ΔΙΪΔΡΥΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΤΗ ΝΑΥΤΙΛΙΑ ΚΑΙ ΤΙΣ ΜΕΤΑΦΟΡΕΣ»

ΤΙΤΛΟΣ ΕΡΓΑΣΙΑΣ

"Κυβερνοασφάλεια και ναυτιλία: οπτικές και προκλήσεις"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Του
Πετρόπουλου Αθανάσιου

Επιβλέπων καθηγητής: Σπυρόπουλος Φώτιος

Υποβληθείσα ως μέρος των απαιτήσεων για την απόκτηση

Μεταπτυχιακού Διπλώματος (MSc) στις Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές

ΑΘΗΝΑ
ΦΕΒΡΟΥΑΡΙΟΣ 2021

Μέλη Εξεταστικής Επιτροπής

Σπυρόπουλος Φωτιος

Digitally signed by FOTIOS SPYROPOULOS
Date: 2021.03.19 09:09:29 EET

Παπουτσιδάκης Μιχαήλ

Νικητάκος Νικήτας

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Πετρόπουλος Αθανάσιος του Δημητρίου, με αριθμό μητρώου 87 φοιτητής του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής της Σχολής Μηχανικών Πανεπιστημίου Δυτικής Αττικής, δηλώνω υπεύθυνα ότι: «Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου».

Ο δηλών

Πετρόπουλος Αθανάσιος

ΠΕΡΙΛΗΨΗ

Στη σημερινή εποχή κυριαρχεί ο κόσμος της πληροφορίας καθώς επίσης και της ανταλλαγής πληροφοριών. Σε αυτή την εποχή, η απαίτηση για ασφάλεια συνεχώς και αυξάνεται. Ο σύγχρονος επιχειρησιακός κόσμος εμφανίζει ολοένα και μεγαλύτερο ενδιαφέρον σε ό,τι έχει να κάνει με την ασφάλεια στον κυβερνοχώρο, που αποτελεί πεδίο έρευνας αυτής της εργασίας.

Είναι δεδομένο πως τα τελευταία χρόνια η τεχνολογία αναπτύσσεται με ραγδαίους ρυθμούς και αυτό την κάνει πιο δύσκολη στην προσαρμογή των ανθρώπων με αυτή. Ο τομέας της ναυτιλίας αποτελεί ένα σημαντικό κομμάτι του σύγχρονου επιχειρησιακού κόσμου, που εκτίθεται σε καθημερινή βάση σε αρκετούς και διαφορετικούς κινδύνους και αυτό είναι κάτι που τα τελευταία χρόνια αναπτύσσεται τεράστιους προβληματισμούς.

Ο IMO τα τελευταία χρόνια έχει αναπτύξει καθορισμένους κανόνες, που έχουν σαν βασικότερο σκοπό να προσφέρουν υψηλότερη ασφάλεια στον θαλάσσιο κυβερνοχώρο. Οι επιχειρήσεις του εν λόγω τομέα ακολουθούν όλες τις οδηγίες που έχουν λάβει από την BIMCO που έχουν πάρει την απαιτούμενη έγκριση από τον IMO και με αυτόν τον τρόπο καλύπτονται σε ό,τι έχει να κάνει με το κομμάτι του ISM. Οι νηογνώμονες από την άλλη μεριά, παίζουν εξίσου σημαντικό ρόλο στις συγκεκριμένες επιχειρήσεις, προκειμένου να κατορθώσουν να εφαρμόζουν ορθά όλες τις δράσεις και να κάνουν τις απαραίτητες δοκιμές διείσδυσης στα συστήματά τους.

Γενικότερα, είναι ζωτικής σημασίας όλες αυτές οι εταιρίες να έχουν την ευχέρεια να αντιλαμβάνονται συνεχώς τις ευκαιρίες αλλά και τους κινδύνους, οι οποίοι έχουν άρρηκτη σχέση με την ψηφιακή καινοτομία, να εξισορροπήσουν την απαίτηση της προστασίας τους από τις διάφορες απειλές που υπάρχουν καθώς επίσης και την απαίτηση υιοθέτησης καινούριων επιχειρηματικών σχεδίων και καινούριων τακτικών, οι οποίες αξιοποιούν την τεχνολογία και βάζουν καινούριες βάσεις εξέλιξης. Για αυτό

το λόγο είναι σημαντικό να αντιληφθούν το βάθος και το προφίλ του εκάστοτε κινδύνου και να αξιολογήσουν το υφιστάμενο επίπεδο ασφαλείας.

ABSTRACT

The world of information as well as the exchange of information dominates today. In this day and age, the demand for security is constantly increasing. The modern business world is increasingly interested in cybersecurity, which is a field of research in this field.

It is a given that in recent years technology is developing rapidly and this makes it more difficult for people to adapt to it. The shipping sector is an important part of the modern business world, which is exposed on a daily basis to several different risks and this is something that in recent years has developed enormous concerns.

In recent years, the IMO has developed set rules, which have as their main purpose to offer higher security in the marine cyberspace. The companies in this sector follow all the instructions they have received from BIMCO that have received the required approval from the IMO and in this way they are covered in everything that has to do with the part of ISM. The classification societies, on the other hand, play an equally important role in these companies, in order to be able to properly implement all the actions and to make the necessary penetration tests in their systems.

In general, it is vital that all these companies have the ability to be constantly aware of the opportunities and risks, which are inextricably linked to digital innovation, to balance the need to protect themselves from the various threats that exist as well as the demand for the adoption of new business plans and new tactics, which utilize technology and lay new foundations for development. For this reason it is important to understand the depth and profile of each risk and to assess the existing level of safety.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

ΕΙΣΑΓΩΓΗ

Στη σύγχρονη εποχή, η ασφάλεια των θαλάσσιων μεταφορών αποτελεί έναν από τους βασικότερους σκοπούς του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) τα τελευταία έτη. Ο Διεθνής Κώδικας Διαχείρισης Ασφάλειας (ISM) καθώς επίσης και ο Διεθνής Κώδικας Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ISPS) αναπτύχθηκαν με απώτερο στόχο να καταφέρουν να διασφαλίσουν στο βέλτιστο εφικτό επίπεδο την ασφάλεια στις πλωτές εξέδρες καθώς επίσης και στις λιμενικές εγκαταστάσεις, αλλά και στα εμπορικά και επιβατηγά σκάφη.

Οι συγκεκριμένοι κώδικες έχουν άρρηκτη σχέση με την ανίχνευση των κινδύνων στα σύγχρονα σκάφη, την πρόληψη ατυχημάτων αλλά και την αντιμετώπιση επικίνδυνων συνθηκών με καθοριστικές επιπτώσεις, όπως είναι για παράδειγμα η απώλεια ζωής, η καταστροφή του περιβάλλοντος κλπ. Στη σημερινή εποχή, οι προβληματισμοί για την ασφάλεια δεν περιορίζονται μονάχα σε φυσικές καταστροφές κλπ.

Ιστορικά, όταν ένα σκάφος έφευγε από τον λιμένα, ήταν ουσιαστικά αποκομμένο και μια αρνητική έκβαση του πλου οφειλόταν μονάχα σε ανθρώπινο λάθος είτε μηχανική αποτυχία. Παρά το γεγονός αυτό, όμως, λόγω της ραγδαίας εξέλιξης της τεχνολογίας και των ανοιχτών επικοινωνιών με τις εγκαταστάσεις ξηράς, τα σύγχρονα σκάφη έχουν εισχωρήσει σε ένα καινούριο και εξαιρετικά υποσχόμενο περιβάλλον, που είναι η ψηφιακή εποχή.

Η συγκεκριμένη εποχή έχει καταφέρει να μεταβάλλει ριζικά την εν λόγω βιομηχανία. Η δράση λήψης καθοριστικών αποφάσεων τις περισσότερες φορές υλοποιείται σε αρκετά μεγαλύτερο επίπεδο διαμέσου των ψηφιακών πληροφοριών, οι οποίες συλλέγονται κατά την περίοδο ενός ταξιδιού και μεταδίδονται στα κεντρικά γραφεία όλων των εταιριών.

Παρόλα αυτά, η αναδυόμενη ευκαιρία για αυτόν τον τομέα κρύβει και σημαντικούς κινδύνους. Η αισθητή ανοδική τάση της δια-λειτουργικότητας αναπτύσσει καινούριες προκλήσεις στον εν λόγω κλάδο, όπως είναι για παράδειγμα ο κυβερνο-πόλεμος, που περιέχεται από υψηλότερο επίπεδο αβεβαιότητας καθώς επίσης και από έλλειψη κατανόησης των σημαντικότερων κινδύνων.

Η αισθητή ανοδική τάση της πολυπλοκότητας, η ψηφιοποίηση, η ολοκλήρωση αλλά και η αυτοματοποίηση των συστημάτων όπου εστιάζει αυτός ο τομέας έχει ανάγκη από ολιστική διαχείριση του συγκεκριμένου θέματος. Στη σημερινή εποχή πιο συχνά διαφοροποιημένα συστήματα διασυνδέονται όχι μονάχα στο τοπικό δίκτυο του σκάφους αλλά και στο internet, κάτι το οποίο βοηθάει στην αισθητή ανοδική τάση των κινδύνων αυτής της μορφής.

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως η ασφάλεια των ψηφιακών συστημάτων είναι πλέον αναγκαστική όχι μονάχα με απώτερο στόχο την προστασία των πληροφοριών αλλά και με στόχο την βέλτιστη εφικτή διασφάλιση ασφαλών αλλά και αξιόπιστων δράσεων. Χαρακτηριστικό παράδειγμα παρόμοιας μορφής κινδύνων είναι η διάπραξη εγκληματικών πράξεων, όπως είναι για παράδειγμα η αρπαγή του σκάφους είτε η κλοπή του φορτίου, η απώλεια ελέγχου του είτε η απώλεια δεδομένων κλπ.

Η χρησιμότητα των καινούριων τεχνολογιών είναι εφικτό να παίξει καθοριστικό ρόλο στην αποδοτικότητα αλλά και στην ασφάλεια των σύγχρονων σκαφών, παρόλο που βοηθάει στην αισθητή ανοδική τάση των πιθανοτήτων να υπάρξει πρόβλημα κυβερνοασφάλειας. Στόχος της συγκεκριμένης εργασίας αποτελεί η διεξοδική μελέτη και η εκτενής έρευνα για το ζήτημα της κυβερνοασφάλειας στη ναυτιλία. Για να επιτευχθεί αυτός ο στόχος θα υλοποιηθεί μια βιβλιογραφική ανασκόπηση μέσα από διεθνείς, ελληνικές καθώς επίσης και διαδικτυακές βιβλιογραφικές πηγές.

Κεφάλαιο

1

Η ΨΗΦΙΟΠΟΙΗΣΗ ΤΗΣ ΝΑΥΤΙΛΙΑΣ

1.1 Πληροφορική στη ναυτιλία

Η ραγδαία ανάπτυξη του τομέα της πληροφορικής και της τεχνολογίας γενικότερα αποτελούν μια από τις κυριότερες παραμέτρους για τη σημαντική πρόοδο που έχει παρουσιάσει τα τελευταία χρόνια η ναυτιλιακή βιομηχανία, που αποτελεί πεδίο έρευνας αυτής της εργασίας. Στην αρχή, τα δεδομένα και οι πληροφορίες οι οποίες στη σημερινή εποχή είναι εφικτό να εκλάβουν από την εξέλιξη των ψηφιακών δεδομένων, έχουν επιτρέψει την πιο εύκολη επικοινωνία ανάμεσα στην ξηρά και στη θάλασσα (Δημοβασίλη, 2018).

Παράλληλα, προσφέρουν την ευχέρεια να γίνει πιο εύκολη η διαχείριση των σύγχρονων σκαφών, να παίρνουν εξυπνότερες, ορθότερες αλλά και αμεσότερες αποφάσεις, να ελαττώσουν σε μεγάλο βαθμό το κόστος των δαπανών αλλά και το χρόνο ο οποίος απαιτείται προκειμένου να υλοποιηθεί μια δράση. Με αυτόν τον τρόπο παίζουν καθοριστικό ρόλο στο να βελτιστοποιηθούν τα σκάφη και οι δυνατότητες που έχουν (Νικητάκος, 2011).

Ταυτόχρονα διαμέσου της εξέλιξης των συγκεκριμένων παραμέτρων, υφίσταται αισθητά ανοδική τάση του ανταγωνισμού σε αυτή τη βιομηχανία. Ο τομέας της πληροφορικής έχει την ευχέρεια να παίξει σημαντικό ρόλο στην πρόοδο αυτού του τομέα, με την απαίτηση για διαρκή online επικοινωνία. Η τεχνολογία όλα αυτά τα χρόνια παρέχει μεθόδους να παραμένουν διασυνδεδεμένοι οι χρήστες, δίχως να υφίσταται καμία απολύτως εξάρτηση από τα συστήματα τα οποία χρησιμοποιούν, την τοποθεσία στην οποία είναι είτε τη διαφορά ώρας (Visvikis and Panayides, 2017).

Ακόμα, εξαιτίας του τεράστιου όγκου δεδομένων που έχουν την ευχέρεια να μεταφέρουν, καθώς επίσης και του μόνιμου κινδύνου hacking, οι επιχειρήσεις είτε οι οργανισμοί του εν λόγω κλάδου είναι ζωτικής σημασίας να εξετάσουν ξανά τα επίπεδα ασφαλείας ακόμη και των ευέλικτων συστημάτων είτε ακόμα και των υποδομών τους (Κοκοτος και συν., 2010).

Η σύγχρονη τεχνολογία αυτού του κλάδου είναι εφικτό να παρέχει τις πιο σωστές επιλογές, οι οποίες έχουν την ευχέρεια να συνδυάσουν εξελιγμένα γνωρίσματα ασφαλείας ενώ την ίδια ώρα παρέχουν την απαιτούμενη προστασία από πιθανούς κινδύνους σε πραγματικό χώρο είτε και χρόνο, με βασικότερο στόχο να ικανοποιούν τους τελικούς καταναλωτές, βελτιώνοντας σε τεράστιο επίπεδο τις επιδόσεις των επιχειρήσεων αυτού του τομέα (Varun, 2019).

1.2 Η ανάγκη για ανάπτυξη πληροφοριακών συστημάτων στη ναυτιλία

Στη σημερινή εποχή, τα ιδιαίτερα γνωρίσματα των επιχειρήσεων του συγκεκριμένου τομέα φέρνουν σαν καθοριστικό ζητούμενο και την απαίτηση ανάπτυξης συστημάτων αυτής της μορφής. Η απαίτηση για περισσότερη και καλύτερη

ενημέρωση και πληροφόρηση είναι φυσικά πιο μεγάλη σε σχέση με αυτή που έχει μια άλλη εταιρία που βρίσκεται στην ξηρά (Δημοβασίλη, 2018).

Η ιδιαιτερότητα στην οποία εστιάζει στη σημασία του όγκου των δεδομένων σε έναν τομέα αυτού του είδους, όπως είναι για παράδειγμα ο τομέας που μελετάμε σε αυτή την εργασία, δεν είναι καμία άλλη παρά μονάχα του γεγονότος πως είναι σημαντικό να κινεί τα εργοστάσια της στο διεθνές περιβάλλον. Για παράδειγμα, είναι εφικτό ένα από τα αρκετά σκάφη τα οποία διαχειρίζεται μια τέτοια εταιρία να είναι στις όχθες της Αυστραλίας ενώ η βάση της να είναι στην Ελλάδα (Κοκοτος και Λιναρδάτος, 2010).

Από την άλλη μεριά, ένας εξίσου σημαντικός λόγος που κάνει αυτά τα συστήματα ζωτικής σημασίας είναι ο τεράστιος όγκος δεδομένων ο οποίος χρειάζεται με απώτερο στόχο την ορθότερη ολοκλήρωση των δράσεων που έχει η εκάστοτε εταιρία αυτού του είδους. Για παράδειγμα τα επίπεδα των ναύλων μεταβάλλονται ριζικά σε μικρή χρονική περίοδο, ενώ οι τιμές των καυσίμων εκτός του ότι μεταβάλλονται σε μικρή χρονική περίοδο είναι και διαφοροποιημένες από μια περιοχή σε άλλη. Είναι εξαιρετικά δύσκολο, επομένως, έως και απίθανο πολλές φορές, μια τέτοια εταιρία να μην κάνει χρήση καθορισμένων τακτικών και εφαρμογών ενημέρωσης με κυριότερο σκοπό να είναι πιο αποδοτική (Visvikis and Panayides, 2017).

Ένα εξίσου καθοριστικό δεδομένο το οποίο εστιάζει σε μεγάλο βαθμό στην αξία των συγκεκριμένων τεχνολογιών είναι το γεγονός πως οι σύγχρονες εταιρίες αποτελούν από μόνες τους ένα ολοκληρωμένο σύστημα. Στην περίπτωση των οργανισμών και των εταιριών αυτού του τομέα, σε περίπτωση που αφαιρέσουμε την απαίτηση για συντονισμό με τα σκάφη-εργοστάσια και εστιάσουμε στην επιχειρησιακή τους οργάνωση και σύσταση είναι εύκολο να αντιληφθούμε ότι τα επιμέρους τμήματα έχουν την απαίτηση για ενημέρωση, προκειμένου να δρουν σωστά καθώς το

περιβάλλον στο οποίο δραστηριοποιούνται είναι εξαιρετικά πολύπλοκο (Tapaninen and Andelin, 2020).

