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

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων»

Η εξάπλωση της οικονομικής και βιομηχανικής κατασκοπείας μετά τον ψυχρό πόλεμο και η επίδραση των απειλών κυβερνοασφάλειας

Μεταπτυχιακή Διπλωματική Εργασία Ειδίκευσης

«Ανάλυση δεδομένων στην παγκόσμια πολιτική»

Αλέξιος Τσαπικούνης

Τριμελής επιτροπή:

Αναπληρωτής Καθηγητής Ν. Σ. Κουτσούκης

Επίκουρος Καθηγητής Ι. Κωνσταντόπουλος (ε)

Επίκουρος Καθηγητής Ν. Ραχανιώτης

(ε) – Επιβλέπων

Τελική έκδοση

Κόρινθος, 2020

UNIVERSITY OF THE PELOPONNESE

SCHOOL OF SOCIAL & POLITICAL SCIENCES

DEPARTMENT OF POLITICAL SCIENCE &INTERNATIONAL RELATIONS

MASTER'S PROGRAMME IN

"GLOBAL RISKS AND ANALYTICS"

The expansion of economic and industrial espionage after the cold war and the effect of cyber security threats

Master's dissertation specializing in

"Data analysis in global politics"

Alexios Tsapikounis

Committee:

Associate Professor N. S. Koutsoukis

Assistant Professor I. Konstantopoulos (s)

Assistant Professor N. Rachaniotis

(s) – Supervisor

Final version

Corinth, 2020

Abstract

There are several types of espionage: Political, military, scientific and technological, economic, industrial, commercial, etc. Although international law defines espionage only during war, espionage is most often taking place in peacetime and is committed by nationals of a particular country as well as by foreigners. Each country has its own definition of economic espionage and industrial espionage. These two forms of espionage share a similar definition, as they are both forms of espionage that are conducted for commercial purposes rather than purely national security matters. Furthermore, one of the issues in the field of data security is the lack of reliable knowledge of the existing threats to information protection. Governments and companies are observing a deficit in finding and collecting information in this area and are facing a growing problem of industrial espionage. Economic espionage has flourished in recent years, following the end of the Cold War, mainly between the United States of America and its traditional rival power Russia, but also the new great power, China and the growing threat posed by Iran. On the other hand, industrial espionage is a reality, the methods of which, whether legal or illegal, have been growing rapidly in recent years. Internet development, however, seems to play a huge role in this.

Περίληψη

Υπάρχουν διάφοροι τύποι κατασκοπείας: Η πολιτική, η στρατιωτική, η επιστημονική και η τεχνολογική, η οικονομική, η βιομηχανική, η εμπορική κλπ. Παρόλο που το διεθνές δίκαιο ορίζει την κατασκοπεία μόνο κατά τη διάρκεια του πολέμου, η κατασκοπεία λαμβάνει χώρα πολύ συχνά σε περίοδο ειρήνης και διαπράττεται από υπηκόους μιας συγκεκριμένης χώρας καθώς και από αλλοδαπούς. Κάθε χώρα έχει τον δικό της ορισμό της οικονομικής και της βιομηχανικής κατασκοπείας. Αυτές οι δύο μορφές κατασκοπείας μοιράζονται έναν παρόμοιο ορισμό, καθώς είναι και οι δύο μορφές κατασκοπείας που διεξάγονται για εμπορικούς σκοπούς αντί για καθαρά θέματα εθνικής ασφάλειας. Εξάλλου, ένα από τα θέματα αντιπαράθεσης στον τομέα της ασφάλειας των δεδομένων είναι η έλλειψη αξιόπιστων γνώσεων σχετικά με τις υφιστάμενες απειλές κατά της προστασίας των πληροφοριών. Οι κυβερνήσεις και οι εταιρείες παρατηρούν ένα έλλειμμα διαπίστωσης και συλλογής πληροφοριών σε αυτόν τον τομέα και αντιμετωπίζουν ένα αυξανόμενο πρόβλημα βιομηχανικής κατασκοπείας. Η οικονομική κατασκοπεία έχει γνωρίσει άνθιση μετά τη λήξη του Ψυχρού Πολέμου, κυρίως μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και αφενός της παραδοσιακής ανταγωνίστριας δύναμης, της Ρωσίας, αλλά και της νέας μεγάλης δύναμης, της Κίνας καθώς και της ολοένα αυξανόμενης απειλής που αποτελεί το Ιράν. Από την άλλη πλευρά, η βιομηχανική κατασκοπεία αποτελεί μια πραγματικότητα, οι μέθοδοι της οποίας, είτε νόμιμες είτε παράνομες, αναπτύσσονται ραγδαία τα τελευταία χρόνια. Σε αυτό ωστόσο φαίνεται να παίζει τεράστιο ρόλο η ανάπτυξη του διαδικτύου.

Περιεχόμενα

1. Εισαγωγή

Ενώ η κατασκοπεία δεν είναι ένα νέο γεγονός, έχει λάβει εξαιρετικά μικρή ερευνητική προσοχή στην Ευρώπη. Τα εγκλήματα κατά της κατασκοπείας είναι μικτού χαρακτήρα και περιλαμβάνουν δύο χωριστά φαινόμενα. Από την μία είναι η «κλασική» ή οικονομική κατασκοπεία από υπηρεσίες πληροφοριών ενός ξένου κράτους και από την άλλη πλευρά, υπάρχουν τα περιστατικά ανταγωνιστικής εταιρικής ή βιομηχανικής κατασκοπείας, εμπορικής κατασκοπείας ή βιομηχανικής κλοπής. Και τα δύο φαινόμενα χαρακτηρίζονται από ουσιαστικά όμοια modi operandi, που είναι ο σκοπός της παράνομης απόκτησης τεχνογνωσίας και άλλων πληροφοριών καθώς και οι κατά το μάλλον ή ήττον πανομοιότυποι στόχοι ή θύματα, με τη μορφή ιδιοκτητών τεχνογνωσίας και πνευματικής ιδιοκτησίας, όπως οι επιχειρήσεις και τα εμπορικά μυστικά. Τα τελευταία μπορεί να προέρχονται είτε από την οικονομία είτε από την επιστήμη. Στην ουσία η διαφορά ανάμεσα στην οικονομική και την βιομηχανική κατασκοπεία είναι μόνο το διαφορετικό κίνητρο, δηλαδή στην επίτευξη είτε ενός πολιτικού είτε ενός οικονομικού πλεονεκτήματος, ενώ υπάρχουν περιπτώσεις που αυτές οι δύο ταυτίζονται, με την συνεργασία του κράτους και της υφιστάμενης εταιρίας ή βιομηχανίας. Και οι δύο μορφές κατασκοπείας εντοπίζονται στη διασταύρωση του συμβατικού (φυσικού) εγκλήματος και του κυβερνο-εγκλήματος.

Η βασική κατανόηση αυτών των εγκλημάτων, το νομικό τους πλαίσιο καθώς και ο οργανωτικός σχεδιασμός των διοικητικών αρμοδιοτήτων και δικαιοδοσιών διαμορφώνεται σε μεγαλύτερο βαθμό από την περίοδο του Ψυχρού Πολέμου και έπειτα. Οι νομικοί εκσυγχρονισμοί δεν τήρησαν τους μεταβαλλόμενους πολιτικούς όρους. Οι πρώην πολιτικές πρώτες γραμμές διαλύθηκαν και σε ορισμένες περιπτώσεις αντικαταστάθηκαν από την οικονομική συνεργασία. Ταυτόχρονα, αναπτύχθηκαν νέοι τύποι φίλων-εχθρών κατά μήκος των διαχωριστικών γραμμών των σύγχρονων πολιτικών συμφερόντων. Ενώ οι επιθέσεις κατά της οικονομικής τεχνογνωσίας που προέρχονται από ορισμένες περιοχές εξακολουθούν να διώκονται ως κρατικά εγκλήματα, οι παραβάτες που προέρχονται από φιλικά έθνη ονομάζονται «φιλικοί κατάσκοποι» και διώκονται με δισταγμό μόνο, ή και καθόλου.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η αναλυτική ενασχόληση με το θέμα της οικονομικής και βιομηχανικής κατασκοπείας, με την ραγδαία εξάπλωση αυτών μετά το τέλος του Ψυχρού Πολέμου και η απάντηση στο ερώτημα κατά πόσο κρίνεται αναγκαία η εφαρμογή τους από κράτη και εταιρίες για την επίτευξη των στόχων τους. Για τον σκοπό αυτό, λαμβάνει χώρα μια αναλυτική βιβλιογραφική επισκόπηση, η οποία αποτελείται από τα

κεφάλαια που ακολουθούν. Το πρώτο από αυτά είναι στοχευμένο στην οικονομική κατασκοπεία, ενώ το επόμενο είναι αφιερωμένο στην βιομηχανική κατασκοπεία. Στο επόμενο κεφάλαιο γίνεται αναφορά στην δυσκολία που υπάρχει σχετικά με τον υπολογισμό του κόστους από μια επίθεση οικονομικής κατασκοπείας, με την παράθεση παραδειγμάτων, καθώς και σε περιπτωσιολογικές μελέτες. Στο τελευταίο κεφάλαιο γίνεται ανάλυση της επίδρασης των απειλών κυβερνοασφάλειας με την χρήση των μεθόδων ανάλυσης συσχέτισης και παλινδρόμησης, με στατιστικά δεδομένα από τις σύγχρονες μεθόδους βιομηχανικής κατασκοπείας, όπως θα αναλύσουμε παρακάτω. Η εργασία κλείνει με την εξαγωγή των σημαντικότερων συμπερασμάτων και την παράθεση καταλόγου πηγών.

2. Η οικονομική κατασκοπεία

2.1 Εισαγωγικά στοιχεία

Για δεκαετίες μετά τον Δεύτερο Παγκόσμιο Πόλεμο, η γεωστρατηγική αντιπαράθεση μεταξύ των αμερικανικών και των σοβιετικών συνασπισμών καθόρισε τη διπολική οργάνωση της παγκόσμιας τάξης. Αυτή η ιδεολογική αντιπαράθεση Ανατολής-Δύσης απέκρυψε τις οικονομικές συγκρούσεις μεταξύ των εθνικών κρατών. Στη συνέχεια, στις αρχές της δεκαετίας του 1990, η ξαφνική κατάρρευση του κομμουνιστικού μπλοκ έπληξε βίαια την καθιερωμένη σειρά διεθνών σχέσεων. Τα στρατιωτικά ζητήματα Ανατολής-Δύσης έγιναν γρήγορα παρωχημένα και έδωσαν τη θέση τους σε μια καθαρή καπιταλιστική λογική (Calder & Watkins, 2006).

Πράγματι, ο οικονομικός πόλεμος ακολούθησε τον ψυχρό πόλεμο. Ο στόχος των εθνών, σήμερα, δεν είναι πλέον η κατάκτηση των εδαφών ή των αποικιών, αλλά η κατάκτηση των αγορών και των τεχνολογιών σε μια παγκοσμιοποιημένη οικονομία. Κάθε έθνος πρέπει να ενθαρρύνει τις εταιρείες του, θέτοντάς τους σε θέση να καινοτομούν, να εξάγουν όλο και περισσότερο, να εγκατασταθούν στο εξωτερικό κλπ. Ωστόσο, ενώ τα ιστορικά έθνη θέτουν τέλος στις διαφορές τους υπογράφοντας συνθήκες, αυτό δεν συμβαίνει για τις επιχειρήσεις που καταδικάζονται, σύμφωνα με τους νόμους της οικονομίας της αγοράς, σε κατάσταση διαρκούς και συνεχούς ανταγωνισμού (Calder & Watkins, 2006).

2.2 Αποσαφήνιση της έννοιας της κατασκοπείας

Στην κατασκοπεία, που θεωρείται ένα από τα αρχαιότερα επαγγέλματα στον κόσμο, έχουν γίνει προσπάθειες να αποδοθούν διάφοροι ορισμοί. Εμείς θα αποτυπώσουμε σε αυτό το σημείο τους επικρατέστερους. Σύμφωνα με τον Bob Burton, κατασκοπεία είναι η δραστηριότητα αναζήτησης πληροφοριών εκ μέρους μιας κυβέρνησης, τις οποίες μια άλλη κυβέρνηση επιθυμεί να κρατήσει μυστικές. Ενώ σύμφωνα με τον Arthur S. Hulnick, κατασκοπεία είναι η συλλογή πληροφοριών μέσω μυστικής παρακολούθησης ή μέσω της χρήσης κατασκόπων, οι οποίοι υποκλέπτουν τις απαραίτητες πληροφορίες.

Υπάρχουν διάφοροι τύποι κατασκοπείας: Η πολιτική, η στρατιωτική, η επιστημονική και η τεχνολογική, η οικονομική, η βιομηχανική, η εμπορική κλπ. Οι ορισμοί αυτών των μορφών κατασκοπείας δυστυχώς δεν αποτελούν το αντικείμενο κάποιας διεπιστημονικής συναίνεσης.

Κάθε χώρα έχει τους δικούς της ορισμούς. Η φύση του πελάτη (κυβέρνηση / εταιρεία / άτομο) ή και οι πληροφορίες που ζητούνται είναι οι βασικές αιτίες για τις οποίες είναι υπαρκτές αυτές οι διαφορές (Bitton, 2014).

Η κατασκοπεία κατά τη διάρκεια του πολέμου είναι ένας ορισμός στον οποίο συμφωνούν οι περισσότερες χώρες. Σύμφωνα με το άρθρο 29 της σύμβασης της Χάγης του 1907 που ασχολείται με τους νόμους και τα έθιμα της πολεμικής δράσης, ένα πρόσωπο μπορεί να θεωρηθεί ως κατάσκοπος, όταν ενεργώντας κρυφά ή με ψευδή χαρακτηριστικά, αποκτά ή προσπαθεί να λάβει πληροφορίες που αναφέρονται στη ζώνη των επιχειρήσεων ενός στρατού, με σκοπό την επικοινωνία του με το εχθρικό στράτευμα. Στην πραγματικότητα, η κατασκοπεία είναι όρος που αποτελεί μέρος του νόμου περί ένοπλων συγκρούσεων. Κατά τον ίδιο τρόπο, ένας κατάσκοπος ορίζεται επίσης ως ένα άτομο που συνεργάζεται με τους εχθρούς για να τους κατασκοπεύει. Οι πληροφορίες που συλλέγονται πρέπει να είναι εμπιστευτικές και να έχουν στρατιωτικό ενδιαφέρον. Συνήθως, οι εθνικοί νόμοι κάθε χώρας καθορίζουν τον ορισμό των ενοχοποιητικών κατασκοπικών πράξεων, καθώς και τις πληροφορίες που προστατεύονται (Bitton, 2014).

Για παράδειγμα, στις Ηνωμένες Πολιτείες, ο νόμος περί κατασκοπείας του 1917, που δημιουργήθηκε δύο μήνες μετά την κήρυξη πολέμου από το Κογκρέσο, κατέστησε παράνομη τη συλλογή πληροφοριών σχετικά με τις αμυντικές εγκαταστάσεις με πρόθεση ή λόγο να πιστεύουν ότι οι πληροφορίες που θα ληφθούν θα χρησιμοποιηθούν για τον τραυματισμό των Ηνωμένων Πολιτειών ή προς όφελος οποιουδήποτε ξένου έθνους (18 κώδικας των ΗΠΑ § 793). Στην εφαρμογή του ο εν λόγω νόμος ξεπέρασε αυτό το γεγονός και κατέστησε παράνομη τη μεταφορά εγγράφων, φωτογραφιών και πληροφοριών με άλλες μορφές που σχετίζονται με την εθνική άμυνα σε οποιαδήποτε ξένη κυβέρνηση ή κάποιον ξένο πολίτη ή κάποιες αρχές μιας ξένης κυβέρνησης, αν υπήρχε πρόθεση ή λόγος να γίνει πιστευτό ότι πρόκειται να χρησιμοποιηθεί για τον τραυματισμό των Ηνωμένων Πολιτειών ή προς όφελος ενός ξένου έθνους. Αυτή η διάταξη οδηγούσε σε τιμωρία τα άτομα που ενέπιπταν σε αυτήν κατά τη διάρκεια του πολέμου με θάνατο ή φυλάκιση μέχρι και 30 χρόνια (Bitton, 2014).

Η κατασκοπεία δεν είναι από μόνη της απαγορευμένη από το δίκαιο του πολέμου, αλλά τιμωρείται σύμφωνα με το εθνικό ποινικό δίκαιο κάθε χώρας. Ωστόσο, όταν συλλαμβάνονται οι κατάσκοποι αντιμετωπίζονται σαν προδότες και συχνά δέχονται σκληρές τιμωρίες. Οι κατάσκοποι σε μια ένοπλη σύγκρουση δεν είναι μαχητές και δεν απολαμβάνουν τα δικαιώματα των στρατιωτών ή ακόμα και των saboteurs ή των μισθοφόρων. Δεδομένου ότι η κατασκοπεία ήταν πάντα πρωταρχικά συνδεδεμένη με τον πόλεμο, οι χώρες προσπάθησαν να οργανώσουν τις συνθήκες για το καθεστώς των συλληφθέντων κατασκόπων, προκειμένου να τους παράσχουν καλύτερη προστασία. Η προσωπική ευθύνη του κατασκόπου μπορεί να προσληφθεί εάν έχει συλληφθεί με αποδεικτικά στοιχεία και δικαιούται δίκη. Όπως ήδη αναφέρθηκε, η παράγραφος 29 της Σύμβασης της Χάγης παρέχει σαφή ορισμό της κατασκοπείας, ο οποίος αποτελείται από δύο βασικά στοιχεία, τις συγκεκαλυμμένες πράξεις

αυτές καθαυτές και το γεγονός ότι λαμβάνουν χώρα σε μια ζώνη πολεμικών επιχειρήσεων (Bitton, 2014).

