πλοίων, όπως το κλειστό κύκλωμα τηλεόρασης - CCTV, το Σύστημα Ειδοποίησης Ασφαλείας του Πλοίου (Ship Security Alert System - SSAS), η πρόσβαση στα συστήματα ελέγχου, οι αισθητήρες, τα συστήματα αναγγελιών, οι

γενικοί συναγερμοί, τα θυροτηλέφωνα, το κύριο ρολόι (master clock), ο έλεγχος υδροσυλλεκτών, η μονάδα γλυκού νερού, η παραγωγή και η διανομή ηλεκτρικής ενέργειας και η διανομή του νερού ψύξης.

- Τα Συστήματα χειρισμού φορτίου, όπως το σύστημα τηλεχειρισμού βαλβίδων, τα συστήματα παρακολούθησης στάθμης/πίεσης, τα συστήματα καταπόνησης, η παρακολούθηση και η ηλεκτρονική ανταλλαγή δεδομένων για διαχείριση, τα συστήματα εμπορίου και μεταφορών (Electronic Data Interchange for Administration, Commerce and Transport - EDIFACT).



Σχήμα 9: Παρουσίαση των δικτύων επικοινωνιών ενός πλοίου [1]

Τα συστήματα γέφυρας είναι το κέντρο διοίκησης ενός πλοίου. Όλα τα ενσωματωμένα συστήματα έρχονται μαζί στη γέφυρα, παρέχοντας έναν ολοκληρωμένο μηχανισμό για τον πλοίαρχο ή το πλήρωμα για διοίκηση, γνωρίζοντας συνολικά την κατάσταση του σκάφους. Τα συστήματα γεφυρών παραμένουν ευάλωτα σε hacking λόγω, κυρίως, της κακής ασφάλειας στα πρωτόκολλα επικοινωνίας του πλοίου και στο σχεδιασμό του δικτύου, όπως τα δορυφόρικά τερματικά επικοινωνίας που εκτίθενται στο Διαδίκτυο, οι διοικητικές διεπαφές πρόσβασης με μη ασφαλή πρωτόκολλα (π.χ. Telnet και HTTP). Επειδή τα δίκτυα πλοίων γενικά δεν χρησιμοποιούν έλεγχο ταυτότητας μηνύματος, κρυπτογράφηση ή έλεγχο ακεραιότητας αυτό αποτελεί έναν επίσης παράγοντα για την έλλειψη ασφάλειας σε μία επίθεση. Αυτό επιδεινώνεται περαιτέρω, από την πλημμελή εφαρμογή των κανόνων ασφαλείας εκ μέρους των χρηστών, που χρησιμοποιούν πολύ συχνά προεπιλεγμένα (default) διαπιστευτήρια σύνδεσης που είναι εύκολα να εντοπιστούν (όπως το να βασίζονται σε ένα κοινό για όλους όνομα χρήστη και έναν κοινό κωδικό πρόσβασης στον λογαριασμό για την ταυτοποίηση), ή τη μη συχνή αλλαγή κωδικών πρόσβασης.Ένας πιθανός λόγος για την κακή πρακτική χρησιμοποίησης default κωδικών στα συστήματα ίσως είναι και το γεγονός ότι τα πληρώματα των εμπορικών πλοίων εναλλάσονται διαρκώς οπότε πιθανή μη καταγραφή αλλαγής κωδικών, να μπορούσε να αποκλείσει την πρόσβαση σε κάποιο σύστημα.

Ένα χαρακτηριστικό παράδειγμα απεικόνισης του επιπέδου κυβερνοασφάλειας στα εμπορικά πλοία απεικονίστηκε στο ακόλουθο παράδειγμα. Μια Ισραηλινή εταιρεία κυβερνοασφάλειας, εξειδικευμένη για τη Ναυτιλία, η Naval Dome, πραγματοποίησε μια σειρά από δοκιμές διείσδυσης (hacking) στο πλοίο ZIM GENEVOA το 2017. Η εταιρεία επέφερε τρεις

διαφορετικούς τύπους επιτυχημένων κυβερνο-επιθέσεων, που πραγματοποιήθηκαν όλες χωρίς τη συνεργασία του πληρώματος του πλοίου. Η πρώτη ευπάθεια σχετιζόταν με το ECDIS. Χρησιμοποιώντας την δορυφορική σύνδεση του πλοίου, οι επιτιθέμενοι έστειλαν ένα e-mail με συνημμένο κακόβουλου λογισμικού στον υπολογιστή του πλοιάρχου. Ο υπολογιστής αυτός συνδεόταν τακτικά με το ECDIS για μια ενημέρωση γραφήματος. Κατά τον επόμενο κύκλο ενημέρωσης γραφήματος, ο ιός μετακινήθηκε στον υπολογιστή του ECDIS. Το κακόβουλο λογισμικό σχεδιάστηκε ειδικά, για να αλλάξει τη θέση του πλοίου κατά τις βραδινές ώρες, χωρίς αλλαγή της οθόνης. Οι αλλαγές ήταν ανεπαίσθητες και προσαρμοσμένες σε πληροφορίες θέσης, κατεύθυνσης, βάθους και ταχύτητας χωρίς καμμία συμμετοχή από την γέφυρα του πλοίου.

Η δεύτερη ευπάθεια εντοπίστηκε στο σύστημα ραντάρ. Αυτή η επίθεση χρησιμοποίησε το δίκτυο Ethernet που συνέδεε το ραντάρ, το ECDIS, και την συσκευή εγγραφής δεδομένων ταξιδιού (Voyage Data Recorder - VDR) και τα δίκτυα συστήματος ειδοποίησης γέφυρας. Το κακόβουλο λογισμικό κατάφερε να διαγράψει στόχους ραντάρ από την οθόνη του ραντάρ της γέφυρας αποτελεσματικά, "τυφλώνοντας" το πλοίο σε κοντινά σκάφη. Η διεπαφή συστήματος έδειξε το ραντάρ να λειτουργεί κανονικά, συμπεριλαμβανομένων όλων των ορίων ανίχνευσης που έχουν ρυθμιστεί σωστά, έτσι ώστε οι αξιωματικοί της γέφυρας δεν είχαν κανένα λόγο να υποπτεύονται συστημική αποτυχία.

Η τελική παραβίαση σημειώθηκε στα Συστήματα Ελέγχου Μηχανημάτων (Machinery Control System - MCS). Σε αυτήν την περίπτωση, ένας ιός εισήχθη στο MCS μέσω μιας μολυσμένης μονάδας USB. Ο ιός έτρεξε αυτόματα και κινήθηκε για να επιτεθεί σε άλλα βοηθητικά συστήματα υπολογιστών. Ο πρώτος στόχος ήταν το σύστημα έρματος. Οι βαλβίδες και οι αντλίες διακόπηκαν και σταμάτησαν να λειτουργούν, αλλά η οθόνη του χειριστή παρουσίασε κανονική λειτουργία. Άλλοι πιθανοί στόχοι βοηθητικού συστήματος MCS περιλάμβαναν τον κλιματισμό, τις γεννήτριες και τα συστήματα καυσίμων.

Από την παραπάνω επίθεση, γίνεται λοιπόν εμφανές ότι η καθολική δικτύωση και διασύνδεση των υπολογιστικών συστημάτων του πλοίου, με χρήση κακόβουλου λογισμικού το οποίο είναι στοχευμένο για καθορισμένες λειτουργίες, μπορεί να προκαλέσει σημαντικά προβλήματα στον έλεγχο και κατ'επέκταση στην ασφάλεια πλεύσης ενός πλοίου.

2.2.3 Τα Συστήματα Πλοήγησης ως υποδομή κυβερνο-επίθεσης

Τα συστήματα πλοήγησης στο πλοίο, έχουν εξελιχθεί σημαντικά σε σχέση με τα πρώτα ταξίδια του ανθρώπου στον ανοικτό ωκεανό. Οι ναυτικοί παλαιότερα βασίζονταν στην εμπειρία τους, στην διαίσθηση και γνώση της φύσης και των θαλασσών, για περισσότερα από δύο χιλιάδες χρόνια πριν από την εισαγωγή των οργάνων στα πλοία. Τα τελευταία 100 χρόνια, οι ραδιοσυχνότητες, το ραντάρ και οι δορυφόροι βοηθούν στην ακριβή θέση, την πλοήγηση, και στα συστήματα χρονισμού και εντοπισμού των πλοίων (PNT).

Το κέντρο διοίκησης ενός σκάφους είναι η γέφυρα, το μέρος όπου γίνεται η παρακολούθηση και η διαχείριση όλων των συστημάτων ελέγχου του πλοίου. Ενα ολοκληρωμένο σύστημα πλοήγησης (Integrated Navigation System - INS), περιλαμβάνει το υλικό πλατφόρμας (hw), το λογισμικό (sw), τη γέφυρα όπου βρίσκονται όλες οι λειτουργίες που σχετίζονται με την πλοήγηση και την ασφαλή λειτουργία, ενοποιημένα σε μια ενιαία κονσόλα ή ομάδα οθονών. Ένα INS ενσωματώνει τα στοιχεία από πολλά από τα υποσυστήματα του πλοίου, συμπεριλαμβανομένων των [1], [6], [9]:

- AIS
- Autopilot
- Echo sounder
- Electronic Chart Display and Information System (ECDIS)
- GPS/GNSS
- Navigational telex (NAVTEX)
- Gyroscope
- Navigation workstation
- Radar

- Sonar
- Sensors (ρυθμός στροφής, θέση πηδαλίου, αλατότητα, θερμοκρασία νερού και καιρός)

Τα προαναφερόμενα υποσυστήματα παρέχουν στον πλοίαρχο του πλοίου επίγνωση σχετικά με την κατάσταση του πλοίου και του περιβάλλοντος. Όλες οι συσκευές είναι διασυνδεδεμένες μέσω τυπικών διεπαφών, όπως σειριακές γραμμές, του Δικτύου Περιοχής Ελεγκτή (Controller Area Network - CAN) ή Ethernet για την επικοινωνία, χρησιμοποιώντας τυπικά πρωτόκολλα. Οι περισσότερες από τις συσκευές χρησιμοποιούν λειτουργικό σύστημα Windows ή ειδικού τύπου λειτουργικό σύστημα, προερχόμενο από τον κατασκευαστή του κάθε υποσυστήματος.

Ένα INS είναι επιρρεπές σε έναν αριθμό φορέων κυβερνο-επιθέσεων από κάποιον που εκμεταλλεύεται τις γραμμές ή τα πρωτόκολλα επικοινωνίας που βασίζονται σε καθορισμένα και γνωστά πρότυπα. Σε μια επίδειξη, οι ερευνητές χρησιμοποίησαν μια μονάδα USB που περιείχε ένα κακόβουλο λογισμικό, και το σύνδεσαν σε μία από τις συσκευές που είναι συνδεδεμένες στο δίκτυο του INS. Το κακόβουλο λογισμικό μόλυνε το ECDIS, και ήταν σε θέση να χειραγωγήσει το GPS, πλαστογραφώντας τα μηνύματα GPS στο πρωτόκολλο επικοινωνίας που χρησιμοποιείται μεταξύ των συσκευών που είναι συνδεδεμένες με το INS. Αυτή η επίθεση θα μπορούσε επίσης να συντρίψει το σταθμό χειριστή, "τυφλώνοντας" ουσιαστικά το πλοίο.

2.3 Εργαλεία των Κυβερνο-επιθέσεων και Στρατηγικές αντιμετώπισης τους

Στις προηγούμενες ενότητες παρουσιάστηκαν τα εργαλεία των κυβερνο-επιθέσεων καθώς και οι υποδομές εκδήλωσης τους. Τα εργαλεία αφορούσαν κυρίως σε λογισμικό ειδικού τύπου καθώς και εργαλεία που άπτονται συνηθειών των χρηστών ή μειωμένα επίπεδα διασφάλισης των πληροφοριών λόγω μη ασφαλούς διακίνησης τους (ακούσια ή εκούσια). Οι υποδομές εισάγουν καθορισμένα σημεία λειτουργικότητας και υπηρεσιών, όπως αυτές προκύπτουν από τις ναυτιλιακές δραστηριότητες, εκτεινόμενες από την ίδια την φυσική οντότητα του πλοίου, στους λιμένες αλλά και στις τεχνολογίες που όλες οι υποδομές χρησιμοποιούν.

Ο θαλάσσιος κίνδυνος στον κυβερνοχώρο αναφέρεται σε ένα μέτρο του βαθμού στον οποίο ένα τεχνολογικό περιουσιακό στοιχείο θα μπορούσε να απειληθεί από μια πιθανή περίσταση ή γεγονός, το οποίο μπορεί να οδηγήσει σε αποτυχίες λειτουργίας ή ασφάλειας (φυσικής ή/και μη) σχετιζόμενες με τη ναυτιλία, ως συνέπεια της αλλοίωσης, της απώλειας ή παραβίασης συστήματος ή πληροφοριών [5].

Ως διαχείριση κινδύνων στον κυβερνοχώρο νοείται η διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης του κινδύνου που μία επίθεση εισάγει και της κοινοποίησης ενός κινδύνου που σχετίζεται με τον κυβερνοχώρο, συμπεριλαμβάνοντας και τις απαιτούμενες ενέργειες αποδοχής, αποφυγής, μεταφοράς ή μετριασμού σε αποδεκτό επίπεδο, λαμβάνοντας υπόψη το κόστος και τα ωφέλη των ενεργειών που λαμβάνονται για τα ενδιαφερόμενα μέρη.

Ο γενικός στόχος είναι να υποστηριχθεί η ασφαλής ναυτιλία, η οποία είναι επιχειρησιακά ανθεκτική στους κινδύνους στον κυβερνοχώρο. Οι κατευθυντήριες γραμμές παρέχουν συστάσεις υψηλού επιπέδου για τη διαχείριση των θαλάσσιων κινδύνων στον κυβερνοχώρο, για την προστασία της ναυτιλίας από τρέχουσες και αναδυόμενες απειλές και ευπάθειες στον κυβερνοχώρο, και περιλαμβάνουν λειτουργικά στοιχεία που υποστηρίζουν την αποτελεσματική διαχείριση του κυβερνοχώρου. Οι συστάσεις μπορούν να ενσωματωθούν στις υπάρχουσες διαδικασίες διαχείρισης κινδύνου και είναι συμπληρωματικές με τις πρακτικές διαχείρισης ασφάλειας που έχουν ήδη καθιερωθεί από τον IMO.

Οι τεχνολογίες του κυβερνοχώρου έχουν καταστεί ουσιαστικές για τη λειτουργία και τη διαχείριση πολλών συστημάτων κρίσιμων για την γενικότερη ασφάλεια αλλά και την ασφάλεια της ναυτιλίας και την προστασία του θαλάσσιου περιβάλλοντος [12]. Σε ορισμένες περιπτώσεις, αυτά τα συστήματα πρέπει να συμμορφώνονται με τα διεθνή πρότυπα και τις απαιτήσεις/κανονισμούς της χώρας της οποίας τη σημαία φέρει το εκάστοτε πλοίο. Ωστόσο, τα τρωτά σημεία που δημιουργούνται από την πρόσβαση, τη διασύνδεση ή τη δικτύωση αυτών των συστημάτων, μπορεί να οδηγήσουν σε κινδύνους στον κυβερνοχώρο που πρέπει να αντιμετωπιστούν [2]. Τα ευάλωτα συστήματα θα μπορούσαν να περιλαμβάνουν, αλλά δεν περιορίζονται σε:

- Συστήματα γεφυρών
- Συστήματα διακίνησης και διαχείρισης φορτίου
- Συστήματα διαχείρισης πρόωσης, μηχανημάτων και ελέγχου ισχύος
- Συστήματα ελέγχου πρόσβασης
- Συστήματα εξυπηρέτησης και διαχείρισης επιβατών
- Συστήματα που χρησιμοποιούν δημόσια δίκτυα
- Διοικητικά συστήματα και συστήματα του πληρώματος
- Συστήματα επικοινωνιών

Αυτές οι οδηγίες [2] παρουσιάζουν τα λειτουργικά στοιχεία που υποστηρίζουν την αποτελεσματική διαχείριση κινδύνων στον κυβερνοχώρο. Αυτά τα λειτουργικά στοιχεία δεν έχουν κάποια αλληλουχία, πρέπει να εφαρμόζονται ταυτόχρονα θα πρέπει να ενσωματώνονται κατάλληλα σε ένα πλαίσιο διαχείρισης κινδύνου:

- Προσδιορισμός: Καθορισμός των ρόλων και των αρμοδιοτήτων του προσωπικού για τη διαχείριση κινδύνων στον κυβερνοχώρο και προσδιορισμός των συστημάτων, των περιουσιακών στοιχείων, των δεδομένων και των συστημάτων που, όταν διακόπτονται, ενέχουν κινδύνους για τις λειτουργίες του πλοίου.
- Προστασία: Εφαρμογή διαδικασιών και μέτρων ελέγχου κινδύνου και σχεδιασμός έκτακτης ανάγκης για την προστασία από ένα συμβάν στον κυβερνοχώρο για τη διασφάλιση της συνέχειας των ναυτιλιακών εργασιών.
- Ανίχνευση: Ανάπτυξη και εφαρμογή δραστηριοτήτων που είναι απαραίτητες για τον έγκαιρο εντοπισμό ενός συμβάντος στον κυβερνοχώρο.
- Απόκριση: Ανάπτυξη και εφαρμογή δραστηριοτήτων και σχεδίων για την παροχή ανθεκτικότητας και την αποκατάσταση συστημάτων που είναι απαραίτητα για ναυτιλιακές λειτουργίες ή υπηρεσίες που έχουν υποστεί βλάβη λόγω ενός συμβάντος στον κυβερνοχώρο.
- Ανάκτηση: Προσδιορισμός μέτρων για τη δημιουργία αντιγράφων ασφαλείας και την αποκατάσταση συστημάτων στον κυβερνοχώρο που είναι απαραίτητα για ναυτιλιακές λειτουργίες που επηρεάζονται από ένα συμβάν στον κυβερνοχώρο.

Στα πλαίσια των γενικότερων οδηγιών (προσδιορισμός, προστασία, ανίχνευση, απόκριση, ανάκτηση), οι διαδικασίες που αφορούν σε κυβερνο-επιθέσεις στις υποδομές της ναυτιλίας, θα πρέπει να ακολουθήσουν τις ακόλουθες κατευθυντήριες γραμμές:

- Εξουσιοδοτημένη χρήση των συστημάτων με κωδικούς πρόσβασης - ταυτοποίησης
- Κλιμάκωση επιπέδου για τη χρήση και διαχείριση των πληροφοριών (υλοποίηση συστήματος διαχείρισης πληροφορίας)
- Μη δυνατότητα διαχείρισης των πληροφοριακών συστημάτων σε ανώτατο επίπεδο (κρισιμότητα) από μη εξουσιοδοτημένο προσωπικό
- Περιοδικός έλεγχος της λειτουργικότητας των συστημάτων
- Παρακολούθηση και καταγραφή των διεργασιών που εκτελούνται από το προσωπικό στα πληροφοριακά συστήματα
- Δυνατότητα αποκατάστασης και επαναφοράς υπολογιστικών συστημάτων
- Χρήση κρυπτογράφησης στα φυσικά μέσα και στα πρωτόκολλα επικοινωνιών

3 Κυβερνο-Επιθέσεις, Απειλές στις Δορυφορικές Επικοινωίας στα συστήματα της Ναυτιλίας. Δράσεις Αντιμετώπισης τους

Η ναυτιλία περιγράφεται συχνά ως ένας συντηρητικός κλάδος που καθυστερεί να υιοθετήσει τις νέες τεχνολογίες. Στην πραγματικότητα αυτό δεν ισχύει, ειδικά όταν πρόκειται για θέματα επικοινωνιών των πλοίων. Τα πλοία επικοινωνούσαν με την ακτή μέσω ραδιοζεύξεων ήδη από το 1899. Αρχικά τα μηνύματα αποστέλλονταν χρησιμοποιώντας κώδικα Morse και όχι με χρήση απευθείας μηνύματος φωνής. Από τότε όλες οι επερχόμενες τεχνολογίες ασυρμάτου χρησιμοποιήθηκαν εκτενώς από τα πλοία για απευθείας φωνητική επικοινωνία. Μέχρι τα τέλη της δεκαετίας του 1970, τα δορυφορικά συστήματα και τα δίκτυα επικοινωνιών χρησιμοποιούνταν από μικρό αριθμό πολιτικών σκαφών και περισσότερο από στρατιωτικά πλοία. Ο λόγος για αυτό οφειλόταν στον ακριβό εξοπλισμό καθώς και την τεχνολογία ειδικού τύπου που απαιτούσε η χρήση εξειδικευμένων και δαπανηρών συστημάτων.

Προφανώς, η τεχνολογική εξέλιξη υιοθετείται μόνο όταν φτάσει σε ένα κρίσιμο στάδιο όπου μπορεί να ανταποκριθεί στις απαιτήσεις της ναυτιλιακής βιομηχανίας, και ειδικότερα όταν είναι αξιόπιστη. Εάν η ναυτιλία ήταν πιο αργή για να ενστερνιστεί σε ορισμένες πτυχές, της σύγχρονης τεχνολογίας, αυτό οφείλεται συχνά, στο ότι οι δυσκολίες και το υψηλό κόστος των επικοινωνιών των πλοίων στις τεράστιες αποστάσεις μετακίνησης τους, δεν επέτρεπαν στους φορείς εκμετάλλευσης των πλοίων ώστε να επινοήσουν τρόπους για να ελαχιστοποιήσουν την "ποσότητα" των επικοινωνιών που απαιτούνται για εμπορικούς σκοπούς.

Λίγοι χειριστές πλοίων ή πληρώματά ασχολούνται με την υψηλή τεχνολογία και τη μηχανική των ίδιων των δορυφόρων. Οι τεχνολογίες αυτές χρειάζονται κατανόηση των βασικών στοιχείων των δορυφορικών επικοινωνιών και του ραδιοφάσματος. Καταρχάς, η δορυφορική επικοινωνία δεν διαφέρει από την ραδιο-επικοινωνία. Στην πραγματικότητα, και τα δύο συστήματα λειτουργούν με τον ίδιο τρόπο, χρησιμοποιώντας ηλεκτρομαγνητικά κύματα. Ο συμβατικός ραδιο-εξοπλισμός προορίζεται για επικοινωνίες πλοίου μεταξύ δύο μόνο σημείων. Εξαίρεση σε αυτόν τον τρόπο μετάδοσης, αποτελεί η περίπτωση αποστολής σήματος κινδύνου (broadcasting). Η ραδιοζεύξη έχει σαφώς ένα χαρακτηριστικό που υπήρξε περιοριστικός παράγοντας, διότι το σήμα έχει πολύ περιορισμένη εμβέλεια σε σύγκριση με τα δορυφορικά δίκτυα. Ενώ ορισμένα σήματα ραδιοζεύξης (σε χαμηλές συχνότητες), μπορούν να ανακλαστούν από την ιονόσφαιρα, επεκτείνοντας έτσι την εμβέλεια επικοινωνίας, αυτό δεν είναι δυνατό για τα σήματα υψηλών συχνοτήτων μετάδοσης - λήψης (δορυφόροι).

Ένας δορυφόρος είναι μια ενδιάμεση συσκευή σε τροχιά γύρω από τη γη, που επιτρέπει τη μετάδοση δεδομένων σε ένα πλοίο ή τη λήψη δεδομένων από ένα πλοίο, ανεξάρτητα από τις διαφορετικές θέσεις των σημείων στην επιφάνεια της υδρογείου. Το άλλο μέρος μπορεί να είναι ένα γραφείο στην ξηρά ή ένα άλλο πλοίο. Όλοι οι δορυφόροι χρησιμοποιούν μια δέσμη που είναι ένα διαμορφωμένο σήμα ηλεκτρομαγνητικών κυμάτων, που λαμβάνονται ή μεταδίδονται από τον δορυφόρο. Η μετάδοση από έναν δορυφόρο έχει ένα καθορισμένο σχέδιο και η δέσμη μπορεί να είναι ευρεία ή στενή (άνοιγμα λοβών των κεραιών εκπομπής - λήψης), καλύπτοντας μια μεγάλη ή μικρή επιφάνεια στη γη. Χρησιμοποιώντας ένα σύστημα διαφορετικών συχνοτήτων και ευθυγράμμισης των κεραιών επί του δορυφόρου, κάθε δορυφόρος μπορεί να έχει πολλές παράλληλα εκπεμπόμενες/λαμβανόμενες δέσμες εντός των οποίων συγκεντρώνεται όλη ή το μεγαλύτερο μέρος της ισχύος επικοινωνίας του δορυφόρου. Οι κεραίες στο πλοίο σπάνια είναι ακίνητες, λόγω της συνεχούς κίνησης του σκάφους, όταν βρίσκεται σε πλεύση. Επομένως, απαιτείται η κεραία επικοινωνίας (plate - πιάτο), να είναι ένας κινητός μηχανισμός και στις τρεις διαστάσεις. Η ίδια η κεραία συνήθως είναι κρυμμένη από το κάλυμμα του radome, αλλά εξετάζοντας μία δορυφορική κεραία από κοντά φαίνεται ότι συνίσταται από εξελιγμένα τμήματα εξοπλισμού με κινητήρες και γρανάζια που επιτρέπουν στην επιφάνεια της κεραίας να διατηρείται "κλειδωμένη" με περιστροφή, προς την κατεύθυνση του δορυφόρο επικοινωνίας, σχεδόν σε όλες τις συνθήκες. Τα περισσότερα συστήματα δορυφορικών επικοινωνιών είναι δομημένα έτσι ώστε, τα πλοία να υποχρεούνται να μοιράζονται τα κανάλια επιοινωνίας με άλλα πλοία. Αυτό είναι απολύτως πιο οικονομικό για τις απλές ανάγκες επικοινωνίας των πλοίων. Αυτό όμως μπορεί να καταλήξει εξαιρετικά αναποτελεσματικό, όταν απαιτούνται μεταδόσεις μεγάλου "όγκου δεδομένων" που παράγουν ορισμένοι χειριστές πλοίων. Αυτό μπορεί να ξεπεραστεί χρησιμοποιώντας μια υπηρεσία τερματικού πολύ μικρού διαφράγματος (Very Smal Aperture Technology - VSAT) [7].

Δεν χρειάζονται όλοι οι τύποι πλοίων μεγάλες ροές δεδομένων για εμπορικούς λόγους. Μεγάλο όγκο δεδομένων συχνά χρειάζονται οι επιχειρήσεις επιβατών, υπεράκτιων πλοίων καθώς και μεταφοράς εμπορευματοκιβωτίων. Για τα επιβατηγά πλοία, οι δορυφορικές επικοινωνίες δίνουν τη δυνατότητα στους επιβάτες, ώστε να χρησιμοποιούν υπολογιστές, tablet και έξυπνα τηλέφωνα, καθώς και την παροχή υπηρεσιών ψυχαγωγίας εν πλω. Στην υπεράκτια βιομηχανία επιτρέπει τη

μετάδοση ερευνητικών και άλλων δεδομένων κατά βούληση, ενώ για τα πλοία μεταφοράς εμπορευματοκιβωτίων, οι δορυφορικές επικοινωνίες καλύπτουν την ανάγκη για μεγάλο όγκο δεδομένων για σχέδια φορτο-εκφορτώσεων και εξυπηρέτησης πελατών.

3.1 Τα δίκτυα των Δορυφόρων

Τα δουφορικά συστήματα επικοινωνιών είναι διαφορετικών τύπων. Υπάρχουν τρεις κύριοι τύποι κατάταξης των δορυφόρων με βάση τα ύψη τροχιάς [7], [15]:

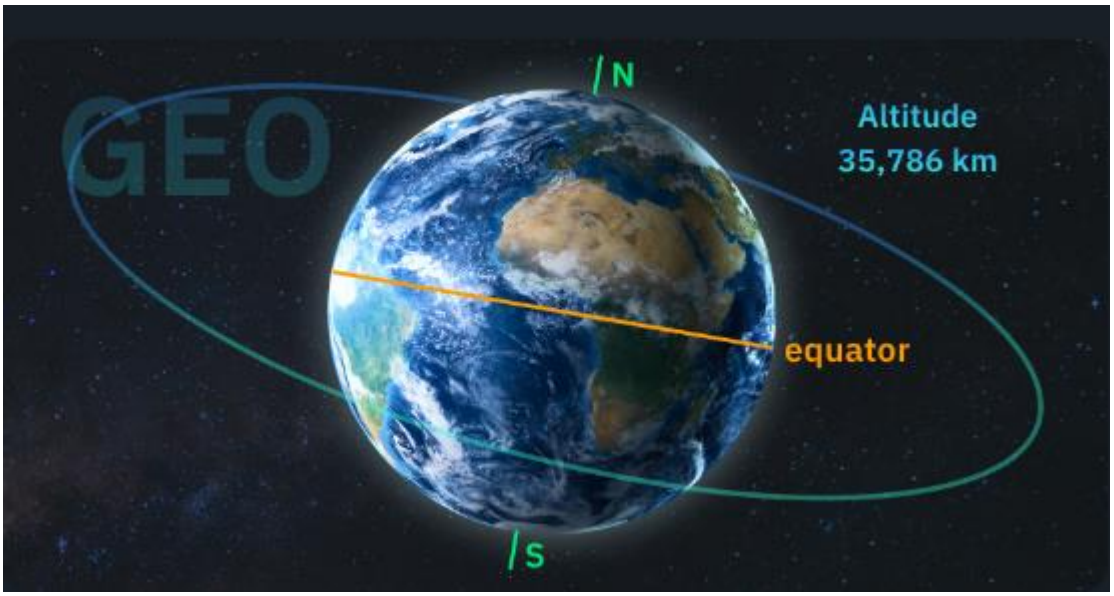
- **LEO** (Low Earth Orbit - χαμηλή γήινη τροχιά)
- **MEO** (Medium Earth Orbit - μεσαία γήινη τροχιά)
- **GEO** (Geosynchronous Equatorial Orbit - Γεωσύγχρονη Ισημερινή Τροχιά ή πιο κοινά αποκαλούμενοι γεωστατική).

Καθένας από αυτούς τους τύπους συστημάτων έχει τα πλεονεκτήματα και τα μειονεκτήματά του.

3.1.1 GEO Δίκτυα Δορυφόρων

Οι δορυφόροι αυτού του τύπου είναι ο πιο διαδεδομένος τύπος δορυφόρου. Αυτοί τοποθετούνται σε τροχιά στα 35,768 χιλιόμετρα πάνω από την επιφάνεια της γης σε ζώνη σημείων πάνω από τον ισημερινό. Καθώς η ταχύτητα και η κατεύθυνσή τους ταιριάζουν με την ταχύτητα περιστροφής της γης, οι δορυφόροι αυτοί είναι πάντα σταθεροί στον ορίζοντα, δικαιολογώντας τον όρο γεωστατικοί [15].

Οι δορυφόροι αυτοί χρησιμοποιούν κεραίες ευρείας δέσμης και καλύπτουν εκτεταμένες περιοχές. Αυτό σημαίνει ότι απαιτούνται λιγότεροι δορυφόροι για να καλύψουν την ίδια επιφάνεια στη γη, σε σχέση με άλλους τύπους δορυφόρων. Το Inmarsat [9], [10], το πρώτο εμπορικό σύστημα θαλάσσιων δορυφορικών επικοινωνιών, είναι αυτού του τύπου. Ο συγκεκριμένος πάροχος, δεν είναι ο μόνος καθώς υπάρχουν αρκετοί άλλοι πάροχοι που προσφέρουν θαλάσσιες επικοινωνίες και υπηρεσίες VSAT, χρησιμοποιώντας δορυφόρους GEO, συμπεριλαμβανομένου του Thuraya που βρίσκεται σε διαδικασία ανανέωσης του στόλου των δορυφόρων του (ο παλαιότερος από τους οποίους είναι πλέον άνω των 12 ετών).



Σχήμα 10: Παρουσίαση τροχιάς GEO δορυφόρων [15]

Το Inmarsat αρχικά λειτουργούσε με τρεις δορυφόρους πάνω από τον ισημερινό, με κάθε δορυφόρο να καλύπτει περίπου το ένα τρίτο της επιφάνειας του πλανήτη. Οι δορυφόροι αυτοί όμως δεν παρέχουν κάλυψη στις πολικές περιοχές (γεωγραφικό πλα΄τος μεγαλύτερο από 70 μοίρες). Το συγκεκριμένο δίκτυο από τη δεκαετία του 1990, διαθέτει τουλάχιστον τέσσερις δορυφόρους σε λειτουργία.

Το Inmarsat βρίσκεται επί του παρόντος στην 5η γενιά δορυφόρων του. Οι τέσσερις πρώτες γενιές περιορίστηκαν στην χρήση της L-Band, με την τελευταία γενιά να λειτουργεί στην Ka-Band. Το 2021, δύο δορυφόροι τρίτης γενιάς παρέχουν μόνο εφεδρικές υπηρεσίες θαλάσσιας ασφάλειας. Η τέταρτη γενιά (4 δορυφόροι L-Band) και η πέμπτη γενιά (5 δορυφόροι Ka-Band), παρέχουν επίσης θαλάσσια ασφάλεια και πλήρως εμπορικές επικοινωνίες πλοίων. Η αυξανόμενη ζήτηση για VSAT και η βελτιωμένη συνδεσιμότητα 5G, τόσο για εμπορική όσο και για προσωπική χρήση στη θάλασσα, οδηγεί στην ανάπτυξη σε αυτόν τον τομέα.

Οι φορείς εκμετάλλευσης δορυφόρων επενδύουν πολλά σε νέους δορυφόρους για να αυξήσουν τις θαλάσσιες δυνατότητες VSAT. Οι νέοι δορυφόροι είναι τύπου HTS (High Throughput Satellite - δορυφόρος υψηλής απόδοσης). Τον Ιούνιο του 2021, η Inmarsat ανακοίνωσε τη νέα της υπηρεσία Orchestra, η οποία θα οδηγήσει τις δορυφορικές και 5G επικοινωνίες, ένα βήμα παραπέρα. Η ORCHESTRA θα είναι μια απρόσκοπτη διαμόρφωση των δικτύων L-Band και Ka-Band, προσφέροντας επίγειο 5G, με στοχευμένη χωρητικότητα LEO και δυναμικές τεχνολογίες πλέγματος.

3.1.2 LEO Δίκτυα Δορυφόρων

Πιο κοντά στη γη είναι οι αστερισμοί (constellation) LEO δορυφόρων, που συνήθως περιλαμβάνουν πολλούς μικρούς δορυφόρους που περιφέρονται γύρω από τη γη, σε υψόμετρο μεταξύ 800 km έως 1,600 km πάνω από την επιφάνεια της. Οι ταχύτητες περιστροφής τους, ολοκληρώνουν μια περιφορά γύρω από τη γη σε λιγότερο από δύο ώρες. Αυτοί οι τύποι δορυφόρων καταστρώνουν ιδανικά δίκτυα για επικοινωνίες πολύ υψηλής ταχύτητας, προσφέροντας χαμηλή καθυστέρηση (καθυστέρηση μόλις 0.05 δευτερολέπτων) [7], [15].

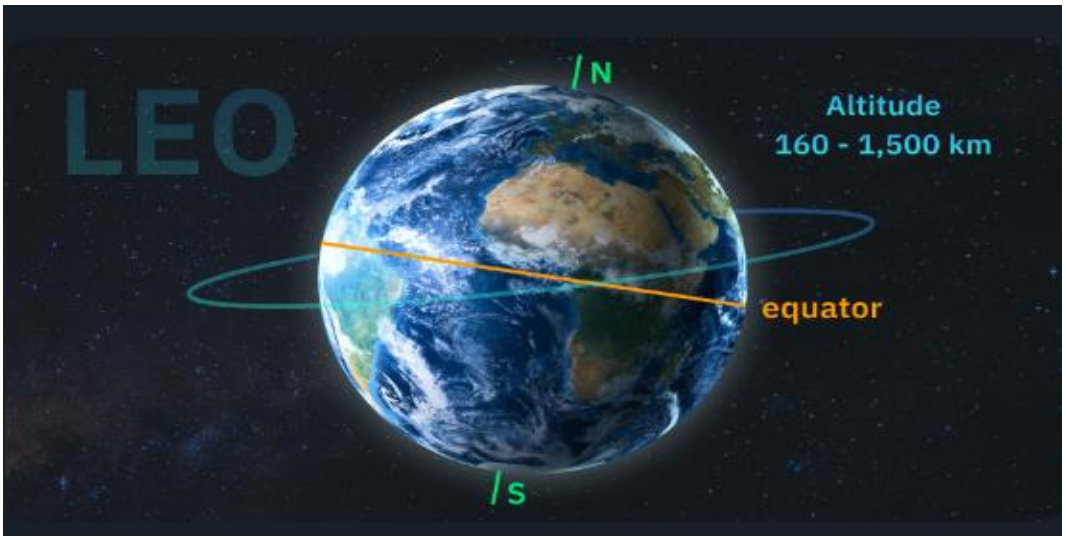
Το μικρό τους μέγεθος και η περιορισμένη κάλυψη κάθε δορυφόρου σημαίνει ότι χρειάζεται ένας αστερισμός (στόλος) που περιλαμβάνει δεκάδες ή εκατοντάδες δορυφόρους. Αυτό δίνει επίσης τη δυνατότητα για πλήρη κάλυψη της επιφάνειας της γης, συμπεριλαμβανομένων των πολικών περιοχών όπου τα συστήματα GEO δεν μπορούν να λειτουργήσουν. Οι δορυφόροι τύπου LEO είναι πολύ μικρότεροι και λιγότερο δαπανηροί σε σχέση με άλλους τύπους, καθιστώντας τους ιδανικούς για νέες υπηρεσίες.

Ο πιο γνωστός πάροχος σε αυτόν τον τομέα είναι το Iridium [9], [10]. Η εταιρεία έχει επενδύσει πολλά, για να αντικαταστήσει τους γηρασμένους δορυφόρους που απέκτησε φθηνά στις αρχές της δεκαετίας του 2000, λίγα μόλις χρόνια μετά την ίδρυση του αρχικού αστερισμού. Υπήρχαν 99 δορυφόροι στο αρχικό δίκτυο. 66 σε χρήση, άλλοι σε τροχιά ως βοηθητικοί και άλλοι χωρίς να έχουν ακόμη τεθεί σε τροχιά.

Από το 2017, το Iridium ανέπτυξε και εκτόξευσε έναν εντελώς νέο αστερισμό που περιλαμβάνει 66 ενεργούς δορυφόρους, με άλλους εννέα σε διαθεσιμότητα τροχιάς και έξι σε διαθεσιμότητα στο έδαφος. Οι νέοι δορυφόροι της επόμενης γενιάς έχουν μεγαλύτερη χωρητικότητα δεδομένων, και συνέβαλαν καθοριστικά στην αναγνώριση του Iridium ως του μόνου παρόχου υπηρεσιών GMDSS (εκτός από την Inmarsat).

Το Iridium έχει αποδεδειγμένο ιστορικό στις θαλάσσιες επικοινωνίες. Οι νέοι δορυφόροι του και το ευρυζωνικό Certus μαζί με την έγκριση GMDSS υπηρεσιών, θα διασφαλίσουν το μέλλον του. Πιθανότατα θα υπάρχει ανταγωνισμός για μελλοντικές επικοινωνίες πλοίων από το δίκτυο Starlink της Space-X. Το δίκτυο αυτό φιλοδοξούν να αποτελείται από δεκάδες χιλιάδες δορυφόρους που θα παρέχουν ευρυζωνική συνδεσιμότητα. Το δίκτυο αυτό όμως ήταν αμφιλεγόμενο για διάφορους λόγους, συμπεριλαμβανομένου του αντίκτυπου στο περιβάλλον. Αρκετοί επιστήμονες ισχυρίζονται ότι θα επηρεάσει την ορατότητα του νυχτερινού ουρανού και οι ανταγωνιστές έχουν αμφισβητήσει ανοιχτά τη νομιμότητα των αδειών που εκδόθηκαν στην Space-X [9], [10]. Όμως οι εκτοξεύσεις έχουν ξεκινήσει και περισσότεροι από 1,000 δορυφόροι τέθηκαν σε λειτουργία από το καλοκαίρι του 2021. Η αναμενόμενη πρόσθετη ζήτηση επικοινωνίας πλοίων, ως συνέπεια της αυξανόμενης ψηφιοποίησης της ναυτιλίας, καθώς επίσης και η επικείμενη άφιξη της ηλεκτρονικής πλοήγησης (είτε

είναι υποχρεωτική είτε εθελοντική), αναμένεται ήδη από τους νέους παρόχους δορυφορικών υπηρεσιών.