1.3 Πλεονεκτήματα και μειονεκτήματα χρήσης ΤΠΕ στη ναυτιλία

Στη σημερινή εποχή, με τον όρο ΤΠΕ καλούμε τις Τεχνολογίες Πληροφορικής και Επικοινωνιών. Τα κυριότερα οφέλη τα οποία παρέχουν τα μέσα αυτής της μορφής στον τομέα που μελετάμε σε αυτή την εργασία είναι η αμεσότερη πρόσβαση σε όλα τα δεδομένα, η αισθητή βελτίωση και το γεγονός πως έγιναν πιο άμεσες οι επικοινωνίες με προμηθευτές, συνεργάτες κλπ, ο περιορισμός του κόστους επικοινωνιών, η αισθητή ανοδική τάση της παραγωγικής δράσης, η πιο επαρκής εποπτεία και παρακολούθηση καθώς επίσης και η βελτίωση όλων των παρεχόμενων υπηρεσιών (Λιναρδάτος και Λιναρδάτος, 2016).

Καθοριστικά, όμως, λογίζονται πως είναι και τα οφέλη τα οποία υφίστανται από τη χρησιμότητα αυτών των εφαρμογών και σε επίπεδο εσωτερικής δράσης αυτών των επιχειρήσεων. Επομένως, μερικά από αυτά τα οφέλη είναι ο πιο κεντρικός έλεγχος δράσεων, η βελτίωση της εποπτείας των χρηστών, η ικανότητα υπολογισμού αλλά και αξιολόγησης των εργαζομένων σύμφωνα με την αποτελεσματικότητα, την παραγωγικότητα αλλά και τις δράσεις τους, η ικανότητα έκδοσης εκθέσεων και αναφορών συγκριτικά με όλες τις δράσεις οι οποίες υλοποιούνται στο εσωτερικό μιας τέτοιας επιχείρησης καθώς επίσης και η ανάπτυξη βάσεων δεδομένων σύμφωνα με καθορισμένες ημερομηνίες κλπ (Song and Panayides, 2012).

Ο κλάδος που μελετάμε σε αυτή την εργασία εξαιτίας των αλληλεπιδράσεων περιέχει ένα μεγάλο φάσμα διαφοροποιημένων σχέσεων των ενδιαφερόμενων μερών. Για παράδειγμα υφίστανται πλοιοκτήτες, ναυλωτές, κατασκευαστές, διεθνείς

οργανισμοί, λιμενικές αρχές, προμηθευτές κλπ, οι οποίοι είναι μερικοί από τους οποίους είναι σημαντική η παραπάνω αλληλεπίδραση, δίχως όμως να έχουν οριοθετηθεί ορισμένα πρότυπα σε ό,τι έχει να κάνει με την επικοινωνία ανάμεσά τους (Δημοβασίλη, 2018).

Επομένως, ο κάθε ένας εξ αυτών κάνει χρήση των δικών του εφαρμογών και εφαρμόζει τα δικά του μέσα και ικανότητες τις οποίες έχει στην ευχέρειά του με απώτερο στόχο την βέλτιστη εφικτή επικοινωνία είτε ακόμα και την ανταλλαγή χρήσιμων δεδομένων κλπ.. Η παροχή λογισμικού διαδραματίζει καθοριστικό ρόλο σε μια προσπάθεια, προκειμένου να δοθούν όλες οι απαιτούμενες απαντήσεις στα ζητήματα καθώς επίσης και να υπάρξει η απαιτούμενη αναβάθμιση σε όλες τις υπηρεσίες τους, που στόχο έχουν να παρέχουν ένα μεγαλύτερο επίπεδο συμβατότητας των εφαρμογών τους με τις υπόλοιπες υπηρεσίες, οι οποίες χρησιμεύουν και κυκλοφορούν στην εν λόγω αγορά (Νικητάκος, 2011).

Ορισμένα από τα οφέλη της συντήρησης της απλής δομής, χωρίς τη χρησιμοποίηση εφαρμογών και τεχνολογιών που θα εποπτεύουν όλες τις δράσεις του σκάφους είναι το χαμηλότερο κόστος δράσης, το γεγονός πως δεν διακρίνεται η απαίτηση για πολύπλοκο δικτυακό περιβάλλον, το γεγονός πως δεν υφίσταται απαίτηση για ειδικό ανθρώπινο δυναμικό ενώ εξίσου καθοριστικό όφελος είναι η χρησιμοποίηση απλών τεχνολογιών με στόχο τον έλεγχο της σωστής δράσης των σύγχρονων σκαφών (Κοκοτος και Λιναρδάτος, 2010).

Από την άλλη μεριά, υφίστανται και μερικά οφέλη τα οποία έχουν άρρηκτη σχέση με την εφαρμογή τακτικών επεξεργασίας σήματος. Παρόμοιας μορφής οφέλη είναι η απαλοιφή θορύβου και η αισθητή ανοδική τάση της αντοχής στα παράσιτα, η ανίχνευση αλλά και η απομόνωση ιδιαίτερων γνωρισμάτων σήματος, η σχέση σήματος με τράπεζα δεδομένων και η ένταξή του σε κατηγορία, η εκτέλεση με ψηφιακά φίλτρα τεράστιας ακρίβειας αυτόματου ελέγχου σκαφών, η βέλτιστη εφικτή διαχείριση αλλά

και η επεξεργασία των συγκεκριμένων δεδομένων και τέλος η αισθητή ελάττωση του κόστους εξοπλισμού (Song and Panayides, 2012).

Από την άλλη πλευρά, όμως, υφίστανται και σημαντικά ελαττώματα. Η κοινωνική ζωή σε ένα σκάφος και κυρίως σε εκείνα τα οποία υλοποιούν τεράστιας διάρκειας ταξίδια είναι ήδη τεταμένη. Το internet λαμβάνει καθοριστικό κομμάτι της μείωσης της κοινωνικότητας στη σημερινή εποχή. Μέσα από την ανάπτυξη των φορητών Η/Υ και των smartphones, ο χρόνος επικοινωνίας στους χώρους καπνίσματος του σκάφους κλπ γίνεται ολοένα και πιο λίγος, με βασικότερη συνέπεια να μειώνεται διαρκώς η κοινωνικότητα στο σκάφος (Λιναρδάτος και Λιναρδάτος, 2016).

Επίσης, πολλές φορές η πρόσβαση από το σκάφος είναι σημαντικό να εποπτεύεται εξαιτίας της υπερβολής χρήσης δεδομένων, τα οποία είναι αρκετά ακριβά. Ένα εξίσου σημαντικό πρόβλημα το οποίο υφίσταται από τη χρήση των συγκεκριμένων τεχνολογιών στο σκάφος έχει άμεση σχέση με τις ώρες ξεκούρασης, την απεριόριστη και ολοένα μεγαλύτερης διάρκειας πρόσβασης στο διαδίκτυο που αναπτύσσει υπερβολική χρήση.

Ως εξίσου καθοριστικό πρόβλημα λογίζεται το γεγονός πως με την αισθητή ανοδική τάση της ψηφιοποίησης του εξοπλισμού της γέφυρας, όπως συμβαίνει για παράδειγμα στην περίπτωση του συστήματος ECDIS, οι ναυτικές εκδόσεις κλπ, υφίσταται μια αισθητή ανοδική τάση της απαίτησης να επιτρέπεται η πρόσβαση στο internet στη γέφυρα για ενημερώσεις, λήψεις δεδομένων κλπ (Visvikis and Panayides, 2017).

Ο καπετάνιος είναι σημαντικό να το κάνει απολύτως κατανοητό στις πάγιες εντολές του πως θα πρέπει να υφίσταται η απαιτούμενη πειθαρχία στη γέφυρα ενώ είναι σημαντικό να απαγορεύεται η χρήση smartphones στη γέφυρα. Κάτι αντίστοιχο συμβαίνει και στην περίπτωση των μέσων κοινωνικής δικτύωσης που αποτελεί ένα εξίσου σοβαρό και αρνητικό ζήτημα (Tapaninen and Andelin, 2020).

Τέλος, δεν θα πρέπει να ξεχνάμε πως το σημαντικότερο ελάττωμα της χρήσης της τεχνολογίας είναι η κυβερνοασφάλεια, που μελετάμε στη συγκεκριμένη εργασία και θα μελετήσουμε στα επόμενα κεφάλαια. Παρόλα αυτά, όμως, τα οφέλη είναι περισσότερα σε σχέση με τα ελαττώματα. Για αυτό το λόγο θα πρέπει να υπάρξουν κατάλληλες οδηγίες και με αυτόν τον τρόπο τα παραπάνω ελαττώματα είναι εφικτό να μειωθούν ακόμα περισσότερο. Αυτό αποτελεί συνέπεια των ενεργειών του πληρώματος καθώς επίσης και της διοίκησης του σκάφους με απώτερο στόχο την εξασφάλιση πως αυτή η καθοριστική εξέλιξη της τεχνολογίας η οποία βοηθάει τον εν λόγω κλάδο χρησιμεύει με στόχο την ευημερία, την ασφάλεια αλλά και την αισθητή βελτίωση των συνθηκών του συγκεκριμένου κλάδου (Νικητάκος, 2011).

1.4 Ροή πληροφοριών και τεχνολογία στη ναυτιλία

Στην περίπτωση στην οποία θα υπήρχε η ευχέρεια ένας άνθρωπος να μπορούσε να δει τη μέθοδο δράσης μιας σύγχρονης εταιρίας αυτού του τομέα, θα έβλεπε ότι η ροή μηνυμάτων μεταξύ των διαφοροποιημένων τμημάτων είναι πραγματικά εξαιρετικά συχνή και έχει άμεση σχέση με την αποδοτικότητά της. Τα τμήματα έχουν διαρκή αλληλεπίδραση ανάμεσά τους και αυτό κατά κύριο λόγο προέρχεται από τον χαρακτήρα αυτών των εταιριών και των οργανισμών (Δημοβασίλη, 2018).

Μια τέτοια επιχείρηση εξαιτίας του ότι έχει σαν βασικό της γνώρισμα τον τεράστιο κίνδυνο, με απώτερο στόχο να δράσει η ίδια και τα σκάφη της κάτω από συνθήκες ασφάλειας, είναι ζωτικής σημασίας να υφίσταται διαρκής και ορθή ενημέρωση των γεγονότων υπό των οποίων διακυβεύεται η εξέλιξή της. Αρκετές είναι εκείνες οι περιπτώσεις στις οποίες έχει τύχει κατά την περίοδο μιας τηλεφωνικής κλήσης μεταξύ διαφορετικών τμημάτων της ίδιας εταιρίας, η γραμμή να μην είναι καθαρή είτε να υφίστανται παρεμβολές. Στη συγκεκριμένη περίσταση οι χρήστες,

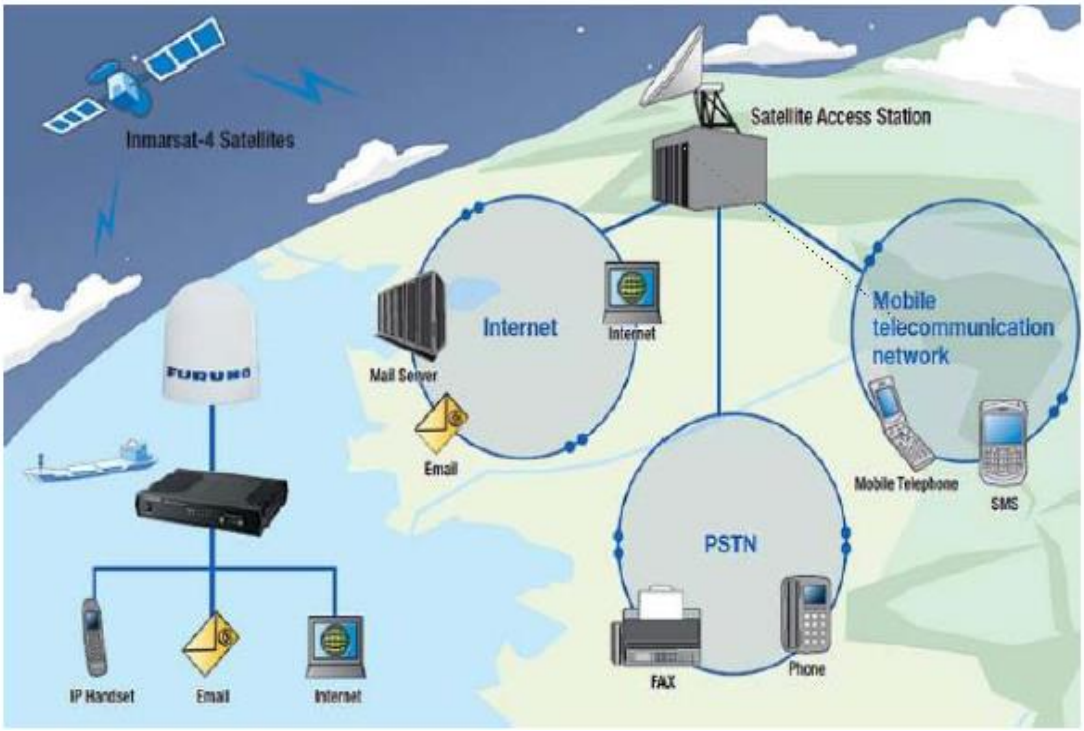
δεδομένου της σημασίας που μπορεί να έχει η εν λόγω επικοινωνία θα υποχρεωθούν να κάνουν χρήση διαφορετικών τακτικών, όπως ήταν για παράδειγμα η χρήση του φωνητικού αλφάβητου ΝΑΤΟ κλπ (Varun, 2019).

Εκτός, επομένως, από τα συστήματα τηλεφωνικών γραμμών και τη χρήση των μηνυμάτων από το ηλεκτρονικό ταχυδρομείο και γενικότερα τη χρήση του διαδικτύου, θα πρέπει να δρουν και να διαχειρίζονται τις ροές δεδομένων διαμέσου του τοπικού δικτύου. Πιο συγκεκριμένα ένα σύστημα client-server είναι ένα χρήσιμο σύστημα όπου το δίκτυο ενώνει τους διάφορους υπολογιστικούς πόρους, προκειμένου οι clients να έχουν τη δυνατότητα να ζητήσουν υπηρεσίες από έναν server, που παρέχει δεδομένα είτε επιπλέον υπολογιστική ισχύ (Λιναρδάτος και Λιναρδάτος, 2016).

Ο client, σε αυτές τις περιπτώσεις αποτελεί τον αιτών των συγκεκριμένων υπηρεσιών και η μόνη πιθανότητα είναι να είναι Η/Υ. Οι υπηρεσίες οι οποίες ζητούνται από το συγκεκριμένο σύστημα είναι εφικτό να υφίστανται στους ίδιους σταθμούς εργασίας είτε ακόμα και σε απομακρυσμένους σταθμούς αυτής της μορφής, οι οποίοι διασυνδέονται μεταξύ τους διαμέσου ενός δικτύου (Κοκοτος και Λιναρδάτος, 2010).

Ο συγκεκριμένος Η/Υ αρχίζει πάντοτε την επικοινωνία. Στην περίπτωση των επιχειρήσεων του εν λόγω κλάδου, αυτός ο Η/Υ αφορά όλους τους προσωπικούς Η/Υ. Ο server απαντάει στις αιτήσεις οι οποίες υλοποιούνται από τους παραπάνω Η/Υ. Ένας τέτοιος Η/Υ έχει τη δυνατότητα να δράσει σαν server στην περίπτωση στην οποία λαμβάνει και επεξεργάζεται αιτήσεις (Κοκοτος και συν., 2010).

Τα δίκτυα των συγκεκριμένων εταιριών εποπτεύονται από το λογισμικό λειτουργικών συστημάτων αλλά και διαχείρισης με απώτερο στόχο να παρακολουθούν τις υπηρεσίες επικοινωνίας του server και να προστατεύουν τα προγράμματα του client και του server από το να έχουν άμεση διασύνδεση μεταξύ τους. Ως επί το πλείστον το παραπάνω λογισμικό επικεντρώνεται στην παροχή κατάλληλων αλλά και αξιόπιστων υπηρεσιών, στην αισθητή μείωση των ζητημάτων δικτύου καθώς επίσης και στη μείωση των χρόνων πτώσης του δικτύου (Song and Panayides, 2012).



Εικόνα 1.1 : Δορυφορική επικοινωνία σκαφών (Κοκοτος και συν., 2010)

Κατά συνέπεια, σε μια τέτοια εταιρία έχοντας σαν βάση το παραπάνω δίκτυο, της προσφέρεται η ευχέρεια να εξελίξει πάνω σε αυτό μια εφαρμογή ανεπτυγμένη από εξειδικευμένους οργανισμούς, οι οποίοι σχεδιάζουν παρόμοιας μορφής εφαρμογές είτε από το δικό της τμήμα IT, προκειμένου να είναι δυνατή η αμεσότερη αλλά και ευκολότερη ανταλλαγή δεδομένων, με στόχο την υλοποίηση καθορισμένων δράσεων (Varun, 2019).

