



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

Πρόγραμμα Μεταπτυχιακών Σπουδών  
«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

**Οικονομική Κατασκοπεία**  
**Υποκλοπή Οικονομικών Πληροφοριών και Τεχνολογίας**  
**από Υπηρεσίες Πληροφοριών**

*Μεταπτυχιακή Διπλωματική Εργασία*

**Κωνσταντίνος Ι. Ψυχογιός**

Τριμελής Επιτροπή:

Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος

Επίκουρος Καθηγητής Ε. Φακιολάς

Αναπληρωτής Καθηγητής Ν. Κουτσούκης

**Κόρινθος, 2018**



**UNIVERSITY OF PELOPONNESE  
SCHOOL OF SOCIAL AND POLITICAL SCIENCES  
DEPARTMENT OF POLITICAL SCIENCES AND  
INTERNATIONAL RELATIONS**

Master of Arts in  
“Global Risks and Analytics”

**Economic Espionage  
Interception of Economic Information and Technology  
by Intelligence Services**

*Master’s Dissertation*

**Constantinos I. Psychogyios**

Supervisors:

Assistant Professor I. Konstantopoulos

Assistant Professor E. Fakiolas

Associate Professor N. Koutsoukis

**Corinth, 2018**

## Φύλλο Αξιολόγησης

Η διπλωματική εργασία με τίτλο «Οικονομική Κατασκοπεία. Υποκλοπή Οικονομικών Πληροφοριών και Τεχνολογίας από Υπηρεσίες Πληροφοριών» του Κωνσταντίνου Ψυχογιού 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 ... / ... /.....

με γενική επίδοση:

- Καλώς
- Λίαν Καλώς
- Άριστα

Τα μέλη της Τριμελούς Επιτροπής:

1. Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος
2. Επίκουρος Καθηγητής Ε. Φακιολάς
3. Αναπληρωτής Καθηγητής Ν. Κουτσούκης

## **Abstract**

The dissertation research focuses on economic espionage activities in modern times. The researcher wonders, what is the role of the intelligence services, what methods are used to gather the information they need for the benefit of their employers, and whether these methods follow ethical standards. Below are some cases of economic espionage that occurred in the past and which have been made public, either because they were perceived or classified as non-confidential by the actors. The main objective of this dissertation is to demonstrate the ways and means used by intelligence services to obtain the necessary information from the economy and technology. The researcher analyzes the methods of practice of economic espionage through computer interceptions, wireless and wired telecommunications, and interceptions through speeches in space. The researcher wonders whether the action of economic espionage involves increasing product efficiency, reducing production costs or, where appropriate, increasing the growth rate of businesses supported by the actors. Is there a risk of causing political and social problems due to the interception of sensitive information? Are political crises inside and outside the state addressed by economic espionage? The researcher analyzes the prevention strategies of economic espionage in a company or a government organization through literature review and interviews with people working in the intelligence field.

## **Key Words**

Espionage, Economic Espionage, Interception, Intelligence, Information, Intelligence Services, Counterintelligence, Signals Intelligence.

## Περίληψη

Η έρευνα της διπλωματικής εργασίας εστιάζει στις δραστηριότητες της οικονομικής κατασκοπείας στην σύγχρονη εποχή. Ο ερευνητής διερωτάται ποιος είναι ο ρόλος των υπηρεσιών πληροφοριών, με ποιες μεθόδους δρουν για να αποσπάσουν τις πληροφορίες που επιθυμούν προς όφελος των εργοδοτών τους, κι αν αυτές οι εφαρμοζόμενες μέθοδοι τηρούν πρότυπα δεοντολογίας. Γίνεται αναφορά σε περιστατικά οικονομικής κατασκοπείας που έλαβαν χώρα κατά το παρελθόν και τα οποία έχουν δημοσιοποιηθεί, είτε γιατί έγιναν αντιληπτά, είτε γιατί χαρακτηρίστηκαν ως μη απόρρητα, από τους δρώντες. Ο βασικός στόχος της παρούσας μελέτης είναι να επιδείξει τους τρόπους και τα μέσα που χρησιμοποιούνται από τα στελέχη των υπηρεσιών πληροφοριών για να αποκτήσουν τις πληροφορίες που επιθυμούν, από τον τομέα της οικονομίας και της τεχνολογίας. Ο ερευνητής αναλύει τις μεθόδους εφαρμογής της οικονομικής κατασκοπείας μέσω υποκλοπών από ηλεκτρονικούς υπολογιστές, ασύρματες και ενσύρματες τηλεπικοινωνίες, καθώς επίσης και υποκλοπές μέσα από ομιλίες στον χώρο. Επίσης, ο ερευνητής διερωτάται για το εάν η άσκηση της οικονομικής κατασκοπείας, συνεπάγεται την αύξηση της αποδοτικότητας των προϊόντων, την μείωση του κόστους παραγωγής ή ανάλογα με την περίπτωση, τον ρυθμό ανάπτυξης των επιχειρήσεων που υποστηρίζουν με την δράση τους οι δρώντες της οικονομικής κατασκοπείας. Παράλληλα, είναι υπαρκτός ο κίνδυνος της πρόκλησης πολιτικών και κοινωνικών προβλημάτων, λόγω της υποκλοπής ευαίσθητων πληροφοριών; Αντιμετωπίζονται μέσω της οικονομικής κατασκοπείας πολιτικές κρίσεις εντός κι εκτός κράτους; Τέλος, αναλύονται οι στρατηγικές αποτροπής της οικονομικής κατασκοπείας εντός μιας επιχείρησης ή ενός κρατικού οργανισμού. Η έρευνα διεξήχθη μέσω βιβλιογραφικής ανασκόπησης και προσωπικών συνεντεύξεων με άτομα που εργάζονται στον χώρο των πληροφοριών.

## Λέξεις Κλειδιά

Κατασκοπεία, Οικονομική Κατασκοπεία, Υποκλοπή, Πληροφόρηση, Πληροφορία, Υπηρεσίες Πληροφοριών, Αντικατασκοπεία, Παρακολούθηση.

## Ευχαριστίες

Θα ήθελα καταρχάς να ευχαριστώ όλες και όλους όσους συνέβαλαν στην επιτυχή εκπόνηση της διπλωματικής μου εργασίας. Πρωτίστως και κυρίως τον επιβλέποντα καθηγητή μου, κ. Ιωάννη Κωνσταντόπουλο για την εμπιστοσύνη που έδειξε στο πρόσωπο μου για την εκπόνηση της παρούσας διπλωματικής εργασίας, καθότι ως πρωτοπόρος στην χώρα μας στο επιστημονικό αντικείμενο της Οικονομικής Διπλωματίας και Κατασκοπείας αποτελεί φάρο γνώσεως για όλους εμάς, τους φοιτητές του, αλλά και πυρήνα της έρευνας σε εθνικό επίπεδο.

Εν συνεχεία, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του Μεταπτυχιακού Προγράμματος Σπουδών για την μεταλαμπάδευση του εξαιρετικού επιπέδου γνώσεων που μου προσέφεραν, καθώς επίσης και τους λοιπούς ακαδημαϊκούς και αξιωματικούς των Ενόπλων Δυνάμεων της χώρας μας, που κατά την διάρκεια των σπουδών μου είχα ως καθοδηγητές και οι οποίοι εκτός από γνώσεις, με γέμισαν και με εμπειρίες.

Επιπροσθέτως, θα ήθελα να ευχαριστήσω όλους εκείνους τους ανθρώπους, πέραν του ακαδημαϊκού περιβάλλοντος, που στάθηκαν δίπλα μου. Τους γονείς μου, τους συγγενείς μου, τους συναδέλφους, τις φίλες και τους φίλους μου, οι οποίοι έστω κι αν βρισκόμουν μακριά τους τον περισσότερο καιρό, με βοήθησαν να διατηρήσω την ψυχική μου ηρεμία αυτούς τους δύσκολους μήνες, της μελέτης και συγγραφής της διπλωματικής εργασίας, στην διάρκεια των οποίων προέκυψαν πάρα πολλές υποχρεώσεις.

Την παρούσα διπλωματική εργασία την αφιερώνω σε όλους αυτούς που υπηρετούν Αρχές, Αξίες και Ιδανικά και θυσιάζονται για αυτά τους τα πιστεύω, καθότι αποτελούν πρότυπο και πηγή έμπνευσης για εμένα.

## Πρόλογος

Στο 1<sup>ο</sup> κεφάλαιο γίνεται η θεωρητική θεμελίωση του θέματος της διπλωματικής εργασίας. Στην συνέχεια γίνεται η περιγραφή των ορισμών της πληροφορίας (information), της πληροφορόρησης (intelligence), της κατασκοπείας (espionage), της αντικατασκοπείας (counter intelligence), της ηλεκτρονικής παρακολούθησης (signals intelligence), της υποκλοπής (interception) και της τεχνολογίας πληροφοριών (I.T.) και των δεδομένων (data). Τέλος, γίνεται βιβλιογραφική ανασκόπηση και περιγράφεται η μεθοδολογία της έρευνας.

Στο 2<sup>ο</sup> κεφάλαιο γίνεται αναφορά στις υπηρεσίες πληροφοριών (intelligence services), τις κατηγορίες που διαχωρίζονται και τον ρόλο τους. Επίσης, αναφέρονται εξειδικευμένα τμήματα που διαθέτουν οι υπηρεσίες πληροφοριών και ο τρόπος δράσης τους.

Στο 3<sup>ο</sup> κεφάλαιο δίνεται ο ορισμός της οικονομικής κατασκοπείας (economic espionage), των και πώς αυτή εφαρμόζεται. Απαντάται το ερώτημα για το αν ένα κράτος που κάνει υποκλοπές οικονομικών πληροφοριών και τεχνολογίας ωφελείται ή ζημιώνεται από αυτή του την δραστηριότητα. Και τέλος γίνεται αναφορά στην ανταγωνιστική ευφυΐα (competitive intelligence).

Στο 4<sup>ο</sup> κεφάλαιο αυτό αναλύονται η έννοια του διπλώματος ευρεσιτεχνίας, των εμπορικών μυστικών, γίνεται ο προσδιορισμός των ιδιοκτησιακών πληροφοριών, περιγράφονται οι στόχοι της οικονομικής κατασκοπείας εντός ενός οργανισμού και οι τρόποι διεξαγωγής των υποκλοπών.

Στο 5<sup>ο</sup> κεφάλαιο αναφέρονται τα συμπεράσματα που προέκυψαν από την έρευνα επί του θέματος της διπλωματικής εργασίας.

## Πίνακας Περιεχομένων

Abstract .....	I
Περίληψη .....	II
Ευχαριστίες.....	III
Πρόλογος .....	IV
Περιεχόμενα .....	V
<b>1. Εισαγωγή.....</b>	<b>1</b>
1.1. Θεωρητική θεμελίωση .....	1
1.2. Ορισμοί και σημασία του θέματος .....	2
1.2.1. Πληροφορία (information) και πληροφόρηση (intelligence) .....	2
1.2.2. Κατασκοπεία (espionage) και αντικατασκοπεία (counterintelligence).....	3
1.2.3. Παρακολούθηση (signals intelligence) και υποκλοπή (interception) .....	4
1.2.4. Τεχνολογία πληροφοριών (information technology) και δεδομένα (data) .....	6
1.3. Βιβλιογραφική ανασκόπηση.....	8
1.4. Μεθοδολογία της έρευνας .....	8
<b>2. Υπηρεσίες πληροφοριών (intelligence services ή agencies).....</b>	<b>9</b>
2.1. Οι υπηρεσίες πληροφοριών και ο ρόλος τους .....	9
2.2. Μυστικές ή συγκεκαλυμμένες επιχειρήσεις (covert operations) και μετωπικές οργανώσεις (front organizations) .....	13
2.3. Επιχειρήσεις παραπληροφόρησης (disinformation campaigns) και ψυχολογικές επιχειρήσεις (psychological operations) .....	14
2.4. Αξιωματικός πληροφοριών (intelligence officer) .....	14
2.5. Συλλογή πληροφοριών (intelligence collection ή gathering) ....	15
<b>3. Οικονομική κατασκοπεία (economic espionage) .....</b>	<b>17</b>
3.1. Ορισμός και εφαρμογή οικονομικής κατασκοπείας.....	17
3.2. Πληροφορίες οικονομικού περιεχομένου (economic intelligence).....	18
3.3. Ανάλυση πληροφοριών (intelligence analysis) .....	19
3.4. Ωφελείται ή ζημιώνεται το κράτος που ασκεί οικονομική κατασκοπεία;.....	21
3.5. Ανταγωνιστική ευφυΐα (competitive intelligence) .....	23



<b>4. Προστασία από την οικονομική κατασκοπεία.....</b>	<b>26</b>
4.1. Δίπλωμα ευρεσιτεχνίας .....	28
4.2. Τεχνογνωσία και εμπορικά μυστικά.....	29
4.3. Οι στόχοι της οικονομικής κατασκοπείας εντός ενός οργανισμού .....	30
4.4. Προσδιορισμός και ένδειξη απειλής .....	31
4.5. Τρόποι διεξαγωγής των υποκλοπών.....	31
<b>Συμπεράσματα .....</b>	<b>33</b>
Κατάλογος Πηγών .....	35
Συντομογραφίες.....	39

# 1. Εισαγωγή

Το θέμα της διπλωματικής εργασίας εντάσσεται στον τομέα των Σπουδών Οικονομίας, Άμυνας και Ασφάλειας, που αποτελούν κλάδο των Διεθνών Σχέσεων και της Πολιτικής Επιστήμης γενικότερα. Η οικονομία και η κατασκοπεία είναι δυο τομείς που απασχολούν την ανθρωπότητα από την αρχαιότητα. Ο άνθρωπος πάντοτε αντιμετώπιζε το δίλημμα ανάμεσα στον πόλεμο και την διπλωματία.

Σε αυτό το κεφάλαιο γίνεται η θεωρητική θεμελίωση του θέματος της διπλωματικής εργασίας. Στην συνέχεια γίνεται η παρουσίαση των βασικών όρων: πληροφορία (information), πληροφόρηση (intelligence), υποκλοπή (interception), κατασκοπεία (espionage) και αντικατασκοπεία (counter espionage). Επίσης, γίνεται βιβλιογραφική ανασκόπηση και περιγράφεται η μεθοδολογία της έρευνας.

## 1.1. Θεωρητική θεμελίωση

Είναι γνωστό από τους αρχαίους συγγραφείς, ότι οι ηγέτες και οι στρατηγοί εφήρμοζαν σχέδια πολιτικά και στρατιωτικά, χρησιμοποιούσαν τεχνάσματα ή τακτικές της επιστήμης των Διεθνών Σχέσεων, για την επίτευξη των στόχων τους. Από την αρχαιότητα μέχρι και σήμερα, η οικονομία αποτελεί θεμέλιο της στρατιωτικής ισχύος και αυτόνομο εργαλείο της άσκησης εξωτερικής πολιτικής ενός κράτους. Διαχρονικά στην ανθρώπινη ιστορία η οικονομική ευρωστία είναι βασικός παράγοντας για την διαμόρφωση και την ανάπτυξη των κρατών, καθώς τα επηρεάζει απόλυτα. Κατά τον θεωρητικό του πολιτικού ρεαλισμού, Kenneth Waltz, η ενδυνάμωση της συγκριτικής θέσης ισχύος αποτελεί τον πρωταρχικό στόχο ενός κράτους για να κινηθεί με μεγαλύτερη ευχέρεια, μεγαλύτερη επιρροή, να έχει περισσότερες δυνατότητες και λιγότερους κινδύνους στη διεθνή σκηνή, έτσι ώστε να επιβιώσει αλώβητο.

Στην σύγχρονη εποχή, η ισχύς των κυβερνήσεων είναι ανάλογη του οικονομικού επιπέδου των κρατών και ο συνδυασμός στρατηγικής και οικονομικής ισχύος οδηγεί τα κράτη που τις κατέχουν, σε θέση υπεροχής έναντι των άλλων. Αντιθέτως, τα κράτη που είναι οικονομικά αδύναμα, εξαρτώνται από τα άλλα για την ανάπτυξη τους, κάτι το οποίο τους δημιουργεί ανασφάλεια. Η άποψη που έχει διατυπώσει ο Barry Buzan – ομότιμος καθηγητής Διεθνών Σχέσεων του London School of Economics & Political Science (L.S.E.), είναι ότι οικονομική ασφάλεια είναι η επίτευξη εκείνων των οικονομικών συνθηκών που είναι απαραίτητες για την επιβίωση (Κωνσταντόπουλος 2010). Τα κράτη για να περιορίσουν την αστάθεια και την αβεβαιότητα στο πολιτικό και οικονομικό τους τομέα και να διαμορφώσουν ένα πιο σταθερό και ασφαλές περιβάλλον, δημιουργούν διακρατικές συμμαχίες.

Η άποψη που είχε διατυπώσει ο Hans Morgenthau – θεωρητικός του πολιτικού ρεαλισμού, είναι ότι η διεθνής πολιτική και κάθε είδους πολιτική είναι ένας αγώνας για ισχύ. Τα ισχυρά κράτη, σύμφωνα με την ρεαλιστική προσέγγιση, έχουν την επιθυμία να μεγιστοποιούν την

δύναμη τους και την ανάγκη διατήρησης της θέσης που κατέχουν. Αυτό επιτυγχάνεται μέσα από την συνεχή άσκηση επιρροής σε αδύναμα κράτη, αλλά και του περιορισμού της ανάπτυξης των άμεσων ανταγωνιστών τους. Μεταξύ άλλων, αυτό το καταφέρνουν μέσα από την αναζήτηση, απόκτηση και ανάλυση όσο το δυνατόν περισσότερων δεδομένων και πληροφοριών που θα τα οδηγήσουν στην επιθυμητή γνώση, μέσω της οποίας θα διατηρήσουν το πλεονέκτημα έναντι των αντιπάλων τους. Η διαδικασία μέσω της οποίας επιδιώκουν να αποκτήσουν αυτά τα δεδομένα και τις πληροφορίες που δεν έχουν στην κατοχή τους είναι η κατασκοπεία (espionage). Αυτή η γνώση, με τα δυνατά και τα αδύναμα σημεία των αντιπάλων, δίνει την δυνατότητα στις κυβερνήσεις των κρατών να λάβουν τις βέλτιστες αποφάσεις για την εθνική τους άμυνα και ασφάλεια.

Η ορθή πληροφόρηση, επομένως είναι ένα μέσο ενίσχυσης ενός κράτους αναφορικά με τους ανταγωνιστές του. Οι μεταβολές που έγιναν σε παγκόσμιο επίπεδο τους τελευταίους δύο αιώνες σε πολιτικό και οικονομικό επίπεδο, δημιούργησαν ένα νέο διεθνές σύστημα. Όπως αναφέρει ο Κωνσταντόπουλος (2010) η άριστη ανάπτυξη προκάλεσε μια ανακατανομή στον πλούτο και την ισχύ μεταξύ των κρατών και μετέβαλε την φύση του διεθνούς ανταγωνισμού, κάτι το οποίο επηρέασε σημαντικά τις αντιλήψεις για την εθνική ασφάλεια. Η πληροφορία και η τεχνολογία αποτελούν τις πιο σημαντικές παραγωγικές πηγές και ο νέος τους ρόλος συνέβαλε στην σύνδεση μεταξύ των πληροφοριών οικονομικού περιεχομένου και της οικονομικής ισχύος.

