Πρόγραμμα Μεταπτυχιακών Σπουδών στις Διεθνείς και Ευρωπαϊκές Σπουδές
Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών
Πανεπιστήμιο Πειραιώς

Ενεργειακή Ασφάλεια και Γεωπολιτική στον Ινδικό Ωκεανό

διπλωματική εργασία

Κωνσταντίνος Καραγιάννης

Πειραιάς, 2018

Εγώ, ο Κωνσταντίνος Καραγιάννης βεβαιώνω ότι το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

Στους γονείς μου,
Γεώργιο και Άννα

Ευχαριστίες

Θα επιθυμούσα να εκφράσω τις πιο θερμές μου ευχαριστίες στον Αναπληρωτή Καθηγητή Παραβάντη Ιωάννη για την επίβλεψη της παρούσας διπλωματικής εργασίας. Ειδικότερα θα ήθελα να τον ευχαριστήσω για την πολύτιμη καθοδήγησή του, τις εποικοδομητικές παρατηρήσεις και σχόλια του καθώς και για τα μεθοδολογικά εργαλεία που αποκόμισα από τη συνεργασία μαζί του.

Ευχαριστώ επίσης τα υπόλοιπα μέλη της Τριμελούς Επιτροπής για το χρόνο που αφιέρωσαν στην παρούσα εργασία και τις εποικοδομητικές παρατηρήσεις τους.

Επιπρόσθετα θα ήθελα να ευχαριστήσω το σύνολο των καθηγητών του τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς για την ευκαιρία που μου έδωσαν να εντρυφήσω στο πεδίο των διεθνών σχέσεων.

Τέλος θα ήθελα να εκφράσω τις ευχαριστίες και την ευγνωμοσύνη μου στην οικογένεια μου για τη στήριξη που μου παρείχε καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κεφάλαιο 1: Εισαγωγή

1.1. Προλεγόμενα

Με τον κόσμο να προσεγγίζει ξανά το πολυπολικό μοντέλο και με τη μετατόπιση του κέντρου βάρους των διεθνών εξελίξεων από τον άξονα Η.Π.Α-Ευρώπης στην Ασία, πρωτίστως λόγω της αυξανόμενης ισχύος της Κίνας αλλά και άλλων χωρών της περιοχής, παρουσιάζει ιδιαίτερο ενδιαφέρον η μελέτη των νέων δεδομένων αλλά και προκλήσεων που συνεπάγονται οι εν λόγω εξελίξεις. Η οικονομική ανάπτυξη αποτελεί απαραίτητη προϋπόθεση αύξησης της ισχύος για τα κράτη και βρίσκεται σε άμεση συνάρτηση με την εξασφάλιση της συνεχούς ροής και σε προσιτή τιμή των απαιτούμενων ενεργειακών πόρων. Το γεγονός αυτό καθιστά την ενεργειακή ασφάλεια παράμετρο ζωτικής σημασίας για τις ασιατικές οικονομίες. Με το μεγαλύτερο μέρος των ενεργειακών τους απαιτήσεων να καλύπτεται με εισαγωγές από τα κράτη της Μέσης Ανατολής και τη διακίνησή τους να γίνεται δια θαλάσσης και διαμέσου της κύριας θαλάσσιας εμπορικής οδού με άκρα τα στενά του Hormuz και της Malacca, η ασφάλεια της μεταφοράς θαλάσσιων (ενεργειακών) φορτίων στον Ινδικό ωκεανό αποτελεί ύψιστη προτεραιότητα τόσο για τους εισαγωγείς όσο και για τους εξαγωγείς. Πέραν των καιρικών συνθηκών και της πειρατείας, φαίνεται ότι η εκδήλωση κυβερνοεπιθέσεων στον ναυτιλιακό κλάδο αποτελεί μια από τις σημαντικότερες σύγχρονες απειλές τόσο για τη ναυσιπλοΐα και το εμπόριο όσο και για τα ίδια τα κράτη καθώς αποτελεί ασύμμετρη απειλή για τη λειτουργία τους λόγω της πιθανής χρήσης πλοίων ως φορείς εκδήλωσης επιθέσεων σε μεταφορικές δομές και σημαντικές εγκαταστάσεις.

Στόχος της παρούσας εργασίας αποτελεί η (καταρχήν) διερεύνηση της τρωτότητας της ασφάλειας, προερχόμενη από κυβερνοεπιθέσεις σε επίπεδο πλοίου, αναφορικά με τη μεταφορά (ενεργειακών) φορτίων στην περιοχή του Ινδικού ωκεανού.

1.2. Δομή διπλωματικής

Στη δεύτερο κεφάλαιο μέσω ανασκόπησης της υπάρχουσας βιβλιογραφίας επιχειρείται η παρουσίαση των εννοιών της ενεργειακής και θαλάσσιας ασφάλειας, γίνεται μια σύντομη αναφορά στα χαρακτηριστικά των κυβερνοαπειλών στο θαλάσσιο περιβάλλον και αναλύονται οι τρωτότητες των συστημάτων των εμπορικών

πλοίων σε ποικίλες μορφές κυβερνοεπιθέσεων. Στο επόμενο κεφάλαιο αναπτύσσονται τα ερευνητικά ερωτήματα που τίθενται προς απάντηση στην παρούσα εργασία ενώ στο τέταρτο κεφάλαιο παρουσιάζονται η γεωγραφία και τα χαρακτηριστικά της κύριας θαλάσσιας εμπορικής οδού του Ινδικού ωκεανού, αναλύονται περιπτώσεις εκδήλωσης κυβερνοεπιθέσεων στο θαλάσσιο περιβάλλον και επιτελείται σύνθεση των δύο ανωτέρω με σκοπό την αξιολόγηση της ασφάλειας όσον αφορά τη μεταφορά (ενεργειακών) φορτίων στον Ινδικό ωκεανό. Τέλος στο πέμπτο κεφάλαιο παρατίθενται τα συμπεράσματα αναφορικά με τα ερευνητικά ερωτήματα και προτείνονται προεκτάσεις της παρούσας εργασίας για περαιτέρω μελέτη.

Κεφάλαιο 2: Επισκόπηση βιβλιογραφίας

2.1. Εισαγωγή

Στο παρόν κεφάλαιο επιτελείται η επισκόπηση της βιβλιογραφίας. Στην ενότητα 2.2 παρουσιάζονται οι διάφορες προσεγγίσεις της έννοιας της ενεργειακής ασφάλειας ενώ στη ενότητα 2.3 τίθεται το πλαίσιο και οι παράμετροι της θαλάσσιας ασφάλειας. Ακολούθως η ενότητα 2.4 αναφέρεται στους δρώντες και τα μέσα από όπου προέρχονται οι κυβερνοαπειλές στο θαλάσσιο περιβάλλον ενώ στην ενότητα 2.5 γίνεται ανάλυση των τρωτοτήτων βασικών συστημάτων των σύγχρονων εμπορικών πλοίων.

2.2. Ενεργειακή ασφάλεια

Η ενέργεια αποτελεί αναμφίβολα μία από τις σημαντικότερες πτυχές στην ανθρώπινη ιστορία και κατέχει διαχρονικά ξεχωριστή θέση στην επιβίωση, ομαλή λειτουργία και ευημερία της κοινωνίας. Αποτελεί προϋπόθεση τόσο της ανθρώπινης ασφάλειας όσο και της οικονομικής ανάπτυξης. Παρά τη σημασία της, η έννοια της ενεργειακής ασφάλειας αποτέλεσε αντικείμενο προσοχής τη δεκαετία του 1970 στο δυτικό κόσμο, κυρίως λόγω της πετρελαϊκής κρίσης του 1973, άμεσα συνδεδεμένη με τη γενικότερη έννοια περί ασφάλειας του κράτους (Paravantis & Kontoulis, 2017).

Δύο διαφορετικές προσεγγίσεις του όρου ενεργειακή ασφάλεια φαίνεται να κυριαρχούν. Η παραδοσιακή προσέγγιση υποστηρίζει ότι κάθε κράτος αντιλαμβάνεται διαφορετικά τον όρο λόγω διαφοροποίησης των δομικών χαρακτηριστικών του όπως γεωγραφική θέση, πολιτικό σύστημα, οικονομικά δεδομένα, ίδιοι ενεργειακοί πόροι, ιδεολογικό υπόβαθρο και ιστορικές εμπειρίες (Luft & Korin, 2009· Marquina, 2008). Απεναντίας, η σχολή της Κοπεγχάγης θεωρώντας την ύπαρξη ενός πολυεπίπεδου διεθνούς συστήματος αποτελούμενο από τέσσερα επίπεδα, το διεθνές, το περιφερειακό, το εθνικό και το εσωτερικό (De Wilde, 1995) και λαμβάνοντας υπόψη ότι τα σύγχρονα ενεργειακά δίκτυα συνίστανται από πλέγμα ενεργειακών διασυνδέσεων (Johansson, 2013) προσεγγίζει τον όρο ανά επίπεδο. Συνεπώς η ενεργειακή ασφάλεια αφορά σε παγκόσμιο επίπεδο την εξασφάλιση ενεργειακών πόρων, σε περιφερειακό την διασφάλιση του απρόσκοπτου εμπορίου και της ανταλλαγής ενεργειακών πόρων, σε κρατικό την συνεχή και επαρκή παροχή ενέργειας και σε επίπεδο καταναλωτή την κάλυψη των απαιτήσεων.

Η ενεργειακή ασφάλεια μπορεί να ειδωθεί είτε από ρεαλιστική είτε από φιλελεύθερη οπτική ενώ συνδέεται άμεσα με την εθνική ασφάλεια καθώς και τη μακροοικονομική και μικροοικονομική θεωρία (Paravantis & Kontoulis, 2017). Μπορεί να υποστηριχθεί ότι ο όρος διαιρείται σε ασφάλεια της προσφοράς και της ζήτησης (Luft & Korin, 2009) με ιδιαίτερη έμφαση στο κομμάτι της προσφοράς (Kruyt, van Vuuren, de Vries & Groenenberg, 2009), η οποία συχνά είναι σε άμεση συνάρτηση με την συνεχή και ανεμπόδιστη ροή (IEA, 2007) σε προσιτή τιμή (Narula & Reddy, 2015).

Οι απόπειρες ορισμού του όρου ενεργειακή ασφάλεια διαφέρουν ανά εποχή λόγω των διαφορετικών προκλήσεων στον τομέα της ενέργειας (Winzer, 2012). Δεν υφίσταται κοινώς αποδεκτός ορισμός (Yergin, 2006· IEA, 2007) συνεπώς το εκάστοτε κράτος αντιλαμβάνεται διαφορετικά τον όρο συναρτήσει των ενεργειακών του πόρων, της τρωτότητάς του σε ενεργειακές κρίσεις και της θέσης του στην ενεργειακή αλυσίδα και επομένως αντιδρά διαφορετικά στις ενεργειακές προκλήσεις (Luft & Korin, 2009). Υπό αυτό το πρίσμα τα κράτη διαιρούνται σε τρεις ευρύτερες ομάδες, τους παραγωγούς-εξαγωγείς που στοχεύουν στην εξασφάλιση αξιόπιστης ζήτησης, τους καταναλωτές που επιθυμούν διαφοροποίηση των πηγών προμήθειας και τα ενδιάμεσα κράτη από τα οποία διέρχονται οι οδεύσεις που ενώνουν τους ανωτέρω (Luft & Korin, 2009). Η κατηγοριοποίηση αυτή αναδεικνύει εξίσου τις διαστάσεις της προμήθειας και της ζήτησης, με έμφαση για κάθε κράτος ανάλογα με την ομάδα στην οποία εντάσσεται, με εξαίρεση τους εξαγωγείς οι οποίοι ενδιαφέρονται για την διασφάλιση και των δύο (Johansson, 2013).

Η Διεθνής Υπηρεσία Ενέργειας (International Energy Agency, IEA) προσδιορίζει την ενεργειακή ασφάλεια ως την ανεμπόδιστη, επαρκή, αξιόπιστη και σε προσιτή τιμή διαθεσιμότητα των ενεργειακών πόρων αναδεικνύοντας περαιτέρω τη μακροχρόνια και βραχυχρόνια διάσταση της. Η πρώτη αναφέρεται σε επενδύσεις στον ευρύτερο τομέα για την παροχή ενέργειας σε αρμονία με την οικονομική ανάπτυξη και τις περιβαλλοντολογικές ανάγκες ενώ η δεύτερη στην εν γένει ικανότητα του ενεργειακού συστήματος να αντιδρά αποτελεσματικά σε ξαφνικές και απρόβλεπτες αλλαγές στο ισοζύγιο προσφοράς και ζήτησης (Kisel et al., 2016· IEA, 2011a· IEA, 2011b).

Η Ευρωπαϊκή Επιτροπή (European Commission) όρισε την ενεργειακή ασφάλεια ως την απρόσκοπτη και συνεχή ροή ενεργειακών προϊόντων σε προσιτή τιμή για το σύνολο των καταναλωτών με σεβασμό στις περιβαλλοντολογικές

ανησυχίες και την βιώσιμη ανάπτυξη (European Commission, 2000) ενώ το Κέντρο Ενεργειακών Ερευνών Ασίας-Ειρηνικού (Asia Pacific Energy Research Center, APERC) ανέδειξε τέσσερις πτυχές του όρου και συγκεκριμένα τη διαθεσιμότητα, προσβασιμότητα, προσιτότητα από οικονομικής άποψης και βιωσιμότητα περιγράφοντας την ενεργειακή ασφάλεια ως τη δυνατότητα μίας οικονομίας να εγγυηθεί την διαθεσιμότητα των ενεργειακών πόρων με συνεχή και αδιάλειπτο τρόπο με τρόπο που δε θα επηρεάσει αρνητικά τις οικονομικές επιδόσεις (APERC, 2007).

Αναφορικά με τις διαστάσεις του όρου υφίστανται πλήθος προσεγγίσεων με καθεμία να τονίζει διαφορετικές πτυχές και προεκτάσεις. Το Εμπορικό Επιμελητήριο των Η.Π.Α (U.S. Chamber of Commerce) έθεσε τέσσερις διαστάσεις και συγκεκριμένα τη γεωπολιτική, κυρίως όσον αφορά τις εισαγωγές ενέργειας από κράτη και περιοχές με συνθήκες αστάθειας, την αξιοπιστία ως προς την επάρκεια των υποδομών, την οικονομική συσχετιζόμενη με το εμπορικό ισοζύγιο και την περιβαλλοντολογική με έμφαση στην χρήση άνθρακα στην ενεργειακή παλέτα (U.S. Chamber of Commerce, 2010). Σύμφωνα με άλλη προσέγγιση, κυριότερες πτυχές αποτελούν η οικονομία, το περιβάλλον, η ανθρώπινη ασφάλεια, διεθνείς παράμετροι όπως η γεωπολιτική, η διαχείριση της ζήτησης, η διαμόρφωση της ενεργειακής πολιτικής και κοινωνιολογικά χαρακτηριστικά των κοινωνιών (Vivoda, 2010). Επιπρόσθετα οι Sovacool και Mukherjee (2010) απέδωσαν πέντε διαστάσεις τού όρου με περαιτέρω διάκριση σε είκοσι παραμέτρους. Αναλυτικά παρατίθενται η προσιτότητα από οικονομικής άποψης με επιμέρους τη σταθερότητα τιμών, πρόσβαση και αμεροληψία, αποκέντρωση και χαμηλό επίπεδο τιμών, η διαθεσιμότητα με παραμέτρους την εξάρτηση, διαφοροποίηση καθώς και ασφάλεια παραγωγής και παροχής, η βιωσιμότητα σε σχέση με τη χρήση της ξηράς, το νερό, τη μόλυνση του αέρα και τη κλιματική αλλαγή, η τεχνολογική ανάπτυξη εξεταζόμενη ως προς την επένδυση, την ικανότητα ανακαμψιμότητας, την έρευνα και καινοτομία, την ασφάλεια και αξιοπιστία, καθώς και την ενεργειακή επάρκεια και τέλος το κανονιστικό πλαίσιο που αφορά το εμπόριο, τη διακυβέρνηση, τον ανταγωνισμό και τη γνώση επί του κανονιστικού πλαισίου λειτουργίας. Με κάθε κράτος να διαφέρει ως προς το είδος και την ποσότητα των αξιοποιήσιμων ίδιων ενεργειακών πόρων, οι εθνικές προτεραιότητες, η οικονομική ανάπτυξη, η γεωγραφική θέση και η κοινωνική διαμόρφωση παίζουν πρωταρχικό ρόλο στη λειτουργία του τομέα της ενέργειας (Chester, 2010).

Οι έρευνες που χρησιμοποιούν δείκτες με στόχο την προσέγγιση της ενεργειακής ασφάλειας χωρίζονται σε δύο μεγάλες κατηγορίες, εκείνες που ποσοτικοποιούν την απόδοση σε βάθος χρόνου και εκείνες που συγκρίνουν την απόδοση μεταξύ κρατών (Paravantis & Kontoulis, 2017). Σύμφωνα με τους Ang, Choong και Ng (2015) επί συνόλου 53 ερευνών βασιζόμενων στη χρήση δεικτών ενεργειακής ασφάλειας, η πλειονότητα των δεικτών αποτελούνται από μερικές μεταβλητές έως 60, με τα δύο τρίτα των ερευνών να εξετάζουν έως 20. Κάθε έρευνα, και συνεπώς ο αντίστοιχος δείκτης, εστιάζει σε ποσοτικοποίηση διαφορετικών πτυχών της ενεργειακής ασφάλειας. Ο δείκτης Προσφοράς-Ζήτησης (Supply-Demand Index, SD Index) αξιολογεί 30 μεταβλητές προσπαθώντας να ενσωματώσει το σύνολο του ενεργειακού φάσματος με έμφαση στην ζήτηση, τη προσφορά και τη μεταφορά σε μεσο-μακροπρόθεσμη διάσταση (Kruyt et al., 2009). Ο Δείκτης Τρωτότητας (Vulnerability Index) αποτελείται από πέντε μεταβλητές (Gnansounou, 2008), ο Κοινωνικο-οικονομικός Δείκτης Ενεργειακού Κινδύνου (Socio-economic Energy Risk Index) από 8 (Radovanović, Filipović & Pavlović, 2017) ενώ ο Δείκτης Κινδύνου Ενεργειακής Ασφάλειας (Energy Security Risk Index) αποτελείται από 83 μεταβλητές που αξιολογούν τις γεωπολιτικές συνθήκες, την αξιοπιστία, περιβαλλοντολογικές παραμέτρους και οικονομικά μεγέθη (US Chamber of commerce, 2010). Τέλος ο Δείκτης Ενεργειακού Τριλήμματος (Energy Trilemma Index) βασίζεται σε δείκτες ενταγμένους σε τρεις κατηγορίες, σύμφωνα με την προσέγγιση του ενεργειακού τριλήμματος, το οποίο αναδεικνύει τη αλληλεπίδραση μεταξύ της ενεργειακής ασφάλειας, της οικονομικής ανάπτυξης και της περιβαλλοντικής βιωσιμότητας (Ang et al., 2015· Radovanović et al., 2017).

Πέραν των ανωτέρω προσεγγίσεων των διαστάσεων του όρου, υφίσταται και η άποψη ότι δέον είναι η διεύρυνση του πεδίου μελέτης προκειμένου η ενεργειακή ασφάλεια να ενσωματώσει σύγχρονες προκλήσεις και παράγοντες, συχνά μεταβαλλόμενους, καθώς είναι σε άμεση συνάρτηση με τις γεωπολιτικές εξελίξεις και τις διαμορφούμενες σχέσεις μεταξύ των κρατών (Paravantis & Kontoulis, 2017). Ως σύγχρονες προκλήσεις νοούνται οι εξελίξεις στην τεχνολογία, η ανθρώπινη ασφάλεια, το περιβάλλον, οι διεθνείς ζυμώσεις σε πολιτικό επίπεδο, η διαχείριση προσφοράς-ζήτησης, οι κοινωνικο-πολιτιστικοί παράγοντες και οι ενεργειακές στρατηγικές και επιδιώξεις των κρατών (Vivoda, 2010).

Αναφορικά με τη γεωπολιτική έχει επισημανθεί πληθώρα σημαντικών παραμέτρων που εντάσσονται στο ευρύτερο πλαίσιο της ενεργειακής ασφάλειας με

αποτέλεσμα να ανακύψει ο όρος νέα γεωπολιτική, που περιλαμβάνει παράγοντες όπως το πέρας του Ψυχρού Πόλεμου, την αυξανόμενη σημασία του φυσικού αερίου, τις τεχνολογικές εξελίξεις στον τομέα της ενέργειας και τον μετασχηματισμό του διεθνούς ενεργειακού εμπορίου λόγω της ένταξης σε αυτό του ρωσικού πετρελαίου και αερίου (Paravantis & Kontoulis, 2017). Σημαντική διάσταση αποτελούν τα συγκρουόμενα συμφέροντα εξαγωγέων και εισαγωγέων με διακύβευμα τον καθορισμό των τιμών που τείνουν να ενισχύουν τη συνεργασία μεταξύ των κρατών της κάθε ομάδας (Esakova, 2012). Η πιθανή ύπαρξη υποθαλάσσιων κοιτασμάτων πυροδοτεί εδαφικές διεκδικήσεις και συγκρούσεις μεταξύ κρατών για την κυριαρχία σε νησιωτικά συμπλέγματα και θαλάσσιες περιοχές, όπως στη Νότια Σινική θάλασσα (Johansson, 2013) ενώ οι προβλέψεις για εξάντληση των αξιοποιήσιμων αποθεμάτων των ορυκτών καυσίμων στο κοντινό μέλλον, οι κοινωνικές ανησυχίες σχετικά με την κλιματική αλλαγή, οι υψηλές τιμές των καυσίμων και η αύξηση των ενεργειακών απαιτήσεων αποτυπώνονται στις γεωπολιτικές εξελίξεις. Με δέκα από τις σημαντικότερες οικονομίες, και συγκεκριμένα τις Η.Π.Α, Ρωσία, Κίνα, Ινδία, Καναδά, Νότια Κορέα, Ιαπωνία, Μεξικό, Ινδονησία και Αυστραλία να παράγουν το 54% του παγκόσμιου Ακαθάριστου Εθνικού Προϊόντος (Gross Domestic Product, GDP), να καταναλώνουν το 61% της παγκόσμιας ενέργειας και να ευθύνονται για το 66% των εκπομπών διοξειδίου του άνθρακα (CO2) γίνεται εμφανής η άμεση συνάρτηση της ενέργειας με την οικονομικής ανάπτυξη, την κοινωνική ευημερία και την ισχύ των κρατών στη διεθνή κοινωνία (Vivoda, 2010). Η εν λόγω ανάλυση επισήμανε και ένα οξύμωρο, πως οι τέσσερις σημαντικότερες χώρες ως προς την κατανάλωση πετρελαίου, ήτοι οι Κίνα, Ινδία, Ιαπωνία και Η.Π.Α, ενώ αντιπροσωπεύουν το 42% της παγκόσμιας ζήτησης ελέγχουν μόνο το 4% των παγκόσμιων αποθεμάτων. Η συγκεκριμένη ασυμμετρία ενδέχεται να πυροδοτήσει ανταγωνισμούς και συγκρούσεις, σε παγκόσμια κλίμακα και ιδιαίτερα στην ευρύτερη περιοχή του Ινδικού και Ειρηνικού ωκεανού, λόγω της ύπαρξης στην περιοχή της Κίνας και της Ινδίας, που εμφανίζουν υψηλούς ρυθμούς οικονομικής ανάπτυξης, αλλά και των αραβικών πετρελαιοπαραγωγών κρατών που ενδέχεται να καλύψουν, κατά το μεγαλύτερο ποσοστό, τις αυξανόμενες ενεργειακές απαιτήσεις των εν λόγω κρατών.

2.3. Θαλάσσια ασφάλεια

Ο όρος θαλάσσια ασφάλεια, εάν και υπό έννοια της κυριαρχίας επί των θαλασσίων οδών εμφανίζεται στο πεδίο των διεθνών σχέσεων από τα από τα χρόνια της αρχαιότητας, εντούτοις επανήλθε στο επίκεντρο σχετικά πρόσφατα. Γεγονότα όπως η τρομοκρατική επίθεση της 11ης Σεπτεμβρίου 2001, η έξαρση της πειρατείας στις ακτές της Σομαλίας την περίοδο 2008-2011, οι συγκρούσεις κρατών με αφορμή διεκδικήσεις για την κυριαρχία σε νησιωτικά συμπλέγματα και θαλάσσιες περιοχές, όπως στη Ανατολική και Νότια Σινική θάλασσα (Johansson, 2013) και η επιδίωξη κρατών για απόκτηση ναυτικών δυνάμεων με δυνατότητα προβολής ισχύος στην ανοικτή θάλασσα καθώς και ο μεταξύ τους ανταγωνισμός (Brewster et al., 2016) συνετέλεσαν ώστε να αποτελέσει η ασφάλεια στο θαλάσσιο περιβάλλον αντικείμενο μελέτης καθώς και να συμπεριληφθεί είτε ως κομμάτι είτε ως ξεχωριστή στρατηγική στην ατζέντα διεθνών οργανισμών και κρατών (African Union, 2014· European Union, 2014· NATO, 2011· UK, 2014).

Ο προσδιορισμός της σημασίας και του περιεχόμενου της θαλάσσιας ασφάλειας υπόκειται σε προσεγγίσεις διαφορετικής οπτικής και δεν διαφαίνεται να υπάρχει κοινώς αποδεκτός ορισμός (Klein, 2011). Μια πρώτη προσέγγιση επιχειρεί να θέσει την θαλάσσια ασφάλεια στο επίκεντρο ενός πλαισίου αποτελούμενο από υπάρχουσες έννοιες, όπου τα επιμέρους χαρακτηριστικά τους δημιουργούν ένα πλέγμα αλληλεπιδράσεων οριοθετώντας τον όρο. Στις ανωτέρω έννοιες πρωταρχικό ρόλο κατέχουν το θαλάσσιο περιβάλλον, η οικονομική ανάπτυξη, η εθνική ασφάλεια και η ανθρώπινη επιβίωση (Bueger, 2015). Περεταίρω ανάλυση των εν λόγω πεδίων αναδεικνύει δραστηριότητες που εντάσσονται στο πεδίο ενδιαφέροντος της θαλάσσιας ασφάλειας, με κυριότερες τους κανόνες ναυσιπλοΐας, την κλιματική αλλαγή, την πειρατεία, τις παράνομες θαλάσσιες δραστηριότητες όπως το λαθρεμπόριο, η παράνομη διακίνηση όπλων, το εμπόριο λευκής σαρκός και το δουλεμπόριο, την αλιεία, την προστασία της βιωσιμότητας του θαλάσσιου περιβάλλοντος και των παραθαλάσσιων πληθυσμών, την προβολή ναυτικής ισχύος και τις διακρατικές συγκρούσεις.