Λόγω της ευρείας χρήσης της, θα περίμενε κανείς ότι η κατασκοπεία είναι τοποθετημένη κατά μία έννοια σε στέρεες ηθικές και νομικές βάσεις, αλλά στην πραγματικότητα, αυτή η δαπανηρή και επιβλαβής δραστηριότητα στερείται σαφούς νομικής και ηθικής δικαιολογίας. Στην πραγματικότητα, νομικοί και φιλόσοφοι λόγιοι μπορούν να δικαιολογήσουν τη νομιμότητα του πολέμου μεταξύ των εθνών και ακόμη και την εγχώρια χρήση της κυβερνητικής δύναμης, όμως όταν πρόκειται για κατασκοπεία, οι ηθικοί θεωρητικοί είναι τόσο ακανόνιστοι όσο οι κατάσκοποι. Η πραγματικότητα αυτή μπορεί να οφείλεται στο γεγονός ότι οι κατάσκοποι κατά κανόνα λειτουργούν σε ένα αφιλόξενο πεδίο επειδή διώκονται και χρεώνονται συχνά καταδικαστικές αποφάσεις (Bitton, 2014).

2.3 Η ανάλυση της οικονομικής κατασκοπείας

Στην διεθνή βιβλιογραφία περί πληροφοριών και μυστικών υπηρεσιών παρατηρείται μία σύγχυση σχετικά με τον ορισμό της οικονομικής κατασκοπείας. Ομοίως με τον ορισμό της κατασκοπείας θα αποτυπώσουμε τους δύο επικρατέστερους. Σύμφωνα με τον Porteous, οικονομική κατασκοπεία είναι η χρησιμοποίηση από μια κυβέρνηση ή εκπροσώπους της παράνομων, μυστικών, εξαναγκαστικών ή παραπλανητικών μέσων ή η διευκόλυνση τους, προκειμένου να αποκτήσουν πληροφορίες οικονομικού περιεχομένου. Σύμφωνα με τον Burton, οικονομική κατασκοπεία είναι οι πληροφορίες που σχετίζονται με την έκταση και τη χρησιμοποίηση των φυσικών και ανθρώπινων πόρων και με τη βιομηχανική δυνατότητα των κρατών (Κωνσταντόπουλος, 2010).

Η οικονομική κατασκοπεία χωρίζεται σε δύο επιμέρους κατηγορίες, την μακροοικονομική και την μικροοικονομική κατασκοπεία. Στην πιο βασική μορφή της η μακροοικονομική κατασκοπεία έχει ως στόχο την υποβοήθηση της πολιτικής ηγεσίας ενός κράτους, ώστε να διαχειριστεί με τον καλύτερο δυνατό τρόπο την εσωτερική και εξωτερική οικονομική πολιτική. Βασικό σημείο αυτού του στόχου είναι η απόκτηση οικονομικών πληροφοριών που δεν είναι διαθέσιμες από ελεύθερες πηγές, σχετικά με τη λήψη ζωτικών οικονομικών αποφάσεων, όπως η υποτίμηση του νομίσματος ενός κράτους, είτε οι προσπάθειες τρίτων κρατών να επηρεάσουν με μυστικές μεθόδους τα οικονομικά συμφέροντα ενός άλλου κράτους (Porteous, 1998). Η μικροοικονομική κατασκοπεία από την άλλη αφορά τη συλλογή και ανάλυση οικονομικών πληροφοριών με στόχο την υποστήριξη συγκεκριμένων επιχειρήσεων έναντι των ξένων ανταγωνιστών τους. Όπως έχει υποστηρίξει και ο πρώην Αμερικανός, Γενικός Διευθυντής της Κεντρικής Υπηρεσίας Πληροφοριών (DCI) James Woolsey: «Η κατασκοπεία εναντίον ξένων επιχειρήσεων προς όφελος των εγχώριων επιχειρήσεων» (Evans J.C., 1995).

Τα περισσότερα κράτη αναθέτουν στις υπηρεσίες πληροφοριών τους τη συλλογή και ανάλυση μακροοικονομικών πληροφοριών βάσει συγκεκριμένων κριτηρίων. Με βάση αυτά τα κριτήρια, οι ηγεσίες των κρατών αποφασίζουν την εμπλοκή ή μη των μυστικών τους υπηρεσιών σε αυτή τη δραστηριότητα.

Σε αυτό το σημείο χρήζουν ιδιαίτερης μνείας τα διλήμματα που αντιμετωπίζει η ηγεσία ενός κράτους σχετικά με την άσκηση ή μη της μακροοικονομικής κατασκοπείας καθώς η πολιτική ηγεσία μιας χώρας που αναθέτει στις μυστικές της υπηρεσίες τη διεξαγωγή μακροοικονομικής κατασκοπείας έχει συνήθως συγκεκριμένα ορθολογικά κίνητρα για να πράξει τούτο. Τα κίνητρα αυτά θα τα χωρίσουμε σε τρεις κατηγορίες.

Η πρώτη κατηγορία αναφέρεται στην αποτελεσματικότερη παρακολούθηση των διεθνών, οικονομικών και τεχνολογικών εξελίξεων. Σύμφωνα με τον Randall M. Fort, υπάρχει ένας ιστορικός και νομιμοποιημένος ρόλος για τις υπηρεσίες πληροφοριών ενός ανεπτυγμένου κράτους, η υποστήριξη της κυβερνητικής πολιτικής όσον αφορά τα οικονομικά ζητήματα. Το κρίσιμο στοιχείο εδώ είναι το γεγονός ότι, η κοινότητα των υπηρεσιών πληροφοριών παρέχει την κατάλληλη υποστήριξη στους κυβερνητικούς αξιωματούχους στα πλαίσια της διαμόρφωσης της οικονομικής πολιτικής. Αυτό, το επιτυγχάνει παρακολουθώντας τις παγκόσμιες τάσεις στον τομέα της τεχνολογίας, που μπορεί να επηρεάσουν την εθνική ασφάλεια του κράτους ενώ παράλληλα ασχολείται με την ανάλυση των διμερών ή πολυμερών διαπραγματεύσεων, την αναγνώριση των οικονομικών τάσεων και την κατανόηση των προθέσεων των οικονομικών ανταγωνιστών, την ενοποίηση ενός μεγάλου όγκου διάσπαρτων δεδομένων, προκειμένου να παρουσιαστεί μία ολοκληρωμένη εικόνα των οικονομικών και πολιτικών παραγόντων που επηρεάζουν τη διεθνή σταθερότητα, βοηθώντας κατά αυτόν τον τρόπο τους διαμορφωτές της πολιτικής να κατανοήσουν τους κανόνες του οικονομικού παιχνιδιού (Κωνσταντόπουλος, 2010).

Η δεύτερη κατηγορία αναφέρεται στο θετικό αποτέλεσμα της μακροοικονομικής κατασκοπείας στη ζυγαριά οφελών-κόστους. Εδώ, λίγες κατάλληλα οργανωμένες επιχειρήσεις αποδίδουν σημαντικά κέρδη σε κράτη που αντιμετωπίζουν οικονομικά προβλήματα, ενώ το κόστος τους είναι ελάχιστο (Porteous, 1994).

Αναμφισβήτητα πάντοτε είναι φθηνότερη για ένα κράτος η κλοπή οικονομικών, επιστημονικών και τεχνολογικών πληροφοριών σε σύγκριση με την επένδυση και την ανάληψη των εξόδων για έρευνα και ανάπτυξη. Κλασική περίπτωση αποκόμισης σημαντικού οφέλους με ελάχιστο κόστος αποτελεί η αποκάλυψη της επιχείρησης των γαλλικών μυστικών υπηρεσιών το 1971 σχετικά με την εκμετάλλευση της έγκυρης πληροφορίας περί υποτίμησης του δολαρίου. Αυτό αποτέλεσε πολύ σημαντικό κίνητρο για τις χώρες του πρώην ανατολικού συνασπισμού, που προσπαθούσαν να ξαναχτίσουν την οικονομία τους και να προσαρμοστούν στους κανόνες του παγκόσμιου καπιταλιστικού συστήματος, καθώς και για τις αναπτυσσόμενες χώρες που προσπαθούσαν να προλάβουν το τρένο της ανάπτυξης. Παρ' όλα αυτά, η κοινότητα των μυστικών υπηρεσιών των ΗΠΑ απέτυχε να προβλέψει την

κατάρρευση του μεξικανικού νομίσματος και την οικονομική κρίση που ακολούθησε. Κατά τη διάρκεια αυτής της κρίσης ο Αμερικανός Πρόεδρος δεν είχε στη διάθεσή του τις απαραίτητες πληροφορίες, ώστε να λάβει τις βέλτιστες για το συμφέρον της χώρας του αποφάσεις, διότι η πληροφόρηση δεν μοιραζόταν επαρκώς μέσα στην κυβέρνηση, όπως ακριβώς είχε συμβεί και στο Pearl Harbor το 1941. Πιο συγκεκριμένα, κανείς εντός ή εκτός των μυστικών υπηρεσιών δεν είχε συμβιβαστεί με τη νέα εποχή των μαζικών οικονομικών συναλλαγών που διαπερνούσαν τα εθνικά σύνορα, γεγονός που οδήγησε αλυσιδωτά στο ως άνω αναφερθέν αποτέλεσμα (Κωνσταντόπουλος, 2010).

Τέλος, η τρίτη κατηγορία αφορά το συγκριτικό πλεονέκτημα που διαθέτουν οι υπηρεσίες πληροφοριών σε σχέση με άλλες κυβερνητικές υπηρεσίες. Αναλύοντας οικονομικές πληροφορίες, οι μυστικές υπηρεσίες διαδραματίζουν έναν μοναδικό ρόλο, τον οποίο δεν μπορούν να αναλάβουν τα Υπουργεία Οικονομικών και Εμπορίου, καθόσον οι υπηρεσίες αυτές έχουν πρόσβαση σε ειδικές μυστικές πηγές και μεθόδους που δεν διατίθενται στις υπόλοιπες κυβερνητικές και μη κυβερνητικές υπηρεσίες (Κωνσταντόπουλος, 2010).

Στη συνέχεια, είναι άξια μνείας και η ανάλυση των αντικινήτρων, ήτοι των λόγων εκείνων που αποθαρρύνουν τα κράτη από την εμπλοκή τους σε επιχειρήσεις μακροοικονομικής κατασκοπείας. Σε αντιστοιχία με τα κίνητρα, θα ομαδοποιήσουμε και τα αντικίνητρα σε δύο κατηγορίες.

Η πρώτη κατηγορία εστιάζει στο γεγονός πως η μακροοικονομική κατασκοπεία δημιουργεί προβλήματα στην άσκηση αποτελεσματικής διμερούς και πολυμερούς διπλωματίας από το κράτος-δρώντα. Πιο συγκεκριμένα, αποξενώνει συμμάχους είτε ακόμη δημιουργεί προβλήματα στους σχηματιζόμενους εμπορικούς συνασπισμούς. Στο διπλωματικά δύσκολο πεδίο της οικονομικής κατασκοπείας δεν εφαρμόζονται πάντοτε βολικοί διαχωρισμοί μεταξύ εχθρών-αντιπάλων και φίλων-συμμάχων. Και τούτο διότι στο πεδίο αυτό οι πιθανοί αντίπαλοι μιας χώρας μπορεί να είναι οι πολιτικοί και στρατιωτικοί σύμμαχοί της. Λόγω της απουσίας της πειθαρχίας που επέβαλε ο ψυχρός πόλεμος, τα κράτη, όπως και οι σύγχρονες επιχειρήσεις, είναι ελεύθερα να ανταγωνιστούν και να συνεργαστούν ταυτόχρονα. Σε έναν κόσμο στον οποίο τα οικονομικά δεν αποτελούν δευτερεύοντα θέματα και οι αθέμιτες εμπορικές πρακτικές θεωρούνται από κάποιους το οικονομικό αντίστοιχο μίας πράξης πολέμου, οι πολύτιμες οικονομικές και εμπορικές πληροφορίες μοιράζονται λιγότερο ελεύθερα μεταξύ στρατιωτικών και πολιτικών συμμαχιών (Porteous, 1993).

Η δεύτερη κατηγορία σχετίζεται με την κοινότητα των υπηρεσιών πληροφοριών. Έχει υποστηριχθεί από ορισμένους αναλυτές και πολιτικούς ότι οι υπηρεσίες πληροφοριών δεν δημιουργήθηκαν για να μελετούν τη διεθνή οικονομία, αλλά για να διασφαλίζουν την ασφάλεια των κρατών. Σύμφωνα με την άποψη αυτή, η πολιτική και στρατιωτική ασφάλεια των κρατών προέχει έναντι της οικονομικής τους ασφάλειας.

Για όλους τους παραπάνω λόγους, γίνεται αντιληπτό ότι η μακροοικονομική κατασκοπεία αποτελεί μία παραδοσιακή συμπεριφορά των κρατών, τα οποία δεν διστάζουν να τη

χρησιμοποιούν όχι μόνο εναντίον αντιπάλων αλλά και εναντίον συμμάχων. Σε έναν κόσμο που χαρακτηρίζεται από ραγδαία οικονομική και τεχνολογική πρόοδο είναι ζωτικής σημασίας, τόσο για τη στρατιωτική όσο και για την οικονομική του ασφάλεια, ένα κράτος να ασκεί μακροοικονομική κατασκοπεία, προκειμένου να μην υστερεί οικονομικά και τεχνολογικά, διότι κάτι τέτοιο επηρεάζει αρνητικά τη σχετική του ισχύ σε σχέση με τα υπόλοιπα κράτη-συμμάχους και ανταγωνιστές-αντιπάλους (Κωνσταντόπουλος, 2010).

Είναι πολλές οι περιπτώσεις χωρών που θεωρούν τη μικροοικονομική κατασκοπεία μία δίκαιη τακτική και μέρος του οικονομικού παιχνιδιού. Οι διαφορετικές κουλτούρες της ηπειρωτικής Ευρώπης και της Ασίας αντιλαμβάνονται τη σχέση μεταξύ του κράτους και των επιχειρήσεων διαφορετικά απ' ότι οι ΗΠΑ. Πολλές κυβερνήσεις διευκολύνουν τη συνεργασία μεταξύ των υπηρεσιών πληροφοριών και των εγχώριων επιχειρήσεων με στόχο τη βελτίωση της ανταγωνιστικότητας της βιομηχανίας τους.

Σε αυτό το σημείο θα κατηγοριοποιήσουμε τα κίνητρα που δυνητικά ωθούν ένα κράτος στην άσκηση μικροοικονομικής κατασκοπείας. Και σε αυτή την περίπτωση συναντάμε δύο κατηγορίες. Η πρώτη κατηγορία εστιάζει στα οικονομικά κίνητρα άσκησης μικροοικονομικής κατασκοπείας. Μία πιθανή εξήγηση για την παρέμβαση της κυβέρνησης στην οικονομία μιας χώρας αποτελεί με βάση τα οικονομικά κίνητρα η στρατηγική εμπορικής πολιτικής (Strategic Trade Policy - STP). Ο Robert Gilpin ορίζει την στρατηγική εμπορικής πολιτικής ως μία προσπάθεια του κράτους να αλλάξει το διεθνές στρατηγικό περιβάλλον, έτσι ώστε να δίνει ορισμένα πλεονεκτήματα στις ολιγοπωλιακές εταιρείες της χώρας (Gilpin, 1995).

Σύμφωνα με την STP, οι υπάρχουσες μορφές του διεθνούς εμπορίου αντανακλούν τόσο τα προσωρινά όσο και τα μόνιμα πλεονεκτήματα των εξαγωγικών χωρών. Στα προσωρινά πλεονεκτήματα περιλαμβάνονται εκείνα που απορρέουν από τον ατελή ανταγωνισμό, τις οικονομίες κλίμακας, τη συσσωρευμένη εμπειρία ή τις τεχνολογικές εξελίξεις. Δεδομένου ότι πολλά από αυτά τα πλεονεκτήματα βασίζονται στη γνώση, συχνά διαχέονται μεταξύ των κρατών. Σε έναν κόσμο όπου η εξειδίκευση μίας χώρας εξαρτάται από την τεχνολογική πρόοδο και όπου ορισμένες βιομηχανίες μπορούν να αποκομίσουν υπερκέρδη και να δημιουργήσουν θετικές επιδράσεις, οι υπέρμαχοι της STP πιστεύουν ότι οι κυβερνήσεις μπορούν και πρέπει να δράσουν, ώστε να εκμεταλλευτούν το στρατηγικό περιβάλλον που δημιουργείται. Για να επιτευχθεί ωστόσο αυτό, πρέπει να ανατρέξουμε στη μέθοδο της παροχής κυβερνητικής βοήθειας, μέσω των κατάλληλων επιχορηγήσεων σε εγχώριες επιχειρήσεις που θεωρούνται στρατηγικής σημασίας. Η παροχή κυβερνητικής βοήθειας στόχο έχει τη μείωση του κόστους παραγωγής των επιχειρήσεων έτσι ώστε να προκύψουν υψηλότερα κέρδη, τα οποία σε τελική ανάλυση ευνοούν όλη τη χώρα. Σύμφωνα με τους οπαδούς της άποψης αυτής, μία πολυεθνική επιχείρηση που δημιουργεί θέσεις εργασίας και προσθέτει αξία στην εγχώρια οικονομία αξίζει να απολαμβάνει την κρατική προστασία, ανεξάρτητα από το γεγονός ότι δεν έχει εθνική ταυτότητα (Κωνσταντόπουλος, 2010).

Στη δεύτερη κατηγορία συναντάμε τα οφέλη που θα παρουσιάζουν οι υπηρεσίες πληροφοριών συγκριτικά με άλλες κυβερνητικές υπηρεσίες. Εδώ, το βασικό πλεονέκτημα των υπηρεσιών αυτών εδράζεται στη δομή τους. Πρόκειται για υπηρεσίες που όταν συλλέγουν και αναλύουν οικονομικές πληροφορίες, διαδραματίζουν έναν ρόλο που δεν μπορεί να αναληφθεί ούτε από το Υπουργείο οικονομικών ούτε από το Υπουργείο εμπορίου. Πιο συγκεκριμένα, η ειδοποιός διαφορά τους συνίσταται στο ότι οι διαθέτουν μοναδική πρόσβαση σε ειδικές μυστικές πηγές και μεθόδους (π.χ. ικανότητες υποκλοπής σημάτων), που δεν είναι διαθέσιμες σε άλλες κυβερνητικές και μη κυβερνητικές υπηρεσίες (Κωνσταντόπουλος, 2010).