Σχήμα 11: Παρουσίαση τροχιάς LEO δορυφόρων [15]

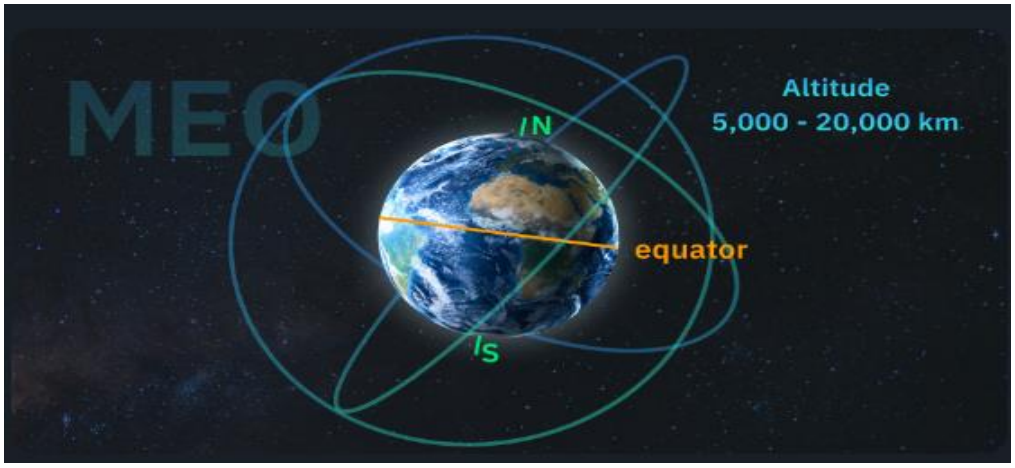
Η πρόοδος στη δορυφορική τεχνολογία σημαίνει ότι οι δορυφόροι μπορούν τώρα να είναι πολύ μικρότεροι και λιγότερο δαπανηροί από ό,τι στο παρελθόν. Οι μικρο- και νανο-δορυφόροι έχουν τη δυνατότητα να φέρουν νέες υπηρεσίες και μειωμένο κόστος για τους φορείς εκμετάλλευσης πλοίων, ειδικά σε εξειδικευμένους τομείς.

3.1.3 MEO Δίκτυα Δορυφόρων

Οι δορυφόροι τύπου MEO περιφέρονται σε χαμηλότερο υψόμετρο από τους GEO, καταλαμβάνοντας συνήθως το διάστημα μεταξύ 5,000 έως 12,000 km. Η σχετική εγγύτητά τους προς τη γη, σημαίνει ότι επιτυγχάνουν πολύ χαμηλότερη καθυστέρηση από τις μονάδες GEO, καθιστώντας τις κατάλληλες για τηλεφωνικά δίκτυα υψηλής ταχύτητας [7], [15].

Ανάλογα με το υψόμετρο τους, οι δορυφόροι MEO συνήθως ολοκληρώνουν μια περιοφρά γύρω από τη γη, μεταξύ δύο έως οκτώ ωρών. Ορισμένοι μπορεί να χρειαστούν έως και 24 ώρες για μία περιφορά. Το μικρότερο μέγεθος και η χαμηλότερη τροχιά τους σημαίνει ότι θα απαιτηθούν μεταξύ 8 έως 20 τέτοιοι δορυφόροι για την πλήρη κάλυψη της επιφάνειας της γης.

Αν και χρειάζονται περισσότεροι δορυφόροι για ένα πλήρες δίκτυο MEO κάλυψης της γης, εταιρείες όπως η SES [9], [10] με τον αστερισμό O3b και η Globalstar είναι μεταξύ εκείνων που επενδύουν σε αυτόν τον τομέα και στοχεύουν σε πελάτες ναυτιλίας.



Σχήμα 12: Παρουσίαση τροχιάς MEO δορυφόρων [15]

3.2 Καλυψη υψηλού γεωγραφικού πλάτους

Η συντριπτική πλειονότητα των εμπορικών ναυτιλιακών εμπορικών συναλλαγών διεξάγεται σε περιοχές μεταξύ του Αρκτικού και του Ανταρκτικού Κύκλου. Αυτές οι περιοχές αναλογούν σε γεωγραφικά πλάτη πάνω από 66 μοίρες Βορρά και Νότου αντίστοιχα. Αυτό είναι κοντά στο όριο των 70 μοιρών των δορυφόρων GEO της Inmarsat. Το γεγονός αυτό σημαίνει ότι οι δορυφορικές επικοινωνίες (συμπεριλαμβανομένου του GMDSS) [9], σε γεωγραφικά πλάτη πάνω από 66 μοίρες δεν είναι εγγυημένες. Αυτός είναι ένας από τους λόγους που το Iridium έγινε αποδεκτό ως πάροχος GMDSS, καθώς το δίκτυό του από LEO δορυφόρους δεν έχει περιορισμούς γεωγραφικού πλάτους και είναι διαθέσιμο απευθείας στον Βόρειο και Νότιο Πόλο.

Η θαλάσσια δραστηριότητα εντός του Αρκτικού Κύκλου αυξάνεται σταθερά με τον εντοπισμό πετρελαίου και φυσικού αερίου στην περιοχή. Σε αυτό συμβάλλει και η εγχώρια αυξανόμενη εμπορική κίνηση της Βόρειας Θαλάσσιας γύρω από τη Ρωσία, που συνδέει την Ασία και την Ευρώπη. Υπάρχει επίσης αυξανόμενη δραστηριότητα πλοίων κρουαζιέρας εντός του Αρκτικού Κύκλου [7], [15].

Κατά συνέπεια, η Inmarsat επεκτείνει το δίκτυό της GlobalXpress με ωφέλιμο φορτίο με δύο δορυφόρους που εκτοξεύτηκαν από τη Space Norway και τη θυγατρική της Space Norway HEOSAT ως μέρος της αποστολής Arctic Satellite Broadband Mission. Οι δορυφόροι που μεταφέρουν τα ωφέλιμα φορτία GX εκτοξεύτηκαν το 2022.

Το Iridium έχει από καιρό δημιουργήσει μεγάλο μέρος του πραγματικά παγκόσμιου δορυφορικού του δικτύου, και με τους νέους δορυφόρους του αστερισμού NEXT έχει προσθέσει ευρυζωνική ικανότητα με την προσφορά του Iridium Certus.

3.3 Ραδιοφάσμα επικοινωνίας των Δορυφόρων

Τόσο οι συμβατικές ραδιοζεύξεις, όσο και οι δορυφορικές επικοινωνίες, λαμβάνουν και μεταδίδουν ηλεκτρομαγνητικά σήματα ή ραδιο-κύματα. Το μήκος ή η συχνότητα των ραδιοκυμάτων ποικίλλει πάρα πολύ και για να γίνει διάκριση μεταξύ διαφορετικών μηκών κυμάτων, ομαδοποιούνται σε ζώνες εντός του ραδιοφάσματος. Οι ζώνες ονομάζονται με έναν αριθμό ή γράμμα, αλλά στους θαλάσσιους κύκλους, οι ζώνες που χρησιμοποιούνται από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers - IEEE) αναγνωρίζονται πιο συχνά με τους χαρακτηρισμούς κάθε μπάντας (band) [7], [13], [16].

Ορισμένες ζώνες (bands) έχουν ευρύτερη εξάπλωση από άλλες και κάθε μία από αυτές χρησιμοποιείται για διαφορετικό σκοπό. Οι ραδιο-επικοινωνίες σε ζώνες χαμηλής συχνότητας (LF), μεσαίας συχνότητας (MF), υψηλής συχνότητας (HF), πολύ υψηλής συχνότητας (VHF) και υπερ-υψηλών συχνοτήτων (UHF), είναι όλες σε συχνότητες κάτω από 1 GHz. Αυτή είναι η χαμηλότερη συχνότητα στο εκχωρημένο φάσμα για τις δορυφορικές επικοινωνίες και τα ραντάρ του πλοίου.

Όταν πρόκειται για εξοπλισμό επικοινωνιών σε ένα πλοίο, το VSAT απαιτεί ως επί το πλείστον μια επιλογή μεταξύ συστημάτων που λειτουργούν είτε σε ζώνες συχνοτήτων C είτε σε ζώνη συχνοτήτων Ku. Τα σκάφη με μέτρια κίνηση θα πρέπει να επιλέξουν τη ζώνη Ku-band, η οποία απαιτεί λιγότερη ισχύ και μικρότερες κεραίες. Για την χρήση της δορυφορικής σύνδεσης απαιτούνται μεγαλύτερα πιάτα (κεραίες) και περισσότερη ισχύς για το μεγαλύτερο εύρος ζώνης και την καλύτερη ποιότητα των συστημάτων C-band.

Ένα πλεονέκτημα του VSAT, είναι ότι όποια ζώνη και να επιλεγεί, ο εξοπλισμός συνήθως αποτελεί μέρος ενός πακέτου μίσθωσης με σταθερή μηνιαία πληρωμή. Το γεγονός αυτό εξασφαλίζει μεγαλύτερο έλεγχο των δαπανών επικοινωνίας. Σε πολλά σύγχρονα πλοία το επιχειρησιακό στοιχείο της χρήσης δορυφορικής επικοινωνίας επεκτείνεται γρήγορα, και τα πληρώματα αρχίζουν να αναμένουν τα είδη των υπηρεσιών email, διαδικτύου και κλήσεων, όπως ακριβώς και οι πελάτες στην ξηρά.

Μεγαλύτερο εύρος ζώνης χρησιμοποιείται τώρα για να ανταποκριθεί στην αναπτυσσόμενη αγορά χρησιμοποιώντας το Ka-Band. Η Inmarsat έχει επενδύσει σε πέντε δορυφόρους για τη χρήση ραδιοσυχνοτήτων Ka-band και την παροχή κινητών ευρυζωνικών ταχυτήτων έως 50 Mbps.

3.3.1 Η ζώνη L-Band (1 - 2 GHz)

Σχεδόν όλες οι υπηρεσίες Inmarsat και όλες οι υπηρεσίες Iridium λειτουργούν στο τμήμα του ραδιοφάσματος που χαρακτηρίζεται ως L-band. Η συγκεκριμένη ζώνη είναι πολύ στενή και σχεδόν γεμάτη από υπηρεσίες. Επειδή η συχνότητα της ζώνης είναι χαμηλή, η ζώνη L είναι ευκολότερη στην διαχείριση και επεξεργασία, απαιτώντας λιγότερο εξελιγμένο και φθηνότερο εξοπλισμό ραδιοσυχνοτήτων [16]. Λόγω του μεγαλύτερου εύρους δέσμης των κεραιών της, οι κεραίες της ζώνης δεν χρειάζεται να προσανατολιστούν ακριβώς, όπως οι ζώνες που λειτουργούν σε υψηλότερες συχνότητες. Μόνο ένα μικρό μέρος (1.3 - 1.7 GHz) της ζώνης L κατανέμεται σε επικοινωνίες δορυφορικών πλοίων στο Inmarsat για τις υπηρεσίες Fleet Broadband, Inmarsat-B και C. Το L-Band χρησιμοποιείται επίσης για δορυφόρους χαμηλής τροχιάς, στρατιωτικούς δορυφόρους και επίγειες ασύρματες συνδέσεις όπως τα κινητά τηλέφωνα GSM. Επίσης χρησιμοποιείται ως ενδιάμεση συχνότητα για δορυφορική τηλεόραση όπου τα σήματα της ζώνης Ku ή Ka μειώνονται και μετατρέπονται σε L-Band στην κεραία [7].

Αν και ο εξοπλισμός που απαιτείται για τις επικοινωνίες L-Band δεν είναι ακριβός, δεδομένου ότι δεν υπάρχει μεγάλο εύρος ζώνης διαθέσιμο στη ζώνη L, δεν παύει να αποτελεί ένα δαπανηρό προϊόν. Για το λόγο αυτό, καθώς η χρήση εφαρμογών με μεγάλο όγκο δεδομένων έχει αυξηθεί, η ναυτιλία έχει στραφεί σε πιο εξελιγμένες τεχνολογίες για εμπορικές επικοινωνίες.

3.3.2 Η ζώνη S-Band (2 - 4 GHz)

Η ζώνη χρησιμοποιείται για την λειτουργία των Radar των πλοίων.

3.3.3 Η ζώνη C-Band (4 - 8 GHz)

Η ζώνη C [7], [16] χρησιμοποιείται συνήθως από μεγάλα πλοία και ιδιαίτερα κρουαζιερόπλοια που απαιτούν αδιάλειπτη, αποκλειστική, πάντα διαθέσιμη συνδεσιμότητα, καθώς πλέουν από περιοχή σε περιοχή. Οι διαχειριστές (operators) των πλοίων συνήθως μισθώνουν ένα τμήμα του δορυφορικού εύρους ζώνης που παρέχεται στα πλοία σε μόνιμη βάση, παρέχοντας συνδέσεις με το Διαδίκτυο, τα δημόσια τηλεφωνικά δίκτυα και τη μετάδοση δεδομένων στην ξηρά. Η ζώνη C χρησιμοποιείται επίσης για επίγειες ζεύξεις μικροκυμάτων, οι οποίες μπορεί να παρουσιάσουν πρόβλημα όταν τα πλοία εισέρχονται στα λιμάνια και παρεμβάλλουν τις επίγειες ζεύξεις. Αυτό είχε ως αποτέλεσμα σοβαρούς περιορισμούς σε απόσταση 300 χιλιομέτρων από την ακτή, απαιτώντας την απενεργοποίηση αυτών των τερματικών σταθμών όταν τα πλοία πλησιάζουν στην ξηρά.

3.3.4 Η ζώνη X-Band (8 - 12 GHz)

Η ζώνη χρησιμοποιείται για την λειτουργία των Radar των πλοίων [16].

3.3.5 Η ζώνη Ku-Band (12 - 18 GHz)

Το Ku-Band αναφέρεται ως το κατώτερο τμήμα του K-Band. Το "u" προέρχεται από τον γερμανικό όρο που αναφέρεται στο "κάτω" ενώ το "a" στο Ka-Band αναφέρεται στο "πάνω" μέρος του K-Band. Το Ku-Band χρησιμοποιείται για τα περισσότερα συστήματα VSAT στα πλοία. Υπάρχει πολύ μεγαλύτερο εύρος ζώνης διαθέσιμο στο Ku-Band και είναι λιγότερο ακριβό από το C ή το L-band [16].

Το κύριο μειονέκτημα του Ku-Band είναι η εξασθένηση λόγω βροχής (fading βροχής). Το μήκος κύματος των σταγόνων βροχής είναι συγκρίσιμο με το μήκος κύματος του Ku-Band, προκαλώντας την εξασθένηση του σήματος κατά τη διάρκεια βροχοπτώσεων. Αυτό μπορεί να

ξεπεραστεί με περισσότερη ισχύ κατά τη μετάδοση. Η ακρίβεια προσανατολισμού των κεραιών είναι πολύ πιο σημαντική σε σχέση με τις L-Band Inmarsat, λόγω των στενότερων δεσμών των κεραιών. Κατά συνέπεια, οι κεραίες πρέπει να είναι πιο καλά προσανατολισμένες και τείνουν να αυξάνουν το κόστος της διασύνδεσης.

Η κάλυψη της ζώνης Ku γίνεται γενικά από τοπικές δέσμες κεραιών τύπου σποτ (spot), καλύπτοντας μεγάλες χερσαίες περιοχές με τηλεοπτική λήψη. Τα σκάφη VSAT που μετακινούνται από περιοχή σε περιοχή πρέπει να αλλάζουν δέσμες δορυφόρων, μερικές φορές χωρίς κάλυψη μεταξύ περιοχών. Στις περισσότερες περιπτώσεις, τα δορυφορικά τερματικά και τα modems μπορούν να προγραμματιστούν έτσι ώστε να αλλάζουν αυτόματα δορυφόρους. Τα μεγέθη κεραιών VSAT κυμαίνονται συνήθως από τυπική διάμετρο 1 m έως 1.5 m για λειτουργία σε περιθωριακές περιοχές και, πιο πρόσφατα, έως και 60 cm για λειτουργία ευρέως φάσματος.

3.3.6 Η ζώνη Ka-Band (26.5 - 40 GHz)

Το Ka-Band είναι μια εξαιρετικά υψηλή συχνότητα που απαιτεί μεγάλη ακρίβεια προσανατολισμού των κεραιών και εξελιγμένο εξοπλισμό RF. Όπως και το Ku-band, είναι ευαίσθητο στη βροχή. Χρησιμοποιείται συνήθως για δορυφορική τηλεόραση υψηλής ευκρίνειας. Το εύρος ζώνης Ka-Band είναι μεγάλο και μόλις εφαρμοστεί αναμένεται να είναι αρκετά φθηνό σε σύγκριση με το Ku-Band [16].

Η Inmarsat ήταν η πρώτη εταιρεία που παρείχε μια παγκόσμια υπηρεσία Ka-Band VSAT, καθώς η υπηρεσία GlobalXpress κυκλοφόρησε το 2016. Η υπηρεσία χρησιμοποιεί δορυφόρους πέμπτης γενιάς της Inmarsat. Ο πρώτος από αυτούς τέθηκε σε τροχιά το 2014 και εισήλθε σε εμπορική υπηρεσία τον Ιούλιο του 2014, τροφοδοτώντας την περιφερειακή Παγκόσμια Υπηρεσία Xpress για την Ευρώπη, την Μέση Ανατολή, την Αφρική και την Ασία [9], [10].

Καθώς γίνεται διαθέσιμο περισσότερο εύρος ζώνης από την Ka-Band, άλλοι δορυφορικοί πάροχοι προσφέρουν το Ka-Band VSAT σε πιο περιφερειακή βάση. Το ωφέλιμο φορτίο ζώνης THOR 7 HTS Ka της Telenor Satellite Broadcasting προσφέρει απόδοση 6 - 9 Gbps με έως και 25 ταυτόχρονα ενεργές δέσμες σημείων και κάλυψη στη Βόρεια Θάλασσα, τη Νορβηγική Θάλασσα, την Ερυθρά Θάλασσα, τον Περσικό Κόλπο και τη Μεσόγειο. Το Ka-Sat καλύπτει το μεγαλύτερο μέρος της Ευρώπης. Η Yahsat 1b, η NewSat Australia, η Eutelsat και η Avanti Communications παρέχουν επίσης κάλυψη στη Μέση Ανατολή, προσφέροντας στα πλοία που πλέον ασυτηρά εντός Ευρώπης και Μέσης Ανατολής μια εναλλακτική Ka-Band του Global Xpress.

Μια αξιοσημείωτη εξέλιξη είναι ότι καθώς νέες υπηρεσίες σε διαφορετικές ζώνες έρχονται σε εμπορική διαθεσιμότητα, ορισμένοι πάροχοι λειτουργούν υβριδικές υπηρεσίες που εκμεταλλεύονται το φθηνότερο δίκτυο ανά πάσα στιγμή.

Οι τεχνολογίες που απαιτούνται για τη διευκόλυνση των υβριδικών δικτύων αποτελούνται από δορυφορικές κεραίες διπλής ζώνης, κεραίες μεταγωγής Ku και Ka-Band και τη χρήση ισοδύναμης υποδομής modems/hubs.

3.4 Συστήματα Ναυτιλίας που βασίζονται σε δορυφόρους

Στη συνέχεια θα παρουσιαστούν τα συστήματα που χρησιμοποιούνται στη ναυτιλία και βασίζονται σε υπηρεσίες από τις τεχνολογίες των δορυφόρων. Μέρος της λειτουργικότητας και των χαρακτηριστικών αυτών των συστημάτων παρουσιάστηκε και στην προηγούμενη ενότητα με αναφορά στα δίκτυα χρήσης και τα συστήματα του πλοίου [1], [6], [8]. Τα βασικά συστήματα που κάνουν χρήση της δορυφορικής τεχνολογίας είναι:

- Global Navigation Satellite System (**GNSS**)
- Global Positioning System (**GPS**)
- Automatic Identification System (**AIS**)

Στη συνέχεια παρουσιάζεται αναλυτικά η λειτουργικότητα των συστημάτων καθώς και οι προκύπτουσες απειλές από ενδεχόμενες κυβερνο-επιθέσεις.

3.4.1 Το GNSS ως υποδομή κυβερνο-επίθεσης

Το GNSS είναι ο γενικός όρος για τα τέσσερα συστήματα δορυφορικής πλοήγησης με παγκόσμια κάλυψη. Συγκεκριμένα η υπηρεσία παρέχεται στο BeiDou της Κίνας, στο Galileo της Ευρωπαϊκής Ένωσης, στο Global'naya Navigazionnaya Sputnikovaya Sistema (GLONASS) της Ρωσίας, και στο Παγκόσμιο Σύστημα Εντοπισμού των Η.Π.Α. Υπάρχουν επίσης δύο περιφερειακά συστήματα, το Ινδικό περιφερειακό δορυφορικό σύστημα πλοήγησης (Indian Regional Navigation Satellite System - IRNSS), γνωστό και με την επιχειρησιακή ονομασία Navigation with Indian Constellation (NavIC), και το Ιαπωνικό Δορυφορικό σύστημα Quasi-Zenith (QZSS). Το καθένα από αυτά τα συστήματα λειτουργεί ανεξάρτητα και χωρίς αλληλο-εξάρτηση από τα υπόλοιπα συστήματα [1].

Κάθε σύστημα πλοήγησης έχει τον δικό του αστερισμό (constellation) που περιλαμβάνει 18 - 30 Δορυφόρους γήινης τροχιάς (Medium Earth Orbit- MEO). Οι δορυφόροι αυτοί λειτουργούν σε πολλά τροχιακά επίπεδα σε ένα υψόμετρο της τάξης των 12,000 - 15,000 μιλίων (περίπου 19,000 - 23,000 km). Ένας δέκτης GNSS καθορίζει τη θέση του στην επιφάνεια της γης δηλ. το γεωγραφικό πλάτος, το γεωγραφικό μήκος και το υψόμετρο θέσης. Ο εντοπισμός χρησιμοποιεί μια διαδικασία που ονομάζεται τριγωνοποίηση (trilateration), όπου η συσκευή μετρά την απόσταση της από γνωστή θέση τριτών δορυφόρων. Επειδή οι δορυφόροι κινούνται με ταχύτητα της τάξης των 2.4 μιλίων ανά δευτερόλεπτο (περίπου 4 χλμ. ανά δευτερόλεπτο), το σφάλμα της διαδικασίας εντοπισμού μπορεί να είναι έως και ένα μίλι (1.6 km). Ο δέκτης πρέπει να επικοινωνήσει με έναν τέταρτο δορυφόρο για να διορθώσει το ρολόι χρονισμού του και την απόκλιση εντοπισμού, λαμβάνοντας τον ακριβή χρονισμό. Μία χρονική απόκλιση της τάξης του ενός νανοδευτερόλεπτου (1 nsec = 10^{-9} sec) μπορεί να οδηγήσει σε ένα σφάλμα θέσης της τάξεως του ενός ποδιού (περίπου 30 cm). Η εκτίμηση θέσης του συστήματος GNSS μπορεί να είναι ακριβής σε απόκλιση της τάξεως περίπου 3 ποδιών (περίπου 1 m).

Η σημασία του GNSS για την παροχή ακριβούς χρονισμού για υποδομές ζωτικής σημασίας, δεν μπορεί να υπερεκτιμηθεί. Όλα τα τηλεπικοινωνιακά δίκτυα μεταδίδουν φωνή, βίντεο ή δεδομένα σε πολύ υψηλούς ρυθμούς μετάδοσης. Αυτά τα συστήματα δεν μπορούν να λειτουργήσουν, εκτός εάν ο αποστολέας και ο δέκτης βρίσκονται σε συγχρονισμό μετάδοσης. Ο συγχρονισμός για να επιτευχθεί χρειάζεται πολύ ακριβή χρονισμό μεταξύ του πομπού - δέκτη. Επιπλέον, το ηλεκτρικό δίκτυο, οι server που βασίζονται στο Network Time Protocol (NTP), τα οικονομικά δίκτυα, τα συστήματα μεταφορών και άλλα κρίσιμα στοιχεία υποδομής, βασίζονται στην ακρίβεια του χρονισμού που παρέχεται από το GNSS.

Αναφορές παρεμβολών του σήματος GNSS, ή απώλειας σήματος και μειωμένης ακρίβειας θέσης, αναφέρθηκαν στην Ανατολική Μεσόγειο Θάλασσα για πρώτη φορά το 2018 και συνεχίζονται μέχρι και σήμερα. Τα φαινόμενα αυτά επηρεάζουν περιοχές από την Κύπρο και τις ακτές της Αιγύπτου προς το Ισραήλ και τη Σαουδική Αραβία.Ο IMO, USCG, U.S. Maritime (MARAD), καθώς και άλλες ναυτιλιακές ομάδες έχουν εκδώσει πολλαπλές συστάσεις σχετικά με αυτά τα φαινόμενα, τα οποία φαίνεται να συνεχίζονται αμείωτα. Μερικοί ερευνητές έχουν καταλήξει ότι οι "διακοπές GNSS" είναι ένα σύνηθες φαινόμενο παντού στον κόσμο γύρω από τις εμπορικές ναυτιλιακές λωρίδες.

Η πλαστογράφηση GNSS (GNSS Spoofing) πιστεύεται ότι έπαιξε ρόλο στην κατάσχεση του STENA IMPERO στα στενά του Ορμούζ τον Ιούλιο του 2019. Το πετρελαιοφόρο, υπό σημαία UK, κατασχέθηκε όταν το Ιράν, ισχυρίστηκε ότι το πλοίο βρισκόταν σε λάθος κανάλι στην έξοδο από τα Στενά παραβιάζοντας έτσι το διεθνές δίκαιο. Ένα δορυφορικό σύστημα του πλοίου έδειξε ότι το STENA IMPERO προχωρούσε κανονικά μέσω του στενού, πριν κάνει μια ξαφνική στροφή προς τα χωρικά ύδατα του Ιράν. Επίσης, ευρέως πιστεύεται ότι το Ιράν κατέλαβε το δεξαμενόπλοιο ως αντίποινα για την κατάσχεση ενός δικό του πετρελαιοφόρου από το Ηνωμένο Βασίλειο στο Γιβραλτάρ λίγες εβδομάδες νωρίτερα λόγω των κυρώσεων της Ευρωπαϊκής Ένωσης (ΕΕ) προς το Ιράν.

3.4.2 Το GPS ως υποδομή κυβερνο-επίθεσης

Το NAVSTAR, το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS), ξεκίνησε στα τέλη της δεκαετίας του 1960, από την Πολεμική Αεροπορία και το Ναυτικό των ΗΠΑ. Ο πρώτος δορυφόρος για την εφαρμογή αυτή εκτοξεύτηκε το 1978. Σιγά σιγά, ο μη στρατιωτικός εξοπλισμός GPS έγινε διαθέσιμος για το ευρύ κοινό, τη δεκαετία του 1990. Επί του παρόντος, τον δορυφόρο διαχειρίζεται η Διαστημική Υπηρεσία των ΗΠΑ. Το GPS παρέχει υπηρεσίες εντοπισμού στρατιωτικής και πολιτικής χρήσεως, σε όλο τον κόσμο. Ο αστερισμός δορυφόρων για το GPS, χρησιμοποιεί 31 δορυφόρους, καθένας από τους οποίους περιφέρεται γύρω από τη γη, με συχνότητα περιστορφής περίπου δύο φορές την ημέρα [1], [8].

Στην αρχική του υλοποίηση, το GPS προσέφερε μια κρυπτογραφημένη υπηρεσία ακριβούς εντοπισμού (Precise Positioning Service - PPS) για στρατιωτικές εφαρμογές των ΗΠΑ και των συμμάχων τους. Επίσης παρείχε μία μη κρυπτογραφημένη υπηρεσία εντοπισμού θέσης (Standard Positioning System - SPS) για άλλες μη στρατιωτικές εφαρμογές. Το SPS παρείχε ελαφρώς μικρότερη ακρίβεια εντοπισμού, σε σχέση με το PPS. Αυτό γινόταν με την εισαγωγή ελεγχόμενου σφάλματος χρονισμού. Από το 2000, η ακρίβεια γεωεντοπισμού του GPS και για στρατιωτικές αλλά και για πολιτικές εφαρμογές ταυτίστηκε. Το GPS υποφέρει από δύο τύπους κυβερνο-επιθέσεων:

- GPS Jamming
- GPS Spoofing

Jamming είναι η σκόπιμη διαδικασία μετάδοσης σήματος ισχύος στη ζώνη συχνοτήτων που χρησιμοποιείται για την ασύρματη ζεύξη μίας υπηρεσίας. Αυτό έχει ως αποτέλεσμα, να "κατακλύζει" τον δέκτη του σήματος της υπηρεσίας με έντονη ισχύ, με σκοπό να "σκεπάσει" το μεταδιδόμενο σήμα που έπρεπε να ληφθεί. Με τον τρόπο αυτό είναι δυνατόν να καταστήσει αδύνατη την λήψη και την εφαρμογή της υπηρεσίας.

Το GPS jamming, το οποίο είναι ένας χαμηλού κόστους μηχανισμός επίθεσης για το GPS, μπορεί να έχει σοβαρές επιπτώσεις. Λαμβάνοντας υπόψη ότι οι καπετάνιοι των πλοίων και οι πλοηγοί βασίζονται στη λειτουργία του GPS για να κάνουν επιτυχή διέλευση όλο και μεγαλύτερων πλοίων μέσω στενών περασμάτων ναυτιλίας (όπως το στενό του Βοσπόρου, το κανάλι του Παναμά, τα Στενά του Γιβραλτάρ, το Στενό του Ορμούζ, το Στενό της Μαλάκας ή τη Διώρυγα του Σουέζ), τότε το πρόβλημα που μπορεί να δημιουργηθεί από μία κυβερνο-επίθεση και απώλεια ακριβούς στίγματος από το GPS, μπορεί να οδηγήσει σε ατυχήματα μεγάλης κλίμακας.Επιπλέον οι οικονομικές επιπτώσεις από μια πιθανή παρεμπόδιση διέλευσης πλοών από κάποιο στενό μεγάλης εμπορικής κινήσης όπως η Διώρυγα του Σουέζ λόγω πχ προσάραξης αποτέλεσμα GPS jamming θα ήταν πολύ μεγάλες.

Είναι δυνατό για τους δέκτες GPS να ανιχνεύουν προσπάθειες παρεμβολής σήματος (jamming). Πολλά προϊόντα GPS περιλαμβάνουν αυτή τη δυνατότητα. Αυτά τα προϊόντα μπορούν, σε πολλές περιπτώσεις, να αγνοήσουν (βάσει της κατεύθυνσής του) ή χρησιμοποιώντας AI να φιλτράρουν το μπλοκαρισμένο σήμα και να ανακτήσουν το αρχικό σήμα GPS. Ίσως ο καλύτερος μετριασμός κατά της παρεμβολής, είναι η χρήση δεκτών GNSS που χρησιμοποιούν πολλαπλούς αστερισμούς δορυφόρων, όπως το GPS και το GLONASS, χρησιμοποιώντας περισσότερους από έναν δορυφόρους. Έτσι το σύστημα πλοήγησης, όχι μόνο παρέχει πλεονασμό, σε περίπτωση που ένα σύστημα αποτύχει, αλλά επίσης δίνει τη δυνατότητα διασταύρωσης της ακρίβειας από πολλαπλά συστήματα κατά τον εντοπισμό θέσης.

Spoofing (πλαστογράφηση) είναι η διαδικασία σκόπιμης μετάδοσης λανθασμένων δεδομένων, με σκοπό να αλλοιωθεί η ακρίβεια εφαρμογής μίας υπηρεσίας. Το spoofing δεν καταργεί το δίαυλο επικοινωνίας του GPS όπως το jamming, αλλά μεταδίδει σκόπιμα λανθασμένα σήματα εντοπισμού, με σκοπό την παραπλάνηση και τον εντοπισμό λανθασμένων θέσεων για τον λήπτη της υπηρεσίας.

Η πλαστογράφηση περιλαμβάνει γενικά ένα τρίτο μέρος που χρησιμοποιεί εξειδικευμένο εξοπλισμό, για να παράγει ψευδή σήματα πλοήγησης GPS με στόχο να παραπλανήσουν μια συσκευή λήψης. Το Meaconing (ή το masking beaconing) είναι μια μορφή πλαστογράφησης, όπου κάποιος τρίτος λαμβάνει και επαναμεταδίδει τα νόμιμα σήματα πλοήγησης στη σωστή συχνότητα, αλλά σε μεγαλύτερη ισχύ από τα αρχικά σήματα στα οποία ο δέκτης κλειδώνει. Σε αυτήν την φάση ο δέκτης GPS προτιμά με βάση τα πρωτόκολλα λειτουργίας του να κλειδώσει στο σταθμό μετάδοσης που εμφανίζει το ισχυρότερο σήμα. Έτσι ο επιτιθέμενος αφού κλειδώσει το GPS "στόχο", αρχίζει να του μεταδίδει ψευδείς πληροφορίες θέσεως.

Τα περιστατικά πλαστών σημάτων GPS έχουν αυξηθεί σημαντικά τα τελευταία χρόνια, ώστε αυτή η τεχνική κυβερνο-επίθεσης να έχει καταστεί στρατηγικό όπλο σύγκρουσης και μεγάλη απειλή για την εμπορική ναυτιλία. Το πρώτο περιστατικό πλαστογράφησης GPS με μεγάλη δημοσιότητα, συνέβη στη Μεσόγειο Θάλασσα το 2013. Αυτό το περιστατικό προκλήθηκε και μελετήθηκε από ερευνητές από το Πανεπιστήμιο του Τέξας στο Όστιν (UT), και προκάλεσε στη θαλαμηγό WHITE ROSE OF DRACHS ύψους 213 ποδιών (περίπου 65μ), αλλαγή της πορείας της, εν αγνοία του πληρώματος. Η ομάδα χρησιμοποίησε εμπορικά προϊόντα για την κατασκευή της συσκευής πλαστογράφησης. Το γεγονός ξεκίνησε με τη μετάδοση σημάτων GPS πολύ χαμηλής ισχύος. ενώ στη συνέχεια η ισχύς του σήματος αυξήθηκε αργά έως ότου ο δέκτης του πλοίου να "κλειδώσει" στο νέο σήμα και να σταματήσει να παρακολουθεί το νόμιμο. Τα σήματα της ομάδας UT έκαναν να φαίνεται ότι το WHITE ROSE είχε παρασυρθεί τρεις μοίρες προς τα αριστερά (μια μετατόπιση πολύ μικρή που το πλήρωμα υπέθεσε ότι οφειλόταν στον αέρα και τα θαλάσσια ρεύματα). Το πλήρωμα μετατόπισε το σκάφος ελαφρώς προς τα δεξιά, κάτι που τελικά τους πήρε περίπου 3,300 πόδια μετακίνησης (1 χλμ) εκτός πορείας.

Μια ποικιλία μεθόδων μπορούν να χρησιμοποιηθούν για τον εντοπισμό πλαστογράφησης των συστημάτων GPS/GNSS. Ορισμένες από αυτές είναι ήδη ενσωματωμένες σε ορισμένα προϊόντα GNSS. Μια μέθοδος που χρησιμοποιείται για τον εντοπισμό της πλαστογράφησης, είναι η παρακολούθηση της παραμόρφωσης του σήματος που εμφανίζεται τη στιγμή που το ψεύτικο σήμα υπερισχύει σε σχέση με το νόμιμο σήμα. Μια δεύτερη μέθοδος, ανιχνεύει το γεγονός ότι το ψευδές σήμα προέρχεται από διαφορετική κατεύθυνση σε σχέση με τα νόμιμα σήματα. Στην πραγματικότητα, ενώ τα σήματα GNSS απαιτούν επικοινωνία με τέσσερις δορυφόρους, ένα ψεύτικο σήμα GPS προέρχεται γενικά από μία και μοναδική πηγή. Μια τρίτη μέθοδος χρησιμοποιεί μία τεχνική όπου η μονάδα GPS συσχετίζει το κρυπτογραφημένο σήμα για να διασφαλίσει ότι είναι αυθεντικό. Παρόλο που μία μονάδα δεν μπορεί να διαβάσει το κρυπτογραφημένο σήμα, τουλάχιστον μπορεί να διασφαλίσει ότι είναι παρόν και αυθεντικό. Μια άλλη προστασία, είναι η χρήση ενός δέκτη που μπορεί να παρακολουθεί πολλαπλούς αστερισμούς GNSS ταυτόχρονα.

Το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ, έχει αναπτύξει έναν εντοπισμό θέσης, για το Πρόγραμμα πλοήγησης και χρονισμού (Positioning Navigation and Timing - PNT) με στόχο την προστασία από Spoofing GNSS/GPS. Το πρόγραμμα τους περιλαμβάνει την PNT Integrity Library, σε επεκτάσιμο πλαίσιο για ανίχνευση παραποίησης PNT που βασίζεται σε GNSS. Το πρότυπο αυτό προορίζεται για χρήση από κατασκευαστές δεκτών GNSS και διακομιστών χρονισμού που βασίζονται σε GNSS υπηρεσίες, για την επαλήθευση της ακεραιότητας των ληφθέντων δεδομένων GNSS και των σημάτων εμβέλειας. Επίσης, το Epsilon Algorithm Suite, είναι ένα σύνολο αλγορίθμων κατά της πλαστογράφησης. Τον Μάιο του 2021, η IEEE ενέκρινε την P1952 ομάδα εργασίας για την ανάπτυξη προτύπων για ανθεκτικό εξοπλισμό χρηστών PNT. Δορυφορικά συστήματα αύξησης της ακρίβειας του PNT, που χρησιμοποιούν σε μεγάλο βαθμό δορυφόρους LEO βρίσκονται υπό ανάπτυξη για να συμπληρώσουν το GPS. Οι δορυφόροι LEO, ειδικότερα, μπορούν να παρέχουν σήματα μεγαλύτερης ακρίβειας και μεγαλύτερης ισχύος.

3.4.3 Το AIS ως υποδομή κυβερνο-επίθεσης

Το AIS είναι ένα σύστημα που βασίζεται σε ραδιοζεύξη συχνοτήτων VHF, με εμβέλεια λειτουργίας σε ακτίνα 10 - 20 ναυτικών μιλίων (nm), και παρέχει την ικανότητα των πλοίων στη θάλασσα, ώστε να αναγνωρίζουν το ένα την παρουσία του άλλου. Τα μηνύματα AIS [1], [8] που μεταδίδονται, περιγράφονται στο πρότυπο από την International Telecommunication Union RadioCommunication Sector (ITU-R) και βασίζονται στο NMEA 0183. Η δεύτερη γενιά των συσκευών AIS βασίζεται σε χρήση δορυφορικής τεχνολογίας.

Ο σκοπός του AIS είναι να δώσει στις ναυτιλιακές αρχές, τη δυνατότητα να εντοπίζουν και να παρακολουθούν τα πλοία και το φορτίο του, στην περιοχή ευθύνης τους, καθώς και για πλοία και παράκτιους σταθμούς για ανταλλαγή δεδομένων πλοήγησης, μετεωρολογικών, ασφάλειας καθώς και άλλες πληροφορίες σχετικά με το σκάφος.

Το AIS σχεδιάστηκε τη δεκαετία του 1990 και εγκρίθηκε διεθνώς στη Διεθνή Σύμβαση του 2002 για την Ασφάλεια ζωής στη θάλασσα (Safety of Life at Sea - SOLAS), χωρίς να περιλαμβάνει θέματα προστασίας από ενεργές επιθέσεις.