## 1.2. Ορισμοί και σημασία του θέματος

Προκειμένου να απαντηθεί το βασικό ερώτημα της θεωρίας, θα πρέπει πρωτίστως να οριστούν οι έννοιες της πληροφορίας και της πληροφόρησης, της κατασκοπείας και της αντικατασκοπείας, της παρακολούθησης και υποκλοπής, της τεχνολογίας πληροφοριών, των δεδομένων και της κατασκοπείας στον κυβερνοχώρο.

### 1.2.1. Πληροφορία (information) και πληροφόρηση (intelligence)

Ως πληροφορία θεωρείται το αποτέλεσμα της εξόρυξης και της επεξεργασίας ακατέργαστων δεδομένων, τα οποία διαμορφώνονται με τέτοιο τρόπο έτσι ώστε να αποκτούν νόημα και να είναι χρήσιμα στους ανθρώπους (Laudon & Laudon 2014). Πληροφορία, λοιπόν, είναι οποιασδήποτε μορφής δεδομένα (data) που έχουν συλλεχθεί και δεν έχουν αναλυθεί και μπορεί να καταστούν γνωστά ανεξάρτητα από την πηγή τους. Όταν αυτά περάσουν στο στάδιο της επεξεργασίας μπορούν να παράγουν πληροφόρηση (Κωνσταντόπουλος 2010). Ανεξαρτήτως αντικειμένου η πληροφορία είναι ένας στρατηγικός παράγων, η αξία του οποίου εξαρτάται από την ταχύτητα απόκτησής της ορθής πληροφορίας από το κατάλληλο άτομο. Σύμφωνα με τον θεωρητικό των πολιτικών επιστημών Joseph Nye (2003) – που διατέλεσε Αναπληρωτής Υπουργός Άμυνας για θέματα διεθνούς ασφάλειας (A.S.D.-I.S.A.) και Πρόεδρος του Εθνικού Συμβουλίου Πληροφοριών (N.I.C.) των Ηνωμένων

Πολιτειών της Αμερικής (Η.Π.Α.) κατά την περίοδο της Προεδρίας του Bill Clinton, οι πληροφορίες διακρίνονται σε τρεις διαστάσεις, ως ακολούθως:

- σε αυτές που περιλαμβάνουν δεδομένα, που εκτέμονται, μεταδίδονται και αναπαράγονται μέσα από ανοιχτές πηγές πληροφοριών (O.S.Int),
- σε αυτές που χρησιμοποιούνται από κρατικούς ή ιδιωτικούς οργανισμούς για να αποκτήσουν πλεονέκτημα έναντι των αντιπάλων τους (competitive intelligence), και
- σε αυτές που δίνουν γνώσεις ανεκτίμητης αξίας για τα σχέδια του αντιπάλου (strategic information).

Υπάρχουν πολλοί ορισμοί της έννοιας της πληροφόρησης (intelligence) η οποία είναι ευρύτερη της έννοιας της πληροφορίας (information) και έχει πολλές προεκτάσεις, διαστάσεις και τρόπους προσέγγισης. Η πληροφορία μετατρέπεται σε γνώση όταν χρησιμοποιείται για να ληφθούν αποφάσεις και όταν αναπτύσσονται οι κατάλληλες ενέργειες για τη λήψη αυτών των αποφάσεων. Έτσι λοιπόν, ως γνώση θεωρούνται εκείνες οι πληροφορίες που ένα άτομο, σε συνδυασμό με την εμπειρία και τις ικανότητές του, αξιοποιεί προκειμένου να λάβει μία απόφαση ή να επιλύσει κάποιο σύνθετο πρόβλημα (Vercellis 2009).

Σύμφωνα με τον Mark Lowenthal – που έχει διατελέσει Αντιπρόεδρος του Εθνικού Συμβουλίου Πληροφοριών (N.I.C.) των Η.Π.Α. και Αναπληρωτής Διευθυντής της Κεντρικής Υπηρεσίας Πληροφοριών (C.I.A.) για θέματα ανάλυσης και παραγωγής, η πληροφόρηση είναι ένα υποσύνολο της ευρύτερης κατηγορίας των πληροφοριών. Ενώ το σύνολο της πληροφόρησης αποτελεί πληροφορία, όλες οι πληροφορίες δεν αποτελούν πληροφόρηση (Κωνσταντόπουλος 2010). Η πληροφόρηση αναφέρεται στις πληροφορίες που δίνει μια υπηρεσία πληροφοριών στην πολιτική ηγεσία του κράτους για να λάβει τις αποφάσεις που χρειάζονται για τα θέματα εθνικής ασφάλειας.

### 1.2.2. Κατασκοπεία (espionage) και αντικατασκοπεία (counterintelligence)

Η κατασκοπεία, κατά τους πολιτικούς επιστήμονες Edward Luttwak και Stuart Koehl (1991), είναι μια μυστική μέθοδος για την συλλογή πληροφοριών από ανθρώπινες πηγές, οι οποίες είτε είναι αξιωματούχοι πληροφοριών ή άτομα άλλης εθνικότητας που λειτουργούν υπό κάλυψη σε μια ξένη χώρα, είτε συνεργαζόμενα άτομα ξένης εθνικότητας. Η κατασκοπεία από ανθρώπινες πηγές παρέχει ένα μικρό μέρος του συνόλου των πληροφοριών που συλλέγονται από τις μεγάλες δυνάμεις, όμως σε αντίθεση με την συλλογή πληροφοριών μέσω των τεχνικών μέσων, μπορεί να αποκαλύψει δραστηριότητες και να παρέχει κρίσιμες πληροφορίες για τα κίνητρα και τις προθέσεις πιθανών αντιπάλων (Κωνσταντόπουλος 2010).

Στις Ηνωμένες Πολιτείες της Αμερικής η κατασκοπεία ορίζεται ως η πράξη κατά την οποία η απόκτηση, παράδοση, εκπομπή, γνωστοποίηση ή λήψη πληροφοριών για την εθνική άμυνα,

γίνεται με πρόθεση η χρήση αυτών των πληροφοριών να πλήξουν τις Ηνωμένες Πολιτείες της Αμερικής ή να ωφελήσουν κάποιο άλλο κράτος. Σε αντίθεση με άλλες μορφές συγκέντρωσης πληροφοριών οι οποίες εφαρμόζονται εξ αποστάσεως, η κλασική κατασκοπεία σχετίζεται κυρίως με την πρόσβαση στον χώρο όπου φυλάσσονται οι επιθυμητές πληροφορίες και οι άνθρωποι που τις κατέχουν. Καθότι, λοιπόν, είναι η πρακτική της συγκέντρωσης εμπιστευτικών πληροφοριών, εν αγνοία των κατόχων τους, για να αποσπαστούν από τα εξουσιοδοτημένα άτομα που τις κατέχουν, χρησιμοποιείται κάποιο τέχνασμα ή γίνεται χρήση εξοπλισμού για να γίνει η υποκλοπή.

Η αντικατασκοπεία (counterintelligence ή counter espionage) αναφέρεται στις δραστηριότητες που έχουν σχεδιαστεί για την πρόληψη, την αναγνώριση και την αποτροπή της κατασκοπείας που γίνεται από ξένους κρατικούς οργανισμούς ή άλλες οντότητες. Αφορά το κομμάτι των απειλών που γίνεται από έναν ή περισσότερους αντιπάλους και έχουν ως στόχο να πλήξουν τους οργανισμούς μιας χώρας, μέσω της συγκέντρωσης πληροφοριών και την δολιοφθορά.

Με την ευρεία έννοια του όρου, η συλλογή και ανάλυση πληροφοριών και εν συνεχεία η δράση με σκοπό την προστασία ενός κράτους, έναντι των δραστηριοτήτων άλλων δρώντων, είναι αντικατασκοπεία. Σε αυτή συμπεριλαμβάνονται και οι δραστηριότητες των υπηρεσιών πληροφοριών του ίδιου του κράτους. Υπό την στενή έννοια η αντικατασκοπεία είναι η παρεμπόδιση ενός αντιπάλου από την απόκτηση γνώσεων-πληροφοριών, οι οποίες θα του προσδίδουν ένα πλεονέκτημα (Κωνσταντόπουλος 2010).

Η άποψη του Arthur Hulnick – που υπήρξε αξιωματούχος της C.I.A. και ομότιμος αναπληρωτής καθηγητής στο Πανεπιστήμιο της Βοστώνης, ήταν ότι αντικατασκοπεία είναι όταν συλλαμβάνονται οι κατάσκοποι του αντιπάλου και αυτή η δραστηριότητα αποτελεί μεγάλο μέρος της καθημερινότητας των μυστικών υπηρεσιών των Ηνωμένων Πολιτειών.

### 1.2.3. Παρακολούθηση (signals intelligence) και υποκλοπή (interception)

Η παρακολούθηση είναι άμεσα συνδεδεμένη με την κατασκοπεία αφού αποτελεί υποσύνολο της. Δεν είναι ένα σύγχρονο φαινόμενο, καθότι εάν ανατρέξει κανείς στην ιστορία θα διαπιστώσει ότι από την αρχαιότητα πραγματοποιούνταν παρακολουθήσεις, αλλά αυτό συνέβαινε κυρίως σε περίοδο πολέμου. Στη σημερινή εποχή αυτό δε φαίνεται να συμβαίνει και τα γεγονότα δείχνουν ότι δεν υπάρχει κανείς περιορισμός στην άσκηση της παρακολούθησης και της υποκλοπής του αντιπάλου.

Η έννοια της παρακολούθησης, στην παρούσα μελέτη, αφορά στη συλλογή πληροφοριών μέσω υποκλοπής σημάτων (Sig.Int.), είτε από επικοινωνία μεταξύ ατόμων (Com.Int.), είτε από ηλεκτρονικά σήματα (El.Int.). Η υποκλοπή θα πρέπει να διακριθεί από την έννοια της κατασκοπείας. Καθότι η διεξαγωγή μυστικών επιχειρήσεων ενός κράτους για να αποκτήσει πληροφορίες από ένα άλλο, η στρατολόγηση ενός ξένου αξιωματούχου μέσω της χρήσης

ανθρώπινου δυναμικού, η υποκλοπή τηλεφωνικών συνομιλιών και η χρήση δορυφόρου για τον εντοπισμό ενός στόχου, έχουν το ίδιο αντικειμενικό σκοπό, που είναι η πληροφόρηση, αλλά γίνονται με εντελώς διαφορετικό τρόπο.

Γενικά ο όρος της ηλεκτρονικής κατασκοπείας ή παρακολούθησης αναφέρεται σε στοχευμένες ενέργειες διείσδυσης σε συστήματα και ηλεκτρονικά δίκτυα του αντιπάλου, με σκοπό την απόκτηση πληροφοριών που βρίσκονται σε αυτά, είτε διέρχονται από αυτά. Μια από τις βασικές δράσεις της Sig.Int. είναι να υποκλέπτει τις επικοινωνίες μεταξύ δύο ή περισσότερων ατόμων, έτσι ώστε να δώσει στο αρμόδιο τμήμα την στοχευμένη πληροφορία που χρειάζοταν. Αυτό πραγματοποιείται με την χρήση αλγορίθμων κι άλλων ερευνητικών διαδικτυακών μεθόδων, προκειμένου να συλλεχθούν και να ταξινομηθούν οι πληροφορίες από έναν τεράστιο όγκο επικοινωνιών.

Η παρακολούθηση διαχωρίζεται σε δύο κατηγορίες, ως ακολούθως:

- την εσωτερική παρακολούθηση, που εστιάζει στις επικοινωνίες των πολιτών ενός κράτους από τις μυστικές του υπηρεσίες, εντός της επικράτειας του, και
- την εξωτερική παρακολούθηση, που εστιάζει στις επικοινωνίες, εν καιρώ ειρήνης, αξιωματούχων ή των πολιτών ενός κράτους από τις μυστικές του υπηρεσίες, εκτός της επικράτειας του.

Η εξωτερική παρακολούθηση που διενεργεί ένα κράτος, μπορεί να διαχωριστεί σε δύο επιμέρους τύπους:

- την διακρατική παρακολούθηση, που λαμβάνει χώρα πέραν της επικράτειας του σε περισσότερα από ένα κράτη, συμπεριλαμβανομένων των περιπτώσεων όπου μπορεί να διενεργηθεί και στη δική του, αλλά να ολοκληρωθεί εκτός,
- και την παρακολούθηση εκτός εδάφους, που λαμβάνει χώρα αποκλειστικά εκτός της επικράτειας του.

Και οι δυο κατηγορίες παρακολούθησης γίνονται με τη χρήση ηλεκτρονικών μέσων. Συμπεριλαμβανομένων των τηλεφωνικών υποκλοπών, της διαδικτυακής παρακολούθησης, την χρήση δορυφόρων και μη επανδρωμένων αεροσκαφών, με σκοπό τη συλλογή των ηλεκτρονικών και μη πληροφοριών, για να ακολουθήσει η αποθήκευση, η επεξεργασία και η μεταφορά των δεδομένων στους λήπτες αποφάσεων.

Η εξωτερική παρακολούθηση γίνεται αντιληπτή με τρεις τρόπους:

- ως την ενέργεια ενός κράτους που στοχεύει στην παρακολούθηση αξιωματούχων ή υπαλλήλων ενός ξένου κρατικού ή μη οργανισμού,

- ως την ενέργεια ενός κράτους που στοχεύει στην παρακολούθηση πολιτών ξένου κράτους, και
- ως την ενέργεια ενός κράτους που στοχεύει στην παρακολούθηση πολιτών που βρίσκονται εκτός της εδαφικής του επικράτειας, οι οποίοι μπορεί να είναι υπήκοοι αυτού του κράτους, είτε κάποιου άλλου (Milanovic 2015).

Οι διαρροές που έγιναν στην ιστοσελίδα WikiLeaks, όσον αφορά τις υποκλοπές που διενεργούν οι υπηρεσίες πληροφοριών των Η.Π.Α. δημιούργησαν μεγάλο πλήγμα στις σχέσεις μεταξύ των κρατών και των ηγετών που είχαν γίνει στόχοι. Ωστόσο αυτά που δημοσιεύθηκαν ήταν ένα μικρό μέρος των όσων διαδραματίζονται καθημερινά σε παγκόσμιο επίπεδο.

#### 1.2.4. Τεχνολογία πληροφοριών (information technology) και δεδομένα (data)

Η τεχνολογία ορίζεται ως είναι η συλλογή τεχνικών, δεξιοτήτων, μεθόδων και διαδικασιών που χρησιμοποιούνται στην παραγωγή αγαθών ή υπηρεσιών ή στην επίτευξη στόχων, όπως η επιστημονική έρευνα με ιδιαίτερη έμφαση στην βιομηχανία. Στη σημερινή εποχή η τεχνολογία είναι σε πολύ υψηλό επίπεδο και ο ανταγωνισμός μεταξύ των κρατών, των επιχειρήσεων και άλλων οντοτήτων, σε αυτόν τον τομέα είναι εξίσου πολύ υψηλός. Η τεχνολογική εξέλιξη ενός κράτους επηρεάζει αναμφισβήτητα την οικονομική και στρατιωτική του ισχύ (Κωνσταντόπουλος 2010).

Η τεχνολογία επηρεάζει την ισορροπία ισχύος μέσω:

- τεχνολογιών που ευνοούν την άμυνα σε σχέση με την επίθεση, δυσκολεύοντας τα αναθεωρητικά κράτη να αλλάξουν την υπάρχουσα κατάσταση,
- του εκσυγχρονισμού των οπλικών συστημάτων που μπορεί να αναπροσαρμόσει το στρατιωτικό δόγμα ενός κράτους και να μεταβάλλει τη σχετική του δύναμη,
- της μεταβολής της σχέσης μεταξύ οικονομικής και στρατιωτικής δύναμης ενός κράτους και ανάλογα με την περίπτωση είτε ενισχύει, είτε αποδυναμώνει τη σχέση μεταξύ τους και κατά συνέπεια την ισχύ του.

Καθότι είναι το αποτέλεσμα της εφαρμογής της επιστημονικής γνώσης για την δημιουργία ενός αντικειμένου το οποίο θα έχει πρακτικό όφελος, τα κράτη και οι επιχειρήσεις επιδιώκουν να την αποκτήσουν, έτσι ώστε να βελτιωθεί η οικονομική τους θέση έναντι των ανταγωνιστών τους. Η κατοχή της υψηλής τεχνολογίας εξυψώνει τις οικονομικές δυνατότητες τους και η επίτευξη αυτού του στόχου γίνεται με τεχνικά μέσα τα οποία χρήζουν γνώσεις τεχνολογίας.

Οι κρατικοί οργανισμοί και οι επιχειρήσεις μέσω της τεχνολογίας πληροφοριών (I.T.) χρησιμοποιούν τους υπολογιστές για την αποθήκευση, την ανάκτηση, την μετάδοση και τον χειρισμό δεδομένων ή πληροφοριών. Τα δεδομένα – data, αυτά είναι ροές πρωτογενών στοιχείων που αντιπροσωπεύουν γεγονότα, πριν αυτά οργανωθούν και διευθετηθούν σε μορφή κατανοητή και χρήσιμη στους ανθρώπους (Laudon & Laudon 2014).

Καθημερινά διακινείται ένας τεράστιος όγκος από δεδομένα, ο οποίος προέρχεται είτε από εσωτερικές συναλλαγές, διοικητικής, εμπορικής ή υποστηρικτικής φύσης, είτε από εξωτερικές πηγές. Τα δεδομένα που συλλέγονται για να μπορούν να χρησιμοποιηθούν, θα πρέπει να υποβληθούν σε επεξεργασία μέσω εργαλείων ανάλυσης και εξόρυξης δεδομένων τα οποία θα τα μετατρέψουν σε πληροφορία και μετέπειτα σε γνώση (Vercellis 2009).

Τα δεδομένα διαχωρίζονται σε τρεις κατηγορίες, ως ακολούθως:

- στα εσωτερικά δεδομένα, τα οποία κυρίως αποθηκεύονται στις βάσεις δεδομένων και χαρακτηρίζονται ως λειτουργικά συστήματα,
- στα εξωτερικά δεδομένα, τα οποία προέρχονται από το εξωτερικό περιβάλλον και, μπορεί να έχουν έμμεσο αντίκτυπο, και
- στα προσωπικά δεδομένα, τα οποία συνηθίζουν να αποθηκεύονται οι προσωπικές εκτιμήσεις ή πληροφορίες στις βάσεις δεδομένων.