Σύμφωνα με άλλη προσέγγιση, που εστιάζει στις ζυμώσεις σε επίπεδο διαμόρφωσης πολιτικής, οι οποίες αναδεικνύουν και προσδιορίζουν απειλές κατά της ασφάλειας και των προτεραιοτήτων που θέτει κάθε κράτος, οργανισμός ή φορέας για την επίτευξη της, το πλαίσιο της θαλάσσιας ασφάλειας δύναται να καθοριστεί από

απειλές οι οποίες εκδηλώνονται εναντίον παραμέτρων που διαμορφώνουν το θαλάσσιο περιβάλλον (Weaver & Buzan, 1998) . Η έκθεση με τίτλο Ωκεανοί και το Δίκαιο της Θάλασσας (Oceans and the law of the sea, 2008) του Γενικού Γραμματέα του Ο.Η.Ε επιχειρεί να θέσει ένα κοινώς αποδεκτό πλαίσιο με την αναφορά συγκεκριμένων απειλών όπως πειρατεία και ένοπλη ληστεία, τρομοκρατικές πράξεις, παράνομη διακίνηση και λαθρεμπόριο όπλων μαζικής καταστροφής, ναρκωτικών και ανθρώπων, παράνομη αλιεία και ηθελημένη καταστροφή του θαλάσσιου περιβάλλοντος (United Nations, 2008). Παράλληλα διεθνείς οργανισμοί και κράτη έχουν προβεί σε δημοσίευση επίσημων κειμένων αναφορικά με τη χάραξη στρατηγικής με στόχο την ασφάλεια στο θαλάσσιο περιβάλλον, όπως η Ευρωπαϊκή Ένωση (European Union, E.U) με την Στρατηγική Θαλάσσιας Ασφάλειας (Maritime security strategy, 2014) και το Ηνωμένο Βασίλειο (United Kingdom, U.K) με την Εθνική Στρατηγική για τη Θαλάσσια Ασφάλεια, ενσωματώνοντας και εμπλουτίζοντας τις ανωτέρω απειλές αλλά και θέτοντας νέες. Πιο συγκεκριμένα, η Ε.Ε εντάσσει στις απειλές, μεταξύ άλλων, την τρομοκρατία και κάθε παράνομη ενέργεια που εκδηλώνεται στη θάλασσα και σε λιμάνια, ενάντια σε πλοία, φορτία, πληρώματα και επιβάτες, εγκαταστάσεις λιμένος, σημαντικές θαλάσσιες και ενεργειακές υποδομές, συμπεριλαμβανομένου και των κυβερνοεπίθεσεων. Επιπλέον ως απειλή θεωρούνται επιπτώσεις στο σύστημα θαλασσίων μεταφορών, προερχόμενες από φυσικά αίτια, όπως η κλιματική αλλαγή ή ως αποτέλεσμα ανθρώπινης δραστηριότητας και ακραίων γεγονότων (European Union, 2014). Αντίστοιχα, το Ηνωμένο Βασίλειο θεωρεί ως απειλή κατά της θαλάσσιας ασφάλειας τη μη προσβασιμότητα στις διεθνείς θαλάσσιες εμπορικές οδούς (Sea Lines of Communications, SLOCs) λόγω πολέμου, εγκληματικότητας, πειρατείας ή αλλαγής των διεθνών κανονισμών όπως επίσης και την διεξαγωγή κυβερνοεπίθεσεων ενάντια σε εμπορικά πλοία και θαλάσσιες υποδομές (UK, 2014).

Τέλος ο όρος θαλάσσια ασφάλεια δύναται να προσδιοριστεί, ως αποτέλεσμα ενεργειών, μέσω των πράξεων των διαφόρων δρώντων, όπως διεθνείς οργανισμοί και κράτη, στο πλαίσιο επίτευξης των στόχων τους αναφορικά με την έννοια της ασφάλειας. Η εν λόγω προσέγγιση εστιάζει εξίσου τόσο στις δράσεις όσο και στα χρησιμοποιούμενα μέσα. Ο Διεθνής Οργανισμός Ναυσιπλοΐας (International Maritime Organization, IMO) θέσπισε ως Επίγνωση επί του Θαλασσίου Περιβάλλοντος (Maritime Domain Awareness, MDA) την πληροφόρηση αναφορικά με κάθε δραστηριότητα που σχετίζεται με το θαλάσσιο περιβάλλον και μπορεί να έχει

αντίκτυπο στην ασφάλεια, την οικονομία και το περιβάλλον (IMO, 2010). Απορρέουσες ενέργειες θεωρούνται η παρακολούθηση μέσω ραντάρ και δορυφόρων, η τήρηση βάσεων δεδομένων και η ανταλλαγή πληροφοριών μεταξύ οργανισμών και κρατών. Συνεπώς οι θαλάσσιες περιπολίες, οι επιθεωρήσεις σε ύποπτα πλοία, οι συλλήψεις και προσαγωγές για παραβίαση διεθνών κανονισμών, η ναυτική διπλωματία, η προβολή ναυτικής ισχύος στις ανοικτές θάλασσες, η διεξαγωγή συνεδρίων συναφούς θεματολογίας, η τυποποίηση πρακτικών ασφαλείας επί πλοίων και λιμενικών εγκαταστάσεων καθώς και η ανάληψη συλλογικών δράσεων στο θαλάσσιο περιβάλλον φαίνεται να ορίζουν τη θαλάσσια ασφάλεια (Bueger, 2015).

Η θαλάσσια ασφάλεια είναι έννοια που έχει έντονη γεωπολιτική χροιά. Πέραν από τη γεωγραφική διάσταση, η οποία είτε με άμεσο είτε με έμμεσο τρόπο, επηρεάζει την υιοθέτηση πρακτικών αναφορικά με τη θαλάσσια ασφάλεια, η πολιτική κατεύθυνση και βούληση, οι δυνατότητες προβολής ισχύος και η διάχυση σε περιφερειακή ή παγκόσμια κλίμακα των επιπτώσεων των απειλών που προέρχονται από το θαλάσσιο περιβάλλον, ωθούν κράτη και διεθνείς οργανισμούς, όπως η Ε.Ε, να επιχειρούν εκτός των συνόρων τους, σε θαλάσσιες ζώνες τις οποίες χαρακτηρίζουν ως ζωτικής σημασίας για την προάσπιση της ασφάλειας και των συμφερόντων τους (Germond, 2015). Ως απώτεροι στόχοι τίθενται η ελευθερία της ανοικτής θάλασσας, η προάσπιση των παγκόσμιων αγαθών, η αστυνόμευση των ωκεανών και η χρηστή διακυβέρνηση των θαλασσών.

2.4. Κυβερνοαπειλές στο θαλάσσιο περιβάλλον

Η διεθνής θαλάσσια κοινότητα αποτελεί ένα μωσαϊκό διασυνδέσεων και απαρτίζεται από αλληλοσυμπληρούμενους και αλληλοεξαρτώμενους οργανισμούς. Στους κόλπους της εντάσσονται το σύνολο του παγκόσμιου στόλου, οι ναυτιλιακές εταιρείες, οι λιμένες και συναφείς υπηρεσίες όπως υπηρεσίες διαχείρισης λιμένος, οι αποβάθρες, οι τερματικοί σταθμοί φορτοεκφόρτωσης αγαθών, οι υδατοφράκτες, τα κανάλια, οι αποβάθρες εξόρυξης, οι παγκόσμιοι ή περιφερειακοί ναυτιλιακοί οργανισμοί όπως ο IMO, οι ασφαλιστικές εταιρείες, οι εθνικοί συναφείς διοικητικοί φορείς, η ακτοφυλακή και οι ναυτικές δυνάμεις των κρατών.

Η αλληλεπίδραση μεταξύ των ανωτέρω είναι καθημερινή, με τη συνεχή και αξιόπιστη ροή πληροφορίας, πρωτίστως μέσω του διαδικτύου (internet), να αποτελεί απαραίτητη προϋπόθεση για την ομαλή λειτουργία του ευρύτερου κλάδου.

Παράλληλα όμως με την ώθηση και τις διευκολύνσεις που παρέχονται μέσω του διαδικτύου, η ναυτιλιακή κοινότητα εκτίθεται στους κινδύνους που απορρέουν από τη χρήση του, τις επονομαζόμενες κυβερνοαπειλές (cyber threats), τόσο σε επίπεδο κρατικών δομών, οργανισμών και πολυεθνικών επιχειρήσεων όσο και στο χαμηλότερο δυνατό επίπεδο, δηλαδή στο πλοίο. Ειδικότερα το πλοίο, καθόσον αποτελεί μονάδα που δρα αυτόνομα σε απομονωμένο περιβάλλον και εξαρτάται σε μεγάλο βαθμό από τα επικοινωνιακά συστήματα και τη ροή πληροφοριών από το εξωτερικό περιβάλλον, εκτίθεται σε ευρύ φάσμα κυβερνοαπειλών.

Ως κυβερνοαπειλή ορίζεται η μη εξουσιοδοτημένη προσπάθεια πρόσβασης σε ένα σύστημα ελέγχου ή δίκτυο, μέσω της χρήσης ενός διαύλου ροής πληροφοριών (Γιαννακόπουλος, 2010). Μπορεί να είναι ένα προβλέψιμο ή μη περιστατικό που αποσκοπεί ή επιφέρει αρνητικές συνέπειες για τον οργανισμό και εκδηλώνεται με τη μορφή κυβερνοεπιθέσεων (cyber attacks).

Οι δρώντες που δύνανται να επιτελέσουν κυβερνοεπιθέσεις στην θαλάσσια κοινότητα ποικίλουν καθώς επίσης και τα κίνητρα που τους ωθούν. Μερικοί από τους κυριότερους υπαίτιους κυβερνοεπιθέσεων και τα πιθανά κίνητρά τους παρατίθενται στη συνέχεια (IET, 2017· BIMCO, 2016):

α. Κράτη (states) και χρηματοδοτούμενοι από αυτά οργανισμοί (state sponsored actors). Τα κράτη χρησιμοποιούν τον κυβερνοχώρο για την συλλογή πληροφοριών, την κατασκοπεία, τη διατάραξη της ομαλής λειτουργίας των υποδομών και υπηρεσιών άλλων κρατών, την απορύθμιση του ευρύτερου συστήματος μεταφορών καθώς και την πρόκληση δυσλειτουργιών σε συγκεκριμένους τύπους πλοίων, με σκοπό την διατάραξη της λειτουργίας της οικονομίας και την υπονόμευση της ενεργειακής ασφάλειας.

β. Τρομοκρατικές οργανώσεις (terrorist groups). Εμφανίζουν παρόμοια κίνητρα με τα κράτη ενώ παράλληλα δύνανται να αποσκοπούν στην επίδειξη ικανοτήτων με σκοπό τον επηρεασμό της κοινής γνώμης, την πρόκληση φόβου και την απόκτηση οικονομικού οφέλους για τη χρηματοδότηση των δραστηριοτήτων τους.

γ. Εγκληματικές οργανώσεις (cyber criminals). Αποσκοπούν στην απόσπαση πληροφοριών με σκοπό είτε την πώληση τους στο πλαίσιο της βιομηχανικής κατασκοπείας είτε την απαίτηση λύτρων για τη μη διαρροή τους και την επαναφορά της λειτουργικότητας των συστημάτων του οργανισμού. Επιπρόσθετα δύνανται να

αποβλέπουν σε κλοπή, διεξαγωγή λαθρεμπορίου και παραποίηση δεδομένων μεταφοράς φορτίων.

δ. Ακτιβιστικές οργανώσεις (hacktivism). Με τελικό στόχο το πλοίο και τον οργανισμό που το διαχειρίζεται ή ακόμη και τον αποδέκτη των υπηρεσιών έχουν ως σκοπό την παρεμπόδιση της επιτελούμενης λειτουργίας, την προσβολή της φήμης και αξιοπιστίας του στόχου τους και την προώθηση της πολιτικής τους ατζέντας μέσω της προβολής από τα Μέσα Μαζικής Ενημέρωσης (ΜΜΕ).

ε. Εμπορικοί ανταγωνιστές (commercial competitors). Χρησιμοποιώντας ίδιους πόρους ή μέσω τρίτων διεξάγουν βιομηχανική κατασκοπεία και πλήττουν την φήμη και αξιοπιστία των ανταγωνιστών τους.

στ. Εσωτερικοί χρήστες (Individuals). Υπάγονται σε δύο γενικές κατηγορίες, εκείνους χωρίς πρόθεση (unintentional insiders) και εκείνους με πρόθεση (intentional insiders). Οι μεν πρώτοι δεν έχουν κίνητρο να βλάψουν τον οργανισμό αλλά αποτελούν άθελα τους κυβερνοαπειλή μέσω της μη εξουσιοδοτημένης χρήσης συστημάτων ή της μη τήρησης των προβλεπόμενων διαδικασιών ασφαλείας. Οι δεύτεροι μπορεί να είναι υπάλληλοι του οργανισμού ή συνδεόμενες επιχειρήσεις όπως εταιρείες υποστήριξης λογισμικού με πρόσβαση σε συστήματα και επιδιώκουν να παρεμποδίσουν την λειτουργία, να υποκλέψουν ή να παραποιήσουν πληροφορίες, να αποκομίσουν οικονομικά οφέλη και να πλήξουν την φήμη του οργανισμού.

ζ. Οι μεμονωμένοι Χάκερς και ομάδες αυτών (Hackers-Crackers). Βασικό τους κίνητρο αποτελεί η πρόκληση να αποδείξουν αλλά και να βελτιώσουν τις ικανότητες τους ενώ σε κάποιες περιπτώσεις αποσκοπούν σε οικονομικά οφέλη από την πώληση δεδομένων ή την απαίτηση λύτρων για την επανάκτησή τους.

Οι κυβερνοεπιθέσεις κατηγοριοποιούνται βάση πληθώρας κριτηρίων όπως ο σκοπός, η πρόθεση, το νομικό καθεστώς που διέπει την απειλή, η δριμύτητα της επίθεσης και η φύση του προσβαλλόμενου δικτύου (Uma & Padmavathi, 2013). Αναφορικά με τη διάκριση βάση σκοπού, οι κυβερνοεπιθέσεις κατηγοριοποιούνται σε επιθέσεις αναγνώρισης (reconnaissance attacks) που πλήττουν αδύναμα σημεία του συστήματος με κύριο σκοπό την χαρτογράφηση του για μελλοντική εκμετάλλευση, σε επιθέσεις πρόσβασης (access attacks) για πρόσκτηση ευαίσθητων πληροφοριών προς διατάραξη της λειτουργίας του συστήματος ή για παραποίηση, πώληση και απαίτηση καταβολής λύτρων και σε επιθέσεις άρνησης παροχής υπηρεσίας (Denial of service attacks, DoS) με στόχο την διακοπή της λειτουργίας του συστήματος ή την επιβράδυνση της σε βαθμό ικανό ώστε να αδυνατεί να εκπληρώσει το σκοπό του.

Εξίσου σημαντική διάκριση αποτελεί το νομικό καθεστώς που διέπει την απειλή με επιμέρους κατηγορίες το κυβερνοέγκλημα, την κατασκοπεία, την τρομοκρατία και τον κυβερνοπόλεμο. Ανεξάρτητα από την εκάστοτε διάκριση, κάποιες από τις συνηθέστερα χρησιμοποιούμενες τεχνικές εκδήλωσης των κυβερνοεπιθέσεων είναι το κακόβουλο πρόγραμμα (Malware), το κατασκοπευτικό πρόγραμμα (Spyware), ο ιός (Virus), το σκουλήκι (Worm), ο δούρειος ίππος (Trojan), η πλαστογράφηση (Spoofing), η λογική βόμβα (Logic bomb), το ψάρεμα (Phishing), η κατανεμημένη επίθεση άρνησης υπηρεσίας (Distributed denial of service attack, DDoS), η εκμετάλλευση των άγνωστων τρωτοτήτων ενός συστήματος (Zero Day Vulnerabilities) κ.α.

2.5. Τρωτότητες συστημάτων εμπορικών πλοίων σε κυβερνοεπιθέσεις

Το πλοίο ανάλογα με το μέγεθος και τον σκοπό του χαρακτηρίζεται από αντίστοιχο αριθμό και πολυπλοκότητα όσον αφορά τα συστήματα που το απαρτίζουν. Πέραν των βασικών συστημάτων που ρυθμίζουν λειτουργικές παραμέτρους, όπως συστήματα προώσεως και ενέργειας, ναυτιλίας, διαχείρισης φορτίου και ασφαλείας, το πλοίο αποτελεί μια μονάδα που δρα, ως επί το πλείστον, σε απομονωμένο περιβάλλον με μόνη σύνδεση με τη στεριά μέσω διαφόρων επικοινωνιακών διαύλων που επιτρέπουν την ανταλλαγή ψηφιακών και φωνητικών δεδομένων. Η έκθεση αυτών των συστημάτων στον κυβερνοχώρο τα καθιστά εκτεθειμένα σε κυβερνοαπειλες, παράλληλα με άλλες τρωτότητες, με κυριότερη την προσβολή λογισμικού μέσω φυσικών σημείων πρόσβασης στο εκάστοτε σύστημα όπως θύρες ενιαίου σειριακού διαύλου (Universal Serial Bus, USB). Επιπρόσθετα η διασύνδεση των διαφόρων συστημάτων καθιστά ευάλωτη σε κυβερνοεπίθεση το σύνολο της αλληλουχίας των αλληλοϋποστηριζόμενων συστημάτων. Προσδιορίζοντας το πλοίο με γνώμονα τη συγκεκριμένη οπτική μπορεί να ισχυριστεί κανείς ότι αποτελεί ένα σύστημα συστημάτων που λειτουργεί σε απομονωμένο περιβάλλον. Τα κυριότερα εγκατεστημένα σε πλοία συστήματα τα οποία εμφανίζονται ως ευάλωτα σε κυβερνοεπιθέσεις παρατίθενται στη συνέχεια, σύμφωνα με τις κατευθυντήριες οδηγίες αναφορικά με τη κυβερνοασφάλεια επί πλοίων όπως αυτές εξεδόθησαν από το Βαλτικό Διεθνές Ναυτιλιακό Συμβούλιο (Baltic and International Maritime Council, BIMCO) και υιοθετήθηκαν από τον IMO (BIMCO, 2016):

α. Συστήματα επικοινωνιών τόσο ενδοεπικοινωνίας όσο και εξωτερικών επικοινωνιών όπως δορυφορικά συστήματα επικοινωνίας, ασύρματα δίκτυα (Wireless networks, WLANs), μεγαφωνικά συστήματα (Public Address Systems), εσωτερικό τηλεφωνικό δίκτυο, συστήματα επικοινωνίας στις ζώνες Πολύ Υψηλών Συχνοτήτων (Very High Frequency, VHF), το δορυφορικό σύστημα INMARSAT.

β. Συστήματα γεφύρας όπως το Σύστημα Ηλεκτρονικής Απεικόνισης Χαρτών και Πληροφοριών (Electronic Chart Display Information System, ECDIS), τα Συστήματα Δυναμικού Προσδιορισμού Θέσης (Dynamic Positioning systems, DP), το Παγκόσμιο Σύστημα Προσδιορισμού θέσης (Global Positioning System, GPS), το Σύστημα Αυτόματης Ταυτοποίησης (Automatic Identification System, AIS), το Σύστημα Ναυτιλιακού Κινδύνου Ασφάλειας (Global Maritime Distress and Safety System, GMDSS), ο ραδιοεντοπιστής (Radio Detection and Ranging, RADAR), το Σύστημα Καταγραφής Δεδομένων Ταξιδιού (Voyage Data Recorder, VDR), το Σύστημα Συναγερμού Γεφύρας (Bridge Navigational Watch Alarm System, BNWAS).

γ. Συστήματα βιομηχανικού ελέγχου (Industrial Control Systems, ICS) λειτουργίας μηχανικών και ηλεκτρικών συστημάτων όπως κύριες μηχανές, γεννήτριες, βοηθητικά μηχανήματα, δεξαμενές ερμάτων, δίκτυο καυσίμου, σύστημα προώσεως, σύστημα συναγερμού, σύστημα διαχείρισης φορτίου (Cargo Management Systems, CCR), σύστημα υγροποίησης αερίου.

δ. Συστήματα ελέγχου όπως το σύστημα παρακολούθησης (Closed-Circuit Television, CCTV) και συστήματα ασφαλείας (όπως Shipboard Security Alarm Systems, SSAS).

ε. Συστήματα Εξυπηρέτησης και Διαχείρισης Επιβαινόντων (Passenger Servicing and Management Systems, PSMS) όπως το Σύστημα Διαχείρισης Περιουσίας (Property Management System, PMS), η παρεχόμενη πρόσβαση στο διαδίκτυο μέσω Wi-Fi ή LAN δικτύου, το σύστημα κλιματισμού, το σύστημα Ιατρικών Αρχείων Επιβατών (Medical Records) καθώς και το σύστημα Τηλεϊατρικής (TeleMed).

στ. Διάφορα συστήματα υποδομής όπως Virtual Private Network (VPN), Virtual Local Area Network (VLAN).

Από τα ανωτέρω συστήματα κάποια είναι δυνατό να ενταχθούν σε περισσότερες από μία κατηγορίες και σε πολλές περιπτώσεις συστήματα της ιδίας ή

διαφορετικών κατηγοριών αλληλεπιδρούν ανταλλάσοντας δεδομένα σε πραγματικό χρόνο (IET, 2017).

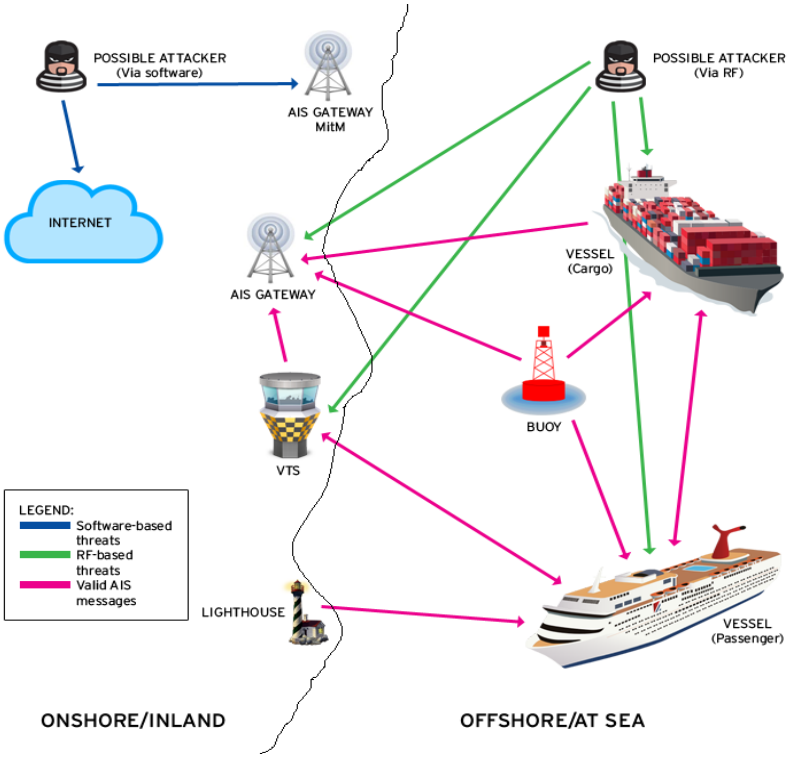
Οι τρωτότητες των ναυτικών συστημάτων οφείλονται ως επί το πλείστον σε δομικά χαρακτηριστικά τους όπως παραλείψεις και αβλεψίες κατά τον σχεδιασμό, την κατασκευή και λειτουργία τους, την ύπαρξη πολλαπλών κόμβων διασύνδεσης τόσο μεταξύ τους όσο και με την ξηρά και τη μικρή σημασία που απέδιδε έως πρόσφατα η ναυτιλιακή κοινότητα στην έννοια της κυβερνοασφάλειας τόσο στο κατασκευαστικό όσο και στο επιχειρησιακό περιβάλλον. Ακολουθεί η ανάλυση των τρωτοτήτων βασικών ναυτικών συστημάτων και συγκεκριμένα του Συστήματος Αυτόματης Ταυτοποίησης (Automated Identification System, AIS), του Παγκόσμιου Συστήματος Προσδιορισμού θέσης (Global Positioning System, GPS), του Συστήματος Ηλεκτρονικής Απεικόνισης Χαρτών και Πληροφοριών (Electronic Chart Display Information System, ECDIS) και του Βιομηχανικό Συστήματος Ελέγχου (Industrial Control System, ICS).

2.5.1. Σύστημα Αυτόματης Ταυτοποίησης

Το Σύστημα Αυτόματης Ταυτοποίησης (Automated Identification System, AIS) είναι ένα ψηφιακό σύστημα ανταλλαγής πληροφοριών εκπεμπόμενων στην συχνότητα VHF, μέσω δύο καναλιών στους 161.975MHz και 162.025MHz, που επιτρέπει την επικοινωνία μεταξύ πλοίων και σταθμών AIS εγκατεστημένων στη στεριά, συνήθως σε φάρους ή σε Υπηρεσίες Εξυπηρέτησης Κυκλοφορίας Πλοίων (Vessel Traffic Services, VTS), με σκοπό την αλληλοενημέρωση των ναυτιλλομένων, την ασφάλεια της ναυσιπλοΐας, τον έλεγχο της θαλάσσιας κυκλοφορίας και τον αποτελεσματικότερο συντονισμό επιχειρήσεων έρευνας και διάσωσης. Ο IMO με το ψήφισμα A.917(22) στο πλαίσιο των τροποποιήσεων που επήλθαν στη Διεθνή Σύμβαση για την Ασφάλεια της Ζωής στη Θάλασσα (International Convention for the Safety of Life at Sea, SOLAS), θέτει ως απαιτούμενο την εγκατάσταση του συστήματος AIS σε όλους τους τύπους πλοίων. Οι πληροφορίες που ανταλλάσσονται μέσω του AIS διακρίνονται σε στατικές, οι οποίες δε δύναται να μεταβληθούν παρά μόνο κατόπιν μεταβίβασης της ιδιοκτησίας ή μετασκευής και αφορούν στα στοιχεία ταυτοποίησης του πλοίου όπως ο αριθμός αναγνώρισης IMO, το διεθνές διακριτικό σήμα και όνομα, ο Αριθμός Ταυτοποίησης Κινητών Θαλασσίων Υπηρεσιών (Maritime Mobile Service Identity, MMSI), οι διαστάσεις και ο τύπος του πλοίου, σε

δυναμικές που αφορούν σε μεταβαλλόμενες πληροφορίες όπως η θέση του πλοίου με ένδειξη περί της σχετικής ακρίβειας, η ταχύτητα, η πορεία και η κατάσταση πλεύσης και σε πληροφορίες ναυσιπλοΐας όπως το βύθισμα, το είδος του φορτίου, ο λιμένας προορισμού και τα σημεία διέλευσης κατά τον πλου (IMO Resolution A.917(22), 2002). Τα ανωτέρω στοιχεία απεικονίζονται σε πραγματικό χρόνο μέσω του ECDIS με σκοπό να αντιλαμβάνεται ο ναυτιλλόμενος τη θέση και τη σχετική κίνηση των υπολοίπων πλοίων ακόμη και αν δεν τα έχει εντοπίσει με άλλα μέσα, όπως οπτικά ή με τη χρήση του RADAR. Η λήψη των δεδομένων από τα πλοία που βρίσκονται στην ανοικτή θάλασσα επιτυγχάνεται με αναμεταδότες εγκατεστημένους σε νησιά ή μέσω δορυφόρων. Η συγκέντρωση και σύνθεση των εκπεμπόμενων δεδομένων γίνεται σε σταθμούς AIS στην ξηρά, οι οποίοι διαμοιράζουν την διαμορφούμενη εικόνα σε πραγματικό χρόνο μέσω του διαδικτύου (AIS online). Συνεπώς, κάθε χρήστης με δυνατότητα σύνδεσης στο διαδίκτυο έχει πρόσβαση σε πραγματικό χρόνο και σε παγκόσμια κλίμακα στα στοιχεία, στη θέση και στην κίνηση όλων των πλοίων που απεικονίζονται στο σύστημα AIS.