Η συμφωνία SOLAS έχει ευρύ πεδίο εφαρμογής και καλύπτει μια σειρά από κρίσιμα θέματα που συνδέονται με την επίγνωση της θαλάσσιας κατάστασης. Η Ασφάλεια περί Ναυτιλίας της συμφωνίας SOLAS, καθορίζει τους απαιτούμενους τύπους πλοίων για να μεταφέρει πομποδέκτες

AIS κλάσης Α, και περιλαμβάνει πλοία 300 και πλέον τόνων που ταξιδεύουν διεθνώς, εμπορικά πλοία μήκους άνω των 64 ποδών (περίπου 19.5μ) και μηχανοκίνητα πλοία πιστοποιημένα να μεταφέρουν περισσότερα από 150 επιβάτες. Τα στρατιωτικά σκάφη εξαιρούνται από την συγκεκριμένα απαίτηση για τη μετάδοση πληροφοριών AIS, αν και τα περισσότερα σύγχρονα πολεμικά πλοία διαθέτουν και τα δύο (δημόσια και κρυπτογραφημένη δυνατότητα για αποστολή μηνυμάτων AIS).

Οι πομποδέκτες AIS κατηγορίας Β, χρησιμοποιούνται σε μεγάλα γιοτ, μικρά αλιευτικά, καθώς και άλλα εμπορικά ή προσωπικά σκάφη. Σε άλλα πλοία που μεταφέρουν Εξοπλισμό AIS δεν υπάρχει νομική απαίτηση για κάτι τέτοιο. Συσκευές κατηγορίας Α γενικά μεταδίδουν πιο λεπτομερείς πληροφορίες με μεγαλύτερη ισχύ από ό,τι οι συσκευές κλάσεως Β, συμπεριλαμβανομένου του ονόματος του πλοίου, του αριθμού εγγραφής του Διεθνούς Ναυτιλιακού Οργανισμού (IMO), της Ταυτότητας Mobile Maritime Service Identity (MMSI), διαστάσεις, γεωγραφικό πλάτος και μήκος, πορεία, κατεύθυνση, ταχύτητα στροφής, προορισμός, τύπος φορτίου και επιχειρησιακή κατάσταση. Οι απαιτήσεις AIS στις Η.Π.Α καθορίζονται στον Κώδικα Ομοσπονδιακών Κανονισμών των Ηνωμένων Πολιτειών (CFR).

Το AIS σήμερα είναι ένα ουσιαστικό μέρος του ολοκληρωμένου συστήματος πλοήγησης ενός πλοίου, που χρησιμοποιείται κυρίως για την επίγνωση της κατάστασης και την αποφυγή σύγκρουσης μεταξύ σκαφών. Οι συσκευές AIS κλάσης Β λαμβάνουν πληροφορίες θέσης από το GNSS του πλοίου και επομένως εξαρτώνται σε μεγάλο βαθμό από την ακεραιότητα του συστήματος εντοπισμού θέσης. Το AIS επίσης χρησιμοποιείται ευρέως από λιμάνια, υπηρεσίες διαχείρισης κυκλοφορίας πλοίων και υπηρεσίες ακτοπλοϊκής επιτήρησης.

Υπάρχει μια σειρά από γνωστά "τρωτά σημεία" με τα πρωτόκολλα του AIS:

- Έλλειψη γεωγραφικής επικύρωσης: Είναι δυνατό για μια συσκευή να μεταδίδει ένα μήνυμα AIS από μια τοποθεσία, ενώ η συσκευή μπορεί να βρίσκεται σε άλλη τοποθεσία.
- Έλλειψη πληροφοριών χρονικού καθορισμού (timestamp): Οι μεταδόσεις AIS δεν περιλαμβάνουν ημερομηνία και ώρα. Επομένως, ένα έγκυρο μήνυμα AIS μπορεί σκόπιμα να περιλαμβάνει λανθασμένη ώρα, παραπλανώντας για την παρουσία του πλοίου στη δεδομένη χρονική στιγμή.
- Έλλειψη ελέγχου ταυτότητας μηνύματος: Χωρίς μηχανισμό ελέγχου ταυτότητας του αποστολέα ενός μηνύματος, οποιουδήποτε έχει τη δυνατότητα μετάδοσης ενός μηνύματος AIS, και μπορεί να μιμηθεί οποιαδήποτε άλλη συσκευή AIS.
- Έλλειψη ακεραιότητας μηνύματος: Δεν υπάρχει μηχανισμός που να διασφαλίζει ότι τα μηνύματα AIS στέλνουν σωστές και έγκυρες πληροφορίες. Ενα αλιευτικό σκάφος θα μπορούσε για παράδειγμα, να παρουσιάζεται ως διαφορετικού τύπου σκάφος.

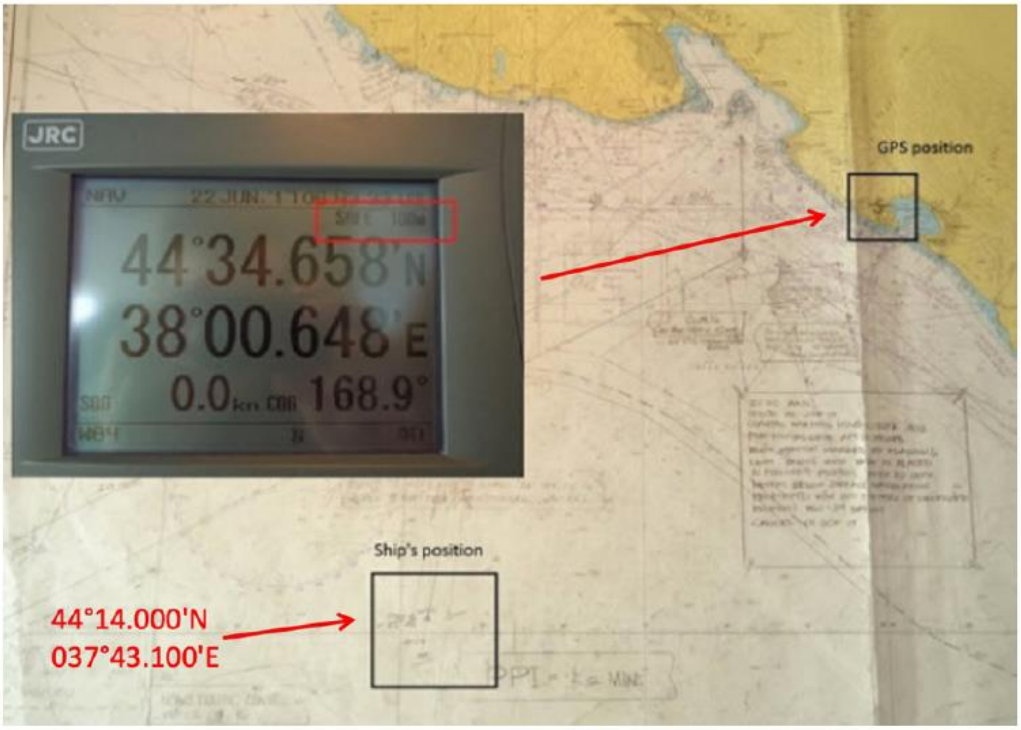
Προφανώς τα παραπάνω "τρωτά σημεία" είναι εξαιρετικά σημαντικά στα πλαίσια μίας κυβερνο-επίθεσης, διότι ένας επιτιθέμενος μπορεί να τα εκμεταλλευτεί για να "καλύψει - εξαφανίσει" ένα σκάφος, δίνοντας τα χαρακτηριστικά που αυτός επιθυμεί στην περιγραφή και την τοποθεσία του.

Αυτά τα τρωτά σημεία θα επέτρεπαν σε οποιονδήποτε να δημιουργήσει σκόπιμα ψεύτικα μηνύματα για να παραπλανήσουν με την παρουσία ενός σκάφος φαντάσματος (δηλαδή, ανύπαρκτο), ζητώντας βοήθεια για την πλοήγηση (ATONs), ή να μπερδέψει την κατάσταση των νόμιμων σκαφών, να ενεργοποιήσει ψευδείς ειδοποιήσεις Situational Awareness - SAR ή να επηρεάσει το πλησιέστερο σημείο προσέγγισης Closest Point-of-Approach CPA ή να προκαλέσει την αποστολή ψευδών πληροφοριών καιρού ή πλοήγησης. Κάθε ένα από αυτά τα σενάρια θα μπορούσε πιθανόν να προκαλέσει ένα άλλο σκάφος να αλλάξει την πορεία του. Όλοι οι πομποδέκτες AIS εκπέμπουν σε δημόσιες συχνότητες VHF. Επομένως ο καθένας μπορεί να "ακούει" τον ραδιοδίαυλο και, στην πραγματικότητα, οποιοσδήποτε θα μπορούσε να μπλοκάρει τα σήματα AIS, προκαλώντας αποτελεσματικά μια επίθεση DoS που στη συνέχεια "σκοτεινιάζει" μια μικρή περιοχή του δικτύου AIS. Αυτές οι επιθέσεις ενεργοποιούνται από εργαλεία λογισμικού που μπορούν να δημιουργήσουν και ερμηνεύουν μηνύματα AIS και είναι συνήθως εμπορικά διαθέσιμα στο Διαδίκτυο.

Οι κυβερνο-απειλές μπορεί να γίνουν ακόμη οξύτερες, στην περίπτωση όπου συνδυαστούν παραπάνω από μία επιθέσεις ταυτόχρονα σε πολλαπλά συστήματα (π.χ. AIS και GPS ταυτόχρονο Spoofing) [1].

Το Πανεπιστήμιο του Τέξας έκανε μία θεωρητική επίδειξη πλαστογράφησης GPS το 2013, με τη συμμετοχή 20 πλοίων στη Μαύρη Θάλασσα. Σε αυτό το περιστατικό, η πλοίαρχος του ATRIA,

ενός τάνκερ 37,500 τόνων στα ανοιχτά του ρωσικού λιμανιού Novorossiysk, ανέφερε ότι το GPS του πλοίου έδειξε ότι το πλοίο ήταν 20 nm (περίπου 37km) μακριά από το Αεροδρόμιο του Gelendzhik. Τα συστήματα πλοήγησης από τουλάχιστον 20 πλοία κοντά τους, έδειξαν ότι βρίσκονταν όλοι στην ίδια τοποθεσία. Κατά συνέπεια, οι "συναγερμοί σύγκρουσης" σε πολλά σκάφη, έδειχναν επικείμενες συγκρούσεις.



Σχήμα 13: Οθόνη του συστήματος GPS του πλοίου ATRIA κατά την φάση επίθεσης GPS spoofing [1]

Υπήρχαν ευρέως εικασίες εκείνη την εποχή, ότι το συμβάν πλαστογράφησης στη Μαύρη Θάλασσα συνέβη λόγω του ρωσικού ηλεκτρονικού πολέμου. Μεταγενέστερες αναφορές έδειξαν ότι αυτό το περιστατικό ήταν μέρος μιας ευρύτερης παρέμβασης GNSS στα ρωσικά ύδατα, οπότε παρατηρήθηκε τοποθέτηση πλοίων σε πολλά αεροδρόμια, συμπεριλαμβανομένων του Σότσι, της Αγίας Πετρούπολης και του Βλαδιβοστόκ.

3.4.4 Παράλληλες Κυβερνο-επιθέσεις σε δορυφορικά συστήματα

Η πλαστογράφηση των συστημάτων GPS και AIS έχουν εξελιχθεί σε σοβαρότητα, πολυπλοκότητα και επικινδυνότητα από τα πρώυα συμβάντα του 2017. Το πρώτο από μια νέα τάση ήταν ένα περιστατικό, τον Ιούλιο του 2019, στο Λιμάνι της Σαγκάης. Σύμφωνα με αναφορές, το πλοίο μεταφοράς εμπορευματοκιβωτίων μήκους 700 ποδιών (περίπου 213μ), MANUKAI βρισκόταν στον ποταμό Χουανγκπού κατευθυνόμενο προς τη θέση που είχε προγραμματισθεί. Ο πλοίαρχος του πλοίου ανέφερε ότι το AIS έδειξε ένα άλλο σκάφος να κινείται με 7 κόμβους (kn) στο ίδιο κανάλι. Το άλλο πλοίο στη συνέχεια εξαφανίστηκε ξαφνικά και, μετά από σύντομο χρονικό διάστημα, εμφανίστηκε ξανά στην αποβάθρα. Αυτό το μοτίβο αργότερα επαναλήφθηκε, με το άλλο πλοίο να εμφανίζεται στην οθόνη, να κινείται στο κανάλι με 5 kn, και μετά με 2 kn, στη συνέχεια να εξαφανίζεται τελείως και μετά να επανεμφανίζεται πίσω στην αποβάθρα. Ο πλοίαρχος του MANUKAI μπόρεσε να εντοπίσει οπτικά το άλλο σκάφος και επιβεβαιώστε ότι ουδέποτε είχε φύγει από την αποβάθρα του λιμανιού. Το MANUKAI έφτασε στο καθορισμένο αγκυροβόλιο, οπότε οι δέκτες GPS και όλα τα συστήματα πλοήγησης ξαφνικά έπαψαν να λειτουργούν και ο πλοίαρχος δεν μπόρεσε να βρει μια σαφή εξήγηση για το συμβάν [1], [8].

Πρόσθετη ανάλυση των δεδομένων AIS έδειξε ότι παρόμοιο περιστατικό πλαστογράφησης GPS είχε συμβεί στην περιοχή της Σαγκάης για τουλάχιστον ένα χρόνο πριν από το περιστατικό του MANUKAI. Εκείνη τη χρονιά, η ένταση και το πλήθος των συμβάντων πλαστογράφησης GPS

αυξήθηκε, φτάνοντας στο μέγιστο των σχεδόν 300 συμβάντων την ημέρα της εκδήλωσης του περιστατικού που αφορούσε στο MANUKAI. Σε άλλο περιστατικό που αναφέρθηκε στην προηγούμενη ενότητα, μία ρωσική πλαστογράφηση, τοποθέτησε όλα τα πληγέντα πλοία μαζί σε ένα και μοναδικό σημείο. Στη Σαγκάη, τα πλαστογραφημένα πλοία φάνηκαν να μετανικούνται ασυνεχώς ("χοροπήδημα" στο χάρτη) σε τοποθεσίες που έμοιαζαν να συγκεντρώνονται σε μεγάλους κύκλους, κυρίως στην ανατολική όχθη του ποταμού Huangpu. Μια ανάλυση των δεδομένων έδιεξε σχεδόν καθημερινές επιθέσεις πλαστογράφησης που επηρεάζουν τα πλοία του Huangpu Maritime Safety Administration (MSA). Η θέση ενός σκάφους στην περιοχή παραποιήθηκε 394 φορές σε ένα εννιάμηνο.

Αυτά τα περιστατικά πλαστογράφησης GPS και AIS δεν περιορίζονται σε καμία περίπτωση στην Κίνα και τη Ρωσία, και σίγουρα δεν δείχνουν σημάδια μείωσης. Ο λεγόμενος "κύκλος πλαστογράφηση του GPS" έχει αναφερθεί στο Ιράν και σε άλλες τοποθεσίες στον κόσμο. Σε μια ανησυχητική κλιμάκωση επιθέσεων σε GPS και AIS, αρκετά σκάφη το 2018 και το 2019 ανέφεραν ότι τα δεδομένα AIS τους έδειξαν ότι ταξίδευαν σε κύκλο στην περιοχή του Point Reyes, ακριβώς βόρεια του Σαν Φρανσίσκο, αν και οι πραγματικές τους θέσεις επιβεβαιώθηκε ότι βρίσκονται σε διαφορετικές τοποθεσίες στο Ανατολικό ημισφαίριο, χιλιάδες μίλια μακριά .

Σχήμα 14: GPS spoofing στην περιοχή του ποταμού Huangpu [1]

3.5 Εργαλεία των Κυβερνο-επιθέσεων στα δορυφορικά συστήματα και Στρατηγικές αντιμετώπισης τους

Στις προηγούμενες ενότητες παρουσιάστηκαν τα εργαλεία των κυβερνο-επιθέσεων που αφορούσαν στα δορυφορικά συστήματα που χρησιμοποιούνται στη ναυτιλία. Οι επιθέσεις διακρίνουν δύο μοτίβα δράσης:

- Jamming
- Spoofing

Στις επιθέσεις τύπου jamming, όπως διευκρίνηστηκε και στην αντίστοιχη ενότητα, οι επιτιθέμενοι προσπαθούν να θέσουν εκτός λειτουργίας την λήψη ενός σήματος φέροντος (carrier) μίας υπηρεσίας, με παράλληλη εκπομπή σήματος μεγαλύτερης ισχύος στην ίδια συχνότητα. Αυτό έχει ως αποτέλεσμα, το δορυφορικό σύστημα του πλοίου να καθίσταται ανενεργό, και μη ικανό για την παροχή της υπηρεσίας. Οι επιθέσεις αυτού του τύπου απαιτούν μεγάλα ποσά ισχύος, τα οποία μπορεί να επιτευχθούν, είτε από γειτονικά πλοία είτε από επίγειους σταθμούς στην ακτή, έτσι ώστε να μπορούν να είναι επιτυχείς για μεγάλο χρονικό διάστημα, δεδομένου ότι τα κινούμενα πλοία αλλάζουν, λόγω της ρώτας τους, δορυφόρο κάλυψης. Εντούτοις όμως αυτές οι επιθέσεις μπορεί να είναι επιτυχείς και συντηρούμενες κατά περιοχές με ειδικά χαρακτηριστικά (π.χ. ζώνη εχθροπραξιών γειτονικών χωρων).

Η άλλη μορφή επίθεσης, η πλαστογράφηση (spoofing) είναι γενικά χειρότερης μορφής, δεδομένου ότι οι επιτιθέμενοι εκπέμπουν στη ίδια συχνότητα μίας υπηρεσίας, με στόχο να "παγιδεύσουν" τους πομπο-δέκτες των πλοίων, οι οποίοι λόγω της μεγαλύτερης ισχύος του σήματος

των επιτιθέμενων, "κλειδώνουν" σε αυτούς. Τότε έχουν την δυνατότητα να μεταδώσουν ψευδή στοιχεία, για πιθανή θέση, και τροχιά πλεύσης των πλοίων [2]. Επομένως, οι επιθέσεις τύπου spoofing, οι οποίες μπορεί να είναι συνδυαστικές σε παραπάνω από ένα δορυφορικά συστήματα παράλληλα, μπορεί να προκαλέσουν σημαντικούς κινδύνους και ανασφάλειες για την πλεύση των πλοίων.

Δεδομένου ότι οι παρεχόμενες υπηρεσίες γίνονται με χρήση τεχνολογίας δορυφόρων, μία σημαντική λύση στο τεχνολογικό πεδίο, είναι η χρήση πρωτοκόλλων κρυπτογράφησης, τα οποία δυσκολεύουν τις επιδράσεις τύπου spoofing, στα μεταδιδόμενα σήματα. Από πλευράς εξοπλισμού, θα πρέπει να σημειωθεί, ότι ο απαιτούμενος εξοπλισμός είναι εύκολα προσβάσιμος στην αγορά μέσω του διαδικτύου, γεγονός που καθιστά πιο εύκολη την συγκρότηση ομάδων κυβερνο-επιθέσεων. Μία άλλη λύση, παρά το καθορισμένο των συχνοτήτων των καναλιών επικοινωνίας, είναι η χρήση τεχνικών εξαπλωμένου φάσματος με αναπήδηση συχνότητας (spread spectrum modulations and frequency hopping techniques) [14], για την δυσκολία εντοπισμού των σημάτων επικοινωνίας.

4 Κυβερνο-Επιθέσεις, Απειλές στα Αυτοματοποιημένα Πλοία. Δράσεις Αντιμετώπισης τους

Η φυσική εξέλιξη των έξυπνων συσκευών, η τεχνητή νοημοσύνη, η μηχανική μάθηση, η ικανότητα χειρισμού μεγάλου όγκου δεδομένων από επεξεργαστικά συστήματα (Big Data) και το Internet of Things - IoT, είναι νέες ψηφιακές τεχνολογίες, που επεκτείνουν την λειτουργία των αυτόνομων και αυτοματοποιημένων συστημάτων. Τα συστήματα που βασίζονται στις παραπάνω τεχνολογίες μπορεί να χρησιμοποιηθούν για την ανάπτυξη εφαρμογών στην στεριά, στην θάλασσα και στο διάστημα, επηρεάζοντας τη λειτουργικότητα και διαχειρισιμότητα των συσκευών/σκαφών. Αυτή η ενότητα περιγράφει το μέλλον που ανοίγεται για το MTS λόγω της ανάπτυξης της ναυτιλιακής τεχνολογίας, της πληροφορικής και των επικοινωνιών[1].

Η έννοια του αυτόνομου (autonomous) στη ναυτιλία, αφορά την πλήρως αυτοματοποιημένη λειτουργία των συστημάτων των πλοίων. Τα πλοία αυτά θα βασίζονται στις δυνατότητες επικοινωνίας και ελέγχου σε οποιοδήποτε σημείο της επιφάνειας της γης, οποιαδήποτε χρονική στιγμή. Μια κοινή ταξινόμηση της κλιμάκωσης των αυτόνομων διεργασιών, είναι η χρήση μιας τροποποιημένης έκδοσης της ταξινόμησης για τα αυτόνομα αυτοκίνητα, από την Κονότητα των Μηχανικών Αυτοκινήτων (Society of Automotive Engineers - SAE), όπως παρουσιάζεται στον πίνακα που ακολουθεί:

Πίνακας 2: Ταξινόμηση της Αυτονομίας Συστημάτων Αυτοκινήτων

Επίπεδο Αυτονομίας	Αυτονομία Συστήματος
0	No autonomy
1	Minimal Crew Required
2	Partial autonomation; local crew for simple tasks
3	Conditional autonomy, potential intervention by local crew
4	High autonomy, mostly self-running
5	Complete autonomy

Όπως υποδηλώνει και ο πίνακας, η αυτονομία μπορεί να κυμαίνεται από πλοίο με τηλεκατευθυνόμενο σκάφος ή σε τηλεκατευθυνόμενο σκάφος με πλήρωμα επιφυλακής στα χειριστήρια ή σε ένα πλήρως αυτόνομο πλοίο.

Η εμπορική ναυτιλιακή βιομηχανία επιδιώκει ενεργά την έρευνα στον τομέα των αυτόνομων πλοίων για διάφορους πρακτικούς λόγους. Ο πρώτος λόγος είναι η ασφάλεια της πλεύσης. Τα περισσότερα ναυτικά ατυχήματα προκαλούνται από τον ανθρώπινο παράγοντα και το ανθρώπινο λάθος κατά τους χειρισμούς. Πολλά από αυτά οφείλονται σε κούραση των ανθρώπων του πληρώματος του πλοίου. Τα αυτόνομα σκάφη, με ή χωρίς τηλεχειριστή, μπορούν να παραμείνουν σε συνεχή πλεύση και εγρήγορση των συστημάτων τους σε λειτουργία 24/7. Επιπλέον, τα αυτοματοποιημένα συστήματα μπορούν να ανταποκριθούν πιο γρήγορα και πιο αποτελεσματικά σε απροσδόκητα γεγονότα, σε σχέση με τον χρόνο αντίδρασης που βασίζεται στην εμπειρία ενός ανθρώπου. Ένας δεύτερος λόγος είναι η αυξημένη χωρητικότητα φορτίου ενός πλοίου χωρίς πλήρωμα. Ένας αυτόνομος μεταφορέας φορτίου μπορεί να σχεδιαστεί εξαρχής, για τη βελτιστοποίηση του χώρου για το φορτίο του πλοίυο, εφόσον σε αυτό δεν υπάρχει ανάγκη για κατασκευές όπως καταστρώματα, γέφυρα, πλήρωμα, καταλύματα και μαγειρεία, ούτε για περιβαλλοντικά συστήματα διατήρησης ζωής (κλιματισμός, πόσιμο νερό, κ.λπ.) και συστήματα ασφαλείας που προσανατολίζονται στο πλήρωμα. Ο τρίτος λόγος είναι ότι, τα αυτόνομα πλοία υπόσχονται πιο αποτελεσματική λειτουργία. Τα πλοία μπορούν να είναι σχεδιασμένα για να είναι πιο ανθεκτικά στον άνεμο, με αποτέλεσμα να είναι ελαφρύτερα, περισσότερο αποδοτικά, λιγότερο δαπανηρά στη λειτουργία τους και πιο αποδοτικά όσον αφορά στην κατανάλωση καυσίμων και ενέργειας [18].

Ένας επιπλέον επιτακτικός λόγος για τη χρήση αυτόνομων σκαφών είναι η δυσκολία εντοπισμού εκπαιδευμένων πληρωμάτων, ειδικότερα για νεοσύστατες και αναπτυσσόμενες ναυτιλιακές εταιρείες. Τα πλοία εξαρτώνται όλο και περισσότερο από υπολογιστές, συστήματα ΟΤ,

και άλλους αυτοματισμούς. Επομένως οι ναυτικοί που προορίζονται ως πλήρωμα σε σύγχρονα πλοία χρειάζονται και τα δύο χαρακτηριστικά, δηλαδή παραδοσιακές ναυτικές και σύγχρονες τεχνικές δεξιότητες. Στη σύγχρονη ναυτιλία, είναι πιο δύσκολο να προσελκυστούν ως πληρώματα, νέοι από ανεπτυγμένες χώρες. Ιδιαίτερα αυτό ισχύει, δεδομένου του μεγάλου χρόνου παραμονής των ναυτικών στη θάλασσα, μακριά από φίλους και οικογένεια, καθώς και λόγω κινδύνων όπως ο καιρός, η πειρατεία και τα ατυχήματα. Ειδικότερα, για τα θέματα πειρατείας, ορισμένοι υποστηρίζουν ότι ένα σκάφος χωρίς πλήρωμα, μπορεί να είναι λιγότερο πιθανό να στοχοποιηθεί ως αντικείμενο πειρατείας επειδή σε αυτήν την περίπτωση δεν μπορούν να αποκομιστούν λύτρα.

4.1 Οι ψηφιακές τεχνολογίες και η αυτονόμηση των πλοίων

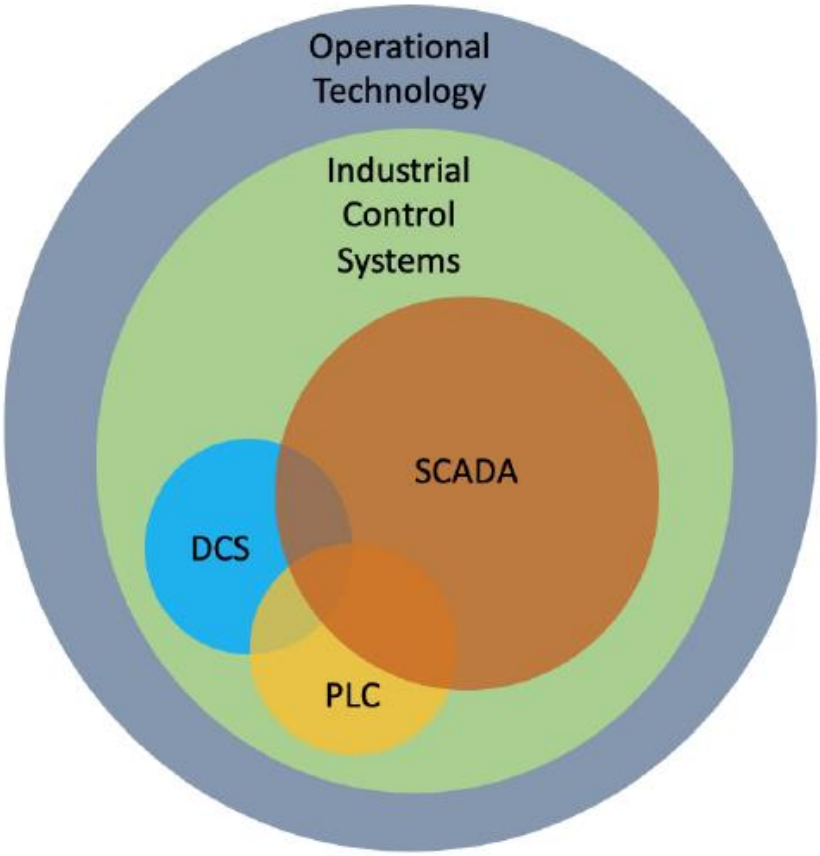
Οι αισθητήρες σε αυτόνομα πλοία είναι πολύ κρίσιμοι για την εύρυθμη και ομαλή λειτουργία του. Αυτές οι συσκευές περιλαμβάνουν: ραντάρ, lidar, σόναρ και κάμερες. Το ραντάρ και το lidar βοηθούν τα πλοία να ανιχνεύουν το περιβάλλον τους, λαμβάνοντας ανακλώμενα σήματα από γειτονικά αντικείμενα. Το σόναρ αποτελεί ένα υποβρύχιο ραντάρ, που χρησιμοποιεί ηχητικά κύματα για να ανιχνεύσει τα υποβρύχια εμπόδια. Οι κάμερες παρέχουν οπτικά δεδομένα, επιτρέποντας στα πλοία να αναγνωρίζουν άλλα σκάφη, βοηθήματα πλοήγησης και πιθανούς κινδύνους [19].

Η τεχνητή νοημοσύνη (Artificial Intelligence - AI) είναι ο "εγκέφαλος" των αυτόνομων συστημάτων. Είναι μια μηχανή λήψης αποφάσεων που επεξεργάζεται όλες τις πληροφορίες που παράγονται από τους αισθητήρες, και άλλες πηγές. Η μηχανική μάθηση είναι ένας τύπος τεχνητής νοημοσύνης που επιτρέπει στα συστήματα, να μαθαίνουν από τις εμπειρίες τους. Βοηθά να λαμβάνουν καλύτερες αποφάσεις με την πάροδο του χρόνου, καθώς συγκεντρώνουν περισσότερα δεδομένα και "μαθαίνουν" πώς να αντιδρούν σε διαφορετικές καταστάσεις.

Τα αυτόνομα πλοία βασίζονται σε εξελιγμένα συστήματα πλοήγησης, συμπεριλαμβανομένης της δορυφορικής πλοήγησης GNSS, του GPS, καθώς και στα συστήματα αδρανειακής πλοήγησης. Αυτά τα συστήματα παρέχουν ακριβείς πληροφορίες θέσης, προσανατολισμού και ταχύτητας, επιτρέποντας στα πλοία να σχεδιάζουν την πορεία τους και να προσαρμόζουν τις διαδρομές τους σε πραγματικό χρόνο. Ένα άλλος σημαντικός παράγοντας προς την αυτονόμηση της ναυσιπλοΐας είναι η δορυφορική επικοινωνία που χρησιμοποιούν τα αυτόνομα πλοία. Τα πλοία ήδη χρησιμοποιούν δορυφορική επικοινωνία για να συνδεθούν με άλλα πλοία, λιμάνια και κέντρα ελέγχου στην ξηρά. Αυτή η επικοινωνία βοηθά τα πλοία να μοιράζονται πληροφορίες σχετικά με την τοποθεσία, τη διαδρομή τους και τυχόν πιθανούς κινδύνους. Τα συστήματα ελέγχου (control systems) διαχειρίζονται τους κινητήρες, τους προωθητήρες, τα πηδάλια και άλλα εξαρτήματα του πλοίου για να εκτελούν εντολές από το AI. Αυτά τα συστήματα διασφαλίζουν ότι το πλοίο πλοηγείται, επιταχύνει και μπορεί να εκτελέσει ελιγμούς με ασφάλεια και αποτελεσματικότητα.

Στον κόσμο της τεχνολογίας, η ασφάλεια είναι ζωτικής σημασίας. Τα αυτόνομα πλοία θα πρέπει να χρησιμοποιούν μέτρα κυβερνο-ασφάλειας για να προστατευθούν από πιθανές απειλές στον κυβερνοχώρο. Αυτά τα μέτρα περιλαμβάνουν κρυπτογράφηση, τείχη προστασίας (firewalls) και συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems - IDS) [2] για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και την προστασία των συστημάτων του πλοίου από hackers [1], [19]. Στο σχήμα που ακολουθεί παρουσιάζεται μία συναρμογή των τεχνολογιών και των OT συστημάτων, που απαιτούνται για την αυτονόμηση των λειτουργιών στη ναυτιλία [1].

Η επιχειρησιακή τεχνολογία (OT) περιλαμβάνει τις τεχνολογίες και τις μεθόδους που επιτρέπουν στον κυβερνοχώρο και τον φυσικό κόσμο να ενωθούν. Οι υπολογιστές παρέχουν άμεσα παρακολούθηση και έλεγχο σε πραγματικό χρόνο, σε συσκευές και αισθητήρες όπως διακόπτες, γραμμές διασύνδεσης, δίκτυα ηλεκτρικής ενέργειας, ρομπότ και συστήματα μεταφορών. Τα συστήματα βιομηχανικού ελέγχου (Industrial Control Systems - ICS) [31] αποτελούν το μεγαλύτερο τμήμα των συσκευών OT. Το ICS γενικά αναφέρεται σε υπολογιστικά συστήματα που διαχειρίζονται βιομηχανικές λειτουργίες και εφαρμογές CPS και ελέγχει τον εξοπλισμό στον φυσικό κόσμο. Το ICS διαφέρει από τα συστήματα τεχνολογίας πληροφοριών και επικοινωνιών, τα οποία γενικά διαχειρίζονται διοικητικές λειτουργίες και δεδομένα. Οι απαιτήσεις απόδοσης, αξιοπιστίας και ασφάλειας του λογισμικού ICS και το υλικό του (hw), είναι διαφορετικά από εκείνα των παραδοσιακών ICT συσκευών. Η συνολική διαφορά είναι ότι το ICS διαχειρίζεται λειτουργικά περιβάλλοντα σε χρονικά σχήματα 24/7/365 δηλαδή αδιάκοπα. Επιπλέον, οι έλεγχοι του απαιτούν διαχείριση σε πραγματικό χρόνο (real time), επικοινωνία χαμηλής καθυστέρησης (Low latency), και υλικό και λογισμικό υψηλής αποκρισιμότητας (High responsiveness).



Σχήμα 15: Κατηγοριοποίηση των συσκευών OT [1]

Τα αποτελέσματα δράσης του ICS λόγω βλάβης μιας συσκευής ή κυβερνο-επίθεσης μπορεί να είναι καταστροφικά, όχι μόνο για τη συσκευή αλλά και για το συνολικό περιβάλλον λειτουργίας και την ασφάλεια των ανθρώπων. Τα ICS περιλαμβάνουν μια ποικιλία υποσυστημάτων ελέγχου. Ο ελεγκτής Προγραμματιζόμενης λογικής Programmable Logic Controller - PLC, είναι ένας υπολογιστής ειδικής χρήσης που ελέγχει τις συσκευές σε περιβάλλον βιομηχανικού αυτοματισμού. Το PLC λαμβάνει δεδομένα από αισθητήρες και άλλες συσκευές εισόδου (αναλογικά και ψηφιακά), επεξεργάζεται τα δεδομένα και στέλνει εντολές ελέγχου στο διαχειριζόμενο υλικό. Τα PLC λόγω της κρισιμότητας τους στις τεχνικές ελέγχου συστημάτων, επίσης μπορεί να τύχουν αντικείμενο κυβερνο-επιθέσεων. Για παράδειγμα, η επίθεση Stuxnet απευθυνόταν στα PLC που ελέγχουν συγκεκριμένα μοντέλα φυγοκεντρητών Siemens, γι' αυτό και το Stuxnet δεν είχε καμία επίδραση στα συστήματα Windows που λειτουργούσαν στο ίδιο το σύστημα.

Ένα κατανεμημένο σύστημα ελέγχου Distributed Control System - DCS, διαχειρίζεται διαδικασίες που συνήθως έχουν πολλούς βρόχους ανάδρασης και διανέμονται μεταξύ πολλών ελεγκτών, αλλά χωρίς ένα κεντρικό σύστημα διαχείρισης. Ένα DCS, για παράδειγμα, μπορεί να περιλαμβάνει πολλά PLC δικτυωμένα μαζί, το καθένα εκ των οποίων λειτουργεί ανεξάρτητα από τα άλλα. Όλα μαζί όμως συνεργάζονται στον σταθμό ελέγχου ενός κεντρικού χειριστή. Σε αυτή την περίπτωση, το DCS παρέχει τη λογική του κατανεμημένου συστήματος εμφανιζόμενο ως ένα ενιαίο σύστημα, ενώ τα PLC υλοποιούν αυτόνομα τη λειτουργία των επιμέρους ελέγχων. Ένα παράδειγμα μπορεί να είναι το σύστημα πρόωσης του πλοίου, όπου η παρακολούθηση και η διαχείριση των κινητήρων, των αξόνων των κινητήρων και των ελίκων του, μπορεί να πραγματοποιηθεί σε μια κεντρική κονσόλα, η οποία γνωρίζει την κατάσταση των επιμέρους εξαρτημάτων του κινητήρα από μια ποικιλία αισθητήρων που έχουν προσαρμοστεί σε κάθε ένα από τα προηγούμενα υποσυστήματα.

Τέλος, τα συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων Supervisory Control and Data Acquisition - SCADA, παρέχουν ένα περιβάλλον κεντρικής διαχείρισης υψηλού επιπέδου, στο οποίο οι φορείς εκμετάλλευσης μπορεί να διατηρήσούν την επίγνωση της κατάστασης και να διαχειριστούν ένα κατανεμημένο ICS. Τα συστήματα SCADA ενσωματώνουν επικοινωνίες δικτύου,

ένα γραφικό περιβάλλον χειρισμού και πολλαπλές δυνατότητες λήψης και επεξεργασίας απεικόνισης των δεδομένων, έτσι ώστε ένας ανθρώπινος χειριστής να μπορεί να παρακολουθεί την κατάσταση ενός συστήματος. Επίσης μπορεί να ανιχνεύει μία μη φυσιολογική δραστηριότητα ή κατάσταση συστήματος, σχεδόν σε πραγματικό χρόνο και να προσαρμόζει τις διαδικασίες χειρισμού του συστήματος.

4.2 Πλεονεκτήματα των Αυτόνομων Πλοίων

Το βασικό ώφελος ενός αυτόνομου πλοίου είναι η αυξημένη ασφάλειά του. Η ασφάλεια στα αυτόνομα πλοία πηγάζει απλώς από τη μείωση του ανθρώπινου παράγοντα. Τα μικρότερα πληρώματα λειτουργούν πιο ευέλικτα και έξυπνα στα πλοία, με υψηλούς βαθμούς αυτοματισμού και ενισχυμένη υποστήριξη για τη λήψη αποφάσεων. Υπάρχουν τομείς στους οποίους η τεχνολογία μπορεί να αποδειχθεί πιο ακριβής από τις ανθρώπινες αισθήσεις. Για παράδειγμα, η ανίχνευση αντικειμένων με χρήση αισθητήρων, αντί της ανίχνευσης που βασίζεται στην ανθρώπινη όραση.

Τα αυτόνομα πλοία χρησιμοποιούν έξυπνους αισθητήρες για να παρακολουθούν τις διεργασίες και τους αναπτυσσόμενους κινδύνους κατά την πλεύση, αποφεύγοντας ατυχήματα που μπορεί να συμβούν λόγω ανθρώπινων λαθών. Αυτά τα έξυπνα πλοία θα εντοπίζουν πιο γρήγορα τα εμπόδια και θα τροποποιούν την πορεία τους, καθιστώντας τα ταξίδια πιο ασφαλή για αυτά και τα άλλα παραπλέοντα πλοία [18], [19]. Τα αυτόνομα πλοία δεν έχουν μόνο την δυνατότητα άμεσης αντίδρασης για αποφυγή κινδύνων, αλλά μπορούν επίσης να σχεδιάσουν για την πλεύση τους, τις καλύτερες διαδρομές. Επιλέγουν έτσι, τις βέλτιστες διαδρομές πλεύσης, λαμβάνοντας υπόψη τον καιρό (μετεωρολογικά δεδομένα) και την κυκλοφορία (δεδομένα πλεύσεων άλλων πλοίων). Αυτό σημαίνει ότι η κατανάλωση καυσίμων είναι μειωμένη, φτάνοντας πιο γρήγορα στον προορισμό τους. Η μείωση των καταναλώσεων ενός πλοίου, αυτόματα συνεπάγεται μείωση των εκπομπών αερίου θερμοκηπίου - ρύπων (green house effect), γεγονός που τα καθιστά φιλικότερα προς το οικοσύστημα. Επιπλέον, μπορούν να πλεύσουν αδιάκοπα (μέρα και νύχτα) χωρίς διακοπές και στάσεις, κάνοντας τη ναυτιλία ταχύτερη και πιο αποτελεσματική. Για την λειτουργία τους θα πρέπει να κάνουν χρήση ήδη εφαρμοσμένων αλλά και νέων ερευνητικών τεχνολογιών. Με τον τρόπο αυτό συμβάλλουν επίσης ως φορείς ανάπτυξης και εξέλιξης της τεχνολογίας. Η χρήση ειδικότερα, της τεχνολογίας AI, αναμένεται να αποτελέσει έναν βασικό πυρήνα για την οργάνωση και διαχείριση των λειτουργιών και κατ'επέκταση των συστημάτων IT/OT των σκαφών.