Οι συγκεκριμένες εφαρμογές, επομένως, έχουν διαφορετική βάση δεδομένων που είναι διασυνδεδεμένη με τον κεντρικό server, τον οποίο έχει στη διάθεσή της μιας τέτοια εταιρία. Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως τα πληροφοριακά συστήματα, τα οποία κυκλοφορούν στη σύγχρονη αγορά με στόχο να καταφέρουν να

καλύψουν πλήρως τις απαιτήσεις αυτών των εταιριών χωρίζονται σύμφωνα με το είδος χρήσης τους σε καθορισμένες κατηγορίες που είναι οι παρακάτω :

- Συστήματα ελέγχου κώδικα ISM και ISPS
- Συστήματα τηλεδιάσκεψης και εποπτείας είτε καταγραφής εμπορευμάτων
- Συστήματα ηλεκτρονικών προμηθειών και θαλάσσιων ηλεκτρονικών αγορών
- Συστήματα διαχείρισης πληρώματος, ταξιδιού και ναυλώσεων
- Συστήματα οικονομικής διαχείρισης (Visvikis and Panayides, 2017)

Στη σημερινή εποχή το βασικότερο μοντέλο ΠΣ το οποίο εφαρμόζεται στις εταιρίες αυτής της μορφής στη χώρα μας είναι το ERP. Εξαιτίας της ραγδαίας εξέλιξης της τεχνολογίας και κατά συνέπεια των απαιτήσεων αυτών των εταιριών, λογίζεται ως το καταλληλότερο είδος αυτών των συστημάτων διαμέσου του οποίου μια τέτοια εταιρία εποπτεύει όλες τις δράσεις της (Δημοβασίλη, 2018).

Τα συγκεκριμένα συστήματα αποτελούν ένα εξαιρετικά χρήσιμο μέσο το οποίο παίζει καθοριστικό ρόλο για αυτές τις εταιρίες, στην αποθήκευση όλων των πληροφοριών τους στο ίδιο δικτυακό περιβάλλον. Γενικότερα, η εφαρμογή αυτών των συστημάτων έχει επιφέρει τεράστιες μεταβολές σε αρκετούς και διαφορετικούς επιχειρηματικούς κλάδους. Οι επιρροές των συγκεκριμένων μεταβολών σε αυτές τις εταιρίες έχει άρρηκτη σχέση με την ποιότητα αυτών των συστημάτων αλλά και τη διάθεση των μελών της εταιρίας να το χρησιμοποιήσουν στο έπακρο προς όφελός τους (Tapaninen and Andelin, 2020).

1.5 Έξυπνη ναυτιλία

Στον τομέα που μελετάμε σε αυτή την εργασία έχουν εντοπιστεί ελάχιστες εξελίξεις τα τελευταία χρόνια συγκριτικά με τη μέθοδο ελλιμενισμού φόρτωσης και μεταφοράς εμπορευμάτων των σκαφών σε διαφορετικούς λιμένες σε παγκόσμιο επίπεδο. Αντίθετα, σε άλλους τομείς, η ύπαρξη ψηφιακής τεχνολογίας κατόρθωσε να επιφέρει σημαντική και ολοκληρωτική αλλαγή (Varun, 2019).

Βασικός στόχος του εν λόγω κλάδου στο παρελθόν ήταν η μεταφορά των ανθρώπων είτε ακόμα και των εμπορευμάτων. Παρά το γεγονός αυτό, όμως, η ραγδαία εξέλιξη της τεχνολογίας και των επιστημών μαζί με την αισθητή ανοδική τάση των απαιτήσεων για άμεση μεταφορά εμπορευμάτων έχουν επιφέρει την έξυπνη ναυτιλία (Visvikis and Panayides, 2017).

Κυριότερος σκοπός της ναυτιλίας αυτής της μορφής είναι οι πλήρως αυτοματοποιημένοι λιμένες καθώς επίσης και τα μη επανδρωμένα σκάφη αυτού του είδους, η πιο αξιόπιστη από ποτέ πρόγνωση καιρού σύμφωνα με τις περιοχές καθώς επίσης και η συγκέντρωση είτε η επεξεργασία των πληροφοριών των σκαφών στο υπολογιστικό νέφος.

Καθοριστικότερος σκοπός αυτής της ναυτιλίας αποτελεί η οριοθέτηση από την αρχή της μεθόδου με την οποία ενεργούν οι συγκεκριμένες επιχειρήσεις. Ταυτόχρονα, η εν λόγω μορφή ναυτιλίας παρέχει ένα γενικότερο φάσμα διαφοροποιημένων υπηρεσιών, όπως είναι για παράδειγμα οι δορυφορικές επικοινωνίες, ο έλεγχος μεταφοράς φορτίων, η πλοήγηση, η διαχείριση πληρωμάτων καθώς επίσης και η ενεργειακή αποδοτικότητα (Tapaninen and Andelin, 2020).

Παράλληλα, όμως δεν σταματάει να εστιάζει στο μέλλον ανακαλύπτοντας χωρίς σταματημό περισσότερες επιλογές σε ζητήματα, όπως είναι για παράδειγμα η

βέλτιστη εφικτή διαχείριση των big data καθώς επίσης και του αυτοματισμού είτε ακόμα και πιο κοινότυπων πλαισίων όπως είναι οι ΤΠΕ, που αναφέρθηκαν παραπάνω, κλπ (Δημοβασίλη, 2018).

Οι υπηρεσίες, που αναφέρθηκαν παραπάνω, όπως είναι για παράδειγμα οι δορυφορικές επικοινωνίες κλπ, αποτελούν τους κυριότερους κλάδους της διεθνούς ναυτιλίας που είναι εφικτό να εμφανίσουν τεράστια βελτίωση με τις καινοτόμες δράσεις και τεχνολογίες αυτού του τομέα, όπως φυσικά και το στοίχημα της ενεργειακής απόδοσης (Varun, 2019).

Τα τελευταία έτη σε εθνικό αλλά και σε διεθνές επίπεδο εντοπίζεται ο ενεργός ρόλος ενός συνεχώς αυξανόμενου συνόλου επιχειρήσεων από τον τομέα της Πληροφορικής, που έχουν φέρει στην επιφάνεια περισσότερες και καλύτερες επιλογές για τις προκλήσεις αυτού του κλάδου, διαδραματίζοντας καθοριστικό ρόλο με αυτόν τον τρόπο στη μετάδοση από τις κλασσικές τακτικές στο ψηφιακό μέλλον. Επομένως, η συγκεκριμένη μορφή αυτού του τομέα λογίζεται σε όλες τις περιπτώσεις ως εξαιρετικά χρήσιμη και παρά τη μεταβολή φιλοσοφίας την οποία χρειάζεται για αυτήν, θα επέλθουν καθοριστικές μεταβολές σε αυτή την αγορά προς τη συγκεκριμένη κατεύθυνση η οποία θα τείνει προς την έξυπνη δράση αυτού του τομέα (Tapaninen and Andelin, 2020).

Κεφάλαιο

2

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

2.1 Κυβερνοχώρος

Είναι ένα νέο σύμπαν, ένα παράλληλο σύμπαν δημιουργημένο και συντηρούμενο από ένα σύνολο υπολογιστών του κόσμου και τις γραμμές επικοινωνίας τους. Ένας κόσμος στον οποίο η παγκόσμια διακίνηση γνώσης, μυστικών, μετρήσεων, δεικτών, ψυχαγωγίας και εξωγήινων επιδράσεων παίρνει μορφή: εικόνες, ήχοι, παρουσίας απούσες στη γη ανθίζουν σε μια τεράστια ηλεκτρονική νύκτα.(Benedikt,1991, Cyberspace:First Steps)

Η αγγλική λέξη cyberspace που στα ελληνικά μεταφραζόταν ως Κυβερνοδιάστημα αρχικά παρέπεμπε σε άλλους τομείς αφού οι άνθρωποι το συνέδεαν με τα αστέρια τους πλανήτες κ.λ.π.. Για το λόγο αυτό χρησιμοποιήθηκε η λέξη "χώρος" αντί για την λέξη διάστημα ώστε να γίνεται πιο κατανοητό. Σαν κυβερνοχώρος νοείται ο χώρος που δημιουργείται χάρη στην Επιστήμη της Κυβερνητικής (της επικοινωνίας μεταξύ μηχανικών και ηλεκτρικών συσκευών). Ως σημείο αναφοράς σε αυτόν τον χώρο μπορεί να οριστεί μόνο ο άνθρωπος και οι ενέργειες που αυτός εκτελεί. Κυβερνοχώρος λοιπόν, θεωρείται το σύνολο των αποτυπωμένων ενεργειών του ανθρώπου σε μαγνητικό υλικό.

Στη σημερινή εποχή, τα όρια του κυβερνοχώρου διαρκώς αυξάνονται. Η εκτενής χρησιμοποίηση των προσωπικών Η/Υ, οι οποίοι συνδέονται στο internet καθώς επίσης και όλων των άλλων κυβερνητικών είτε επιχειρηματικών δικτύων, παίζουν σημαντικό ρόλο στην εν λόγω κατεύθυνση. Εξίσου σημαντικό ρόλο, όμως, διαδραματίζουν και τα smartphones (Αποστόλου, 2014).

Το γεγονός πως οι Η/Υ στη σημερινή εποχή γίνονται πιο σύνθετοι βοηθάει σε μεγάλο βαθμό στη διευκόλυνση των κυβερνοεπιθέσεων. Αρκετές εφαρμογές στη σύγχρονη εποχή αναβαθμίζονται και γράφουν από την αρχή δεδομένα στους Η/Υ των χρηστών ακόμα και δίχως την άδειά τους. Όσο τα συγκεκριμένα συστήματα αντικαθιστούν τη δουλειά αλλά και την ανθρώπινη κρίση, τόσο πιο ευάλωτοι θα γινόμαστε με το πέρασμα των ετών και την ραγδαία ανάπτυξη της τεχνολογίας (Castro, 2018).

Οι επιθέσεις αυτής της μορφής υφίστανται μονάχα λόγω του ότι τα συστήματα αυτού του είδους εμφανίζουν σοβαρά μειονεκτήματα. Όσο οι χώρες θα εστιάζουν στα δίκτυα Η/Υ για στρατιωτική και χρηματοοικονομική δύναμη και όσο τα εν λόγω δίκτυα είναι προσιτά από εξωτερικούς φορείς, τόσο μεγαλύτερος θα είναι και ο κίνδυνος (Singer and Friedman, 2014).

Οι κακόβουλοι χρήστες έχουν την ευχέρεια να υποκλέψουν δεδομένα και να τα αλλοιώσουν, με βασικότερη συνέπεια τόσο τα συστήματα όσο και οι άνθρωποι να καταλήγουν εν τέλει σε εσφαλμένα συμπεράσματα και να προβαίνουν σε εσφαλμένες αποφάσεις. Οι τρωτότητες αναπτύσσονται λόγω του ότι υφίστασαι τεράστιο κενό μεταξύ της θεωρίας και της πράξης (Καμπαρίδου, 2015).

Θεωρητικά, ένα τέτοιο σύστημα είναι ζωτικής σημασίας να κάνει μονάχα ότι θέλει ο κατασκευαστής είτε ο χρήστης του. Πρακτικά, όμως, κάνει οτιδήποτε του υπαγορεύει ένας κώδικας. Η απόσταση μεταξύ αυτών των δυο είναι τεράστια και αναπτύσσεται ολοένα και περισσότερο με το πέρασμα των ετών και την εξέλιξη της τεχνολογίας και του τομέα της πληροφορικής. Η μοναδική τακτική να υπάρξει μια

αισθητή βελτίωση σε αυτά τα σφάλματα είναι διαμέσου των κυβερνοεπιθέσεων οι οποίες εκθέτουν τα τρωτά σημεία (Holzsager, 2015).

Η διαρκής ανάπτυξη της συνεργασίας ανάμεσα στο διαδίκτυο και στους χρήστες του, οι οποίοι το χρησιμοποιούν με διαφορετικές ταυτότητες, για διαφορετικούς λόγους και διαφορετικές προθέσεις, έχει μια καθοριστική συνέπεια στο διεθνές περιβάλλον των απειλών καθώς επίσης και των επιθέσεων αυτής της μορφής. Η σύγχρονη ανοιχτή διεθνής ψηφιακή δομή η οποία διασυνδέει οντότητες, όπως είναι για παράδειγμα οι σημερινές εταιρίες, οι κυβερνήσεις, οι άνθρωποι κλπ, απειλούνται από επιθέσεις αυτού του είδους, οι οποίες τις περισσότερες φορές διαφοροποιούνται από απλές απειλές έως και εξαιρετικά σύνθετες επιθέσεις (Castro, 2018).

Παρά το γεγονός πως ο όρος του κυβερνοχώρου είναι ιδεατός και αμφιλεγόμενος, γενικότερα είναι δυνατόν να λογιστεί πως είναι ανάλογος με τον όρο του διαδικτύου. Η συγκεκριμένη έννοια είναι δυνατόν να λογιστεί σαν μια συλλογή ατομικών ηλεκτρονικών συστημάτων τα οποία έχουν συνδεθεί το ένα με το άλλο καθώς επίσης και με τον εξωτερικό κόσμο.

Αυτός ο όρος δεν είναι σαφώς οριοθετημένος αφού τις περισσότερες φορές συγχέεται με την έννοια του διαδικτύου. Τις περισσότερες φορές οριοθετείται σαν ο χώρος του περιβάλλοντος των δεδομένων που περιέχεται από αλληλεξαρτώμενα δίκτυα πληροφοριακών δομών, τα οποία κατά κύριο λόγο περιέχουν το διαδίκτυο, τα τηλεφωνικά δίκτυα, τα συστήματα Η/Υ κλπ (Moschovitis, 2018).

Η έννοια αυτή αποτελεί έναν όρο σημαντικών αντιθέσεων. Επί της ουσίας αφορά ένα περιβάλλον που μοιάζει με τα υπόλοιπα τοπία μαχών, όπως συμβαίνει για παράδειγμα στην ξηρά, στη θάλασσα κλπ. Παρά το γεγονός αυτό, όμως, αποτελεί ένα περιβάλλον το οποίο δεν εμφανίζει ομοιότητες με τους υπόλοιπους χώρους. Το συγκεκριμένο περιβάλλον χρειάζεται να εκτιμηθεί με τις δικές του προϋποθέσεις καθώς αποτελεί μια ανακάλυψη των ανθρώπων (Singer and Friedman, 2014).

Επί της ουσίας αφορά ένα εικονικό μέσο, πολύ λιγότερο απτό από τη γη, το νερό κλπ. Μια σημαντική τακτική προκειμένου να κατανοήσουμε καλύτερα αυτή την έννοια είτε την έννοια των επιθέσεων αυτής της μορφής, είναι η θεώρηση πως περιέχεται από 3 διαφοροποιημένα επίπεδα, που είναι το φυσικό, το συντακτικό το οποίο κινείται πάνω από το προηγούμενο και τέλος το σημασιολογικό που βρίσκεται στην κορυφή (Meeuwisse, 2018).

Το πρώτο εξ αυτών αποτελεί τη βάση καθώς εκεί υφίστανται όλα τα άλλα συστήματα. Αυτό το επίπεδο περιέχεται από διάφορα κουτιά αλλά και από καλώδια. Με την εξαφάνιση του συγκεκριμένου επιπέδου, εξαφανίζονται και όλα τα άλλα συστήματα. Είναι συνεπώς πιθανή η επίθεση σε ένα σύστημα αυτού του είδους με διάφορα κινητικά μέσα (Αποστόλου, 2014).

Σε ό,τι έχει να κάνει με το δεύτερο επίπεδο, θα πρέπει να σημειωθεί πως περιέχει διάφορες οδηγίες που οι προγραμματιστές και οι χρήστες δίνουν στη μάχη και στα πρωτόκολλα διαμέσου των οποίων έχουν την ευχέρεια να επικοινωνούν τα συστήματα το ένα με το άλλο. Στο εν λόγω επίπεδο κινούνται κατά κύριο λόγο οι κακόβουλοι χρήστες αφού ενεργούν με απώτερο στόχο να έχουν τη δική τους κυριότητα σε σχέση με τους προγραμματιστές και τους λοιπούς χρήστες (Castro, 2018).

Τέλος, υφίσταται το σημασιολογικό επίπεδο όπου περιέχονται χρήσιμα δεδομένα τα οποία υπάρχουν μέσα σε ένα τέτοιο σύστημα. Επί της ουσίας είναι δυνατόν να υλοποιηθεί μια επίθεση μονάχα στο συγκεκριμένο επίπεδο, τροφοδοτώντας το σύστημα με λάθος δεδομένα, όπως για παράδειγμα περιλαμβάνοντας επισυνάψεις με κακόβουλα προγράμματα (ιούς), αναπτύσσοντας υπερχειλίσεις φορτίου με την αποστολή επιπλέον bits είτε ακόμα και περιλαμβάνοντας κακόβουλο κώδικα σε ιστότοπους κλπ (Singer and Friedman, 2014).

2.2 Κυβερνοασφάλεια

Η συγκεκριμένη έννοια αποτελεί μια ευρέως χρησιμοποιούμενη ορολογία, ο όρος της οποίας πολλές φορές διαφοροποιείται. Βάσει μελετών, η ασφάλεια αυτής της μορφής συνεπάγεται την εξασφάλιση των δικτύων Η/Υ καθώς επίσης και των δεδομένων περιέχοντας τη μη νόμιμη εισχώρηση στο σύστημα αλλά και διάφορα κακόβουλα προβλήματα σε αυτό (Καμπαρίδου, 2015).