Η τρωτότητα του AIS έγκειται στο γεγονός ότι όλα τα εκπεμπόμενα δεδομένα λαμβάνονται υπόψη ως αληθή καθώς δεν υφίστανται κρυπτογράφηση των εκπεμπόμενων πληροφοριών καθώς και διαδικασίες ελέγχου της αυθεντικότητας, ακεραιότητας και εγκυρότητας τους (Bothur, Zeng & Valli, 2017). Το ίδιο το πλοίο μπορεί να εκπέμψει παραπλανητικά και αναληθή στοιχεία, καθώς οι πληροφορίες ναυσιπλοΐας εισάγονται στο AIS από το προσωπικό του. Επίσης παρατηρείται συχνά το φαινόμενο πλοία να απενεργοποιούν το AIS σε σημεία υψηλού κινδύνου κατά την πορεία τους ως μέτρο κατά της πειρατείας (Cyberkeel, 2014). Επιπρόσθετα η διαμορφούμενη εικόνα του AIS είναι διαθέσιμη μέσω ιστοσελίδων διανομής, που στερούνται ισχυρών πρωτοκόλλων ασφαλείας και συνεπώς είναι ευάλωτες σε κυβερνοεπιθέσεις, οπότε είναι δυνατόν να παραποιηθούν τα διατιθέμενα στοιχεία (Trend Micro, 2014).



Σχήμα 2.1. Πιθανές περιπτώσεις επιθέσεων στο σύστημα AIS (Trend Micro, 2014)

Επιθέσεις κατά της εύρυθμης λειτουργίας του ευρύτερου πλέγματος λειτουργίας του συστήματος AIS μπορούν να γίνουν, με σχετικά φθηνό τεχνικό εξοπλισμό, είτε μέσω του διαδικτύου είτε μέσω των ραδιοσυχνοτήτων (radiofrequencies, RF) που χρησιμοποιούνται για τη μετάδοση των πληροφοριών (Middleton, 2014), όπως φαίνεται στο Σχήμα 2.1. Επιδιώξεις των επιθέσεων αποτελούν η προσποίηση ταυτότητας (spoofing) που αποσκοπεί στην αληθοφανή προσομοίωση μίας μη υπαρκτής μονάδας AIS, ο έλεγχος των δεδομένων (hijacking) με στόχο την τροποποίηση των εκπεμπόμενων δεδομένων υπαρχόντων μονάδων AIS και η διακοπή της διαθεσιμότητας (availability disruption) υπαρχόντων μονάδων AIS (Trend Micro, 2014). Η επίτευξη των ανωτέρω δύναται να επιφέρει τα ακόλουθα αποτελέσματα (Cyberkeel, 2014· Trend Micro, 2014):

α. Τροποποίηση των στοιχείων του πλοίου όπως ταυτότητα, θέση, φορτίο, ταχύτητα και πορεία με σκοπό την παραπλάνηση των αρχών επιβολής του νόμου και την απρόσκοπτη κίνησή του για την αποκόμιση κέρδους από παράνομες δραστηριότητες όπως μεταφορά όπλων μαζικής καταστροφής και εμπόριο ναρκωτικών.

β. Δημιουργία "πλοίου-φάντασμα" ("ghost-ship") οπουδήποτε στην υφήλιο, που να θεωρείται από το σύστημα υπαρκτό, με αποτέλεσμα η κίνησή του να δημιουργεί παραπλανητικές συνθήκες συναγερμού ως προς επικείμενη σύγκρουσή του με άλλα πλοία με σκοπό την παρέκκλιση από την πορεία τους. Ακόμη μπορεί να χρησιμοποιηθεί για την προσομοίωση πολεμικού πλοίου εντός των χωρικών υδάτων έτερου κράτους με σκοπό την πρόκληση εντάσεως στις διμερείς σχέσεις.

γ. Εκπομπή ψευδών ειδοποιήσεων δυσμενών καιρικών φαινομένων με σκοπ ό την εκτροπή της ναυτιλιακής κίνησης από μια γεωγραφική περιοχή ή την παραπλάνηση πλοίων ώστε να διέλθουν από μια επιλεγμένη γεωγραφική περιοχή.

δ. Εκπομπή ψευδών ειδοποιήσεων τύπου "Άνθρωπος στη Θάλασσα" (Man Overboard, MOB) επιφέροντας σύγχυση και παρέκκλιση πλοίων από την πορεία τους με σκοπό την πειρατεία.

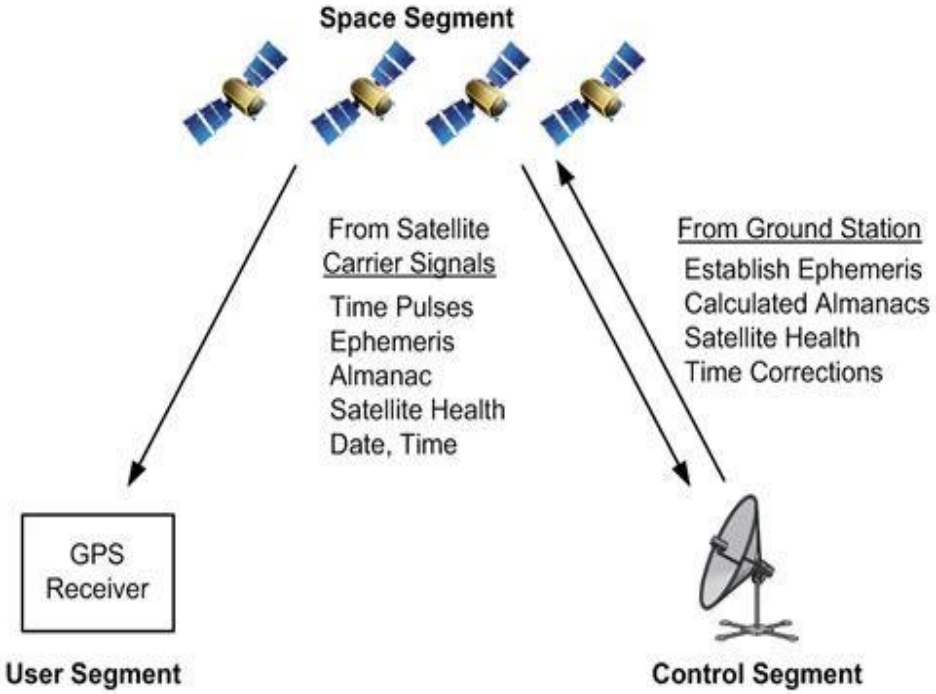
ε. Προσποίηση των αρχών επιβολής νόμου με σκοπό την χειραγώγηση πλοίων ώστε να προβούν σε ενέργειες που τα καθιστούν ευάλωτα σε επιθέσεις όπως απενεργοποίηση του συστήματος AIS πριν από επικείμενη επίθεση.

στ. Αύξηση της συχνότητας εκπομπής πραγματικών ή ψευδών δεδομένων και κατακλυσμό του συστήματος με πληροφορίες με σκοπό είτε την δυσχέρεια διαχωρισμού πραγματικών και παραπλανητικών δεδομένων είτε την υπερφόρτωση του συστήματος προκειμένου να τεθεί εκτός λειτουργίας στο πλαίσιο επίθεσης DoS.

ζ. Εκπομπή ψευδών πληροφοριών από μονάδες υποβοήθησης ναυτιλίας που φέρουν μονάδες AIS, όπως σημαντήρες και φάροι, σε αποτέλεσμα την εκτέλεση επικίνδυνων ελιγμών σε λιμένες με κίνδυνο πρόκλησης καταστροφών σε άλλα πλοία και λιμενικές εγκαταστάσεις.

2.5.2. Παγκόσμιο Σύστημα Προσδιορισμού Θέσης

Το Παγκόσμιο Σύστημα Προσδιορισμού θέσης (Global Positioning System, GPS) είναι ένα αυτόματο σύστημα προσδιορισμού θέσης με ακρίβεια και σε πραγματικό χρόνο βασιζόμενο σε ένα δίκτυο δορυφόρων. Ξεκίνησε ως πρόγραμμα με την ονομασία NAVSTAR GPS των ενόπλων δυνάμεων των ΗΠΑ με σκοπό την υποβοήθηση της ναυσιπλοΐας πολεμικών πλοίων και σταδιακά η χρήση του επεκτάθηκε σε άλλους τομείς όπως η ναυτιλία, οι τηλεπικοινωνίες, η αεροπλοΐα και οι μεταφορές. Το GPS αποτελείται από το πλέγμα των δορυφόρων, το τμήμα ελέγχου και τους δέκτες, όπως φαίνεται στο Σχήμα 2.2 (Achanta, Watt & Sagen, 2015).



Σχήμα 2.2. Τμήματα του συστήματος GPS

(https://selinc.com/solutions/synchrophasors/report/111935/)

Με περισσότερους από είκοσι τέσσερις δορυφόρους να κινούνται σε έξι τροχιές το διαμορφούμενο δίκτυο προσφέρει παγκόσμια κάλυψη έτσι ώστε τουλάχιστον 6 δορυφόροι να είναι πάντα ταυτόχρονα ορατοί από κάθε σημείο της επιφάνειας της Γης. Οι δορυφόροι εκπέμπουν πληροφορίες σε RF συχνότητες, με την ονομασία L1 οι οποίες αφορούν σε όλες τις εφαρμογές μεταξύ των οποίων και η ναυτιλία πλην των στρατιωτικών εφαρμογών, όπου οι εκπεμπόμενες συχνότητες L2 υπόκεινται σε κρυπτογράφηση. Το τμήμα ελέγχου αλληλεπιδρά με τους δορυφόρους ρυθμίζοντας τις παραμέτρους και ελέγχοντας τη λειτουργία τους ενώ τα δεδομένα των δορυφόρων λαμβάνονται από δέκτες που αποτελούνται από μια εγκατεστημένη κεραία λήψης σήματος GPS συνδεδεμένη σε έναν υπολογιστή με ενσωματωμένη μονάδα απεικόνισης. Οι εκπεμπόμενες πληροφορίες τουλάχιστον τριών δορυφόρων επεξεργάζονται από τον υπολογιστή και απεικονίζονται στην οθόνη ως στοιχεία εξαιρετικής ακρίβειας αναφορικά με τη γεωγραφική θέση (συντεταγμένες και υψόμετρο) καθώς και την ταχύτητα του δέκτη. Για τον υπολογισμό του χρόνου αξιοποιούνται δεδομένα από έναν ακόμη δορυφόρο. Σε επίπεδο πλοίου, μέσω του συστήματος GPS απεικονίζονται ηλεκτρονικά η θέση και η ταχύτητά του και θεωρείται βασικό σύστημα ναυτιλίας. Παράλληλα μέσω διασύνδεσης οι πληροφορίες

του είναι αξιοποιήσιμες και από άλλα συστήματα γεφύρας του πλοίου όπως το ECDIS, το AIS και το GNSS.

Η τρωτότητα του συστήματος GPS έγκειται στο γεγονός ότι δεν υφίστανται κρυπτογράφηση των εκπεμπόμενων δεδομένων για πολιτική χρήση, παρά μόνο για στρατιωτική, καθώς και διαδικασίες ελέγχου της αυθεντικότητας, ακεραιότητας και εγκυρότητας τους (Bhatti & Humphreys, 2016). Συνεπώς το GPS εμφανίζει τρωτότητες οι οποίες είναι εκμεταλλεύσιμες από κυβερνοεπιθέσεις που αποσκοπούν στην προσποίηση ταυτότητας (spoofing) ή στην παρεμβολή (jamming). Σε περίπτωση επίθεσης τύπου spoofing, η οποία είναι δύσκολο να εφαρμοστεί αλλά είναι τεχνικώς εφικτή, απαιτείται ακρίβεια στην προσομοίωση σήματος GPS στη συχνότητα L1. Με τη χρήση κατάλληλου εξοπλισμού ο επιτιθέμενος εκπέμποντας ελαφρώς ισχυρότερο σήμα από το υπάρχον, παραπλανά τον υπολογιστή του δέκτη, ο οποίος λαμβάνει ως αξιόπιστα παραποιημένα δεδομένα (Bhatti & Humphreys, 2016). Κατά την επίθεση με τη μέθοδο jamming, η οποία είναι υλοποιήσιμη με τη χρήση εξοπλισμού χαμηλού κόστους περί τα 100 δολάρια και με σχετική ευκολία ως προς την πρόσκτηση του, στόχο των επιτιθέμενων αποτελεί η παρεμπόδιση λήψης του δορυφορικού σήματος GPS (Grant et al., 2009· Bhatti & Humphreys, 2016).

Αμφότερες οι ανωτέρω μέθοδοι, προσβάλλοντας την ορθή λειτουργία του συστήματος και σε συνδυασμό με την αξιοποίηση των πληροφοριών του και από άλλα συστήματα γεφύρας όπως το AIS και το ECDIS, επιφέρουν την απεικόνιση στους ηλεκτρονικούς χάρτες ναυσιπλοΐας παραποιημένων ή στατικών στοιχείων τα οποία μέσω του AIS εκπέμπονται σε έτερα πλοία και αναπαρίστανται στις διαδικτυακές του πλατφόρμες. Συνεπώς, οι κυβερνοεπιθέσεις στο σύστημα GPS καθιστούν δυνατή τόσο την παραπλάνηση του πληρώματος, ειδικά σε ώρες μειωμένης παρουσίας προσωπικού στη γέφυρα, με σκοπό τον έλεγχο και εκτροπή της πορείας του πλοίου όσο και τη δημιουργίας σύγχυσης και ψευδούς εικόνας για την ναυσιπλοΐα σε επιλεγμένη θαλάσσια περιοχή.

2.5.3. Σύστημα Ηλεκτρονικής Απεικόνισης Χαρτών και Πληροφοριών

Το Σύστημα Ηλεκτρονικής Απεικόνισης Χαρτών και Πληροφοριών (Electronic Chart Display Information System, ECDIS) είναι ένα σύστημα απεικόνισης χαρτών και πληροφοριών ναυτιλίας σε ηλεκτρονική μορφή με τη χρήση

υπολογιστών που χρησιμοποιούν συνήθως παρωχημένο λογισμικό όπως Windows XP. Σύμφωνα με τον κανονισμό 19.2 επί του Κεφαλαίου V της SOLAS επιβάλλεται η εγκατάσταση του επί του συνόλου των επιβατικών αλλά και των πλοίων μεταφοράς εμπορευμάτων. Η εφαρμογή του πραγματοποιήθηκε υπό την αιγίδα του IMO με σκοπό την δυνατότητα πλήρους αντικατάστασης των παραδοσιακών ναυτιλιακών χαρτών και την υποβοήθηση των ναυτιλλομένων (IMO Resolution MCS.232(82), 2006). Στο ECDIS απεικονίζονται οι Ηλεκτρονικοί Ναυτιλιακοί Χάρτες (Electronic Navigational Charts, ENC) όπου γίνεται σύνθεση δεδομένων που λαμβάνονται από διάφορα συστήματα και συσκευές, τα οποία είναι συνδεδεμένα στο ECDIS, όπως το AIS, το GPS, το δρομόμετρο, η γυροπυξίδα, το βαθύμετρο, το RADAR και τα συστήματα αυτόματης πλοήγησης και κίνησης πηδαλίων. Ως αποτέλεσμα στην οθόνη του ECDIS υποτυπώνεται το σύνολο των βασικών στοιχείων του πλου όπως το στίγμα, η πορεία, η ταχύτητα, οι σχετικές θέσεις έτερων πλοίων και τα μετεωρολογικά δεδομένα.

Η τρωτότητα του συστήματος έγκειται εν πολλοίς στην απαίτηση τακτικής επικαιροποίησης των ναυτιλιακών χαρτών είτε μέσω ανανέωσης τους με ασύρματη σύνδεση του ECDIS στο διαδίκτυο είτε στην εισαγωγή των ενημερώσεων μέσω θυρών CD/USB (NCCGROUP, 2014). Και στις δύο περιπτώσεις είναι πιθανή η εκδήλωση κυβερνοεπίθεσης με χρήση κατάλληλου κακόβουλου λογισμικού το οποίο δύναται να αποσπάσει, να αντικαταστάσει, να τροποποιήσει και να διαγράψει δεδομένα καθώς και να προσβάλει όλα τα συνδεδεμένα συστήματα στο εσωτερικό δίκτυο του πλοίου, προκαλώντας δυσλειτουργίες ακόμη σε μηχανολογικά συστήματα. Επιπλέον η αξιοποίηση πληροφοριών από άλλα ευπρόσβλητα συστήματα, όπως τα AIS και GPS, καθιστά το ECDIS εκτεθειμένο και στις δικές τους εγγενείς τρωτότητες.

2.5.4. Βιομηχανικό Σύστημα Ελέγχου

Ο όρος Βιομηχανικό Σύστημα Ελέγχου (Industrial Control System, ICS) χρησιμοποιείται για το προσδιορισμό ηλεκτρονικών συστημάτων τα οποία αποτελούνται από διάφορα υποσυστήματα, όπως Συστήματα Εποπτείας Ελέγχου και Συγκέντρωσης Δεδομένων (Supervisory Control and Data Acquisition Systems, SCADA), και ελέγχουν την λειτουργία συσκευών και μηχανημάτων. Αυτοματοποιημένες ή εισαγόμενες από την χειριστή εντολές δίνονται στα επιμέρους

ελεγχόμενα μηχανήματα τοπικά ή μέσω κόμβων στο σύστημα καθορίζοντας τις παραμέτρους λειτουργίας τους. Παράλληλα δεδομένα από τα μηχανήματα ανατροφοδοτούν την εικόνα που έχει ο χειριστής σε πραγματικό χρόνο (US Department of Transportation, 2013). Σε επίπεδο πλοίου το ICS αποτελείται από υποσυστήματα όπως πρόωσης, πηδαλιουχίας, καυσίμου, διαχείρισης έρματος, ηλεκτρικά συστήματα, κλιματισμού, συστήματα ευστάθειας, φορτίου, εντοπισμού πυρκαγιάς, με σκοπό τον έλεγχο των επιμέρους λειτουργιών του πλοίου (Zaghloul, 2014). Τα ανωτέρω συστήματα τροφοδοτούν με δεδομένα ένα κεντρικό δίκτυο και διαμέσου μια κεντρική μονάδας ελέγχονται και αλληλοσυνδέονται. Το εν λόγω σύστημα περιέχει σημεία πρόσβασης, τους λεγόμενους κόμβους, μέσω των οποίων οι ναυτιλλόμενοι αποκτούν πρόσβαση στα επιμέρους στοιχεία του πλοίου. Η απαίτηση απόκτησης εικόνας σε πραγματικό χρόνο αναφορικά με τη λειτουργία μηχανολογικών συστημάτων που επηρεάζουν την ναυσιπλοΐα και την ασφάλεια οδηγεί στην διασύνδεση του ICS με τα συστήματα γέφυρας όπως το ECDIS, το GPS και το AIS. Παράλληλα δεδομένα από τα επιμέρους συστήματα του πλοίου αποστέλλονται μέσω του δικτύου Τεχνολογίας της Πληροφορίας (Information Technology Network, IT) στις εγκαταστάσεις των ναυτιλιακών εταιρειών, χωρίς κρυπτογράφηση και διαδικασίες ελέγχου της αυθεντικότητας τους, για στατιστική ανάλυση, έλεγχο της ορθής λειτουργίας τους και παραμετροποίηση (BIMCO, 2017· Bothur et. al., 2017).

Η τρωτότητα του συστήματος ICS συνίσταται στις τρωτότητες των συστημάτων που το απαρτίζουν. Αποτελείται από συστήματα διαφόρων κατασκευαστών, οι οποίοι κατά τη φάση της σχεδίασης και του προγραμματισμού δεν λαμβάνουν συνήθως υπόψη την παράμετρο της ασφάλειας, μετακυλύοντάς την ως εκκρεμότητα στο τελικό χρήστη που με τη σειρά του αδιαφορεί, θεωρώντας την πρόβλεψη για ασφάλεια υποχρέωση των πρώτων (Shoultz, 2017). Με την ομαλή συνδεσιμότητα και λειτουργία συστημάτων διαφορετικών κατασκευαστών να αποτελεί προτεραιότητα, η ασφάλεια σε επίπεδο σχεδιασμού αποτελεί δευτερεύων στοιχείο. Παρόμοια αντιμετώπιση παρατηρείται και σε επίπεδο καθημερινότητας με τους χειριστές να παρακάμπτουν τα πρωτόκολλά και τις διαδικασίες ασφαλείας υπό το πνεύμα της διευκόλυνσης και της αποτελεσματικότητας τους (Zurich, 2014). Παράλληλα το ICS είναι ευάλωτο και στις τρωτότητες των διασυνδεδεμένων συστημάτων όπως το GPS, το AIS ,το ECDIS καθώς και του σχεδιασμού των IT δικτύων. Κυβερνοεπιθέσεις, είτε με την εισαγωγή εσφαλμένων δεδομένων και

κακόβουλου λογισμικού στους κόμβους του συστήματος είτε λόγω της σύνδεσης με το διαδίκτυο μέσω του IT δικτύου, μπορούν να θέσουν εκτός ή να τροποποιήσουν τις παραμέτρους λειτουργίας των υποστηριζόμενων μηχανημάτων και συσκευών, να προκαλέσουν πυρκαγιά ή έκρηξη εν πλω με αποτέλεσμα τραυματισμούς ή θάνατο χειριστών ή να έχουν καταστροφικές συνέπειες όπως βύθιση του πλοίου, σύγκρουση με άλλα πλοία και εγκαταστάσεις, περιβαλλοντολογικές καταστροφές και υπονόμευση της αξιοπιστίας του συστήματος μεταφορών. Υπό προϋποθέσεις ο επιτιθέμενος έχει τη δυνατότητα να πάρει τον έλεγχο της πλοήγησης ενός πλοίου εν πλω και να το πηδαλιουχεί κατά βούληση, με χαρακτηριστική περίπτωση τον συνδυασμό επίθεσης στο σύστημα GPS με τη μέθοδο spoofing και πλου με ενεργοποιημένο τον αυτόματο πιλότο. Στην προκειμένη περίπτωση, η παρούσα θέση που λαμβάνει το πλοίο μέσω του GPS είναι λανθασμένη, οπότε μπορεί το πλοίο να παρεκκλίνει από την ορθή πορεία του, διότι ο αυτόματος πιλότος πηδαλιουχεί το πλοίο συγκρίνοντας την παρούσα θέση του με το στίγμα προορισμού.

Κεφάλαιο 3: Μεθοδολογία

3.1. Ερευνητικά ερωτήματα

Η έννοια της ενεργειακής ασφάλειας, ανεξάρτητα από των τρόπο προσέγγισης της, αποτελεί για τα κράτη έναν σημαντικό παράγοντα χάραξης στρατηγικής και λήψης αποφάσεων. Με σχεδόν το σύνολο των μεταφορών των εμπορευμάτων, ακόμη και των ενεργειακών πόρων όπως πετρέλαιο και φυσικό αέριο, να διενεργείται δια θαλάσσης, η θαλάσσια ασφάλεια βρίσκεται στο επίκεντρο των συζητήσεων τα τελευταία χρόνια, με αφορμή και τα περιστατικά πειρατείας έναντι εμπορικών πλοίων. Ο όρος είναι πολυδιάστατος και χαρακτηρίζεται από τη διασύνδεση διαφόρων τομέων της ανθρώπινης δραστηριότητας και τις μεταξύ τους αλληλεπιδράσεις. Η κυβερνοασφάλεια του ναυτιλιακού κλάδου, τόσο σε επίπεδο επιχείρησης όσο και σε επίπεδο πλοίου, αποτελεί σημαντική διάσταση του όρου λόγω της τρωτότητας των ναυτιλιακών συστημάτων αλλά και του μεγάλου οφέλους που δύνανται να αποφέρουν οι κυβερνοεπιθέσεις σε σχέση με τους χρησιμοποιούμενους πόρους.

Στο πλαίσιο των ανωτέρω, τα ερευνητικά ερωτήματα τα οποία επιχειρεί να απαντήσει η παρούσα εργασία παρατίθενται ως ακολούθως:

Ερώτημα Ε1: Πως αξιολογείται η ασφάλεια των (ενεργειακών) μεταφορών στον Ινδικό ωκεανό (γεωγραφία);

Ερώτημα Ε2: Πως μπορούν οι κυβερνοεπιθέσεις να απειλήσουν τη θαλάσσια μεταφορά (ενεργειακών) φορτίων;

Ερώτημα Ε3: Συνθέτοντας τις απαντήσεις στα ερωτήματα Ε1 και Ε2, πως αξιολογείται συνολικά η ασφάλεια των θαλάσσιων (ενεργειακών) μεταφορών στον Ινδικό ωκεανό;

3.2. Ερευνητικές μέθοδοι

Προκειμένου να απαντηθεί το ερευνητικό ερώτημα Ε1 θα εξεταστούν η γεωγραφία του Ινδικού ωκεανού, οι κυριότερες θαλάσσιες εμπορικές οδοί που τον διασχίζουν και τα κυριότερα στρατηγικά στενά της περιοχής, με έμφαση στον όγκο των διακινούμενων ενεργειακών φορτίων.

Αναφορικά με την απάντηση του ερευνητικού ερωτήματος Ε2 θα εξετασθούν περιπτώσεις εκδήλωσης κυβερνοεπιθέσεων σε εμπορικά πλοία μέσω της προσβολής

βασικών συστημάτων λειτουργίας τους και θα αναλυθούν τα αποτελέσματα αυτών στη λειτουργία του πλοίου και γενικότερα στη ναυσιπλοΐα.

Η απάντηση του ερευνητικού ερωτήματος Ε3 θα προκύψει από τη σύνθεση των αναλύσεων αναφορικά με την απάντηση των προηγούμενων ερωτημάτων Ε1 και Ε2 λαμβάνοντας υπόψη και τις γεωπολιτικές παραμέτρους της περιοχής.

Κεφάλαιο 4: Αποτελέσματα

4.1. Εισαγωγή

Στο παρόν κεφάλαιο παρουσιάζονται η γεωγραφία και τα χαρακτηριστικά των κύριων θαλάσσιων εμπορικών οδών στον Ινδικό ωκεανό με έμφαση στα choke points του Hormuz και της Malacca, αναλύονται περιπτώσεις εκδήλωσης κυβερνοεπιθέσεων στο θαλάσσιο περιβάλλον και επιτελείται σύνθεση των δύο ανωτέρω με σκοπό την αξιολόγηση της ασφάλειας όσον αφορά τη μεταφορά (ενεργειακών) φορτίων στον Ινδικό ωκεανό

4.2. Ινδικός ωκεανός – απάντηση σε ερώτημα Ε1

4.2.1. Γεωγραφία

Ο Ινδικός ωκεανός με εμβαδό περί τα 68 556 εκατομμύρια τετραγωνικά χιλιόμετρα, αποτελεί την τρίτη μεγαλύτερη θαλάσσια έκταση του πλανήτη, περικλείοντας το 20% της συνόλου της παγκόσμιας μάζας νερού. Καταλαμβάνει την επιφάνεια που οριοθετείται από την Ασία στο βορρά, την Αφρική στα δυτικά, τη νοητή γραμμή που διαμορφώνεται από τις ακτές της Ινδοκίνας, της Ινδονησίας και της Αυστραλίας στα ανατολικά και την ήπειρο της Ανταρκτικής στο νότο (Fatima & Jamshed, 2015). Η απόσταση Βορρά-Νότου, και συγκεκριμένα μεταξύ του κόλπου της Βεγγάλης και της Ανταρκτικής υπολογίζεται σε 9 600 χιλιόμετρα, ενώ η απόσταση Ανατολής-Δύσης, από τις ακτές της ανατολικής Αφρικής έως τη δυτική Αυστραλία αντιστοιχεί σε 7 800 χιλιόμετρα (Rumley, Chaturvedi & Yasin, 2007). Μεταξύ άλλων τμήμα του αποτελούν η Αραβική θάλασσα, η Ερυθρά θάλασσα, οι κόλποι της Βεγγάλης, του Ομάν και του Άντεν, ο Περσικός κόλπος, το κανάλι της Μοζαμβίκης και τα στενά της Malacca.

