ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

Μεταπτυχιακή Διπλωματική Εργασία

Η σημασία της οικονομικής κατασκοπείας στις Διεθνείς Σχέσεις.

Χουτέα Ελεάνα

Τριμελής Επιτροπή:
Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος
Αναπληρωτής Καθηγητής Ν. Σ. Κουτσούκης
Επίκουρος Καθηγητής Ε. Τ. Φακιολάς

Τελική έκδοση

Κόρινθος, 2017

UNIVERSITY OF THE PELOPONNESE

SCHOOL OF SOCIAL AND POLITICAL SCIENCE

DEPARTMENT OF POLITICAL SCIENCES & INTERNATIONAL RELATIONS

Master of Arts in

"Global Risks and Analytics"

Master's Dissertation

The importance of the economic espionage in International Affairs.

What is the importance of the economic espionage?

Choutea Eleana

Supervisors:

Assistant Professor I. Konstantopoulos

Associate Professor N. S. Koutsoukis

Assistant Professor E. T. Fakiolas

Final Version

Corinth, 2017

Φύλλο αξιολόγησης

Η διπλωματική εργασία με τίτλο «Η σημασία της οικονομικής κατασκοπείας στις Διεθνείς Σχέσεις. Ποια η σημασία της οικονομικής κατασκοπειάς;» από την Ελεάνα Χουτέα αξιολογήθηκε από την τριμελή επιτροπή, τόσο ως προς την ποιότητα του κειμένου, όσο και ως προς την ποιότητα της προφορικής παρουσίασης και υπεράσπισης της διπλωματικής εργασίας ενώπιον ακροατηρίου.

Η διαδικασία αξιολόγησης της διπλωματικής εργασίας ολοκληρώθηκε την 30 /10 /2017 με γενική επίδοση:

☐ Καλώς

☑ Λίαν Καλώς

☐ Άριστα

Τα μέλη της τριμελούς επιτροπής

Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος

Αναπληρωτής Καθηγητής Ν. Σ. Κουτσούκης

Επίκουρος Καθηγητής Ε. Τ. Φακιολάς

Περίληψη

Η εργασία σκοπό έχει να αναφέρει και να καταγράψει τη σημασία της οικονομικής κατασκοπείας στις Διεθνείς Σχέσεις.

Η οικονομία είναι μια μορφή πολέμου και η ισχύς ανήκει σε αυτόν που την κατάλληλη στιγμή επιτυγχάνει να αποκτήσει, να αναλύσει και να ανασυνθέσει με τη μεγαλύτερη ταχύτητα δεδομένα και πληροφορίες που είναι διαθέσιμα στο ανταγωνιστικό περιβάλλον. Το νόμισμα της νέας εποχής είναι η πληροφορία και επιδιώκεται να αποκτηθεί με κάθε μέσο, θεμιτό ή αθέμιτο. Ο τρόπος για να αποκτηθεί αυτή η πληροφορία είναι η οικονομική κατασκοπεία. Η οικονομική κατασκοπεία ως τμήμα της ανθρώπινης ιστορίας, δεν είναι δημιούργημα των τελευταίων ετών αλλά εφαρμόζεται πολλούς αιώνες.

Στα πλαίσια των διεθνών σχέσεων η τεχνολογία διαδραματίζει σημαντικό ρόλο, μιας και η διάδοση των παγκόσμιων συστημάτων επικοινωνίας και πληροφοριών προστίθεται ως ακόμα μια διάσταση της οικονομικής κατασκοπείας. Ένα από τα πιο σημαντικά διεθνή προβλήματα που σχετίζονται με την τεχνολογία αποτελεί η κυβερνοκατασκοπεία.

Η Κίνα και η Ρωσία προσπαθούν να κερδίσουν ξανά την επιρροή που είχαν γεωπολιτικά με το να μειώσουν ταυτόχρονα την επιρροή που απέκτησαν οι ΗΠΑ από την απουσία τους στις ίδιες περιοχές.

Στο τελευταίο κεφάλαιο γίνεται απεικόνιση και αξιολόγηση των κινδύνων με τις οποίες έρχονται αντιμέτωπα τα κράτη και οι εταιρείες. Γίνεται ανάλυση ρίσκου σε δύο στάδια, αρχικά με τον εντοπισμό των βασικών χαρακτηριστικών και εν συνεχεία υπολογίζεται ο αντίκτυπος της εκάστοτε απειλής. Επιπρόσθετα, χρησιμοποιώντας το πρόγραμμα CORAS απεικονίζονται οι δρώντες, οι ευαίσθητες πληροφορίες και το υλικό καθώς και ο αντίκτυπος σε περίπτωση διαρροής αυτών.

Όροι κλειδιά: Ασφάλεια, Εθνική Ασφάλεια, Οικονομική κατασκοπεία, Κατασκοπεία, Κυβερνοκατασκοπεία, Γεωοικονομία, Γεωπολιτική, Διαχείριση Κινδύνου.

Abstract

The dissertation aims to report and record the importance of economic espionage in International Relations.

The economy is a form of war, and power belongs to the one who at the right time succeeds in acquiring, analyzing and reconstructing at the fastest speed data and information available in the competitive environment. The currency of the new era is information and is intended to be acquired by any means, fair or unfair. The way to get this information is economic espionage. Economic espionage as part of human history is not a creation of recent years but has been applied for many centuries.

In the context of international relations, technology plays an important role, as the spread of global communication and information systems is added as yet another dimension of economic espionage. One of the most important international problems associated with technology is cyberguarding.

China and Russia are trying to regain their geopolitical influence by simultaneously reducing the influence that the US has gained from their absence in the same areas.

The last chapter presents and assesses the risks faced by states and companies. Risk analysis is carried out in two steps, initially by identifying the key features and then assessing the impact of the threat. Additionally, using the CORAS program, the actors, sensitive information and material, as well as the impact in the event of leakage, are depicted.

Key Words: Security, National Security, Economic espionage, Espionage, Cyberespionage, Geoeconomics, Geopolitics, Risk management.

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων» του τμήματος Πολιτικής Επιστήμης και Διεθνών Σχέσεων του Πανεπιστημίου Πελοποννήσου.

Πρώτο από όλους θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα της διπλωματικής, κύριο Κωνσταντόπουλο Ιωάννη, για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον αντικείμενο, καθώς και για την καθοδήγηση και την εμπιστοσύνη που μου έδειξε.

Στη συνέχεια θα ήθελα να ευχαριστήσω τον Καθηγητή Νικόλαο Κουτσούκη, καθώς συνέβαλε ουσιαστικά στην ολοκλήρωση αυτής της παρούσας εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συνεχή συμπαράσταση και υλική και ηθική στήριξη των επιλογών μου.

Πίνακας περιεχομένων

Περίληψη I

Abstract II

Κατάλογος Πινάκων V

Κατάλογος Εικόνων V

1. Εισαγωγή 1

1.1 Ιστορική αναδρομή 3

1.2 Πλαίσιο αναφοράς (τι είναι κατασκοπεία, πληροφορία, ασφάλεια, κυβερνοεπιθέσεις, γεωοικονομία) 6

Κεφάλαιο 2 8

2.1 Οικονομική ασφάλεια και Οικονομική κατασκοπεία 8

2.2 Μίκρο – μακροοικονομική κατασκοπεία 11

Κεφάλαιο 3 14

3.1 Τεχνολογία και cyber intelligence 14

3.2 Η στάση των εταιρειών και της κυβέρνησης σχετικά με την κυβερνοκατασκοπεία 17

3.3 Η περίπτωση Snowden 19

Κεφάλαιο 4 21

4.1 Εφαρμογή οικονομικής κατασκοπείας σε εχθρούς και σε συμμάχους 21

4.2 Η περίπτωση της Ρωσίας 23

4.3 Η περίπτωση της Κίνας 26

Κεφάλαιο 5 29

5.1 Η γεωπολιτική και γεωστρατηγική σημασία της οικονομικής κατασκοπείας 29

Κεφάλαιο 6 33

6.1 Η οικονομική κατασκοπία υπό το πρίσμα του Risk Management 33

7. Συμπεράσματα – Επίλογος 39

Βιβλιογραφία – Κατάλογος πηγών 1

Κατάλογος Πινάκων

Πίνακας 1 Πιθανότητα διαρροής και επιπτώσεις 34
Πίνακας 2. Παράγοντες απειλής, Δρώντες και Τρόποι απόκτησης πληροφοριών (ENISA, 2016)..... 36

Κατάλογος Εικόνων

Εικόνα 1. Απεικόνιση αντίληψης επικινδυνότητας σε εταιρικό και διπλωματικό επίπεδο διαρροής πληροφοριών..... 35

1. Εισαγωγή

Μετά τον Ψυχρό Πόλεμο, η σκέψη της εισόδου σε μία εποχή που θα επικρατούσε η ειρήνη και οι φιλικές σχέσεις έμοιαζε με ένα όνειρο. Ο ανταγωνισμός για στρατιωτική και πολιτική υπεροχή φαίνεται να αντικαταστάθηκε από έναν διαφορετικό αλλά εξίσου άκαμπτο αγώνα για οικονομική κυριαρχία. Ο ανταγωνισμός αυτός είναι τόσο σοβαρός που έγινε αντιληπτός από τα κράτη, με αποτέλεσμα τόσο σύμμαχοι όσο και εχθροί να έρχονται αντιμέτωποι. (Erdogan, 2009)

Παρακολουθώντας την ανθρώπινη ιστορία διαπιστώνει κανείς πως η οικονομία είναι μια μορφή πολέμου και η ισχύς ανήκει σε αυτόν που την κατάλληλη στιγμή επιτυγχάνει να αποκτήσει, να αναλύσει και να ανασυνθέσει με τη μεγαλύτερη ταχύτητα δεδομένα και πληροφορίες που είναι διαθέσιμα στο ανταγωνιστικό περιβάλλον. Η πληροφορία επιδιώκεται να αποκτηθεί με κάθε μέσο, θεμιτό ή αθέμιτο. Ο τρόπος για να αποκτηθεί αυτή η πληροφορία είναι η οικονομική κατασκοπεία.

Ίσως το οπλοστάσιο του οικονομικού πολέμου να μην περιλαμβάνει όλμους και τεθωρακισμένα και να μην πεθαίνουν με άμεσο τρόπο άνθρωποι, αλλά θύματα υπάρχουν ˙ οι επιχειρήσεις που καταστρέφονται, η ανεργία και η φτώχεια που αυξάνονται, η κοινωνική συνοχή διαρρηγνύεται κ.ο.κ. (Κάτσουρα, 2017)

Ανατρέχοντας προσεκτικά στην παγκόσμια ιστορία, επιβεβαιώνεται η μεγάλη σημασία της κατασκοπείας. Οι οικονομικές και επιστημονικές – τεχνολογικές πληροφορίες διαδραμάτιζαν πάντα σημαντικό ρόλο.

Το αντικείμενο της οικονομικής κατασκοπείας άρχισε να ανθεί την εποχή του Ψυχρού Πολέμου, λόγω της διαμάχης Ανατολής – Δύσης, τόσο σε πολιτικό όσο και σε οικονομικό επίπεδο. Είναι πιθανό ο Ψυχρός Πόλεμος με εκείνους τους όρους να είναι παρελθόν, ωστόσο εξακολουθούν να είναι οικονομικά τα μέτρα που πρωτίστως επιβάλλονται όταν ασκούνται πολιτικές πιέσεις. Πρόσφατα παραδείγματα αποτελούν οι κυρώσεις έναντι της Ρωσίας για το ουκρανικό ζήτημα ή έναντι του Ιράν για το πυρηνικό του πρόγραμμα. Επίσης το εμπάργκο προς την Κούβα ίσως είναι ιστορικά το πιο περιγραφικό παράδειγμα της πρακτικής αυτής. (Κάτσουρα, 2017)

Η διάδοση των παγκόσμιων συστημάτων επικοινωνίας και πληροφοριών, συμπεριλαμβανομένου του διαδικτύου, πρόσθεσε ακόμα μια διάσταση στην αυξανόμενη απειλή που δημιουργεί η οικονομική κατασκοπεία. (Erdogan, 2009)

Η αλλαγή του κόσμου μας σε μια κοινωνία της πληροφορίας δεν είναι σαν τη Βιομηχανική Επανάσταση. Το νόμισμα της νέας εποχής είναι οι πληροφορίες. Το πρόβλημα δύναμης στη νέα εποχή είναι η δυσκολία συγκέντρωσης, χρήσης και ελέγχου της πληροφορίας. Στο ξεκίνημα αυτής της δυσκολίας είναι που έληξε ο Ψυχρός Πόλεμος, καθώς μια σειρά από άρτια εκπαιδευμένους συλλέκτες πληροφοριών προσπαθούν να ανταπεξέλθουν με τη νέα οικονομία. (Schiller, 13, pp. 1044-1045)

Οι ΗΠΑ συνεχίζουν να είναι η πηγή της πιο εξελιγμένης τεχνολογίας του κόσμου και πολλές βιομηχανίες –ξένες κυρίως- εξαρτώνται από αυτή την καινοτομία προκειμένου να βελτιώσουν τη δική τους ανταγωνιστικότητα.

Οι μυστικές υπηρεσίες σε Ρωσία και Κίνα αντιλαμβανόμενες τη στροφή από το στρατιωτικό ανταγωνισμό στον παγκόσμιο οικονομικό ανταγωνισμό, έχουν ολοκληρώσει πλήρως τη στροφή σε ό, τι χρειάζεται η συλλογή πληροφοριών και πλέον έχουν γίνει ειδικοί στην οικονομική και βιομηχανική κατασκοπεία. (Poteat, p. 16)

Ο αυξημένος διεθνής οικονομικός ανταγωνισμός σε αυτή τη μετά-ψυχροπολεμική εποχή θα συνεχίσει να τοποθετεί ξένες υπηρεσίες πληροφοριών στη διεξαγωγή οικονομικής κατασκοπείας προκειμένου τα κράτη να αυξήσουν περαιτέρω την ευημερία τους και η λογική των διεθνών σχέσεων εξακολουθεί να είναι η ίδια ˙ οι διεθνείς σχέσεις ήταν και είναι κατά βάση συγκρουσιακές και ανταγωνιστικές. Το μόνο που αλλάζει κατά περιόδους είναι οι όροι με τους οποίους διεξάγεται ο ανταγωνισμός. Η οικονομία, η γεωπολιτική και γεωοικονομία είναι ουσιαστικά διαφορετικές όψεις του ίδιου νομίσματος, δηλαδή του διεθνή ανταγωνισμού. Σε αυτό το διεθνές ανταγωνιστικό και κατασκοπευτικό παιχνίδι δεν υπάρχουν εχθροί ή φίλοι. (Fraumann, 2013, p. 308)

1.1 Ιστορική αναδρομή

Η οικονομική κατασκοπεία, όπως φαίνεται από την παρούσα μελέτη, είναι μια τακτική η οποία δεν κάνει την πρωταρχική εμφάνισή της τα τελευταία χρόνια, αλλά υπάρχει πολλούς αιώνες τώρα.

Η κατασκοπεία αποτελούσε πάντοτε μέρος της ανθρώπινης ιστορίας, καθώς η ιστορία της κατασκοπείας χρονολογείται τουλάχιστον από το 500 π.Χ. Η σημασία της κατασκοπείας εν καιρώ πολέμου αναγνωρίζεται από τις αρχές της καταγεγραμμένης ιστορίας. Για παράδειγμα, οι Αιγύπτιοι διέθεταν πολύ καλά οργανωμένη μυστική υπηρεσία, ενώ για τους Κινέζους το ζήτημα των πληροφοριών και της κατασκοπείας θεωρείτο –και θεωρείται ακόμα και σήμερα- θεμελιώδες. Σύμφωνα με το Νικόλαο Ευθυμιάδη: «*Η εξάσκηση της κατασκοπείας στην Κίνα χρονολογείται τουλάχιστον από τον 5ο αιώνα π.Χ., όταν ο Sun Tzu περιέγραψε λεπτομερώς την κατάλληλη χρήση των κατασκόπων στο στρατιωτικό εγχειρίδιο "Sun Tzu Bing Fa" (Sun Tzu's Art of War)*». Ο Sun Tzu με την έμφαση που δίνει στις πληροφορίες, ξεκινά μια μεγάλη παράδοση στη στρατηγική σκέψη της Ανατολής, σήμα κατατεθέν της οποίας είναι όχι μόνο η έμφαση στη συλλογή πληροφοριών –μέσω κατασκόπων- αλλά και στην παραπλάνηση και στον αιφνιδιασμό (Κωνσταντόπουλος, 2010).

Η τέχνη της κατασκοπείας, εκτός από την Κίνα, αναπτύχθηκε και στην Ινδία. Στο πιο σημαντικό έπος της Ινδίας, τη Μαχαμπχαράτα, περιλαμβάνονται σαφείς συμβουλές προς τους βασιλιάδες, σχετικά με την κατασκοπεία. Για παράδειγμα, αναφέρει πως οι κατάσκοποι ουσιαστικά πρέπει να είναι με τέτοιον τρόπο ντυμένοι που δεν θα τραβούν την προσοχή πάνω τους, πχ να είναι τυφλοί, χαζοί, κωφάλαλοι. Οι ικανότητές τους πρέπει να έχουν ελεγχθεί ώστε να μπορούν να αντέξουν δυσμενείς καταστάσεις. Ο βασιλιάς θα πρέπει να έχει παντού κατασκόπους, να τους ξέρει όλους αλλά αυτοί να μη γνωρίζονται μεταξύ τους (Κωνσταντόπουλος, 2010).

Αλλά και στο Βυζάντιο είχαν πλήρη γνώση για τη σημασία της κατασκοπείας και της πληροφόρησης (Κωνσταντόπουλος, 2010, σ. 179).

Την περίοδο της Αναγέννησης (15ος – 16ος αιώνας) εγκαθιδρύθηκαν στην Ευρώπη τα θεμέλια των σύγχρονων υπηρεσιών πληροφοριών (Κωνσταντόπουλος, 2010, σ. 191).

Κατά τη διάρκεια του Πολέμου για την Ανεξαρτησία της Αμερικής από τους Βρετανούς (1775-1783) ο στρατηγός George Washington και άλλοι πατριώτες όπως ο Benjamin Franklin και ο John Jay συνέβαλαν στην ανεξαρτησία των αποικιών, χρησιμοποιώντας μια σειρά από μυστικές επιχειρήσεις. Χρησιμοποιούσαν δίκτυα κατασκόπων και διπλών πρακτόρων, παραπλανούσαν το Βρετανικό στρατό, προέβαιναν σε σαμποτάζ και παραστρατιωτικές επιχειρήσεις, χρησιμοποιούσαν κώδικες, κρυπτογραφήματα και παραπληροφόρηση προκειμένου να επηρεάσουν ξένες κυβερνήσεις. Ακόμη και σήμερα παραμένει θεμελιώδης η ρήση του George Washington: «*Η ανάγκη παραγωγής αξιόπιστων πληροφοριών είναι εμφανής και δεν χρειάζεται να τονιστεί περαιτέρω*» (Κωνσταντόπουλος, 2010, σ. 192).

Ο στρατός της Αγγλίας τον 16ο και 17ο αιώνα διέθετε τους ανιχνευτές (scoutmasters), οι οποίοι ήταν υπεύθυνοι για τη συλλογή πληροφοριών στο πεδίο της μάχης. Στις εκστρατείες του 18ου αιώνα, η συλλογή πληροφοριών σχετικά με το πεδίο μάχης (δηλαδή τακτικής φύσεως) ήταν καθήκον των αξιωματικών επιμελητείας της στρατιάς, ενώ οι γραμματείς τους χειρίζονταν πληροφορίες πολιτικής και στρατηγικής υφής (Κωνσταντόπουλος, 2010, σ. 192).

Από το 1660 στο προσωπικό των περισσότερων πρεσβειών συγκαταλέγονται μυστικοί πράκτορες, ενώ από το 1700 οι πρέσβεις θεωρούνταν κατάσκοποι που είχαν την άδεια του κράτους υποδοχής (Κωνσταντόπουλος, 2010, σ. 192).

Ο Joseph Fouche θεωρείται ότι ανέπτυξε το πρώτο σύγχρονο σύστημα πολιτικής κατασκοπείας και ο Φρειδερίκος ο Β' της Πρωσίας ως ο ιδρυτής της σύγχρονης στρατιωτικής κατασκοπείας (Κωνσταντόπουλος, 2010, σσ. 193-194).