Η κυβερνοασφάλεια είναι η πρακτική της προστασίας συστημάτων, δικτύων και προγραμμάτων από ψηφιακές επιθέσεις. Αναμφίβολα, οι τεχνολογικές εξελίξεις ωθούν στην ταχύτατη εκτέλεση των διαδικασιών, δημιουργούν όμως και αδυναμίες και κινδύνους οι οποίοι είναι κρίσιμοι για τη οικονομία, τις πληροφορίες και όλους τους τομείς που επεκτείνονται. Η πορεία που χαρακτηρίζεται από την τεχνολογία συνεπάγεται τη διακοπή του κινδύνου στον κυβερνοχώρο και γενικά την ανάπτυξη πρακτικών διαχείρισης και λύσεων σε όλα τα επίπεδα. Το 2018, ένα μεγάλο ποσοστό (περίπου 58%) των εταιρειών στις ΗΠΑ και το Ηνωμένο Βασίλειο δήλωσαν ότι είχαν παραβιαστεί τα δεδομένα τους μέσω τρίτων παραγόντων αλλά μόνο το 35% των εταιρειών αυτό δήλωσε ότι κατέχει ένα πρόγραμμα διαχείρισης κινδύνων που δουλεύει αποτελεσματικά. Σύμφωνα με την Διεθνή Ένωση Τηλεπικοινωνιών (ITU - International Telecommunications Union) ορίζεται ως ασφάλεια στον κυβερνοχώρο το σύνολο των ενεργειών, πολιτικών, εννοιών ασφαλείας, κατευθυντήριων γραμμών, μεθόδων διαχείρισης κινδύνου, δράσεων, εκπαίδευσης, βέλτιστων πρακτικών, ασφαλίσεων και τεχνολογιών που θα μπορούν να χρησιμοποιηθούν για την προστασία των περιουσιακών στοιχείων, της οργάνωση και των χρηστών στο κυβερνο-περιβάλλον. Αυτά τα περιουσιακά στοιχεία είναι οι συνδεδεμένες υπολογιστικές συσκευές, οι χρήστες, οι υπηρεσίες, τα συστήματα επικοινωνίας και οι πληροφορίες στο σύνολό τους που μεταδίδονται ή αποθηκεύονται στο κυβερνο-περιβάλλον. (ITU, 2018).

Η ασφάλεια αυτού του είδους σαν οργανωτική δράση και σαν συλλογή πόρων, δράσεων είτε ακόμα και δομών, αποτελεί την βέλτιστη εφικτή προστασία του κυβερνοχώρου, που παρουσιάστηκε παραπάνω, καθώς επίσης και των συστημάτων τα οποία διασυνδέονται με αυτόν, προκειμένου να μην είναι εφικτή η μη νόμιμη πρόσβασή σε αυτά (Meeuwisse, 2018).

Η εν λόγω μορφή ασφάλειας είναι δυνατόν, παράλληλα, να λογιστεί και σαν μια συλλογή χρήσιμων μέσων, τακτικών, εννοιών είτε ακόμα και εξασφαλίσεων ασφαλείας, κατευθυντήριων οδηγιών, τακτικών διαχείρισης κινδύνων, δράσεων, κατάρτισης, ασφαλίσεων είτε ακόμα και εφαρμογών. Η συγκεκριμένη συλλογή είναι εφικτό να χρησιμεύσει με απώτερο στόχο την βέλτιστη εφικτή προστασία αυτού του χώρου, των εταιριών αλλά και των ίδιων των χρηστών (Singer and Friedman, 2014).

Έρευνες, επίσης, έχουν οριοθετήσει τη συγκεκριμένη ασφάλεια σαν μια τακτική, η οποία συμβάλλει στην εξασφάλιση της ασφάλειας σε αυτό το περιβάλλον από απειλές οι οποίες έχουν την ευχέρεια να πάρουν αρκετές και διαφορετικές μορφές, όπως είναι για παράδειγμα η κατασκοπεία είτε η απόκρυψη μυστικών δεδομένων από εθνικές είτε διεθνείς επιχειρήσεις κα οργανισμούς είτε ακόμα και κυβερνητικά ιδρύματα κλπ (Holzsager, 2015).

Τα τελευταία χρόνια μελέτες κάνουν λόγο πως δεν είναι μονάχα οι κυβερνήσεις οι οποίες είναι σημαντικό να είναι αρμόδιες για ζητήματα ασφαλείας αυτής της μορφής, αλλά το ίδιο αρμόδιοι είναι σημαντικό να είναι και οι άνθρωποι, οι επιχειρήσεις είτε ακόμα και τα ιδρύματα, σε ό,τι έχει να κάνει με τις τακτικές με τις οποίες χρησιμοποιούν αυτό το μέσο. Δεν θα πρέπει να ξεχνάμε, εξάλλου, πως οι σύγχρονες εταιρίες έχουν την ευχέρεια πλέον να ελέγξουν και να βρουν τα δικά τους ελαττώματα είτε τα κενά ασφαλείας, σε περίπτωση που οι διευθύνσεις ασφαλείας τους πληρούν τις κατάλληλες αρχές, δράσεις κα τακτικές (Αποστόλου, 2014).

Με βασικότερο στόχο να βρεθούν τα επίπεδα απειλών για τη βέλτιστη εφικτή ασφάλεια σε αυτό το περιβάλλον, είναι χρήσιμο να αντιληφθούμε πλήρως τι

συνεπάγεται η εν λόγω δράση. Οι άνθρωποι, τα έθνη αλλά και οι σύγχρονες εταιρίες κάθε είδους καλούνται να έρθουν αντιμέτωπες με τις ίδιες απειλές σε αυτό το περιβάλλον και είναι ζωτικής σημασίας να κατανοήσουν πως οι συγκεκριμένες απειλές εμφανίζουν σημαντική ανοδική τάση σε συχνότητα, ποπλυπλοκότητα και πλαίσιο εφαρμογής (Meeuwisse, 2018).

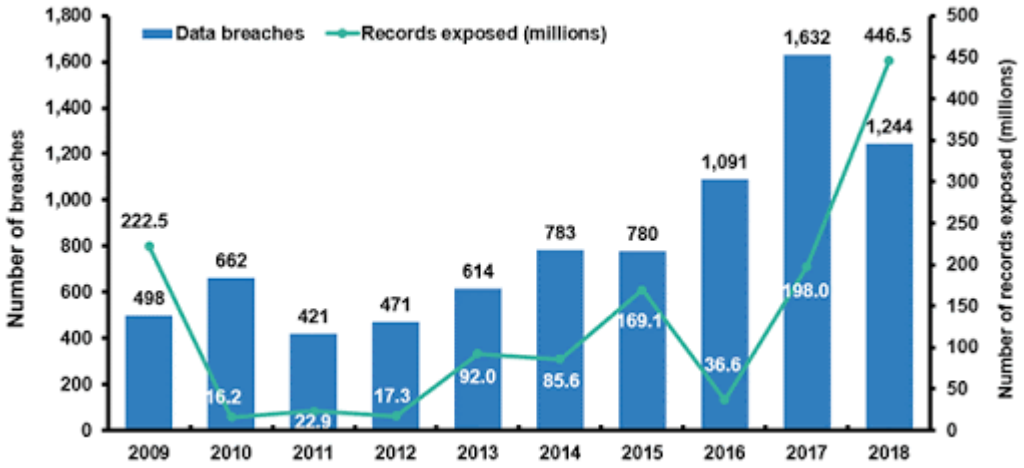
Οι ειδικοί χρήστες αυτού του μέσου δεν διστάζουν να κάνουν χρήση όλων των κατάλληλων τακτικών και εργαλείων με κυριότερο στόχο να κατορθώσουν σταδιακά να αποκτήσουν την απαιτούμενη πρόσβαση ακόμα και σε εξαιρετικά ευαίσθητα στοιχεία. Ένα χαρακτηριστικό παράδειγμα αποτελεί η διεθνής επίθεση ransomware της WannaCry, που είχε σαν βασικότερο σκοπό τους Η/Υ οι οποίοι δρούσαν με το λειτουργικό σύστημα των Windows.

Η επίθεση αυτή άρχισε στα μέσα της περιόδου του 2017 και επέφερε σημαντικές προβλήματα σε πιο πολλούς από 300 χιλιάδες Η/Υ σε 150 διαφορετικά κράτη σε ολόκληρο τον κόσμο. Μεταξύ αυτών ήταν και η Εθνική Υπηρεσία Υγείας της Μεγάλης Βρετανίας, η τηλεπικοινωνιακή εταιρεία Telefonica στην Ισπανία, ο σιδηροδρομικός φορέας της Γερμανίας κλπ (Castro, 2018).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως οι συγκεκριμένες απειλές έχουν την ευχέρεια να εκμεταλλευτούν την ανοδική τάση της πολυπλοκότητας αλλά και της συνδεσιμότητας των υποδομών που είναι σημαντικές, βάζοντας σε τεράστιο κίνδυνο την ασφάλεια, την οικονομία, τον τομέα της υγείας είτε ακόμα και τη δημόσια ασφάλεια ολόκληρων κρατών (Holzsager, 2015).

Οι κίνδυνοι για την ασφάλεια αυτής της μορφής είναι δυνατόν να επιφέρουν καθοριστικές επιρροές και επιδράσεις σε μια σύγχρονη εταιρία κάθε κλάδου, παίζοντας καθοριστικό ρόλο στην αισθητή ανοδική τάση του κόστους και επιφέροντας σημαντικές επιρροές στις εισροές τους. Έχουν τη δυνατότητα, ακόμα, να δημιουργήσουν τεράστια προβλήματα στην ικανότητα εξέλιξης της εταιρίας,

αναπτύσσοντας ζητήματα στη συντήρηση είτε ακόμα και στην προμήθεια των καταναλωτών κλπ (Καμπαρίδου, 2015).



Εικόνα 2.1 : Παραβιάσεις δεδομένων και αρχεία που εκτίθενται από την περίοδο του 2009 μέχρι και το 2018[1]

Όσο οι σύγχρονες εταιρίες αξιολογούν την ασφάλεια όλων των δράσεών τους καθώς επίσης και την πιθανότητα απειλών, κινδύνων, ελαττωμάτων, τρωτών σημείων κλπ, είναι ζωτικής σημασίας να απαντήσουν σε 3 σημαντικά ερωτήματα που είναι ποια είναι η απειλή που θα πρέπει να αντιμετωπίσουν, τι προσπαθούν να προστατέψουν αλλά και με ποιον τρόπο θα καταφέρουν να προστατευτούν (Καμπαρίδου, 2015).

Στη σημερινή εποχή, οι σύγχρονες εταιρίες είναι σημαντικό να λάβουν μια απόφαση για το τι είναι εκείνο το οποίο χρειάζεται να προστατευθεί αρχικά και πόσο αποδοτικά είναι εφικτό να δράσουν σε περίπτωση που δεν πετύχει το σχέδιο δράσης

[1] [https://www.proshred.com/minnesota/10-cyber-security-statistics/]

τους και τα συστήματα ασφαλείας που θα επιλέξουν να χρησιμοποιήσουν. Ακόμα, οι σύγχρονες εταιρίες είναι ζωτικής σημασίας να βρουν πιθανές απειλές διαμέσου ανάλυσης περιπτώσεων απειλών ίδιας μορφής (Αποστόλου, 2014).

Ακόμα, χρειάζεται να διερευνήσουν τα κατάλληλα μέτρα και τις δράσεις τις οποίες είναι σημαντικό να εφαρμόσουν όλες οι σύγχρονες εταιρίες, προκειμένου να κατορθώσουν να διασφαλίσουν την ασφάλεια ενός αντικειμένου από την παράμετρο που τους απειλεί. Σε μια έρευνα όπου οι εταιρίες πίστευαν ότι οι πιο μεγάλες απειλές τους ήταν το internet, εντοπίστηκε πως το πιο μεγάλο ζήτημα ήταν το phising, τα malwares αλλά και οι ιοί worms (Holzsager, 2015).

Από την πλευρά των σύγχρονων εταιριών, δεν δίνεται τεράστια βαρύτητα σε αυτές τις επιθέσεις που αφορούν το λογισμικό του διαδικτύου, στις στοχευμένες επιθέσεις, τα κακόβουλα προγράμματα τα οποία αφορούν τις κινητές συσκευές, στην αδράνεια των υπηρεσιών κλπ. Αυτός είναι και ο κυριότερος λόγος που τα τελευταία χρόνια διάφοροι οργανισμοί έχουν βρει επιθέσεις, οι οποίες εστιάζουν κατά κύριο λόγο σε ιστότοπους είτε εφαρμογές ιστού, κλοπές ταυτότητας, διάφορες επιθέσεις οι οποίες εκμεταλλεύονται διαρροές δεδομένων και προγράμματα τα οποία έχουν την ευχέρεια να καταστρέψουν είτε να σταματήσουν την εύρυθμη δράση των εταιριών (Meeuwisse, 2018).

2.3 Κύρια αντικείμενα της κυβερνοασφάλειας

Με απώτερο στόχο να βρεθούν τα επίπεδα απειλών που έχουν άμεση σχέση με την ασφάλεια του κυβερνοχώρου είναι χρήσιμο να αντιληφθούμε τι συνέπειες έχει η εν λόγω δράση. Οι άνθρωποι, τα έθνη αλλά και οι οργανισμοί καλούνται να αντιμετωπίσουν παρόμοιες απειλές σε αυτό το περιβάλλον και είναι σημαντικό να κατανοήσουν πως οι παραπάνω απειλές παρουσιάζουν αισθητή ανοδική τάση σε

συχνότητα, πολυπλοκότητα καθώς επίσης και στο πλαίσιο δράσης τους (George, 2020).

Οι ειδικοί χρήστες του internet δεν διστάζουν να κάνουν χρήση όλων των κατάλληλων εργαλείων με κυριότερο σκοπό να κατορθώσουν να αποκτήσουν πρόσβαση ακόμα και σε ευαίσθητα δεδομένα. Ένα χαρακτηριστικό παράδειγμα αποτελεί η διεθνής επίθεση ransomware της WannaCry, που είχε σαν στόχο τους Η/Υ οι οποίοι δρούσαν με το λειτουργικό σύστημα των Windows. Η επίθεση άρχισε στα μέσα της περιόδου του 2017 και ήταν εξαιρετικά επιβλαβής σε πιο πολλούς από 300 χιλιάδες Η/Υ σε 150 διαφορετικά κράτη (Moschovitis, 2018).

Οι απειλές στο συγκεκριμένο περιβάλλον εκμεταλλεύονται την ανοδική τάση της πολυπλοκότητας αλλά και της συνδεσιμότητας των καθοριστικών υποδομών, βάζοντας σε τεράστιο κίνδυνο την ασφάλεια, την οικονομία, την υγεία αλλά και τη δημόσια ασφάλεια ολόκληρων κρατών. Οι κίνδυνοι που έχουν άρρηκτη σχέση με την ασφάλεια αυτού του είδους είναι εφικτό να επιφέρουν καθοριστικές επιρροές και επιδράσεις σε μια σύγχρονη εταιρία, παίζοντας σημαντικό ρόλο στην ανοδική τάση του κόστους και επηρεάζοντας σε μεγάλο βαθμό τις εισροές της (Castro, 2018).

Είναι δυνατόν, ακόμα, να δημιουργήσουν τεράστια προβλήματα σε ό,τι έχει να κάνει με την ευχέρεια ανάπτυξης της επιχείρησης, αναπτύσσοντας παράλληλα τεράστια ζητήματα σε ό,τι έχει να κάνει με τη συντήρηση είτε ακόμα και την προμήθεια των καταναλωτών. Όσο οι οργανώσεις αξιολογούν την ασφάλεια των δράσεών τους καθώς επίσης και την πιθανότητα απειλών, κινδύνων κλπ, χρειάζεται να απαντήσουν σε καθορισμένα ζητήματα, όπως ποια είναι η απειλή, τι προστατεύουν, πως θα προστατευτούν κλπ (Meeuwisse, 2018).

Οι σύγχρονες εταιρίες είναι σημαντικό να λάβουν τις απαντήσεις στα παραπάνω ερωτήματα. Ακόμα, οι εταιρίες είναι χρήσιμο να βρουν πιθανές απειλές διαμέσου ανάλυσης ίδιων περιπτώσεων. Παράλληλα, χρειάζεται να διερευνήσουν διεξοδικά τα μέτρα είτε ακόμα και τις δράσεις που θα πρέπει να εφαρμόσουν οι εταιρίες

με απώτερο στόχο να καταφέρουν να διασφαλίσουν στο βέλτιστο εφικτό επίπεδο την ασφάλεια ενός αντικειμένου από την παράμετρο που τους απειλεί (George, 2020).

Σε έρευνες που έχουν υλοποιηθεί τα τελευταία χρόνια έχει αποδειχτεί πως αρκετές εταιρίες πιστεύουν πως οι πιο μεγάλες απειλές του διαδικτύου είναι το phising, τα malwares κλπ. Από την πλευρά των εταιριών, υφίσταται λιγότερη εστίαση στις κυβερνοεπιθέσεις στο λογισμικό του διαδικτύου, στις στοχευμένες επιθέσεις, τους ιούς οι οποίοι έχουν να κάνουν με τα κινητά, στην αδράνεια των υπηρεσιών κλπ. Οι ίδιες έρευνες κάνουν λόγο πως στη σημερινή εποχή υφίστανται επιθέσεις, οι οποίες εστιάζουν σε ιστότοπους είτε εφαρμογές ιστού, κλοπές ταυτότητας, επιθέσεις οι οποίες έχουν την ευχέρεια να εκμεταλλευτούν διαρροές δεδομένων και προγράμματα (Singer and Friedman, 2014).