Επομένως, η χρήση των αυτόνομων πλοίων λόγω μειωμένων λειτουργικών εξόδων, που βασίζεται στην χρήση των συστημάτων και την απομείωση του ανθρώπινου παράγοντα, αναμένεται να μειώσει τα κόστη λειτουργίας και διαχείρισης τους, και κατά συνέπεια και τα επαγόμενα κόστη στις τιμές μεταφοράς των επιβατών και των εμπορευμάτων. Η αυτόνομη πλοήγηση των πλοίων λειτουργεί συνεπικουρικά για τις ναυτιλιακές εταιρείες, δεδομένου ότι διασφαλίζει βέλτιστη αξιοποίηση των πόρων ενός στόλου, μειώνοντας την ανάγκη ναυπήγησης νέων σκαφών για επέκταση των δραστηριοτήτων στην αγορά. Κατά συνέπεια, αυτό μειώνει το κόστος ίδρυσης και λειτουργίας νέων ναυτιλιακών εταιρειών συμβάλλοντας συνολικά και στην προστασία του οικοσυστήματος.

Οι ναυτιλιακοί κανονισμοί λειτουργίας συνεπάγονται χρήση πρωτοκόλλων επικοινωνίας με τα πλοία, που με την σειρά τους εισάγουν ένα σημαντικό θέμα επικοινωνίας και ανταλλαγής εγγράφων και εντολών από/προς τα πληρώματα των πλοίων. Η μη συμμόρφωση με τους ισχύοντες κανονισμούς επισύρει σημαντικά πρόστιμα, και ενδεχόμενο κίνδυνο για απώλειες ανθρώπων και φορτίου. Τα πρωτόκολλα επικοινωνίας είναι πολύπλοκα και η εφαρμογή τους εξαρτάται από την εμπειρία των πληρωμάτων και των υποδομών της ναυτιλιακής εταιρείας. Η εφαρμογή της αυτόνομης ναυτιλίας αναμένεται να συμβάλλει καθοριστικά και στην διευκόλυνση των πρωτοκόλλων επικοινωνίας για την αναταλλαγή εγγράφων διαδικασίων, δεδομένου ότι οι παραπάνω διαδικασίες θα αυτοματοποιηθούν και ίσως ορισμένες από αυτές στο μέλλον να εξαλειφθούν, δεδομένης της αμεσότητας των επικοινωνιών (πλοίου - εταιρείας - λιμένων), που διασφαλίζει η αυτοματοποίηση τους.

Ένα συνολο από σημαντικά ωφέλη από την χρήση των αυτόνομων πλοίων είναι τα παρακάτω [18], [19], [22]:

- Αυξημένη ασφάλεια
- Βέλτιστη πλοήγηση

- Μείωση Κατανάλωσης Καυσίμων
- Μείωση εκπομπών ρύπων
- Μείωση Κόστους μεταφορών επιβατών/εμπορευμάτων
- Μείωση Κόστους Λειτουργίας Ναυτιλιακών Εταιρειών
- Μείωση Κόστους Δημιουργίας Ναυτιλιακών Εταρειών
- Αδιάκοπη λειτουργία πλεύσης
- Διασφάλιση και Αυτοματοποίηση πρωτοκόλλων λειτουργίας/επικοινωνίας πλοίου

4.3 Τεχνικές προκλήσεις για την ανάπτυξη Αυτόνομων Πλοίων

Οι τεχνικές προκλήσεις που εισάγουν στον χώρο της ναυτιλίας τα αυτόνομα πλοία, συμπεριλαμβάνουν πολλούς και σημαντικούς τομείς. Οι τομείς συτοί, πέρα από την αυτοματοποίηση της λειτουργίας των συστημάτων IT/OT που η αυτόνομη πλεύση συνεπάγεται, αφορούν και σε τεχνολογικές αιχμές όπως είναι η τεχνητή νοημοσύνη (AI), η ρομποτική (robotics) και το Διαδίκτυο των Πραγμάτων (IoT).

Τα Κυβερνο-φυσικά συστήματα (Cyber-physical Systems - CPS) είναι ένας γενικός όρος που συγκεντρώνει ανθρώπους, υπολογιστές και φυσικές συσκευές σε ένα λειτουργικό [1]. Το CPS εκμεταλλεύεται την ανάπτυξη πιο εξελιγμένων αισθητήρων, οργάνων, πρωτοκόλλων δικτύου, ενσωματωμένους υπολογιστές και συνδυασμούς αυτών, με στόχο να δημιουργήσει έξυπνες υποδομές και βιομηχανικές εφαρμογές. Οι εφαρμογές CPS περιλαμβάνουν το έξυπνο δίκτυο, την ιατρική παρακολούθηση, τα αυτονόμα οχήματα (αυτοκίνητα, πλοία και αεροσκάφη), συστήματα ελέγχου διαδικασιών, συστήματα ρομποτικής, και αυτόματα συστήματα αεροπλοίας και θαλάσσιας πλοήγησης.

Το CPS και το IoT αποτελούν μέρος της εξέλιξης των υπολογιστών και των τηλεπικοινωνιών που προκύπτει από τις διεργασίες της διακριτοποίησης (digitization) και της ψηφιοποίησης (digitalization) της πληροφορίας. Και οι δύο αυτοί όροι αναφέρονται σε εξελίξεις στην τεχνολογία που μεταμορφώνουν το MTS, και άλλες κρίσιμες υποδομές. Αν και οι δύο προηγούμενοι όροι είναι παραπλανητικά παρόμοιοι, αυτοί οι όροι απευθύνονται σε δύο διαφορετικά σημαντικές έννοιες. Η διακριτοποίηση αναφέρεται στη μετατροπή μιας αναλογικής διαδικασίας σε ψηφιακή (δειγματοληψία - sampling), χωρίς απαραίτητα να αλλοιώνεται η ίδια η διαδικασία. Η ψηφιοποίηση είναι ένα "μετασχηματιστικό άλμα", παρέχοντας τη δυνατότητα ενσωμάτωσης όλων των μορφών πληροφοριών, μέσω ενός ενιαίου κορμού δικτύου και, ως εκ τούτου, παρέχει μια υποδομή που υποστηρίζει εφαρμογές και υλικό που μπορεί να διαχειριστεί και να συνθέσει όλα αυτά τα δεδομένα ταυτόχρονα. Η ψηφιοποίηση παρέχει επίσης τη δυνατότητα συλλογής, αποθήκευσης, ανάλυσης, και μελέτης ιστορικών δεδομένων. Η ψηφιοποίηση επέτρεψε τη συγκέντρωση δεδομένων από πολλαπλές εισόδους (σημεία καταγραφής), παρέχοντας τεράστια σύνολα δεδομένων (Big Data), με τα οποία μπορούμε καλύτερα να κατανοήσουμε τα συστήματά. Αυτό οδήγησε σε μια εποχή δεδομένων μεγάλου όγκου (Big Data), μηχανικής μάθησης (Machine Learning - ML) και τεχνητής νοημοσύνης (AI). Η επιτάχυνση της αλλαγής στον ψηφιακό κόσμο συνεχίζεται με γρήγορους ρυθμούς και θα επηρεάσει όλες τις πτυχές της ναυτιλιακής βιομηχανίας, από τις ναυτιλιακές γραμμές και τα λιμάνια μέχρι τους κανονισμούς και την ασφάλεια των πληροφοριών. Αυτή είναι η διασταύρωση του MTS και της 4ης Βιομηχανικής Επανάστασης (Fourth Industrial Revolution-4IR) [109].

Η τεχνητή νοημοσύνη (AI) οδηγεί την αυτόνομη ναυτιλία σε μια νέα εποχή. Αναδιαμορφώνει την πλοήγηση, τις λειτουργίες και τις διαδικασίες λήψης αποφάσεων. Η τεχνητή νοημοσύνη χρησιμοποιεί μηχανική μάθηση για να προβλέψει με ακρίβεια τις κινήσεις των πλοίων. Η AI μπορεί επίσης να συντελέσει και στα ακόλουθα [19], [20]:

- Τα AI αναλύει τα καιρικά δεδομένα για ασφαλέστερες διαδρομές
- Εντοπίζει τα σφάλματα πριν γίνουν προβλήματα/κίνδυνοι
- Βελτιστοποιεί την κατανάλωση καυσίμου για μείωση του κόστους και των εκπομπών ρύπων

Η τεχνητή νοημοσύνη μεταμορφώνει και τα logistics. Τα πλοία φτάνουν από τον ένα λιμένα

στον άλλο πιο γρήγορα, και πιο ασφαλή. Η McKinsey [110] αναφέρει λειτουργική εξοικονόμηση εξόδων έως και 20% με χρήση τεχνητής νοημοσύνης. Επομένως είναι σαφές γιατί ο κλάδος κινείται γρήγορα προς ένα απόλυτα αυτοματοποιημένο μέλλον [20].

Η αυτόνομη ναυτιλία δεν αφορά μόνο πλοία με τεχνητή νοημοσύνη. Αφορά επίσης στη χρήση ρομποτικής για συντήρηση, διακίνηση φορτίου στο λιμάνι και άλλες εργασίες στο πλοίο. Για παράδειγμα, η DP World των HAE, είναι ένας εξέχων εμπορικός διακινητής. Η DGWorld, ειδικός στα αυτόνομα οχήματα, τη ρομποτική και την τεχνητή νοημοσύνη. Σε συνεργασία μεταξύ τους, βελτίωσαν το λιμάνι Jebel Ali εισάγοντας έναν στόλο αυτόνομων εσωτερικών τερματικών οχημάτων (AITV) το 2020. Με την υποστήριξη της Τεχνητής Νοημοσύνης, αυτοματοποίησαν τις διαδικασίες και τις λειτουργίες μετακίνησης και μεταφοράς των εμπορευματοκιβωτίων, που απαιτούν ανθρώπινη παρέμβαση μόνο για εξαιρετικές περιπτώσεις ή αντιμετώπιση προβλημάτων[20].

Τα αυτοματοποιημένα συστήματα μπορούν επίσης να φροντίσουν τους ελέγχους του κινητήρα και ακόμη και να διορθώσουν προβλήματα που εμφανίζονται κατά τη διάρκεια του ταξιδιού ενός πλοίου. Επομένως αυτή η τεχνολογία λειτουργεί ως μία ομάδα μηχανικών-ρομπότ με συνεχή επίβλεψη επί του σκάφους (24/7).

Σχήμα 16: Ρομποτική φορτο-εκφόρτωση εμπορευματοκιβωτίων [20]

Τα λιμάνια και οι τερματικοί σταθμοί, καθώς και οι κορυφαίες ναυτιλιακές εταιρείες, χρησιμοποιούν ήδη αυτές τις εξελίξεις στην τεχνολογία αυτή τη στιγμή. Με τις εξελίξεις στους αλγόριθμους και τους αισθητήρες μηχανικής μάθησης, τα ρομπότ γίνονται πιο ικανά στην εκτέλεση σύνθετων εργασιών σε δύσκολα και απαιτητικά θαλάσσια περιβάλλοντα.

4.4 Τύποι Αυτόνομων Πλοίων και προγράμματα έρευνας αυτόνομης ναυτιλίας

Τα αυτόνομα σκάφη, είναι πολλών τύπων. Κάθε κατηγορία έχει τις δικές της μοναδικές δυνατότητες και εφαρμογές [20]. Ο πρώτος τύπος αφορά στα Πλήρως Αυτόνομα Πλοία (Fully Autonomous SHips - FAS). Αυτά τα πλοία μπορούν να περιηγηθούν στους ωκεανούς, τελείως αυτόνομα δηλαδή χωρίς πλήρωμα. Η λειτουργία τους είναι ανάλογη με τα αυτοοδηγούμενα και τα μη επανδρωμένα ιπτάμενα οχήματα (Unmanned Air Vehicles - UAVs). Στη δεύτερη κατηγορία συγκαταλέγονται τα

τηλεκατευθυνόμενα πλοία (Remote Controlled Ships - RCS). Αυτά είναι ελεγχόμενα από χειριστές από χερσαία κέντρα. Τα πλοία αυτά λειτουργούν όπως τα drones αλλά σε πολύ μεγαλύτερη κλίμακα. Η τρίτη κατηγορία εντάσσει τα Ημιαυτόνομα Πλοία (Semi-Autonomous Ships - SAS). Αυτή η κατηγορία, διαθέτει ορισμένα αυτοματοποιημένα συστήματα αλλά τα πλοία εξακολουθούν να χρειάζονται ανθρώπινη παρέμβαση για την εκτέλεση συγκεκριμένων εργασιών. Η λειτουργία τους είναι ανάλογη όπως η λειτουργία του αυτόματου πιλότου στα αεροπλάνα που εξακολουθούν να βρίσκονται σε πτήση με την συνδρομή του ανθρώπου - πιλότου παρά την ύπαρξη του συστήματος "αυτόματου πιλότου". Στην τελευταία κατηγορία ανήκουν τα Ηλεκτρικά Σκάφη με Πλήρωμα (Crewed Electric Vessels - CEV). Τα σκάφη αυτά αντί να χρησιμοποιούν ορυκτά καύσιμα, βασίζονται στην ηλεκτρική ενέργεια και για την πρόωση τους, καθιστώντας τα πιο οικονομικά και φιλικά προς το περιβάλλον.

Η έρευνα και δοκιμές για την αυτονομία στην εμπορική ναυτιλία συνεχίζονται από το 2012 [1], κυρίως στην Ασία και την Ευρώπη. Μία από τις παλαιότερες δοκιμές έγιναν τον Δεκέμβριο του 2018, όταν το οχηματαγωγό FALCO της εταιρείας Finferries, πλοηγήθηκε σε μια πλήρως αυτόνομη λειτουργία σε μια εξερχόμενη διαδρομή ενός μιλίου (1664 m), ενώ στο ταξίδι της επιστροφής χρησιμοποιήθηκε τηλεχειρισμός. Ένας καπετάνιος παρακολουθούσε το σκάφος από ένα αυτόνομο κέντρο επιχειρήσεων, 30 μίλια (περίπου 50 Km) μακριά. Το FALCO αποτέλεσε το ασφαλέστερο σκάφος της Rolls-Royce με αυτόνομη τεχνολογία πλοήγησης (FAS/RCS).

Τον Φεβρουάριο του 2020, οι Bastø Fosen, Kongsberg και η Norwegian Maritime ξεκίνησαν μια δοκιμή στο ημιαυτόνομο επιβατικό και οχηματαγωγό πλοίο BASTØ FOSEN VI. Το πλοίο, μήκους 469 ποδιών (περίπου 142.9 μ.), λειτούργησε πλήρως με αυτοματοποιημένο έλεγχο (FAS) από αποβάθρα σε αποβάθρα, με καπετάνιο και πλήρες πλήρωμα επί του σκάφους για επίβλεψη, σε μια διαδρομή επτά μιλίων (περίπου 11 Km), η οποία διήρκησε 30 λεπτά.

Τον Απρίλιο του 2020, η Royal Caribbean πραγματοποίησε μια απρογραμμάτιστη εξ αποστάσεως δοκιμή του αυτόνομου συστήματος επί πλοίου. Λόγω των ταξιδιωτικών περιορισμών για τον COVID-19, ο ολλανδός ναυπηγός De Hoop δεν μπορούσε να φέρει υπεργολάβους στο πλοίο για θαλάσσιες δοκιμές. Σε προετοιμασία για ένα παρθενικό ταξίδι στα τέλη του 2020, του SILVER ORIGIN της εταιρείας Silversea Cruises, διεξήχθη μια απομακρυσμένη δοκιμή του δυναμικού συστήματος εντοπισμού θέσης, που προοριζόταν να διατηρήσει το πλοίο σε απόσταση τεσσάρων ιντσών (10 cm) από ένα σταθερό σημείο. Κατά τη διάρκεια της δοκιμής, ένας υπεργολάβος συντόνισε και βαθμολόγησε το σύστημα μέσω μιας γρήγορης Διαδικτυακής σύνδεσης από 1,120 μίλια (περίπου 1,800 Km) μακριά, στην Αγία Πετρούπολη της Ρωσίας. Ο καπετάνιος του πλοίου ήταν στο πλοίο σε επιφυλακή, εάν και εφόσον χρειαζόταν να παρέμβει.

Το έργο Mayflower Autonomous Ship (MAS) είναι μια παγκόσμια κοινοπραξία, υπό την ηγεσία της IBM και της Promare, που προορίζεται ως η πρώτη δοκιμή ενός πλήρους αυτόνομου σκάφους ανοιχτού ωκεανού. Το πλήρως αυτόνομο σκάφος MAYFLOWER [23] μήκους 15 μέτρων, βασίζεται σε ηλιακή ενέργεια, μηχανές diesel και αιολική ενέργεια και τα συστήματα του βασίζονται στην τεχνητή νοημοσύνη, σε τεχνικές μηχανικής μάθησης (deep learning) και άλλες τυπικές ναυτιλιακές τεχνολογίες για τη διαχείριση της πλεύσης και διέλευσης. Αρχικά είχε προγραμματιστεί να ξεκινήσει το ταξίδι των 3,220 μιλίων (περίπου 5,182 km) από το Πλύμουθ της Αγγλίας προς το Πλίμουθ της Μασαχουσέτης, τον Σεπτέμβριο του 2020. Το ταξίδι αναβλήθηκε λόγω COVID-19.

Τον Ιούνιο του 2021 ξεκίνησε το ταξίδι του, αλλά χρειάστηκε να στρίψει λόγω μιας μικρής μηχανικής βλάβης, καθώς δεν υπήρχε κανείς στο πλοίο για να εκτελέσει μια απαιτούμενη επισκευή. Το σκάφος επαναδρομολογήθηκε τον Σεπτέμβριο του 2021 και προγραμματίστηκε η επόμενη προσπάθεια του για τη διάσχιση του Ατλαντικού, το 2022. Το πλοίο τελικά έφτασε στον προορισμό του στις 30 ΙΟυνίου του 2022, στέφοντας με επιτυχία το project [23].

Η Ιαπωνία επίσης διαθέτει μια σειρά από αυτόνομα ερευνητικά προγράμματα ναυτιλίας στο πλαίσιο διοίκησης του Ιδρύματος Nippon. Το έργο MEGURI 2040, που ανακοινώθηκε στις αρχές του 2020, εστιάζει στην ανάπτυξη πλήρως αυτόνομων συστημάτων πλοήγησης σκαφών. Το ίδρυμα υποστηρίζει πέντε κοινοπραξίες έργων. Στα μέσα του 2020, ανακοινώθηκε το σχέδιο σχεδίασης του πλήρους αυτόνομου πλοίου του μέλλοντος (DFFAS). Στο project συνεργάζονται 30 εταιρείες βιομηχανίας και έρευνας. Το DFFAS Fleet Operation Center (FOC) ολοκληρώθηκε τον Σεπτέμβριο του 2021. Οι βασικοί στόχοι του DFFAS είναι η οικοδόμηση μιας βιώσιμης κοινωνίας και η προώθηση της ναυτιλιακής τεχνολογίας, με στόχο το ήμισυ των ιαπωνικών εγχώριων παράκτιων πλοίων που λειτουργούν να γίνουν αυτόνομα έως το 2040.

Τον Σεπτέμβριο του 2019, η NYK Line πραγματοποίησε την πρώτη δοκιμή ενός αυτόνομου φορτηγού πλοίου, του IRIS LEADER, στα ανοικτά των ακτών της Ιαπωνίας με πλήρωμα ως εποπτεία της αυτόνομης λειτουργίας. Η NYK Line ξεκίνησε τη μετατροπή ολόκληρου του στόλου των 800 πλοίων της για χρήση αυτόνομης ναυτιλιακής τεχνολογίας.

Σχήμα 17: Το πλοίο MAYFLOWER [23]

Σχήμα 18: Το επιτυχημένο ταξίδι των 3,220 μιλίων του MAYFLOWER [23]

Τον Αύγουστο του 2021, η Nippon Yusen Kabushiki Kaisha (NYK Line) [24] ανακοίνωσε τα σχέδια για τη δοκιμή του πρώτου αυτόνομου φορτηγού πλοίου που θα διασχίσει ύδατα με μεγάλη θαλάσσια κυκλοφορία. Το πλοίο μεταφοράς εμπορευματοκιβωτίων πιλοτάρεται αυτόνομα, με τη βοήθεια της Orca AI τεχνολογίας, από τον κόλπο του Τόκιο στον κόλπο Ise, δηλαδή σε ένα ταξίδι 236 μιλίων (περίπου 380 Km). Τα δεδομένα ταξιδιού, από τον καιρό και την κατάσταση της θάλασσας μέχρι το ραντάρ και την πληροφορία κυκλοφορίας, συλλέχθηκαν και αναλύθηκαν σε ένα κέντρο υποστήριξης στην ξηρά. Στο πλοίο μπορούσαν να σταλούν οδηγίες και, εάν κρινόταν απαραίτητο, οδηγίες μπορούσαν να σταλούν και στους χειριστές του κέντρου δεδομένων, το οποίο μπορούσε να κατευθύνει εξ αποστάσεως το σκάφος με την παρέμβαση του.

4.5 Επίδραση των Αυτόνομων Πλοίων στη Ναυτιλία

Το κύμα της τεχνολογίας αυτόνομων πλοίων αναδιαμορφώνει τα επιχειρηματικά μοντέλα με τρόπο, που ο ψηφιακός μετασχηματισμός έχει εξορθολογίσει τον τομέα του λιανικού εμπορίου. Η McKinsey [110] προβλέπει ότι αυτή η αλλαγή θα οδηγήσει σε αύξηση της αποτελεσματικότητας, μειώνοντας το λειτουργικό κόστος της λιανικής αγοράς έως και 40%. Αυτό είναι ένα "οικονομικό τσουνάμι" για το

παγκόσμιο εμπόριο. Οι εταιρείες στρέφουν τώρα τις στρατηγικές τους προς την ενσωμάτωση αυτών των τεχνολογικών εξελίξεων. Ωστόσο, υπάρχουν και προκλήσεις. Η προσαρμογή των αλυσίδων εφοδιασμού και η κατανόηση των νέων ναυτιλιακών νόμων μπορεί να μοιάζει με πλοήγηση σε "αχαρτογράφητα ύδατα". Τα αυτόνομα πλοία δεν αλλάζουν απλώς τον τρόπο με τον οποίο τα αγαθά μετακινούνται στους ωκεανούς του πλανήτη μας προς τους καταναλωτές, αλλά μεταμορφώνουν ολόκληρες βιομηχανίες, από τη μεταποίηση μέχρι τις τοπικές υπηρεσίες παράδοσης.

4.5.1 Εμπορική Βιωσιμότητα

Μία από τις προκαταρκτικές συζητήσεις στο θέμα της αυτόνομης ναυτιλίας είναι ότι οι μεταφορές ταξινομούν την κατανόηση της εμπορικής βιωσιμότητας και της οικονομικής καταλληλότητας των πλοίων [25], [26] σε υπάρχουσες και μελλοντικές αλυσίδες εφοδιασμού.Η συστηματική έρευνα για τη μοντελοποίηση του κόστους του πλοίου είναι εξαιρετικά περιορισμένη, και μέχρι σήμερα, δεν υπάρχει διεθνώς αναγνωρισμένο πρότυπο για την ταξινόμηση του κόστους [25]. Ενώ υπάρχουν ομοιότητες στις δομές κόστους, αρκετές διαφορές υπάρχουν μεταξύ του λειτουργικού κόστους των συμβατικών και των αυτόνομων σκαφών, τα οποία είναι απαραίτητο να αναγνωριστούν και να αξιολογηθούν για πολλούς λόγους.

Στο πλαίσιο της αυτόνομης ναυτιλίας, η διεθνής έρευνα βρίσκεται ακόμη σε εξέλιξη, με έναν αναδυόμενο αριθμό μελετών που αρχίζουν να διερευνούν τη βιωσιμότητα της μη επανδρωμένης ναυτιλίας από οικονομικής και δημοσιονομικής πλευράς. Ένα Ευρωπαικό έργο με όνομα Maritime Unmanned Navigation through Intelligence in Networks - MUNIN [28], αποτέλεσε πλατφόρμα έρευνας, αντιμετωπίζοντας ένα ευρύ φάσμα θεμάτων που θα φέρουν επανάσταση στο τοπίο της ναυτιλιακής βιομηχανίας. Τα προκαταρκτικά αποτελέσματα του MUNIN ήταν ο βασικός καταλύτης για την κατανόηση των οικονομικών, τεχνικών, και περιβαλλοντικών επιπτώσεων και τις κανονιστικές απαιτήσεις για αυτόνομα θαλάσσια συστήματα. Στο έργο αυτό περιλαμβάνεται μια Ποσοτική Αξιολόγηση για την κατανόηση των οικονομικών και χρηματοοικονομικών πτυχών της λειτουργίας μη επανδρωμένων σκαφών. Η μελέτη συγκρίνει την αναμενόμενη παρούσα αξία ενός αυτόνομου πλοίου μεταφοράς φορτίου, με ένα συμβατικό πλοίο, με αποτέλεσμα την εξοικονόμηση έως και 7 εκατομμυρίων δολαρίων ΗΠΑ κατά τη μέση διάρκεια ζωής των 25 ετών ενός πλοίου. Σε σύγκριση με το επανδρωμένο σκάφος αναφοράς, η MUNIN ισχυρίζεται ότι η κύρια εξοικονόμηση σχετίζεται με την απομάκρυνση του πληρώματος και την ενίσχυση από την αποδοτικότητα καυσίμου, ενώ προκύπτουν πρόσθετα έξοδα με υψηλότερες ανάγκες για υπηρεσίες υποστήριξης που βασίζονται στα λιμάνια. Με τα πιο αισιόδοξα αποτελέσματα, το έργο ReVolt από τον Όμιλο DNV GL εκτιμά ετήσια εξοικονόμηση άνω του 1 εκατομμυρίου USD για το πρωτότυπο μη επανδρωμένου σκάφος τους. Με την αύξηση της χωρητικότητας φορτίου, που επιτυγχάνεται μέσω της απομάκρυνσης των εγκαταστάσεων του πληρώματος, και τα χαμηλότερα έξοδα λειτουργίας και συντήρησης, εκτιμάται ότι η ReVolt θα εξοικονομήσει έως και 34 εκατομμύρια δολάρια σε μια διάρκεια ζωής 30 ετών ενός πλοίου.

4.5.2 Ναυπήγηση Πλοίων

Πολλοί ερευνητές πιστεύουν ότι με την υπάρχουσα τεχνολογία, η ανάπτυξη και οι λειτουργίες των μη επανδρωμένων πλοίων είναι εφικτές. Ωστόσο, υπάρχουν αρκετές προκλήσεις και άγνωστες περιοχές για μεγάλης κλίμακας ναυπήγηση και συντήρηση τέτοιων σκαφών, που θα μπορούσε ενδεχομένως να διαταράξει τη ναυπηγική βιομηχανία με πολλούς τρόπους [25]. Ο Milner (1971) αναφέρει ότι σε βιομηχανίες όπως η ναυπηγική,δεν είναι εύκολο να διακρίνεις την καινοτομία δεδομένου ότι η ανάπτυξη σε διαφορετικά module και υποσυστήματα μπορούν να επισκιαστούν από το συνολικό προϊόν. Οι εξελίξεις στην τεχνολογία οδηγούν πλέον πολλές καινοτομίες στον τομέα της ναυπηγικής βιομηχανίας, και είναι δίκαιο να θεωρηθεί ότι κατά την τελευταία δεκαετία η ναυπηγική έχει υιοθετήσει αποτελεσματικά ένα ευρύ φάσμα τεχνολογιών για την αντιμετώπιση των προβλημάτων που προκύπτουν από το αυξανόμενο κόστος των καυσίμων, τις περιβαλλοντικές επιπτώσεις, την αποδοτικότητα του πληρώματος και την ασφάλεια πλοήγησης. Μερικές από αυτές τις τεχνολογίες περιλαμβάνουν, την τρισδιάστατη εκτύπωση για ανταλλακτικά, τη ρομποτική, τους κινητήρες με αποδοτικά καύσιμα και μειωμένη ρύπανση, την ηλεκτρική πρόωση και τα Integrated Building Management Systems - IBMS συστήματα διαχείρισης. Ωστόσο, πολλές από αυτές τις

προόδους υποστηρίζονται ως σταδιακές βελτιώσεις, ενώ ορισμένες οδηγούν σε πιο μεταμορφωτικές καινοτομίες όπως η ανάπτυξη πλήρως αυτόνομων σκαφών.

Ερευνητικές πλατφόρμες όπως η MUNIN [28], η Yara Birkeland, η ReVolt και η Rolls-Royce έχουν αποκαλύψει θεμελιώδεις διαφορές στο σχεδιασμό των τεχνικών προδιαγραφών αυτόνομων πλοίων, οι οποίες θα έχουν σημαντικές επιπτώσεις στον τρόπο κατασκευής εμπορικών πλοίων στο μέλλον. Με τη μετάβαση στη λήψη αποφάσεων από πλοίο στην ξηρά και τη μετάβαση των ευθυνών από άνθρωπο σε μηχανή, απαιτείται συντονισμός και ανταλλαγή δεδομένων, στα πλοία και στην ακτή, για να διατηρηθούν τα απαραίτητα πρότυπα ασφαλείας για τη λειτουργία των αυτόνομων σκαφών (IMO 2007).

Τέτοιο επίπεδο ασφαλούς αυτονομίας δεν είναι εφικτό χωρίς ανάπτυξη προηγμένων αισθητήρων, την ανάλυση δεδομένων και άλλα συστήματα IT/OT. Τα συστήματα για τη λειτουργία του κινητήρα, της πρόωσης, της δεξαμενής έρματος ενός σκάφους και άλλα μηχανήματα για μεγάλα χρονικά διαστήματα χωρίς την επίβλεψη του ανθρώπινου παράγοντα, μπορεί να οδηγήσει σε κινδύνους. Η συμμετοχή των συστημάτων IT/OT πρέπει να είναι εξαιρετικά αξιόπιστη και προηγμένη. Το πιο σημαντικό, είναι η ανάπτυξη του συστήματος ελέγχου, ικανό για συνεχή παρακολούθηση και διοίκηση του σκάφους σε πραγματικό χρόνο. Η ανταλλαγή πληροφοριών αποτελεί βασική τεχνολογική πρόκληση όταν εξετάζεται η προσβασιμότητα του Διαδικτύου στους ωκεανούς. Επιπλέον, υπάρχει μια "γκρίζα περιοχή ευθύνης" που αφορά στην ανάπτυξη και τη συντήρηση ενός τέτοιου συστήματος ελέγχου (του ναυπηγού ή του προμηθευτή τεχνολογίας).

4.5.3 Συντήρηση Πλοίων

Τα μη επανδρωμένα σκάφη θα περιλάμβαναν προηγμένα και πολύπλοκα συστήματα για την ασφαλή και αξιόπιστη λειτουργία του πλοίου. Η τεχνολογία επισκευής και συντήρησης δεν είναι πιθανό να είναι άμεσα διαθέσιμη. Αυτό ίσως απαιτεί νέα μοντέλα συνεργασίας μεταξύ ναυπηγών, αποβάθρων και προμηθευτών αυτόνομων τεχνολογιων, για την από κοινού εκτέλεση της συντήρησης και της επισκευής. Αυτές οι δραστηριότητες, ενδέχεται να προσθέσουν περισσότερα έξοδα στο κόστος απόκτησης ενός αυτόνομου πλοίου.

4.5.4 Επιπτώσεις στη Λειτουργία των Λιμένων

Ενώ υπάρχει ένας αυξανόμενος όγκος έρευνας για διάφορες πτυχές στα αυτόνομα πλοία, οι έρευνες για τις μακροπρόθεσμες επιπτώσεις τους στα λιμάνια είναι εξαιρετικά περιορισμένες. Επομένως, είναι σημανική η αναγνώριση των προκλήσεων που αντιμετωπίζουν τα λιμάνια στην προετοιμασία για μη επανδρωμένα πλοία στο μέλλον, και να εξερευνηθούν τα πιθανά ωφέλη που θα αποκομιστούν από την εξυπηρέτησή τους [25].

Ενώ οι αυτόνομες θαλάσσιες μεταφορές βρίσκονται ακόμη στο στάδιο έρευνας και ανάπτυξης, η πρόοδος στους αυτοματισμούς των λιμένων έχει συντελεστεί εδώ και δεκαετίες. Ωστόσο, οι περισσότερες από αυτές τις εξελίξεις παρατηρούνται σε εργασίες διακίνησης φορτίου, ενώ οι κινήσεις των πλοίων που εισέρχονται/εξέρχονται από τα λιμάνια, εξακολουθούν να εκτελούνται με χρήση του ανθρώπινου δυναμικού των λιμένων. Ίσως μια από τις μεγαλύτερες τεχνικές προκλήσεις για τα λιμάνια στην εξυπηρέτηση των αυτόνομων σκαφών, θα είναι γύρω από την ασφαλή ναυσιπλοΐα, τον ελλιμενισμό και τους ελιγμούς εντός του λιμένα. Οι πλατφόρμες έρευνας και ανάπτυξης όπως η MUNIN έχουν εκφράσει την ανάγκη για μια ομάδα ελέγχου επί του οχήματος (On-board Control Team - OCT). Η ομάδα θα είναι υπεύθυνη για την ανάληψη του ελέγχου του σκάφους για την άφιξή του στο λιμάνι, και ομοίως, στο τελικό σκέλος από το λιμάνι για το αυτόνομο σημείο ελέγχου. Ως εκ τούτου, είναι αναμενόμενο ότι τα λιμάνια θα διαδραματίσουν κρίσιμο ρόλο στο μέλλον, παρέχοντας υπηρεσίες που υποστηρίζονται από τις προηγμένες επίγειες τηλεπικοινωνίες.

Ωστόσο, για να αξιολογηθεί η ετοιμότητα των λιμένων για την αντιμετώπιση του μελλοντικού τους ρόλου σε τέτοια επιχειρησιακά περιβάλλοντα, είναι σημαντικό να εξεταστεί η πρόοδός τους στην υιοθέτηση πρακτικών απομακρυσμένης πλοήγησης. Αν και αυτά είναι δύο ξεχωριστά θέματα, αντιμετωπίζουν το ίδιο πρόβλημα, που είναι η ασφαλής φιλοξενία των σκαφών γύρω από την

επιχειρησιακή ζώνη του λιμανιού. Ο Hadley (1999) ορίζει την απομακρυσμένη πλοήγηση ως "πράξη πλοήγησης που πραγματοποιείται σε καθορισμένο χώρο από αδειούχο χειριστή για τη συγκεκριμένη περιοχή από θέση διαφορετική από αυτή του οικείου σκάφους". Δυστυχώς, μέχρι σήμερα, η απομακρυσμένη πλοήγηση δεν έχει υιοθετηθεί από τον λιμενικό τομέα, και πολύ μικρή τεχνολογική και κανονιστική πρόοδος έχει συντελεστεί σε αυτόν τον τομέα κατά το παρελθόν.Τα εμπόδια στην υιοθέτηση της απομακρυσμένης πλοήγησης δεν είναι απαραίτητα αμιγώς τεχνολογικά, δηλαδή, διαχειριστικοί και πολιτισμικοί παράγοντες θα μπορούσαν επίσης να εμποδίσουν την υιοθέτηση τέτοιων τεχνολογιών από τα λιμάνια. Ενώ υπάρχουν ορισμένες τεχνικές προκλήσεις σε όρους συμβατότητας συστημάτων, με την υπάρχουσα τεχνολογία είναι εφικτό να εφαρμοστούν συστήματα απομακρυσμένης πλοήγησης ως μέρος των πρακτικών πλοήγησης των λιμένων .Λαμβάνοντας υπόψη τα διδάγματα από την υιοθέτηση του τηλεχειριστηρίου πλοήγησης, για την προετοιμασία λιμένων για ασφαλή και αποτελεσματική διαμονή αυτόνομων πλοίων, θα απαιτηθεί μια πιο συνεργατική κουλτούρα μεταξύ των λιμένων, των ναυτιλιακών εταιρειών, των ναυτιλιακών πρακτορείων και όσους εμπλέκονται στην προώθηση των τεχνολογιών αυτόνομης ναυτιλίας.

Από την άλλη πλευρά, με την απουσία πληρώματος επί του σκάφους, από τα λιμάνια θα απαιτείται παροχή ευρύτερου φάσματος υπηρεσιών στα πλοία. Όπως αναφέρθηκε και πριν, ένα πλήρωμα με βάση το λιμάνι απαιτείται να αναλάβει μια σειρά από δραστηριότητες που προηγουμένως εκτελούνταν από το πλήρωμα του πλοίου. Ειδικότερα, η τακτική συντήρηση είναι ένας τομέας στον οποίο αναμένεται να συμμετέχουν ενεργά και να διευκολύνουν τα λιμάνια. Αυτό μπορεί ενδεχομένως να οδηγήσει στο άνοιγμα νέων επιχειρήσεων επισκευών και συντήρησης εντός της λιμενικής περιοχής, για την εξυπηρέτηση αυτόνομων πλοίων (British Ports Association - BPA 2018). Ομοίως, οι περισσότερες εργασίες διακίνησης φορτίου όπως, ο καθαρισμός, οι αξιολογήσεις ευστάθειας, οι ρυθμίσεις έρματος, και άλλες διαδικασίες ασφαλείας που εκτελούνται επί του παρόντος από το προσωπικό του πλοίου, αναμένεται να προσφερθούν από πλήρωμα με έδρα το λιμάνι. Ενώ αναμένεται ότι ένας αριθμός εργασιών θα αφαιρεθεί ενδεχομένως, ως αποτέλεσμα απλοποιημένου και αυτόνομου πλοίου, η ανάγκη για πλήρωμα με βάση το λιμάνι είναι ακόμα αναπόφευκτη. Η άφιξη των αυτόνομων σκαφών έρχεται με κάποιες άλλες επιχειρησιακές προκλήσεις για τα λιμάνια, όσον αφορά την παραγωγικότητα. Το γεγονός ότι μια σειρά από συντήρηση και εργασίες διακίνησης φορτίου που εκτελούνταν προηγουμένως κατά τη διάρκεια του ταξιδιού, θα πραγματοποιηθούν σε λιμάνια από πλήρωμα στην ξηρά, αυτό θα ανοίξει νέες προκλήσεις όσον αφορά τον μέσο χρόνο ολοκλήρωσης των εργασιών του πλοίου (Average Turnaround Time - ATT). Προσθέτοντας τον απαιτούμενο χρόνο για τακτική συντήρηση και άλλες σχετικές δραστηριότητες, το ATT θα αυξήσει σημαντικά την πληρότητα των θέσεων και την κατοχή περιουσιακών στοιχείων. Κατά συνέπεια, η αυξημένη πληρότητα αγκυροβολίου ανά σκάφος, μεταφράζεται σε λιγότερο αριθμό πλοίων που εξυπηρετούνται από το λιμάνι, συμφόρηση και ενδεχομένως μικρότερη παραγωγικότητα των υποδομών και των περιουσιακών στοιχείων, τόσο για τη ναυτιλιακή εταιρεία, όσο και για τον φορέα εκμετάλλευσης των λιμένων. Τέτοιες επιπτώσεις είναι σημαντικές, αν και υποτιμημένες, και πιθανώς να επιδείνωσουν την ελκυστικότητα της αυτόνομης ναυτιλίας για πολλά λιμάνια.