Οι συνορεύουσες χώρες ανέρχονται σε 35, όπως απεικονίζονται στο Σχήμα 4.1, με κυριότερες τις Ινδία, Σιγκαπούρη, Ταϋλάνδη, Αυστραλία, Σαουδική Αραβία, Ηνωμένα Αραβικά Εμιράτα (Η.Α.Ε), Ιράν, Πακιστάν, Νότιος Αφρική ενώ σημαντικά νησιά και νησιωτικά συμπλέγματα αποτελούν η Μαδαγασκάρη, ο Άγιος Μαυρίκιος, η Σρι Λάνκα, οι Μαλδίβες και οι Σεϋχέλλες.

Σχήμα 4.1. Παράκτιες και νησιωτικές χώρες στον Ινδικό Ωκεανό (https://chellaney.net/2015/07/01/worlds-geopolitical-center-of-gravity-shifts-to-indian-ocean/)

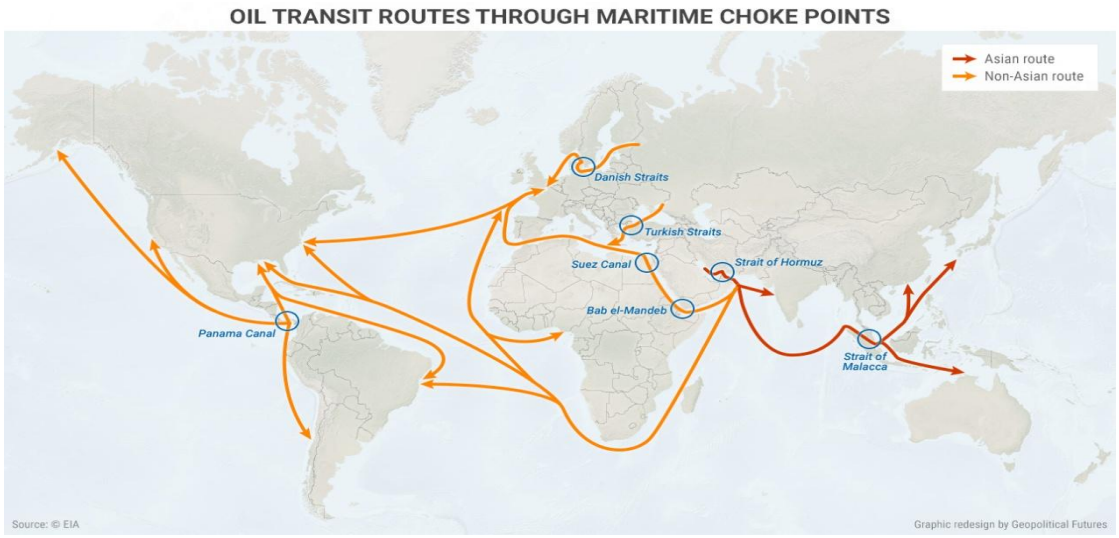
4.2.2. Κύριες θαλάσσιες εμπορικές οδοί

Η συνεχής αύξηση των ενεργειακών απαιτήσεων σε παγκόσμιο επίπεδο αποτελεί αναμφισβήτητο γεγονός. Η σταθερή αύξηση του παγκόσμιου πληθυσμού μεγεθύνει συνεχώς τις απαιτήσεις ενεργειακών πόρων για την επιτέλεση καθημερινών λειτουργιών όπως θέρμανση και μετακίνηση. Η επιδίωξη της σύγχρονης οικονομίας για ελαχιστοποίηση του κόστους παραγωγής και μεγιστοποίηση των κερδών οδηγεί σε πιέσεις για συνεχή και ανεμπόδιστη ροή φθηνών και άφθονων ενεργειακών πρώτων υλών, κυρίως πετρελαίου και φυσικού αερίου. Παράλληλα η τεχνολογική πρόοδος επιτρέπει την ανάπτυξη εξελιγμένων τεχνικών εξόρυξης ορυκτών καυσίμων, όπως η μέθοδος της υδραυλικής διάρρηξης για την εξόρυξη σχιστολιθικού αερίου και πετρελαίου, την εκμετάλλευση απρόσιτων μέχρι πρότινος κοιτασμάτων και την ανάπτυξη εξελιγμένων μεθόδων μεταφοράς, όπως η μεταφορά δια θαλάσσης υγροποιημένου φυσικού αερίου (Liquefied Natural Gas, LNG). Επιπρόσθετα η παγκοσμιοποίηση της οικονομίας επέτρεψε την εμφάνιση πολυεθνικών κολοσσών, συνήθως με καθετοποίηση της παραγωγής και με διαχωρισμό της έδρας σχεδιασμού των προϊόντων από την τοποθεσία των μονάδων παραγωγής, την περαιτέρω ανάπτυξη του διεθνούς εμπορίου και τη στενή αλληλεπίδραση των χρηματοπιστωτικών τομέων του συνόλου των κρατών.

Οι ανωτέρω παρατηρούμενες τάσεις και αλλαγές σε παγκόσμιο επίπεδο καθώς και το ευρύ φάσμα των εφαρμογών του πετρελαίου και των παραγώγων του

ενδυναμώνουν την σημασία του για την παγκοσμία οικονομία. Η σταθερή οικονομική ανάπτυξης τη Κίνας αλλά και των όμορων ασιατικών οικονομιών, παρά τις τάσεις για ενεργειακή απεξάρτηση των δυτικών οικονομιών και ιδιαίτερα των Η.Π.Α από το αραβικό πετρέλαιο και φυσικό αέριο, οδηγεί σε σταθερή αύξηση της ζήτησής και της σημασίας τους. Ειδικότερα για τις εν λόγω ασιατικές χώρες αναμένεται ότι σε σχέση με το 2014 οι απαιτήσεις σε εισαγωγές πετρελαίου και φυσικού αερίου για το 2040 θα αυξηθούν κατά 76% και 120% αντίστοιχα (ERIA, 2015).

Η διακίνηση του κύριου όγκου του εμπορευόμενου πετρελαίου και φυσικού αερίου παγκοσμίως, όπως και του συνόλου των εμπορευμάτων, γίνεται δια θαλάσσης. Ειδικότερα το 2015 από τα συνολικά 96.7 εκατομμύρια βαρέλια ανά ημέρα του διακινούμενου πετρελαίου και παραγώγων του παγκοσμίως, τα 58.9 εκατομμύρια, περίπου το 61%, μεταφέρθηκαν δια της θαλάσσιας οδού (EIA, 2017). Η θαλάσσια μεταφορά ενεργειακών πόρων γίνεται διαμέσου προκαθορισμένων διαδρομών, τις επονομαζόμενες κύριες θαλάσσιες εμπορικές οδούς (Sea Lines of Communications, SLOCs). Οι κυριότερες SLOCs διακίνησης πετρελαίου, παραγώγων του και LNG επισημαίνονται στο Σχήμα 4.2. Όπως φαίνεται, η κύρια εμπορική οδός που ενώνει τον περσικό κόλπο με τις χώρες της νοτιοανατολικής Ασίας διέρχεται διαμέσου του Ινδικού ωκεανού και ειδικότερα από τα στενά του Hormuz και της Malacca.



Σχήμα 4.2. Κύριες θαλάσσιες εμπορικές οδοί διακίνησης πετρελαίου (https://geopoliticalfutures.com/major-choke-points-persian-gulf-east-asia/)

Η πλειονότητα των SLOCs, όπως φαίνεται στο Σχήμα 4.2, διέρχεται από θαλάσσια περάσματα, τα οποία ονομάζονται διεθνή στενά. Για να χαρακτηριστεί ένα

θαλάσσιο πέρασμα ως διεθνές στενό θα πρέπει να είναι ένα φυσικό πέρασμα που διαχωρίζει δύο όγκους στεριάς ενώνοντας δύο θαλάσσιες εκτάσεις, να περικλείει εθνικά χωρικά ύδατα ενός ή περισσοτέρων κρατών και να χρησιμοποιείται για διεθνή ναυσιπλοΐα (de Quadros Rocha et al., 2016). Σύμφωνα με το άρθρο 38 της Συνθήκης για το Δίκαιο της Θάλασσας του 1982 (United Nations Convention on the Law of the Sea, UNCLOS) προβλέπεται το δικαίωμα της ασφαλούς διέλευσης, οριζόμενο ως η ελευθερία της ναυσιπλοΐας και της υπέρπτησης, με σκοπό την συνεχή και γρήγορη διέλευση από τα στενά. Επιπλέον στα άρθρα 39 έως 45 της ίδιας Συνθήκης προβλέπονται, μεταξύ άλλων, οι υποχρεώσεις των παράκτιων κρατών, όπως η υποχρέωση προειδοποίησης για την ύπαρξη οποιουδήποτε κινδύνου σχετικά με τη διέλευση, οι διαδικασίες κατάρτισης σχεδίων πλου για την εξασφάλιση της ασφαλούς ναυσιπλοΐας, συμπεριλαμβανομένου και της χάραξης εναλλακτικών διαδρομών, καθώς και οι υποχρεώσεις των διερχόμενων πλοίων κατά τη διάρκεια της διέλευσης. Αξίζει να σημειωθεί ότι η UNCLOS δεν έχει υπογραφεί από το σύνολο των κρατών ενώ κάποια που την έχουν υπογράψει αλλά δεν την έχουν επικυρώσει, γεγονός που δημιουργεί εντάσεις ως προς την αντίληψη του περί θαλάσσης δικαίου, που εκφράζονται κυρίως στην οριοθέτηση των θαλασσίων ζωνών μεταξύ των κρατών.

Τα διεθνή στενά τα οποία δεν μπορούν εύκολα να παρακαμφθούν, έχουν μεγάλη σημασία στο διεθνές εμπόριο πετρελαίου και φυσικού αερίου και προσφέρουν την δυνατότητα παρεμπόδισης των κινήσεων μιας αντίπαλης στρατιωτικής δύναμης ορίζονται ως στρατηγικά στενά (choke points) (de Quadros Rocha et. al., 2016). Τα choke points εμφανίζουν υψηλή συχνότητα καθημερινών διελεύσεων, η αποφυγή τους επιφέρει δυσανάλογα μεταφορικά κόστη και επιμήκυνση του χρόνου μεταφοράς, ενώ η σημαντικότητα τους έγκειται στα φυσικά τους χαρακτηριστικά όπως βάθος, πλάτος, πλωτότητα, στον αριθμό των διελεύσεων και στην ύπαρξη εναλλακτικών διαδρομών συνυπολογιζομένης της προσβασιμότητας αυτών (Rodrigue, 2004).

Με περίπου το 63% του εμπορεύσιμου πετρελαίου να διακινείται δια θαλάσσης, γίνεται αντιληπτό πως τυχόν απαγόρευση ή παρεμπόδιση της διέλευσης σε ένα choke point μπορεί να έχει τεράστιες οικονομικές συνέπειες λόγω της εκτροπής των τάνκερ σε εναλλακτικές διαδρομές. Αποτέλεσμα να αυξάνεται ο χρόνος μεταφοράς και επομένως το κόστος, να υφίσταται πιθανότητα αδυναμίας διέλευσης λόγω ασυμβατότητας μεταξύ των φυσικών περιορισμών του εκάστοτε στενού και της διαφορετικότητας των τύπων τάνκερ ως προς τη χωρητικότητα και το βύθισμα,

σύμφωνα με την κατηγοριοποίηση κατά το σύστημα AFRA, καθώς και δημιουργία ανησυχητικών προσδοκιών ή σημαντικής διαφοράς μεταξύ προσφερόμενης και ζητούμενης ποσότητας στις αγορές πετρελαίου (de Quadros Rocha et. al., 2016)

Στην τελευταία περίπτωση, και ειδικότερα εάν υπάρξει παρεμπόδιση της ροής, οι τιμές του πετρελαίου είναι δυνατόν να παρουσιάσουν σημαντική διακύμανση, η οποία εξαρτάται από το μέγεθος και την έκταση της αναστάτωσης, τις συνθήκες λειτουργίας της αγοράς και την τοποθεσία του συμβάντος. Η τιμή των διαφόρων τύπων του πετρελαίου διαμορφώνεται από τη διάδραση δύο αγορών, οι οποίες αλληλεπιδρούν και καθορίζουν το ύψος των τιμών, την εμπράγματη αγορά και την αγορά πετρελαϊκών παραγώγων. Οι αγοραπωλησίες πραγματικών ποσοτήτων πετρελαίου (wet barrel market) γίνονται είτε με τη μορφή μακροχρόνιων συμβάσεων (term contracts), δεσμεύσεων μεταξύ των αντισυμβαλλομένων παράδοσης προϊόντων σε προκαθορισμένη τιμή και για συγκεκριμένο χρονικό διάστημα είτε με τη μορφή βραχυχρόνιων συμφωνιών (spot deals), άμεσων συμφωνιών παραδόσεως, οι οποίες είναι συνήθως εμπιστευτικές και μη δημοσιεύσιμες. Από την άλλη, στην αγορά παραγώγων (paper barrel market), διαπραγματεύονται συμβόλαια μελλοντικής εκπλήρωσης (future contracts). Στην αγορά παραγώγων οι αντισυμβαλλόμενοι δεσμεύονται να προβούν σε αγοραπωλησία θέσεων, που αφορούν σε μια προκαθορισμένη ποσότητα ενός αγαθού, σε μία προκαθορισμένη ημερομηνία στο μέλλον και σε μία προκαθορισμένη τιμή συναλλαγής. (Mileva & Siegfried, 2007). Κινητήριο μοχλό αποτελούν οι διαφορετικές αντιλήψεις επί της διακύμανσης των τιμών των πετρελαϊκών αγαθών καθώς και ο υψηλός βαθμός μόχλευσης που παρατηρείται στις εν λόγω αγορές. Οι ανωτέρω δύο αγορές είναι συνδεόμενες και αλληλοεξαρτώμενες. Η μεν πρώτη συμβουλεύεται τη δεύτερη αναφορικά την τάση των τιμών ενώ η δεύτερη την πρώτη σχετικά με την ύπαρξη ελλείψεων ή πλεονασμάτων των προσφερόμενων ποσοτήτων (Emmerson & Stevens, 2012).

Συγκεκριμένα ενδεχόμενη απαγόρευση της διέλευσης από ένα choke point θα δημιουργήσει άμεσο ή μεσοπρόθεσμο έλλειμμα στην προσφερόμενη ποσότητα. Με δεδομένο ότι η ζήτηση παραμένει αμετάβλητη , δημιουργούνται προσδοκίες αύξησης της τιμής στην αγορά παραγώγων συνυπολογιζομένου του μεγέθους της παρεμποδιζόμενης ποσότητας, των διαθέσιμων αποθεμάτων που μπορούν να καλύψουν τη προκύπτουσα διαφορά μεταξύ προσφοράς και ζήτησης ,του απαιτούμενου χρόνου διανομής τους και της πιθανής απαίτησης αύξησης της παραγωγής (Blumsack, 2017). Αναλόγως μια κρίση, όπως κλιμακούμενη πολιτική

ένταση μεταξύ παράκτιων χωρών σε ένα choke point προκαλεί αντίστοιχες προσδοκίες και ανασφάλεια, οι οποίες εκφράζονται σε ενδεχόμενες μεταβολές της τιμής (Emmerson & Stevens, 2012).

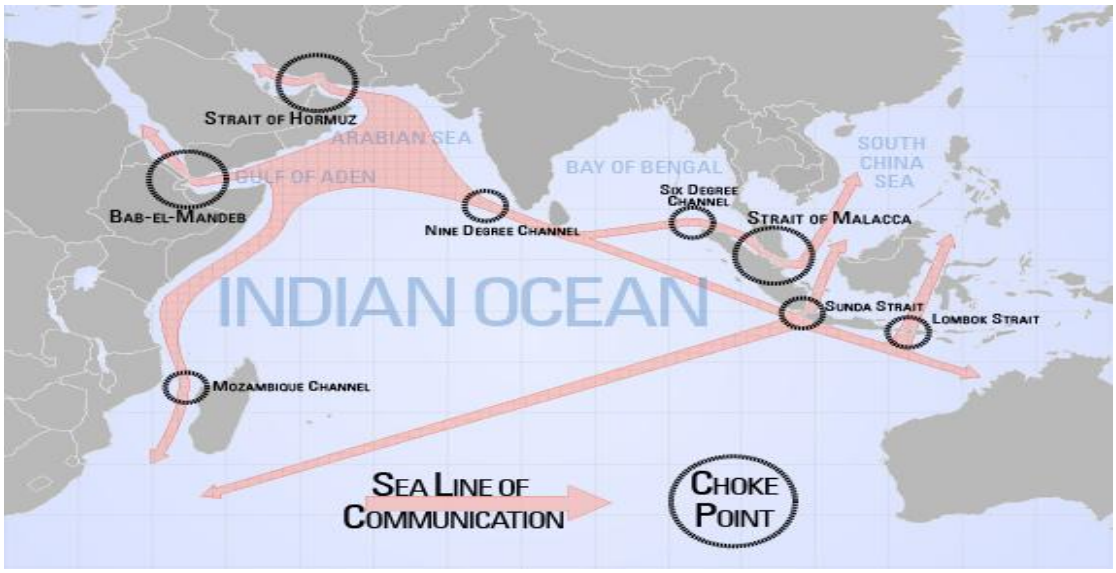
Αναφορικά με τα ανωτέρω, η παρεμπόδιση της διέλευσης από τα choke points που μπορεί να επιβάλλει ένα παράκτιο κράτος ή μια εξωτερική ναυτική δύναμη και η οποία γίνεται εφικτότερη όσο πιο στενό είναι το θαλάσσιο πέρασμα, έχει αμεσότερο αντίκτυπο συγκρινόμενη με πολιτικές εντάσεις μεταξύ κρατών, που πιθανόν να εκφράζονται με στρατικοποίηση των στενών, όπου η αύξηση των στρατιωτικών εξοπλισμών και δυνατοτήτων οδηγούν σε έναν αυτοτροφοδοτούμενο κύκλο εξοπλιστικού ανταγωνισμού, καλλιεργώντας κλίμα ανασφάλειας και περιφερειακές εντάσεις, υποδαυλίζοντας τελικά την ασφάλεια στην περιοχή. Η απειλή χρήσης βίας αποσταθεροποιεί την περιοχή και έτσι σημαντικό ρόλο στην ασφάλεια παίζουν οι στρατιωτικές δυνατότητες των παράκτιων κρατών, το εσωτερικό πολιτικό περιβάλλον, οι σύμμαχοι και οι αντίπαλοί τους. Η στρατικοποίηση εκφράζεται στα παράκτια κράτη κυρίως σε μονάδες πυροβολικού όπως πυραυλικά συστήματα ενώ στις λοιπές ενδιαφερόμενες δυνάμεις σε συνδυασμό αεροπορικών και αμφίβιων δυνάμεων. Τόσο η απαγόρευση της διέλευσης όσο και η στρατικοποίηση αποτελούν προσφιλείς τακτικές αποτροπής των παρακτίων κρατών απέναντι σε εξαναγκασμούς και απειλές των μεγάλων δυνάμεων (de Quadros Rocha et. al., 2016).

Η γεωλογική διαμόρφωση της περιοχής όπου εκτείνεται ο Ινδικός ωκεανός, το γεγονός ότι σε αυτήν συμπεριλαμβάνονται οι αραβικές χώρες, που αποτελούν από τους σημαντικότερους παραγωγούς και εξαγωγείς πετρελαίου και φυσικού αερίου, η εγγύτητα των ασιατικών χωρών με υψηλούς ρυθμούς οικονομικής ανάπτυξης με προεξέχουσα την Κίνα και οι διακινούμενες ποσότητες πετρελαίου και υγροποιημένου φυσικού αερίου μέσω των SLOCs και συνεπώς των choke points της περιοχής καθιστούν την διατήρηση της ασφάλειας των θαλάσσιων οδών μεταφοράς ενεργειακών πόρων ύψιστη προτεραιότητα (Forbes, 2014). Παράγοντες όπως η κλιματική αλλαγή, οι γεωπολιτικές εξελίξεις, η αντίληψη της έννοιας περί του θαλασσίου δικαίου και τα όρια της εθνικής κυριαρχίας, η γεωγραφία της περιοχής, το βιοτικό επίπεδο των παράκτιων κρατών και η συμφόρηση των στενών, μεμονωμένα και συνδυαστικά, οδηγούν στην εμφάνιση απειλών όπως πειρατεία, τρομοκρατία, ατυχήματα ναυσιπλοΐας, ακραία θαλάσσια φαινόμενα και περιφερειακές συγκρούσεις. Τα ανωτέρω επιφέρουν αποσταθεροποίηση στις τιμές των εμπορεύσιμων αγαθών, διαταράσσουν την ροή στον εφοδιασμό πρώτων υλών,

αυξάνουν το επιχειρηματικό ρίσκο, γεγονός που εκφράζεται και με την αύξηση των μεταφορικών ασφαλίστρων, και μεγεθύνουν εκθετικά το ρίσκο απώλειας ανθρώπινων ζωών.

4.2.3. Στρατηγικά στενά στην περιοχή του Ινδικού ωκεανού

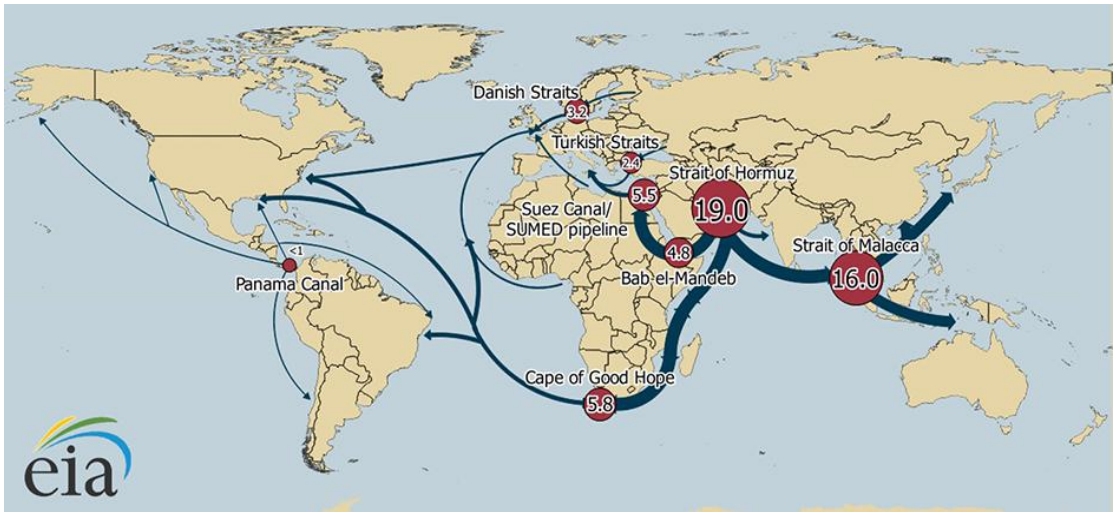
Γίνεται εύκολα αντιληπτό ότι σε μία ολιγοπωλιακή αγορά, όπως αυτή του πετρελαίου, τόσο από την πλευρά των παραγωγών χωρών όσο και από εκείνη των μεγάλων πολυεθνικών πετρελαϊκών εταιρειών, ενδεχόμενη παρεμπόδιση της ροής ή μείωση της παραγωγής, με τη συνεπακόλουθη αύξηση των τιμών αποτελεί μείζων σενάριο παγκόσμιας πολιτικής και οικονομικής αποσταθεροποίησης. Παράλληλα με το 80% των θαλάσσιων εισαγωγών πετρελαίου της Κίνας και το 60% των αντίστοιχων εισαγωγών της Ιαπωνίας να διέρχονται από τα στενά της Malacca (Friedman & Ligon, 2017) και με το 68% και 85% αντίστοιχα των εισαγωγών πετρελαίου και φυσικού αερίου της Ινδίας να διακινούνται μέσω των SLOCs του Ινδικού ωκεανού (Cordner, 2014) και ειδικότερα από τα στενά του Hormuz καθώς προέρχονται από τις χώρες της Περσικού κόλπου, γίνεται αντιληπτή η σημασία της εγγύησης της ασφάλειας διέλευσης των εν λόγω στενών για τα εν λόγω κράτη.



Σχήμα 4.3. Κύριες θαλάσσιες εμπορικές οδοί και στρατηγικά στενά στον Ινδικό ωκεανό (https://www.flickr.com/photos/mrdevlar/4922429758)

Τα κυριότερα choke points της περιοχής του Ινδικού ωκεανού, όπως φαίνεται στο Σχήμα 4.3, είναι τα στενά του Hormuz και της Malacca ενώ μικρότερη σημασία

εμφανίζουν τα στενά του Bab el-Mandeb, του Lombok, της Sunda και το κανάλι της Μοζαμβίκης. Η σπουδαιότητα τους έγκειται στο γεγονός ότι αποτελούν τα άκρα της SLOC που ενώνει τον Περσικό κόλπο και την Αραβική χερσόνησο με τις οικονομίες της Νοτιοανατολικής Ασίας καθώς και στο σημαντικό όγκο διερχόμενου πετρελαίου και υγροποιημένου φυσικού αερίου συγκριτικά με τα λοιπά choke points της περιοχής όπως φαίνεται στο Σχήμα 4.4 και απεικονίζεται διαχρονικά στον Πίνακα 4.1.



Σχήμα 4.4. Ημερήσιες διακινούμενες ποσότητες πετρελαίου, υπολογιζόμενες ανά εκατομμύρια βαρέλια, διαμέσου των κυριότερων στρατηγικών στενών κατά το έτος 2016 (EIA, U.S. Energy Information Administration)

Πίνακας 4.1. Ημερήσιες ποσότητες διακινούμενου πετρελαίου και παραγώγων, υπολογιζόμενες ανά εκατομμύρια βαρέλια, διαμέσου των κυριότερων στρατηγικών στενών (EIA, U.S. Energy Information Administration)

	ΠΟΣΟΤΗΤΑ ΑΝΑ ΕΤΟΣ					
ΤΟΠΟΘΕΣΙΑ	2011	2012	2013	2014	2015	2016
Στενά του Hormuz	17.0	16.8	16.6	16.9	17.0	18.5
Στενά της Malacca	14.5	15.1	15.4	15.5	15.5	16.0
Διώρυγα του Suez και αγωγός SUMED	3.8	4.5	4.6	5.2	5.4	5.5
Στενά Bab el-Mandab	3.3	3.6	3.8	4.3	4.7	4.8
Στενά Δανίας	3.0	3.3	3.1	3.0	3.2	3.2
Στενά του Βοσπόρου	2.9	2.7	2.6	2.6	2.4	2.4
Διώρυγα του Παναμά	0.8	0.8	0.8	0.9	1.0	0.9
Ακρωτήριο της Καλής Ελπίδας	4.7	5.4	5.1	4.9	5.1	5.8
Διακινούμενο πετρέλαιο δια θαλάσσης (σε παγκόσμιο επίπεδο)	55.5	56.4	56.5	56.4	58.9	Μη διαθέσιμα
Συνολική διακινούμενη ποσότητα πετρελαίου και παραγώγων (σε παγκόσμιο επίπεδο)	88.8	90.8	91.3	93.8	96.7	97.2

Υφίσταται πρόβλεψη για αύξηση της ζήτησης πετρελαίου και LNG από τις ασιατικές οικονομίες, με τις ανάγκες αυτές να καλύπτονται κυρίως από τα κράτη της Μέσης Ανατολής, τα οποία και θα διατηρήσουν το προβάδισμα στις εξαγωγές των εν λόγω ενεργειακών αγαθών στην παγκόσμια αγορά (ERIA, 2015). Πιο συγκεκριμένα και αναφορικά με το αργό πετρέλαιο, οι εισαγωγές των ασιατικών χωρών φαίνεται πως θα εμφανίσουν αύξηση κατά 76% (Πίνακας 4.2) ενώ παράλληλα οι αντίστοιχες εξαγωγές των χωρών της Μέσης Ανατολής θα αυξηθούν κατά 50%, αποτελώντας παράλληλα το 52% των συνολικών παγκόσμιων εξαγωγών (Πίνακας 4.3). Η διασύνδεση αποτυπώνεται στις διακινούμενες ποσότητες διαμέσου των choke points του Hormuz και της Malacca, σύμφωνα με τον Πίνακα 4.4.