2.4 Απειλές και κίνδυνοι

Στη σημερινή εποχή υφίστανται αρκετές και διαφορετικές ταξινομήσεις των συγκεκριμένων επιθέσεων σύμφωνα με τις κατάλληλες προϋποθέσεις. Πρώτα από όλα, σύμφωνα με το χώρο διακρίνονται σε εξωτερικές και εσωτερικές. Οι πρώτες εξ αυτών πραγματοποιούνται από μέσα τα οποία υφίστανται εξωτερικά του δικτύου. Αντίθετα, οι δεύτερες εξ αυτών υλοποιούνται από έναν χρήστη ο οποίος είναι μέσα στο δίκτυο και ενεργεί με βασικότερο στόχο να καταφέρει να αποπροσανατολίσει τους διαχειριστές είτε να εντάξει λανθασμένο κώδικα σε ένα δίκτυο, προκειμένου να δημιουργήσει αργή αλλοίωσή του (Castro, 2018).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως οι επιθέσεις αυτής της μορφής τις περισσότερες φορές εξαπολύονται εξωτερικά του δικτύου από χάκερς είτε εσωτερικές από διάφορους πράκτορες. Από τις παραπάνω κατηγορίες, η πρώτη ως επί το πλείστον έχει να κάνει με καθορισμένους σκοπούς που είναι πολίτες, ενώ η δεύτερη αφορά κυρίως στρατιωτικές επιστασίες είτε υπηρεσίες χρήσιμων δεδομένων κλπ. Σύμφωνα με την προέλευσή τους ταξινομούνται στα εξής :

- Φυσικές είτε αναπόφευκτες επιθέσεις, οι οποίες κατά κύριο λόγο περιέχουν διάφορα ατυχήματα τα οποία αναπτύσσονται από φυσικές καταστροφές (όπως είναι για παράδειγμα φωτιά, πλημμύρες, σεισμοί κλπ) που τις περισσότερες φορές συμβαίνουν άμεσα και δίχως καμία απολύτως προειδοποίηση και επιφέρουν τεράστια προβλήματα
- Ανθρώπινα σφάλματα και παραλείψεις (όπως για παράδειγμα ανθρώπινες ενέργειες δίχως να υφίσταται δόλος)
- Εσκεμμένες απειλές (όπως είναι για παράδειγμα παράνομες είτε εγκληματικές ενέργειες) από εξωτερικούς είτε ακόμα και εσωτερικούς χρήστες (Visvikis and Panayides, 2017)

Από την άλλη μεριά, σε ό,τι έχει να κάνει με τους κινδύνους, είναι σημαντικό να τονιστεί πως περιέχονται στους λειτουργικούς κινδύνους όπου εκτίθενται οι σύγχρονες εταιρίες αλλά και οι οργανισμοί. Ειδικότερα, οι κίνδυνοι αυτής της μορφής έχουν να κάνουν με την πιθανή ζημιά, η οποία είναι εφικτό να αναπτυχθεί από μη εξουσιοδοτημένη χρήση, αποκάλυψη, διακοπή, αλλαγή είτε ακόμα και καταστροφή δεδομένων (George, 2020).

Οι κίνδυνοι αυτού του είδους οριοθετούνται σαν οι λειτουργικοί κίνδυνοι των δεδομένων είτε ακόμα και των τεχνολογικών περιουσιακών στοιχείων, που κατ' επέκταση επιφέρουν καθοριστικές επιρροές και επιδράσεις σε διάφορους τομείς, όπως είναι για παράδειγμα η εμπιστευτικότητα, η διαθεσιμότητα είτε ακόμα και η ακεραιότητα των δεδομένων. Έρευνες αναφέρουν πως οι κυριότερες πηγές κινδύνων αυτής της μορφής ταξινομούνται σε 4 επίπεδα που είναι οι ανθρώπινες δράσεις, οι αποτυχίες συστημάτων και τεχνολογιών, οι αποτυχημένες εσωτερικές δράσεις καθώς επίσης και οι εξωτερικές συνθήκες (Αποστόλου, 2014).

Σε αυτό το σημείο είναι χρήσιμο να επισημανθεί πως για την περίοδο του 2018, σαν τη βασικότερη πηγή κινδύνων αυτής της μορφής στην ΕΕ ήταν οι κακόβουλες και εγκληματικές ενέργειες (ανήκουν στις εσκεμμένες ανθρώπινες δράσεις) και αφορούσαν σχεδόν το 40% παρουσιάζοντας μια σημαντική ανοδική τάση συγκριτικά με την περίοδο του 2017 (7%) και τα λάθη συστήματος που αφορούσαν το 39% παρουσιάζοντας αισθητή ανοδική τάση από το 36% που ήταν κατά την περίοδο του 2017. Αντίθετα, τα ακούσια ανθρώπινα σφάλματα αφορούσαν ποσοστό λίγο μεγαλύτερο από το 10% ενώ το υπόλοιπο ποσοστό αφορούσε τις αποτυχίες άλλων μελών (George, 2020).

2.5 Βέλτιστες πρακτικές κυβερνοασφάλειας

Η σημερινή εποχή έχει ανάγκη από έναν καλό σχεδιασμό αλλά και την εφαρμογή ολιστικής πολιτικής κυβερνοασφάλειας με απώτερο στόχο την αποδοτική διαχείριση των διαρκών αυξανόμενων κινδύνων αυτής της μορφής διαμέσου της εφαρμογής σωστών οργανωτικών καθώς επίσης και τεχνολογικών μέτρων προστασίας. Σε περίπτωση σημαντικού περιστατικού μιας τέτοιας επίθεσης υφίσταται ο κίνδυνος διαταραχής της σωστής δράσης και της βιωσιμότητας των εταιριών (Holzsager, 2015).

Αυτός είναι και ο κυριότερος λόγος που λογίζεται ως καθοριστικό οι σύγχρονες εταιρίες να ανταποκριθούν στις σύγχρονες συνθήκες και να αναπτυχθούν διαμέσου αυτών. Στο συγκεκριμένο πλαίσιο, παγκόσμιες εταιρίες έχουν δημιουργήσει καθορισμένες τακτικές με κυριότερο στόχο να μπορέσουν να βοηθήσουν τις εταιρίες στην παραπάνω προσπάθεια. Χαρακτηριστικά παραδείγματα παρόμοιων τακτικών είναι το Cybersecurity Best Practices, το Special Publication SP 800-53 αλλά και διάφορες άλλες δημοσιεύσεις που αφορούν την ENISA (George, 2020).

Οι σύγχρονες εταιρίες είναι σημαντικό να υλοποιήσουν μια ολιστική προσέγγιση εστιάζοντας κατά βάση στις επιχειρησιακές τους απαιτήσεις καθώς επίσης

και τις απειλές οι οποίες υφίστανται στο περιβάλλον δράσης τους, με κυριότερο στόχο τη βέλτιστη εφικτή διαχείριση των κινδύνων, οι οποίοι έχουν άρρηκτη σχέση με ζητήματα κυβερνοασφάλειας (Καμπαρίδου, 2015).

Όσο η ασφάλεια των παραπάνω δράσεων μιας σύγχρονης εταιρίας λογίζεται ως ζωτικής σημασίας, οι όροι της προστασίας, της επίγνωσης αλλά και της ανθεκτικότητας συγκριτικά με αυτές τις επιθέσεις αποτελούν καθοριστική απαίτηση για μια σύγχρονη εταιρία. Οι κίνδυνοι σε ό,τι έχει να κάνει με την ασφάλεια αυτής της μορφής, που απασχολούν αυτές τις εταιρίες από παλαιότερα, εξακολουθούν μέχρι και σήμερα να παραμένουν στο προσκήνιο (George, 2020).

Ο βαθμός ετοιμότητας μιας σύγχρονης εταιρίας σε σχέση με αυτές τις επιθέσεις είναι εξαιρετικά πιθανό να μειωθεί, εξαιτίας των ελαττωμένων ικανοτήτων του τμήματος πληροφορικής, της μη κατάλληλης ενημέρωσης του λογισμικού είτε της έλλειψης ειδικού ανθρώπινου δυναμικού για την ασφάλεια αυτής της μορφής, με βασικότερη συνέπεια να υφίσταται αισθητή ανοδική τάση της σοβαρότητας αυτών των επιθέσεων (Moschovitis, 2018).

Μερικές χρήσιμες τακτικές είναι το ΔΣ να εστιάσει στην επιμέλεια, στην υπευθυνότητα αλλά και στην αποδοτικότητα της διαχείρισης αυτής της ασφάλειας, η εταιρία θα πρέπει να αναπτύξει τη θέση του επικεφαλή ασφάλειας δεδομένων που θα έχει ενεργό ρόλο σε όλες τις εκτελεστικές επιτροπές και θα μπορεί να στελεχώσει το συγκεκριμένο τμήμα όπως κρίνει σωστό, η διοίκηση είναι ζωτικής σημασία σαν προάγει τη φιλοσοφία της εν λόγω ασφάλειας διαμέσου της εφαρμογής διάφορων προγραμμάτων κατάρτισης του ανθρώπινου δυναμικού, η εταιρία θα πρέπει να αναπτύξει ένα σωστό πλαίσιο κλιμάκωσης με στόχο τη βέλτιστη εφικτή διαχείριση των συγκεκριμένων κινδύνων ενώ τέλος η εκτελεστική διοίκηση χρειάζεται να έχει ενεργό ρόλο στην αξιολόγηση των προγραμμάτων ασφαλείας (George, 2020).

Κεφάλαιο

3

ΝΑΥΤΙΛΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

3.1 Η ναυτιλία σαν στόχος επιθέσεων

Ο συγκεκριμένος κλάδος περιέχεται στον τομέα των μεταφορών, που με τη σειρά του εντάσσεται στις σημαντικές υποδομές ενός κράτους. Οι εταιρίες οι οποίες εντάσσονται στον παραπάνω τομέα αποτελούν τους δεύτερους πιο συχνούς στόχους των επιθέσεων που μελετάμε σε αυτή την εργασία μετά από τις εταιρίες του οικονομικού τομέα, παρουσιάζοντας ένα ποσοστό της τάξης του 13% (Καβαλλιεράτος, 2018).

Ο λόγος που η βιομηχανία των μεταφορών αποτελούν έναν από τους βασικότερους στόχους, που προσελκύει τις κακόβουλες επιθέσεις είναι το γεγονός πως ως τομέας έχει άμεση σχέση από την τεχνολογία των δεδομένων, έτσι ώστε να βελτιστοποιήσει τις δράσεις της, να μπορέσει να εμφανίσει αισθητή ανοδική τάση της παραγωγικής δράσης, να παραμείνει το ίδιο ανταγωνιστική, να ελαττώσει σε μεγάλο

βαθμό το κόστος και τέλος να μπορέσει να βελτιώσει σε σημαντικό επίπεδο τη διαχείριση των φορτίων (Varun, 2019).

Με αυτόν τον τρόπο, επομένως, και ο τομέας που μελετάμε στη συγκεκριμένη εργασία εστιάζει σε σημαντικό επίπεδο σε ένα μεγάλο σύνολο διαφοροποιημένων τεχνολογικών συστημάτων, όπως είναι για παράδειγμα ειδικά συστήματα επικοινωνίας τα οποία ως επί το πλείστον χρησιμεύουν στην πλοήγηση, συστήματα ανταλλαγής δεδομένων από σκάφος σε σκάφος είτε μεταξύ σκάφους και στεριάς, διάφορα συστήματα διαχείρισης και σχεδιασμού των φορτίων είτε ακόμα και διάφορα συστήματα ψυχαγωγίας, ασφάλειας των επιβατών κλπ (Visvikis and Panayides, 2017).

Τα πιο πολλά εξ αυτών των συστημάτων, όμως, αναπτύχθηκαν δίχως να εστιάζουν στην ολοένα και πιο συχνή παρουσία περιπτώσεων κυβερνοεπιθέσεων. Επιθέσεις οι οποίες είναι δυνατόν να επιφέρουν καθοριστικές επιπτώσεις, όπως είναι για παράδειγμα η απώλεια ανθρώπινων ζωών, οι τραυματισμοί, η ρύπανση των θαλασσών, η αναχαίτιση των δράσεων των εταιριών αλλά και σε αρκετές περιπτώσεις η ανεπανόρθωτη βλάβη στη φήμη της εκάστοτε εταιρίας (American Bureau of Shipping, 2018).

Δεν χωράει καμία απολύτως αμφιβολία πως η ανοδική τάση της χρήσης της τεχνολογίας σε αυτόν τον τομέα αναμένεται να είναι ευεργετική τόσο σε ό,τι έχει να κάνει με την ανάπτυξη όσο και σε ό,τι αφορά την ασφάλεια. Τα συγκεκριμένα συστήματα διακρίνεται να είναι εξαιρετικά σημαντικά παίζοντας καθοριστικό ρόλο για παράδειγμα στην αποφυγή προσθαλασσώσεων, συγκρούσεων κλπ (Tapaninen and Andelin, 2020).

Παρά το γεγονός αυτό, όμως, η τεχνολογία μπορεί να επιφέρει και σοβαρούς κινδύνους, όπως αυτοί που αναλύθηκαν στο προηγούμενο κεφάλαιο. Οι εν λόγω κίνδυνοι αποτελούν έναν τεράστιο προβληματισμό για αυτόν τον τομέα, δεδομένου πως ολοένα και πιο πολλά συστήματα έχουν ανάγκη από συνδεσιμότητα με την ακτή,

έτσι και τα πλοία γίνονται ολοένα και πιο ευάλωτα σε επιθέσεις αυτής της μορφής (Polemi, 2017).

Σύμφωνα με έρευνες των τελευταίων ετών, οι επιθέσεις αυτής της μορφής και οι υποκλοπές δεδομένων περιέχονται στα πιο σημαντικά θέματα τα οποία είναι ζωτικής σημασίας να αντιμετωπιστούν άμεσα. Οι μελέτες αυτές τοποθετούν τις εν λόγω επιθέσεις σαν το 3ο κατά σειρά πρόβλημα το οποίο σε περίπτωση που υπάρξει έχει την ευχέρεια να επιφέρει μεγάλες επιπτώσεις στο θαλάσσιο εμπόριο, μετά την παγκόσμια χρηματοοικονομική ύφεση και τη διακύμανση των τιμών της ενέργειας (Dadiani, 2018).

Τεράστιο ενδιαφέρον, όμως, έχουν και διάφορα συμπεράσματα από άλλες έρευνες που αφορούν τον συγκεκριμένο τομέα στην Αμερική. Οι έρευνες αυτές τονίζουν πως ένα ποσοστό της τάξης του 70% πιστεύει πως η βιομηχανία αυτή είναι μερικώς είτε καλά προετοιμασμένη να αντιμετωπίσει περιπτώσεις τέτοιων επιθέσεων. Από αυτό το ποσοστό σχεδόν το 35% πιστεύει πως είναι σε ετοιμότητα να αντιμετωπίσει μια παρόμοια περίπτωση σε ό,τι έχει να κάνει με τη δική τους εταιρία (Kessler, 2020).

3.2 Κυβερνοασφάλεια στη ναυτιλία

Την ώρα που η πληροφορική περιέχει διάφορα συστήματα μηχανογράφησης και λογισμικά σε γραφεία, λιμένες κλπ, η επιχειρησιακή τεχνολογία έχει εφαρμογές στην εποπτεία των επιχειρησιακών συστημάτων, όπως είναι για παράδειγμα η εποπτεία μηχανών, η διαχείριση φορτίου, συστημάτων πλοήγησης κλπ. Στις σύγχρονες εταιρίες αυτού του τομέα υφίστανται τεχνολογίες και συστήματα που είναι ενσωματωμένα σε συστήματα γέφυρας, σε δορυφορικές επικοινωνίες, σε αυτόματα συστήματα αναγνώρισης, σε ραντάρ κλπ (Καβαλλιεράτος, 2018).

Την ώρα που οι παραπάνω τεχνολογίες αλλά και τα συστήματα συμβάλλουν σημαντικά στην επίτευξη της βέλτιστης εφικτής αποδοτικότητας για τον εν λόγω τομέα, την ίδια ώρα είναι εξαιρετικά ευάλωτα στις επιθέσεις που μελετάμε σε αυτή την εργασία, καθώς προσφέρουν χρήσιμα δεδομένα που έχουν να κάνουν με το στίγμα, την πορεία, την ταχύτητα του σκάφους, το φορτίο κλπ (American Bureau of Shipping, 2018).