Από την άλλη πλευρά, όπως και στην περίπτωση της μακροοικονομικής κατασκοπείας, έτσι και στη μικροοικονομική, υπάρχουν αντικίνητρα, δηλαδή λόγοι που αναχαιτίζουν ένα κράτος από την άσκηση μικροοικονομικής κατασκοπείας. Ομοίως και εδώ συναντάμε δύο βασικές κατηγορίες, η πρώτη εκ των οποίων, σύμφωνα με τους επικριτές της οικονομικής κατασκοπείας, βασίζεται στο γεγονός πως ένα πρόγραμμα μικροοικονομικής κατασκοπείας συχνά προκαλεί προβλήματα στην άσκηση αποτελεσματικής διπλωματίας. Βασικό επιχείρημα αυτής της άποψης είναι ότι η μικροοικονομική κατασκοπεία μπορεί να προκαλέσει σοβαρές και επιζήμιες επιπτώσεις στην εξωτερική πολιτική του κράτους. Παίρνοντας ως παράδειγμα τις ΗΠΑ, παρά το γεγονός ότι παραμένουν μέχρι στιγμής η μοναδική υπερδύναμη στο διεθνές σύστημα, η επιρροή τους εξαρτάται ολοένα και περισσότερο από την ικανότητά τους να δημιουργούν και να διατηρούν συνασπισμούς διαφορετικών κρατών, προκειμένου να υποστηρίξουν μία συγκεκριμένη πολιτική ή να επιτύχουν τους επιθυμητούς σκοπούς τους. Στο κέντρο των περισσότερων συνασπισμών βρίσκονται οι χώρες που αποτελούν την παραδοσιακή δυτική συμμαχία των ΗΠΑ, οι οποίες είναι ταυτόχρονα και οικονομικοί ανταγωνιστές τους. Εάν οι χώρες αυτές και οι επιχειρήσεις τους αποτελέσουν στόχο οικονομικής κατασκοπείας για τις αμερικανικές μυστικές υπηρεσίες προς όφελος των αμερικανικών επιχειρήσεων, θα υπονομευτεί η εμπιστοσύνη μεταξύ των χωρών αυτών και των ΗΠΑ, η οποία αποτελεί την ιστορική βάση για την ύπαρξη της υπάρχουσας πολιτικής συμμαχίας και θα εμποδιστούν οι διπλωματικές προσπάθειες δημιουργίας των αναγκαίων συνασπισμών για την επίτευξη των σκοπών της αμερικανικής εξωτερικής πολιτικής (Κωνσταντόπουλος, 2010).

Βασικός πυλώνας της δεύτερης κατηγορίας είναι τα προβλήματα που δημιουργεί η άσκηση μικροοικονομικής κατασκοπείας στην οικονομία ενός κράτους. Σύμφωνα με την παραδοσιακή οικονομική ανάλυση των ΗΠΑ, οι αναλυτές και οι πολιτικοί που αντιμάχονται την άσκηση μικροοικονομικής κατασκοπείας εξισώνουν τις πληροφορίες που αποκτώνται με αυτή τη μέθοδο με τις επιχορηγήσεις. Ουσιαστικά, οι κυβερνήσεις που συμμετέχουν στην άσκηση μικροοικονομικής κατασκοπείας μπορεί να κατηγορηθούν ότι δημιουργούν προσκόμματα στην αγορά και δυσλειτουργίες, είτε ότι επιβραβεύουν την αντιγραφή έναντι της καινοτομίας, ότι ευνοούν αναποτελεσματικούς παραγωγούς έναντι των καταναλωτών και τέλος ότι αντιλαμβάνονται εσφαλμένα τον οικονομικό ανταγωνισμό ως μία απειλή για την

εθνική ασφάλεια και όχι ως ένα απαραίτητο και καλοδεχούμενο στοιχείο της οικονομικής ανάπτυξης. Οι επικριτές της μικροοικονομικής κατασκοπείας υποστηρίζουν πως αυτή η νέα μορφή κυβερνητικής βοήθειας θα είναι καλοδεχούμενη από επιχειρήσεις υπό κατάρρευση και μη ανταγωνιστικές εταιρείες. Κατά την άποψή τους, ακριβώς αυτές οι επιχειρήσεις που αποδέχονται τις κυβερνητικές επιχορηγήσεις και άλλες μορφές προστατευτισμού, όχι μόνο θα καλωσορίσουν τις μικροοικονομικές πληροφορίες που τους παρέχει απλόχερα η κυβέρνηση και οι υπηρεσίες πληροφοριών, αλλά θα δημιουργήσουν και ομάδες πίεσης, ώστε να τις αποκτήσουν. Αυτό το περιβάλλον, είναι πιθανό να οδηγήσει μακροπρόθεσμα την εθνική οικονομία που ασκεί μικροοικονομική κατασκοπεία σε ένα αποτέλεσμα παρόμοιο με εκείνα των άλλων αποτυχημένων προσπαθειών στον τομέα της βιομηχανικής πολιτικής, δηλαδή σε ένα οικονομικό περιβάλλον όπου μη ανταγωνιστικοί εγχώριοι παραγωγοί θα κερδίζουν εις βάρος των καταναλωτών και των φορολογούμενων. (Porteous, 1998)

2.4 Μέθοδοι οικονομικής κατασκοπείας

Υπάρχουν τέσσερις βασικές μέθοδοι άσκησης κατασκοπείας που εμπίπτουν στην υπόθεση της οικονομικής κατασκοπείας, οι οποίες μπορεί να επηρεάσουν τον τρόπο με τον οποίο οι χώρες συμπεριφέρονται μεταξύ τους. Κάθε μέθοδος έχει τη δική της σειρά γραπτών και άγραφων κανόνων και εθίμων σχετικά με τον τρόπο επίλυσης του θέματος μεταξύ των χωρών.

2.4.1 Αντιπρόσωπος υπό επίσημη κάλυψη

Οι υπάλληλοι υπό επίσημη κάλυψη ή νομικοί κατάσκοποι εργάζονται στο εξωτερικό και συνήθως ανήκουν σε δύο ιδρύματα. Είτε σε διπλωματικές ή προξενικές αποστολές, είτε σε διεθνείς οργανισμούς. Έχουν υπάρξει πολλές υποθέσεις σχετικά με πράξεις οικονομικής κατασκοπίας που διαπράττονται από διπλωματικούς αντιπροσώπους. Η Σύμβαση της Βιέννης για τις διπλωματικές σχέσεις του 1961 και η Σύμβαση της Βιέννης περί Προξενικής Σχέσης του 1963 ρυθμίζουν τέτοιες περιπτώσεις. Το 1860, ένας Ολλανδός διπλωμάτης σφυρηλατούσε την έκφραση «ο πρεσβευτής είναι ένας αξιότιμος κατάσκοπος». Παρόλο που σήμερα υπάρχει σαφής διάκριση μεταξύ ανθρώπων που κάνουν καριέρα στη διπλωματία και ανθρώπων που χρησιμοποιούν αυτό το καθεστώς με μοναδικό σκοπό τη συλλογή πληροφοριών κρυφά, οι στόχοι και τα προβλήματα της διπλωματίας και των πληροφοριών είναι τα ίδια (Navasardian, 2013).

Από τη μία πλευρά, ένας διπλωμάτης υποτίθεται ότι συλλέγει τις απαραίτητες πληροφορίες για το έθνος του, έτσι ώστε το έθνος του να μπορεί να λαμβάνει οικονομικές, πολιτικές και στρατιωτικές αποφάσεις. Στην περίπτωση αυτή, ο διπλωμάτης είναι ένας καταφανής κατάσκοπος. Από την άλλη πλευρά, το έθνος υποδοχής υποτίθεται ότι παρέχει προνόμια για να βοηθήσει τους διπλωμάτες να ολοκληρώσουν τα καθήκοντά τους. Ένας διπλωμάτης έχει μια αποστολή, η οποία συγκεντρώνει πληροφορίες, ακριβώς όπως κάνει ένας κατάσκοπος,

εκτός από το ότι τα μέσα για την επίτευξη αυτού του στόχου είναι διαφορετικά. Όμως, ο διπλωματικός πράκτορας υποχρεούται να σέβεται το δίκαιο της χώρας υποδοχής, κάτι που δεν συμβαίνει πάντα, ειδικά αν το άτομο ασχολείται με την κατασκοπεία. Όταν ένας διπλωμάτης, είτε ένας κατάσκοπος, συλλαμβάνεται, το έθνος υποδοχής του τον δηλώνει ως persona non grata (αναξιόπιστος πολίτης) (Porteous, 1994).

Η πλειοψηφία των χωρών σε όλο τον κόσμο καταχράται τη Σύμβαση της Βιέννης. Μόλις το Μάρτιο του τρέχοντος έτους, το Bloomberg ανέφερε ότι οι Ηνωμένες Πολιτείες εκδιώκουν εξήντα Ρώσους κατασκόπους που έχουν εγγραφεί ως Ρώσοι διπλωμάτες. Η κατασκοπεία, αν και σκοτεινή, ενδεχομένως δυσάρεστη και συχνά παράνομη, είναι μια αποδεκτή διεθνής πρακτική. Όλες οι χώρες κατασκοπεύουν και οι περισσότερες, αν όχι όλες, στέλνουν τους κατάσκοπους τους στο εξωτερικό όπου συγκαλύπτονται από διπλωμάτες (Lee & Lederman, 2018).

Κατά τη διάρκεια του Ψυχρού Πολέμου, αυτή ήταν μια πολύ κοινή πρακτική. Στο τέλος του Ψυχρού Πολέμου, υπήρχαν λιγότεροι διπλωματικοί πράκτορες που δηλώνονταν ως «persona non grata» για δραστηριότητες ασυμβίβαστες με το καθεστώς τους, κάτι που συχνά αποτελεί ευφημισμό για κατασκοπεία. Ωστόσο, θα ήταν χρήσιμο να αναφερθεί ότι δεν είναι πάντα εύκολο να οριστεί η διπλωματική λειτουργία σε σχέση με τις οικονομικές υποθέσεις, όπως παρατηρούν οι Baheri και Fard (2015). Το αποτέλεσμα είναι μια γκρίζα περιοχή μεταξύ νόμιμων οικονομικών ερευνών και παράνομης οικονομικής κατασκοπείας.

Τα στοιχεία δείχνουν ότι ήδη από το 1995 οι αμερικανικές υπηρεσίες πληροφοριών, συνέχιζαν να προσπαθούν να υλοποιήσουν οικονομικούς στόχους κατασκοπείας. Οι New York Times ανέφεραν τα εξής μετά το φιάσκο του σταθμού του Παρισιού της CIA(Central Intelligence Agency) το 1995: «*Οι προσπάθειες στο σταθμό του Παρισιού για να κλέψουν τα οικονομικά στοιχεία από τους Γάλλους και η παγίδευση των αξιωματικών του γραφείου από τη γαλλική αντικατασκοπεία αντικατοπτρίζουν το γεγονός ότι η CIA πιστεύει ότι οι κίνδυνοι απόκρυψης εμπορικών μυστικών αξίζουν την πιθανή αποπληρωμή*» (Weiner, 1995).

Αυτό που είχε συμβεί στο Παρίσι ήταν ότι οι Γάλλοι συνεργάτες έφεραν ένα συμβασιούχο υπάλληλο της CIA με μερική απασχόληση, συνδέοντάς τον τελικά με τους τέσσερις υπαλλήλους της CIA που λειτουργούσαν υπό διπλωματική κάλυψη από την Πρεσβεία των ΗΠΑ στο Παρίσι. Το ρεπορτάζ από τους New York Times ανέφερε τότε ότι, οι γαλλικές αρχές δεν συνέλαβαν ποτέ κανέναν από τους αξιωματικούς της CIA και αφού η δημοσιότητα γύρω από την υπόθεση έσβησε, τους επέτρεψε να εγκαταλείψουν ήσυχα τη χώρα. Στην πραγματικότητα, η γαλλική κυβέρνηση δεν μπόρεσε να συλλάβει αξιωματικούς της CIA επειδή είχαν διπλωματική ασυλία και δεν τους επέτρεπε να φύγουν, αλλά μάλλον τους απέβαλαν σύμφωνα με την αρχή της persona non grata.

2.4.2 Αντιπρόσωπος χωρίς επίσημη κάλυψη

Οι κατάσκοποι χωρίς επίσημη κάλυψη είναι μυστικοί πράκτορες χωρίς επίσημους δεσμούς με την κυβέρνηση στην οποία εργάζονται. Ο όρος «κάλυψη» αναφέρεται στο αμάλγαμα ψεμάτων και στηρίξεων, από τα ψεύτικα ονόματα έως τις ψεύτικες εταιρείες που χρησιμοποιούνται με στόχο να συγκαλύπτουν την πραγματική ταυτότητα και τον σκοπό του κατασκόπου (Miller, 2005). Μια περίφημη περίπτωση αντιπροσώπου χωρίς κάλυψη είναι αυτή του Valerie Plame, ενός λειτουργού της CIA, του οποίου η κάλυψη εκτέθηκε στα μέσα ενημέρωσης από τη διοίκηση του George W. Bush. Η ιστορία κάλυψης του Plame ήταν ότι ήταν ιδιωτικός σύμβουλος ενέργειας, ενώ εργαζόταν στην πραγματικότητα για ένα τμήμα της CIA που παρακολούθησε τη διάδοση των όπλων σε όλο τον κόσμο. Με άλλα λόγια, ήταν πράκτορας της CIA χωρίς επίσημη κάλυψη που εργάστηκε στο εξωτερικό ως ιδιώτης χωρίς εμφανή σύνδεση με την κυβέρνηση των ΗΠΑ.

Αυτού του είδους οι πράκτορες αποτελούν κάποια από τα πιο καλά φυλαγμένα μυστικά της εκάστοτε κυβέρνησης, επειδή συχνά εργάζονται για πραγματικές ή φιλόδοξες ιδιωτικές εταιρείες στο εξωτερικό και είναι ελεύθεροι να κατασκοπεύουν από μόνοι τους (Duffy & Burge, 2003). Επιπλέον, είναι πιο δύσκολο να εκπαιδευτούν, πιο κοστοβόρο να τοποθετηθούν στο πεδίο και μπορεί να παραμείνουν μυστικοί περισσότερο από τους τακτικούς πράκτορες. Το σημαντικότερο πλεονέκτημα των κατασκόπων χωρίς κάλυψη είναι το ότι μπορούν επίσης να πάνε σε μέρη και να δουν τους ανθρώπους τους οποίους, εκείνοι υπό επίσημη κάλυψη δεν μπορούν.

Επειδή δεν έχουν καμία αξίωση για διπλωματική ασυλία αν τους πιάσουν, αυτοί οι παράνομοι πράκτορες είναι οι πιο ευάλωτοι από όλους τους κατασκόπους. Εάν γίνουν αντιληπτοί, υπάρχουν δύο πιθανά σενάρια σχετικά με την ευθύνη της χώρας προέλευσης. Η πρώτη πιθανότητα είναι ότι η εν λόγω χώρα αναγνωρίζει τον πράκτορα ως δικό του και στη συνέχεια αναλαμβάνει τη δική του ευθύνη, διότι υπάρχει σχέση μεταξύ του ατόμου και της χώρας προέλευσης. Η δεύτερη πιθανότητα είναι ότι δεν υπάρχει καθιερωμένη σύνδεση μεταξύ της χώρας και του κατασκόπου και η εν λόγω χώρα δεν παρεμβαίνει υπέρ του κατασκόπου.

2.4.3 Αντιπρόσωπος διεθνούς οργανισμού

Οι κατάσκοποι που εργάζονται σε διεθνείς οργανισμούς είναι πράκτορες που έχουν επίσημη κάλυψη. Παρ’ ότι οι πράκτορες αυτοί έχουν επίσης ορισμένα προνόμια και ασυλίες λόγω της εργασίας τους, η οποία απαιτεί ανεξαρτησία για την επίτευξη στόχων, στην πραγματικότητα αυτά τα προνόμια είναι λιγότερο σημαντικά από αυτά των διπλωματών. Διεθνείς οργανισμοί όπως το ΝΑΤΟ(North Atlantic Treaty Organization), ο ΠΟΕ(Παγκόσμιος Οργανισμός Εμπορίου), η Διεθνής Διαφάνεια κ.λπ. είναι γεμάτοι από κατασκόπους. Για παράδειγμα, ο Bosco (2012) αναφέρει ότι μυστικοί πράκτορες μερικές φορές τοποθετήθηκαν σε περίπτερα διερμηνέων στα Ηνωμένα Έθνη, ελπίζοντας να σπάσουν τις φωτογραφίες των

διαβαθμισμένων εγγράφων στα χέρια των επισφαλών διπλωματών. Ο Gowan (2018) προχωράει ακόμη περισσότερο και ισχυρίζεται ότι οι διεθνείς οργανισμοί προσφέρουν στους κατασκόπους απίστευτα εύκολο έργο για να πραγματοποιήσουν τους στόχους τους και ότι η κατασκοπεία μπορεί να είναι η σημαντικότερη συμβολή αυτών των θεσμών στη διεθνή σταθερότητα.

Η συζήτηση που υπάρχει και πάλι αντιτίθεται σε δύο συμφέροντα: το συμφέρον του κράτους υποδοχής στη δική του ασφάλεια και το συμφέρον του πράκτορα να διεξάγει το έργο του με πλήρη ανεξαρτησία. Προφανώς είναι προτιμότερο το κράτος να χρησιμοποιεί προληπτικά και όχι κατασταλτικά μέσα. Σε αντίθεση με ό, τι συμβαίνει με έναν διπλωμάτη, η χώρα υποδοχής δεν μπορεί να δηλώσει τον πράκτορα persona non grata. Για να γίνει αυτό, οι δύο οντότητες πρέπει να είναι της ίδιας φύσης, και οι δύο πρέπει να έχουν διεθνή κυριαρχία για να επωφεληθούν από την αμοιβαιότητα, κάτι που δεν ισχύει για τον διεθνή οργανισμό.

