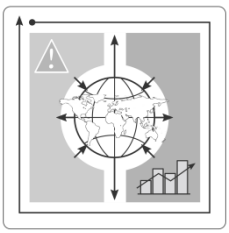
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ



ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«*Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων*»

Οικονομική Κατασκοπεία και Ασφάλεια

Ένας παγκόσμιος αγώνας υπεροχής

ΗΠΑ vs ΚΙΝΑ

Μεταπτυχιακή Διπλωματική Εργασία Ειδίκευσης
«Ανάλυση δεδομένων στην παγκόσμια πολιτική»
«Διοικητική της διακινδύνευσης στην παγκόσμια πολιτική»

Γεώργιος Κούρκουλος

Τριμελής επιτροπή:
Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος
Αναπληρωτής Καθηγητής Ν. Κουτσούκης
Επίκουρος Καθηγητής Σ. Πετρόπουλος

Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος

Τελική έκδοση

Κόρινθος, 2021

UNIVERSITY OF THE PELOPONNESE
SCHOOL OF SOCIAL & POLITICAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCE &INTERNATIONAL RELATIONS

MASTER'S PROGRAMME IN
"GLOBAL RISKS AND ANALYTICS"

Economic Espionage and Security

A global fight for supremacy

USA vs CHINA

Master's dissertation specializing in
"Data analysis in global politics"
"Risk management in global politics"

George Kourkoulos

Committee:
Assistant Professor I. Konstantopoulos
Associate Professor N. Koutsoukis
Assistant Professor S. Petropoulos

Assistant Professor I. Konstantopoulos

Final version

Corinth, Greece, 2021

Φύλλο αξιολόγησης

Η διπλωματική εργασία με τίτλο *«Οικονομική Κατασκοπεία και Ασφάλεια» του Γεώργιου Κούρκουλου* 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 / /2021 με γενική επίδοση:

- Καλώς
- Λίαν Καλώς
- Άριστα

Τα μέλη της τριμελούς επιτροπής:

1. Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος
2. Αναπληρωτής Καθηγητής Ν. Κουτσούκης
3. Επίκουρος Καθηγητής Σ. Πετρόπουλος

Abstract

This project addresses the effect of economic espionage on security, as well as the role it may play on the unregulated international environment. These are hereby achieved through the analysis of risk-taking during crisis.

Economic espionage is not a modern phenomenon, its roots are lost in the mists of time. It has been one of the most crucial issues in international politics since the post cold war era. The economic development has an impact on the development of science and technology, fields which are inherently connected to a state's national security and power.

Despite the extent of economic espionage, the current research focuses on the countries of interest, namely the United States of America and China. Over the years, the USA have been the biggest victim of economic espionage leading the country to strengthen the field of economic counter-espionage trying to preserve their "status quo" and supremacy in the area of science and technology. On the contrary, China has been the biggest perpetrator of economic espionage aiming at the USA in an attempt to increase its international power via economy, science and technology. There's an ongoing "secret" war which, under the cover of discussions, negotiations, cooperations and political decisions, poses many "threats" to both the internal and the international environment of a country.

Περίληψη

Η παρούσα εργασία εξετάζει την επίδραση της οικονομικής κατασκοπείας στην ασφάλεια, καθώς επίσης και το ρόλο που μπορεί να διαδραματίσει στο άναρχο διεθνές περιβάλλον μέσα από την ανάλυση της Διακινδύνευσης της Κρίσης.

Η οικονομική κατασκοπεία δεν αποτελεί ένα φαινόμενο της σήμερον εποχής, οι ρίζες της χάνονται στα βάθη των αιώνων. Από τη μεταψυχροπολεμική εποχή μέχρι και σήμερα έχει αποτελέσει ένα από τα πιο σημαντικά θέματα της διεθνούς πολιτικής σκηνής. Η ανάπτυξη της οικονομίας επιδρά στην ανάπτυξη της επιστήμης και της τεχνολογίας, τομείς άρρηκτα συνδεδεμένοι με την εθνική ασφάλεια και την ισχύ ενός κράτους.

Παρόλη την έκταση του φαινομένου της οικονομικής κατασκοπείας, η εν λόγω έρευνα θα επικεντρωθεί στις χώρες ενδιαφέροντος, τις Ηνωμένες Πολιτείες Αμερικής και την Κίνα. Οι ΗΠΑ έχουν αποτελέσει διαχρονικά το μεγαλύτερο ¨θύμα¨ οικονομικής κατασκοπείας ενισχύοντας τον τομέα της οικονομικής αντικατασκοπείας της, προσπαθώντας να διατηρήσουν το «status quo» και την πρωτοκαθεδρία τους στον επιστημονικό - τεχνολογικό τομέα. Στην αντίπερα όχθη, η Κίνα έχει αποτελέσει το μεγαλύτερο ¨θύτη¨ άσκησης οικονομικής κατασκοπείας των ΗΠΑ, στην προσπάθεια της να αυξήσει την ισχύ της στην παγκόσμια σκακιέρα μέσα από τον τομέα της οικονομίας, της επιστήμης και της τεχνολογίας. Ένας συνεχής μυστικός ¨πόλεμος¨, υπό το πέπλο συνομιλιών, διαπραγματεύσεων, συνεργασιών και πολιτικών αποφάσεων, που δημιουργεί πολλούς ¨κινδύνους¨ στο εσωτερικό και στο διεθνές περιβάλλον μιας χώρας.

Πρόλογος

Αφιερώνω την εργασία στη γυναίκα μου και τα παιδιά μου.

Θα ήθελα να ευχαριστήσω τους καθηγητές που με υποστήριξαν για τη διεκπεραίωση της εργασίας, καθώς και το σύνολο των καθηγητών και συμμαθητών μου που συνεργαστήκαμε κατά τη διάρκεια του μεταπτυχιακού προγράμματος.

Πίνακας Περιεχομένων

Abstract I

Περίληψη II

Πρόλογος III

1. Εισαγωγή 1

1.1 Σκοπός 2

1.2 Μεθοδολογία 2

2. Βασικές έννοιες 4

2.1 Πληροφόρηση 4

2.2 Ασφάλεια 5

2.3 Risk 6

2.4 Risk management 6

2.5 Οικονομική Κατασκοπεία 7

2.6 Κύκλος Πληροφοριών 8

2.7 Μέσα-Κατηγορίες συλλογής πληροφοριών 9

3. Η Οικονομική κατασκοπεία στο πέρασμα του χρόνου 10

3.1 ΗΠΑ εναντίον ΚΙΝΑΣ 11

4. Κίνητρα - αντικίνητρα οικονομικής κατασκοπείας 15

4.1 Μακροοικονομική κατασκοπεία 15

4.1.1 Κίνητρα 15

4.1.2 Αντικίνητρα 16

4.2 Μικροοικονομική κατασκοπεία 18

4.2.1 Κίνητρα 18

4.2.2 Αντικίνητρα 19

5. Οικονομική κατασκοπεία και ασφάλεια στις ΗΠΑ και Κίνα 21

5.1 Η περίπτωση των ΗΠΑ ως ¨θύμα¨ οικονομικής κατασκοπείας 21

5.2 Η περίπτωση της ΚΙΝΑ ως ¨θύτης¨ οικονομικής κατασκοπείας 26

6. Διοίκηση της Διακινδύνευση και οικονομική κατασκοπεία 31

6.1 Αναγνώριση - ομαδοποίηση κινδύνων 31

6.2 Μήτρα κινδύνων - Πίνακες Matrix 33

6.3 Ανάλυση σημαντικότερου κινδύνου 36
6.3.1 Δεντρική ανάλυση κινδύνου – Event tree analysis 37
6.3.2 Πιθανές Εκβάσεις 38
7. Συμπεράσματα – Επίλογος 40
Κατάλογος πηγών – Βιβλιογραφία 43

1. Εισαγωγή

Η πληροφόρηση και η ασφάλεια αποτελούν δύο έννοιες άρρηκτα συνδεδεμένες μεταξύ τους *(Κωνσταντόπουλος Ι., 2018).* Δύο έννοιες πολυδιάστατες, διατηρώντας ωστόσο την ισχυρή σχέση που τους συνδέει. Η ύπαρξη ενός άναρχου διεθνούς συστήματος, σε συνδυασμό με την απουσία ενός ¨διεθνούς Λεβιάθαν¨, όπου θα ελέγχει και θα ρυθμίζει το διεθνές σύστημα παρέχοντας ασφάλεια στα κράτη και στις κοινωνίες, επιβεβαιώνει τη σημαντικότητα της σχέσης αυτής. Μελετώντας και αναλύοντας την πληροφόρηση, παρατηρούμε ότι μέρος της αποτελεί η κατασκοπεία/μυστική δράση και κατά επέκταση η οικονομική κατασκοπεία.

Μετά το τέλος του Ψυχρού Πολέμου, η οικονομική ασφάλεια εμφανίστηκε δυναμικά στο διεθνές προσκήνιο, οδηγώντας τις υπηρεσίες πληροφοριών στην άσκηση οικονομικής κατασκοπείας ή αντικατασκοπείας. Ο James R. Woolsey ως Διευθυντής της CIA το 1993 ανέφερε ότι η οικονομική κατασκοπεία αποτελεί «το πιο καυτό τρέχον θέμα στην πολιτική των υπηρεσιών πληροφοριών» *(Strong, 1994).* Μελετώντας τη βιβλιογραφία συνειδητοποιούμε όλο και περισσότερο την αλληλεπίδραση της οικονομικής κατασκοπείας και της ασφάλειας. Ωστόσο, ζούμε σε μια εποχή όπου το ενδεχόμενο σενάριο πραγματοποίησης άμεσου πολέμου στο δυτικό κόσμο και σε χώρες ανεπτυγμένες, με την παλαιά κλασική στρατιωτική μορφή του, είναι σχεδόν απίθανο. Οι συνεχείς παγκόσμιες οικονομικές μεταβολές έχουν δημιουργήσει ένα καθορισμένο οικονομικό πλαίσιο για τα κράτη. Η άνιση ανάπτυξη μεταξύ των κρατών και η ανακατανομή της ισχύς και του πλούτου μεταξύ των κρατών έχει επιφέρει αλλαγές στο διεθνές οικονομικό σύστημα *(Kennedy Paul, 1988).* Στη σήμερον εποχή η πληροφορία σε συνδυασμό με την τεχνολογία αποτελούν τις σημαντικότερες πηγές παραγωγικότητας *(Stonier T., 1983).* Οι πληροφορίες που έχουν σχέση με οικονομικούς παράγοντες μπορούν να παρέχουν πληροφόρηση ζωτικής σημασίας στους υπεύθυνους χάραξης πολιτικής, καθώς επίσης να επηρεάσουν ή και να ενισχύσουν την οικονομική ισχύ ενός κράτους. Η οικονομική ισχύς μπορεί να συνεισφέρει στην ανάπτυξη της επιστήμης και της τεχνολογίας, δύο τομείς αρκετά ισχυροί και καθοριστικοί τόσο σε πολιτικό όσο και σε στρατιωτικό επίπεδο. Επιπλέον, Η ραγδαία εξέλιξη της τεχνολογίας επηρεάζει όχι μόνο την καθημερινότητας μας, μεταφράζοντας την με μια έννοια ευημερίας, αλλά μπορεί να παίξει σημαντικό ρόλο σε μια έννοια που ονομάζεται «ισχύς». Η οικονομική κατασκοπεία λοιπόν δεν περιορίζεται μόνο στον οικονομικό

τομέα, καθώς η οικονομία μέσα στο άναρχο διεθνές περιβάλλον αποτελεί από μόνη της ένα ισχυρό, αν όχι τον πιο ισχυρό, δείκτη ισχύος, δύναμης και παγκόσμιας επιρροής.

Είναι λοιπόν σαφές, ότι οι πληροφορίες οικονομικού περιεχομένου μπορούν να οδηγήσουν όχι μόνο στην αύξηση της οικονομικής και της στρατιωτικής ισχύς, αλλά και να συμβάλλουν στην πραγματοποίηση σημαντικών παγκόσμιων αλλαγών που αφορούν τη διεθνή τεχνολογική υπεροχή, επηρεάζοντας τις παγκόσμιες ισορροπίες.

1.1 Σκοπός

Σκοπός της εργασίας είναι αρχικά η μελέτη των εννοιών που σχετίζονται με την οικονομική κατασκοπεία και την ασφάλεια. Μέσα από τις έννοιες αυτές θα μπορέσουμε να κατανοήσουμε το φαινόμενο της οικονομικής κατασκοπείας, την ευρεία και πολυδιάστατη έννοια της ασφάλειας, καθώς να διαπιστώσουμε και να επιβεβαιώσουμε τη σχέση αλληλεπίδρασης μεταξύ τους. Επιπλέον μέσω της διεθνούς βιβλιογραφίας και συλλέγοντας πληροφορίες για τις δύο χώρες ενδιαφέροντος μας, τις ΗΠΑ και την Κίνα, και χρησιμοποιώντας εργαλεία της Διακινδύνευση της Κρίσης (Risk management) να οδηγηθούμε σε κεραία και τεκμηριωμένα αποτελέσματα, έχοντας ως γνώμονα τα παρακάτω κεντρικά ερωτήματα: «*Ποια λοιπόν είναι τα κίνητρα και τα αντικίνητρα που ωθούν τους υπευθύνους χάραξης πολιτικής και λήξης αποφάσεων στη διεξαγωγή της μακροοικονομικής και μικροοικονομικής κατασκοπείας;», «Ποιοι είναι οι κίνδυνοι που προκύπτουν από την άσκηση οικονομικής κατασκοπείας από μια ξένη χώρα;» και «Μπορεί η οικονομική κατασκοπεία να συμβάλλει στην απόκτηση τεχνολογικού πλεονεκτήματος ανάμεσα σε δύο χώρες αλλάζοντας τις υπάρχουσες ισορροπίες;».*

1.2 Μεθοδολογία

Η παρούσα εργασία αφορά τη μελέτη του φαινομένου της οικονομικής κατασκοπείας σε συνδυασμό με την επίδραση της στην ασφάλεια ενός κράτους. Αρχικά μέσα από βιβλία και συγγράμματα θα αναγνωριστούν κύριες έννοιες όπως πληροφόρηση, ασφάλεια (διαστάσεις), οικονομική κατασκοπεία (διαστάσεις-διαφορές με στρατιωτική και βιομηχανική κατασκοπεία), κύκλος πληροφοριών, μέσα συλλογής πληροφοριών, καθώς και όροι που σχετίζονται με τις παραπάνω έννοιες, οδηγώντας μας σε μια ασφαλή αποσαφήνιση του φαινομένου της οικονομικής κατασκοπείας και ασφάλειας.

Στη συνέχεια θα γίνει μια νύξη της οικονομικής κατασκοπείας στο πέρασμα του χρόνου, αποδεικνύοντας ότι δεν αποτελεί φαινόμενο του 21ου αιώνα. Επιπλέον χρησιμοποιώντας έρευνες και μελέτες θα αποτυπώσουμε τα σημαντικότερα

παραδείγματα οικονομικής κατασκοπείας ανάμεσα στις ΗΠΑ και στην Κίνα την τελευταία 20ετία, τεκμηριώνουν την έντονη ύπαρξη της μεταξύ τους.

Επιπροσθέτως θα απαντήσουμε στο πρώτο κεντρικό ερώτημα μας, *«Ποια λοιπόν είναι τα κίνητρα και τα αντικίνητρα που ωθούν τους υπευθύνους χάραξης πολιτικής και λήξης αποφάσεων στη διεξαγωγή της μακροοικονομικής και μικροοικονομικής κατασκοπείας;».*

Έπειτα θα μελετήσουμε τις δύο χώρες ενδιαφέροντος δίνοντας έμφαση στην Περίπτωση των ΗΠΑ ως ¨θύμα¨ οικονομικής κατασκοπείας και της Κίνας ως ¨θύτης¨, αναλύοντας πτυχές και γεγονότα από το παρελθόν μέχρι και σήμερα.

Τέλος θα αναγνωρίσουμε τους κινδύνους που προκύπτουν από την άσκηση οικονομικής κατασκοπείας εις βάρος μιας χώρας (θύμα), μέσω εργαλείων της Διακινδύνευσης της Κρίσης. Κατά την ανάλυση θα πραγματοποιηθεί ομαδοποίηση των κινδύνων, εκτίμηση προτεραιότητας, και αναγνώριση του σημαντικότερου κινδύνου με την υψηλότερη προτεραιότητα μέσω της πιθανότητας και του αντίκτυπου. Η μελέτη θα ολοκληρωθεί με τη Δεντρική ανάλυση του σημαντικότερου κινδύνου (Event tree analysis), καταλήγοντας στις αναμενόμενες εκβάσεις, επιθυμώντας να μας απαντήσουν στο ερώτημα: «*Ποιοι είναι οι κίνδυνοι που προκύπτουν από την άσκηση οικονομικής κατασκοπείας από μια ξένη χώρα;».*

Ολοκληρώνοντας θα αναφερθούν τα γενικά συμπεράσματα, απαντώντας στο τελευταίο κεντρικό ερώτημά: *«Μπορεί η οικονομική κατασκοπεία να συμβάλλει στην απόκτηση τεχνολογικού πλεονεκτήματος ανάμεσα σε δύο χώρες αλλάζοντας τις υπάρχουσες ισορροπίες;».*

2. Βασικές έννοιες

2.1 Πληροφόρηση

Η έννοια της πληροφόρησης δεν αντικατοπτρίζεται μέσα από έναν απλά διατυπωμένο ορισμό. Αποτελεί μια διαδικασία μέσα από την οποία προκύπτει το τελικό επεξεργασμένο προϊόν. Ο Alexander Cadogan, πρώην υπουργός εξωτερικών της Βρετανίας (1938-1945), στις αρχές του 1980 αναφέρθηκε στον όρο πληροφόρηση περιγράφοντας τον ως «την παραμελημένη διάσταση των διεθνών υποθέσεων». Έννοια με την οποία ταυτίσθηκαν οι Len Scott και Peter Jackson, λέγοντας ότι η σύνδεση της θεωρίας των διεθνών σχέσεων και της πληροφόρησης αποτελούν ένα αβάδιστο ερευνητικό πεδίο και μια παραμελημένη διάσταση. Μελετώντας λοιπόν την έννοια της πληροφόρησης, παρατηρούμε ότι το σύνολο της πληροφόρησης αποτελεί κομμάτι της πληροφορίας, αλλά δεν αποτελούν όλες οι πληροφορίες μέρος της πληροφόρησης. *(Lowenthal, 2003).* Οι Edward Luttwak και Stuart Koehl στον όρο πληροφόρηση αποδίδουν «τη συλλογή, σύνδεση, ανάλυση και διανομή των πληροφοριών σχετικά με τις ικανότητες και προθέσεις πραγματικών ή δυνητικών αντιπάλων» *(Luttwak and Koehl, 1999).* Ο Sherman Kent, ως ¨πατέρας¨ στον τομέα της ανάλυσης της CIA, αναφέρει ότι η πληροφόρηση είναι η γνώση που πρέπει να διαθέτουν τα υψηλά ιστάμενα στελέχη σε πολιτικό και στρατιωτικό επίπεδο, για τη διασφάλιση της εθνικής ευημερίας. Η πληροφόρηση γενικότερα αποτελεί μια διαδικασία μέσα στην οποία ενσωματώνεται η συλλογή, η επεξεργασία και η εκμετάλλευση, καθώς και η σωστή διανομή και ανατροφοδότηση πληροφοριών. Γενικότερα η πληροφόρηση περιλαμβάνει πληροφορίες από διάφορους παράγοντες (πηγές), όπως από ανοιχτές πηγές (Internet, deep web, dark web), από ανάλυση φωτογραφιών (αεροφωτογραφιών και μη), από ανθρώπινες πηγές, από κρυφές ανώνυμες πηγές, μυστική δράση (κατασκοπεία) και από συνδυασμό των παραπάνω. Το τελικό προϊόν της διαδικασίας αυτής αποτελείται από τις επεξεργασμένες πλέον πληροφορίες που έχουν συλλεχθεί, ελεγχθεί και επεξεργαστεί, ώστε να προσφέρουν εν τέλη ένα στρατηγικό πλεονέκτημα στους λήπτες αποφάσεων *(Lowenthal, 2003).*