Με βασικότερο στόχο να αντιμετωπιστούν αποδοτικά οι παραπάνω απειλές σε αυτό το περιβάλλον, είναι ζωτικής σημασίας να υπάρξει η απαιτούμενη εστίαση στα εξής :

- Τα συστήματα ΟΤ θα πρέπει να εποπτεύουν το φυσικό περιβάλλον του σκάφος
- Τα συστήματα ΟΤ είναι αρμόδια για την απόδοση σε πραγματικό χρόνο
- Η πρόσβαση σε αυτά τα συστήματα χρειάζεται να εποπτεύεται αυστηρά δίχως να σταματάει η απαιτούμενη αλληλεπίδραση ανθρώπων και μηχανών (Roberts et al., 2017)
- Η ασφάλεια των συγκεκριμένων συστημάτων είναι ζωτικής σημασίας και είναι χρήσιμη η εποπτεία των λαθών
- Έχουν τεράστιο κύκλο και πιθανές ενημερώσεις χρειάζεται να γίνονται με τεράστια προσοχή με στόχο να αποφευχθεί η ελάττωση της αξιόπιστης δράσης τους
- Τα συστήματα αυτής της μορφής έχουν αναπτυχθεί με κυριότερο στόχο να υποστηρίζουν την προβλεπόμενη επιχειρησιακή δράση και είναι πιθανόν να μην έχουν μεγάλη μνήμη είτε υπολογιστικούς πόρους με στόχο να υποστηρίξουν ικανότητες ασφάλειας

- Η απώλεια εποπτείας της δράσης αυτών των συστημάτων είναι δυνατόν να αποτελέσει καθοριστικό κίνδυνο για την ασφάλεια του σκάφους, του πληρώματος αλλά και του φορτίου, ενώ υφίσταται η δυνατότητα να επιφέρει τεράστια προβλήματα στο θαλάσσιο περιβάλλον (Λιναρδάτος και Λιναρδάτος, 2016)

Γενικότερα, το εν λόγω ζήτημα σε αυτόν τον τομέα έχει απασχολήσει και έχει αναπτύξει τεράστιους προβληματισμούς σε όλες τις σύγχρονες επιχειρήσεις αυτού του κλάδου. Η διαρκής εξέλιξη της τεχνολογίας έχει παίξει καθοριστικό ρόλο και πλέον αποτελεί την πιο καθοριστική παράμετρο σε ό,τι έχει να κάνει με ζητήματα ασφαλείας σε αυτόν τον τομέα (George, 2020).

Επί της ουσίας πρόκειται για μια ιδιαίτερη περίπτωση, και αυτό οφείλεται στο γεγονός πως δεν φτάνει μονάχα να υφίσταται κυβερνοασφάλεια στο γραφείο, αλλά και στα σκάφη της εκάστοτε επιχείρησης καθώς σε όλες τις περιπτώσεις αυτά θα πρέπει να επικοινωνούν μεταξύ τους. Στην περίπτωση της ασφάλειας αυτής της μορφής στον συγκεκριμένο τομέα και δεδομένου πως η εν λόγω βιομηχανία γίνεται ολοένα και πιο μηχανογραφημένη, αρκετές έρευνες τα τελευταία χρόνια έχουν εστιάσει στον έλεγχο, στην κλοπή αλλά και στη βύθιση σκαφών (American Bureau of Shipping, 2018).

Αυτά κατά κύριο λόγο προέρχονται από έλλειψη διαχωρισμού δικτύων στην πλειονότητα των σκαφών, στο ότι το σύστημα ECDIS είναι εξαιρετικά ευάλωτο στις επιθέσεις των κακόβουλων χρηστών καθώς επίσης και στο γεγονός πως οι περισσότεροι ιδιοκτήτων των πλοίων είτε ακόμα και οι φορείς εκμετάλλευσης είναι ζωτικής σημασίας να αντιμετωπίσουν άμεσα παρόμοια προβλήματα (Tapaninen and Andelin, 2020).

Οι παραπάνω καταστάσεις είναι δυνατόν να αποτελούν συνέπεια από εσκεμμένες κακόβουλες πρακτικές, ακούσια επίθεση κακόβουλων χρηστών είτε ακόμα

και από λάθος κάποιου χρήστη ενός συστήματος. Είναι σημαντικό, επομένως, να υφίστανται 2 διαφοροποιημένα επίπεδα ασφαλείας, ένα σε επιχειρησιακό επίπεδο γραφείου σκάφους και ένα που να έχει να κάνει με τους εξωτερικούς κινδύνους σε ό,τι έχει να κάνει με τη δορυφορική πλοήγηση, τις λιμενικές εγκαταστάσεις κλπ (Kessler, 2020).

Στην ΕΕ υφίσταται ασφάλεια δικτύων αλλά και συστημάτων πληροφοριών από τα μέσα της περιόδου του 2016, διαμέσου της οδηγίας EU 2016/1148. Το συγκεκριμένο νομοθετικό πλαίσιο είχε εφαρμοστεί στους λιμένες και όχι στα σκάφη. Ο κανονισμός γενικής προστασίας δεδομένων (GDPR) βρίσκεται σε εφαρμογή από τα μέσα της περιόδου του 2018 (διαμέσου της οδηγίας EU 2016/679) (Roberts et al., 2017).

Είναι εφικτό, επομένως, να υπάρξει το ερώτημα, τι επηρεάζει τη συγκεκριμένη μορφή ασφαλείας. Πρώτα από όλα θα πρέπει να υλοποιηθεί διαχωρισμός των συστημάτων σε συστήματα OT, που εποπτεύουν το φυσικό κόσμο και σε συστήματα πληροφορικής IT που έχουν την ευχέρεια της διαχείρισης πληροφοριών. Τα πρώτα εξ αυτών διαφοροποιούνται από τα δεύτερα καθώς αφορούν το υλικό και το λογισμικό που άμεσα εποπτεύει φυσικές συσκευές και δράσεις. Από την άλλη πλευρά, τα δεύτερα εξ αυτών έχουν τη δυνατότητα να καλύψουν ένα μεγάλο φάσμα διαφοροποιημένων τεχνολογιών υλικού αλλά και επικοινωνιών (McNicholas, 2016).

Επίσης, είναι χρήσιμο να γνωρίζουμε πως με τη διακοπή της δράσης των πρώτων εξ αυτών είναι δυνατόν να υπάρξει καθοριστικός κίνδυνος για την ασφάλεια του πλοίου, του ανθρώπινου δυναμικού, του φορτίου, να υπάρξει πρόβλημα στο θαλάσσιο περιβάλλον είτε να υπάρξει σημαντικά εμπόδιση της εύρυθμης δράσης του σκάφους. Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως υφίστανται καθοριστικές διαφοροποιήσεις ανάμεσα σε αυτά τα δυο (Polemi, 2017).

Η αγορά παρόμοιων συστημάτων είναι σημαντικό να περιέχει έναν αρμόδιο μηχανικό, που γνωρίζει τον αντίκτυπο στα συστήματα επί των σκαφών και έχει γνώσεις IT, αλλά πιθανόν οι γνώσεις του να είναι περιορισμένες σε ό,τι έχει να κάνει με το λογισμικό είτε ακόμα και τη διαχείριση των κυβερνοεπιθέσεων. Συνεπώς, είναι ζωτικής σημασίας να υφίσταται επικοινωνία με την υπηρεσία πληροφορικής με απώτερο στόχο να εξασφαλιστεί πως οι κίνδυνοι αυτής της μορφής θα ληφθούν υπόψη κατά την περίοδο της αγοράς αυτών των συστημάτων (American Bureau of Shipping, 2018).

Ακόμα, είναι χρήσιμο να επισημανθεί πως οι διαχειριστές των συστημάτων OT, είναι σημαντικό να επικοινωνούν με το τμήμα πληροφορικής, με κυριότερο στόχο να υφίσταται μια ευρύτερη εικόνα των πιθανών κινδύνων και με αυτόν τον τρόπο θα υπάρξει τεράστια υποστήριξη στην ανάπτυξη της κατάλληλης τακτικής και των δράσεων με στόχο τη συντήρηση του λογισμικού (Androjna et al., 2020).

Γενικότερα, θα πρέπει να γνωρίζουμε πως στα συστήματα πληροφορικής IT επηρεάζονται δίκτυα πληροφορικής, ηλεκτρονικά ταχυδρομεία, η διοίκηση, οι λογαριασμοί, οι λίστες πληρωμάτων, η σχεδιασμένη συντήρηση, η διαχείριση καθώς επίσης και η ανακύκλωση ανταλλακτικών, τα ηλεκτρονικά εγχειρίδια και πιστοποιητικά, οι άδειες εργασίες, οι φορτωτικές κλπ. Επί της ουσίας στα συγκεκριμένα συστήματα υφίσταται τεράστιος κίνδυνος των χρηματοοικονομικών δεδομένων της επιχείρησης όπως επίσης και για τη φήμη της (Dadiani, 2018).

Αντίθετα, στα συστήματα OT τα οποία έχουν να κάνουν με την εύρυθμη δράση του υλικού και του λογισμικού υφίστανται επιρροές στα PLC, στα SCADA, στην εποπτεία επί του πλοίου, στα GPS, στα ECDIS, στην απομακρυσμένη υποστήριξη για κινητήρες, στην καταγραφή πληροφοριών, στην εποπτεία μηχανών και φορτίου κλπ. Στα συστήματα αυτού του είδους είναι ως επί το πλείστον σε κίνδυνο η ζωή, η ιδιοκτησία αλλά και το περιβάλλον (Λιναρδάτος και Λιναρδάτος, 2016).

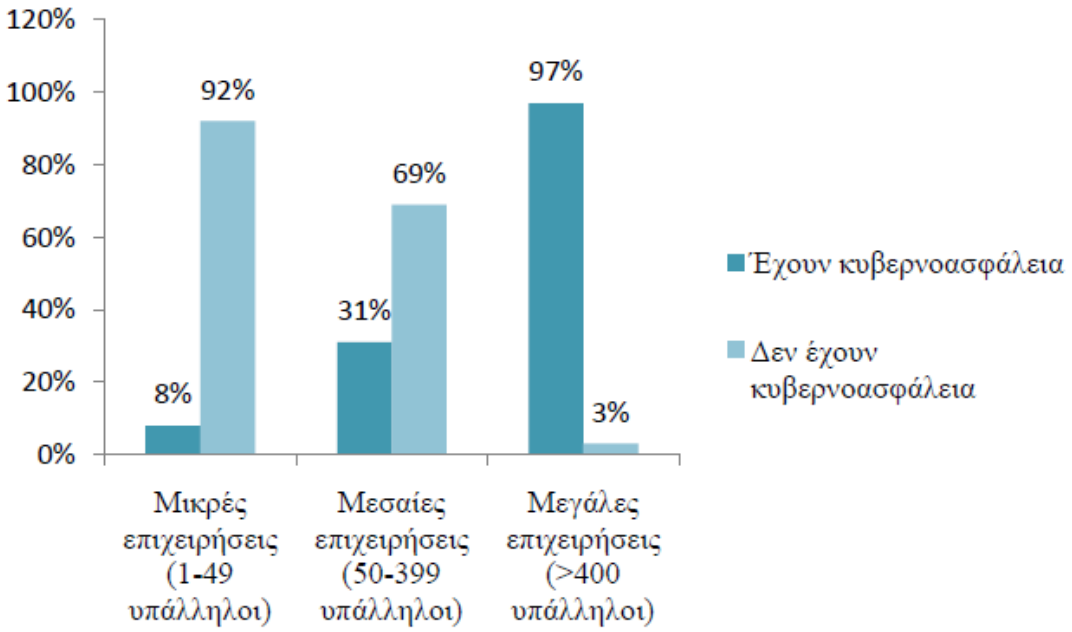
Οι κατευθυντήριες οδηγίες σε ό,τι έχει να κάνει με την ασφάλεια αυτής της μορφής σε αυτόν τον κλάδο εστιάζουν κατά κύριο λόγο σε IMO, BIMCO, ISO/IEC, Classification Bodies και IACS, P&I Clubs κλπ. Είναι χρήσιμο να γνωρίζουμε πως μέχρι πριν μερικά χρόνια δεν υπήρχε ένα νομοθετικό πλαίσιο το οποίο να συσχετίζεται αποκλειστικά με την ασφάλεια αυτού του είδους στον συγκεκριμένο κλάδο και που να είναι αναγκαστική η τήρησή του (Visvikis and Panayides, 2017).

Την περίοδο του 2017, ο IMO πρότεινε ένα σχέδιο με κυριότερο στόχο τη διαχείριση των κινδύνων θαλάσσιου κυβερνοχώρου εξαιτίας της αισθητής ανοδικής τάσης των απειλών αυτών των επιθέσεων με απώτερο σκοπό τον εν λόγω κλάδο. Αυτό το σχέδιο θα τεθεί σε ισχύ από το ξεκίνημα της περιόδου του 2021. Το συγκεκριμένο σχέδιο εφαρμόζει ένα αποδοτικό πλαίσιο διαχείρισης κινδύνων του NIST με απώτερο στόχο την κυβερνοασφάλεια με την εύρυθμη δράση 5 σταδίων, που είναι της αναγνώρισης, της προστασίας, της ανίχνευσης, της ανταπόκρισης αλλά και της ανάκτησης (American Bureau of Shipping, 2018).

Εξίσου σημαντικό ρόλο, όμως, έχει παίξει και η εφαρμογή του GDPR που ισχύει από τα μέσα της περιόδου του 2018 και είχε καθοριστικό αντίκτυπο σε όλες τις εταιρίες αυτού του τομέα, καθώς με αυτόν τον τρόπο συντηρούνται αρκετά προσωπικά δεδομένα. Το συγκεκριμένο πλαίσιο αναγκάζει όλες αυτές τις εταιρίες να υλοποιούν εκτιμήσεις των συνεπειών της προσωπικής ιδιωτικότητας στην περίπτωση στην οποία υφίσταται αισθητή ανοδική τάση του κινδύνου παραβίασης ενώ θα πρέπει να αναφέρουν μέσα σε διάστημα 72 ωρών κάθε περίπτωση παραβίασης, προκειμένου να υφίσταται η δυνατότητα άμεσης και αποδοτικής αντίδρασης (Kessler, 2020).

Την ίδια περίοδο αναπτύχθηκε και η οδηγία της ΕΕ NIS που αναγκάζει τους μεγαλύτερους παρόχους υπηρεσιών, όπως είναι για παράδειγμα οι μεγαλύτεροι λιμένες και οι θαλάσσιες υπηρεσίες μεταφορών να αποδείξουν πως έχουν λάβει τα κατάλληλα μέτρα με κυριότερο σκοπό να διαχειριστούν τους κινδύνους που μελετάμε σε αυτή την εργασία (Tapaninen and Andelin, 2020).

Σύμφωνα με έρευνες των τελευταίων ετών, όμως, το πιο μεγάλο ζήτημα εκτός από την έως τώρα έλλειψη του κατάλληλου νομοθετικού πλαισίου, ήταν οι άνθρωποι. Γενικότερα, υφίσταται μια δυσμένεια στην βαθύτερη κατανόηση από μεριάς των ανθρώπων μέσα στη συγκεκριμένη βιομηχανία στο τι είναι ακριβώς οι εν λόγω επιθέσεις και τι επιπτώσεις μπορούν να επιφέρουν (American Bureau of Shipping, 2018).



Εικόνα 3.1 : Ποσοστό εταιριών σύμφωνα με το μέγεθός τους που διαθέτουν ή όχι κυβερνοασφάλεια (Καβαλλιεράτος, 2018)

Πολλές φορές το γεγονός πως κάποιοι άνθρωποι του πληρώματος έχουν ελάχιστες έως και καθόλου γνώσεις για το συγκεκριμένο ζήτημα, η εσφαλμένη διαχείριση ορισμένων δράσεων κλπ έχουν σαν βασικότερη συνέπεια τα εν λόγω συστήματα να είναι εξαιρετικά εκτεθειμένα και ιδιαίτερα ευάλωτα σε πιθανές

επιθέσεις. Με αυτόν τον τρόπο, η ευαισθητοποίηση του ανθρώπινου δυναμικού διαδραματίζει σημαντικό ρόλο στην εύρυθμη δράση της εκάστοτε εταιρίας αυτού του κλάδου (Dadiani, 2018).

Βάσει μελετών των τελευταίων ετών, όλες οι μεγάλες εταιρίες αυτού του τομέα υλοποιούν προγράμματα κατάρτισης για αυτό το θέμα στους υπαλλήλους οι οποίοι έχουν πρόσβαση σε αυτά τα συστήματα. Κάτι τέτοιο, όμως, δεν ισχύει για τις μικρότερες εταιρίες καθώς μονάχα το 11% από αυτές θέτει σε εφαρμογή παρόμοιας μορφής προγράμματα, κάτι το οποίο εξηγεί σε μεγάλο βαθμό το λόγο που οι συγκεκριμένες εταιρίες είναι σε τεράστιο κίνδυνο (Polemi, 2017).

3.3 Προκλήσεις

Η ραγδαία ανάπτυξη της χρήσης αλλά κυρίως της εξάρτησης από τις σύγχρονες τεχνολογίες, αλλά και η εξέλιξη της αυτοματοποίησης έχουν παίξει καθοριστικό ρόλο στην αισθητή ανοδική τάση του ρόλου της αντιμετώπισης όλων των πιθανών προκλήσεων. Η κλασσική μέθοδος επικοινωνίας διαμέσου της φωνής κλπ έχει αντικατασταθεί από τις σύγχρονες και αυτοματοποιημένες ανταλλαγές δεδομένων (Androjna et al., 2020).