Τα δεδομένα περιέχουν πληροφορίες οι οποίες όμως χρήζουν περαιτέρω ανάλυσης για να μπορούν να αξιολογηθούν. Για τον λόγο αυτό, διακρίνονται σε δύο βασικές κατηγορίες:

- στα δεδομένα παρατήρησης, τα οποία έχουν κάποιο νόημα και είναι οργανωμένα για συγκεκριμένο σκοπό τα οποία και υπόκεινται σε ανάλυση και αξιολόγηση, και
- στα δεδομένα πληροφορικής, τα οποία περιγράφουν μόνο μέρος ενός συμβάντος, δεν περιλαμβάνουν καμία ανάλυση, κριτική ή αξιόπιστη βάση για περαιτέρω ενέργεια. Τα δεδομένα δεν αναφέρουν τίποτα για τη σημαντικότητά τους ή τη σχέση τους προς οτιδήποτε.

Μέσω της διαχείρισης των υπολογιστικών πληροφοριακών τους συστημάτων οι αναλυτές που ασκούν I.T. κάνουν διακριτά τα νοήματα από αυτές τις πληροφορίες που εμπεριέχονται στα δεδομένα. Η ανάκτηση αυτών των πληροφοριών και η ενσωμάτωσή τους με τα δομημένα εσωτερικά και εξωτερικά δεδομένα βοηθούν στη λήψη αποφάσεων (Vercellis, 2009).

Στο κομμάτι των επιχειρήσεων, η διαχείριση των δεδομένων πληροφοριών αντιμετωπίζεται ως μια καλή λειτουργία οργάνωσης η οποία μπορεί να χρησιμοποιηθεί για την απόκτηση ανταγωνιστικού πλεονεκτήματος.



### 1.3. Βιβλιογραφική ανασκόπηση

Έχοντας ορίσει τις βασικές έννοιες του θέματος της διπλωματικής εργασίας, σε αυτή την ενότητα γίνεται μια ανασκόπηση της βιβλιογραφίας σχετικά με το ζήτημα της οικονομικής κατασκοπείας. Η κατασκοπεία απασχολεί το διεθνές γίνεσθαι εδώ και πολλούς αιώνες, με τις πρώτες αναφορές να γίνονται στην αρχαιότητα από τον έλληνα ιστορικό Θουκυδίδη – που θεωρείται ο «πατέρας» του Πολιτικού Ρεαλισμού κατά τις Διεθνείς Σχέσεις και τον επίσης ρεαλιστή κατά την Θεωρία των Διεθνών Σχέσεων, κινέζο στρατηγό Σουν Τσου.

Η οικονομική κατασκοπεία, υφίσταται εδώ και αρκετά χρόνια ως επιστημονικό πεδίο μελέτης, στη διεθνή ακαδημαϊκή κοινότητα των Πολιτικών Επιστημών και των Διεθνών Σχέσεων, και κυρίως στις Η.Π.Α. και το Ηνωμένο Βασίλειο (Η.Β.). Ωστόσο, για την ελληνική ακαδημαϊκή κοινότητα, το επιστημονικό αντικείμενο της οικονομικής κατασκοπείας είναι κάτι πολύ εξειδικευμένο, κι ως μη διαδεδομένο είναι δύσκολο να βρεθούν λήμματα των βασικών εννοιών της στην ελληνική γλώσσα. Αυτό έχει σαν αποτέλεσμα η ξενόγλωσση βιβλιογραφία να αποτελεί την μόνη επιλογή για μελέτη και έρευνα.

### 1.4. Μεθοδολογία της έρευνας

Η παρούσα διπλωματική εργασία περιγράφει «το φαινόμενο της οικονομικής κατασκοπείας» (Κωνσταντόπουλος 2010) εστιάζοντας στις δραστηριότητες της. Πιο συγκεκριμένα τους τρόπους με τους οποίους τα στελέχη των υπηρεσιών πληροφοριών υποκλέπτουν οικονομικές και τεχνολογικές πληροφορίες. Η έρευνα διεξήχθη μέσω βιβλιογραφικής ανασκόπησης. Πέραν της ξενόγλωσσης βιβλιογραφίας, ο ερευνητής βασίστηκε και σε άλλες ανοιχτές πηγές πληροφοριών (O.S.Int.), όπως είναι τα επιστημονικά άρθρα και τα δημοσιεύματα περί οικονομικής κατασκοπείας, καθώς επίσης και σε πληροφορίες που συνέλεξε από ανθρώπους που εργάζονται στον χώρο των πληροφοριών (Hum.Int).

Ένα ζήτημα που προκύπτει είναι ότι εξαιτίας της μυστικότητας που καλύπτει τις υπηρεσίες πληροφοριών και των πρακτικών που ακολουθούν περιορίζεται αρκετά η δυνατότητα ανάπτυξης του θέματος με επικαιροποιημένα στοιχεία. Αυτό είχε σαν συνέπεια μέσα από την έρευνα που έγινε, η διπλωματική εργασία να περιγράφει κυρίως τους τρόπους με τους οποίους γίνονται στη σύγχρονη εποχή οι υποκλοπές πληροφοριών και τα μέτρα πρόληψης, αποτροπής και αντιμετώπισης που λαμβάνονται ή θα πρέπει να λαμβάνονται, μέσω της οικονομικής αντικατασκοπείας, από κρατικούς ή μη οργανισμούς .

Γίνεται αναφορά σε περιστατικά οικονομικής κατασκοπείας που έλαβαν χώρα κατά το παρελθόν και τα οποία έχουν δημοσιοποιηθεί, είτε γιατί έγιναν αντιληπτά, είτε γιατί χαρακτηρίστηκαν ως μη απόρρητα, από τους δρώντες. Ο ερευνητής διερωτάται εάν οι εφαρμοζόμενες μέθοδοι που ασκούν οι υπηρεσίες πληροφοριών, για να αποσπάσουν τις πληροφορίες που επιθυμούν προς όφελος των εργοδοτών τους, τηρούν κανόνες δεοντολογίας.

Εν συνεχεία, αναλύει τις μεθόδους εφαρμογής της οικονομικής κατασκοπείας μέσω υποκλοπών από ηλεκτρονικούς υπολογιστές, ασύρματες και ενσύρματες τηλεπικοινωνίες, καθώς επίσης και υποκλοπές μέσα από ομιλίες στον χώρο. Επίσης, ο ερευνητής διερωτάται για το εάν η άσκηση της οικονομικής κατασκοπείας, συνεπάγεται την αύξηση της αποδοτικότητας των προϊόντων, την μείωση του κόστους παραγωγής ή ανάλογα με την περίπτωση, τον ρυθμό ανάπτυξης των επιχειρήσεων που υποστηρίζουν με την δράση τους οι δρώντες της οικονομικής κατασκοπείας. Παράλληλα, είναι υπαρκτός ο κίνδυνος της πρόκλησης πολιτικών και κοινωνικών προβλημάτων, λόγω της υποκλοπής ευαίσθητων πληροφοριών; Αντιμετωπίζονται μέσω της οικονομικής κατασκοπείας πολιτικές κρίσεις εντός κι εκτός ενός κράτους; Τέλος, αναλύονται οι στρατηγικές αποτροπής της οικονομικής κατασκοπείας εντός μιας επιχείρησης ή ενός κρατικού οργανισμού.

Αρχικά, εξετάστηκαν οι γενικές έννοιες και εν συνεχεία θα εξετασθούν οι επιμέρους πιο ειδικές. Γίνεται αντιληπτό ότι το βασικό ερώτημα της έρευνας απαντάται δια της παραγωγικής μεθόδου. Και αυτό γιατί το θέμα της μελέτης είναι συνυφασμένο με γεγονότα που έχουν έρθει στο φως της δημοσιότητας για τις δράσεις των υπηρεσιών πληροφοριών που έχουν πραγματοποιηθεί κατά το παρελθόν. Το όλο εγχείρημα δυσχεραίνει η παραδοχή ότι τα γεγονότα που λαμβάνουν χώρα κατά την περίοδο της μελέτης, είναι αδύνατο να βρεθούν μέσω O.S.Int. και κατά συνέπεια να τεκμηριωθούν οι ισχυρισμοί των Hum.Int. Αυτό είναι κάτι το οποίο περιορίζει τον ερευνητή και δε τον βοηθά να εξάγει συμπεράσματα δια της επαγωγικής μεθόδου.

## **2. Υπηρεσίες πληροφοριών (intelligence services ή agencies)**

Σε αυτό το κεφάλαιο γίνεται αναφορά στις υπηρεσίες πληροφοριών, τις κατηγορίες που διαχωρίζονται και τον ρόλο τους. Επίσης, αναφέρονται τα εξειδικευμένα τμήματα που διαθέτουν οι υπηρεσίες πληροφοριών και ο τρόπος δράσης τους.

### **2.1. Οι υπηρεσίες πληροφοριών και ο ρόλος τους**

Οι υπηρεσίες πληροφοριών είναι κρατικοί οργανισμοί που έχουν ως αποστολή την συλλογή και ανάλυση πληροφοριών που έχουν σχέση με την εθνική ασφάλεια και την μεταφορά αυτών των πληροφοριών στην ηγεσία του κράτους τους. Οι πληροφορίες που είναι επιφορτισμένες να συλλέγουν είναι σχετικές με την πολιτική ηγεσία της χώρας και χρησιμοποιούνται για την προάσπιση της εθνικής ασφάλειας (Born & Caparini 2007).

Οι υπηρεσίες πληροφοριών διαχωρίζονται σε δύο μεγάλες κατηγορίες ανάλογα με τον ρόλο τους, ως ακολούθως:

- σε αυτές που έχουν ως κύρια αποστολή την ασφάλεια, και κατά συνέπεια την άμυνα εντός της επικράτειας της χώρας τους, (αμυντική υπηρεσία πληροφοριών)
- και σε αυτές που έχουν ως κύρια αποστολή την κατασκοπεία, δραστηριότητα την οποία υλοποιούν εκτός της επικράτειας τους, (επιθετική υπηρεσία πληροφοριών).

Η αποστολή μιας αμυντικής υπηρεσίας πληροφοριών είναι η πρόληψη και η αποτροπή απειλών που εκδηλώνονται στην επικράτεια του, απέναντι στο σύνταγμα, την κυβέρνηση και την εύρυθμη λειτουργία του κράτους του, καθώς επίσης και η προάσπιση των εθνικών του συμφερόντων.

Ο προσανατολισμός των υπηρεσιών πληροφοριών κάθε χώρας διαφέρει. Τα περισσότερα κράτη διαθέτουν και αμυντική και επιθετική υπηρεσία πληροφοριών οι αρμοδιότητες των οποίων διαφέρουν. Και ο λόγος διάκρισης εναπόκειται στην άποψη της εκάστοτε ηγεσίας του κράτους για τις ανάγκες που θεωρεί ότι έχει, ή αντίστοιχα τις απειλές.

Η ραγδαία ανάπτυξη της τεχνολογίας οδήγησε στην ανάγκη για δημιουργία εξειδικευμένων τμημάτων υπηρεσιών πληροφοριών για να καλυφθεί όλο το φάσμα των ενεργειών στο νέο περιβάλλον. Καθεμία από τις νέες υπηρεσίες έχει εστιάσει σε διαφορετικό αντικείμενο. Άλλες στην τρομοκρατία, άλλες στα όπλα μαζικής καταστροφής και άλλες στην κατασκοπεία άλλων κρατών. Οι νέες υπηρεσίες δημιουργήθηκαν για να επιμεριστούν τα ζητήματα για τα οποία θα εργάζονται, εντός ή εκτός της επικράτειας του κράτους τους. Ωστόσο, σε μερικά κράτη τα εξειδικευμένα τμήματα αποτελούν κομμάτι της αστυνομίας τους και κάποια άλλα διαθέτουν υπηρεσία που ασχολείται και με το εσωτερικό της χώρας, αλλά και με το εξωτερικό.

Ο ρόλος των υπηρεσιών πληροφοριών είναι ζωτικής σημασίας για ένα κράτος και κυρίως για τους πολίτες του. Πέραν της συλλογής και ανάλυσης των πληροφοριών που σχετίζονται με την εθνική ασφάλεια, οι υπηρεσίες πληροφοριών είναι υπεύθυνες να ασκούν δραστηριότητες αντικατασκοπίας, καθώς επίσης και να διασφαλίζουν τις πληροφορίες υψίστης σημασίας, τα πληροφοριακά συστήματα και τις εγκαταστάσεις του κράτους τους.

Ο Παύλος Αποστολίδης – που έχει διατελέσει πρώην Διοικητής της Εθνικής Υπηρεσίας Πληροφοριών, Υπουργός Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης και είναι Πρέσβης επί τιμή, αναφέρει ότι οι αμυντικού χαρακτήρα αποστολές των υπηρεσιών πληροφοριών συνίστανται στην αντικατασκοπεία, τις αντιδολιοφθορές, την αντιανατρεπτική δράση και την αντιπροπαγάνδα, ενώ τα μέσα που χρησιμοποιούν είναι:

- δίκτυο πληροφοριοδοτών στους τομείς ενδιαφέροντος τους, είτε επί πληρωμή, είτε με άλλο αντάλλαγμα,
- ομάδες φυσικής παρακολούθησης, προς παρακολούθηση ατόμων ή ξένων οργανισμών,

- τεχνικά μέσα, είτε προς διευκόλυνση της φυσικής παρακολούθησης, είτε προς παγίδευση χώρων, είτε προς παρακολούθηση επικοινωνιών υπόπτων προσώπων και ενίοτε,
- ομάδες προστασίας υψηλών προσώπων,
- ομάδες αντιτρομοκρατικών επιχειρήσεων.

Στην Ευρώπη οι εσωτερικές υπηρεσίες ασφαλείας – πληροφοριών ή αντικατασκοπείας προηγούνται χρονικά των εξωτερικών Υπηρεσιών Πληροφοριών (Αποστολίδης 2014).

Οι υπηρεσίες πληροφοριών κατηγοριοποιούνται ανάλογα με, τον χώρο ευθύνης, το πεδίο δράσης το αντικείμενο της αποστολής τους και τα μέσα που χρησιμοποιούν για να φέρουν εις πέρας την αποστολή τους.

Στην κατηγορία με τις υπηρεσίες εξωτερικών πληροφοριών και κατασκοπείας (foreign intelligence services), ανήκουν οι:

- Κεντρική Υπηρεσία Πληροφοριών, Ηνωμένες Πολιτείες Αμερικής  
C.I.A. (Central Intelligence Agency)
- Μυστική Υπηρεσία Πληροφοριών, Ηνωμένο Βασίλειο  
M.I.6 ή S.I.S. (Military Intelligence – Section 6 ή Secret Intelligence Service)
- Γενική Διεύθυνση Εξωτερικής Ασφάλειας, Γαλλική Δημοκρατία  
D.G.S.E (General Directorate for External Security)
- Υπηρεσία Εξωτερικών Πληροφοριών, Ρωσική Ομοσπονδία  
S.V.R. (Foreign Intelligence Service)
- Ομοσπονδιακή Υπηρεσία Πληροφοριών, Ομοσπονδιακή Δημοκρατία της Γερμανίας  
B.N.D. (Federal Intelligence Service)
- Ινστιτούτο Πληροφοριών και Ειδικών Επιχειρήσεων, Κράτος του Ισραήλ  
Mossad (Institute for Intelligence and Special Operations).

Στην κατηγορία με τις υπηρεσίες εσωτερικής ασφάλειας και αντικατασκοπείας (domestic intelligence & security services), ανήκουν οι:

- Ομοσπονδιακό Γραφείο Ερευνών, Ηνωμένες Πολιτείες Αμερικής  
F.B.I. (Federal Bureau of Investigation)

- Υπηρεσία Ασφαλείας, Ηνωμένο Βασίλειο  
M.I.5 ή S.S. (Military Intelligence – Section 5, Security Service)
- Ομοσπονδιακή Υπηρεσία Ασφαλείας, Ρωσική Ομοσπονδία  
F.S.B. (Federal Security Service)
- Ομοσπονδιακό Γραφείο για την Προστασία του Συντάγματος, Ομοσπονδιακή Δημοκρατία της Γερμανίας  
B.F.V. (Federal Office for the Protection of the Constitution)
- Υπηρεσία Εσωτερικής Ασφάλειας, Κράτος του Ισραήλ  
Shabak ή Shin Bet (Israel Security Agency)
- Γενική Διεύθυνση Εσωτερικής Ασφάλειας, Γαλλική Δημοκρατία  
D.G.S.I. (General Directorate for Internal Security).

Στην κατηγορία με τις υπηρεσίες πληροφοριών που χρησιμοποιούν αποκλειστικά τεχνικά μέσα για τη συλλογή και επεξεργασία πληροφοριών (signals intelligence), ανήκουν οι:

- Εθνική Υπηρεσία Ασφαλείας, Ηνωμένες Πολιτείες Αμερικής  
N.S.A. (National Security Agency)
- Κεντρικά Γραφεία Κυβερνητικών Επικοινωνιών, Ηνωμένο Βασίλειο  
G.C.HQ. (Government Communications Headquarters).

Στην κατηγορία με τις ενιαίες υπηρεσίες πληροφοριών (unitary intelligence services), οι οποίες συνδυάζουν τις λειτουργίες των τριών προηγούμενων κατηγοριών ανήκει η Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.), Ελληνική Δημοκρατία.

Στην κατηγορία με τις στρατιωτικές υπηρεσίες πληροφοριών (military intelligence services), ανήκουν οι ακόλουθες:

- Στρατιωτική Υπηρεσία Πληροφοριών, Ηνωμένες Πολιτείες Αμερικής  
D.I.A. (Defense Intelligence Agency)
- Κεντρική Διεύθυνση του Γενικού Επιτελείου των Ενόπλων Δυνάμεων, Ρωσική Ομοσπονδία  
G.R.U. (Main Directorate of the General Staff of the Armed Forces)
- Διεύθυνση Στρατιωτικών Πληροφοριών, Κράτος του Ισραήλ  
Aman (Military Intelligence Directorate)

- Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (Δ.Δ.Σ.Π.), Ελληνική Δημοκρατία.

## 2.2. Μυστικές ή συγκεκαλυμμένες επιχειρήσεις (covert operations) και μετωπικές οργανώσεις (front organizations)

Το Υπουργείο Άμυνας των Στρατιωτικών και Συνδεδεμένων Όρων (D.O.D.) των Η.Π.Α. (Κοινή Δημοσίευση JP1-02), ορίζει συγκεκαλυμμένη επιχείρηση «μια επιχείρηση που σχεδιάζεται και εκτελείται έτσι ώστε να αποκρύπτει την ταυτότητα της ή να επιτρέπει την αληθοφανή άρνηση συσχέτισης από τον ανάδοχο. Διαφέρει από μια παράνομη επιχείρηση κατά την οποία δίδεται έμφαση στην απόκρυψη της ταυτότητας του χορηγού και όχι στην απόκρυψη της επιχείρησης». Ο ορισμός του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών έχει χρησιμοποιηθεί από τις Ηνωμένες Πολιτείες και το Ν.Α.Τ.Ο. από τον Δεύτερο Παγκόσμιο Πόλεμο (United States Department of Defense).