2.2 Ασφάλεια

Αναφορικά με την έννοια της ασφάλειας παρατηρείτε μια δυσκολία στη διατύπωση ενός ξεκάθαρου ορισμού της, αποθαρρύνοντας τους μελετητές. Το 1966 οι Morton Berkowitz και P.G. Bock αναφέρθηκαν στην έννοια της εθνικής ασφάλειας, λέγοντας ότι «υπήρχαν πολύ λίγες προσπάθειες προκειμένου να οριστεί η έννοια της» (*Bock and Berkowitz, 1966).* Παρόλο που η έννοια της ασφάλειας συμπίπτει με αυτή της ισχύος, αποτελεί μια έννοια παραμεληµένη, όπως χαρακτηρίσθηκε, μέχρι τη δεκαετία του 1980, η μελέτη της οποίας ξεκινά από τις αρχές του 1990, όπου το 1991 ο Barry Buzan χαρακτήρισε την ασφάλεια ως «υπό-αναπτυγμένη έννοια» (underdeveloped concept). Ο ορισμός της ασφάλειας αποτελεί ακόμα και σήμερα μια έννοια αρκετά ασαφής, αμφιλεγόμενη και ευέλικτη. Παρόλα αυτά οι διαμορφωτές των αποφάσεων θεωρούν βολική την ασαφή αυτή έννοια της ασφάλειας *(Buzan, 1991).* Γενικότερα η πλειοψηφία της επιστημονικής κοινότητας αποδέχεται ότι η έννοια της ασφάλειας υποδηλώνει ελευθερία από απειλές προς κύριες αξίες, είτε ομάδων είτε μεμονωμένων ατόμων, έχοντας ως κοινό παρονομαστή τη φράση ¨Free Form Threat¨, με βασικούς πυλώνες την παροχή ασφάλειας και την προστασία της δημοκρατίας. Οι Lawrence Krause και Joseph Nye Jr. διακρίνουν τρεις κατηγορίες αξιών: την ευημερία, την ανεξαρτησία και το πολιτικό κύρος/γόητρο *(Murdock, 1984).* Σύμφωνα με τον Buzan, η έννοια της διεθνούς ασφάλειας δεν περιορίζεται μόνο στη στρατιωτική διάσταση, αλλά επεκτείνεται στην πολιτική, την οικονομική, την κοινωνική και την περιβαλλοντική διάσταση *(Buzan, 1991).* Ας αναφέρουμε λίγα λόγια για την εκάστοτε διάσταση: (1) Η στρατιωτική ασφάλεια αφορά στην αλληλεπίδραση μεταξύ δρώντων, ένοπλες επιθετικές και αμυντικές δυνατότητες και δραστηριότητες των κρατών, καθώς και τις αντιλήψεις και επιθετικές προθέσεις ετέρου κράτους σε θέματα στρατιωτικής φύσεως. (2) Η οικονομική ασφάλεια αφορά την πρόσβαση στους πόρους, τη χρηματοδότηση και τις αγορές στις οποίες είναι απαραίτητες για τη διατήρηση αποδεκτών επιπέδων ευημερίας και κρατικής εξουσίας. (3) Η πολιτική ασφάλεια αφορά την οργανωτική σταθερότητα των κρατών, τα συστήματα διακυβέρνησης και τις ιδεολογίες που τους παρέχουν νομιμότητα. (4) Η κοινωνική ασφάλεια αναφέρεται στη βιωσιμότητα, σε συνθήκες αποδεκτές για την εξέλιξη την κοινωνίας, τα παραδοσιακά πρότυπα της γλώσσας, την κουλτούρα, τα ήθη και τα έθιμα και τη θρησκευτική και εθνική ταυτότητα. (5) Η περιβαλλοντική ασφάλεια ασχολείται με τη «διατήρηση της πλανητικής βιόσφαιρας ως το βασικό σύστημα υποστήριξης από το οποίο εξαρτώνται όλες οι άλλες ανθρώπινες επιχειρήσεις» *(Buzan, 1991).* Παρατηρούμε λοιπόν την πολυδιάστατη μορφή της ασφάλειας και τη δυσκολία αποτύπωσης της μέσα σε έναν απλό ορισμό.

2.3 Risk

Η απόλυτη αποτύπωση του όρου ¨risk¨ δεν υπάρχει. Μελετώντας τη βιβλιογραφία διαπιστώνουμε ότι η έννοια του κινδύνου χρησιμοποιείται άλλοτε ως αναμενόμενη τιμή, κατανομή πιθανότητας, ως αβεβαιότητα ή ως γεγονός. Οι Aven και Renn μας δίνουν κάποιους ορισμούς σχετικά με το τι είναι κίνδυνο: (1) ισούται με την αναμενόμενη ζημία *(Willis, 2007),* (2) ισούται με την αναμενόμενη ανικανότητα *(Campbell, 2005),* (3) είναι η πιθανότητα αρνητικής έκβασης *(Graham and Weiner, 1995),* (4) είναι ένα μέτρο της πιθανότητας και της σοβαρότητας των ανεπιθύμητων ενεργειών *(Lowrance 1976),* (5) είναι ο συνδυασμός πιθανότητας και έκτασης των συνεπειών *(Ali, 2002),* (6) ισούται με το τρίδυμο (si, pi, ci), όπου si είναι το σενάριο, το pi είναι το πιθανότητα αυτού του σεναρίου, και ci είναι η συνέπεια του σεναρίου *(Kaplan and Garrick 1981), (Kaplan 1991),* (7) ισούται με τον δισδιάστατο συνδυασμό συμβάντων/συνεπειών και σχετικές αβεβαιότητες *(Aven, 2007α, 2008α, 2009α, 2010).*

Επιπλέον με τον όρο ¨risk¨ αναφερόμαστε στην επίδραση της αβεβαιότητας στους στόχους, όπου κομβικό σημείο είναι το περιστατικό (risk event) με το οποίο συγκεκριμενοποιείται η αβεβαιότητα. *(ISO 31000:2009).* Γενικότερα μπορούμε να αναφέρουμε ότι ο κίνδυνος αναφέρεται στην αβεβαιότητα του αποτελέσματος, των ενεργειών, των στόχων και τη σοβαρότητα των συνεπειών (ή των αποτελεσμάτων) μιας δραστηριότητας σε σχέση με κάτι που οι άνθρωποι εκτιμούν.

2.4 Risk management

Οι αναμενόμενοι και μη κίνδυνοι χρειάζονται κατάλληλη και αποτελεσματική διαχείριση κινδύνων. Η διαχείριση κινδύνων περιλαμβάνει το σχεδιασμό και την εφαρμογή των ενεργειών και των διορθωτικών μέτρων που απαιτούνται για την αποφυγή, μείωση, μεταφορά ή διατήρηση των κινδύνων. Με βάση την ανάπτυξη μιας σειράς επιλογών και την εξέταση των καταλληλότερων από αυτές, λαμβάνονται και εφαρμόζονται στην πράξη αποφάσεις διαχείρισης κινδύνου. Η διαχείριση κινδύνων περιλαμβάνει τη δημιουργία, την αξιολόγηση και την επιλογή κατάλληλων επιλογών μείωσης του κινδύνου, καθώς και την εφαρμογή των επιλεγμένων μέτρων, την παρακολούθηση της αποτελεσματικότητάς τους και την επανεξέταση της απόφασης, εάν είναι απαραίτητο. Γενικότερα αποτελεί μια διαδικασία διαχείρισης κινδύνων η ροή και διαδικασία της οποίας εξαρτάται από τα πρότυπά ή τη μέθοδο που θα ακολουθηθεί, ανάλογα με την εκάστοτε περίσταση. Η κατανόηση των κινδύνων και η ορθή διαχείριση τους στις διάφορες μορφές της, μπορεί να βοηθήσει τους ενδιαφερόμενους να κατανοήσουν καλύτερα τις ευκαιρίες, συμβιβασμούς, και το

κόστος που ενδέχεται να έχουν στην οποιαδήποτε λήψη απόφασης, όχι μόνο σε εταιρικό, αλλά σε εθνικό και ακόμα και σε διεθνές επίπεδο *(IRGC, 2005).*

2.5 Οικονομική Κατασκοπεία

Η οικονομική κατασκοπεία αποτελεί ένα μέρος της κατασκοπείας/μυστικής δράσης. Ασκείται κυρίως από την κυβέρνηση ενός κράτους μέσω των μυστικών υπηρεσιών του με σκοπό την υποστήριξη των οικονομικών και όχι μόνο συμφερόντων ενός κράτους. Αφορά την απόκτηση μυστικών και ευαίσθητων πληροφοριών σχετικά με θέματα χρηματοοικονομικά, οικονομικής και εμπορικής πολιτικής φύσεως, ιδιωτικές πληροφορίες, καθώς και πληροφορίες σχετικά με τεχνολογίες καίριας σημασίας (critical technologies). Λαμβάνοντας υπόψιν ότι η οικονομία ενός κράτους είναι άμεσα συνδεδεμένη με την ευημερία του, τις κοινωνικές παροχές, την ισχύ του και την εξασφάλιση της εθνικής του ασφάλειας, συνειδητοποιούμε ποσό σημαντική είναι στις μέρες μας η μελέτη της οικονομικής κατασκοπείας. Ο Samuel D. Porteous, αναλυτής ασφαλείας της καναδικής ασφάλειας Υπηρεσία πληροφοριών, στον όρο «οικονομική κατασκοπεία» αναφέρεται στις «κρυφές ή παράνομες απόπειρες ξένων να βοηθήσουν τα οικονομικά τους συμφέροντα αποκτώντας οικονομικά πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για να σαμποτάρουν ή να επηρεάσουν με άλλο τρόπο την οικονομική ασφάλεια άλλης χώρας». Ο Randall M. Fort, επί του παρόντος Διευθυντής Προγράμματος Ασφαλείας, ορίζει την οικονομική κατασκοπεία ως απόκτηση πληροφοριών με μυστικά μέσα, σχετικά με την οικονομία, το εμπόριο και την πνευματική ιδιοκτησία. Ο Hedieh Nasheri, καθηγητής Εγκληματολογίας και Δικαιοσύνης στο Τμήμα Κοινωνιολογίας του Πανεπιστημίου Kent State, η οικονομική κατασκοπεία ορίζεται όταν ένα έθνος συλλέγει οικονομικά δεδομένα από ένα άλλο έθνος.

Εμβαθύνοντας λοιπόν στην έννοια της οικονομική κατασκοπεία, παρατηρούμε ότι διακρίνεται σε τρία επίπεδα: την μακροοικονομική κατασκοπεία (macroeconomic espionage), την μικροοικονομική κατασκοπεία (microeconomic espionage) και την οικονομική αντικατασκοπεία (economic counterespionage) *(J. C. Evans, 1994).* Η μακροοικονομική κατασκοπεία, αναφέρεται στη χρήση μυστικών υπηρεσιών για λογαριασμό της κυβέρνησης προκειμένου να αποκτήσει πληροφορίες σχετικά με τις παγκόσμιες οικονομικές εξελίξεις και δραστηριότητες. Σκοπός είναι η ενίσχυση της πολιτικής ηγεσίας να ασκήσει και να διαμορφώσει ορθά την εσωτερική και εξωτερική οικονομική της πολιτική. Κατά την μικροοικονομική κατασκοπεία, η κυβέρνηση ενός κράτους μέσω των μυστικών του υπηρεσιών της συμμετέχει στη συλλογή πληροφοριών για να βοηθήσει μια εταιρεία (συνήθως πολυεθνική), δημιουργώντας μια συνεργασία μεταξύ της κυβέρνησης και της εταιρείας, στόχος της οποίας είναι να επικρατήσει

έναντι κάποιου ανταγωνιστή της στη διεθνή οικονομική σκηνή. Σχετικά με τον όρο οικονομική αντικατασκοπεία, αναφερόμαστε στην προστασία των οικονομικών, εμπορικών και τεχνολογικών μυστικών, καθώς και την εξουδετέρωση ξένων υπηρεσιών πληροφοριών που αποσκοπούν στην υποκλοπή αυτών των πληροφοριών *(Randall M. Fort, 1995, Evans J. C., 1995).*

Παρόλα αυτά η έννοια της οικονομικής κατασκοπείας διαφοροποιείται από τη στρατιωτική και βιομηχανική. Η στρατιωτική κατασκοπεία αφορά την έγκαιρη και έγκυρη προειδοποίηση ενός κράτους σχετικά με τις προθέσεις ενός άλλου κράτους για να διαπράξει στρατιωτικές επιχειρήσεις εις βάρους του. Επιπλέον η βιομηχανική κατασκοπεία ασκείται μεταξύ επιχειρήσεων χωρίς την εμπλοκή κυβερνήσεων ή άλλου κυβερνητικού οργανισμού και αφορά τη δραστηριότητα συλλογής πληροφοριών από μία ιδιωτική επιχείρηση άλλης χώρας, με σκοπό την απόκτηση εμπορικών μυστικών πληροφοριών και στοιχείων. Η διαφορά των τριών εννοιών είναι σαφής, έχοντας ωστόσο ως κοινό παρονομαστή τη συλλογή πληροφοριών.

2.6 Κύκλος Πληροφοριών

Ο κύκλος πληροφοριών αποτελεί μια διαδικασία, αποκορύφωμα της οποίας είναι το τελικό προϊόν που θα προκύψει μέσα από αυτήν. Η διαδικασία αυτή αποτελεί ένα συνεχόμενο κύκλο ο οποίος περιλαμβάνει το σχεδιασμό και τη διεύθυνση, τη συλλογή πληροφοριών, την επεξεργασία των πληροφοριών και την ανάλυση των πληροφοριών με τελικό σκοπό την παραγωγή του τελικού προϊόντος και τη διανομή του στους λήπτες αποφάσεων. Ωστόσο η διαδικασία αυτή δεν τελειώνει ποτέ. Οι ραγδαίες εξελίξεις και αλλαγές που πραγματοποιούνται στο διεθνές περιβάλλον, σε συνδυασμό με τον αντίκτυπο που έχουν στην εκάστοτε κατάσταση, αναγκάζουν τη συνεχή λειτουργία του κύκλου μέσω της ανατροφοδότησης, και την επανεκκίνηση της διαδικασίας με νέα και ίσως διαφορετικά δεδομένα.

Το τελικό προϊόν που θα προκύψει θα πρέπει κάθε φορά να απαντά στα εξής ερωτήματα: (1) ποιος θα κάνει κάτι, (2) εάν θα το κάνει (εκτίμηση πιθανότητας της δράσης), (3) τι θα κάνει (ποια θα είναι η δράση του), (4) που θα το πράξει (προσδιορισμός της θέσης), (5) πότε θα γίνει (εκτίμηση χρονοδιαγράμματος της δράσης) και (6) γιατί θα το κάνει (προσδιορισμός του κινήτρου πίσω από την πρωτοβουλία). Όλη αυτή η διαδικασία αποτελεί ένα σημαντικό παράγοντα εκτίμησης και αντιμετώπισης μελλοντικής πολιτικής.

2.7 Μέσα-Κατηγορίες συλλογής πληροφοριών

Μέσα συλλογής πληροφοριών καθορίζουμε τα μέσα που χρησιμοποιούνται για να συλλέξουμε πληροφορίες. Αυτά κατηγοριοποιούνται ανάλογα με τον τρόπο συλλογής και τη φύση τους. Τα βασικά μέσα συλλογής πληροφοριών είναι από: (1) ανοιχτές πηγές OSINT (Open Source Intelligence), όπου αφορούν πληροφορίες που δημοσιεύονται ανοιχτά στο διαδίκτυο, εφημερίδες, περιοδικά, καθώς και ομιλίες, συνεντεύξεις και επίσημα έγγραφα που κοινοποιούνται, (2) social media SOCMINT (Social Media Intelligence), όπου είναι πληροφορίες που συλλέγονται σε πλατφόρμες κοινωνικής δικτύωσης όπως Facebook, Twitter, Instagram κ.λπ. (3) φωτογραφίες IMINT (Imagery Intelligence), όπως δορυφορικές εικόνες, αεροφωτογραφίες, ηλεκτρονικές εικόνες κ.α. (4) σήματα SIGINT (Signals Intelligence), που αφορούν πληροφορίες που προέρχονται από την παρεμπόδιση επικοινωνιών και άλλων ηλεκτρονικών σημάτων. Υποκατηγορίες του SIGINT είναι το ELINT (Electronic Intelligence), πληροφορίες που μπορούν να αποκτηθούν από την παρακολούθηση ηλεκτρονικών μαγνητικών ακτινοβολιών από στρατιωτικό εξοπλισμό, το TELINT (Telemetry Intelligence) για πληροφορίες που αποκτήθηκαν από την παρακολούθηση της τηλεμετρίας, όπου στη σήμερον εποχή έχει αντικατασταθεί με τον όρο FISINT (Foreign Instrumentation Signals Intelligence) που αφορά την παρακολούθηση ξένων ηλεκτρομαγνητικών εκπομπών και το COMINT (Communications Intelligence) που αφορά πληροφορίες από την παρακολούθηση τηλεφωνικών κλήσεων, μηνυμάτων κειμένου, ραδιοεπικοινωνιών και του διαδικτύου, (5) μετρήσεις και ηλεκτρονικές υπογραφές MASINT (Measurement and Signatures Intelligence) που προέρχονται από συσκευές ανίχνευσης όπως σεισμόμετρα, σόναρ και αισθητήρες που χρησιμοποιούνται για την ανίχνευση αντικειμένων όπως ναρκωτικών και εκρηκτικών και (6) ανθρώπινες πηγές HUMINT (Human Intelligence), όπου αφορά πληροφορίες που λαμβάνονται από τη χρήση ανθρώπινων παραγόντων ή πληροφοριοδοτών. Σε αυτή την κατηγορία συμπεριλαμβάνεται η κατασκοπεία/μυστική δράση και κατά επέκταση η οικονομική κατασκοπεία.

3. Η Οικονομική κατασκοπεία στο πέρασμα του χρόνου

Κατά την αναζήτηση της παγκόσμιας βιβλιογραφίας και ιστορίας, οι οικονομικές και τεχνολογικές-επιστημονικές πληροφορίες κατείχαν πάντα καθοριστικό ρόλο στη εξέλιξη της παγκόσμιας ιστορίας, αποδεικνύοντας ότι η οικονομική κατασκοπεία δεν αποτελεί μια σύγχρονη κρατική δραστηριότητα, αλλά ένα ιστορικά διαχρονικό φαινόμενο.