Κατά τη διάρκεια των δύο Παγκόσμιων Πολέμων η σύγκρουση μεταξύ των δύο αντίπαλων συνασπισμών ήταν διττή: στο πεδίο της μάχης και στον τομέα των πληροφοριών, δηλαδή στο πεδίο της κατασκοπείας. Το κατά πόσο η κατασκοπεία συνέβαλε στην έκβαση των πολέμων αυτών αποτελεί ένα σημείο διαφωνίας μεταξύ της επιστημονικής κοινότητας των διεθνών σχέσεων και της ιστορίας.

Κατά τον Α΄ Παγκόσμιο Πόλεμο ο πλοίαρχος Ρέτζιναλντ Χολ, διοικητής του κλάδου πληροφοριών του επιτελείου του βρετανικού ναυαρχείου, ενώ από τη μια πλευρά αναγνώριζε τις δυσκολίες που αντιμετώπιζαν οι μυστικοί πράκτορες στη συλλογή πληροφοριών σχετικά με τις κινήσεις του εχθρικού στόλου, από την άλλη αποδεχόταν την αποτελεσματικότητα του κατασκοπευτικού δικτύου όσον αφορά στις αναφορές για το στρατιωτικό υλικό και τους πόρους του εχθρού.

Σύμφωνα με τον Michael Barret «*Η κατασκοπεία είναι το δεύτερο αρχαιότερο επάγγελμα στον κόσμο και το ίδιο έντιμο όπως και το πρώτο*».

Η πρώτη μυστική υπηρεσία δημιουργήθηκε το 1909 στη Βρετανία, λειτουργούσε κατά τη διάρκεια τόσο ειρηνικών περιόδων, όσο και περιόδων πολέμου, και αποτελούσε μια κυβερνητική υπηρεσία, χρηματοδοτούμενη από τον κρατικό προϋπολογισμό, απαρτιζόμενη κυρίως από πολίτες, με στόχο την κλοπή μυστικών άλλων χωρών και την προστασία των εγχώριων μυστικών. Το παράδειγμα της Βρετανίας το ακολούθησαν οι περισσότερες χώρες: η Γερμανία απέκτησε τις δικές της μυστικές υπηρεσίες το 1913, η Ρωσία το 1917, η Γαλλία το 1935 και οι ΗΠΑ το 1947 (Κωνσταντόπουλος, 2010, σ. 196).

Σήμερα ακόμη και οι κυβερνήσεις χωρών του επονομαζόμενου Τρίτου Κόσμου δεν αισθάνονται ότι έχουν αποκτήσει κρατική κυριαρχία αν δεν έχουν δημιουργήσει τις δικές τους μυστικές υπηρεσίες (Κωνσταντόπουλος, 2010, σ. 197).

Ακόμη και στις μέρες μας, οι μυστικές υπηρεσίες λειτουργούν πάντοτε στο ομιχλώδες περιβάλλον της «εθνικής ασφάλειας» και αναλαμβάνουν δύο καθήκοντα ˙ ένα επιθετικό και

ένα αμυντικό. Το πρώτο περιλαμβάνει την ανάληψη δράσης με στόχο την προαγωγή των στρατηγικών συμφερόντων της κυβέρνησης και του κράτους που υπηρετούν. Το δεύτερο αφορά την έγκαιρη προειδοποίηση για την ύπαρξη απειλών για την εθνική ασφάλεια, καθώς και στους τρόπους αντιμετώπισής τους (Κωνσταντόπουλος, 2010, σ. 197).

1.2 Πλαίσιο αναφοράς (τι είναι κατασκοπεία, πληροφορία, ασφάλεια, κυβερνοεπιθέσεις, γεωοικονομία)

Για την εκπόνηση της παρούσας διπλωματικής εργασίας χρησιμοποιείται η περιπτωσιολογική έρευνα για τη δημιουργία θεωρίας και πιο συγκεκριμένα η ελεγχόμενη σύγκριση, όπου συγκρίνονται παρατηρήσεις, οι οποίες προκύπτουν μέσα από μια σειρά παρατηρήσεων, και η δελφική μέθοδος, μέσω της οποίας γίνεται αναφορά στις απόψεις των συμμετεχόντων στις περιπτώσεις που αναφέρονται. Ο αναγνώστης θα συναντήσει τις παρακάτω λέξεις, επομένως, για την καλύτερη κατανόηση του κειμένου κρίνεται αναγκαία η διασαφήνισή τους.

Πληροφορία (information): ονομάζεται οποιασδήποτε μορφής δεδομένα που δεν έχουν αναλυθεί και μπορεί να καταστούν γνωστά ανεξάρτητα από την πηγή τους. Όταν αυτά περάσουν από το στάδιο της επεξεργασίας μπορεί να παράγουν «πληροφόρηση» (intelligence).

Πληροφόρηση (intelligence): είναι εκείνη η κατηγορία των πληροφοριών που έχει περάσει από το στάδιο της ανάλυσης και επεξεργασίας προκειμένου να διανεμηθεί στους διαμορφωτές λήψης των αποφάσεων, προκειμένου να λάβουν τις βέλτιστες αποφάσεις.

Κατασκοπεία: θεωρείται από τα αρχαιότερα επαγγέλματα. Οι επικρατέστεροι ορισμοί που έχουν δοθεί είναι οι εξής δύο:

1. Η δραστηριότητα αναζήτησης πληροφοριών εκ μέρους μιας κυβέρνησης, τις οποίες μια άλλη κυβέρνηση επιθυμεί να κρατήσει μυστικές.
2. Η συλλογή πληροφοριών μέσω μυστικής παρακολούθησης ή μέσω της χρήσης κατασκόπων, οι οποίοι υποκλέπτουν τις απαραίτητες πληροφορίες.

Οικονομική κατασκοπεία: Σύμφωνα με τον Porteous είναι η χρησιμοποίηση από μια κυβέρνηση ή εκπροσώπους της παράνομων, μυστικών, εξαναγκαστικών ή παραπλανητικών μέσων ή η διευκόλυνση τους, προκειμένου να αποκτήσουν πληροφορίες οικονομικού περιεχομένου.
Σύμφωνα με τον Burton είναι οι πληροφορίες (intelligence) που σχετίζονται με την έκταση και τη χρησιμοποίηση των φυσικών και ανθρώπινων πόρων και με τη βιομηχανική δυνατότητα των κρατών.

Ασφάλεια: Η ασφάλεια , με κάθε αντικειμενική έννοια, μετράει την απουσία απειλών σε αποκτώμενες αξίες και με μία υποκειμενική έννοια, την απουσία φόβου ότι τέτοιες αξίες θα υποστούν επίθεση. Η έννοια της ασφάλειας συμπίπτει εν μέρει με την έννοια της ισχύος, κάτι που δυσκολεύει τον ακριβή ορισμό της.

Κυβερνοεπιθέσεις: Η παράνομη πρακτική εισβολής στα ηλεκτρονικά συστήματα εταιρειών, δημοσίων οργανισμών, τραπεζών, επιχειρήσεων και ιδιωτών, με απώτερο σκοπό την κλοπή δεδομένων.

<u>Γεωοικονομία</u>: Με τον όρο «γεωοικονομία» προσδιορίζεται το κομμάτι εκείνο της επιστήμης το οποίο μελετά τα γεωοικονομικά δεδομένα μιας περιοχής, τα οποία σχετίζονται με οικονομικές δραστηριότητες ως προς το γεωγραφικό περιβάλλον με σκοπό την αξιοποίησή τους. Μεταξύ άλλων μελετάται ο ρόλος της οικονομικής αλληλεξάρτησης για την επίλυση ή πρόληψη συγκρούσεων · τα όρια της οικονομίας στην επίλυση ή πρόληψη των συγκρούσεων · τη σχέση μεταξύ της οικονομικής ανάπτυξης και των πολιτικών και κοινωνικών συνθηκών στις διάφορες χώρες.

Κεφάλαιο 2

2.1 Οικονομική ασφάλεια και Οικονομική κατασκοπεία

Τα οικονομικά και η εθνική ασφάλεια πάντα έμοιαζαν να συνδέονται μέχρι ένα σημείο. Η σχέση μεταξύ των οικονομικών και της ασφάλειας παραδοσιακά είναι τέτοια όπου τα πρώτα μοιάζουν να είναι κατώτερα του τελευταίου (Sheehan, 2005).

Η ασφάλεια έχει συσχετισθεί με την πρακτική της πολιτικής και υπάρχει μια οικονομική διάσταση στην επιτυχή πρακτική της πολιτικής ασφάλειας. Μια απόλυτη διάκριση δεν δύναται να γίνει μεταξύ της πολιτικής και οικονομικής δύναμης, καθώς η καθεμιά είναι παρούσα στην άλλη. (Sheehan, 2005, σ. 65)

Παρόλο που, σαν θέμα, τέθηκε υπό εξέταση κατά τη διάρκεια της πρώτης περιόδου του Ψυχρού Πολέμου, είναι κοινώς αποδεκτό ότι οι συνέπειες του εμπάργκο πετρελαίου του ΟΠΕΚ και οι αυξήσεις των τιμών στη δεκαετία του 1970 οδήγησαν σε λεπτομερείς μελέτες πετρελαίου και άλλων φυσικών πόρων, ως δυνητικά μέσα εξωτερικής πολιτικής και στην ανάπτυξη μοντέλων για την πρόβλεψη των μελλοντικών τάσεων. (Sheehan, 2005, σ. 65)

Στο πλαίσιο μιας ευρύτερης προσέγγισης της ασφάλειας, εν είδει απουσίας μιας ξεκάθαρης και ολοκληρωμένης ατζέντας, η έννοια της οικονομικής ασφάλειας ανοίγει ορισμένους κρίσιμους τομείς των διεθνών σχέσεων στην ανάλυση του πλαισίου της ασφάλειας. (Sheehan, 2005, σ. 67)

Υπάρχουν τουλάχιστον τέσσερις πολύ διαφορετικοί τρόποι με τους οποίους η οικονομική ασφάλεια έχει αναλυθεί από το τέλος του Ψυχρού Πολέμου. Η πρώτη είναι η παραδοσιακή, ιστορική έννοια στην οποία αναγνωρίζεται ότι η οικονομική δύναμη είναι γενικά απαραίτητη προϋπόθεση για τη στρατιωτική δύναμη. Η δεύτερη εκδοχή της οικονομικής ασφάλειας –ως προσέγγιση- είναι η νέο-δαρβινιστική προσέγγιση της σχολής της «γεωοικονομίας», η οποία προσδιορίζει τις απειλές και τους εχθρούς στο διεθνές οικονομικό περιβάλλον. Τρίτον, υπάρχουν εκείνοι που επικεντρώνονται στην «ανθρώπινη ασφάλεια» ή τη χειραφέτηση και οι οποίοι υπογραμμίζουν ότι η ιδέα της καλής διαβίωσης των ανθρώπων χρειάζεται ένα ζήτημα ασφάλειας παρά μια στρατηγική και στρατιωτική ατζέντα ασφάλειας. Τέλος υπάρχουν και εκείνοι που επικεντρώνονται στο επιχείρημα ότι ο πόλεμος και οι συγκρούσεις στις μεταμοντέρνες διεθνείς σχέσεις μειώνονται από τα θετικά αποτελέσματα της οικονομικής ανάπτυξης και της οικονομικής ολοκλήρωσης. (Sheehan, 2005, σ. 68)

Η οικονομική ολοκλήρωση έχει μια δική της δυναμική. Όλες οι οικονομίες καθίστανται πιο ανεξάρτητες μέσω βελτιωμένων επικοινωνιών, ροών κεφαλαίου και εμπορίου. Σε ένα φιλελεύθερο διεθνές οικονομικό σύστημα, η ευπάθεια στα εξωτερικά οικονομικά γεγονότα και η εξάρτηση από ξένους είναι μια απαραίτητη συνέπεια της βύθισης στις παγκόσμιες αγορές. Είναι η πηγή των ευκαιριών για βελτιωμένες συνθήκες διαβίωσης και όχι η απειλή που πρέπει να αποφευχθεί. Παρόλα αυτά κάποιος βαθμός ανασφάλειας είναι εγγενής σε οποιοδήποτε

οικονομικό σύστημα της αγοράς. Υπάρχουν ορισμένα σημεία ανασφάλειας που μπορούν πιθανώς να απομονωθούν μέσω της συμμετοχής των υπηρεσιών ασφαλείας. (Cable, 1995, pp. 305-306)

Οι κυβερνήσεις δεν αντιμετωπίζουν τις εθνικές οικονομίες μόνο ως μέσο πλουτισμού των πολιτών τους. Ο Βρετανός οικονομολόγος Hawtrey έγραψε για αυτό πως «*το κύριο μέλημα του κράτους είναι το κύρος. Τα μέσα για το κύρος είναι δύναμη. Η ισχύς είναι η οικονομική παραγωγικότητα εκφρασμένη ως δύναμη*». Με τη σειρά του ο Samuel Huntington σημειώνει για το θέμα «*Οι οικονομολόγοι είναι τυφλοί στο γεγονός ότι η οικονομική δραστηριότητα είναι πηγή εξουσίας και ευημερίας. Είναι μάλλον η πιο σημαντική πηγή εξουσίας και σε έναν κόσμο όπου η στρατιωτική σύγκρουση μεταξύ μεγάλων κρατών είναι απίθανη, η οικονομική δύναμη θα είναι όλο και πιο σημαντική για τον προσδιορισμό της υπεροχής ή υποταγής των κρατών*». (Cable, 1995, p. 308)

Διαφαίνεται ότι το 1980 ήταν η δεκαετία όπου τα οικονομικά έγιναν πιο σημαντικά από τις ιδεολογίες. «*Στην παγκόσμια οικονομία, τα οικονομικά ζητήματα σχεδόν πάντα ξεπερνούν τα πολιτικά ζητήματα*».
Καθώς αλλάζει η παγκόσμια οικονομική τάξη, οι χώρες –όπως για παράδειγμα η Ιαπωνία- ανταγωνίζονται οικονομικά χρησιμοποιώντας ένα διαφορετικό σύνολο κανόνων. Κάθε έθνος προσπαθεί να κλίνει το πεδίο δράσης προς όφελός του. Υποθέτοντας ότι η προώθηση και ο έλεγχος του εμπορίου είναι μια λειτουργία της κυβέρνησης, η κυβέρνηση πρέπει να διαθέσει όλους τους νόμιμους διαθέσιμους πόρους για να προωθήσει το εμπόριο ˙ θα ήταν προς το εθνικό συμφέρον και όφελός της να το πράξει. (Jeffrey, 1991, pp. 203-204)

Το πεδίο μάχης του προβλέψιμου μέλλοντος γίνεται οικονομικό και ενδεχομένως περιβαλλοντικό παρά στρατιωτικό. Μια διαμάχη σχετικά με τη χρήση των κυβερνητικών πληροφοριών για το εμπόριο είναι σε εξέλιξη. Ο πρώην διευθυντής της CIA το ξεκαθάρισε «*Υπάρχει πλέον μια παγκόσμια αναγνώριση ότι η οικονομική δύναμη είναι το κλειδί για την παγκόσμια επιρροή και δύναμη. Μέσα στην επόμενη δεκαετία θα συνεχίσουμε να βλέπουμε μια αυξανόμενη έμφαση στην οικονομική ανταγωνιστικότητα ως ένα θέμα κατασκοπείας*». Ο Γερουσιαστής Boren συμφώνησε λέγοντας «*Όταν ψάχνουν για πληροφορίες εναντίον των ΗΠΑ –οι ξένες κυβερνήσεις- , εμείς θα πρέπει να αναπτύξουμε οικονομικές ικανότητες μέσα στην κοινότητα των μυστικών υπηρεσιών. Θα πρέπει να προστατεύσουμε τις δικές μας εμπορικές επιχειρήσεις από την κλοπή εμπορικών μυστικών. Θα πρέπει να αρχίσουμε να σκεφτόμαστε το ρόλο που θέλουμε να διαδραματίσουν οι δικές μας υπηρεσίες πληροφοριών, όσον αφορά την προστασία των οικονομικών και εμπορικών συμφερόντων της Αμερικής σε όλο τον κόσμο*». (Cable, 1995) (Jeffrey, 1991, p. 204)

Πρόσφατες αναφορές της CIA για τις προτεραιότητες της υπογράμμισαν τη σημασία της αντιμετώπισης ενός μεγάλου εύρους απειλών –επονομαζόμενων και ως «γκρίζα περιοχή»- για την εθνική ασφάλεια, που θα μπορούσαν να θεωρηθούν ως πτυχές ή παρενέργειες της αυξημένης διεθνούς οικονομικής ολοκλήρωσης. Κατά τη διάρκεια του Ψυχρού Πολέμου, τα θέματα οικονομικής κατασκοπείας συχνά τοποθετούνταν σε ένα πλαίσιο

εθνικής ασφάλειας. Με το τέλος του Ψυχρού Πολέμου, η επέκταση δράσης της CIA στην οικονομική κατασκοπεία έγινε περισσότερο ορατή.

Τέσσερις παράγοντες είναι ιδιαίτερα αξιοσημείωτοι στην εξέταση ευκαιριών για την επέκταση της κοινότητας των πληροφοριών στην οικονομική κατασκοπεία.
Πρώτον, η οικονομική κατασκοπεία δεν είναι μια μοναδική δραστηριότητα. Μερικοί βλέπουν την οικονομική κατασκοπεία σαν μια αναλυτική διαδικασία στην οποία τα κενά της γνώσης καλύπτονται και οι αβεβαιότητες διαλευκαίνονται.
Δεύτερον, οι ερωτήσεις οικονομικής κατασκοπείας δεν αυτοπροσδιορίζονται. Είναι επιρρεπείς σε συγκρουόμενες ερμηνείες σχετικά με το τι πρέπει να εξετάσουμε, πώς να μετρήσουμε τι παρατηρείται, ποιες ερωτήσεις πρέπει να ψάξουμε από τις πληροφορίες που συλλέγονται και πώς να τις ερμηνεύσουμε.
Τρίτον, τα ερωτήματα σχετικά με τις πληροφορίες πρέπει να δημιουργούνται παρά να θεωρούνται δεδομένα.
Τέταρτον, το πρόβλημα της σύνδεσης των πολιτικών και των αναλυτών, που τόσο συχνά αναφέρεται για λογαριασμό πολιτικών ή στρατιωτικών πληροφοριών, είναι αρκετά ζωντανό στην οικονομική κατασκοπεία. (Hastedt, pp. 388-390)

Η κατασκοπεία και η συλλογή πληροφοριών είναι βασικά εργαλεία στα οικονομικά χαρτοφυλάκια πολλών εθνών, τόσο φιλικών όσο και εχθρικών.
Ο πρώην διευθυντής της CIA, William Webster, αναφέρει: «*Είναι δουλειά των υπηρεσιών πληροφοριών να εξετάσουν τι συμβαίνει, τις δυνάμεις που είναι στο παιχνίδι και τους τρόπους με τους οποίους οι ενέργειες που αναλαμβάνονται στο εξωτερικό μπορούν να επηρεάσουν συμφέροντα εθνικής ασφάλειας. Με σαφή κατανόηση των όρων ανταγωνισμού, οι υπεύθυνοι για τη χάραξη πολιτικής μπορούν να καθορίσουν καλύτερα εάν είναι ή όχι φρόνιμο, όσον αφορά τα συμφέροντα των ΗΠΑ. Η κατανόηση των δυνατοτήτων και των προθέσεων των ανταγωνιστών θα βοηθήσει τους υπεύθυνους χάραξης πολιτικής να αποφασίσουν πως θα πράξει το έθνος μας. Νομίζω ότι είναι πολύ σημαντικό να αναγνωρίζουμε ότι άλλες χώρες μπορεί να μην παίζουν βάσει κανόνων. Όσο πιο σύντομα και καλύτερα το καταλάβουμε, σε τόσο καλύτερη θέση θα είμαστε. Αυτό μπορεί να μην επηρεάζει τους δικούς μας κανόνες παιχνιδιού ή τα δικά μας πρότυπα, αλλά σίγουρα επηρεάζει αυτά που διακυβεύονται, το αποτέλεσμα, ακόμα και την απόφαση για το αν θα παίξουμε ή όχι σε αυτόν τον συγκεκριμένο οικονομικό χώρο*.» (Jeffrey, 1991, p. 205)

2.2 Μίκρο – μακροοικονομική κατασκοπεία

Η οικονομία αποτελεί θεμέλιο της στρατιωτικής ισχύς και αυτόνομο εργαλείο άσκησης εξωτερικής πολιτικής. Παρακολουθώντας την ανθρώπινη ιστορία διαπιστώνεται πως η οικονομία είναι μια μορφή πολέμου και η ισχύς ανήκει σε αυτόν που την κατάλληλη στιγμή επιτυγχάνει να αποκτήσει, αναλύσει και ανασυνθέσει με τη μεγαλύτερη ταχύτητα τα δεδομένα και τις πληροφορίες που είναι διαθέσιμα στο ανταγωνιστικό περιβάλλον. Η πληροφορία επιδιώκεται να αποκτηθεί με κάθε μέσο, θεμιτό ή αθέμιτο. Ο τρόπος για να αποκτηθεί αυτή η πληροφορία είναι η οικονομική κατασκοπεία. Η οικονομική κατασκοπεία διακρίνεται σε μακροοικονομική και μικροοικονομική, έχοντας αντίστοιχα η καθεμιά κίνητρα και αντικίνητρα.