Οι μυστικές ή συγκεκαλυμμένες επιχειρήσεις οργανώνονται και εκτελούνται από τις μυστικές υπηρεσίες και στις κύριες δράσεις τους περιλαμβάνονται ειδικές αποστολές παραστρατιωτικών ομάδων σε ξένο έδαφος που έχουν ως στόχο την ανατροπή εχθρικών καθεστώτων ή την ενίσχυση φίλα προσκείμενων ανταρτικών ή τρομοκρατικών οργανώσεων. Ενεργούν αποκρύπτοντας την πραγματική τους ταυτότητα. Ειδικεύονται στην δημιουργία κοινωνικοπολιτικών αναταραχών με απώτερο σκοπό να δημιουργηθεί ρήγμα στον πολιτικό, στρατιωτικό, και νομικό τομέα του κράτους που είναι στοχευμένο. Αυτό συμβαίνει καθώς επηρεάζουν είτε τον εσωτερικό πληθυσμό μιας χώρας, είτε άτομα εκτός αυτής.

Οι συγκαλυμμένες επιχειρήσεις σκοπεύουν να εκπληρώσουν κρυφά όλους τους στόχους της αποστολής τους, χωρίς να γνωρίζουν ποιος τους χρηματοδότησε ή πραγματοποίησε την επιχείρηση ή σε ορισμένες περιπτώσεις, χωρίς να γνωρίζει κανείς ότι έχει ήδη δράσει.

Μετωπικές οργανώσεις ονομάζονται οι οντότητες, των οποίων η σύσταση και διαχείριση γίνεται από μια άλλη οντότητα, χωρίς αυτή να φαίνεται. Αυτή μπορεί να είναι μια υπηρεσία πληροφοριών, μια ομάδα οργανωμένου εγκλήματος, μια απαγορευμένη οργάνωση, μια θρησκευτική ομάδα – αίρεση, μία πολιτική ομάδα, μια ομάδα υπεράσπισης δικαιωμάτων συλλογικότητας ή μια εταιρεία. Απώτερος σκοπός των μετωπικών οργανώσεων είναι να προωθούν τα συμφέροντά του δημιουργού τους, χωρίς όμως αυτό να είναι φανερό στη κοινή γνώμη, έτσι ώστε να μπορούν να εκτελούν ανενόχλητα την αποστολή τους. Αυτού του τύπου οι οργανώσεις είναι διαδεδομένες ως βιτρίνες.

### 2.3. Επιχειρήσεις παραπληροφόρησης (disinformation campaigns) και ψυχολογικές επιχειρήσεις (psychological operations)

Οι υπηρεσίες πληροφοριών πέραν των παραδοσιακών τους λειτουργιών συχνά προβαίνουν και σε επιχειρήσεις παραπληροφόρησης που έχουν ως στόχο τον αποπροσανατολισμό των αντιπάλων τους. Οι επιχειρήσεις αυτές παραπληροφόρησης αρκετές φορές αποκτούν το χαρακτήρα του ψυχολογικού πολέμου (psychological warfare).

Οι ψυχολογικές επιχειρήσεις ορίζονται ως προγραμματισμένες ψυχολογικές δραστηριότητες που έχουν σχεδιαστεί για να διαμορφώνουν τις νοοτροπίες και τις συμπεριφορές που επηρεάζουν την επίτευξη των πολιτικών και στρατιωτικών στόχων. Χρησιμοποιούνται διάφορες τεχνικές και στοχεύουν στο να επηρεάσουν το σύστημα αξιών του στόχου, το σύστημα πεποιθήσεων, τα συναισθήματα, τα κίνητρα, το σκεπτικό ή τη συμπεριφορά του (Clow 2008).

Χρησιμοποιείται για να διεγείρει εξομολογήσεις ή να ενισχύει νοοτροπίες και συμπεριφορές ευνοϊκές για τους στόχους του δημιουργού και μερικές φορές συνδυάζεται με μαύρες λειτουργίες ή τακτικές σημαίας. Χρησιμοποιείται επίσης για να καταστρέψει το ηθικό των εχθρών μέσω τακτικών που αποσκοπούν στην καταστολή των ψυχολογικών καταστάσεων των στρατευμάτων (Chekinov & Bogdanov 2013).

Κατά τη διάρκεια του Ψυχρού Πολέμου η Κ.Γ.Β. της Ένωσης Σοβιετικών Σοσιαλιστικών Δημοκρατιών έδινε περισσότερη έμφαση σε αυτού του τύπου τις επιχειρήσεις (active measures) παραπληροφόρησης και εξαπάτησης του αντιπάλου με στόχο τον επηρεασμό της κοινής γνώμης και των κυβερνήσεων του δυτικού κόσμου. Για παράδειγμα, στη σημερινή εποχή η Τουρκική Εθνική Οργάνωση Πληροφοριών (M.I.T.) δίνει έμφαση στις επιχειρήσεις ψυχολογικού πολέμου, που ως στόχο έχουν κυρίως την Ελλάδα και την Κύπρο.

### 2.4. Αξιωματικός πληροφοριών (intelligence officer)

Ο αξιωματικός πληροφοριών είναι το στέλεχος μιας υπηρεσίας πληροφοριών που έχει ως αποστολή του την στρατολόγηση (recruitment) ανθρώπων για την συλλογή πληροφοριών (Hum.Int.). Οι άνθρωποι αυτοί αποκαλούνται κατάσκοποι (spies) ή πράκτορες (agents) ή πληροφοριοδότες (informants). Πρόκειται για μεμονωμένες ή για ένα σύνολο πληροφοριών που συσχετίζονται άμεσα με τον ανθρώπινο παράγοντα, καθότι η συλλογή, εκτίμηση και χρήση πληροφοριών προέρχονται κυρίως από διαπροσωπικές σχέσεις (Central Intelligence Agency 2010).

Το προσωπικό για τη συλλογή, αποθήκευση, ανάλυση και εκτίμηση των πληροφοριών δέχεται εντολές και αναλαμβάνει ευθύνες, έχοντας συγκεκριμένους στόχους. Συχνά γίνεται σύγχυση με τους επιτελείς πληροφοριών (spy ή agent handlers) που αποκαλούνται από το ευρύ κοινό ως κατάσκοποι. Ωστόσο, οι επιτελείς πληροφοριών είναι αυτοί που καθοδηγούν τους κατασκόπους για το είδος των πληροφοριών που επιθυμούν να συλλέξουν. Οι κατάσκοποι μπορεί να είναι ειδικά εκπαιδευμένα και εξειδικευμένα άτομα, τα οποία λαμβάνουν συγκεκριμένες αποστολές, είτε μη-επίσημο προσωπικό, το οποίο ταξιδεύει και έρχεται σε επαφές με συγκεκριμένο κόσμο, ο οποίος έχει σημασία για μία συγκεκριμένη δράση της υπηρεσίας πληροφοριών (Margolis, 2013). Οι επιτελείς πληροφοριών έχουν ως αποστολή τη στρατολόγηση ατόμων σε ξένα κράτη και συνήθως απολαμβάνουν διπλωματικής κάλυψης (cover) ή άλλου είδους καλύψεις, όπως επιχειρηματίες, δημοσιογράφοι, πανεπιστημιακοί.

Την περίοδο του Ψυχρού Πολέμου στις υπηρεσίες πληροφοριών της Ε.Σ.Σ.Δ. ακολουθούσαν η πρακτική επιτελών πληροφοριών, οι οποίοι εισέρχονταν στη χώρα στόχο και διαβιούσαν εκεί για χρόνια με αποστολή να αποκτήσουν νόμιμα την υπηκοότητα της χώρας στόχου και να διεισδύσουν (penetration) σε κρατικούς οργανισμούς υψηλού ενδιαφέροντος, όπως είναι τα υπουργεία. Αυτή η πρακτική των παρανόμων (illegals), όπως ονομάζονται, εφαρμόζεται και στη σημερινή εποχή από αρκετές υπηρεσίες πληροφοριών των Μεγάλων Δυνάμεων και όχι μόνο.

Οι επιτελείς πληροφοριών δρουν και εντός του κράτους τους με στόχο να στρατολογήσουν πληροφοριοδότες και πράκτορες στο εσωτερικό της χώρας, προκειμένου να λάβουν χρήσιμες πληροφορίες που μπορούν να αποβούν κρίσιμες για την εθνική ασφάλεια, όπως για παράδειγμα είναι μια τρομοκρατική επίθεση.

## 2.5. Συλλογή πληροφοριών (intelligence collection ή gathering)

Συλλογών πληροφοριών είναι η διαδικασία διαχείρισης και οργάνωσης του συνόλου των πληροφοριών από τις διάφορες πηγές. Το τμήμα συλλογής ενός οργανισμού πληροφοριών μπορεί να επιχειρήσει βασική επικύρωση αυτού που συλλέγει, αλλά δε θα πρέπει να αναλύσει τη σημασία του. Η διαφορά μεταξύ της επικύρωσης και ανάλυσης υποστηρίζεται στην κοινότητα των Μυστικών Υπηρεσιών των Η.Π.Α., όπου η Εθνική Υπηρεσία Ασφαλείας (N.S.A.) μπορεί (κατά τη γνώμη της C.I.A. ή της Στρατιωτικής Υπηρεσίας Πληροφοριών D.I.A.) να προσπαθήσει να ερμηνεύσει τις πληροφορίες, ασχέτως αν η ερμηνεία αυτή είναι δουλειά ενός άλλου οργανισμού.

Η συλλογή πληροφοριών κατηγοριοποιείται, ως ακολούθως:



- σε Hum.Int. (human intelligence) που αναφέρεται στις πληροφορίες που συλλέγονται από ανθρώπινες πηγές, όπως είναι οι πράκτορες, οι κατάσκοποι και οι πληροφοριοδότες. Επίσης μπορεί να αναφέρεται:
  - σε κατοχή φωτογραφικού υλικού,
  - σε κατοχή ψηφιακών αρχείων,
  - σε πληροφορίες από διάφορα άτομα διαφόρων ειδικοτήτων, που τις κατέχουν είτε με μυστικό τρόπο, είτε με ανοιχτή συλλογή πληροφοριών και ο ρόλος τους είναι τέτοιος, ώστε να θεωρούνται έγκυρες πηγές,
  - σε συζητήσεις και απολογισμούς από αλλοδαπούς που μένουν σε κάποια χώρα, αλλά και
  - σε ημεδαπούς που έχουν ταξιδέψει σε άλλες χώρες, και
  - σε επίσημες επαφές με κρατικούς ή κυβερνητικούς εκπροσώπους τρίτων χωρών.
- σε O.S.Int. (open source intelligence) που αναφέρεται στις πληροφορίες που συλλέγονται από ανοικτές πηγές, όπως τα Μέσα Μαζικής Επικοινωνίας και το διαδίκτυο. Εκτιμάται μάλιστα ότι το 90% περίπου των πληροφοριών που αναλύουν οι υπηρεσίες πληροφοριών προέρχεται από ανοικτές πηγές, και μόνο το 10% από μυστικές πηγές.
- σε Sig.Int. (signals intelligence) που αναφέρεται στις πληροφορίες που συλλέγονται με τεχνικά μέσα, όπως είναι οι υποκλοπές τηλεπικοινωνιών και ηλεκτρονικού ταχυδρομείου και η αποκρυπτογράφηση σημάτων.
- σε Im.Int. (imagery intelligence) που αναφέρεται στις πληροφορίες που συλλέγονται με τη χρήση κατασκοπευτικών δορυφόρων και μη επανδρωμένων αεροσκαφών.

Η συλλογή πληροφοριών από ανθρώπινους πόρους είναι η μόνη που μπορεί να αποδειχθεί πολύτιμη σχετικά με τις πραγματικές προθέσεις και δυνατότητες (intentions and capabilities) των φίλων και εχθρών.

Για παράδειγμα, η χρήση κατασκοπευτικών δορυφόρων μπορεί να βοηθήσει στην αποκάλυψη κάποιων μυστικών στρατιωτικών εγκαταστάσεων, αλλά δεν μπορεί να αποκαλύψει τις προθέσεις για το πότε ακριβώς ο εχθρός προτίθεται να τις χρησιμοποιήσει. Αυτή την πληροφόρηση μόνο ένας πράκτορας (Hum.Int.) μπορεί να την δώσει. Η πληροφόρηση από

ανθρώπους ακολουθεί τις τεχνολογικές εξελίξεις της εποχής. Μία από τις νέες μορφές της πληροφόρησης ανθρώπινων πηγών είναι το crowd source και αναφέρεται στη μαζική συλλογή πληροφοριών και στοιχείων που προέρχονται από τις διαπροσωπικές επαφές ανθρώπων, συνήθως μέσω του διαδικτύου και των μέσων κοινωνικής δικτύωσης.

### **3. Οικονομική κατασκοπεία (economic espionage)**

Η οικονομική κατασκοπεία διαδραματίζει έναν συνεχώς αυξανόμενο ρόλο στην επιστήμη των Διεθνών Σχέσεων. Αναπτύχθηκε την περίοδο του Ψυχρού Πολέμου, στην διαμάχη μεταξύ Ανατολής και Δύσης σε πολιτικό και οικονομικό επίπεδο ωστόσο συνεχίζει να εφαρμόζεται σήμερα, με μεθόδους που ακολουθούν την τεχνολογική πρόοδο. Σε αυτό το κεφάλαιο δίνεται ο ορισμός της οικονομικής κατασκοπείας και πως αυτή εφαρμόζεται. Τέλος, απαντάται το ερώτημα για το αν ένα κράτος που κάνει υποκλοπές οικονομικών πληροφοριών και τεχνολογίας ωφελείται ή ζημιώνεται από αυτή του την δραστηριότητα.

#### **3.1. Ορισμός και εφαρμογή της οικονομικής κατασκοπείας**

Η οικονομική κατασκοπεία είναι η λειτουργία των υπηρεσιών πληροφοριών ενός κράτους που έχει ως αποστολή την απόκτηση, με μυστικά μέσα, πληροφοριών σχετικών με την οικονομία, το εμπόριο, την τεχνολογία και την πνευματική ιδιοκτησία, χρησιμοποιώντας μυστικές πηγές και μεθόδους. Στις πράξεις της οικονομικής κατασκοπείας περιλαμβάνονται η κλοπή εμπορικών μυστικών με την χρήση τεχνολογικά προηγμένων ηλεκτρονικών μέσων παρακολούθησης και υποκλοπών, καθώς επίσης η δωροδοκία και ο εκβιασμός.

Σύμφωνα με τον Joseph Evans – που υπήρξε διακεκριμένος πράκτορας της C.I.A., η οικονομική κατασκοπεία διακρίνεται σε τρεις διαστάσεις, ως ακολούθως:

- Την μικροοικονομική κατασκοπεία (microeconomic espionage) που εφαρμόζει το εξειδικευμένο τμήμα της υπηρεσίας πληροφοριών και έχει ως κύρια αποστολή την συλλογή πληροφοριών για την υποστήριξη των επιχειρήσεων του κράτους, έναντι των ξένων επιχειρήσεων που δραστηριοποιούνται σε αυτό. Πιο συγκεκριμένα, ο ρόλος του είναι να εξασφαλίσει τις πληροφορίες που θα οδηγήσουν στην επικράτηση των επιχειρήσεων του, έναντι των επιχειρήσεων άλλων κρατών, στα πλαίσια του διεθνούς ανταγωνισμού.
- Την μακροοικονομική κατασκοπεία (macroeconomic espionage) που εφαρμόζει το εξειδικευμένο τμήμα της υπηρεσίας πληροφοριών και έχει ως κύρια αποστολή την συλλογή πληροφοριών που σχετίζονται με τις οικονομικές ικανότητες του κράτους. Πιο συγκεκριμένα, ο ρόλος του είναι να εξασφαλίζει πληροφορίες σχετικά με τις παγκόσμιες οικονομικές εξελίξεις και δραστηριότητες με απώτερο στόχο την εξυπηρέτηση των στρατηγικών συμφερόντων του κράτους.

- Και την οικονομική αντικατασκοπεία (economic counterespionage) που εφαρμόζει το αντίστοιχα εξειδικευμένο τμήμα της υπηρεσίας πληροφοριών και έχει ως κύρια αποστολή την προστασία των εμπορικών μυστικών του κράτους. Πιο συγκεκριμένα, ο ρόλος του είναι ο εντοπισμός και η εξουδετέρωση των ξένων μυστικών υπηρεσιών που κατασκοπεύουν εναντίον των πολιτών και των επιχειρήσεων του κράτους. Ανάμεσα στις λειτουργίες της οικονομικής αντικατασκοπείας περιλαμβάνεται η προστασία των πληροφοριών των υπηρεσιών πληροφοριών που σχετίζονται με τις μεθόδους και τους τρόπους λειτουργίας τους.

Ο Louis Freeh – που είχε διατελέσει πέμπτος Διευθυντής του F.B.I. επί Προεδρίας του Bill Clinton και του George Bush Jr., έχει δηλώσει ότι: «η οικονομική κατασκοπεία αποτελεί πλέον τη μεγαλύτερη απειλή για την εθνική ασφάλεια των Ηνωμένων Πολιτειών, μετά τον Ψυχρό Πόλεμο». Ο Κωνσταντόπουλος (2010) αναφέρει ότι οι αμερικανικές ιδιωτικές επιχειρήσεις έχουν συνειδητοποιήσει τον κίνδυνο και έχουν υιοθετήσει αυστηρότερα μέτρα ασφάλειας. Οι αμερικανικές μυστικές υπηρεσίες έχουν κινητοποιηθεί, έτσι ώστε να αντιμετωπίσουν αυτές τις απειλές.

Με ζητούμενο την οικονομική υπεροχή, οι ασκούντες οικονομική κατασκοπεία πρέπει να έχουν την ικανότητα να αναγνωρίζουν το περιβάλλον γύρω τους και να προσαρμόζονται κατάλληλα. Είτε είναι κρατικός οργανισμός, είτε επιχείρηση, πρέπει να έχει πλήρη γνώση όσων περιβάλλουν τον στόχο του, όπως οι νόμοι, τα ήθη, τα έθιμα, οι παραδόσεις, η θρησκευτική και πολιτιστική ταυτότητα της κοινωνίας και η διαστρωμάτωση της. Οι κοινωνίες φέρουν ασταθή χαρακτηριστικά και όποιος μπορεί να τα αποκρυπτογραφήσει έχει ουσιαστικό πλεονέκτημα έναντι των αντιπάλων του.