Πίνακας 4.2. Πρόβλεψη εισαγωγών αργού πετρελαίου την περίοδο 2014 έως 2040, υπολογιζόμενη σε χιλιάδες βαρέλια ανά ημέρα (http://www.eria.org/RPR_FY2015_14.pdf)

	ΕΤΟΣ			
ΧΩΡΕΣ	2014	2020	2030	2040
Κίνα	6 186	8 519	11 040	12 200
Ιαπωνία	3 237	3 183	2 991	2 620
Ταιβάν	822	834	836	834
Κορέα	2 469	2 481	2 483	2 408
ASEAN	1 987	3 920	5 026	6 525
Ν. Ασία	3 900	5 880	8 494	8 911
Ωκεανία	566	556	516	360
Σύνολο χωρών Ασίας-Ειρηνικού	19 167	25 373	31 386	33 858
Η.Π.Α	7 388	6 628	6 422	5 300
Καναδάς	564	161	80	40
Λατινική Αμερική	925	988	1 090	1 106
Σύνολο Αμερικής	8 877	7 777	7 592	6 446
Ευρώπη	10 307	8 228	6 792	6 250
Πρώην Σοβιετική Ένωση	584	210	106	-
Αφρική	656	701	773	796
Μέση Ανατολή	492	526	580	588
Σύνολο	40 083	42 813	47 228	47 938

Πίνακας 4.3. Πρόβλεψη εξαγωγών αργού πετρελαίου ανά περιοχή την περίοδο 2014 έως 2040, υπολογιζόμενη σε χιλιάδες βαρέλια ανά ημέρα (http://www.eria.org/RPR_FY2015_14.pdf)

ΕΤΟΣ				
ΧΩΡΕΣ	2014	2020	2030	2040
ASEAN	848	441	230	120
Αυστραλία	161	302	420	472
Λοιπές χώρες Ασίας Ειρηνικού	212	198	175	112
Σύνολο χωρών Ασίας-Ειρηνικού	1 221	942	825	704
Η.Π.Α	345	209	424	591
Καναδάς	2 266	2 844	3 452	3 707
Λατινική Αμερική	5 001	4 166	3 889	3 509
Σύνολο Αμερικής	7 612	7 219	7 764	7 807
Ευρώπη	1 885	158	-	-
Πρώην Σοβιετική Ένωση	6 798	6 876	7 254	7 847
Αφρική	5 774	5 832	6 390	6 454
Μέση Ανατολή	16 793	21 786	24 995	25 127
Σύνολο	40 083	42 813	47 228	47 938

Πίνακας 4.4. Πρόβλεψη διακινούμενων ποσοτήτων αργού πετρελαίου από τα κύρια στρατηγικά στενά του Ινδικού Ωκεανού την περίοδο 2014 έως 2040 (http://www.eria.org/RPR_FY2015_14.pdf)

ΕΤΟΣ							
CHOKE POINTS		2014		2030		2040	
		Χιλιάδες βαρέλια ανά ημέρα	Αριθμός διελεύσεων τάνκερ	Χιλιάδες βαρέλια ανά ημέρα	Αριθμός διελεύσεων τάνκερ	Χιλιάδες βαρέλια ανά ημέρα	Αριθμός διελεύσεων τάνκερ
Στενά του Hormuz	Προς Ασία	12 419	7 815	23 414	14 735	23 994	15 100
	Προς Ατλαντικό	4 443	2 796	1 573	990	-	-
	Σύνολο	16 862	10 611	24 987	15 725	23 994	15 100
Στενά της Malacca		12 272	7 723	18 456	11 615	19 404	12 211

Σημείωση: Ο αριθμός των διελεύσεων αφορά σε διαδρομές μετ' επιστροφής και η μέση χωρητικότητα ανά τάνκερ εκτιμάται σε 1,1 εκατομμύρια βαρέλια

Αναφορικά με τις προβλέψεις για τις απαιτήσεις σε LNG φαίνεται πως οι εισαγωγές των ασιατικών χωρών και τον όμορων περιοχών του Ειρηνικού ωκεανού θα εμφανίσουν αύξηση κατά 120% (Πίνακας 4.5) ενώ οι εξαγωγές των χωρών της Μέσης Ανατολής και της Αφρικής θα αυξηθούν κατά 34% και 140% αντίστοιχα (Πίνακας 4.6). Η διασύνδεση αποτυπώνεται στις διακινούμενες ποσότητες διαμέσου των choke points του Hormuz και της Malacca, σύμφωνα με τον Πίνακα 4.7.

Πίνακας 4.5. Πρόβλεψη εισαγωγών LNG την περίοδο 2014 έως 2040, υπολογιζόμενη σε εκατομμύρια τόνους (http://www.eria.org/RPR_FY2015_14.pdf)

		ΕΤΟΣ			
ΠΕΡΙΟΧΗ	**ΧΩΡΑ**	2014	2020	2030	2040
Ασία - Ειρηνικός	Ιαπωνία	89	75	85	86
	Κορέα	38	36	44	45
	Κίνα	19	47	82	99
	Ταϋλάνδη	1	8	19	25
	Σιγκαπούρη	2	8	11	14
	Μαλαισία	2	5	6	8
	Ινδονησία	0	5	9	12
	Βιετνάμ	0	1	3	6
	Φιλιππίνες	0	1	4	5
	Ινδία	15	23	50	62
	Ν. Ζηλανδία	0	0	1	1
	Ταιβάν	13	15	21	23
	Πακιστάν	0	2	2	4
	Σρι Λάνκα	0	0	1	1
	Μπαγκλαντές	0	0	2	2
	Σύνολο	179	227	339	394
Μέση Ανατολή	Περσικός Κόλπος	4	7	13	21
	Εκτός Περσικού Κόλπου	0.1	3	4	5
	Σύνολο	4	10	17	26
Ευρώπη	Βαλτική	0.1	4	5	9
	Ατλαντικός	13	31	32	33
	Μεσόγειος	19	44	46	46
	Σύνολο	32	78	83	88
Αμερική	Βόρεια Αμερική	10	10	11	12
	Νότια Αμερική	12	12	15	17
	Σύνολο	23	22	26	29
Αφρική	Βόρεια Αφρική	0	0	2	3
	Υποσαχάρια Αφρική	0	1	5	7
	Σύνολο	0	1	7	10
Γενικό Σύνολο		238	338	472	547

Πίνακας 4.6. Πρόβλεψη εξαγωγών LNG ανά περιοχή την περίοδο 2014 έως 2040 (http://www.eria.org/RPR_FY2015_14.pdf)

ΕΤΟΣ				
ΠΕΡΙΟΧΗ	2014	2020	2030	2040
ASEAN	48	45	43	39
Ωκεανία	27	67	85	98
Η.Π.Α	0.3	31	66	95
Καναδάς	0	0	24	32
Κεντρική & Νότια Αμερική	17	14	13	11
Σύνολο Αμερικής	17	45	103	138
Ευρώπη	4	3	2	1
Πρώην Σοβιετική Ένωση	11	15	31	55
Αφρική	36	45	56	87
Μέση Ανατολή	96	89	109	129
Σύνολο	239	309	429	547

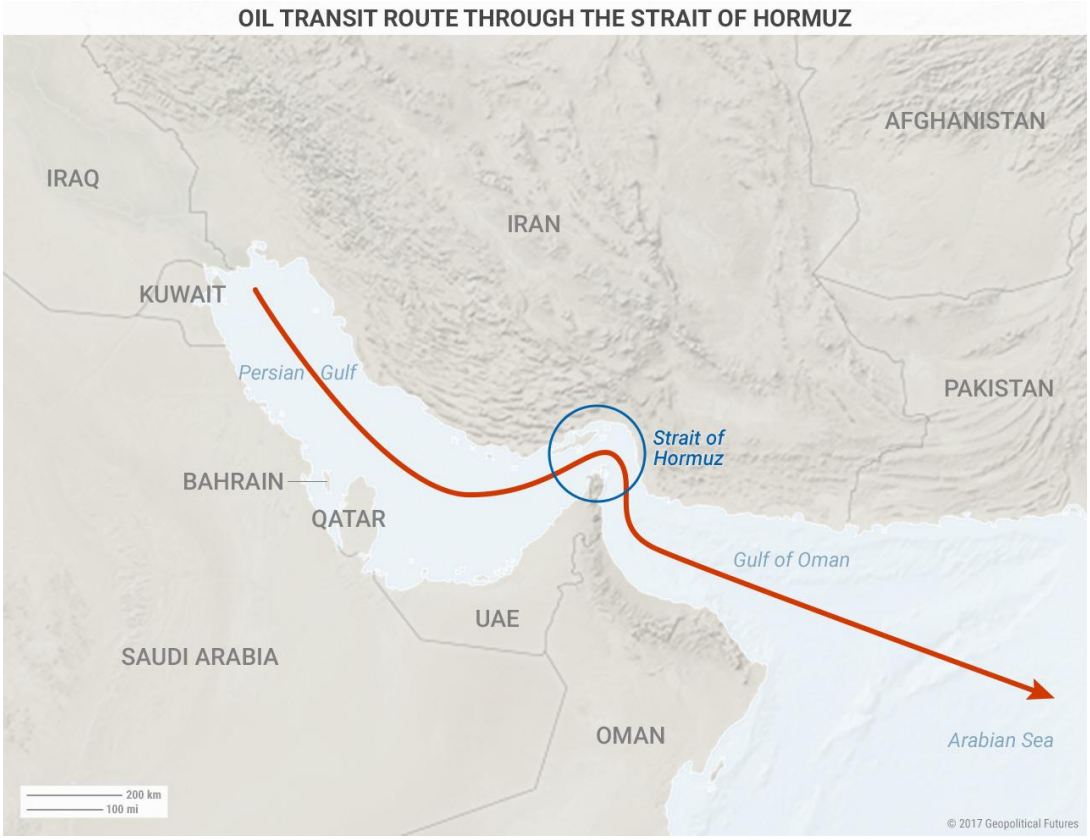
Πίνακας 4.7. Πρόβλεψη διακινούμενου LNG από τα κύρια στρατηγικά στενά του Ινδικού Ωκεανού την περίοδο 2014 έως 2040 (http://www.eria.org/RPR_FY2015_14.pdf)

ΕΤΟΣ							
CHOKE POINTS		2014		2030		2040	
		Εκατ/ρια τόνοι	Αριθμός διελεύσεων τάνκερ	Εκατομμύρια τόνοι	Αριθμός διελεύσεων τάνκερ	Εκατομμύρια τόνοι	Αριθμός διελεύσεων τάνκερ
Στενά του Hormuz	Προς Ασία	61	1 537	62	1 580	72	1 820
	Προς Ατλαντικό	20	503	24	608	28	700
	Σύνολο	81	2 040	96	2 188	11	2 520
Στενά της Malacca	Προς Ασία	94	2 388	67	1 693	102	2 589
	Προς Ατλαντικό	0.5	13	9	215	11	278
	Σύνολο	95	2 401	75	1 908	113	2 867

Σημείωση: Ο αριθμός των διελεύσεων αφορά σε διαδρομές μετ' επιστροφής και η μέση χωρητικότητα ανά τάνκερ εκτιμάται σε 79 000 τόνους

4.2.4. Στενά του Hormuz

Τα στενά του Hormuz ενώνουν τον Περσικό κόλπο με τον κόλπο του Ομάν και κατ' επέκταση με τον Ινδικό ωκεανό. Οριοθετούνται από τις ακτές του Ιράν στο βορρά και από εκείνες του Ομάν και των Η.Α.Ε στο νότο και εμφανίζουν πλάτος από 48 έως 80 χιλιόμετρα (Σχήμα 4.5). Η ναυσιπλοΐα επιτελείται σε δύο ρεύματα αντίθετης ροής πλάτους 3 χιλιομέτρων έκαστο, όπως φαίνεται στο Σχήμα 4.6, τα οποία διαχωρίζονται με μία θαλάσσια ζώνη ομοίου πλάτους (Fatima & Jamshed, 2015).



Σχήμα 4.5. Τα στενά του Hormuz (http://www.mauldineconomics.com/this-week-in-geopolitics/major-choke-points-in-the-persian-gulf-and-east-asia)

Σχήμα 4.6. Η ναυσιπλοΐα στα στενά του Hormuz (https://www.pakistancargo4u.co.uk/blog/gwadar-vs-chabahar-a-warfield-on-the-world-economic-gateway)

Με δεδομένη την ύπαρξη στην περιοχή πληθώρας πετρελαιοπαραγωγών χωρών, υφίσταται και αντίστοιχη συσσώρευση τερματικών σταθμών φόρτωσης αργού πετρελαίου σε τάνκερ. Η συντριπτική πλειονότητα αυτών βρίσκεται εντός του περσικού κόλπου με μόνη εξαίρεση τον τερματικό Mina Al Fahal του Ομάν. Πλέον του συγκεκριμένου σταθμού οι κυριότεροι είναι οι σταθμοί Ras Tanura και Ju'aymah της Σαουδικής Αραβίας, Kharg Island του Ιράν, Al Basra του Ιράκ, Jebel Dhanna των H.A.E και Mina al Ahmadi του Κουβέιτ. Παράλληλα το Κατάρ αποτελεί τον μεγαλύτερο εξαγωγέα LNG στην περιοχή με τον τερματικό του Ras Laffan ενώ σημαντικές εγκαταστάσεις έχουν το Ομάν και τα H.A.E σε Qualhat και Das Island αντίστοιχα. Ως σημαντικότερο διυλιστήριο της περιοχής φέρεται το σύμπλεγμα Abqaiq-Ras Tanura-Jubail της Σαουδικής Αραβίας που αποτελεί εγκατάσταση στρατηγικής σημασίας για τη προμήθεια πετρελαϊκών προϊόντων και παραγώγων αυτού σε χώρες της Αφρικής και της Ασίας που δεν διαθέτουν αντίστοιχες εγκαταστάσεις επεξεργασίας (Forbes, 2014).

Η εξασφάλιση εναλλακτικών οδεύσεων πετρελαίου και φυσικού αερίου για την παράκαμψη των στενών του Hormuz επιτυγχάνεται μέσω των αγωγών Petroline (East-West Pipeline) της Σαουδικής Αραβίας, που καταλήγει στον κύριο τερματικό

του Yanbu στην Ερυθρά θάλασσα και του Abu Dhabi Crude Oil Pipeline που καταλήγει στο Fujairah στον κόλπο του Ομάν (EIA, 2017). Ωστόσο η χωρητικότητα των αγωγών της περιοχής δεν φαίνεται να επαρκεί για να αποσυνδεθεί η απρόσκοπτη διακίνηση πετρελαίου και φυσικού αερίου από την απαίτηση εγγύησης της ασφάλειας της ναυσιπλοΐας στα εν λόγω στενά (Πίνακας 4.8).

Πίνακας 4.8. Αγωγοί παράκαμψης των στενών του Hormuz (EIA, U.S. Energy Information Administration)

ΟΝΟΜΑΣΙΑ ΑΓΩΓΟΥ	ΧΩΡΑ	ΚΑΤΑΣΤΑΣΗ	ΧΩΡΗΤΙΚΟΤΗΤΑ	ΔΙΑΚΙΝΟΥΜΕΝΗ ΠΟΣΟΤΗΤΑ	ΕΠΙΠΡΟΣΘΕΤΗ ΔΥΝΑΤΟΤΗΤΑ
Petroline (East-West Pipeline)	Σαουδική Αραβία	Ενεργός	4.8	1.9	2.9
Abu Dhabi Crude Oil Pipeline	Η.Α.Ε	Ενεργός	1.5	0.5	1.0
Abqaiq-Yanbu Natural Gas Liquids Pipeline	Σαουδική Αραβία	Ενεργός	0.3	0.3	0.0
Iraqi Pipeline in Saudi Arabia (IPSA)	Σαουδική Αραβία	Μετατράπηκε σε αγωγό φυσικού αερίου	0.0	-	0.0
ΣΥΝΟΛΟ			6.6	2.7	3.9

Σημείωση: Η χωρητικότητα υπολογίζεται σε εκατομμύρια βαρέλια ανά ημέρα

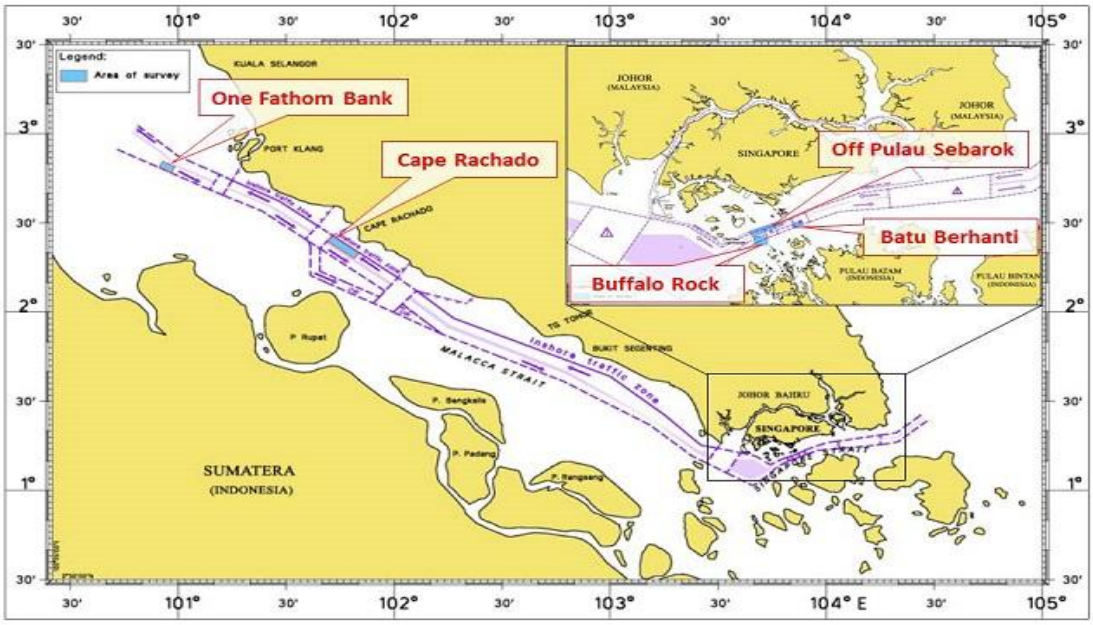
Η σταθερότητα του καθεστώτος των στενών είναι αποτέλεσμα της γενικότερης γεωπολιτικής κατάστασης στην περιοχή με τις αλληλεπιδράσεις μεταξύ των κρατών, των μη κρατικών δρώντων και των εμπλεκόμενων εξωτερικών δυνάμεων να δημιουργούν ένα δυναμικά εξελισσόμενο περιβάλλον. Μερικές από τις παραμέτρους που επηρεάζουν την ασφάλεια στην περιοχή αποτελούν η διαμάχη Σουνιτών και Σιιτών, όπως αποτυπώνεται στην σύγκρουση μεταξύ Σαουδικής Αραβίας και Ιράν, στους εμφυλίους σε Υεμένη και Συρία αλλά και γενικότερα στην αντιπαλότητα του Ιράν με τον αραβικό κόσμο, η τήρηση της συμφωνίας για το πυρηνικό πρόγραμμα του Ιράν, οι εδαφικές διαφορές μεταξύ Η.Α.Ε και Ιράν για την κυριαρχία στα νησιά Abu Musa, Great Tunb και Lesser Tunb στην περιοχή των στενών του Hormuz, τα κατάλοιπα της Αραβικής Άνοιξης, το Ισλαμικό Χαλιφάτο (Islamic State of Iraq and Syria**,** ISIS), το ευρύτερο κουρδικό ζήτημα, οι

τρομοκρατικές επιθέσεις από μη κρατικούς δρώντες σε επιλεγμένους στόχους τόσο στην περιοχή όσο και στον δυτικό κόσμο, η ύπαρξη κρατών υπό κατάρρευση (rogue nations) σε εγγύτητα με την περιοχή σε Αφρική και Ασία, η ολοένα και μεγαλύτερη ενεργειακή εξάρτηση της Κίνας και της Ινδίας από το εξαγόμενο πετρέλαιο και LNG της περιοχής και το υπάρχον καθεστώς εγγύησης της ασφάλειας των SLOCs για την μεταφορά τους, κυρίως από τις ναυτικές δυνάμεις των ΗΠΑ.

4.2.5. Τα στενά της Malacca

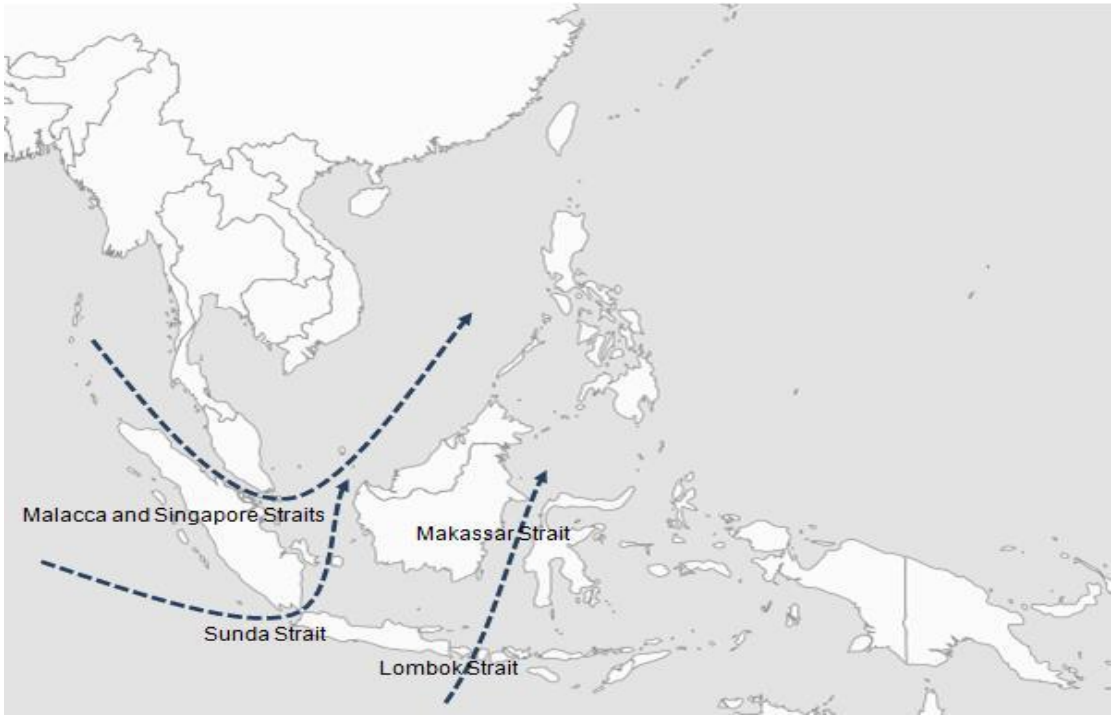
Τα στενά της Malacca βρίσκονται μεταξύ των ακτών της Ινδονησίας ,της Μαλαισίας και της Σιγκαπούρης και ενώνουν τον Ινδικό ωκεανό με τη νότια Σινική θάλασσα και τον Ειρηνικό ωκεανό (Σχήμα 4.7). Με μήκος περί τα 800 χιλιόμετρα και πλάτος έως 320 χιλιόμετρα, εμφανίζουν στο πιο στενό τους σημείο πλάτος 2.5 χιλιόμετρα και βάθος 23 μέτρα (Σχήμα 4.8).

Σχήμα 4.7. Τα στενά της Malacca (http://www.mauldineconomics.com/this-week-in-geopolitics/major-choke-points-in-the-persian-gulf-and-east-asia)



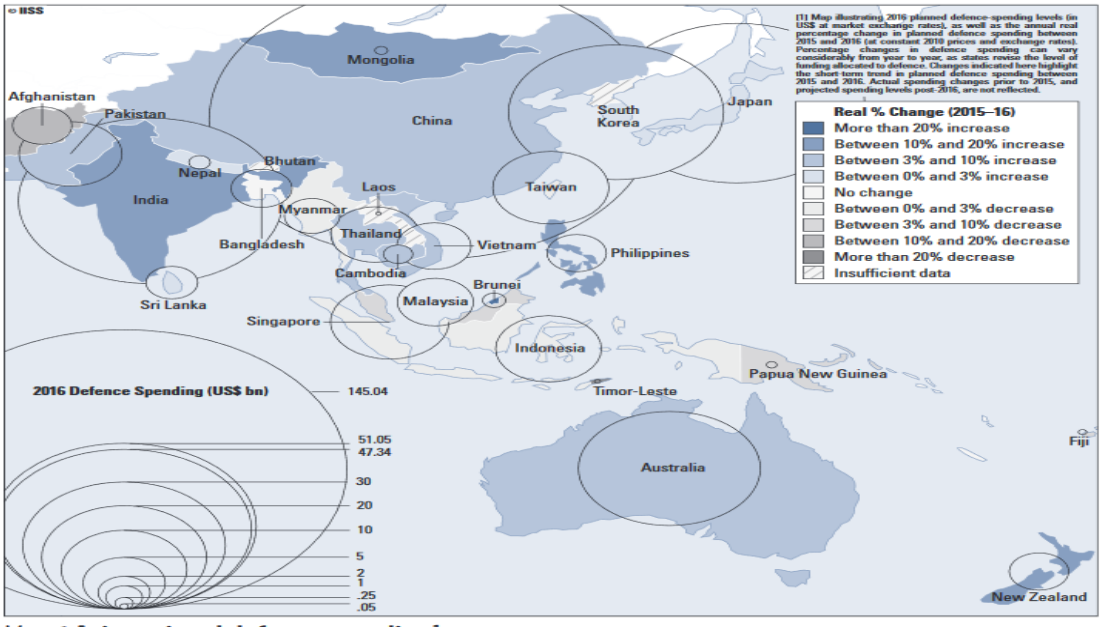
Σχήμα 4.8. Ναυσιπλοΐα στα στενά της Malacca (https://www.maritime-executive.com/article/hydrographic-survey-of-malacca-strait-underway#gs.FVgAHBU)

Αποτελούν τμήμα της κύριας οδού μεταφοράς πετρελαίου και LNG στις ασιατικές οικονομίες. Με το 80% των θαλάσσιων εισαγωγών πετρελαίου της Κίνας (Friedman & Ligon, 2017), το 93% και 97% αντίστοιχα των ενεργειακών αναγκών της Ιαπωνίας και της Κορέας και το 70% της ποσότητας του παγκόσμιου εμπορίου φυσικού αερίου να εισάγεται από τις ασιατικές οικονομίες διαμέσου αυτών, γίνεται αντιληπτή η σημασία της διασφάλισης της ελεύθερης ναυσιπλοΐας των εν λόγω στενών. Εναλλακτικές διαδρομές αποτελούν τα στενά του Lombok και της Sunda (Σχήμα 4.9) αλλά ενδεχόμενη εκτροπή σχεδόν του μισού παγκόσμιου στόλου στις εν λόγω διαδρομές, θα επιφέρει σημαντικές καθυστερήσεις και αύξηση του κόστους μεταφοράς (de Quadros Rocha et. al., 2016). Συγκεκριμένα υπολογίζεται ότι η διέλευση από τα στενά του Lombok αυξάνει τη διαδρομή κατά 2 500 ναυτικά μίλια, που αντιστοιχούν περίπου σε 168 επιπλέον ώρες ταξιδίου και σε αύξηση κατά 20% του κόστους μεταφοράς (ERIA, 2015).