Εντούτοις, η υιοθέτηση της νέας τεχνολογίας των αυτόνομων πλοίων απαιτεί σημαντικά επίπεδα προσοχής στα ακόλουθα πεδία [20]:

- Η υιοθέτηση της νέας τεχνολογίας απαιτεί χρόνο και επένδυση
- Η κυβερνο-ασφάλεια γίνεται ακόμη πιο κρίσιμη
- Η πλοήγηση μέσα από τα υφιστάμενα ρυθμιστικά πλαίσια χρειάζεται ειδικευμένους ναυτικούς, που η αυτόνομη πλοήγηση θα αντικαταστήσει;

4.6 Ρυθμιστικές Αρχές και Αυτόνομα Πλοία

Η εισαγωγή των νέων τεχνολογιών, της επέκτασης των αυτοματισμών, του εμπλουτισμού των υπηρεσιών IT/OT, είναι σημαντικό να εξετασθούν υπό το πρίσμα των κανονισμών και του ρυθμιστικού πλαισίου που ισχύει στη ναυτιλία. Στόχος είναι ο εντοπισμός κενών, τα οποία δημιουργούνται από την υιοθέτηση των νέων τεχνολογιών προς την υλοποίηση αυτόνομων πλοίων, με στόχο να συμπληρωθούν από τα ισχύοντα πλαίσια.

Θα πρέπει να τονισθεί, ότι τα ρυθμιστικά πλαίσια αφοορύν σε όλη την αλυσίδα των ναυτιλιακών δραστηριοτήτων (πλοία, λιμένες, κ.λπ.).

4.6.1 IMO

Η τεχνολογική καινοτομία στη ναυτιλιακή βιομηχανία έχει ως αποτέλεσμα ραγδαίες εξελίξεις που θα δουν την εμπορική χρήση αυτόνομων πλοίων, είτε ελέγχονται εξ αποστάσεως είτε είναι πλήρως αυτόνομα. Μια τέτοια αλλαγή απαιτεί αυστηρή ρύθμιση για τη διασφάλιση της ζωής στη θάλασσα, του φορτίου του πλοίου, καθώς και του ίδιου του πλοίου.

Ο IMO [12], [17] στοχεύει να ενσωματώσει νέες και προηγμένες τεχνολογίες στο ρυθμιστικό του πλαίσιο, εξισορροπώντας τα ωφέλη που προκύπτουν από τις νέες και προηγμένες τεχνολογίες έναντι ανησυχιών για την ασφάλεια, τον αντίκτυπο στο περιβάλλον, τη διευκόλυνση του διεθνούς εμπορίου, το πιθανό κόστος για τη βιομηχανία και τον αντίκτυπό τους στο προσωπικό, τόσο στο πλοίο όσο και στην ξηρά. Ο IMO θέλει να διασφαλίσει ότι το ρυθμιστικό πλαίσιο για τα αυτόνομα πλοία επιφανείας (Maritime Autonomous Surface Ships - MASS), συμβαδίζει με τις τεχνολογικές εξελίξεις που μεταβάλλονται ταχέως.

Το 2021, ο IMO διεξήγαγε μια ρυθμιστική άσκηση οριοθέτησης για τα αυτόνομα πλοία επιφανείας, που σχεδιάστηκε για να αξιολογήσει τα υπάρχοντα μέσα του IMO, εξετάζοντας πώς θα μπορούσαν να εφαρμοστούν σε πλοία που χρησιμοποιούν διαφορετικούς βαθμούς αυτοματισμού. Η άσκηση ρυθμιστικού πεδίου εφαρμογής (Regulatory Scoping Exercise - RSE) για τις συνθήκες ασφάλειας, οριστικοποιήθηκε στην 103η σύνοδο του MSC τον Μάιο του 2021, και για τις συνθήκες υπό την αρμοδιότητα της Νομικής Επιτροπής, στην 108η σύνοδό της, τον Ιούλιο του 2021. Η Επιτροπή (Facilitation Commitee - FAL) [26], ενέκρινε το αποτέλεσμα της RSE, των συνθηκών υπό την αρμοδιότητα του στο FAL 46, τον Μάιο του 2022.

Μετά την ολοκλήρωση της άσκησης οριοθέτησης και των εργασιών που ξεκίνησαν κατά την 105η σύνοδο του MSC, η 107η σύνοδος της Επιτροπής τον Ιούνιο του 2023, σημείωσε περαιτέρω πρόοδο στην ανάπτυξη ενός βασισμένου σε στόχους, μέσου, που ρυθμίζει τη λειτουργία των αυτόνομων θαλάσσιων πλοίων επιφανείας. Συστάθηκε μια ομάδα εργασίας MASS, για την πρόοδο των εργασιών σχετικά με τον Κώδικα MASS (MASS Code) [17] και τον εντοπισμό ζητημάτων που σχετίζονται με τα μέσα που υπάγονται στην αρμοδιότητα της Νομικής Επιτροπής και της Επιτροπής Διευκόλυνσης. Αυτά θα εξεταστούν από την κοινή ομάδα εργασίας MSC/LEG/FAL για τη MASS. Στόχος είναι, η υιοθέτηση ενός μη υποχρεωτικού Κώδικα MASS βάσει στόχου που θα τεθεί σε ισχύ το 2025. Ο κώδικας θα αποτελέσει τη βάση για έναν υποχρεωτικό Κώδικα MASS, βάσει στόχου, ο οποίος αναμένεται να τεθεί σε ισχύ την 1η Ιανουαρίου 2028.

Μια κοινή ομάδα εργασίας MSC/LEG/FAL έχει συσταθεί ως οριζόντιος μηχανισμός για την αντιμετώπιση κοινών ζητημάτων που προσδιορίζονται από τις ασκήσεις ρυθμιστικού πεδίου εφαρμογής για τη χρήση του MASS, που διεξάγονται από καθεμία από τις τρεις Επιτροπές MSC, την Νομική Επιτροπή και την Επιτροπή Διευκόλυνσης. Η κοινή ομάδα εργασίας MSC/LEG/FAL για το MASS (MASS-JWG) συνεδρίασε τον Σεπτέμβριο του 2022, και τον Απρίλιο του 2023. Το MSC 107 (Ιούνιος 2023), σημείωσε ότι η κοινή ομάδα εργασίας MSC/LEG/FAL για το MASS είχε αναπτύξει έναν πίνακα, προοριζόμενο ως ζωντανό έγγραφο, για τον εντοπισμό προτιμώμενων επιλογών για την αντιμετώπιση κοινών ζητημάτων, όπως ο ρόλος, οι αρμοδιότητες που απαιτούνται από τον πλοίαρχο και το πλήρωμα για MASS, και η αναγνώριση και η έννοια του όρου "απομακρυσμένου χειριστή" καθώς και οι αρμοδιότητές τους.

Η Επιτροπή Ναυτικής Ασφάλειας (MSC), στην 101η σύνοδο τον Ιούνιο του 2019, ενέκρινε ενδιάμεσες κατευθυντήριες γραμμές για δοκιμές θαλάσσιων αυτόνομων πλοίων επιφανείας (MSC.1-Circ.1604). Μεταξύ άλλων, οι κατευθυντήριες γραμμές αναφέρουν ότι οι δοκιμές πρέπει να διεξάγονται με τρόπο που να παρέχει τουλάχιστον τον ίδιο βαθμό ασφάλειας και προστασίας του περιβάλλοντος, όπως προβλέπεται από τα σχετικά όργανα. Οι κίνδυνοι που σχετίζονται με τις δοκιμές, θα πρέπει να προσδιορίζονται κατάλληλα και να ληφθούν μέτρα για τη μείωση τους, στο χαμηλότερο δυνατό και αποδεκτό επίπεδο. Οποιοδήποτε προσωπικό εμπλέκεται σε δοκιμές MASS, είτε χειριστές εξ αποστάσεως είτε επί του σκάφους, θα πρέπει να διαθέτει τα κατάλληλα προσόντα και εμπειρία για την ασφαλή διεξαγωγή δοκιμών MASS. Θα πρέπει να ληφθούν τα κατάλληλα μέτρα για να εξασφαλιστεί επαρκής διαχείριση κινδύνων στον κυβερνοχώρο, των συστημάτων και της υποδομής που χρησιμοποιούνται κατά τη διεξαγωγή δοκιμών MASS.

Η άσκηση οριοθέτησης, θεωρήθηκε ως ένα σημείο εκκίνησης που έθιξε ένα ευρύ φάσμα θεμάτων, συμπεριλαμβανομένου του ανθρώπινου στοιχείου, της ασφάλειας, της ευθύνης και της αποζημίωσης για ζημιές, των αλληλεπιδράσεων με λιμάνια, της πλοήγησης, των αντιδράσεων σε συμβάντα και της προστασίας του θαλάσσιου περιβάλλοντος. Περιλάμβανε την αξιολόγηση ενός σημαντικού αριθμού πράξεων της συνθήκης του IMO και τον προσδιορισμό διατάξεων που:

- Εφαρμόστηκαν στο MASS και απέτρεψαν λειτουργίες MASS

- Εφαρμόστηκαν στο MASS, δεν απέτρεψαν τις λειτουργίες MASS και δεν απαιτούσαν καμία ενέργεια
- Εφαρμόστηκαν στο MASS και δεν εμπόδισαν τις λειτουργίες MASS, αλλά ενδέχεται να χρειαστεί τροποποίηση ή διευκρίνιση και/ή ενδέχεται να περιέχει κενά
- δεν έχουν εφαρμογή στις λειτουργίες MASS

Οι βαθμοί αυτονομίας που προσδιορίστηκαν για τους σκοπούς της άσκησης οριοθέτησης ήταν:

- Πρώτος βαθμός: Αποστολή με αυτοματοποιημένες διαδικασίες και υποστήριξη αποφάσεων. Οι ναυτικοί επιβιβάζονται για να χειρίζονται και να ελέγχουν τα συστήματα και τις λειτουργίες του πλοίου. Ορισμένες επιχειρήσεις μπορεί να είναι αυτοματοποιημένες και μερικές φορές χωρίς επίβλεψη, αλλά με ναυτικούς επί του σκάφους έτοιμους να πάρουν τον έλεγχο.
- Βαθμός δύο: Τηλεχειριζόμενο πλοίο με ναυτικούς επί του σκάφους. Το πλοίο ελέγχεται και λειτουργεί από άλλη τοποθεσία. Οι ναυτικοί είναι διαθέσιμοι επί του πλοίου για να αναλάβουν τον έλεγχο και να χειριστούν τα συστήματα και τις λειτουργίες του πλοίου.
- Βαθμός τρίτος: Τηλεχειριζόμενο πλοίο χωρίς ναυτικούς επί του σκάφους: Το πλοίο ελέγχεται και λειτουργεί από άλλη τοποθεσία. Δεν υπάρχουν ναυτικοί στο πλοίο.
- Βαθμός τέταρτος: Πλήρως αυτόνομο πλοίο: Το λειτουργικό σύστημα του πλοίου είναι σε θέση να λαμβάνει αποφάσεις και να καθορίζει ενέργειες από μόνο του.

Το αποτέλεσμα τόνισε ορισμένα ζητήματα υψηλής προτεραιότητας, τα οποία καλύπτουν πολλά μέσα, που θα έπρεπε να αντιμετωπιστούν σε επίπεδο πολιτικής για να καθοριστεί η μελλοντική εργασία. Αυτά περιελάμβαναν την ανάπτυξη της ορολογίας και των ορισμών MASS, συμπεριλαμβανομένου ενός διεθνώς συμφωνημένου ορισμού του MASS και διευκρίνισης της έννοιας του όρου "κύριος", "πλήρωμα" ή "υπεύθυνο πρόσωπο", ιδιαίτερα στους βαθμούς Τρία (τηλεκατευθυνόμενο πλοίο) και Τέσσερα (πλήρως αυτόνομο πλοίο).

Άλλα βασικά ζητήματα που εντοπίστηκαν, περιελάμβαναν την ανάγκη αντιμετώπισης των λειτουργικών και επιχειρησιακών απαιτήσεων του σταθμού/κέντρου τηλεχειρισμού, και τον πιθανό ορισμό ενός τηλεχειριστή ως ναυτικού.

Περαιτέρω κοινά πιθανά κενά και θέματα που εντοπίστηκαν σε διάφορες συνθήκες ασφάλειας, που σχετίζονται με διατάξεις που περιέχουν χειροκίνητες λειτουργίες και συναγερμούς στη γέφυρα. Διατάξεις που σχετίζονται με ενέργειες του προσωπικού (όπως πυρόσβεση, στοιβασία, ασφάλιση φορτίων και συντήρηση), τήρηση κανόνων, επιπτώσεις για έρευνα και διάσωση, και πληροφορίες που απαιτούνται για την ασφαλή λειτουργία του πλοίου.

4.6.2 EU Operational Guidelines

Η εφαρμογή νέων τεχνολογιών πληροφοριών, η ψηφιοποίηση και ο αυτοματισμός ενδέχεται να αλλάξουν γρήγορα τον τρόπο λειτουργίας των θαλάσσιων μεταφορών. Η ανάπτυξη προς πλήρως ή εν μέρει αυτόνομων πλοίων, θα δημιουργήσει ευκαιρίες και προκλήσεις για τον κλάδο, όσον αφορά, την ασφάλεια, τη βιωσιμότητα, τα υφιστάμενα νομικά πλαίσια και τις λειτουργίες, σύμφωνα με τους δύο βασικούς στόχους της Επιτροπής για την ψηφιοποίηση και τη βιωσιμότητα [21].

Η ταχέως μεταβαλλόμενη και ταχεία υιοθέτηση τεχνολογιών που επιτρέπουν τη δοκιμή και λειτουργία αυτόνομων πλοίων επιφανείας, απαιτεί έναν ενημερωμένο ρόλο, όχι μόνο για κάθε χειριστή, αλλά και για τις Υπηρεσίες Κυκλοφορίας Πλοίων, συμπεριλαμβανομένης της παρακολούθησης, διαχείρισης, επικοινωνίας και ελέγχου της κυκλοφορίας πλοίων.

Η ήδη ισχύουσα νομοθεσία της ΕΕ, η οδηγία 2002/59/ΕΚ για την παρακολούθηση της κυκλοφορίας σκαφών, και το σύστημα πληροφοριών (Vessel Traffic Monitoring and Information System - VTMIS), περιλαμβάνει διατάξεις που πρέπει να εξεταστούν υπό την προοπτική των αυτόνομων σκαφών:

- πώς θα επηρεάσουν τις Υπηρεσίες Κυκλοφορίας Πλοίων (Vessel Traffic Services - VTS) και

- τι θα μπορούσε να γίνει για την αντιμετώπιση μελλοντικών προκλήσεων, συμπεριλαμβανομένου του ενδοκοινοτικού εμπορίου από σημείο σε σημείο.

Μια άλλη πτυχή που σχετίζεται άμεσα με την Οδηγία VTMIS, είναι η χρήση εργαλείων επικοινωνίας και παρακολούθησης (Ολοκληρωμένες Ναυτιλιακές Υπηρεσίες που παρέχονται από τον EMSA). Η πρώτη έκδοση των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ [4], [21], για τις δοκιμές θαλάσσιων αυτόνομων πλοίων επιφανείας, έχει αναπτυχθεί για καθοδήγηση και χρήση, προς το συμφέρον της προστασίας της ασφάλειας στη θάλασσα και του θαλάσσιου και παράκτιου περιβάλλοντος. Οι κατευθυντήριες γραμμές είναι το αποτέλεσμα κοινής προσπάθειας των ναυτιλιακών αρχών των κρατών μελών της Ευρωπαϊκής Ένωσης, μαζί με βασικούς ενδιαφερόμενους φορείς του κλάδου, υπό την αιγίδα της ομάδας εμπειρογνωμόνων της MASS, υπό την προεδρία της Ευρωπαϊκής Επιτροπής, με την υποστήριξη του Ευρωπαϊκού Οργανισμού Ναυτιλιακής Ασφάλειας (EMSA).

Αυτές οι επιχειρησιακές κατευθυντήριες γραμμές της ΕΕ, οι οποίες βασίζονται και συμπληρώνουν τις ενδιάμεσες κατευθυντήριες γραμμές για τη MASS που αναπτύχθηκαν από τον Διεθνή Ναυτιλιακό Οργανισμό IMO, δεν αποτελούν τελικό προϊόν. Μάλλον προσαρμόζονται και βελτιώνονται συνεχώς, καθώς θα αποκτάται εμπειρία από δοκιμές καθώς και αποτελέσματα από σχετική έρευνα και μελέτες που χρηματοδοτούνται από την ΕΕ.

Εκτεταμένες δοκιμές έχουν αναγνωριστεί ως προαπαιτούμενο και κρίσιμο βήμα, για την ασφαλή και επιτυχή λειτουργία της μαζικής κυκλοφορίας αυτόνομων πλοίων. Για τη διευκόλυνση των εξελίξεων σε μια ασφαλή προβλέψιμη περιοχή/περιβάλλον, και για την ασφάλεια της ναυσιπλοΐας στο μέλλον, σε κατάσταση μικτής κυκλοφορίας, όπου τόσο επανδρωμένα όσο και μη επανδρωμένα πλοία θα πλέουν στις ίδιες διαδρομές/λιμένες, ξεκίνησε η επίσημη ομάδα διακυβέρνησης σύμφωνα με τη νομοθεσία της ΕΕ να εξετάζει τις διάφορες πτυχές, προληπτικά, ήδη από το 2018. Το έργο έχει τελειοποιηθεί από τότε. Το έργο είναι προσανατολισμένο στο μέλλον και απαιτεί "προκλητικές συμβατικές έννοιες και λειτουργίες".

Με την ευκαιρία της 2ης Διεθνούς Συνόδου Κορυφής για την Αυτονομία και την Αειφορία Πλοίων, στις 30 Νοεμβρίου 2020, τα μέλη της ομάδας εμπειρογνωμόνων EU MASS, προωθώντας ένα συνεχές θετικό πνεύμα και ενισχυμένη συνεργασία και συντονισμό μεταξύ όλων των εμπλεκόμενων μερών, συμπεριλαμβανομένης της ενδιαφερόμενης βιομηχανίας, για την ασφαλή, βιώσιμη και αποτελεσματική ανάπτυξη της αυτόνομης ναυτιλίας, ενέκρινε τις ακόλουθες βασικές αρχές:

- Αρχή για τη χρήση των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ για δοκιμές MASS και ανταλλαγή πληροφοριών εντός και μεταξύ των κρατών μελών της ΕΕ. για να εντοπιστούν οι ανάγκες για περαιτέρω ανάπτυξη καθώς προκύπτουν νέες προκλήσεις
- Παρουσίαση και δημοσιοποίηση των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ με κατάλληλα μέσα
- Ενημέρωση για τις Επιχειρησιακές Κατευθυντήριες Γραμμές της ΕΕ στον Διεθνή Ναυτιλιακό Οργανισμό IMO, και σε άλλα κατάλληλα forum ενδιαφερομένων, καθώς και σε διεθνείς εταίρους
- Εργασία για τη συμπερίληψη των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ σε περιφερειακές συμφωνίες/σχέδια
- Υποστήριξη της χρήσης του Συστήματος Ναυτιλιακών Πληροφοριών και Ανταλλαγών της Ένωσης, που παρέχει Ολοκληρωμένες Ναυτιλιακές Υπηρεσίες και την περαιτέρω ανάπτυξή του για την ασφαλή διαχείριση, παρακολούθηση, επικοινωνία και έλεγχο αυτόνομων πλοίων και ναυτιλίας
- Συνέχιση της εργασίας στο πλαίσιο της ομάδας εμπειρογνωμόνων MASS, μεταξύ άλλων, για:

- Συνεχή βελτίωση των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ, σε όλες τις πτυχές της, συμπεριλαμβανομένης της υιοθέτησης από σχετικά έργα και μελέτες έρευνας και ανάπτυξης, για την αντιμετώπιση των προκλήσεων και την επίτευξη ευθυγράμμισης προτύπων και κοινής κατανόησης για δοκιμές και λειτουργίες θαλάσσιων αυτόνομων πλοίων επιφανείας, συμπεριλαμβανομένων των λιμένων.
- Συγκέντρωση και ανταλλαγή εμπειριών και ανάπτυξη πρακτικών διαδικασιών για

την επιχειρησιακή χρήση των επιχειρησιακών κατευθυντήριων γραμμών της ΕΕ, συμπεριλαμβανομένων ασκήσεων, εικονικών ασκήσεων, με βάση το έργο του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στη Θάλασσα (EMSA) και επαφές με άλλα forum, πολιτικά και στρατιωτικά.

- Ανάπτυξη, σε εύθετο χρόνο, με την υποστήριξη του EMSA, κατάλληλης εκπαίδευσης σχετικά με τις επιχειρησιακές κατευθυντήριες γραμμές της ΕΕ, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, της επικοινωνίας και της χρήσης του συστήματος θαλάσσιων πληροφοριών και ανταλλαγής πληροφοριών της Ένωσης.

- Βελτίωση της μεθοδολογίας εκτίμησης κινδύνου, με βάση την έρευνα αιχμής.

- Περαιτέρω διερεύνηση αναγκών, απαιτήσεων και προτύπων για απρόσκοπτες και ολοκληρωμένες ροές πληροφοριών και επικοινωνίας μεταξύ αυτόνομων πλοίων/κέντρων τηλεχειρισμού με εθνικές/περιφερειακές υπηρεσίες κυκλοφορίας πλοίων, καθώς και μεταξύ αρχών και φορέων εκμετάλλευσης.

Από το 2019, οι Διεθνείς Σύνοδοι Κορυφής για την Αυτονομία και την Αειφορία των Πλοίων, πραγματοποιούνται εναλλάξ μεταξύ του Νορβηγικού Forum για Αυτόνομα Πλοία (NFAS), και της Ευρωπαϊκής Επιτροπής, με την υποστήριξη του νορβηγικού υπουργείου Εμπορίου και Βιομηχανίας. Με βάση την καθιερωμένη συνεργασία, η Σύνοδος λαμβάνει χώρα σε διάφορες τοποθεσίες, παρέχοντας ένα forum για διεθνείς ανταλλαγές, σχετικά με έξυπνα και βιώσιμα αυτόνομα πλοία, ενισχύοντας το διάλογο της βιομηχανίας, των ερευνητών, των δοκιμαστικών έργων και των διοικήσεων. Τα ενδιαφερόμενα μέρη και οι αρχές καλούνται πάντα να παρακολουθούν τις επόμενες εκδόσεις των Διεθνών Συνόδων Κορυφής για την Αυτονομία και την Αειφορία των Πλοίων.

Οι ντιρεκτίβες (guidelines) της Ευρωπαϊκής Ένωσης συμπληρώνουν τις αντίστοιχες κατευθυντήριες γραμμές του οργανισμού IMO.

4.7 Κίνδυνοι από Κυβερνο-επιθέσεις. Δράσεις αντιμετώπισης τους

Η αυτόνομη μεταφορά εμπορευμάτων και επιβατών αναμένεται να αλλάξει ριζικά τη θαλάσσια κυκλοφορία. Τσ σκάφη με ανθρώπινο πλήρωμα και τα αυτόνομα σκάφη, θα πρέπει να μοιράζονται τις θάλασσες, στο εγγύς μέλλον. Καθώς τα αυτόνομα σκάφη λειτουργούν σε διάφορα επίπεδα αυτονομίας ή ελέγχου, αυτό συνεπάγεται ότι η κυβερνο-ασφάλεια επί του πλοίου θα ποικίλλει. Τα σχήματα αυτόνομης ναυτιλίας, επιφανείας ή υποβρύχια, εμπορικά ή στρατιωτικά, παρέχουν πλεονεκτήματα για συγκεκριμένες αποστολές. Οι επιπτώσεις των κυβερνο-επιθέσεων σε αυτόνομα σκάφη δεν είναι ακόμη εμφανείς, και είναι πιο αποτελεσματικό να εξετασθούν τα θέματα ασφάλειας στην αρχική φάση ανάπτυξης και σχεδιασμού αυτής της τεχνολογίας. Αρχικά αυτό περιλαμβάνει την εξέταση πιθανών απειλών και αντιμέτρων σε προγενέστερο στάδιο. Η έλλειψη ασφάλειας των αυτόνομων πλοίων, θα μπορούσε να οδηγήσει σε περιβαλλοντικές καταστροφές, που θα προκληθούν από συγκρούσεις με άλλα πλοία και λιμενικές εγκαταστάσεις, ενδεχόμενη πειρατεία πλοίων, κλοπή ή εκβιασμός για τα πλοία και τα εμπορεύματα τους και ενδεχόμενα ανθρώπινες απώλειες. Ωστόσο, έχει δοθεί σχετικά λίγη προσοχή μέχρι στιγμής, στην ασφάλεια των αυτόνομων σκαφών, σε σύγκριση με άλλες παρόμοιες εφαρμογές, όπως π.χ τα αυτόνομα αυτοκίνητα, τα drones και τα μη επανδρωμένα αεροσκάφη [27].

Η εμπορευματοποίηση μη επανδρωμένων ή πλήρως αυτόνομων πλοίων, δεν αναμένεται σε πλήρη εφαρμογή μέχρι τις δεκαετίες του 2030 έως 2040, με βάση το ρυθμό εξέλιξης και αποδοχής της τεχνολογίας. Ωστόσο, οι κίνδυνοι ασφάλειας που συνδέονται με τη λειτουργία αυτών των πλοίων, θα πρέπει να λαμβάνονται υπόψη από τις αρχικές φάσεις της κατάρτισης του σχεδιασμού, για να καταστεί δυνατός ο εμπλουτισμός των διαδικασιών ασφαλείας εξαρχής, με πλήρη αντίληψη των πιθανών επιπτώσεων στην ασφάλεια και των πιθανών αντίμετρων.

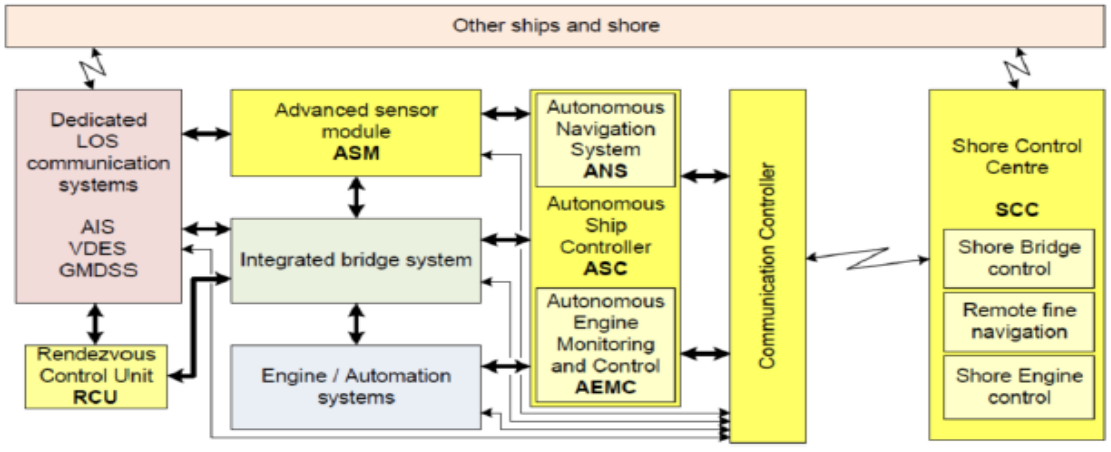
Η κυβερνο-ασφάλεια είναι επίσης σημαντική, ακόμη και με τα πλοία που διαθέτουν πληρώματα για τη λειτουργία με αυτοματοποιημένα συστήματα IT/OT, καθώς ορισμένες λειτουργίες από αυτά τα πλοία, εξαρτώνται επίσης σε μεγάλο βαθμό από την πληροφορική. Με βάση τις τρέχουσες συνθήκες οι ναυτικοί επί του σκάφους είναι απίθανο να είναι ειδικοί σε θέματα ασφάλειας Πληροφοριακών Συστημάτων.

4.7.1 Δομικά Συστήματα Αυτόνομου Πλοίου

Το έργο MUNIN, είναι ένα συλλογικό ερευνητικό έργο από οκτώ οργανισμούς, με διάρκεια από το 2012 έως το 2015, συγχρηματοδοτούμενο από την Ευρωπαϊκή Επιτροπή, που προσδιόρισε τα κύρια στοιχεία/συστήματα ενός αυτόνομου πλοίου ως εξής [28], [29]:

- Δίκτυο Αισθητήρων (Advanced Sensor Module - ASM): Περιλαμβάνει ραντάρ, βίντεο και άλλα συστήματα για παρακολούθηση, ανίχνευση αντικειμένων και γενικά ανίχνευση του περιβάλλοντος του πλοίου.
- Ολοκληρωμένο Σύστημα Γέφυρας (Integrated Bridge System - IBS): Περιλαμβάνει όλα τα συστήματα και τον εξοπλισμό γέφυρας που σχετίζονται με την ναυσιπλοΐα του πλοίου.
- Συστήματα Κινητήρα/Αυτοματισμού (Engine Automation Systems - EAS:) Περιλαμβάνει όλα τα συστήματα που σχετίζονται με την παραγωγή ενέργειας και την πρόωση. Το έργο MUNIN υπέθεσε επίσης ότι θα περιλάμβανε αυτοματισμούς που σχετίζονται με τα συστήματα ασφαλείας, τα θαλασσέρματα, τον έλεγχο φορτίου, κ.λπ.
- Αυτόνομος Ελεγκτής Πλοίου (Autonomous Ship Controller - ASC): περιλαμβάνει τις πρόσθετες λειτουργίες ελέγχου και παρακολούθησης που πρέπει να ενεργοποιηθούν για την αυτόνομη λειτουργία. Περιλαμβάνει την Αυτόνομη Παρακολούθηση και τον Έλεγχο του Κινητήρα (Autonomous Engine Monitoring and Control - AEMC), περιλαμβάνει επίσης λειτουργίες διαχείρισης επικοινωνίας για όλες τις επικοινωνίες μεταξύ του σκάφους και του SCC μέσω του Ελεγκτή Επικοινωνιών.
- Τα αποκλειστικά συστήματα επικοινωνίας οπτικής επαφής με άλλα πλοία και εγκαταστάσεις στην ξηρά, συμπεριλαμβανομένων του Συστήματος Πληροφοριών Διαχείρισης Κυκλοφορίας Πλοίων (VTMIS) και τα Κέντρα Συντονισμού και Διάσωσης (Maritime Rescue Coordination Centres - MRCC). Περιλαμβάνει AIS, VDES (VHF Data Exchange System), τη 2η γενιά AIS με χρήση δορυφορικών επικοινωνιών και το GMDSS και το Safety System (το υποχρεωτικό σύστημα επικοινωνίας σημάτων έκτακτης ανάγκης).
- Η Μονάδα Ελέγχου Ραντεβού (Rendezvous Control Unit - RCU): είναι ένα σύστημα που επιτρέπει σε μια Ενσωματωμένη Ομάδα Ελέγχου να αναλάβει τον έλεγχο του πλοίου προσωρινά, ή Ομάδα Ελέγχου Έκτακτης Ανάγκης για την ανάκτηση του σκάφους κατά τη διάρκεια βλάβης.
- Το SCC περιέχει όλες τις χερσαίες λειτουργίες για τη διαχείριση ενός αυτόνομου πλοίου. Περιλαμβάνει και απομακρυσμένη δυνατότητα ναυσιπλοίας, μονάδες ελέγχου γέφυρας και κινητήρα, που μπορούν να χρησιμοποιηθούν για τον άμεσο έλεγχο του πλοίου. Ο αρχικός προγραμματισμός του ταξιδιού εκτελείται από το SCC.

Το σχήμα που ακολουθεί παρουσιάζει έναν εποπτικό έλεγχο των προηγούμενων συστημάτων και τη διασύνδεση τους, για τα αυτόνομα πλοία:



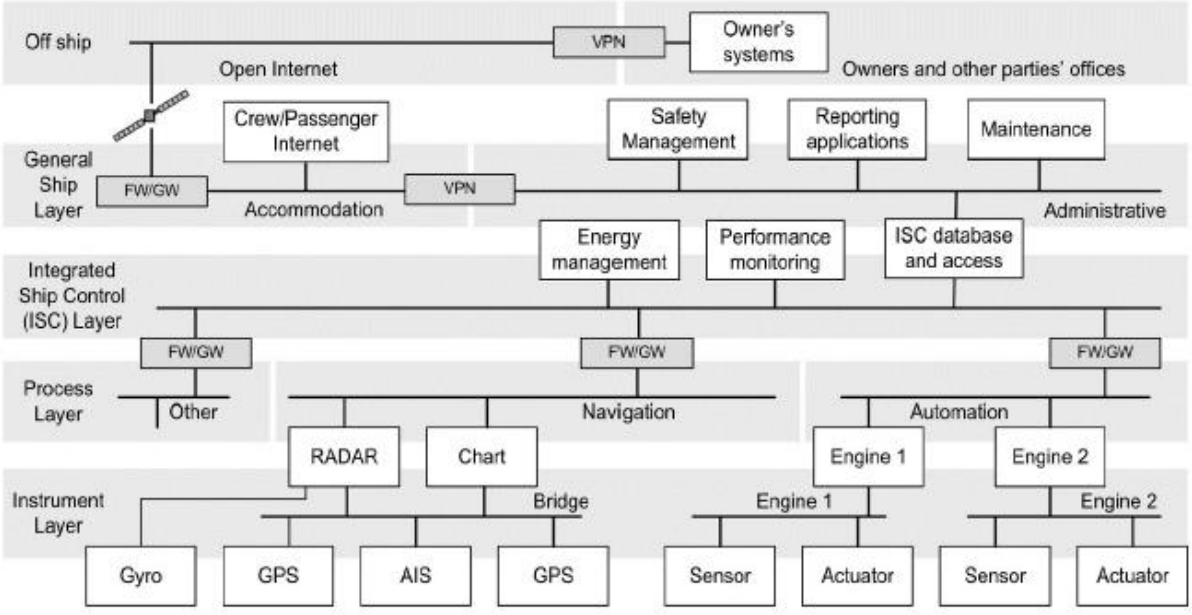
Σχήμα 19: Εποπτική παρουσίαση των συστημάτων και των αλληλεπιδράσεων για αυτόνομο πλοίο [27]

4.7.2 Αρχιτεκτονική Διαστρωμάτωση των Συστημάτων Αυτόνομου Πλοίου

Στο σχήμα που ακολουθεί, το επίπεδο οργάνων στο κάτω μέρος αποτελείται από αισθητήρες πλοήγησης, όπως το γυροσκόπιο, το AIS και το GNSS, που απαιτούνται για την πλοήγηση, τους εσωτερικούς αισθητήρες αυτοματισμού, όπως αυτοί για την πίεση, θερμοκρασία, ροπή και κραδασμούς, και συναφείς ενεργοποιητές (actuators) για τις λειτουργίες των μηχανημάτων του πλοίου. Στη συνέχεια, οι διάφοροι αισθητήρες και ενεργοποιητές, θα ομαδοποιηθούν με βάση τους ρόλους τους στο επίπεδο διαδικασίας και θα συνδεθούν στα στοιχεία του συστήματος στο Ενσωματωμένο Επίπεδο Ελέγχου του Πλοίου, όπου πραγματοποιούνται βασικές λειτουργίες που σχετίζονται με την θέση του πλοίου. Το Γενικό Επίπεδο Διοίκησης του Πλοίου (General Ship Layer) στην κορυφή του Integrated Ship Control Layer, είναι το επίπεδο, στο οποίο εκτελούνται επιπλέον διοικητικές δραστηριότητες όπως, η υποβολή εκθέσεων και η τήρηση αρχείων. Στην κορυφή της αρχιτεκτονικής είναι το Off Ship Layer, το οποίο παρέχει δυνατότητες επικοινωνίας με εξωτερικά μέρη, συμπεριλαμβανομένου του SCC. Αυτή η αρχιτεκτονική κατάτμηση των λειτουργιών, είναι παρόμοια με το μοντέλο αναφοράς Purdue14 που χρησιμοποιείται ευρέως για την αντιπροσώπευση γενικών συστημάτων βιομηχανικού ελέγχου (ICS) [31], με τη διαφορά ότι εδώ δεν υπάρχουν ανθρώπινες διεπαφές.

Η πρώτη έρευνα που εξέτασε διάφορους τύπους δυνατοτήτων για απειλές κυβερνο-ασφάλειας για αυτόνομα πλοία, εντόπισε επτά σημεία επίθεσης τα οποία οι επιτιθέμενοι θα μπορούσαν να εκμεταλλευτούν:

- Συστήματα εντοπισμού θέσης
- Αισθητήρες
- Αναβαθμίσεις υλικού - λογισμικού
- Καταγραφείς δεδομένων ταξιδιού (παρόμοιες συσκευές με το "μαύρο κουτί" των αεροπλάνων)
- Ενδοπλοϊκά δίκτυα
- Επικοινωνίες σκάφους προς ξηρά, συμπεριλαμβανομένων των δορυφορικών και κυψελοειδών (cellular) συστημάτων και
- Απομακρυσμένα συστήματα στο σκάφος, προσβάσιμα από το SCC



Σχήμα 20: Αρχιτεκτονική διασύνδεση των συστημάτων Αυτόνομου πλοίου [27]

Εντόπισαν επίσης, τύπους επίθεσης που ισχύουν για αυτές τις διεπαφές με έγχυση κακόβουλου κώδικα μέσω δικτύου, με αφαιρούμενες συσκευές ή ενημέρωση υλικού/λογισμικού, παραποίηση ή τροποποίηση πακέτων ενδοπλοϊκού δικτύου, πλαστογράφηση GNSS, πλαστογράφηση AIS, εμπλοκή σήματος (jamming) ενάντια στο GNSS και διάφορους αισθητήρες, και υποκλοπή και διακοπή της σύνδεσης επικοινωνίας μεταξύ του σκάφους και του SCC. Άλλοι ερευνητές υποστήριξαν ότι τα τυπικά σενάρια απειλής στα αυτόνομα πλοία, θα βασίζονταν σε: αφαιρούμενες συσκευές που εισάγονται στο ενσωματωμένο σύστημα αναλαμβάνοντας τον έλεγχο του σκάφους μέσω συνδέσμου επικοινωνίας, εμπλοκή GNSS, παρεμπόδιση των επικοινωνιών μεταξύ του σκάφους και του SCC, και πλαστογράφηση GNSS. Ωστόσο, αυτά τα έργα δεν κάλυπταν όλο το φάσμα των κυβερνο-απειλών στα αυτόνομα πλοία και δεν δίνουν κατευθύνσεις - οδηγίες για την αντιμετώπιση τους. Σχετικά με τη διοικητική και τεχνική ασφάλεια, οι απαιτήσεις για τα αυτόνομα ή μη επανδρωμένα πλοία, οι κάποιοι ερευνητές πρότειναν ένα ευρύ φάσμα ελέγχου ασφαλείας, παρόμοιο με το ISO/IEC 27001 σε 13 κατηγορίες:

- Ασφάλεια ανθρώπινου δυναμικού
- Διαχείριση περιουσιακού στοιχείου
- Έλεγχος πρόσβασης
- Κρυπτογραφία
- Φυσική και περιβαλλοντική ασφάλεια
- Ασφάλεια λειτουργιών
- Ασφάλεια επικοινωνιών
- Απόκτηση συστήματος
- Ανάπτυξη και συντήρηση
- Σχέσεις προμηθευτών
- Διαχείριση συμβάντων
- Διαχείριση επιχειρηματικής συνέχειας και
- Συμμόρφωση

4.7.3 Κυβερνο-απειλές για τα Αυτόνομα Πλοία

Τα αυτόνομα πλοία έχουν πλεονεκτήματα, όπως μειωμένο λειτουργικό κόστος, και εξάλειψη ανθρώπινων απωλειών σε επικίνδυνες αποστολές. Ωστόσο, η φύση των αυτόνομων επιχειρήσεων, αυξάνει την επίθεση επιφάνειας για κυβερνο- και φυσικές επιθέσεις. Ειδικότερα, ο έλεγχος των αυτόνομων πλοίων, θα μπορούσε να έχει ως αποτέλεσμα ολική ή μερική καταστροφή. Οι επιτιθέμενοι μπορεί να παραβιάσουν αυτόνομα πλοία, να αλλάξουν τη διαδρομή του πλοίου και να ξεκινήσουν μια "επίθεση αυτοκτονίας", να κλέψουν το φορτίο, να αιχμαλωτίσουν το σκάφος για οικονομικό εκβιασμό ή να αιχμαλωτίσουν αυτόνομα πλοία για να κλέψουν τεχνολογίες ή οπλικά συστήματα επί των πλοίων.