Η πρώτη ιστορικά περίπτωση κατασκοπείας που συγκαταλέγεται στα περιστατικά μακροοικονομικής κατασκοπείας, είναι του Μωυσή και των δώδεκα απεσταλμένων του, με σκοπό τη συλλογή πληροφοριών όχι μόνο σχετικά με την άμυνα της πόλης Χαναάν, αλλά και με την ποιότητα του εδάφους και τη διαπίστωση της εύφορης γης. Αξιοσημείωτο είναι ότι υπηρεσίες πληροφοριών του 20ου αιώνα προσπάθησαν να αντλήσουν μαθήματα από τη βιβλική αφήγηση της κατασκοπείας στην εποχή του Μωυσή, κάτι που αποδεικνύεται και από μελέτη του 1978 στο διαβαθμισμένο εσωτερικό περιοδικό της CIA, «Ένα μάθημα της Βίβλου για Κατασκοπεία», όπου ο συγγραφέας, John M.Cardwell, είδε αναλογίες σχετικά με τις κατασκοπευτικές αναφορές του Μωυσή για την Χαναάν και τα δεινά της CIA στα μέσα της δεκαετίας του 1970. Επιπλέον ο Efraim Halevy, πρώην επικεφαλής της Mossad, σε συνέντευξή του στις 11 Μαρτίου 2013 ανέφερε ότι σε συνομιλίες με νέους νεοσύλλεκτους στις αρχές του 21ου αιώνα, φέρει ως παράδειγμα προς μίμηση την αφοσίωση στην αποστολή των απεσταλμένων του Μωυσής για να κατασκοπεύσει τη γη της Χαναάν *(Andrew, 2018).*

Πιο χαρακτηριστικά το 551 μ.Χ., ο αυτοκράτορας Ιουστινιανός διέταξε μοναχούς που γνώριζαν την Άπω Ανατολή, να κλέψουν μεταξοσκώληκες από την Κίνα, «μία από τις μεγαλύτερες επιτυχίες οικονομικής κατασκοπείας στην ιστορία, μέσω της οποίας το Βυζάντιο απεξαρτήθηκε από εισαγωγές μεταξιού». Επιπλέον από το 1250 μ.Χ. η Βενετία δημιούργησε το τελειότερο σύστημα συλλογής πληροφοριών, λαμβάνοντας πληροφορίες σχετικά με νέες τεχνολογίες που αναπτύσσονταν στον τότε πολιτισμένο κόσμο. Τέλος η κλοπή μυστικού κατασκευής της πορσελάνης στην Κίνα, από τον Πατέρα Francis Xavier d' Entrecolles, το 1712 μ.Χ. μετά από επίσκεψη στη μυστική πόλη King-t tchen. Μυστικό όπου μετέπειτα κλάπηκε από Άγγλο κατάσκοπο που κατάφερε να διεισδύσει στο γαλλικό εργοστάσιο, δίνοντας στην Αγγλία τη δυνατότητα να ηγηθεί στην αγορά της πορσελάνης. *(Κωνσταντόπουλος Ι., 2010).*

Από τις αρχές του 20ου αιώνα, η κατασκοπεία αποτέλεσε διαχρονικά τον ¨άσσο στο μανίκι¨ για τους πολιτικούς ηγέτες. Η Βρετανία, η Γερμανία, η Γαλλία, οι ΗΠΑ, η ΕΣΣΔ, η Ιαπωνία και τη Κίνα αποτέλεσαν χώρες αρκετά ενεργές στον τομέα της οικονομικής κατασκοπείας. Διπλοί πράκτορες, μισθοφόροι πληροφοριοδότες, διπλωμάτες, κατάσκοποι με πολλαπλές ταυτότητες και διαβατήρια, πολίτες πάσης υποψίες αποτέλεσαν το μοτίβο της εποχής εκείνης, έχοντας όλοι ένα κοινό σκοπό, τη συλλογή πληροφοριών στρατιωτικής, οικονομικής και τεχνολογικής φύσεως.

Μετά τα μαθήματα του Ά Παγκοσμίου Πολέμου, παρατηρούμε μια έξαρση άσκησης οικονομικής κατασκοπείας, με τις οικονομικές πληροφορίες να συμβάλλουν καθορίστηκα στις εξελίξεις του Β΄ Παγκοσμίου Πολέμου. Η συλλογή πληροφοριών σχετικά με την παραγωγή ρουλεμάν και βολφραμίου, το λαθρεμπόριο, τον εφοδιασμό σιδηρομεταλλευμάτων, τη μεταφοράς υλικών-εφοδίων, τη δημιουργία νέων τεχνολογικών συστημάτων κ.α., αποτέλεσαν θέματα υψίστης σημασίας για τους λήπτες αποφάσεων και την εν τέλει διεξαγωγή του πολέμου. Οι Βρετανοί μάλιστα δημιούργησαν Επιτροπή Οικονομικού Πολέμου για τη μελέτη της ιαπωνικής οικονομίας και από τη μεριά της η Γερμανία ανέπτυξε σε μεγάλο βαθμό τη συλλογή οικονομικών, επιστημονικών-τεχνολογικών πληροφοριών. Το 1981, ο Pierre Marion, επικεφαλής των γαλλικών μυστικών υπηρεσιών, ανέφερε ότι η άσκηση οικονομικής κατασκοπείας αποτελεί μια φυσιολογική δραστηριότητα και οι συμμαχίες γίνονται για αμυντικά θέματα, καθώς στους τομείς της τεχνολογίας και της οικονομίας είμαστε όλοι ανταγωνιστές. Την ίδια περίοδο ο πρόεδρος της Γαλλίας Francois Mitterrand συμπεριέλαβε την βελτίωση των οικονομικών, τεχνολογικών και βιομηχανικών πληροφοριών στην τρίτη θέση προτεραιοτήτων *(Κωνσταντόπουλος Ι., 2010).*

Η οικονομική κατασκοπεία με την πάροδο των χρόνων αποτέλεσε «το πιο καυτό τρέχον θέμα στην πολιτική των υπηρεσιών πληροφοριών», όπως ανέφερε ο James R. Woolsey ως Διευθυντής της CIA το 1993 *(Strong, 1994).* Ας δώσουμε ωστόσο έμφαση σε δύο χώρες όπου οι έννοιες ¨οικονομική κατασκοπεία και ασφάλεια¨ έχουν αποτελέσει σημαντικό παράγοντα όχι μόνο μελέτης και ανάλυσης, αλλά και λήψης πολιτικών αποφάσεων, στις ΗΠΑ και στην Κίνα.

3.1 ΗΠΑ εναντίον ΚΙΝΑΣ

Η οικονομική κατασκοπεία έχει απασχολήσει έντονα την τελευταία 20ετία της ΗΠΑ και την Κίνα. Περιστατικά οικονομικής κατασκοπείας μεταξύ των δύο χωρών από την περίοδο εκείνη θα μας επιβεβαιώσουν όχι μόνο την ύπαρξη ανάμεσά τους, αλλά και το εύρος και τη συχνότητά της. Η συλλογή των παρακάτω περιστατικών βασίστηκε κυρίως σε έκθεση του Εκτελεστικού γραφείου του Προέδρου των ΗΠΑ το 2013 «Διοικητική στρατηγική για τον μετριασμό της κλοπής των εμπορικών μυστικών των ΗΠΑ», σε

πολυετή έρευνα που πραγματοποίησε το CSIS (Center of strategic & International Studies) με τη συμβολή των Evan Burke, Matthew Serrone, Khristal Thomas, Arthur Nelson, Ian Haimowitz and David Robusto, σε άρθρο του Mattis Peter L. το 2012 (International Journal of Intelligence and CounterIntelligence) και σε άρθρο του Holt Alexander το 2020 (MIT technology review).

Το 2003 Κινέζοι χάκερς αποκάλυψαν πληροφορίες εθνικής ασφάλειας από το σταθμό Naval Air Weapons Station China Lake, συμπεριλαμβανομένων δεδομένων δοκιμών και σχεδιασμού πυρηνικών όπλων, καθώς και δεδομένων αεροσκαφών stealth.

Το 2005, ο Chi Mak, πολιτογραφημένος Αμερικάνος γεννημένος στην Κίνα, και Κινέζοι πράκτορες πληροφοριών συλλέγουν τεχνικές πληροφορίες για τις τρέχουσες και μελλοντικές τεχνολογίες πλοίου του Πολεμικού Ναυτικού. Ο Chi Mak σκόπευε να εξάγει τις πληροφορίες στην Κίνα μέσω του αδερφού του, αλλά συνελήφθη και καταδικάστηκε. Επιπλέον ο Moo Ko-Suen, εκπρόσωπος μιας αμερικανική αεροδιαστημική εταιρεία για 10 χρόνια στην Ταϊβάν, ενήργησε ως αντιπρόσωπος της κινεζικής κυβέρνησης και προσπάθησε να αγοράσει εξελιγμένα στρατιωτικά ανταλλακτικά και όπλα, συμπεριλαμβανομένου κινητήρα μαχητικού αεροσκάφους F-16 και βλήματα, για την Κίνα.

Τον 2006, Κινέζοι χάκερς διείσδυσαν σε δίκτυα της NASA, τα οποία διαχειρίζονται οι Lockheed Martin και Boeing και απέσπασαν πληροφορίες σχετικά με το πρόγραμμα Space Shuttle Discovery.

Το 2007, Κινέζοι χάκερς παραβίασαν το έργο Joint Strike Fighter του Πενταγώνου κλέβοντας δεδομένα σχετικά με το μαχητικό F-35. Επιπλέον έκλεψαν με επιτυχία πληροφορίες από το Εθνικό Εργαστήριο Oak Ridge, το Εθνικό Εργαστήριο Los Alamos και την Εθνική Διοίκηση Πυρηνικής Ασφάλειας.

Το 2008, ο Tai Shen Kuo, πολίτης των ΗΠΑ, συνελήφθη επειδή παρέσχε στην Κίνα διαβαθμισμένες πληροφορίες από έναν αναλυτή πολιτικών συστημάτων όπλων του Πενταγώνου, τον Gregg Bergersen. Επίσης Κινέζοι αξιωματούχοι εισήγαγαν λογισμικό υποκλοπής spyware σε φορητό υπολογιστή του Υπουργού Εμπορίου των ΗΠΑ Carlos Gutierrez κατά τη διάρκεια εμπορικής αποστολής.

Από το 2009, η Κίνα πραγματοποίησε μια σειρά επιθέσεων στον κυβερνοχώρο για να κλέψει πληροφορίες εμπορικού μυστικού από δεκάδες αμερικανικές εταιρείες, συμπεριλαμβανομένων των Google, Yahoo, Adobe, Dow Chemical, Morgan Stanley, καθώς επίσης διεισδύθηκαν στα δίκτυα υπολογιστών της Coca-Cola και έκλεψαν πληροφορίες σχετικά με το εμπορικό απόρρητο.

Το 2010, ο Dongfan “Greg” Chun, αποτέλεσε το πρώτο πρόσωπο που καταδικάστηκε στο πλαίσιο του νόμου περί Οικονομικής κατασκοπείας, σε 15 χρόνια φυλάκισης. Από το 1970, είχε μεταφέρει διαβαθμισμένες πληροφορίες για το βομβαρδιστικό αεροσκάφος B-1, το μαχητικό αεροσκάφος F-15, το ελικόπτερο Chinook, το πρόγραμμα διαστημικών λεωφορείων των ΗΠΑ και τον πύραυλο Delta IV, ενώ εργαζόταν για τη Rockwell και, αργότερα, την Boeing. Ο Chun βρέθηκε να έχει εκατομμύρια δολάρια πωλώντας μυστικά στην Κίνα.

Το 2011 Κινέζοι χάκερς κατάφεραν να διεισδύσουν σε τουλάχιστον 48 εταιρείες χημικών και άμυνας, κλέβοντας εμπορικές και ευαίσθητες στρατιωτικές πληροφορίες.

Το 2012, Κινέζοι χάκερς έκλεψαν διαβαθμισμένες πληροφορίες σχετικά με τις τεχνολογίες του F-35 Joint Strike Fighters.

Το 2014, ο Amin Yu έκλεψε συστήματα και εξαρτήματα για θαλάσσια υποβρύχια οχήματα από κατασκευαστές των ΗΠΑ προς όφελος μιας κρατικής οντότητας στην Κίνα. Το Μάιο, το Υπουργείο Δικαιοσύνης των ΗΠΑ ανακοινώνει το κατηγορητήριο πέντε Κινέζων στρατιωτών, που ανήκουν στη Μονάδα 61398, για κλοπή πνευματικής ιδιοκτησίας, επιχειρηματικά σχέδια και στρατηγικές διαπραγματεύσεων από εταιρείες (Westinghouse και US Steel), για να βοηθήσουν ανταγωνιστικές κινεζικές κρατικές εταιρείες. Τον Ιούνιο, ο Su Bin, ένας Κινέζος υπήκοος που διευθύνει μια αεροδιαστημική εταιρεία στον Καναδά, συνελήφθη εξ ονόματος της κυβέρνησης των ΗΠΑ επειδή βοήθησε δύο Κινέζους στρατιώτες κλέβουν πληροφορίες για το αεροσκάφος C-17 και τα μαχητικά F-22 και F-35. Το κινεζικό φορτηγό αεροπλάνο Xian Y-20, που παρουσιάστηκε το 2014, εμφανίζει μια αξιοσημείωτη ομοιότητα με το C-17. Έπειτα το Σεπτέμβριο, η T-Mobile υποβάλλει αγωγή εναντίον της Huawei ισχυριζόμενη ότι έκλεψαν οι υπάλληλοί της λογισμικό και υλικό από ένα εργαστήριο της, συμπεριλαμβανομένου ενός ρομποτικού χεριού. Το 2019 η δικαιοσύνη των ΗΠΑ κατηγορεί την Huawei για κλοπή σκόπιμων εμπορικών μυστικών από την T-Mobile, έχοντας στην κατοχή της email που δείχνουν ότι η Huawei προσέφερε υπαλλήλους μπόνους για κλοπή τεχνολογίας από άλλες εταιρείες.

Το 2015, αποδείχθηκε ότι Κινέζοι αξιωματικοί πληροφοριών διείσδυσαν σε δίκτυα αποκτώντας πληροφορίες εμπορικού μυστικού, σχετικά με κινητήρες turbofan από αμερικανικές και ευρωπαϊκές αεροδιαστημικές εταιρείες.

Το 2018, πρώην πράκτορας της CIA, Jerry Chun Shing Lee, συνελήφθη στο αεροδρόμιο JFK για συνεργασία με Κινέζους πράκτορες. Σύμφωνα με εισαγγελείς, οι πληροφορίες του Lee βοήθησαν στη διάλυση του δικτύου της CIA στην Κίνα το 2010. Επιπλέον τον Οκτώβριο, ο Yanjun Xu, αξιωματικός πληροφοριών του κινεζικού Υπουργείου Κρατικής

Ασφάλειας, συνελήφθη στο Βέλγιο και εκδόθηκε στο Ηνωμένες Πολιτείες για απόπειρα κλοπής των σχεδίων των λεπίδων του ανεμιστήρα Jet από τη General Electric.

Το 2019, ο Πρόεδρος Τραμπ εκδίδει εκτελεστική εντολή που απαγορεύει στις εταιρείες των ΗΠΑ την πώληση εξοπλισμού στην Huawei, αναφέροντας ότι ενέχει κίνδυνο στην εθνική ασφάλεια.

Το 2020, ο Charles Lieber, επικεφαλής του τμήματος χημείας του Πανεπιστημίου του Χάρβαρντ και πρωτοπόρος στο νανοτεχνολογία, κατηγορείται για ψεύτικους ισχυρισμούς σχετικά με την αποδοχή χρημάτων από την κινεζική κυβέρνηση. Ο Lieber είναι ο υψηλότερου προφίλ ακαδημαϊκός που έχει συλληφθεί για σύνδεση με την κινεζική-αμερικανική τεχνολογική αντιπαλότητα. Τον Ιουλίου 2020, η κυβέρνηση Τραμπ διατάζει το κλείσιμο του προξενείου της Κίνας το Χιούστον, «για την προστασία της αμερικανικής πνευματικής ιδιοκτησίας και των αμερικανικών προσωπικών πληροφοριών», ισχυριζόμενος ότι το προξενείο έχει συντονίζει τη βιομηχανική κατασκοπία εναντίον των ΗΠΑ. Η Κίνα σε αντίποινα κλείνει τον Αμερικανό προξενείο στο Chengdu.

Από τις παραπάνω έρευνες και τα ενδεικτικά περιστατικά που αναφέρθηκαν, διαπιστώνουμε μία έντονη δραστηριότητα οικονομικής κατασκοπείας που ασκείται κυρίως από την Κίνα στις ΗΠΑ, με αποκορύφωμα την τελευταία δεκαετία. Ενδεικτικό είναι ότι σε σύνολο είκοσι ετών, στο διάστημα 2000-2009 παρουσιάζονται περίπου το 26% των περιστατικών, ενώ στο διάστημα 2010-2020 το 74% αυτών.

4. Κίνητρα - αντικίνητρα οικονομικής κατασκοπείας

Έχοντας ως γνώμονα τα περιστατικά οικονομικής κατασκοπείας των χωρών ενδιαφέροντος μας, καθώς και τα διαχρονικά παραδείγματα της, οδηγούμαστε στο ερώτημα: «*Ποια λοιπόν είναι τα κίνητρα και τα αντικίνητρα που ωθούν τους υπευθύνους χάραξης πολιτικής και λήξης αποφάσεων στη διεξαγωγή της μακροοικονομικής και μικροοικονομικής κατασκοπείας;».*

4.1 Μακροοικονομική κατασκοπεία

4.1.1 Κίνητρα

Αναζητώντας στη διεθνή βιβλιογραφία, όπως αναφέρει και ο Διδάκτωρ Διεθνών Σχέσεων και Στρατηγικών Σπουδών καθηγητής Κωνσταντόπουλος Ι., τα κίνητρα μπορούν να διαχωρισθούν σε τρείς κατηγορίες: «Αποτελεσματικότερη παρακολούθηση των διεθνών οικονομικών και τεχνολογικών παγκόσμιων εξελίξεων», «Οικονομικά οφέλη», και «Κίνητρα που σχετίζονται με την κοινότητα υπηρεσιών πληροφοριών» *(Κωνσταντόπουλος, 2010).*

Η πρώτη κατηγορία αφορά τη στοχευμένη και αποτελεσματική παρακολούθηση των διεθνών εξελίξεων στον οικονομικό και τεχνολογικό τομέα. Σύμφωνα με τον Robert Galvan η μακροοικονομική κατασκοπεία οφείλει να συμβαδίζει με τις νέες οικονομικές και τεχνολογικές εξελίξεις, ικανοποιώντας τις ανάγκες των διαμορφωτών αποφάσεων. Οι ραγδαίες εξελίξεις της τεχνολογίας, οι νέες οικονομικές τάσεις, οι διακρατικές οικονομικές συνεργασίες, οι διμερής συνεργασίες ανταλλαγής τεχνολογικής γνώσης, οι οικονομικές και μη διαπραγματεύσεις μεταξύ των χωρών και η κατανόηση της στρατηγικής των ανταγωνιστών στον οικονομικό και τεχνολογικό τομέα, αποτελούν ένα ¨άσσο¨ στο μανίκι των διαμορφωτών αποφάσεων και των πολιτικών ηγεσιών (policymakers). Οι υπηρεσίες πληροφοριών αποτελούν το πρωταρχικό τοίχος αμύνης μια χώρας και είναι υπεύθυνοι για την έγκαιρη και έγκυρη πληροφόρηση των διαμορφωτών αποφάσεων. Η παρακολούθηση και η πληροφόρηση των παγκόσμιων οικονομικών και τεχνολογικών τάσεως και εξελίξεων είναι μείζονος σημασίας για τη διατήρηση και την εξασφάλιση της εθνική ασφάλεια ενός κράτους. Από το 13ο αιώνα ο κινέζος στρατηγός Tzu Sun είχε αναφερθεί στον τομέα της κατασκοπείας αναφέροντας

τη σημαντικότητα της γνώσεις των δυνατοτήτων του αντιπάλου, κάτι το οποίο ακόμα και στις μέρες μας έχει μεγάλο αντίκτυπο στον παγκόσμιο αγώνα υπεροχής *(Galvan, 1995), (Κωνσταντόπουλος, 2010).*

Η δεύτερη κατηγορία αναφέρεται στη διαφορά οικονομικού οφέλους και κόστους. Η επένδυση στην έρευνα, στην ανάπτυξη, στη δημιουργία νέων τεχνολογιών, η πραγματοποίηση πειραμάτων και γενικότερα η δημιουργία κάτι νέου απαιτεί μεγάλο κόστος για ένα κράτος αναλογικά με την υποκλοπή οικονομικών πληροφοριών. Το διαδίκτυο στις μέρες μας αποτελεί το πιο φθηνό μέσο υποκλοπής, παρακολουθήσεις και άσκησης κατασκοπείας, κάτι το οποίο γνωρίζουν οι μεγάλες δυνάμεις. Επιπλέον η αποκόμιση οικονομικού οφέλους δεν αφορά μόνο την εξοικονόμηση πόρων, αλλά και την αποτροπή οικονομικής χρεωκοπίας. Όπως αναφέρει ο καθηγητής Κωνσταντόπουλος Ι., «..μια κλασική περίπτωση αποκόμισης σημαντικού οφέλους με ελάχιστο κόστος..», όπου αποτελεί ακόμα και στις μέρες ένα χαρακτηριστικό παράδειγμα πρόληψης και προσαρμογής στην παγκόσμια οικονομία, είναι η εκμετάλλευση της έγκυρης πληροφόρησης από τις γαλλικές μυστικές υπηρεσίες το 1971, σχετικά με την υποτίμηση του δολαρίου *(Κωνσταντόπουλος, 2010).*

Η τρίτη κατηγορία αναφέρεται στην ισχυρή υπεροχή των υπηρεσιών πληροφοριών σε σύγκριση με άλλες υπηρεσίες της κυβέρνησης. Ο τρόπος συλλογής πληροφοριών, οι μεθόδους, οι αναλύσεις και γενικότερα οι προσβάσεις που διαθέτουν, υποστηρίζουν την πολιτική ηγεσία και τους διαμορφωτές αποφάσεων στη λήψη αποφάσεων *(Κωνσταντόπουλος, 2010).* Οι μυστικές υπηρεσίες αποτελούν την πρώτη γραμμή αμύνης ενός κράτους μέσω της έγκυρης και έγκαιρης πληροφόρησης, κάτι το οποίο οι υπόλοιπες κυβερνητικές υπηρεσίες δε μπορούν να προσφέρουν.