Σχήμα 4.9. Εναλλακτικές διαδρομές στα στενά της Malacca (http://www.eria.org/publications/research_project_reports/FY2015/No.14.html)

Η ύπαρξη εναλλακτικών διαδρομών μειώνει τον αντίκτυπο πιθανής απαγόρευσης διέλευσης και καθιστά τη διατάραξη του ενεργειακού θαλάσσιου εμπορίου στην περιοχή ενδεχόμενο χαμηλή πιθανότητας-υψηλού κόστους (low probability-high impact) παρά την ύπαρξη παραγόντων αποσταθεροποίησης. Σε αυτούς περιλαμβάνονται η εγγύτητα των στενών με τη νότια Σινική θάλασσα, πεδίο αμφισβητήσεων και εκατέρωθεν εδαφικών διεκδικήσεων μεταξύ κρατών της περιοχής, όπως στις περιπτώσεις των νήσων Spratly και Paracels, η αξίωση από πλευράς της Κίνας του συνόλου της νότιας Σινικής θάλασσας ως Αποκλειστικής Οικονομικής Ζώνης (AOZ) (de Quadros Rocha et. al., 2016), το "δίλλημα της Malacca" όπως εκφράστηκε από τον προέδρο Hu Jintao το 2003, η διακίνηση του ήμισυ των εισαγωγών πετρελαίου από τάνκερ κινεζικής ιδιοκτησίας (Graham, 2015) και οι αυξημένες στρατιωτικές δαπάνες των χωρών της περιοχής (Σχήμα 4.10) ύψους 367,7 δις δολαρίων το 2016, αυξημένες κατά 5,3% σε σχέση με το 2015 και με μέση ετήσια αύξηση της τάξεως του 5-6% από το 2012 έως σήμερα (IISS, 2017).



Σχήμα 4.10. Δαπάνες των ασιατικών χωρών για άμυνα ως ποσοστό επί του ΑΕΠ. (http://emagazinepdf.com/2017/08/the-military-balance-2017/)

Η ύπαρξη πλήθους εταιρειών παραγωγής και αποθήκευσης καθιστά την νήσο Jurong έναν από τους σημαντικότερους κόμβους πετρελαίου και πετροχημικών. Το διυλιστήριο της Σιγκαπούρης είναι από τα πιο σημαντικά παγκοσμίως συναγωνιζόμενο τα αντίστοιχα του Ρόττερνταμ και του Χιούστον και σε συνδυασμό με την επιδιωκόμενη επέκταση των εγκαταστάσεων αποθήκευσης πετρελαίου και LNG θα εδραιώσει τον ρόλο της Σιγκαπούρης ως τον σημαντικότερο ενεργειακό κόμβο στην Ασία, λαμβάνοντας υπόψη και το γεγονός ότι υπολείπεται μόνο του Λονδίνου και της Νέας Υόρκης ως κέντρο εμπορίας πετρελαίου (Forbes, 2014).

Η σημασία των στενών είχε ως αποτέλεσμα τη σύσταση και λειτουργία διάφορων μηχανισμών για την παροχή υπηρεσιών διαχείρισης και ασφάλειας. Αναφορικά με τη εξασφάλιση της ασφαλούς ναυσιπλοΐας η Ινδονησία, η Μαλαισία και η Σιγκαπούρη από το 1977 έθεσαν σε εφαρμογή το σχέδιο Ελέγχου και Καθορισμού Ροής (Traffic Separation Scheme, TSS). Επιπλέον, το 2007, σχετική πίεση της Ιαπωνίας απέφερε τη σύσταση του Μηχανισμού Συνεργασίας (Cooperation Mechanism) υπό την αιγίδα το IMO (Graham, 2015). Το ταμείο του οργανισμού (Aids to Navigation Fund) τελεί υπό τη διαχείριση των προαναφερόμενων χωρών ενώ χρηματοδοτείται από πλήθος κρατών, όπως η Ιαπωνία, η Κίνα και η Ελλάδα. Αποστολή του είναι η παροχή υπηρεσιών πλοήγησης και χαρτογράφησης. Τέλος τα ανωτέρω κράτη έχουν δημιουργήσει το μηχανισμό Περιπολιών των Στενών της

Malacca (Malacca Strait Patrol, MSP) με σκοπό το συντονισμό διεξαγωγής περιπολιών από θαλάσσης και αέρος προς αποτροπή ενεργειών πειρατείας (Graham, 2015). Τα ανωτέρω σε συνδυασμό με το Κέντρο Πληροφοριών (Information Fusion Centre, IFC) στη Σιγκαπούρη και την εφαρμογή του Διεθνούς Κανονισμού Ασφαλείας Πλοίων και Λιμενικών Εγκαταστάσεων (International Ship and Port Facility Security Code, ISPS) όπως υιοθετήθηκε το 2002 από τον IMO, αποτελούν το βασικό συνεργατικό πλαίσιο ασφάλειας των στενών.

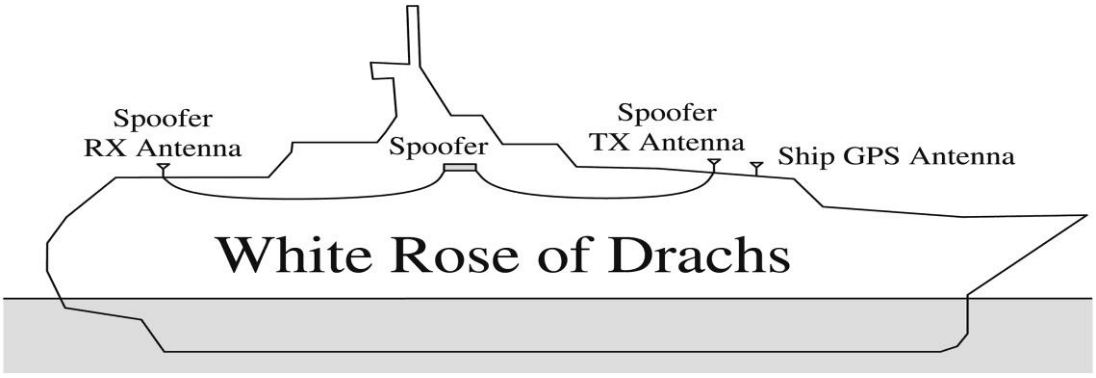
4.3. Περιπτωσιολογικές μελέτες κυβερνοεπιθέσεων σε θαλάσσιο περιβάλλον – απάντηση σε ερώτημα Ε2

Τα τελευταία χρόνια απασχολεί ολοένα και περισσότερο τον ναυτιλιακό τομέα η ύπαρξη κυβερνοαπειλών στο θαλάσσιο περιβάλλον. Τα περιστατικά κυβερνοεπιθέσεων ως επί το πλείστον αποκρύπτονται από τις ναυτιλιακές εταιρείες όμως η αύξηση τους έχει εγείρει σημαντικούς προβληματισμούς αναφορικά με την τρωτότητα της ασφάλειας στον κλάδο. Περιστατικά επίθεσης έχουν καταγραφεί ενάντια σε ναυτιλιακές εταιρείες όπως η Maersk, επιφέροντας ζημιές πολλών εκατομμυρίων και δυσχέρειες στα ηλεκτρονικά συστήματα υποστήριξης της λειτουργίας της εταιρείας καθώς και σε λιμενικές εγκαταστάσεις, όπως στο λιμένα του Antewp, με την προσβολή του ICS συστήματος διαχείρισης φορτίων, όπου φορτία εξαφανίστηκαν από το σύστημα για να ακολουθήσει και η φυσική κλοπή τους. Επιπρόσθετα επιθέσεις έχουν καταγράφει σε πλωτές πλατφόρμες εξόρυξης με απόκτηση ελέγχου των μηχανικών συστημάτων προς επηρεασμό των παραμέτρων λειτουργίας τους και συγκεκριμένα αλλαγή στην κλίση της πλατφόρμας.

Σε αντίθεση με τη συχνότητα των επιθέσεων σε παράκτιες εγκαταστάσεις ή έδρες των εταιρειών, είναι ελάχιστα τα καταγεγραμμένα περιστατικά διεξαγωγής κυβερνοεπιθέσεων σε πλοία. Πάραυτα, τα εν λόγω συμβάντα, σε συνδυασμό με διεξαγόμενες επιθέσεις από πανεπιστήμια ή εταιρείες παροχής ασφάλειας, έχουν καταδείξει την τρωτότητα πλήθους συστημάτων. Στη συνέχεια παρατίθενται ορισμένα καταγεγραμμένα περιστατικά επιθέσεων σε πλοία κατά τη διάρκεια πλου.

4.3.1. Επίθεση ομάδας του πανεπιστημίου Austin του Texas σε πολυτελές σκάφος αναψυχής

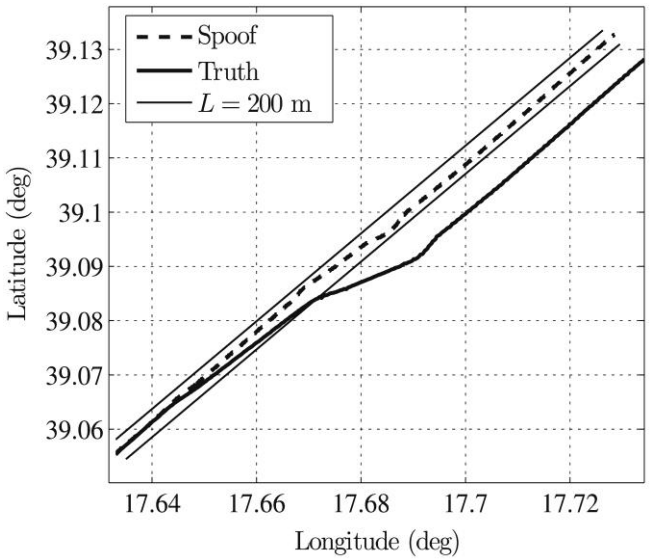
Τον Ιούνιο του 2013 ομάδα ερευνητών του πανεπιστημίου Austin του Texas, με επικεφαλής τον Todd Humphreys, διεξήγαγε ένα πείραμα στο πολυτελές σκάφος αναψυχής "White Rose of Drachs" μήκους 65 μέτρων, ύστερα από πρόσκληση του καπετάνιου και ενώ το σκάφος έπλεε στη Μεσόγειο θάλασσα. Σκοπός του πειράματος ήταν να καταδείξει την τρωτότητα του συστήματος GPS σε επίθεση τύπου spoofing. Για την επίθεση χρησιμοποιήθηκε φορητή συσκευή διεξαγωγής spoofing, κατασκευής της ερευνητικής ομάδας και χαμηλού κόστους, τοποθετημένη επί του πλοίου (Humphreys et. al., 2008) (Σχήμα 4.11). Η συσκευή λάμβανε αυθεντικό σήμα GPS και εξέπεμπε τεχνητό σήμα προς τις κεραίες GPS του σκάφους. Εντέλει τα δύο σήματα, αυθεντικό και τεχνητό, συντονίζονται και φτάνουν με τέλειο συγχρονισμό στο βαλλόμενο σύστημα και σταδιακά η δύναμη του τεχνητού σήματος υπερκαλύπτει το αυθεντικό και εν τέλει το εξαφανίζει (Bhatti & Humphreys, 2016).



Σχήμα 4.11. Διάταξη εξοπλισμού επίθετης τύπου spoofing επί του σκάφους "White Rose of Drachs" (https://onlinelibrary.wiley.com/doi/full/10.1002/navi.183)

Η επίθεση σχεδιάστηκε να διεξαχθεί με στόχο την απόκλιση από την προκαθορισθείσα, εντός ενός στενού διαδρόμου, πορεία πλεύσης, η οποία μπορούσε να εξηγηθεί ως πιθανή επίδραση θαλάσσιου ρεύματος. Η επίθεση αποτελούνταν από τρία διακριτά στάδια με διαφοροποίηση των τιμών των παραμέτρων της ταχύτητας και της επιτάχυνσης. Κατά τη διάρκεια του πειράματος ο καπετάνιος διόρθωνε συνεχώς τη πορεία του πλοίου σύμφωνα με τις ενδείξεις του GPS, με σκοπό εκείνη να διατηρηθεί εντός του καθορισμένου διαδρόμου, στην πραγματικότητα όμως το

σκάφος απέκλινε της πορείας του όπως φαίνεται στο Σχήμα 4.12 (Bhatti & Humphreys, 2015).



Σχήμα 4.12. Σύγκριση πραγματικής πορείας του σκάφους "White Rose of Drachs" σε σχέση με την πορεία βάσει των ενδείξεων του GPS κατά τη διάρκεια της επίθεσης spoofing (https://onlinelibrary.wiley.com/doi/full/10.1002/navi.183)

Η επίθεση έγινε αντιληπτή από το πλήρωμα μόνο κατά την στιγμή που το σκάφος παρέκκλινε της πορείας του κατά 3 μοίρες προς βορρά με παράλληλη ένδειξη του GPS ότι η θέση του εμφανίζονταν κάτω από το επίπεδο επιφάνειας της θάλασσας (Bhatti & Humphreys, 2015).

Το εν λόγω πείραμα κατέδειξε πως είναι εφικτή η επίθεση τύπου spoofing στο σύστημα GPS που φέρουν τα πλοία. Η διασύνδεση του GPS με συστήματα πλοήγησης και αποφυγής συγκρούσεων τα οποία αξιοποιούν τις ενδείξεις του, όπως το AIS και το ECDIS, μπορεί να επιφέρει πληθώρα κινδύνων κατά τη διάρκεια της επίθεσης για το πλοίο και το προσωπικό του (Bhatti & Humphreys, 2015).

4.3.2. Επίθεση στο πλοίο NLV Pole Star και το φαρικό σύστημα του Ηνωμένου Βασιλείου

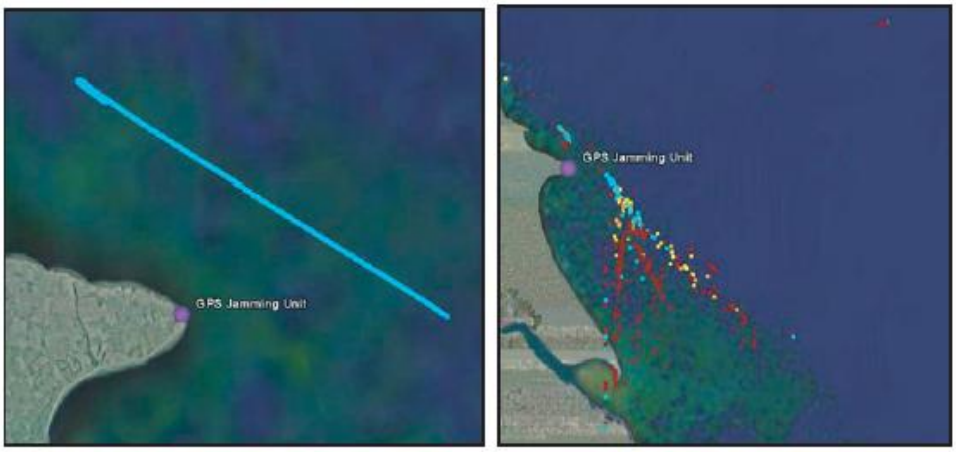
Τον Απρίλιο του 2008 στην τοποθεσία Flamborough Head στις ανατολικές ακτές του Ην. Βασιλείου η Γενική Αρχή Φάρων (General Lighthouse Authorities, GLA) διεξήγαγε επίθεση τύπου jamming στο σύστημα GPS του πλοίου Pole Star και των εγκαταστάσεων της με σκοπό να αξιολογήσει τις τρωτότητες του εν λόγω

συστήματος. Η επίθεση πραγματοποιήθηκε με τη χρήση επαγγελματικού τηλεχειριζόμενου εξοπλισμού χαμηλής έως μεσαίας ισχύος ο οποίος παρήγαγε σήμα παρεμπόδισης σε όλο του εύρος των 2MHz της συχνότητας L1 του GPS, η οποία χρησιμοποιείται για μη στρατιωτικούς σκοπούς.

Το πλοίο Pole Star κινούμενο εντός της περιοχής jamming και σε πορεία κατά μήκος της ακτογραμμής απώλεσε την ένδειξη GPS και κατέφυγε σε εναλλακτικό τρόπο πλοήγησης. Η μετάβαση έγινε επιτυχημένα, καθώς το πλήρωμα είχε προειδοποιηθεί για την επικείμενη επίθεση. Επιπλέον εκτέλεσε έγκαιρα τις απαραίτητες ενέργειες σίγασης των ενεργοποιηθέντων συναγερμών διαφόρων συστημάτων, όπως το AIS και το σύστημα βαθμονόμησης γυροσκοπίου, λόγω της απώλειας του σήματος GPS. Παρόλα τα ανωτέρω το πλοίο δεν μπόρεσε να διατηρήσει την ικανότητα εκτέλεσης ελιγμών ακριβείας ενώ εκτιμάται ότι η απώλεια του σήματος σε πραγματικές συνθήκες κατά τη διάρκεια της νυχτερινής βάρδιας ή κατά την εκτέλεση ελιγμών ακριβείας σε καταστάσεις που απαιτούν υψηλό βαθμό συγκέντρωσης, όπως ο κατάπλους σε συνθήκες περιορισμένης ορατότητας, θα επέφεραν δυσμενέστερα αποτελέσματα. Παράλληλα το ECDIS απέτυχε να ανανεώσει την εικόνα στους χάρτες λόγω της απώλειας των δεδομένων του GPS με αποτέλεσμα η εικόνα να παραμένει στατική. Το γεγονός αυτό σε συνδυασμό με τη μετάβαση σε καθεστώς παραδοσιακής ναυσιπλοΐας με χρήση έντυπων χαρτών δημιούργησε εκνευρισμό σε μέλη του πληρώματος, που εικάζεται ότι οφείλεται στην εξάρτηση από τα αυτοματοποιημένα συστήματα πλοήγησης (Grant et. al., 2009).

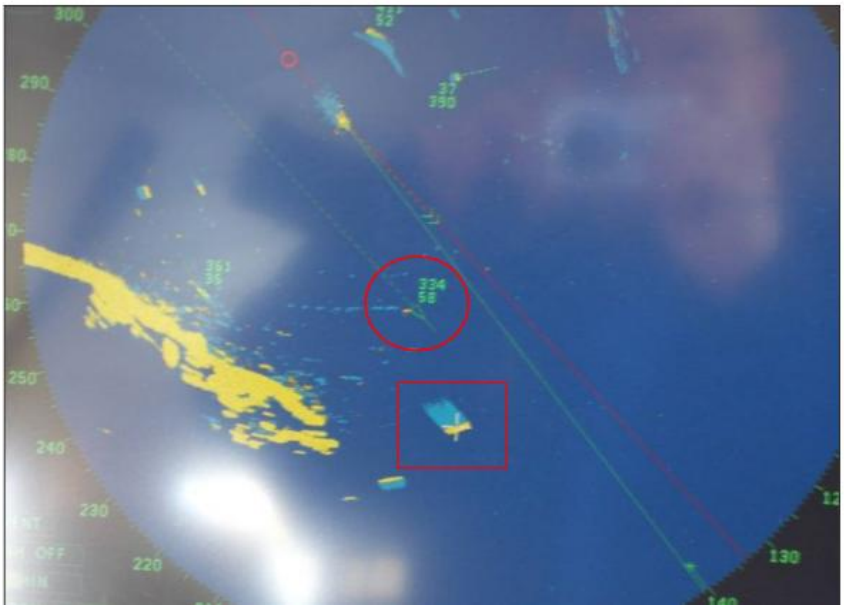
Κατά μήκος των ακτών του Ηνωμένου Βασιλείου υπάρχουν 14 σταθμοί της GLA οι οποίοι με τη χρήση του GPS παρέχουν στους ναυτιλλόμενους δεδομένα για να προσδιορίσουν με μεγαλύτερη ακρίβεια το στίγμα τους. Ο κάθε σταθμός αποτελείται από δύο συστήματα, το σταθμό αναφοράς (Reference Station, RS) και τη μονάδα παρακολούθησης ακεραιότητας (Integrity Monitor Unit, IM) τα οποία είναι αμφότερα σε σύνδεση με δορυφόρους λαμβάνοντας δεδομένα GPS για μεγαλύτερη ακρίβεια. Κατά τη διάρκεια της επίθεσης jamming σε έναν από αυτούς διαπιστώθηκε ότι η σταδιακή αύξηση της ισχύος του εκπεμπόμενου σήματος επέφερε σταδιακή απώλεια της επαφής με τους συνδεδεμένους δορυφόρους και στις δύο ανωτέρω μονάδες. Όταν ο αριθμός των δορυφόρων έπεσε κάτω του επιθυμητού ορίου ο σταθμός τέθηκε σε κατάσταση συναγερμού αποδεικνύοντας ότι το σύστημα εμφανίζει τρωτότητα σε επιθέσεις τύπου jamming (Grant et. al., 2009). Αντίστοιχος εξοπλισμός δέκτης των πληροφοριών του εν λόγω συστήματος τοποθετήθηκε στο

πλοίο Pole Star ο οποίος επηρεάστηκε αισθητά εντός της περιοχής jamming εμφανίζοντας ενδείξεις με μεγάλη απόκλιση από την πραγματικότητα τόσο ως προς τη θέση όσο και ως προς την ταχύτητα του πλοίου (Σχήμα 4.13).



Σχήμα 4.13. Εικόνα Google Earth με τις καταγεγραμμένες θέσεις του πλοίου NLV Pole Star χωρίς GPS jamming (αριστερά) και με GPS jamming (δεξιά) με τα χρώματα να αντιπροσωπεύουν την αποδιδόμενη στο πλοίο ταχύτητα (u) όπου μπλε u<15 κόμβων, κίτρινο u<50 κόμβων, πορτοκαλί u<100 κόμβων και κόκκινο u>100 κόμβων (http://www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf)

Όσον αφορά το σύστημα AIS, το jamming του GPS επηρέασε πέρα από την εμφανιζόμενη θέση του πλοίου στο σύστημα και τον συγχρονισμό με τα δεδομένα των υπολοίπων χρηστών. Αν και υφίσταται η δυνατότητα συγχρονισμού με δεδομένα προερχόμενα από σταθμό ξηράς, επίθεση με στόχο την άρνηση παροχής υπηρεσιών, όπως πραγματοποιήθηκε από την GLA, εκτιμάται ότι θα αχρήστευε το σύστημα AIS (Grant et. al., 2009). Αποδεικτικό στοιχείο αποτελεί η απόκλιση της εικόνας του ραντάρ σε σχέση με εκείνη του AIS αναφορικά με τη θέση του σκάφους υπ' αριθμόν 33458 (Σχήμα 4.14).



Σχήμα 4.14. Εικόνα του ραντάρ του NLV Pole Star με επικάλυψη εικόνας του συστήματος AIS επί του πλοίου όπου στο κόκκινο τετράγωνο εμφανίζεται η θέση του πλοίου υπ' αριθμόν 33458 κατά το ραντάρ ενώ στον κόκκινο κύκλο η θέση του κατά το AIS (http://www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf)

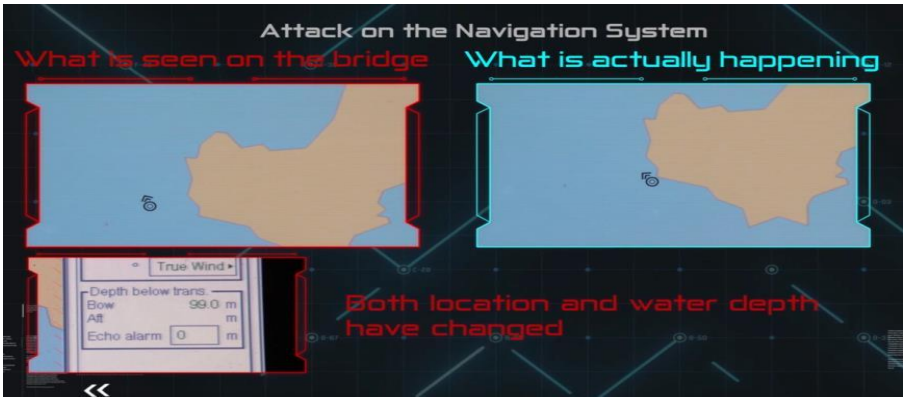
Το εν λόγω πείραμα απέδειξε ότι η διεξαγωγή επίθεσης τύπου jamming στο σύστημα GPS μπορεί να επηρεάσει την πλοήγηση, τα συστήματα ναυτιλίας, όπως το AIS και το ECDIS, και να επιφέρει παραπλανητική εικόνα σε σχέση με την πραγματικότητα. Επίθεση κατά τη διάρκεια αυτόματης πλοήγησης μπορεί να περάσει απαρατήρητη από το πλήρωμα και να οδηγήσει σε επικίνδυνες καταστάσεις για την ασφάλεια πλοίου και πληρώματος. Η αδιαμφισβήτητη αποδοχή της ορθότητας των δεδομένων του GPS, η απώλεια της οικειότητας με τη χρήση εναλλακτικών μεθόδων ναυσιπλοΐας και η εξάρτηση του πληρώματος από το ECDIS αυξάνουν αισθητά την πιθανότητα ατυχήματος.

4.3.3. Διεξαγωγή κυβερνοεπιθέσεων σε βασικά συστήματα λειτουργίας πλοίου από την εταιρεία Naval Dome

Η εταιρεία Naval Dome, με έδρα το Ισραήλ, διεξήγαγε σειρά επιθέσεων με σκοπό να καταδείξει την τρωτότητα των συστημάτων που χρησιμοποιούνται

ευρύτατα από εμπορικά πλοία παντός τύπου. Με την συναίνεση και υπό την επίβλεψη εταιρειών και ιδιοκτητών επιτέθηκε σε συστήματα ναυτιλίας, ελέγχου μηχανών, αντλιών και προώσεως. Η επιτυχία των επιθέσεων είχε ως αποτέλεσμα την μεταβολή της θέσεως του πλοίου μέσω της παραποίησης των χαρτών στο ραντάρ, την ακινητοποίηση μηχανημάτων, την παραποίηση ενδείξεων καυσίμου και δεξαμενών ερμάτων και τη χειραγώγηση του συστήματος πηδαλιούχησης (Wee, 2017).