Η μακροοικονομική κατασκοπεία αναφέρεται στη συλλογή και ανάλυση πληροφοριών οικονομικού περιεχομένου που σχετίζονται με τις οικονομικές δυνατότητες ενός κράτους. Συμπεριλαμβάνει την εκτίμηση των οικονομικών στρατηγικών και προθέσεων ξένων κυβερνήσεων και τον αντίκτυπο που έχουν αυτές στα κρατικά συμφέροντα. (Κωνσταντόπουλος, 2010, σσ. 281,283)

Αρχικά, η μακροοικονομική κατασκοπεία στοχεύει στη βοήθεια της πολιτικής ηγεσίας ενός κράτους, ούτως ώστε η τελευταία να διαχειριστεί με το βέλτιστο δυνατό τρόπο την οικονομική πολιτική της, εσωτερική και εξωτερική. Επίσης, περιλαμβάνει την απόκτηση πληροφοριών που δεν είναι διαθέσιμες από ελεύθερες πηγές. (Κωνσταντόπουλος, 2010, σ. 281)

Τα κίνητρα που σχετίζονται με την μακροοικονομική κατασκοπεία έχουν ως στόχο την αποτελεσματικότερη παρακολούθηση και καταγραφή των διεθνών εξελίξεων, τόσο σε οικονομικό όσο και σε τεχνολογικό τομέα, παρέχοντας την κατάλληλη υποστήριξη στους κυβερνητικούς αξιωματούχους στα πλαίσια της διαμόρφωσης οικονομικής πολιτικής, μέσω της κοινότητας των υπηρεσιών πληροφοριών. (Κωνσταντόπουλος, 2010, σσ. 423-424)

Δεδομένου ότι, πλέον, η ισχύς των κυβερνήσεων εξαρτάται όλο και περισσότερο από την οικονομική ισχύ, η επίτευξη των συμφερόντων αποτελεί προτεραιότητα αυξημένης σημασίας για τις υπηρεσίες πληροφοριών. Η μακροοικονομική κατασκοπεία βοηθά τους διαμορφωτές της πολιτικής να συμβαδίζουν με τις τελευταίες εξελίξεις στον οικονομικό και τεχνολογικό τομέα. (Κωνσταντόπουλος, 2010, σσ. 425-428)

Ένα θετικό αποτέλεσμα που προκύπτει από τη μακροοικονομική κατασκοπεία αφορά τη σχέση οφέλους – κόστους, καθώς για ένα κράτος είναι φθηνότερη η κλοπή οικονομικών, επιστημονικών και τεχνολογικών πληροφοριών από ότι η επένδυση και η ανάληψη κόστους για έρευνα και ανάπτυξη. Επίσης, το συγκριτικό πλεονέκτημα που διαθέτουν οι υπηρεσίες πληροφοριών συγκρίσει άλλων κυβερνητικών υπηρεσιών άπτεται στην πρόσβαση που έχουν σε μυστικές πηγές, οι οποίες δεν διατίθενται σε άλλες υπηρεσίες, κυβερνητικές και μη. (Κωνσταντόπουλος, 2010, σ. 426)

Οι λόγοι που λειτουργούν ως ανασταλτικοί παράγοντες εμπλοκής σε επιχειρήσεις μακροοικονομικής κατασκοπείας στα κράτη είναι τρεις.
Πρώτον, η μακροοικονομική κατασκοπεία προκαλεί κωλύματα στην άσκηση διπλωματίας από το κράτος, καθώς δεν είναι πάντα ευδιάκριτος ο διαχωρισμός αντιπάλων – συμμάχων. Επιπρόσθετα, διάφοροι αναλυτές υποστηρίζουν πως οι υπηρεσίες πληροφοριών δεν δημιουργήθηκαν για να μελετούν τη διεθνή οικονομία, αλλά αναπτύχθηκαν κυρίως στην περιοχή της εθνικής ασφάλειας και πρέπει να συνεχίσουν πάνω σε αυτόν τον τομέα, καθώς η διεύρυνση του πεδίου δράσης της κοινότητας των πληροφοριών εξασθενεί στο συγκριτικό τους πλεονέκτημα ˙ την ενασχόλησή τους, δηλαδή, με μυστικές πληροφορίες. Στον αντίποδα αυτής της άποψης οι υποστηρικτές της μακροοικονομικής κατασκοπείας παραθέτουν το εξής επιχείρημα, ότι ακόμα και στην εποχή του Ίντερνετ υπάρχουν μυστικά. Ο Ray Cline χαρακτηρίζει την κατασκοπεία ως την αναζήτηση των μη διαθέσιμων πληροφοριών από ανοιχτές πηγές. Κύριες πηγές οικονομικών πληροφοριών είναι οι ανοιχτές πηγές, οι ανοιχτές αναφορές και οι μυστικές αναφορές.
Επιπλέον, υπάρχουν προβλήματα ανάλυσης παρόμοια με εκείνα που προκύπτουν και στην ανάλυση άλλου είδους πληροφοριών. Η συλλογή και ανάλυση πληροφοριών βοηθάει τους αναλυτές να διαμορφώσουν απαντήσεις, αλλά αυτές δεν είναι οριστικές καθώς στοιχεία αβεβαιότητας και αμφιβολίας συνεχίζουν να υπάρχουν.
Στην πράξη αποδεικνύεται πως τα παραπάνω αντικίνητρα δεν λειτούργησαν αποθαρρυντικά για τα κράτη ώστε να μην ασκήσουν μακροοικονομική δραστηριότητα. (Κωνσταντόπουλος, 2010, σσ. 431-436, 439-441)

Η μικροοικονομική κατασκοπεία σχετίζεται με τη συλλογή και ανάλυση των οικονομικών πληροφοριών με στόχο την υποστήριξη συγκεκριμένων επιχειρήσεων έναντι των ξένων ανταγωνιστών τους. Μετά τον Ψυχρό Πόλεμο, τίθεται το ερώτημα σε ποιο βαθμό οι μυστικές υπηρεσίες μπορούν να χρησιμοποιήσουν και κατ' επέκταση να βοηθήσουν τις επιχειρήσεις. (Κωνσταντόπουλος, 2010, σ. 446)

Όσον αφορά, λοιπόν, τα κίνητρα για τη μικροοικονομική κατασκοπεία, τα οικονομικά κίνητρα δικαιολογούν την κρατική συμπεριφορά επειδή, πρώτον, όπως υποστηρίζει ο Robert Gilpin «*πρόκειται για μια προσπάθεια του κράτους να αλλάξει το διεθνές στρατηγικό περιβάλλον, ούτως ώστε να δίνει ορισμένα πλεονεκτήματα στις εταιρείες της χώρας καταγωγής*». Δεύτερον, οι πληροφορίες κατονομάζονται ως δημόσια αγαθά και εξαιτίας αυτού μπορεί κάποιος να θεωρήσει ότι αυτή η οικονομική λογική δικαιολογεί την άσκηση οικονομικής κατασκοπείας. Τρίτον, η οικονομική λογική της οικονομικής κατασκοπείας γίνεται βάσει της έννοιας της αστυνόμευσης που έδωσε ο Brander σύμφωνα με την οποία «*οι υπηρεσίες αστυνόμευσης παρέχονται καλύτερα από το κράτος. Η συλλογή οικονομικών πληροφοριών όσο και η αντικατασκοπεία αποτελούν νομιμοποιημένες δραστηριότητες αστυνόμευσης, σημαντικές για την ασφάλεια του συστήματος*».
Οι επιχειρήσεις μικροοικονομικής κατασκοπείας είναι επικερδείς και για τις ίδιες τις υπηρεσίες πληροφοριών. Όπως χαρακτηριστικά αναφέρει ο Count de Marenches, ένας από τους τελευταίους επικεφαλής των Γαλλικών υπηρεσιών πληροφοριών, «*Υπάρχουν περιπτώσεις στις*

οποίες ολόκληρος ο ετήσιος προϋπολογισμός της λειτουργίας τους καλύπτεται από μια και μόνο επιχείρηση μικροοικονομικής κατασκοπείας». (Κωνσταντόπουλος, 2010, σσ. 447,525, 532-534)

Στον αντίποδα όμως των κινήτρων της μικροοικονομικής κατασκοπείας, βρίσκονται έξι αντικίνητρα. (Κωνσταντόπουλος, 2010, σσ. 541-575)

1. Πολίτικά ή διπλωματικά αντικίνητρα: σύμφωνα με τα οποία η μικροοικονομική κατασκοπεία αποτελεί σπατάλη των πλεονεκτημάτων των υπηρεσιών πληροφοριών
2. Οικονομικά αντικίνητρα: Η μικροοικονομική κατασκοπεία εξισώνεται με την κλοπή και διαβρώνει την επιστημονική και τεχνολογική βάση ενός κράτους.
3. Νομικά αντικίνητρα: η μικροοικονομική κατασκοπεία θεωρείται ως η δραστηριότητα που αποτελεί μια καταφανή παραβίαση της ισχύουσας αστικής και ποινικής νομοθεσίας καθώς και των διεθνών συμβάσεων σχετικά με την πνευματική ιδιοκτησία. Θεωρείται πως ένα κράτος που ασκεί μικροοικονομική κατασκοπεία εναντίον άλλου κράτους επεμβαίνει στις εσωτερικές του υποθέσεις.
4. Πρακτικά αντικίνητρα: υπάρχει πρόβλημα σχετικά με τον προσδιορισμό της ταυτότητας και της αφοσίωσης των επιχειρήσεων.
5. Αντικίνητρα που σχετίζονται με την κοινότητα των υπηρεσιών πληροφοριών: Οι υπηρεσίες πληροφοριών δεν ιδρύθηκαν για να συλλέγουν πληροφορίες που είναι δημόσια διαθέσιμες. Η διατήρηση της ασφάλειας των πηγών και των μεθόδων, παράλληλα με την προετοιμασία για την ανάληψη από τις μυστικές υπηρεσίες σκοπών. Μια διευρυμένη διανομή των οικονομικών μυστικών συνεπάγεται έναν σημαντικό κίνδυνο αποκάλυψης ευαίσθητων πηγών και μεθόδων
6. . Αντικίνητρα που σχετίζονται με την επιχειρηματική κοινότητα: Στους κύκλους της επιχειρηματικής κοινότητας δεν έχει διατυπωθεί κάποια θέση δημόσια για το πρόγραμμα μικροοικονομικής κατασκοπείας. Υπάρχουν φόβοι για τα αντίποινα που μπορεί να προκληθούν από τις ξένες κυβερνήσεις αλλά ακόμα και από την έλλειψη εμπιστοσύνης που θα προκύψει από τους μετόχους της ίδιας της εταιρείας. Ακόμα, οι επιχειρήσεις προβάλλουν και το φόβο παρακολούθησης των ίδιων, εν τέλει, από τη CIA. Αναγνωρίζουν, παρόλα αυτά, ότι η υποστήριξη από τις υπηρεσίες πληροφοριών ναι μεν θα ήταν ωφέλιμη αλλά δεν είναι επιτακτική ανάγκη.

Η μικροοικονομική κατασκοπεία είναι προβληματική καθώς συνεπάγεται όχι μόνο την κατασκοπεία εις βάρος εχθρών αλλά και συμμάχων. Βάσει των ανωτέρω προκύπτει πως το σημαντικότερο κίνητρο οικονομικής κατασκοπείας είναι τα οικονομικά οφέλη, από την μακροοικονομική σκοπιά, για μια χώρα, μιας και περιορίζει αισθητά μια cost-benefit analysis. Στον αντίποδα, τα σημαντικότερα αντικίνητρα εφαρμογής, ή τουλάχιστον παραδοχής, οικονομικής κατασκοπείας εστιάζονται στον μικροοικονομικό τομέα και αφορούν αφενός το να χαθεί η εμπιστοσύνη μεταξύ συμμάχων, καθώς δεν θα παρατηρηθεί ρωγμή μόνο σε διεθνές διπλωματικό επίπεδο αλλά και στις μεταξύ τους οικονομικές σχέσεις, και αφετέρου να διαρρεύσουν ευαίσθητες πληροφορίες.

Κεφάλαιο 3

3.1 Τεχνολογία και cyber intelligence

Οι αλλαγές που έλαβαν χώρα στην βιομηχανία από τα τέλη του 19ου αιώνα και τον 20ο αιώνα, με τη Βιομηχανική Επανάσταση, έδωσαν ώθηση στην οικονομική δραστηριότητα και επηρέασαν ριζικά τις κοινωνίες μέσα στις οποίες πραγματοποιήθηκαν οι αλλαγές αυτές. Η διαδικασία που άρχισε με τη Βιομηχανική Επανάσταση συνεχίζεται ακόμα και σήμερα, αποτελώντας βασική αρχή των οικονομικών ότι η διαρκής εισροή σημαντικών τεχνολογιών αποτελεί απαραίτητη προϋπόθεση για την επίτευξη και διατήρηση της οικονομικής ανάπτυξης. (Rubenstein, 2014)

Στα πλαίσια των διεθνών σχέσεων η τεχνολογία διαδραματίζει σημαντικό ρόλο στα ζητήματα στρατιωτικής ασφάλειας γενικότερα και ιδιαίτερα στη διεξαγωγή πολέμου. Στην εποχή μας, όπου ορθώς χαρακτηρίζεται ως η εποχή της πληροφορίας, οι σχέσεις μεταξύ της πολιτικής τεχνολογίας και της στρατιωτικής τεχνολογίας γίνονται πιο στενές καθώς η πρώτη παράγει τεχνολογικά προϊόντα διπλής χρήσης (dual use), τα οποία χρησιμοποιεί η δεύτερη. Η τεχνολογική εξέλιξη ενός κράτους επηρεάζει αδιαμφισβήτητα την οικονομική και στρατιωτική ισχύ τόσο σε περιόδους πολέμου όσο και ειρήνης. Επειδή η έννοια της ισχύος σε όλες τις διαστάσεις είναι σχετική, συνεπάγεται ότι η τεχνολογική εξέλιξη επηρεάζει τη σχετική ισχύ ενός κράτους σε σχέση με τα άλλα κράτη. Η τεχνολογία μεταμορφώνει τον κόσμο και ασκεί επιρροή στις σχέσεις μεταξύ των κρατών. (Rubenstein, 2014)

Ένα από τα πιο σημαντικά διεθνή προβλήματα που σχετίζονται με την τεχνολογία αποτελεί η κυβερνοκατασκοπεία και εξίσου δύσκολος ο ορισμός της. Οι ορισμοί που έχουν δοθεί είναι πολλοί, αφού είναι δύσκολο να δοθεί ένας ομόφωνος και κοινά αποδεκτός. Το πώς γίνεται αντιληπτή η κυβερνοκατασκοπεία, ως ορισμός, εξαρτάται από πολλούς παράγοντες, όπως είναι η έκταση και η φύση της ζημιάς που δημιουργείται, η ταυτότητα των επιθέσεων και ο τρόπος με τον οποίο εκλάπησαν οι πληροφορίες. Το 2013 στο συνέδριο που πραγματοποιήθηκε στο Tallin της Εσθονίας από το ΝΑΤΟ η κυβερνοκατασκοπεία ορίστηκε ως «εκείνη η πράξη που έχει αναληφθεί κρυφά ή από ψευδείς προθέσεις και χρησιμοποιεί τις ικανότητες του κυβερνοχώρου για τη συλλογή (ή προσπάθεια συλλογής) πληροφοριών με σκοπό τη μεταβίβαση αυτών στον αντίπαλο». Περιέργως, δεν είναι τεχνικά τα εμπόδια που υπάρχουν προκειμένου να παρασχεθεί βοήθεια στα κράτη που γίνονται θύματα αυτών των επιθέσεων, αλλά νομικά και πολιτικά εμπόδια είναι αυτά που καθιστούν δύσκολο για ένα κράτος να αμυνθεί. (Rubenstein, 2014)

Υπάρχουν δυο σημαντικές τάσεις που σχετίζονται με τη μοντέρνα κυβερνοκατασκοπεία των κρατών, οι οποίες έχουν διαμορφώσει όχι μόνο το τοπίο του κυβερνοχώρου αλλά ακόμα και τη δημόσια αντίληψη σχετικά με την κυβερνοκατασκοπεία και τον πόλεμο. Η πρώτη αναφέρει πως η κυβερνοκατασκοπεία γίνεται όλο και πιο εξελιγμένη, αποτελεσματική και επαγγελματική. Κάτι που είναι φυσικό, καθώς ο κόσμος μας αυξάνει όλο και περισσότερο την

εξάρτησή του στους υπολογιστές · κατ' επέκταση, οι εγκληματικές δραστηριότητες μεταφέρονται στον ψηφιακό κόσμο. Αυτό αποδεικνύει ότι η κυβερνοκατασκοπεία δεν αποτελεί πλέον σενάριο επιστημονικής φαντασίας. (Rubenstein, 2014)

Συνεπώς, αυτό οδηγεί στη δεύτερη τάση, σύμφωνα με την οποία η κυβερνοκατασκοπεία γίνεται αποδεκτή -ακόμα και προτιμούμενος ως- τρόπος πολέμου, επηρεάζοντας τη φύση της διαμάχης μεταξύ των κρατών χωρίς να αντικαθιστά τα παραδοσιακά μέσα πολέμου. Το γεγονός ότι ένας πραγματικός πόλεμος μεταξύ μεγάλων δυνάμεων στον μοντέρνο κόσμο είναι λιγότερο αποδεκτός κάνει λογική την προτίμηση περισσότερο λανθανουσών στρατηγικών. Αυτή η στροφή τακτικής ξεκίνησε από τον Ψυχρό Πόλεμο, όταν οι ΗΠΑ και η Ρωσία είχαν επικεντρώσει τις προσπάθειές τους συλλογή μυστικών πληροφοριών. Με την τεχνολογία να εξελίσσεται όλο και περισσότερο τις τελευταίες δεκαετίες, τα εργαλεία της κυβερνοκατασκοπείας αποτελούν αναπόσπαστο κομμάτι στις μοντέρνες στρατιωτικές επιχειρήσεις. (Rubenstein, 2014)

Τα κράτη έχουν, πια, διαθέσιμα πολλά διαφορετικά εργαλεία κυβερνοκατασκοπείας, πολλά εκ των οποίων δεν διαφέρουν από τις επιθέσεις που πιθανό να δεχτεί κάποιος στον προσωπικό του υπολογιστή, η διαφορά έγκειται στο ότι εφαρμόζονται σε μεγαλύτερη κλίμακα. Η ψηφιακή τεχνολογία επηρεάζει με απροσδόκητους τρόπους την κυβερνοκατασκοπεία. Για παράδειγμα, μπορεί κάποιος να αποκτήσει πρόσβαση στο δίκτυο του θύματος και να χειριστεί τι βλέπει το θύμα σε πραγματικό χρόνο. (Rubenstein, 2014)

Επιπρόσθετα, η κυβερνοκατασκοπεία δεν λαμβάνει χώρα μόνο στον τομέα του πολέμου. Τα κράτη χρησιμοποιούν τα εργαλεία του κυβερνοχώρου ανταγωνιζόμενα μεταξύ τους προκειμένου να κλέψουν οικονομικά και χρηματοπιστωτικά δεδομένα, σκοπεύοντας, μέσα από τη χρήση αυτών των εμπιστευτικών πληροφοριών, να αποκτήσουν προβάδισμα στις αγορές · αποσκοπούν, δηλαδή, περισσότερο σε οικονομικό πλεονέκτημα παρά σε πολιτικό. Οι περισσότερες καταγεγραμμένες επιθέσεις φαίνονται να έχουν στόχο χρηματοπιστωτικές πληροφορίες από ιδιωτικές επιχειρήσεις, επειδή είναι μεν πιο εύκολο να προσβληθούν από ότι οι κυβερνητικές υπηρεσίες και αυτού του είδους τα δεδομένα είναι περισσότερο επικερδή. (Rubenstein, 2014)

Για τους σημερινούς χρήστες του Ίντερνετ, η διεθνής κυβερνοκατασκοπεία μπορεί να φαντάζει σαν κάτι τόσο μακρινό όσο και μικρής σημασίας. Οι ιδιώτες δεν βλέπουν την επίδραση της κυβερνοκατασκοπείας στις ζωές τους αλλά για ένα κράτος είναι ιδιαίτερα σημαντική. Ο αντίκτυπος μπορεί να ποικίλει και να κινείται μεταξύ οικονομικής ζημιάς έως ζημιά σε πολιτικές υλικές υποδομές.