Στην παρούσα εργασία, οι σημαντικές απειλές που περιβάλλουν τα αυτόνομα πλοία ταξινομούνται σε εννέα κατηγορίες. Είναι επιθέσεις για να:

- Διαταράξουν τα σήματα RF
- Εξαπάτησουν ή υποβαθμίσουν τους αισθητήρες
- Υποκλέψουν ή τροποποιήσουν τις επικοινωνίες
- Παρεμβάλλουν τα συστήματα ΟΤ
- Προκαλέσουν ζημιά σε συστήματα πληροφορικής
- Προκαλέσουν ζημιά στο AI που χρησιμοποιείται για αυτόνομες λειτουργίες
- Προκαλέσουν ζημιά σε αλυσίδες συστημάτων
- Αποκτήσουν φυσική πρόσβαση και
- Βλάψουν το SCC

4.7.4 Αντιμετώπιση των κυβερνο-απειλών στα Αυτόνομα Πλοία

Όταν τα αυτόνομα πλοία επιχειρούν στην ανοιχτή θάλασσα, μακριά από το SCC ή βάσεις στην στεριά, θα είναι λιγότερο ευάλωτα λόγω του περιορισμένου εύρους ζώνης στις επικοινωνίες. Εάν επιβαίνουν ναυτικοί, μπορούν να παρακάμψουν τα αυτόνομα συστήματα σε χειροκίνητο έλεγχο ή απλά να σταματήσουν το πλοίο, εάν συμβεί κάποιο απρόβλεπτο γεγονός. Ωστόσο, όταν ένα σκάφος χωρίς πλήρωμα δέχεται επίθεση και το κανάλι Ελέγχου και Διοίκησης (C2) του έχει διακοπεί, θα χρειαστεί πολύς χρόνος για μια ομάδα μηχανικών ώστε να επιβιβαστούν στο σκάφος για να ανακτήσουν τον έλεγχο του. Κατά τη διάρκεια αυτής της περιόδου, οι επιτιθέμενοι μπορεί να έχουν ήδη επιτύχει τους στόχους τους. Τα αυτόνομα στρατιωτικά πλοία που δεν έχουν επικοινωνία με βάση για πολύ καιρό και κινούνται σε ξένα χωρικά ύδατα, διατρέχουν πολύ υψηλότερο επίπεδο κινδύνου, απαιτώντας περισσότερες δικλείδες ασφάλειας για την παροχή ανθεκτικότητας σε κυβερνο- και φυσικές επιθέσεις. Ωστόσο, τα αυτόνομα σκάφη που συνεχώς ταξιδεύουν μεταξύ δύο τελικών σημείων σε μια διαδρομή, μπορεί να έχουν χαμηλότερο επίπεδο κινδύνου, επειδή μπορεί να είναι κοντά σε σημεία παρακολούθησης και μια ομάδα μηχανικών μπορεί να έχει φυσική πρόσβαση στο σκάφος πιο γρήγορα.

Θα πρέπει να εφαρμοστεί μια προσέγγιση διαχείρισης κινδύνου κατά τον σχεδιασμό, την ανάπτυξη και την λειτουργία για τα αυτόνομα πλοία, που να εντοπίσουν και να εφαρμόσουν κατάλληλα αντίμετρα ανάλογα με τον κίνδυνο. Είναι ακόμη ασαφές πότε θα είναι διαθέσιμα πλήρως αυτοματοποιημένα αυτόνομα σκάφη για πρακτικές εμπορικές ή στρατιωτικές επιχειρήσεις. Ωστόσο, είναι ζωτικής σημασίας να διασφαλιστεί ότι οι παράγοντες ασφαλείας εφαρμόζονται από τον σχεδιασμό και τις αρχικές του φάσεις (security by design), διότι η εξέταση της ασφάλειας στα πρώτα στάδια της ανάπτυξης θα επιτρέψει την ανάπτυξη μέτρων ασφαλείας που πρέπει να εφαρμοστούν με αποτελεσματικό τρόπο, εξοικονομώντας παράλληλα κόστος, σε σύγκριση με την προσθήκη τους μετά την ανάπτυξη.

5 Μέτρα Περιορισμού - Πρόληψης - Αντιμετώπιση Κυβερνο-επιθέσεων

Η κατανόηση των θαλάσσιων απειλών στον κυβερνοχώρο, των τρωτών σημείων και των κινδύνων, είναι η βάση προκειμένου ένας οργανισμός να προετοιμάσει την πολιτική, τις διαδικασίες και δράσεις/ενέργειές του για την καθοδήγηση, τις απαιτούμενες αγορές εξοπλισμού, την οργάνωσης της αρχιτεκτονικής των δικτύων, το σχεδιασμό, την στελέχωση, την κατάρτιση, τις συμφωνίες παροχής υπηρεσιών με εξωτερικούς φορείς τηλεπικοινωνιών και τους πωλητές των υπηρεσιών, τις πολιτικές συνεργατών εφοδιαστικής αλυσίδας και άλλες σχετικές λειτουργίες και εργασίες που σχετίζονται με το MTS. Οι πολιτικές δράσης και οι διαδικασίες, καθοδηγούν τις καθημερινές δραστηριότητες στο χώρο της ναυτιλίας για τα θέματα κυβερνο-ασφάλειας. Επίσης, οι οργανισμοί που χειρίζονται τα θέματα της ναυτιλίας χρειάζεται να καθορίσουν διαδικασίες αντιμετώπισης των περιστατικών κυβερνο-επιθέσεων, να καταστρώσουν τα σχέδια έκτακτης ανάγκης (Emergency Response Plan) και τις διαδικασίες επιχειρησιακής συνέχειας (Business Continuity Plan) [1], [3].

Ο σωστός σχεδιασμός της κυβερνο-ασφάλειας είναι ένα μεγάλο και σύνθετο πρόβλημα. Αυτή η ενότητα παρέχει μία εισαγωγή σε ορισμένα και τα πλαίσια που είναι διαθέσιμα στη ναυτιλιακή βιομηχανία, ώστε να βοηθήσει στην ανάπτυξη πολιτικών και διαδικασιών κυβερνο-άμυνας, καθώς και τις απαιτούμενες ενέργειες για ορισμένους κλάδους και κυβερνητικούς οργανισμούς που παρέχουν οδηγίες για το MTS και τα θέματα που πρέπει να αντιμετωπίσουν στον κυβερνοχώρο.

Οι φορείς - οργανισμοί που ασχολούνται με τα θέματα κυβερνο-ασφάλειας στο MTS, σε παγκόσμιο επίπεδο, είναι οι ακόλουθοι [1]:

- National Institute of Standards and Technology (NIST)
- BIMCO et al Industry Consortium
- International Maritime Organization (IMO)
- American Bureau of Shipping (ABS)
- European Union Agency for Cybersecurity (ENISA)
- Institution of Engineering and Technology (IET)
- International Association of Ports and Harbors (IAPH)
- U.S. Coast Guard (USCG)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Industry Groups

Όλοι οι παραπάνω φορείς έχουν ως στόχο την δημιουργία διεργασιών - διαδικασιών (procedures), καθώς και να καθορίσουν τις διοικητικές και όποιες άλλες δομές απαιτούνται για την αντιμετώπιση των θεμάτων κυβερνο-ασφάλειας στο MTS.

Το Εθνικό Ινστιτούτο Κυβερνοασφάλειας των ΗΠΑ NIST [111], αναδείχθηκε διεθνώς ως μία κοινή αναφορά για μεγάλο αριθμό οδηγιών, που σχετίζονται με την κυβερνο-άμυνα και τις συστάσεις βέλτιστων πρακτικών στο χώρο αυτό. Οι οδηγίες που χει εκδόσει το NIST, μπορούν να χρησιμοποιηθούν ως πρότυπα με τα οποία μπορεί να δημιουργηθεί ένα προφίλ διεργασιών, κατηγοριών, υπο-κατηγοριών και συνιστώμενων πρακτικών που σχετίζονται με συγκεκριμένους οργανισμούς. Η Ακτοφυλακή των ΗΠΑ (USCG), για παράδειγμα, έχει υιοθετήσει το πρότυπο θαλάσσιας ασφάλειας στον κυβερνοχώρο που σχετίζεται με τη μεταφορά υγρών, τις υπεράκτιες δραστηριότητες, τις επιχειρήσεις επιβατηγών πλοίων και το μοντέλο Energy's Cybersecurity Capability Maturity Model (C2M2), από το NIST.

Η Κοινοπραξία Baltic and International Maritime Council - BIMCO et al [112], συγκροτήθηκε από περισσότερες από 20 ναυτιλιακές εταιρειες και οργανισμούς, συμπεριλαμβανομένου του Βαλτικού και Διεθνούς Ναυτιλιακού Συμβουλίου (BIMCO), του Διεθνούς Ναυτιλιακού Επιμελητηρίου, τη Διεθνή Ένωση Ναυτικών Insurance, και το Παγκόσμιο Συμβούλιο Ναυτιλίας. Η κοινοπραξία κυκλοφόρησε την έκδοση 4 για τις κατευθυντήριες γραμμές για την κυβερνο-ασφάλεια των πλοίων, το 2020. Οι στόχοι της έκδοσης είναι:

- Δημιουργία επίγνωσης της ασφάλειας, και του εμπορίου από κινδύνους που συνδέονται με την ανεπαρκή προστασία από κυβερνο-απειλές

- Προστασία των υποδομών πληροφορικής (IT/OT) των πλοίων και των δεδομένων που χρησιμοποιούνται στο περιβάλλον των πλοίων
- Διαχειριση και έλεγχος της πρόσβασης των χρηστών IT στις πληροφορίες
- Διαχειριση της επικοινωνίας μεταξύ πλοίου και ακτής
- Αναπτύξη και εφαρμογή ενός σχεδίου αντιμετώπισης περιστατικών στον κυβερνοχώρο που βασίζεται σε ένα μοντέλο αξιολόγησης κινδύνου

Σχήμα 21: Το σχήμα προστασίας Cybersecurity από την BIMCO [1]

Ο IMO [5] είναι μια υπηρεσία του OHE. Δεν είναι ένας οργανισμός προτύπων, αλλά αναπτύσσει ένα ρυθμιστικό πλαίσιο για τη διεθνή ναυτιλία που ασχολείται με την ασφάλεια, τις περιβαλλοντικές επιδράσεις, τα νομικά ζητήματα, και γενικότερα την ασφάλεια και τη διεθνή τεχνική συνεργασία.

Ενώ ο IMO δεν έχει παρουσιάσει λεπτομερείς προδιαγραφές κυβερνο-άμυνας για τη ναυτιλιακή βιομηχανία, τα έγγραφα καθοδήγησής του, προορίζονται να υποστηρίξουν την ασφάλεια που είναι επιχειρησιακά ανθεκτική στις κυβερνο-απειλές. Τα πρωτογενή έγγραφα κυβερνο-ασφάλειας του IMO, αποτελούν ένα σύνολο υψηλού επιπέδου συστάσεων για την προστασία της ναυτιλίας από τρέχουσες και αναδυόμενες απειλές στον κυβερνοχώρο. Αυτά τα έγγραφα καθοδήγησης, περιγράφουν ευάλωτα συστήματα επί του πλοίου, συμπεριλαμβανομένων των συστημάτων γεφυρών, διαχείρισης, τα συστήματα διαχείρισης φορτίου, τα συστήματα πρόωσης, και τα συστήματα επικοινωνίας. Οι οδηγίες του περιγράφουν τα βήματα διαχείρισης κινδύνου που πρέπει να εφαρμόζονται κατά τη δημιουργία ενός σχεδίου κυβερνο-άμυνας. Οι συστάσεις σημειώνουν επίσης, ότι τα συστήματα IT και OT έχουν διαφορετικούς σκοπούς και χαρακτηριστικά, που οδήγησαν στην αναφορά της αυτοματοποίησης επί των πλοίων. Ενώ αυτό το έγγραφο δεν αφορά άμεσα τα αυτόνομα σκάφη, παρήγαγε κατευθυντήριες γραμμές που αφορούν στην ασφαλή, και περιβαλλοντικά ορθή Επιχείρηση των θαλάσσιων αυτόνομων πλοίων επιφανείας (MASS).

Το έγγραφο της ABSG Consulting CYBERSAFETY® [113] ναυτιλιακής καθοδήγησης στον κυβερνοχώρο, ακολουθεί μια προσέγγιση από πάνω προς τα κάτω (top-down), για τη διαχείριση κινδύνου. Το πλαίσο της ABSG είναι δομημένο γύρω από ένα σύνολο βασικών εργασιών, που θα έπρεπε να είναι μέρος της υπάρχουσας στρατηγικής κυβερνο-άμυνας ενός ναυτιλιακού οργανισμού, οργανωμένη σε τρεις κατηγορίες: πρακτικές και διαδικασίες (Εργασίες 1 - 3), διαχείριση κινδύνου (Εργασίες 4 - 6) και προστασία πόρων και περιουσιακών στοιχείων (Εργασίες 7 - 9). Οι Εργασίες 10 - 23 περιγράφουν επιπλέον 14 προηγμένες δυνατότητες σε αυτές τις ίδιες τρεις κατηγορίες,

προσθέτοντας βάθος και εύρος στην κυβερνο-άμυνα του οργανισμού εφαρμογής, συμπεριλαμβανομένων των προτύπων κυβερνο-άμυνας, των πληροφοριακών απειλών, την αξιολόγηση ευπάθειας και τη δοκιμή συστημάτων.

Σχήμα 22: Το σχήμα διαχείρισης κινδύνων Cybersecurity από την ABSG [1]

Ο ENISA [114] παρέχει συστάσεις και εργαστήρια για την ασφάλεια στον κυβερνοχώρο, για την υποστήριξη, ανάπτυξη και εφαρμογή πολιτικής, και συνεργάζεται με επιχειρησιακές κυβερνο-ομάδες (CERT) σε όλη την Ευρώπη. Είναι το όργανο της ΕΕ που δημιουργεί τις πολιτικές (πχ NIS2), κρατάει υποτύπωση των περιστατικών που συμβαίνουν στον Ευρωπαικό χώρο σε κρίσιμες υποδομές και συμβουλεύει την Κομισιόν και το Ευρωκοινοβούλιο σε θέματα Κυβερνοασφάλειας, συμπεριλαμβανομένης και της Ναυτιλίας.Ο ρόλος του εξαπλώνεται σε τεχνικό και επιχειρησιακό επίπεδο μέσω του CSIRT Network (που συμμετάσχουν τα Ευρωπαικά Κέντρα Απόκρισης σε Κυβερνοπεριστατικά (CERT/CSIRT)) και μέσω του CyClone (Cyber Crisis Liaison Organization Network) που συμμετάσχουν οι Εθνικές Αρχές Κυβερνοασφάλειας των Ευρωπαικών χωρών. Ο ENISA έχει εκδόσει δύο συστάσεις σχετικά με το MTS.

Το IET [115] είναι ένα πολυ-επιστημονικό ινστιτούτο μηχανικής και τεχνολογίας στο Η.Β. Όπως και ο ENISA, το IET δεν έχει συγκεκριμένο ρόλο στα ναυτιλιακά πρότυπα, αν και έχει δύο οδηγούς βέλτιστων πρακτικών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο για τη θάλασσα.

Η IAPH [116] είναι μια παγκόσμια συμμαχία, ενας μη-κυβερνητικός Οργανισμός που αντιπροσωπεύει περισσότερα από 300 λιμάνια και επιχειρήσεις σχετιζόνενες με τα λιμάνια σε 88 χώρες. Το 2021 εξέδωσε μια οδηγία με κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο για λιμενικές εγκαταστάσεις. Το ακροατήριο στο οποίο κυρίως απευθύνεται το εγγράφο, είναι οι υπεύθυνοι λήψης εκτελεστικών αποφάσεων στα λιμάνια. Οι κατευθυντήριες γραμμές είναι σε μεγάλο βαθμό μη τεχνικού χαρακτήρα, όπου το πρώτο ήμισυ του εγγράφου παρέχει μια ευρεία κάλυψη της διαχείρισης κινδύνων στον κυβερνοχώρο για τον ναυτιλιακό τομέα. Το υπόλοιπο του εγγράφου περιγράφει ορισμένες τεχνικές - αντίμετρα στον κυβερνοχώρο, ανταλλαγή πληροφοριών στον κλάδο, εργατικό δυναμικό και εκπαίδευση, αντιμετώπιση περιστατικών και αποκατάσταση και βελτίωση της διαδικασίας.

Η Ακτοφυλακή των ΗΠΑ USCG [117] είναι μια υπηρεσία του Department of Homeland Security - DHS. Η USCG έχει μοναδικό ρόλο στον αμερικανικό στρατό, με λειτουργία επιβολής του νόμου, τόσο στις ΗΠΑ όσο και στα διεθνή ύδατα με μια ομοσπονδιακή ρυθμιστική λειτουργία. Οι λειτουργίες της USCG περιλαμβάνουν έρευνα και διάσωση, ασφάλεια σε όλο το MTS, δίωξη ναρκωτικών, επιθεώρηση λιμενικών εγκαταστάσεων, συντήρηση βοηθημάτων ναυσιπλοΐας και επιβολή κανονισμών στην αλιεία. Τα τελευταία χρόνια, η USCG έχει εισαγάγει αρκετές πρωτοβουλίες για βελτίωση της άμυνας στον κυβερνοχώρο και στο MTS, συμπεριλαμβανομένων:

- Δημιουργία αναπτυσσόμενων Ομάδων Κυβερνο-προστασίας που μπορούν να προσφέρουν απόκριση σε συμβάντα στον κυβερνοχώρο σε πραγματικό χρόνο
- Δημιουργία υπο-επιτροπής κυβερνο-ασφάλειας για καθεμία από τις 41 Περιοχές Ναυτικής Ασφάλειας (Area Maritime Security Committees - AMSC), για παροχή συμβουλών σχετικά με τα σχετικά ζητήματα θαλάσσιας ασφάλειας στον κυβερνοχώρο
- Ορισμό ειδικού για την ασφάλεια στον κυβερνοχώρο του MTS, σε κάθε τομέα που θα αναλάβει τα θέματα κυβερνο-άμυνας, τόσο για το USCG όσο και για το μη στρατιωτικό MTS
- Δημιουργία ειδικότητας Cyber Systems στην Ακαδημία USCG για να βοηθήσει στην προετοιμασία των στελεχών αξιωματικών

Η Υπηρεσία Κυβερνο-ασφάλειας και Ασφάλειας Υποδομής CISA [118] είναι μια υπηρεσία εντός του DHS, το οποίο είναι επιφορτισμένο με την προστασία των ομοσπονδιακών δικτύων των ΗΠΑ (στον τομέα .gov), και την οικοδόμηση της ικανότητας του έθνους να κατανοεί, να διαχειρίζεται και να ανταποκρίνεται στον κυβερνοχώρο και σε φυσικούς κινδύνους στους τομείς υποδομών ζωτικής σημασίας της χώρας. Ο CISA είναι επιφορτισμένος επίσης με την καθοδήγηση των στρατηγικών κυβερνο-ασφάλειας του δημόσιου τομέα, μέσω της ενίσχυσης της κυβερνο-άμυνας σε όλα τα επίπεδα διακυβέρνησης, τα προγράμματα συντονισμού του κράτους για την κυβερνο-ασφάλεια και τη βελτίωση της ικανότητας απόκρουσης των κυβερνο-επιθέσεων (που κυμαίνονται από ransomware έως επιθέσεις στην αλυσίδα εφοδιασμού). Ο CISA δεν είναι φορέας εκτέλεσης, αλλά εστιάζει στη διαχείριση κινδύνων και σε συνεργασία με τον δημόσιο και τον ιδιωτικό τομέα και άλλους συνεργάτες, μοιράζεται πληροφορίες για τις απειλές και δημιουργεί μια πιο ανθεκτική υποδομή στον κυβερνοχώρο. Το Τμήμα Κυβερνο-ασφάλειας της CISA, απευθύνεται σε έναν αριθμό φυσικών απειλών στον κυβερνοχώρο, συμπεριλαμβανομένης της ασφάλειας ICS/OT και των κυβερνο-φυσικών συστημάτων.

Από την παρουσίαση όλων των φορέων και των οργανισμών που σχετίζονται με τα θέματα της κυβερνο-ασφάλειας (στο MTS αλλά και γενικότερα), καθίσταται εμφανές ότι όλοι οι συμμετέχοντες φορείς αναγνωρίζουν την σπουδαιότητα και τους κινδύνους από κυβερνο-επιθέσεις. Δεδομένου όμως ότι το έργο των φορέων παραμένει σε απλά κατευθυντικό επίπεδο, χωρίς να μπορεί να δώσει καθορισμένες οδηγίες που σχετίζονται επακριβώς με τα τεχνολογικά θέματα, αφήνει σημαντικά κενά και αναπάντητο το θέμα των μηχανισμών της κυβερνο-προστασίας για όλα τα συστήματα που έχουν παρουσία στον κυβερνοχώρο.

5.1 Εργαλεία και Τύποι Κυβερνο-επιθέσεων. Ανάλυση Ρίσκου

Όπως παρουσιάστηκαν και στις προηγούμενες ενότητες, οι κυβερνο-επιθέσεις που αφορούν στην ναυτιλία, κάνουν χρήση τεχνικών που σχετίζεται με τα πληροφοριακά IT συστήματα, με στόχο την πρόσβαση αρχικά στην πληροφορία αυτών των συστημάτων. Στη συνέχεια, έχοντας πρόσβαση στα IT συστήματα, αποκομίζουν την απαιτούμενη πληροφορία για διείσδυση στα OT συστήματα, που χρησιμοποιούνται για την επιβολή των λειτουργιών στη ναυτιλία (πλοία, λιμένες, άλλες υποδομές). Στα λειτουργικά OT συστήματα που διαθέτει η ναυτιλία, συγκαταλέγονται αυτά που χρησιμοποιούν τους ραδιοδιαύλους για επίγειες ή δορυφορικές επικοινωνίες. Τα εργαλεία των κυβερνο-επιθέσεων στη ναυτιλία συμπεριλαμβάνουν:

- Τεχνικές Hacking
- Αλίευση Δεδομένων - Phishing
- Λογισμικό τύπου ransomware

- Διαρροή δεδομένων
- Εμπλοκή - Jamming
- Πλαστογράφηση - Spoofing

Οι τεχνικές hacking, το Phishing, και τα ransomwares, αποτελούν συνήθως αναπτυγμένο λογισμικό από τις ομάδες που εκδηλώνουν την κυβερνο-επίθεση. Η διαρροή δεδομένων αφορά τη γενικότερη εκροή "ευαίσθητων πληροφοριών", η οποία προκύπτει από αλίευση της μέσω κοινωνικών ή άλλων δικτύων και κυρίως εκμεταλλεύεται την ακούσια και μη διαβαθμισμένη/διαπιστευμένη ανταλλαγή πληροφοριών μεταξύ των ανθρώπων. Οι τεχνικές jamming και spoofing, κάνουν συνδυασμό τόσο υλικού πλατφόρμας (hw) όσο και λογισμικού (sw). Οι κυβερνο-επιθέσεις εκμεταλλεύονται τα κενά ασφαλείας, τα οποία έχουν προκύψει από την εφαρμογή των ίδιων των συστημάτων IT/OT, ή κενά ασφαλείας που οφείλονται στον ανθρώπινο παράγοντα.

Η εκδήλωση των κυβερνο-επιθέσεων με χρήση των προηγούμενων μηχανισμών, έχουν ως στόχο την πρόκληση ζημίας, απόκτησης ελέγχου των συστημάτων ή/και αποκόμιση λύτρων/χρηματικών ποσών, ή άλλους λόγους (π.χ. τρομοκρατία, διεθνές έγκλημα, πολεμική σύγρουση). Οι κυβερνο-επιθέσεις μπορούν να κατηγοριοποιηθούν με βάση τα πληττόμενα IT/OT συστήματα και συμπεριλαμβάνουν:

- IT συστήματα (πλοίων - λιμένων - εταιρειών - οργανισμών)
- OT συστήματα (πλοίων - λιμένων - εταιρειών - οργανισμών)
- Συστήματα Επικοινωνιών (επίγεια - δορυφορικά)

Η αποτίμηση μίας κυβερνο-επιθέσεως, είτε πρόκειται για τη ναυτιλία είτε για άλλες υποδομές, γίνεται συνήθως με χρήση διαδικασιών ανάλυσης ρίσκου (Risk Management Analysis - RMA). Οι αναλύσεις αυτές έχουν ως στόχο την οικονομική αποτίμηση των κινδύνων και των επισφαλειών, σταθμίζοντας το κόστος των μηχανισμών πρόληψης και αποτροπής αυτών των κινδύνων σε σχέση με τις προκύπτουσες ζημιές από την εκδήλωση τους. Οι μορφές αποτίμησης του κινδύνου είναι ποσοτικές και ποιοτικές.

Οι ποσοτικές προσεγγίσεις είναι αντικειμενικές και μετρήσιμες. Μία κλασική ποσοτική προσέγγιση θα ήταν ο εντοπισμός εκμεταλλεύσιμων τρωτών σημείων στον κυβερνοχώρο, ο προσδιορισμός του δυνητικού κόστους εάν επρόκειτο να γίνει εκμετάλλευση της ευπάθειας και ο υπολογισμός πώς μια τέτοια εκμετάλλευση συμβαίνει στην πραγματικότητα. Με τους επίσημους όρους της αξιολόγησης κινδύνου, το κόστος εκμετάλλευσης Single Loss Expectancy - SLE και η συχνότητα με την οποία γίνεται η εκμετάλλευση είναι ο Ετήσιος Ρυθμός Εμφάνισης Annual Rate of Occurrence - ARO. Για μια δεδομένη ευπάθεια, το Ετήσιο Προσδόκιμο Απώλειας Annualized Loss Expectancy - ALE, είναι το γινόμενο των δεικτών SLE και ARO.

Έχοντας μια λίστα τρωτών σημείων που απαιτούν μετριασμό, μπορούν να σχεδιαστούν και να τεθούν σχετικές τιμές ALE, άμυνες ή έλεγχοι ασφαλείας για μείωση του SLE και/ή του ARO. Μετά τη σύγκριση του ALE μετά την μετριασμό του κινδύνδου συν το κόστος των μέτρων που ελήφθησαν, με τον αρχικό ALE, οι διαχειριστές μπορούν να καθορίσουν εάν οι δαπάνες έχουν νόημα και αν είναι αναγκαίες και συμφέρουσες. Αν το κόστος των μέτρων που θα πάρουμε είναι μεγαλύτερο από το κέρδος του ALE, η λύση μπορεί κάλλιστα να απορριφθεί. Μία τέτοια προσέγγιση μπορεί να χρησιμοποιηθεί για την αποτίμηση και τους ενδεχόμενους μηχανισμούς απομείωσης των κυβερνο-κινδύνων στη ναυτιλία, όπως εξάλλου εφαρμόζεται και σε όλες τις διαδικασίες ανάλυσης και διαχείρισης ρίσκου.

Μια ποιοτική προσέγγιση για την αξιολόγηση κινδύνου είναι υποκειμενική και απροσδιόριστη. Η προσέγγιση είναι πιο ευέλικτη και, κατά κάποιο τρόπο, πιο ρεαλιστική, αλλά όχι ακριβής, όσον αφορά τα οικονομικά μεγέθη. Η ποιοτική μέθοδος βασίζεται σε σενάρια, όπου οι σχεδιαστές περιγράφουν γεγονότα που μπορεί να επιφέρουν κινδύνους στα συστήματα. Για κάθε "σενάριο καταστροφής", αποδίδεται βαθμολογία που περιγράφει συνήθως τον αντίκτυπο του γεγονότος στην υποδομή και την πιθανότητα εμφάνισης του σεναρίου. Για κάθε σενάριο, οι διαχειριστές κινδύνου πρέπει να καθορίσουν πώς να διαχειριστούν τον κίνδυνο, προκειμένου να μειώσουν τον αντίκτυπο ή/και τη συχνότητα εμφάνισης του σε αποδεκτά επίπεδα. Από αυτή τη βάση, μπορούν να αναπτυχθούν σχέδια έκτακτης ανάγκης που περιλαμβάνουν, συστήματα ανάκτησης, προσωπικό, αλληλοβοήθεια και πολλά άλλα. Αυτός ο τύπος σχεδιασμού βοηθά στον εντοπισμό και χαρακτηρισμό των σημείων επίθεσης σε μία υποδομή.

RISK ASSESSMENT MATRIX				PROBABILITY				
				Likelihood of Mishap if Hazard is Present				
				A Almost Certain (Continuously experienced)	B Likely (Will occur frequently)	C Possible (Will occur several times)	D Unlikely (Remotely possible but not probable)	E Rare (Improbable; but has occurred in the past)
SEVERITY	Consequence if Mishap Occurs	Catastrophic (Death, Loss of Asset, Mission Capability or Unit Readiness)	I	1	1	1	2	3
		Critical (Permanent Disabling Injury or Damage, Significantly Degraded Mission Capability or Unit Readiness)	II	1	1	2	3	3
		Moderate (Non-Permanent Disabling Injury or Damage, Degraded Mission Capability or Unit Readiness)	III	2	2	3	4	4
		Negligible (Minimal Injury or Damage, Little or No Impact to Mission Capability or Unit Readiness)	IV	3	3	4	4	4
				Risk Assessment Codes (RAC)				
				1=Extremely High 2=High 3=Medium 4=Low				

Σχήμα 23: Πίνακας Ανάλυσης Κινδύνου [1]

Μία τέτοιου τύπου ανάλυση μπορεί να εφαρμοστεί για όλα τα συστήματα/υπο-συστήματα που συνιστούν τα ΟΤ συστήματα της ναυτιλίας, με στόχο να αξιολογηθεί κατά πόσον χρειάζεται η εφαρμογή μέτρων κυβερνο-ασφάλειας για κάθε σύστημα. Η ποσοστική μέθοδος στοχεύει να καταδείξει τα απαιτούμενα κόστη από τους μηχανισμούς πρόληψης και αποτροπής κυβερνο-επιθέσεων, έναντι των επαγόμενων ζημιών που μία κυβερνο-επίθεση μπορεί να επιφέρει. Στη συνέχεια παρουσιάζεται ένα παράδειγμα ανάλυσης ρίσκου για τα συστήματα AIS της ναυτιλίας, στον πίνακα που ακολουθεί.

Στον πίνακα αυτό αναλύεται ποιος μπορεί να είναι ο λόγος της επίθεσης (φυσική καταστροφή ή επίθεση από άνθρωπο), τι πιθανότητα να συμβεί, πόσο καταστροφικό θα είναι και πόσο εύκολο να επιτευχθεί η επίθεση.

Οι αναλύσεις ρίσκου σε αυτήν την καθαρά οικονομική προέγγιση μπορεί να εφαρμοστούν για την στάθμιση κόστους σε υποδομές, αλλά δεν μπορούν να αποδώσουν την σοβαρότητα των κινδύνων από την εφαρμογή κυβερνο-επιθέσεων στη ναυτιλία. Αυτό οφείλεται κυρίως στην επαγόμενη δυναμική των κινδύνων από κυβερνο-επιθέσεις στη ναυτιλία, οι οποίες μπορεί να καταλήξουν σε σημαντική βλάβη/καταστροφή των υποδομών που σχετίζονται με τη μεταφορά, την οικονομία καθώς και τον κίνδυνο απώλειας ανθρώπινων ζωών που μπορεί να ανακύψει (π.χ. τρομοκρατική ένέργεια με ανάληψη ελέγχου αυτοματοποιημένου ή πλήρως αυτόνομου πλοίου). Επομένως, γίνεται ξεκάθαρο ότι παρά το επαγόμενο κόστος για την κυβερνο-ασφάλεια, αυτή είναι αναγκαία, δεδομένου ότι τα πλήγματα που μπορεί να προκύψουν από τους κινδύνους της, μπορεί να είναι ασύγκριτα πιο σημαντικά, με αμφισβήτιση κοινωνικών και κρατικών υποδομών και άλλες προεκτάσεις.

Πίνακας 3: Ανάλυση Ρίσκου για το ναυτιλιακό σύστημα AIS [1]

Attack	Source	Likelihood	Severity	Ease
GPS jamming	A	4	2	3
GPS failure/poor transmission	H	3	3	n/a
AIS device off	A	4	1	1
AIS malfunction	H	5	1	n/a
AIS bad data	A	3	3	1
AIS jamming	A	5	2	3
AIS bit errors	H	3	3	n/a
Vessel spoofing	A	4	2	2
Eavesdropping	A	1	4	1
Flooding	A	4	3	3
Ghost vessel	A	4	3	3
CPA/AIS-SART spoofing	A	5	2	3
Disappearance	A	4	2	3
AtoN spoofing	A	4	2	3
Data diddling	A	3	2	3
Weather spoofing	A	4	3	3

Source: A = human-initiated attack, H = natural hazard
Likelihood: 1 = Frequent, 2 = Probable, 3 = Occasional, 4 = Remote, 5 = Unlikely
Severity: 1 = Catastrophic, 2 = Critical, 3 = Marginal, 4 = Negligible
Ease of attack: 1 = Trivial, 2 = Simple, 3 = Difficult, 4 = Very difficult

5.2 Το θέμα της Αντιμετώπισης των Κυβερνο-επιθέσεων. Βασικές Αρχές

Παρόλο που για το MTS υπάρχουν συγκεκριμένες μορφές κυβερνοεπιθέσεων, οι κατευθυντήριες γραμμές,ξεκινούν με μερικές βασικές αρχές.Η κουλτούρα στη Ναυτιλία δυστυχώς έως πριν λίγα χρόνια ήταν ξένη προς τις απειλές του κυβερνοχώρου. Σαν όλους τους άλλους τομείς, οι βασικές αρχές προκειμένου να δομήσεις ένα σύστημα κυβερνοασφάλειας συμπίπτουν.Σε υψηλό επίπεδο, παρατίθενται 10 απλές αρχές ασφάλειας για τα συστήματα πληροφοριών που απευθύνονται στις διοικήσεις σε ολόκληρη την αλυσίδα της ναυτιλιακής βιομηχανίας[1]:

- Μην αρνείστε το πρόβλημα
- Μην υποτιμάτε το πρόβλημα
- Μην είστε εχθρικοί προς την κυβέρνηση και τις ρυθμιστικές αρχές
- Μην κάνετε την άμυνα στον κυβερνοχώρο ένα ζήτημα "θαμμένο" στη γραφειοκρατία
- Μην επιχειρήσετε να υπερασπιστείτε ολόκληρο το δίκτυο πληροφοριακών συστημάτων ταυτόχρονα. Δώστε προτεραιότητα στα περιουσιακά στοιχεία του φορέα που εκτίθενται στον κυβερνοχώρο
- Συμμετέχετε στην ανταλλαγή πληροφοριών του κλάδου
- Επενδύστε σε έργα έρευνας και ανάπτυξης της βιομηχανίας για τα θέματα κυβερνο-ασφάλειας
- Προσσεγίστε το θέμα ολιστικά
- Εξετάστε τα χειρότερα σενάρια
- Θεσπίστε μια στρατηγική σαν αυτές που υλοποιούν οι βιομηχανίες

Οι παραπάνω 10 αρχές προσέγγισης, αποτελούν μία γενικότερη τεχνική προσέγγισης για οποιοδήποτε πρόβλημα που αφορά σε πληροφοριακά συστήματα. Η άρνηση του προβλήματος των κυβερνο-επιθέσεων οφείλεται κυρίως στο γεγονός ότι δεν δημοσιοποιούνται, καθώς και δεν ξεκαθαρίζονται οι μηχανισμοί τους. Η μη κοινοποίηση οφείλεται σε πολλούς λόγους, κυρίως στην ζημιά που καταλήγουν να προκαλούν στην εταιρεία ή στον φορέα που αποδέχεται ότι δέχτηκε μία κυβερνο-επίθεση. Η ζημιά μπορεί να αφορά στην φήμη καθώς και σε ενδεχόμενες απώλειες πληροφοριών που μπορεί να ωθήσουν πελάτες των συστημάτων σε αξιώσεις αποζημιώσεων. Ευτυχώς στις ημέρες μας, η σύγχρονη τάση και η παγκόσμια διαδικτύωση δίνει την δυνατότητα κοινοποίησης πολλών περιστατικών κυβερνο-επιθέσεων, συμβάλλοντας σημαντικά στην αποδοχή του προβλήματος από όλες τις εμπλεκόμενες δομές στην ναυτιλία.

Η υποτίμηση του προβλήματος είναι ένας ακόμη παράγοντας που δρα με αρνητικό τρόπο στην γενικότερη προώθηση διεργασιών και δράσεων για την αντιμετώπιση των κυβερνο-επιθέσεων. Οι εταιρείες καθώς και οι δομές που σχετίζονται με την σύγχρονη ναυτιλία, έχουν αρχίσει να διαβλέπουν τουλάχιστον τα οικονομικά προβλήματα - ζημιές (πλέον των υπολοίπων), που δημιουργεί μία κυβερνο-επίθεση, η οποία θέτει εκτός λειτουργίας πληροφοριακά και υπολογιστικά συστήματα ζωτικών λειτουργιών. Αυτό αφήνει αδρανοποιημένη μία εταιρεία - φορέα για αρκετό χρονικό διάστημα, μέχρι την πλήρη αποκατάσταση των διεργασιών που βασίζονται στα πληροφοριακά συστήματα που δέχτηκαν την κυβερνο-επίθεση.Ειδικά στη Ναυτιλία που οι ρήτρες για καθυστέρηση πχ παράδοσης φορτίων αφορούν υπέρογκα ποσά, αυτό και μόνο θα έπρεπε να αποτελεί εφαλτήριο για σοβαρότερη αντιμετώπιση του προβλήματος.

Ο ρόλος των ρυθμιστικών αρχών ειδικότερα για τα θέματα των κυβερνο-επιθέσεων, είναι ακόμη ανοικτός και πρέπει να καθορισθεί. Η προσέγγιση από πλευράς κυβερνήσεων, για την ίδρυση ρυθμιστικών αρχών, οι οποίες καλούνται να αντιμετωπίσουν ένα πρόβλημα, δεν σημαίνει ότι τις καθιστά ικανές για την άμεση αντιμετώπιση του προβλήματος. Οι ρυθμιστικές αρχές δεν πρέπει να "χάνονται" σε νομοθετικές βάσεις και κανόνες, αλλά πρέπει να προσεγγίζουν το αντίστοιχο πρόβλημα με την απαιτούμενη τεχνολογική κατάρτιση, κάνοντας χρήση των ειδικών επιστημονικών ομάδων που οφείλουν να συγκροτήσουν. Προφανώς η λύση δεν είναι η θέσπιση νόμων και κανόνων για την επιβολή ποινών και κυρώσεων σε ένα κυβερνο-επιτιθέμενο, αλλά η ανάπτυξη μηχανισμών για την προστασία αυτών που δέχονται την επίθεση.Επιπλέον, η επιβολή προστίμων που προβλέπεται από Ευρωπαικές και Εθνικές νομοθεσίες σε περιπτώσεις όπως διαρροή προσωπικών δεδομένων από κυβερνοπεριστατικό θα πρέπει να αποτελεί μοχλό πίεσης για τη Διοίκηση των Ναυτιλιακών Οργανισμών (και χείρα βοηθείας για τους CISO) ώστε να αυξήσουν τα μέτρα ασφαλείας.