4.1.2 Αντικίνητρα

Τα αντικίνητρα που αποτρέπουν τα κράτη στην άσκηση μακροοικονομικής κατασκοπείας κατηγοριοποιούνται ως εξής: «πολιτικά–διπλωματικά αντικίνητρα», «αντικίνητρα σχετικά με την κοινότητα των υπηρεσιών πληροφοριών» και «πρακτικά αντικίνητρα» *(Κωνσταντόπουλος, 2010).*

Τα πολιτικά-διπλωματικά αντικίνητρα που προκύπτουν, αφορούν τη δημιουργία αρνητικών εκβάσεων στις διπλωματικές και πολιτικές σχέσεις του κράτους που την ενεργή. Οι διμερής και πολυμερής διπλωματικές σχέσεις δύναται να κλονιστούν, καθώς το διεθνές οικονομικό περιβάλλον εναλλάσσεται συνεχώς. Η δημιουργία νέων οικονομικών συμμαχιών είναι εμφανής στο παγκόσμιο προσκήνιο. Οικονομικές συμμαχίες διαφορετικές από τις παλαιότερες ήδη υπάρχουσες, με αποτέλεσμα η υπόνοια άσκησης οικονομικής κατασκοπείας να τείνει να διχάσει τις χώρες. Όπως αναφέρει ο Porteous Samuel, είναι αναπόφευκτο να εξασθενίσουν παλαιότερες

πολιτικές και στρατιωτικές συμμαχίες, από τη στιγμή που οι χώρες εμπλέκονται σε διαφορετικές ανταγωνιστικές οικονομικές συνεργασίες και σε ανταγωνιστικά δίκτυα συλλογής οικονομικών πληροφοριών *(Porteous Samuel, 1993).*

Τα αντικίνητρα που αφορούν την κοινότητα των υπηρεσιών πληροφοριών, αναφέρονται στην άποψη πολιτικών και αναλυτών των ΗΠΑ, ότι οι υπηρεσίες πληροφοριών δημιουργήθηκαν για να διασφαλίσουν την εθνική ασφάλεια της χώρας, και όχι για τη μελέτη της διεθνούς οικονομίας *(Κωνσταντόπουλος, 2010).* Ο Michael Herman, πρώην βρετανός αξιωματικός πληροφοριών και ακαδημαϊκός, ανέφερε: «Οι υπηρεσίες πληροφοριών αναπτύχθηκαν κυρίως στον τομέα της εθνικής ασφάλειας και πρέπει να περιορισθούν στη δουλειά τους». Πολλές είναι οι αναφορές και οι απόψεις σχετικά με την εξειδίκευση και τις γνώσεις που πρέπει να διακατέχει έναν αναλυτή οικονομικών πληροφοριών. Παρότι ο Porteous Samuel υποστηρίζει ότι ίδιες τεχνικές με τη συλλογή στρατιωτικών μπορούν να χρησιμοποιηθούν στη συλλογή οικονομικών πληροφοριών, σύμφωνα με τον Lock Johnson η συλλογή πληροφοριών από ανοιχτές πηγές είναι καλύτερες από τους κατάσκοπους, δεδομένου ότι το 90% με 95% των πληροφοριών προέρχεται από αυτές *(Johnson, 2000).*

Τα πρακτικά αντικίνητρα προκύπτουν από τα προβλήματα της ανάλυσης λόγω της πολυπλοκότητας του οικονομικού και τεχνολογικού τομέα και σε συνδυασμό με την εκάστοτε πολιτική βούληση. Μια πληροφορία οικονομικού ενδιαφέροντος δεν είναι μια πληροφόρηση που από μόνη της δύναται να μας οδηγήσει σε κάποιο επιθυμητό αποτέλεσμα. Το ζητούμενο είναι μέσα από αυτήν να αναλυθεί η τάση, οι προθέσεις του αντιπάλου ανταγωνιστή και οι στόχοι του. Μια διαδικασία δύσκολη και χρονοβόρα που απαιτεί προσοχή, ορθή κρίση κα γνώσεις *(Κωνσταντόπουλος, 2010).* Γενικότητα στην κατηγορία αυτή εντάσσονται όλες εκείνες οι αντικειμενικές δυσκολίες που εμπεριέχονται στην ανάλυση μιας οικονομικής πληροφορίας, τα αποτελέσματα αυτής σε τι μονοπάτια θα μας οδηγήσουν, τα ερωτήματα αν δύνανται να απαντηθούν και γενικότερα οι δυσκολίες που υπάρχουν ανάμεσα στο συντονισμό των μυστικών υπηρεσιών και των υπουργείων οικονομικών και ανάπτυξης. Η χρυσή τομή των πρακτικών αντικινήτρων είναι ο ορθός συντονισμός των υπηρεσιών, η σωστή χρήση των μυστικών υπηρεσιών αφενός μεν για την επίτευξη των στόχων της πολιτικής ηγεσίας και αφετέρου την αποφυγή ενός οικονομικού και τεχνολογικού αιφνιδιασμού.

4.2 Μικροοικονομική κατασκοπεία

4.2.1 Κίνητρα

Μεταβαίνοντας στην μικροοικονομική κατασκοπεία, αναζητούμε αρχικά τα κίνητρα άσκησης της. Οι δύο κύριες κατηγορίες που διαπιστώνονται είναι «οικονομικά κίνητρα» και «κίνητρα που σχετίζονται με την κοινότητα των υπηρεσιών πληροφοριών» *(Κωνσταντόπουλος, 2010).*

Στην πρώτη κατηγορία, αναζητούμε αν το κράτος πρέπει να επεμβαίνει στην ελεύθερη ιδιωτική αγορά και αν ναι σε ποιες περιπτώσεις. Οι απόψεις στη διεθνή βιβλιογραφία διίστανται, σύμφωνα με το Brander James A., Καναδός οικονομολόγος και καθηγητής του Διεθνούς Εμπορίου Ασίας-Ειρηνικού στο Πανεπιστήμιο της Βρετανικής Κολομβίας, «η κυβέρνηση μπορεί να παρέμβει σε τρείς περιπτώσεις: για να πετύχει τη μακροοικονομική σταθεροποίηση, να αναλάβει την οικονομική ανακατανομή για λόγους ισότητας και δικαιοσύνης και σε συγκεκριμένες συνθήκες δυσλειτουργίας/αποτυχίας της αγοράς *(Brander, 1998), (Κωνσταντόπουλος, 2010).* Σύμφωνα λοιπόν με τον Brander η αποτυχία της αγοράς είναι εκείνη που καθορίζει την επέμβαση του κράτους. Η συνεργασία κράτους και ιδιωτική επιχείρησης στις μέρες μας είναι ένα σύνηθες φαινόμενο, δεδομένου του παγκόσμιου οικονομικού ανταγωνισμού ο οποίος ωθεί τα κράτη σε τέτοιου είδους συνεργασίες, παρέχοντας ισχυρό πλεονέκτημα στην τεχνολογική ισχύ των κρατών. Οι τεχνολογικές εξελίξεις ιδιωτικών βιομηχανιών, οι νέες τεχνολογικές πρωτοτυπίες και οι διεθνείς επιτυχίες τους μπορούν να ενισχύσουν τόσο τη στρατιωτική όσο και την οικονομική δύναμη ενός κράτους. Η οικονομία, ευνοεί την τεχνολογία και αυτή το στρατιωτικό εξοπλισμό. Η Κίνα αποτελεί μια από τις χώρες όπου η συνεργασία της με ιδιωτικές επιχειρήσεις και η άσκηση μικροοικονομικής κατασκοπείας στις ΗΠΑ αποτελεί ένα δεδομένο, σε μια προσπάθεια αύξησης της οικονομικής και τεχνολογικής υπεροχής.

Η δεύτερη κατηγορία αναφέρεται στην ισχυρή υπεροχή των υπηρεσιών πληροφοριών σε σύγκριση με άλλες υπηρεσίες της κυβέρνησης. Ο τρόπος συλλογής πληροφοριών, οι μεθόδους, οι αναλύσεις και γενικότερα οι προσβάσεις που διαθέτουν και τα μέσα δε μπορούν να συγκριθούν με τις μειωμένες δυνατότητες του Υπουργείου Οικονομικών και Μεταφορών. Επιπλέον οι υπηρεσίες πληροφοριών μέσα από την άσκηση μικροοικονομικής κατασκοπείας μπορούν να λάβουν πληροφορίες σε εξειδικευμένους τομείς που μέσα από ανάλυση και μεθοδικότητα θα αποδώσουν ισχυρά αποτελέσματα.

4.2.2 Αντικίνητρα

Τα αντικίνητρα που προκύπτουν από την άσκηση μικροοικονομικής κατασκοπείας χωρίζονται σε έξι κατηγορίες: «πολιτικά-διπλωματικά», «οικονομικά», «νομικά», «πρακτικά αντικίνητρα», «αντικίνητρα που σχετίζονται με την κοινότητα των υπηρεσιών πληροφοριών» και «αντικίνητρα που σχετίζονται με την επιχειρηματική κοινότητα» *(Κωνσταντόπουλος, 2010).*

Η πρώτη κατηγορία αναφέρεται στο ότι τα κράτη που ασκούν μικροοικονομική κατασκοπεία διακινδυνεύουν τις σχέσεις τους με τους συμμάχους. Οι διμερής και πολυμερής διπλωματικές σχέσεις δύναται να κλονιστούν, στην προσπάθεια επικράτησης μέσα στον οικονομικό και τεχνολογικό ανταγωνισμό. Συμμαχικές χώρες στον αμυντικό τομέα εμφανίζονται ως ανταγωνίστριες χώρες στον τομέα της τεχνολογίας, εκεί που οι ισορροπίες των σχέσεων είναι λεπτές και χρήζουν προσοχή.

Η δεύτερη αφορά τα οικονομικά αντικίνητρα. Η επέμβαση ενός κράτους στην αγορά μπορεί να προκαλέσει προβλήματα και να οδηγήσει σε δυσλειτουργίες την αγορά. Ο McCurdy Dave, Αμερικάνος πολιτικός και δικηγόρος, αναφέρει ότι μακροπρόθεσμα μέσω της μικροοικονομικής κατασκοπείας ανταγωνιστικές βιομηχανίες που δεν έχουν την ανάγκη του κράτους θα αναζητούν μια κυβέρνηση που θα παρέχει «ένα δίκαιο, σταθερό και προβλέψιμο επιχειρηματικό περιβάλλον». Επιπλέον όπως αναφέρει ο Valero Larry, η μικροοικονομική κατασκοπεία επιδρά αρνητικά στο διεθνές εμπόριο, διαβρώνοντας «την επιστημονικής και τεχνολογική βάση ενός κράτους». Κάτι το οποίο ενδέχεται να αποθαρρύνει το κίνητρο δημιουργίας νέων τεχνολογιών από τις επιχειρήσεις όπου το κράτος ελέγχει και εκμεταλλεύεται τους πόρους της *(Κωνσταντόπουλος, 2010).*

Τα νομικά αντικίνητρα αναφέρονται στις παραβιάσεις που προκύπτουν σχετικά με το Δίκαιο Πνευματικής Ιδιοκτησίας (Intellectual Property Law), διατάξεις περί πνευματικής ιδιοκτησία της GAAT (General Agreement on Rates and Tariffs – Γενική Συμφωνία Δασμών και Εμπορίου), τον Παγκόσμιο Οργανισμό Πνευματικής Ιδιοκτησίας (World Intellectual Property Organization - WIPO), τον Παγκόσμιο Οργανισμό Εμπορίου (World Trade Organization) και άλλες συνθήκες και συμβάσεις αναφορικά με τα εμπορικά, πνευματικά και οικονομικά δικαιώματα *(Κωνσταντόπουλος, 2010).*

Στην κατηγορία των πρακτικών αντικινήτρων εντάσσονται οι δυσκολίες ως προς τον τρόπος λειτουργίας και οργάνωσης μιας τέτοιου είδους επιχείρησης, καθώς επίσης και το αρνητικό αντίκτυπο που ενδέχεται να έχει στις υπόλοιπες εγχώριες επιχειρήσεις. Επιπλέον αναπτύσσονται ερωτήματα όπως: Ποιες είναι οι κατάλληλες επιχειρήσεις που μπορούν να βοηθήσουν τις υπηρεσίες πληροφοριών; Σε ποιο μέρος θα πρέπει να βρίσκεται μια τέτοιου είδους επιχείρηση; Σε ποιους οικονομικούς τομείς θα μπορέσει η

εκάστοτε επιχείρηση να είναι αποτελεσματική για τις μυστικές υπηρεσίες; Τι ποσοστού κέρδους θα έχει το κράτος έναντι της επιχείρησης; Τι εθνικότητας θεωρείτε μια πολυεθνική επιχείρηση την εποχή της παγκοσμιοποίησης; Ένα από τα σημαντικότερα πρακτικά αντικίνητρα είναι η επίδραση στον εγχώριο ανταγωνισμό. Οι επιχειρήσεις που θα συμβάλλουν στη συλλογή οικονομικών πληροφοριών θα λαμβάνουν περισσότερα πλεονεκτήματα από το κράτος έναντι τον υπολοίπων. Επιπλέον σε περιπτώσεις όπου η συγκεκριμένη επιχείρηση είναι θυγατρική μίας ξένης επιχείρησης, θα υπάρχει η προνομιακή μεταχείριση της έναντι των εγχώριων επιχειρήσεων. Όπως αναφέρει ο Fort Randall είναι πιθανό τη μεγαλύτερη πολιτική υποστήριξη, να την απολαμβάνουν επιχειρήσεις που διαθέτουν τη μεγαλύτερη πολιτική επιρροή, «προσδίδοντας ένα αθέμιτο πλεονέκτημα στις ισχυρές επιχειρήσεις» *(Κωνσταντόπουλος, 2010).*

Η κατηγορία σχετικά με την κοινότητα των υπηρεσιών πληροφοριών, αφορά την αποστολή των υπηρεσιών πληροφοριών που σχετίζεται με την αντιμετώπιση απειλών ασφαλείας όπως η τρομοκρατία, η διασπορά όπλων μαζικής καταστροφής, το οργανωμένο έγκλημα και όχι την υποστήριξη πολυεθνικών εταιριών. Η οργάνωση και ο τρόπος ενεργείας των μυστικών υπηρεσιών δεν έχει σχεδιαστεί για να παράγει πληροφορίες τις οποίες θα τις διανέμει σε ιδιωτικές επιχειρήσεις. Επιπλέον σημαντικό αντικίνητρο στην κοινότητα των υπηρεσιών πληροφοριών, είναι ότι η μικροοικονομική κατασκοπείας δύναται να υλοποιηθεί σε συμμαχικές χώρες, ή σε χώρες όπου έχουν γίνει μυστικές συμφωνίες ή υπάρχουν συμφωνίες ανταλλαγής πληροφοριών. Μία συνεργασία η οποία τίθεται αυτομάτως σε κίνδυνο σε περιπτώσεις ύπαρξης μικροοικονομικής κατασκοπείας μεταξύ των κρατών *(Κωνσταντόπουλος, 2010).*

Ολοκληρώνοντας, στα αντικίνητρα που σχετίζονται με την επιχειρηματική κοινότητα επικρατεί η αβεβαιότητα της αναγκαιότητας συμμετοχής σε μία τέτοιου είδους επιχείρησης. Πολλές επιχειρήσεις αποφεύγουν την ¨ταμπέλα¨ συνεργασίας με τις μυστικές υπηρεσίες, καθώς και οποιαδήποτε πιθανότητα διαρροής μια πληροφορίας που μπορεί να επηρεάσει αρνητικά την εμπιστοσύνη των μετόχων *(Porteous, 1998).* Χαρακτηριστικές είναι οι απόψεις των John F. Hayden, αντιπρόεδρου της Boeing, και του Thomas F. Faught Jr, προέδρου της Boyden Associates, όπου αναφέρουν ότι «..οι εταιρίες μπορούν να προστατεύσουν τα μυστικά τους..», «..οι μυστικές υπηρεσίες δεν είναι αναγκαίο να εξασφαλίσουν με μυστικές μεθόδους τα μυστικά των ανταγωνιστών μας..» και ότι «..δεν χρειαζόμαστε συγκαλυμμένη βοήθεια..» *(Κωνσταντόπουλος, 2010).*

5. Οικονομική κατασκοπεία και ασφάλεια στις ΗΠΑ και Κίνα

Από την ίδρυση της Λαϊκής Δημοκρατίας της Κίνας το 1949, οι υπηρεσίες πληροφοριών του Πεκίνου και της Ουάσιγκτον έχουν δεσμευτεί να αποκαλύψουν ο ένας τα μυστικά του άλλου, προστατεύοντας τα δικά τους και επιδιώκοντας στρατιωτικό, οικονομικό και τεχνολογικό πλεονέκτημα. Πολλοί καλόπιστοι κατάσκοποι και στις δύο πλευρές έχουν συλληφθεί, πολλοί αθώοι έχουν εμπλακεί άδικα και άλλοι έχουν μείνει στην αφάνεια μέσα σε αυτό τον αόρατο ¨πόλεμο¨ της οικονομικής κατασκοπείας.

5.1 Η περίπτωση των ΗΠΑ ως ¨θύμα¨ οικονομικής κατασκοπείας

Οι ΗΠΑ αποτέλεσαν διαχρονικά το μεγαλύτερο ¨θύμα¨ οικονομικής κατασκοπείας, χωρίς αυτό να σημαίνει ότι δεν υπήρξε και ¨θύτης¨. Από τα τέλη του 1776 οι ΗΠΑ ξεκίνησαν τις επιχειρήσεις πληροφοριών, με την τότε πρώτη υπηρεσία πληροφοριών την ¨Επιτροπή Μυστικής Αλληλογραφίας του Ηπειρωτικού Κογκρέσου¨ (Committee of Secret Correspondence of the Continental Congress) *(Konstantopoulos, 2007).* Οι Ηνωμένες Πολιτείες αποτέλεσαν την πρώτη χώρα που αμφισβήτησε το παγκόσμιο προβάδισμα της πληροφόρησης στην Ευρώπη μετά τη Διακήρυξη της Ανεξαρτησίας τους, το 1776.