Αρχικά η εταιρεία επιτέθηκε στο σύστημα ECDIS μέσω μηνύματος ηλεκτρονικής αλληλογραφίας (email) που στάλθηκε στον ηλεκτρονικό υπολογιστή του κυβερνήτη, ο οποίος είναι συνδεδεμένος με το διαδίκτυο μέσω δορυφορικής σύνδεσης και μεταξύ των άλλων χρησιμοποιείται για την επικαιροποίηση των χαρτών ναυτιλίας του ECDIS καθώς και την ανταλλαγή λογιστικών-διαχειριστικών δεδομένων με τις βάσεις διαχείρισης δεδομένων της εταιρείας. Ο ιός εγκαταστάθηκε στο σύστημα κατά την πρώτη επικαιροποίηση των ηλεκτρονικών χαρτών και ενεργοποιήθηκε σε επιλεγμένο σημείο κατά τη διάρκεια του πλου, και συγκεκριμένα σε στενό πέρασμα κατά τη νυκτερινή βάρδια, όπου συνήθως υπάρχει μειωμένο προσωπικό και ορατότητα στη γέφυρα του πλοίου. Όλες οι ενδείξεις του ECDIS όπως θέση, κατεύθυνση, βύθισμα και ταχύτητα, αν και παραποιημένες, παρουσίαζαν συλλογικά μια λογική εικόνα, η οποία όμως απείχε από την πραγματική (Σχήμα 4.15).

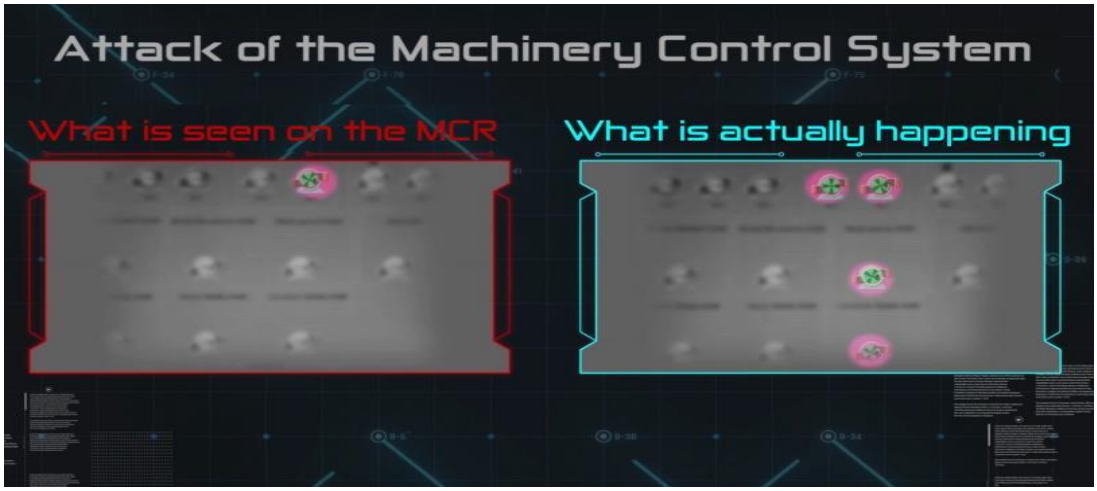


Σχήμα 4.15. Εικόνα του ECDIS (αριστερά) κατά την επίθεση της εταιρείας Naval Dome και πραγματική κατάσταση (δεξιά) (https://worldmaritimenews.com/archives/238869/nightmare-scenario-ship-critical-systems-easy-target-for-hackers/)

Η επόμενη επίθεση έλαβε χώρα στο ραντάρ του πλοίου, το οποίο θεωρείται σε γενικές γραμμές ένα απομονωμένο σύστημα και συνεπώς μη διαβλητό σε

κυβερνοεπιθέσεις. Η επίθεση έγινε διαμέσου του διακόπτη μεταγωγής του τοπικού δικτύου (Local Ethernet Switch Interface) που συνδέει το ραντάρ με το ECDIS, το BAS και το VDR. Κατά την επίθεση κατέστη δυνατή η απόκρυψη στόχων απλά και μόνο διαγράφοντάς τους από την οθόνη ενώ το ραντάρ εμφανίζονταν να λειτουργεί κανονικά (Wee, 2017).

Τέλος η εταιρεία επιτέθηκε στο κέντρο ελέγχου μηχανικών συστημάτων (Machinery Control System, MCS). Η μέθοδος που ακολουθήθηκε ήταν η επίθεση με την εισαγωγή κακόβουλου λογισμικού στο σύστημα από μολυσμένο USB μέσω θύρας εισόδου-υποδοχής. Ο ιός προσέβαλλε άμεσα όλα τα βοηθητικά συστήματα, όπως τον κεντρικό εξαερισμό, το σύστημα διαχείρισης καυσίμου, το σύστημα των γεννητριών και κατέστη εφικτός ο επηρεασμός των παραμέτρων λειτουργίας τους. Συγκεκριμένα στο σύστημα ερμάτων, ενώ η ένδειξη λειτουργίας εμφανίζονταν ως κανονική, η λειτουργία των μερών του συστήματος, όπως εκείνη των αντλιών, είχε σταματήσει (Σχήμα 4.16). Ο συγκεκριμένος τρόπος επίθεσης γεννά έντονους προβληματισμούς ως προς το γεγονός ότι κατασκευαστές συστημάτων ή επισκευαστικοί φορείς, κατά τη διάρκεια διεξαγωγής διαγνωστικών ελέγχων, εργασιών επισκευής και συντήρησης ή αναβαθμίσεις λογισμικού, μπορεί εν αγνοία τους ή μη, να καταστούν φορείς κυβερνοεπίθεσης με εισαγωγή μολυσμένου λογισμικού, επηρεάζοντας την λειτουργία του συνόλου των διασυνδεδεμένων συστημάτων (Wee, 2017).



Σχήμα 4.16. Εικόνα του πίνακα ελέγχου του MCR (αριστερά) κατά την επίθεση της εταιρείας Naval Dome και πραγματική κατάσταση (δεξιά) (https://worldmaritimenews.com/archives/238869/nightmare-scenario-ship-critical-systems-easy-target-for-hackers/)

4.3.4. Επίθεση τύπου spoofing σε GPS πλοίου στη Μαύρη Θάλασσα

Στις 24 Ιουνίου 2017 πλοίο ανοικτά του λιμένα Novorossiysk της Ρωσίας στη Μαύρη θάλασσα ανέφερε στη υπηρεσία ναυσιπλοΐας της Ακτοφυλακής των Η.Π.Α (US Coast Guard Navigation Center) πως σύμφωνα με την ένδειξη στο σύστημα GPS η θέση του εμφανίζονταν 32 χιλιόμετρα μακριά από την πραγματική και συγκεκριμένα κοντά στο αεροδρόμιο Gelendyhik (Hampling, 2017). Το GPS τοποθετούσε το πλοίο στην ενδοχώρα και μάλιστα, σύμφωνα με την αντίστοιχη ένδειξη, με ακρίβεια προσδιορισμού θέσεως της τάξεως των 100 μέτρων, όπως φαίνεται στο σχήμα 4.17 (Goward, 2017).

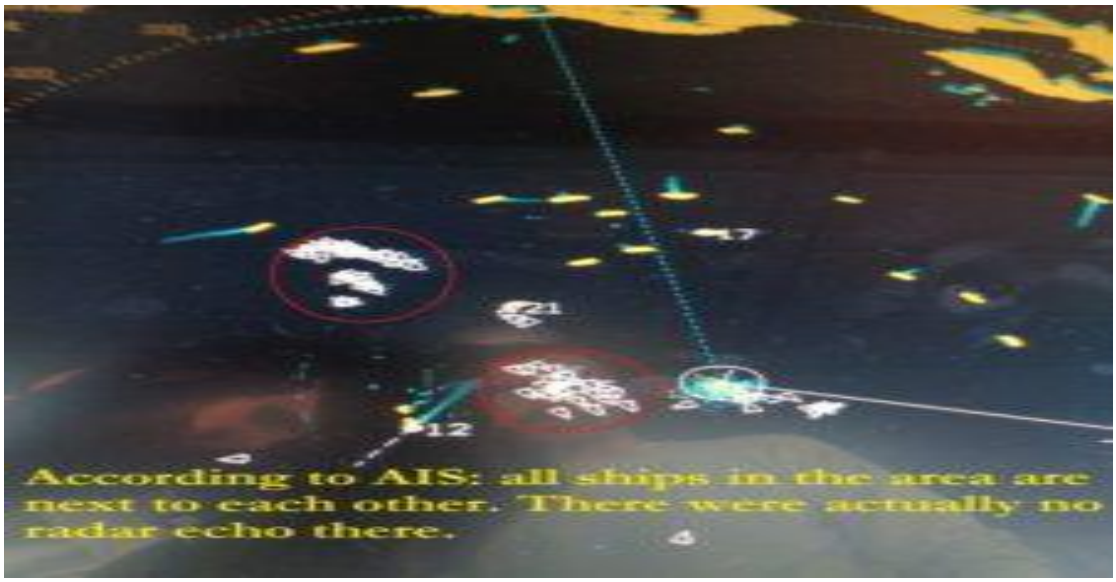
Σχήμα 4.17. Ένδειξη GPS σε αντιπαραβολή με τις πραγματικές συντεταγμένες θέσεως (https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)

Η Ακτοφυλακή αφού επιβεβαίωσε ότι δεν υπήρχε κώλυμα στην παροχή σήματος GPS στην περιοχή, ενημέρωσε το πλοίο για την κανονικότητα του GPS και την ακρίβεια των ενδείξεών του με απόκλιση 3 μέτρων και απέδωσε το περιστατικό

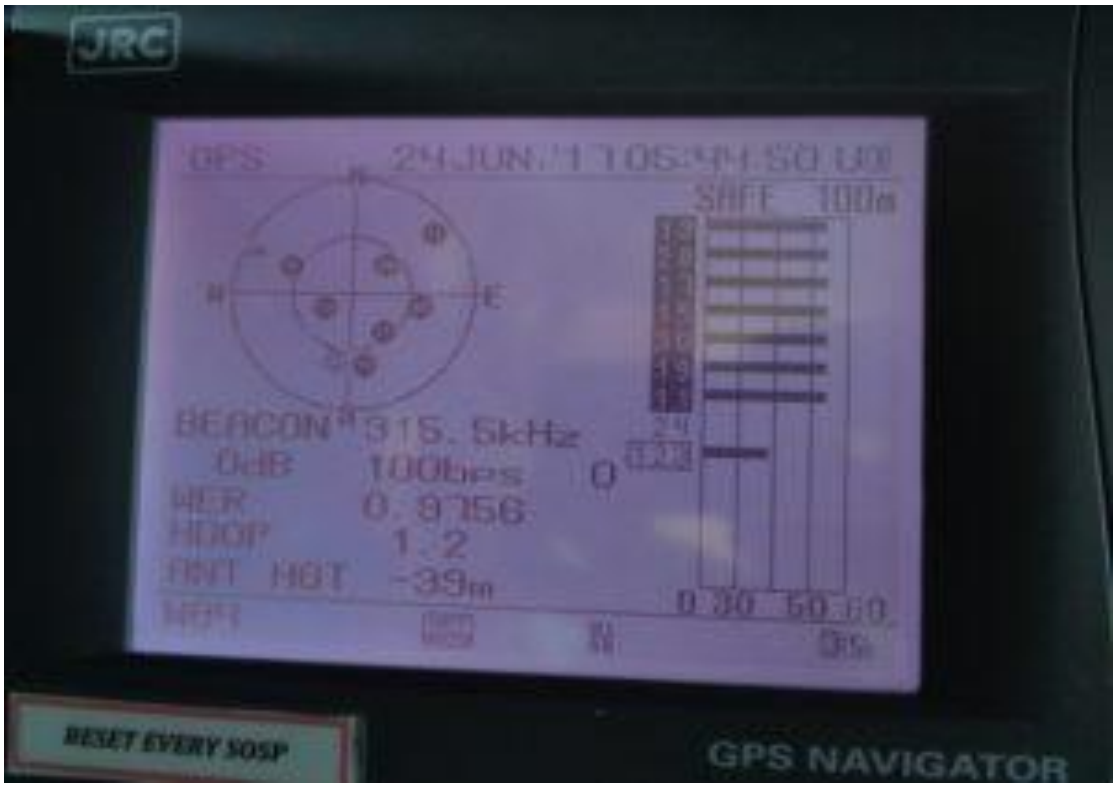
σε πιθανό πρόβλημα αναβαθμίσεως του λειτουργικού συστήματος. Το πλοίο επιβεβαίωσε την σωστή λειτουργία του λειτουργικού συστήματος και ανέφερε πως κατά την διάρκεια των τελευταίων ημερών και κατόπιν επικοινωνίας με άλλα πλοία το GPS εμφάνιζε διαλλειματική λειτουργία ως προς την ορθότητα των ενδείξεων. Προς επιβεβαίωση των ανωτέρω το πλοίο απέστειλε φωτογραφικό υλικό της 24ης Ιουνίου από τις οθόνες πλοήγησης με εμφανή την ένδειξη προσδιορισμού της θέσης του από το GPS καθώς και έντυπο ναυτιλιακό χάρτη με προσδιορισμό της πραγματικής θέσης του πλοίου προς αντιπαραβολή (Σχήμα 4.18).

Σχήμα 4.18. Ένδειξη GPS και αντίστοιχη απεικόνιση σε έντυπο ναυτιλιακό χάρτη (https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)

Επιπρόσθετα απέστειλε οθόνη από το σύστημα AIS στο οποίο τα πλοία της περιοχής εμφανίζονται το ένα δίπλα στο άλλο (Σχήμα 4.19) καθώς και οθόνη του GPS όπου εμφανίζεται ένδειξη ότι το πλοίο ευρίσκεται 39 μέτρα κάτω από την επιφάνεια της θάλασσας, όλοι οι συνδεδεμένοι δορυφόροι φαίνεται εκπέμπουν σε συχνότητα ίδιας ισχύος και ο βαθμός λάθους της ένδειξης σφάλματος (Word Error Rate, WOR) εμφανίζει τιμή 97 με την κανονική να είναι μικρότερη του 10 (Σχήμα 4.20) (Goward, 2017).



Σχήμα 4.19. Εικόνα AIS με λανθασμένη ένδειξη θέσεως πλοίων(https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)



Σχήμα 4.20. Εικόνα οθόνης GPS με προσδιορισμό θέσεως πλοίου 39 μέτρα κάτω από την επιφάνεια της θάλασσας (https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/)

Οι ενδείξεις του GPS, όπως εμφανίζονται στη Σχήμα 4.20, θεωρούνται από ειδικούς, μεταξύ των οποίων ο David Last, πρώην πρόεδρος του Βασιλικού Οργανισμού Ναυσιπλοΐας του Ην. Βασιλείου (UK Royal Institute of Navigation) και ο καθηγητής Todd Humphreys του Πανεπιστημίου Austin του Τέξας, ως το πρώτο επίσημα καταγεγραμμένο περιστατικό GPS spoofing. Ο Humphreys θεωρεί ότι το συγκεκριμένο περιστατικό αποτελεί αποτέλεσμα δοκιμών νέας τακτικής ηλεκτρονικού πολέμου. Η συγκεκριμένη τεχνολογία, όπως υποστηρίζει, είναι προσβάσιμη σε επίπεδο τρομοκρατικών οργανώσεων αλλά η χρήση της από κράτη αποτελεί το πιο πιθανό σενάριο, με σκοπό να εκτρέψουν από την πορεία τους οχήματα, μη επανδρωμένα αεροσκάφη (Unmanned Aerial Vehicles - UAV) και να αποκτήσουν τον έλεγχο αυτόνομων πλοίων (Hampling, 2017).

4.4. Σύνθεση – απάντηση σε ερώτημα Ε3

Ο όρος γεωπολιτική προσδιορίζει την μελέτη των διεθνών σχέσεων υπό το πρίσμα της γεωγραφίας, δίνοντας έμφαση στη διάσταση του χώρου και ειδικότερα στους περιορισμούς που αυτή θέτει στα κράτη, τους τρόπους με τους οποίους προσπαθούν να ξεπεράσουν τους εν λόγω περιορισμούς και το πως τη χρησιμοποιούν προς όφελός τους (Germond, 2015). Στην πορεία η χρήση του όρου ως επιχείρημα των ναζί για τη νομιμοποίηση του γερμανικού επεκτατισμού του προσέδωσε αρνητική χροιά. Όμως γεωπολιτικές προσεγγίσεις επηρέασαν τις διεθνείς σχέσεις του 20ου αιώνα. Ο Mackinder, όρισε ως Καρδιά (Heartland) την έκταση που ορίζεται από την Ανατολική Ευρώπη και το μεγαλύτερο ασιατικό τμήμα της πρώην Ρωσικής αυτοκρατορίας θεωρώντας ότι περιβάλλεται από δύο ημικύκλια, το εσωτερικό (Κίνα, Ινδία, Ιράν ,Τουρκία, Γερμανία) και το εξωτερικό (Δυτική Ευρώπη, Αμερική, Αφρική). Ορίζοντας ως Παγκόσμια Νήσο την ηπειρωτική μάζα Ευρώπης-Ασίας-Αφρικής υποστήριξε πως όποιος ελέγχει την Καρδία ελέγχει την Παγκόσμια Νήσο και συνεπώς ελέγχει τον κόσμο, αναθεωρώντας όμως στην πορεία καθώς υποστήριξε την ύπαρξη του Ατλαντικού Βάθρου Ισχύος το οποίο εξισορροπεί τον έλεγχο της Καρδιάς. (Κολιόπουλος, 2008). Ο Spykman βασίστηκε στην ανωτέρω θεωρία, προσδιόρισε ως Στεφάνη (Rimland) τις περιοχές του εσωτερικού ημικυκλίου και τόνισε τη σημασία τους υποστηρίζοντας πως όποιος ελέγχει τη Στεφάνη εξουσιάζει την Ευρασία και συνεπώς τον κόσμο (Κολιόπουλος, 2008). Σε μεταγενέστερο χρόνο, ο Mearsheimer, στο πλαίσιο της ανάλυσης του επιθετικού ρεαλισμού, υποστήριξε

πως επειδή η παγκόσμια κυριαρχία είναι ανέφικτη, σε αντίθεση με την κυριαρχία σε μια περιφέρεια, στόχος κάθε μεγάλης δύναμης είναι να κυριαρχήσει στην περιφέρεια της εμποδίζοντας παράλληλα τις άλλες μεγάλες δυνάμεις να επιτύχουν το ίδιο στις δικές τους περιφέρειες (Mearsheimer, 2006). Έκτοτε έχει διατυπωθεί πλήθος γεωπολιτικών προσεγγίσεων καθώς και θεωρίες διεθνών σχέσεων που λαμβάνουν υπόψη τη γεωπολιτική ως παράμετρο. Οι σύγχρονες γεωπολιτικές προσεγγίσεις δίνουν έμφαση στην συνεχώς αυξανόμενη γεωπολιτική δυναμική της Ευρασίας σε σχέση πρωτίστως με την Αμερική και δευτερευόντως με την Αφρική, τη ζωτική σημασία των θαλασσίων οδών επικοινωνίας τόσο για εμπορικούς όσο και για στρατιωτικούς σκοπούς καθώς και στον έλεγχο της εξόρυξης, εκμετάλλευσης και διανομής των ενεργειακών πόρων σε παγκόσμια κλίμακα (Κολιόπουλος, 2008).

Στον αντίποδα της νεοφιλελεύθερης προσέγγισης περί του εφικτού της προώθησης της δημοκρατίας και της συνεργασίας των κρατών μέσω διεθνών θεσμών σε έναν άναρχο κόσμο, με βασική παραδοχή την αποδοχή ύπαρξης απόλυτων κερδών, η νεορεαλιστική προσέγγιση αντιτάσσει το επιχείρημα πως εφόσον ο κόσμος παραμένει άναρχος και ανταγωνιστικός τα σχετικά κέρδη έχουν ουσιώδη σημασία στη διαμόρφωση των διακρατικών σχέσεων (Baylis, Smith & Owens, 2011). Η συνεχής ανακατανομή ισχύος μεταξύ των μεγάλων δυνάμεων σε σχέση και με τον ανταγωνισμό για την επίτευξη ή αποτροπή περιφερειακής κυριαρχίας κατά τον Mearsheimer, η πληθώρα των μη κρατικών διεθνών δρώντων ιδιαίτερα με τη μορφή τρομοκρατικών οργανώσεων, το εύρος και η σημασία του διεθνούς εμπορίου σε σχέση με τις αλληλεπιδράσεις και διασυνδέσεις που δημιουργεί μεταξύ των κρατών καθώς και ο ρόλος του στην ευημερία των σύγχρονων κοινωνιών, η άμεση μετάδοση των οικονομικών κρίσεων ανά την υφήλιο όπως η διάχυση της αστάθειας που προκλήθηκε από το δυτικό χρηματοπιστωτικό σύστημα στο σύνολο των κρατών και οδήγησε σε μείωση της τάξης του 9% στο παγκόσμιο εμπόριο (World Trade Organization, 2009) αποτελούν βασικά στοιχεία του πλαισίου συνύπαρξης των δρώντων στο σύγχρονο κόσμο.

Η οικονομική ανάπτυξη, που αποτελεί τόσο μέτρο ευημερίας των κοινωνιών όσο και παράγοντα ισχύος των κρατών, εξαρτάται πρωτίστως από την απρόσκοπτη και προσιτή παροχή ενεργειακών πόρων και συνεπώς το πεδίο της ενεργειακής ασφάλειας αποτελεί σημαντική παράμετρο χάραξης της υψηλής στρατηγικής των κρατών. Με τη συντριπτική πλειοψηφία των σημαντικότερων ενεργειακών πόρων, ήτοι πετρέλαιο και φυσικό αέριο, να μεταφέρονται δια θαλάσσης, γίνεται αντιληπτό

πως η εξασφάλιση και εγγύηση της ασφάλειας του ενεργειακού εμπορίου διαμέσου των κύριων θαλασσιών εμπορικών οδών (SLOCs) αποτελεί ύψιστη προτεραιότητα για καταναλωτές και παραγωγούς. Παράλληλα το γεωπολιτικό κέντρο του πλανήτη μεταφέρεται από το δυτικό κόσμο στην ευρύτερη περιοχή της ανατολικής Ασίας, κυρίως λόγω των υψηλών ρυθμών οικονομικής ανάπτυξης των ασιατικών οικονομιών όπως η Κίνα και η Ινδία. Το γεγονός ότι οι εν λόγω χώρες καλύπτουν την πλειοψηφία των ενεργειακών τους απαιτήσεων μέσω εισαγωγών από χώρες της Μέσης Ανατολής, αναδεικνύει τη σπουδαιότητα της περιοχής του Ινδικού ωκεανού και των διερχόμενων SLOCs. Στο πλαίσιο της θαλάσσιας ενεργειακής ασφάλειας στον Ινδικό ωκεανό, η εξασφάλιση της ελεύθερης ναυσιπλοΐας και η ανεμπόδιστη διακίνηση του πετρελαίου και του φυσικού αερίου αποτελούν προτεραιότητα για τις εμπλεκόμενα κράτη (Forbes, 2014). Τα ανωτέρω επιτυγχάνονται με αποτελεσματική αντιμετώπιση συναφών απειλών, όπως περιορισμοί ή απαγόρευση της ναυσιπλοίας σε choke points ή γενικότερα σε διεθνείς εμπορικές οδούς, τρομοκρατικές ενέργειες ή ασύμμετρες επιθέσεις όπως κυβερνοεπιθέσεις σε πλοία και παράκτιες εγκαταστάσεις προερχόμενες κυρίως από μη κρατικούς δρώντες και την παρεμπόδιση ή διακοπή της ροής δια θαλάσσης των ενεργειακών πόρων (Forbes, 2014). Στις κυριότερες απειλές κατά της ναυσιπλοΐας, πέραν των περιστατικών πειρατείας στα σημαντικότερα choke points της περιοχής (Kosai & Unesaki, 2016), ήτοι τα στενά του Hormuz, της Malacca και του Bab el mandeb, καθώς και των καταστροφών εξαιτίας των καιρικών συνθηκών, φαίνεται να συγκαταλέγεται και η εκδήλωση κυβερνοεπίθεσης στο θαλάσσιο περιβάλλον και ειδικότερα σε επίπεδο πλοίου.

Η τεχνολογική εξέλιξη και σε μεγάλο βαθμό το διαδίκτυο έφεραν επανάσταση και στον τομέα της ναυτιλίας. Τα πλοία διαθέτουν πληθώρα συστημάτων που ρυθμίζουν λειτουργικές παραμέτρους όπως συστήματα προώσεως και ενέργειας, ναυτιλίας, διαχείρισης φορτίου, ασφαλείας και ανταλλάσουν ψηφιακά δεδομένα μέσω του διαδικτύου με τη στεριά όντας συνδεδεμένα με τις βάσεις δεδομένων της μητρικής εταιρείας μέσω της ανάπτυξης των συστημάτων IT και επικοινωνίας. Τα σύγχρονα πλοία λειτουργούν ολοένα και περισσότερο μέσα στο ψηφιακό περιβάλλον με την τάση αυτή να γίνει πιο έντονη καθώς εταιρείες όπως η Rolls Royce και η Yara Bikerland φιλοδοξούν να αναπτύξουν πλήρως λειτουργικά, μη επανδρωμένα, αυτόνομα πλοία (Ong, 2017· Paris, 2017). Η αυξανόμενη έκθεση στο διαδίκτυο και αυτοματοποίηση της λειτουργίας συνεπάγονται ανάλογες τρωτότητες και έκθεση σε κυβερνοαπειλές, οι οποίες μπορούν να πλήξουν κύρια συστήματα του πλοίου όπως τα

GPS, AIS, ECDIS και ICS συστήματα. Πανεπιστημιακές ομάδες, εταιρείες κυβερνοασφάλειας και πραγματικά περιστατικά έχουν αποδείξει την εφικτότητα εκδήλωσης διαφόρων τύπων κυβερνοεπιθέσεων στα συστήματα πλοίων. Η υπαρκτή απειλή κυβερνοεπιθέσεων παραπέμπει σε τακτικές και αντιλήψεις που εκφράστηκαν από τον Σουν Τσου στο έργο Η Τέχνη του Πολέμου και που ενέπνευσαν τον William Cohen να εκφράσει την άποψη ότι η ολοένα αυξανόμενη εξάρτηση από συστήματα πληροφορικής θα αύξανε την τρωτότητα σε κυβερνοεπιθέσεις καθιστώντας ευάλωτα ενεργειακά δίκτυα, υποδομές, επικοινωνιακά και τραπεζικά συστήματα (Πλατιάς & Κολιόπουλος, 2015).

Τα τάνκερ ως μέσο μεταφοράς των ενεργειακών πόρων, μπορούν να αποτελέσουν στόχο κυβερνοεπιθέσεων προερχόμενες τόσο από μη κρατικούς δρώντες, όπως τρομοκρατικές οργανώσεις, οργανωμένο έγκλημα ή ομάδες hackers χρηματοδοτούμενες από εμπορικούς ανταγωνιστές, όσο και από κράτη. Ειδικότερα τα τελευταία, μπορούν να επιλέξουν έμμεσες μεθόδους αντιπαράθεσης μεταξύ τους, προσπαθώντας να πλήξουν τα ζωτικά συμφέροντα των αντιπάλων τους, όπως το δίκτυο μεταφοράς των ενεργειακών πόρων και συνεπώς τη στρατηγική ενεργειακής ασφάλειας άλλων κρατών. Συναφή με τα ανωτέρω είναι η θεωρία των πέντε ομόκεντρων κύκλων του John Warden, η οποία παρά το γεγονός ότι αναφέρεται σε αεροπορική στρατηγική μπορεί να έχει και μερικές ευρύτερες προεκτάσεις. Ο αντίπαλος αναλύεται υπό το πρίσμα ομόκεντρων σφαιρών όπου η κεντρική αναφέρεται στην ηγεσία ενώ οι υπόλοιπές στα ουσιώδη στοιχεία (ενέργεια, οικονομία), την υποδομή μεταφορών (δρόμοι, λιμάνια), τον πληθυσμό και τις ένοπλες δυνάμεις. Σύμφωνα με τη θεωρία εάν δεν είναι εφικτή η εξόντωση της ηγεσίας, επόμενος στόχος είναι η παράλυση του συστήματος με επιθέσεις στα ουσιώδη του στοιχεία και στα δίκτυα μεταφορών. Η εν λόγω θεωρία αναδεικνύει τη σημασία της ενέργειας και των μεταφορών για κάθε κράτος.