Η γραφειοκρατία αποτελεί ένα εγγενές πρόβλημα διαδικασιών και ανάθεσης/επιμερισμού ευθυνών, στην παράλληλη λειτουργία των κρατικών δομών. Στις εταιρείες τα προβλήματα γραφειοκρατίας εντοπίζονται και επιλύονται αρκετά γρήγορα, δεδομένου ότι μειώνουν την παραγωγικότητα και κατά συνέπεια συντελούν στην απομείωση των κερδών μίας εταιρείας. Η τρέχουσα προσέγγιση για τα θέματα των κυβερνο-επιθέσεων, όπως αναλύθηκε και στην προηγούμενη ενότηατα, συνίστατατι στις παράλληλες, επικαλυπτόμενες ή/και συχνά αντικρουόμενες δράσεις φόρέων όπως ο IMO, ENISA, USCG, IET, κ.α. Ο κοινός γνώμονας για την αντιμετώπιση των κυβερνο-επιθέσεων από όλους αυτούς τους φορείς, δεν συνεπάγεται απαραίτητα ένα κοινό σύνολο δράσης και ενεργειών, δεδομένου ότι προέρχονται από διαφορετικά γεωγραφικά διαμερίσματα του πλανήτη, με ετερογενείς προσεγγίσεις και τρόπους δράσεως (κανονιστικά πλαίσια και νομοθεσία), εξυπηρετώντας διαφορετικές βιομηχανίες, τεχνολογίες διαφορετικού επιπέδου και σε τελική ανάλυση, διαφορετικού επιπέδου οικονομικά συμφέροντα στην ναυτιλία.

Οι κυβερνο-επιθέσεις και τα περιστατικά που έχουν γίνει γνωστά στην τελευταία δεκαετία, δηλώνουν την ευρύτητα των τομέων της ναυτιλιακής υποδομής που μπορεί να πλήξουν. Οι δίοδοι μέσω των οποίων μπορούν να επιτεθούν οι κακόβουλοι στης ναυτιλιακής αλυσίδα είναι παρα πολλοί, ξεκινώντας από τα IT/OT συστήματα των πλοίων, των λιμένων, των επικοινωνιών, των εταιρειών, των οργανισμών, κ.λπ. Επομένως, η απόπειρα θωράκισης όλων των σημείων υποδομής που ενδεχόμενα μπορούν να δεχθούν κυβερνο-επιθέσεις, είναι αδύνατη. Σημαντικό βαθμό στην προσπάθεια θωράκισης από κυβερνο-απειλές, θα πρέπει να λαμβάνουν τα δίκτυα λειτουργίας κάθε φορέα που διασφαλίζουν τις εντοπισμένες δραστηριότητες στο σύνολο της ναυτιλιακής αλυσίδας υποδομών.

Η ανταλλαγή πληροφοριών και τεχνογνωσίας στα θέματα των κυβερνο-απειλών μεταξύ όλων των εμπλεκόμενων φορέων της ναυτιλίας, θα ενδυναμώσει την εμπειρία που αποκτάται από τρέχουσες και μελλοντικές κυβερνο-επιθέσεις. Επομένως, λύσεις σε προβλήματα που έχουν αναζητηθεί από έναν φορέα προφανώς θα διευκολύνουν την επίλυση τους σε ένναν άλλο φορέα της ναυτιλιακής αλυσίδας. Σηματικό ρόλο σε αυτό θα μπορεί να παίξει μελλοντικά η ίδρυση

θεματικών/τομεακών ομάδων απόκρισης σε κυβερνοπεριστατικά (sectorial CERT) οι οποίες θα υποτυπώνουν και διαμοιράζουν πληροφορίες για συμβάντα/ευπάθειες σε ναυτιλιακά συστήματα.Επιπλέον θα περιέχουν εξειδικευμένο προσωπικό που θα ειδικεύεται σε ναυτιλιακά συστήματα και θα μπορεί να εκπαιδεύει και να συνδράμει σε τυχόν κυβερνοπεριστατικό σε τομέα ναυτιλίας. Η ίδρυση τομεακών CERT θεωρείται το επόμενο βήμα που θα πρέπει να υλοποιήσουν οι ευρωπαικές χώρες μετά την εκτόξευση του αριθμού των εποπτευόμενων κρίσιμων υποδομών με το NIS2.

Το πρόβλημα των κυβερνο-επιθέσεων είναι ένα αμιγώς τεχνολογικό πρόβλημα, με ευρύτερες κοινωνικές και οικονομικές προεκτάσεις. Οι κυβερνο-επιθέσεις είναι ένα πρόβλημα που οφείλεται στην παγκοσμιοποίηση στον χειρισμό των πληροφοριών και στην αντίστοιχη παγκόσμια διασύνδεση που παρέχουν οι υποδομές διαδικτύου και τηλεπικοινωνιών. Εάν δεν υπήρχε η διασυνδεσιμότητα του παγκόσμιου ιστού, προφανώς η έννοια των κυβερνο-επιθέσεων δεν θα υφίστατο. Η παγκόσμια διασύνδεση πληροφοριακών συστημάτων έχει να επιδείξει σημαντικά τεχνολογικά και άλλα ωφέλη στην καθημερινότητα των ανθρώπων. Κατά συνέπεια, η μετάβαση σε αυτήν είναι ένα μη αντιστρεπτό βήμα, το οποίο η κυβερνο-άμυνα οφείλει να θωρακίσει από επισφάλειες. Τα τεχνολογικά ανοικτά θέματα προάγονται και επιλύονται με την δημιουργία νεώτερων μηχανισμών και εξέλιξης των τεχνολογιών, από την έρευνα που συντελείται στην ίδια την τεχνολογία. Προφανώς, ο ρόλος των ναυτιλιακών υποδομών είναι να προωθήσουν την τεχνολογική έρευνα στη ναυτιλία, παρέχοντας οικονομική και όποια άλλη στήριξη απαιτείται, προσδοκώντας στην ανάπτυξη νεώτερων μηχανισμών και τεχνολογιών που θα αντιμετωπίσουν αποδοτικά τα προβλήματα που έχουν ανακύψει στον κυβερνοχώρο. Οι δραστηριότητες στον κυβερνοχώρο δεν αφορούν μόνο στην ναυτιλία, γεγονός το οποίο επιδρά συνεπικουρικά για παράλληλη ενεργοποίηση και σε άλλες υποδομές και συστήματα που κάνουν χρήση των υπηρεσιών διασύνδεσης του παγκόσμιου ιστού.

Οι παραπάνω προσεγγίσεις δίνουν μία συνολική εικόνα στο πρόβλημα των κυβερνο-επιθέσεων. Θα ωθήσουν στην ανάπτυξη στρατηγικής για την ναυτιλιακή βιομηχανία, η οποία θα ωφεληθεί σε σημαντικό βαθμό τόσο από την επίλυση των κυβερνο-προβλημάτων, καθώς και από την επερχόμενη έλευση των τεχνολογιών αυτόνομης ναυτιλίας. Όπως παρουσιάστηκε και στην προηγούμενη ενότητα, η αυτόνομη ναυτιλία βασίζει πολλά στην αυτοματοπιημένη δράση και στις τεχνολογίες παγκόσμιας διασύνδεσης των πληροφοριακών και λειτουργικών συστημάτων.

Για τους χρήστες και τους διαχειριστές συστημάτων ηλεκτρονικών υπολογιστών ναυτιλίας, η πλειοψηφία των προβλημάτων κυβερνο-ασφάλειας μπορούν να αμβλυνθούν απλά ακολουθώντας την τήρηση των στοιχειωδών βέλτιστων πρακτικών "Cybersecurity 101" κανόνων [1]:

- Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης και έλεγχο ταυτότητας των χρηστών των IT/OT συστημάτων
- Παρακολουθήστε προσεκτικά τις κινήσεις των εργαζομένων. Διαγράψτε τους λογαριασμούς για άτομα που δεν θα πρέπει πλέον να έχουν πρόσβαση στα συστήματα
- Χρησιμοποιήστε μεμονωμένα προφίλ και κωδικούς πρόσβασης. Μην χρησιμοποιείτε γενικούς λογαριασμούς πρόσβασης
- Ελαχιστοποιήστε τη χρήση των διαχειριστικών λογαριασμών και των προνομίων διαχείρισης των πληροφοριών
- Εκχώρηση δικαιωμάτων πρόσβασης χρήστη μόνο ανάλογα με τις ανάγκες και το επίπεδο/θέση του χρήστη στην υποδομή. Χρησιμοποιείστε Πρακτικές "Zero Trust" όπου χρειάζεται
- Ελέγξτε το δίκτυο για να γνωρίζετε ποιο υλικό είναι συνδεδεμένο και ποιες εφαρμογές λογισμικού είναι εγκατεστημένες και εκτελούνται στα συστήματα
- Τμηματοποιήστε τα δίκτυα του πλοίου σε μεμονωμένα υποδίκτυα, όπου αυτό είναι δυνατόν
- Διατηρήστε το λογισμικό των συστημάτων ενημερωμένο
- Εκπαιδεύστε τους χρήστες των συστημάτων ώστε να δημιουργήσουν μια "κουλτούρα ασφάλειας" στον κυβερνοχώρο
- Δημιουργήστε αντίγραφα ασφαλείας των κρίσιμων συστημάτων
- Χρησιμοποιήστε λογισμικό προστασίας κατά του κακόβουλου λογισμικού και όποια άλλη άμυνα με "βάθος στρατηγικής"
- Να είστε προσεκτικοί με τα εξωτερικά δίκτυα και διασυνδεόμενα φορητά μέσα

- Αν δεν γνωρίζετε πως να χειριστείτε μία κατάσταση, ενημερωθείτε

Οι άμυνες στον κυβερνοχώρο περιγράφονται συχνά με τον όρο "άμυνα σε βάθος". Αυτό σημαίνει ότι καμία υποδομή ναυτιλίας δεν μπορεί να βασιστεί σε ένα μόνο επίπεδο προστασίας (π.χ. network security βάζοντας ένα πολύ καλό δικτυακό firewall για προστασία περιμέτρου). Το πιο εξωτερικό επίπεδο επαφής με την κυβερνο-επίθεση είναι το φυσικό στρώμα (Physical layer). Σε αυτό θα πρέπει να χρησιμοποιούνται μηχανισμοί που κρατούν μη εξουσιοδοτημένα άτομα μακριά από τα συστήματα υποδομών της ναυτιλίας. Το δεύτερο επίπεδο είναι το λογικό (logical layer), χρησιμοποιώντας μια αρχιτεκτονική δικτύου που διαχωρίζει τις συσκευές από διαφορετικά λειτουργικά δίκτυα/υπο-δίκτυα. Το τελικό στρώμα (higher layer) πρέπει να δυσχεραίνει την απόπειρα πρόσβασης και να την αποτρεψει, σε κάθε μη εξουσιοδοτημένο άτομο στο σύστημα. Αυτός είναι ο σκοπός της ύπαρξης πολιτικών ασφαλείας, διαδικασιών, και εκπαίδευσης του προσωπικού με "στρατηγική βάθους".

Όπως γενικότερα έχει αποδειχθεί από τον χειρισμό των πληροφοριακών συστημάτων, ο πιο "αδύναμος κρίκος" στην αλυσίδα των διεργασιών ασφαλείας, είναι ο ανθρώπινος παράγοντας. Επομένως, η ανάπτυξη μηχανισμών ασφαλείας για την ελαχιστοποίησης της πρόσβασης στα συστήματα IT/OT των ναυτιλιακών εταιρειών, ξεκινά από το ίδιο το προσωπικό και τους χειριστές αυτών των συστημάτων. Οι κωδικοί πρόσβασης σε κάθε σύστημα θα πρέπει να είναι προσωπικοί και με σαφώς καθορισμένα τα επίπεδα πρόσβασης τους στο σύστημα. Όσο υψηλότερα βρίσκεται ένας άνθρωπος στην ιεραρχία ενός οργανισμού - εταιρείας, τόσο μεγαλύτερη η ευθύνη και η επίδραση των αποφάσεων του στον οργανισμό - εταιρεία. Τα δίκτυα των συστημάτων θα πρέπει να είναι αντικείμενο διαχείρισης ΜΟΝΟ από τον διαχειριστή (administrator), ο οποιος διαθέτει και το προνόμιο του απόλυτου ελέγχου του συστήματος.Φυσικά θα πρέπει να υπάρχει και δεύτερος διαχειριστής, καθώς έχουν υπάρξει στο παρελθόν συμβάντα εκβιασμού από διαχειριστές, ασυδοσίας καθώς κανείς δεν είχε εικόνα τι πραγματικά γίνεται αλλά και συνέχειας λειτουργίας όταν ο διαχειριστής παραιτείτο ή απολυόταν. Εκκινώντας από την βάση ότι "ο απόλυτος διαχειριστής αποτελεί ένα άτομο εμπιστοσύνης", ρυθμίζει τα επίπεδα πρόσβασης των υπολοίπων χρηστών των συστημάτων, όπως αυτά απαιτούνται ανάλογα με την ιεραρχία και τα αντικείμενα που απαιτούν διαφορετικά επίπεδα πρόσβασης στην πληροφορία. Προυπόθεση για αυτό αποτελεί η ύπαρξη ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) όπου έχουν καθοριστεί τα πληροφοριακά περιουσιακά στοιχεία, οι κτήτορές τους και το ποιοί πρέπει να έχουν πρόσβαση σε αυτά, εκ του ρόλου τους. Ο διαχειριστής είναι υπεύθυνος και για την ενημέρωση του λογισμικού και του υλικού όπου αυτό απαιτείται, αλλά και για την παρακολούθηση του δικτύου (monitoring). Η παρακολούθηση του δικτύου, ειδικότερα σε εταιρείες και οργανισμούς που μπορεί να διαθέτουν εκατοντάδες ή ακόμη και χιλιάδες υπαλλήλους, εκκινεί από τα επίπεδα πρόσβασης, τις επιτρεπόμενες ενέργειες και την πρόσβαση, μέχρι την καταγραφή και παρακολούθηση των διεργασιών και ενεργειών κάθε χρήστη (monitoring) προς το σύστημα. Από τον κανόνα αυτόν ΔΕΝ εξαιρείται ούτε ο διαχειριστής των πληροφοριακών συστημάτων. Οι διεργασίες παρακολούθησης ενός δικτύου μπορεί να απομονώσουν κακόβουλες ενέργειες, ακούσιες ή εκούσιες, και να εντοπίσουν τον ανθρώπινο παράγοντα που συνετέλσε σε αυτές. Οι διαιδκασίες παρακολούθησης σε συνδυασμό με αυτοματοποιημένα εργαλεία λογισμικού ανάλυσης, μπορούν να ανιχνεύσουν συνθήκες και καταστάσεις για ένα δίκτυο, οι οποίες δεν ανταποκρίνονται σε ομαλή λειτουργία π.χ. αυξημένος όγκος ανταλλαγής emails, πρόσβασης σε δεδομένα διαδικτύου, ασυνήθιστες ώρες ενεργοποίησης εξυπηρετητών (servers), αυτοματοποιημένες διατραπεζικές συναλλαγές - transactions, κ.λπ. Αυτές οι παρατηρήσεις μπορεί να εντοπίσουν την εγκατάσταση κακόβουλου λογισμικού, το οποίο αυτοματοποιημένα μπορεί να αποτρέπει την εκτέλεσή τους. Επιπλέον, εξαιρετικά σημαντικό στα συστήματα που διαθέτουν πρόσβαση πολλών χρηστών και τερματικά χειρισμού, είναι η ΑΠΑΓΟΡΕΥΣΗ (και με φυσικό τρόπο), της χρήσεως φορητών συσκευών (π.χ. USB sticks, memory cards, Κ.α.), ακόμη και για διεργασίες που αφορούν στοιχεία και ηλεκτρονικά έγγραφα μίας εταιρείας/οργανισμου. Όλες οι διαδικασίες μεταφοράς και ανάκτησης δεδομένων και πληροφοριών σε οποιαδήποτε μορφή, θα πρέπει να βασίζονται στο Intra/Internet και να καταγράφονται από το σύστημα. Ο διαχειριστής του συστήματος θα πρέπει να είναι επίσης επιφορτισμένος με την διαμόρφωση των δικτύων και των τοπικών υποδικτύων του συστήματος, διαχωρίζοντας τα εσωτερικά από τα εξωτερικά δίκτυα, καθώς και τα δίκτυα που μπορεί να έχουν πρόσβαση σε "ευαίσθητες πληροφορίες". Οι διασυνδέσεις εξωτερικών δικτύων στα εσωτερικά δίκτυα μίας εταιρείας - οργανισμού αν δεν μπορούν να αποτραπούν από τις λειτουργίες, θα πρέπει να επιτρέπονται με χρήση αυστηροποιημένων προδιαγραφών και πρωτοκόλλων πρόσβασης με κρυπτογραφία.

Τα τελευταία χρόνια τα πληροφοριακά συστήματα των ναυτιλιακών οργανισμών γίνονται όλο και πιο πολύπλοκα με αποτέλεσμα μεγάλο φόρτο για τους διαχειριστές.Επιπλέον έχει παρατηρηθεί ότι οι διαχειριστές είτε δεν είχαν βαθιά γνώση κυβερνοασφάλειας είτε δεν είχαν χρόνο να ελέγχουν τα logs των συστημάτων ασφαλείας που είχαν εγκαταστήσει, πέρα από τη μη διαθεσιμότητά τους όλο το 24ωρο.Για αυτό τον λόγο η κοινή βέλτιστη πρακτική είναι τουλάχιστον οι μεγάλες ναυτιλιακές εταιρείες να αναθέτουν σε εξωτερικές εταιρείες που παρέχουν 24/7 υπηρεσίες Security Operation Center-SOC την παρακολούθησή τους από πλευράς Κυβερνοασφάλειας, αυξάνοντας την παραγωγικότητά τους και το επίπεδο επαγρύπνησης.

Οι παραπάνω αποτελούν μερικές θεμελιώδεις βάσεις, που πρέπει να διέπουν την οποιαδήποτε πληροφοριακή δομή με χρήση υπολογιστικών συστημάτων. Επομένως σε γενικές γραμμές, η προστασία των ναυτιλιακών υποδομών δεν διαφέρει από πλευράς προστασίας δικτύου, από οποιαδήποτε άλλη πληροφοριακή ICT υποδομή.

Στη συνέχεια θα παρουσιαστούν τεχνολογικά πιο εξειδικευμένες και διοικητικές προτάσεις για την αντιμετώπιση των κυβερνο-απειλών στην ναυτιλία, εξειδικευμένα για τα συστήματα IT/OT που αυτή χρησιμοποιεί.

5.3 Προτάσεις για θωράκιση της Ναυτιλίας από Κυβερνο-επιθέσεις. Εξειδικευμένοι Μηχανισμοί

Η κυβερνο-ασφάλεια στο χώρο του MTS, απαιτεί εκτός από γενικές κατευθυντήριες γραμμές για δράσεις και αντίμετρα, συγκεκριμένες τεχνολογικές προτάσεις, οι οποίες θα πρέπει να βασίζονται στις υφιστάμενες τεχνολογίες ICT που χρησιμοποιούνται από τα ναυτιλιακά συστήματα. Στην ενότητα παρατίθενται συγκεκριμένες τεχνολογικές προτάσεις οι οποίες θα θωρακίσουν την λειτουργία των IT/OT συστημάτων από κυβερνο-απειλές.

5.3.1 Πρωτόκολλα Εξουσιοδότησης - Ελέγχου ταυτότητας (Authorization - Authentication protocols)

Όπως έχει διαπιστωθεί η βάση για τις κυβερνο-επιθέσεις στα συστήματα IT/OT του MTS, εκκινεί από το ανθρώπινο προσωπικό που κάνει χρήση αυτών των συστημάτων. Η ανάπτυξη του αισθήματος κυβερνο-ασφάλειας πηγάζει από δύο βασικές διαδικασίες για την είσοδο των χρηστών στα πληροφοριακά συστήματα. Οι διαδικασίες αυτές είναι γνωστές ως Έλεγχος Ταυτότητας (Authentication) και Εξουσιοδότηση (Authorization) των χρηστών.

Η διαδικασία του Ελέγχου Ταυτότητας του χρήστη είναι βασική στα πληροφοριακά συστήματα και προορίζεται να εξακριβώσει κατά πόσον ένας χρήστης δικαιούται να έχει πρόσβαση στο μηχανισμό/υπηρεσία ενός συστήματος μέσω των διαδικασιών εισόδου (login). Στην ναυτιλία έχει διαπιστωθεί ότι γίνεται κακή χρήση κοινών λογαριασμών πρόσβασης, οι οποίοι είναι γενικοί και διαθέσιμοι από όλο σχεδόν το αρμόδιο προσωπικό ενός πλοίου. Ένας κοινός λογαριασμός δεν ταυτοποιεί μοναδικά ένα χρήστη. Κανονικά σε όλα τα πληροφοριακά συστήματα θα πρέπει κάθε χρήστης να διαθέτει τον δικό του (εξατομικευμένο - προσωπικό) κωδικό πρόσβασης, ο οποίος να πληρεί τις προϋποθέσεις ενός ισχυρού κωδικού (strong password), που να μην επιτρέπει με έυκολο τρόπο τις διαδικασίες αναζήτησης του με χρήση τεχνικών brute-force. Οι κωδικοί αυτοί θα πρέπει να αλλάζουν στο χρόνο με ευθύνη του διαχειριστή του συνολικού συστήματος των δικτύων του πλοίου, και επιπλέον θα πρέπει να διατηρούνται μυστικοί και προσωπικοί. Θα πρέπει να γίνει κοινή πεποιήθηση των εργαζομένων στο χώρο της ναυτιλίας, ότι ένας κωδικός αφενώς δίνει πρόσβαση σε ένα πληροφοριακό σύστημα και αφετέρου ταυτοποιεί μοναδικά τον χρήστη που αιτείται την πρόσβαση. Αυτό διασφαλίζει ότι το σύστημα γνωρίζει ποιός έχει πρόσβαση και τι ενέργειες έχει επιτελέσει μέσω του πληροφοριακού συστήματος.

Η διαδικασάι της Εξουσιοδότησης (Authorization), αφορά στον καθορισμό των "προνομίων χρήστη" ενός συστήματος, με βάση την θέση του και την ιεραρχία στη λειτουργία του πλοίου. Αυτό διασφαλίζει ότι μόνο το κατάλληλο προσωπικό, το οποίο κατέχει την δεδομένη θέση ευθύνης, μπορεί να επιβάλλει σημαντικές ενέργειες στα συστήματα, διαχωρίζοντας θέσεις, ρόλους και ζώνες ευθύνης για το πλήρωμα.

Οι παραπάνω διαδικασίες δεν έχουν τίποτε το διαφορετικό για το MTS και τα πληροφοριακά του συστήματα, σε σχέση με άλλα πληροφοριακά συστήματα που αξιοποιούν τις τεχνολογίες ICT

(π.χ. τραπεζικά δίκτυα). Επομένως, δεν απαιτείται ιδιαίτερη τεχνολογική αναβάθμιση και έρευνα στον τομέα αυτό, παρά χρήση των ήδη υπαρχουσών τεχνολογιών που χρησιμοποιούνται παντού και διασφαλίζουν τις παραπάνω διαδικασίες.

Γενικότερα ένα πρωτόκολλο ελέγχου ταυτότητας επιτρέπει στον παραλήπτη (όπως ένας διακομιστής) να επαληθεύσει την ταυτότητα ενός άλλου μέρους (όπως ένα άτομο που χρησιμοποιεί μια κινητή συσκευή για να συνδεθεί). Σχεδόν κάθε σύστημα υπολογιστή χρησιμοποιεί κάποιο είδος ελέγχου ταυτότητας δικτύου, για την επαλήθευση των χρηστών. Καθώς περισσότερες κρίσιμες πληροφορίες αποθηκεύονται ηλεκτρονικά, και καθώς οι hackers γίνονται όλο και πιο έμπειροι στην κλοπή τους, ο έλεγχος ταυτότητας γίνεται όλο και πιο σημαντικός. Χωρίς αυτόν, οι απώλειες πληροφορίας μπορεί να είναι σημαντικές. Για παράδειγμα, η Deloitte αντιμετώπισε μια παραβίαση δεδομένων το 2017, που αποκάλυψε τα μηνύματα ηλεκτρονικού ταχυδρομείου πελατών της (συμπεριλαμβανομένων ορισμένων συνδεδεμένων με κυβερνητικούς φορείς). Ο έλεγχος ταυτότητας δεν μπορεί ποτέ να διατηρήσει τις πληροφορίες απόλυτα ασφαλείς. Μπορεί όμως να κάνει την κλοπή τους πιο δύσκολη. Οι hackers μπορεί να μετακινηθούν σε διαφορετικό στόχο εάν οι διακομιστές ενός δικτύου, είναι πολύ δύσκολο να επιτρέψουν διείσδυση [119].

Οι πέντε πιο συνηθισμένες μέθοδοι ελέγχου ταυτότητας που χρησιμοποιούν οι εταιρείες περιλαμβάνουν τα ακόλουθα:

- Kerberos: Σε περιβάλλοντα Windows, το πρωτόκολλο Kerberos χρησιμοποιείται ευρύτατα. Το σύστημα βασίζεται σε συμμετρικά κλειδιά που έχουν καθοριστεί από ένα κεντρικό κέντρο διανομής κλειδιών. Αν και το επίπεδο προστασίες που παρέχει είναι σημαντικό, το Kerberos δεν είναι τέλειο
- LDAP: Οι εταιρείες αποθηκεύουν ονόματα χρήστη, κωδικούς πρόσβασης, διευθύνσεις email, συνδέσεις φορητών συσκευών και άλλα στατικά δεδομένα σε καταλόγους. Το Lightweight Directory Access Protocol - LDAP είναι ένα ανοιχτό, ουδέτερο ως προς τον προμηθευτή πρωτόκολλο εφαρμογής, για την πρόσβαση και τη διατήρηση αυτών των δεδομένων.
- OAuth 2.0: Για διασύνδεση από μία εφαρμογή στον ιστότοπο σε μία άλλη, χρησιμοποιείται το πρωτόκολλο OAuth 2.0. Μια εφαρμογή εγγυητή τρίτου μέρους, αντλεί πόρους για τον λογαριασμό πρόσβασης και δεν χρειάζεται να μοιράζονται διαπιστευτήρια μεταξύ των διασυνδεόμενων πλευρών (credentials).
- Υπηρεσία απομακρυσμένου ελέγχου ταυτότητας (Remote authentication dial-in user service - RADIUS): Παρέχεται ένα όνομα χρήστη και ένας κωδικός πρόσβασης και το σύστημα RADIUS επαληθεύει τις πληροφορίες συγκρίνοντάς τις με τις καταχωρήσεις σε μια βάση δεδομένων.
- Security assertion markup language - SAML: Αυτό το πρωτόκολλο που βασίζεται σε eXtensible markup language - XML, ανταλλάσσει δεδομένα ελέγχου ταυτότητας μεταξύ IdPS και παρόχων υπηρεσιών.

Οι ενσωματώσεις κάποιων από τις παραπάνω τεχνολογίες πρωτοκόλλων, στα θέματα του Ελέγχου Ταυτότητας και της Εξουσιοδότησσης δεν εξαλείφουν απόλυτα τον κίνδυνο από κυβερνο-επίθεση στα MTS συστήματα, αλλά μειώνουν την πιθανοτητα επιτυχίας των επιτιθέμενων σε αυτά. Θα πρέπει να σημειωθεί ότι ακόμη και τα πρωτόκολλα που εξαρτώνται από την άμεση προσβασιμότητα των συστημάτων στο διαδίκτυο δεν αποτελούν πλέον πρόβλημα, δεδομένου ότι τα συστήματα επικοινωνιών των πλοίων διασφαλίζουν διαρκή προσβασιμότητα μέσω επίγειων ή δορυφορικών συνδέσεων στον παγκόσμιο ιστό.

5.3.2 Κρυπτογραφία Δεδομένων και Επικοινωνιών (encryption for data and communications)

Η κρυπτογράφηση (encryption) χρησιμοποιείται καθημερινά για την ασφάλεια των διαδικτυακών επικοινωνιών μεταξύ δύο ατόμων ή μεταξύ πελατών και διακομιστών. Αν και μπορεί να μην γίνεται αντιληπτό για τους χρήστες των υπηρεσιών, η κρυπτογράφηση αποκρύπτει τα δεδομένα που ανταλλάσσονται από εξωτερικούς εισβολείς που δυνητικά παρακολουθούν τις επικοινωνίες των υπολογιστικών συστημάτων. Η κρυπτογράφηση λειτουργεί λαμβάνοντας δεδομένα απλού κειμένου

ή δεδομένα που είναι αναγνώσιμα σε κάποια μορφή, και μετατρέπει αυτό σε κρυπτογραφημένα δεδομένα. Το κρυπτογραφημένα δεδομένα είναι μια τυχαία συλλογή γραμμάτων, αριθμών και μερικές φορές συμβόλων (αλφαρηθμιτικά), που κρύβει "ευαίσθητα δεδομένα" από οποιονδήποτε άλλον εκτός των χρηστών που συναλλάσσονται μεταξύ τους. Τα κρυπτογραφημένα δεδομένα μπορεί να αντιστραφούν στην αρχική - μη κρυπτογραφημένη μορφή, αρκεί είτε να χρησιμοποιηθεί ένα κλειδί για την αποκρυπτογράφηση των δεδομένων είτε να βρεθεί ένα μοτίβο (pattern) στο κρυπτογραφημένα δεδομένα για την αποκρυπτογράφηση τους. Η δυνατότητα αποκρυπτογράφησης δεδομένων είναι ζωτικής σημασίας στη διαδικασία της διαδικτυακής επικοινωνίας, καθώς ο παραλήπτης των πληροφοριών θα πρέπει να μπορεί να αποκρυπτογραφήσει τα δεδομένα, κάτι που συνήθως γίνεται μέσω της χρήσης κλειδιού. Η κρυπτογράφηση είναι ζωτικής σημασίας για να διασφαλιστεί ότι τα ευαίσθητα δεδομένα παραμένουν μυστικά από ανεπιθύμητους εισβολείς και η κρυπτογράφηση ως διαδικασία βασίζεται σε πρωτόκολλα κρυπτογράφησης.

Η κρυπτογράφηση γίνεται μέσω αλγορίθμων κρυπτογράφησης. Αυτοί οι αλγόριθμοι κάνουν όλες τις κρυπτογραφικές λειτουργίες, χρησιμοποιώντας το κλειδί κρυπτογράφησης στα δεδομένα. Αυτοί οι αλγόριθμοι χρησιμοποιούνται στη συνέχεια στα πρωτόκολλα κρυπτογράφησης. Ο σκοπός ενός πρωτοκόλλου κρυπτογράφησης είναι να εκπληρώσει μια συγκεκριμένη λειτουργία. Οι λειτουργίες που μπορούν να εκτελέσουν τα πρωτόκολλα κρυπτογράφησης ποικίλλουν, από επικοινωνίες με TLS/SSL έως απομακρυσμένες συνδέσεις σε υπολογιστές με SSH.

Η συμμετρική κρυπτογράφηση (symmetric encryption) είναι η πιο απλή μορφή κρυπτογράφησης. Η συμμετρική κρυπτογράφηση χρησιμοποιεί ένα κλειδί για την κρυπτογράφηση δεδομένων, είτε αυτά τα δεδομένα είναι κατά τη μεταφορά είτε σε κατάσταση αποθήκευσης. Σε σχέση με την κρυπτογράφηση δεδομένων σε κίνηση, το κλειδί δημιουργείται και μοιράζεται τόσο με τον αποστολέα όσο και με τον παραλήπτη του μηνύματος (κοινό κλειδί). Τα δεδομένα στο μήνυμα κρυπτογραφούνται με το συμμετρικό κλειδί, που σημαίνει ότι το μόνο άτομο που μπορεί να διαβάσει αυτά τα δεδομένα είναι κάποιος που κατέχει το κλειδί κρυπτογράφησης. Μόλις το μήνυμα φτάσει στον παραλήπτη, μπορεί να χρησιμοποιήσει το συμμετρικό κλειδί για να αποκρυπτογραφήσει τα δεδομένα. Η χρήση συμμετρικής κρυπτογράφησης από μόνη της δεν συνιστάται, καθώς είναι πολύ πιο επισφαλής σε σύγκριση με την ασύμμετρη κρυπτογράφηση (asymmetric encryption). Αυτό οφείλεται στο γεγονός, ότι με τη συμμετρική κρυπτογράφηση, το κλειδί που δημιουργείται πρέπει κάποια στιγμή να παραδοθεί στον παραλήπτη των δεδομένων. Εάν αυτή η μεταφορά δεν γίνει με ασφάλεια, το κλειδί θα μπορούσε να υποκλαπεί κατά την παράδοση του, πράγμα που σημαίνει ότι οποιαδήποτε κρυπτογράφηση γίνεται με αυτό το κλειδί είναι πλέον άχρηστη.

Η ασύμμετρη κρυπτογράφηση (asymmetric encryption), όπως αναφέρθηκε και προηγουμένως, είναι ο πιο ασφαλής από τους δύο τύπους κρυπτογράφησης. Με την ασύμμετρη κρυπτογράφηση δημιουργείται ένα ζεύγος κλειδιών που αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί διατηρείται διαθέσιμο για οποιονδήποτε, ενώ το ιδιωτικό κλειδί το γνωρίζει μόνο ο δημιουργός του ζεύγους κλειδιών. Για ασύμμετρη κρυπτογράφηση δεδομένων, ο δημιουργός του ζεύγους κλειδιών κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο παραλήπτης μπορεί στη συνέχεια να χρησιμοποιήσει το δημόσιο κλειδί, που βρίσκεται γενικά από μια αποθήκη δημόσιου κλειδιού (public key repository), για να αποκρυπτογραφήσει το μήνυμα. Αποκρυπτογραφώντας το μήνυμα με το δημόσιο κλειδί, ο παραλήπτης των δεδομένων μπορεί να διακρίνει ότι το μήνυμα προέρχεται από αυτόν που πιστεύει ότι είναι ο αποστολέας του, και ότι τα δεδομένα στο μήνυμα δεν έχουν αλλάξει. Εάν τα δεδομένα στο μήνυμα είχαν αλλάξει, η αποκρυπτογράφηση με το δημόσιο κλειδί δεν θα παράγει ένα αναγνώσιμο μήνυμα, καθώς τα δεδομένα θα παραμένουν κρυπτογραφημένα. Αν και η ασύμμετρη κρυπτογράφηση είναι πιο ασφαλής σε σχέση με τη συμμετρική κρυπτογράφηση, και οι δύο τείνουν να χρησιμοποιούνται παράλληλα για την κρυπτογράφηση επικοινωνιών. Η αρχική σύνδεση θα δημιουργηθεί με ασύμμετρη κρυπτογράφηση, θα κατασκευάσει ένα συμμετρικό κλειδί συνεδρίας και στη συνέχεια το κλειδί συνεδρίας θα χρησιμοποιηθεί για την κρυπτογράφηση μηνυμάτων στη συνεδρία.

Η συνεργασία με τα πρωτόκολλα ασύμμετρης κρυπτογράφησης είναι τα Public Key Infrastructures ή PKI. Μια υποδομή PKI χρησιμοποιεί ψηφιακά πιστοποιητικά και ασύμμετρα ζεύγη κλειδιών για τον έλεγχο ταυτότητας χρηστών και συσκευών εντός ενός δικτύου. Όταν κάποιος θέλει να χρησιμοποιήσει ένα δίκτυο που χρησιμοποιεί μια υποδομή PKI, πρέπει να ζητήσει πιστοποιητικό από μια Αρχή έκδοσης πιστοποιητικών (Certificate Authority - CA) εντός του PKI. Το αίτημα, γνωστό και ως Αίτημα Υπογραφής Πιστοποιητικού ή Certificate Signing Request - CSR, περιέχει πληροφορίες για τον αιτούντα, καθώς και το δημόσιο κλειδί ενός ζεύγους ασύμμετρων κλειδιών του οποίου είναι ο κάτοχος. Οι πληροφορίες εντός του αιτήματος επαληθεύονται από την CA και, εάν είναι έγκυρες, εκδίδεται πιστοποιητικό στον αιτούντα που περιέχει το δημόσιο κλειδί του μαζί με μια

σειρά από άλλα στοιχεία. Τώρα, όταν γίνεται σύνδεση μεταξύ αυτού του κατόχου πιστοποιητικού και ενός διακομιστή ή άλλου χρήστη, μπορούν να κοιτάξουν την Αλυσίδα εμπιστοσύνης του ψηφιακού πιστοποιητικού τους για να επαληθεύσουν ότι το πιστοποιητικό εξακολουθεί να ισχύει. Η αλυσίδα αξιοπιστίας ενός πιστοποιητικού είναι μια διαδρομή από το τρέχον πιστοποιητικό που οδηγεί μέχρι το τέλος στο πιστοποιητικό της CA ρίζας (root) . Κάθε πιστοποιητικό σε αυτήν την αλυσίδα ελέγχεται για την εγκυρότητά του, προκειμένου να διασφαλιστεί ότι ο κάτοχος του πιστοποιητικού δεν χρησιμοποιεί πιστοποιητικό που έχει λήξει ή έχει ανακληθεί. Εάν αυτό ισχύει για κάθε πιστοποιητικό στην αλυσίδα, τότε το πιστοποιητικό επικυρώνεται και μπορεί να προκύψει σύνδεση [120].