Η Κεντρική Υπηρεσία Πληροφοριών (CIA) αποτέλεσε ένα σημαντικό παράγοντα στον τομέα της πληροφόρησης και στη λήψη καθοριστικών πολιτικών αποφάσεων. Ο οργανισμός ιδρύθηκε βάση του Νόμου περί Εθνικής Ασφάλειας του 1947 και οι ρόλοι του ήταν περιορισμένοι. Μοναδικός ρόλος της ήταν να παρέχει «εθνική πληροφόρηση» σε υπερβατικά ζητήματα και ο συντονισμός των πληροφοριών που συλλέγονται από τα διάφορα τμήματα της κυβέρνησης. Η οικονομική, η επιστημονική και η τεχνολογική πληροφόρηση ανατέθηκαν στον αντίστοιχο οργανισμό. Σταδιακά υπήρξε η αναγνώριση, ότι υπήρχαν πληροφορίες οικονομικού ενδιαφέροντος με μεγάλη αξία για την κυβέρνηση των ΗΠΑ. Σε μια οδηγία μάλιστα στο NSC του 1951, η κυβέρνηση των ΗΠΑ κατέστησε τη CIA υπεύθυνη για τον καθορισμό των συνολικών απαιτήσεων για την ¨ξένη οικονομική πληροφόρηση¨. Η CIA επρόκειτο να διασφαλίσει ότι ¨η πλήρης οικονομική γνώση και τεχνική που διατίθεται στην κυβέρνηση¨ θα ασχολείται με

θέματα που σχετίζονται με την εθνική ασφάλεια. Επιπλέον ο οργανισμός διατάχθηκε να αξιολογήσει τη συνάφεια, την έκταση και την ποιότητα των διαθέσιμων ξένων οικονομικών δεδομένων που σχετίζονται με θέματα εθνικής ασφάλειας, αναπτύσσοντας τρόπους βελτίωσης της ποιότητας. Αργότερα το 1965, ο τότε διευθυντής της CIA John A. McCone πέτυχε μια συμφωνία με τον Υπουργό Εξωτερικών Dean Rusk, εξουσιοδοτώντας επίσημα τη CIA να συνεχίσει παγκοσμίως την οικονομική πληροφόρηση. Γενικότερα παρέμεινε μια κρίσιμη πηγή πληροφοριών για τις κομμουνιστικές οικονομίες, ειδικά την Κίνα, μια χώρα που δεν δημοσίευε οικονομικά στατιστικά από το τέλος της δεκαετίας του 1950. Η βαρύτητα της πληροφόρησης για τις ΗΠΑ φάνηκε έμπρακτα και το 1975 όπου χαρακτηρίσθηκε ως «Έτος Πληροφοριών». Παρατηρούμε με την πάροδο του χρόνου ότι οι ευθύνες και οι υποχρεώσεις της CIA αυξήθηκαν. Οι δυνατότητές βελτιώθηκαν ικανοποιητικά αποτελώντας ένα διαχρονικά σημαντικό παράγοντα υποστήριξης των υπεύθυνων χάραξης πολιτικής, ως κρίσιμη πηγή πληροφοριών. Μέχρι και σήμερα εκατοντάδες εργάζονται στο γραφείο έρευνας και μεταφοράς τεχνολογίας (RTT), που ασχολούνται με κυρώσεις διεθνών συναλλαγών, την παράνομη χρηματοδότηση, διεθνές οικονομικά και περιβαλλοντικά ζητήματα, αγορές άμυνας και εφοδιασμού, γεωγραφικοί πόροι, δημογραφικά στοιχεία, πολιτική τεχνολογία (όπως αεροδιαστημικής και αναδυόμενες τεχνολογίες) και ενεργειακούς πόρους *(Zelikow, 1997).*

Με την πάροδο του χρόνου και μετά το τέλος του Ψυχρού Πολέμου, η Αμερική της δεκαετίας του 1990 είχε «γίνει ο κύριος στόχος των παγκόσμιων κατασκόπων» *(Fialka, 1999).* Τα περιστατικά οικονομικής κατασκοπείας από ξένες κυβερνήσεις εναντίον αμερικανικών εταιρειών, ατόμων και ιδρυμάτων είναι πολυάριθμα. Η αντιμετώπιση αυτής της πρόκλησης έχει καταστεί υψηλής εθνικής προτεραιότητας από την Ουάσιγκτον. Στη σύγχρονη εποχή, τα εμπορικά μυστικά μπορούν εύκολα να οικειοποιηθούν μέσω του διαδικτύου και άλλων συσκευών επικοινωνίας που βρίσκονται σε ξένες χώρες. Ο Λευκός Οίκος την περίοδο του Προέδρου Bill Clinton αναγνώρισε αυτό το πρόβλημα: *«Ορισμένες ξένες υπηρεσίες πληροφοριών υιοθετούν γρήγορα νέες τεχνολογίες και καινοτόμες μεθόδους για να αποκτήσουν τέτοια μυστικά, συμπεριλαμβανομένων των προσπαθειών χρήσης της παγκόσμιας υποδομής πληροφοριών για την απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες μέσω διείσδυσης συστημάτων και δικτύων υπολογιστών».* Ο Πρόεδρος Bill Clinton υπέγραψε το νόμο περί οικονομικής κατασκοπείας στις 11 Οκτωβρίου 1996, ο οποίος αποτέλεσε τον πρώτο ομοσπονδιακό νόμο που είχε ποινικές κυρώσεις για την κλοπή εμπορικών μυστικών *(Bellocchi, 2001), (Lewis, 2009).* Ο νόμος ασχολείται με τη βιομηχανική κατασκοπεία, καλύπτοντας τα εμπορικά μυστικά και την οικονομική κατασκοπεία, τέσσερις άλλους τομείς δράσης που κρίθηκαν κατάλληλοι από το Κογκρέσο, καθώς και εκθέσεις της Επιτροπής καταδίκης των ΗΠΑ σχετικά με την κρυπτογράφηση τεχνολογίας ανακατασκευής. Γενικότερα μπορεί να χρησιμοποιηθεί και για την

προστασία της πολύτιμης πνευματικής ιδιοκτησίας μιας εταιρείας και ενάντια σε μια εταιρεία που βρίσκεται με εμπορικά μυστικά που ανήκουν σε έναν ανταγωνιστή *(Leighton Johnson, 2020).* Παρόλα αυτά βάση της ενημέρωσης του Ιανουαρίου 2020, ο νόμος δεν προορίζεται για να ποινικοποίηση κάθε κλοπή εμπορικών μυστικών για τα οποία ενδέχεται να υπάρχουν πολιτικά μέσα βάσει του κρατικού δικαίου. Ψηφίστηκε ως αναγνώριση της αξίας της πνευματικής ιδιοκτησίας γενικότερα και των εμπορικών μυστικών ειδικότερα, για την οικονομική ευημερία και ασφάλεια των Ηνωμένων Πολιτειών και για να κλείσει ένα κενό ομοσπονδιακής επιβολής σε αυτόν τον σημαντικό τομέα δικαίου. Οι κατάλληλοι διακριτικοί παράγοντες που πρέπει να ληφθούν υπόψη κατά την απόφαση για την έναρξη δίωξης, αναγράφονται στις παραγράφους 1831-1832 *(The United States – Department of Justice, 2020).*

Η αναγκαιότητα λήψης μέτρων και η βαρύτητα που δείχνουν οι ΗΠΑ σχετικά με την οικονομική κατασκοπεία είναι εμφανής. Ο Λευκός Οίκος το 1996 υπολόγισε απώλεια 100 δισεκατομμυρίων δολαρίων στις επιχειρήσεις των ΗΠΑ ανά έτος, λόγω της ξένης οικονομικής κατασκοπείας στους τομείς της επιστήμης και της τεχνολογίας *(Bellocchi, 2001).* Τα τελευταία χρόνια έχει αναγνωρίσει την προστασία των εμπορικών μυστικών ως ζωτικής σημασίας και έχουν αναφερθεί εντατικά στην προστασία τους και στην επιτυχία των οικονομικών σχέσεων που θα πρέπει να αναπτύσσεται και να διατηρείται μεταξύ των κρατών. Για την επιτυχία των σχέσεων αυτών, οι ΗΠΑ αναφέρουν ότι οι άλλες κυβερνήσεις πρέπει να λάβουν μέτρα για να ενισχύσουν την επιβολή τους κατά της κλοπής εμπορικών μυστικών. Σύμφωνα με έγγραφο του Εκτελεστικού γραφείου του Προέδρου των Ηνωμένων Πολιτειών το 2013 (¨Διοικητική Στρατηγική για τον μετριασμό της κλοπής των εμπορικών μυστικών των ΗΠΑ¨), η κλοπή εμπορικών μυστικών των ΗΠΑ από ξένους ανταγωνιστές ή ξένες κυβερνήσεις υπήρχε και θα συνεχίσει να αυξάνεται από τα ανώτερα επίπεδα διοίκησης των ενδιαφερομένων. Επιπλέον, τα Τμήματα Εμπορίου και Πολιτείας και ο Εκπρόσωπος Εμπορίου των ΗΠΑ επιδιώκουν να δημιουργήσουν συνασπισμούς με άλλες χώρες μεταδίδοντας παρόμοια μηνύματα σε ενδιαφερόμενες χώρες για να πιέσουν από κοινού, για τη βελτίωση της προστασίας των εμπορικών μυστικών. Το Υπουργείο Εξωτερικών και το Γραφείο Διπλωμάτων Ευρεσιτεχνίας και Εμπορικών Σημάτων των ΗΠΑ (USPTO), θα διασφαλίσει επίσης ότι οι πρεσβείες των ΗΠΑ που βρίσκονται σε χώρες που παρουσιάζουν συνθήκες υψηλού κινδύνου για κλοπή εμπορικού απορρήτου, θα ενσωματώσουν την προστασία του εμπορικού απορρήτου στα καθιερωμένα σχέδια της Ομάδας Εργασίας τους για τα Δικαιώματα Πνευματικής Ιδιοκτησίας (IPR), με πληροφορίες από τις κατάλληλες υπηρεσίες. Η διεθνής συνεργασία για την επιβολή του νόμου αποτελεί ένα κρίσιμο μέρος για την καταπολέμηση της παγκόσμιας φύσης της κλοπής εμπορικών μυστικών. Όπως αναφέρει ο τότε Πρόεδρος Barack Hussein Obama:

«Θα προστατεύσουμε επιθετικά την πνευματική μας ιδιοκτησία. Το μοναδικό μας πλεονέκτημα είναι η καινοτομία και η εφευρετικότητα και η δημιουργικότητα του αμερικανικού λαού. Είναι απαραίτητο για την ευημερία μας και θα γίνει πολύ περισσότερο αυτόν τον αιώνα».

«Δεν μπορούμε να κοιτάξουμε πίσω χρόνια από τώρα και να αναρωτηθούμε γιατί δεν κάναμε τίποτα ενόψει πραγματικών απειλών για την ασφάλειά μας και την οικονομία μας » (Executive Office of the President of the United States, 2013).

Επιπλέον την ίδια περίοδο δόθηκαν ιδιαίτερες οδηγίες και κατευθύνσεις αναφορικά με τα «Εργαλεία Εμπορικής Πολιτικής». Σύμφωνα με το Εκτελεστικό γραφείο του Προέδρου των ΗΠΑ (2013), η διοίκηση θα χρησιμοποιήσει εργαλεία εμπορικής πολιτικής για να αυξήσει τη διεθνή επιβολή κατά της κλοπής εμπορικού μυστικού για την ελαχιστοποίηση του αθέμιτου ανταγωνισμού κατά των αμερικανικών εταιρειών. Ο Αμερικανός εμπορικός αντιπρόσωπος (USTR) κατέβαλε προσπάθειες για την προώθηση επαρκούς και αποτελεσματικής προστασίας και επιβολής του εμπορικού απορρήτου, με ενέργειες όπως βαθύτερη συνεργασία με εμπορικούς εταίρους, στόχευση αδυναμιών στην προστασία του εμπορικού απορρήτου, αναζήτηση νέων εμπορικών διαπραγματεύσεων υπό την καθοδήγηση του USTR (εταιρική σχέση Trans Pacific), αύξησης των εμπορικών απορρήτων ως ζήτημα προτεραιότητας σε όλες τις διμερής, περιφερειακές και πολυμερείς εμπορικές συζητήσεις, καθώς και στα κατάλληλα φόρουμ που σχετίζονται με τα δικαιώματα πνευματικής ιδιοκτησίας. *(Executive Office of the President of the United States, 2013).*

Έπειτα το Γραφείο του Διευθυντή Εθνικής Πληροφόρησης (ODNI), συντόνιζε εντός της κοινότητας πληροφοριών την ενημέρωση του ιδιωτικού τομέα σχετικά με το πώς να προσδιορίζουν και να αποτρέπουν την κλοπή εμπορικών μυστικών που ωφελούν έναν κρατικό χορηγό ή μια οντότητα που έχει δεσμούς με ξένη κυβέρνηση. Οι τέσσερις κύριες πτυχές της απειλής από την κλοπή εμπορικών μυστικών ήταν (1) ο αριθμός και η ταυτότητα των ξένων κυβερνήσεων που εμπλέκονται στην υπεξαίρεση εμπορικών μυστικών, (2) οι βιομηχανικοί τομείς και οι τύποι πληροφοριών και τεχνολογίας που στοχεύουν σε μια τέτοια κατασκοπεία, (3) οι μέθοδοι που χρησιμοποιούνται για τη διεξαγωγή της και (4) η διάδοση, η χρήση και ο σχετικός αντίκτυπος των πληροφοριών που χάνονται από την υπεξαίρεση του εμπορικού απορρήτου. Εν συνεχεία ο Πρόεδρος Obama υπέγραψε δύο σημαντικές νομοθετικές πράξεις με άμεσο και θετικό αντίκτυπο στις μελλοντικές διώξεις εμπορικού μυστικού: (1) Δημόσιο Δίκαιο 112-236 — Ο νόμος περί κλοπής εμπορικών μυστικών του 2012 (S. 3642), ο οποίος έκλεισε ένα κενό στον νόμο περί οικονομικής κατασκοπείας που είχε επιτρέψει την κλοπή πολύτιμου εμπορίου μυστικού πηγαίου κώδικα και (2) Δημόσιο Δίκαιο 112-269 — Ο νόμος για την ενίσχυση της ποινής εξωτερικής και οικονομικής κατασκοπείας του 2012 (H.R. 6029/S.

678), όπου ενισχύθηκαν οι ποινικές κυρώσεις για οικονομική κατασκοπεία και κατευθύνθηκε η επιτροπή καταδίκης να εξετάσει το ενδεχόμενο αύξησης των επιπέδων αδικήματος για εμπορικά μυστικά εγκλήματα *(Executive Office of the President of the United States, 2013).*

Ο Πρόεδρος Donald Trump το Μάιο του 2020, γνωρίζοντας την άσκηση οικονομικής κατασκοπείας που προέρχονταν από την Κίνα, εξέδωσε εκτελεστική εντολή απαγορεύοντας στις εταιρείες των ΗΠΑ την πώληση εξοπλισμού στην Huawei, αναφέροντας ότι ενέχει κίνδυνο στην εθνική ασφάλεια. Επιπλέον διέταξε το κλείσιμο του προξενείου της Κίνας στο Houston, «για την προστασία της αμερικανικής πνευματικής ιδιοκτησίας και των αμερικανικών προσωπικών πληροφοριών», ισχυριζόμενος ότι το προξενείο έχει συντονίζει τη βιομηχανική κατασκοπία εναντίον των ΗΠΑ *(Holt, 2020).* Πρόσφατα στη NSG2021 (Interim National Security Strategic Guidance) το Μάρτιο 2021, ο νυν Πρόεδρος Joe Biden αναφέρθηκε στη συνέχιση των επενδύσεων και στην ενίσχυση της Κοινότητας των Πληροφοριών. Αναγνώρισε ως υψίστης σημασίας την ικανότητά της να παρέχει έγκαιρη ανάλυση και προειδοποίηση που απαιτείται για την ενημέρωση της χάραξης πολιτικής, τον εντοπισμό ευκαιριών και την αποτροπή των απειλών προτού μετατραπούν σε κρίσεις. Αναφερόμενος στην Κίνα, ειδικότερα, ανέφερε ότι έγινε γρήγορα πιο διεκδικητική και αποτελεί το μόνο ανταγωνιστής που μπορεί να συνδυάσει την οικονομική, διπλωματική, στρατιωτική και τεχνολογική του δύναμη για να αντιμετωπίσει μια σταθερή πρόκληση σε ένα σταθερό και ανοιχτό διεθνές σύστημα.

Είναι σαφές ότι οι ΗΠΑ έχουν αποτελέσει διαχρονικά το μεγαλύτερο θύμα οικονομικής κατασκοπείας, τόσο στον τομέα της επιστήμης όσο και της τεχνολογίας. Η προσπάθεια και τα μέτρα που έχει λάβει ο Λευκός Οίκος μέχρι στιγμής καθιστούν το φαινόμενο της οικονομικής κατασκοπείας ζωτικής σημασίας για την εθνική ασφάλεια των ΗΠΑ. Η στρατιωτική, επιστημονική, τεχνολογική και οικονομική υπεροχή που κατείχαν οι ΗΠΑ για πολλά χρόνια αποτέλεσαν αντικείμενο έλξης αρκετών οικονομικά ανταγωνιστικών χωρών. Μία από αυτές είναι και η Κίνα, μία χώρα ταχέως εξελισσόμενη στον επιστημονικό και τεχνολογικό τομέα, με μεγάλες βλέψεις ενίσχυσης της θέσης της στην παγκόσμια οικονομική σκακιέρα.

5.2 Η περίπτωση της ΚΙΝΑ ως ¨θύτης¨ οικονομικής κατασκοπείας

Τα πρώτα βιβλία που υποστηρίζουν ότι η πληροφόρηση πρέπει να έχει κεντρικό ρόλο τόσο στον πόλεμο όσο και στην ειρήνη, γράφτηκαν στην αρχαία Κίνα και την Ινδική υποήπειρο. Το βιβλίο ¨Η τέχνη του πολέμου¨ (The Art of War) του Κινέζου Στρατηγού Sun Tzu χρονολογείται τον 5ο αιώνα π.Χ. Στο βιβλίο ο Στρατηγός δίνει ιδιαίτερη σημασία στην κατασκοπεία, αφιερώνοντας σε αυτήν το 13ο και το τελευταίο κεφάλαιο. Ο Sun Tzu εκτιμήθηκε στην Κουμμουνιστική Κίνα πολύ περισσότερο από οποιαδήποτε αυτοκρατορική δυναστεία. Ακόμα και στις ΗΠΑ αναφέρεται πιο συχνά από κάθε άλλο προηγούμενο δυτικό συγγραφέα πληροφοριών προ του 20ου αιώνα *(Andrew, 2018).* Σύμφωνα με το Sun Tzu*: «Εάν κατανοείς τον εαυτό σου καθώς και τον αντίπαλο, δεν θα κινδυνεύσεις να ηττηθείς σε καμία μάχη. Εάν αγνοείς τον αντίπαλο αλλά κατανοείς τον εαυτό σου, οι πιθανότητες νίκης και ήττας είναι μοιρασμένες. Εάν αγνοείς τόσο τον αντίπαλο όσο και τον εαυτό σου, θα ηττηθείς σε κάθε μάχη»,* μια αρχή που με την πάροδο του χρόνου έχει αποτελέσει γνώμονα της Λαϊκής Δημοκρατίας της Κίνας σε θέματα εξωτερικής πολιτικής.