Σε περιπτώσεις οικονομικής κατασκοπείας, η αντίδραση μπορεί να είναι διττή: εκείνη του ίδιου του διεθνούς οργανισμού και εκείνη της χώρας υποδοχής όπου βρίσκεται. Για τον διεθνή οργανισμό, εάν η πράξη στρέφεται εναντίον του, μπορεί να απολύσει το εν λόγω πρόσωπο για σοβαρό παράπτωμα. Εάν ο πράκτορας έχει ξεπεράσει τα όρια της νόμιμης συμπεριφοράς εντός της χώρας υποδοχής, μπορεί να αρθεί η ασυλία του και αν έχει κατασκοπεύσει και ενεργήσει κατά της χώρας, το κράτος μπορεί να τον παραπέμψει στα δικά του δικαστήρια ή να το απομακρύνει, ή και τα δύο (Baker, 2003).

2.4.4 Πράκτορες του ιδιωτικού τομέα

Οι πράκτορες του ιδιωτικού τομέα είναι άτομα ή οργανώσεις που κατασκοπεύουν προς όφελος ιδιωτών ή δημόσιων πελατών. Από την πτώση του τείχους του Βερολίνου, αυτοί οι τύποι ατόμων και οργανισμών έχουν αυξηθεί. Η οικονομική κατασκοπεία έχει γίνει μεγάλη επιχείρηση από το τέλος του ψυχρού πολέμου. Βεβαίως, πιστεύεται ότι πολλές υπηρεσίες πληροφοριών σε όλο τον κόσμο έχουν μετατοπίσει τους κατασκοπευτικούς τους πόρους μακριά από τους πολιτικούς στόχους, σε περισσότερο βιομηχανικούς και οικονομικούς στόχους (Nasheri, 2005). Ο Christopher Steele, ο βρετανός συγγραφέας του φακέλου της Ρωσίας που περιέχει όλες τις συμβιβαστικές πληροφορίες για τον πρόεδρο Trump, είναι ένας πράκτορας του ιδιωτικού τομέα. Επίσης, η Cambridge Analytica, η βρετανική εταιρεία που συμμετείχε στην εξαπάτηση μέρους του αμερικανικού εκλογικού σώματος μέσω του Facebook, είναι ιδιωτική υπηρεσία κατασκοπείας (Gonzalez, 2019).

Αυτοί οι πράκτορες δεν ενεργούν εξ ονόματος μιας χώρας και μπορεί να μην συμμορφωθούν με τις εντολές και τους νόμους της. Ως εκ τούτου, το κράτος δεν μπορεί να θεωρηθεί υπεύθυνο. Η εξαίρεση από αυτή την αρχή μπορεί να είναι η κατάσταση όπου η χώρα δεν λαμβάνει προληπτικά μέτρα για την προστασία των θυμάτων από πιθανή επίθεση. Σε αυτή την περίπτωση, εμπλέκεται η ευθύνη τόσο του κράτους όσο και του ιδιωτικού φορέα ή

οντότητας. Αντίθετα, όταν δημιουργείται μια σύνδεση μεταξύ πράκτορα και χώρας, οι πράξεις του πράκτορα μπορούν να αποδοθούν σε αυτό το κράτος (Gonzalez, 2019).

Το πρόβλημα είναι ότι η απόδειξη μιας τέτοιας σχέσης είναι δύσκολο να επιτευχθεί. Και από πολιτική άποψη, στην πραγματικότητα αυτό δεν είναι επιθυμητό. Όπως διαπιστώνεται στις υποθέσεις Cambridge Analytica και Christopher Steele, η Μεγάλη Βρετανία δεν είχε ουσιαστικές συνέπειες, ούτε κανένας δημόσιος υπάλληλος από τις Ηνωμένες Πολιτείες τιμωρήθηκε. Πράγματι, ακόμη και αν οι πράξεις καταλογίζονται σε μια συγκεκριμένη χώρα, εξακολουθεί να είναι απαραίτητο να αποδειχθεί ότι η πράξη αυτή παραβιάζει ένα διεθνές δίκαιο και όπως αναλύεται στο παρόν κεφάλαιο, δεν υπάρχουν διεθνείς νόμοι που να τιμωρούν την πράξη κατασκοπείας (Gonzalez, 2019).

2.4.5 Η κυβερνοκατασκοπεία και οι τεχνολογίες που στοχεύονται τα τελευταία χρόνια

Η κυβερνοκατασκοπεία αποτελεί μία μέθοδο της οικονομικής κατασκοπείας που έχει απασχολήσει ιδιαίτερα την παγκόσμια κοινότητα τα τελευταία χρόνια. Ο τρόπος με τον οποίο γίνεται αντιληπτή η κυβερνοκατασκοπεία, εξαρτάται από διάφορους παράγοντες, όπως η έκταση και η φύση της ζημιάς που δημιουργείται, η ταυτότητα των επιθέσεων και ο τρόπος με τον οποίο κλάπηκαν οι πληροφορίες. Το 2013 στο συνέδριο που πραγματοποιήθηκε στο Tallin της Εσθονίας από το NATO(North Atlantic Treaty Organization) η κυβερνοκατασκοπεία ορίστηκε ως «εκείνη η πράξη που έχει αναληφθεί κρυφά ή από ψευδείς προθέσεις και χρησιμοποιεί τις ικανότητες του κυβερνοχώρου για τη συλλογή (ή προσπάθεια συλλογής) πληροφοριών με σκοπό τη μεταβίβαση αυτών στον αντίπαλο». Είναι γεγονός πως η εξάρτηση των ανθρώπων από τους υπολογιστές αυξάνεται όλο και περισσότερο, με τις εγκληματικές δραστηριότητες να μεταφέρονται στον ψηφιακό κόσμο. Το γεγονός αυτό αποδεικνύει πως η κυβερνοκατασκοπεία δεν αποτελεί πλέον σενάριο επιστημονικής φαντασίας, αντιθέτως εξελίσσεται και γίνεται όλο και πιο αποτελεσματική (Rubenstein, 2014).

Για τις ΗΠΑ η κυβερνοκατασκοπεία, ως μέθοδος της οικονομικής κατασκοπείας, θεωρείται στρατηγική απειλή. Όπως επισημαίνεται στην αναφορά του NCSC(National Counterintelligence and Security Center), το 2018 με τίτλο Foreign Economic Espionage in Cyberspace, η ξένη οικονομική και βιομηχανική κατασκοπεία εναντίον των Ηνωμένων Πολιτειών εξακολουθεί να αποτελεί σημαντική απειλή για την ευημερία, την ασφάλεια και το ανταγωνιστικό πλεονέκτημα της Αμερικής. Ο κυβερνοχώρος αποτελεί τον προτιμώμενο επιχειρησιακό τομέα για ένα ευρύ φάσμα απειλών, από εχθρικές χώρες έως εμπορικές επιχειρήσεις που λειτουργούν υπό κρατική επιρροή. Οι τεχνολογίες της επόμενης γενιάς, όπως η τεχνητή νοημοσύνη και το ίντερνετ των πραγμάτων, θα αποκαλύψουν νέα τρωτά σημεία στα δίκτυα των ΗΠΑ για τα οποία η κοινότητα του κυβερνοχώρου παραμένει σε μεγάλο βαθμό απροετοίμαστη. Η προετοιμασία μιας αποτελεσματικής αντίδρασης απαιτεί την κατανόηση της οικονομικής κατασκοπείας ως παγκόσμια απειλή για την ακεραιότητα της

αμερικανικής οικονομίας και του παγκόσμιου εμπορίου (National Counterintelligence and Security Center, 2018).

Οι Ηνωμένες Πολιτείες παραμένουν ένα παγκόσμιο κέντρο έρευνας, ανάπτυξης και καινοτομίας σε πολλούς τομείς υψηλής τεχνολογίας. Το γεγονός αυτό οδηγεί τα ομοσπονδιακά ερευνητικά ιδρύματα, τα πανεπιστήμια και τις εταιρείες να αποτελούν πολύ συχνά θύματα κυβερνοκατασκοπείας και αυτή η μακροπρόθεσμη τάση παραμένει ιδιαίτερα ανησυχητική για τις υπηρεσίες πληροφοριών των ΗΠΑ (National Counterintelligence and Security Center, 2018)

Παρόλο που πολλές πτυχές της οικονομικής δραστηριότητας και τεχνολογίας των ΗΠΑ είναι πιθανό να ενδιαφέρουν ξένους συλλέκτες πληροφοριών, το μεγαλύτερο ενδιαφέρον παρουσιάζουν οι ακόλουθοι τομείς: ενέργεια/εναλλακτικές μορφές ενέργειας(βιοκαύσιμα, τεχνολογία ηλιακής ενέργειας και ανεμογεννήτριες), βιοτεχνολογία(θεραπεία λοιμωδών νόσων, νέα εμβόλια και φάρμακα και εξελιγμένες ιατρικές συσκευές), αμυντική τεχνολογία(αεροναυπηγική και αεροναυτικά συστήματα, οπλισμός και ραντάρ νέας τεχνολογίας), περιβαλλοντική προστασία(ενεργειακά αποδοτικές συσκευές, ηλεκτρικά και υβριδικά αυτοκίνητα και ο έλεγχος ρύπανσης του νερού και του αέρα), κατασκευές υψηλής ποιότητας(προηγμένη ρομποτική, σύνθετα υλικά υψηλής απόδοσης, εξοπλισμός παραγωγής ολοκληρωμένων κυκλωμάτων και τεχνολογία συναρμολόγησης), τεχνολογία πληροφοριών και επικοινωνιών(τεχνητή νοημοσύνη, το ίντερνετ των πραγμάτων, κβαντική υπολογιστική και επικοινωνίες) (National Counterintelligence and Security Center, 2018).

2.4.6 Αναφορά στην διπλωματική διαμάχη της Βραζιλίας με τις Ηνωμένες Πολιτείες

Μετά τις μαζικές διαρροές του Snowden, ο Jonathan Watts της εφημερίδας Guardian ανέφερε το Σεπτέμβριο του 2013 ότι η NSA(National Security Agency) όχι μόνο κατασκοπεύει τους κορυφαίους πολιτικούς της Βραζιλίας αλλά και την πετρελαϊκή εταιρεία της Βραζιλίας Petrobras. Αυτό σήμαινε ότι η NSA διεξήγαγε πράξεις συγκέντρωσης πληροφοριών που ήταν οικονομικού ή εμπορικού χαρακτήρα και ξεπερνούσαν την κύρια αποστολή της εθνικής ασφάλειας. Η Βραζιλία αντέδρασε με το να είναι ένας αυστηρός κριτικός της NSA, η οποία όπως δήλωσε ο πρόεδρός της έχει ενσωματώσει την εθνική ασφάλεια στο όνομά της και ακύρωσε μια προγραμματισμένη κρατική επίσκεψη στον Λευκό Οίκο, ενώ παράλληλα, προέβη σε αλλαγή των κανονισμών που θα είχαν υποβάλει υπό διαφορετικές συνθήκες, εταιρείες όπως το Facebook και το Google σχετικά με την αποθήκευση των δεδομένων τους στη Βραζιλία (Reid, 2016).

Οι σχέσεις ήταν πολύ παγωμένες και όμως, δύο χρόνια μετά τις αποκαλύψεις, τόσο οι Αμερικανοί όσο και οι Βραζιλιάνοι πρόεδροι έδωσαν το παρών στη Σύνοδο Κορυφής της Αμερικής το 2015. Σύμφωνα με τα δημοσιεύματα εκείνης της εποχής, παρόλο που η Βραζιλία δεν έλαβε ποτέ δημόσια συγγνώμη από τις Ηνωμένες Πολιτείες, όπως είχε απαιτήσει

μπροστά από τον ΟΗΕ(Οργανισμός Ηνωμένων Εθνών) ή ακόμα και τη δημόσια εγγύηση ότι η συμπεριφορά δεν θα επαναληφθεί, η Ουάσιγκτον έκανε κάποιες παραχωρήσεις, ώστε να ζητούν πλέον επίσημη πληροφόρηση από την Βραζιλία, αντί να χρησιμοποιούν άλλα μέσα (Reid, 2016).

Οι χώρες είναι ελεύθερες ως προς τον τρόπο με τον οποίο αντιμετωπίζουν περιπτώσεις κατασκοπείας. Ο ορισμός της κατασκοπείας είναι τόσο λεπτός για τα δικαστήρια, επειδή πρέπει να αποδείξουν ότι οι ενέργειες κατασκοπείας βλάπτουν τα συμφέροντα του κράτους. Όσον αφορά τους διπλωματικούς υπαλλήλους, όπως σημειώθηκε προηγουμένως, η διαδικασία που πρέπει να ακολουθηθεί είναι η δήλωση του persona non grata ακολουθούμενη από την ανάκλησή του εκάστοτε υπαλλήλου. Σε αυτή την περίπτωση, η Βραζιλία δεν είχε κανέναν να απελάσει πίσω στις Ηνωμένες Πολιτείες. Στην αρχή του σκανδάλου, η Βραζιλία είδε το όριο, πέρα από το οποίο η κατασκοπεία έδωσε περισσότερες δυσκολίες από ότι πλεονεκτήματα. Με την πάροδο του χρόνου αυτό δεν συνέβαινε πλέον. Στην ουσία, ο συμβιβασμός που διαπιστώθηκε, είναι ότι και οι δύο χώρες χρειάστηκε να προχωρήσουν και ότι η κατασκοπεία θα συνεχιστεί.

3. Η βιομηχανική κατασκοπεία

3.1 Εισαγωγικά στοιχεία

Το τέλος του Ψυχρού Πολέμου δεν σημαίνει ότι δεν υπάρχει πλέον ισορροπία δυνάμεων σε παγκόσμιο επίπεδο. Απλώς δεν είναι πλέον η πολιτική ιδεολογία που κυριαρχεί στον κόσμο, αλλά το καπιταλιστικό δόγμα. Ολόκληρος ο κόσμος επικεντρώνεται στα καθαρά κέρδη, τον κύκλο εργασιών, τα αποτελέσματα της χρηματιστηριακής αγοράς και τα μερίσματα. Οι πολίτες δεν έχουν εχθρούς, έχουν ανταγωνιστές. Το κράτος δεν είναι πλέον ο κύριος παίκτης στην παγκόσμια κοινότητα, καθώς έχει εκχωρήσει σε εταιρείες που είναι ολοένα και περισσότερο στην πρώτη γραμμή, σημαντικές ιδιότητες. Όλος ο κόσμος γίνεται ένα τεράστιος ψηφιακός ιστός, χάρη στο διαδίκτυο και στην παγκοσμιοποίηση. Ο κόσμος των ηλεκτρονικών υπολογιστών επηρεάζει τώρα όλες τις σφαίρες της ανθρώπινης ζωής. Συμπεριλαμβανομένης της οικονομίας, η ανάγκη να συλλέγουν και να εκμεταλλεύονται οι άνθρωποι την νοημοσύνη γρηγορότερα από ότι η ανταγωνιστική χώρα έχει καταστεί πρωταρχικής σημασίας.

Όλα αυτά σημαίνουν ότι εμφανίζονται νέες άγνωστες απειλές. Η ξαφνική έξαρση της ψηφιακής επεξεργασίας δεδομένων και αποθήκευσης έφερε μαζί της μια σειρά από νέες τεχνικές και νέες απειλές με νέους οικονομικούς κυβερνοχώρους που οι χάκερς οι οποίοι, όπως και οι πειρατές των παλαιότερων εποχών, πλέουν τις θάλασσες του κόσμου του διαδικτύου υπό τη σημαία τους ή, περιστασιακά, ακόμη είναι ικανοί να προσφέρουν τις υπηρεσίες τους στα διάφορα κράτη. Οι παράγοντες της αγοράς αναγκάζονται να προσαρμοστούν γρήγορα σε αυτές τις αλλαγές. Οι εταιρείες αγωνίζονται μεταξύ τους για νέα μερίδια αγοράς και για να είναι πιο ανταγωνιστικές. Οι συνέπειες στις οικονομίες είναι σημαντικές: η αποσταθεροποίηση των αγορών, οι πτωχεύσεις, η ανεργία κ.λπ. (Robert, 2014).

Όντας ο κύριος καινοτόμος, η μεγαλύτερη οικονομία και ο καπιταλιστικός κινητήρας του κόσμου, οι Ηνωμένες Πολιτείες είναι ο πιο συνηθισμένος στόχος. Πράγματι, αμερικανικές εταιρείες, βιομηχανίες και κυβέρνηση αποτελούν συχνά το θύμα οικονομικής ή βιομηχανικής κατασκοπείας με θύτη ξένες υπηρεσίες πληροφοριών και ξένες εταιρείες ώστε να αποκτήσουν τις γνώσεις και τα δεδομένα τους. Η τεχνολογία, η παγκοσμιοποίηση και η διεθνής ανταγωνιστικότητα αποτελούν συνεχώς πρόκληση για τις εταιρείες να δημιουργήσουν ακόμα πιο καινοτόμα προϊόντα και να ξεπεράσουν τον ανταγωνισμό. Υπάρχει μόνο ένας τρόπος να επιβιώσει κανείς στην καπιταλιστική ζούγκλα, σύμφωνα με τον

οποίο, πρέπει να είναι μπροστά από τους άλλους από ένα σημείο πληροφόρησης ή από τεχνολογική άποψη. Υπάρχουν μόνο δύο τρόποι να προχωρήσουν και να ανταποκριθούν σε αυτό ακριβώς, ο ένας είναι νόμιμος και αναφέρεται βέβαια στην επένδυση και στην έρευνα και ανάπτυξη και τον έλεγχο του επιχειρηματικού περιβάλλοντος γύρω από την εταιρεία. Αυτή είναι η ιδανική κατάσταση που υποθέτει ότι η εταιρεία έχει χρόνο και χρήμα. Αν όχι, η εταιρεία μπορεί να μπει στον πειρασμό να χρησιμοποιήσει τη δεύτερη επιλογή, λαμβάνοντας παράνομα πληροφορίες μέσω παράνομων μέσων. Αυτός είναι ο λόγος για τον οποίο υπάρχει η βιομηχανική κατασκοπεία και το γεγονός ότι ολόκληρος ο κόσμος είναι ένα καπιταλιστικό χωριό που χρησιμοποιεί το διαδίκτυο, έχει επιταχύνει το φαινόμενο σε ακαθάριστα και απρόβλεπτα επίπεδα (Calder & Watkins, 2006).