Όσον αφορά το κόστος, παρουσιάζεται και εκεί μια ποικιλομορφία αναλόγως την έκταση · υπάρχουν, όμως, περιπτώσεις όπου είναι αρκετά υψηλό. Για το κράτος που επιτίθεται, το κόστος είναι αισθητά χαμηλό, από ότι αν πραγματοποιούσε επίθεση άλλης φύσης, και τα πλεονεκτήματα αρκετά. Πρώτον, η κυβερνοκατασκοπεία έχει το πλεονέκτημα της ανωνυμίας και τα κράτη-θύματα δύσκολα μπορούν να αποδείξουν την ταυτότητα του δράστη. Αυτό

σημαίνει πως μπορεί να διεξαχθεί ακόμα και σε καιρό ειρήνης χωρίς να ενέχει το φόβο αποκάλυψης. Επίσης, θεωρείται πως είναι καλύτερη η τακτική το να εστιάσει κανείς στην επίθεση από το να είναι σε θέση άμυνας. Ο αμυνόμενος πρέπει να σχεδιάσει την προστασία όλων των πιθανών τρωτών σημείων, ενώ στην αντίπερα όχθη για αυτόν που πραγματοποιεί την επίθεση, μονάχα ένα τρωτό σημείο είναι αρκετό. Επομένως, κάθε κράτος που διαθέτει σημαντικές πληροφορίες είναι αυτόματα και πιθανός στόχος. (Rubenstein, 2014)

Αν και πολλές είναι οι χώρες που διαπράττουν κυβερνοκατασκοπεία, οι ΗΠΑ, η Ρωσία και η Κίνα είναι αυτές που θεωρούνται οι πιο εξελιγμένοι και αποδοτικοί κυβερνοκατάσκοποι. Την τελευταία δεκαετία οι ΗΠΑ έχουν αρχίσει να εισάγουν τον κυβερνοπόλεμο στην άποψη που έχουν για τον πόλεμο. Αρχικά, ξεκίνησαν οι προετοιμασίες το 2002 με την Προεδρική Οδηγία για την Εθνική Ασφάλεια, η οποία υπογράμμιζε στρατηγικές, θεωρίες, διαδικασίες και πρωτόκολλα για τον κυβερνοπόλεμο. Ακολούθησε ο Χάρτης Πορείας για τις Πράξεις Πληροφόρησης το 2003, ο οποίος άρχισε να ενσωματώνει προετοιμασίες για τον κυβερνοπόλεμο, όπως για παράδειγμα την εκπαίδευση στρατιωτικού προσωπικού στην άμυνα του κυβερνοχώρου, ως μέρος μιας συνήθους στρατιωτικής επιχείρησης. Επίσης, οι ΗΠΑ έχουν αρχίσει να χορηγούν περισσότερες χρηματοδοτήσεις για την εξασφάλιση των υποδομών που ενδέχεται να είναι περισσότερο ευάλωτες στις επιθέσεις, όπως είναι συστήματα ηλεκτροδότησης, νερού, πετρελαίου και αερίου. (Rubenstein, 2014)

Η Κίνα, ένας ακόμα μεγάλος παράγοντας στο παιχνίδι της κυβερνοκατασκοπείας, τα τελευταία χρόνια έχει αυξήσει το ποσοστό χρόνου, πόρων και ανθρώπινου δυναμικού που διαθέτει σχετικά με την κυβερνοκατασκοπεία. Αν και συνήθως είναι δύσκολη η επαλήθευση και επιβεβαίωση της πηγής οποιασδήποτε κυβερνοεπίθεσης, έχει επιβεβαιωθεί πως η Κίνα είναι υπεύθυνη για την επίθεση στα δίκτυα των ΗΠΑ και για την κλοπή δεδομένων ασφαλείας σε πολλές υποθέσεις. Παρόλα αυτά, αυτό που προκύπτει είναι πως η Κίνα μοιάζει να κλέβει χρηματοπιστωτικά και οικονομικά μυστικά με σκοπό να ενισχύσει την οικονομία της. (Rubenstein, 2014)

Τελευταίος και εξίσου μεγάλος παράγοντας σήμερα στην κυβερνοκατασκοπεία είναι η Ρωσία. Υπάρχουν υποψίες ότι ο Ρωσικός στρατός έχει στην κατοχή του κυβερνο-όπλα περισσότερο εξελιγμένα από αυτά που έχει η Κίνα. Η Ρωσία, όπως και η Κίνα, έχει ειδικές στρατιωτικές μονάδες που ασχολούνται αποκλειστικά με τον κυβερνοπόλεμο ˙ χάκερς, τους οποίους στρατολογεί κατευθείαν από το πανεπιστήμιο. Σε αντίθεση όμως με την Κίνα, η Ρωσία χρησιμοποιεί τη δύναμή της στον κυβερνοχώρο, ώστε να συμπληρώσει περισσότερες επιθετικές μορφές πολέμου από το να κλέψει απλά οικονομικά μυστικά. (Rubenstein, 2014)

3.2 Η στάση των εταιρειών και της κυβέρνησης σχετικά με την κυβερνοκατασκοπεία

Η κυβέρνηση των ΗΠΑ, περίπου τα τελευταία δέκα χρόνια, συνεργάζεται εθελοντικά με ιδιωτικές επιχειρήσεις και μη κερδοσκοπικούς συνεργάτες προκειμένου να εκμεταλλευτεί την εμπειρογνωμοσύνη που δεν έχει πάνω σε πλήθος θεμάτων, όπως για παράδειγμα της ασφάλειας. Στον απόηχο της 11ης Σεπτεμβρίου η έννοια της συμμετοχής επεκτάθηκε ακόμα περισσότερο στον τομέα των πληροφοριών. Εξαιτίας της παγκοσμιοποίησης και της επανάστασης των επικοινωνιών στον κυβερνοχώρο, οι παράγοντες και οι δυνάμεις που καθορίζουν την ευημερία και την ασφάλεια, τις καθιστούν περισσότερο περίπλοκες και αλληλένδετες. Επομένως, λόγω του νέου περιβάλλοντος η κυβέρνηση των ΗΠΑ εργάζεται ούτως ώστε να αξιοποιήσει τις δυνατότητες του ιδιωτικού τομέα ώστε να πετύχει τους στόχους που σχετίζονται με την εθνική ασφάλεια. Ακόμα και η κοινότητα των πληροφοριών συμμετέχει στη σχέση δημόσιου και ιδιωτικού τομέα. Αυτό υποστηρίζεται και από δήλωση που έκανε η Υπουργός Εξωτερικών Hillary Clinton «*Τα προβλήματα που αντιμετωπίζουμε σήμερα δεν μπορούν να λυθούν μόνο από τις κυβερνήσεις, αλλά μέσω συνεργασιών*». Στο ίδιο μήκος κυμαίνονται και οι δηλώσεις Ευρωπαίων αξιωματούχων λέγοντας πως «*Η ασφάλεια εξ ορισμού είναι διατομεακή και διασυνοριακή. Συνεπώς πρέπει να ενεργείς εξωτερικά για να πετύχεις εσωτερική ασφάλεια και το αντίστροφο*». (James Stavridis, 2013, pp. 7-11)

Η συνεργασία δημόσιου και ιδιωτικού τομέα εμπίπτει σε αρκετές κατηγορίες δραστηριοτήτων όπως είναι η ανταλλαγή τεχνογνωσίας, η ανταλλαγή πληροφοριών και η εκτέλεση έργων και επιχειρήσεων. Αμφότερα τα μέρη ωφελούνται. Όσον αφορά την κυβέρνηση, στο σημερινό οικονομικά περιορισμένο οικονομικό περιβάλλον, τα οφέλη είναι εμφανή. Το βασικό πλεονέκτημα είναι η πρόσβαση που αποκτά σε εμπειρογνωμοσύνη, ανάλυση, δεξιότητες, προοπτικές και πόρους που δεν είναι πάντα διαθέσιμα στο δημόσιο τομέα. Από την άλλη πλευρά, οργανισμοί και εταιρείες που συνεργάζονται με την κυβέρνηση μπορούν να προωθήσουν τον πατριωτισμό, τη συμμετοχή των πολιτών και να συμβάλλουν στη χρηστή διακυβέρνηση. (James Stavridis, 2013, pp. 12-16)

Είθισται η κυβέρνηση να είναι εκείνη που θα οδηγήσει σε καινοτομία όλους τους τομείς της άμυνας και της επιστήμης, μειώνοντας το κίνητρο για συνεργασία. Κάτι τέτοιο πλέον δεν ισχύει. Μεγάλο μέρος των έργων αιχμής πραγματοποιείται από τον ιδιωτικό τομέα. Είναι περισσότερο εμφανές στον τομέα των υπολογιστών και της τεχνολογίας των πληροφοριών αλλά, μεταξύ άλλων, εκτείνεται μέχρι τον τομέα της ενέργειας και της νανοτεχνολογίας. Αυτό έχει ως αποτέλεσμα η κυβέρνηση να εξαρτάται από την εξειδίκευση του ιδιωτικού τομέα ώστε να διατηρήσει το προβάδισμά της στην άμυνα, το διάστημα και άλλους τομείς που συνδέονται με την ασφάλεια. Παρόλα αυτά, αυτή η εξάρτηση σημαίνει πως η κυβέρνηση είναι το ίδιο εκτεθειμένη στα ίδια σημεία με τον ιδιωτικό τομέα ˙ πιθανότατα και πέρα από περιοχές όπου ο ιδιωτικός τομέας έχει το τεχνολογικό προβάδισμα. Αναφορικά, λοιπόν, τόσο η κυβέρνηση όσο και ο ιδιωτικός τομέας μπορούν να παρακολουθήσουν τις αναπτυσσόμενες κοινές απειλές

μέσω της συνεργασίας, όπως, για παράδειγμα, είναι η οικονομική απάτη και η οικονομική κατασκοπεία. (James Stavridis, 2013, p. 12)

Στον αντίποδα των πλεονεκτημάτων υπάρχουν τα εμπόδια για αυτή τη συνεργασία. Τέτοια είναι οι νομικοί και κανονιστικοί περιορισμοί, η απουσία εμπιστοσύνης και η έλλειψη κατάλληλης θεσμοθέτησης των προσπαθειών του δημοσίου και ιδιωτικού τομέα.
Η έλλειψη εμπιστοσύνης εμφανίζεται και στις δύο πλευρές όταν πρόκειται για τον κλάδο του κυβερνοχώρου. Οι επιφυλάξεις της κυβέρνησης σχετίζονται με τον ιδιωτικό τομέα, καθώς είναι αυτός που κατασκευάζει το λογισμικό και το υλικό που χρειάζεται ο κυβερνοχώρος για να λειτουργήσει. Συνεπώς, οποιεσδήποτε αδυναμίες που θα παρουσιαστούν σε αυτές τις υποδομές, οι ιδιωτικές επιχειρήσεις δεν είναι διατεθειμένες να τις μοιραστούν με κανέναν, πόσο μάλλον με την κυβέρνηση. Δεδομένου αυτού, η κυβέρνηση διατηρεί μια επιφύλαξη με συγκεκριμένες εταιρείες, κυρίως με εκείνες που η δραστηριότητά τους εκτείνεται ανά τον κόσμο και έχουν παγκόσμια συμφέροντα. (James Stavridis, 2013, pp. 16-19)
Περαιτέρω ανησυχίες που έχουν εκφραστεί αναφέρουν πως μια τέτοια σύμπραξη θα ενισχύσει την ύπαρξη μονοπωλίων στις μεγάλες επιχειρήσεις και κυβερνητικό έλεγχο. Ειδικότερα, οι επιχειρήσεις που θα ασχοληθούν με τον τομέα της οικονομικής κατασκοπείας εκφράζουν φόβους πως η συνεργασία αυτή θα καταλήξει στην παρακολούθηση των ίδιων από τις μυστικές υπηρεσίες. Η σύνδεσή τους, επομένως, με τις μυστικές υπηρεσίες, θεωρούν πως, θα τους αποφέρει σημαντικές ζημιές, καθώς οι εμπορικές τους σχέσεις και η φερεγγυότητά τους θα πληγούν. Υπάρχουν όμως και οι υποστηρικτές του συγκεκριμένου προγράμματος, οι οποίοι αναφέρουν την παραδοσιακή σχέση που έχει η Αμερικανική βιομηχανία με την κοινότητα των πληροφοριών, έχοντας ως παράδειγμα τη Lockheed. (Κωνσταντόπουλος, 2010, σ. 575)

Και τα δύο μέρη είναι καλό να θεωρούν πως ο άλλος θα προστατεύσει τις πληροφορίες και την ιδιωτικότητα εκείνων για τους οποίους είναι υπεύθυνοι. Η εμπιστοσύνη, επομένως, είναι ένα σημαντικό θέμα που πηγάζει μέσα από την ιδιωτικότητα. Τα στελέχη των επιχειρήσεων ανησυχούν σχετικά με την ιδιωτικότητα της επιχείρησής καθώς επίσης και με την ιδιωτικότητα των πελατών και των καταναλωτών τους ˙ συνεπώς, με την ιδιωτικότητα των Αμερικανών πολιτών. Εν τω μεταξύ, η κυβέρνηση είναι αυτή που είναι υπεύθυνη για την προστασία της ιδιωτικότητας των πολιτών της, αλλά στο όνομα της διασφάλισης της τάξης και της εθνικής ασφάλειας στρέφει το προνόμιο αυτό εναντίον τους. (James Stavridis, 2013)

3.3 Η περίπτωση Snowden

Τον Ιούνιο 2013 δημιουργήθηκε πλήγμα στη σχέση εμπιστοσύνης και ιδιωτικότητας μεταξύ της κυβέρνησης και των εταιρειών, μετά την αποκάλυψη εμπιστευτικών εγγράφων και πληροφοριών από τον πρώην πράκτορα της CIA Edward Snowden, στα οποία φαίνεται η δράση της Εθνικής Υπηρεσίας Ασφαλείας των ΗΠΑ (National Security Agency – NSA). Ειδικότερα, εστιάζει σε ένα πρόγραμμα της NSA (PRISM) που στόχευε στις επικοινωνίες μέσω Ίντερνετ και αποθήκευε δεδομένα μη Αμερικανών πολιτών εκτός Ηνωμένων Πολιτειών – και με όσους εκείνοι επικοινωνούσαν- καθώς, επίσης, και μέχρι ποιο σημείο εκτείνεται η συνεργασία αμερικανικών εταιρειών με την κυβέρνηση. (Landau, 2013, p. 66)

Ο ίδιος ο Snowden υποστηρίζει πως προέβη σε αυτή την κίνηση ορμώμενος από ένα αίσθημα δικαίου και ευθύνης απέναντι στους Αμερικανούς πολίτες, και όχι μόνο, θεωρώντας πως πρέπει να γνωρίζουν με τι ασχολείται η NSA. Η διαρροή των πληροφοριών αποκάλυψε πως η NSA συνέλεγε «μεταδεδομένα» - τις καταγραφές, δηλαδή, των τηλεφωνικών αριθμών που πληκτρολογήθηκαν και τη διάρκεια των κλήσεων – σχεδόν στο 1/3 του συνόλου των τηλεφωνικών κλήσεων που πραγματοποιούνταν από Αμερικανούς πολίτες είτε βρίσκονταν στις ΗΠΑ είτε εκτός. Επιπλέον, η υπηρεσία συνέλεγε και δεδομένα από τη χρήση των μέσων κοινωνικής δικτύωσης που έκαναν Αμερικανοί πολίτες.

Αρχικά, αυτού του τύπου η κατασκοπεία , και οι ικανότητες της NSA να το εκμεταλλεύεται, δεν αποτελεί κάτι καινούριο, μιας και η NSA έχει ξεκινήσει την προσπάθεια εκμετάλλευσης των δικτύων από το 1990. Στον απόηχο των γεγονότων της 11ης Σεπτεμβρίου, τα κριτήρια διεξαγωγής παρακολούθησης, είτε πρόκειται για ηλεκτρονική είτε για άλλου είδους, χαλάρωσαν. Λίγο μετά τις τρομοκρατικές επιθέσεις του 2001, ο τότε Πρόεδρος George W. Bush διεύρυνε την αρμοδιότητα της Εθνικής Υπηρεσίας Ασφαλείας να υποκλέπτει χωρίς ένταλμα διεθνείς συνομιλίες, των οποίων το ένα μέρος θα βρίσκεται εκτός ΗΠΑ. (Landau, 2013, σσ. 66-71)

Η διαφωνία που προκύπτει από αυτό έγκειται στο ότι ο όρος «μαζική παρακολούθηση» ουσιαστικά είναι μια εσφαλμένη ονομασία. Μαζική παρακολούθηση θα συνιστούσε τα εμπλεκόμενα κράτη να παρακολουθούν συστηματικά τις επικοινωνίες που έχουν οι πολίτες τους και δυνητικά να στρέφονται εναντίον τους σύμφωνα με τις πληροφορίες που αποκόμιζαν από αυτή τη διαδικασία. Παρόλα αυτά δεν υπάρχουν στοιχεία που να αποδεικνύουν πως κάποιος υπέστη άδικη συμπεριφορά ή διάκριση, ως αποτέλεσμα της παραπάνω πράξης. (Inkster, 2014, p. 52)

Η διαρροή του Snowden, χαρακτηρίστηκε από τον σε σύνταξη διευθυντή της NSA, στρατηγό Keith B. Alexander ως «*Η μεγαλύτερη ζημιά στα εθνικά συστήματα πληροφοριών που έχουμε υποστεί ποτέ*» (Johnson, 2014, p. 794) και από την Πρόεδρο της Επιτροπής Πληροφοριών της Γερουσίας ως «*πράξη προδοσίας*» (Landau, 2013, σ. 66).
Η διαρροή αυτή δεν αποτελεί, όμως, το πρώτο περιστατικό, καθώς το 1960 δύο νέοι υπάλληλοι της Εθνικής Υπηρεσίας Ασφάλειας των ΗΠΑ, οι Bernon Mitchell και William Martin,

αποστάτησαν και κατέφυγαν στη Σοβιετική Ένωση, αποκαλύπτοντας διάφορες πολιτικές των ΗΠΑ –κυρίως προκλητικές επιδρομές στον εναέριο χώρο άλλων κρατών- και τη διάπραξη κατασκοπείας σε συμμάχους τους. Σύμφωνα με τον David M. Barrett, ο Snowden δείχνει να έχει τα ίδια χαρακτηριστικά ˙ να είναι, δηλαδή, αφελής και αλαζόνας, που επιθυμεί να κάνει κάτι καλό. Ο ίδιος ο Snowden σε δήλωσή του αναφέρει πως «*Καμιά φορά χρειάζεται να παραβείς το νόμο προκειμένου να κάνεις κάτι καλό.. εφόσον δεν βλάπτεις κάποιον άλλο*». Ο David M. Barrett αντιπαρατίθεται στη συγκεκριμένη άποψη αναφέροντας πως «*οι ξένες κυβερνήσεις, προφανώς, έμαθα ακόμα περισσότερα πράγματα για τις μυστικές υπηρεσίες των ΗΠΑ, από ό, τι θα έπρεπε να ξέρουν*». (Barrett, 2014, pp. 796-797)