### 3.2. Πληροφορίες οικονομικού περιεχομένου (economic intelligence)

Από τα τέλη του περασμένου αιώνα οι οικονομικές μεταβολές σε παγκόσμιο επίπεδο δημιούργησαν ένα νέο οικονομικό μοντέλο, μέσα στο οποίο τα κράτη ανταγωνίζονται μεταξύ τους. Σε αυτό το νέο μοντέλο του διεθνούς οικονομικού ανταγωνισμού οι σημαντικότερες πηγές παραγωγικότητας είναι οι πληροφορίες και η τεχνολογία. Η αναθεώρηση των αντιλήψεων για την εθνική ασφάλεια συνέβαλε, ώστε οι πληροφορίες οικονομικού περιεχομένου να ταυτίζονται με την οικονομική ισχύ.

Οι πληροφορίες οικονομικού, εμπορικού και βιομηχανικού περιεχομένου (commercial intelligence), καθώς επίσης και οι επιχειρηματικές πληροφορίες (corporate intelligence) αναφέρονται στο ίδιο αντικείμενο. Οι κύριες πηγές συλλογής οικονομικών πληροφοριών είναι οι ανοιχτές πηγές (overt sources), οι ανοιχτές αναφορές (overt reporting) και οι μυστικές αναφορές (clandestine reports).

Η άντληση των πληροφοριών οικονομικού περιεχομένου, γίνεται κυρίως από τις ανοιχτές πηγές που ως επί το πλείστον είναι διαθέσιμες σε επίσημες εκδόσεις οικονομικών στατιστικών μελετών, οικονομικών εφημερίδων και λοιπών περιοδικών εκδόσεων, τηλεοπτικών και ραδιοφωνικών εκπομπών που ασχολούνται με το αντικείμενο της οικονομίας και του εμπορίου. Επίσης, αστείρευτη πηγή οικονομικών πληροφοριών είναι και οι περιοδικές αναφορές και μελέτες τραπεζικών ομίλων και χρηματοπιστωτικών ιδρυμάτων, της Παγκόσμιας Τράπεζας (World Bank), του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α), του Διεθνούς Νομισματικού Ταμείου (I.M.F.), και άλλων οργανισμών, που εξετάζουν άμεσα τα οικονομικά στοιχεία των κρατών. Αυτές οι μη διαβαθμισμένες πληροφορίες συνιστούν τη βάση κάθε οικονομικής ανάλυσης κι έτσι με μεγαλύτερη ευκολία οι αναλυτές πληροφοριών (intelligence analyst) των υπηρεσιών πληροφοριών μπορούν να ερμηνεύσουν το διαβαθμισμένου υλικού που έχουν στην κατοχή τους.

Οι κυβερνήσεις των κρατών επίσημα αρνούνται να παραδεχτούν ότι εφαρμόζουν οικονομική κατασκοπεία ακόμα και στους συμμάχους τους. Ωστόσο, η απόκτηση πληροφοριών οικονομικού περιεχομένου συνιστά σημαντικό μέρος της δουλειάς των υπηρεσιών πληροφοριών σχεδόν όλων των κρατών.

Ο Pierre Marion – ο οποίος είχε διατελέσει πρώτος Διευθυντής της Γενικής Διεύθυνσης Εξωτερικής Ασφάλειας της Γαλλικής Δημοκρατίας (D.G.S.E.), είχε δηλώσει: «η οικονομική κατασκοπεία αποτελεί σημαντική δραστηριότητα για την Γαλλία, προκειμένου να παραμείνει πρωτοπόρα στην διεθνή αγορά και την τεχνολογία. Φυσικά και έχει χρησιμοποιηθεί κατά των Η.Π.Α., όσο και άλλων χωρών. Θα πρέπει να θυμόμαστε ότι παρά το γεγονός ότι είμαστε σύμμαχοι σε θέματα άμυνας, στον οικονομικό τομέα είμαστε ανταγωνιστές». Αυτή η δημόσια τοποθέτηση είχε προκαλέσει αίσθηση, καθώς όλοι μεν γνωρίζουν ότι οι υπηρεσίες πληροφοριών δρουν ανεξαρτήτως και «χωρίς συναισθηματισμούς», αλλά μεταξύ συμμάχων είναι πέραν της ηθικής. Βέβαια αυτός ο αόρατος πόλεμος μεταξύ των υπηρεσιών πληροφοριών, όχι μόνο διατηρείται, αλλά εντείνεται με την πάροδο των ετών.

### 3.3. Ανάλυση πληροφοριών (intelligence analysis)

Η ανάλυση των πληροφοριών είναι μια διαδικασία συλλογής και δημιουργίας πληροφοριών από πολλαπλές πηγές, όπως δεδομένα και πληροφορίες. Είναι μια μορφή διαχείρισης που προάγει την ενοποιημένη προσέγγιση στην αναγνώριση, την αξιολόγηση, τον εμπλουτισμό και τον ορθό διαμοιρασμό των πληροφοριών σε έναν κρατικό οργανισμό ή μία επιχείρηση. Η διαδικασία της ανάλυσης πληροφοριών περιλαμβάνει τη συγκέντρωση των πληροφοριών από ένα πλήθος θεματικών και ποικιλία περιστάσεων από τα άτομα που έχουν γνώσεις σε τομείς που περιλαμβάνουν την στρατηγική, τις τακτικές επιχειρήσεις και την πληροφόρηση.

Ενώ οι τεχνολογίες κατέχουν πολύ σημαντικό ρόλο στη συλλογή πληροφοριών, η ανάλυση είναι αναμφισβήτητα ως η πιο σημαντική από τις τεχνολογίες που χρησιμοποιούνται για τη συλλογή αυτών των δεδομένων. Η ανάλυση πληροφοριών είναι η διαδικασία με την οποία οι πληροφορίες που συλλέγονται για έναν εχθρό χρησιμοποιούνται για να απαντηθούν τακτικά ερωτήματα σχετικά με τις τρέχουσες εξελίξεις κρατικών οργανισμών και επιχειρήσεων ή για να προβλεφθεί η μελλοντική τους συμπεριφορά (RAND Corporation 2018).

Στις υπηρεσίες πληροφοριών τα αρχικά δεδομένα που συλλέγονται, είναι ακατέργαστες πληροφορίες (raw intelligence) και πρέπει να αναλυθούν και να αξιολογηθούν από τους εξειδικευμένους αναλυτές της για να μπορούν να διαμορφώσουν μιας ορθολογική εκτίμηση και να γνωμοδοτήσουν για την λήψη απόφασης.

Η ανάλυση των πληροφοριών είναι η εφαρμογή ατομικών και συλλογικών γνωστικών μεθόδων για τον υπολογισμό των δεδομένων και των υποθέσεων σε ένα μυστικό κοινωνικοπολιτισμικό πλαίσιο. Η ικανότητα ανάπτυξης έγκαιρων και καλά διατυπωμένων στρατηγικών πληροφοριών είναι ζωτικής σημασίας (C.I.A. 2008). Η ακριβής ανάλυση πληροφοριών είναι ζωτικής σημασίας για την ασφάλεια και αυτό γιατί προστατεύει το κράτος από πιθανές απειλές. Οι αναλυτές πληροφοριών πρέπει να παράγουν ακριβείς πληροφορίες έτσι ώστε οι πιθανές απειλές να μπορούν να περιοριστούν πριν εμφανιστούν. Σε πολλά κράτη οι ηγέτες λαμβάνουν καθημερινά ολοκληρωμένες αναφορές με επεξεργασμένες πληροφορίες και εκτιμήσεις που αφορούν θέματα εσωτερικής και εξωτερικής ασφάλειας.

Οι αναλυτές πληροφοριών θα συλλέξουν πληροφορίες από ένα ευρύ φάσμα πηγών και θα συνδέσουν τις ομοιότητες μεταξύ αυτών, οι οποίες θα δημιουργήσουν μια κοινή αλήθεια. Παρά το γεγονός ότι η αμυντική βιομηχανία βασίζεται στην ανάλυση πληροφοριών ως μια μορφή συλλογής πληροφοριών, υπάρχουν πολλοί οργανισμοί που χρησιμοποιούν αναλυτές πληροφοριών για τη συλλογή και παραγωγή πληροφοριών.

Όταν οι πληροφορίες δεν είναι ακριβείς, ονομάζονται σφάλματα πληροφοριών (intelligence errors). Η C.I.A. (2008) περιγράφει τα σφάλματα πληροφοριών ως πραγματικές ανακρίβειες στην ανάλυση, που προκύπτουν από ανεπαρκή ή ελλιπή δεδομένα. Η αποτυχία πληροφοριών είναι συστηματική οργανωτική έκπληξη που προκύπτει από λανθασμένες, εξαφανισμένες, απορριπτόμενες ή ανεπαρκείς υποθέσεις. Τα λάθη της πληροφόρησης θα μπορούσαν να είναι το αποτέλεσμα ενός αναλυτή της υπηρεσίας πληροφοριών που παρερμήνευσε την πρόθεση του εχθρού, κάτι που δεν συμβαίνει επειδή ο αναλυτής παρερμήνευσε τις πληροφορίες που υπήρχαν, αλλά επειδή κακώς κρίνει την πρόθεση του αντιπάλου, λόγω πληροφοριών που δεν υπήρχαν.

### 3.4. Ωφελείται ή ζημιώνεται το κράτος που κάνει υποκλοπές οικονομικών πληροφοριών και τεχνολογίας;

Η υποκλοπή οικονομικών πληροφοριών και τεχνολογίας όπως αναλύθηκε σε προηγούμενη ενότητα, αποδίδει και κατά συνέπεια ωφελεί το κράτος που την ασκεί. Ωστόσο αυτό είναι ένα βραχυπρόθεσμο πλεονέκτημα, κι αυτό γιατί με την εφαρμογή της οικονομικής κατασκοπείας, το κράτος, μπορεί να μείνει πίσω από τις εξελίξεις σε σχέση με τα κράτη που ανταγωνίζεται. Το κράτος που ασκεί οικονομική κατασκοπεία, αν δεν επιδιώξει, άμεσα, να γίνει καινοτόμο και ανταγωνιστικό με τις δικές του δυνάμεις, δε θα μπορέσει να διατηρήσει το προβάδισμα που έλαβε μέσα από τις υποκλοπές. Με γνώμονα αυτό γεννάται το ερώτημα αν οι υποκλοπές οικονομικών πληροφοριών και τεχνολογίας μπορούν να έχουν αρνητικό οικονομικό αντίκτυπο για το κράτος που τις απέκτησε μέσω των υπηρεσιών. Το ερώτημα αυτό απαντάται μέσα από παραδείγματα με δράσεις υπηρεσιών πληροφοριών που αποκαλύφθηκαν από τα αντίστοιχα τμήματα που ασκούν οικονομική αντικατασκοπεία.

Το 2017 οι Albrecht Glitz – από το Τμήμα Οικονομικών Επιστημών και Επιχειρήσεων του Πανεπιστημίου Pompeu Fabra της Βαρκελώνης, και Erik Meyersson – από την Σχολή Οικονομικών Επιστημών της Στοκχόλμης, δημοσίευσαν στο περιοδικό του Γερμανικού Ινστιτούτου Οικονομικών Ερευνών - Institute of Labor Economics (IZA), την έρευνα τους για την βιομηχανική κατασκοπεία (industrial espionage), με το κεντρικό ερώτημα αυτής να είναι το κατά πόσο αποδίδει η κατασκοπεία οικονομικών πληροφοριών και τεχνολογίας, για τη χώρα που την ασκεί. Οι ερευνητές έπειτα από πολυετείς διαπραγματεύσεις με τον Οργανισμό του Ομοσπονδιακού Επιτρόπου για τα αρχεία της Υπηρεσίας Κρατικής Ασφάλειας της Λαοκρατική Δημοκρατία της Γερμανίας (B.St.U.), κατάφεραν να αποκτήσουν πρόσβαση και να μελετήσουν απόρρητες αναφορές πρακτόρων της που αφορούσαν οικονομικά, επιχειρηματικά και τεχνολογικά μυστικά, τα οποία είχαν υποκλέψει κατά την περίοδο του Ψυχρού Πολέμου. Πιο συγκεκριμένα, οι ερευνητές μελέτησαν τα αρχεία της περιόδου 1970 – 1989 από το Υπουργείο Κρατικής Ασφάλειας (M.F.S.) της Λαοκρατικής Δημοκρατίας της Γερμανίας (Λ.Δ.Γ.), που υπαγόταν η Υπηρεσία Κρατικής Ασφάλειας (Stasi) και η οποία την εποχή εκείνη είχε πολύ μεγάλο δίκτυο δράσης με πολλές επιτυχίες στην υποκλοπή μυστικών υψίστης οικονομικής και τεχνολογικής σημασίας, από τους αντιπάλους της. Οι υποκλοπές που έγιναν την περίοδο που εστίασε η έρευνα, αφορούσαν ένα ευρύ φάσμα αντικειμένων, όπως η στρατιωτική τεχνολογία, η μεταλλουργία, οι κατασκευές μηχανών και οχημάτων, οπλικών συστημάτων, ηλεκτρονικών υπολογιστών και μικροϋπολογιστών, καθώς επίσης και η παραγωγή χημικών και πυρηνικής ενέργειας.

Οι Glitz και Meyersson ταξινόμησαν τις υποκλοπές ανά παραγωγικό τομέα σε 16 επιμέρους τομείς και στη συνέχεια μελέτησαν πώς εξελίχθηκε διαχρονικά η συνολική παραγωγικότητα σε καθένα από αυτούς τους τομείς στην οικονομία της Λαοκρατικής Δημοκρατίας της Γερμανίας συγκρίνοντας την παράλληλα με αυτή της Ομοσπονδιακής Δημοκρατίας της Γερμανίας (Ο.Δ.Γ.). Κατά τους ερευνητές, η εξέλιξη της ολικής παραγωγικότητας (total

productivity) – που αφορά την αποτελεσματικότητα της αξιοποίησης του συνόλου των χρησιμοποιούμενων συντελεστών παραγωγής, αποτελεί βασικό δείκτη καινοτομίας σε έναν κλάδο και γενικότερα σε ένα κράτος. Από την έρευνα προέκυψε ότι οι υποκλοπές που έκαναν οι πράκτορες της Stasi, ώθησαν την παραγωγικότητα της Λ.Δ.Γ. με αποτέλεσμα να πλησιάσει τα επίπεδα της Ο.Δ.Γ. Οι υποκλοπές που έγιναν στον τομέα της πληροφορικής και των τηλεπικοινωνιών, έπαιξαν καθοριστικό ρόλο στο να μειωθεί η διαφορά παραγωγικότητας μεταξύ των δύο κρατών.

Σύμφωνα με τα στοιχεία της έρευνας, η σχέση μεταξύ του οφέλους και του κόστους (B.C.R.) για την άσκηση της κατασκοπείας είναι θετική. Καθότι, τα ετήσια έσοδα της Λαοκρατικής Δημοκρατίας της Γερμανίας για την άσκηση της κατασκοπείας ήταν περίπου 7,3 δισεκατομμύρια γερμανικά μάρκα το 1988, ενώ αντιστοίχως τα έξοδα ανέρχονταν σε περίπου 17,5 εκατομμύρια γερμανικά μάρκα. Συνεπώς αυτά τα στοιχεία δείχνουν μια πολύ υψηλή απόδοση της επένδυσης στη κατασκοπεία. Ωστόσο, κατά τους Glitz και Meyersson (2017), η οικονομική κατασκοπεία κατέστρεψε τις μακροπρόθεσμες επενδύσεις της Λ.Δ.Γ. για έρευνα και ανάπτυξη (R&D). Επίσης, όπως αναφέρει ο Κωνσταντόπουλος (2010) δείκτης τεχνολογικής προόδου είναι και το ποσό που δαπανάται από ένα κράτος για R&D στον στρατιωτικό τομέα (military R&D). Η άποψη των Glitz και Meyersson είναι ότι οι κρατικές δημόσιες επενδύσεις, αλλά και οι ιδιωτικές επενδύσεις για R&D, θα πρέπει να συνυπολογίζονται στο κόστος της κατασκοπείας. Επιπροσθέτως, θα πρέπει να συνυπολογίζονται και τα τεχνολογικά προγράμματα και οι πατέντες που δεν υλοποιήθηκαν, λόγω του συντηρητικού πνεύματος που υπήρχε στο κράτος και το οποίο δεν επέτρεψε την ανάπτυξη της καινοτομίας. Χαρακτηριστικά ο Meyersson αναφέρει ότι: «η κατασκοπεία μπορεί να είναι ένας τρόπος να προλάβεις τον ανταγωνιστή σου, αλλά αυτό δεν αποτελεί στρατηγική για να γίνεις παγκόσμιος ηγέτης».

Όπως υποστηρίζει η Kristie Macrakis – του Ινστιτούτου Τεχνολογίας της Τζόρτζια (Georgia Tech) στην Ατλάντα των Ηνωμένων Πολιτειών, το πρόγραμμα οικονομικής και βιομηχανικής κατασκοπείας που εφήρμοσε η Stasi, βοήθησε την Λ.Δ.Γ. να εξοικονομήσει περίπου 17 εκατομμύρια γερμανικά μάρκα σε δαπάνες για περαιτέρω R&D. Ωστόσο, το πρόγραμμα της οικονομικής κατασκοπείας που εφήρμοσε στον τομέα της πληροφορικής και της τεχνολογίας δεν επέφερε τα αποτελέσματα που ήθελε η Λ.Δ.Γ. (Macrakis, 2008).

Από τη συγκεκριμένη μελέτη, που αποτελεί παράδειγμα άσκησης οικονομικής κατασκοπείας, προκύπτει το συμπέρασμα ότι η Λ.Δ.Γ. ωφελήθηκε από τις αποδόσεις της κατασκοπείας που άσκησε, επιτρέποντας στην οικονομία της να συμβαδίζει με την αύξηση της παραγωγικότητας που επικρατούσε στις χώρες της Δύσης. Ο εμπορικός αποκλεισμός που έκαναν οι χώρες της Δύσης στην Ανατολή, σε συνδυασμό με την αφθονία των πηγών πληροφοριών σε στρατηγικά σημαντικές τοποθεσίες, μείωσαν το κόστος της βιομηχανικής κατασκοπείας σε σχέση με την R&A. Η Stasi μπόρεσε κατά την διάρκεια του Ψυχρού Πολέμου να καταστήσει την βιομηχανική κατασκοπεία ως ένα αποτελεσματικό εργαλείο, που ακόμα και στην σημερινή εποχή είναι κάτι αρκετά δύσκολο. Τα οφέλη της βιομηχανικής κατασκοπείας όπως

εφαρμοζόταν την εποχή του Ψυχρού Πολέμου ενδέχεται να έχουν μειωθεί και αυτό εξαιτίας των πιο ολοκληρωμένων διεθνών αγορών που υφίστανται σήμερα, αλλά και λόγω της ευκολότερης πρόσβασης σε νέες καινοτόμες ιδέες, μέσω νόμιμων καναλιών.