Σε αυτή τη νέα καπιταλιστική παγκόσμια τάξη, με έντονο ανταγωνισμό, ο πραγματικός πλούτος δεν είναι πια η πρώτη ύλη, αλλά η δημιουργικότητα και η καινοτομία. Ωστόσο, η ανάλυση της οικονομικής απειλής και των πρακτικών της αποκαλύπτει τον κίνδυνο γενίκευσης ενός νέου προβλήματος που ονομάζεται βιομηχανική κατασκοπεία. Το φαινόμενο αυτό είναι πρωτοφανές τα τελευταία χρόνια και η αντίδραση των επιχειρήσεων σε αυτή τη δραστηριότητα, αν και υπόγεια αλλά εξαιρετικά καλά οργανωμένη, μπορεί να είναι δαπανηρή για τις επιχειρήσεις και τα εκβιομηχανισμένα έθνη (Calder & Watkins, 2006).

Ενώ η κατασκοπεία δεν είναι μια πρόσφατη δραστηριότητα, είναι γεγονός ότι η βιομηχανική κατασκοπεία έχει εντατικοποιηθεί τουλάχιστον από τον Ψυχρό Πόλεμο και έπειτα. Το γεγονός αυτό αποτελεί αντικείμενο πολλών ανησυχιών. Αξίζει να σημειωθεί ότι η κυβέρνηση των ΗΠΑ παρουσιάζει ετησίως στο Κογκρέσο την ετήσια έκθεσή της σχετικά με την ξένη βιομηχανική κατασκοπεία που απευθύνεται στις αμερικανικές τεχνολογίες, το ρεκόρ των οποίων φαίνεται κάθε φορά και πιο συντριπτικό.

Η ανθρωπότητα γνωρίζει ποικίλα παραδείγματα βιομηχανικής κατασκοπείας μέσω της ιστορίας. Έτσι, οι βρετανικοί νόμοι για τα διπλώματα ευρεσιτεχνίας της δεκαετίας του 1780 αποσκοπούσαν στην αποτροπή της κλοπής τεχνολογιών στην αναδυόμενη κλωστοϋφαντουργία. Κατά τη διάρκεια του αμερικανικού εμφυλίου πολέμου, ο κ. Μπέϊκερ απομνημόνευε τη διάταξη πυροπροστασίας και τις τεχνολογίες των υποβρυχίων των Συνομοσπονδιακών Κρατών ώστε να διαβιβάζει τις πληροφορίες στο Πολεμικό Ναυτικό των Νοτίων Κρατών (Mendell, 2011).

Ο Herring σημειώνει το μεγάλο παράδειγμα συλλογής πληροφοριών, το οποίο αργότερα βοήθησε να οικοδομηθεί μια από τις πιο ισχυρές οικονομικές αυτοκρατορίες στη Βόρεια Ευρώπη. Με τη βοήθεια ενός από τους υπαλλήλους του, ο σουηδός τραπεζίτης Marcus Wallenberg κατάφερε να αντιγράψει την ιδέα της συνεργασίας πληροφοριών μεταξύ της γαλλικής κυβέρνησης και των τοπικών τραπεζών (Herring, 1992).

3.2 Η ανάλυση της βιομηχανικής κατασκοπείας

Διάφοροι μελετητές δίνουν ορισμούς και ονόματα στη βιομηχανική κατασκοπεία. Οι Wright & Roy (1999) το ονομάζουν ως εταιρική ή οικονομική κατασκοπεία και βιομηχανική νοημοσύνη. Ο Soilen (2016) διακρίνει την οικονομική και βιομηχανική κατασκοπεία, εξηγώντας ότι η τελευταία εξαιρείται από τη συμμετοχή της κυβέρνησης στη συλλογή πληροφοριών και την κλοπή της γνώσης. Ωστόσο, οι στρατιωτικοί χρησιμοποιούν μια εκδοχή οικονομικής κατασκοπείας ως πόλεμο μέσω του διαδικτύου για να καταστρέψουν την βασική υποδομή της χώρας του εχθρού. Ο Nasheri (2005) εξηγεί τις στρατηγικές συνδέσεις μεταξύ των κυβερνητικών υπηρεσιών πληροφοριών και την επιτυχία του έθνους για το οποίο έλαβε χώρα μια τέτοια στάση. Οι πρώτες μετατοπίσεις των μεθόδων βιομηχανικής κατασκοπείας ξεκίνησαν μαζί με την ύπαρξη της εποχής της πληροφορίας και της γενικευμένης παγκοσμιοποίησης. Ο αμερικανικός νόμος οικονομικής κατασκοπείας περιγράφει τις νομικές πτυχές της βιομηχανικής κατασκοπείας αφήνοντας ανοιχτή τη συζήτηση είτε για να κρατήσει το εμπορικό μυστικό, είτε για να προωθήσει την ανοιχτή παγκόσμια κοινωνία.

Ο Peter Hamilton υποστηρίζει πως η βιομηχανική κατασκοπεία αποτελεί απειλή για την εθνική ασφάλεια ενός κράτους. Η προστασία της βιομηχανίας και των συμφερόντων της αποτελεί ζήτημα υψίστης σημασίας για ένα κράτος και εν συνεχεία για την ίδια την επιχείρηση. Η Βιομηχανική κατασκοπεία έχει να κάνει με την απόκτηση εμπορικών πληροφοριών από τους ανταγωνιστές μίας επιχείρησης με σκοπό την μεγιστοποίηση των συμφερόντων αυτού που την ασκεί. Η πληροφορία του οικονομικού περιεχομένου είναι αλληλένδετη με τον όρο βιομηχανική κατασκοπεία και ορίζεται ως εξής: «*πληροφορία σχετική με το εμπόριο και την οικονομία, συμπεριλαμβανομένων των τεχνολογικών στοιχείων, εμπορικών και κυβερνητικών πληροφοριών, η απόκτηση των οποίων εκ μέρους ξένων συμφερόντων μπορεί άμεσα ή έμμεσα να υποβοηθήσει τη σχετική παραγωγικότητα ή την ανταγωνιστική θέση της οικονομίας της χώρας που θα την αποκτήσει*» (Porteous, 1994).

3.3 Μέθοδοι βιομηχανικής κατασκοπείας

Υπάρχουν στοιχεία που αποδεικνύουν τις ενέργειες των πρώην σοβιετικών πρακτόρων για τη βιομηχανική κατασκοπεία καθώς και μικρές ομάδες πρακτόρων που προσλαμβάνονται από τις κυβερνήσεις των χωρών και ενεργούν προς όφελος της βιομηχανικής κατασκοπείας, με στόχο να παρέχουν ασύμμετρη πληροφόρηση σε ξένα κράτη (Pasternak & Witkin, 1996). Σε πολλές περιπτώσεις, οι μέθοδοι που εφαρμόζονται από αυτούς τους επαγγελματίες κατασκόπους μπορούν να σπάσουν οποιαδήποτε προστασία στο σύστημα πληροφοριών των εταιρειών. Στην συνέχεια, παρουσιάζονται οι σημαντικότερες μέθοδοι, οι οποίες είναι δυνατόν να έχουν νομική κάλυψη, αλλά από την άλλη πλευρά, είναι δυνατόν να είναι και εντελώς παράνομες.

3.3.1 Νόμιμες μέθοδοι

Υπάρχουν μερικά είδη νόμιμης βιομηχανικής κατασκοπείας. Οι ανταγωνιστές μπορούν να αγοράσουν προϊόντα από την εταιρεία, ως πελάτες, να πάρουν το πρωτότυπο ή μια τεχνολογία εργασίας και πάνω σε αυτήν να εξερευνήσουν πιθανούς τρόπους εκμετάλλευσής της από αυτούς. Η αγορά μιας εταιρείας είναι μια άλλη νόμιμη μέθοδος για την απόκτηση της βασικής τεχνολογίας της εταιρίας αυτής. Αυτή η μέθοδος εφαρμόζεται ευρέως στην Παγκόσμια Οικονομία και κανένας από τους μάνατζερ των μεγάλων πολυεθνικών εταιριών, αλλά και των μικρότερων, δεν μπορεί να δημιουργήσει ένα πλαίσιο πλήρους προστασίας των προϊόντων τους και να αποτρέψει τη συλλογή των πληροφοριών σε αυτή την περίπτωση (House, 1995).

Στην περίπτωση της απροθυμίας της εταιρείας να εισέλθει στην ξένη αγορά, είναι δυνατό να χρησιμοποιηθεί άλλη μέθοδος απόκτησης νόμιμων πληροφοριών. Για παράδειγμα, η εταιρεία μπορεί να πιέζεται από την κυβέρνηση ή τον εταίρο της ξένης εταιρείας για να εκπαιδεύσει τους τοπικούς εργαζόμενους και τους διαχειριστές στην κρίσιμη τεχνολογία. Οι διευθυντές εταιρικής ασφάλειας δεν συμμετέχουν πάντοτε σε μια διαδικασία λήψης αποφάσεων για την είσοδο στην αγορά και η ανώτερη διοίκηση αποφασίζει εάν στο τέλος, η όλη διαδικασία αξίζει τον κόπο με την έννοια της πρόσθετης κερδοφορίας. (House, 1995)

Οι βιομηχανικοί ανταγωνιστές είναι συχνά σε θέση να συγκεντρώσουν τις πολύτιμες πληροφορίες μέσω των πληροφοριών ανοιχτής πηγής (Open Source Information, OSI). Η εμπεριστατωμένη επισκόπηση των εφημερίδων, των επιστημονικών άρθρων, των ετήσιων οικονομικών εκθέσεων, των αιτήσεων για διπλώματα ευρεσιτεχνίας, των υλικών μάρκετινγκ, των διαφημίσεων, των εφαρμογών, των στόχων κ.λπ. μπορεί να δώσει πολλές γνώσεις σχετικά με την εταιρεία και τα προϊόντα της. Πολύ συχνά η ίδια η εταιρεία μπορεί να συνειδητοποιήσει την αξία των πληροφοριών που δίνονται μέσω των πληροφοριών ανοιχτής πηγής (House, 1995).

3.3.2 Παράνομες μέθοδοι

Σε πολλές περιπτώσεις, η αξία της επιθυμίας να αποκτηθούν οι απαραίτητες πληροφορίες ωθεί τους αντιπάλους να τις κλέψουν ή να τις αντιγράψουν χωρίς άδεια. Πολύ συχνά οι εσωτερικοί συνεργάτες χρησιμοποιούνται για τον σκοπό αυτό, καθώς είναι οι μόνοι που είναι δυνατόν να έχουν πρόσβαση στην εταιρεία. Παραδοσιακά, κάποιοι συνεργάτες ή κάποιοι με καλές επαφές στην εταιρεία, είναι πρόθυμοι να συνεργαστούν με εγκληματίες. Αυτοί οι άνθρωποι συχνά έχουν πρόσβαση στις απαραίτητες πληροφορίες ή μπορούν να παρέχουν πρόσβαση στους κατασκόπους με αντάλλαγμα τα χρήματα. Σε ορισμένες περιπτώσεις, οι εργαζόμενοι θα μπορούσαν να είναι οι ιδρυτές για το ίδιο το έγκλημα πληροφοριών, προσφέροντας τα εταιρικά μυστικά στους ανταγωνιστές προς πώληση (Pasternak & Witkin, 1996).

Ενώ ταξιδεύουν σε κάποιο επαγγελματικό ταξίδι, οι υπάλληλοι της εταιρείας μπορούν να γίνουν αντικείμενο περίπλοκων μεθόδων εταιρικής κατασκοπείας. Ειδικές συσκευές παρακολούθησης, κρυφές κάμερες και άλλες μέθοδοι επιστρατεύονται και είναι σε θέση να συλλέξουν τις απαραίτητες πληροφορίες για την εταιρεία. Στελέχη των μεγάλων αμερικανικών εταιρειών ανέφεραν συχνά έρευνα στα δωμάτια των ξενοδοχείων τους (House, 1995).

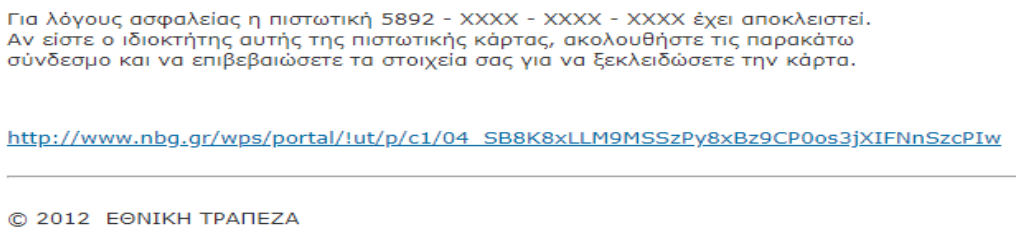
Οι μέθοδοι της βιομηχανικής κατασκοπείας περιορίζονται μόνο από τη φαντασία των κατασκόπων. Ωστόσο, η φυσική κλοπή πληροφοριών είναι πολύ αποτελεσματική και μπορεί να δώσει πληροφορίες στους κατασκόπους, τις οποίες δεν θα ήταν δυνατόν να συλλέξουν με άλλο τρόπο. Θα μπορούσε για παράδειγμα να γίνει κάποιου είδους διάρρηξη σε κτήρια και γραφεία, να ακολουθήσει σύνδεση με καλώδια στους ηλεκτρονικούς υπολογιστές, λήψη αρχείων σε μονάδα flash ή σε δίσκο. Οι κατάσκοποι μπορούν επίσης να χρησιμοποιήσουν τον έλεγχο των απορριμμάτων στα δοχεία απορριμμάτων για να συγκεντρώσουν τις απαραίτητες πληροφορίες. Πολύ συχνά η μέθοδος αυτή δίνει περισσότερες πληροφορίες στους αντιπάλους απ' ότι μπορεί να σκεφτεί ο άνθρωπος που ρίχνει ασυζητητί τα έγγραφα στο κάδο απορριμμάτων.

3.3.3 Σύγχρονες μέθοδοι μέσω του κυβερνοχώρου

Πέρα από τις μεθόδους που αναφέραμε στις προηγούμενες παραγράφους, τα τελευταία χρόνια σημαντικές μέθοδοι για την απόσπαση πληροφοριών τόσο από ιδιώτες όσο και από επιχειρήσεις, που κατ’ επέκταση βοηθούν στην επίτευξη των στόχων της βιομηχανικής κατασκοπείας προέρχονται από τον κυβερνοχώρο. Μεταξύ πολλών άλλων οι πιο σημαντικές είναι:

Phishing

Με τον όρο Phishing (Ηλεκτρονικό Ψάρεμα) αναφερόμαστε στην τεχνική εξαπάτησης χρηστών του διαδικτύου με απώτερο σκοπό την παράνομη πρόσβαση σε ευαίσθητα προσωπικά δεδομένα, όπως πρόσβαση σε αρχεία, κωδικούς και ιδιωτικά στοιχεία. Σε αυτές τις περιπτώσεις ο επιτιθέμενος υποδύεται έναν αξιόπιστο φορέα όπως τράπεζα (Εικόνα 1), υπηρεσία διαχείρισης αρχείων κλπ. και προσελκύει χρήστες μέσω παραπλανητικών email ή μέσω της τεχνικής ανακατεύθυνσης (redirection) ισοτόπων (Βικιπαιδεία, 2020).


Για λόγους ασφαλείας η πιστωτική 5892 - XXXX - XXXX - XXXX έχει αποκλειστεί.
Αν είστε ο ιδιοκτήτης αυτής της πιστωτικής κάρτας, ακολουθήστε τις παρακάτω
σύνδεσμο και να επιβεβαιώσετε τα στοιχεία σας για να ξεκλειδώσετε την κάρτα.

http://www.nbg.gr/wps/portal/!ut/p/c1/04_SB8K8xLLM9MSSzPy8xBz9CP0os3jXIFNnSzcPIw

© 2012 ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Εικόνα 1. Παράδειγμα παραπλανητικού μηνύματος (Phishing) ηλεκτρονικής αλληλογραφίας. (NBG, 2012)

Malware

Ο όρος Malware (Κακόβουλο Λογισμικό) αναφέρεται στην κατηγορία λογισμικών τα οποία ως απώτερο στόχο έχουν να βλάψουν υπολογιστικά συστήματα. Τα κακόβουλα λογισμικά μπορούν είτε να περιέχονται σε άλλα λογισμικά (ξενιστές) είτε να είναι αυθύπαρκτα όπως και άλλα προγράμματα. (Βικιπαιδεία, 2020)

Οι πιο γνωστές κατηγορίες κακόβουλων λογισμικών είναι οι εξής:

- *Ιοί.* Πρόκειται για λογισμικά με την ιδιότητα να εξαπλώνονται γρήγορα στα διάφορα προγράμματα του υπολογιστή και μπορούν να προσβάλουν αρχεία και δεδομένα είτε ακόμα και να καταστρέψουν το σύστημα. (Βικιπαιδεία, 2020)
- *Trojans (Δούρειοι Ίπποι).* Πρόκειται για λογισμικά τα οποία με την προκάλυψη μιας χρήσιμης λειτουργίας εξαπατούν τον χρήστη και καταφέρνουν να υποκλέψουν δεδομένα ή να ανακτήσουν τον έλεγχο του υπολογιστικού συστήματος. (Βικιπαιδεία, 2020)
- *Worms (Σκουλήκια).* Λογισμικά τα οποία διαδίδονται είτε μέσω δικτυακών δομών είτε μέσω ηλεκτρονικού ταχυδρομείου. Πολλαπλασιάζονται αυτόματα εντός του συστήματος στο οποίο διεισδύουν και μεταδίδουν προσωπικά δεδομένα και κωδικούς ενώ ταυτόχρονα υπερφορτώνουν το δίκτυο με εικονική δραστηριότητα. (Βικιπαιδεία, 2020)

Ransomware

Το Ransomware είναι μια μορφή λογισμικού που κλειδώνει τα δεδομένα του χρήστη και απειλεί είτε να διακόψει την οριστική πρόσβαση σε αυτά είτε να τα δημοσιοποιήσει, εκτός αν το θύμα (ιδιώτης ή εταιρεία) καταβάλει λύτρα. Οι εξελιγμένες μορφές Ransomware κρυπτογραφούν τα δεδομένα του θύματος και αποδίδουν τον κωδικό αποκρυπτογράφησης στον χρήστη μόνο μετά την καταβολή των λύτρων που συνήθως γίνεται με κρυπτονομίσματα (Βικιπαιδεία, 2020).