Η καινούρια αυτή τάση αναπτύσσει καινούριες ανάγκες σε ό,τι έχει να κάνει με την εξακρίβωση της ταυτότητας του παραγόμενου εγγράφου, την ακεραιότητα των μηνυμάτων αλλά και την εμπιστευτικότητα στην περίπτωση που χρειάζεται. Ορισμένες από τις πιο σημαντικές προκλήσεις που χρειάζεται να αντιμετωπίσει ο συγκεκριμένος τομέας πριν την εφαρμογή αυτών των πολλά υποσχόμενων καινοτόμων δράσεων έχουν άμεση σχέση με την ποιότητα των πληροφοριών, την προσαρμογή των εταιριών στις οδηγίες και τους κανόνες σε ό,τι έχει να κάνει με την ασφάλεια αλλά και τον ανθρώπινο ρόλο στην αυτονομία (Λιναρδάτος και Λιναρδάτος, 2016).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως η εμπιστοσύνη αποτελεί μια από τις πιο καθοριστικές παραμέτρους που σχετίζεται με την επιτυχή εφαρμογή της 4ης βιομηχανικής επανάστασης σε αυτόν τον κλάδο. Η εμπιστοσύνη στην ποιότητα των πληροφοριών που αναπτύσσουν οι αισθητήρες, η εμπιστοσύνη στους ανθρώπους οι οποίοι διαχειρίζονται όλες αυτές τις πληροφορίες αλλά και η εμπιστοσύνη στους αλγόριθμους οι οποίοι βγάζουν χρήσιμα συμπεράσματα από τα αναπτυσσόμενα στοιχεία είναι χρήσιμα κριτήρια για τη συντήρηση αλλά και την ανοδική τάση της λογοδοσίας μεταξύ των διάφορων μερών (McNicholas, 2016).

Η αισθητή ανοδική χρήση των big data, τα έξυπνα πλοία και το internet of things (IoT) έχουν παίξει και θα παίξουν και στο μέλλον καθοριστικό ρόλο στην ανοδική τάση του όγκου δεδομένων που θα είναι διαθέσιμα στους επιτιθέμενους και την πιθανή επιφάνεια επιθέσεων σε επίδοξους κακόβουλους χρήστες του διαδικτύου. Όλα αυτά κάνουν ζωτικής σημασίας την απαίτηση για ισχυρές προσεγγίσεις στην ασφάλεια αυτής της μορφής, καθοριστικές τόσο για το παρόν όσο και για το μέλλον (Dadiani, 2018).

Γενικότερα, είναι σημαντικό να γνωρίζουμε πως σαν ένας μεγάλος και σε τεράστιο επίπεδο μη ελέγξιμος χώρος, ο συγκεκριμένος κλάδος είναι επιρρεπής στη διάδοση των εγκληματικών φορέων που επωφελούνται από τα ανοιχτά θαλάσσια σύνορα. Η πειρατεία όπως επίσης και η τρομοκρατία στο θαλάσσιο περιβάλλον, το λαθρεμπόριο όπλων κλπ είναι μερικές από τις πιο διαδεδομένες παράνομες πρακτικές οι οποίες υφίστανται σε αυτόν τον τομέα (American Bureau of Shipping, 2018).

Παρά το γεγονός αυτό, όμως, ένας από τους πιο σημαντικούς κινδύνους της σύγχρονης εποχής είναι η ψηφιοποίηση αλλά και η αισθητή ανοδική τάση της διασύνδεσης των συστημάτων που έχει να κάνει με την ασφάλεια στον κυβερνοχώρο. Στη σύγχρονη εποχή, ανταλλαγές πληροφοριών κλπ υφίστανται σε καθημερινή βάση ανάμεσα σε σκάφη, επιχειρήσεις, λιμένες, ναυτιλιακούς πράκτορες κλπ. τα σκάφη δεν επωφελούνται πλέον από ένα ψηφιακό επίπεδο ασφαλείας απομονώνοντας το από όλα

τα άλλα δίκτυα. Στη σημερινή εποχή τα σκάφη είναι σύνθετα σύνολα βιομηχανικών συστημάτων. Η δράση αυτών των συστημάτων, όμως, δεν εξαιρείται από πιθανά ψηφιακά λάθη. Συνεπώς, τα εν λόγω συστήματα έχουν την ευχέρεια να αποτελέσουν ένα από τα κυριότερα σημεία εισόδου για κακόβουλες ενέργειες (Polemi, 2017).

Μια δυνητική επίθεση στα συστήματα ενός σκάφους είναι δυνατόν να οδηγήσει σε τραυματισμό είτε ακόμα και απώλεια μιας ανθρώπινης ζωής, καταστροφή περιβάλλοντος κλπ. Ακόμα, μια παραβίαση αυτής της μορφής είναι εξαιρετικά πιθανό να επιφέρει καθοριστικές διαταραχές στις επιχειρησιακές δράσεις, με βασικότερη συνέπεια να υφίστανται τεράστιες χρηματοοικονομικές απώλειες για την εταιρία και αρνητικές συνέπειες στη φήμη και στην εικόνα της (Androjna et al., 2020).

Εστιάζοντας στους παραπάνω κινδύνους, μια επιχείρηση αυτού του τομέα είναι εξαιρετικά πιθανό να κληθεί να έρθει αντιμέτωπη με τεράστιες οικονομικές ζημιές είτε ακόμα και νομικά θέματα αλλά και με την πρόκληση να ανακάμψει άμεσα και να επανέλθει στους φυσιολογικούς της ρυθμούς. Η προστασία ενός σκάφους σημαίνει συντήρηση των λειτουργικών αλλά και οργανωτικών δράσεων (McNicholas, 2016).

Ο τελικός σκοπός στοχεύει στη βέλτιστη εφικτή διασφάλιση πως η κακόβουλη ενέργεια δεν έχει την ευχέρεια να βάλει σε κίνδυνο την εύρυθμη δράση του σκάφους. Τα σύγχρονα σκάφη αποτελούν ένα χρήσιμο μέσο μεταφοράς μεταξύ αρκετών ακόμα. Παρά το γεγονός αυτό, όμως, ο συγκεκριμένος τομέας είναι σημαντικό να γνωρίζει πως βρίσκεται στο επίκεντρο αυτών των απειλών, καθώς διακυβεύονται χρήματα, ευαίσθητα δεδομένα, δράσεις ακτιβισμού, τρομοκρατικές ενέργειες κλπ (Roberts et al., 2017).

Η ασφάλεια αυτής της μορφής δεν περιορίζεται μονάχα στην αποτροπή της πρόσβασης κακόβουλων χρηστών σε συστήματα και δεδομένα, με ενδεχόμενη απώλεια εμπιστευτικότητας και την εποπτεία τους. Έχει να κάνει κυρίως με τη συντήρηση της ακεραιότητας καθώς επίσης και της διαθεσιμότητας των δεδομένων

είτε ακόμα και των συστημάτων διασφαλίζοντας τη συνέχεια της εταιρίας και τη διαρκή χρησιμότητα των ψηφιακών δεδομένων και συστημάτων (Tapaninen and Andelin, 2020).

Με κυριότερο στόχο να επιτευχθούν όλα τα παραπάνω είναι καθοριστικό να υπάρξει η απαιτούμενη εστίαση όχι μονάχα στην προστασία των συστημάτων των σκαφών από φυσικές επιθέσεις αλλά θα πρέπει να εξασφαλιστεί η σχεδιαστική δράση των συστημάτων αλλά και η υποστήριξη των δράσεων, προκειμένου να είναι ανθεκτικές από πιθανές επιθέσεις (Kessler, 2020).

Είναι εξίσου σημαντικό, όμως, να υφίστανται κατάλληλες τακτικές επαναφοράς σε περίπτωση παραβίασης των εν λόγω συστημάτων. Οι απειλές εκ των έσω, από εργαζομένους στα γραφεία των εταιριών είτε ακόμα και από διάφορους ναυτικούς οι οποίοι αποφασίζουν να δράσουν με κακόβουλες ή μη μεθόδους δεν είναι δυνατόν να αγνοηθούν. Οι περισσότεροι ιδιοκτήτες των σκαφών είναι σημαντικό να αντιληφθούν τη συγκεκριμένη μορφή ασφάλειας και να προβάλλουν την ευαισθητοποίηση σε ό,τι έχει να κάνει με το εν λόγω ζήτημα στα ενδιαφερόμενα μέρη, περιέχοντας και το ίδιο το ανθρώπινο δυναμικό του σκάφους (Androjna et al., 2020).

Τέλος, η διαφοροποιημένη φύση των απειλών αυτής της μορφής σημαίνει πως υφίσταται ενιαία προσέγγιση που να έχει την ευχέρεια να καταπολεμήσει όλους αυτούς τους κινδύνους. Ο ρυθμός αλλαγών και εξελίξεων της τεχνολογίας σε συνδυασμό με τη σταθεροποιημένη ροή σημαντικών αδύνατων σημείων στα λειτουργικά συστήματα, τις βιβλιοθήκες λογισμικού, τις εφαρμογές κλπ σημαίνει πως κάθε τακτική χρειάζεται να ελέγχεται σε συχνά χρονικά διαστήματα (Καβαλλιεράτος, 2018).

3.4 Αντιμετώπιση

Στη σημερινή εποχή, τα αυτόνομα σκάφη αναπτύσσουν σημαντικές προοπτικές για τη συγκεκριμένη βιομηχανία. Παρά το γεγονός αυτό, όμως, υφίστανται ακόμα αρκετά επίπεδα τα οποία χρειάζεται να υλοποιηθούν έως τα αυτόνομα σκάφη να καταστούν εντελώς λειτουργικά. Όπως τονίστηκε και στα παραπάνω κεφάλαια, στη σύγχρονη εποχή, ο ανθρώπινος παράγοντας είναι εκείνος ο οποίος αλληλεπιδρά με τα συστήματα των σκαφών. Αυτός είναι και ο κυριότερος λόγος που το μη ενημερωμένο και μη κατάλληλα καταρτισμένο ανθρώπινο δυναμικό αποτελεί τη βασικότερη αιτία ανοδικής τάσης των συγκεκριμένων επιθέσεων (George, 2020).

Συνεπώς, για την ορθότερη αντιμετώπιση των εν λόγω επιθέσεων σε αυτόν τον τομέα, είναι χρήσιμη η εφαρμογή μιας ανθρωποκεντρικής προσέγγισης εστιάζοντας κατά κύριο λόγο στη σωστή αλληλεπίδραση των ανθρώπων με τα συστήματα. Ο ISO έχει αναπτύξει διάφορα πρότυπα με απώτερο στόχο τη βέλτιστη εφικτή ενίσχυση του καθοριστικού ρόλου των ανθρώπων σε ολόκληρο τον κύκλο ζωής των συστημάτων (Dadiani, 2018).

Για παράδειγμα το ISO 2010 προσφέρει τις κατάλληλες απαιτήσεις οι οποίες είναι σημαντικό να εφαρμοστούν από τις επιχειρήσεις οι οποίες σχεδιάζουν και αναπτύσσουν το υλικό είτε ακόμα και το λογισμικό το οποίο θα χρησιμεύσει σε αυτόν τον τομέα, προκειμένου το τελικό σύστημα να λειτουργεί σε αρμονία με τους τελικούς χειριστές. Κυριότερος στόχος των ανθρωποκεντρικών προσεγγίσεων είναι η παροχή μιας δομής, που θα παίξει καθοριστικό ρόλο στην αισθητή ελάττωση των κινδύνων, οι οποίοι αναπτύσσονται από λάθη των ανθρώπων. Σε όλα αυτά καθοριστικό ρόλο θα παίξει και η κατάρτιση του προσωπικού (Visvikis and Panayides, 2017).

Εξίσου σημαντικό ρόλο, όμως, έχουν και τα συστήματα και τα δεδομένα. Ο κυριότερος σκοπός των σύγχρονων δικτύων και συστημάτων επικοινωνίας είναι να διασφαλίσουν πως προσφέρονται υπηρεσίες στα συστήματα τα οποία ανταποκρίνονται

στις ανάγκες ασφαλείας και δια-λειτουργικότητας για την εύρυθμη δράση των σκαφών. Ο σκοπός των συγκεκριμένων αναγκών είναι να αποτελέσουν καθοριστικό κομμάτι των δράσεων του συστήματος εξασφαλίζοντας πως υφίσταται η απαιτούμενη εστίαση στις απαιτήσεις όλων των χρηστών (American Bureau of Shipping, 2018).

Ακόμα, η ανίχνευση μιας περίπτωσης είναι καθοριστική με κυριότερο στόχο την αποτροπή της εξάπλωσης είτε την εμπόδιση αμέσως μόλις βρεθεί. Ελέγχοντας πιθανές περιπτώσεις στα συστήματα, η εταιρία έχει την ευχέρεια να ενεργοποιήσει τα συστήματα αντιμετώπισης αυτών των επιθέσεων και να ανταποκριθεί όπως πρέπει. Είναι σημαντικό να προσφέρονται δεδομένα με απώτερο σκοπό την εύρυθμη δράση των αισθητήρων και των λοιπών συστημάτων (Varun, 2019).

Σημαντική, όμως, λογίζεται πως είναι και η δικτυακή υποδομή. Μια βασική ανησυχία κατά τη σχεδιαστική δράση ενός δικτύου είναι σημαντικό να είναι οι διασυνδέσεις ανάμεσα σε διαφοροποιημένα συστήματα του σκάφους και της στεριάς. Η κυριότερη ιδέα με στόχο την ανάπτυξη μιας σωστής τοπολογίας δικτύου είναι η εφαρμογή του όρου «Άμυνα σε βάθος», η οποία έχει την ευχέρεια να βοηθήσει στην αισθητή ανοδική τάση της ανθεκτικότητας των δικτύων διαμέσου της κατάτμησης των δεδομένων τους. Επί της ουσίας πρόκειται για μια τακτική εξασφάλισης η οποία έχει σαν κυριότερο σκοπό να παρέχει πλεονασμό σε περιστατικά αποτυχίας μιας εποπτείας ασφαλείας είτε εκμετάλλευσης μιας ευπάθειας (Tapaninen and Andelin, 2020).

Μερικές από τις πιο χρήσιμες τακτικές διαμέσου των οποίων είναι εφικτή η ανοδική τάση της ασφάλειας στον κυβερνοχώρο είναι η ανάληψη υποχρεώσεων των χωρών, η ανάπτυξη της ψηφιακής ενιαίας αγοράς, οι επενδύσεις, η σωστή κατάρτιση, η ανάπτυξη της ανθεκτικότητας, η διεθνής συνεργασίας, η ενίσχυση της αμυντικής πολιτικής, η αντιμετώπιση του κυβερνοεγκλήματος κλπ (Λιναρδάτος και Λιναρδάτος, 2016).

3.5 Προοπτικές

Στη σημερινή εποχή, υφίστανται πολλά σημεία τα οποία κάνουν τη συγκεκριμένη μορφή ασφάλειας εξαιρετικά σύνθετη. Καθοριστικότερα είναι το ότι υφίστανται πολλά και διαφορετικά είδη σκαφών, που από τη μια δρουν αντίστοιχα σε διαφοροποιημένα περιβάλλοντα αλλά και συνθήκες και από την άλλη το κάθε ένα εξ αυτών χρησιμοποιεί διαφοροποιημένο λογισμικό (American Bureau of Shipping, 2018).

Μερικά εξ αυτών, μάλιστα, έχουν τόσο παλιά συστήματα τα οποία είναι εφικτό να αποτελέσουν μια εξαιρετικά εύκολη λεία σε σχέση με τις επιθέσεις αυτής της μορφής. Ακόμα, στη σημερινή εποχή υφίστανται αρκετά και διαφορετικά παραδείγματα παραποίησης του σήματος GPS και των ηλεκτρονικών χαρτών (ECDIS) από τρίτους παράγοντες (όπως είναι για παράδειγμα πειρατές, ανταγωνίστριες εταιρίες κλπ, κάτι το οποίο είναι εφικτό σταδιακά να οδηγήσει σε στοχευμένη πρόσκρουση σκάφους και επομένως σε τραυματισμό του πληρώματος) (Polemi, 2017).

Σε ό,τι έχει να κάνει με την ασφάλεια των σκαφών από επιθέσεις του κυβερνοχώρου, οι σύγχρονες επιχειρήσεις είναι ζωτικής σημασίας να εφαρμόζουν τους κανόνες που έχουν εκδοθεί από τον IMO, που εστιάζουν στην αναγνώριση συστημάτων, πληροφοριών αλλά και δυνατοτήτων που βάζουν σε τεράστιο κίνδυνο τη δράση τους. Με κυριότερο στόχο να επιτευχθεί κάτι τέτοιο, όμως, οι σύγχρονες επιχειρήσεις είναι καθοριστικό να αναπτύξουν μια εποπτεία ρίσκου με ικανότητα όχι μονάχα εντοπισμού περιστατικών αλλά και άμεσης καταπολέμησής τους σε πραγματικό χρόνο (Dadiani, 2018).

Εκτός, όμως, από το τεχνικό μέρος, η εποπτεία σε συνδυασμό με την αισθητή ελάττωση των διαρροών χρήσιμων δεδομένων χρειάζεται να περιέχει και ένα πλάνο καταπολέμησης με αποδέκτη τους ανθρώπους. Είναι εξαιρετικά καθοριστικό το

ανθρώπινο δυναμικό της κάθε επιχείρησης να είναι κατάλληλα εκπαιδευμένο και ενημερωμένο για όλους αυτούς τους κινδύνους.

Από όλα όσα έχουν αναλυθεί μέχρι τώρα, γίνεται εύκολα αντιληπτό πως η τεχνολογία και η συγκεκριμένη βιομηχανία έχουν ξεκινήσει να έχουν άμεση σχέση. Αυτός είναι και ο κυριότερος λόγος που πλέον είναι ζωτικής σημασίας οι εταιρίες αυτού του τομέα να κατανοήσουν πλήρως όσο πιο γρήγορα γίνεται την αξία αυτής της ασφάλειας, αφού η εν λόγω μορφή ασφάλειας δεν έχει να κάνει μονάχα με τη δυνατότητα αποτροπής παρείσφρησης κακόβουλων χρηστών στις πληροφορίες της επιχειρήσεις και προστασίας τους, αλλά διαμέσου αυτών των τακτικών διακυβεύεται η δυνατότητα της κάθε επιχείρησης να εξασφαλίζει τη φήμη της, την εικόνα της αλλά και την εμπιστοσύνη που έχει από τους πελάτες της. Η επένδυση των συγκεκριμένων επιχειρήσεων στην προστασία των πληροφοριών χρειάζεται να αντιμετωπιστεί από εδώ και πέρα ως ένα καινούριο πλαίσιο επένδυσης και λειτουργίας που είναι ζωτικής σημασίας (Polemi, 2017).