Η τεχνολογική και βιομηχανική κατασκοπεία βοήθησε την Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών (Ε.Σ.Σ.Δ) να αποκτήσει την τεχνολογία για να κατασκευάσει λίγα χρόνια μετά τις Η.Π.Α. την ατομική βόμβα. Αλλά και οι Η.Π.Α., πολύ νωρίτερα, στις αρχές του 19ου αιώνα, είχαν θέσει τα θεμέλια για να γίνουν παγκόσμια δύναμη, χάρη στη συστηματική υποκλοπή τεχνολογικών μυστικών και εξειδικευμένων επιστημόνων που έκαναν από άλλες χώρες της Ευρώπης.

### 3.5. Ανταγωνιστική ευφυΐα (competitive intelligence)

Η πληροφορία στον 21<sup>ο</sup> αιώνα τείνει να γίνει το πολυτιμότερο αγαθό για τους κρατικούς οργανισμούς και για τις επιχειρήσεις. Αυτοί που μπορούν να διαχειριστούν σωστά τα δεδομένα τους έχουν συγκριτικό πλεονέκτημα έναντι των ανταγωνιστών τους. Οι σύγχρονες επιχειρήσεις επικεντρώνονται στην μετατροπή της διαθέσιμης μη-δομημένης πληροφορίας σε ένα επιχειρηματικό πλεονέκτημα και με αυτό τον τρόπο ωφελούνται.

Εκτός της κλασσικής, εννοιολογικά και εφαρμοστικά, κατασκοπείας που περιγράφηκε νωρίτερα, υπάρχουν και άλλες μορφές κατασκοπείας που αφορούν κυρίως τον ιδιωτικό τομέα. Η ανταγωνιστική ή επιχειρηματική ευφυΐα (competitive ή business intelligence) είναι μια από αυτές τις πρακτικές που χρησιμοποιούνται στο άκρως ανταγωνιστικό επιχειρηματικό περιβάλλον της εποχής.

Ουσιαστικά η C.I. είναι ένας τρόπος να βοηθηθεί μια επιχείρηση να αποκτήσει και στη συνέχεια να διατηρήσει ένα ανταγωνιστικό πλεονέκτημα έναντι των αντιπάλων. Η χρήση νόμιμων και δεοντολογικών διαδικασιών για τη συλλογή δεδομένων, τα οποία στη συνέχεια αναλύονται για να βοηθήσουν μια επιχείρηση, κερδοσκοπική, μη κερδοσκοπική ή κυβερνητική να ανταγωνιστεί καλύτερα τις άλλες (McGonagle 2016). Οι επιχειρήσεις μπορούν να συγκεντρώσουν τις πληροφορίες που θέλουν από πλήθος μέσων που έχουν πρόσβαση με νόμιμο τρόπο. Αυτές οι πηγές άντλησης πληροφοριών είναι τα Μ.Μ.Ε., ο ηλεκτρονικός και έντυπος τύπος, οι δημοσιεύσεις στα επιστημονικά περιοδικά, οι ισολογισμοί των ανταγωνιστών και φυσικά το διαδίκτυο.

Η δυνατότητα συλλογής πληροφοριών σε όλο το ανταγωνιστικό περιβάλλον, που περιλαμβάνει ανταγωνιστές μιας επιχείρησης, προμηθευτές, πελάτες και δυνητικούς ανταγωνιστές, καθώς και το ρυθμιστικό και πολιτικό περιβάλλον (McGonagle 2016). Αποτελεί πάγια τακτική στις συναντήσεις των στελεχών των επιχειρήσεων σε επαγγελματικές εκθέσεις και συνέδρια να επιδιώκεται η άντληση πληροφοριών από τους ανταγωνιστές τους. Μέσα από αυτές τις κοινωνικές εκδηλώσεις προσπαθούν να προωθήσουν τα δικά τους συμφέροντα με κίνδυνο κάποιες φορές να αποκαλύπτουν πληροφορίες που θα ήταν πολύ



χρήσιμες στους ανταγωνιστές τους. Σε αυτή την άτυπη μάχη μεταξύ των επιχειρήσεων, μετέχει εξειδικευμένο προσωπικό με στόχο να αποσπάσει όσο το δυνατόν περισσότερες πληροφορίες από την άλλη επιχείρηση. Συχνά τα άτομα αυτά παρουσιάζονται ως πελάτες ή ερευνητές, οπότε και είναι πιο δόκιμο να πληροφορηθούν εκτενώς για το προϊόν ή την υπηρεσία που έχουν ως στόχο. Με την κατάλληλη εκπαίδευση αποσπών αυτές τις πληροφορίες από τους υπαλλήλους που δεν αντιλαμβάνονται το τέχνασμα.

Τα συστήματα της ανταγωνιστικής ευφυΐας έχουν σχεδιασθεί για την υποστήριξη της διαδικασίας λήψης αποφάσεων. Έτσι, με έναν έμμεσο τρόπο η επιχείρηση κοινοποιεί τα μυστικά της, βάσει των οποίων οι ανταγωνιστές διαμορφώνουν άποψη για το πως θα κινηθούν στο δικό τους περιβάλλον. Η ανακάλυψη της διαρροής αυτών των πληροφοριών μπορεί να αργήσει να γίνει αντιληπτή και να μην μπορούν να αντιμετωπιστούν οι συνέπειες. Δεν αποτελούν καινούρια τεχνολογία, αλλά μια σειρά από προηγούμενα συστήματα που είχαν σχεδιασθεί για τον ίδιο σκοπό από τις υπηρεσίες πληροφοριών. Ο ρόλος της επιχειρηματικής ευφυΐας είναι να συλλέξει εκείνα τα δεδομένα που κρίνονται ως σημαντικά για την επιχείρηση και να τα μετατρέψει σε χρήσιμες πληροφορίες για τους ιθύνοντες (Gibson et al, 2004).

Οι επιχειρήσεις όταν αναζητούν προσωπικό, δείχνουν πολύ μεγάλο ενδιαφέρον στα άτομα που κατά το παρελθόν έχουν εργασθεί σε μεγάλους ομίλους. Πέραν της εμπειρίας που έχουν αποκτήσει αυτά τα άτομα, οι επιχειρήσεις με αυτό τον τρόπο μπορούν να βελτιώσουν το δικό τους επίπεδο, καθώς αποκτούν μέσω αυτών των υπαλλήλων, μια τεχνογνωσία που μέχρι πριν δεν είχαν. Σε εθνικό επίπεδο μάλιστα, κάποιος που έχει εργαστεί σε επιχειρήσεις εκτός της χώρας του και επιστρέφει σε αυτή, έχει το πλεονέκτημα σε σχέση με αυτόν που έχει εργαστεί σε επιχειρήσεις μόνο της χώρας του. Τυπικά ένα άτομο θα δείξει περισσότερη αφοσίωση σε επιχείρηση της χώρας του συγκριτικά με μια ξένη εταιρεία και είναι πιο πιθανό εάν του ζητηθεί να αποκαλύψει πληροφορίες προς όφελος του εθνικού συμφέροντος, να το κάνει.

Υπάρχουν και περιπτώσεις όπου στο επιχειρηματικό αυτό «παιχνίδι» εμπλέκονται και κρατικοί οργανισμοί. Για παράδειγμα, οι υπηρεσίες πληροφοριών σε ειδικές περιπτώσεις μεσολαβούν στο να προσληφθεί ένας υπήκοος της χώρας τους σε μια ξένη εταιρεία, προκειμένου να μπορούν στο μέλλον να πάρουν από αυτόν τις πληροφορίες που επιθυμούν για την εταιρεία ή την ξένη χώρα γενικότερα. Όπως επίσης συμβαίνει να επιθυμεί μια εταιρεία να δραστηριοποιηθεί σε μια ξένη χώρα και να δέχεται πιέσεις από συγκεκριμένες κρατικές υπηρεσίες της χώρας για να έχει ανταποδοτικά οφέλη ή δραστηριότητα της εκεί.

Μια άλλη άποψη είναι ότι η μετακίνηση στελεχών από μια εταιρεία σε μια άλλη, συνεπάγεται την μεταφορά γνώσης στους ανταγωνιστές. Οι επιχειρηματικοί όμιλοι που κάνουν κοινοπραξίες διακινδυνεύουν μέσω αυτής της ενέργειας να γίνει διαρροή των μυστικών τους σε μικρότερες επιχειρήσεις και να χάσουν το πλεονέκτημα που είχαν. Βέβαια σε μια τέτοια περίπτωση συνήθως χρησιμοποιείται ένα άλλο τέχνασμα που είναι η εξαγορά της μικρότερης επιχείρησης, οπότε κατά συνέπεια δε θα υπάρξει απώλεια τεχνογνωσίας.

Στην ανταγωνιστική ευφυΐα όπως περιγράφηκε, οι δρώντες είναι πολλοί, ανταγωνιστές εντός και εκτός συνόρων που επιθυμούν να αποκτήσουν το πλεονέκτημα, ξένοι κυβερνητικοί οργανισμοί, μικρές εταιρείες που δε διαθέτουν τους απαραίτητους πόρους για να αναπτύξουν την τεχνολογία που επιθυμούσαν ή δεν είχαν την τεχνογνωσία.

Μια ακόμα περίπτωση είναι η διαρροή των πληροφοριών της εταιρείας να γίνεται ηθελημένα από τους υπαλλήλους. Και εδώ διακρίνονται δυο πιθανά σενάρια για την απόφαση των εργαζομένων:

- είτε να είναι δυσαρεστημένοι από την εργασία τους στην επιχείρηση,
- είτε γιατί επιθυμούν το κέρδος μέσω της συναλλαγής με τους ανταγωνιστές, πουλώντας τις οικονομικές πληροφορίες και τα εμπορικά μυστικά που επιθυμούν.

Ωστόσο, είναι εξίσου πιθανό οι οικονομικές πληροφορίες, η τεχνολογία και τα εμπορικά μυστικά να πωλούνται από έναν πρώην υπάλληλο μιας εταιρείας. Και πάλι, εδώ διακρίνονται δυο πιθανά σενάρια για τα αίτια της απόφασης του:

- είτε επειδή είναι δυσαρεστημένος που έφυγε/απολύθηκε από την επιχείρηση και θέλει να εκδικηθεί,
- είτε γιατί επιθυμεί το κέρδος.

Για τον λόγο αυτό, το προσωπικό εντός των εταιρειών αποτελεί το πρώτο τρωτό σημείο. Ιδιαίτερα οι εργαζόμενοι σε τμήματα που έχουν άμεση πρόσβαση στη βάση δεδομένων της επιχείρησης και ακόμα περισσότερο οι διαχειριστές των πληροφοριακών συστημάτων οι οποίοι έχουν πρόσβαση σε ευαίσθητες πληροφορίες, κώδικες, σχέδια και τυχόν απόρρητες πληροφορίες.

Ένα μέτρο πρόληψης για να περιορίσει τον κίνδυνο η επιχείρηση αφενός, αλλά και να ανακάμψει εάν δεχτεί πλήγμα, είναι να δράσει πρώτη, στέλνοντας ένα άτομο να εργαστεί στην εταιρεία που ανταγωνίζεται. Ανεξαρτήτως της θέσης που θα κατέχει αυτό το άτομο, αποτελεί στρατηγικό πλεονέκτημα να βρίσκεται εντός του «στρατοπέδου του αντιπάλου» ένας πληροφοριοδότης. Το άτομο αυτό, σαν κατάσκοπος, θα προσπαθήσει να αποσπάσει τις πληροφορίες από τους υπαλλήλους – συναδέλφους του, οι οποίοι έχουν την νομιμοποίηση να γνωρίζουν τα στοιχεία που έχει βάλει ως στόχο.

Ωστόσο, ο ρόλος των πληροφοριοδοτών παραμένει σημαντικός. Σε έρευνα του 2014 τα στοιχεία που έγιναν από ένα αντιπροσωπευτικό δείγμα περίπου 7.000 γερμανικών επιχειρήσεων, έδειξαν ότι το 33% των εμπλεκόμενων στις επιχειρήσεις αυτές πιστεύει πως οι δράστες που υποκλέπτουν δεδομένα με οικονομικές πληροφορίες είναι μεταξύ των δικών τους εργαζομένων (Corporate Trust, 2014).

Μια άλλη μέθοδος που χρησιμοποιείται από τις εταιρείες, είναι η προσπάθεια δωροδοκίας ενός υπαλλήλου της ανταγωνίστριας εταιρείας ή ακόμα και ο εκβιασμός του. Σε πολλές περιπτώσεις παράλληλα δημιουργούνται από το εξειδικευμένο προσωπικό ενοχοποιητικά στοιχεία με τεχνικά μέσα, για την μεταξύ τους συναλλαγή, έτσι ώστε να διατηρήσουν το πλεονέκτημα και να επιτύχουν τον σκοπό τους.

#### **4. Προστασία από την οικονομική κατασκοπεία**

Η άνθιση της κατασκοπείας, όπως ειπώθηκε σε προηγούμενο κεφάλαιο, έγινε την περίοδο του Ψυχρού Πολέμου. Καθότι η οικονομική κατασκοπεία εφαρμόζεται για να αποσπάσει πληροφορίες, τα μέτρα προστασίας είναι απαραίτητα. Στο κεφάλαιο αυτό αναλύονται η έννοια του διπλώματος ευρεσιτεχνίας, των εμπορικών μυστικών, γίνεται ο προσδιορισμός των ιδιοκτησιακών πληροφοριών, περιγράφονται οι στόχοι της οικονομικής κατασκοπείας εντός ενός οργανισμού και οι τρόποι διεξαγωγής των υποκλοπών.

Λόγω της παγκόσμιας διαθέσιμης υποδομής και της ανάπτυξης των δυνατοτήτων στον τομέα των υπολογιστών και των τηλεπικοινωνιών σε παγκόσμιο επίπεδο, η τεχνολογία επέτρεψε στις υπηρεσίες πληροφοριών και τις εταιρείες να ανταγωνίζονται παγκοσμίως με όρους ακραίου ανταγωνισμού.

Όπως αναφέρθηκε σε προηγούμενη ενότητα η οικονομική κατασκοπεία εστιάζει στην υποκλοπή πληροφοριών οικονομικού περιεχομένου που δίνουν πλεονέκτημα. Αναλυτικότερα τέτοιες πληροφορίες είναι τα εμπορικά μυστικά και οι πληροφορίες σχετικά με τα διπλώματα ευρεσιτεχνίας καθώς και οι τεχνικές και οι διαδικασίες βιομηχανικής κατασκευής, οι ιδέες και οι τύποι. Όπως επίσης μπορεί να περιλαμβάνει, τη δέσμευση ιδιοκτησιακών ή επιχειρησιακών πληροφοριών, όπως είναι τα δεδομένα για τους πελάτες, τις πωλήσεις, την τιμολόγηση, την έρευνα και ανάπτυξη (R&D), τις πολιτικές που ακολουθούνται, τις προοπτικές προσφορών, τις στρατηγικές σχεδιασμού ή μάρκετινγκ ή τις μεταβαλλόμενες συνθέσεις και τις τοποθεσίες παραγωγής. Ουσιαστικά θα μπορούσε να περιλαμβάνει οτιδήποτε δίνει στην επιχείρησή ένα πλεονέκτημα στην αγορά και την κάνει επιτυχημένη.

Οι προκλήσεις και τα προβλήματα που αντιμετωπίζει μια σύγχρονη επιχείρηση είναι πάρα πολλά, γιατί το περιβάλλον στην σημερινή εποχή είναι πολύ ανταγωνιστικό. Οι πληροφορίες μεταδίδονται με ασύλληπτες ταχύτητες και αυτό πολλές φορές εγκυμονεί κινδύνους για την ασφάλεια. Την ίδια στιγμή που εφαρμόζονται νέες τεχνολογίες, δημιουργούνται και νέα τρωτά σημεία στα συστήματα. Γίνεται άμεσα αντιληπτό ότι η προστασία της πνευματικής ιδιοκτησίας για τις εταιρείες είναι ζωτικής σημασίας, όχι μόνο για να διατηρηθεί το ανταγωνιστικό πλεονέκτημα που έχουν, αλλά για να διατηρήσουν την ύπαρξη τους στο επιχειρηματικό περιβάλλον. Με αυτό τον τρόπο διασφαλίζουν τα ηθικά και πνευματικά τους δικαιώματα.

Η προστασία έχει πάντα σκοπό την διατήρηση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των δεδομένων και περιλαμβάνει:

- νομικές λεπτομέρειες, όπως είναι τα διπλώματα ευρεσιτεχνίας και τα εμπορικά μυστικά,
- φυσική και τεχνολογική ασφάλεια, για τον εξοπλισμό και το λογισμικό,
- πληροφορική διακυβέρνηση, όπως η πολιτική που θα ακολουθείται, η εφαρμογή κανόνων και ελεγκτικούς μηχανισμούς,
- οικονομικούς περιορισμούς, μέσα από τον προϋπολογισμό,
- και εκπαίδευση του προσωπικού.

Το 2007 στην σύνοψη με τα συμπεράσματα της η Αμερικανική Επιτροπή Ελέγχου Οικονομικών και Ασφάλειας Ηνωμένων Πολιτειών – Κίνας (U.S.C.C.) προς την αμερικανική κυβέρνηση αναφέρει ότι η κινεζική κατασκοπεία αποτελεί την μεγαλύτερη απειλή για την τεχνολογία των Ηνωμένων Πολιτειών, μέσω της οποίας αποκτούνται βαρυσήμαντες πληροφορίες στρατιωτικού και βιομηχανικού περιεχομένου που έχουν σαν αποτέλεσμα την ενδυνάμωση της Κίνας. Στις συστάσεις της η U.S.C.C. κάνει λόγο για την αναγκαιότητα του ελέγχου των εξαγωγών και της λήψης μέτρων κατά της κατασκοπείας, ενώ κάνει ιδιαίτερη μνεία στην οικονομική κατασκοπεία η οποία είναι επιδοτούμενη, σύμφωνα με τον νόμο περί οικονομική κατασκοπείας του 1996 (Economic Espionage Act of 1996).

Η επιλογή της βέλτιστης στρατηγικής προστασίας της πνευματικής ιδιοκτησίας εξαρτάται από το είδος και τον βαθμό προστασίας που παρέχουν, το κόστος τους και τελικά την αξία που έχει η συγκεκριμένη πνευματική αξία για τον ιδιοκτήτη της.

Η προστασία και η ασφάλεια των πληροφοριών χρειάζεται ανθρώπινο δυναμικό, τεχνολογίες, οικονομικούς πόρους και κατάλληλες πολιτικές πληροφοριακής διακυβέρνησης (Μαυρίδης 2015).

Ο Peter Schweizer – αμερικανός ερευνητής, δημοσιογράφος και συγγραφέας, έχει γράψει στο Foreign Affairs ότι το νομικό πλαίσιο για εκείνους που συλλαμβάνονται να ασκούν οικονομική κατασκοπεία πρέπει να γίνει πιο αυστηρό, καθότι και η πιο επιτυχημένη οργάνωση αντικατασκοπείας, δεν μπορεί να βοηθήσει σε αυτό.