Οι κυβερνοεπιθέσεις σε τάνκερ μπορούν να οδηγήσουν σε απώλεια του ελέγχου των συστημάτων ναυσιπλοΐας, πρόωσης και ενέργειας, βοηθητικών μηχανημάτων, διαχείρισης φορτίου και ασφαλείας. Επιπτώσεις των ανωτέρω δύναται να είναι η βύθιση λόγω έκρηξης, πιθανής σύγκρουσης με όγκους στεριάς ή άλλα πλοία, η απώλεια ανθρωπίνων ζωών ή τραυματισμός μελών του πληρώματος, η απώλεια του φορτίου με παράλληλη πρόκληση εκτεταμένης περιβαλλοντολογικής καταστροφής, η παρέκκλιση από την πορεία και η παραβίαση συμμόρφωσης με οδηγίες αρμόδιων αρχών. Παράλληλα σε επίπεδο επιχείρησης, η ιδιοκτήτρια εταιρεία

αντιμετωπίζει επιπρόσθετα υψηλά κόστη λόγω απώλειας φορτίου, απαίτησης ανάληψης ενεργειών αποκατάστασης περιβαλλοντολογικών καταστροφών, αδυναμίας τήρησης συμβατικών υποχρεώσεων ως προς την έγκαιρη παράδοση, αμφισβήτηση φήμης και αξιοπιστίας καθώς επίσης και πιθανή απώλεια ζωτικών πληροφοριών λόγω υποκλοπής στις βάσεις δεδομένων. Επιπρόσθετα, πέραν των οικονομικών συνεπειών δημιουργείται κλίμα αβεβαιότητας στον ευρύτερο ναυτιλιακό κλάδο τόσο ως προς την ίδια τη λειτουργία του όσο και ως προς την ασφάλεια της περιοχής όπου λαμβάνει χώρα το όποιο περιστατικό.

Πέραν των ανωτέρω, οι κυβερνοεπιθέσεις στο ναυτιλιακό κλάδο είναι πιθανό να έχουν ως απώτερο στόχο την ενεργειακή ασφάλεια κράτους ή ομάδας κρατών. Ένα τάνκερ υπό τον έλεγχο μιας τρομοκρατικής οργάνωσης αποτελεί ασύμμετρη απειλή με ποικίλους τρόπους. Δύναται να χρησιμοποιηθεί για να προκαλέσει σύγκρουση με άλλα πλοία με σκοπό να επιφέρει αβεβαιότητα και παρεμπόδιση της ναυσιπλοΐας σε κάποιο choke point για ορισμένο χρονικό διάστημα ή σε συγκεκριμένη συγκυρία, διαταράσσοντας την ροή των ενεργειακών πόρων και αυξάνοντας τις τιμές τους. Τα ίδια αποτελέσματα μπορούν να επιτευχθούν με παρέκκλιση ενός ή ομάδας τάνκερ από τον προκαθορισμένο πλου. Επιπρόσθετα μπορεί να χρησιμοποιηθεί για την καταστροφή ζωτικών υποδομών με το να εμβολίσει εγκαταστάσεις διυλιστηρίων, πλωτές πλατφόρμες εξόρυξης και σημαντικές λιμενικές εγκαταστάσεις. Παράλληλα η απώλεια τάνκερ ναυτιλιακών εταιρειών συμφερόντων σε στενή σύνδεση με συγκεκριμένες κρατικές οικονομίες, όπως το γεγονός ότι η διακίνηση του ήμισυ των εισαγωγών πετρελαίου της Κίνας επιτελείται από τάνκερ κινεζικής ιδιοκτησίας (Graham, 2015), απαιτεί σημαντικό χρόνο αναπλήρωσης των απωλειών σε επίπεδο δομών και δυνατοτήτων και μπορεί να αποτελέσει μοχλό άσκησης πίεσης στα εν λόγω κράτη.

Κεφάλαιο 5: Συμπεράσματα

5.1. Ανασκόπηση

Η παρούσα διπλωματική επιχειρεί να αναδείξει τη διάσταση της ασφάλειας των θαλασσίων μεταφορών ενεργειακών φορτίων στον Ινδικό ωκεανό υπό την απειλή εκδήλωσης κυβερνοεπιθέσεων σε πλοία, συνυπολογιζομένων των γεωγραφικών δεδομένων της περιοχής.

Η ενεργειακή ασφάλεια είναι άρρηκτα συνδεδεμένη με την συνεχή ροή και σε προσιτή τιμή των ενεργειακών πόρων. Με το μεγαλύτερο ποσοστό του παγκόσμιου εμπορίου να διεξάγεται διαμέσου των SLOCs, η κυβερνοασφάλεια σε επίπεδο πλοίου αποτελεί σημαντική παράμετρο της θαλάσσιας ασφάλειας. Η πολυπλοκότητα και αλληλεπίδραση μεταξύ των βασικών συστημάτων λειτουργίας των πλοίων αυξάνει την τρωτότητα σε περίπτωση εκδήλωσης κυβερνοεπιθέσεων, γεγονός που ενισχύεται και από τη γεωγραφία του Ινδικού ωκεανού, όπου η κυριότερη SLOC διέρχεται από τα πολυσύχναστα choke points του Hormuz και της Malacca. Τα πλοία μεταφοράς ενεργειακών φορτίων, όπως τα τάνκερ, είναι ευάλωτα σε κυβερνοεπίθεσεις, που ως στόχο μπορεί να έχουν την ενεργειακή ασφάλεια των κρατών, τα δίκτυα θαλασσίων μεταφορών, την καταστροφή ενεργειακών δομών και εγκαταστάσεων και τη δημιουργία έντασης σε επιλεγμένες χρονικές στιγμές και σε συγκεκριμένες περιοχές του πλανήτη.

Υπό το πρίσμα των ανωτέρω και όσον αφορά τα εξεταζόμενα ερευνητικά ερωτήματα όπως αυτά προσδιορίστηκαν στην παρούσα εργασία, προέκυψαν τα ακόλουθα συμπεράσματα:

Ερώτημα Ε1: Οι θαλάσσιες (ενεργειακές) μεταφορές στον Ινδικό ωκεανό χαρακτηρίζονται από την ύπαρξη πολυσύχναστων choke points, με σημαντικότερα εκείνα των στενών της Malacca και του Hormuz. Διαφαίνεται ότι η διακίνηση μεγάλου όγκου ενεργειακών φορτίων, η σημασία τους για σημαντικά κράτη του διεθνούς συστήματος, η γεωγραφική διαμόρφωση της κύριας SLOC με άκρα τα δύο ανωτέρω στενά και το πλήθος των διερχόμενων πλοίων σε συνδυασμό και με τη στρατικοποίηση των στενών, τις εδαφικές διεκδικήσεις και τις ιδεολογικές αντιθέσεις μεταξύ των κρατών δημιουργούν περιβάλλον στο οποίο υπάρχουν οι προϋποθέσεις εκδήλωσης απειλών κατά τις ασφάλειας των θαλάσσιων (ενεργειακών) μεταφορών.

Ερώτημα Ε2: Τα λειτουργικά συστήματα των πλοίων μεταφοράς ενεργειακών φορτίων εμφανίζονται ευάλωτα σε κυβερνοεπιθέσεις τόσο μέσω του διαδικτύου όσο

και από πιθανή προσβολή του λογισμικού τους μέσω φυσικών σημείων πρόσβασης. Παράλληλα η διασύνδεσή τους καθιστά ευάλωτη σε κυβερνοεπίθεση το σύνολο της αλληλουχίας των αλληλοϋποστηριζόμενων συστημάτων. Ο επιτιθέμενος μπορεί να αποκτήσει τον έλεγχο βασικών συστημάτων όπως ναυσιπλοΐας, προώσεως, διαχείρισης φορτίου αποκτώντας ουσιαστικά τον έλεγχο του πλοίου με ενδεχόμενες συνέπειες την εκτροπή από την πορεία του, τη βύθισή του, την απώλεια φορτίου και τη χρήση του ως μέσο εκδήλωσης ασύμμετρης επίθεσης τόσο σε εγκαταστάσεις όπως διυλιστήρια, λιμένες και πλωτές πλατφόρμες εξόρυξης όσο και για την πρόκληση μείζονος ναυτικού ατυχήματος σε choke points με σκοπό την παρεμπόδιση της ναυσιπλοΐας.

Ερώτημα Ε3: Ο κυριότερος όγκος των συνεχώς αυξανόμενων ενεργειακών απαιτήσεων των ασιατικών οικονομιών καλύπτεται κυρίως με εισαγωγές ενεργειακών φορτίων από τις χώρες της Μέσης Ανατολής διαμέσου της SLOC που οριοθετείται από τα choke points της Malacca και του Hormuz. Η γεωγραφική διαμόρφωση του Ινδικού ωκεανού σε συνδυασμό με την τρωτότητα των πλοίων σε κυβερνοεπιθέσεις φαίνεται πως καθιστά ευάλωτη την ασφάλεια των θαλάσσιων ενεργειακών μεταφορών στην περιοχή.

5.2. Προτάσεις για περαιτέρω μελέτη

Σκοπός της παρούσας εργασίας υπήρξε η ανάδειξη της τρωτότητας της ασφάλειας, προερχόμενη από κυβερνοεπιθέσεις σε επίπεδο πλοίου, αναφορικά με τη μεταφορά (ενεργειακών) φορτίων στην περιοχή του Ινδικού ωκεανού. Υπό το πνεύμα των ανωτέρω εκτιμάται ότι απαιτείται περαιτέρω εμβάθυνση σε συνάφεια με τα εξαχθέντα συμπεράσματα, με τη μελέτη των ακόλουθων προεκτάσεων να παρουσιάζει ιδιαίτερο ενδιαφέρων:

α. Προσδιορισμός των επιπτώσεων στις οικονομίες της Ασίας και της Μέσης Ανατολής λόγω διατάραξης της ροής ενεργειακών φορτίων προερχόμενη από την εκδήλωση κυβερνοεπίθεσεων στην SLOC που οριοθετείται από τα choke points της Malacca και του Hormuz.

β. Υπολογισμός των συνεπειών από την καταστροφή εγκαταστάσεων, όπως διυλιστήρια, λιμένες και πλωτές πλατφόρμες εξόρυξης, που δύναται να προκληθεί από την χρήση ως μέσου επίθεσης πλοίων μεταφοράς ενεργειακών φορτίων, τα οποία έχουν προσβληθεί μέσω κυβερνοεπίθεσης.

γ. Υπολογισμός της σχέσης κόστους-οφέλους από την εκδήλωση κυβερνοεπιθέσεων σε πλοία μεταφοράς ενεργειακών φορτίων στα choke points της Malacca και του Hormuz.

δ. Υπολογισμός της σχέσης κόστους-οφέλους από την εκδήλωση κυβερνοεπίθεσης σε καθεστώς αποκλειστικής χρήσης αυτόνομων πλοίων για τη μεταφορά ενεργειακών φορτίων στον Ινδικό ωκεανό.

Βιβλιογραφικές αναφορές

Achanta, S., Watt. S., & Sagen, E. (2015, March). *Mitigating GPS vulnerabilities*. Paper presented at the Power and Energy Automation Conference Spokane, Washington. Ανακτήθηκε από https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6644_MitigatingGPS_SA_20140205_Web.pdf?v=20150812-075912

African Union. (2012). *2050 Africa's Integrated Maritime Strategy*. Ανακτήθηκε από http://cggrps.org/wp-content/uploads/2050-AIM-Strategy_EN.pdf

Ang, B. W., Choong, W. L., & Ng, T. S. (2015). Energy security: Definitions, dimensions and indexes. *Renewable and Sustainable Energy Reviews, 42*, 1077–1093. https://doi.org/10.1016/j.rser.2014.10.064

Asia Pacific Energy Research Center (APERC) (2007). *A quest for energy security in the 21st century: Resources and constraints.* Ανακτήθηκε από https://aperc.ieej.or.jp/file/2010/9/26/APERC_2007_A_Quest_for_Energy_Security.pdf

Bhatti, J. & Humphreys, T. (2016). Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation, 64*(1) https://doi.org/10.1002/navi.183

Baylis, J., Smith, S., & Owens, P. (2013). *Η Παγκοσμιοποίηση της Διεθνούς Πολιτικής: Μία Εισαγωγή στις Διεθνείς Σχέσεις* (5η Εκδ.). Αθήνα: Εκδόσεις Επίκεντρο

BIMCO (2016). *The Guidelines on cyber security onboard ships*. Ανακτήθηκε από http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

Blumsack, S. (2017) *Futures contracts for refined petroleum products*. Document posted in The Pennsylvania State University EME 801 online classroom. Ανακτήθηκε από https://www.e-education.psu.edu/eme801/node/513

Bothur, D., Zheng, G., & Valli, C. (2017). *A critical analysis of security vulnerabilities and countermeasures in a smart ship system*. Paper presented at the Australian Information Security Management Conference, Perth, Australia. Ανακτήθηκε από http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism

Brewster, D., Ji, Y., Li, Zh., Chaudhuri, Pr., Singh, A., Menon, R., Baruah, D., Garver, J., & Medcalf, R. (2016, Ιούλιος). India and China at sea: A contest of status

and legitimacy in the Indian ocean. *Asia Policy, 22*(1), 4-10. Ανακτήθηκε από http://nbr.org/publications/asia_policy/free/AP22/AsiaPolicy22_IndiaChinaAtSeaRT_July2016.pdf

Bueger, Chr. (2015, Μάρτιος). What is maritime security?. *Marine Policy, 53*, 159-164. https://doi.org/10.1016/j.marpol.2014.12.005

Buzan, B., Wæver O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder London,: Lynne Rienner Publishers.

Chester, L. (2010). Conceptualising energy security and making explicit its polysemic nature. *Energy Policy, 38*, 887–895. https://doi.org/10.1016/j.enpol.2009.10.039

Cordner, L. (2014, 28 Φεβρουαρίου). Risk managing maritime security in the Indian Ocean Region. *Journal of the Indian Ocean Region, 10*(1), 46-66. https://doi.org/10.1080/19480881.2014.882148

Cyberkeel. (2014). Maritime Cyber – Risks. Ανακτήθηκε από https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

De Quadros Rocha, D., dos Santos, G-F., Alves, J-P., dos Santos, J-E. & Monteiro, V-F. (2016). Militarization of international straits and maritime chokepoints. *UFRGS Model United Nations. 4*, 313-375, Ανακτήθηκε από https://www.ufrgs.br/ufrgsmun/2016/assets_b/files/disec.pdf

De Wilde, J. (1995). 'Security levelled out: the dominance of the local and the regional'. In Dunay, P., Kardos, G., and Williams, A. (eds), *New Forms of Security: Views from Central, Eastern and Western Europe* (pp.88-102). Dartmouth

Emmerson, Ch. & Stevens, P. (2012). Maritime choke points and the global energy system: Charting a way forward, Ανακτήθηκε από https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Energy%2C%20Environment%20and%20Development/bp0112_emmerson_stevens.pdf

Economic Research Institute of ASEAN and East Asia (ERIA) (2015) *Sea lane security of oil and liquefied natural gas in the East Asia summit region.* Ανακτήθηκε από http://www.eria.org/RPR_FY2015_14.pdf

Esakova, N. (2012). *European energy security. Analysing the EU-Russia energy security regime in terms of interdependence theory*. Frankfurt, Germany: Springer.

European Commission (EC) (2000). *Towards a European strategy for the security of energy supply*. Green Paper, Luxembourg: Office for Official Publications of the European Communities.

European Union (2014). *European Union Maritime Security Strategy*. Council of the European Union. Doc. 11205/14. Ανακτήθηκε από http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT

Fatima, Q., & Jamshed, A. (2015, Ιούλιος-Δεκέμβριος). The political and economic significance of Indian ocean: An analysis. *South Asian Studies A Research Journal of South Asian Studies, 30*(2), 73-89 Ανακτήθηκε από http://pu.edu.pk/images/journal/csas/PDF/5%20Qamir%20Fatima_30_2.pdf

Forbes, A. (2014). Protecting the ability to trade in the Indian Ocean maritime economy. Ανακτήθηκε από http://www.navy.gov.au/sites/default/files/documents/SPS3_Protecting_Trade_Indian Ocean.pdf

Friedman, G. & Ligon, Ch. (2017, 10 Απριλίου). Major choke points in the Persian Gulf and East Asia, Ανακτήθηκε από http://www.mauldineconomics.com/this-week-in-geopolitics/major-choke-points-in-the-persian-gulf-and-east-asia

Germond, B. (2015, Απρίλιος). The geopolitical dimension of maritime security. *Marine Policy, 54*, 137-142. https://doi.org/10.1016/j.marpol.2014.12.013

Gnansounou, E. (2008). Assessing the energy vulnerability: case of industrialized countries. *Energy Policy, 36*, 3734–3744. https://doi.org/10.1016/j.enpol.2008.07.004

Goward, D. (2017, 11 Ιουλίου) Mass GPS spoofing attack in Black sea? Ανακτήθηκε από https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.=0r20Ys

Graham, E. (2015, Απρίλιος-Μάιος). Maritime Security and Threats to Energy Transportation in Southeast Asia. *The RUSI Journal, 160*(2), 20-31. https://doi.org/10.1080/03071847.2015.1031522

Grant, A., Williams, P.,Ward, N., & Basker, S. (2009). GPS jamming and the impact on maritime security. *The Journal of Navigation, 62*(2), 173-187. Ανακτήθηκε από https://www.researchgate.net/publication/228897052_GPS_Jamming_and_the_Impact_on_Maritime_Navigation

Hambling, D. (2017, Αύγουστος). Hints of a new cyberweapon. *NewScientist, 235*(3139), 6. https://doi.org/10.1016/S0262-4079(17)31594-4

Humphreys, T.E, Ledvina, B.M., Psiaki, M.L, O'Hanlon, B.W. & Kintner, P.M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Ανακτήθηκε από https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf.

Institution of Engineering and Technology (IET) (2017). *Code of practice cyber security on ships.* Ανακτήθηκε από https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

International Institute for Strategic Studies (IISS) (2017). *Military Balance 2017: The annual assessment of global military capabilities and defense economics*. Ανακτήθηκε από http://emagazinepdf.com/2017/08/the-military-balance-2017/

International Energy Agency (IEA) (2010). *World energy outlook 2010.* Ανακτήθηκε από http://www.worldenergyoutlook.org/media/weo2010.pdf

International Energy Agency (IEA) (2011a). *The IEA model of short-term energy security (MOSES): Primary energy sources and secondary fuels.* Ανακτήθηκε από https://www.iea.org/media/freepublications/oneoff/moses_paper.pdf

International Energy Agency (IEA) (2011b). *Measuring short-term energy security.* Ανακτήθηκε από https://www.iea.org/publications/freepublications/publication/Moses.pdf.

International Energy Agency (IEA) (2007). *Energy security and climate policy: assessing interactions*. Ανακτήθηκε από https://www.iea.org/publications/freepublications/publication/energy_security_climate_policy.pdf

IMO (2006). *Adoption of the revised performance standards for Elecronic Chart Display and Information Systems (ECDIS).* (Publication No MSC 82/24/Add.2). Ανακτήθηκε από http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-(MSC)/Documents/MSC.232(82).pdf

IMO (2010). *Amedments to the international aeronautical and maritime search and rescue (IAMSAR) manual.* (Publication No MSC.1/Circ.1367). Ανακτήθηκε από https://officerofthewatch.files.wordpress.com/2013/07/msc-1-circ-

1415-amendments-to-the-international-aeronautical-and-maritime-search-and-rescue-iamsar-manual-secretariat.pdf

IMO (2002). *Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS)*. (Publication No A 22/Res.917). Ανακτήθηκε από
https://www.navcen.uscg.gov/pdf/AIS/IMO_A_917(22)_AIS_OPS_Guidelines.pdf

Johansson, B. (2013). A broadened typology on energy and security. *Energy, 53*, 199–205. https://doi.org/10.1016/j.energy.2013.03.012

Kisel, E., Hamburg, A., Harm, M., Leppiman, A., & Ots, M. (2016). Concept for energy security matrix. Energy *Policy, 95*, 1–9. https://doi.org/10.1016/j.enpol.2016.04.034

Klein, N. (2011). *Maritime security and the law of the sea.* Oxford & New York: Oxford University Press

Kruyt, B., van Vuuren, D. P., de Vries H. J. M., & Groenenberg H. (2009). Indicators for energy security. *Energy Policy, 37*, 2166–81. https://doi.org/10.1016/j.enpol.2009.02.006

Luft, G., & Korin, A. (2009). *In Energy security challenges for the 21st century: A reference handbook*, Santa Barbara, California, USA: Praeger Security International

Marquina, A. (2008). *Energy security: Visions from Asia and Europe: The southeast–southwest European energy corridor.*, UK: Palgrave Macmillan

Mearsheimer, J. (2007) *Η Τραγωδία της πολιτικής των Μεγάλων Δυνάμεων.* Αθήνα: Εκδόσεις Ποιότητα

Middleton, Al. (2014), Hide and seek, *The Coast Guard Journal of Safety & Security at Sea, 71*(4), pp.48-49. Ανακτήθηκε από www.uscg.mil/proceedings

Mileva, E. & Siegfried, N. (2007, Δεκέμβριος). Oil market structure, network affects and the choice of currency for oil invoicing, *Occasional Paper Series by European Central Bank, 77* Ανακτήθηκε από https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp77.pdf

Narula, K., & Reddy S. (2015). Three blind men and an elephant: The case of energy indices to measure energy security and energy sustainability. *Energy, 80*, 148–158. https://doi.org/10.1016/j.energy.2014.11.055

NATO (2011). *Alliance maritime strategy*. Ανακτήθηκε από https://www.nato.int/cps/ua/natohq/official_texts_75615.htm

NCCGROUP, (2014). *Preparing for cyber battleships - electronic chart display and information system security*. Ανακτήθηκε από https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/

Ong, Th. (2017, 13 Σεπτεμβρίου). Rolls-Royce has plans for autonomous naval ship Ανακτήθηκε από https://www.theverge.com/2017/9/13/16300866/rolls-royce-autonomous-ship-navy

Paravantis, J.A, & Kontoulis, N. (2017, Ιανουάριος-Ιούνιος). A Geopolitical Approach to Conceptualizing and Measuring Energy Security. *Archives of Economic History, XXIX*(4), 41-67. Ανακτήθηκε από http://archivesofeconomichistory.com/

Paris, C. (2017, 24 Ιουλίου). Norway takes lead in race to build autonomous cargo ships. Ανακτήθηκε από https://www.wsj.com/articles/norway-takes-lead-in-race-to-build-autonomous-cargo-ships-1500721202

Radovanović, M., Filipović S., & Pavlović, D. (2017). Energy security measurement– A sustainable approach. Renewable and Sustainable *Energy Reviews, 68*, 1020–1032. https://doi.org/10.1016/j.rser.2016.02.010

Rodrigue, J-P. (2004, Δεκέμβριος). Straits, passages and chokepoints: A maritime geostrategy of petroleum distribution. *Cahiers de Géographie du Québec, 48*(135), 357-374. https://doi.org/10.7202/011797ar

Rumley, D., Chaturvedi, S., & Yasin, M. (2007). *The security of sea lanes of communication in the Indian ocean region* Kaula Lampur: Maritime Institute of Malaysia.

Shoultz, D. (2017, 23 Ιανουαρίου). Securely connected vessels: vessel communications and maritime cyber security. Ανακτήθηκε από https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communications-and-maritime-15176

Sovacool, B. K., and Mukherjee, I. (2011). Conceptualizing and measuring energy security: A synthesized approach. *Energy, 36*, 5343–5355. https://doi.org/10.1016/j.energy.2011.06.043

Trend Micro (2014). *A security evaluation of AIS*. Ανακτήθηκε από https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

UK HM Government (2014). *The UK national strategy for maritime security*. Ανακτήθηκε από

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/310323/National_Strategy_for_Maritime_Security_2014.pdf

United Nations Convention on the Law of the Sea (UNCLOS), 10 Δεκεμβρίου, 1982, Ανακτήθηκε από http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations (2008). *Oceans and the law of the sea*. (Document A/63/63). Ανακτήθηκε από http://www.refworld.org/docid/48da24e72.html

Uma, M., & Padmavathi, G. (2013, Σεπτέμβριος) A Survey on various cyber attacks and their classification. *International Journal of Network Security, 22*(5), 390-396. Ανακτήθηκε από https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf

U.S. Chamber of Commerce (2010). *Index of U.S. energy security risk: Assessing America's vulnerabilities in a global energy market*. Ανακτήθηκε από https://www.uschamber.com/sites/default/files/documents/files/2013-esri.pdf

US Department of Transportation. (2013). *ICS Security in Maritime Transportation: White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure*, (Publication No DOT-VNTSC-MARAD-13-01). https://doi.org/10.13140/RG.2.1.2140.2963

US Energy Information Administration (EIA) (2017, 25 Ιουλίου). *World oil transit checkpoints*. Ανακτήθηκε από https://www.eia.gov/beta/international/regions-topics.php? RegionTopicID=WOTC

Vivoda, V. (2010). Evaluating energy security in the Asia-Pacific region: A novel methodological approach. *Energy Policy, 38*, 5258–5263. https://doi.org/10.1016/j.enpol.2010.05.028

Wee, V. (2017, 22 Δεκεμβρίου). Naval Dome exposes vessel vulnerabilities to cyber attack. Ανακτήθηκε από http://www.seatrade-maritime.com/news/europe/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html

World Trade Organization (WTO) (2009). *WTO sees 9% global trade decline in 2009 as recession strikes.* Ανακτήθηκε από https://www.wto.org/english/news_e/pres09_e/pr554_e.htm

Winzer, C. (2012). Conceptualizing energy security. *Energy Policy, 46*, 36–48. https://doi.org/10.1016/j.enpol.2012.02.067

Yergin, D. (2006). Ensuring energy security. *Foreign Affairs, 85*(2), 69–82. Ανακτήθηκε από https://www.foreignaffairs.com/articles/2006-03-01/ensuring-energy-security

Zaghloul, M. S. (2014, Φεβρουάριος). Online ship control system using supervisory control and data Acquisition (SCADA). *International Journal of Computer Science and Application, 3*(1). https://doi.org/10.14355/ijcsa.2014.0301.

Zurich. (2014). *Beyond data breaches: global interconnections of cyber risk.* Ανακτήθηκε από http://www.atlanticcouncil.org/images/publications/Zurich_Cyber_Risk_April_2014.pdf

Γιαννακόπουλος, Β. (2010). *Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή*. Ανακτήθηκε από http://www.geostrategy.gr

Κολιόπουλος, Κ. (2008). *Η Στρατηγική Σκέψη από την Αρχαιότητα έως Σήμερα*. Βάρη Αττικής: Εκδόσεις Ποιότητα.

Πλατιάς, Α., & Κολιόπουλος, Κ. (2015). *Η Τέχνη του Πολέμου του Σουν Τσου.* Αθήνα: Εκδόσεις Δίαυλος.