4. Υπολογισμός κόστους και περιπτωσιολογικές μελέτες

4.1 Υπολογισμός κόστους από την εφαρμογή οικονομικής κατασκοπείας

Υπάρχουν αρκετά δεδομένα σχετικά με τις ζημίες που έχει επιφέρει η οικονομική κατασκοπεία ή η κλοπή εμπορικών μυστικών σε μεμονωμένες εταιρείες ή οργανισμούς. Για παράδειγμα, ένας υπάλληλος της Valspar Corporation κατέβαλε παρανόμως τύπους χρωμάτων με συγκεκριμένη άδεια, αξίας 20 εκατομμυρίων δολαρίων, τους οποίους σκόπευε να τους παραχωρήσει στην Κίνα, σύμφωνα με δημοσιεύματα. Αυτή η κλοπή αντιπροσώπευε περίπου το ένα όγδοο των κερδών της Valspar το 2009, το έτος που συνελήφθη ο εργαζόμενος (Office of the National Counterintelligence Executive, 2011).

Ένα παράδειγμα για το ύψος του κόστους σε μια εταιρία, από μια επίθεση οικονομικής κατασκοπείας μέσω του κυβερνοχώρου, αποτελεί η επίθεση από χάκερ στο ευρέως διαδεδομένο λογισμικό ουκρανικής κατασκευής MEDoc το 2017, το οποίο χρησιμοποιείται από πολλές εταιρίες και οργανισμούς παγκοσμίως. Αυτή η επίθεση, η οποία αποδόθηκε στη Ρωσία, παρέλυσε πολλά δίκτυα παγκοσμίως, επηρεάζοντας τις λειτουργίες τραπεζών, επιχειρήσεων και μεταφορών. Ενδεικτικά, το κόστος αυτής της επίθεσης στις εταιρίες FedEx και Maersk εκτιμήθηκε στα 300 εκατομμύρια δολάρια στην καθεμία (National Counterintelligence and Security Center, 2018).

Στην συνέχεια παρατίθενται περεταίρω παραδείγματα οικονομικής κατασκοπείας με την αναφορά του υπολογιζόμενου κόστους που αυτή επέφερε:

- Η Ομοσπονδιακή Υπηρεσία Προστασίας του Συντάγματος της Γερμανίας(BfV) εκτιμά ότι οι γερμανικές εταιρείες χάνουν 28-71 δισεκατομμύρια δολάρια και 30.000-70.000 θέσεις εργασίας ετησίως από την ξένη οικονομική κατασκοπεία. Περίπου το 70% όλων των περιπτώσεων αφορούν άτομα που κατέχουν θέσεις εμπιστοσύνης. (Schiller, 2013)

- Η Νότια Κορέα αναφέρει ότι το κόστος από την ξένη οικονομική κατασκοπεία το 2008 ήταν 82 δισεκατομμύρια δολάρια, έναντι 26 δισεκατομμυρίων δολαρίων το 2004. Οι Νοτιοκορεάτες αναφέρουν ότι το 60% των θυμάτων είναι μικρές και μεσαίες

επιχειρήσεις και ότι το ήμισυ της οικονομικής κατασκοπείας προέρχεται από την Κίνα. (Schiller, 2013)

Οι χώρες αναγνωρίζουν την αυξανόμενη χρήση του διαδικτύου για την άσκηση οικονομικής κατασκοπείας και συχνά παρατηρούν δυσκολίες στην κατανόηση των απωλειών που συνδέονται με αυτές τις μεθόδους συλλογής δεδομένων μέσω του κυβερνοχώρου. Μια έρευνα του 2010 για 200 στελέχη της βιομηχανίας από τους τομείς της ενέργειας, του πετρελαίου, του φυσικού αερίου και των υδάτων σε 12 χώρες της Δύσης, την Κίνα και τη Ρωσία δείχνει ότι το 85% των ερωτηθέντων αντιμετώπισε εισβολές από το δίκτυο και ότι η κυβερνητική δολιοφθορά και κατασκοπεία ήταν η πιο συχνά αναφερόμενη ως απειλή από τον κυβερνοχώρο. (Szabo, 2014) Επίσης:

• Έκθεση της καναδικής κυβέρνησης του 2010 ισχυρίστηκε ότι το 86% των μεγάλων καναδικών εταιρειών έχει πληγεί από την κυβερνητική κατασκοπεία και ότι η κυβερνητική κατασκοπεία κατά του ιδιωτικού τομέα είχε διπλασιαστεί σε δύο χρόνια, σύμφωνα με την έρευνα αυτή. (Szabo, 2014)

• Η γερμανική BfV δεν παρέχει αξιόπιστα στοιχεία σχετικά με τον αριθμό των περιπτώσεων και το ύψος των ζημιών που προκαλεί η οικονομική κατασκοπεία μέσω του κυβερνοχώρου, προσθέτοντας ότι οι υπηρεσίες πληροφοριών τους «χάνονται στο σκοτάδι». Η γερμανική κυβέρνηση υποστηρίζει ότι 99 εκατομμύρια δολάρια δαπανώνται ετησίως για την ασφάλεια στο διαδίκτυο. (Szabo, 2014)

• Οι υπάλληλοι του Ηνωμένου Βασιλείου σημειώνουν ότι το κόστος ενός συμβάντος ασφάλειας πληροφοριών κυμαίνεται μεταξύ 16.000 και 32.000 δολαρίων για μια μικρή επιχείρηση και μεταξύ 1,6 και 3,2 εκατομμυρίων δολαρίων για επιχειρήσεις με περισσότερους από 500 υπαλλήλους. Το Ηνωμένο Βασίλειο εκτιμά ότι οι επιθέσεις σε συστήματα πληροφορικής, συμπεριλαμβανομένης της βιομηχανικής κατασκοπείας και της κλοπής εμπορικών μυστικών της εταιρείας, κοστίζουν στον ιδιωτικό τομέα 34 δισεκατομμύρια δολάρια ετησίως, εκ των οποίων πάνω από το 40% αντιπροσωπεύει κλοπή πνευματικής ιδιοκτησίας, όπως σχέδια, φόρμουλες και εταιρικά μυστικά (Szabo, 2014).

Το Ευρωπαϊκό Κέντρο Διεθνούς Πολιτικής Οικονομίας(ECIPE), περιγράφει σε έκθεσή του για το έγκλημα στον κυβερνοχώρο το οικονομικό αντίκτυπο που προκαλείται από την κλοπή μέσω του κυβερνοχώρου. Αυτό ανέρχεται στα 60 δισεκατομμύρια Ευρώ, ως απώλεια οικονομικής ανάπτυξης της ΕΕ και ως δυνητική απώλεια 289.000 θέσεις εργασίας (European Commission, 2018).

Ακόμη και στις περιπτώσεις όπου μια εταιρεία αναγνωρίζει ότι έχει πέσει θύμα οικονομικής κατασκοπείας και αναφέρει το περιστατικό, ο υπολογισμός των ζημιών αποτελεί σημαντική πρόκληση και μπορεί να προκαλέσει αμφίσημα αποτελέσματα. Μπορούν να

χρησιμοποιηθούν διάφορες μέθοδοι που αποφέρουν διαφορετικές εκτιμήσεις, γεγονός που αυξάνει τη δυσκολία σύγκρισης των υποθέσεων ή της ομαδοποίησης των εκτιμώμενων απωλειών. Για παράδειγμα, ένα διοικητικό στέλεχος από μια μεγάλη βιομηχανική εταιρεία δήλωσε στους εκπρόσωπους της ONCIX(Office of the National Counterintelligence Executive), στα τέλη του 2010, ότι η εταιρεία του χρησιμοποίησε ιστορικά κόστη για την εκτίμηση ζημιών από περιπτώσεις κλοπής των εμπορικών μυστικών της. Αυτή η μέθοδος έχει το πλεονέκτημα ότι χρησιμοποιεί γνωστά και αντικειμενικά δεδομένα, αλλά σε πολλές περιπτώσεις υποτιμά την έκταση των ζημιών, επειδή δεν αποτυπώνει το αποτέλεσμα της απώλειας της πνευματικής ιδιοκτησίας στις μελλοντικές πωλήσεις και τα κέρδη (Office of the National Counterintelligence Executive, 2011).

Επιπλέον, στις περιπτώσεις αμερικανικών αστικών υποθέσεων που αφορούν την κλοπή εμπορικών μυστικών, η ζημία υπολογίζεται μετρώντας τα «χαμένα κέρδη» ή τα «εύλογα δικαιώματα» που μια εταιρεία δεν είναι σε θέση να κερδίσει λόγω της υφιστάμενης κλοπής. Παρόλο που αυτή η μέθοδος απαιτεί υποκειμενικές υποθέσεις σχετικά με το μερίδιο αγοράς, την κερδοφορία και παρόμοιους παράγοντες, προσφέρει έναν πληρέστερο υπολογισμό του κόστους από το να βασίζεται κανείς αποκλειστικά στα ιστορικά λογιστικά στοιχεία. Οι εκτιμήσεις από την ακαδημαϊκή βιβλιογραφία σχετικά με τις απώλειες από την οικονομική κατασκοπεία κυμαίνονται τόσο πολύ, ώστε να μην υπάρχει πραγματικό νόημα στον υπολογισμό του. Ενδεικτικά αναφέρεται το εύρος, το οποίο κυμαίνεται μεταξύ 2 έως 400 δισεκατομμύρια δολάρια ή περισσότερο το χρόνο, γεγονός που αντικατοπτρίζει την έλλειψη δεδομένων και την ποικιλία των μεθόδων που χρησιμοποιούνται για τον υπολογισμό των απωλειών (Office of the National Counterintelligence Executive, 2011).

4.2 Περιπτωσιολογικές μελέτες οικονομικής κατασκοπείας

4.2.1 Η περίπτωση της οικονομικής κατασκοπείας μεταξύ της Κίνας και των ΗΠΑ, τα τελευταία χρόνια

Οι κινέζοι ηγέτες θεωρούν τις πρώτες δύο δεκαετίες του 21ου αιώνα ως ένα παράθυρο στρατηγικής ευκαιρίας για τη χώρα τους να επικεντρωθεί στην οικονομική ανάπτυξη, την ανεξάρτητη καινοτομία, την επιστημονική και τεχνολογική πρόοδο και την ανάπτυξη του τομέα των ανανεώσιμων πηγών ενέργειας. Οι υπηρεσίες πληροφοριών της Κίνας, καθώς και πολλές ιδιωτικές εταιρείες και άλλες οντότητες, συχνά επιδιώκουν να εκμεταλλευτούν κινέζους πολίτες ή άτομα που έχουν οικογενειακούς δεσμούς με την Κίνα και μπορούν να χρησιμοποιήσουν την εμπιστευτική τους πρόσβαση σε εταιρικά δίκτυα των ΗΠΑ για να κλέψουν εμπορικά μυστικά χρησιμοποιώντας αφαιρούμενες συσκευές πολυμέσων ή ηλεκτρονικό ταχυδρομείο. Αξίζει να σημειωθεί ότι από τις επτά υποθέσεις που εκδόθηκαν βάσει του νόμου περί οικονομικής κατασκοπείας κατά το οικονομικό έτος 2010, οι έξι

αφορούσαν μια σύνδεση με την Κίνα (Office of the National Counterintelligence Executive, 2011).

Οι αμερικανικές εταιρείες και οι ειδικοί στον τομέα της ασφάλειας στον κυβερνοχώρο ανέφεραν επίσης μια επίθεση διαρροών δικτύων ηλεκτρονικών υπολογιστών που προέρχονται από διευθύνσεις πρωτοκόλλου Internet (IP) στην Κίνα, οι οποίοι ειδικοί του ιδιωτικού τομέα αποκαλούν «προηγμένες συνεχιζόμενες απειλές». Ορισμένες από αυτές τις αναφορές κατέδειξαν έναν κινεζικό εταιρικό ή κυβερνητικό ανάδοχο σε κάθε τέτοια δραστηριότητα, αλλά η επίσημη υπηρεσία των Η.Π.Α. δεν μπόρεσε να αποδώσει πολλές από αυτές τις παραβιάσεις δεδομένων ιδιωτικού τομέα σε έναν κρατικό χορηγό. Η αναφορά είναι ιδιαίτερα δύσκολο να εξακριβωθεί, ειδικά όταν το συμβάν εμφανίζεται εβδομάδες ή μήνες πριν τα θύματα της οικονομικής κατασκοπείας ζητήσουν βοήθεια από τις αρμόδιες υπηρεσίες (Office of the National Counterintelligence Executive, 2011).

Σε μια μελέτη του Φεβρουαρίου 2011, η McAfee απέδωσε ένα πακέτο εισβολής με την ονομασία "Night Dragon" σε μια διεύθυνση IP που βρίσκεται στην Κίνα και ανέφερε ότι οι εισβολείς είχαν αποκαλύψει δεδομένα από τα συστήματα πληροφορικής των πολυεθνικών πετρελαϊκών, ενεργειακών και πετροχημικών εταιρειών. Από τον Νοέμβριο του 2009, οι υπάλληλοι των στοχευόμενων εταιρειών υποβλήθηκαν σε εξονυχιστικούς ελέγχους από τους εισβολείς. Ο στόχος των εισβολέων ήταν να αποκτήσουν πληροφορίες σχετικά με ευαίσθητες ανταγωνιστικές ιδιόκτητες δραστηριότητες και τη χρηματοδότηση προσφορών και λειτουργιών στο πεδίο του πετρελαίου και του φυσικού αερίου (Office of the National Counterintelligence Executive, 2011).

Επιπλέον, τον Ιανουάριο του 2010, η VeriSign iDefense προσδιόρισε την κινεζική κυβέρνηση ως χορηγό εισβολών στα δίκτυα της Google. Στη συνέχεια, η Google υπέβαλε κατηγορίες ότι ο πηγαίος κώδικάς της είχε υποκλαπεί, μια κατηγορία που το Πεκίνο συνεχίζει να αρνείται. Επιπρόσθετα, η Mandiant ανέφερε το 2010 ότι οι πληροφορίες απορρίφθηκαν από τα εταιρικά δίκτυα μιας αμερικανικής κατασκευαστικής εταιρίας που ανήκει στην λίστα του Fortune 500, κατά τη διάρκεια επιχειρηματικών διαπραγματεύσεων στις οποίες την εν λόγω εταιρεία επιθυμούσε να αποκτήσει μια κινεζική εταιρεία. Η έκθεση της Mandiant ανέφερε ότι η κατασκευαστική εταιρεία των ΗΠΑ απώλεσε ευαίσθητα δεδομένα σε εβδομαδιαία βάση και ότι αυτό ίσως βοήθησε την κινεζική επιχείρηση να επιτύχει καλύτερη διαπραγματευτική και τιμολογιακή θέση. Οι συμμετέχοντες σε μια διάσκεψη της ONCIX τον Νοέμβριο του 2010, ανέφεραν ότι προέρχονται από εταιρικά δίκτυα αμερικανικών βιομηχανιών του ιδιωτικού τομέα - κυρίως εκείνων που συνεργάζονται με την Κίνα - λίστες πελατών, στοιχεία συγχωνεύσεων και εξαγορών, και πληροφορίες σχετικά με την τιμολόγηση και οικονομικά στοιχεία (Office of the National Counterintelligence Executive, 2011). Τον Νοέμβριο του 2017, οι Wu Yingzhuo, Dong Hao και Xia Lei, Κινέζοι υπήκοοι και κάτοικοι της Κίνας, κατηγορήθηκαν για ηλεκτρονική πειρατεία, κλοπή εμπορικών μυστικών, συνωμοσία και κλοπή ταυτότητας. Αυτές οι προσπάθειες απευθύνονταν σε Αμερικανούς και ξένους

υπαλλήλους καθώς και στους υπολογιστές τριών εταιρειών που υπήρξαν θύματα οικονομικών, μηχανικών και τεχνολογικών βιομηχανιών μεταξύ 2011 και 2017 (National Counterintelligence and Security Center, 2018).

Η κοινότητα των υπηρεσιών πληροφοριών και οι εμπειρογνώμονες του ιδιωτικού τομέα συνεχίζουν να παρατηρούν κινεζική δραστηριότητα στον κυβερνοχώρο, αν και σε χαμηλότερα επίπεδα απ' ότι παρατηρούνταν πριν από τις διμερείς δεσμεύσεις περί κυβερνοχώρου μεταξύ ΗΠΑ – Κίνας τον Σεπτέμβριο του 2015. Οι περισσότερες κινεζικές επιχειρήσεις στον κυβερνοχώρο που εντοπίζονται εναντίων της ιδιωτικής βιομηχανίας των ΗΠΑ επικεντρώνονται σε τομείς της άμυνας ή σε τομείς πληροφορικής και επικοινωνιών, τα προϊόντα και οι υπηρεσίες των οποίων υποστηρίζουν δίκτυα δημόσιου και ιδιωτικού τομέα παγκοσμίως (National Counterintelligence and Security Center, 2018).