Κατ' επέκταση, αν κάποιος ζημιώθηκε από αυτό, αυτές είναι οι ΗΠΑ. Από τη μία πλευρά, οι εταιρείες που συνεργάζονταν με την Υπηρεσία ανησυχούσαν πως πιθανόν θα έρχονταν αντιμέτωποι με έναν αποκλεισμό από τους διεθνείς πελάτες τους, εξαιτίας της συνεργασίας τους ˙ θα έχαναν την αξιοπιστία τους και οι πελάτες τους θα θεωρούσαν πως τα προσωπικά τους δεδομένα είναι εκτιθέμενα και δεν προστατεύονται, όπως θα έπρεπε. Από την άλλη πλευρά, υπήρχε έντονη δυσαρέσκεια από τους συμμάχους των ΗΠΑ. Μάλιστα, ο Πρόεδρος της Ευρωπαϊκής Ένωσης, σε δήλωσή του, προειδοποίησε πως «*Εάν οι ισχυρισμοί αποδειχτούν αληθείς, θα ήταν ένα εξαιρετικής σημασίας θέμα με ιδιαίτερα σοβαρές επιπτώσεις στις σχέσεις της Ευρωπαϊκής Ένωσης με τις Ηνωμένες Πολιτείες*». (Landau, 2013, σ. 70)

Αυτή η έντονη αντίδραση των Ευρωπαίων συμμάχων μπορεί να δικαιολογηθεί, καθώς, σε αντίθεση με τις ΗΠΑ, υπάρχει σαφώς καθορισμένο πλαίσιο από το Ευρωπαϊκό Δικαστήριο των Ανθρωπίνων Δικαιωμάτων σχετικά με το δικαίωμα της ελευθερίας και της ασφάλειας για κάθε άτομο ανεξαρτήτως χώρας προέλευσης πολιτικών δικαιωμάτων ˙ η Ευρωπαϊκή Ένωση θεωρεί πως η διεύθυνση IP συγκαταλέγεται στην προστασία των προσωπικών δεδομένων – συμπεριλαμβανομένων και των διασυνοριακών ροών - ενώ στην Αμερικανική νομοθεσία δεν υφίσταται. (Landau, 2013, σ. 70)

Θα ήταν καλό να αναγνωριστεί πως προκαλούν ζημιά στην παγκόσμια ασφάλεια οι αποκαλύψεις που έγιναν όχι μόνο από τον Snowden αλλά και από τη Wikileaks. Η Wikileaks το Νοέμβριο του 2010 δημοσιοποίησε περισσότερα από 250.000 αμερικανικές διπλωματικές αναφορές, εκθέτοντας ένα ευρύ φάσμα τρεχόντων διεθνών θεμάτων, σε συνεργασία με αναγνωρισμένες εφημερίδες. Οι εφημερίδες από την πλευρά τους, μπορεί μεν να έχουν επεξεργαστεί κατάλληλα τις ιστορίες ώστε να αποκρύψουν εμφανείς κινδύνους, αλλά δεν συνειδητοποιούν που βρίσκονται οι πραγματικά ευαίσθητες πληροφορίες, επιτρέποντας σε τρομοκράτες και εγκληματίες να αλλάξουν τη συμπεριφορά τους, θέτοντας σε κίνδυνο τη σχέση με εταιρείες που δραστηριοποιούνται στο χώρο του διαδικτύου, καθιστώντας ακόμα πιο δύσκολη τη συλλογή στοχευόμενων πληροφοριών σχετικά με σημαντικούς υπόπτους. (Omand, 2014, pp. 804-806)

Κεφάλαιο 4

4.1 Εφαρμογή οικονομικής κατασκοπείας σε εχθρούς και σε συμμάχους

Η οικονομία, τα χρηματοοικονομικά, το εμπόριο, η βιομηχανία, η τεχνολογία αιχμής, είναι οι τομείς που μετατρέπονται σε χώρους μάχης τόσο μεταξύ φίλων όσο εχθρών. Ήδη από το 1989 οι απαιτήσεις της εθνικής ασφάλειας έχουν γίνει «*πλαστικά άμορφες και ασαφείς. Ο καθένας είναι εν δυνάμει ανταγωνιστής των υπολοίπων και σε αυτό το βαθμό δυνάμει στόχος των υπηρεσιών πληροφοριών. Ο ανταγωνισμός είναι συνεταιριστικός και η συνεργασία ανταγωνιστική*» ˙ με αυτό τον τρόπο ο Peter Schweizer στο "The Friendly Spies" αντιλαμβάνεται την οικονομική κατασκοπεία μεταξύ των υποτιθέμενων συνεργατών κρατών. Ακόμα και ανάμεσα σε υποτιθέμενα στενούς φίλους και παλιούς συμμάχους, πάντα υπάρχουν μυστικά και από τις δύο πλευρές. Αμφότερες οι πλευρές επιδιώκουν να αποκτήσουν πρόσβαση, ακόμα και εισχώρηση, και θα προσπαθήσουν να χρησιμοποιήσουν τους αξιωματικούς της υπηρεσίας πληροφοριών των συνεργατών, προκειμένου να μοιραστούν περισσότερες πληροφορίες σχετικά με τις υπηρεσίες και τους πολιτικούς αρχηγούς, από όσες οι αρχηγοί τους θα ήθελαν ή θα ενέκριναν. (Alexander, 2010, p. 7) (Easley, 2014, p. 151)

Η εμπιστοσύνη κάνει τις διεθνείς αλληλεπιδράσεις περισσότερο αποτελεσματικές και αποδοτικές με το να διατηρεί τις κοινές προσδοκίες καλής πίστης και αμοιβαιότητας. Περιλαμβάνει, επίσης, την παραμονή μέσα στα πλαίσια των κανόνων και των κανονισμών, παρά τις αλλαγές που τυχόν επέλθουν στην εσωτερική πολιτική και στη διεθνή κατάσταση. (Easley, 2014, σ. 143)

Λαμβάνοντας υπόψη το πόσο σημαντική είναι η εμπιστοσύνη στις διεθνείς σχέσεις και το ρόλο των υπηρεσιών πληροφοριών σχετικά με την προστασία των εθνικών συμφερόντων, οι πρόσφατες αποκαλύψεις σχετικά με τις δραστηριότητες της Εθνικής Υπηρεσίας Ασφάλειας των ΗΠΑ ταιριάζουν καλύτερα στο μοντέλο «επαληθεύσιμη εμπιστοσύνη» παρά στην παραβίαση της εμπιστοσύνης. (Easley, 2014)

Αυτό σημαίνει πως μια συμμαχία δεν συνεπάγεται τυφλή εμπιστοσύνη. Σύμφωνα με τον Le Goyet «*τα συμφέροντα σε μια συμμαχία σπάνια ταυτίζονται, καθώς κάθε έθνος επικεντρώνεται στην προάσπιση των δικών του συμφερόντων πάνω από αυτά των υπολοίπων*». (Alexander, 2010, p. 4)
Βάσει των παραπάνω, το φαινόμενο όπου κράτη κατασκοπεύουν φίλους τους, προκειμένου να επεκτείνουν τα δικά τους συμφέροντα δεν είναι καινούριο. Για αυτό, εξάλλου, δεν προκαλεί έκπληξη το γεγονός ότι η NSA παρακολουθούσε και συνέταξε τις ενημερώσεις σχετικά με τις παρακολουθήσεις ξένων αρχηγών κρατών (Easley, 2014, σ. 144). Άλλωστε, τις τελευταίες δύο δεκαετίες, Αμερικανοί και Ευρωπαίοι έχουν ενεργοποιήσει τις δράσεις οικονομικής κατασκοπείας εναντίον των φίλων τους, οι οποίες συχνά είναι επαναλαμβανόμενες. (Lefebvre, 2008, p. 601)

Όπως ο Seth Jones της RAND Corporation αναφέρει «*Το τέλος του Ψυχρού Πολέμου και η ανάδειξη των ΗΠΑ ως τη μοναδική παγκόσμια υπερδύναμη κατέστησε την Αμερική ως έναν ελκυστικό στόχο για τους κατασκόπους των υπόλοιπων κρατών, συμπεριλαμβανομένων ακόμα και των συμμαχικών. Οι συνεχείς καινοτομίες στις στρατιωτικές, οικονομικές και διπλής χρήσης τεχνολογίες από αμερικανικές εταιρείες έβαλαν σε πειρασμό τις άλλες χώρες να θέλουν να αποκτήσουν αυτές τις καινοτομίες μέσω τις κατασκοπείας*». Συνεπώς, δεν εκπλήσσει κανένα το γεγονός ότι εχθροί και φίλοι κατασκοπεύουν για πολύ καιρό τις Ηνωμένες Πολιτείες. Η κατασκοπεία εναντίον των ΗΠΑ δεν έχει μειωθεί ούτε από τότε που πραγματοποιήθηκαν οι τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001. Για την ακρίβεια, σύμφωνα με μια κυβερνητική αναφορά «*τα τελευταία χρόνια οι δραστηριότητες των ξένων υπηρεσιών πληροφοριών έχουν αυξηθεί σε ποικιλομορφία και πολυπλοκότητα».* Επιπλέον, τα κονδύλια που διατίθενται στους αξιωματούχους της αντικατασκοπείας μειώνονται για να καλυφθούν άλλα έξοδα που συνδέονται με τον πόλεμο ενάντια της τρομοκρατίας. (Lefebvre, 2008, σ. 613)

Οι διαρροές που έγιναν εξαιτίας του Snowden, αν και δεν κατέστρεψαν την εμπιστοσύνη των συμμάχων των ΗΠΑ, μακροπρόθεσμα δημιούργησαν σοβαρά διπλωματικά και οικονομικά κόστη. Επομένως, παρά τις αντιδράσεις των συμμαχικών κρατών για τις δραστηριότητες της NSA, τόσο για τη Γερμανία και τη Γαλλία όσο και τη Βραζιλία ή την Ιαπωνία, υπάρχουν καταγεγραμμένα περιστατικά κατασκοπείας. Η δε Γερμανία κατηγορήθηκε ότι συλλέγει δεδομένα επικοινωνιών και αναζήτησης στο ίντερνετ τόσο σε εγχώριο επίπεδο όσο και στο εξωτερικό. Επίσης, παρά την ιστορική ευαισθησία που έχει η Γερμανία για την παρακολούθηση των πολιτών της από κυβερνητικές οργανώσεις, είναι γνωστό πως η εθνική μυστική υπηρεσία μοιράζεται πληροφορίες με την NSA, στο πλαίσιο συνεργασίας συλλογής παγκόσμιων δεδομένων. Σε μια συνάντηση που ακολούθησε μετά το σκάνδαλο της NSA, κεκλεισμένων των θυρών, λέγεται πως Γερμανοί και Γάλλοι αξιωματούχοι επέκριναν το πρόγραμμα, όχι τόσο διότι δημιουργεί ρήγμα στις μεταξύ τους σχέσεις αλλά διότι δεν συμμετείχαν και εκείνοι. Επιπρόσθετα, υπάρχουν ενδείξεις πως οι συσχετισμοί με την Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ είχαν αρνητικές επιπτώσεις σε εταιρείες όπως οι Google, Facebook, Apple και μεγάλες εταιρείες κινητών και πιστωτικών καρτών, όπου αθροιστικά αυτές οι εταιρείες έχουν περισσότερα στοιχεία για τον μέσο πολίτη από ότι η ίδια η NSA. (Easley, 2014, σσ. 144-148)

Οι πολίτες γνωρίζουν πως οι κυβερνήσεις τους έχουν σε λειτουργία προγράμματα παρακολούθησης. Η δημόσια συγκατάθεση κάνει κατανοητή τη θυσία κάποιων όρων ιδιωτικότητας , επομένως, σχετικά με την κυβερνητική παρακολούθηση, συναρτήσει των απειλών για την ασφάλεια και της προσπάθειας των υπηρεσιών ασφαλείας για διαφύλαξη της ασφάλειας των πολιτών. Οι υπηρεσίες πληροφοριών έχουν πολλά αμοιβαία συμφέροντα. Συνεπώς, είναι πολλά αυτά που μπορούν να κερδηθούν μέσω της συνεργασίας των κρατών, με τις πιθανότητες επιτυχίας να είναι περισσότερες, σε πολλούς τομείς, όπως για παράδειγμα εναντίον της τρομοκρατίας. Αυτό που χρειάζεται να μελετηθεί, όμως, είναι το πώς και το πόσο

θα κατασκοπεύει ένα κράτος τους φίλους τους και αντίστοιχα πώς και πόσο θα αντιδράσει αυτό το κράτος όταν οι φίλοι του κατασκοπεύσουν το ίδιο. (Alexander, 2010)

4.2 Η περίπτωση της Ρωσίας

Η εισβολή της Γερμανίας στη Σοβιετική Ένωση και η Ιαπωνική επίθεση στο Pearl Harbor ήταν δύο γεγονότα που κατάφεραν να κάνουν τις ΗΠΑ και τη Ρωσία να παραμερίσουν τις ιδεολογικές τους διαφορές και να συμμαχήσουν ενάντια στο φασισμό που επέβαλε η Ναζιστική Γερμανία. Η συμμαχία των ΗΠΑ και της Ρωσίας έληξε μαζί με το τέλος του Β' Παγκοσμίου Πολέμου το 1945, όπου και ξεκίνησε ο Ψυχρός Πόλεμος μεταξύ των δύο τότε στρατηγικών συμμάχων · ονομάστηκε έτσι καθώς ήταν περισσότερο ιδεολογικός πόλεμος παρά μια συμβατική στρατιωτική διαμάχη, μιας και αντιμαχόταν η καπιταλιστική οικονομία και πολιτική δημοκρατία των ΗΠΑ με την κεντρική οικονομία και το κομμουνιστικό πολιτικό σύστημα της Σοβιετικής Ένωσης. Αμφότερες ήθελαν να πείσουν τόσο τους πολίτες τους όσο και τον υπόλοιπο κόσμο να ακολουθήσουν το κυβερνητικό μοντέλο που είχε υιοθετήσει και αντιπροσώπευε η καθεμιά χώρα. Η διαμάχη αυτή έγινε πιο έντονη από το 1949 και έπειτα, όπου η Ρωσία ακολούθησε το παράδειγμα των ΗΠΑ, διότι έγινε η δεύτερη χώρα που είχε στην κατοχή της πυρηνικά όπλα. Επομένως, ο κόσμος ήταν όμηρος των δυο υπερδυνάμεων και της παράνοιας που επικρατούσε μέχρι το 1991, διότι και οι δύο χρησιμοποιούσαν ως απειλή τη χρήση των πυρηνικών τους όπλων για τον έλεγχο της παγκόσμιας πολιτικής σκηνής.

Ως συνέπεια της καχυποψίας που χαρακτήριζε τον Ψυχρό Πόλεμο ήταν η αυξημένη χρήση της κατασκοπείας μεταξύ των δυο χωρών. Οι τεχνικές συγκέντρωσης πληροφοριών αναπτύχθηκαν κυρίως την περίοδο του Β' Παγκοσμίου Πολέμου, όπου και οι μυστικές πληροφορίες μπορούσαν -και πράγματι το έκαναν- να καθορίσουν την έκβαση του πολέμου. Κατά τη διάρκεια του Ψυχρού Πολέμου η κατασκοπεία της Σοβιετικής Ένωσης στις ΗΠΑ επικεντρωνόταν στην απόκτηση τεχνολογικών πληροφοριών ούτως ώστε να ξεπεράσουν την Αμερικάνική τεχνολογική υπεροχή. Ένα μεγάλο μέρος αυτών των επιχειρήσεων από την πλευρά των Σοβιετικών ήταν η απόπειρα, μέσω κατασκοπείας, να μάθουν τα μυστικά των Αμερικανών σχετικά με την πυρηνική ενέργεια προκειμένου να φτάσουν τις πυρηνικές δυνατότητες αυτών · οι προσπάθειες αυτές ήταν επιτυχείς καθώς το 1949 οι Σοβιετικοί κατάφεραν να φτάσουν στην ανάπτυξη πυρηνικών όπλων.

Το 1950 γίνεται η πρώτη σύλληψη Ρώσου κατασκόπου σε αμερικανικό έδαφος. Η υπόθεση Rosenberg σχετίζεται με την απόκτηση αμερικανικών τεχνολογιών σχετικές με τα πυρηνικά από τους Ρώσους. Η δίκη και η εκτέλεση λόγω προδοσίας των Rosenberg προκάλεσαν ξέσπασμα της κοινή γνώμης, επειδή έλαβαν αυτή την πράξη ως αντικομουνιστική πολιτική της Αμερικανικής κυβέρνησης (Encyclopedia.com). Αυτές οι απόψεις υποστηρίζονταν και από το γεγονός ότι, φαινομενικά, η υπόθεση πλαισιώθηκε από ελλιπή στοιχεία · στην πραγματικότητα όμως η κυβέρνηση είχε πληθώρα στοιχείων αλλά αδυνατούσε να τα προσκομίσει στο δικαστήριο καθώς διακυβευόταν η μυστικότητα των επιχειρήσεων αντικατασκοπείας (υπόθεση

Venona). Επομένως, αν τα στοιχεία ήταν γνωστά στο ευρύ κοινό η γνώμη που θα διαμόρφωνε θα ήταν αρκετά διαφορετική.

Οι κατάσκοποι εκείνης της δεκαετίας υποκινούνταν από τον ιδεολογικό παράγοντα, τον κομμουνισμό, θεωρώντας τον Στάλιν ως υπέροχο αρχηγό και τη Σοβιετική Ένωση ως την ιδανική χώρα και πως οι ΗΠΑ δεν έπρεπε να έχουν το μονοπώλιο στα μυστικά που σχετίζονται με την πυρηνική ενέργεια. Ο θάνατος όμως του Στάλιν το 1953 άλλαξε ριζικά το τοπίο στην κατασκοπεία, κυρίως εξαιτίας των εγκλημάτων που διαπράχθηκαν υπό τις εντολές του εναντίον ανθρώπων στη Σοβιετική Ένωση, διαψεύδοντας ουσιαστικά τη φράση που είχε πει «*δεν υπάρχει φόνος στον παράδεισο*».

Από τη δεκαετία του 1970 και μέχρι τις δεκαετίες του 1980 και 1990, οι Σοβιετικοί κατάσκοποι δρούσαν με κύριο γνώμονα τις χρηματικές απολαβές. Οι ανησυχίες, και για τις δύο χώρες, σχετικά με την εθνική ασφάλεια άλλαξαν μετά τον Ψυχρό Πόλεμο. Η Ρωσία μετά την κατάρρευση της Σοβιετικής Ένωσης έχει επικεντρωθεί στα εσωτερικά της προβλήματα. Όσον αφορά το πολιτικό της σύστημα υποφέρει από την κομμουνιστική κληρονομιά με την εκτεταμένη γραφειοκρατία του κομμουνισμού και την έλλειψη εμπιστοσύνης των πολιτών προς τις εκλογικές διαδικασίες. Σχετικά με την οικονομία, η ανάκαμψη είναι δύσκολη, καθώς δεν μπορεί να υποστηρίξει τους δημόσιους λειτουργούς της και το φορολογικό σύστημα είναι ακανθώδες. Επίσης, μεγάλο πρόβλημα για τη Ρωσία αποτελεί το ζήτημα της Τσετσενίας -μια ισλαμική δημοκρατία η οποία επιθυμεί την ανεξαρτητοποίησή της από το 1994- και των Τσετσένων τρομοκρατών, αλλά και η πιθανότητα εξάπλωσης της επαναστατικής διάθεσης των υπόλοιπων ισλαμικών κρατών, με τα οποία συνορεύει η Ρωσία. Οι υπηρεσίες κατασκοπείας της Ρωσίας είναι πλέον προσανατολισμένες σε αυτή την κατεύθυνση, παρά στις ΗΠΑ. Παρόλα αυτά, η κύρια ανησυχία της σχετίζεται με την επέκταση της Βορειοατλαντικής Συμμαχίας (ΝΑΤΟ), καθώς η τελευταία προσπαθεί να απορροφήσει χώρες που ανήκαν στη σφαίρα επιρροής της Σοβιετικής Ένωσης. Η ρωσική κατασκοπεία στρέφεται στην επέκταση που διενεργεί το ΝΑΤΟ προς τα σύνορά της.