Επίσης είναι σημαντικό να κατανοήσουμε πως οι μεταβολές αυτής της μορφής, τις οποίες επιφέρουν οι συγκεκριμένες τεχνολογίες δεν έχουν να κάνουν μονάχα με τους καθημερινούς χρήστες είτε τις εταιρίες, αλλά και τους ίδιους τους κακόβουλους χρήστες, που έχουν την ευχέρεια να εκμεταλλευτούν τις καινούριες προοπτικές οι οποίες τους προσφέρονται, καθώς πλέον έχουν τη δυνατότητα να αναπτύξουν καινούριες μεθόδους επιθέσεων (McNicholas, 2016).

Φυσικά καθοριστικό ρόλο στη μείωση των προοπτικών των κακόβουλων χρηστών έχουν παίξει οι τελευταίες νομοθετικές τροποποιήσεις που έχουν γίνει σε διεθνές επίπεδο. Νομοθετικά πλαίσια (όπως είναι για παράδειγμα το GDPR κλπ) αλλά και διάφορα διεθνή πρότυπα (όπως είναι τα ISO), ενθαρρύνουν τη συνεχή βελτίωση των ικανοτήτων θωράκισης, με απώτερο σκοπό την βέλτιστη εφικτή ασφάλεια των δεδομένων όλων αυτών των συστημάτων. Για να υπάρξει η σωστή αντιμετώπιση,

όμως, χρειάζονται επενδύσεις, κατάρτιση του ανθρώπινου δυναμικού, τήρηση των παραπάνω κανονισμών, ανάπτυξη κουλτούρας ασφάλειας κλπ (Kessler, 2020).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως η βιομηχανία που μελετήσαμε σε αυτή την εργασία έχει ξεκινήσει πλέον να εφαρμόζει τις σημερινές τεχνολογίες αφού ο κύκλος ζωής των συστημάτων στα σκάφη προσεγγίζει κατά μέσο όρο τα 20 έτη, σε ένα απαιτητικό καθώς επίσης και ιδιαίτερα εχθρικό περιβάλλον. Παρά το γεγονός αυτό, όμως, τα τελευταία έτη το σύνολο των σκαφών τα οποία βρίσκονται στον αυτοματισμό παρουσιάζουν σημαντική ανοδική τάση και οι επιχειρήσεις επιλέγουν να επενδύσουν ολοένα και περισσότερα χρήματα στην ανάπτυξη αυτών των συστημάτων, που τους προσφέρουν τη δυνατότητα επικοινωνίας από οπουδήποτε και οποτεδήποτε (Καβαλλιεράτος, 2018).

Μια προοπτική εξέλιξης των τελευταίων ετών είναι τα μη επανδρωμένα σκάφη. Πρόκειται για σκάφη τα οποία λειτουργούν με απομακρυσμένη πρόσβαση και είναι εντελώς αυτόνομα, κάτι το οποίο έρευνες αναφέρουν πως μπορεί να γίνει μέχρι και την περίοδο του 2035. Τα συγκεκριμένα σκάφη, όμως, θα είναι ιδιαίτερα ευάλωτα σε επιθέσεις του κυβερνοχώρου, αφού η δράση τους θα έχει άμεση σχέση με τις ICT τεχνολογίες, την υψηλότερη ενσωμάτωση συστημάτων καθώς επίσης και την αισθητή ανοδική τάση της συνδεσιμότητας με τα συστήματα της ξηράς και το internet (Polemi, 2017).

Παρά την ευρεία αποδοχή πως οι κίνδυνοι έχουν προέλευση κυρίως από τη θέληση για αυτονομία, η διεθνής βιβλιογραφία είναι ιδιαίτερα φτωχή μέχρι σήμερα για το εν λόγω ζήτημα. Με βασικότερο στόχο να καταπολεμηθούν οι πιθανές απειλές και να υπάρξει διεξοδική μελέτη αυτού του θέματος, είναι καθοριστικό να υφίσταται μια καθορισμένη αρχιτεκτονική δικτύων σύμφωνα με την οποία θα αξιολογούνται τα συστήματα που δημιουργούνται (George, 2020).

Δεν θα πρέπει να ξεχνάμε, άλλωστε, πως από τα κυριότερα ελαττώματα της εν λόγω βιομηχανίας είναι πως τα σκάφη είναι εξαιρετικά σύνθετα σύνολα

συστημάτων, διαφοροποιημένων προμηθευτών, με τεράστιο κύκλο ζωής και είναι σύνηθες φαινόμενο η ύπαρξη σκαφών τα οποία έχουν λίγες είτε ακόμα και καθόλου ομοιότητες μεταξύ τους σε ό,τι έχει να κάνει με την τοπολογία των δικτύων τους (Varun, 2019).

Συνεπώς, γίνεται εύκολα αντιληπτό πως είναι εξαιρετικά δύσκολο να αναπτυχθεί και να διερευνηθεί μια πιθανή αρχιτεκτονική δικτύου, έτσι ώστε να υφίσταται μια ολιστική προσέγγιση του ζητήματος. Είναι καθοριστικό να καταφέρει η βιομηχανία να αντιμετωπίσει τα συγκεκριμένα ζητήματα, έτσι ώστε να είναι ανθεκτική στις απειλές οι οποίες έχουν προέλευση από τον κυβερνοχώρο (Dadiani, 2018).

Αυτός είναι και ο κυριότερος λόγος που είναι εξαιρετικά σημαντική η διερεύνηση και η βέλτιστη εφικτή αξιολόγηση διαφορετικών αρχιτεκτονικών δικτύων, επικεντρώνοντας το ενδιαφέρον στα ιδιαίτερα γνωρίσματα αυτού του τομέα. Εξίσου σημαντική, όμως, λογίζεται πως είναι και η ύπαρξη περισσότερων επιλογών όπου τα σύγχρονα συστήματα θα είναι εφικτό να είναι πιο ανθεκτικά σε σχέση με αυτές τις απειλές (Polemi, 2017).

Εκτός, όμως, από τη σημαντική ανάπτυξη των συστημάτων ΟΤ, η τεράστια πρόκληση στη σημερινή εποχή έχει να κάνει με τα MAS (αυτόματα συστήματα ναυτιλίας). Με την εξέλιξη της τεχνητής νοημοσύνης και την ευρεία χρήση του διαδικτύου, η καινούρια γενιά σκαφών θα εποπτεύεται από απόσταση από τη στεριά. Τα συγκεκριμένα συστήματα στη σύγχρονη εποχή βρίσκονται στο επίπεδο των πιλοτικών εφαρμογών και αναμένεται να μπουν σε λειτουργία στο μέλλον (Kessler, 2020).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως η σύγχρονη ψηφιοποίηση όλων αυτών των συστημάτων και των δράσεων των σκαφών έχει σαν βασικότερο στόχο την αισθητή ανοδική τάση της αποδοτικότητας αλλά και τη βελτίωση της συνεργασίας σε αυτόν τον τομέα. Παρόλα αυτά, παράλληλα, σημαίνει καθοριστική ανοδική τάση της

πιθανότητας αυτών των επιθέσεων από κακόβουλα λογισμικά, με κυριότερο σκοπό την απώλεια της εποπτείας αυτών των συστημάτων από το σκάφος (Καβαλλιεράτος, 2018).

Οι καλύτερες τακτικές που είναι σημαντικό να εξελιχτούν σε αυτές τις περιπτώσεις είναι η οριοθέτηση του περιβάλλοντος της απειλής για τις εξωτερικές αλλά και τις εσωτερικές απειλές αυτής της μορφής, ο καθορισμός των ευάλωτων συστημάτων όπου είναι εφικτό να υπάρξει μια απειλή κατανοώντας τις κυριότερες επιπτώσεις στα συγκεκριμένα συστήματα, η αξιολόγηση της έκθεσης σε κίνδυνο, η ανάπτυξη κατάλληλων μέτρων προστασίας με στόχο την ελάττωση των συνεπειών αλλά και η ανάπτυξη σχεδίων έκτακτης ανάγκης με απώτερο σκοπό την αισθητή ελάττωση πιθανών κινδύνων σε αυτό το περιβάλλον (American Bureau of Shipping, 2018).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως είδαμε στη συγκεκριμένη εργασία, ο κυβερνοχώρος αποτελεί μια ολοζώντανη υπόσταση η οποία εμφανίζει ραγδαία ανάπτυξη και μεταβάλλει διαρκώς τη μορφή, αναπτύσσοντας καινούριες και συνεχώς πιο πολλές προκλήσεις αλλά και προοπτικές. Το μεγαλύτερο ποσοστό των επιχειρήσεων, δίχως να υφίσταται καμία απολύτως εξάρτηση από τη γεωγραφική τοποθεσία και τον κλάδο απασχόλησης επαφίεται με το πέρασμα των ετών ολοένα και πιο πολύ στο διαδίκτυο, κάτι το οποίο βοηθάει στην ανοδική τάση των κινδύνων που κρύβει η συγκεκριμένη χρήση.

Οι επιθέσεις αυτής της μορφής κατηγοριοποιούνται από αρκετές και διαφορετικές έρευνες μέσα στους 5 πιο σημαντικούς κινδύνους, που θα πρέπει να αντιμετωπίσουν οι σύγχρονες εταιρίες όλων των τομέων, αποτελώντας ένα τεράστιο εμπόδιο για όλους τους CEOs, καθώς το κόστος τους εμφανίζει διαρκώς ανοδική τάση και είναι κάτι που μπορεί να επιφέρει τεράστια προβλήματα.

Σε ό,τι έχει να κάνει με το θεσμικό πλαίσιο το οποίο έχει αφορά διάφορα ζητήματα τριγύρω από τις κυβερνοεπιθέσεις και την προστασία από αυτές γίνεται εύκολα κατανοητό ότι βρίσκεται σε μια ατέρμονη μεταβολή μέσα στα έτη ενεργώντας με απώτερο στόχο να προλάβει και να καλύψει τις καινούριες ανάγκες καθώς επίσης και τους κινδύνους του κυβερνοχώρου όπως επίσης και τις νέες τακτικές παραβίασης πληροφοριών που αναπτύσσονται σε καθημερινή βάση.

Όπως είδαμε στη συγκεκριμένη εργασία βασικότερος στόχος αυτών των επιθέσεων είναι οι οικονομικές αλλά και οι ασφαλιστικές εταιρίες, με τις εταιρίες στον τομέα των μεταφορών να βρίσκονται στην 3^{η} θέση. Σε αυτόν τον τομέα, όμως, περιέχεται και η ναυτιλιακή βιομηχανία, που αποτέλεσε πεδίο έρευνας αυτής της εργασίας. Η συγκεκριμένη βιομηχανία δέχεται διαρκώς νέα χτυπήματα από τους

επίδοξους ψηφιακούς εγκληματίες με μεγάλες και αρνητικές συνέπειες (όχι μόνο οικονομικές), εξαιτίας της τεράστιας σχέσης και εξάρτησης που έχει αναπτύξει με την τεχνολογία αλλά και το διαδίκτυο.

Σύμφωνα με όσα παρουσιάστηκαν σε αυτή την εργασία, οι μεγαλύτερες εταιρίες αυτού του τομέα ενημερώνουν συνεχώς τα συστήματά τους και για αυτό το λόγο οι περισσότερες εξ αυτών έχουν κρατήσει σε ένα υψηλό επίπεδο την κυβερνοασφάλειά τους. Καθοριστικό ρόλο, όμως, παίζει και τα συχνά προγράμματα κατάρτισης που χρησιμοποιούν για τους εργαζομένους τους. Οι περισσότερες ανησυχίες, όμως, εντοπίζονται στις μικρότερες επιχειρήσεις αυτού του τομέα, καθώς το μεγαλύτερο ποσοστό τους δεν είναι κατάλληλα προετοιμασμένο να αντιμετωπίσει περιπτώσεις παραβίασης δεδομένων.

Γενικότερα, παρά το γεγονός πως η ψηφιοποίηση του συγκεκριμένου τομέα έχει επιφέρει αρκετά οφέλη, στη σημερινή εποχή υφίστανται και αρκετές απειλές και κίνδυνοι, που μπορεί να δημιουργήσουν τεράστια προβλήματα. Μια από τις κυριότερες αιτίες αυτών των προβλημάτων είναι και ο ανθρώπινος παράγοντας. Για αυτό το λόγο όλες οι εταιρίες αυτού του τομέα είναι σημαντικό να λάβουν όλα τα κατάλληλα μέτρα και να επενδύσουν στην κυβερνοασφάλεια, καθώς μόνο έτσι θα μπορέσουν να εκμεταλλευτούν στο βέλτιστο εφικτό επίπεδο όλα τα οφέλη του κυβερνοχώρου, μειώνοντας όσο γίνεται περισσότερα τους κινδύνους και τις απειλές του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική βιβλιογραφία

- Αποστόλου Μ., (2014), *Συγκριτική ανάλυση της κατάστασης κυβερνοασφάλειας των χωρών-μελών της ΕΕ*, Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, Πειραιάς.
- Δημοβασίλη Ι., (2018), *Η ψηφιακή καινοτομία και ο ψηφιακός μετασχηματισμός στις ναυτιλιακές επιχειρήσεις: Οι περιπτώσεις της Capital και της Avin*, Διπλωματική εργασία, Πανεπιστήμιο Αιγαίου, Σάμος.
- Καβαλλιεράτος Γ., (2018), *Κυβερνοεπιθέσεις στο cyber-enabled πλοίο,* Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, Πειραιάς.
- Καμπαρίδου Ε.Γ., (2015), *Η Στρατηγική Κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση,* Διπλωματική εργασία, Πανεπιστήμιο Αιγαίου, Σάμος.
- Κοκοτος Δ., Λιναρδάτος Δ., Τζανατος Σ.Ε., Νικητάκος Ν., (2010), *Τεχνολογίες Πληροφορικής και Επικοινωνιών στη Ναυτιλία*, Εκδόσεις Σταμούλη, Αθήνα.
- Κοκοτος Δ., Λιναρδάτος Δ., (2010), *Εφαρμογές πληροφορικής στη ναυτιλία,* Εκδόσεις Σταμούλης, Αθήνα.
- Λιναρδάτος Γ.Σ., Λιναρδάτος Δ., (2016), *Ραντάρ*, Β' Έκδοση, Εκπαιδευτικό Κείμενο Ακαδημιών Εμπορικού Ναυτικού, Αθήνα.
- Νικητάκος Β.Ν., (2011), *Θέματα ηλεκτρονικής τεχνολογίας στη ναυτιλία και τις μεταφορές,* Εκδόσεις Σιδέρης, Αθήνα.

Διεθνής βιβλιογραφία

- American Bureau of Shipping, (2018), *Cybersecurity implementation for the marine and offshore industries*, ABS, Houston, USA.
- Androjna A., Brcko T., Pavic I., Greidanus H., (2020), *Assessing Cyber Challenges of Maritime Navigation*, Journal of Marine Science and Engineering, pp. 1-21.
- Castro S., (2018), *Beginners guide to Hacking and Cyber Security*, Kindle Direct Publishing.
- Dadiani D., (2018), *Cyber-security and marine insurance*, World Maritime University.
- George H., (2020), *Cybersecurity: Essential Guide for Beginners to Learn Basic Methods of Cybersecurity*, Independently published.
- Holzsager F.W., (2015), *A Business Owner's Practical Guide to Cybercrime and Business Continuity*, CreateSpace Independent Publishing Platform.
- Kessler G.C., (2020), *Maritime Cybersecurity: A Guide for Leaders and Managers*, Independently published.
- McNicholas M., (2016), *Maritime Security: An Introduction*, 2nd Edition, Butterworth-Heinemann.
- Meeuwisse R., (2018), *Cybersecurity for Beginners*, 2nd Edition, Cyber Simplicity Ltd/
- Moschovitis C., (2018), *Cybersecurity Program Development for Business: The Essential Planning Guide*, Wiley.
- Polemi N., (2017), *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*, Elsevier.

- Roberts F.S., Drumhiller N.K., DiRenzo J., (2017), *Issues in Maritime Cyber Security*, Westphalia Press.
- Singer P.W., Friedman A., (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press.
- Song D.W., Panayides P.M., (2012), *Maritime Logistics: A Complete Guide to Effective Shipping and Port Management,* Kogan Page.
- Tapaninen U., Andelin J., (2020), *Maritime Transport: Shipping Logistics and Operations*, Kogan Page.
- Varun S., (2019), *A Practical guide to Shipping & Freight Forwarding: Your key to success in the shipping industry*, Independently published.
- Visvikis I.D., Panayides P.M., (2017), *Shipping Operations Management (WMU Studies in Maritime Affairs)*, Springer.
- ITU, (2018). Global Cybersecurity Index (2017). *International Telecommunications Union (ITU),*. Geneva, CH

Διαδικτυακή βιβλιογραφία

- https://www.proshred.com/minnesota/10-cyber-security-statistics/