Σύμφωνα με τον Qian Xuesen, Κινέζος μαθηματικός, κυβερνητικός, μηχανικός αεροδιαστημικής και φυσικός, στον 21ο αιώνα εάν μια συγκεκριμένη χώρα αποτύχει να πρωτοστατήσει στην επιστήμη και την τεχνολογία, θα είναι δύσκολο να διατηρήσει τις οικονομικές της δραστηριότητες και τη διεθνή της θέση. Η σύγχρονη Κίνα προκειμένου να καταστεί μια ισχυρή περιφερειακή δύναμη, έδωσε έμφαση στην αύξηση της στρατιωτικής και οικονομικής της ισχύς *(Hannas, Mulvenon, and Puglisi, 2013).* Η οικονομική ισχύς σχετίζεται με την ανάπτυξη της επιστήμης και της τεχνολογίας, δύο έννοιες που αποτέλεσαν τις κινητήριες δυνάμεις για την επίτευξη του εκσυγχρονισμού της σε τέσσερεις τομείς: «(1) το βιομηχανικό, (2) τον αγροτικό, (3) της επιστήμης και της τεχνολογίας και (4) της άμυνας» *(Κωνσταντόπουλος, 2010).* Από την ίδρυση της Λαϊκής Δημοκρατίας της Κίνας το 1949, οι υπηρεσίες πληροφοριών της Κίνας διαδραματίζουν ολοένα και μεγαλύτερο ρόλο στηρίζοντας τους εθνικούς στόχους πολιτικής, εκμεταλλευόμενοι την τεχνολογική, οικονομική, πολιτική και στρατιωτική υποδομή άλλων σύγχρονων βιομηχανικών κρατών. Σύμφωνα με το William Overend (1988), αξιωματούχοι των ΗΠΑ συμφώνησαν δημόσια ότι η Κίνα είναι «η πιο ενεργή ξένη δύναμη που ασχολείται με την παράνομη απόκτηση αμερικανικής τεχνολογίας» *(Eftimiades, 1993).* Επιπλέον το 2005 ο Dave Szady, τότε βοηθός διευθυντή του τμήματος αντιπληροφόρησης του FBI, στην εφημερίδα της Wall Street αναφέρει «η Κίνα είναι η μεγαλύτερη απειλή (κατασκοπείας) για τις ΗΠΑ σήμερα» *(Hannas, Mulvenon, and Puglisi, 2013).*

Η σύγχρονη Κίνα αγωνίστηκε να ανακτήσει την τεχνική της ικανότητα εν μέσω πολιτικών ανατροπών, εξωτερικών επεμβάσεων και εμφυλίου πολέμου. Από τα τέλη

της Δυναστείας του Τσινγκ (1644–1912), οι Κινέζοι ηγέτες ξεκίνησαν προσπάθειες για την εισαγωγή τεχνολογίας και την αποστολή ελπιδοφόρων φοιτητών στο εξωτερικό με στόχο η Κίνα να «μάθει από τη Δύση». Με την πάροδο των χρόνων πολλοί από αυτούς τους μαθητές επέστρεψαν για να ηγηθούν πτυχών της ανάπτυξης της Κίνας. Ακόμα και στα μεταγενέστερα κύματα συνέχισαν να παίζουν κρίσιμους ρόλους σε πυρηνικά και διαστημικά προγράμματα της Κίνας. Η γενική ιδέα παρουσιάστηκε το 1878 από τον Κινέζο αξιωματούχο Zhang Zhidong στο δοκίμιό του ¨Quan Xue Pian¨, όπου η αρχή είναι το «tǐ-yòng». Ο όρος αποτελείται από δύο κινέζικα μορφώματα: tǐ, που σημαίνει «ουσία» και yòng, που σημαίνει «Πρακτική χρήση», για να περιγράψει μια μέθοδο αυτοενίσχυσης, σύμφωνα με την οποία η Κίνα θα διατηρούσε το δικό της στυλ μάθησης για να διατηρηθεί η «ουσία» της κοινωνίας, ενώ ταυτόχρονα χρησιμοποιείται η δυτική μάθηση για «Πρακτική εφαρμογή» στην ανάπτυξη των υποδομών και της οικονομίας της. Παρά την πάροδο του χρόνου οι ιδρυτικοί ηγέτες της Λαϊκής Δημοκρατίας της Κίνας δεν απέρριψαν την έννοια του «tǐ-yòng». Κοινός παράγοντας σε όλη την έκταση υπήρξε η σημασία της ξένης τεχνολογίας στο στρατηγικό όραμα της Κίνας, που εφαρμόστηκε σε μεγάλο βαθμό από φοιτητές και μελετητές, οι οποίοι χρησιμοποιούν τις δεξιότητες, τις γνώσεις και την καλή θέληση που τους παρείχαν στο εξωτερικό για να μεταμορφώσει τα πανεπιστήμια, τις εταιρείες και την άμυνα της Κίνας σε άμεσο ανταγωνιστή των Ηνωμένων Πολιτειών. Χαρακτηριστικό είναι ότι από τους πρώτους μαθητές πολλοί βετεράνοι της αποστολής συνέβαλαν στην ανάπτυξη της Κίνας. Μάλιστα ο πρώτος πρωθυπουργός της Δημοκρατίας της Κίνας, δεκαεπτά ναυτικοί αξιωματικοί, δεκατρείς που υπηρέτησαν σε διπλωματικές θέσεις και δώδεκα αρχιμηχανικοί ή διευθυντές στους σιδηροδρόμους, ανήκαν στους μαθητές της πρώτης «αποστολής» εκσυγχρονισμού *(Hannas, Mulvenon, and Puglisi, 2013).*

Ωστόσο η μεταφορά της τεχνολογίας από τις ΗΠΑ στην Κίνα υλοποιείται με τη χρήση ¨πολλαπλών καναλιών¨. Οι διπλωματικές αποστολές της Κίνας στις Ηνωμένες Πολιτείες επικεντρώνονται σε εξαιρετικό βαθμό στη μεταφορά αμερικανικής τεχνολογίας, άμεσα με την προώθηση επιχειρήσεων με τεχνολογικό προσανατολισμό και των σχέσεων ¨συνεργασίας¨, και έμμεσα αξιοποιώντας τις σχέσεις τους με ομάδες υπεράσπισης της Κίνας με έδρα τις ΗΠΑ. Σοβαρές προσπάθειες για τη συμμετοχή Κινέζων επιστημόνων σε έργα S&T (Science and Technology) της ΛΔΚ ξεκίνησαν στα μέσα της δεκαετίας του 1990, με το προξενείο της Νέας Υόρκης να σχηματίσει μια επιτροπή εμπειρογνωμόνων στο εξωτερικό «Βοηθήστε τους σπουδαστές στο εξωτερικό να συνειδητοποιήσουν τις ελπίδες τους να υπηρετήσουν τη χώρα». Εκτός από τις διπλωματικές αποστολές της στις ΗΠΑ, η κινεζική κυβέρνηση διευκολύνει τη μεταφορά τεχνολογίας μέσω κρατικών οργανώσεων που έχουν συσταθεί απευθείας στο έδαφος των ΗΠΑ. Όπως το γραφείο της SAFEA (State Administration of Foreign Experts Affairs) στη Νέα Υόρκη και η Triway Enterprise Inc., ένα «ινστιτούτο εξωτερικής κατάρτισης» που ιδρύθηκε υπό τον SAFEA υπό την αιγίδα της Falls Church, με υποκαταστήματα στο Πεκίνο και το Ναντζίνγκ. Η

εταιρεία από το 1993 προωθεί την ανταλλαγή και συνεργασία μεταξύ της Κίνας και των ΗΠΑ στους τομείς του S&T, του πολιτισμού, της εκπαίδευσης και της διαχείρισης με μεγάλη επιτυχία *(Hannas, Mulvenon, and Puglisi, 2013).* Επιπλέον η Κινεζική Ένωση για την Επιστήμη και την Τεχνολογία (CAST-USA) ιδρύθηκε και εγγράφηκε τον Αύγουστο του 1992 στην πολιτεία της Νέας Υόρκης ως μη πολιτικός κερδοσκοπικός επαγγελματικός οργανισμός, με σκοπό να προωθήσει τις ακαδημαϊκές ανταλλαγές και την επαγγελματική ανάπτυξη των μελών της. Χρησιμεύει ως «γέφυρα» μεταξύ των δύο χωρών για την ανταλλαγή προσωπικού, πληροφοριών και για τη συνεργασία σε επιστήμη και τεχνολογία, οικονομικούς, εμπορικούς και άλλους τομείς, μέσω της οργάνωσης σεμιναρίων, συνεδρίων, προγραμμάτων ανταλλαγής και ειδικών δραστηριοτήτων μεταξύ τον δύο λαών. Το CAST-USA απαριθμεί μεταξύ των «συμβούλων» του, νυν και πρώην μέλη της Κινεζικής Ακαδημίας Επιστημών και της Κινεζικής Ακαδημίας Μηχανικών, τα υψηλότερα επιστημονικά όργανα της ΛΔΚ. Αυτοί κατέχουν ενεργούς ρόλους στις διαδικασίες του οργανισμού στις ΗΠΑ χαράζοντας συγκεκριμένες πολιτικές. Ωστόσο η Κίνα πέρα των εταιριών που διαθέτει στις ΗΠΑ, επενδύει στην εκμετάλλευση ξένων πληροφοριών S&T και διαμέσων της συλλογής από πηγές ανοικτού τύπου (OSINT). Η συστηματική αυτή προσπάθεια αποσκοπεί στην επιτάχυνση της επιστημονικής ανάπτυξης της Κίνας μέσω της συλλογής και ανάλυσης στοιχείων από ανοιχτές πηγές, όπως αρμόζει σε ένα έθνος του οποίου η πρόοδος εξαρτάται περισσότερο από την προσαρμογή παρά από την καινοτομία. Ενώ οι υπηρεσίες της Δύση συνήθως θεωρούν τον ανοιχτό κώδικα ως το ¨φτωχό ξάδερφο¨ της «πραγματικής» πληροφόρησης, η Κίνα στελεχώνει τους οργανισμούς του OSINT με προσωπικό κορυφαίας σταδιοδρομίας, υποστηριζόμενο από έναν βιομηχανικό οργανισμό, δίνοντας μεγάλη βαρύτητα στον τομέα τον ανοιχτών πηγών *(Hannas, Mulvenon, and Puglisi, 2013).*

Μελετώντας τα ¨πολλαπλά¨ κανάλια της Κίνας, διαπιστώνουμε ότι η κινεζική διασπορά των φοιτητών στις Ηνωμένες Πολιτείας αποτελεί το πιο διαχρονικό μέσο. Εκτιμάται ότι 30.000 Κινέζοι μαθητές στάλθηκαν στις ΗΠΑ μεταξύ 1860 και 1950 και από το 1905 έως το 1953 πάνω από το 40% σπούδασε μηχανική και επιστήμες. Μετά την ίδρυση της ΛΔΚ, πολλοί επέστρεψαν στην Κίνα για να διευθύνουν έρευνες στην πυρηνική φυσική και τη φυσική υψηλής ενέργειας παίζοντας σημαντικό ρόλο στα προγράμματα ανάπτυξης ατομικής βόμβας της Κίνας και του υδρογόνου. Ο πολιτικός Ντενγκ Σιαόπινγκ το 1978, τάχθηκε υπέρ της αύξησης του αριθμού των μαθητών που πηγαίνουν στο εξωτερικό για εκπαίδευση λέγοντας «Πρέπει να στείλουμε δεκάδες χιλιάδες φοιτητές στο εξωτερικό, όχι μόνο μια χούφτα». Τα σχόλια του ενέπνευσαν τις προσπάθειες της κυβέρνησης να επεκτείνει γρήγορα τον αριθμό των Κινέζων φοιτητών που πηγαίνουν για μεταπτυχιακή εκπαίδευση στη Δύση. Ως αποτέλεσμα, «η αποστολή μαθητών για σπουδές στο εξωτερικό έχει γίνει ένα από τα κύρια κανάλια της Κίνας για την καλλιέργεια ειδικευμένου προσωπικού». Το ακαδημαϊκό έτος 1983–1984, περίπου

12.000 Κινέζοι φοιτητές και μελετητές επισκέφθηκαν τις ΗΠΑ, αριθμός που αυξήθηκε ραγδαία τη δεκαετία του 1980 και 1990. Το 2010 αντιπροσώπευαν σχεδόν το 22% του ξένων φοιτητών, με 158.000 Κινέζους μαθητές εγγεγραμμένους στα πανεπιστήμια των ΗΠΑ *(Hannas, Mulvenon, and Puglisi, 2013).*

Σε όλη αυτή τη μεταφορά επιστήμης και τεχνολογίας το Υπουργείο Κρατικής Ασφάλειας (MSS) έχει διαδραματίσει ένα ιδιαίτερο ρόλο. Το 2007, ο τότε επικεφαλής του τμήματος αντιπληροφόρησης του FBI, Bruce Carlson, ανέφερε στο ¨USA Today¨ ότι «περίπου το ένα τρίτο των ερευνών οικονομικής κατασκοπείας συνδέονται με κινεζικές κυβερνητικές υπηρεσίες, ερευνητικά ινστιτούτα ή επιχειρήσεις». Κινέζοι λόγιοι και επιστήμονες στις ΗΠΑ αποτελούν δυνητικούς στόχους για τις υπηρεσίες πληροφοριών της Κίνας, ειδικά όταν ταξιδεύουν στην Κίνα για να παρακολουθήσουν συνέδρια, σύμφωνα με πρώην αξιωματούχος της αντιπληροφόρησης του FBI. Σε ορισμένες περιπτώσεις μάλιστα, το MSS προσέγγισε Κινέζους μαθητές που προετοιμάζονταν να σπουδάσουν στις ΗΠΑ πριν από την αναχώρησή τους, για να δημιουργήσουν μια μυστική σχέση. Επιπλέον, Κινέζοι επιστήμονες και λόγιοι που έχουν σπουδάσει ή επισκεφθεί τις ΗΠΑ αρκετές φορές, ενημερώνονται με την επιστροφή τους στην Κίνα και η MSS προσλαμβάνει επιλέγοντας μερικούς από αυτούς ως μέρος εκπαιδευτικών προγραμμάτων ανταλλαγής ή ως μέλη επιστημονικών αντιπροσωπειών, που τους αναθέτουν την απόκτηση πληροφοριών ή την εκτέλεση άλλων επιχειρησιακών δραστηριοτήτων *(Hannas, Mulvenon, and Puglisi, 2013).* Αξιοσημείωτη είναι μία ανάλυση, που επιβεβαιώνει τη μέχρι τώρα μελέτη, των εκτεθειμένων τεχνολογιών κατασκοπείας που σχετίζονται με την Κίνα στις ΗΠΑ, όπου καταδεικνύει τρία βασικά επιχειρησιακά πρότυπα: πρώτον η στρατολόγηση πρακτόρων στην Κίνα και η αποστολή τους στο εξωτερικό για να αποκτήσουν την τεχνολογία, δεύτερον αγορά αμερικανικών εταιρειών με πρόσβαση στα επιθυμητά επίπεδα τεχνολογίας και τρίτον αγορά εξοπλισμού υψηλής τεχνολογίας μέσω αντιπροσώπων που συνεργάζονται με τοπικές εταιρείες στο Χονγκ Κονγκ *(Eftimiades, 1993).* Επιπλέον αξιοσημείωτο είναι ο διαφορετικός τρόπος λειτουργίας του Κύκλου Πληροφοριών από τις υπηρεσίες της Κίνας. Οι Κινέζοι έχουν αντιστρέψει τον Κύκλο Πληροφοριών, αφήνοντας τις υπηρεσίες να καθοδηγήσουν τη διαδικασία, σε αντίθεση με του Δυτικούς όπου οι κυβερνητικοί υπεύθυνοι χάραξης πολιτικής καθοδηγούν τη διαδικασία. Μια διαφορά που μας υποδουλώνει ένα διαφορετικό τρόπο αντίληψης και ανάλυσης των θεμάτων πληροφόρησης *(Mattis, 2012).*

Ολοκληρώνοντας, παρατηρούμε το 13ο πενταετές σχέδιο της Κίνας (2016-2020) να επικεντρώνεται στην αιχμή της τεχνολογίας και της κοινωνικοοικονομικής μεταρρύθμισης. Το σχέδιο απαιτεί καινοτόμα τεχνολογία για τη βελτίωση της εθνικής υποδομής και περιβαλλοντικά φιλική τεχνολογία για την ανακούφιση του οικολογικού αποτυπώματος της Κίνας. Έως το 2025, η Κίνα επιθυμεί να βελτιώσει τον εθνικό της

τεχνολογικό πυρήνα, να μειώσει την παγκόσμια αντίληψη ότι τα προϊόντα της είναι κατώτερης ποιότητας (πιθανώς εκσυγχρονίζοντας τη βιομηχανική υποδομή), και να διαφοροποιήσει τις εγχώριες βιομηχανικές αγορές της. Παρόλο που έχει αναπτύξει τεχνολογικές ικανότητες, η πλειοψηφία πιθανότατα θα επιτευχθεί ως κλεμμένη πνευματική ιδιοκτησία από τις ΗΠΑ και άλλα έθνη. Το υπόλοιπο σχέδιο επικεντρώνεται στην εξισορρόπηση των κενών ευημερίας και τη γεφύρωση των κοινωνικοοικονομικών διαφορών. Δεδομένου ότι είναι απίθανο το Κινεζικό Κομμουνιστικό Κόμμα να μεταρρυθμίσει τη δομή του για να υποστηρίξει μια πιο περιεκτική προσέγγιση διακυβέρνησης, προσπάθειες βελτίωσης του βιοτικού επιπέδου των Κινέζων πιθανότατα θα συλλεχθούν από λειτουργικά μοντέλα που ανήκουν στη Δύση. Εν ολίγοις η πλειοψηφία του δέκατου τρίτου σχεδίου της Κίνας εξαρτάται από τη συνεχή κατασκοπεία σε χώρες όπως οι ΗΠΑ, ο Καναδάς και η Αυστραλία, καθιστώντας την προσοχή των μυστικών υπηρεσιών των χωρών αυτών *(Scott and Spaniel, 2016).*

6. Διοίκηση της Διακινδύνευση και οικονομική κατασκοπεία

Ολοκληρώνοντας τη μελέτη της διεθνούς βιβλιογραφίας, στο κεφάλαιο αυτό θα απαντήσουμε στο ερώτημα: *«Ποιοι είναι οι κίνδυνοι που προκύπτουν από την άσκηση οικονομικής κατασκοπείας από μια ξένη χώρα;».*

Αρχικά θα αναγνωριστούν και ομαδοποιηθούν οι κίνδυνοι που προκύπτουν σε μια χώρα ¨θύμα¨ από την άσκηση οικονομικής κατασκοπείας και έπειτα θα προβούμε στην εκτίμηση της πιθανότητας και του αντιτύπου δημιουργώντας μήτρες κινδύνων. Τέλος θα αναλύσουμε το πιο σημαντικό κίνδυνο αποτυπώνοντας τις πιθανές εκβάσεις του.

6.1 Αναγνώριση - ομαδοποίηση κινδύνων

Η αναγνώριση των κινδύνων πραγματοποιήθηκε από ανάλυση των περιστατικών οικονομικής κατασκοπείας, των στοιχείων και των αναφορών που συλλέχθηκαν κυρίως από τις παρακάτω πηγές: (1) έκθεση του Εκτελεστικού γραφείου του Προέδρου των ΗΠΑ το 2013 «Διοικητική στρατηγική για τον μετριασμό της κλοπής των εμπορικών μυστικών των ΗΠΑ», (2) πολυετή έρευνα του CSIS (Center of strategic & International Studies) με τη συμβολή των Evan Burke, Matthew Serrone, Khristal Thomas, Arthur Nelson, Ian Haimowitz and David Robusto, (3) άρθρο του Mattis Peter L. το 2012 (International Journal of Intelligence and CounterIntelligence), (4) άρθρο του Holt Alexander το 2020 (MIT technology review), (5) ετήσιες αναφορές του Κογκρέσου για τα έτη 2018, 2019 και 2020, (6) αναφορές ¨Foreign Economic Espionage in Cyberspace (2018)¨ και ¨Report to Congress on Foreign Economic Collection and Industrial Espionage¨ του «The National CounterIntelligence and Security Center», (7) αναφορά ¨Insider Threats and Commercial Espionage: Economic and National Security Impacts (2021)¨ του «Insa's Insider Threat Subcommittee» και (8) βιβλίο ¨Οικονομία και Κατασκοπεία (2010)¨ του Κωνσταντόπουλου Ιωάννη. Επιπλέον, λήφθηκε υπόψιν το σύνολο της βιβλιογραφίας και των πηγών που χρησιμοποιήθηκε για τη δημιουργία πιθανών απορρεουσών κινδύνων, καθώς και το προσωπικό που εμπλέκεται στον εκάστοτε τομέα κινδύνου.