Οι ΗΠΑ από την πλευρά τους ομοίως δεν είναι προσανατολισμένες στη Ρωσία, χωρίς να παύουν να τη θεωρούν απειλή. Με την κατάρρευση του διπολικού συστήματος Δύση-Ανατολή οι απειλές προς τις ΗΠΑ πολλαπλασιάστηκαν. Όπως έγινε εμφανές και από τον Πόλεμο του Κόλπου τον Απρίλιο 1990, οι Ηνωμένες Πολιτείες ανησυχούν για τις δραστηριότητες επιθετικών κρατών, όπως το Ιράκ, τα οποία διοικούνται από δικτατορικές ή εξτρεμιστικές ιδεολογίες, έχοντας στη διάθεσή τους μια σειρά από βιολογικά και χημικά όπλα και γίνεται γνωστό πως αυτά τα κράτη χορηγούν τρομοκράτες προκειμένου να πετύχουν πολιτικούς σκοπούς. Αυτά τα κράτη καλλιεργούν το μίσος προς την Αμερική –όχι όμως από τη σκοπιά της καπιταλιστικής ιδεολογίας, αλλά πραγματικά ενάντια στην Αμερική ως χώρα- σε τέτοιο βαθμό που η Ρωσία δεν είχε κάνει ποτέ. Οι μυστικές υπηρεσίες των ΗΠΑ στρέφουν το ενδιαφέρον τους κυρίως προς αυτά τα κράτη, έχοντας ως σκοπό τη διασφάλιση της ασφάλειας από μη προβλέψιμες επιθετικές πράξεις από αυτά.

Οι ΗΠΑ μη έχοντας εγκαταλείψει τελείως το ενδιαφέρον τους για τη Ρωσία, ανησυχούν ιδιαίτερα για τις ελλιπώς φυλασσόμενες τοποθεσίες των όπλων μαζικής καταστροφής και την πολιτική αστάθεια που επικρατεί στις δημοκρατίες των χωρών της πρώην Σοβιετικής Ένωσης. Η Ρωσία ούσα θορυβημένη από την αδυναμία και την έλλειψη ελέγχου αυτής της κατάστασης προσπαθεί να διαβεβαιώσει τόσο τις ΗΠΑ όσο και τον υπόλοιπο κόσμο πως τα πυρηνικά της όπλα φυλάγονται με ασφάλεια. Η Ρωσία παραμένει σημαντική για τις ΗΠΑ εξαιτίας της γεωπολιτικής θέσης-κλειδί που έχει ˙ η εγγύτητα που έχει σε Ευρώπη, Ασία και Μέση Ανατολή καθιστά τη Ρωσία ένα σημαντικό παράγοντα και παίκτη σε αυτές τις περιοχές και οι ΗΠΑ αντιλαμβάνονται τον κίνδυνο της υποτίμησης της θέσης της Ρωσίας. Η κατασκοπεία στη Ρωσία μπορεί να βοηθήσει την Αμερική στην επίτευξη των γεωπολιτικών στρατηγικών της στις γείτονες περιοχές (Encyclopedia.com).

Το σημείο όπου οι ΗΠΑ υποτίμησαν τη Ρωσία είναι στον τομέα της κυβερνοκατασκοπείας και των κυβερνοεπιθέσεων. Ως συνέπεια και αποκορύφωμα αυτής της πράξης αποτελεί η διείσδυση των τελευταίων το 2016 τόσο σε ηλεκτρονικούς λογαριασμούς ανώτατων αξιωματούχων τις κυβέρνησης των ΗΠΑ όσο και στο ίδιο το σύστημα αποτελεσμάτων των ψήφων, κατά τη διάρκεια των εκλογών. Αυτό το χαμηλού κόστους αλλά μεγάλου αντίκτυπου όπλο η Ρωσία το δοκίμασε αρχικά στις εκλογές στην Ουκρανία και το εφάρμοσε στις Ηνωμένες Πολιτείες, με καταστροφική αποτελεσματικότητα.

Για δύο δεκαετίες οι ΗΠΑ προειδοποιούνταν για την προσπάθεια των μυστικών υπηρεσιών την Ρωσίας να εισβάλουν στα πιο ευαίσθητα υπολογιστικά δίκτυα της Αμερικής. Για χρόνια, οι Ρώσοι παρέμεναν εκτός του πεδίου ενδιαφέροντος των Ηνωμένων Πολιτειών σε αυτόν τον τομέα, χάρη στους Κινέζους, οι οποίοι έπαιρναν μεγαλύτερο ρίσκο και συχνά ανακαλύπτονταν. Εν αντιθέσει οι Ρώσοι πάντα κατάφερναν να βρίσκονται ένα βήμα πιο μπροστά και να μη γίνονται αντιληπτοί – κατάφεραν να υποκλέψουν τα σχέδια των μαχητικών αεροσκαφών F-35, εμπορικά μυστικά για τις λαμαρίνες θερμής έλασης, ακόμα και σχέδια για τους αγωγούς αερίου που θα εφοδιάζουν τις ΗΠΑ (Eric Lipton, Dec.13 2016)

4.3 Η περίπτωση της Κίνας

Τις τελευταίες δεκαετίες η διασύνδεση στον κυβερνοχώρο και η οικονομική ολοκλήρωση έχουν μετατρέψει την παγκόσμια αγορά σε μια αρένα όπου κρατικοί φορείς και μη μπορούν να χρησιμοποιήσουν τα μέσα της πληροφορικής προκειμένου να διεξάγουν οικονομική κατασκοπεία και να προωθήσουν τους στρατηγικούς τους στόχους. Έχουν παρατηρηθεί περιπτώσεις στις οποίες ιδιωτικές ή κρατικές επιχειρήσεις λειτουργούν ως Δούρειοι Ίπποι, οι οποίοι διεξάγουν κατασκοπεία στον οικονομικό τομέα με σκοπό να αποκομίσουν νέες τεχνολογίες, τις οποίες δεν θα μπορούσαν να αποκτήσουν με άλλο τρόπο. Το φαινόμενο της κυβερνοκατασκοπείας στον οικονομικό τομέα λαμβάνεται ως αδιαμφισβήτητη απειλή για την εθνική ασφάλεια των κρατών. Όλες οι χώρες σήμερα διεξάγουν ως κάποιο βαθμό οικονομική κατασκοπεία, αλλά με το παραπάνω παράδειγμα έχει ως κύριο αποδέκτη την Κίνα, από την πλευρά των ΗΠΑ.

Η Κίνα κυριαρχούσε στην περιοχή της Ασίας – Ειρηνικού από το 500 μέχρι το 1500 · προσπάθησε να είναι αυτάρκης και απομονωμένη από τον κόσμο αλλά απέτυχε από το 1960 έως το 1978. Με την είσοδό της στην παγκόσμια σκηνή από τη δεκαετία του 1990 ως «οικονομικός γίγαντας» αναζητά όχι μόνο να αποκαταστήσει την δύναμη και την επιρροή που είχε στην περιοχή –Ταϊβάν, Θιβέτ και Νότια Θάλασσα της Κίνας- αλλά να περιορίσει την επιρροή των ΗΠΑ σε αυτή την περιοχή (Broomfield, 2013, pp. 265-267)

Η Κίνα προκαλεί ζημιά στην οικονομία και την ασφάλεια των ΗΠΑ μέσω δύο πολιτικών. Πρώτον, μέσω συντονισμένης και υποστηριζόμενης –από την κυβέρνηση- κλοπή πληροφοριών από διάφορες εμπορικές επιχειρήσεις που έχουν ως έδρα τις ΗΠΑ και δεύτερον μέσω επιβολής περιορισμών όσον αφορά το περιεχόμενο, τα πρότυπα και τις εμπορικές ευκαιρίες για τις αμερικανικές επιχειρήσεις. Οι χάκερς που εργάζονται για την Κινεζική κυβέρνηση –ή υποστηρίζονται και ενθαρρύνονται από αυτή- διεισδύουν στα δίκτυα ηλεκτρονικών υπολογιστών αμερικανικών υπηρεσιών και εταιρειών, κλέβοντας εμπορικά μυστικά, συμπεριλαμβανομένων του υλικού που κατοχυρώνεται με το δίπλωμα ευρεσιτεχνίας, διαδικασίες κατασκευής και άλλες πληροφορίες. Η κινεζική κυβέρνηση παρέχει αυτές τις πληροφορίες σε κινεζικές εταιρείες και κρατικές επιχειρήσεις (Section 4: Commercial Cyber Espionage And Barriers to Digital Trade in China)(p.192).

Επιπρόσθετα, η κινεζική κυβέρνηση επιβάλλει ιδιαίτερα έντονη λογοκρισία στο περιεχόμενο του Ίντερνετ και των δικτύων κοινωνικής δικτύωσης, κάτι που οδηγεί τις αμερικανικές επιχειρήσεις να είναι απρόθυμες να ακολουθήσουν τακτικές δικτατορικού τύπου.

Η Κίνα από την πλευρά της συνήθως αρνείται κάθε επίσημη ανάμειξη σχετικά με κυβερνοκατασκοπεία εναντίον της κυβέρνησης των ΗΠΑ ή αμερικανικών εμπορικών δικτύων · προσθέτει πως τέτοιου είδους κατηγορίες είναι «*αβάσιμες, ανεύθυνες και μη αποδεδειγμένες*» και επιλέγει να κατηγορήσει τις Ηνωμένες Πολιτείες για κυβερνοκατασκοπεία (Section 4: Commercial Cyber Espionage And Barriers to Digital Trade in China)(p.197). Αμερικανικές εταιρείες οι οποίες ειδικεύονται στην διερεύνηση κυβερνοεπιθέσεων και κατασκοπείας

ανίχνευσαν πολλές εισβολές από σέρβερ και χάκερ που βρίσκονται στην Κίνα. Μάλιστα, η εταιρεία ασφάλειας Ίντερνετ Mandiant ανέφερε πως οι εκατοντάδες διερευνήσεις που έκανε έδειξαν πως οι εισβολές που σημειώθηκαν σε αμερικανικές εφημερίδες, κυβερνητικές υπηρεσίες και εταιρείες «*έχουν την έδρα κυρίως στην Κίνα και η κινεζική κυβέρνηση είναι ενήμερη σχετικά με αυτές*».

Σε συνέχεια αυτών των περιστατικών, στις 19 Μαΐου 2014 το Υπουργείο Δικαιοσύνης των ΗΠΑ ανακοίνωσε τις κατηγορίες σε ένα περιφερειακό δικαστήριο των ΗΠΑ εις βάρος πέντε Κινέζων στρατιωτικών για βιομηχανική κατασκοπεία με βάση τις οικείες τους στην Κίνα (China's Cyberespionage: The National Security Distinction and US Diplomacy). Αναγγέλλοντας τα κατηγορίες ο Γενικός Εισαγγελέας Eric Holder σημείωσε πως πρόκειται για την «*πρώτη φορά που απαγγέλλονται κατηγορίες σε μια χώρα για αυτού του είδους την πειρατεία*». Επίσης, ανέφερε πως η Κίνα αναλαμβάνει ως κρατική πολιτική την κλοπή βιομηχανικών πληροφοριών προκειμένου να ενισχύσει τις κινεζικές εταιρείες –οι εταιρείες που ήταν θύματα δραστηριοποιούνταν στους τομείς της ηλιακής και πυρηνικής ενέργειας, του αλουμινίου και του χάλυβα-, υπονοώντας πως δεν ενείχε σκοπός εθνικής ασφάλειας.

Η Κίνα αντέδρασε εντόνως για αυτές τις κατηγορίες σημειώνοντας πως ήταν μια πρακτική στη διεθνή διπλωματία άνευ προηγουμένου και λειτουργεί ως ανασταλτικός παράγοντας στο διάλογο σχετικά με το διαδίκτυο. Κινέζοι αξιωματούχοι δηλώνουν πως οι ΗΠΑ ασκούσαν επί μακρόν απομακρυσμένη παρακολούθηση στην Κίνα μέσω μυριάδων ηλεκτρονικών μέσων και πως από τον Ιούνιο 2013 παγκοσμίου εμβέλειας εφημερίδες είχαν ως θέμα τις εκθέσεις κυβερνητικής κατασκοπείας που ασκούσαν οι ΗΠΑ τόσο στην Κίνα όσο και σε άλλες χώρες.

Παρατηρείται, επομένως, ένας κύκλος κατηγοριών, όπου αμφότερες Κίνα και Ηνωμένες Πολιτείες θεωρούν την άλλη πλευρά απειλή. Θα έλεγε κανείς πως είναι ένα απτό παράδειγμα του Ρεαλισμού και κυρίως του διλήμματος ασφάλειας, σύμφωνα με τον οποίο μια χώρα αυξάνει τις προσπάθειες και τα μέσα προστασίας της όταν διαπιστώνει πως μια άλλη χώρα, εξίσου δυνατή, αυξάνει τα εφόδιά της.

Το 2011 το Υπουργείο Άμυνας των ΗΠΑ δημοσίευσε μια θεωρία όπου εξισώνει τις πιο καταστροφικές κυβερνοεπιθέσεις –κυρίως αυτές που έχουν ως στόχο δημόσιες υποδομές- ως μια πράξη πολέμου.

Στον απόηχο αυτών των περιστατικών, οι πρόεδροι Αμερικής και Κίνα, Barack Obama και Xi Jinping, στις 24 – 25 Σεπτεμβρίου 2015 συναντήθηκαν προκειμένου να συνάψουν συμφωνία σχετικά με την κυβερνοκατασκοπεία. Ο Πρόεδρος Xi στην άφιξή του συναντήθηκε με τους επικεφαλής των τεχνολογικών κολοσσών στο Seattle πριν τη συνάντησή του στην Washington.

Ο Πρόεδρος Obama τόνισε τις ανησυχίες του σχετικά με τις αυξανόμενες κυβερνοαπειλές ενάντια σε αμερικανικές εταιρείες και τους αμερικανούς πολίτες και διευκρίνισε πως αμφότερες, ΗΠΑ και Κίνα, κίνουνται προς την ίδια κατεύθυνση απέναντι στην κυβερνοκατασκοπεία (Kelly & Foran, 2015) .

Οι δύο χώρες συμφώνησαν πως πρέπει να παρέχονται έγκαιρες απαντήσεις σε δραστηριότητες σχετικές με την κακόβουλη χρήση του διαδικτύου. Συμφώνησαν να συνεργάζονται με τρόπο συμβατό προς τις εθνικές τους νομοθεσίες και διεθνείς υποχρεώσεις για τη διερεύνηση εγκλημάτων στον κυβερνοχώρο, τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων και την άμβλυνση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο που προέρχονται από την επικράτειά τους (Secretary, 2015).

Οι Ηνωμένες Πολιτείες και η Κίνα συμφωνούν ότι καμία από τις κυβερνήσεις της χώρας δεν θα διεξαγάγει ή δεν υποστηρίζει συνειδητά την κλοπή πνευματικής ιδιοκτησίας - συμπεριλαμβανομένων εμπορικών μυστικών ή άλλων εμπιστευτικών επιχειρηματικών πληροφοριών- με σκοπό την παροχή ανταγωνιστικών πλεονεκτημάτων σε εταιρείες ή εμπορικούς τομείς.

Επιπρόσθετα και οι δύο πλευρές δεσμεύονται να καταβάλουν κοινή προσπάθεια για τον περαιτέρω εντοπισμό και την προώθηση κατάλληλων κανόνων κρατικής συμπεριφοράς στον κυβερνοχώρο εντός της διεθνούς κοινότητας., συμφωνώντας στη δημιουργία ομάδας εμπειρογνωμόνων υψηλού επιπέδου για περαιτέρω συζητήσεις επί του θέματος. Ακόμα, συμφωνούν με την έκθεση του ομίλου κυβερνητικών εμπειρογνωμόνων του ΟΗΕ στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας, η οποία εξετάζει τους κανόνες συμπεριφοράς και άλλα κρίσιμα ζητήματα για τη διεθνή ασφάλεια στον κυβερνοχώρο.

Τέλος, συμφώνησαν για τη δημιουργία ενός μηχανισμού, ο οποίος θα είναι υπεύθυνος για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο.

Αυτή η συνεργασία των Ηνωμένων Πολιτειών με την Κίνα δείχνει πως, παρόλο την ύπαρξη στρατηγικού ανταγωνισμού, δεν εμποδίζεται η δημιουργία συνεργασίας ˙ παρά τις υπάρχουσες διαφορές, συνεχίζουν να υπάρχουν κοινά συμφέροντα (Lewis, 2015) .

Κεφάλαιο 5

5.1 Η γεωπολιτική και γεωστρατηγική σημασία της οικονομικής κατασκοπείας

Με τον όρο «γεωοικονομία» προσδιορίζουμε εκείνο το κομμάτι της επιστήμης, το οποίο μελετά τα γεωοικονομικά δεδομένα μιας γεωγραφικής περιοχής, τα οποία σχετίζονται με τις οικονομικές δραστηριότητες ως προς το γεωγραφικό περιβάλλον με σκοπό την αξιοποίησή τους. Μεταξύ άλλων, η γεωοικονομία μελετά το ρόλο της οικονομικής αλληλεξάρτησης για την επίλυση ή πρόληψη συγκρούσεων, τα όρια της οικονομίας στην επίλυση ή πρόληψη συγκρούσεων, τη σχέση μεταξύ της οικονομικής ανάπτυξης και των πολιτικών και κοινωνικών συνθηκών στις διάφορες χώρες (Πλατιάς, pp. 591-619)

Μετά το τέλος του Ψυχρού Πολέμου, στην κοινότητα των διεθνών σχέσεων κυριαρχούσε η αισιοδοξία καθώς η περίοδος των μεγάλων γεωπολιτικών ανταγωνισμών είχε παρέλθει (Πλατιάς, σ. 591). Παρ' όλα αυτά, η λογική των διεθνών σχέσεων εξακολουθεί να είναι η ίδια. Οι διεθνείς σχέσεις ήταν και είναι κατά βάση συγκρουσιακές και ανταγωνιστικές. Αν αλλάζει κάτι κατά περιόδους και εποχές είναι οι όροι με τους οποίους διεξάγεται ο ανταγωνισμός. Η γεωπολιτική και η γεωοικονομία αποτελούν διαφορετικές όψεις του ίδιου νομίσματος (Πλατιάς, σσ. 591-592).

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, Ρωσία και Κίνα προσπαθούν να κερδίσουν την αίγλη και την επιρροή που είχαν στην περιοχή, δεδομένου ότι στην εποχή που διανύουμε η ισχύς μετριέται από τον οικονομικό παράγοντα και τα τεχνολογικά επιτεύγματα που έχει στην κατοχή της η κάθε χώρα. Επομένως, αν και φαινομενικά κάποιες χώρες θεωρούνται σύμμαχοι, επί της ουσίας ενδιαφέρονται για τα σχετικά κέρδη και χρησιμοποιούν, ει δυνατόν, όχι μόνο την τεχνολογική τους ανάπτυξη για την οικονομική άνθηση, αλλά και την γεωπολιτική τους θέση.

Το εμπόριο και τα χρηματοοικονομικά καθορίζουν σε μεγάλο βαθμό την εξωτερική πολιτική (Szabo, 2014, p. 119). Οι γεωπολιτικές δυνάμεις καθορίζουν τα εθνικά συμφέροντα με οικονομικούς όρους και χρησιμοποιούν την οικονομική επιρροή τους ως το πρωταρχικό μέσο επιβολής των εθνικών προτιμήσεων σε άλλα κράτη. Η Γερμανία αποτελεί μια οικονομική δύναμη, από τότε που η Δυτική Γερμανία αναδύθηκε από το Β΄ Παγκόσμιο Πόλεμο ˙ έκτοτε είναι ένα πρωτότυπο παράδειγμα γεωπολιτικής δύναμης που δοκιμάζει την παλιού τύπου βασισμένη σε στρατό δύναμη, η οποία ενσαρκώνεται από τις ΗΠΑ και τη Ρωσία, και έχει καταφέρει να γίνει ένας παίκτης-κλειδί, όχι μόνο στην Ευρωπαϊκή ήπειρο, αλλά γενικότερα στη διαμόρφωση της Δυτικής πολιτικής απέναντι στη Ρωσία.