4.2.2 Η περίπτωση της οικονομικής κατασκοπείας μεταξύ της Ρωσίας και των ΗΠΑ, τα τελευταία χρόνια

Με βάση την υψηλή εξάρτηση της Ρωσίας από τους φυσικούς πόρους, την ανάγκη διαφοροποίησης της οικονομίας της και την πεποίθηση ότι το παγκόσμιο οικονομικό σύστημα είναι στραμμένο προς τα αμερικανικά και άλλα δυτικά συμφέροντα εις βάρος της Ρωσίας, οι εξαιρετικά ικανές υπηρεσίες πληροφοριών της Μόσχας χρησιμοποιούν την οικονομική κατασκοπεία και οργανώνουν πολλές επιχειρήσεις συλλογής οικονομικών πληροφοριών και τεχνολογίας για την υποστήριξη της οικονομικής ανάπτυξης και της ασφάλειας της Ρωσίας. Για παράδειγμα, οι 10 Ρώσοι ξένοι υπάλληλοι που συνελήφθησαν τον Ιούνιο του 2010 στις ΗΠΑ είχαν την εντολή να συλλέξουν οικονομικές και τεχνολογικές πληροφορίες, υπογραμμίζοντας τη σημασία αυτών των ζητημάτων στη Μόσχα. Ενδεικτικά, αναφέρεται ο επόμενος πίνακας, ο οποίος παρέχει στοιχεία σχετικά με περιπτώσεις οικονομικής κατασκοπείας με στόχο τις ΗΠΑ (Office of the National Counterintelligence Executive, 2011).

Η πλέον διαδεδομένη μέθοδος που χρησιμοποιεί η Ρωσία για να αποκτήσει τεχνογνωσία και να εξελιχθεί η οικονομία της είναι η χρήση του κυβερνοχώρου. Άλλες μέθοδοι είναι η χρήση ρωσικών και ακαδημαϊκών επιχειρήσεων που αλληλοεπιδρούν με αντίστοιχες δυτικές, η στρατολόγηση Ρώσων μεταναστών, οι οποίοι εκπαιδεύονται από τις μυστικές υπηρεσίες της Ρωσίας και η εισβολή τους σε δημόσιες ή ιδιωτικές επιχειρήσεις με σκοπό να αποκτήσουν πληροφορίες και τεχνογνωσία (National Counterintelligence and Security Center, 2018).

Το 2016, η χάκερ "Eas7" εμπιστεύτηκε στον δυτικό τύπο ότι συνεργάστηκε με τη Ρωσική Ομοσπονδιακή Υπηρεσία Ασφαλείας (FSB) σε αποστολές οικονομικής κατασκοπείας. Εκτίμησε ότι "μεταξύ των καλών χάκερ, τουλάχιστον οι μισοί δουλεύουν για την κυβέρνηση", υποδεικνύοντας ότι η Μόσχα απασχολεί εγκληματίες του κυβερνοχώρου ώστε να καταστήσουν αυτές τις επιχειρήσεις εύλογα αμφισβητήσιμες (National Counterintelligence and Security Center, 2018).

Τον Μάρτιο του 2017, το υπουργείο δικαιοσύνης των ΗΠΑ καταδίκασε δύο αξιωματούχους της FSB και τους Ρώσους χάκερ-υπαλλήλους τους, κατηγορώντας τους για ηλεκτρονική πειρατεία και συνωμοσία μέσω της συλλογής ηλεκτρονικών μηνυμάτων των Αμερικανών και ευρωπαίων εργαζομένων σε επιχειρήσεις μεταφορών και χρηματοπιστωτικών υπηρεσιών. Οι κατηγορίες περιλάμβαναν τη συνωμοσία για εμπλοκή σε επιχειρήσεις οικονομικής κατασκοπείας και την κλοπή εμπορικών μυστικών (National Counterintelligence and Security Center, 2018).

4.2.3 Η περίπτωση της οικονομικής κατασκοπείας μεταξύ του Ιράν και των ΗΠΑ, τα τελευταία χρόνια

Παρόλο που οι δραστηριότητες οικονομικής κατασκοπείας του Ιράν είναι επικεντρωμένες κατά κύριο λόγο στη Μέση Ανατολή, με θύματα χώρες όπως η Σαουδική Αραβία και το Ισραήλ, το 2017 το Ιράν στοχοποίησε σε πολλές περιπτώσεις δίκτυα των ΗΠΑ, γεγονός που ανησύχησε ιδιαίτερα τις μυστικές τους υπηρεσίες. Η απώλεια ευαίσθητων πληροφοριών και τεχνολογιών αποτελεί σημαντική απειλή για την εθνική ασφάλεια των ΗΠΑ, ενώ ταυτόχρονα παρέχει την δυνατότητα στο Ιράν να αναπτύξει προηγμένες τεχνολογίες για την τόνωση της εγχώριας οικονομικής ανάπτυξης, τον εκσυγχρονισμό των στρατιωτικών της δυνάμεων και την αύξηση των πωλήσεων στο εξωτερικό (National Counterintelligence and Security Center, 2018).

Η μέθοδος οικονομικής κατασκοπείας που χρησιμοποιήθηκε κυρίως είναι η κυβερνοκατασκοπεία. Ομάδες χάκερ ιρανικής καταγωγής στοχοποίησαν αμερικανικές εταιρίες που δραστηριοποιούνται στον τομέα της άμυνας, με απώτερο σκοπό να υποβοηθήσουν την Τεχεράνη να βελτιώσει τα ήδη ισχυρά πυραυλικά και διαστημικά της προγράμματα. Επίσης, θύματα αποτέλεσαν αμερικανικές εταιρίες αεροναυπηγικής, εταιρίες πολιτικής αεροπορίας, οικονομικά και ακαδημαϊκά ινστιτούτα και εταιρίες που δραστηριοποιούνται στον ενεργειακό τομέα, ώστε να βοηθηθεί η πετροχημική παραγωγή και τεχνολογία του Ιράν (National Counterintelligence and Security Center, 2018).

Τον Ιούλιο του 2017, οι Ιρανοί υπήκοοι Mohammed Reza Rezakhah και Mohammed Saeed Ajily κατηγορήθηκαν για κλοπή λογισμικού από αμερικανικές εταιρίες παραγωγής λογισμικού, πουλώντας το σε ιρανικά πανεπιστήμια, στρατιωτικούς και κυβερνητικούς φορείς και άλλους αγοραστές εκτός των ΗΠΑ (National Counterintelligence and Security Center, 2018).

Τον Μάρτιο του 2018, εννέα Ιρανοί χάκερ που συσχετίστηκαν με το ινστιτούτο Mabna, το οποίο δραστηριοποιείται στην παραγωγή λογισμικού και εξαρτημάτων Η/Υ και τηλεπικοινωνιών, κατηγορήθηκαν για κλοπή πνευματικής ιδιοκτησίας από περισσότερα από 144 πανεπιστήμια των ΗΠΑ, τα οποία δαπάνησαν περίπου 3,4 δισεκατομμύρια δολάρια για να προμηθευτούν και να έχουν πρόσβαση στα δεδομένα που κλάπηκαν. Τα δεδομένα αυτά χρησιμοποιήθηκαν προς όφελος της κυβέρνησης του Ιράν και των ιρανικών πανεπιστημίων.

Οι συντελεστές του ινστιτούτου Mabna στόχευσαν και παραβίασαν 36 επιχειρήσεις στις ΗΠΑ (National Counterintelligence and Security Center, 2018).

4.2.4 Περιπτώσεις συνεργασίας του κράτους με την υφιστάμενη εταιρία-δρώντα

Υπάρχουν περιπτώσεις όπου εταιρίες τεχνολογίας πληροφοριών και επικοινωνιών ασκούν οικονομική κατασκοπεία υπό την επιρροή του κράτους. Οι εταιρίες αυτές παρέχουν πολύτιμες πληροφορίες στα κράτη τους με την παροχή πρόσβασης στους υπολογιστές και στα δίκτυά τους. Αυτή η πρόσβαση παρέχει τη δυνατότητα στα κράτη να αποκτήσουν ευαίσθητες πληροφορίες ιδιοκτησίας. Παρακάτω παραθέτουμε κάποια παραδείγματα στα οποία απεικονίζονται οι κίνδυνοι που θέτει η συνεργασία μίας τεχνολογικής εταιρίας με το ομώνυμο κράτος, το οποίο συχνά διαθέτει μυστικές υπηρεσίες υψηλής απειλής (National Counterintelligence and Security Center, 2018).

Πρόσφατες αλλαγές στο νομοθετικό πλαίσιο της Κίνας, συμπεριλαμβανομένων των νόμων για την εθνική ασφάλεια και την ασφάλεια στον κυβερνοχώρο, παρέχουν στο Πεκίνο την νομική βάση για να αναγκάσουν τις εταιρείες τεχνολογίας που δραστηριοποιούνται στην Κίνα να συνεργαστούν με τις κινεζικές υπηρεσίες ασφαλείας (National Counterintelligence and Security Center, 2018).

Τον Σεπτέμβριο του 2017, το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ έδωσε οδηγία στις ομοσπονδιακές υπηρεσίες της να καταργήσουν τα προϊόντα της εταιρίας Kaspersky, λόγω των κινδύνων που διέπουν οι δεσμοί της εταιρίας με τη Ρωσία (National Counterintelligence and Security Center, 2018).

Τον Δεκέμβριο του 2017, το Υπουργείο Δικαιοσύνης των ΗΠΑ δημοσιοποίησε την συμφωνία με την εταιρεία Netcracker Technology, η οποία απέβλεπε στην απαγόρευση αποθήκευσης ευαίσθητων πληροφοριών και δεδομένων από πελάτες, με βάσεις οι οποίες εδρεύουν στις ΗΠΑ και έχουν οποιαδήποτε σύνδεση με την Ρωσία (National Counterintelligence and Security Center, 2018).

5. Ανάλυση της επίδρασης των απειλών κυβερνοασφάλειας

5.1 Στατιστική Ανάλυση

Στη παρούσα μελέτη έγινε ανάλυση συσχέτισης μεταξύ του πλήθους των πιο συχνών παραβιάσεων κυβερνοασφάλειας καθώς και των οικονομικών απωλειών που είχαν αυτές ως συνέπεια με το ποσό που δαπανάται ετησίως στις ΗΠΑ σε ηλεκτρονικές αγορές καθώς και το ποσοστό που αποτελούν οι τελευταίες ως προς το συνολικό ποσό αγορών. Τα δεδομένα για συχνές παραβιάσεις κυβερνοασφάλειας και τις αντίστοιχες παραβιάσεις αντλήθηκαν από τις σχετικές αναφορές του FBI (FBI IC3, 2001-2019), ενώ τα δεδομένα για τα ποσά που δαπανήθηκαν σε ηλεκτρονικές αγορές καθώς και το ποσοστό που αυτά αποτελούν σε σχέση με το σύνολο των αγορών στις ΗΠΑ αντλήθηκαν από την ιστοσελίδα στατιστικών του υπουργείου εμπορίου των ΗΠΑ (US Census Bureau, 2001-2019).

Για τα δεδομένα μας, αρχικά έγινε έλεγχος κανονικότητας. Λόγω του μικρού μεγέθους του δείγματος ο έλεγχος κανονικότητας πραγματοποιήθηκε με το Shapiro-Wilk test. Το γεγονός ότι τα δεδομένα μας δεν ακολουθούν κανονική κατανομή καθώς και ότι το δείγμα είναι μικρό μας οδήγησε στο να πραγματοποιήσουμε την ανάλυση συσχέτισης με χρήση του συντελεστή ρ του Spearman. Όλες οι αναλύσεις πραγματοποιήθηκαν με χρήση του λογισμικού στατιστικής ανάλυσης SPSS V.23.

5.2 Ανάλυση Συσχέτισης

Αρχικά μελετήθηκε η συσχέτιση μεταξύ του πλήθους αναφερόμενων περιστατικών κακόβουλου λογισμικού και του κόστους που είχαν αυτές οι παραβιάσεις ασφάλειας με τα ποσά που δαπανώνται στις ΗΠΑ μέσω ηλεκτρονικών αγορών και του αντίστοιχου ποσοστού των ποσών αυτών ως προς τα συνολικά ποσοστά που δαπανώνται στις ΗΠΑ.

Η ανάλυση συσχέτισης καταδεικνύει ότι υπάρχει μέτρια συσχέτιση ανάμεσα στα ποσά που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ και του κόστους που είχαν παραβιάσεις ασφάλειας μέσω κακόβουλου λογισμικού. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 ($\rho(4) = 0.429$, $p = 0.397$).

Παράλληλα εμφανίζεται μηδενική συσχέτιση ανάμεσα στα ποσά που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ και στο πλήθος των παραβιάσεων ασφάλειας μέσω

κακόβουλου λογισμικού. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = 0.029, p = 0.957).

Αντίστοιχα με τις δύο προηγούμενες περιπτώσεις, η ανάλυση συσχέτισης καταδεικνύει ότι υπάρχει μέτρια συσχέτιση ανάμεσα στο ποσοστό των ποσών που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ ως προς το συνολικό ποσό αγορών και του κόστους που είχαν παραβιάσεις ασφάλειας μέσω κακόβουλου λογισμικού. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = 0.429, p = 0.397).

Τέλος, εμφανίζεται μηδενική συσχέτιση ανάμεσα στο ποσοστό των ποσών που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ ως προς το συνολικό ποσό αγορών και στο πλήθος των παραβιάσεων ασφάλειας μέσω κακόβουλου λογισμικού. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = 0.029, p = 0.957).

Αυτή η έλλειψη συσχέτισης θα μπορούσε να ερμηνευτεί από το γεγονός ότι όπως αναφέραμε νωρίτερα, η ύπαρξη κακόβουλων λογισμικών δεν σχετίζεται απαραίτητα με την διαρροή προσωπικών δεδομένων και κατ' επέκταση με σχετική οικονομική ζημιά.

Στην συνέχεια εξετάστηκε η συσχέτιση μεταξύ του πλήθους αναφερόμενων περιστατικών διαρροής στοιχείων πιστωτικής κάρτας και του κόστους που είχαν αυτές οι παραβιάσεις ασφάλειας με τα ποσά που δαπανώνται στις ΗΠΑ μέσω ηλεκτρονικών αγορών και του αντίστοιχου ποσοστού των ποσών αυτών ως προς τα συνολικά ποσοστά που δαπανώνται στις ΗΠΑ.

Η ανάλυση συσχέτισης υποδεικνύει ότι υπάρχει ισχυρή συσχέτιση ανάμεσα στα ποσά που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ καθώς και του ποσοστού που αποτελούν αυτές σε σχέση με το σύνολο των αγορών, με το κόστος που είχαν παραβιάσεις ασφάλειας μέσω διαρροής στοιχείων πιστωτικών καρτών. Η συσχέτιση αυτή είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = 0.99, p = 0.00).

Κατόπιν μελετήθηκε η συσχέτιση μεταξύ των αναφερόμενων περιστατικών phishing και του κόστους που είχαν αυτές οι παραβιάσεις ασφάλειας με τα ποσά που δαπανώνται στις ΗΠΑ μέσω ηλεκτρονικών αγορών και του αντίστοιχου ποσοστού των ποσών αυτών ως προς τα συνολικά ποσοστά που δαπανώνται στις ΗΠΑ.

Η εφαρμογή της ανάλυσης συσχέτισης καταδεικνύει ότι υπάρχει ισχυρή συσχέτιση ανάμεσα στα ποσά που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ καθώς και του ποσοστού που αποτελούν αυτές σε σχέση με το σύνολο των αγορών, με το κόστους που είχαν παραβιάσεις ασφάλειας μέσω Phising. Η συσχέτιση αυτή είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = 0.949, p = 0.005).

Τέλος, διερευνήθηκε η συσχέτιση μεταξύ των αναφερόμενων περιστατικών παραβίασης ασφάλειας μέσω Ransomware και του κόστους που είχαν αυτές οι παραβιάσεις ασφάλειας με τα ποσά που δαπανώνται στις ΗΠΑ μέσω ηλεκτρονικών αγορών και του αντίστοιχου ποσοστού των ποσών αυτών ως προς τα συνολικά ποσοστά που δαπανώνται στις ΗΠΑ.

Η ανάλυση συσχέτισης υποδεικνύει μέτρια αρνητική συσχέτιση ανάμεσα στα ποσά που δαπανούνται σε ηλεκτρονικές αγορές στις ΗΠΑ, με το κόστος που είχαν παραβιάσεις ασφάλειας μέσω ransomware. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = -0.484, p = 0.224).

Παράλληλα, η ανάλυση συσχέτισης υποδεικνύει μέτρια αρνητική συσχέτιση ανάμεσα στο ποσοστό που αποτελούν οι ηλεκτρονικές σε σχέση με το σύνολο των αγορών, με το κόστους που είχαν παραβιάσεις ασφάλειας μέσω ransomware. Η συσχέτιση αυτή δεν είναι στατιστικά σημαντική σε επίπεδο σημαντικότητας 0,05 (ρ(4) = -0.469, p = 0.241).

Αυτή η απουσία σημαντικής συσχέτισης θα μπορούσε να ερμηνευτεί από το γεγονός ότι όπως αναφέραμε νωρίτερα, η παραβίαση ασφάλειας μέσω Ransomware είναι ουσιαστικά μια πράξη ψηφιακού εκβιασμού που δεν σχετίζεται απαραίτητα με την πραγματοποίηση ηλεκτρονικών αγορών και η ύπαρξη κακόβουλων λογισμικών δεν σχετίζεται απαραίτητα με την διαρροή προσωπικών δεδομένων και κατ' επέκταση με σχετική οικονομική ζημιά.