Τα πιο διαδεδομένα - ευρέως χρησιμοποιούμενα πρωτόκολλα κρυπτογράφησης είναι:

- TLS/SSL: Το TLS/SSL είναι το πιο κοινό πρωτόκολλο κρυπτογράφησης, το οποίο χρησιμοποιείται καθημερινά στο Διαδίκτυο. Το TLS/SSL σημαίνει Transport Layer Security/Secure Sockets Layer, το οποίο είναι ένα πρωτόκολλο κρυπτογράφησης που διασφαλίζει ότι οι επικοινωνίες μεταξύ πελάτη και διακομιστή διατηρούνται ασφαλείς. Όταν το πρόγραμμα περιήγησής συνδέεται σε έναν ιστότοπο, εάν η σύνδεση είναι ασφαλής με TLS/SSL, τότε εμφανίζεται ένα λουκέτο και η λέξη "https" στη γραμμή URL διεύθυνσης. Το TLS/SSL δεν κάνει την κρυπτογράφηση από μόνο του, αλλά χρησιμοποιεί μια ποικιλία αλγορίθμων κρυπτογράφησης, όπως RSA ή AES, για την κρυπτογράφηση των επικοινωνιών. Αυτός είναι ο λόγος που το SSL/TLS θεωρείται πρωτόκολλο κρυπτογράφησης. Η χρήση TLS/SSL για την κρυπτογράφηση των επικοινωνιών είναι πολύ συνηθισμένη, καθώς χρησιμοποιούνται πολλοί διαφορετικοί αλγόριθμοι κρυπτογράφησης. Το TLS/SSL μπορεί να χρησιμοποιηθεί για τον έλεγχο ταυτότητας χρήστη, την κρυπτογράφηση της κυκλοφορίας και την απόδειξη ότι τα δεδομένα δεν έχουν τροποποιηθεί κατά τη μεταφορά. Ο τρόπος που λειτουργεί το TLS/SSL είναι ότι ένα ασύμμετρο ζεύγος κλειδιών χρησιμοποιείται σε μια διαδικασία "Χειραψίας - Handshake" για να διασφαλίσει την αρχική σύνδεση μεταξύ του πελάτη και του διακομιστή. Αυτό το "Handshake" είναι το σημείο όπου επιλέγεται η συγκεκριμένη έκδοση πρωτοκόλλου που θα χρησιμοποιηθεί, επαληθεύονται τα πιστοποιητικά TLS/SSL τόσο του διακομιστή όσο και του πελάτη, επιλέγεται ο αλγόριθμος για τη διαδικασία "Record" και το κοινό κλειδί δημιουργείται με συμμετρική κρυπτογράφηση. Το κοινό κλειδί χρησιμοποιείται στη συνέχεια στο επόμενο βήμα της επικοινωνίας, στη φάση "εγγραφής". Σε αυτή τη φάση, τα πακέτα που μοιράζονται μεταξύ των δύο χρηστών κρυπτογραφούνται με το κοινό κλειδί για να διασφαλιστεί η ασφαλέστερη μορφή επικοινωνίας.
- IPsec: Το IPsec ή Internet Protocol Security, είναι ένα πρωτόκολλο κρυπτογράφησης που χρησιμοποιεί αλγόριθμους κρυπτογράφησης όπως 3DES, AES, SHA και CBC για την κρυπτογράφηση δεδομένων σε εφαρμογές, δρομολόγηση ή εικονικά ιδιωτικά δίκτυα. Χρησιμοποιώντας τις δύο λειτουργίες του, τη λειτουργία σήραγγας - tunnel και τη λειτουργία μεταφοράς - transport, το IPsec προστατεύει τα δεδομένα που μεταδίδονται από τη μια τοποθεσία στην άλλη. Η λειτουργία μεταφοράς κρυπτογραφεί μόνο το ωφέλιμο φορτίο του μηνύματος, όχι την επικεφαλίδα του IP πρωτοκόλλου. Καθώς ορισμένες πληροφορίες μπορούν να ληφθούν από την επικεφαλίδα, αυτό χρησιμοποιείται μόνο για απλές καταστάσεις μεταφοράς δεδομένων, όπως σύνδεση σε διακομιστή ή σταθμό εργασίας. Η λειτουργία Tunneling, από την άλλη πλευρά, κρυπτογραφεί και επαληθεύει τόσο το ωφέλιμο φορτίο όσο και την επικεφαλίδα. Η λειτουργία σήραγγας χρησιμοποιείται συχνότερα σε εικονικά ιδιωτικά δίκτυα (VPN). Αν και η χρήση VPN με IPsec είναι γενικά πιο γρήγορη, καθώς το IPsec είναι πιο γρήγορο στη ρύθμιση μιας σύνδεσης, άλλα μέρη του TLS/SSL το καθιστούν την προτιμώμενη μέθοδο κρυπτογράφησης και ελέγχου ταυτότητας κατά τη μεταφορά δεδομένων.
- SSH: Το Secure Shell, γνωστό και ως SSH, είναι ένας άλλος τύπος πρωτοκόλλου κρυπτογράφησης. Ο τρόπος που λειτουργεί το SSH είναι παρόμοιος με ένα VPN. Δημιουργώντας ένα κρυπτογραφημένο τούνελ (tunnel), οι χρήστες μπορούν να χρησιμοποιήσουν το SSH για ασφαλή και απομακρυσμένη σύνδεση σε υπολογιστές, μεταφορά αρχείων κ.α. Το SSH λειτουργεί σε 3 διαφορετικά επίπεδα: το επίπεδο μεταφοράς, το επίπεδο ελέγχου ταυτότητας χρήστη και το επίπεδο σύνδεσης. Το επίπεδο μεταφοράς είναι το επίπεδο που συνδέει με ασφάλεια δύο μέρη, κρυπτογραφεί με ασφάλεια τυχόν δεδομένα που αποστέλλονται μεταξύ τους, πιστοποιεί την ταυτότητα των χρηστών μεταξύ τους και διασφαλίζει ότι τα δεδομένα που μοιράζονται μεταξύ των χρηστών δεν αλλάζουν με κανέναν τρόπο κατά τη μεταφορά. Για την ανταλλαγή κλειδιών, τα δύο μέρη στη σύνδεση SSH συνδέονται και τα κλειδιά του πελάτη και του διακομιστή

διαπραγματεύονται μέσω της ανταλλαγής κλειδιών Diffie-Hellman. Κατά τη διάρκεια αυτής της φάσης του SSH, επιλέγεται ο συμμετρικός αλγόριθμος, ο ασύμμετρος αλγόριθμος, ο αλγόριθμος ελέγχου ταυτότητας μηνυμάτων και ο αλγόριθμος κατακερματισμού (segmentation) που θα χρησιμοποιηθεί στη μεταφορά δεδομένων και μηνυμάτων. Στο επίπεδο ελέγχου ταυτότητας, ο πελάτης επαληθεύει την ταυτότητά του μέσω μιας υποστηριζόμενης μεθόδου ελέγχου ταυτότητας που καθορίζεται από τον διακομιστή από το επίπεδο μεταφοράς. Η εν λόγω μέθοδος ελέγχου ταυτότητας μπορεί να είναι οτιδήποτε, από κωδικό πρόσβασης έως ψηφιακή υπογραφή. Το επίπεδο σύνδεσης χειρίζεται όλες τις συνδέσεις που δημιουργούνται μεταξύ διακομιστή και πελάτη. Ένα διαφορετικό κανάλι ανοίγει για κάθε επικοινωνία μεταξύ διακομιστή και πελάτη. Ένα παράδειγμα αυτού είναι εάν δημιουργούνται πολλές συνεδρίες στον ίδιο διακομιστή, τότε για κάθε περίοδο λειτουργίας ανοίγει ένα διαφορετικό κανάλι επικοινωνίας. Είτε ο πελάτης είτε ο διακομιστής μπορούν να ανοίξουν ένα νέο κανάλι επικοινωνίας, εφόσον οι παράμετροι για το κανάλι είναι διαθέσιμες για χρήση τόσο από τον πελάτη όσο και από τον διακομιστή.

- PGP: Το OpenPGP, γνωστό και ως PGP, είναι ένα πρωτόκολλο κρυπτογράφησης που επιτρέπει στους χρήστες να κρυπτογραφούν τα μηνύματά τους και να τα υπογράφουν ψηφιακά, δίνοντας στον αποστολέα του μηνύματος μια ισχυρότερη μέθοδο ελέγχου ταυτότητας και προστασίας της ακεραιότητας των δεδομένων. Κυρίως, το PGP χρησιμοποιείται για την προστασία ευαίσθητων πληροφοριών email. Το PGP αναπτύχθηκε τη δεκαετία του '90 σε μια προσπάθεια να γίνει ένα παγκοσμίως χρησιμοποιούμενο και διαλειτουργικό σύστημα. Το PGP είναι δωρεάν για χρήση και ενσωμάτωση σε πολλούς διαφορετικούς πελάτες email (mailers). Διαφορετικοί αλγόριθμοι κρυπτογράφησης είναι διαθέσιμοι για χρήση με το PGP, όπως RSA και DSA για ασύμμετρη κρυπτογράφηση, AES, 3DES και Twofish για συμμετρική κρυπτογράφηση και SHA για κατακερματισμό. Έχουν βρεθεί διαφορετικά τρωτά σημεία για το PGP όλα αυτά τα χρόνια, αλλά αυτά τα ελαττώματα πάντα αντιμετωπίζονταν με ενημερώσεις ή συστάσεις.
- S/MIME: Οι επεκτάσεις αλληλογραφίας ασφαλούς/πολλαπλών χρήσεων Διαδικτύου ή S/MIME είναι ανταγωνιστής του OpenPGP ως πρωτόκολλο κρυπτογράφησης που βασίζεται σε email. Ακριβώς όπως το PGP, το S/MIME επιτρέπει στους χρήστες να κρυπτογραφούν και να υπογράφουν δεδομένα email για να τα προστατεύουν περαιτέρω από εισβολείς. Η διαφορά με το PGP και το S/MIME είναι ότι το S/MIME χρησιμοποιεί διαφορετικούς αλγόριθμους κρυπτογράφησης για την ασφάλεια των δεδομένων.
- Kerberos: Το πρωτόκολλο κρυπτογράφησης Kerberos λειτουργεί ως πρωτόκολλο ελέγχου ταυτότητας ενιαίας σύνδεσης. Το πρωτόκολλο ελέγχει την ταυτότητα των χρηστών του έναντι ενός κεντρικού διακομιστή ελέγχου ταυτότητας και διανομής κλειδιών. Στους χρήστες του πρωτοκόλλου δίνονται "εισιτήρια - tickets", αφού πιστοποιηθούν, επιτρέποντάς τους να χρησιμοποιούν τις διάφορες υπηρεσίες εντός του δικτύου. Όταν ένας πελάτης με "εισιτήριο" προσεγγίζει έναν διακομιστή, αυτός ο διακομιστής επαληθεύει το "εισιτήριο" και παραχωρεί στον χρήστη πρόσβαση. Η κύρια χρήση του Kerberos είναι σε τοπικά δίκτυα (LAN) και για τη δημιουργία κοινών μυστικών. Το Kerberos είναι ένα πολύ γνωστό και συχνά χρησιμοποιούμενο πρωτόκολλο κρυπτογράφησης, αλλά τόσο ο πελάτης όσο και ο διακομιστής πρέπει να περιλαμβάνουν κώδικα για τη χρήση του Kerberos, ο οποίος απομακρύνει ορισμένους οργανισμούς από τη χρήση του.

Επομένως, μετά από αυτήν την σύντομη παρουσίαση των πρωτοκόλλων κρυπτογράφησης, αποδεικνύεται ότι η προσφερόμενη τεχνολογία πληροφορικής είναι αρκετά ώριμη έτσι ώστε να παρέχει λύσεις και στα θέματα κρυπτογραφίας που προορίζονται για το MTS. Η κρυπτογράφηση με την επιλογή κάποιων από τα προαναφερόμενα πρωτόκολλα μπορεί να προστατέψει την ανταλλασσόμενη πληροφορία, εντός - εκτός πλοίου. Η κρυπτογράφηση αφορά τόσο τους μηχανισμούς authorization - authentication καθώς και τα ίδια τα δεδομένα από τις βάσεις δεδομένων των πληροφοριακών συστημάτων IT/OT που χρησιμοποιεί η ναυτιλία για τις διεργασίες της. Στη συνέχεια θα παρουσιαστεί η χρήση της κρυπτογραφίας στις δορυφορικές επικοινωνίες [121].

Οι τεχνικές δορυφορικής κρυπτογράφησης χρησιμοποιούνται για την προστασία δεδομένων που μεταδίδονται μέσω δορυφορικών καναλιών επικοινωνίας από μη εξουσιοδοτημένη πρόσβαση και υποκλοπή. Υπάρχουν διάφορες τεχνικές κρυπτογράφησης που χρησιμοποιούνται για δορυφορική επικοινωνία, όπως:

- Advanced Encryption Standard - AES: Ο AES είναι ένας ευρέως χρησιμοποιούμενος αλγόριθμος συμμετρικής κρυπτογράφησης που θεωρείται εξαιρετικά ασφαλής. Χρησιμοποιεί ένα κλειδί 128, 192 ή 256 bit για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.
- Πρότυπο τριπλής κρυπτογράφησης δεδομένων Triple Data Encryption Standard - 3DES: Ο 3DES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιεί τρεις γύρους κρυπτογράφησης για τη βελτίωση της ασφάλειας. Βασίζεται στον αρχικό αλγόριθμο Data Encryption Standard (DES) και χρησιμοποιεί ένα κλειδί 168 bit.
- Rivest-Shamir-Adleman - RSA: Ο RSA είναι ένας δημοφιλής αλγόριθμος ασύμμετρης κρυπτογράφησης που χρησιμοποιεί ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση δεδομένων, ενώ το ιδιωτικό κλειδί για την αποκρυπτογράφηση.
- Κρυπτογραφία Ελλειπτικής Καμπύλης Elliptic Curves Codes - ECC: Το ECC είναι ένας άλλος αλγόριθμος ασύμμετρης κρυπτογράφησης που βασίζεται στα μαθηματικά των ελλειπτικών καμπυλών. Θεωρείται ότι είναι εξαιρετικά ασφαλές και χρησιμοποιείται συχνά σε συστήματα δορυφορικών επικοινωνιών.
- Διανομή Κβαντικού Κλειδιού Quantum key distribution - QKD: Το QKD είναι μια τεχνική κρυπτογράφησης που βασίζεται στην κβαντική μηχανική για να επιτύχει την ασφάλεια της μετάδοσης των δεδομένων. Είναι μια εξαιρετικά ασφαλής τεχνική που είναι ανθεκτική στην υποκλοπή.

Οι παραπάνω αλγόριθμοι κρυπτογραφίας μπορούν να εφαρμοστούν στις δορυφορικές επικοινωνίες για τη μετάδοση των δεδομένων των χρηστών. Επιπλέον, θα πρέπει να τονισθεί ότι ενδεχόμενα, εφόσον έχουν εφαρμοστεί τεχνικές κρυπτογραφίας κατά την ανάκτηση και μεταφορά των δεδομένων πριν την μετάδοση τους προς τον δορυφορικό δίαυλο, η χρήση των παραπάνω τεχνικών δεν είναι αναγκαία εφόσον τα δεδομένα έχουν ήδη κρυπτογραφηθεί.

Οι τεχνικές κρυπτογράφησης των δεδομένων από και προς τις επικοινωνίες των πλοίων θα διασφαλίσουν το απόρρητο των επικοινωνιών μεταξύ πλοίου - εταιρείας - φορέων - ακτής, σε συνδυασμό με την δυσκολία που εισάγουν σε ενδεχόμενες κυβερνο-επιθέσεις, οι οποίες δεν μπορούν να έχουν άμεση πρόσβαση στα ανταλλασσόμενα δεδομένα.

5.3.3 Καταγραφή Διεργασιών και Επικοινωνιών Πλοίου

Οι δύο προηγούμενες προτάσεις παρουσίασαν τους μηχανισμούς που θα πρέπει να χρησιμοποιηθούν για την εξατομίκευση και ταυτοποίηση των χρηστών και της κρυπτογράφησης των πληροφοριών από/προς το πλοίο. Επίσης πολύ σημαντική είναι η διαδικασία παρακολούθησης των διεργασιών και των επικοινωιών του πλοίου. Η παρακολούθηση αφορά κυρίως στην δυνατότητα καταγραφής και μετα-ανάλυσης των επικοινωνιών (monitoring processes). Οι διαδικασίες παρακολούθησης στο πλοίο δεν διαφέρουν από τις διαδικασίες παρακολούθησης ενός δικτύου επικοινωνιών. Η τεχνολογία είναι αρκετά ώριμη για να προσφέρει γενικές σουίτες (suites) λογισμικού για την παρακολούθηση και χαρτογράφηση των συνδέσεων (communication ports) ενός δικτύου [122].

Οι διαδικασίες παρακολούθησης των εσωτερικών - εξωτερικών διασυνδέσεων του πλοίου, δεν περιορίζονται μόνο στο επίπεδο των IP συνδέσεων, αλλά επεκτείνονται και με τη χρήση εξειδικευμένου λογισμικού, που θα πρέπει να προσφέρεται από τις κατασκευάστριες εταιρείες των IT/OT συστημάτων των πλοίων. Ειδικότερα τα συστήματα OT λειτουργιών, θα πρέπει να συνοδεύονται και με το απαιτούμενο λογισμικό για την παρακολούθηση και καταγραφή των διεργασιών του συγκεκριμένου λειτουργικού συστήματος. Η διαδικασία καταγραφής μέσω των παραγόμενων αρχείων καταγραφής (logs), διευκολύνει τις διαδικασίες εντοπισμού λαθών - σφαλμάτων δρασεως, αποσφαλμάτωσης, χρονικών διεργασιών και κρισίμων ενεργειών, κ.λπ. Τα καταγραφόμενα αρχεία και η διαδικασία παρακολούθησης των διεργασιών και των ενεργειών των χρηστών μέσω των λειτουργικών συστημάτων, θα πρέπει να γίνεται ερήμην του προσωπικού χειρισμού αυτών και με προσωπική ευθύνη του διαχειριστή του συνόλου των δικτύων του πλοίου.

5.3.4 Αντίγραφα Ασφαλείας και Αποκατάσταση Συστημάτων Πλοίου

Τα αντίγραφα ασφαλείας αποτελούν μία θεμελιώδη τεχνική για την προστασία δεδομένων των πληροφοριακών συστημάτων. Οι βάσεις δεδομένων που περιλαμβάνουν τα πληροφοριακά δεδομένα για τη χρήση των συστημάτων, ακόμη και αν δεν τύχουν αντικείμενο κυβερνο-επιθέσεων, μπορεί να καταστραφούν από άλλους παράγοντες (π.χ. όρια ζωής αποθηκευτικών μοναδών, φυσικές καταστροφές, κλοπή, κ.α.). Τα αντίγραφα ασφαλείας θα πρέπει να αφορούν κάθε λειτουργικό σύστημα ξεχωριστά και συνολικά για όλο το σύνολο των λειτουργιών. Τα αντίγραφα ασφαλείας συνήθως γίνονται όταν τα δίκτυα βρίσκονται σε καταστάσεις χαμηλού επιπέδου ενεργότητας (low utilization), για να μην επιβαρύνουν τη συνολική λειτουργία των συστημάτων. Η διαδικασία αυτή γίνεται με περιοδικό τρόπο για να διασφαλίσει ότι η απώλεια πληροφορίας θα είναι μικρή σε ενδεχόμενο απώλειας.

Στόχος των αντιγράφων ασφαλείας είναι η χρήση τους σε καταστάσεις όπου απαιτείται αποκτάσταση της λειτουργίας των πληροφοριακών συστημάτων (recovery backups). Ο διαχειριστής των πληροφοριακών συστημάτων του πλοίου θα πρέπει να προβαίνει στις απαιτούμενες ενέργειες και διαδικασίες για την ύπαρξη διασυνεχώς αντιγράφων ασφαλείας για όλα τα συστήματα - υποσυστήματα. Οι διαδικασίες για την δημιουργία των αντιγράφων ασφαλείας είναι αυτοματοποιημένες και χρονο-καθοριζόμενες (time scheduled) από τον διαχειρστή του συστήματος.

Οι διαδικασίες αποκατάστασης για ένα λειτουργικό σύστημα, αποτελούν την έσχατη λύση στο ενδεχόμενο που η δυσλειτουργία ενός συστήματος, από πλευράς λογισμικού, είναι μη αναστρέψιμη. Οι διαδικασίες αποκατάστασης ενός συστήματος εξαρτώνται από την αλληλεπίδραση που αυτό έχει με τα άλλα συστήματα και τον βαθμό εξάρτησης και συσχέτισης των γενικότερων λειτουργιών. Ο διαχειριστής του συστήματος του πλοίου θα πρέπει να είναι καταρτισμένος ως προς τις διαδικασίες αποκατάστασης σε συνδυασμό με την διοίκηση και να γνωρίζει επακριβώς χρόνους και μεθόδους για την αποκατάσταση. Το ενεδεχόμενο κυβερνο-επιθεσεων αντιμετωπίζεται ως μία αντίστοιχη κατάσταση μη αποκαταστάσιμου σφάλματος, που απαιτεί επαναφορά του λειτουργικού λογισμικού,των βάσεων δεδομένων και επανασύνδεσης του πληροφοριακού συστήματος επικοινωνιών.

5.3.5 Πρωτοκολλικές δομές για τα συστήματος AIS, GNSS και GMDSS

Από τις μεγαλύτερες ελλείψεις που έχουν διαπιστωθεί στις επικοινωνίες μέσω των συστημάτων IAS, GNSS και GMDSS, είναι η έλλειψη δομών πιστοποίησης των ανταλλασσόμενων πληροφοριών. Στα κεφάλαια 3 και 4 της εργασίας παρουσιάστηκαν αναλυτικά τα προβλήματα που δημιουργούνται με τις επικοινωνίες και την λειτουργία των ανωτέρω συστημάτων. Για τον λόγο αυτό, τα λειτουργικά αυτά συστήματα τυγχάνουν αντικείμενο κυβερνο-επιθέσεων που είναι ικανές να αδρανοποιήσουν ή ακόμη χειρότερα να προκαλέσουν καθυστερήσεις ή/και να θέσουν σε κίνδυνο τα πλοία, το προσωπικό και τα εμπορεύματα τους.

Επομένως, και μέσω των τεχνικών κρυπτογραφίας που προτάθηκαν, είναι χρήσιμο να επανακαθοριστούν τα πρότυπα (standards), επάνω στα οποία βασίζονται τα λειτουργικά αυτά συστήματα. Όπως γίνεται γενικότερα αποδεκτό, ειδικά για το AIS, τα πρότυπα - πρωτόκολλα τους βασίστηκαν σε παλαιότερες χρονικές περιόδους, όπου η παγκόσμια διασύνδεση δεν ήταν ώριμη από τις ICT τεχνολογίες, και επομένως δεν κινδύνευαν από κυβερνο-επιθέσεις ή άλλου τύπου κινδύνους. Στην περίπτωση όπου η αναθεώρηση των προτύπων για αυτά τα συστήματα θα δημιουργήσει σημαντική αναστάτωση στους παρόχους των αντίστοιχων τεχνολογιών, η χρήση της κρυπτογραφημένης ανταλλαγής πληροφορίας μπορεί να επιλύσει σε σημαντικό βαθμό το πρόβλημα των κυβερνο-επιθέσεων, δεδομένης της ασφάλειας που παρέχει στις επικοινωνίες.

5.3.6 Ο ρόλος του CISO στο Πλοίο

Όπως έχει διαφανεί και από τις προηγούμενες ενότητες της εργασίας, τα σύγχρονα πλοία καθώς και οι μελλοντικές τάσεις για την αυτόνομη ναυτιλία, τείνουν να μετατρέψουν τα παραδοσιακά πλοία σε δομικά και λειτουργικά πληροφοριακά συστήματα. Ήδη από τις προηγούμενες προτάσεις της

ενότητας, διαφαίνεται ο σημαντικός ρόλος του Διαχειριστή του συνολικού συστήμαος. Στα κλασικά πληροφοριακά συστήματα, ο ρόλος του είναι ο αντίστοιχος ρόλος του Chief Information Security Officer - CISO. Στις παραδοσιακές διοικητικές δομές του πλοίου (καπετάνιος, α/β/γ μηχανικός, κ.λπ.), θα πρέπει να προστεθεί και η διοικητική θέση του αξιωματικού CISO, ο οποίος θα είναι υπεύθυνος για τα ακόλουθα:

- Διαχείριση Δικτυακών Δομών και Επικοινωνιών Πλοίου
- Παρακολούθηση Δικτυακών Δομών και Επικονωνιών Πλοίου
- Διαχείριση IT/OT συστημάτων
- Έλεγχος λειτουργίας και αποκατάσταση τους
- Ιεραρχική Πρόσβαση στα Συστήματα
- Συμμόρφωση των υπολοίπων δομών στα πρότυπα ασφαλείας

Η ύπαρξη του CISO ως αξιωματικού υπεύθυνου για τα πληροφοριακά και λειτουργικά συστήματα του πλοίου από πλευράς ICT, θα διασφαλίσει την λειτουργικότητα του πλοίου, θα επιμερίσει τις επαγόμενες ευθύνες από τα πληρώματα (που τις περισσότερες φορές δεν γνωρίζουν από τεχνολογίες ICT), και θα διασφαλίσει την απρόσκοπτη λειτουργία αλλά και την έγκαιρη παρέμβαση του σε περιπτώσεις κυβερνο-επιθέσεων. Ο CISO ίσως να είναι και η τελευταία ανθρώπινη παρουσία επί των πλοίων, πριν την καθολική μετάβαση προς την αυτόνομη ναυτιλία. Φορείς όπως ο USCG έχουν αρχίσει να διαβλέπουν την θέση αξιωματικών CISO για την επικείμενη αντιμετώπιση των κυβερνο-επιθέσεων στο άμεσο μέλλον.Αντίστοιχη βαρύτητα δίνεται πλέον και στα πολεμικά πλοία, καθώς σε πολλά σύγχρονα πολεμικά πλοία υφίσταται πέρα από τον CISO προσωπικό 24/7 το οποίο παρακολουθεί σε μια κονσόλα τους διάφορους «συναγερμούς» (alert) τα οποία προέρχονται από τα logs κα τα EDR που είναι εγκατεστημένα στα συστήματα του πλοίου, καθώς και αποστέλλουν αντίστοιχα logs στο SOC το οποίο βρίσκεται στην ξηρά.

6. Σύνοψη

Η κυβερνοασφάλεια στη ναυτιλία είναι ένα συνεχώς εξελισσόμενο πεδίο που απαιτεί διαρκή επαγρύπνηση και προσαρμογή στις νέες απειλές. Παρά τις υπάρχουσες στρατηγικές και μέτρα αντιμετώπισης, η ανάγκη για περαιτέρω έρευνα και ανάπτυξη είναι επιτακτική. Μελλοντικές πρωτοβουλίες θα μπορούσαν να περιλαμβάνουν την ενίσχυση της εκπαίδευσης του προσωπικού, την ανάπτυξη πιο προηγμένων τεχνολογιών ανίχνευσης και πρόληψης, καθώς και τη συνεργασία μεταξύ των ναυτιλιακών εταιρειών και των κυβερνητικών φορέων για την ανταλλαγή πληροφοριών (Cyber Threat Intelligence) και βέλτιστων πρακτικών. Επιπλέον για την Ελλάδα, που είναι μεγάλη ναυτική χώρα, με αρκετές ελληνικές εταιρείες θα μπορούσε να υλοποιηθεί τομεακό Κέντρο Αντιμετώπισης Κυβερνοαπειλών,(CERT) στα πρότυπα του BIMCO, το οποίο θα κρατάει υποτύπωση των Κυβερνοπεριστατικών, θα έχει προσωπικό εξειδικευμένο για κυβερνοεπιθέσεις σε ναυτιλιακά συστήματα, θα διαμοιράζει CTI μεταξύ των φορέων, θα επεμβαίνει σε κυβερνοπεριστατικά και θα συνεργάζεται με ρυθμιστικές Αρχές και αντίστοιχους φορείς του εξωτερικού. Το σχέδιο αυτό θα μπορούσε να υλοποιηθεί και από τους φορείς Ναυτιλίας με ιδίους πόρους και θα εκτιμάται ότι θα ήταν ιδιαίτερα επωφελές

Βιβλιογραφία - Διαδικτυακές Πηγές

[1] Maritime Cybersecurity A Guide for Leaders and Managers, G.C. Kessler, S.D. Shepard, © 2020

[2] The Guidelines on Cybersecurity onboard ships, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and WORLD SHIPPING COUNCIL

[3] The National Strategy of Maritime Security, Sep 2005

[4] Cybersecurity in Maritime Critical Infrastructure, European Commission, 20/03/2023

[5] IMO: Maritime Cyber Risk https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[6] A Retrospective Analysis of Maritime Cyber Security Incidents, P.H. Meland, K. Bernsmed, E. WilleO.J. Rodseth, D.A. Nesheim, TRANSNAV, Vol. 15, No 3, Sep 2021

[7] Satellite Systems and Networks Explained https://www.gtmaritime.com/resources/satellite-systems-and-networks-explained/

[8] Communication Systems in the Maritime Industry https://gmdsstesters.com/radio-survey/gmdss-radio/communication-systems-in-the-maritime-industry.html

[9] Top 7 Maritime satellite communication companies https://www.verifiedmarketresearch.com/blog/top-maritime-satellite-communication-companies/

[10] Maritime Communications Satellite Systems and Equipment, MCSSE Handbook 2019

[11] Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends, M.B. Farah, E. Ukwandu, H. Hindy, D. Brosset, Inofrmation 2022, 13, 22, MDPI

[12] Guidelines of Maritime Cyber Risk Management, IMO, MSC-FAL.1/Circ.3/Rev.2, 7 June 2022

[13] Cybersecurity threats to satellite communications: Towards a typology of state actor responses, D. Housen-Couriel, Acta Astronautica 128 (2016) 409-415

[14] Satellite applications of spread spectrum frequency hopping techniques, F. Ananasso, G. Gallinaro, E. Saggese, Conf. Paper, Dec 1989, DOI: 10.1109/GLOCOM.1989.64241 · Source: IEEE Xplore

[15] Types Of Satellites: Different Orbits & Real-World Uses https://eos.com/blog/types-of-satellites/

[16] Radio Spectrum Definitiion https://en.wikipedia.org/wiki/Radio_spectrum

[17] Autonomous shipping https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

[18] Autonomous Ships https://marine-offshore.bureauveritas.com/marine/autonomous-ships

[19] Autonomous ships https://www.ils.be/autonomous-ships/

[20] What is Autonomous Shipping? https://www.searates.com/gr/blog/post/what-is-autonomous-shipping

[21] Maritime Autonomous Ships and Shipping https://transport.ec.europa.eu/transport-modes/maritime/maritime-autonomous-ships-and-shipping_en

[22] Can shipping autonomous navigation systems lead us to a safer future? https://www.orca-ai.io/blog/benefit-of-adopting-maritime-autonomous-navigation-systems/

[23] A Historic Journey with Modern Technology https://www.iridium.com/blog/mayflower-autonomous-ship-voyage/

[24] The Nippon Foundation MEGURI2040 Fully Autonomous Ship Program https://www.nippon-foundation.or.jp/en/what/projects/meguri2040

[25] Wider implications of autonomous vessels for the maritime industry: Mapping the unprecedented challenges, H. Ghaderi, 2020

[26] Facilitation Committee (FAL 46), 9 to 13 May 2022 https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/FAL-46th-Session.aspx

[27] Cybersecurity Considerations in Autonomous Ships, S. CHO, E. ORYE, G. VISKY, V. PRATES, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is

[28] 'D8.6: Final Report: Autonomous Bridge,' The MUNIN Project Deliverable, 6 August 2015,

[29] Jia Wang, Yang Xiao, Tieshan Li and C. L. Philip Chen, 'A Survey of Technologies for Unmanned Merchant Ships,' IEEE Access, Vol. 8, pp. 224461-224486, 2020, doi: 10.1109/ACCESS.2020.3044040.

[30] Cybermarétique: a short history of cyberattacks against ports https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/

[31] Cyber risk The emerging Cyber threat to industrial control systems, G. Carpenter, Lloyd's 2021

[32] Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III) Cybersecurity in Maritime Critical Infrastructure Reflection on African Ports, EUROPEAN COMMISSION, EuropeAid Co-operation Office Instrument for Stability/ Contract no. No. IFS/2019/410-525

[33] IACS unified requirements E26 and E27 Cyber security beyond compliance, ClassNK, Cuber Security, Inmarsat

[34] Greenberg, M.D., Chalk, P., Willis, H.H., Khilko, I., Ortiz, D.S.: Maritime Terrorism. RAND Corporation (2006).

[35] Weldemichael, A.T., Schneider, P., Winner, A.C.: Maritime Terrorism and Piracy in the Indian Ocean Region. Routledge (2017).

[36] Cimpean, D., Meire, J., Bouckaert, V., Casteele, S.V., Pelle, A., Hellebooge, L.: Analysis of Cyber Security Aspects in the Maritime Sector. (2011).

[37] Nesheim, D.A., Rødseth, Ø., Bernsmed, K., Frøystad, C., Meland, P.H.: D1.1 Risk Model and Analysis. (2017).

[38] Jones, K.D., Tam, K., Papadaki, M.: Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference. 1, 1, (2016).

[39] Tam, K., Jones, K.: Cyber-Risk Assessment for Autonomous Ships. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). pp. 1–8 (2018).

[40] Tam, K., Moara-Nkwe, K., Jones, K.: A Conceptual Cyber-Risk Assessment of Port Infastructure. Presented at the 2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs , Parede, Portugal January 29 (2021).

[41] Aven, T.: On the meaning of a black swan in a risk context. Safety Science. 57, 44–51 (2013).

[42] Drougkas, A., Sarri, A., Kyranoudi, P., Zisi, A.: Port Cybersecurity: Good practices for cybersecurity in the maritime sector. (2019).

[43] Caprolu, M., Pietro, R.D., Raponi, S., Sciancalepore, S., Tedeschi, P.: Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Communications Magazine. 58, 6, 90–96 (2020).

[44] Boyes, H., Isbell, R.: Code of Practice: Cyber Security for Ships. IET Standard, Department for Transport (UK) (2017).

[45] Sfakianakis, A., Drougkas, A., Douligeris, C., Marinos, L., Lourenço, M., Raghimi, O.: ENISA threat landscape report 2018 - 15 top cyberthreats and trends. (2019).

[46] PST: Nasjonal trusselvurdering 2020, https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

[47] NSM: Helhetlig digitalt risikobilde 2019. (2019).

[48] NSM: RISIKO 2020. (2020).

[49] CyberKeel: Maritime Cyber-Risks,

[50] Shauk, Z.: Malware on the offshore rig: Danger lurks where the chips fail, https://www.houstonchronicle.com/business/energy/article/Malware-on-the-offshore-rig-Danger-lurks-where-4470723.php

[51] Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020).

[52] Kristoffersen, P.B., Hartvigsen, T., Myrvang, P., Torjusen, A.: Digitale Sårbarheter Maritim Sektor. DNV-GL, Lysneutvalget (2015).

https://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html

[53] Nguyen, L.: Collaboration in the Shipping Industry: Innovation and Technology, https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/

[54] Walker, J., Spencer, J.: Cyber Marine: Risks & Loss Scenarios,

[55] GREAT: The Icefog APT: A Tale of Cloak and Three Daggers, https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/

[56] CyberKeel: Maritime Cyber-Risks,

[57] Torbati, J., Saul, Y.: Iran's top cargo shipping line says sanctions damage mounting, https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022

[58] Singh, H.: Cyber Security in Maritime Industry. University of Oslo (2019).

[59] Kristiansen, T.: DR: Kina hackede sig ind i Søfartsstyrelsen, https://shippingwatch.dk/Rederier/article7043149.ece

[60] Athens Group: Cybersecurity – There Is No Silver Bullet, https://hbr.org/2023/04/theres-no-silver-bullet-for-cybersecurity

[61] Knox, J.: Coast Guard Commandant on Cyber in the maritime domain

[62] Windward: AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea. (2014)

[63] Schnelle, S.: Kartlegging av maritime hybride trusler. Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet? Forsvarets Høgskole (2018).

[64] Wallace, T., Mesko, F.: The Odessa Network Mapping Facilitators of Russian and Ukrainian Arms Transfers

[65] ASCStaff: Cyberattack on Clarkson's shipbroker reaffirms industry's vulnerability, https://www.logisticsmiddleeast.com/transport/article-13696-cyberattack-on-clarksons-shipbroker-reaffirms-industrys-vulnerability

[66] Cimpanu, C.: Shipping Firm Avoids Customer Data Dump in Last Year's Hack & Ransom Incident, https://www.theguardian.com/technology/2017/nov/29/shipping-charksons-data-hacker-cyber-attack

[67] Cimpanu, C.: Ransomware Infection Cripples Shipping Giant COSCO's American Network, https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

[68] Greenberg, A.: The Untold Story of NotPetya, the Most Devastating Cyberattack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[69] Maritime Executive: Naval Dome: Cyberattacks on OT Systems on the Rise, https://maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise

[70] Vold, L.B.: Den Norske Krigsforsikring for Skib

[71] Lubold, G., Volz, D.: Chinese Hackers Breach U.S. Navy Contractors - WSJ, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401

[72] Volz, D.: Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets, https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

[73] Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility, https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/

[74] Safety4Sea: 2018 Highlights: Major cyber attacks reported in maritime industry, https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/

[75] Reynolds, Z.: Australian defence shipbuilder Austral victim of Iranian cyber attack, https://www.rcc.int/swp/news/155/iranian-hackers-suspected-in-cyber-breach-and-extortion-attempt-on-navy-shipbuilder-austal

[76] Secureworks: GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry, https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

[77] Cimpanu, C.: Ransomware Infection Cripples Shipping Giant COSCO's American Network, https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

[78] INTERPOL: Cybercrime: COVID-19 IMPACT

[79] Maritime Executive: Saipem's Servers Hit by Cyberattack, https://maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack

[80] Lemos, R.: Coast Guard Warns Shipping Firms of Maritime Cyberattacks, https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks

[81] Goud, N.: Cyber Attack on James Fisher and Sons, https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/

[82] Buurma, C., Sebenius, A.: Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days, https://www.carriermanagement.com/news/2020/02/20/203485.htm

[83] Dragos, Inc.: Assessment of Ransomware Event at U.S. Pipeline Operator | Dragos, https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/

[84] Grinter, M.: Maritime cyber-attacks up 900% in three years, https://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/

[85] Warrick, J., Nakashima, E.: Officials: Israel linked to a disruptive cyberattack on Iranian port facility, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

[86] Goud, N.: Ransomware attack on Norwegian Ship yard results in job loss to many, https://www.cybersecurity-insiders.com/ransomware-attack-on-norwegian-ship-yard-results-in-job-loss-to-many/

[87] Safety4Sea: Vard shipbuilder experiences ransomware attack, https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/

[88] Maritime Executive: Carnival Corporation Reports Ransomware Attack Accessed Data, https://maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data

[89] Agius, M.: TM mum on whether cyber-attack affected ship, air registries

[90] Azzopardi, K.: Transport Malta cyber attack investigation has not yet determined whether data was stolen, https://www.maltatoday.com.mt/news/national/105593/watch_transport_malta_cyber_attack_investigation_has_not_yet_determined_whether_data_was_stolen

[91] Asplem, A.: Norwegian Maritime Cyber Resilience Centre (NORMA Cyber), (2021).

[92] Lejon, J.: Kryptera.se Ransomware lista

[93] Coble, S.: Ransomware Attack on Shipping Giant, https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships

[94] Shen, C., Baker, J.: CMA CGM confirms ransomware attack, https://lloydslist.com/LL1134044/CMA-CGM-confirms-ransomware-attack

[95] Kovacs, E.: UN Maritime Agency Hit by "Sophisticated Cyberattack,", https://smartmaritimenetwork.com/2020/10/01/imo-latest-to-fall-victim-to-cyber-attack/

[96] O'Dwyer, R.: IMO latest to fall victim to cyber attack

[97] BBC: Red Funnel ferry firm's IT system hit by "malicious attack,", https://www.bbc.com/news/uk-england-hampshire-54368110

[98] Toogood, D.: Red Funnel siffers "malicious attack" on IT systems causing major disruption, https://www.islandecho.co.uk/red-funnel-suffers-malicious-attack-on-it-systems-causing-major-disruption/

[99] Matson: Matson Reports Cyber Attack

[100] Cary, A.: Update: Hacker demands $200K ransom from Tri-Cities port to unlock computer data, https://www.govtech.com/security/hackers-demand-200k-from-washington-port-to-unlock-data.html

[101] Maritime Executive: Ransomware Cripples IT Systems of Inland Port in Washington State, https://maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state

[102] Bøe, E., Jordheim, H.: Politiet etterforsker dataangrepet mot Hurtigruten, https://www.itromso.no/nyheter/i/Qx6zaV/politiet-etterforsker-dataangrepet-mot-hurtigruten

[103] Maritime Executive: Hurtigruten Reports Passenger Data Exposed in Cyberattack, https://maritime-executive.com/article/hurtigruten-reports-passenger-data-exposed-in-cyberattack

[104] Safety4Sea: Hurtigruten hit by cyber-attack, https://safety4sea.com/hurtigruten-hit-by-cyber-attack/

[105] Walker, J.: AIDA Cruise Ships Under Cyber Attack - Are Costa Ships Also Affected?, https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/

[106] ISO/IEC 27000:2018: Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC (2018), https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

[107] Alcaide, J.I., Llave, R.G.: Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia. 45, 547–554 (2020). https://doi.org/10.1016/j.trpro.2020.03.058.

[108] Kretschmann, L., Rødseth, Ø., Tjora, Å., Fuller, B.S., Noble, H., Horahan, J.: D9.2: Qualitative assessment. (2015),

[109] What are Industry 4.0, the Fourth Industrial Revolution, and 4IR? https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir

[110] McKinsey https://www.myconsultingoffer.org/cover-letter/is-mckinsey-good-place-to-work/

[111] NIST https://www.nist.gov

[112] BIMCO BIMCO et al Industry Consortium

[113] ABS https://ww2.eagle.org/en.html

[114] ENISA https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

[115] IET https://www.theiet.org

[116] IAPH https://www.iaphworldports.org

[117] USCG https://www.uscg.mil

[118] CISA https://www.cisa.gov

[119] What are authentication protocols? https://www.okta.com/identity-101/authentication-protocols/

[120] What are Encryption Protocols and How Do They Work? https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/

[121] Satellite Encryption Techniques https://yesway.co.uk/satellite-encryption-techniques/

[122] 28 Best Network Monitoring Software Reviewed For 2024 https://thectoclub.com/tools/best-network-monitoring-software/