Οι σχέσεις μεταξύ Ρωσίας – Γερμανίας βασίζονται στο 90% στην οικονομία και οδηγούνται από το ρόλο της Γερμανίας ως ένας από τους κορυφαίους εξαγωγείς στον κόσμο ˙ παρόλα

αυτά εξαρτάται σε μεγάλο βαθμό από φυσικούς πόρους, κυρίως ενέργεια, προκειμένου να λειτουργήσει η βασισμένη στη βιομηχανία οικονομία της. Η σχέση Ρωσία – Γερμανίας έχει επιπτώσεις όχι μόνο σε ευρωπαϊκό επίπεδο αλλά και στη διεθνή πολιτική γενικά.

Τα στοιχεία που προκύπτουν από μια έρευνα που έγινε δείχνουν πως το Βερολίνο, περισσότερο από κάθε άλλη ευρωπαϊκή πρωτεύουσα, έχει πιο εκτεταμένους οικονομικούς και εμπορικούς δεσμούς με τη Μόσχα απ' ότι η Ουάσινγκτον. Όσον αφορά τον τομέα της ενέργειας, η Γερμανία λαμβάνει περισσότερο από το 1/3 που χρειάζεται σε αέριο και πετρέλαιο από τη Ρωσία ˙ κάτι που πιθανότατα να αυξηθεί, βασιζόμενοι στην πρόθεση της καγκελαρίου Μέρκελ να απομακρυνθεί από την πυρηνική ενέργεια και να στραφεί στις ανανεώσιμες πηγές ενέργειας. Ωστόσο, η εξάρτηση της Γερμανίας για εισαγωγές φυσικών πόρων από χώρες με αυταρχικά καθεστώτα και διεφθαρμένες κυβερνήσεις αποτελούν πραγματικό εμπόδιο στην προώθηση της δημοκρατικής αναδιαμόρφωσης και των ανθρώπινων δικαιωμάτων. Η Γερμανία οδηγείται από τα οικονομικά συμφέροντα που καθορίζουν τα εθνικά της. Αυτό έγινε εμφανές από το γεγονός ότι δεν είχε προβεί σε χρήση της οικονομικής της δύναμης απέναντι στη Ρωσία μέχρι το ξέσπασμα της κρίσης στην Ουκρανία ή και την κατάρριψη του αεροσκάφους των Μαλαισιανών Αερογραμμών MH17 . Ακόμα και μέσα από τα περιστατικά αυτά, μια διακοπή των σχέσεων με την Ρωσία θα λειτουργούσε αρνητικά για τη Γερμανία, όχι μόνο εξαιτίας της γεωγραφικής έκτασης της Ρωσίας αλλά και γιατί συνεχίζει να έχει σημαντικά εμπορικά ενδιαφέροντα μαζί της, δεδομένης της ενεργειακής εξάρτησης που θα συνεχίζει να έχει, καθώς οι πόροι που χρειάζεται δεν μπορούν να καλυφτούν ούτε από την Ευρώπη αλλά ούτε από την Αμερική.

Επίσης, η καγκελάριος Μέρκελ αντιμετωπίζει δυσκολίες και στο εσωτερικό της χώρας στο να υποστηρίξει τις ΗΠΑ, καθώς οι πολίτες, μετά τις αποκαλύψεις που έκανε ο πρώην πράκτορας της CIA Edward Snowden, έχουν χάσει την εμπιστοσύνη τους προς τις αμερικανικές πολιτικές και διάκεινται περισσότερο φιλικά προς τη Ρωσία. Περιστατικά σαν αυτά δημιουργούν εντάσεις στη σχέση μεταξύ της Αμερικής και της Ρωσίας.

Η Ρωσία στην προσπάθειά της να ανακτήσει την ισχύ και την επιρροή που είχε και ασκούσε σε Ευρωπαϊκές, πλέον, χώρες, επεκτείνει την γεωπολιτική της ατζέντα και εμπλουτίζει τα μέσα με τα οποία θα το καταφέρει. Τα μέσα που χρησιμοποιεί κυρίως είναι οι υπηρεσίες πληροφοριών της, με τις οποίες προσπαθεί να διεισδύσει και να διαμορφώσει τις πολιτικές άλλων κρατών. Ήδη από το 2010 η Βρετανική Υπηρεσία Πληροφοριών (MI5) είχε προειδοποιήσει πως «*η απειλή από τη Ρωσία συνεχίζει να είναι εξίσου σημαντική και παρόμοια αυτής που υπήρχε κατά τη διάρκεια του Ψυχρού Πολέμου*» (Galeotti, 2016, pp. 1-16).
Οι υπηρεσίες πληροφοριών ορισμένες φορές δρουν μέσω ή παράλληλα με άλλες συγκεκαλυμμένες υπηρεσίες, όπως είναι οι φιλανθρωπικές οργανώσεις ή χρηματοπιστωτικά ιδρύματα –όπως για παράδειγμα Ρώσικες τράπεζες που δάνεισαν εκατομμύρια ευρώ στο γαλλικό εθνικιστικό κόμμα της Marine Le Pen. Έκθεση που εκδόθηκε καλεί τις κυβερνήσεις της Ευρωπαϊκής Ένωσης να δείξουν μηδενική ανοχή στις επιχειρήσεις των ρωσικών μυστικών υπηρεσιών, μέσω της ενίσχυσης της ανταλλαγής πληροφοριών, της αντικατασκοπείας και του

εντοπισμού παράνομων κινήσεων που βρίσκονται πίσω από τέτοιες δραστηριότητες. Παραδείγματα άλλων χωρών, όπου έχει κατηγορηθεί η Ρωσία για παρέμβασή της προκειμένου να αξιοποιήσει τα εθνικά της συμφέροντα, είναι η Εσθονία, η Μολδαβία, η Λετονία και η Τσεχία.

Πολλές είναι οι φορές που ο Ρώσος Πρόεδρος έχει χαρακτηρίσει την κατάρρευση της Σοβιετικής Ένωσης ως τη «μεγαλύτερη γεωπολιτική καταστροφή του 20ου αιώνα» , καθώς η απώλεια της θέσης ως υπερδύναμης ικανής να αντισταθεί στις ΗΠΑ είναι ένα γεγονός που δύσκολα μπορεί να ξεπεραστεί. Η επιρροή που προσπαθεί να ασκήσει η Ρωσία σε συμμάχους και γείτονες χώρες των ΗΠΑ δεν είναι τακτική του αιώνα που διανύουμε. Αν και η Λατινική Αμερική δεν αποτελούσε στρατηγική προτεραιότητα για τη Ρωσία μέχρι το ξέσπασμα της Επανάστασης της Κούβας τον Ιανουάριο 1959, όπου και το εξέλαβε ως μια ευκαιρία επέκτασης της σφαίρας επιρροής της στο Δυτικό Ημισφαίριο, καθιστώντας ταυτόχρονα την Κούβα την πρώτη μη ευρωπαϊκή-ασιατική χώρα που ασπάστηκε την ιδεολογία του κομμουνισμού (Neeb, 2017). Αυτή η ευκαιρία έδωσε τη δυνατότητα στις ρωσικές υπηρεσίες πληροφοριών να εισχωρήσουν στην ευρύτερη περιοχή της Λατινικής Αμερικής.

Η παρουσία της Ρωσίας στην Αμερική έχει πολλές διαστάσεις αλλά ο σκοπός παραμένει ο ίδιος με αυτόν που επικρατούσε στον Ψυχρό Πόλεμο ˙ να διαρρυχθεί η επιρροή των Ηνωμένων Πολιτείων στην περιοχή. Συνεπώς η χρήση της κατασκοπείας και αντικασκοπείας της Ρωσίας στη Λατινική Αμερική αυξάνεται όλο και πιο επιθετικά. Μετά την επίθεση της 11ης Σεπτεμβρίου το ενδιαφέρον των ΗΠΑ προσανατολίστηκε στη Μέση Ανατολή. Με την έλλειψη προσοχής των ΗΠΑ στην περιοχή της Λατινικής Αμερικής η Ρωσία ήθελε να εφαρμόσει ένα σχέδιο απομόνωσης και αποξένωσης των ΗΠΑ από τις γειτονικές χώρες. Η αυξανόμενη, επομένως, δραστηριότητα της Ρωσίας στην περιοχή έχει τις εξής προτεραιότητες. Αρχικά στοχεύει στη συλλογή στρατηγικών πληροφοριών για τις ΗΠΑ και τους συμμάχους της. Δεύτερον, να στρατολογήσει εκούσια ή ακούσια συμμάχους και πράκτορες με επιρροή. Το σημαντικότερο όμως είναι ότι αποσκοπεί στη χρήση των χωρών την Λατινικής Αμερικής ως μέσο για να διεισδύσουν πράκτορες και να αποκτήσει πρόσβαση σε σημαντικές πληροφορίες μέσα στις Ηνωμένες Πολιτείες (Neeb, 2017).

Η ευρύτερη περιοχή, όμως, της Λατινικής Αμερικής δεν έχει δεχθεί το ενδιαφέρον μόνο της Ρωσίας. Ομοίως η Κίνα εξελίσσεται ως ένας σημαντικός οικονομικός δρων στην περιοχή, γεγονός που είναι εμφανές από τα ποσά που προκύπτουν από τις εμπορικές συναλλαγές μεταξύ Κίνας – Λατινικής Αμερικής. Αυτό εγείρει σημαντικές ερωτήσεις σχετικά με το είδος της επιρροής που έχει η Κίνα στην οικονομική και πολιτική ανάπτυξη της περιοχής και κατά πόσο αυτή η επιρροή σχετίζεται με στρατηγική από την Κίνα για να πετύχει να επηρεάσει πολιτικά τις χώρες της Λατινικής Αμερικής ούτως ώστε να προκαλέσει ή να μειώσει σημαντικά την ηγεμονία και επιρροή των ΗΠΑ στις χώρες αυτές (Piccone, 2016).

Η παγκοσμιοποίηση της οικονομίας είναι ουσιαστικά η βάση της εντυπωσιακής οικονομικής ανάπτυξης της Κίνας τα τελευταία 30 χρόνια καθιστώντας την παγκοσμίως τη δεύτερη μεγαλύτερη οικονομία. Η Κίνα έχοντας ως στόχο να επηρεάσει και να διαμορφώσει την

παγκόσμια γεωοικονομία και πολιτική, αναζητά να ξεπεράσει τις ΗΠΑ στοχεύοντας στον τομέα των επικοινωνιών και των τεχνολογιών των μυστικών υπηρεσιών και προσπαθεί να αυξήσει το επίπεδο της εμπορικής και διπλωματικής επιρροής της στην Ευρασία , ούτως ώστε να μειώσει αντίστοιχα την επιρροή των Ηνωμένων Πολιτειών από την Μέση Ανατολή εως τον Ειρηνικό.

Σε ηπειρωτικό επίπεδο δυο είναι οι μεγάλες δυνάμεις σε Ευρώπη και Ασία, η Κίνα και η Ρωσία, οι οποίες έχουν κοινά συμφέροντα στις περιοχές του Ειρηνικού και της Μέσης Ανατολής. Παρόλο που η Μόσχα δεν δείχνει να αποσκοπεί στη ρήξη της σχέσης μεταξύ Πεκίνο και Ουάσινγκτον, έχει υπόψιν της την αμφισβήτηση της Κίνας για την ηγεμονία των ΗΠΑ σε Ασία και Ειρηνικό και τον ανταγωνισμό που υπάρχει μεταξύ των δυο στην Λατική Αμερική και την Αφρική.

Η αυξανόμενη συνεργασία μεταξύ Ρωσίας και Κίνας στην στρατιωτική, διπλωματική και οικονομική σφαίρα θεωρείται ως ιδιαιτέρως μεγάλη απειλή για την εθνική ασφάλεια των ΗΠΑ (Lyle Goldstein, 2017) (Lewis, 2015), καθώς Κίνα και Ρωσία έχουν από τις πιο αναπτυγμένες δυνατότητες στον κυβερνοχώρο με τα υψηλότερη δυνατότητα σοβαρού αντικτύπου (Korolov, 2017).

Κεφάλαιο 6

6.1 Η οικονομική κατασκοπία υπό το πρίσμα του Risk Management

Είναι αποδεκτό πως πλέον ο οικονομικός ανταγωνισμός είναι παγκόσμιος. Οι εδαφικές και αποικιακές κατακτήσεις έχουν αντικατασταθεί από την κατάκτηση των αγορών και των τεχνολογιών (Economic Espionage). Η γνώση, λοιπόν, και η κατάκτηση των πληροφοριών, μπορεί να αποτελέσει σημαντική πηγή εξουσίας και για αυτό πρέπει να αξιοποιηθεί και να προστατευθεί. Αντίστοιχα σημαντικής σημασίας είναι και η κλοπή των πληροφοριών. Ο επαγγελματικός κόσμος έχει γίνει περισσότερο ευάλωτος από οποιαδήποτε άλλη εποχή στην εταιρική κατασκοπεία αφού τα συστήματα πληροφοριών αλλάζουν μορφή, η παραδοσιακή γραφειοκρατία με τον καιρό υποχωρεί και δίνει τη θέση της στα πληροφοριακά δίκτυα μέσω διαδικτύου. Στο παγκοσμιοποιημένο περιβάλλον του σήμερα, η γνώση και το τεχνολογικό πλεονέκτημα που αυτή παρέχει είναι εκτεθειμένα στην οποιαδήποτε απειλή. Αυτό πρέπει να το αντιληφθούν και οι εταιρείες, πως παράλληλα με τη μεταφορά των εμπορικών τους πληροφοριών στο διαδίκτυο, τα πληροφοριακά συστήματα που διαθέτουν, άρα και οι πληροφορίες τους, είναι εκτεθειμένα. Η σπουδαιότητα της επένδυσης σε έρευνα και ανάπτυξη πρέπει να εξισωθεί με τη σπουδαιότητα της προστασίας των πληροφοριών που αυτές συνεπάγονται.

Από αρχαιοτάτων χρόνων, οι εκάστοτε κυβερνήσεις προστάτευαν τις πληροφορίες εκείνες που θα τους έδιναν το πλεονέκτημα απέναντι στους αντιπάλους. Ο ρόλος των μυστικών πληροφοριών που λειτουργούν επικουρικά στην εξωτερική πολιτική των εθνών δεν είναι καινούριος. Στην αλλαγή του 20^{ου} αιώνα, τα επιστημονικά και τεχνολογικά επιτεύγματα στους τομείς της πυρηνικής φυσικής και της αεροδιαστημικής είχαν τρομερό αντίκτυπο στους τομείς της αναγνώρισης, παρακολούθησης και της ασφάλειας των πληροφοριών (Daniel Javorsek II, 2015). Επίσης, τα τεχνολογικά επιτεύγματα έχουν διαδραματίσει έναν όλο και αυξανόμενο σημαντικό ρόλο στην αλλαγή της λογικής σε στρατηγικό, επιχειρησιακό και τακτικό επίπεδο. Το τωρινό πεδίο μάχης είναι περισσότερο διασυνδεδεμένο δικτυακά από ότι στο παρελθόν. Τέτοια κρυπτογραφημένα συστήματα κρύβουν πληθώρα ευαίσθητων πληροφοριών, δημιουργώντας μια μοναδική πρόκληση σχετικά με τον τρόπο που θα μπορούσαν να προστατευθούν εμπορικές και εθνικές ευαίσθητες πληροφορίες μέσα στις πλατφόρμες και τις υπηρεσίες.

Παρακάτω γίνεται η απεικόνιση αξιολόγησης απειλών και κινδύνων με τις οποίες έρχονται αντιμέτωπες τόσο εταιρείες και βιομηχανίες όσο και τα ίδια τα κράτη. Η ανάλυση ρίσκου αποτελείται από δύο μέρη. Αρχικά πρέπει να γίνει ο εντοπισμός των βασικών χαρακτηριστικών και σε δεύτερο στάδιο να υπολογιστεί η πιθανότητα που η απειλή, καθώς και ο αντίκτυπος αυτής, θα πραγματοποιηθεί.

Βάσει της Εφημερίδας της Κυβέρνησης με αριθμό φύλλου 336 και ημερομηνία έκδοσης την 16η Μαρτίου 2005[1], οι πληροφορίες διαβαθμίζονται σε πέντε βασικές κατηγορίες:

1. ΕΤΝΑ Άκρως Απόρρητο (ΕΤΝΑ – ΑΑΠ)
2. Άκρως Απόρρητο (ΑΑΠ)
3. Απόρρητο (ΑΠ)
4. Εμπιστευτικό (ΕΜΠ ή ΕΠ)
5. Περιορισμένης Χρήσης (ΠΕΡ ή ΠΧ)
6. Αδιαβάθμητο (ΑΔ)

Στον Πίνακα 1 γίνεται απεικόνιση σχετικά με την πιθανότητα διαρροής ευαίσθητης πληροφορίας ή τεχνολογίας που διαθέτει ο στρατός και τον αντίστοιχο αντίκτυπο που αυτή θα είχε αναλόγως το επίπεδο ασφαλείας στο οποίο θα ήταν διαβαθμισμένη.

Πίνακας 1 Πιθανότητα διαρροής και επιπτώσεις

		Στρατιωτικές Επιπτώσεις				
		Αμελητέες	Ήπιες	Οριακές	Κρίσιμες	Καταστροφικές
Πιθανότητα	Υψηλή	ΑΔ	ΕΠ, ΠΧ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ
	Μεγάλη	ΑΔ	ΕΠ, ΠΧ	ΕΠ, ΠΧ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ
	Ενδεχόμενη	ΑΔ	ΕΠ, ΠΧ	ΕΠ, ΠΧ	ΕΠ, ΠΧ	ΕΤΝΑ – ΑΑΠ, ΑΑΠ
	Ελάχιστη	ΑΔ	ΑΔ	ΑΔ	ΕΠ, ΠΧ	ΕΠ, ΠΧ
	Μικρή	ΑΔ	ΑΔ	ΑΔ	ΕΠ, ΠΧ	ΕΠ, ΠΧ

Ο αντίκτυπος από τη διαρροή υλικού και πληροφορίας, με διαβάθμιση ΕΤΝΑ Άκρως Απόρρητο και Άκρως Απόρρητο, αναμένεται να προκαλέσει εξαιρετικά βαριές ζημιές στην Εθνική Άμυνα, την ασφάλεια και τα συμφέροντα της χώρας.

Ο χαρακτηρισμός «Απόρρητο» αποδίδεται στις πληροφορίες ή το υλικό που τυχόν διαρρεύσει είναι αυτός, διότι οι επιπτώσεις από τη διαρροή είναι δυνατό να προκαλέσουν ζημιές στην Εθνική Άμυνα, την ασφάλεια και τα ζωτικά συμφέροντα της χώρας.

Όσον αφορά τους βαθμούς «Εμπιστευτικό» και «Περιορισμένης Χρήσης» η επίπτωση διαρροής μειώνεται αλλά συνεχίζει να υφίσταται, καθώς η διαρροή αφορά εκείνο το υλικό και τις πληροφορίες με τις οποίες να επηρεαστεί δυσμενώς η Εθνική Άμυνα, η ασφάλεια και τα συμφέροντα της χώρας, σε μικρότερο ωστόσο βαθμό από αυτό που απεικονίζεται για τα επίπεδα ασφάλειας «ΕΤΝΑ Άκρως Απόρρητο» και «Απόρρητο».

[1] http://www.sekpy.gr/wp-content/uploads/2016/12/1_FEKB336.pdf

Διπλωματικές Επιπτώσεις						
Πιθανότητα		Αμελητέες	Ήπιες	Οριακές	Κρίσιμες	Καταστροφικές
	Υψηλή					
	Μεγάλη					
	Ενδεχόμενη					
	Ελάχιστη					
	Μικρή					

Επιπτώσεις						
Πιθανότητα		Αμελητέες	Ήπιες	Οριακές	Κρίσιμες	Καταστροφικές
	Υψηλή					
	Μεγάλη					
	Ενδεχόμενη					
	Ελάχιστη					
	Μικρή					

Εικόνα 1. Απεικόνιση αντίληψης επικινδυνότητας σε εταιρικό και διπλωματικό επίπεδο διαρροής πληροφοριών

Η διαρροή υλικού και πληροφοριών μπορεί να επηρεάσει εξίσου μια χώρα και σε διπλωματικό επίπεδο.

Οι επιπτώσεις ποικίλλουν ανάλογα με τις διαβάθμιση των πληροφοριών που θα διαρρεύσουν. Αν οι πληροφορίες είναι εξαιρετικά σημαντικές αντιστοίχως καταστροφικές και κρίσιμες θα είναι και οι επιπτώσεις, οι οποίες ενδέχεται να οδηγήσουν σε ένα παγκόσμιο ντόμινο αλληλεπιδράσεων. Αν οι πληροφορίες συνεχίζουν να είναι σημαντικές, σε μικρότερο όμως επίπεδο και με μικρότερη πιθανότητα διαρροής, οι επιδράσεις ενδέχεται να περιοριστούν σε εγχώριο επίπεδο . Αντίστοιχα, αν η φύση των πληροφοριών δεν είναι ιδιαιτέρως σημαντική, ο αντίκτυπος που αναμένεται να υπάρξει εκδηλώνεται μέσω δυσαρέσκειας των μερών .

Τέλος, στην Εικόνα 1 γίνεται μια απεικόνιση του αντίκτυπου της διαρροής, όπως τον αντιλαμβάνεται μια εταιρεία ή μια βιομηχανία.

Ο αντίκτυπος από την κλοπή ή διαρροή που αφορά μια εταιρεία ή βιομηχανία διαμορφώνεται από το κόστος και το χρόνο που χρειάστηκε προκειμένου να αποκτήσει ή να αναπτύξει την εν λόγω πληροφορία ή τεχνολογία. Επομένως, αν το υλικό ή η πληροφορία που αποσπάστηκε χρειάστηκε μεγάλο χρονικό διάστημα και αντίστοιχα υψηλό κόστος για να υλοποιηθεί, ο αντίκτυπος θα είναι από κρίσιμος έως και καταστροφικός. Αν το κόστος και το διάστημα απόκτησης κυμαίνεται σε ανεκτά για την εταιρεία επίπεδα, τότε ο αντίκτυπος είναι πιο υποβαθμισμένος. Στην περίπτωση που το κόστος ήταν χαμηλό και το διάστημα απόκτησης σύντομο, ο αντίκτυπος είναι σαφώς περιορισμένος.

Πίνακας 2. Παράγοντες απειλής, Δρώντες και Τρόποι απόκτησης πληροφοριών (ENISA, 2016)

	Παράγοντες Απειλής/ Δρώντες						
	Κυβερνο-εγκληματίες	Εσωτερικοί Δρώντες	Online social hackers	Κράτη	Εταιρείες	Hacktivists	Κυβερνο-τρομοκράτες
Κακόβουλο Λογισμικό	✓	✓	✓	✓	✓	✓	✓
Επιθέσεις βάσει διαδικτύου	✓			✓	✓	✓	✓
Εσωτερική Απειλή	✓	✓		✓	✓		✓
Ψάρεμα	✓	✓	✓	✓	✓	✓	✓
Ανεπιθύμητη & ενοχλητική αλληλογραφία	✓		✓	✓	✓	✓	✓
Διαρροή δεδομένων	✓	✓		✓	✓	✓	✓
Κλοπή ταυτότητας	✓	✓		✓	✓	✓	✓
Διαρροή πληροφοριών	✓	✓	✓	✓	✓	✓	✓
Κυβερνο-κατασκοπεία		✓		✓	✓		

Οι σημαντικές πληροφορίες που έχουν στην κατοχή τους οι εταιρείες και το κράτος απειλούνται, όπως απεικονίζεται στον Πίνακα 2 και τις Εικόνες 1 και 2, από αντίπαλα κράτη, εταιρείες, hackers, τρομοκράτες που έχουν μεταφέρει το πεδίο δράσης τους στο διαδίκτυο, ομάδα ακτιβιστών που δραστηριοποιούνται στον κυβερνοχώρο, μεμονωμένους δρώντες αλλά και άτομα που προέρχονται από το προσωπικό των εταιρειών ή των κρατικών υπηρεσιών. Όλοι αυτοί είναι δρώντες που έχουν ως στόχο την απόσπαση και απόκτηση πληροφοριών ώστε να τις χρησιμοποιήσουν για να μεγιστοποιήσουν το προσωπικό τους όφελος.

Αν και όλοι οι τρόποι που απεικονίζονται στον Πίνακα 2 χρησιμοποιούνται από σχεδόν όλους τους προαναφερθέντες δρώντες, η κυβερνοκατασκοπεία χρησιμοποιείται μόνο από κράτη, εταιρείες και εσωτερικούς δρώντες σε αυτές τις οντότητες. Δεδομένης της κοινής απειλής υπάρχουν κάποιες κοινές δράσεις που μπορούν να γίνουν, ώστε να αυξηθούν τα μέτρα προστασίας και να μειωθούν τα περιστατικά εισβολής και κλοπής.

Η ανταλλαγή πληροφοριών μεταξύ των δρώντων είναι σημαντική. Αυτό που κάνει όμως τη διαφορά δεν είναι η ποσότητα των πληροφοριών αλλά η ποιότητα, το επίπεδο και η συνοχή. Το περιεχόμενο των πληροφοριών που σχετίζονται με απειλές πρέπει να είναι χρήσιμα και να αναλυθούν έγκαιρα. Εξίσου απαραίτητο είναι να δημιουργηθεί ένας τυποποιημένος τρόπος αναφοράς σε απειλές, κατηγορίες απειλών και ορολογίας απειλών, καθώς η σωστή παρουσίαση των πληροφοριών σχετικά με τις απειλές είναι αρκετά σημαντικές για τη διάδοσή τους μεταξύ των ενδιαφερόμενων μερών. Κρίσιμο ζήτημα που χρήζει περαιτέρω εξέτασης είναι η ταχύτητα αντίδρασης στις απειλές του κυβερνοχώρου.

Η ανάπτυξη και εξέλιξη των κυβερνοαπειλών στην εποχή που διανύουμε είναι εντυπωσιακή για δύο λόγους. Πρώτον επειδή δρα με τρόπο εξαιρετικά απλό χρησιμοποιώντας μέσα χαμηλού κόστους και τεχνολογίας αλλά υψηλής απόδοσης. Δεύτερον λόγω της πολύπλοκης δράσης από τη χρήση επόμενης γενιάς κακόβουλου λογισμικού.

Στον τομέα των επιχειρήσεων οι μικρομεσαίες επιχειρήσεις είναι εκείνες που βρίσκονται σε έναν φαύλο κύκλο ˙ αφενός δεν διαθέτουν τα μέσα για τα κατάλληλα μέτρα ασφαλείας και αφετέρου δεν γνωρίζουν τη σημασία και την ένταση της απειλής στον κυβερνοχώρο. Η έρευνα που έκανε η Ernst & Young για το 2014 δείχνει πως στο 44% των εταιρειών παγκοσμίως είχαν δεχτεί επίθεση από το διαδίκτυο αφορούσαν την κλοπή δεδομένων ή πνευματικής ιδιοκτησίας. Σύμφωνα με την ίδια έρευνα, 40% των εταιρειών παγκοσμίως κατατάσσουν τη βιομηχανική κατασκοπεία ως την πρώτη ή δεύτερη τη τάξει απειλή (Young, 2014).

Σημαντική παραμένει όμως και η διαρροή πληροφοριών που οφείλεται στον ανθρώπινο παράγοντα. Έρευνες που έχουν γίνει δείχνουν την έκταση του προβλήματος. Από έρευνα που έγινε το 2016 φαίνεται πως μεγάλες και μικρές επιχειρήσεις στο Ηνωμένο Βασίλειο σημειώνουν διαρροή πληροφοριών από τους εργαζόμενους –ή πρώην εργαζόμενους- στις αντίστοιχες εταιρείες (GOV.UK, 2016) . Σύμφωνα με την ίδια έκθεση οι ακούσιες διαρροές είναι περισσότερες από της εκ προθέσεως. Το ανθρώπινο λάθος είναι ο πιο κοινός παράγοντας που προκαλεί τις πιο σημαντικές διαρροές. Η έρευνα της Ernst & Young κατατάσσει τις εισβολές από τους εργαζόμενους στο 31% (Young, 2014).

Να σημειωθεί ότι, οι εταιρείες συχνά δεν αντιλαμβάνονται τις αιτίες και τους παράγοντες που οφείλονται για τη διαρροή. Ο χρόνος που χρειάζεται μια εταιρεία για να αντιληφθεί ότι έχει προσβληθεί το σύστημά της υπολογίζεται πως είναι ένας χρόνος και έξι μήνες. Εξίσου δύσκολη είναι η εκτίμηση που αφορά τις οικονομικές ζημίες για τις εταιρείες που προκαλούνται από την κλοπή εμπιστευτικών πληροφοριών. Η McAfee εκτίμησε πως ο

οικονομικός αντίκτυπος του κυβερνοεγκλήματος και της κυβερνοκατασκοπείας σε έρευνα που διεξήγε το 2013 δείχνει πως η οικονομική ζημία κυμαίνεται από 120 μέχρι 280 δις δολάρια μέσα σ'ένα χρόνο στις ΗΠΑ, ενώ το 75% από αυτές τις απώλειες οφείλεται σε κλοπή υλικού πνευματικής ιδιοκτησίας (Iosif & Fragiskos-Emmanouil, 2016).

Εξαιτίας της φύσης των περιστατικών δεν υπάρχουν επαρκή δεδομένα προς μελέτη. Πολλές από αυτές τις περιπτώσεις δεν δημοσιοποιούνται προκειμένου να μην πληγεί περαιτέρω η φήμη της εταιρείας και η εμπιστοσύνη των επενδυτών και του κοινού. Παρόλα αυτά, η ανάλυση των περιστατικών δείχνει πως στις περισσότερες περιπτώσεις δεν πραγματοποιούνται οι βασικοί έλεγχοι ασφάλειας.

7. Συμπεράσματα – Επίλογος

Συμπερασματικά, αυτό που προκύπτει από την έρευνα είναι πως τα κράτη επιδιώκουν την επικράτηση και κυριαρχία τους στη διεθνή πολιτική και οικονομική σκηνή. Η οικονομική αλληλεξάρτηση και η ύπαρξη πυρηνικών όπλων μεταξύ των μεγάλων δυνάμεων. Πλέον τα κράτη χρησιμοποιούν οικονομικά μέσα προκειμένου να ασκήσουν πίεση και να φτάσουν στην επίτευξη των στόχων τους. Σημαντικό μέσο βοήθειας για την επίτευξη αυτού του στόχου είναι η οικονομική κατασκοπεία. Τα κράτη δεν παραδέχονται ανοικτά πως τη χρησιμοποιούν. Οι εταιρείες και οι βιομηχανίες κινούνται στο ίδιο πλαίσιο. Αποσκοπούν στη μεγιστοποίηση των κερδών τους με την κατοχύρωση όλο και περισσότερο τεχνολογικών επιτευγμάτων. Η οικονομική κατασκοπεία διαδραματίζει έναν συνεχώς αυξανόμενο σημαντικό ρόλο στις Διεθνείς Σχέσεις. Η σύνδεσή της με τις πληροφορίες και τις νέες τεχνολογίες δημιουργεί ένα καινούριο πεδίο δράσης στα κράτη και τις επιχειρήσεις.

Μπορούν να εξαχθούν τριών ειδών συμπεράσματα ˙ πολιτικής φύσης, επιχειρησιακής και ερευνητικής. Όσον αφορά τις δράσεις που θα γίνουν από την πολιτική πλευρά, αυτές αφορούν τη δημοσιοποίηση οδηγιών όπου θα αναφέρονται τα μέτρα εκείνα που στοχεύουν στη μείωση των κυβερνοαπειλών. Επίσης, σημαντικό να εκδοθούν οδηγίες σχετικές με τη συγκέντρωση πληροφοριών που σχετίζονται με κυβερνοεπιθέσεις σε κυβερνητικούς οργανισμούς και υπηρεσίες.

Οι επιχειρήσεις που δραστηριοποιούνται στον τομέα της ασφάλειας του κυβερνοχώρου πρέπει να δημιουργήσουν μοντέλα που θα εξετάζουν τις πληροφορίες σε πραγματικό χρόνο (real – time). Αυτού του είδους οι πληροφορίες είναι από τις πιο σημαντικές γιατί όχι μόνο βοηθούν στην αξιολόγηση των κινδύνων αλλά και επειδή μπορούν να υποδείξουν ποιες ενέργειες πρέπει να γίνουν ώστε να ληφθούν τα κατάλληλα μέτρα προστασίας. Πρέπει να γίνει αντιληπτό σε όλες τις εταιρείες πως η διαφύλαξη και προστασία των δεδομένων τους είναι ζωτικής σημασίας για την ίδια τους την ύπαρξη αλλά και την ασφάλεια των πελατών τους. Εξίσου σημαντικό θα ήταν και η ανάπτυξη τρόπων συλλογής πληροφοριών από το dark web[2], αφού αποτελεί μέσο διακίνησης υποκλεμμένων πληροφοριών. Οι πληροφορίες που σχετίζονται με τις απειλές προτείνεται να είναι σαφείς και επαρκείς, ώστε να είναι εύκολα επεξεργάσιμες τόσο για τους αναλυτές όσο και για τους λήπτες των αποφάσεων.

Τέλος, απαραίτητη είναι η επεξεργασία των δεδομένων που προκύπτουν από μελέτη προγενέστερων περιστατικών. Αυτή η επεξεργασία είναι δυνατό να δώσει ποσοτικές αποδείξεις, στοιχεία για τα καταγεγραμμένα περιστατικά και για το πεδίο απειλής, τα οποία να βοηθήσουν στην καλύτερη λήψη μέτρων πρωτίστως πρόληψης και προστασίας και εν συνεχεία αντιμετώπισης.

[2] Dark Web: είναι ένας ανώνυμος διαδικτυακός ιστός, στον οποίο χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες.

Η ασφάλεια των πληροφοριών μπορεί να επιτευχθεί με την αμφότερη συνδρομή και συνεργασίας κράτους και ιδιωτικών εταιρειών. Με τη δημιουργία κλίματος αμοιβαίας εμπιστοσύνης, το κράτος - μέσα από τη σταθερότητα που μπορεί να παρέχει- και οι εταιρείες - μέσα από τις επενδύσεις και τα τεχνολογικά μέσα που διαθέτουν και αναπτύσσουν- δύνανται να διαμορφώσουν την ασφάλεια τόσο της χώρας και των πολιτών της όσο και των συμφερόντων αυτής.

Βιβλιογραφία – Κατάλογος πηγών

Alexander, M. S. (2010, March 24). Introduction: Knowing your friends, assessing your allies - perspectives on intra-alliance intelligence. *Intelligence and National Security* .

Barrett, D. M. (2014, November 27). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security* , pp. 793-810.

Broomfield, E. V. (2013, March 26). Perceptions of Danger: The China Threat theory. *Journal of Contemporary China* .

Cable, V. (1995, April). What is International Economic Security? *International Affairs* , pp. 305-324.

China's Cyberespionage: The National Security Distinction and US Diplomacy.

Daniel Javorsek II, J. R. (2015, August 5). A Formal Risk-Effectiveness Analysis Proposal for the Compartmentalized Intelligence Security Structure. *International Journal of Intelligence and Counterintelligence* , pp. 736-740.

Easley, L.-E. (2014, July 23). Spying on Allies. *Survival: Global Politics and Strategy* .

Economic Espionage. IOSS Intelligence Threat Handbook.

Encyclopedia.com. *Post-Cold War Espionage Between the United States and Russia: How was the Mission changed?*

ENISA. (2016, January). *European Union Agency for Network and Information Security*. Retrieved August 31, 2017, from https://www.enisa.europa.eu/publications/etl2015

Erdogan, I. (2009). Economic Espionage: A New Form of War in the 21st Century.

Eric Lipton, D. E. (Dec.13 2016). The Perfect Weapon: How Russian Cyberpower Invaded the US. *The New York Times* .

Fraumann, E. (2013, 03 17). Economic Espionage: Security Missions Redefined. *Public Administration Reviw* .

Galeotti, M. (2016). *Putin's Hydra: Inside Russia's Intelligence Services.* European Council on Foreign Relations.

GOV.UK. (2016, May). Retrieved September 23, 2017, from Cyber Security Breaches Survey: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Haber, M. (2017, July 6). *BeyondTrust*. Retrieved September 2017, 2, from https://www.beyondtrust.com/blog/what-is-cyberthreat-intelligence/

Hastedt, G. (n.d.). Seeking Economic Security Through Intelligence. *International Journal of Intelligence and Counterintelligence* , pp. 386-401.

Inkster, N. (2014, March 15). The Snowden Revelations: Myths and Misapprehensions. *Survival: Global Politics and Strategy* , pp. 51-58.

Iosif, A., & Fragiskos-Emmanouil, K. (2016). *Industrial Espionage and Technical Surveillance Counter Measurers.* Springer.

James Stavridis, E. N. (2013, March 28). The 21st Century Force Multiplier: Public-Private Collaboration. *The Washington Quarterly* , pp. 7-20.

Jeffrey, W. (1991, January 1). Intelligence and economic security. *International Journal of Intelligence and Counterintelligence* , pp. 203-219.

Johnson, L. K. (2014, November 27). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security* .

Kelly, N., & Foran, C. (2015, September 25). *The Atlantic.* Retrieved September 3, 2017, from https://www.theatlantic.com/politics/archive/2015/09/president-obama-and-chinese-president-xi-jinping-announce-cybersecurity-agreement/444948/

Korolov, M. (2017, January 11). *CSO*. Retrieved September 4, 2017, from https://www.csoonline.com/article/3156554/it-strategy/russia-china-and-the-us-are-biggest-geopolitical-cybersecurity-threats.html

Landau, S. (2013, July/August). *Making Sense: What's Significant in the NSA Surveillance Revelations.* Retrieved July 25, 2017, from IEEE Computer and Reliability Societies: https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf

Lefebvre, S. (2008, February 1). Spying on Friends?: The Franklin Case, AIPAC, and Israel. *International Journal of Intelligence and Counterintelligence* .

Lewis, J. A. (2015, 21 October). *CSIS - Center for Strategic International Studies.* Retrieved September 3, 2017, from https://www.csis.org/analysis/moving-forward-obama-xi-cybersecurity-agreement

Lyle Goldstein, V. K. (2017, February 15). *Fairbank Center for Chinese Studies*. Retrieved September 4, 2017, from http://fairbank.fas.harvard.edu/events/tectonic-geopolitical-shift-the-china-russia-us-strategic-triangle-in-the-trump-era/

Neeb, R. (2017, January). Retrieved 8 24, 2017, from http://www.securefreesociety.org/wp-content/uploads/2017/01/SFS-Global-Dispatch-Issue-2.pdf

Omand, D. (2014, November 27). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security* .

Piccone, T. (2016, November). *Brookings*. Retrieved September 4, 2017, from https://www.brookings.edu/research/the-geopolitics-of-chinas-rise-in-latin-america/

Poteat, S. E. *The Attack on America's Intellectual Property - Espionage after the Cold War.*

Rubenstein, D. (2014, December 1). *Nation State Cyber Espionage and its Impacts*. Retrieved July 23, 2017, from http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/

Schiller, C. A. (13, March 31). Espionage: Counter-Economic. *Encyclopedia of Information Assurance* .

Secretary, T. W.-O. (2015, September 25). *The White House* . Retrieved September 3, 2017, from https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Section 4: Commercial Cyber Espionage And Barriers to Digital Trade in China.

Sheehan, M. (2005). International Security: An analytical survey. In M. Sheehan, *Security: An analytical survey.* Lynne Rienner Publishers.

Szabo, S. F. (2014, September 25). Germany's Commercial Realism and the Russia Problem. *Survival: Global Politics and Strategy* .

Wikipedia. (2015, 12 2). Retrieved 08 28, 2017, from https://el.wikipedia.org/wiki/%CE%93%CE%B5%CF%89%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%AF%CE%B1

Young, E. &. (2014, October). Retrieved September 23, 2017, from www.ey.com: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

Κάτσουρα, Α. (2017, March 12). *Εφημερίδα των Συνακτών*. Retrieved July 19, 2017, from http://www.efsyn.gr/arthro/oikonomiki-kataskopia-enas-aoratos-polemos

Κωνσταντόπουλος, Ι. (2010). *Οικονομία και Κατασκοπεία - Θεωρία και πράξη.* Βάρη, Αττικής: Εκδόσεις ΠΟΙΟΤΗΤΑ.

Πλατιάς, Α. Γ. *Γεωπολιτική, Γεωοικονομία και Διεθνής Ανταγωνισμός.*