Οι κίνδυνοι ομαδοποιήθηκαν σε τέσσερις βασικές κατηγορίες, ανάλογα με το βασικό τομέα που έχει αντίκτυπο ο κάθε κίνδυνος: (Α) «Κρατικοί-Πολιτικοοικονομικοί», (Β) «Εταιρικοί-Κοινωνικοί», (Γ) «Επιστημονικοί-Τεχνολογικοί» και (Δ) «Στρατιωτικοί-Αμυντικοί» και αποτυπώνονται στον Πίνακα 1.

Πίνακας Κινδύνων

Ομάδες κινδύνων	Κίνδυνοι
Κρατικοί-Πολιτικοοικονομικοί	Αύξηση κρατικών δαπανών για άσκηση οικονομικής αντικατασκοπείας
	Αποκάλυψη μυστικών κρατικών οικονομικών συμφωνιών με άλλα κράτη
	Αποκάλυψη μυστικών κρατικών οικονομικών συμφωνιών με εταιρίες
	Υποκλοπή εμπορικών απορρήτων από κρατικές επιχορηγούμενες εταιρίες
	Υποκλοπή οικονομικών προγραμμάτων για μέτρα κατά της κλιματικής αλλαγής
	Αποκάλυψη οικονομικών συμφωνιών κράτους με μη κρατικούς δρώντες
	Υποκλοπή ευαίσθητων πολιτικοοικονομικών δεδομένων
Εταιρικοί-Κοινωνικοί	Αύξηση οικονομικών δαπανών εταιριών για άσκηση οικονομικής αντικατασκοπείας
	Αύξηση ανεργίας λόγω πτώχευσης εταιριών
	Υποκλοπή εμπορικών μυστικών εταιριών
	Παραβίαση πνευματικής ιδιοκτησίας εταιριών ή προσώπων
	Καταπάτηση προσωπικών δεδομένων
	Αποθάρρυνση υλοποίησης νεών τεχνολογιών από εταιρίες
	Αύξηση αθέμιτου ανταγωνισμού μεταξύ εταιριών
Επιστημονικοί-Τεχνολογικοί	Υποκλοπή μυστικών που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων
	Υποκλοπή πληροφοριών σχετικά με τεχνολογίες νέων ενεργειακών πόρων
	Κρυπτογράφηση τεχνολογίας ανακατασκευής και έτερων τροποποιήσεων
	Υποκλοπή σχεδίων ερευνών τεχνητής νοημοσύνης και δεδομένων
	Υποκλοπή πληροφοριών αεροδιαστημικής τεχνολογίας
	Υποκλοπή νέων πρωτότυπων τεχνολογιών
	Υποκλοπή ιατρικών μυστικών από φαρμακοβιομηχανίες
Στρατιωτικοί-Αμυντικοί	Υποκλοπή πληροφοριών εθνικής ασφάλειας
	Υποκλοπή τεχνικών πληροφοριών ανταλλακτικών στρατιωτικού εξοπλισμού
	Υποκλοπή πληροφοριών για τρέχουσες και μελλοντικές τεχνολογίες των Ενόπλων Δυνάμεων
	Αποκάλυψη μυστικής διμερούς συμφωνίας ενίσχυσης άλλου κράτους με στρατιωτικό εξοπλισμό
	Αποκάλυψη συμφωνίας ενίσχυσης μη κρατικού δρώντα με στρατιωτικό εξοπλισμό
	Υποκλοπή απόρρητων πληροφοριών για νέες αναδυόμενες τεχνολογίες στρατιωτικής φύσεως
	Αποκάλυψη μυστικών στρατιωτικών συμφωνιών κράτους με μη κρατικούς δρώντες

Πίνακας 1

6.2 Μήτρα κινδύνων - Πίνακες Matrix

Για την υλοποίηση της μήτρας κινδύνων γίνεται εκτίμηση των κινδύνων ως προς την πιθανότητα εκδήλωσης και το δυνητικό αντίκτυπο στον αντίστοιχο τομέα.

Η εκτίμηση πραγματοποιείται σε 5-βάθμια κλίμακα, «Πολύ Χαμηλή-1», «Χαμηλή-2», «Μέτρια-3», «Υψηλή-4» και «Πολύ Υψηλή-5» ως προς την πιθανότητα εκδήλωσης και ως προς το αντίκτυπο βάση των επιπτώσεων που θα προκύψουν στον εκάστοτε τομέα: (Α) Κρατικό, (Β) Επιχειρηματικό, (Γ) Επιστημονικό-Τεχνολογικό και (Δ) Αμυντικό, σε συνδυασμό με την Εθνική Ασφάλεια του κράτους βάση της διεθνούς βιβλιογραφίας και των ετήσιων αναφορών των ΗΠΑ για θέματα Εθνικής Ασφάλειας.

Η προτεραιότητα του κάθε κινδύνου προκύπτει από το γινόμενο ΠΙΘΑΝΟΤΗΤΑ Χ ΑΝΤΙΚΤΥΠΟ, όπως αποτυπώνεται στον Πίνακα 2 (Μήτρα Κινδύνων) και τους Πίνακες Matrix 3.1 έως 3.4.

Μήτρα Κινδύνων

Ομάδες κινδύνων	Κωδικός	Κίνδυνοι	Π	Α	Πρ
Κρατικοί-Πολιτικοοικονομικοί	Α1	Αύξηση κρατικών δαπανών για άσκηση οικονομικής αντικατασκοπείας	5	4	20
	Α2	Αποκάλυψη μυστικών κρατικών οικονομικών συμφωνιών με άλλα κράτη	1	5	5
	Α3	Αποκάλυψη μυστικών κρατικών οικονομικών συμφωνιών με εταιρίες	4	4	16
	Α4	Υποκλοπή εμπορικών απορρήτων από κρατικές επιχορηγούμενες εταιρίες	4	4	16
	Α5	Υποκλοπή οικονομικών προγραμμάτων για μέτρα κατά της κλιματικής αλλαγής	3	1	3
	Α6	Αποκάλυψη οικονομικών συμφωνιών κράτους με μη κρατικούς δρώντες	3	5	15
	Α7	Υποκλοπή ευαίσθητων πολιτικοοικονομικών δεδομένων	4	4	16
Εταιρικοί-Κοινωνικοί	Β1	Αύξηση οικονομικών δαπανών εταιριών για άσκηση οικονομικής αντικατασκοπείας	4	4	16
	Β2	Αύξηση ανεργίας λόγω πτώχευσης εταιριών	3	5	15
	Β3	Υποκλοπή εμπορικών μυστικών εταιριών	5	4	20
	Β4	Παραβίαση πνευματικής ιδιοκτησίας εταιριών ή προσώπων	5	3	15
	Β5	Καταπάτηση προσωπικών δεδομένων	5	2	10
	Β6	Αποθάρρυνση υλοποίησης νεών τεχνολογιών από εταιρίες	4	4	16
	Β7	Αύξηση αθέμιτου ανταγωνισμού μεταξύ εταιριών	5	3	15
Επιστημονικοί-Τεχνολογικοί	Γ1	Υποκλοπή μυστικών που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων	4	5	20
	Γ2	Υποκλοπή πληροφοριών σχετικά με τεχνολογίες νέων ενεργειακών πόρων	4	4	16
	Γ3	Κρυπτογράφηση τεχνολογίας ανακατασκευής και έτερων τροποποιήσεων	4	4	16
	Γ4	Υποκλοπή σχεδίων ερευνών τεχνιτής νοημοσύνης και δεδομένων	5	4	20
	Γ5	Υποκλοπή πληροφοριών αεροδιαστημικής τεχνολογίας	4	4	16
	Γ6	Υποκλοπή νέων προτότυπων τεχνολογιών	4	4	16
	Γ7	Υποκλοπή ιατρικών μυστικών από φαρμακοβιομηχανίες	5	4	20
Στρατιωτικοί-Αμυντικοί	Δ1	Υποκλοπή πληροφοριών εθνικής ασφάλειας	3	5	15
	Δ2	Υποκλοπή τεχνικών πληροφοριών ανταλλακτικών στρατιωτικού εξοπλισμού	4	4	16
	Δ3	Υποκλοπή πληροφοριών για τρέχουσες και μελλοντικές τεχνολογίες των Ενόπλων Δυνάμεων	3	5	15
	Δ4	Αποκάλυψη μυστικής διμερούς συμφωνιας ενίσχυσης άλλου κράτους με στρατιωτικό εξοπλισμό	3	5	15
	Δ5	Αποκάλυψη συμφωνίας ενίσχυσης μη κράτικού δρώντα με στρατιωτικό εξοπλισμό	4	5	20
	Δ6	Υποκλοπή απόρρητων πληροφοριών για νέες αναδυόμενες τεχνολογίες στρατιωτικής φύσεως	4	5	20
	Δ7	Αποκάλυψη μυστικών στρατιωτικών συμφωνιών κράτους με μη κρατικούς δρώντες	4	5	20

Πίνακας 2

ΠΙΝΑΚΕΣ MATRIX

Κρατικοί-Πολιτικοοικονομικοί

		Αντίκτυπος				
		Πολύ Χαμηλός	Χαμηλός	Μέτριος	Υψηλός	Πολύ Υψηλός
Πιθανότητα	Πολύ Χαμηλή					Α2
	Χαμηλή					
	Μέτρια	Α5				Α6
	Υψηλή				Α3, Α4, Α7	
	Πολύ Υψηλή				Α1	

Πίνακας 3.1

Εταιρικοί-Κοινωνικοί

		Αντίκτυπος				
		Πολύ Χαμηλός	Χαμηλός	Μέτριος	Υψηλός	Πολύ Υψηλός
Πιθανότητα	Πολύ Χαμηλή					
	Χαμηλή					
	Μέτρια					Β2
	Υψηλή				Β1, Β6	
	Πολύ Υψηλή		Β5	Β4, Β7	Β3	

Πίνακας 3.2

Επιστημονικοί-Τεχνολογικοί

		Αντίκτυπος				
		Πολύ Χαμηλός	Χαμηλός	Μέτριος	Υψηλός	Πολύ Υψηλός
Πιθανότητα	Πολύ Χαμηλή					
	Χαμηλή					
	Μέτρια					
	Υψηλή				Γ2, Γ3, Γ5, Γ6	
	Πολύ Υψηλή				Γ4, Γ7	Γ1

Πίνακας 3.3

Στρατιωτικοί-Αμυντικοί

		Αντίκτυπος				
		Πολύ Χαμηλός	Χαμηλός	Μέτριος	Υψηλός	Πολύ Υψηλός
Πιθανότητα	Πολύ Χαμηλή					
	Χαμηλή					
	Μέτρια					Δ1, Δ3, Δ4
	Υψηλή					Δ2, Δ5, Δ6, Δ7
	Πολύ Υψηλή					

Πίνακας 3.4

Αναλύοντας τους παραπάνω Πίνακες, καταλήγουμε στα εξής συμπεράσματα:

(α) Οι μεγαλύτερες τιμές ως προς την πιθανότητα εκδήλωσης αποτυπώνονται στον Επιχειρηματικό τομέα. Κάτι το οποίο αποδεικνύεται και από τα παραδείγματα οικονομικής κατασκοπείας που αναγράφονται στη βιβλιογραφία. Σημαντικό γεγονός αποτελεί ίσως η ύπαρξη ανεπαρκών μέτρων οικονομικής αντικατασκοπείας,

εργαζομένων-ιδιωτών, εξωτερικών παραγόντων και κρατικών φορέων που σε συνδυασμό με τον επιχειρηματικό ανταγωνισμό οδηγεί τον τομέα αυτό στον πιο πιθανό για άσκηση οικονομικής κατασκοπείας. Επιπλέον ο επιχειρηματικός κόσμος αποτελεί ένα πολυδιάστατο τομέα, όπου ο παγκόσμιος ανταγωνισμός αποτελεί ίσως τη μεγαλύτερη πρόκληση για κάθε πολυεθνική εταιρεία.

(β) Το μεγαλύτερο αντίκτυπο από την εκδήλωση τους εμφανίζεται στον Αμυντικό τομέα, τομέας με άμεσα συνδεδεμένος με την εθνική ασφάλεια ενός κράτους.

(γ) Από τη συνολική εικόνα διαπιστώνεται ότι η μεγαλύτερη προτεραιότητα εμφανίζεται στον Επιστημονικό-Τεχνολογικό τομέα και έπειτα στον Αμυντικό, δύο τομείς άρρηκτα συνδεδεμένοι μεταξύ τους. Η ανάπτυξη της επιστήμης και της τεχνολογίας αποτελεί ίσως το πιο σημαντικό τομέα που μπορεί να προσφέρει σε ένα κράτος ευημερία, ανάπτυξη, οικονομική ισχύ, στρατιωτική ισχύ και κατ' επέκταση εθνική ασφάλεια και ένα ισχυρό διεθνές ¨profile¨ στο διεθνές περιβάλλον.

(δ) Επιπροσθέτως οι σημαντικότεροι κίνδυνοι ανά τομέα είναι οι εξής:

- Α1: Αύξηση κρατικών δαπανών για άσκηση οικονομικής αντικατασκοπείας, στον Κρατικό τομέα.

- Β3: Υποκλοπή εμπορικών μυστικών εταιριών», στον Επιχειρηματικό τομέα.

- Γ1: Υποκλοπή μυστικών που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων, Γ7: Υποκλοπή ιατρικών μυστικών από φαρμακοβιομηχανίες, στον Επιστημονικό τομέα.

- Δ5: Αποκάλυψη συμφωνίας ενίσχυσης μη κρατικού δρώντα με στρατιωτικό εξοπλισμό, Δ6: Υποκλοπή απόρρητων πληροφοριών για νέες αναδυόμενες τεχνολογίες στρατιωτικής φύσεως και Δ7: Αποκάλυψη μυστικών στρατιωτικών συμφωνιών κράτους με μη κρατικούς δρώντες», στον Αμυντικό τομέα.

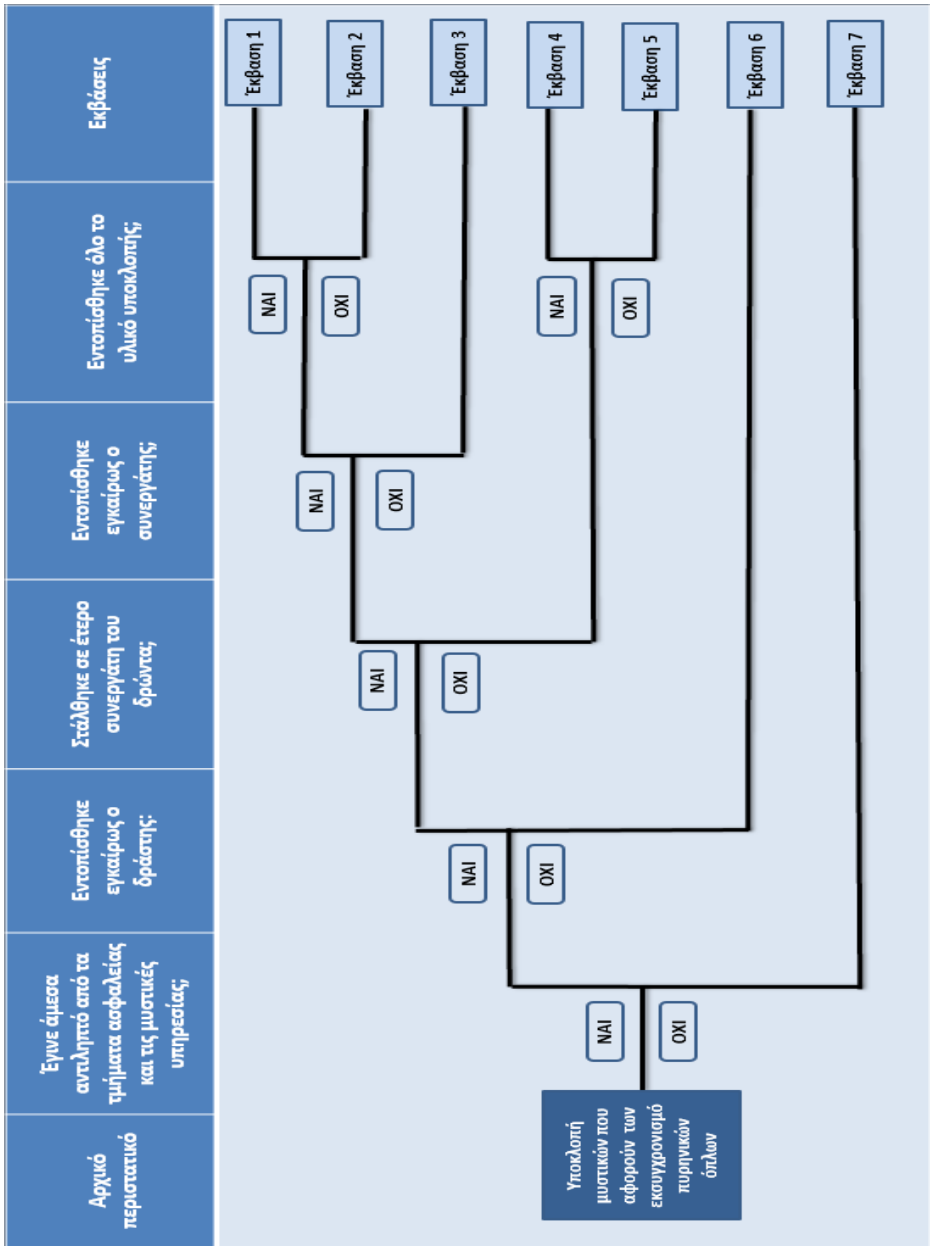
6.3 Ανάλυση σημαντικότερου κινδύνου

Συνεχίζοντας την ανάλυση, ως πιο σημαντικός χαρακτηρίζεται ο κίνδυνος *«Γ1: Υποκλοπή μυστικών που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων».* Ο εν λόγω κίνδυνος εκτιμήθηκε με τη υψηλή κλίμακα πιθανότητας και με το μέγιστο δυνητικό αντίκτυπο και επιλέχθηκε διότι συνδυάζει τον Επιστημονικό-Τεχνολογικό με όλους τους άλλους τομείς. Η απώλεια μυστικών που σχετίζεται με τον εκσυγχρονισμό των πυρηνικών όπλων μπορεί να οδηγήσει σε παγκόσμιες ανακατανομές ισχύος, αλλαγή του «status quo», κοινωνικές αναταραχές και να δημιουργήσει δυνητικές εκβάσεις όχι μόνο στο κράτος ¨θύτη¨, αλλά και στο διεθνές περιβάλλον. Σημαντικός παράγοντας

επιπλέον είναι ότι το προσωπικό που εργάζεται σε αυτό τον τομέα είναι κατά κόρον πολίτες-ιδιώτες, επιστήμονες από διάφορες ξένες χώρες και κρατικό μη διαβαθμισμένο (ορισμένες φορές) προσωπικό, όπου ο κίνδυνος διαρροής πληροφοριών εμφανίζει υψηλή πιθανότητα εκδήλωσης.

6.3.1 Δεντρική ανάλυση κινδύνου – Event tree analysis

Σενάριο: Ως αρχικό περιστατικό ορίζεται η υποκλοπή μυστικών αρχείων που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων από εργοστάσιο κατασκευής τους. Η παραβίαση και η κλοπή πραγματοποιήθηκε από προσωπικό του εργοστασίου που αποτελεί και το πιο πιθανό μέσω, λόγω τον μέτρων που ασφαλείας που υπάρχουν σε τέτοιου είδους εργοστάσια.



Πίνακας 4

6.3.2 Πιθανές Εκβάσεις

- Έκβαση 1: Πρόκληση αναστάτωσης στην πολιτική και στρατιωτική ηγεσία, στις μυστικές υπηρεσίες, στη διοίκηση και το προσωπικό του εργοστασίου. Υλοποίηση έρευνα εύρεσης δικτύου και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου. Επιβολή ποινικών κυρώσεων στους εμπλεκομένους.

- Έκβαση 2: Πρόκληση συναγερμού απώλειας μυστικών αρχείων για τον εκσυγχρονισμό πυρηνικών όπλων. Υλοποίηση έρευνα εύρεσης δικτύου και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Αναστάτωση στην πολιτική και στρατιωτική ηγεσία, στη διοίκηση και το προσωπικό του εργοστασίου. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου και επιβολή ποινικών κυρώσεων στους εμπλεκομένους. Πιθανές καταστροφικές συνέπειες σε παγκόσμιο επίπεδο.

- Έκβαση 3: Απώλεια μυστικών τεχνολογίας πυρηνικών όπλων. Πρόκληση συναγερμού εύρεσης συνεργάτη, δικτύου και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Αναστάτωση στην πολιτική και στρατιωτική ηγεσία, στις μυστικές υπηρεσίες, στη διοίκηση και το προσωπικό του εργοστασίου. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου και επιβολή ποινικών κυρώσεων στους εμπλεκομένους. Πιθανές καταστροφικές συνέπειες σε παγκόσμιο επίπεδο.

- Έκβαση 4: Πρόκληση αναστάτωσης στην πολιτική και στρατιωτική ηγεσία, στις μυστικές υπηρεσίες, στη διοίκηση και το προσωπικό του εργοστασίου. Υλοποίηση έρευνα εύρεσης πιθανού δικτύου και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου και επιβολή ποινικών κυρώσεων στους εμπλεκομένους.

- Έκβαση 5: Πρόκληση αναστάτωσης στην πολιτική και στρατιωτική ηγεσία, στις μυστικές υπηρεσίες, στη διοίκηση και το προσωπικό του εργοστασίου. Υλοποίηση έρευνα εύρεσης πιθανού δικτύου και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου και επιβολή ποινικών κυρώσεων στους εμπλεκομένους. Πιθανή καταστροφή αρχείων από το δράστη.

- Έκβαση 6: Απώλεια μυστικών τεχνολογίας πυρηνικών όπλων. Πρόκληση συναγερμού εύρεσης του δράστη, συνεργάτη, πιθανού δικτύου συνεργασίας και τελικού αποδέκτη των πληροφοριών από μυστικές υπηρεσίες. Αναστάτωση στην πολιτική και στρατιωτική ηγεσία, στις μυστικές υπηρεσίες, στη διοίκηση και το προσωπικό του εργοστασίου. Λήψη επιπρόσθετων μέτρων ασφαλείας, αύξηση καμερών κλειστού κυκλώματος και ελέγχου στις πύλες εισόδου του εργοστασίου και επιβολή κυρώσεων στους εμπλεκομένους. Πιθανές καταστροφικές συνέπειες σε παγκόσμιο επίπεδο.

- Έκβαση 7: Όπως Έκβαση 6.

7. Συμπεράσματα – Επίλογος

Είναι σαφές ότι η οικονομική κατασκοπεία έχει αποτελέσει ένα ισχυρό ¨όπλο¨ στην παγκόσμια ¨μάχη¨ της οικονομικής και τεχνολογικής υπεροχής. Το άναρχο διεθνές περιβάλλον, η απουσία ενός διεθνούς ¨Λεβιάθαν¨ και ο διεθνής ανταγωνισμός ενισχύουν την ύπαρξή της. Τα βαθύτερα κίνητρα άσκησης της είναι τόσο ισχυρά που δεν αφήνει αμέτοχα τα ισχυρά κράτη, με απώτερο σκοπό τη διατήρηση ή αύξηση της ισχύς τους στην παγκόσμια οικονομική σκακιέρα.

Σχετικά με τις χώρες ενδιαφέροντος, οι ΗΠΑ και η Κίνα αποτελούν δύο κράτη όπου μέχρι και σήμερα έχουν βρει κοινό έδαφος ενάντια σε διεθνείς εγκληματικές οργανώσεις, βελτιώνοντας τις σχέσεις συνεργασίας τους σε επιχειρηματικό επίπεδο και τα τελευταία χρόνια έχει παρατηρηθεί βελτίωση στις απόψεις σχετικά με την πνευματική ιδιοκτησία. Παρόλα αυτά η ύπαρξη οικονομικής κατασκοπείας είναι εμφανής. Η μεταφορά οικονομικών πληροφοριών και τεχνολογίας αποτελεί μια από τις μεγαλύτερες προκλήσεις των χωρών αυτών και κυρίως των ΗΠΑ. Ωστόσο μας επανέρχεται το ερώτημα *«Μπορεί η οικονομική κατασκοπεία να συμβάλλει στην απόκτηση τεχνολογικού πλεονεκτήματος ανάμεσα σε δύο χώρες αλλάζοντας τις υπάρχουσες ισορροπίες;».*

Οι ΗΠΑ έχουν αποτελέσει διαχρονικά το μεγαλύτερο ¨θύμα¨ οικονομικής κατασκοπείας, και όχι μόνο της Κίνας. Η συνεχής ανάπτυξη στον τομέα της οικονομίας και της επιστήμης-τεχνολογίας έχουν ορίσει τις ΗΠΑ ως ηγέτιδα δύναμη. Κάτι το οποίο ωθεί τις υπόλοιπες ανταγωνίστριες χώρες στην άσκηση οικονομικής κατασκοπείας κατά της. Η τεχνολογική ανάπτυξη και υπεροχή ενός κράτους προέρχεται μέσα από τους τομείς της οικονομίας και της επιστήμης, τομείς που συνδέονται άμεσα με τη στρατιωτική ισχύ και κατά επέκταση την εθνική ασφάλεια. Οι ΗΠΑ χρησιμοποιούν την οικονομική αντικατασκοπεία ως μέτρο στρατηγικής για την διατήρηση της εθνικής ασφάλειας, την εξασφάλιση της θέσης της ως ηγέτιδα δύναμη, τη διατήρηση του ¨status quo¨, την εξασφάλιση της ευημερίας των πολιτών της και γενικότερα την διατήρηση και αύξηση της παγκόσμιας ισχύς της στη διεθνή σκακιέρα της οικονομικής πολιτικής. Χαρακτηριστικό μάλιστα είναι το πρόσφατο σύμφωνο ασφαλείας, ¨AUKUS¨ (Three Eyes Alliance), στην Ασία-Ειρηνικό των ΗΠΑ με το Ηνωμένο Βασίλειο και την Αυστραλία, με σκοπό την αντιμετώπιση της Κίνας. Ένα σύμφωνο που καλύπτει θέματα

πυρηνικής συνεργασίας, τεχνητής νοημοσύνης, κυβερνοχώρου, θαλάσσιας τεχνολογίας και άλλων θεμάτων αποτελώντας μια από τις μεγαλύτερες συνεργασίες τα τελευταία χρόνια.

Από την αντίπερα όχθη η Κίνα ως μια χώρα που χαρακτηρίζεται τα τελευταία χρόνια για τη ραγδαία ανάπτυξη της οικονομίας και της τεχνολογίας, χρησιμοποιεί την οικονομική κατασκοπεία ως εργαλείο οικονομικής ανάπτυξης και πολιτικής σταθερότητας. Τα παραδείγματα άσκησης της είναι αδιαμφησβήτητα και την τοποθετούν πρωτοπόρα στην άσκηση οικονομικής κατασκοπείας κατά των ΗΠΑ. Επιπροσθέτως από την ίδρυση της Δημοκρατίας της Κίνας και σταδιακά μέχρι σήμερα, παρατηρείτε ένα αξιόλογο σχέδιο ανάπτυξης και εξέλιξης της χώρας που παρά την πάροδο των χρόνων έχει μείνει αναλλοίωτο. Η αφοσίωση στους στόχους της και στις επιδιώξεις της αποτελούν είναι ισχυρό δείκτη πειθαρχίας και μεθοδικότητας. Η διαχρονική προσπάθεια της Κίνας είναι αξιοσημείωτη και αποδεικνύει όχι μόνο τις προθέσεις για την εξασφάλιση της ευημερίας των πολιτών της, αλλά και την αύξηση της ισχύς της στη παγκόσμια διεθνή σκηνή. Επιπλέον η Κίνα ως κράτος-μέλος των BRICS αποτελεί γενικότερα μια χώρα που βρίσκεται στην αντίπερα όχθη από της συμμαχίες των ΗΠΑ και του ΝΑΤΟ, καθώς και την Ευρωπαϊκή Ένωση και το Διεθνές Νομισματικό Ταμείο, εκπροσωπώντας μεγάλο μέρος των αναδυόμενων δυνάμεων επιρροής της.

Όπως προαναφέρθηκε η οικονομική κατασκοπεία μπορεί να χρησιμοποιηθεί ως ένα εργαλείο αύξησης τεχνολογικής - οικονομικής ανάπτυξης, στρατιωτικής ισχύς και ευημερίας. Ο πολυδιάστατος χαρακτήρας της, την καθιστά ως ένα πολύ σημαντικό παράγοντα ισχύος σε παγκόσμιο επίπεδο, δεδομένου ότι συνδέεται και με την κατασκευή πυρηνικών όπλων.

Η πυρηνική αποτροπή αποτελεί από τον 20ο αιώνα το πιο ισχυρό μέσω αποτροπής και εξασφάλισης εθνικής ασφάλειας. Ωστόσο ο ΟΗΕ το 2017 παρουσίασε τη «Συνθήκη Απαγόρευσης Πυρηνικών Όπλων (TPNW)», όπου αποτελεί το πρώτο νομικό κείμενο παγκοσμίως που αφορά την εξάλειψη των πυρηνικών όπλων. Παρά τη συνθήκη, η οποία δεν έχει τεθεί ακόμα σε ισχύ, οι παγκόσμιες πυρηνικές δυνάμεις εκσυγχρονίζουν τα πυρηνικά οπλοστάσια τους. Οι ΗΠΑ διαθέτουν περίπου 6.185 πυρηνικά όπλα με την πρώτη δοκιμή το 1945, ενώ η Κίνα περίπου 290 με πρώτη δοκιμή το 1964. Μάλιστα το Μάιο του 2016 η Κίνα προειδοποίησε το Πεντάγωνο ότι επιδιώκει να γίνει η Τρίτη χώρα με «Πυρηνική Τριάδα».

Από την αναγνώριση και ανάλυση των κινδύνων που προκύπτουν από την άσκηση οικονομικής κατασκοπείας, ως πιο σημαντικός προέκυψε η ¨Υποκλοπή μυστικών που αφορούν τον εκσυγχρονισμό πυρηνικών όπλων¨. Ένας κίνδυνος, η εκδήλωση του οποίου μπορεί να επιφέρει αλλαγές στις παγκόσμιες ισορροπίες, αλλάζοντας το τεχνολογικό πλεονέκτημα μεταξύ δύο χωρών ¨θύμα¨ και ¨θύτης¨. Ωστόσο, ένας τέτοιου

επιπέδου κίνδυνος θα επιφέρει αλλαγές όχι μόνο στο υπάρχον ¨status quo¨ των δύο εμπλεκομένων κρατών, αλλά θα επηρεάσει και τις υπάρχουσες παγκόσμιες ισορροπίες ισχύος.

Συνοψίζοντας και ολοκληρώνοντας τη μελέτη επιβεβαιώνεται η άρρηκτη σχέση της οικονομικής κατασκοπείας με την εθνική ασφάλεια ενός κράτους. Οι ΗΠΑ και η Κίνα, ως χώρες με μεγάλο ανταγωνισμό, τη χρησιμοποιούν ως ένα εργαλείο προστασίας και ανάπτυξης αντίστοιχα. Ένας αόρατος ¨πόλεμος¨ υπό το πρίσμα συμφωνιών, συνεργασιών και διπλωματικών διαπραγματεύσεων που πρόκειται να συνεχιστεί σε μακροπρόθεσμο διάστημα.

Κατάλογος πηγών – Βιβλιογραφία

Andrew, Christopher M. (2018), the Secret World: A History of Intelligence. New Haven: Yale University Press.

Bellocchi, Luke P. (2001), 'Assessing the Effectiveness of the Economic Espionage Act of 1996'. International Journal of Intelligence and CounterIntelligence 14(3): 366–87.

Brander James A. (1998), «The Economics of Economic Intelligence» στο Potter Evan N. (επίμ.), Economic Intelligence and National Security, Carleton University Press.

Buzan Barry (1991), "Is International Security Possible?" in Booth Ken (ed.), New Thinking About Strategy and International Security, HarperCollins.

Buzan Barry (1991), People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era, Harvester Wheatsheaf.

CASTA-USA (2016), ¨Chinese Association for Science and Technology¨, CASTA-USA. Διαθέσιμο στη δνση: https://www.cast-usa.us/organization. Πρόσβαση: 25/8/2021

Costello John-Tsarev Oleg (1993), Deadly Illusions: The KGB Orlov Dossier Reveals Stalin's Master Spy, New York, Crown Publishers, σ. 31, 42

CSIS (Center of strategic & International Studies) Evan Burke, Matthew Serrone, Khristal Thomas, Arthur Nelson, and Ian Haimowitz. Διαθέσιμο στη δ/νση https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000. Πρόσβαση: 26/7/2021

Eftimiades, Nicholas (1993), 'China's Ministry of State Security: Coming of Age in the International Arena'. Intelligence and National Security 8(1): 23–43.

Evans Graham and Newnham Jeffrey (1998), The Penguin Dictionary of International Relation, Penguin Books

Evans Joseph C. (1994), ¨U.S. Business Competitiveness and the Intelligence Community¨. International Journal of Intelligence and Counterintelligence 7, τχ. 3: 353–61.

Executive office of the President of the United States (2013), ¨Administration Strategy on Mitigating the Theft of U.S. Trade Secrets¨, The United States Department of Justice. Διαθέσιμο στη δ/νση: https://www.justice.gov/criminal-ccips/file/938321/download. Πρόσβαση: 2/8/2021

Fialka, John J. (1999), War by Other Means: Economic Espionage in America. New York: Norton.

Fort Randall M. (1995), "Economic Espionage", στο Godson R., May E., Schmitt G., U.S. Intelligence at the Crossroads, p. 181.

Hannas, William C., James Mulvenon, and Anna B. Puglisi (2013), Chinese Industrial Espionage, Routledge. Διαθέσιμο στη δ/νση: https://www.taylorfrancis.com/books/9781135952549. Πρόσβαση 23/7/2021

Holt, Alexander. (2020), 'A Brief History of US- China Espionage Entanglements', MIT Technology Review. Διαθέσιμο στη δ/νση https://www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/. Πρόσβαση: 3/7/2021

IRGC (2005), White Paper No1 "Risk Governance – Towards an Integrative Approach", IRGC, Geneva.

IRGC (2019), ¨Improving Governance of Systemic Risks¨, IRGC. Διαθέσιμο στη δνση: https://irgc.org. Πρόσβαση: 9/7/2021

Jensen, Carl J., David McElreath, και Melissa Graves. 2018. Introduction to Intelligence Studies. Second edition. New York, NY: Routledge.

Johnson K. Loch (1996), Secret Agencies: U.S Intelligence in a Hostile Word, Yale University Press, σ. 147-8

Johnson, Leighton (2019), Security controls evaluation, testing, and assessment handbook. 2ο έκδ. San Diego: Academic press is an imprint of Elsevier. Διαθέσιμο στη δνση: https://www.sciencedirect.com/topics/computer-science/economic-espionage-act. Πρόσβαση: 5/8/2021

Johnson, Loch K. (2009), ¨Think Again: Spies¨, Foreign Policy, Διαθέσιμο στη δ/νση https://foreignpolicy.com/2009/11/19/think-again-spies/. Πρόσβαση: 30/7/2021

Johnson, Loch K. (2009), Handbook of Intelligence Studies. London: Routledge. Διαθέσιμο στη δνση:

http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9780203089323. Πρόσβαση: 3/7/2021

Jonathan E. Lewis (2009), ¨the Economic Espionage Act and the Threat of Chinese Espionage in the United States¨, 8 Chi. -Kent J. Intell. Prop. 189. Διαθέσιμο στη δ/νση: https://scholarship.kentlaw.iit.edu/ckjip/vol8/iss2/2. Πρόσβαση: 1/7/2021

Kent Sherman (1949), Strategic Intelligence for American World Policy (Princeton, NJ: Princeton University Press), σ. 34-5.

Konstantopoulos, Ioannis L. (2007), "Economic Espionage and Economic Security in an Age of Change" Paper to Be Presented at the "Seventh International CISS Millennium Conference", Buçaco, Portugal, June 14-16, 2007'. : 57.

Lindsay, Jon R., Tai Ming Cheung, και Derek S. Reveron (2015), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. New York: Oxford University Press.

Lowenthal, M. M. (2003), Intelligence: from Secrets to Policy, CQ Press.

Luttwak, E.N. & Koehl, S. L. (1999), The Dictionary of Modern War: A Guide to the Ideas, Institutions and Weapons of the Modern Military Power Vocabulary, Gramercy Books.

Malcolm, Noel (2015), Agents of empire: knights, corsairs, Jesuits and spies in the sixteenth-century Mediterranean world. Oxford ; New York: Oxford University Press.

Mattis, Peter L. (2012), 'Assessing Western Perspectives on Chinese Intelligence'. International Journal of Intelligence and CounterIntelligence 25(4): 678–99.

Nasheri Hedieh (2005), Economic Espionage and Industrial Spying, Cambridge University Press, Π. 16.

Neilson, Keith and B. J. C. McKercher (επιμ. 1992), Go spy the land: military intelligence in history, Westport, Conn: Praeger.

Scott James and Drew Spaniel (2016), China's Espionage Dynasty "Economic Death by a Thousand Cuts", Institute for Critical Infrastructure Technology, The Cybersecurity Think Tank

See the White House (1999), A National Security Strategy for a New Century, December 1999, op. cit., pp. 1^3.

Sheldon, Rose Mary. (2005), Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify. 1. publ. London: Cass.

Sherman Kent (1966), Strategic Intelligence for American World Policy, Princeton University Press.

Soll, Jacob (2009), The Information Master: Jean- Baptiste Colbert's Secret State Intelligence System, Ann Arbor: University of Michigan Press.

Terje Aven and Ortwin Renn (2010), Risk Management and Governance, Springer.

The United States – Department of Justice (2020), Διαθέσιμο στη δ/νση: https://www.justice.gov

The United States Department of Justice (2020), ¨ 9-59.110 - Economic Espionage Act-Assignment of Responsibilities¨, The United States Department of Justice. Διαθέσιμο στη δνση: https://www.justice.gov/jm/jm-9-59000-economic-espionage. Πρόσβαση: 10/8/2021

The White House (2021), ¨NSG2021 (Interim National Security Strategic Guidance)¨, The White House. Διαθέσιμο στη δ/νση: https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/. Πρόσβαση: 28/6/2021

Tzu Sun (2003), Η τέχνη του πολέμου, InfoBooks, σ. 24-27.

Zelikow, Philip. (1997), 'American Economic Intelligence: Past Practice and Future Principles'. Intelligence and National Security 12(1): 164–77.

Κωνσταντόπουλος Ι. (2010), Οικονομία και Κατασκοπεία «Θεωρία και πράξη», Εκδ. Ποιότητα)

Κωνσταντόπουλος Ι. (2018), Πληροφόρηση και Ασφάλεια: Μία άρρηκτη σχέση, Πανεπιστήμιο Θεσσαλίας