## 4.1. Δίπλωμα ευρεσιτεχνίας

Το δίπλωμα ευρεσιτεχνίας είναι τίτλος προστασίας με ισχύ 20 χρόνων που χορηγείται στον δικαιούχο για νέα επινοήματα με εφευρετική δραστηριότητα και επιδεκτικά βιομηχανικής εφαρμογής (Οργανισμός Βιομηχανικής Ιδιοκτησίας).

Ένα δίπλωμα ευρεσιτεχνίας παρέχει στον ιδιοκτήτη το δικαίωμα αποκλειστικής χρήσης, πώλησης και εκμετάλλευσης της εφεύρεσης του αποκλείοντας κάθε άλλον. Ωστόσο, χρειάζεται προσοχή στην διατύπωση των στοιχείων και χαρακτηριστικών, έτσι ώστε να παρέχεται επαρκής κάλυψη, διαφορετικά υπάρχει ο κίνδυνος να έχει τρωτά σημεία και οι ανταγωνιστές να επωφεληθούν από αυτά.

Με το δίπλωμα ευρεσιτεχνίας μια εταιρεία έχει επιχειρηματικό πλεονέκτημα στην αγορά καθότι οι ανταγωνιστές δε μπορούν να εκμεταλλευτούν ότι εμπεριέχεται σε αυτό. Έτσι προστατεύεται νομικά και η εμπιστευτικότητα των δεδομένων. Το βασικότερο πλεονέκτημα του είναι ότι η εταιρεία προωθεί το προϊόν της στην αγορά χωρίς ανταγωνισμό.

Το δίπλωμα ευρεσιτεχνίας όσο καλό κι αν είναι από άποψη κατοχύρωσης, άλλο τόσο δύσκολο και χρονοβόρο είναι να το αποκτήσει μια εταιρεία λόγω της διαδικασίας χορήγησης του. Στην Ελλάδα, σύμφωνα με τον Οργανισμό Βιομηχανικής Ιδιοκτησίας που είναι η αρμόδια αρχή ελέγχου, πιστοποίησης και έκδοσης του διπλώματος ευρεσιτεχνίας, η διαδικασία έχει ως εξής:

- την κατάθεση της αίτησης,
- προθεσμία τεσσάρων μηνών για να γίνουν τυχόν διορθώσεις ή να συμπληρωθούν ελλείψεις της εφεύρεσης,
- έλεγχος για το τι νέο είναι και τι εφευρετικό / καινοτόμο έχει, σύνταξη της έκθεσης έρευνας ή έκθεσης έρευνας με αιτιολογημένη γνώμη,
- επιπλέον τρεις μήνες προθεσμία για παρατηρήσεις του καταθέτη στην έκθεση έρευνας,
- σύνταξη της τελικής έκθεσης έρευνας ή τελικής έκθεσης έρευνας με αιτιολογημένη γνώμη, και
- εν συνεχεία γίνεται η έκδοση του διπλώματος ευρεσιτεχνίας.

Υπάρχουν περιπτώσεις, όπου μικρές εταιρείες πούλησαν το δίπλωμα ευρεσιτεχνίας και τα δικαιώματα χρήσης του, σε μεγάλες πολυεθνικές επιχειρήσεις, κάτι το οποίο τους απέφερε μεγάλα κέρδη.

Στον χώρο της πληροφορικής και των τηλεπικοινωνιών είναι σύνηθες φαινόμενο οι διαμάχες μεταξύ εταιρειών, όπως για παράδειγμα η διαμάχη μεταξύ της Apple και τριών εταιρειών – H.T.C., Samsung και Motorola Mobility, που αποτελούν πλέον εταιρείες του Google (New York Times 2012).

## 4.2. Τεχνογνωσία και εμπορικά μυστικά

Οι πληροφορίες που χρησιμοποιούνται από μια εταιρεία για την εμπορική της δραστηριότητα και δεν είναι γνωστές σε άτομα εκτός της εταιρείας ονομάζονται εμπορικά μυστικά. Τα εμπορικά μυστικά μπορεί να είναι είτε υλικά, είτε άυλα, αποθηκευμένα με κάθε τρόπο στην εταιρεία. Ωστόσο, για να θεωρηθούν οι πληροφορίες αυτές εμπιστευτικές θα πρέπει να είναι μυστικές και να έχουν εμπορική αξία που να δίνει στην εταιρεία που τις κατέχει ανταγωνιστικό πλεονέκτημα.

Η μεθοδολογία για την προστασία μέσω των εμπορικών μυστικών περιλαμβάνει:

- την αναγνώριση τους,
- την καταγραφή τους,
- την εκτίμηση της αξίας τους, και
- την κατηγοριοποίηση τους ανάλογα με τις επικείμενες απειλές και την τρωτότητα που μπορεί να έχουν και να καθορίζουν την επικινδυνότητα τους.

Η προστασία των εμπορικών μυστικών γίνεται μέσω προγραμμάτων εμπορικής διακυβέρνησης, συμφωνητικά εμπιστευτικότητας, σήμανση, ιχνηλάτηση, ασφαλή αποθήκευση των εμπιστευτικών πληροφοριών, εκπαίδευση του προσωπικού και νομική προστασία που θα δράση άμεσα σε περίπτωση διαρροής τους.

Οι υπάλληλοι που παράγουν και διαχειρίζονται πληροφορίες υψίστης εμπορικής αξίας, καθώς επίσης και οι συνεργάτες, θα πρέπει να γνωρίζουν την ευθύνη που φέρουν όσον αφορά τα εμπορικά μυστικά. Για τον λόγο αυτό χρειάζεται να τους παρέχεται εκπαίδευση για τους πιθανούς κινδύνους από την κατασκοπεία και την υποκλοπή των ευαίσθητων πληροφοριών, της πνευματικής ιδιοκτησίας, της πειρατείας και της αντιγραφής αυτών.

Αν τα εμπορικά μυστικά δημοσιοποιηθούν χωρίς την έγκριση αυτών που έχουν την νομιμοποίηση να τα γνωρίζουν, τότε θα πρέπει να αποδεικνύεται ότι αυτές οι πληροφορίες ήταν όντως εμπιστευτικές και ότι είχαν ληφθεί όλα τα απαραίτητα μέτρα προστασίας, έτσι ώστε να μπορούν να έχουν νομική ισχύ οι ισχυρισμοί του παθόντα. Οι ελεγκτικοί μηχανισμοί για την προστασία των πληροφοριών είναι σε θέση να συγκεντρώσουν στοιχεία και να βρουν τα ίχνη του δράστη και να τον εντοπίσουν.

#### 4.3. Οι στόχοι της οικονομικής κατασκοπείας εντός ενός οργανισμού

Συνήθως οι εταιρίες επικεντρώνονται πολύ περισσότερο στις εξωτερικές απειλές και στη συνέχεια εντοπίζουν απειλές στα πληροφοριακά τους συστήματα. Αυτοί οι τομείς εντός των εταιρειών που είναι σημαντικοί και οι οποίοι θα πρέπει να διασφαλίζονται γιατί είναι εν γένει στόχοι από υπηρεσίες πληροφοριών και ανταγωνιστές είναι οι εξής:

- Τα εμπορικά μυστικά και τα διπλώματα ευρεσιτεχνίας

Πρέπει να προστατεύονται νομικά. Είτε πρόκειται για τύπους, είτε για πρακτικές, είτε για σχέδια διεργασιών ή εφευρέσεις, καθώς είναι τα σημαντικότερα όλων και πρέπει να έχουν περισσότερες από τις κατάλληλες διασφαλίσεις.

- Τα στελέχη και τα μέλη του διοικητικού συμβουλίου

Οι ευαίσθητες συζητήσεις, η τεχνογνωσία, οι συναντήσεις σχετικά με την στρατηγική και το όραμα, τα σχέδια επέκτασης, οι συγχωνεύσεις, οι εξαγορές και οι εταιρικές σχέσεις.

- Οι ανθρώπινοι πόροι

Οι διαδικασίες πρόσληψης, οι μισθοί και η αποζημίωση βασικών υπαλλήλων, καθώς και οι αξιολογήσεις της απόδοσης τους.

- Η έρευνα και η ανάπτυξη

Οι ευαίσθητες πληροφορίες για νέα σχέδια, εφευρέσεις, εκκρεμείς ευρεσιτεχνίες, έρευνα και άτομα με πολύτιμες γνώσεις.

- Οι πωλήσεις και το μάρκετινγκ

Οι στρατηγικές πωλήσεων, τα σχέδια τιμολόγησης, οι προϋπολογισμοί μάρκετινγκ, οι πληροφορίες προσφορών, το πελατολόγιο και οι πληροφορίες σχετικά με το δίκτυο των μεταπωλητών.

- Οι εταιρικές λειτουργίες

Το κόστος, τα στοιχεία προϋπολογισμού, οι υποδομές πληροφορικής και τα σχέδια συνέχειας των επιχειρήσεων.

- Στην βιομηχανία

Οι συνεργάτες και τα εξαρτήματα της αλυσίδας εφοδιασμού των εταιρειών, οι ειδικές μεθοδολογίες κατασκευής, τα τελικά προϊόντα, οι πρώτες ύλες και οι βασικές διαδικασίες.

#### 4.4. Προσδιορισμός και ένδειξη απειλής

Οι πιθανοί δρώντες της οικονομικής κατασκοπείας είναι:

- Άτομα εμπιστοσύνης

Αυτά συνήθως είναι οι εργαζόμενοι που αφήνουν τις εταιρίες και παίρνουν παράνομα την πνευματική ιδιοκτησία και άλλες βασικές πληροφορίες μαζί τους.

- Εγκληματικοί οργανισμοί

Οι εγκληματικές οργανώσεις σε παγκόσμιο επίπεδο έχουν μάθει ότι αυτό είναι ένας πολύ κερδοφόρος τομέας για αυτούς, με πολύ μικρό κίνδυνο σε σύγκριση με τους παραδοσιακούς τρόπους κερδοφορίας τους και με πολύ μικρό κόστος.

- Ανταγωνιστές

Όπως αναφέρθηκε και σε προηγούμενη ενότητα, η πρόσληψη εργαζομένων – πληροφοριοδοτών, η υποκλοπή βασικών πληροφοριών με ηλεκτρονικά μέσα ή η πληρωμή ενός υπαλλήλου για να δώσει τις εμπιστευτικές πληροφορίες

- Εξωτερικές υπηρεσίες πληροφοριών

Οι ξένες υπηρεσίες πληροφοριών στοχεύουν στις βασικές πληροφορίες των εταιρειών για να τις διοχετεύσουν στις επιχειρήσεις των χωρών τους.

#### 4.5. Τρόποι διεξαγωγής των υποκλοπών

Οι δρώντες συλλογής πληροφοριών που ασκούν οικονομική κατασκοπεία, σπάνια χρησιμοποιούν μόνο μία μέθοδο συλλογής. Χρησιμοποιούν διάφορες μεθόδους για τη συλλογή πληροφοριών μέσα από ένα συντονισμένο πρόγραμμα κατασκοπείας, μέσω του οποίου επιδιώκουν να επιτύχουν τους σκοπούς τους χωρίς να γίνουν οι ίδιοι άμεσα εμπλεκόμενοι. Οι μέθοδοι αυτοί είναι:

- Στρατολόγηση ατόμου

Αναζήτηση ενός αξιόπιστου ατόμου σε έναν οργανισμό, το οποίο μπορεί να παρέχει τις ευαίσθητες πληροφορίες. Οι συλλέκτες πληροφοριών χρησιμοποιούν το ακρωνύμιο "mide" (χρήμα = money, ιδεολογία = ideology, εξαναγκασμός = duress, εγώ = ego) χαρακτηρίζοντας με αυτό τον τρόπο πως είναι σε θέση να προσλάβουν έναν τέτοιο πράκτορα. Η αναπαραγωγή σε μία ή σε περισσότερες περιοχές αυτών των υπαλλήλων, είναι ο τρόπος με τον οποίο οι περισσότεροι συλλέκτες πληροφοριών θα αναπτύξουν πηγές μέσα σε έναν οργανισμό.



- Παρακολούθηση

Διεξαγωγή φυσικής και ηλεκτρονικής επιτήρησης στις πηγές πληροφοριών. Η απειλή αυτή αυξάνεται όταν οι υπάλληλοι βρίσκονται σε ταξίδια στο εξωτερικό, δεν πρέπει να υπάρχει προσδοκία ιδιωτικότητας σε ξένες χώρες, ειδικά όταν η τηλεπικοινωνιακή υποδομή ανήκει ή λειτουργεί από το εθνικό κράτος.

- Τεχνικές λειτουργίες

Αυτό περιλαμβάνει εισβολές υπολογιστών (phishing κλπ.), στόχευση τηλεπικοινωνιών και φύτευση συσκευών ακρόασης ή κακόβουλου λογισμικού.

- Ξένοι φοιτητές ή υπάλληλοι

Πιέζοντάς τους ξένους φοιτητές ή υπαλλήλους να διεξάγουν κατασκοπεία, μέσα από απειλές για τα μέλη της οικογένειας τους πίσω στην πατρίδα τους ή δοκιμάζοντας το εθνικό τους φρόνημα.

- Συναλλαγές διάσκεψης εμπορίου

Οι συλλέκτες πληροφοριών / ανταγωνιστές / μεσίτες πληροφοριών στοχεύουν συνήθως σε αυτά τα γεγονότα για την ανάπτυξη πληροφοριών και ατόμων, ενώ βρίσκονται σε αρκετά ανοιχτό περιβάλλον.

- Εταιρική συγχώνευση ή εξαγορά

Πολλές χώρες χρησιμοποιούν αυτές τις συναλλαγές για την απόκτηση ευαίσθητων τεχνολογιών που κατέχουν οργανισμοί ξένων χωρών.

- Μίσθωση προσωπικού ανταγωνιστών

Οι αλλοδαπές εταιρείες και οι ανταγωνιστές θα προσπαθήσουν να το κάνουν αυτό και να μάθουν τα εταιρικά μυστικά / πλεονεκτήματα και να τα κάνουν δικά τους.

- Κοινωνική μηχανική

Αυτή έρχεται σε πολλές μορφές, όπως ανεπιθύμητες έρευνες μέσω προσωπικών επαφών, τηλεφώνου, ηλεκτρονικού ταχυδρομείου, φαξ και άλλων μορφών επικοινωνίας, σε αναζήτηση ευαίσθητων πληροφοριών. Επίσης, τα κοινωνικά μέσα δικτύωσης χρησιμοποιούνται συχνά ως εργαλείο από τους συλλέκτες πληροφοριών για να μάθουν περισσότερα για τους στόχους και να αναπτύξουν το πλάνο προσέγγισης για τη συλλογή ευαίσθητων πληροφοριών των ατόμων που θέλουν να στρατολογήσουν.

## Συμπεράσματα

Στην εποχή της πληροφορίας η αναπτυσσόμενη παγκόσμια αγορά συνέβαλε στην είσοδο νέων πολιτισμών και οικονομιών σε μια ανταγωνιστική παγκόσμια οικονομία. Η τεχνολογία είναι σε πολύ υψηλό επίπεδο, ο ανταγωνισμός μεταξύ κρατών και επιχειρήσεων σε αυτό τον τομέα είναι εξίσου πολύ υψηλός. Μέσα από την έρευνα αυτό που προκύπτει, είναι ότι τα κράτη επιθυμούν να αποκτήσουν ακόμα μεγαλύτερη δύναμη μέσα από την γνώση των κινήσεων του αντιπάλου και επενδύουν σε αυτή τους την ανάγκη. Απώτερος σκοπός των κρατών που ασκούν οικονομική κατασκοπεία μέσω των υπηρεσιών πληροφοριών τους, είναι να διατηρήσουν την θέση που κατέχουν φαινομενικά, ενώ παράλληλα επιδιώκουν με μυστικούς τρόπους να αναπτύξουν την τεχνολογία τους ιδιαίτερα στον τομέα των ηλεκτρονικών και της πληροφορικής. Η σύνδεσή της οικονομικής κατασκοπείας με τις πληροφορίες και τις νέες τεχνολογίες δημιουργεί ένα καινούριο πεδίο δράσης στα κράτη, τους οργανισμούς στους οποίους μετέχουν συλλογικά, αλλά και στις επιχειρήσεις. Οι μεγάλες εταιρείες που έχουν παρουσία σε όλο τον κόσμο κινούνται με τον ίδιο τρόπο, αποσκοπούν στην αύξηση των εσόδων τους.

Σε αυτό συνέβαλε το κόστος της άσκησης κατασκοπείας, το οποίο συγκριτικά με την εποχή του Ψυχρού Πολέμου, είναι μειωμένο. Ακόμη περισσότερο με την έλευση της ψηφιακής εποχής και της εμφάνισης της κατασκοπείας στον κυβερνοχώρο, καθότι ως νέα και συγκριτικά οικονομικότερη μέθοδος παράνομης μεταφοράς τεχνολογίας γίνεται πολύ πιο εύκολα. Ως εκ τούτου, τα περισσότερα ανεπτυγμένα κράτη από την αρχή του 21<sup>ου</sup> αιώνα βλέπουν την οικονομική κατασκοπεία ως μια σοβαρή και αυξανόμενη απειλή για τις οικονομίες τους. Όπως αναφέρει ο Κωνσταντόπουλος (2010) ο αυξανόμενος ρόλος της τεχνολογίας στη διεθνή οικονομία δυσκολεύει τις υπηρεσίες πληροφοριών των κρατών να εφαρμόσουν τις πρακτικές αντικατασκοπείας, κι αυτό γιατί ο κατάσκοπος βρίσκεται ανά πάσα στιγμή σε κίνδυνο κατά την διάρκεια της αποστολής του, ενώ ο προγραμματιστής ολοκληρώνει την αποστολή του σε ένα ασφαλές περιβάλλον, μακριά από κινδύνους, με έναν ηλεκτρονικό υπολογιστή. Συμπερασματικά, τα οφέλη για το κράτος που ασκεί οικονομική κατασκοπεία είναι μεγάλα με μικρότερο κόστος και μικρότερο κίνδυνο από οποιαδήποτε παλαιότερη πρακτική κατασκοπείας που απαιτούσε να διακινδυνεύσει το προσωπικό της υπηρεσίας πληροφοριών.

Ως φαίνεται η ανάγκη των ηγετών να έχουν στην κατοχή τους στοιχεία που η γνώση των μυστικών του αντιπάλου είναι κάτι που δε φαίνεται να μεταβάλλει την άποψη των ηγετών δύναμης για τις κυβερνήσεις των κρατών ήταν και είναι πάντα μεγάλος. Ωστόσο, κανείς από τους δρώντες δεν παραδέχονται ανοικτά πως εφαρμόζει την οικονομική κατασκοπεία προς όφελος του.