5.3 Ανάλυση Παλινδρόμησης

Για τα ζεύγη δεδομένων που παρουσιάστηκαν στην προηγούμενη παράγραφο και εμφανίζουν ισχυρή συσχέτιση, στατιστικά σημαντική, πραγματοποιήθηκε ανάλυση παλινδρόμησης ώστε να δημιουργηθεί το αντίστοιχο γραμμικό μοντέλο πρόβλεψης. Πιο συγκεκριμένα, σε όλες τις γραμμικές παλινδρομήσεις που θα παρατεθούν θα θεωρηθεί ως ανεξάρτητη μεταβλητή το ποσοστό που αποτελούν οι ηλεκτρονικές σε σχέση με το σύνολο των αγορών που πραγματοποιούνται στις ΗΠΑ, ενώ ως εξαρτημένη το ποσό απωλειών σε δολάρια για τις παραβιάσεις ασφάλειας λόγω διαρροής στοιχείων πιστωτικών καρτών και το ποσό απωλειών σε δολάρια για τις παραβιάσεις ασφαλείας λόγω Phishing.

Η εφαρμογή για την ανάλυση παλινδρόμησης στην περίπτωση παραβιάσεων ασφαλείας με διαρροή στοιχείων πιστωτικής κάρτας δίνει το ακόλουθο μοντέλο

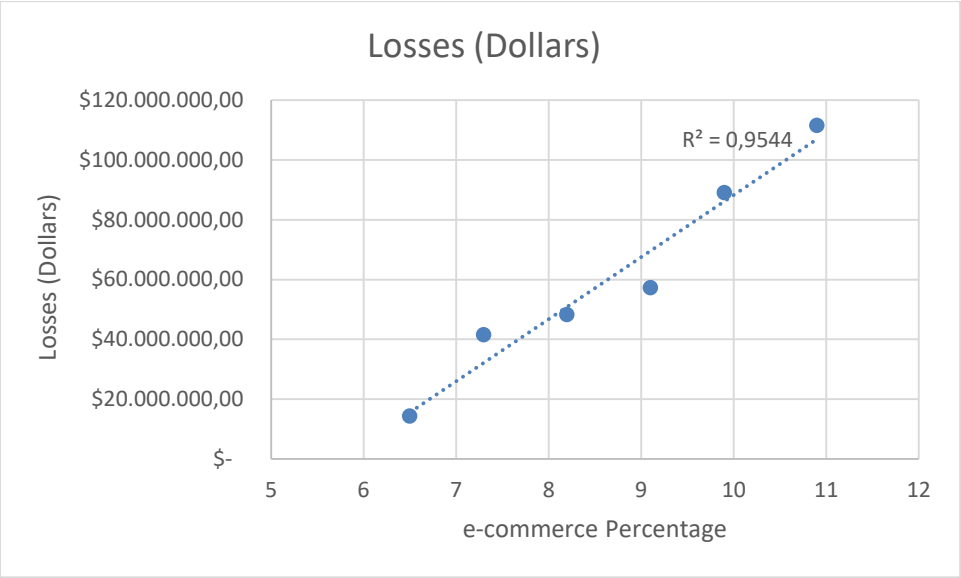
$$y = 119158523{,}53 + 20743148{,}79 * x \qquad \{1\}$$

Όπου:

y: ποσό απωλειών σε δολάρια

x: ποσοστό που αποτελούν οι ηλεκτρονικές αγορές σε σχέση με το σύνολο των αγορών

Στο μοντέλο που προέκυψε ο συντελεστής της ανεξάρτητης μεταβλητής $(20743148{,}79)$ δηλώνει ότι η αύξηση του ποσοστού ηλεκτρονικών αγορών κατά μια μονάδα θα προκαλέσει αύξηση των απωλειών λόγω παραβίασης ασφάλειας με διαρροή στοιχείων κάρτας κατά $20743148{,}79\$$.



Διάγραμμα 1. Διάγραμμα διασποράς και ευθεία παλινδρόμησης ποσοστού ηλεκτρονικών αγορών με τις απώλειες από την παραβίαση ασφάλειας λόγω διαρροής στοιχείων πιστωτικών καρτών

Η ποιότητα του μοντέλου καθορίζεται από τον συντελεστή προσδιορισμού R2. Στην περίπτωσή μας το μοντέλο παρουσιάζει συντελεστή προσδιορισμού R2=0,954, γεγονός που σημαίνει ότι το 95,4% της μεταβλητότητας της μεταβλητής y ερμηνεύεται σωστά από το μοντέλο παλινδρόμησης.

Παράλληλα, η εφαρμογή για την ανάλυση παλινδρόμησης στην περίπτωση παραβιάσεων ασφαλείας με ηλεκτρονικό ψάρεμα δίνει το ακόλουθο μοντέλο:

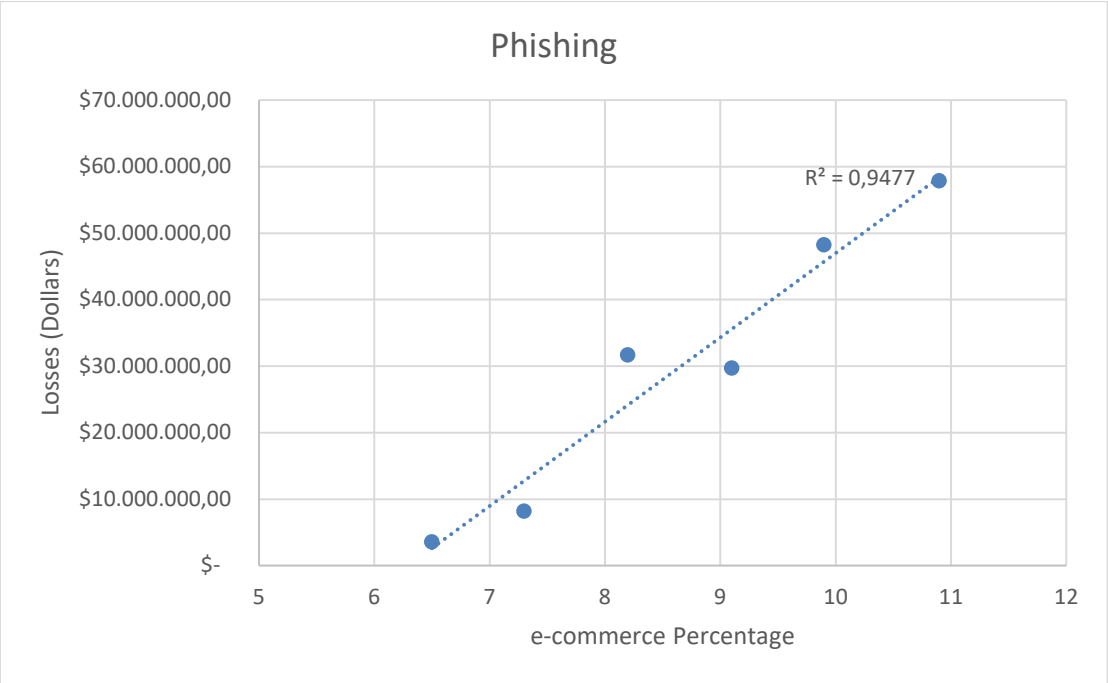
$$y = -79810784{,}64 + 12679390{,}26 * x$$

Όπου:

y: ποσό απωλειών σε δολάρια

x: ποσοστό που αποτελούν οι ηλεκτρονικές αγορές σε σχέση με το σύνολο των αγορών

Στο μοντέλο που προέκυψε, ο συντελεστής της ανεξάρτητης μεταβλητής (12679390,26) δηλώνει ότι η αύξηση του ποσοστού ηλεκτρονικών αγορών κατά μια μονάδα θα προκαλέσει αύξηση των απωλειών λόγω παραβίασης ασφάλειας με ηλεκτρονικό ψάρεμα κατά 12679390,26$.



Διάγραμμα 2. Διάγραμμα διασποράς και ευθεία παλινδρόμησης ποσοστού ηλεκτρονικών αγορών με τις απώλειες από την παραβίαση ασφάλειας λόγω ηλεκτρονικού ψαρέματος

Στην περίπτωσή αυτή το μοντέλο παρουσιάζει συντελεστή προσδιορισμού R2=0,948, γεγονός που σημαίνει ότι το 94,8% της μεταβλητότητας της μεταβλητής y ερμηνεύεται σωστά από το μοντέλο παλινδρόμησης.

6. Συμπεράσματα

Από την μελέτη και την ανάλυση που προηγήθηκε στα προηγούμενα κεφάλαια, γίνεται αντιληπτό πως τα κράτη επιδιώκουν την επικράτηση και κυριαρχία τους στη διεθνή πολιτική και οικονομική σκηνή. Μάλιστα, χρησιμοποιούν οικονομικά μέσα προκειμένου να ασκήσουν πίεση και να φτάσουν στην επίτευξη των στόχων τους. Σημαντικό μέσο βοήθειας για την επίτευξη αυτού του στόχου είναι η οικονομική κατασκοπεία, παρόλο που καμία παραδοχή για τη χρήση της δεν αναφέρεται. Η οικονομική κατασκοπεία διαδραματίζει έναν συνεχώς αυξανόμενο και σημαντικό ρόλο στις διεθνείς σχέσεις και οι περιπτώσεις οικονομικής κατασκοπείας θα αυξάνονται με γεωμετρική ακρίβεια από την στιγμή που ο ανταγωνισμός παραμένει σε οικονομικό επίπεδο και δεν προχωρά σε στρατιωτικό.

Η σύνδεσή της με τις πληροφορίες και τις νέες τεχνολογίες δημιουργεί ένα νέο πεδίο δράσης στα κράτη και τις επιχειρήσεις. Η ανάγκη για οικονομικές και τεχνολογικές πληροφορίες οδηγεί τόσο τα κράτη, όσο και τις ανταγωνιστικές μεταξύ τους επιχειρήσεις στην υποκλοπή οικονομικών και τεχνολογικών στοιχείων. Τα στοιχεία αυτά δίνουν ανταγωνιστικό πλεονέκτημα στα κράτη για να γνωρίζουν τις κόκκινες γραμμές πριν ξεκινήσουν οποιαδήποτε διαπραγμάτευση. Ενώ σε επίπεδο επιχειρήσεων, η υποκλοπή τεχνολογίας σηματοδοτεί την εξοικονόμηση πόρων από τα κεφάλαια της έρευνας και της ανάπτυξης.

Η βιομηχανική κατασκοπεία είναι μια μέθοδος που χρησιμοποιείται σε όλη την ιστορία της ανθρωπότητας, όμως μετά το πέρας του Ψυχρού Πολέμου και της νέας καπιταλιστικής λογικής που επικράτησε μετέπειτα, η μέθοδος αυτή έχει γνωρίσει ραγδαία εξέλιξη. Σε αυτή την εξέλιξη έχει συμβάλει καθοριστικά η ανάπτυξη του διαδικτύου και πιο συγκεκριμένα η χρήση των μεθόδων βιομηχανικής κατασκοπείας μέσω του κυβερνοχώρου. Καθώς 26 δισεκατομμύρια προσωπικές συσκευές, επιχειρηματικοί και βιομηχανικοί εξοπλισμοί πρόκειται να συνδεθούν ως απόρροια του ίντερνετ των πραγμάτων και της τέταρτης βιομηχανικής επανάστασης, το πεδίο δράσης που διατίθεται για τους ανταγωνιστές ενισχύεται, ενθαρρύνοντας τον πολλαπλασιασμό και την εξέλιξη των μέσων και των τεχνικών για την εκπλήρωση των εισβολών στον κυβερνοχώρο.

Τέλος, αξίζει να σημειωθεί πως ο τομέας της πληροφόρησης παρουσιάζει μεγάλο ενδιαφέρον, ενώ ιδιαίτερα χρήσιμη θα ήταν και η περαιτέρω ανάπτυξή του στην Ελλάδα. Η βιβλιογραφία που υπάρχει ωστόσο, κάθε άλλο παρά επαρκής είναι, ιδιαίτερα μάλιστα σε ότι αφορά τις περιπτώσεις της βιομηχανικής κατασκοπείας, οι οποίες δεν αναφέρονται όχι γιατί

δεν υπάρχουν, αλλά απλούστατα επειδή δεν δίνεται η απαιτούμενη βαρύτητα σε επίπεδο ανάλυσης.

Κατάλογος πηγών

Baheri, Z., Fard, S. (2015) Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations, Journal of Scientific Research and Development, 2 (1) 41-45.

Baker, D. (2003) Tolerance of International Espionage: A Functional Approach, American University International Law Review, 19 (5) 1091-1113.

Bitton, R. (2014) The Legitimacy of Spying Among Nations, American University International Law Review, 29 (5) 1009-1070.

Bosco, D. (2012) Espionage in international organizations, Brussels: Foreign Policy.

Button, M. (2015) Industrial espionage and information security, Διαθέσιμο στη δ/νση http://ecis2018.eu/wp-content/uploads/2018/05/Industrial-espionage-and-information-security.pdf. Πρόσβαση: 13/8/2019

Calder, A., Watkins, S. (2006) International IT Governance, London: Kogan Page.

Duffy, M., Burge, T. (2003) NOC, NOC. Who's There? A Special Kind of Agent, Διαθέσιμο στη δ/νση http://content.time.com/time/magazine/article/0,9171,524486,00.html. Πρόσβαση: 5/8/2019

European Commission (2018) The scale and impact of industrial espionage and theft of trade secret through cyber, Διαθέσιμο στη δ/νση https://publications.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-90181868. Πρόσβαση: 14/8/2019

Evans, JC. (1995) US Business Competitiveness and the Intelligence Community, International Journal of Intelligence and Counterintelligence, Vol. 7, No 3

FBI IC3 – Federal Bureau of Investigation Internet Crime Complaint Center (2001-2019), Διαθέσιμο στη δ/νση https://www.ic3.gov/default.aspx. Πρόσβαση: 15/5/2020

Gilpin, R. (1995) Η πολιτική οικονομία των διεθνών σχέσεων, Α' Τόμος, Εκδόσεις Gutenberg.

Gonzalez, F. (2019) Global Reactions to the Cambridge Analytica Scandal: An Inter-Language Social Media Study, Διαθέσιμο στη δ/νση https://faculty.washington.edu/aragon/pubs/LA_WEB_Paper.pdf. Πρόσβαση: 14/4/2020

Gowan, R. (2018) Why Spies and International Organizations Are Natural Allies, Διαθέσιμο στη δ/νση https://www.worldpoliticsreview.com/articles/24123/why-spies-and-international-organizations-are-natural-allies. Πρόσβαση: 6/8/2019

Herring, P. (1992) Business intelligence in Japan and Sweden: Lessons for the US, Journal of Business strategy, 13 (2) 44-49.

House, W. (1995) Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, Διαθέσιμο στη δ/νση https://www.hsdl.org/?view&did=463240. Πρόσβαση: 11/8/2019

Lee, M., Lederman, J. (2018) The Long History of Spies Posing as Diplomats Abroad, London: Bloomberg.

Mendell, L. (2011) The quiet threat: fighting industrial espionage in America, New York: Charles C Thomas Publisher.

Miller, G. (2005) CIA's secret agents hide under a variety of covers, Διαθέσιμο στη δ/νση https://www.seattletimes.com/nation-world/cias-secret-agents-hide-under-a-variety-of-covers/. Πρόσβαση: 4/8/2019

Nasheri, H. (2005) Economic espionage and industrial spying, Cambridge: Cambridge University Press.

National Counterintelligence and Security Center (2018) Foreign Economic Espionage in Cyberspace, Διαθέσιμο στη δ/νση https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf. Πρόσβαση: 7/4/2020

Navasardian, A. (2013) Is the Ambassador Really an Honorable Spy?, Διαθέσιμο στη δ/νση http://www.diplomat.am/dir/diplomatic_essays/is_the_ambassador_really_an_honorable_spy/2-1-0-61. Πρόσβαση: 2/8/2019

NBG – National Bank of Greece (2012), Διαθέσιμο στη δ/νση https://www.nbg.gr/el/transaction-security. Πρόσβαση: 26/5/2020

Office of the National Counterintelligence Executive (2011) Foreign spies stealing US economic secrets in cyberspace, Διαθέσιμο στη δ/νση https://www.hsdl.org/?abstract&did=720057. Πρόσβαση: 12/8/2019

Pasternak, G., Witkin, G. (1996) The Lure of the Steal, US News & World Report, 45 17-23.

Porteous, S. (1994) Economic Espionage: Issues Arising from Increased Government Involvement with the Private Sector, Intelligence and National Security, 9 (4) 85-96.

Porteous, S. (1998) Economic and Commercial Interests and Intelligence Services

Reid, M. (2016) A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?, Διαθέσιμο στη δ/νση https://lawreview.law.miami.edu/wp-content/uploads/2016/06/A-Comparative-Approach-to-Economic-Espionage_-Is-Any-Nation-Effectively-Dealing-With-This-Global-Threat_.pdf. Πρόσβαση: 7/8/2019

Robert, R. (2014) The booming business of industrial spies, Διαθέσιμο στη δ/νση http://parisinnovationreview.com/articles-en/the-booming-business-of-industrial-spies. Πρόσβαση: 1/8/2019

Rubenstein, D. (2014) Nation State Cyber Espionage and its Impacts, Διαθέσιμο στη δ/νση https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/#introduction. Πρόσβαση: 2/4/2020

Schiller, C. (2013) Espionage: Counter-Economic, Encyclopedia of Information Assurance.

Soilen, S. (2016) Economic and industrial espionage at the start of the 21st century–Status quaestionis, Journal of Intelligence Studies in Business, 6(3) 56-69.

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

US Census Bureau (2001-2019), Διαθέσιμο στη δ/νση https://www.census.gov/retail/index.html. Πρόσβαση: 15/5/2020

Weiner, T. (1995) C.I.A. Faces Issue of Economic Spying, Διαθέσιμο στη δ/νση https://www.nytimes.com/1995/10/15/world/emerging-role-for-the-cia-economic-spy.html. Πρόσβαση: 3/8/2019

Wright, C., Roy, G. (1999) Industrial espionage and competitive intelligence: one you do; one you do not, Journal of Workplace Learning, 11(2) 53-59.

Βικιπαιδεία (2020), Διαθέσιμο στη δ/νση https://el.wikipedia.org/wiki. Πρόσβαση: 26/5/2020

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