Οι υποστηρικτές της εφαρμογής της οικονομικής κατασκοπείας υποστηρίζουν ότι ο σκοπός ύπαρξης ενός εθνικού οργανισμού πληροφοριών είναι να προστατεύσει το εθνικό του

συμφέρον. Η οικονομική ανάπτυξη των εγχώριων επιχειρήσεων ασφαλώς μπορεί να χαρακτηριστεί ως μια δραστηριότητα που επηρεάζει την ασφάλεια και την ευημερία των κρατών που ασκούν αυτού του είδους την κατασκοπεία. Κι αυτό γιατί μέσω της εφαρμογής της μπορούν να επιτυγχάνονται οι στρατηγικοί τους στόχοι. Τα κράτη, των οποίων οι υπηρεσίες πληροφοριών ασκούν οικονομική κατασκοπεία, βγαίνουν κερδισμένα ανεξαρτήτως από το εάν η δράση τους γίνει αντιληπτή από το αντίστοιχο τμήμα αντικατασκοπείας του κράτους που στόχευαν. Εξάλλου όπως έχει αναφέρει σε άρθρο του από το 1994 ο William Warner «τα προϊόντα και οι διαδικασίες που σχετίζονται με την τεχνολογία δεν είναι δυνατόν να διαφυλαχτούν όπως το στρατιωτικό υλικό».

Αυτό έχει δημιουργήσει τέτοιες συνθήκες ώστε οι δρώντες να ενεργούν ανεξαρτήτως από το που βρίσκονται και να μπορούν να επιτύχουν τον σκοπό τους και να υποκλέψουν τις πληροφορίες που επιθυμούν.

Σε κάθε περίπτωση οικονομικής κατασκοπείας, το άτομο που την εφαρμόζει έχει πρόσβαση σε πληροφορίες. Είναι πολύ σημαντικό να γίνει κατανοητό από τους απλούς χρήστες το γεγονός ότι υπάρχουν τρόποι ελέγχου των ατόμων που έχουν πρόσβαση στα πληροφοριακά συστήματα και θα πρέπει να εφαρμόζονται για την προστασία των κρίσιμων και μη πληροφοριών.

## Κατάλογος Πηγών

- Banks William (2014), *Cyber Espionage, Surveillance and International Law: Finding Common Ground*, pp,1-10, Institute for National Security and Counterterrorism, Syracuse.
- Born Hans & Caparini Marina (2007), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, pp 4-7. Ashgate Publishing, Bodmil.
- Central Intelligence Agency (2008), *Chapter One. Definitions*. Διαθέσιμο στην ηλεκτρονική διεύθυνση:  
[https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter\\_1.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm).  
Πρόσβαση: 16/09/ 2018.
- Central Intelligence Agency (2010), *Human Intelligence*. Διαθέσιμο στην ηλεκτρονική διεύθυνση:  
<https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html>. Πρόσβαση: 16/09/ 2018.
- Chekinov Sergei & Bogdanov Sergei (2013), *The Nature and Content of a New-Generation War* United States: Military Thought, pp. 16.
- Clow Ryan (2008), *Psychological Operations: The need to understand Psychological Plane to Warfare*, Canadian Military Journal, Volume 9, No.1, pp 21-29.
- CNews (2018), *Affaire des 2 Ex-Espions de la D.G.S.E.: "Des Informations Susceptibles de Porter Atteinte à La Sécurité de l'État"*. Διαθέσιμο στην ηλεκτρονική διεύθυνση:  
<https://www.cnews.fr/france/2018-05-25/affaire-des-2-ex-espions-de-la-dgse-des-informations-susceptibles-de-porter>. Πρόσβαση: 26/09/ 2018.
- Corporate Trust - Business Risk & Crisis Management GmbH (2014), *Studie: Industriespionage 2014. Cybergeddon der deutschen Wirtschaft durch N.S.A. & Co.?*, Corporate Trust, Munich.
- Economic Espionage Act of 1996 (1996), *Public Law 104-294 - 11 Oct. 1996, 104<sup>th</sup> Congress*, Government Publishing Office, Washington.
- Evans Joseph (1994), *U.S. Business Competitiveness and the Intelligence Community*, International Journal of Intelligence and Counterintelligence, Volume 7, Issue 3, pp.353-362, Routledge, London.
- Federal Bureau of Investigation (2017), *Economic Espionage Competing for Trade by Stealing Industrial Secrets*. Διαθέσιμο στην ηλεκτρονική διεύθυνση:  
<https://leb.fbi.gov/2017/september-october/economic-espionage-competing-fortrade-by-stealing-industrial-secrets>. Πρόσβαση: 12/10/ 2018.
- Freeh Louis (1996), *Hearing on Economic Espionage*, 1996 Congressional Hearings Intelligence and Security, Washington, DC.
- Gibson Marcus, Arnott David & Jagielska Ilona (2004), *Evaluating the Intangible Benefits of Business Intelligence: Review and Research Agenda*, pp 295-305.

- Glitz Albrecht & Meyersson Erik (2017), *Industrial Espionage and Productivity*, CESifo Working Papers, No. 6525, Munich.
- Laudon Kenneth & Laudon Jane (2014), *Management Information Systems: Managing the Digital Firm*, 13<sup>th</sup> Edition, Global Edition, Pearson Education Limited, London.
- Lowenthal Mark (2017), *Intelligence: From Secrets to Policy*, 7<sup>th</sup> Edition, CQ Press, Los Angeles.
- Luttwak Edward & Koehl Stuart (1991), *The Dictionary of Modern War*, Revised Edition, pp 307-8, Harper Collins, New York.
- Macrakis Kristie (2004), *Does Effective Espionage Lead to Success in Science and Technology? Lessons from the East German Ministry for State Security*, *Intelligence and National Security*, Volume 19, Issue 1, pp.52–77, Routledge, London.
- Macrakis Kristie (2008), *Seduced by Secrets: Inside the Stasi's Spy-Tech World*, NY: Cambridge University Press, New York.
- Margolis Gabriel (2013), *The Lack of Hum.Int.: A Recurring Intelligence Problem*, *Global Security Studies*, Spring 2013, Volume 4, Issue2, pp.43-60, GSS, New York .
- Marion Pierre (1991), *La Mission Impossible: À la Tête des Services Secrets*, Calmann-Levy, Paris.
- Marion Pierre (1999), *Mémoires de l'Ombre - Un Homme dans Les Secrets de l'État*, Flammarion, Paris.
- McGonagle John (2016), *Competitive Intelligence*, *Intelligencer: Journal of U.S. Intelligence Studies*, Volume 22, No.2, Fall 2016, pp 55-60, A.F.I.O., Falls Church.
- Michal Kristen (1994), *Business Counterintelligence and the Role of the U.S. Intelligence Community*, *International Journal of Intelligence and Counterintelligence*, Volume 7, Issue 4, pp.413-427, Routledge, London.
- Milanovic Marko (2015), *Human Rights Treaties and Foreign Surveillance: Privacy at the Digital Age*, *The Harvard International Law Journal*, Volume 56, Issue 1, Boston.
- New York Times (2001 A), *Technology; F.B.I. Says 3 Stole Secrets from Lucent*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.nytimes.com/2001/05/04/business/technology-fbi-says-3-stole-secrets-from-lucent.html>. Πρόσβαση: 04/09/2018.
- New York Times (2001 B), *Technology Three Indicted in Lucent Trade-Secret Case*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.nytimes.com/2001/06/01/business/three-indicted-in-lucent-trade-secret-case.html>. Πρόσβαση: 04/09/2018.
- New York Times (2012), *The Patent Used as a Sword*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: [https://www.nytimes.com/2012/10/08/technology/patent-wars-among-tech-giants-can-stifle-competition.html?pagewanted=all&\\_r=0](https://www.nytimes.com/2012/10/08/technology/patent-wars-among-tech-giants-can-stifle-competition.html?pagewanted=all&_r=0). Πρόσβαση: 24/11/2018.
- New York Times (2016), *Pardon Edward Snowden*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.nytimes.com/2016/09/15/opinion/pardon-edward-snowden.html>. Πρόσβαση: 09/09/2018.
- Newsit (2018), *Κατασκοπευτικό θρίλερ! Γάλλοι πρόην μυστικοί πράκτορες είχαν προσηλυτιστεί από την Κίνα!*. Διαθέσιμο στην ηλεκτρονική διεύθυνση:

- <https://www.newsit.gr/kosmos/kataskopeytiko-thriller-galloi-proin-mystikoi-praktores-eixan-prosilytistei-apo-tin-kina/2531827/>. Πρόσβαση: 26/09/2018.
- Nye Joseph (2003), *Το Παράδοξο της Αμερικανικής Δύναμης*, Εκδόσεις Παπαζήση, Αθήνα.
- Nye Joseph (2005), *Ηπια Ισχύς. Το Μέσο Επιτυχίας στην Παγκόσμια Πολιτική*, Εκδόσεις Παπαζήση, Αθήνα.
- Nye Joseph & Owens William (1996), *America's information edge*, Volume 75, No. 2, March/April 1996, Foreign Affairs, Council on Foreign Relations, New York.
- Rand (2013), *Intelligence Analysis*, Διαθέσιμο στην διεύθυνση: <https://www.rand.org/topics/intelligence-analysis.html>. Πρόσβαση 23/10/2018.
- Rubenstein Dana (2014), *Nation-State Cyber Espionage and its Impacts*, pp 1-11, Computer Science & Engineering in Washington University in Saint Louis.
- Schweizer Peter (1996), *The Growth of Economic Espionage: America Is Target Number One*, Foreign Affairs, Volume 75, No. 1, Jun-Feb 1996, pp 9-14, Council on Foreign Relations, New York.
- The Guardian (2013 A), *Edward Snowden: The Whistleblower Behind the N.S.A. Surveillance Revelations*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Πρόσβαση: 09/09/2018.
- The Guardian (2013 B), *Edward Snowden, NSA files source: "If they want to get you, in time they will"*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why> Πρόσβαση: 09/09/2018.
- The Guardian (2013 C), *On the Espionage Act charges against Edward Snowden*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.theguardian.com/commentisfree/2013/jun/22/snowden-espionage-charges>. Πρόσβαση: 09/09/2018.
- The Guardian (2016), *"Extreme surveillance" becomes UK law with barely a whimper*". Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper>. Πρόσβαση: 09/09/2018.
- United States-China Economic & Security Review Commission (2007), *Report to Congress of the U.S.C.C.*, 110<sup>th</sup> Congress. Διαθέσιμο στην ηλεκτρονική διεύθυνση: [https://www.uscc.gov/sites/default/files/annual\\_reports/2007-Report-to-Congress-Executive%20Summary.pdf](https://www.uscc.gov/sites/default/files/annual_reports/2007-Report-to-Congress-Executive%20Summary.pdf). Πρόσβαση: 12/10/ 2018.
- United States Department of Defense, *D.o.D. Dictionary of Military and Associated Terms*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: [http://www.dtic.mil/doctrine/new\\_pubs/dictionary.pdf](http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf). Πρόσβαση: 25/10/ 2018.
- Vercellis Carlo (2009), *Business Intelligence: Data Mining and Optimization for Decision Making*, Wiley, West Sussex.
- Waltz Kenneth (2010), *Theory of International Politics*, (Reissued), Waveland Press, Inc., Long Grove.

Warner William (1994), *International Technology Transfer and Economic Espionage*, International Journal of Intelligence and Counterintelligence, Volume 7, Issue 2, pp.143-160, Routledge, London.

Αποστολίδης Παύλος (2014), *Μυστική Δράση: Υπηρεσίες Πληροφοριών στην Ελλάδα*, Εκδόσεις Παπαζήση, Αθήνα.

Κωνσταντόπουλος Ιωάννης (2010), *Οικονομία και Κατασκοπεία. Θεωρία και Πράξη*, Εκδόσεις Ποιότητα, Αθήνα.

Μαυρίδης Ιωάννης (2015), *Ασφάλεια Πληροφοριών στο Διαδίκτυο*, Εκδόσεις Κάλλιπος, Αθήνα.

Οργανισμός Βιομηχανικής Ιδιοκτησίας, *Δίπλωμα Ευρεσιτεχνίας*. Διαθέσιμο στην ηλεκτρονική διεύθυνση: <https://www.obi.gr/OBI/?tabid=158>. Πρόσβαση: 27/11/2018.

## Συντομογραφίες

Aman (*Military Intelligence Directorate*) = Διεύθυνση Στρατιωτικών Πληροφοριών, Κράτος του Ισραήλ

A.S.D.-I.S.A. (*Assistant Secretary of Defense for International Security Affairs*) = Αναπληρωτής Υπουργός Άμυνας για Θέματα Διεθνούς Ασφάλειας, Ηνωμένες Πολιτείες Αμερικής

B.C.R. (*Benefit Cost Ratio*) = Σχέση Οφέλους - Κόστους

B.F.V. (*Federal Office for the Protection of the Constitution*) = Ομοσπονδιακό Γραφείο για την Προστασία του Συντάγματος, Ομοσπονδιακή Δημοκρατία της Γερμανίας

B.I. (*Business Intelligence*) = Επιχειρηματική Ευφυΐα

B.N.D. (*Federal Intelligence Service*) = Ομοσπονδιακή Υπηρεσία Πληροφοριών, Ομοσπονδιακή Δημοκρατία της Γερμανίας

C.I. (*Cyber Intelligence*) = Κυβερνοκατασκοπεία

C.Int. (*Competitive Intelligence*) = Ανταγωνιστική Ευφυΐα

C.I.A. (*Central Intelligence Agency*) = Κεντρική Υπηρεσία Πληροφοριών, Ηνωμένες Πολιτείες Αμερικής

C.T.I. (*Cyber Threat Intelligence*) = Κυβερνοάμυνα

Com.Int. (*Communications Intelligence*) = Πληροφορίες Επικοινωνιών

D.G.S.E (*General Directorate for External Security*) = Γενική Διεύθυνση Εξωτερικής Ασφάλειας, Γαλλική Δημοκρατία

D.G.S.I. (*General Directorate for Internal Security*) = Γενική Διεύθυνση Εσωτερικής Ασφάλειας, Γαλλική Δημοκρατία

D.I.A. (*Defense Intelligence Agency*) = Στρατιωτική Υπηρεσία Πληροφοριών, Ηνωμένες Πολιτείες Αμερικής

D.O.D. (*Department of Defense*) = Υπουργείο Άμυνας, Ηνωμένες Πολιτείες Αμερικής

El.Int. (*Electronic Intelligence*) = Ηλεκτρονικές Πληροφορίες

F.B.I. (*Federal Bureau of Investigation*) = Ομοσπονδιακό Γραφείο Ερευνών, Ηνωμένες Πολιτείες Αμερικής

F.S.B. (*Federal Security Service*) = Ομοσπονδιακή Υπηρεσία Ασφαλείας, Ρωσική Ομοσπονδία

G.C.HQ. (*Government Communications Headquarters*) = Κεντρικά Γραφεία Κυβερνητικών Επικοινωνιών, Ηνωμένο Βασίλειο

G.R.U. (*Main Directorate of the General Staff of the Armed Forces*) = Κεντρική Διεύθυνση του Γενικού Επιτελείου των Ενόπλων Δυνάμεων, Ρωσική Ομοσπονδία

H.V.A. (*Main Directorate for Reconnaissance*) = Κύρια Διεύθυνση Αναγνώρισης, Λαοκρατική Δημοκρατία της Γερμανίας

Hum.Int. (*Human Intelligence*) = Ανθρώπινες Πηγές Πληροφοριών

I.T. (*Information Technology*) = Τεχνολογία Πληροφοριών

K.G.B. (*Committee for State Security*) = Επιτροπή για την Κρατική Ασφάλεια, Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών



L.S.E. (*London School of Economics and Political Science*) = Σχολή Οικονομικών και Πολιτικών Επιστημών του Λονδίνου

M.F.S. (*Ministry for State Security*) = Υπουργείο Κρατικής Ασφάλειας, Λαοκρατική Δημοκρατία της Γερμανίας

M.I.5 ή S.S. (*Military Intelligence – Section 5, Security Service*) = Υπηρεσία Ασφαλείας, Ηνωμένο Βασίλειο

M.I.6 ή S.I.S. (*Military Intelligence – Section 6, Secret Intelligence Service*) = Μυστική Υπηρεσία Πληροφοριών, Ηνωμένο Βασίλειο

M.I.T. (*National Intelligence Organization*) = Εθνική Οργάνωση Πληροφοριών, Δημοκρατία της Τουρκίας

Mossad (*Institute for Intelligence and Special Operations*) = Ινστιτούτο Πληροφοριών και Ειδικών Επιχειρήσεων, Κράτος του Ισραήλ

N.I.C. (*National Intelligence Council*) = Εθνικό Συμβούλιο Πληροφοριών, Ηνωμένες Πολιτείες Αμερικής

N.S.A. (*National Security Agency*) = Εθνική Υπηρεσία Ασφαλείας, Ηνωμένες Πολιτείες Αμερικής

O.S.Int. (*Open Source Intelligence*) = Ανοιχτές Πηγές Πληροφοριών

R&D (*Research and Development*) = Έρευνα και Ανάπτυξη

Shabak ή Shin Bet (*Israel Security Agency*) = Υπηρεσία Εσωτερικής Ασφάλειας, Κράτος του Ισραήλ

Sign.Int. (*Signals Intelligence*) = Σήματα Πληροφοριών

Stasi (*State Security Service*) = Υπηρεσία Κρατικής Ασφάλειας, Λαοκρατική Δημοκρατία της Γερμανίας

S.V.R. (*Foreign Intelligence Service*) = Υπηρεσία Εξωτερικών Πληροφοριών, Ρωσική Ομοσπονδία

U.S.C.C. (*United States – China Economic and Security Review Commission*) = Επιτροπή Ελέγχου Οικονομικών και Ασφάλειας Ηνωμένων Πολιτειών – Κίνας, Ηνωμένες Πολιτείες Αμερικής

Γ.Ε.Εθ.Α. = Γενικό Επιτελείο Εθνικής Άμυνας, Ελληνική Δημοκρατία

Δ.Δ.Σ.Π. = Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών, Ελληνική Δημοκρατία

Ε.Ε. = Ευρωπαϊκή Ένωση

Ε.Σ.Σ.Δ. = Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών

Ε.Υ.Π. = Εθνική Υπηρεσία Πληροφοριών, Ελληνική Δημοκρατία

Η.Π.Α. = Ηνωμένες Πολιτείες Αμερικής

Λ.Δ.Γ. = Λαοκρατική Δημοκρατία της Γερμανίας

M.M.E. = Μέσα Μαζικής Ενημέρωσης

O.B.I. = Οργανισμός Βιομηχανικής Ιδιοκτησίας, Ελληνική Δημοκρατία

O.Δ.Γ. = Ομοσπονδιακή Δημοκρατία της Γερμανίας

O.O.Σ.Α. = Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης