2022-05

þÿ — µ ¾ - » ¹ ¾ · º ± ¹ · Ã · ¼ ± Ã ¯ ± Ä É ½

þÿ ± ½ ¿ ¹ Ç Ä Î ½ À · ³ Î ½ À » · Á ¿ Æ Ì Á · Ã ·

þÿ S o u r c e I n t e l l i g e n c e - O S I N T)

þÿ µ Á ³ ± » µ ¯ ¿ ³ ¹ ± Ä ¹ Â Å À · Á µ Ã ¯ µ Â

þÿ À » · Á ¿ Æ ¿ Á ¹ Î ½ Ã Ä ¿ À » ± ¯ Ã ¹ ¿ Ä

þÿ µ ¸ ½ ¹ º ® Â ± Ã Æ ¬ » µ ¹ ± Â

þÿ œ · » ¹ ¬ ´ · Â , “ Á · ³ Ì Á ¹ ¿ Â

þÿ Á Ì ³ Á ± ¼ ¼ ± ” ¹ µ ¸ ½ Î ½ £ Ç - Ã µ É ½ , £ Ä Á ± Ä · ³ ¹ º ® Â º ± ¹ ‘ Ã Æ ¬ » µ ¹ ± Â , £ Ç ¿ » ® • À ¹ Ã Ä
þÿ ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â ¬ Æ ¿ Å

ΜΗΛΙΑΔΗΣ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ.docx

by Grigorios Miliadis

Submission date: 29-May-2022 04:52PM (UTC+0300)
Submission ID: 1846401841
File name: 81808_Grigorios_Miliadis_ΜΗΛΙΑΔΗΣ_ΔΙΠΛΩΜΑΤΙΚΗ_ΕΡΓΑΣΙΑ_352532_575863514.docx (972.67K)
Word count: 18443
Character count: 113988

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Η εξέλιξη και η σημασία των ανοιχτών πηγών πληροφόρησης (Open Source Intelligence - OSINT) ως εργαλείο για τις υπηρεσίες πληροφοριών στο πλαίσιο της εθνικής ασφάλειας.

Γρηγόριος Μηλιάδης

Μάιος 2022

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Η εξέλιξη και η σημασία των ανοιχτών πηγών πληροφόρησης (Open Source Intelligence - OSINT) ως εργαλείο για τις υπηρεσίες πληροφοριών στο πλαίσιο της Εθνικής Ασφάλειας.

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών Διεθνείς Σχέσεις, Στρατηγική και Ασφάλεια στο Πανεπιστήμιο Νεάπολις

Γρηγόριος Μηλιάδης

Μάιος 2022

Πνευματικά δικαιώματα

Περιεχόμενα

Σελίδα Εγκυρότητας

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Γρηγόριος Μηλιάδης

Τίτλος Μεταπτυχιακής Διατριβής: Η εξέλιξη και η σημασία των ανοιχτών πηγών πληροφόρησης (Open Source Intelligence - OSINT) ως εργαλείο για τις υπηρεσίες πληροφοριών στο πλαίσιο της εθνικής ασφάλειας. Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις ……. [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος):……

[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής:……

[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής:..……...

[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Υπεύθυνη Δήλωση

Ο Γρηγόριος Μηλιάδης, γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Η εξέλιξη και η σημασία των ανοιχτών πηγών πληροφόρησης (Open Source Intelligence - OSINT) ως εργαλείο για τις υπηρεσίες πληροφοριών στο πλαίσιο της εθνικής ασφάλειας.», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο Δηλών,

Γρηγόριος Μηλιάδης

Για την Αναστασία και τη Φανή.

Πάντα, όταν κατορθώνεις κάτι στην ζωή σου υπάρχουν άνθρωποι που έχουν συμβάλει είτε άμεσα είτε έμμεσα στην προσπάθεια σου. Η αναγνώριση της συμβολής και βοήθειας τους, για να επιτευχθούν τα δικά σου τα «θέλω», σε κρατά ταπεινό και ικανό για μελλοντικές επιτυχίες. Γιατί τίποτα δεν είναι ποτέ μόνο για εσένα ή από εσένα. Ευχαριστώ την σύζυγο μου, για την υποστήριξη που μου παρείχε, την υπομονή που έδειξε και την πίεση που μου άσκησε για να ολοκληρώσω το μεταπτυχιακό πρόγραμμα. Ευχαριστώ τον επιβλέποντα καθηγητή μου, για την καθοδήγησή του, που βοήθησε στην ολοκλήρωση της παρούσας εργασίας και για τις διαλέξεις του, μέσω των οποίων μου «άνοιξε τα μάτια» στον υπέροχο κόσμο της πληροφόρησης.

Περίληψη

Η παρούσα εργασία έχει σκοπό την ανάλυση της σημαντικότητας του OSINT, ως εργαλείο για τις υπηρεσίες πληροφοριών, μέσα από την εξέταση κινήτρων και αντικινήτρων της χρήσης του. Σημειώνεται πως η χρήση των κινήτρων και αντικινήτρων αποτελεί την πρωτοτυπία της εργασίας και επεξηγεί τις πιέσεις για χρήση ή μη του OSINT, στο πλαίσιο της εθνικής ασφαλείας. Η εργασία βασίζεται σε ποιοτική ανάλυση της ελληνικής και διεθνούς βιβλιογραφίας και στη χρήση μελέτης περιπτώσεων των υπηρεσιών πληροφόρησης των Ηνωμένων Πολιτειών της Αμερικής (ΗΠΑ) και του Ηνωμένου Βασίλειου (ΗΒ) καθώς αξιολογείται η σημαντικότητα του OSINT για αυτές. Μέσα από την ανάλυση της βιβλιογραφίας βρέθηκε πως τα κίνητρα για την χρήση OSINT βασίζονται σε διεθνείς και κοινωνικές αλλαγές που έχουν επιφέρει η τεχνολογία και η παγκοσμιοποίηση, ενώ, βρέθηκε πως η χρήση OSINT από τις υπηρεσίες και τις κοινότητες πληροφόρησης των ΗΠΑ και του ΗΒ είναι περιορισμένη. Κλείνοντας, υποστηρίζεται η ανεξαρτητοποίηση υπηρεσιών OSINT, η αύξηση χρηματοδοτήσεων και η εκκίνηση του κύκλου πληροφόρησης με την χρήση OSINT.

Λέξεις κλειδιά:

Εθνική Ασφάλεια, Πληροφόρηση, Open Source Intelligence, OSINT

Abstract

The purpose of this paper is to analyze the importance of OSINT, as a tool for intelligence agencies, by examining the incentives and deterrents for its use. It is noted that the use of incentives and disincentives is the originality of the paper and explains the pressures for the use or not of OSINT, in the context of national security. The paper is based on a qualitative analysis of the Greek and the international literature, and the use of a case study of the intelligence agencies of the United States of America (USA) and the United Kingdom (UK) as the importance of OSINT for them is evaluated. Through the literature review it was found that the motivation for using OSINT is based on international and social changes brought about by technology and globalization, while, it was found that the use of OSINT by US and UK intelligence agencies and communities is limited. In conclusion, it supports the independence of OSINT services, the increase of funding and the start of the information cycle using OSINT.

Key words:

National Security, Information, Open Source Intelligence, OSINT

Βραχυγραφίες

BBC	British Broadcasting Corporation
BBCM	British Broadcasting Corporation Monitoring
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
CSIS	Center for Strategic and International Studies
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DNI	Director of National Intelligence
ELINT	Electronic Intelligence
FAS	Federation of American Scientists
FBIS	Federal Broadcast Information Service
FBMS	Foreign Broadcast Monitoring Service
FO	Foreign Office
GC&CS	Government Code and Cypher School
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GEOINT	Geospatial Intelligence
HUMINT	Human intelligence
ICT	Information and Communication Technologies
IMINT	Imagery Intelligence
INTs	Αναφέρεται συλλογικά στις πηγές πληροφόρησης
IRTPA	Intelligence Reform and Terrorism Prevention Act
JIC	Joint Intelligence Committee
MASINT	Measurement and Signature Intelligence
MI1c	Military Intelligence, Section 1, subsection c
MI5	Security Service
MIP	Miliary Intelligence Program
NATO	North Atlantic Treaty Organization
NIP	National Intelligence Program
NSA	National Security Agency
NSC	National Security Council
OSC	Open Source Center

OSD	Open Source Data
OSE	Open Source Enterprise
OSINF	Open Source Information
OSINT	Open Source Information
OSN	Online Social Networks
OSSINT	Open Source Social Network Intelligence
PDB	President's Daily Brief
RFI	Request For Information
RIEAS	Research Institute for European and American Studies
SARS COV	Severe acute respiratory syndrome coronavirus
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service
SOCMINT	Social Media Intelligence
TECHINT	Technical Intelligence
UK	United Kingdom
USA	United States of America
USS	Unites States Ship
WMD	Weapons of Mass Destruction
ΕΥΠ	Εθνική Υπηρεσία Πληροφοριών
ΗΒ	Ηνωμένο Βασίλειο
ΗΠΑ	Ηνωμένες Πολιτείες της Αμερικής
κ.ά.	και άλλα/άλλοι/άλλες
χ.χ.	χωρίς χρονολογία

Κατάλογος Γραφικών Παραστάσεων/Εικόνων/Διαγραμμάτων

Εισαγωγή

Το παρόν κεφάλαιο εισάγει τον αναγνώστη στην εργασία, παρέχοντας και συζητώντας το υπόβαθρο και το γενικό πλαίσιο του θέματος. Στην συνέχεια εκφράζεται το ερευνητικό πρόβλημα, ο σκοπός, οι στόχοι και τα ερευνητικά ερωτήματα. Κλείνοντας, αναλύεται η σημασία αλλά και οι περιορισμοί του θέματος της εργασίας.

Η παρούσα εργασία εντάσσεται στον τομέα των Διεθνών Σχέσεων και της Στρατηγικής, καθώς και στον υπο-τομέα τους, στις Σπουδές Πληροφόρησης. Η πληροφόρηση αποσκοπεί στην υποστήριξη της διαδικασίας λήψης αποφάσεων και χάραξης πολιτικής, παρέχοντας στους κρατικούς αξιωματούχους και φορείς, πληροφορίες, με βάση τις εκάστοτε απαιτήσεις (Johnson, 2010, p. 5). Επομένως, η πληροφόρηση συμβάλλει στην διατήρηση της εθνικής ασφάλειας του κράτους με την προϋπόθεσή ότι παρέχει ακριβή, ολοκληρωμένη και έγκαιρη πληροφόρηση, χρησιμοποιώντας μυστικές και μη πηγές. Οι ανοιχτές πηγές αποτελούν μια από τις πιο πλούσιες δεξαμενές για την μεθοδική συγκέντρωση δημόσιων διαθέσιμων δεδομένων από τις εθνικές υπηρεσίες πληροφοριών. Στην «εποχή της πληροφόρησης» όπου όλο και περισσότερες πληροφορίες και δεδομένα γίνονται διαθέσιμα και άμεσα προσβάσιμα στο ευρύ κοινό, η πληροφόρηση από ανοιχτές πηγές, ή αλλιώς γνωστή με το ακρώνυμο OSINT, είναι ένα ισχυρό εργαλείο για την προάσπιση της εθνικής ασφάλειας κάθε κράτους. Παράλληλα αυτή η νέα εποχή συνοδεύεται από νέες προκλήσεις που χρησιμοποιούν τα ίδια τεχνολογικά μέσα. Όμως, υπάρχουν αλληλοσυγκρουόμενες απόψεις για την σημασία, τον ρόλο και την χρήση του OSINT, ως εργαλείο από τις εθνικές υπηρεσίες πληροφόρησης.

Στη διεθνή ακαδημαϊκή συζήτηση δεσπόζει η αγγλοσαξονική βιβλιογραφία, όπου υπάρχει μια πληθώρα ερευνών στον τομέα της πληροφόρησης, αλλά και για το OSINT (Johnson, 2014). Μέχρι στιγμής, στην ελληνική βιβλιογραφία υπάρχει περιορισμένη μελέτη στο πεδίο της πληροφόρησης (Κωνσταντόπουλος, 2018). Η βιβλιογραφία που υπάρχει είναι διάσπαρτη, καλύπτοντας διάφορες θεματικές της πληροφόρησης όπως η οικονομική κατασκοπεία (Κωνσταντόπουλος, 2010), η ελληνική Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ) (Liaropoulos and Konstantopoulos, 2014), οι προκλήσεις της πληροφόρησης αλλά και γενικότερα την πληροφόρηση (Liaropoulos, 2008; Konstantopoulos and Doga, 2015; Κωνσταντόπουλος, 2015, 2018). Όσον αφορά τις εκδόσεις περιοδικών, η Research Institute for European and

American Studies - RIEAS (2018), εκδίδει το «Journal of European and American Intelligence Studies»[1] και περιέχει άρθρα σχετικά με την πληροφόρηση. Όμως, παρά την συμβολή του περιοδικού και των σποραδικών συγγραμμάτων και άρθρων που έχουν δημοσιευθεί, στην περίπτωση των ανοιχτών πηγών πληροφόρησης η βιβλιογραφία είναι μηδαμινή[2]. Η δυναμική ανάπτυξη στο πεδίο του OSINT σε συνδυασμό με το κενό στην βιβλιογραφία αναδεικνύουν την σημαντικότητα του θέματος της παρούσας εργασίας .

Η παρούσα εργασία έχει σκοπό την ανάλυση της σημαντικότητας του OSINT, ως εργαλείο για τις υπηρεσίες πληροφοριών, μέσα από την εξέταση κινήτρων και αντικινήτρων της χρήσης του. Σημειώνεται πως η χρήση των κινήτρων και αντικινήτρων αποτελεί την πρωτοτυπία της εργασίας και επεξηγεί τις πιέσεις για χρήση ή μη του OSINT, στο πλαίσιο της εθνικής ασφάλειας. Με την χρήση μελέτης περιπτώσεων των υπηρεσιών πληροφόρησης των Ηνωμένων Πολιτειών της Αμερικής (ΗΠΑ) και του Ηνωμένου Βασίλειου (ΗΒ) αξιολογείται η σημαντικότητα του OSINT για αυτές. Για αυτούς τους λόγους, θα παρουσιαστεί η εξέλιξη των ανοιχτών πηγών πληροφόρησης και έπειτα θα αναλυθεί η παρούσα κατάσταση. Επιπλέον, θα γίνει σύγκριση, μεταξύ του πώς χρησιμοποιούνται οι ανοιχτές πηγές πληροφόρησης στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) και πώς στο Ηνωμένο Βασίλειο (ΗΒ).

Είναι απαραίτητο, όμως, να τεθούν επιμέρους στόχοι. Ο διαχωρισμός αυτός, δίνει την δυνατότητα να δομηθεί η απάντηση πάνω σε μια λογική αλληλουχία θεματικών, όπου η κάθε θεματική συνδέεται με την άλλη και παρέχει ένα μέρος της συνολικής εικόνας. Επιπλέον, η καθιέρωση επιμέρους στόχων καθιστά την έρευνα πιο διαχειρίσιμη, διότι δημιουργεί όρια και παρέχει συγκεκριμένη κατεύθυνση, με βάση τα ερωτήματα που πρέπει να απαντηθούν. Στόχοι της εργασίας είναι να:

1. ερευνηθούν τα κίνητρα και τα αντικίνητρα της χρήσης πληροφόρησης από ανοιχτές πηγές.
2. αναλυθεί και να συγκριθεί η χρήση ανοιχτών πηγών πληροφόρησης από τις υπηρεσίες πληροφόρησης των ΗΠΑ και του ΗΒ.

Οι στόχοι της εργασίας χωρίζονται στα εξής ερωτήματα:

[1] Παλαιότερα υπό την ονομασία: «Journal of Mediterranean and Balkan Intelligence»
[2] Με εξαίρεση κάποια άρθρα στο RIEAS

1. Πώς έχει εξελιχθεί η συλλογή πληροφοριών από υπηρεσίες πληροφόρησης χρησιμοποιώντας ανοιχτές πηγές;
2. Ποια είναι τα κίνητρα συλλογής πληροφοριών από ανοιχτές πηγές για τις υπηρεσίες πληροφόρησης;
3. Ποια είναι τα αντικίνητρα συλλογής πληροφοριών από ανοιχτές πηγές για τις υπηρεσίες πληροφόρησης;
4. Πως έχει εφαρμοστεί η πληροφόρηση από ανοιχτές πηγές στις ΗΠΑ;
5. Πως έχει εφαρμοστεί η πληροφόρηση από ανοιχτές πηγές στο ΗΒ;
6. Ποιες οι διαφορές και οι ομοιότητες μεταξύ ΗΠΑ και ΗΒ, όσον αφορά την πληροφόρηση από ανοιχτές πηγές;

Η παρούσα εργασία έχει σκοπό να εκτιμήσει τη σημασία του OSINT ως εργαλείο των υπηρεσιών πληροφόρησης σε στρατηγικό επίπεδο, χρησιμοποιώντας τις ΗΠΑ και το ΗΒ. Ως εκ τούτου, δεν θα εστιάσει σε θεαματικές που αφορούν τεχνικές και μεθόδους εφαρμογής του OSINT. Στην βιβλιογραφική επισκόπηση αναφέρονται επιμέρους θεματικές του OSINT, όμως αυτό γίνεται, ώστε να κατανοήσει ο αναγνώστης την θέση της παρούσας εργασίας ανάμεσα στην διεθνή και στην ελληνική βιβλιογραφία.

Κεφάλαιο 1 - Ασφάλεια και Πληροφόρηση

1.1 Ασφάλεια

Μια βασική λέξη στο λεξιλόγιο των διεθνών σχέσεων, που όμως δεν οριστεί με απόλυτη σαφήνεια. Για λόγους δυσκολίας, έλλειψης ενδιαφέροντος, καθώς και του πολυδιάστατου χαρακτήρα της έννοιας «ασφάλεια» δεν υπήρξε σημαντική έρευνα μέχρι το 1980 (Κωνσταντόπουλος, 2018). Η έννοια της ασφαλείας δεν αναφέρεται μόνο σε στρατιωτικά θέματα, αλλά πλέον εγκολπώνει θέματα όπως η οικονομία, η ενέργεια,, η πολιτική, η τροφή και οι αξίες (Buzan, σελ. 27, 2016). Σε επίπεδο ατόμου υπάρχουν δυσκολίες ορισμού της ασφαλείας, καθώς μπορεί να περιγράψει πραγματικές ή υποκειμενικές απειλές. Επιπλέον η σχέση του ατόμου με το κράτος, όσον αφορά την ασφάλεια, δεν είναι απλή. Το κράτος παρέχει ασφάλεια στο άτομο, όμως μπορεί να αποτελεί και απειλή για αυτό, όπως και το άτομο, με τη σειρά του, μπορεί να αποτελέσει απειλή για το κράτος. Παρά την θεμελιώδη σημασία της ασφαλείας για το άτομο, αυτό αποτελεί υφιστάμενη κατηγορία εθνικής και διεθνούς δομής ασφαλείας. Επομένως, η εθνική και η διεθνής διάσταση δεν πρέπει να αναλύεται σε επίπεδο ατόμου (Buzan, κεφ. 2 2016). Ένας γενικός ορισμός είναι «ελευθερία από απειλές προς κύριες αξίες, τόσο μεμονωμένων ατόμων, όσο και ομάδων» (Κωνσταντόπουλος, 2018). Οι Lawrence Krause και Joseph Nye Jr. (Κωνσταντόπουλος, 2018) ορίζουν την ασφάλεια «ως απουσία έντονων απειλών ή ύπαρξη απειλών σε ανεκτά επίπεδα». Ο (Wolfers, 1952), μας προειδοποιεί γράφοντας πως, ενώ φαίνεται να προσφέρει καθοδήγηση και μια βάση για ευρεία συναίνεση, μπορεί να επιτρέπουν στον καθένα να χαρακτηρίζει όποια πολιτική τον ευνοεί, με ένα ελκυστικό και πιθανώς παραπλανητικό όνομα.

1.2 Εθνική Ασφάλεια

Τι είναι Εθνική Ασφάλεια; Ο Quiggin (2007, σελ. 7) υπογραμμίζει πως αν και φαίνεται πολύ απλή η ερώτηση, η απάντηση ωστόσο δεν είναι. Η απλή απάντηση θα ήταν πως Εθνική Ασφάλεια είναι τα μέτρα που λαμβάνει ένα κράτος για να διασφαλίσει την ασφάλειά του – δηλαδή την επιβίωση του στο διεθνές σύστημα – και των πολιτών του. Όμως το ερώτημα που τίθεται είναι: μέχρι πού μπορεί ή πρέπει να φτάσει ένα κράτος για να ορίσει και να προστατέψει τα συμφέροντά του; Για να

απαντηθεί αυτό το ερώτημα χρειάζεται να προσδιοριστούν τα συμφέροντα του κράτους σε όρους στρατιωτικούς, πολιτικούς, οικονομικούς, κοινωνικούς και περιβαλλοντικούς (Quiggin, 2007). Είναι δικαίωμα και υποχρέωση του κράτους να προστατεύει τους πολίτες του, αλλά από την άλλη, πρέπει να έχει υπόψη του τους πόρους που έχει στην διάθεση του και να ισορροπήσει τις δυνατότητες και τις προσδοκίες. Σημαντικό σε αυτήν την διαδικασία είναι ο εντοπισμός των κρίσιμων σημείων στην Εθνική Ασφάλεια, πράγμα που είναι εξαιρετικά δύσκολο, καθώς το κράτος πρέπει να αξιολογεί την θέση του στο διεθνές σύστημα, σε συνδυασμό με τις απειλές που αντιμετωπίζει. Επιπλέον, οφείλει να προσαρμόζεται στις αλλαγές που δημιουργούν νέες απειλές και να εφαρμόζει νέους τρόπους αντιμετώπισής τους (Quiggin, 2007; Μαυραγάνης, 2019).

Οι απειλές που αντιμετωπίζουν τα κράτη φαίνεται να μεταβιβάζονται προς τα κάτω, από τις απειλές επιπέδου διεθνούς συστήματος συστημάτων (κράτη σε ανταγωνισμό μεταξύ τους) σε επίπεδο ατόμων ή μικρών ομάδων. Οι εθνικές υπηρεσίες πληροφορίων πρέπει να μπορούν να ανιχνεύουν ή να προβλέπουν πιθανές, μη παραδοσιακές απειλές, όπως η διακρατική τρομοκρατία και η αδυναμία κρίσιμων υποδομών, οι οποίες μπορούν να χρησιμοποιηθούν στα πλαίσια υβριδικών απειλών (Μαυραγάνης, 2019). Δυστυχώς, τα περισσότερα από τα εξαιρετικά τεχνολογικά και διαβαθμισμένα συστήματα πληροφόρησης σχεδιάστηκαν για αντιμετωπίζουν συμβατικές απειλές προερχόμενες από κράτη, την περίοδο του Ψυχρού Πολέμου. Αυτά τα συστήματα μπορεί να λειτουργούν καλά ενάντια σε παραδοσιακές στρατιωτικές απειλές μεταξύ κρατών, αλλά δεν μπορούν να αντιληφθούν ή να αντιδράσουν σε δυνατότητες και προθέσεις στο επίπεδο του ατόμου (Quiggin, 2007, σελ. 159).

1.3 Πληροφόρηση

Κεντρικό στοιχείο για την αύξηση της ασφάλειας του κράτους είναι η κατοχή πληροφοριών σχετικά με το ποιες απειλές μπορεί να ελλοχεύουν. Επιπλέον, για να προοδεύσει ένα κράτος, αναζητά τις ευκαιρίες που μπορεί να αξιοποιήσει. Είτε ο στόχος είναι η προστασία είτε η ευημερία, η συλλογή, η ανάλυση και η αξιολόγηση πληροφοριών σχετικά με το διεθνές περιβάλλον, αλλά και το εσωτερικό, είναι ζωτικής σημασίας για την αποτελεσματική λήψη αποφάσεων από την στρατιωτική και πολιτική ηγεσία ενός κράτους (Johnson, 2010, σελ. 5; 2014, σελ. 3). Αυτά φαίνονται και σε ορισμούς που έχουν δοθεί:

> *«Η πληροφόρηση είναι μια επίσημη διαδικασία λήψης πληροφοριών και μετατροπής τους σε γνώση, διασφαλίζοντας παράλληλα ότι οι πληροφορίες συλλέγονται, αποθηκεύονται και διαδίδονται κατάλληλα»*. (Peterson, σελ. 11 2005)

> *«…αν κάποιος είναι εθνικός ηγέτης, η πληροφόρηση είναι κάτι περισσότερο. Είναι μια μυστική κρατική δραστηριότητα για την κατανόηση ή την επιρροή ξένων οντοτήτων»*. (Warner, 2014)

> *«Οι πληροφόρηση περιλαμβάνει, τις κυρίως μυστικές, δραστηριότητες – στόχευση, συλλογή, ανάλυση, διάδοση και δράση – που αποσκοπούν στην ενίσχυση της ασφάλειας και/ή στη διατήρηση της ισχύος σε σχέση με τους ανταγωνιστές προειδοποιώντας για απειλές και ευκαιρίες»*. (Gill and Phythian,, κεφ. 1, 2018)

Οι παραπάνω ορισμοί καλύπτουν τις οπτικές της πληροφόρησης. Στον πρώτο ορισμό η Peterson (2005) δίνει έμφαση στην πληροφόρηση ως διαδικασία. Στον δεύτερο ορισμό ο Warner (2014) δίνει έμφαση στην μυστικότητα, αλλά και στην μυστική δράση. Οι δυο ορισμοί δεν αναφέρουν τις απειλές και την ασφάλεια, τα οποία είναι ο λόγος ύπαρξης της πληροφόρησης. Αν δεν συμπεριληφθούν στον ορισμό, οποιοδήποτε εγχείρημα πληροφόρησης είναι εκτεθειμένο σε αποτυχία, διότι παραμερίζεται ο βασικός στόχος (Gill and Phythian, κεφ.1, 2018). Με βάση αυτό το σκεπτικό, ο τρίτος ορισμός παρέχει μια ισορροπημένη διατύπωση μεταξύ διαδικασιών και του στόχου της πληροφόρησης.

Από τον Sun-Tzu και τον Machiavelli, μέχρι τους συμβούλους της σύγχρονης εποχής, οι στόχοι των πολεμικών σχεδιαστών και των πολιτικών συμβούλων ήταν να βοηθήσουν τους στρατιωτικούς και πολιτικούς ηγέτες να διατηρήσουν την ασφάλεια, να εξασφαλίσουν επιτυχίες στα πεδία της μάχης και να πετύχουν πολιτικούς και οικονομικούς στρατηγικούς στόχους. Οι συμβουλές βασίζονται αναπόφευκτα σε ένα αποτελεσματικό μηχανισμό πληροφόρησης, με την επιφύλαξη ότι στις σχέσεις μεταξύ κρατών υπάρχει πάντα κάποια αβεβαιότητα, που θα στοιχειώνει ακόμη και τα καλύτερα σχέδια. Ωστόσο, μέχρι πρόσφατα, το θέμα της πληροφόρησης δεν είχε μεταπηδήσει στην αποσχιστική αντιμετώπιση της από μερικούς οξυδερκείς στοχαστές, σε ένα θεσμοποιημένο σύστημα υπηρεσιών πληροφόρησης (Johnson, 2014).

Στις αρχές του 20ου αιώνα αναδυθήκαν οι πρώτες υπηρεσίες πληροφόρησης ως κρατικοί θεσμοί. Η τεχνολογική εξέλιξη, σε συνδυασμό με των ανταγωνισμό μεταξύ τον κρατών, έδωσε το έναυσμα, ενώ οι δύο παγκόσμιοι πόλεμοι οδήγησαν σε εξειδικευμένες υπηρεσίες και ο Ψυχρός πόλεμος συντέλεσε στην παγίωση των υπηρεσιών πληροφόρησης ως θεσμών. Επίσης, ο Ψυχρός Πόλεμος, συντέλεσε στην δημιουργία της αίσθησης της μυστικότητας που περιβάλει το πεδίο της πληροφόρησης. Στο πυρήνα του, η πληροφόρηση, περιλαμβάνει τη συλλογή και την ανάλυση πληροφοριών, την αντιπληροφόρηση και τη μυστική δράση (Shulsky and Schmitt, 2002, σελ. 9; Johnson, 2014) τα οποία θα παρουσιάσουμε παρακάτω.

1.3.1 Κύριες λειτουργίες της πληροφόρηση

1.3.1.1 Συλλογή

Σε αυτό το στάδιο αναφερόμαστε στην συλλογή δεδομένων και πληροφοριών, τα οποία αποτελούν την «πρώτη ύλη» για το επόμενο στάδιο, αυτό της ανάλυσης. Η συλλογή των δεδομένων πραγματοποιείται με την χρήση της κατασκοπίας (χρησιμοποιώντας ανθρώπους για να ανακαλύψουμε μυστικά), τεχνικών μέσων (φωτογραφίες, υποκλοπές επικοινωνιών και άλλα τα οποία βασίζονται στις δυνατότητες της τεχνολογίας) και τις ανοιχτές πηγές (δημοσιεύσεις έντυπες ή ηλεκτρονικές από μέσα μαζικής ενημέρωσης και ραδιοφωνικές ή τηλεοπτικές εκπομές και αναμετάδοση) (Shulsky and Schmitt, σελ. 8, 2002).

Κάποια δεδομένα και πληροφορίες θεωρούνται μυστικές, δηλαδή σημαντικά ή πολύ «ευαίσθητα» για να είναι δημόσια, έτσι ελέγχεται η πρόσβαση σε αυτά. Η προσπάθεια συλλογής τους γίνεται μέσω της κατασκοπείας και των τεχνικών μέσων, ώστε να παραβιαστεί ή να παραγκωνιστεί η προστασία τους. Από την άλλη, υπάρχουν δεδομένα και πληροφορίες που δεν προστατεύονται[3], θεωρούνται ανοιχτά, δημοσιεύονται και αναμεταδίδονται ή αναπαράγονται δημόσια και είναι δυνατή η πρόσβαση σε αυτά, χωρίς την ύπαρξη προσπάθειών απόκλεισης τρίτων. Οι Shulsky και Schmitt (2002, σελ 8) αναφέρουν πως μεταξύ των επαγγελματιών πληροφόρησης υπάρχει συζήτηση που αμφισβητεί την σημαντικότητα των δεδομένων και των πληροφοριών από ανοιχτές πηγές. Αντί αυτού, θεωρούν πως η σημαντικότερες πληροφορίες προέρχονται από μυστικές πηγές. Επομένως, δίνουν μεγαλύτερη αξία σε

[3] Υπάρχουν περιπτώσεις όπου μυστικές πληροφορίες διαρρέουν ακούσια ή και εκούσια και μπορούν να συλλεχθούν από ανοιχτές πηγές.

υπηρεσίες που αναπτύσσουν μεθόδους και τεχνολογία για την συλλογή μυστικών πληροφοριών.

1.3.1.2 Ανάλυση

Περνώντας στην φάση της ανάλυσης, τα δεδομένα αξιοποιούνται και επεξεργάζονται, πριν παρουσιαστούν στον τελικό καταναλωτή. Πρέπει να σημειώσουμε πως, όσο καλά και να είναι τα δεδομένα μεμονωμένα, δεν ενισχύουν την κατανόηση ενός θέματος. Τα δεδομένα θα χρειαστεί να υποστούν επεξεργασία, που ονομάζεται ανάλυση, για να είναι χρήσιμα στην πολιτική και στρατιωτική ηγεσία. Σε πολλές περιπτώσεις, τα δεδομένα που συλλέγονται είναι αποσπασματικά, με διφορούμενη σημασία και είναι δυνατόν να αντιφάσκουν. Επομένως, η διαδικασία ανάλυσης των διαθέσιμων δεδομένων είναι κρίσιμη για την δημιουργία της σωστής εικόνας, σχετικά με τις δυνατότητες, τις ενέργειες και τις προθέσεις του αντιπάλου. Η μεγαλύτερη δυσκολία είναι η πρόβλεψη[4] των μελλοντικών δυνατοτήτων, προθέσεων και ενεργειών του αντιπάλου (Shulsky and Schmitt, 2002, σελ. 9).

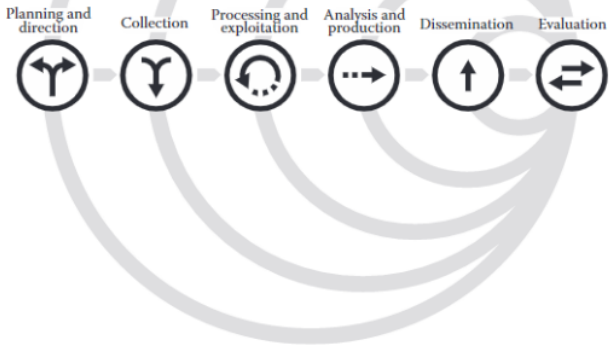
Το στάδιο της ανάλυσης και της παραγωγής απαιτεί άριστα εκπαιδευμένο και εξειδικευμένο προσωπικό – τους αναλυτές – για να δώσουν νόημα στα δεδομένα και τις πληροφορίες. Δεδομένα και πληροφορίες επιβεβαιώνονται και ιεραρχούνται σύμφωνα με τις απαιτήσεις της στρατιωτικής και της πολιτικής ηγεσίας και από τους αναλυτές γίνεται η σύνθεση και η ερμηνεία. Επίσης, οι αναλυτές μπορούν ζητήσουν επιπρόσθετες πληροφορίες (Request For Information – RFI), εκκινώντας ξανά της διαδικασία της συλλογής (Jensen, McElreath and Graves, 2013, σελ. 159). Οι αναλυτές παρέχουν ενημέρωση που πλαισιώνει τη δημιουργία των πολιτικών, ενώ δεν γράφουν οι ίδιοι τις κρατικές πολιτικές. Η σύνθεση των επεξεργασμένων δεδομένων, σε ένα ολοκληρωμένο προϊόν πληροφόρησης με δυνατότητα διάδοσης, επιτρέπει στις υπηρεσίες πληροφοριών να είναι χρήσιμες στην πολιτική και στρατιωτική ηγεσία, τους πελάτες της πληροφόρησης[5] (Jensen, McElreath and Graves, 2013, σελ. 156).

---

[4] Στην αμερικανική ορολογία των πληροφοριών «εκτίμησης»,

[5] Συνηθίζεται να χρησιμοποιούνται οικονομικοί όροι για την περιγραφή της διαδικασίας πληροφόρησης. Ο παραλήπτης ονομάζεται «πελάτης», οι τελικές πληροφορίες «προϊόν»

❖ *Ο κύκλος της πληροφόρησης*



Διάγραμμα 1: Ο κύκλος της πληροφόρησης.

Πηγή: Jensen, McElreath & Graves, 2013, σελ. 154.

Στο διάγραμμα 1 απεικονίζεται ο κύκλος της πληροφόρησης, που μας δίνει γραφικά, με απλοποιημένο τρόπο, τα επιμέρους στάδια της πληροφόρησης, από την συλλογή δεδομένων μέχρι την αξιολόγηση του προιόντος πληροφόρησης από τους τελικούς παραλήπτες και την ανατροφοδότηση, που υπάρχει σε κάθε στάδιο (Jensen, McElreath & Graves, σελ. 152, 2013). Κρίνεται σκόπιμο να αναφερθεί σε αυτό το σημείο ο κύκλος πληροφόρησης, για αναδειχθούν δυο θέματα: πρώτον να σημειωθεί σε ποιο σημείο βρίσκονται οι δύο πιο σημαντικές λειτουργίες της πληροφόρησης (συλλογή και ανάλυση) και δεύτερον, να υπογραμμιστεί η πολυπλοκότητα της διαδικασίας πληροφόρησης. Επιγραμματικά, το στάδιο του σχεδιασμού και της διεύθυνσης ξεκινά με τηζήτηση πληροφοριών από κρατικούς αξιωματούχους, που οδηγεί στο να διατυπωθούν οι ερωτήσεις που πρέπει να απαντηθούν. Με βάση τις ερωτήσεις, καθορίζεται ποιες πηγές πληροφόρησης, πρέπει να αξιοποιηθούν, ώστε να συλλεχθούν τα κατάλληλα δεδομένα. Στην συνέχεια, η επεξεργασία και η εκμετάλλευση μεταποιούν τα ακατέργαστα δεδομένα (π.χ. μεταφράσεις κειμένων, απομαγνητοφωνήσεις, αποκρυπτογραφήσεις, επεξεργασία βίντεο και φωτογραφιών), για να μπορούν να αξιοποιηθούν από τους αναλυτές. Στην διάδοση, το τελικό προιόν πληροφόρησης (finished intelligence) παραδίδεται στον πελάτη σε ηλεκτρονική ή έντυπη μορφή. Τέλος, όλη η πορεία της παραγωγής πληροφόρησης περιβάλλεται από

συνεχή αξιολόγηση, ανατροφοδότηση, συλλογή και αναπροσαρμογή, εάν χρειαστεί. Στη μορφή γραφίματος, ο κύκλος της πληροφόρησης είναι ένα βοήθημα για την εκμάθηση της πληροφόρησης, όμως στην πραγματική ζωή ο κύκλος της πληροφόρησης είναι κάθε άλλο παρά απλό (Davydoff, 2017). Στην πραγματικότητα υπάρχουν υπηρεσίες πληροφοριών, που υλοποιούν συχρόνως ή παραλείπουν μερικά στάδια. Επιπλέον, ο κύκλος δεν λαμβάνει υπόψη του την αντιπληροφόρηση και την μυστική δράση (Hulnick, 2002). Επομένως, υποστηρίζεται πως δεν ανταποκρίνεται πιστά στις πραγματικές διαδικασίες που παράγουν πληροφόρηση (Tropotei, 2018).

1.3.1.3 Αντιπληροφόρηση

Ο στόχος κάθε υπηρεσίας πληροφοριών είναι η απόκτηση και η συντήρηση του πλεονεκτήματος στην λήψη αποφάσεων, έναντι του αντιπάλου. Το πλεονέκτημα λήψης αποφάσεων απαιτεί την τροφοδότηση των ατόμων που θα λάβουν τις αποφάσεις με περισσότερες, πιο ακριβείς-αληθείς πληροφορίες από τον αντίπαλο, στον κατάλληλο χρόνο (Jensen, McElreath & Graves, σελ. 166, 2013; Lowenthal, 2020). Το επιθυμητό αποτέλεσμα είναι η υπεροχή έναντι του αντιπάλου, λόγω καλύτερων επιλογών και αυτό βασίζεται στην εκπλήρωση δύο στόχων. Ο πρώτος στόχος είναι η όσο το δυνατόν καλύτερη και πληρέστερη εικόνα για ένα θέμα και ο δεύτερος είναι η παρεμπόδιση της πληροφόρησης του αντιπάλου (Jensen, McElreath & Graves, σελ. 166, 2013). Οι υπηρεσίες πληροφοριών συλλέγουν και αναλύουν πληροφορίες για να πετύχουν τον πρώτο στόχο και επιδίδονται στην αντιπληροφόρηση (counterintelligence) για να πετύχουν τον δεύτερο στόχο (Jensen, McElreath & Graves, 2013, σελ. 166). Η αντιπληροφόρηση είναι μια λειτουργία που στοχεύει την ικανότητα των αντίπαλων υπηρεσιών πληροφόρησης να αποκτήσουν πρόσβαση σε πληροφορίες. Σε αυτό το σημείο πρέπει να σημειωθεί πως (Jensen, McElreath & Graves, 2013, σελ. 166) η αντιπληροφόρηση δεν αντιμετωπίζει και τις τρομοκρατικές και εγκληματικές οργανώσεις, η δράση των οποίων μπορεί να περιορίζεται αποκλειστικά εντός του κράτους, αλλά και να επεκτείνεται πέρα των κρατικών συνόρων, με την παρουσία τους σε άλλα κράτη. Και οι δύο τύποι οργανώσεων προσπαθούν να αποκτήσουν πληροφορίες για να τις χρησιμοποιήσουν στην δράση τους. Οπότε, σημερινή μορφή της αντιπληροφόρησης περιλαμβάνει και την προάσπιση πληροφοριών από εσωτερικές απειλές (Jensen, McElreath and Graves, 2013, σελ. 166).

Με μια πρώτη ανάγνωση, είναι εύκολο κανείς να σχηματίσει την εντύπωση πως η αντιπληροφόρηση είναι κυρίως παθητική, με έμφαση στα μέτρα προστασίας

ευαίσθητων πληροφοριών και εγκαταστάσεων (Lowenthal, 2020). Τα παθητικά μέτρα εστιάζουν στις εγκαταστάσεις, το προσωπικό των υπηρεσιών και τη διαδικασία πρόσβασης σε πληροφορίες. Παρότι είναι ένα μεγάλο κομμάτι της αντικατασκοπείας, δεν είναι το μόνο. Η αντιπληροφόρηση λαμβάνει και ενεργά μετρά όπως η παραπλάνηση με σκοπό την σύγχυση του αντιπάλου και την αποτροπή απόκτησης των πραγματικών πληροφοριών (Lowenthal, 2009). Οπότε, η αντικατασκοπία εφαρμόζει ένα φάσμα από παθητικά και ενεργά μέτρα, για να πετύχει τον σκοπό της. Τα ενεργά μέτρα περιφρουρούν τις πληροφορίες, στοχεύοντας εσωτερικά, στην ανίχνευση κατασκόπων, ξένων πρακτόρων αλλά και με διεθνείς επιχειρήσεις (Jensen, McElreath & Graves, 2013, p. 167; Lowenthal, 2009). Συνοψίζοντας, η αντιπληροφόρηση καταστέλλει τις δυνατότητες των αντίπαλων υπηρεσιών πληροφόρησης.

1.3.1.4 Μυστική Δράση

Η επιθετική χρήση των υπηρεσιών πληροφοριών είναι γνωστή ως μυστική δράση. Είναι προσπάθειες μυστικής επέμβασης σε γεγονότα στο εσωτερικό μια ξένης χώρας με στόχο να ωθηθούν οι εξελίξεις προς μια πιο ευνοϊκή κατεύθυνση για τον «επιτιθέμενο». Η μυστική δράση διαφέρει από τα άλλες κύριες λειτουργίες της πληροφόρησης στο ότι, ενώ τα άλλα ασχολούνται με την αναζήτηση και τη διαφύλαξη πληροφοριών, η μυστική δράση επιδιώκει να επηρεάσει άμεσα τα πολιτικά γεγονότα, επομένως αποτελεί εργαλείο άσκησης εξωτερικής πολιτικής. Όσον αφορά την ένταση, η μυστική δράση μπορεί να κυμαίνεται από επιχείρηση επιρροής ή προπαγάνδας έως την οργάνωση παραστρατιωτικής δράσης. Έχει περιγράφει ως μια δραστηριότητα στο μέσον της διπλωματίας και του πολέμου. Με αυτόν τον τρόπο, οι υπηρεσίες πληροφοριών ενός κράτους γίνονται μυστικά όπλα για προπαγάνδα, πολιτικές, οικονομικές και παραστρατιωτικές επιχειρήσεις (Shulsky & Schmitt, 2002, σελ. 23), ενώ οι τεχνικές για την άσκηση αυτής της επιρροής είναι πολλές, έχουν το κοινό χαρακτηριστικό της ανωνυμίας, δηλαδή, ο ρόλος της κυβέρνησης που διεξάγει τη δραστηριότητα δεν είναι άμεσα εμφανής ή δεν αναγνωρίζεται δημόσια.

1.3.2 Πηγές Πληροφόρησης

Όπως αναφέρθηκε στον κύκλο της πληροφόρησης, για να ξεκινήσει η συλλογή ορίζονται ποιες πηγές πληροφόρησης θα χρειαστούν. Παρακάτω παρουσιάζονται σύντομα οι βασικές πηγές πληροφόρησης, σύμφωνα με το Γραφείο του Διευθυντή Εθνικής Πληροφόρησης (Office of the Director of National Intelligence – ODNI) των

Ηνωμένων Πολιτειών της Αμερικής (Office of the Director of National Intelligence, χ.χ.).

1.3.2.1 SIGINT

SIGINT είναι συντομογραφία των αγγλικών λέξεων «*Signals Intelligence*» και παράγει πληροφόρηση που προέρχεται από υποκλοπές εκπεμπόμενων σημάτων, είτε ενός είδους είτε διαφορετικών ειδών μαζί. Το SIGINT απαρτίζεται από διαφόρων ειδών πηγές, ανάλογα με το είδος δεδομένων που συλλέγονται, έτσι συστατικά μέρη είναι το «*Communications Intelligence*» – *COMINT* και το «*Electronic Intelligence*» – *ELINT* (Office of the Director of National Intelligence, χ.χ.; Richards, 2014). Τα δεδομένα που συλλέγονται, στα πλαίσια του COMINT, είναι σήματα που περιέχουν ανθρώπινες επικοινωνίες, δηλαδή ομιλία και κείμενο (Steele, 2002; Richards, 2014). Το ELINT συλλέγει δεδομένα τα οποία εκπέμπονται από τμήματα σύγχρονων οπλικών συστημάτων όπως το ραντάρ, σόναρ, συστήματα καθοδήγησης και εύρεσης κατευθύνσεων (Bernard, 2009). Ως είδος πληροφόρησης το SIGINT, ειδικά στην σύγχρονή του μορφή, ξεκινά την πορεία του όταν εφευρέθηκαν οι πρώτοι μέθοδοι για την εκπομπή σημάτων. Αφετηρία είναι ο τηλέγραφος, όμως οι επόμενοι σταθμοί, όπως ο ασύρματος και το διαδίκτυο είναι εξίσου σημαντικοί για τις δυνατότητες που παρείχαν για επικοινωνία και τις προκλήσεις που δημιούργησαν για την πληροφόρηση. Παράλληλα με την τεχνολογική πρόοδο, οι κυβερνήσεις ανέπτυξαν μεθόδους, ώστε να μπορούν να έχουν πρόσβαση στις επικοινωνίες κυβερνήσεων άλλων κρατών (Richards, 2014). Κάθε φορά που ένα μήνυμα εξέπεμπε, ο αποστολέας έχανε έως έναν βαθμό τον έλεγχο της κατεύθυνσης και τελικού προορισμού. Είναι εύκολα κατανοητό πως ένα μήνυμα που αναχαιτίζεται, μπορεί δημιουργήσει ανεπανόρθωτες ζημιές. Η κρυπτογραφία είναι η επιστήμη που συνδέεται άρρηκτα με το SIGINT και συμβάλει στην προσπάθεια προστασίας του μηνύματος του αποστολέα, όσο και στην προσπάθεια ανάγνωσης του από ανεπιθύμητους (Richards, 2014). Επιβεβαίωση της διαχρονικής σημαντικότητας είναι πως εντός της Υπηρεσία Εθνικής Ασφάλειας (National Security Agency – NSA) των ΗΠΑ υπάρχει κέντρο, το οποίο παρέχει υποστήριξη σε θέματα κρυπτολογίας (*Central Security Service*, 2021). Επίσης, σημαντικό στοιχείο υποστήριξης της προσπάθειας του SIGINT είναι το HUMINT, το οποίο παρέχει πρόσβαση σε κωδικούς και την κρυπτογράφηση του αντιπάλου, για να παρακαμφθεί η ασφάλεια του μηνύματος. Στην σύγχρονη εποχή, το διαδίκτυο αποτελεί

μια από τις πιο σημαντικές τεχνολογίες επικοινωνίας και αποτελεί ένα νέο από όπου το SIGINT καλείται να αναχαιτίζει και να εξάγει πληροφορίες (Richards, 2014).

1.3.2.2 IMINT

IMINT είναι η συντομογραφία των αγγλικών λέξεων «*Imagery Intelligence*» και περιλαμβάνει αναπαραστάσεις αντικειμένων που αναπαράγονται ηλεκτρονικά ή οπτικά μέσα σε φιλμ, ηλεκτρονικές συσκευές προβολής ή άλλα μέσα. Οι εικόνες μπορούν να προέρχονται από οπτική φωτογραφία, αισθητήρες ραντάρ και ηλεκτροοπτικά συστήματα (Office of the Director of National Intelligence, χ.χ.).

1.3.2.3 MASINT

MASINT είναι η συντομογραφία των αγγλικών λέξεων «*Measurement and Signature Intelligence*». Είναι η πληροφόρηση που παράγεται από ποιοτικές και ποσοτικές αναλύσεις των φυσικών χαρακτηριστικών στόχων και των γεγονότων για τον χαρακτηρισμό, τον εντοπισμό και την αναγνώρισή τους. Το MASINT εκμεταλλεύεται μια ποικιλία δεδομένων από διάφορους αισθητήρες και πλατφόρμες, ενώ υποστηρίξει την ανάπτυξη και την ανάλυση υπογραφών, καθώς και την εκτέλεση τεχνικής ανάλυσης, για τον εντοπισμό και χαρακτηρισμό στόχων και συμβάντων. Ένα παράδειγμα είναι η χρήση του στην ανίχνευση πυρηνικών δοκιμών (Office of the Director of National Intelligence, χ.χ.).

1.3.2.4 HUMINT

HUMINT είναι η συντομογραφία των αγγλικών λέξεων Human Intelligence και προέρχεται από ανθρώπινες πηγές. Για το ευρύ κοινό το HUMINT παραμένει συνώνυμο με κατασκόπους και την μυστική δράση, όμως στην πραγματικότητα, ένα σημαντικό μέρος των πληροφοριών προέρχονται από φανερούς συλλέκτες, όπως απενημέρωση ατόμων που ταξίδεψαν σε ξένο κράτος, από στρατιωτικούς ακολούθους και άλλους. Είναι από τις παλαιότερες μεθόδους συλλογής πληροφοριών και μέχρι την τεχνολογική επανάσταση στα μέσα του 20^{ου} αιώνα ήταν η κύρια πηγή πληροφόρησης (Office of the Director of National Intelligence, χ.χ.).

1.3.2.5 GEOINT

GEOINT είναι η συντομογραφία των αγγλικών λέξεων Geospatial Intelligence και αποτελεί την ανάλυση και την οπτική αναπαράσταση της ανθρώπινη δραστηριότητας και της φυσικής γεωγραφίας οπουδήποτε στη Γη. Παράγεται μέσω της ενοποίησης εικόνων, IMINT και γεοχωρικών δεδομένων (Office of the Director of National Intelligence, χ.χ.).

1.3.2.6 OSINT

OSINT είναι η συντομογραφία των αγγλικών λέξεων Open Source Intelligence, και συλλέγει πληροφορίες και δεδομένα που είναι δημόσια διαθέσιμα (Office of the Director of National Intelligence, χ.χ.; Shulsky and Schmitt, 2002, σελ. 38). Σε αυτό το σημείο πρέπει να διευκρινιστούν δύο όροι, του *Open Source Data (OSD)* και του *Open Source Information (OSINF)*, καθώς παρέχουν τα πλαίσια μέσα στα οποία ορίζεται το OSINT (Minas, 2010, σελ. 7-9). Το εγχειρίδιο «NATO Open Source Intelligence Handbook» μας παρέχει με τους ορισμούς αυτών των δύο εννοιών. Τα OSD «*είναι η ακατέργαστη εκτύπωση, η εκπομπή, η προφορική ενημέρωση ή άλλη μορφή στοιχείων από μια πρωτογενή πηγή. Μπορεί να είναι μια φωτογραφία, μια ηχογράφηση, μια εμπορική δορυφορική εικόνα ή μια προσωπική επιστολή ενός ατόμου*» (NATO, 2001, σελ.2). Είναι ακατέργαστα δεδομένα, όπως συλλέχθηκαν και δεν έχουν υποστεί καμία μορφή επεξεργασίας που να τα τροποποιεί. Αυτά τα ακατέργαστα δεδομένα όταν «*περάσουν μια διαδικασία επεξεργασίας που φιλτράρει, επικυρώνει και διαχειρίζεται την παρουσίαση τους*» (NATO, 2001, σελ. 2) σχηματίζουν το OSINF. Συνεχίζοντας, ο ορισμός διευκρινίζει ότι πρόκειται για «*…γενικές πληροφορίες που συνήθως διαδίδονται ευρέως. Εφημερίδες, βιβλία, εκπομπές* [πχ. τηλεοπτικές ή ραδιοφωνικές] *και γενικά ημερήσια ρεπορτάζ αποτελούν μέρος του* [OSINF]». Οπότε, πρόκειται για δευτερογενής πηγές που όμως απέχουν από την διάσταση της πληροφόρησης. Για να φτάσουμε στο σημείο να μιλάμε για OSINT θα πρέπει να «είναι *πληροφορίες που να έχουν ανακαλυφθεί σκόπιμα, έχει γίνει διάκριση και απόσταξη ώστε να διανεμηθούν σε επιλεγμένο ακροατήριο,… - … προκειμένου να αντιμετωπιστεί ένα συγκεκριμένο ερώτημα. Το OSINT, με άλλα λόγια, ακολουθεί την αποδεδειγμένη διαδικασία πληροφόρησης* [τον κύκλο της πληροφόρησης] *στην ευρεία ποικιλία των ανοιχτών πηγών πληροφοριών και δημιουργεί πληροφόρηση*». Το OSINT είναι μια αναλυτική διαδικασία η οποία ενσωματώνει υψηλού επιπέδου ανθρώπινη εμπειρία μαζί με μια τεχνική διαδικασία ώστε να πράξει την απαραίτητη πληροφόρηση σε σύντομο χρονικό

διάστημα για να ικανοποιήσει μια ανάγκη για πληροφορία (Steele, 2001, σελ. 108). Επομένως, πολύ σημαντική είναι η φάση της ανάλυσης και της ερμηνείας.

Σύμφωνα με τον Lowenthal (2001) το OSINT τροφοδοτείται από τέσσερις κύριες δεξαμενές: τις εμπορικές βάσεις δεδομένων όπως η Lexus-Nexus, τον παγκόσμιο ιστό με χρήση μηχανών αναζήτησης, τα έντυπα που βρίσκονται σε βιβλιοθήκες και την γκρίζα βιβλιογραφία[6] (grey literature) σε έντυπη ή σε ηλεκτρονική μορφή. Το OSINT αντλεί πληροφορίες από πολλές πηγές που διαφέρουν μεταξύ τους. Ένας από τους μεγαλύτερους μύθους είναι πως το OSINT έχει σχέση μόνο με το διαδίκτυο. Αν και το διαδίκτυο είναι χρήσιμο, δεν προσφέρει όλες τις πληροφορίες και πολλές φορές δεν επιτρέπει την ανακάλυψη των πληροφοριών που αναζητούνται. Αυτό συμβαίνει γιατί οι μηχανές αναζήτησης δεν είναι σχεδιασμένες για ενδελεχή έρευνα ολόκληρου του διαδικτύου και όλων των ειδών πληροφοριών, οπότε απαιτούνται άλλες τεχνικές αναζήτησης (Quiggin, 2007, σελ. 161; Minas, 2010, σελ. 12 ; Fisher, 2019).

Φυσικά, πάντα υπάρχει η περίπτωση συλλογής διαβαθμισμένων πληροφοριών που έχουν διαρρεύσει άθελα ή εσκεμμένα και πλέον είναι προσβάσιμες. Παράδειγμα της πρώτης περίπτωσης, είναι η αναρτήσεις από, Ρώσους στρατιωτικούς, σε μέσα κοινωνικής δικτύωσης, που καταγράφουν τις κινήσεις και τις ενέργειες των Ρωσικών ένοπλων δυνάμεων, κατά την εισβολή στην Ουκρανία το 2022 (Williams and Blum, 2018, σελ. 34-35; Bath, 2022). Παράδειγμα της δεύτερης περίπτωσης είναι η δημοσίευση χιλιάδων διαβαθμισμένων εγγράφων στην ιστοσελίδα της WikiLeaks. Αν και ο καθένας με πρόσβαση στο διαδίκτυο μπορούσε να χρησιμοποιήσει τα αρχεία αυτά, απαγορεύτηκε, παραδόξως, η πρόσβαση στην Βιβλιοθήκη του Κογκρέσου των ΗΠΑ. Κατά συνέπεια, η Υπηρεσία Ερευνών του Κογκρέσου[7] δεν μπορούσε να χρησιμοποιήσει τα δεδομένα στις δικές της αξιολογήσεις, επειδή παρέμεναν απόρρητα (Aftergood, 2010). Θεωρητικά δεν υπάρχει όριο στο τι μπορεί να αποτελέσει πηγή δεδομένων για το OSINT και οι ερευνητές πρακτικά περιορίζονται μόνο από την φαντασία και την ανάπτυξη μεθόδων εξεύρεσης των δεδομένων (Quiggin, 2007, σελ. 161-162).

---

[6] Η γκρίζα βιβλιογραφία είναι ερευνητικό υλικό που παράγεται εκτός των καθιερωμένων εκδοτικών οίκων και κανάλια διανομής. Οι πληροφορίες παράγονται σε όλα τα επίπεδα διακυβέρνησης, από επιχειρήσεις και την ακαδημαϊκή κοινότητα σε έντυπη ή ηλεκτρονική μορφή. Παράδειγμα είναι μεταπτυχιακές διατριβές, πρακτικά ή σημειώσεις συνεδρίων και εσωτερικές αναφορές η δημοσιεύσεις επιχειρήσεων ή κρατικών υπηρεσιών (What is Grey Literature? - Grey Literature - LibGuides at University of Exeter, χ.χ.; Γκρίζα βιβλιογραφία: Τι είναι; | Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης Βιβλιοθήκη, χ.χ.; Lowenthal, 2001).

[7] Η υπηρεσία αυτή έχει «σκοπό να υποστηρίξει το Κογκρέσο στα νομοθετικά, εποπτικά και αντιπροσωπευτικά του καθήκοντα» (About CRS)

1.3.2.7 SOCMINT

Σχετικά πρόσφατα ο παγκόσμιος ιστός, δηλαδή το διαδίκτυο, έχει διευκολύνει την πρόσβαση σε πληροφορίες και δεδομένα που σε προηγούμενες εποχές θα ήταν αδιανόητη. Με την εξέλιξη του διαδικτύου σε web 2.0 έχει αυξηθεί θεαματικά η ποσότητα πληροφοριών, καθώς οι χρήστες πλέον είναι δημιουργοί περιεχομένου και όχι μόνο καταναλωτές. Βρισκόμαστε σε μια εποχή κοινωνικής δικτύωσης, όπου μέσα από κοινωνικά δίκτυα όπως το Facebook, Twitter και LinkedIn[8] ερχόμαστε σε επικοινωνία ανταλλάσσοντας ιδέες και επιχειρήματα. Η αλληλεπίδραση αυτή, μεταφέρει την προσωπική μας ζωή στον ψηφιακό κόσμο, όπου η ταυτότητά μας και η ιδιωτική μας ζωή είναι πλέον δημόσιες. Αν και φαίνεται οξύμωρο είναι πραγματικό, απόψεις που παλαιότερα είχαμε την δυνατότητα να εκφράσουμε μόνο σε κλειστό κύκλο είναι πλέον καταγεγραμμένες ψηφιακά και ορατές σε άτομα που δεν βρίσκονται στην σφαίρα της προσωπικής μας ζωής.

Μεταφέροντας τις προσωπικές πληροφορίες μας στα μέσα κοινωνικής δικτύωσης, δημιουργούμε ένα νέο δημόσιο χώρο και η σημασία του ολοένα αυξάνεται ως μέσω επικοινωνίας, αλλά και άντλησης πληροφοριών. Δημόσιοι φορείς έχουν δείξει ενδιαφέρον για τα μέσα κοινωνικής δικτύωσης, με σκοπό την κατανόηση προβλημάτων και την καλύτερη εξυπηρέτηση των κοινωνιών τους. Παραδείγματα αποτελούν η χρήση του Twitter για την παρακολούθηση πανδημιών και της κοινωνικής ανησυχίας (Signorini, Segre & Polgreen, 2011), του Facebook για την ανίχνευση αναρτήσεων που πιθανόν προμηνύουν παραβατική συμπεριφορά και τρομοκρατία (Hoffman, 2012; Richey & Binz, 2015). Τα κοινωνικά δίκτια έχουν άμεσο αντίκτυπο στην ασφάλεια καθώς μέσα από τις ίδιες πλατφόρμες διενεργούνται αλλά και εξιχνιάζονται εγκλήματα. Σημαντικό γεγονός είναι πως ο αριθμός αυτών των γεγονότων αυξάνεται, πράγμα που υποδηλώνει την αυξημένη σύνδεση του ψηφιακού με τον πραγματικό κόσμο. Κατά προέκταση, στα ίδια κοινωνικά δίκτυα, διατηρούν λογαριασμοί τρομοκρατικές οργανώσεις αλλά και ομάδες ή άτομα που επιδίδονται στην πειρατεία (Omand, Bartlett & Miller, 2012).

Οι Omand, Bartlett και Miller (2012), στο άρθρο τους *«Introducing social media intelligence (SOCMINT)»*, είναι οι πρώτοι που επιχειρηματολογούν υπέρ της χρήσης τω κοινωνικών δίκτυών για την δημιουργία πληροφόρησης. Την ονομάζουν SOCMINT και την προτείνουν ως μια νέα ξεχωριστή πηγή πληροφόρησης. Όμως,

[8] Υπάρχει ένας μεγάλος αριθμός μέσων κοινωνικής δικτύωσης, κάποια έχουν παγκόσμια απήχηση ενώ κάποια άλλα έχουν τοπική απήχηση.

θέτουν ως προϋπόθεση για την ανάπτυξη μεθοδολογίας και ενός ηθικού πλαισίου. Τα δυο αυτά μαζί θα δημιουργούν ένα πλαίσιο μέσα στο οποίο οι υπηρεσίες πληροφόρησης θα μπορούν λειτουργούν με δημόσια αποδοχή. Αν και οι χρήστες δημοσιοποιούν πληροφορίες από την προσωπική τους ζωή, το κοινό που στοχεύουν δεν είναι οι αναλυτές. Κατά αυτόν το τρόπο, σε ακραίες περιπτώσεις, υπάρχει κίνδυνος για την ζωή ατόμων των οποίων μια δημοσίευση τους αποτελεί κομμάτι μιας έκθεσης. Όμως και σε πιο ήπιες περιπτώσεις, όπως οι αστυνομικές έρευνες, υπάρχουν τα εξής ερώτημα: υπό ποιες περιπτώσεις πρέπει να διεξάγεται και που βρίσκεται το όριο στην επιτήρηση των λογαριασμών κοινωνικής δικτύωσης ενός ατόμου. Επιπλέον, υπάρχουν τεχνικές που μπορούν να εκμαιεύσουν πληροφορίες τις οποίες ο χρήστης δεν έχει δημοσιοποιήσει ή έχει ορίσει να μην είναι δημόσιες (Cascavilla κ.ά., 2018). Παρά το γεγονός ότι οι Omand, Bartlett και Miller ορίζουν ως ξεχωριστή πηγή πληροφόρησης το SOCMINT, στην παρούσα εργασία υιοθετείτε η άποψη πως πρόκειται για υποκατηγορία ή συγκεκριμένη πτυχή του OSINT. Αυτό δικαιολογείται διότι το SOCMINT βασίζεται σε OSD και OSINF οι οποίες περνούν από τα ίδια στάδια εξεργασίας. Έτσι παραδίδετε ένα προϊόν πληροφόρησης OSINT του οποίου οι μόνες πηγές είναι οι πλατφόρμες κοινωνικής δικτύωσης.

Κεφάλαιο 2 - Βιβλιογραφική Ανασκόπηση

Σε αυτό το σημείο έχει ενδιαφέρων να συζητηθούν οι κύριες θεματικές των ερευνών που έχουν γίνει αναφορικά με το OSINT. Η βιβλιογραφική ανασκόπηση θα δώσει την δυνατότητα εποπτικής εικόνας της σημασίας του OSINT για τις υπηρεσίες πληροφόρησης και σε ποια πεδία εφαρμογής υπάρχει ιδιαίτερο ενδιαφέρον για έρευνα. Τα σύγχρονα μέσα επικοινωνίας έχουν αλλάξει ριζικά με την ανάδυση του Web 2.0 και τη δυνατότητα δημιουργίας περιεχομένου από τους χρήστες (Kandias κ.ά., 2017; Williams & Blum, 2018). Αυτή η έκρηξη παραγωγής πληροφοριών έχει αναζωπυρώσει το ενδιαφέρον για τις δυνατότητες του OSINT, έχοντας πλέον περισσότερες πηγές. Παρά το ενδιαφέρον που υπάρχει, οι απόψεις διίστανται ως προς το πόσο χρήσιμο είναι τελικά και το εάν είναι η λύση για όλα τα προβλήματα πληροφόρησης ή απλά ένα κομμάτι της (Cumming, 2007).

Οι βασικότερες έρευνες έχουν να κάνουν με την χρήση του OSINT από τις υπηρεσίες πληροφοριών (κυρίως στις ΗΠΑ). Ένας από τους πιο αισιόδοξους υποστηρικτές του OSINT, είναι ο Robert David Steel, που υπήρξε μεταξύ άλλων και αναλυτής της CIA. Επιχειρηματολογεί υπέρ του OSINT, όχι μόνο ως λύση για την παροχή πληροφόρησης, αλλά και ως παγκόσμιο μοντέλο ανάπτυξης, που οδηγεί στην οικονομική αποτελεσματικότητα και στην παγκόσμια ειρήνη. Όσον αφορά τις υπηρεσίες πληροφόρησης, ο Steele, υποστηρίζει ότι στον σύγχρονο διασυνδεδεμένο κόσμο, το OSINT μπορεί αντικαταστήσει άμεσα τις κλειστές πηγές πληροφόρησης. Από νωρίς υποστήριξε τη χρήση του OSINT από τις ένοπλες δυνάμεις (Steele, 1995), αλλά και από τις υπηρεσίες πληροφόρησης (Steele, 2001). Χαρακτηριστική είναι η προειδοποίηση πως για να είναι ένα κράτος ανταγωνιστικό στην ψηφιακή εποχή, πρέπει η χρήση κατασκόπων και τεχνολογίας για την υποκλοπή πληροφοριών, να βασίζεται στην καθοδήγηση από τις ανοιχτές πηγές πληροφόρησης (Steele, 2001, σελ. 680, 2010). Επιπλέον, υποστήριζε πως μια υπηρεσία πληροφόρησης που συλλέγει μόνο OSINT, μπορεί να παρέχει υψηλού επιπέδου πληροφόρηση χωρίς την ανάγκη για κλειστές πληροφορίες.

Οι συντριπτική πλειοψηφία των ερευνητών περιορίζουν την ερευνά τους στην αξιοποίηση του OSINT από τις υπηρεσίες πληροφόρησης, όπου βλέπουν σημαντική συμβολή. Ο Lowenthal (2020, σελ. 234) αναγνωρίζει τη σημασία του OSINT στην αύξηση της αποδοτικότητας των υπόλοιπων πηγών πληροφόρησης. Όμως, διαφοροποιείται από τον Steele, υποστηρίζοντας πως είναι πιθανό να προσφέρει λιγότερη ενόραση, από ότι οι πηγές συλλογής κλειστών πληροφοριών (Lowenthal, 2020, σελ. 140). Θεωρεί το OSINT αδιαίρετη πτυχή πηγών πληροφόρησης και υποστηρίζει την χρήση του στο προκαταρκτικό στάδιο, ώστε να κατευθυνθούν οι πόροι συλλογής κλειστών πληροφοριών (κατάσκοποι,

δορυφόροι), όμως είναι αντίθετος στην ιδέα δημιουργίας μιας ανεξάρτητης υπηρεσίας OSINT (Lowenthal, 2001) ενώ δίνει μεγαλύτερη έμφαση στην ανάπτυξη του OSINT εντός των υπηρεσιών που συλλέγουν κλειστές πληροφορίες. Ο Gibson (2004, 2007, 2014) βλέπει το OSINT ως ένα πλέγμα που δένει τις άλλες πηγές κλειστών πληροφοριών σε μία ολοκληρωμένη εικόνα. Η συνεισφορά του OSINT συνήθως «μετριέται» με όρους αποδοτικότητας – εισροές που σχετίζονται με εκροές. Είναι πιο χρήσιμο να διερευνήσετε την αποτελεσματικότητά του – τι μπορεί να κάνει για τη λειτουργία πληροφόρησης. Όσον αφορά την αποτελεσματικότητα, η OSINT διεκδικεί το 80 τοις εκατό της παραγωγής πληροφοριών, παρόλα αυτά, παραμένει «δεύτερης κατηγορίας» σε σχέση με τις μυστικές πηγές. Όσον αφορά την αποτελεσματικότητα, μπορεί να αναπαράγει «μυστικές» πηγές, να σχηματίζει τη μήτρα για τη σύνδεση όλων των άλλων πηγών πληροφόρησης μεταξύ τους και έχει τα δικά του ξεχωριστά χαρακτηριστικά να προσφέρει. αλλά, δεν είναι μία λύση σε όλα τα προβλήματα της πληροφόρησης, όπως δεν είναι η κλειστή πληροφόρηση (Gibson, 2014). Η Amy Sands (σελ. 67, 2005), από την πλευρά της, υπογραμμίζει πως το OSINT δεν μπορεί να αντικαταστήσει την κλειστή πληροφόρηση. Μπορούν, ωστόσο, να υποδείξουν γενικά πεδία στα οποία πρέπει να κατευθυνθεί η μυστική πληροφόρηση.

Πέρα από την θέση που έχει ή θα πρέπει να έχει το OSINT ανάμεσα στις πηγές πληροφόρησης, μεγάλο μέρος της βιβλιογραφίας ασχολείται με την σχέση του με την παγκοσμιοποίηση, την τεχνολογία και το διαδίκτυο. Ο Leetaru (2010) υποστηρίζει πως η παγκοσμιοποίηση αυξάνει της δυνατότητες του OSINT και την σημαντικότητα για τις υπηρεσίες πληροφοριών, καθώς ακόμα και παραδοσιακά κλειστές κοινωνίες «ανοίγουν» λόγω την παγκοσμιοποίησης. Ανάλογη σκέψη για την επιρροή της παγκοσμιοποίησης διατυπώνουν και οι Shulsky & Schmitt (σελ. 146, 2002). Οι αλλαγές που ενθαρρύνουν την χρήση OSINT, δημιουργούν την ανάγκη προσαρμογής των υπηρεσιών πληροφόρησης. Ο Bărbulescu (2016) εξηγεί πως η ενσωμάτωση και χρήση του OSINT βασίζεται στην ικανότητα των υπηρεσιών πληροφόρησης να προσαρμοστούν στις νέες τεχνολογίες με ταυτόχρονη αύξηση της βαρύτητας στα στάδια συλλογής και ανάλυσης. Οι Glassman & Kang (2011) υποστηρίζουν πως μέσα από την επικοινωνία που προσφέρει το διαδίκτυο είναι δυνατόν να δημιουργηθούν ανοιχτές κοινότητες (Online Social Networks – OSN) με σκοπό την επίλυση προβλημάτων, ενισχύοντας τις δυνατότητες του OSINT. Η ιδέα αυτή μοιάζει εν μέρη με το όραμα που διατυπώνει ο Robert D. Steele για το OSINT και πιθανόν να εξηγεί γιατί ένα πολύ μεγάλο μερίδιο των ερευνών συνδέεται με το διαδίκτυο και τα κοινωνικά δίκτυα. Χαρακτηριστικό σύγγραμμα είναι αυτό των Hassan & Hijazi (2018), που έχει σκοπό να παρουσιάσει τα εργαλεία για την εύρεση και συλλογή πληροφοριών από το διαδίκτυο, ειδικά από τις πλατφόρμες κοινωνικής δικτύωσης και δεν είναι οι μόνοι. Οι Omand, Bartlett

& Miller (2012) όρισαν την πληροφόρηση από τα μέσα κοινωνικής δικτύωσης ως SOCMINT. Πολλοί ερευνητές έχουν χρησιμοποιήσει τα μέσα κοινωνικής δικτύωσης για να αντλήσουν πληροφορίες για την αξιολόγηση ψυχολογικής κατάστασης ατόμων, βάση των αναρτήσεών τους (Kandias κ.ά., 2017; Qusef & Alkilani, 2022), τον εντοπισμό ατόμων σε επιχειρήσεις έρευνας και διάσωσης (Lappas, Karampelas & Fessakis, 2021), την παρακολούθηση πανδημιών (Signorini, Segre & Polgreen, 2011). Ακόμη, μπορεί να γίνει συλλογή πληροφοριών από μια εμπόλεμη ζώνη (Hauter, 2021), ενώ η πρακτική εφαρμογή του OSINT εκτείνεται και στην παρακολούθηση των εν εξέλιξη φυσικών καταστροφών μέσα από κοινωνικά δίκτυα (Backfried κ.ά., 2012). Όμως, οι δυνατότητες πληροφόρησης από ανοιχτές πηγές δίνουν την δυνατότητα να εκτιμηθούν ή να αποκαλυφθούν μη δημόσιες πληροφορίες (Cascavilla κ.ά., 2018). Κατά αυτόν τον τρόπο, αναδεικνύεται η ικανότητα του OSINT να ξεπερνά τα όρια του ορισμού του, πράγμα το οποίο ενέχει ηθικούς κινδύνους.

Ο Hwang κ.ά. (2022) παρουσιάζουν τις νέες τάσεις στην κυβερνοασφάλεια και την δυνατότητα χρήσης OSINT για την προετοιμασία επιθέσεων. Οι επιθέσεις κυβερνοασφάλειας, σε πολλές περιπτώσεις, είναι βασισμένες σε πληροφορίες που αποκτήθηκαν μέσω κοινωνικής μηχανικής (Social engineering). Με το OSINT συλλέγονται δημόσιες πληροφορίες, ώστε να επιλεχθεί ο ανθρώπινος στόχος (Edwards κ.ά., 2017). Όμως, και τα σώματα αστυνόμευσης, από την πλευρά τους κάνουν χρήση του OSINT για την καταπολεμήσουν το κυβερνω-έγκλημα (Kanta, Coisel & Scanlon, 2020). Με βάση το OSINT αναπτύσσονται νέες τεχνικές για την παραβίαση κωδικών πρόσβασης σε ηλεκτρονικές συσκευές που έχουν κατασχεθεί. Η τρομοκρατία είναι και αυτή θεματική για την καταπολέμηση της οποίας έχει χρησιμοποιηθεί το OSINT, που μπορεί να χρησιμοποιηθεί για την πρόληψη ή και εξιχνίαση τρομοκρατικών επιθέσεων, όπως και την ανίχνευση των τρομοκρατών δικτύων (Benavides, 2011; Wiil, 2011; Bartlett & Miller, 2013; Richey & Binz, 2015; Dawson, Lieble & Adeboje, 2018). Οργανώσεις όπως η RAND και η Center for Strategic and International Studies (CSIS) έχουν μια πληθώρα δημοσιεύσεων που αφορούν τις δυνατότητες του OSINT και επιχειρηματολογούν υπέρ την χρήση του OSINT σε θέματα εσωτερικής ασφάλειας (Weinbaum, Chan, κ.ά.., 2018; Katz, 2020; CSIS, Hicks & Katz, 2021; Parachini, Williams & Roberts, 2021; Weinbaum, 2021). Λόγω του μεγάλου όγκου ανοιχτών δεδομένων και πληροφοριών (OSD, OSINF), όλο και περισσότερες έρευνες προτείνουν λύσεις με βάση την τεχνητή νοημοσύνη. Ο Evangelista κ.ά. (2021) στην έρευνα τους αναδεικνύουν πως, από το 2010 έως το 2019, σχεδόν το ένα τέταρτο των δημοσιευμένων άρθρων μελετούσαν την χρήση τεχνίτης νοημοσύνης στο OSINT. Η διαπίστωση αυτή υποστηρίζεται από την βιβλιογραφική έρευνα των Pai and Prasad (021),

όπου διαπιστώνουν πως το OSINT στο πεδίο της κυβερνοασφάλειας επωφελείται από την χρήση τεχνητής νοημοσύνης.

Στον τομέα της πληροφόρησης υπάρχει συζήτηση γύρω από την ηθική και τη νομιμότητα. Συνήθως ερευνάται μέσα από την εφαρμογή δημοκρατικού ελέγχου[9] (Konstantopoulos, 2017; Gill & Phythian, 2018) . Ο ισχυρισμός ότι το OSINT παράγεται από πηγές που συλλέγονται ηθικά και νόμιμα έχει συντελέσει στην ανάλυση αυτής της πλευράς του, καθώς υπάρχουν πολλά αδιευκρίνιστα σημεία. Η ten Hulsen (2020) αναδεικνύει την αυξανόμενη χρήση του OSINT σε ποινικές έρευνες σε συνδυασμό την προστασία των προσωπικών δεδομένων. Επιχειρεί να δημιουργήσει τη κατάλληλη θεωρητική δομή, ώστε να ισορροπηθούν οι ανάγκες της ποινικής έρευνας αλλά και οι ανησυχίες για την προστασία προσωπικών δεδομένων. Ο Κάνδιας κ.ά. (2017) σε ποσοτική έρευνα ανέπτυξαν μέθοδο ανίχνευσης στρες μέσα από την ανάλυση δημόσιου περιεχομένου από χρήσεις σε πλατφόρμες κοινωνικής δικτύωσης. Η έρευνά τους αναδεικνύει, όπως σημειώνουν και οι ίδιοι, πως οι τεχνικές αυτές έχουν την δυνατότητα να καθαιρέσουν των διαχωρισμό μεταξύ δημόσιας και ιδιωτικής ζωής. Αυτό δημιουργεί ηθικές επιπλοκές, διότι οι πληροφορίες δημοσιεύτηκαν χωρίς πρόθεση να αποκαλυφθεί η κατάσταση ψυχικής υγείας. Συμφωνώντας με των Κάνδια, οι Bohm και Lolagar (2021) αναφέρουν πως «*ότι είναι τεχνολογικά δυνατό, δεν είναι πάντα ηθικό».* Από νομικής πλευράς, σχολιάζουν πως στην περίπτωση της Γερμανίας υπάρχει κάποια νομική προστασία των ατόμων που απορρέει από την πανευρωπαϊκή εφαρμογή του General Data Protection Regulation (GDPR). Όμως, ακόμη και αυτό χρίζει περαιτέρω διευκρίνισης, όσον αφορά το επιτρεπόμενο εύρος δράσης του OSINT. Οι Koops, Hoepman και Leenes, (2013) προτείνουν να συνδυασμό μεθόδων κατά τη συλλογή, αλλά και κατά την ανάλυση των δεδομένων, με στόχο την προστασία των ευαίσθητων δεδομένων. Σύμφωνα με αυτούς, είναι απαραίτητο στοιχείο, ώστε το OSINT να καταστεί κοινωνικά αποδεχτό.

Βασικά σημεία που είναι σημαντικά να αναδειχθούν από την βιβλιογραφική ανασκόπηση έχουν να κάνουν με την χρήση του OSINT από υπηρεσίες πληροφόρησης, την σημασία τεχνολογίας και την ηθική-νομική διάσταση. Πρώτον, ξεκινώντας από την βιβλιογραφία που αφορά την το OSINT και την χρήση του από υπηρεσίες πληροφόρησης, φαίνεται πως είναι σε χρήση και έμφαση δίνεται στο να απαντηθεί πόσο θα εξελιχθεί στο μέλλον και αν θα ξεπεράσει τις υπάρχουσες πηγές πληροφόρησης. Όπως έχει αναφερθεί στην εισαγωγή, αυτό αφήνει ανοιχτό το ερώτημα του κατά πόσο σημαντικό είναι το OSINT αυτή την στιγμή στις δομές πληροφόρησης των ΗΠΑ και Η.Β. Δεύτερον, στην χρήση του

[9] Democratic Oversight

OSINT σε πολλαπλά πεδία (τρομοκρατία, κυβερνοασφάλεια, εσωτερική ασφάλεια κ.ά.), φαίνεται πως είναι πολύ σημαντική η ύπαρξη του διαδικτύου και των τεχνολογιών για την άντληση και τη διαχείριση των δεδομένων, καθώς και για τη διάδοσή τους. Τρίτον, η ηθική και η νόμιμη χρήση του OSINT είναι καθοριστικής σημασίας. Σε πολλές περιπτώσεις υπάρχει απόκλιση μεταξύ του σκοπού που έχει ο δημιουργός της πληροφορίας και τον σκοπό που έχει ο τελικός καταναλωτής της πληροφόρησης μέσω OSINT. Το αποτέλεσμα μπορεί υπό περιπτώσεις να είναι επικίνδυνο για τα άτομα που δημιουργούν τις πηγές υποχρεώνοντάς τους (και άλλες πιθανές πηγές) να μην προσφέρουν ελεύθερα πληροφορίες.

Κεφάλαιο 3 - Μεθοδολογία Έρευνας

Σε αυτό το κεφάλαιο θα γίνει περιγραφή της μεθοδολογίας της έρευνας, ενώ παράλληλα θα επεξηγηθεί ο λόγος για τον οποίο έγιναν οι συγκεκριμένες επιλογές. Η αποτίμηση αυτή δίνει τη δυνατότητα ελέγχου της εγκυρότητας, μέσω της επανάληψης και της κριτικής των επιλογών που έγιναν (Παπαγεωργίου, χ.χ.). Χάρη ευκολίας υπενθυμίζεται πως σκοπός της εργασίας είναι να παρουσιάσει την σημαντικότητα των ανοιχτών πηγών πληροφόρησης (OSINT) ως εργαλείο για τις υπηρεσίες πληροφοριών στο πλαίσιο της εθνικής ασφάλειας και στόχοι της εργασίας είναι να:

1. Ερευνηθούν τα κίνητρα και αντικίνητρα της χρήσης πληροφόρησης από ανοιχτές πηγές.
2. Εκτιμηθεί η σημασία της χρήση ανοιχτών πηγών πληροφόρησης από τις υπηρεσίες πληροφόρησης των ΗΠΑ και του ΗΒ.

Οι στόχοι της εργασίας χωρίζονται στα εξής ερωτήματα:

1. Πώς έχει εξελιχθεί ιστορικά η συλλογή πληροφοριών από υπηρεσίες πληροφόρησης χρησιμοποιώντας ανοιχτές πηγές;
2. Ποια είναι τα κίνητρα συλλογής πληροφοριών από ανοιχτές πηγές για υπηρεσίες πληροφόρησης;
3. Ποια είναι τα αντικίνητρα συλλογής πληροφοριών από ανοιχτές πηγές για υπηρεσίες πληροφόρησης;
4. Πως έχει εφαρμοστεί η πληροφόρηση από ανοιχτές πηγές στις ΗΠΑ;
5. Πως έχει εφαρμοστεί η πληροφόρηση από ανοιχτές πηγές στο ΗΒ;
6. Ποιες οι διαφορές, ομοιότητες μεταξύ ΗΠΑ και ΗΒ, όσον αφορά την πληροφόρηση από ανοιχτές πηγές;

Η εργασίας ακολουθεί αφαιρετική προσέγγιση, ξεκινώντας με την θεωρία του OSINT και προσπαθώντας να εντοπιστεί η εφαρμογή του μέσα από την παρατήρηση των πράξεων των υπηρεσιών πληροφόρησης. Με τον τρόπο αυτό μπορεί να ελεγχθεί η θεωρία που έχει διατυπωθεί. Η εργασία βασίζεται σε ποιοτική έρευνα και δεν θα χρησιμοποιηθούν ποσοτικά δεδομένα για να δοκιμαστούν ή να σχηματιστούν νέες θεωρίες. Το θέμα της εργασίας, ο στόχος της και τα ερωτήματα απαντώνται καλύτερα

μέσα από την παρουσίαση και την ανάλυση της θεωρίας, σε συνδυασμό με μελέτη περιπτώσεων. Ο χαρακτήρας της εργασίας και του θέματος δεν δίνει τη δυνατότητα συλλογής ποσοτικών δεδομένων ή ανάθεσης αριθμητικών τιμών σε ποσοτικά δεδομένα. Μέσα από την επιλογή της ποιοτικής μεθόδου μας δίνεται η δυνατότητα παράθεσης της θεωρίας που πλαισιώνει το OSINT και η ευκαιρία για εντοπισμό της χρήσης τους από τις υπηρεσίες πληροφοριών.

Με την επιλογή ποιοτικής μεθόδου δίνεται η δυνατότητα να χρησιμοποιηθεί η στρατηγική της μελέτης περιπτώσεων. Η εργασία θα επικεντρωθεί στη μελέτη της χρήσης του OSINT από τις εθνικές υπηρεσίες ασφάλειας των ΗΠΑ και ΗΒ. Οι δύο χώρες επιλέχτηκαν διότι έχουν πολλαπλά κοινά χαρακτηριστικα όπως η γλώσσα, η αγγλοσαξονική κουλτούρα και το φιλελεύθερο πολιτικό σύστημα (Phythian, 2014). Παράλληλα, αν και υπάρχει εγγενή δυσκολία στην μελέτη υπηρεσιών πληροφόρησης τα οποία προστατεύουν παρά δημοσιοποιούν πληροφορίες, λόγω της κουλτούρας της διαφάνειας υπάρχει μεγάλη δεξαμενή πρωτογενών και δευτερογενών πηγών. Επιπλέον, η ύπαρξη αυτών των πηγών στα αγγλικά δίνει την δυνατότητα χρήσης τους χωρίς τη χρονική και τη χρηματική επιβάρυνση που προκαλεί η μετάφραση τους. Τέλος, με την επιλογή της στρατηγικής αυτής επιχειρείται να εκτιμηθεί εάν και πόσο σημαντικό είναι το OSINT στη λειτουργία τους.

Η συλλογή των πρωτογενών και δευτερογενών πηγών έγινε σε δύο περιόδους Νοέμβριο – Οκτώβριο του 2021 και Ιανουάριο του 2022. Η πρώτη περίοδος συμπίπτει με την εκκίνηση του προγράμματος συγγραφής της εργασίας. Για να εντοπιστούν τυχόν νέες πηγές, διεξήχθη η δεύτερη περίοδος συλλογής, όμως δεν προστέθηκε σημαντικός αριθμός νέων ερευνών. Για την εύρεση σχετικών με το θέμα πηγών η αναζήτηση ξεκίνησε μέσω από το google scholar. Οι λέξεις κλειδιά που χρησιμοποιήθηκαν ήταν: ανοιχτές πηγές πληροφόρησης, open source intelligence, OSINT, national, intelligence, USA, United States of America, UK, United Kingdom. Με βάση τα αποτελέσματα της αναζήτησης αποθηκεύτηκαν όσα αρχεία ήταν ελεύθερα προσβάσιμα και δεν απαιτούσαν πληρωμή. Με την αρχική συλλογή άρθρων εντοπίστηκαν σημαντικοί ερευνητές στον πεδίο της πληροφόρησης και των ανοιχτών πηγών, τα κύρια ακαδημαϊκά περιοδικά και των κύριων εκδοτικών οίκοι. Αυτές οι πληροφορίες χρησιμοποιήθηκαν για να αναζητηθεί περισσότερο υλικό. Τέλος, όλο το υλικό το οποίο βρέθηκε μέσα από αυτήν την διαδικασία αξιολογήθηκε έχοντας ως κριτήριο την σχετικότητα με τα ερωτήματα της εργασίας. Από τις πηγές που κρίθηκαν σχετικές, χρησιμοποιήθηκαν οι βιβλιογραφικές παραπομπές για να εντοπιστούν επιπλέον πηγές. Για την καταγραφή των πηγών χρησιμοποιήθηκε το πρόγραμμα

Mendeley. Η βιβλιογραφία που συλλέχτηκε αναλύθηκε με στόχο των εντοπισμό κοινών θεμάτων, που να απαντούν στις ερωτήσεις της εργασίας. Κατά αυτόν τον τρόπο, έγινε πιο εύκολη η διαχείριση των πηγών και εντοπίστηκαν οι συγκρουόμενες ή και συμπληρωματικές απόψεις.

Με την επιλογή των παραπάνω μεθόδων έρευνας υπάρχουν και περιορισμοί στην ανακάλυψη πηγών. Η επιλογή των ΗΠΑ και ΗΒ για την μελέτη περίπτωσης δεν δίνει την δυνατότητα γενίκευσης των συμπερασμάτων, όμως μπορούν να αντληθούν ιδέες για το πως μπορεί να εφαρμοστεί παρόμοια έρευνα με επιλογή άλλων κρατών. Όσον αφορά την αναζήτηση βιβλιογραφίας, αυτή έγινε στα αγγλικά και στα ελληνικά, αφήνοντας εκτός βιβλιογραφία σχετική σε άλλη γλώσσα. Ωστόσο, αυτό πολύ πιθανόν να έχει μικρή επίπτωση στην θεωρητική ανάλυση, διότι ο κύριος όγκος των ερευνών στο πεδίο της πληροφόρησης και του OSINT είναι στα αγγλικά και προέρχεται από Αμερικανούς και Βρετανούς ερευνητές (Johnson, 2014; Konstantopoulos and Doga, 2015).

Κεφάλαιο 4 - Ανοιχτές Πηγές Πληροφόρησης

« Η πιο επικίνδυνη φράση στην γλώσσα είναι:

Πάντα το κάναμε με αυτόν τον τρόπο.»

- Υποναύαρχος (ΗΠΑ), Γκρέις Χόπερ

4.1 Εξέλιξη των Ανοιχτών Πηγών Πληροφόρησης

Πληροφόρηση από ανοιχτές πηγές δεν είναι σύγχρονο φαινόμενο και υπάρχουν ιστορικές αναφορές που το αποδεικνύουν. Ο Gibson (2014, σελ. 124) αναφέρει πως, το 1808, ο Ουέλλινγκτον συγκέντρωσε τους στρατηγούς του, πριν αναχωρήσει για τον Πόλεμο της Ιβηρικής Χερσονήσου και επέκρινε την άγνοιά που είχα για τους νέους σχηματισμούς πεζικού του Ναπολέοντα, του οποίους ανέφερε ανοιχτά η εφημερίδα «Times». Το 1826, ο Henry Brougham, ριζοσπάστης πολιτικός των Whig, ίδρυσε την Εταιρεία για τη Διάχυση της Χρήσιμης Γνώσης. Στόχος του ήταν: «να μεταδώσει χρήσιμες πληροφορίες σε όλες τις τάξεις της κοινότητας». Η εταιρία έπαυσε να λειτουργεί το 1848 καθώς προϊόν της θεωρήθηκε άτακτο, ετερόκλητο και δεν απέκτησε την απαραίτητη στήριξη. Επίσης, το 1898, για πρώτη φορά, δημοσιεύτηκε εμπορικά η σειρά βιβλίων «Fighting Ships» της Jane. Η εταιρία συνεχίζει ακόμα και σήμερα τη δραστηριότητα της παρέχοντας υπηρεσίες πληροφόρησης από ανοιχτές πηγές (Janes | What we do, χ.χ.).

Ο σχηματισμός θεσμικών οργανώσεων, «κρατικής υποστήριξης», μέσω των οποίων οι ανοιχτές πηγές πληροφοριών αξιοποιούνται σύμφωνα με την σύγχρονη έννοια της πληροφόρησης μπορεί να αποδοθεί στην δημιουργία της υπηρεσίας British Broadcasting Corporation Monitoring (BBCM) το 1938, στο Η.Β.. Το αντίστοιχο στις ΗΠΑ, το Foreign Broadcast Monitoring Service (FBMS), δημιουργήθηκε το 1941 (Williams and Blum, 2018, σελ. 4). Και τα δύο ήρθαν ως αποτέλεσμα της εφεύρεσης του ραδιοφώνου και ιδίως της χρήση του τη δεκαετία του 1930 ως εργαλείο για τη διάδοση προπαγάνδας, από τις Δυνάμεις του Άξονα. Η δραστηριότητα των δύο υπηρεσιών εκτεινόταν πέρα από την δραστηριότητα της συλλογής μέσα από παρακολούθηση των ραδιοτηλεοπτικών μέσων. Μετρούσαν την ανταπόκριση στη εκπομπή προπαγάνδας από τους συμμάχους. Αυτή λέξη «παρακολούθηση» χρησιμοποιούνταν για την συλλογή ανοικτών πηγών και η «αναχαίτιση» για τις μυστικές πηγές. Η κατηγοριοποίηση αντανακλά την φύση των δεδομένων που

διαβιβάζονται – δημόσιο έναντι μυστικό – και την προσπάθεια απόκρυψης από τον στόχο του τρόπου που πραγματοποιείται η συλλογή δεδομένων (Gibson, 2014, σελ. 124).

Στον Ψυχρό Πόλεμο, το TECHINT (Technical Intelligence) και το SIGINT διείσδυαν στη μυστικοπαθή φύση της κοινωνίας του «Ανατολικού Μπλοκ» και ο δορυφόρος έγινε συνώνυμο του διαδικτύου ως μέσω συλλογής πληροφοριών στην εποχή μας. Κατά την διάρκεια του Ψυχρού πολέμου κυριάρχησε η μυστικότητα προκειμένου να προστατεύονται οι τεχνολογικές δυνατότητες, οι πηγές, οι μέθοδοι και το προϊόν από τον «εχθρό». Αν και η προσήλωση στην μυστικότητα δεν χαρακτήριζε μόνο την Σοβιετική Ένωση και το κουμμουνιστικό καθεστώς, αυτή μπορούσε να χρησιμοποιήσει με μεγαλύτερη αποτελεσματικότητα τη λογοκρισία ως όργανο αντιπληροφόρησης. Η βαρύτητα συλλογής ανοιχτών πληροφοριών είναι μικρότερη σε σχέση με την συλλογή μυστικών πληροφοριών, εντούτοις οργανισμοί όπως το Ερευνητικό Κέντρο Σοβιετικών Σπουδών, στο Ηνωμένο Βασίλειο, εξελίχθηκαν παράλληλα με το BBCM για να αποκαλύψουν δυνατότητες και προθέσεις μέσα από την εξέταση ανοιχτών πληροφοριών (Gibson, 2014). Στις ΗΠΑ διάφορες υπηρεσίες πληροφόρησης παρακολουθούσαν και κατέγραφαν για χρόνια τις αυξανόμενες ακαδημαϊκές και δημοσιεύσεις στην Σοβιετική Ένωση (Bagnall, 1958).

Η εκμετάλλευση ανοιχτών πηγών δεν είναι καινούργια. Όμως η σύγχρονη συζήτησή του αντικατοπτρίζει τον αυξανόμενο όγκο, την αμεσότητα και την εύκολη πρόσβαση που προφέρουν οι σημερινές φορητές ψηφιακές τεχνολογίες (Gibson, 2014). Προσφέρουν νέες πλατφόρμες για την πληροφόρηση, καθώς και μια «νέα», πιο «ανοιχτή» παγκοσμιοποιημένη κοινωνία (Shulsky and Schmitt, σελ. 141-142, 2002). Το OSINT ανθίζει εκ νέου, αυτό οφείλεται τόσο στην τεχνολογική εξέλιξη όσο και στο άνοιγμα των πρώην κλειστών κοινωνιών (Williams and Blum, σελ. 4, 2018). Με αφετηρία την επιρροή που φαίνεται να έχει η τεχνολογική και κοινωνική εξέλιξη στην ανάπτυξη του OSINT, διαφαίνονται τα κίνητρα και τα αντικίνητρα εξέλιξης αυτής της πηγής πληροφόρησης από τις υπηρεσίες πληροφοριών. Στα κίνητρα συμπεριλαμβάνονται οι κοινωνικές και πολιτικές αλλαγές που έχουν επέλθει λόγω της παγκοσμιοποίησης και της κατανομής ισχύος στο διεθνές σύστημα κρατών. Ενώ στα αντικίνητρα συγκαταλέγονται οι τάσεις για συντήρηση του status quo από τις υπηρεσίες πληροφόρησης, μαζί με τεχνολογικούς περιορισμούς.

4.2 Κίνητρα και αντικίνητρα χρήσης των Ανοιχτών Πηγών Πληροφόρησης

4.2.1 Κίνητρα

Η εποχή της πληροφόρησης έχει επηρεάσει τον τρόπο με τον οποίο λειτουργούν πολλές οργανώσεις, ειδικά επιχειρήσεις και κυβερνήσεις (Shulsky & Schmitt, σελ. 22 2002). Οι απαιτήσεις για την πληροφόρηση πληθαίνουν από άποψη θεμάτων που πρέπει να καλυφθούν, αλλά και από άποψη ταχύτητας με ζητούμενο τη γρήγορη παράδοση εκθέσεων με βάση τις οποίες μπορούν να ενεργήσουν η πολιτική και η στρατιωτική ηγεσία. Ταυτόχρονα, η πιθανή επίπτωση τόσο των γνωστών απειλών όσο και των ασύμμετρων απειλών αυξάνεται, μεγεθύνοντας το συνολικό κόστος σε περίπτωση αστοχιών (Quiggin, 2006). Η πληροφόρηση ως μέσο προειδοποίησης και κατανόησης είναι βασικό στοιχείο του παγκόσμιου αγώνα για ισχύ. Ο Steele (σελ. 580, 2001) υποστηρίζει πως η ισχύς μετατοπίζεται από κράτη σε οργανώσεις και άτομα, από «μυϊκή δύναμη» σε «εγκεφαλική δύναμη». Χρησιμοποιώντας ως παράδειγμα τις ΗΠΑ, αναφέρει πως οι προκλήσεις των μελλοντικών προέδρων θα περιστρέφονται γύρω από την πληροφόρηση. Η αντιμετώπιση των προκλήσεων οδηγεί στην αλλαγή των σχέσεων μεταξύ προέδρου και γραφειοκρατίας, αλλά και τις σχέσεις του προέδρου με τις μη κυβερνητικές οργανώσεις (Steele, σελ. 580, 2001). Οι αναδυόμενες τεχνολογίες ήδη αναδιαμορφώνουν τον τρόπο με τον οποίο οι υπηρεσίες πληροφόρησης συλλέγουν, αποθηκεύουν και επεξεργάζονται πληροφορίες, αλλά πιθανότατα θα μεταμορφώσουν όλες τις βασικές πτυχές του κύκλου πληροφόρησης τις επόμενες δεκαετίες - από τη συλλογή στην ανάλυση και στη διάδοση (Katz, 2020).

Οι υπηρεσίες πληροφοριών είναι συνηθισμένες να αντιμετωπίζουν απειλές μεγάλων διαστάσεων σε στρατηγικό επίπεδο στην μορφή άλλων κρατών (Steele, 2002, σελ. 8). Οι νέες προκλήσεις και απειλές υπήρχαν και παλαιότερα, όμως οι επιπτώσεις τους για την ασφάλεια των κρατών έχουν μεγεθυνθεί. Έχουν υπάρξει αλλαγές στο διεθνές περιβάλλον μετά τον Ψυχρό Πόλεμο και την ψηφιακή επανάσταση και αυτό δημιουργεί την ανάγκη των κρατών να προσαρμοστούν στις νέες προκλήσεις όπως η τρομοκρατία, τα περιβαλλοντικά ζητήματα και οι υβριδικές/ασύμμετρες απειλές, με την αξιοποίηση της αυξανόμενης ροής ανοιχτών πληροφοριών και δεδομένων (Minas, 2010). Εξετάζοντας τις υπηρεσίες πληροφόρησης των ΗΠΑ η Weinbaum κ.ά. (κεφ. 6, 2018), διακρίνει πως υπάρχει ανεπαρκής συλλογή και αναλυτική κάλυψη σε πολλούς τομείς, επειδή η πλειονότητα των πόρων της αφιερώνεται, εκ σχεδιασμού, στην Κίνα, τη Ρωσία, τη Βόρεια Κορέα, το Ιράν και τον διεθνή βίαιο εξτρεμισμό. Επιπλέον, το σύστημα πληροφόρησης των ΗΠΑ είναι στημένο για συλλογή πληροφοριών σε ειρηνικές περιόδους και δεν ανταποκρίνεται στις

ανάγκες που δημιουργούν οι κρίσεις και οι εντάσεις σε ανυποψίαστες περιοχές και χρονικές στιγμές. Μαζί με τις νέες προκλήσεις αναπτύσσεται και η χρήση του OSINT ως ανταπάντηση, για να καλύψει τα κενά της παραδοσιακής πληροφόρησης προδίδοντας της μια νέα διάσταση (Weaver, 2008; de Bochgrave, Sanderson & MacGaffin, 2006). Παρακάτω τα παρουσιαστούν οι τρόποι με τους οποίους το OSINT απαντούν στις νέες προκλήσεις.

4.2.1.1 Συμπλήρωση δυνατοτήτων και έγκαιρη προειδοποίηση.

Σύμφωνα με τον νόμο του Μέρφι τα πράγματα πάνε πάντα στραβά όταν και όπου δεν αναμένεται. Αυτό μπορεί να συμβεί στους μεγαλύτερους και στους καλύτερα προετοιμασμένους οργανισμούς καθώς και στους μικρότερους. Παράδειγμα αποτελούν οι Γιουγκοσλαβικοί πόλεμοι. Όλη η Ευρώπη και το ΝΑΤΟ είχαν προετοιμαστεί για πιθανό θερμό πόλεμο που θα μπορούσε να ξεσπάσει στην Ευρώπη. Ωστόσο, αμέσως μετά τον Ψυχρό Πόλεμο, ξέσπασαν μάχες στη Γιουγκοσλαβία. Προς έκπληξη πολλών, ανακαλύφθηκε γρήγορα ότι λίγα ήταν γνωστά για αυτήν την ευρωπαϊκή χώρα, σε σημείο που οι πρώτοι στρατιώτες που πήγαν ως μέρος της αποστολής παρακολούθησης της Ευρωπαϊκής Κοινότητας και της Δύναμης Προστασίας των Ηνωμένων Εθνών το έκαναν χρησιμοποιώντας χάρτες από μη στρατιωτικές πηγές - τον Οδηγό Michelin (Quiggin, σελ. 167, 2007). Οι πρόσφατες εμπειρίες έχουν επιβεβαιώσει την ιδέα ότι μια κρίση θα προέλθει από ένα ασήμαντο γεγονός ή μια ξεχασμένη περιοχή. Μεταξύ των πρόσφατων παραδειγμάτων είναι η επίθεση στους δίδυμους πύργους την 11η Σεπτεμβρίου 2001, το SARS COV του 2003 (WHO, 2003), οι βομβιστικές επιθέσεις στο Λονδίνο τον Ιούλιο του 2005 (Κυρανούδη, 2015), οι μάχες στον Λίβανο τον Ιούλιο του 2006, η επίθεση στο USS Cole το 2000, η διαμάχη για τα δανικά καρτούν, η Σρεμπρένιτσα και η Ρουάντα. Είναι αδύνατο για οποιεσδήποτε παραδοσιακές υπηρεσίες πληροφοριών, ανεξάρτητα από το πόσο καλά χρηματοδοτούνται ή εξοπλίζονται, να διατηρήσουν κάλυψη για κάθε πιθανό σενάριο.

Για την αντιμετώπιση αιφνίδιων απειλών ή κρίσεων, η πιο πιθανή πηγή άμεσης πληροφόρησης είναι το OSINT. Ανεξάρτητα από τη γεωγραφική ή θεματική φύση της κρίσης, θα υπάρχουν άνθρωποι που έχουν εμπλακεί και έχουν την δυνατότητα να παρέχουν πληροφορίες όπως ακαδημαϊκοί και μη κυβερνητικοί οργανισμοί (Quiggin, σελ. 167, 2007). Με τις ασύμμετρες απειλές να αυξάνονται, υπάρχει μια ολοένα αυξανόμενη πιθανότητα να προκύψει μια κρίση σε περιοχή ή από μια πηγή που δεν βρίσκεται στη λίστα προτεραιότητας των υπηρεσίας πληροφοριών. Η ικανότητα τους OSINT βρίσκεται στην ικανότητα εύρεσης πληροφορίων από ειδικές πηγές σε ελάχιστο χρόνο. Στις περισσότερες περιπτώσεις, ο

χρόνος παράδοσης μισής έως μίας ώρας θα πρέπει να παρέχει σε έναν οργανισμό επαρκή χρόνο για μια άμεση και γενική αξιολόγηση της φύσης της κρίσης και των εμπλεκόμενων παραγόντων. Μία έως τέσσερις ώρες θα πρέπει να δώσει χρόνο στην υπηρεσία για μια πιο προσεκτική ανασκόπηση των περιπλοκών του ζητήματος και εντός μιας ημέρας, η υπηρεσία θα πρέπει να είναι σε θέση να παρέχει άμεση, σε βάθος εμπειρογνωμοσύνη και συμβουλές στην ηγεσία. Αυτό, φυσικά, προϋποθέτει ότι ο οργανισμός έχει αναπτύξει την παραγωγής OSINT εκ των προτέρων (Quiggin, 2007, σελ. 166-167).

Το πλεονέκτημα των ασύμμετρων/υβριδικών απειλών βρίσκεται στο ότι επισκοτίζουν τις προθέσεις και εκμεταλλεύονται τα «κενά» της παραδοσιακής πληροφόρησης. Το OSINT αναιρεί έως έναν βαθμό το πλεονέκτημα του αιφνιδιασμού (Steele, 2002, κεφ. 3; Quiggin, 2007). Ο συνδυασμός των πληροφοριών από ανοιχτές πηγές μαζί με μυστικές πληροφορίες οδηγεί σε ανώτερο προϊόν πληροφόρησης από ότι η χρήση μόνο ανοιχτών πηγών ή μόνο μυστικών πληροφοριών (Weinbaum, Parachini, κ.ά.., 2018). Οι ανοιχτές πηγές μπορούν και να λειτουργούν ως ένα μέσο για την δημιουργία θεμελιακής πληροφόρησης για ένα ζήτημα ή μια περιοχή. Χαρτογραφώντας το τι είναι διαθέσιμο και «γνωστό» ως πληροφορία, δίνει χρόνο μέχρι να κατευθυνθούν οι παραδοσιακοί μέθοδοι συλλογής και εντοπίζει τις περιοχές όπου πρέπει να χρησιμοποιηθούν για την ανακάλυψη πληροφοριών που δεν είναι δημόσια. Έπειτα παράγεται πληροφόρηση με συνδυασμό ανοιχτών και μυστικών πληροφοριών, παρέχοντας υψηλού επιπέδου καθοδήγηση στην πολιτική και στρατιωτική ηγεσία.

4.2.1.2 Ολοκληρωμένη εικόνα.

Η πληροφόρηση που βασίζεται εξολοκλήρου σε μυστικές πληροφορίες έχει σοβαρούς περιορισμούς, όταν απαιτείται η εκτενής κατανόηση του προβλήματος για να σχηματιστεί μια πολύπλευρη και αποτελεσματική πολιτική. Πολύ συχνά οι εκθέσεις που παρουσιάζονται στην πολιτική ή στην στρατιωτική ηγεσία αποτελούνται από μια σειρά πληροφοριών που δεν συνδέονται μεταξύ τους ή με κάποια θεματική. Αντί αυτού μοιάζουν πιο πολύ με μια συλλογή από ενδιαφέρουσες πληροφορίες, χωρίς να οδηγούν σε ολοκληρωμένη εικόνα και κατανόηση των θεμάτων. Αυτό το χαρακτηριστικό δημιουργεί περισσότερα προβλήματα στην προσπάθεια χάραξης πολιτικής από όσα λύνει. Συνήθως οι εκθέσεις που παράγονται από υπηρεσίες πληροφόρησης αντικατοπτρίζουν τα δεδομένα που έχουν συλλεχθεί από τα ίδιες, απορρίπτοντας πληροφορίες από άλλες υπηρεσίες. Επόμενως, τείνουν να έχουν μια μονόπλευρη οπτική.

Ο Κόλιν Πάουελ, πρώην Πρόεδρος του Γενικού Επιτελείου Στρατού και πρώην Υπουργός Εξωτερικών των ΗΠΑ, δήλωσε πως προτιμούσε το «Early Bird» με τη σύνοψή των εφημερίδων από ότι το «Daily Brief» (Presidents's Daily Brief – PDB) του Προέδρου, που συντάσσεται από την Central Intelligence Agency (CIA) (Quiggin, σελ. 168, 2007). Αναφορικά με την ημερήσια ενημέρωση του Προέδρου των ΗΠΑ (Presidents's Daily Brief – PDB). Ο Treverton (σελ. 106, 2004,) αναφέρει πως, είναι ένα προϊόν σήμα κατατεθέν της CIA του προσωπικού που την στελεχώνουν και την έμφαση σε μυστικές πληροφορίες. Η ημερήσια ενημέρωση παραδίδεται κάθε πρωί σε ανώτατους αξιωματούχους, όμως αντί για ένα συνεκτικό κείμενο, παρουσιάζονται αποσπασματικές πληροφορίες που δεν οικοδομούν συνεκτική εικόνα γύρο από ένα θέμα, ενώ οι πληροφορίες δεν συνδυάζονταν με ενημερώσεις των προηγούμενων ημερών, με αποτέλεσμα να μην υπάρχει δυνατότητα ιεράρχησης την σημαντικότητάς τους.

Η μυστική πληροφόρηση και οι υπηρεσίες που την διεξάγουν έχουν πρόσβαση σε μια σειρά από κομμάτια πληροφοριών που έχουν συλλέξει (Quiggin, 2007, σελ. 168-170). Όμως, αν και είναι πολύτιμες και κάποιες φορές ζωτικής σημασίας πληροφορίες, οι υπηρεσίες πληροφοριών δεν είναι εκπαιδευμένες στο να συνθέτουν μια «μεγάλη εικόνα». Έτσι, πληροφορίες με υψηλή διαβάθμιση αποτελούν ένα μόνο ένα κομμάτι του παζλ και για αυτό τον λόγο είναι αναγκαίο να υπάρχουν επιπλέον πληροφορίες που τις πλαισιώνουν (Treverton, 2004, σελ. 106-107). Σε αυτή την πλαισίωση διαδραματίζει καταλυτικό ρόλο η ενσωμάτωση του OSINT στις εκθέσεις των υπηρεσιών πληροφόρησης.

4.2.1.3 Ευελιξία επικοινωνίας.

Η συλλογή πληροφοριών από μυστικές πηγές οδηγεί, χωρίς εξαίρεση, στο λάβουν κάποιου βαθμού διαβάθμισης. Με την διαβάθμιση πληροφοριών ελέγχεται η πρόσβαση σε αυτές αλλά περιορίζεται και ο αριθμός των ατόμων με πρόσβαση. Αυτό γίνεται στα πλαίσια της αντιπληροφόρησης που προσπαθεί να προστατέψει τις πληροφορίες καθαυτές ή την μέθοδο συλλογής τους. Ένα από τα μεγαλύτερα προβλήματα σε αυτό το σύστημα είναι πως οι υπηρεσίες δεν μοιράζονται πληροφορίες μεταξύ τους και επιπλέον δεν μπορούν να τις μοιραστούν με άτομα και οργανώσεις που δεν έχουν τον απαραίτητο βαθμό διαβάθμισης. Αυτή η πραγματικότητα στερεί από αναλυτές σημαντικό υλικό που επηρεάζει την ποιότητα της ανάλυσής τους. Επιπλέον, η συγκράτηση όλων των πληροφοριών εντός του συστήματος των υπηρεσιών πληροφόρησης έχει επίπτωση στην δυνατότητα επικοινωνίας με τους πολιτικούς, τον ιδιωτικό τομέα, την ακαδημαϊκή κοινότητα, τους εμπειρογνώμονες και τους πολίτες.

Το OSINT επιτρέπει μεγαλύτερη ευελιξία παροχής πληροφοριών όταν οι υπηρεσίες πληροφοριών έχουν να κάνουν με πολιτικούς, γραφειοκράτες, ξένους και εγχώριους εταίρους και άλλες υπηρεσίες. Το ίδιο ισχύει όταν οι υπηρεσίες πληροφοριών και τα σώματα ασφαλείας αντιμετωπίσουν νομικές διαδικασίες ή δημόσιες ακροάσεις. Ο πιο προφανής λόγος για αυτό είναι ότι το OSINT προέρχεται από πληροφορίες που συλλέχθηκαν από πηγές στις οποίες όλοι έχουν πρόσβαση, δηλαδή, όταν οι πληροφορίες διαβιβάζονται στη δημόσια σφαίρα και δεν χρειάζεται προσπάθεια απόκρυψης των πηγών από όπου προήλθαν. Επιπλέον, εάν μια υπηρεσία κατέχει πληροφορίες οι οποίες είναι διαβαθμισμένες, το OSINT δίνει την δυνατότητα να εφαρμοστεί μια διαδικασία «αντίστροφης μηχανικής». Εάν μια υπηρεσία έχει διαβαθμισμένες πληροφορίες που θέλει να χρησιμοποιήσει δημόσια, αλλά υπάρχει έγκυρος λόγος για τον οποίο είναι διαβαθμισμένες, τότε αυτή η υπηρεσία μπορεί να αναζητήσει τις ίδιες πληροφορίες από ανοιχτές πηγές. Η εμπειρία έχει δείξει ότι είτε μπορούν να βρεθούν οι ίδιες πληροφορίες ή τουλάχιστον πληροφορίες που είναι αρκετά κοντά, ώστε να συνθέτουν την ίδια γνώση, αλλά που να μπορούν να δημοσιοποιηθούν (Quiggin, σελ. 168, 2007).

Ο συνδυασμός ανοιχτών και διαβαθμισμένων πηγών μειώνει το επίπεδο της διαβάθμισης και καθιστά την πληροφορία πιο προσιτή για κυβερνητικούς αξιωματούχους και συμμάχους. Έτσι, η πρόσβαση σε πληροφορίες από όλες τις πηγές διευκολύνει την λήψη αποφάσεων, καθώς φτάνει σε χαμηλότερα κλιμάκια και δεν παραμένει κρυμμένη (Weinbaum, Parachini, κ.ά., 2018). Σε θέματα κυβερνοασφάλειας αλλά και τρομοκρατίας είναι ιδιαίτερα σημαντικό να υπάρχει η δυνατότητα αμφίδρομης επικοινωνίας. Πολύ συχνά, μη κυβερνητικές οργανώσεις, κοινωνικά δίκτυα και άτομα είναι πολύ πιο κοντά στην καθημερινότητα και στην πραγματικότητα για την οποία μία υπηρεσία πληροφοριών προσπαθεί να συλλέξει πληροφορίες.

4.2.1.4 Παρακολούθηση Παγκόσμιων Θεμάτων

Μία από τις ανεξερεύνητες, από τις υπηρεσίες πληροφοριών, πτυχή του OSINT, είναι η ικανότητά του να παρακολουθεί παγκόσμια ζητήματα κρίσιμης φύσης όπως οι πανδημίες, το περιβάλλον και ο τζιχαντισμός. Αυτή η τεράστια δυνατότητα χρησιμοποιείται από ακαδημαϊκούς, όμως δεν έχει γίνει ακόμη κοινή πρακτική στις υπηρεσίες πληροφοριών, παρά το χαμηλό κόστος. Σε έκθεσή του ο Παγκόσμιος Οργανισμός Υγείας τάσσεται ξεκάθαρα υπέρ της δημιουργίας δημόσια προσβάσιμων πληροφοριών, μέσα από την συνέργεια διάφορων φορέων και την χρήση τους από τις εθνικές υπηρεσίες υγείας (WHO, 2003). Κρίνοντας από την πρόσφατη πανδημία που έχει προκαλέσει ο SARS CoV 2, η

δυνατότητα παρακολούθησης και πληροφόρησης είναι ζωτικής σημασίας για ένα κράτος (Quiggin, σελ. 175, 2007). Έρευνες έχουν δείξει πως, πέρα από των γνωστό σε όλους SARS CoV 2, υπάρχουν πολλοί άλλοι ιοί που πλέον μεταδίδονται από τα ζώα στους ανθρώπους[10]. Όπως έχει δείξει η ιστορία, το μόνο σίγουρο είναι πως θα υπάρξει κάποια στιγμή ξανά κάποια παγκόσμια υγειονομική κρίση.

Το κύριο ζήτημα για τις πανδημίες είναι η έγκαιρη προειδοποίηση και η αντίδραση. Όμως το ερώτημα είναι, πώς πραγματοποιείται η παγκόσμια παρακολούθηση από την στιγμή που ξένες κυβερνήσεις παρέχουν διαφόρων ποιοτήτων ενημέρωση. Απαιτείται παγκόσμια παρακολούθηση εστιών μόλυνσης μέσα από τα μέσα μαζικής ενημέρωσης, τα κοινωνικά δίκτυα και τις ακαδημαϊκές δημοσιεύσεις. Σε μεγάλο βαθμό αυτό γίνεται ήδη από επιχειρήσεις στον ιδιωτικό τομέα (Quiggin, σελ. 176, 2007). Η ποσότητες πληροφοριών που συλλέγονται θα απαιτούσαν τεράστιο εργατικό δυναμικό, όμως σε αυτό παρέχει απάντηση η τεχνολογία. Μέσα από κατάλληλο λογισμικό και μεθόδους αναζήτησης, το υλικό που έχει συλλεχθεί δύναται να διαχωριστεί σε μικρότερα, πιο φιλικά προς τον αναλυτή πακέτα. Η γνώση που μπορεί να παραχθεί υπερβαίνει τις δυνατότητες των παραδοσιακών πηγών πληροφόρησης, καθώς δεν υπάρχει η δυνατότητα παγκόσμιας κάλυψης για λόγους οικονομικούς όσο και πρακτικούς. Η ίδια διαδικασία μπορεί πλέον να εφαρμοστεί σχεδόν σε οποιαδήποτε άλλο θέμα. Αυτό περιλαμβάνει την διακρατική τρομοκρατία, το οργανωμένο έγκλημα και περιβαλλοντικά θέματα (Quiggin, σελ. 177, 2007)

4.2.2 Αντικίνητρα

Η αλλαγές που έχουν σημειωθεί παγκοσμίως δημιουργούν κίνητρο για αλλαγή και χρήση του OSINT. Όμως για ένα αρκετά μεγάλο χρονικό διάστημα έχει χτιστεί η θεσμική παρουσία των υπηρεσιών πληροφόρησης στην κρατική δομή. Η υπάρχουσα δομή φαίνεται πως είναι η κύρια αντίσταση στην ένταξη του OSINT ως ισάξια πηγή πληροφόρησης. Αντίσταση εντοπίζεται στον ανταγωνισμό μεταξύ υπηρεσιών πληροφόρησης, στην εσωτερική τους οργάνωση αλλά και στα άτομα που τις στελεχώνουν. Γενικότερα φαίνεται πως υπάρχει προσκόλληση στο παλιό και γνώριμο τρόπο λειτουργίας. Παράλληλα, το OSINT στην εποχή της πληροφόρησης απαιτεί την χαλιναγώγηση μεγάλων ποσοτήτων δεδομένων και πληροφοριών που προκύπτουν στον ψηφιακό κόσμο (Clark, κεφ. 7, 2017). Για να επιτευχθεί αυτός ο σκοπός απαιτείται η χρήση σύγχρονων τεχνολογιών, όπως η τεχνητή νοημοσύνη και η έμφαση στο κομμάτι της ανάλυσης. Μέχρι στιγμής ο τομέας αυτός

[10] Κατά την διάρκεια συγγραφής της εργασίας υπήρξε αύξηση κρουσμάτων της ευλογιά των πιθήκων στην Ευρώπη (*Καθημερινή*, 2022).

είναι υπό ανάπτυξη αφήνοντας περιθώρια για την αμφισβήτηση των δυνατοτήτων του OSINT. Επιπλέον, η δυσκολία διαχείρισης μεγάλων ποσοτήτων δεδομένων συμβάλει στις προσπάθειες παραπληροφόρησης που διεξάγουν αντίπαλες υπηρεσίες πληροφοριών.

4.2.2.1 Κοινότητα και Υπηρεσίες πληροφόρησης

Υπάρχουν εγγενή προβλήματα που προέρχονται από τη δομή των συστημάτων πληροφόρησης. Τα διλήμματα μεταξύ συγκέντρωσης και αποκέντρωσης, η ανάγκη διατήρησης μυστικών πληροφοριών – αλλά ταυτόχρονα κοινής χρήσης πληροφοριών – η σχέση μεταξύ παραγωγών και καταναλωτών πληροφόρησης, η ανάγκη ισορροπίας μεταξύ της προστασίας των πηγών και των μεθόδων και της προστασίας των πολιτικών ελευθεριών, είναι μερικά από τα διλήμματα που ταλαντεύουν τα συστήματα πληροφόρησης. Τα εγγενή προβλήματα λαμβάνουν λιγότερη προσοχή από τους υπεύθυνους χάραξης πολιτικής και τους μεταρρυθμιστές των υπηρεσιών πληροφοριών, όμως είναι οι δυσκολότερο να αντιμετωπιστούν (Liaropoulos, 2008). Μέσα στην τελευταία εικοσαετία ο προϋπολογισμός των υπηρεσιών πληροφόρησης, στις ΗΠΑ, έχει αυξηθεί κατακόρυφα, ξεπερνώντας σε ρυθμό αύξησης αυτόν του αμυντικού προϋπολογισμού. Η αύξηση προέρχεται από την χρήση ολοένα και πιο ακριβών συστημάτων συλλογής μυστικών πληροφοριών (Treverton, σελ. 228, 2004) και καταδεικνύει το πόσο έχουν εστιάσει συνολικά οι υπηρεσίες πληροφόρησης στην φάση της συλλογής αλλά και στις μυστικές πληροφορίες.

Σε επίπεδο ατόμου, οι Weinbaum, Parachini κ.ά. (2018) χρησιμοποιούν τα συμπεριφορικά οικονομικά για να εξηγήσουν την εμμονή στην χρήση μυστικών πληροφοριών. Η διαχείρισης διαβαθμισμένων πληροφοριών απαιτεί ένα προστατευμένο περιβάλλον αποθήκευσης αλλά και διαχείρισής τους. Παράδειγμα είναι οι ειδικά διαμορφωμένοι χώροι και οι υπολογιστές για την πρόσβαση πληροφοριών. Για την χρήση ανοιχτών πληροφοριών απαιτείται μετάβαση μεταξύ ενός ασφαλούς και ενός μη ασφαλούς περιβάλλοντος. Αυτό ενέχει τον κίνδυνο διαρροής διαβαθμισμένων πληροφοριών. Για τα στελέχη των υπηρεσιών αυτή η διαδικασία αυξάνει το ρίσκο να κάνουν λάθος και τους αποτρέπει από το να εργάζονται σε μη ασφαλές περιβάλλον. Οι επαγγελματίες πληροφοριών δίνουν προτεραιότητα στο άμεσο όφελος της παραγωγής πληροφόρησης από μυστικές πληροφορίες, παρά στα μακροχρόνια οφέλη που προσφέρει η χρήση ανοιχτών πληροφοριών, γιατί υπάρχει αυξημένο ρίσκο. Αυτό το αντάλλαγμα «ασφάλειας-οφέλους» υπάρχει σε ομαδικό επίπεδο και έχει γίνει μέρος της οργάνωσης των υπηρεσιών πληροφόρησης. Δημιουργούνται, έτσι, καταστάσεις, όπου στελέχη και ηγεσία βάζουν, άθελα τους (Liaropoulos, 2008), εμπόδια μέσα από την αυστηρή οργάνωση.

Γνωστικές προκαταλήψεις, όπως το σύνδρομο «δεν επινοήθηκε εδώ» (Not invented here syndrome) περιγράφει τον αποκλεισμό πληροφοριών και μεθόδων που δεν προέρχονται από αξιόπιστους οργανισμούς. Στη περίπτωση αυτή, το ποιος οργανισμός είναι «αξιόπιστος» δεν αξιολογείται αντικειμενικά, άλλα υποκειμενικά. Αυτή η μεροληψία οδηγεί ορισμένους αναλυτές να πιστεύουν - συνειδητά ή όχι - ότι οι πηγές και οι μέθοδοι της υπηρεσίας τους είναι υψηλής ποιότητας και αξιόπιστες. Αυτό οδηγεί στον αποκλεισμό των ανοιχτών πηγών και όχι μόνο (Weinbaum, Parachini, κ.ά.., 2018; Weinbaum, 2021). Οι αναλυτές που εμπιστεύονται πηγές που αργότερα αποκαλύπτονται ότι είναι δόλιες τιμωρούνται από την υπηρεσία τους ή το εργασιακό τους περιβάλλον. Από την άλλη, οι αναλυτές που ακολουθούν την πεπατημένη, σπάνια τιμωρούνται ή ταπεινώνονται.

Ο David Omand μας περιγράφει την οργανωτική ανεπάρκεια που υπήρχε στην Βρετανική Αστυνομία, που οδήγησε στην αδυναμία χρήσης ανοιχτών πηγών. Παρά το γεγονός ότι η παρατήρησή του αφορά την Βρετανική αστυνομία, ο Omand θίγει ένα σημαντικό ζήτημα, αυτό της οργάνωσης (Omand, Bartlett and Miller, 2012). Υπάρχουν ενδείξεις ότι περίπου το 75% έως το 90% της διαβάθμισης πληροφοριών προέρχεται από την ανάγκη προστασίας της θέσης και της φήμης της εκάστοτε υπηρεσίας πληροφόρησης. Είναι μια προσπάθεια ελέγχου των πληροφοριών, με σκοπό την αύξηση της σημαντικότητας της υπηρεσίας έναντι άλλων υπηρεσιών. Με την αύξηση της σημαντικότητας, η υπηρεσία μπορεί να διεκδικήσει μεγαλύτερο κομμάτι του προϋπολογισμού. Η διαβάθμιση χρησιμοποιείται επίσης σκόπιμα, για να αποφευχθεί η δημοκρατική εποπτεία και η πρόσβαση πολιτών σε πληροφορίες (Quiggin, 2007, σελ. 162-164). Επομένως, αποσκοπεί στην μείωση της κριτικής προς την υπηρεσία και την περαιτέρω ενδυνάμωση της θέσης της.

Οι θεσμικές προκαταλήψεις μπορούν να ξεπεραστούν, σε βάθος χρόνου, μόνο αν εξασφαλιστούν πόροι σε υπηρεσίες ή τμήματα που ασχολούνται με τις ανοιχτέ πηγές και να δομηθεί ένα φιλικότερο περιβάλλον διαχείρισης μέσω της αναδιοργάνωσης τους. Η εξασφάλιση πόρων μεγεθύνει την παρουσία και το αντίτυπο των ανοιχτών πηγών στο τελικό προϊόν πληροφόρησης, ενώ η αναδιοργάνωση δίνει την δυνατότητα στα στελέχη να αλληλοεπιδρούν με περισσότερο υλικό από ανοιχτές πηγές που οδηγεί στην εξοικείωση τους. Κατά τον Mina (2010), το αντικίνητρο αυτό λύνεται εάν υπάρχει θέληση για προσαρμογές.

4.2.2.2 Υπερπληροφόρηση και αξιοπιστία.

Η μεγάλη παραγωγή δεδομένων που διαδίδονται μέσα από το διαδίκτυο θέτει πρόβλημα στην συλλογής και ανάλυσης. Έχοντας συνεχώς καινούρια και περισσότερα

δεδομένα δημιουργούν έναν ατελείωτο κύκλο συλλογής. Λόγω του μεγάλου όγκου αυτά πρέπει να φιλτραριστούν και να δοθούν αναλυτές σε πακέτα που μπορούν να διαχειριστούν. Οι Pai και Prasad (2021) διέκριναν πως υπάρχει ανάγκη ενδυνάμωσης και υποστήριξης της πληροφόρησης από ανοιχτές πηγές με τις δυνατότητες που προσφέρουν η τεχνίτη νοημοσύνη και η τεχνητή μάθηση. Όμως εδώ δημιουργείται προβληματισμός, διότι η ανθρώπινη επικοινωνία είναι περίπλοκη και πολλές φορές απαιτεί γνώση του υπόβαθρου ενός ατόμου για να αποκωδικοποιηθεί σωστά ένα μήνυμα. Τα μέσα κοινωνικής δικτύωσης παρέχουν σημεία στα οποία η ιδιωτική σφαίρα μεταφέρεται σε ένα ψηφιακό δημόσιο χώρο. Μαζί με αυτή μεταφέρονται ιδιωματισμοί, τρόποι έκφρασης και η κουλτούρα των ατόμων (Quiggin, 2007). Μια ακόμη πρόκληση με τις ανοιχτές πηγές αποτελεί το γεγονός ότι ακόμα κι αν οι αναλυτές θέλουν να τις χρησιμοποιήσουν, υπάρχουν απλώς πάρα πολλά δεδομένα για ανάλυση, οι πληροφορίες υπάρχουν σε πάρα πολλές μορφές και οι αναλυτές δεν διαθέτουν τα εργαλεία για την πλήρη ερμηνεία τους. Αυτή η πρόκληση είναι τρομακτική αλλά όχι ανυπέρβλητη: οι αναλυτές χρειάζονται προσεγγίσεις για την επεξεργασία και την ανάλυση δεδομένων για να κατανοήσουν τις ανοιχτές πηγές, καθώς και νέες πολιτικές για να εργαστούν με δεδομένα όπου βρίσκονται, αντί να πρέπει να μεταφέρουν όλα τα δεδομένα σε κυβερνητικά συστήματα. Οι οργανισμοί ασχολούνται ανοιχτές πηγές βοηθούν πολύ σε αυτήν την πρόκληση συλλέγοντας, συνθέτοντας και αναλύοντας. Όμως, αυτοί οι οργανισμοί συνήθως εστιάζουν συγκεκριμένα θέματα δεδομένων ανοιχτού κώδικα και πιθανών οι all source[11] αναλυτές να μην μπορούν να τα χρησιμοποιούν αποτελεσματικά. Οι all source αναλυτές χρειάζονται πρόσβαση σε περισσότερες τεχνικές της επιστήμης δεδομένων και για να κατανοήσουν καλύτερα τις τεχνικές που ήδη προσφέρονται (Weinbaum, Parachini, *et al*., 2018).

4.2.2.3 Η πρωτοκαθεδρία του ιδιωτικού τομέα

Οι περισσότερες απόρρητες υπηρεσίες πληροφοριών μπορεί να μην το σκέφτονται, αλλά η νέα πραγματικότητα (από τη δεκαετία του 1990) είναι ότι ο ιδιωτικός τομέας έχει συχνά περισσότερες πληροφορίες και εμπειρογνώμονες για θέματα εθνικής ασφάλειας από ό,τι αυτές. Στην εποχή της αποκεντρωμένης πληροφόρησης (σε αντίθεση με την κεντρική πληροφόρηση), δεν υπάρχει πλέον η δυνατότητα για τις κυβερνητικές υπηρεσίες να κυριαρχούν στον κόσμο της πληροφόρησης ή της γνώσης. Με απλά λόγια, ακόμη και με

[11] Πληροφόρησης που παράγεται από την ανάλυση πληροφοριών και δεδομένων από πολλές και διαφορετικές πηγές.

τους σημερινούς μεγάλους προϋπολογισμούς τους, οι διαβαθμισμένες υπηρεσίες δεν μπορούν να καλύψουν κάθε χώρα στη γη με κατασκόπους και τεχνολογία. Ούτε μπορούν να παρακολουθούν αποτελεσματικά κάθε πιθανό προβληματικό τομέα ή ζήτημα. Είναι επίσης αποδεκτό από τους περισσότερους ανθρώπους στον κόσμο της πολιτικής, ότι είναι αδύνατο να προβλεφθεί από πού θα προέλθει η επόμενη κρίση (Quiggin, 2007, σελ 165-166).

Ο ιδιωτικός τομέας έχει αναπτύξει σε μεγάλο βαθμό τις τεχνολογικές και τις μεθοδολογικές ικανότητες που απαιτούνται για τη συλλογή και την αξιοποίηση των ανοιχτών πηγών πληροφόρησης, σε σχέση με τις κρατικές υπηρεσίες πληροφόρησης. (Minas, 2010). Έχοντας επίγνωση αυτού, οι κρατικές ανάγκες για πληροφόρηση καλύπτονται ενίοτε από υπηρεσίες που παρέχουν ιδιωτικές επιχειρήσεις. Είναι ορθολογικό φαινόμενο, καθώς οι υπηρεσίες πληροφόρησης αποκτούν πρόσβαση σε πληροφορίες από ανοιχτές πηγές επί πληρωμή, όταν δεν έχουν οι ίδιες την δυνατότητα να καλύψουν την ανάγκη τους. Όμως, σε βάθος χρόνου, η τακτική αυτή αναστέλλει την εξέλιξη των ικανοτήτων που έχουν οι κρατικές υπηρεσίες στον τομέα των ανοιχτών πηγών. Παραπάνω, έχουμε υποστηρίξει πως οι υπηρεσίες πληροφόρησης «μάχονται» για ένα μερίδιο του κρατικού προϋπολογισμού και αυτό είναι ένα σημαντικό εμπόδιο στην ανάπτυξη νέων υπηρεσιών. Η παρατήρηση αυτή, σε συνδυασμό με την ύπαρξη της «φθηνής λύσης» του ιδιωτικού τομέα, λειτουργεί συνολικά ως αντικίνητρο στην ανάδειξη των ανοιχτών πηγών πληροφόρησης και στην αντιμετώπιση τους ως δευτερεύουσας σημασίας. Είναι προφανές πως η δημιουργία μιας υπηρεσίας αφιερωμένης στις ανοιχτές πηγές πληροφόρησης, η οποία θα συνεργαζόταν με τον ιδιωτικό τομέα θα ενίσχυε το προφίλ του OSINT, ενώ θα αναπτυσσόταν οι κρατικές δυνατότητες και παράλληλα θα υποστηριζόταν από ιδιωτικές επιχειρήσεις πληροφόρησης, δημιουργώντας ένα κύκλο μάθησης και συνεργασίας.

Κεφάλαιο 5 - Ανοιχτές Πηγές Πληροφόρησης στις ΗΠΑ και ΗΒ

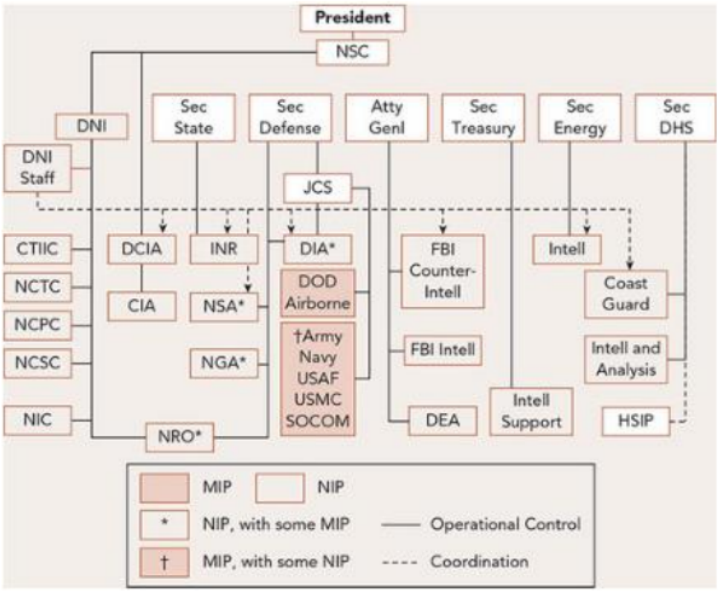
5.1 Ηνωμένες Πολιτικές τις Αμερικής και Ανοιχτές πηγές πληροφόρησης

5.1.1 Δομή της κοινότητας υπηρεσιών πληροφοριών των Ηνωμένων Πολιτειών

Αν και διάφορες υπηρεσίες είχαν προστεθεί στην κοινότητα των πληροφοριών κατά τη διάρκεια των ετών, η βασική δομή υπήρξε σταθερή από το 1947 (Lowenthal, 2020, κεφ. 2). Αυτό άλλαξε στον απόηχο των τρομοκρατικών επιθέσεων της 11ης Σεπτεμβρίου 2001. Η Εθνική Επιτροπή για τις Τρομοκρατικές Επιθέσεις στις Ηνωμένες Πολιτείες, ευρύτερα γνωστή ως η Επιτροπή της 11ης Σεπτεμβρίου, εισηγήθηκε μια σειρά συστάσεων στην έκθεσή της το 2004, για την αναδιάρθρωση της κοινότητας υπηρεσιών πληροφοριών.

Η σημαντική αλλαγή που έγινε από τον επονομαζόμενο νόμο «Intelligence Reform and Terrorism Prevention Act» (IRTPA) του 2004 ήταν η δημιουργία ενός διευθυντή της Εθνικής Πληροφόρησης «Director of National Intelligence» (Director of National Intelligence - DNI), ο οποίος αντικατέστησε το διευθυντή της Κεντρικής Υπηρεσίας Πληροφοριών (Director of Central Intelligence - DCI) ως Ανώτερο Αξιωματούχο πληροφοριών, Επικεφαλή της Κοινότητας Πληροφοριών και Κύριο Σύμβουλο πληροφοριών του Προέδρου και του Συμβουλίου Εθνικής Ασφάλειας (National Security Council - NSC) (Lowenthal, 2020, κεφ. 3). Προηγουμένως, η πρακτική των ΗΠΑ είχε χωρίσει την πληροφόρηση σε δύο τύπους: εξωτερική και εγχώρια. Ο DCI ήταν υπεύθυνος για τις εξωτερικές πληροφορίες. Το IRTPA επαναπροσδιόρισε τον όρο «πληροφόρηση». Τώρα υπάρχει μόνο η Εθνική Πληροφόρηση με τρία υποσύνολα: εξωτερική, εσωτερική και εσωτερικής ασφάλειας. Έτσι, το DNI έχει ευρύτερες ευθύνες από το DCI για πτυχές της εγχώριας πληροφόρησης. Μεγάλο μέρος της ώθησης πίσω από την πράξη ήταν η ανησυχία ότι οι υπηρεσίες δεν μοιράζονταν καλά πληροφορίες, ειδικά σε όλο το φάσμα εξωτερικών-εγχώριων πληροφοριών. Ως εκ τούτου, ο DNI πρέπει να έχει πρόσβαση σε όλες τις πληροφορίες και είναι υπεύθυνος να διασφαλίζει ότι διαδίδονται, όπως απαιτείται σε όλη την κοινότητα πληροφοριών. Η ικανότητα του DNI να εξασφαλίσει την ροή πληροφοριών αποτελεί σημείο επαναλαμβανόμενης ανησυχίας. Ο DNI έχει επίσης νομική ευθύνη για την προστασία των πηγών και των μεθόδων που εφαρμόζονται για την ανάλυση των πληροφοριών. Όμως αν και ο DNI έχει κομβική θέση, με στόχο την διαχείριση της κοινότητας των υπηρεσιών πληροφόρησης, δεν έχει απόλυτο έλεγχο, Όπως φαίνεται στο διάγραμμα 2,

υπάρχουν πολλές υπηρεσίες με ξεχωριστή διοίκηση, πράγμα που αφήνει πολύ μεγάλο περιθώριο ανεξαρτησίας, δίνοντας χώρο στην εμφάνιση δυσλειτουργιών. Επιπλέον, φαίνεται πως δεν υπάρχει καμία υπηρεσία που να παράγει OSINT.



Διάγραμμα 2: Υπηρεσίες Πληροφόρησης των ΗΠΑ και η Διοικητική υπαγωγή τους[12].

Πηγή: (Lowenthal σελ.40, 2020)

5.1.2 Η θεσμική παρουσία του OSINT

Ακόμα και μέσα από μια γρήγορη ματιά στο διάγραμμα 2 φαίνεται πως δεν υπάρχει υπηρεσία με αποκλειστικό σκοπό την παραγωγή OSINT. Αντί αυτού, η μόνο θεσμική δομή αφιερωμένη στο OSINT υπάγεται στην Κεντρική Υπηρεσία Πληροφοριών (Central Intelligence Agency – CIA). Στις ΗΠΑ, το OSINT ξεκίνησε με έμφαση στην άμυνα της χώρας. Στις 26 Φεβρουαρίου 1941, ιδρύθηκε το Foreign Broadcast Monitoring Service (FBMS) με καθήκον την παρακολούθηση και την ανάλυση της προπαγάνδας από τα ραδιοφωνικά προγράμματα των δυνάμεων του Άξονα. Στις 26 Ιουλίου, 1942, μετονομάστηκε σε Federal Broadcast Information Service (FBIS). Το 1946, μετά τον Β' Παγκόσμιο Πόλεμο, υπήρχε το ενδεχόμενο διάλυσης της υπηρεσίας,

[12] *NIP – Εθνικό Πρόγραμμα Πληροφοριών, υποστηρίζει τον στρατηγικό σχεδιασμό και τη χάραξη πολιτικής. MIP – Στρατιωτικό Πρόγραμμα Πληροφοριών, υποστηρίζει στρατιωτικές επιχειρήσεις και σε τακτικό επίπεδο σχεδιασμού* (Devine, 2019).

όμως τελικά μεταφέρθηκε Υπουργείο Πολέμου των ΗΠΑ. Στην συνέχεια τον Ιανουάριο του 1947 η CIA ανέλαβε την FBMS. Από τη δημιουργία του FBIS μέχρι τη δεκαετία του 1990, η αρμοδιότητα της εντός της κοινότητας υπηρεσιών πληροφοριών ήταν η ανάλυση ανοιχτών πηγών, κυρίως μέσα από την παρακολούθηση και τη μετάφραση του ξένου τύπου. Υπάρχουν ορισμένες σημαντικές διαφορές μεταξύ του ιστορικού χαρακτήρα του OSINT - της πρώτης γενιάς του OSINT - και της σημερινής δεύτερης γενιάς. Η συλλογή υλικού ήταν μια σημαντική στην πρώτη γενιά του OSINT. Το FBIS διαχειριζόταν 20 γραφεία σε όλο τον κόσμο για να συλλέγει υλικό για εκμετάλλευση. Με την πάροδο του χρόνου μειώθηκε το εύρος συλλογής προκειμένου να επικεντρωθεί σε υλικό υψηλής προτεραιότητας, όμως η κύρια ενασχόληση ήταν η μεταφράσεις πηγών. Ωστόσο, θα πρέπει να σημειωθεί ότι το FBIS εξυπηρετεί ορισμένες αναλυτικές λειτουργίες - κυρίως ανάλυση των τάσεων (Williams and Blum, 2018).

Κατά την διάρκεια του Ψυχρού Πολέμου το FBIS παρείχε κριτικής σημασίας πληροφόρηση στον Αμερικανικό στρατό. Οι πρώτες ενδείξεις για την απομάκρυνση των Σοβιετικών πυραύλων από την Κούβα και την Σοβιετική αποχώρηση από το Αφγανιστάν είχαν δοθεί χρησιμοποιώντας πληροφόρηση από ανοιχτές πηγές. Επιπλέον, μέσα από ανοιχτές πηγές κατανοήθηκε το γενικό πλαίσιο μέσα στο οποίο εξελίχθηκαν οι κρίσεις στην Ουγγαρία και την Τσεχοσλοβακία. Το τέλος του Ψυχρού Πολέμου είχε ως αποτέλεσμα να μειωθεί ο προϋπολογισμός των υπηρεσιών πληροφόρησης στις ΗΠΑ. Σε μία περίοδο που ο όγκος των ανοιχτών πηγών αυξάνονταν το FBIS κινδύνευε με διάλυση, όμως διασώθηκε από τις προσπάθειες της Ομοσπονδίας Αμερικανών Επιστημόνων (Federation of American Scientists – FAS) που τόνιζε την υψηλή απόδοση και το χαμηλό κόστος των ανοιχτών πηγών για την πληροφόρηση. Παράλληλα, Αξιωματούχοι στην κοινότητα πληροφόρησης των ΗΠΑ διέκριναν τις αλλαγές και τις προκλήσεις του 21ου αιώνα. Η τεχνολογία και η ραγδαία αύξηση των προσωπικών υπολογιστών έμελλαν να μεταμορφώσουν τον κόσμο και να μας μεταφέρουν στην ψηφιακή εποχή (Williams and Blum, 2018).

Οι ηγεσίες των υπηρεσιών πληροφόρησης των ΗΠΑ αναγνώρισαν ότι οι προκλήσεις και η δυναμική του 21ου αιώνα θα έφεραν μεγαλύτερη ζήτηση για OSINT, όχι λιγότερη. Ο αναπληρωτής διευθυντής του FBIS, J. Niles Riddel, στο Πρώτο Διεθνές Συμπόσιο για τις Ανοιχτές Πηγές (First International Symposium on Open Source), το 1992, αναγνώρισε τις αλλαγές στο OSINT που προέκυψαν από την αύξηση των προσωπικών υπολογιστών (Williams and Blum, 2018, σελ. 5). Η Επιτροπή για τις Δυνατότητες Πληροφόρησης των Ηνωμένων Πολιτειών σχετικά με τα Όπλα Μαζικής

Καταστροφής (Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction - WMD Commission) σταμάτησε τις δραστηριότητές της στις 27 Μαΐου 2005. Μία από τις συστάσεις της Επιτροπής WMD ήταν η δημιουργία ενός Κέντρου Ανοιχτών Πηγών (OSC) εντός της CIA (The Commission on the Intelligence, Capabilities of the United States Regarding Weapons of Mass Destruction, 2005, σελ. 569) για να διασφαλιστεί η μέγιστη χρήση των ξένων έντυπων, του ραδιοφώνου, της τηλεόρασης/ειδήσεων και των πληροφοριών στο Διαδίκτυο. Ενεργώντας σύμφωνα με τη σύσταση της Επιτροπής WMD, ο DNI ίδρυσε το Open Source Center (OSC) στο πλαίσιο της CIA στις 8 Νοεμβρίου 2005. Η ίδρυση του OSC δείχνει ότι οι υπηρεσίες πληροφοριών έχουν δυσκολευτεί να διαχειριστούν τις δημόσιες πληροφορίες, λόγω της παγκόσμιας αύξησης του περιεχομένου των μέσων ενημέρωσης και της διάδοσης των νέων τεχνολογιών επικοινωνίας. Το 2006, ψηφίστηκε νόμος για την ίδρυση του OSC. Επιπλέον, περιείχε ρητές αναφορές στα προβλήματα διαχείρισης των ανοιχτών πηγών από το Υπουργείο Άμυνας (DoD) και το Υπουργείο Εσωτερικής Ασφάλειας (Department of Homeland Security – DHS) (Bean, 2007). Το OSC αφομοίωσε το FBIS με την εμπειρία και την τεχνογνωσία που είχε αποκτήσει, παράλληλα επέκτεινε το εύρος των εργασιών του χρησιμοποιώντας το διαδίκτυο και αξιοποιώντας νέες τεχνολογίες. Η τελευταία θεσμική αλλαγή ήρθε τον Οκτώβριο του 2015 όπου το OSC μετονομάστηκε σε Open Source Enterprise (OSE) και ενσωματώθηκε στη νέα Διεύθυνση Ψηφιακής Καινοτομίας (Directorate of Digital Innovation) της CIA (Aftergoood, 2015). Σύμφωνα με την CIA, η Διεύθυνση Ψηφιακής Καινοτομίας ενισχύει την καινοτομία σε όλη τη CIA και διασφαλίζει ότι οι ομάδες έχουν τα εργαλεία και τις τεχνικές που χρειάζονται, για να λειτουργήσουν σε έναν σύγχρονο, συνδεδεμένο κόσμο και να εξακολουθούν να λειτουργούν με μυστικότητα (Organization - CIA, χ.χ.). Πρακτικά, φαίνεται πως πρόκειται για έναν οριζόντιο και υποστηρικτικό ρόλο.

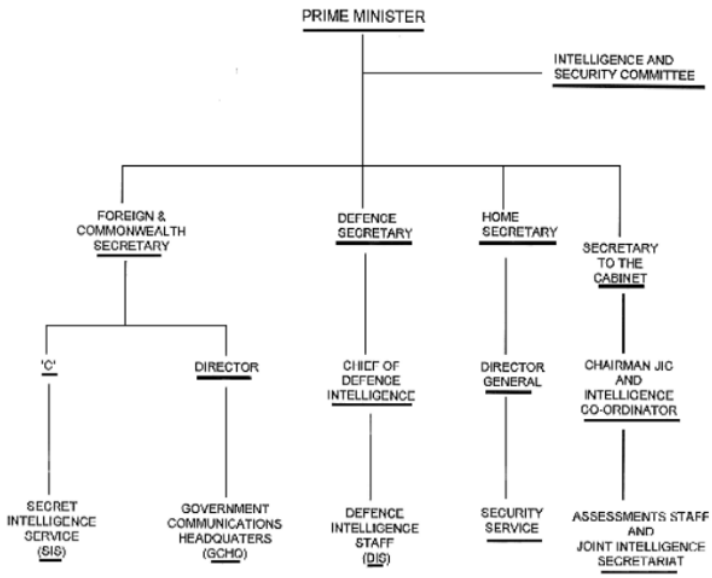
Σε μεγάλο βαθμό, οι υπηρεσίες πληροφόρησης των ΗΠΑ παράγουν OSINT εσωτερικά, ή το αναθέτουν σε εξωτερικούς συνεργάτες μέσω συμβάσεων (Bean, 2007). Η μετατόπιση του OSC από το γραφείο του DNI το 2015 στη CIA και η ενσωμάτωσή του στη νέα Διεύθυνση Ψηφιακής Καινοτομίας φαίνεται να τερματίζει την σχεδόν ανεξάρτητη ύπαρξή του στο πλαίσιο του DNI και να επαναφέρει το OSINT ως μια δραστηριότητα εντός της CIA. Το ζήτημα με αυτή τη ρύθμιση είναι πως, διαχρονικά, η CIA εστιάζει περισσότερο στις κρυφές δραστηριότητές της (κατασκοπεία, μυστική δράση), μαζί με ανάλυση όλων των πηγών (all-source) που

προέρχονται, κατά πλειοψηφία, από κλειστές και διαβαθμισμένες πληροφορίες (Lowenthal, 2020, κεφ. 3).

5.2 Ηνωμένο Βασίλειο και Ανοιχτές πηγές πληροφόρησης

5.2.1 Δομή της κοινότητας υπηρεσιών πληροφοριών του Ηνωμένου Βασιλείου

Το αμερικανικό σύστημα του μεταπολεμικού Β' Παγκοσμίου Πολέμου είδε τις πληροφορίες να είναι προσανατολισμένες στην αποφυγή του αιφνιδιασμού. Στη Βρετανία και την Κοινοπολιτεία έχει θεωρηθεί πολύ περισσότερο ως σημαντικό στοιχείο της διακυβέρνησης, για να βοηθήσει στη βελτίωση της ποιότητας της λήψης αποφάσεων. Με βάση μια γενική πεποίθηση ότι η πληροφόρηση προσθέτει αξία στη λήψη αποφάσεων σε πολιτικούς και στρατιωτικούς, εσωτερικούς και εξωτερικούς τομείς, υπάρχουν αρκετά καθοριστικά και αλληλένδετα χαρακτηριστικά βρετανικής πληροφόρησης που την επηρεάζουν. Αυτό επιτυγχάνεται μέσω μιας ενωμένης κοινότητας πληροφοριών υπό την καθοδήγησης μιας επιτροπής. Η προσπάθεια για συναίνεση είναι κύριο στοιχείο μαζί με την απαίτηση για επικύρωση των πληροφοριών μιας πηγής από τους ίδιους τους φορείς συλλογής, όχι από τους αναλυτές. Επιπλέον, υπάρχει και η δυνατότητα να μεταβεί η πληροφόρηση απευθείας στους πελάτες τους ή να περάσει από κεντρικές all source αξιολογήσεις. Στο επίκεντρο βρίσκεται η Κοινή Επιτροπή Πληροφοριών (Joint Intelligence Committee - JIC), η οποία οργανώνει ό,τι συμβαίνει στην υπόλοιπη κοινότητα, συντονίζει και αξιολογεί τη διαδικασία μέσω της οποίας οι πληροφορίες εξέρχονται από τον μηχανισμό πληροφοριών και εισέρχονται στη σφαίρα χάραξης πολιτικής (Goodman, 2014).



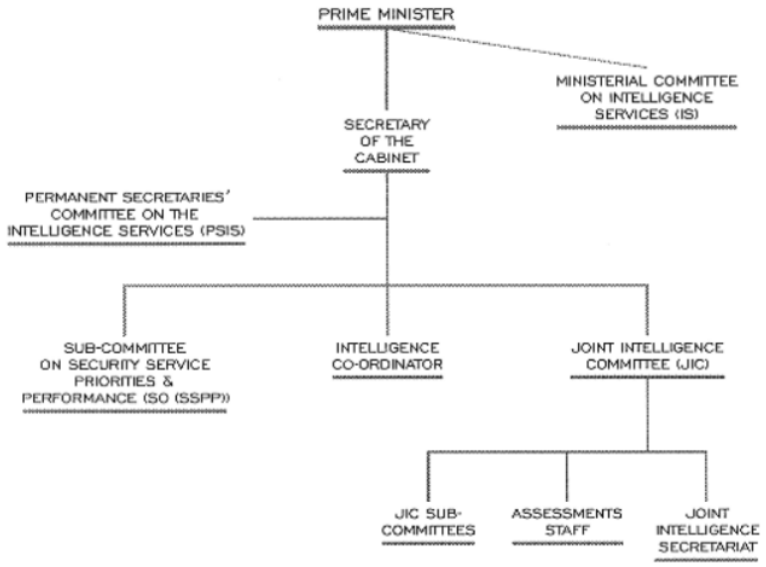
Διάγραμμα 3: Υπηρεσίες Πληροφόρησης του ΗΒ και η Διοικητική υπαγωγή τους

Πηγή: (Central Intelligence Machinery - UK Intelligence Agencies, χ.χ.)

Το σύγχρονο βρετανικό σύστημα πληροφοριών ξεκινά το 1909, με την ίδρυση του Γραφείου Μυστικών Υπηρεσιών (Secret Service Bureau). Αυτό δημιουργήθηκε εν μέσω φόβων για αυξανόμενη γερμανική απειλή για τα βρετανικά συμφέροντα. Σχηματίστηκαν ένα τμήμα εσωτερικού, το MI5, και ένα υπερπόντιο τμήμα, το MI1c (το οποίο θα γινόταν Secret Intelligence Service – SIS). Από τις πρώτες μέρες τους και τα δύο τμήματα είχαν συγκεκριμένα και διαφορετικά καθήκοντα. Η MI5 ήταν υπεύθυνη για την εσωτερική ασφάλεια και ξόδεψε μεγάλο μέρος του χρόνου της στην παρακολούθηση Γερμανών που ζούσαν στο Ηνωμένο Βασίλειο, ενώ ανέλαβε επίσης την ευθύνη για την αντιμετώπιση της Ιρλανδικής τρομοκρατίας. Η MI1c επικεντρώθηκε στις ξένες απειλές και στρατολογούσε πράκτορες στο εξωτερικό για να παρακολουθεί για σημάδια γερμανικής κινητοποίησης (Goodman, 2014, σελ. 136)

Μέχρι το τέλος του Δευτέρου Παγκοσμίου Πολέμου, η βρετανική υπηρεσία πληροφοριών επικεντρώνονταν κυρίως σε στρατιωτικά θέματα. Η MI5 και το SIS (συμπεριλαμβανομένης της οργάνωσης SIGINT GC&CS) ήταν οι μόνες δύο «πολιτικές» υπηρεσίες και συντριπτική πλειοψηφία των στελεχών, αν και πολίτες,

προέρχονταν από τις ένοπλες δυνάμεις. Εκείνη την εποχή το Foreign Office (FO)[13] έβλεπε τον εαυτό του ως το μόνο κυβερνητικό όργανο ικανό να προσφέρει συμβουλές για πολιτικά και διπλωματικά θέματα. Οι βρετανικές μυστικές υπηρεσίες ήταν κατακερματισμένες και δεν υπήρχε καθορισμένη θεσμική διασύνδεση που να προωθεί την συνεργασία τους. Το αντίθετο συνέβαινε: οι ένοπλες δυνάμεις – Στρατός, Ναυτικό και Πολεμική Αεροπορία – είχαν όλες τα δικά τους επιτελεία πληροφοριών, όπως και το FO, με ανεπίσημη ιδιότητα. Το 1936 προτάθηκε από τον Sir Maurice Hankey, η χρήση κάποιου είδος επιτροπής ώστε να ξεπεραστούν τα προβλήματα της διπλής προσπάθειας και να διασφαλιστεί ότι οι Αρχηγοί των Επιτελείων (Chiefs of Staff – COS) και η κυβέρνηση είχαν τις καλύτερες δυνατές πιθανές πληροφορίες στη διάθεσή τους. Το αποτέλεσμα ήταν η δημιουργία της JIC, η οποία έχει γίνει το κέντρο της Βρετανικής πληροφόρησης. Στο Βρετανικό σύστημα, μέσω των επιτροπών, τίθενται οι απαιτήσεις και οι προτεραιότητες για πληροφόρηση, για να προχωρήσουν οι υπηρεσίες στον σχεδιασμό της συλλογής και στην επαλήθευση των πληροφοριών που συλλέγονται. Οι αποφάσεις του JIC βασίζονται στις αρχές της προσέγγισης της επιτροπής και στη σημασία της συναίνεσης. Για την αύξηση του συντονισμού θεσπίστηκαν και άλλες επιτροπές και υποστηρικτικές θέσεις, όπως φαίνεται στο διάγραμμα 4.



Διάγραμμα 4: Επιτροπές για τον συντονισμό των υπηρεσιών πληροφόρησης του ΗΒ

[13] Το υπουργείο εξωτερικών του Ηνωμένου Βασιλείου μέχρι το 1968. Μετέπειτα ονομαστικέ Foreign & Commonwealth Office (FCO) και από το 2020 ονομάζεται Foreign, Commonwealth & Development Office (FCDO).

Πηγή: (Central Intelligence Machinery - UK Intelligence Agencies, χ.χ)

5.2.2 Η θεσμική παρουσία του OSINT

Το ΗΒ πρωτοπόρησε το 1938 στον τομέα του OSINT με την ίδρυση του BBC Monitoring Service. Ήταν ο πρώτος θεσμός που με κρατική χορηγία αξιοποίησε ανοιχτές πηγές για συγχρόνους σκοπούς πληροφόρησης. Σήμερα, υπό την ονομασία BBC Monitoring (BBCM), είναι ο μοναδικός οργανισμός ο οποίος συλλέγει αποκλειστικά ανοιχτές πηγές στο ΗΒ. Σε σχέση με την αντίστοιχη υπηρεσία ανοιχτών πηγών στις ΗΠΑ το OSE, το BBCM έχει περίεργη θέση στην κοινότητα υπηρεσιών πληροφοριών του ΗΒ. Το αξιοσημείωτο είναι πως δεν αποτελεί κομμάτι της κοινότητας πληροφόρησης, όπως φαίνεται και από την απουσία της στο διάγραμμα 3 (Gibson, 2007, σελ. 196). Παρά ταύτα είναι σημαντική η συνεισφορά του καθώς παρέχει πληροφορίες από ανοιχτές πηγές σε κυβερνητικούς και εθνικούς οργανισμούς, αλλά και εμπορικά, σε άλλους οργανισμούς. Ως οργανισμός δεν είναι κυβερνητικό όργανο αλλά χρηματοδοτείται από τον προϋπολογισμό του BBC, που με την σειρά του λαμβάνει χρηματοδότηση από τους «Key Customers», οι οποίοι είναι το Υπουργείο Εξωτερικών (Foreign and Commonwealth Office), το Υπουργείο Αμύνης (Ministry of Defence – MoD), το Γραφείο Υπουργικού Συμβουλίου (Cabinet Office) και οι υπηρεσίες πληροφόρησης και ασφάλειας (Gibson, 2007, σελ. 196-197; BBC Monitoring Agreement - GOV.UK, 2017). Παρ' όλα αυτά, το 2016 υπήρξαν φόβοι για την αποδοτικότητα του BBCM. Μέχρι το 2013 το BBCM χρηματοδοτούνταν απευθείας από την κυβέρνηση του ΗΒ, όμως με την μεταφορά του στη διοίκηση του BBC μεταφέρθηκε και το βάρος της χρηματοδότησης στον προϋπολογισμό του BBC. Η κίνηση αυτή είχε ως αποτέλεσμα τη μείωση της χρηματοδότησης του BBCM και την αναδιάρθρωσή του, για να μειωθούν τα έξοδα.

Η κυβέρνηση του ΗΒ χρησιμοποιεί πληροφορίες από ανοιχτές πηγές ως δείκτες για την έγκαιρη προειδοποίηση, ενημέρωση για εξελίξεις σε περιοχές αστάθειας και πιθανές απειλές για την ασφάλειά του. Το BBCM είναι ένας από τους λίγους οργανισμούς συλλογής πληροφοριών από ανοιχτές πηγές που έχει παγκόσμια εμβέλεια, μέσω της συνεργασίας του με τον ομόλογό του στις ΗΠΑ, το OSE. Επί του παρόντος, το BBCM καλύπτει το 25% του πλανήτη και ο OSE το υπόλοιπο 75%. Η συμφωνία για την ανταλλαγή πληροφοριών από ανοιχτές πηγές δημιουργεί τεράστια απόδοση για το Ηνωμένο Βασίλειο με μέτριο κόστος για την λειτουργία του οργανισμού (που είναι περίπου 25 εκατομμύρια £ ετησίως). Αυτή η παγκόσμια κάλυψη

είναι ζωτικής σημασίας για την κατανόηση όχι μόνο των κυβερνητικών υπηρεσιών, συμπεριλαμβανομένου του Υπουργείου Άμυνας, του Υπουργείου Εξωτερικών και της Κοινοπολιτείας και των Υπηρεσιών Πληροφοριών, αλλά και ΜΚΟ και ιδιωτικών οργανώσεων. (The Defence Committee, 2016). Αν και υπάρχει το BBCM, πολλές υπηρεσίες συλλέγουν και αναλύουν μόνες τους ανοιχτές πηγές για να δημιουργήσουν μια ευρεία εικόνα και στη συνέχεια να οργανώσουν την προσπάθεια τους για συλλογή κλειστών πληροφοριών (Gibson, 2007, σελ. 201).

Ο Sir David Omand, (x.x.), πρώην Διευθυντής της Government Communications Headquarters (GCHQ) και μέλος της JIC, τάσσεται υπέρ και εκθειάζει το έργο του BBCM και υποστηρίζει ότι προσφέρει μια μοναδική ενημέρωση, μέσα από την ανάλυση ομιλιών ξένων ηγετών, ή των πολιτικών αντιπάλων τους. Μερικές φορές η πληροφόρηση θα ενίσχυε την ιστορική κατανόηση και θα ανέλυε την εξέλιξη των πιο σημαντικών απόψεων σε σχέση με το θέμα. Πρόσθετη αξία για τον Omand είναι το γεγονός ότι οι αναλύσεις πραγματοποιούνται όλες από άτομα των οποίων οι γλωσσικές δεξιότητες και η πολιτισμική τους επίγνωση, τους επέτρεψαν να ερμηνεύσουν με αντικειμενικό τρόπο, λαμβάνοντας υπόψη τις κοινωνικές και γλωσσικές ιδιαιτερότητες. Η κλειστή πληροφόρηση έχει μικρή αλλά μοναδική συνεισφορά, που προέρχεται από πληροφορίες τις οποίες ο αντίπαλος προσπαθεί να κρατήσει μυστικές. Αλλά όπως κάθε μεμονωμένη πληροφορία, το νόημα μιας μυστικής πληροφορίας εξαρτάται από τα συμφραζόμενα. Ως προς αυτόν τον σκοπό, το BBCM έχει εντάξει στην διαδικασία συλλογής και ανάλυσης τα μέσα κοινωνικής δικτύωσης. Σύμφωνα με τον (Omand, χ.χ.) έχει γίνει χρήση της ψηφιακής τεχνολογίας που μπορεί να παρέχει στους πελάτες της πληροφόρηση σε σύντομο χρονικό διάστημα για έκτακτες καταστάσεις. Αμφιβολία στις δυνατότητες του BBCM δημιουργεί η πεποίθηση των Omand, Bartlett and Miller, (2012) πως το SOCMINT αποτελεί νέα πηγή πληροφόρησης. Η πρόταση για ισάξια αντιμετώπιση του SOCMINT με τις παραδοσιακές κλειστές πηγές μοιάζει με αυτήν του OSINT. Αν και δεν έχει ειπωθεί ξεκάθαρα, ίσως το BBCM να μην δίνει τόση βαρύτητα στο SOCMINT και για αυτόν τον λόγο οι Omand, Bartlett and Miller να ένιωσαν την ανάγκη ανάδειξης της βαρύτητάς του.

Κεφάλαιο 6 - Συζήτηση Ευρημάτων, Συμπεράσματα και Προτάσεις

6.1 Συζήτηση Ευρημάτων

Ανοιχτές πηγές υπάρχουν εδώ και αιώνες, είτε σε προφορική μορφή είτε σε γραπτή, δίνοντας τη δυνατότητα εφαρμογής του κύκλου πληροφόρησης. Όμως, αυτό που έχει δράσει ως καταλύτης για να φτάσουμε να μιλάμε μέχρι και για SOCMINT είναι η εξέλιξη της τεχνολογίας. Τα σύγχρονα μέσα επικοινωνίας άνοιξαν τον δρόμο στην άμεση πρόσβαση τεράστιων ποσοτήτων δεδομένων και πληροφοριών. Από το ράδιο μέχρι το twitter, οι δυνατότητες του OSINT θα αυξάνονται, όσο η τεχνολογία αναπτύσσεται.

Τα κίνητρα των υπηρεσιών πληροφόρησης που κάνουν χρήση του OSINT φαίνεται να προέρχονται από κοινωνικές και διεθνείς αλλαγές, που σχετίζονται με την παγκοσμιοποίηση. Οι ίδιες οι αλλαγές ενδυναμώνουν την αποτελεσματικότητά του OSINT. Θα μπορούσε κανείς να το παρομοιάσει με το αντίδοτο στο δηλητήριο του φιδιού, το οποίο παράγεται από το ίδιο το δηλητήριο. Τα αντικίνητρα στην χρήση του OSINT από τις υπηρεσίες πληροφόρησης φαίνεται πως είναι ένας συνδυασμός της συντηρητικής κουλτούρας τους και της δυσκολίας ανάπτυξης-εφαρμογής νέων μεθόδων με παράλληλη αξιοποίησης νέων τεχνολογιών.

Τα κίνητρα είναι ισχυρά και θα συνεχίσουν να θέτουν ισχυρά επιχειρήματα υπέρ της εντατικής χρήσης του OSINT. Ενώ τα αντικίνητρα θα εξασθενούν, όσο αυξάνεται η αναποτελεσματικότητα των υπηρεσιών πληροφόρησης. Η σημαντικότητα της ύπαρξης του OSINT φαίνεται στην περίπτωση των ΗΠΑ, παρά τις αλλεπάλληλες θεσμικές αλλαγές που έχει υποστεί ακόμη διατηρείται. Το αρνητικό είναι πως σε κάθε αλλαγή την κοινότητας πληροφόρησης των ΗΠΑ ενισχύονται οι παραδοσιακές υπηρεσίες πληροφόρησης και η συλλογή μυστικών πληροφοριών. Φαίνεται ξεκάθαρα, από θεσμική οπτική, πως οι ανοιχτέ πηγές είναι δευτερεύουσες σε σχέση με τις μυστικές. Οι πολλαπλές αλλαγές στην υπηρεσία συλλογής ανοιχτών πηγών μαρτυρούν πως ακόμα αναζητείται η βέλτιστη θέση της σε σχέση με τις υπόλοιπες υπηρεσίες. Επιπλέον, η τρέχουσα θέση του OSE, ως μη ανεξάρτητη υπηρεσία υπό τον έλεγχο της CIA πιθανόν να προκύπτει από όσες πληροφορίες θεωρούνται δεύτερης κατηγορίας, επιβεβαιώνοντας την προσκόλληση σε κλειστές πληροφορίες, που υπάρχει στις ΗΠΑ. Φαίνεται πως οι αλλεπάλληλες συστάσεις επιτροπών έχουν συντελέσει στην ύπαρξη του OSE, όμως στην πράξη, όλες οι υπηρεσίες ξεχωριστά, επιδίδονται στην παραγωγή

OSINT, όπως παρατηρεί ο Lowenthal (2001). Επιπλέον το OSE έχει μείνει πίσω σε σχέση με τον ιδιωτικό τομέα, που προσφέρει περισσότερες υπηρεσίες.

Στο ΗΒ φαίνεται πως έχουν επικρατήσει τα κίνητρα για την χρήση του OSINT. Φυσικά και υπάρχουν εκφάνσεις των αντικινήτρων, παραδείγματος χάρη στην περίπτωση μείωσης χρηματοδότησης του BBCM. Όμως, η γενικότερη φιλοσοφία και η δομή της κοινότητας υπηρεσιών πληροφοριών του ΗΒ ευθυγραμμίζονται περισσότερο με αυτά που προσφέρει το OSINT. Η υποστήριξη την πολιτικής μέσα από την πληροφόρηση απαιτεί ολοκληρωμένη εικόνα και όχι αποσχιστικές πληροφορίες. Το φιλτράρισμα αλλά και η σύνθεση των πληροφοριών μέσα από επιτροπές είναι καθοριστικής σημασίας για την παροχή μια ολοκληρωμένης εικόνας, ακόμη και να μην περιέχει OSINT. Συγχρόνως, οι απαιτήσεις αλλά και η διαδικασία υποχρεώνουν την αναζήτηση ανοιχτών πηγών, προάγοντας την σημασία του OSINT. Επιπλέον, η τοποθέτηση του BBCM εκτός της κοινότητας υπηρεσιών πληροφοριών, αν και αντισυμβατική, φαίνεται πως λειτουργεί ευεργετικά. Το BBCM, λειτουργώντας υπό το BBC και έχοντας αναπτύξει και εμπορική διάσταση είναι εκτεθειμένο στον ανταγωνισμό του ιδιωτικού τομέα. Η έκθεση στον ιδιωτικό τομέα, χωρίς αμφιβολία, έχει θετική επίδραση στην εξέλιξη και αύξηση της ποιότητας του προϊόντος πληροφόρησης. Συνοψίζοντας, στις ΗΠΑ το σύστημα των υπηρεσιών πληροφόρησης λειτουργεί ανασταλτικά στην ανάπτυξη και χρήση του OSINT, συστέλλοντας τον ρόλο του OSE. Ενώ στο ΗΒ το σύστημα των υπηρεσιών πληροφόρησης λειτουργεί χρησιμοποιώντας το BBCM ως εξωτερικό συνεργάτη επιβραδύνοντας την ανάπτυξη του OSINT.

6.2 Συμπεράσματα και προτάσεις

Πλέον, οι κύριες απειλές που αντιμετωπίζει ένα κράτος δεν είναι η στρατιωτική απειλή από ένα αντίπαλο κράτος. Οι νέες απειλές χαρακτηρίζονται από την περιπλοκότητα τους, τη διεθνή τους έκταση αλλά και την ανάδειξη ατόμων και ομάδων ως απειλές. Αυτό δημιουργεί μια κατάσταση στην οποία η κλειστή πληροφόρηση δεν έχει προσαρμοστεί. Τα κίνητρα είναι πιο ισχυρά από τα αντικίνητρα, καθώς η δεύτερη κατηγορία προέρχεται από την αντίσταση στην αλλαγή, ή με άλλα λόγια, από μια κουλτούρα που έχει δημιουργηθεί και γύρω από την μυστικότητα της πληροφόρησης. Με την πάροδο του χρόνου η κουλτούρα θα αλλάξει, όμως σκοπός είναι να αλλάξει με μεγαλύτερο ρυθμό ώστε να αποφευχθούν μελλοντικές αποτυχίες. Αν και από την ύπαρξη OSINT στους θεσμούς πληροφόρησης φαίνεται πως είναι σημαντικό εργαλείο,

παραμένει παραμελημένο κομμάτι σε σχέση με τις υπόλοιπες πηγές πληροφόρησης. Είναι αναγκαίο επεκταθούν και να ενισχυθούν οι υπηρεσίες που ασχολούνται με το OSINT. Μέτρα που πρέπει να ληφθούν είναι η:

- ανεξαρτητοποίηση των υπηρεσιών που συλλέγουν ανοιχτές πληροφορίες, έτσι ώστε να είναι οργανωτικά αυτοτελείς, ακόμη και εκτός της κοινότητας πληροφόρησης,
- παροχή επαρκής χρηματοδότησης, ανάλογη με την χρηματοδότηση άλλων υπηρεσιών,
- δημιουργία θεσμικού πλαισίου, ώστε η αίτηση για πληροφόρηση να εκκινεί πρώτα απάντηση μέσω OSINT και αν απαιτείται, μέσω άλλης πηγής πληροφόρησης.

Τα παραπάνω μέτρα έχουν ως σκοπό την κανονικοποίηση του OSINT εντός των κοινοτήτων πληροφόρησης και την υποβάθμιση των αντικινήτρων.

Βιβλιογραφία

Ξενόγλωσση Βιβλιογραφία

About CRS (no date). Available at: https://crsreports.congress.gov/Home/About (Accessed: April 5, 2022).

Aftergood, S. (2010) *Blocking Access to Wikileaks May Harm CRS, Analysts Say – Federation Of American Scientists*, *Federation of American Scientists*. Available at: https://fas.org/blogs/secrecy/2010/12/crs_block/ (Accessed: April 5, 2022).

Aftergoood, S. (2015) *Open Source Center (OSC) Becomes Open Source Enterprise (OSE) – Federation Of American Scientists*, *Federation of American Scientists*. Available at: https://fas.org/blogs/secrecy/2015/10/osc-ose/ (Accessed: May 21, 2022).

Backfried, G. *et al*. (2012) "Open source intelligence in disaster management," in *Proceedings - 2012 European Intelligence and Security Informatics Conference, EISIC 2012*, pp. 254–258. doi:10.1109/EISIC.2012.42.

Bagnall, J.J. (1958) "The Exploitation of Russian Scientific Literature for Intelligence Purposes," *Studies in Intelligence*, 2(3), pp. 45–48.

Bărbulescu, C. (2016) "The role of OSINT in reinventing intelligence," *International Scientific Conference Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, pp. 249` – 255. Available at: https://www.cia.gov/library/center-.

Bartlett, J. and Miller, C. (2013) *The State of the Art: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism*. London: Demos. Available at: www.demos.co.uk.

Bath, A. (2022) *Open source intelligence observers gain growing role in how war is viewed | Stars and Stripes*, *Stars and Stripes*. Available at: https://www.stripes.com/theaters/europe/2022-03-29/citizen-osint-analysts-chronicle-russian-navy-role-in-war-in-ukraine-5513788.html (Accessed: April 5, 2022).

BBC Monitoring Agreement - GOV.UK (2017) *The Foreign and Commonwealth Office, the Ministry of Defence, the Cabinet Office and the Security and Intelligence Agencies*. Available at: https://www.gov.uk/government/publications/bbc-monitoring-agreement (Accessed: May 22, 2022).

Bean, H. (2007) "The DNI's open source center: An organizational communication perspective," *International Journal of Intelligence and CounterIntelligence*, 20(2), pp. 240–257. doi:10.1080/08850600600889100.

Benavides, E. ben (2011) *Open Source Intelligence (OSINT) Link Directory Targeting Tomorrow's Terrorist Today (T4) through OSINT*. Creative Commons. Available at: https://search.wikileaks.org/gifiles/attach/10/10459_Open%20Source%20In.pdf (Accessed: February 9, 2022).

Bernard, R.L. (2009) "ELECTRONIC INTELLIGENCE (ELINT) AT NSA," *Center for Cryptologic History, National Security Agency* [Preprint].

de Bochgrave, A., Sanderson, T. and MacGaffin, J. (2006) *Open source information: The missing dimension of intelligence*. Washington, D.C. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/060301_deBorchgrave_OpenSourceInfo_Web.pdf (Accessed: May 5, 2022).

Bohm, I. and Lolagar, S. (2021) "Open source intelligence Introduction, legal, and ethical considerations," *International Cybersecurity Law Review*, 2, pp. 317–337. doi:10.1365/s43439-021-00042-7.

Buzan, Barry. (2016) *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*. ECPR Press.

Cascavilla, G. *et al*. (2018) "OSSINT - Open Source Social Network Intelligence: An efficient and effective way to uncover 'private' information in OSN profiles," *Online Social Networks and Media*, 6, pp. 58–68. doi:10.1016/j.osnem.2018.04.003.

Central Intelligence Machinery - UK Intelligence Agencies (no date). Available at: https://www.globalsecurity.org/intell/world/uk/cim.htm (Accessed: May 22, 2022).

Central Security Service (2021). Available at: https://www.nsa.gov/About/Central-Security-Service/ (Accessed: December 30, 2021).

Clark, R.M. (2017) *Intelligence Analysis: A Target-Centric Approach*. Fifth Edition. Thousand Oaks, California 91320: CQ Press.

CSIS, Hicks, K. and Katz, B. (2021) *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation*. Washington, DC 20036. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf (Accessed: January 9, 2022).

Cumming, A. (2007) *Open Source Intelligence (OSINT): Issues for Congress*.

Davydoff, D. (2017) *What is the intelligence cycle and why do we use it? RETHINKING THE INTELLIGENCE CYCLE FOR THE PRIVATE SECTOR*. Alexandria, VA 22314.

Dawson, M., Lieble, M. and Adeboje, A. (2018) "Open source intelligence: Performing data mining and link analysis to track terrorist activities," in *Advances in Intelligent Systems and Computing*. Springer Verlag, pp. 159–163. doi:10.1007/978-3-319-54978-1_22.

Devine, M.E. (2019) “Intelligence Community Spending: Trends and Issues.” Available at: www.crs.gov (Accessed: May 21, 2022).

Edwards, M. *et al*. (2017) “Panning for gold: Automatically analysing online social engineering attack surfaces,” *Computers and Security*, 69, pp. 18–34. doi:10.1016/J.COSE.2016.12.013.

Evangelista, J.R.G. *et al*. (2021) “Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence,” *Journal of Applied Security Research*, 16(3), pp. 345–369. doi:10.1080/19361610.2020.1761737.

Fisher, T. (2019) *Search Engines: What They Are & How They Work*. Available at: https://www.lifewire.com/how-does-search-engine-work-3482032 (Accessed: January 3, 2022).

Gibson, S. (2004) “Open source intelligence: An intelligence lifeline,” *RUSI Journal*, 149(1), pp. 16–22. doi:10.1080/03071840408522977.

Gibson, S.D. (2007) *Open Source Intelligence: A Contemporary Intelligence Lifeline*. PhD Thesis. Cranfield University.

Gibson, S.D. (2014) “Open Source Intelligence,” in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge Companion to Intelligence Studies*. First Edition. London and New York: Routledge, pp. 123–131.

Gill, P. and Phythian, M. (2018) *Intelligence in an Insecure World*. Third Edition. Polity Press.

Glassman, M. and Kang, M.J. (2011) “Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT),” *Computers in Human Behavior*, 28(2), pp. 673–682. doi:10.1016/j.chb.2011.11.014.

Goodman, M.S. (2014) “The United Kingdom,” in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge companion to intelligence*. First Edition. London and New York: Routledge, pp. 135–144.

Hassan, N.A. and Hijazi, R. (2018) *Open Source Intelligence Methods and Tools A Practical Guide to Online Intelligence*. Apress. Available at: https://douran.academy/wp-content/uploads/ebooks/open-source-intelligence-methods-and-tools.pdf (Accessed: February 24, 2022).

Hauter, J. (2021) “Forensic conflict studies: Making sense of war in the social media age,” *Media, War & Conflict* [Preprint]. doi:10.1177/17506352211037325.

Hoffman, J. (2012) *Facebook Posts Can Offer Clues of Depression - The New York Times*, *The New York Times*. Available at: https://www.nytimes.com/2012/02/24/us/facebook-posts-can-offer-clues-of-depression.html (Accessed: April 13, 2022).

Hulnick, A.S. (2002) "The Downside of Open Source Intelligence," *International Journal of Intelligence and CounterIntelligence*, 15(4), pp. 565–579.

ten Hulsen, L. (2020) "OPEN SOURCING EVIDENCE FROM THE INTERNET – THE PROTECTION OF PRIVACY IN CIVILIAN CRIMINAL INVESTIGATIONS USING OSINT (OPEN-SOURCE INTELLIGENCE)," *Amsterdam Law Forum*, 12(2), p. 3. doi:10.37974/alf.353.

Hwang, Y.-W. *et al*. (2022) "Current Status and Security Trend of OSINT," *Wireless Communications and Mobile Computing*. Edited by Y. Huo, 2022, pp. 1–14. doi:10.1155/2022/1290129.

Janes | What we do (no date). Available at: https://www.janes.com/about-janes/what-we-do (Accessed: May 6, 2022).

Jensen, C.J.I., McElreath, D.H. and Graves, M. (2013) *Intelligence Studies Introduction to*. CRC Press.

Johnson, L.K. (2010) *The Oxford Handbook of National Security Intelligence*. Edited by L.K. Johnson. New York, NY: Oxford University Press.

Johnson, L.K. (2014) "The development of Intelligence Studies," in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge Companion to Intelligence Studies*. London and New York: Routledge, pp. 3–22.

Kandias, M. *et al*. (2017) "Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module," *Computers & Security*, 69, pp. 3–17.

Kanta, A., Coisel, I. and Scanlon, M. (2020) "A survey exploring open source Intelligence for smarter password cracking," *Forensic Science International: Digital Investigation*, 35. doi:10.1016/j.fsidi.2020.301075.

Katz, B. (2020) *The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence, Center for Strategic and International Studies*. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200417_Katz_IntelligenceEdge_WEB%20FINAL.pdf?dWNvglzd.By4.c6nic7X5xkNmOf4t1I4 (Accessed: January 9, 2022).

Konstantopoulos, I.L. (2017) "Democracy and an Open-Economy World Order," in Bitros, G.C. and Kyriazis, N.C. (eds) *Democracy and an Open-Economy World Order*. Cham: Springer International Publishing, pp. 3–24. doi:10.1007/978-3-319-52168-8.

Konstantopoulos, I.L. and Doga, A.M. (2015) "The (R)evolution of Intelligence as an Academic Discipline: Challenges and Constraints," *Journal of Mediterranean and Balkan Intelligence*, 5(1).

Koops, B.-J., Hoepman, J.-H. and Leenes, R. (2013) "Open-source intelligence and privacy by design," *Computer Law & Security Review*, 29, pp. 676–688. doi:10.1016/j.clsr.2013.09.005.

Lappas, D., Karampelas, P. and Fessakis, G. (2021) "Using Social Media Surveillance in Order to Enhance the Effectiveness of Crew Members in Search and Rescue Missions," in Çakırtaş, M. and Ozdemir, M.K. (eds) *Big Data and Social Media Analytics*. *Lecture Notes in Social Networks*. Springer, Cham, pp. 127–151. doi:10.1007/978-3-030-67044-3_7.

Leetaru, K. (2010) "The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)," *Studies in Intelligence*, 54(1), pp. 17–37.

Liaropoulos, A. (2008) "A Review of: 'The Three Foes of Intelligence,'" *International Journal of Intelligence and CounterIntelligence*, 21(2), pp. 405–408. doi:10.1080/08850600701854524.

Liaropoulos, A.N. and Konstantopoulos, I.L. (2014) "Reforming the Greek National Intelligence Service Untying the Gordian Knot," *Journal of Mediterranean and Balkan Intelligence*, 3(1), pp. 19–24.

Lowenthal, M.M. (2001) "OSINT: The State of the Art, the Artless State.," *Studies in Intelligence*, pp. 61–66. Available at: https://www.cia.gov/readingroom/docs/DOC_0006122548.pdf (Accessed: February 17, 2022).

Lowenthal, M.M. (2020) *Intelligence: From Secrets to Policy*. Eighth Edition. Thousand Oaks, California: SAGE/CQ Press.

Minas, H. (2010) "Can the Open Source Intelligence emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?," *Research Institute for European and American Studies*, 139. Available at: www.rieas.gr (Accessed: December 31, 2021).

NATO (2001) *NATO Open Source Intelligence Handbook*.

Office of the Director of National Intelligence (no date) *What is Intelligence?* Available at: https://www.dni.gov/index.php/what-we-do/what-is-intelligence (Accessed: December 27, 2021).

Omand, D. (no date) *The Importance of BBC Monitoring for Intelligence*. Available at: https://www.iwm.org.uk/research/research-projects/listening-to-the-world-bbc-monitoring-collection-ahrc-research-network/blogs (Accessed: May 22, 2022).

Omand, D., Bartlett, J. and Miller, C. (2012a) "Introducing social media intelligence (SOCMINT)," *Intelligence and National Security*, 27(6), pp. 801–823. doi:10.1080/02684527.2012.716965.

Omand, D., Bartlett, J. and Miller, C. (2012b) "Introducing social media intelligence (SOCMINT)," *Intelligence and National Security*, 27(6), pp. 801–823. doi:10.1080/02684527.2012.716965.

Organization - CIA (no date) *CIA*. Available at: https://www.cia.gov/about/organization/ (Accessed: May 21, 2022).

Pai, Y. and Prasad, K. (2021) "Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review," *International Journal of Applied Engineering and Management Letters (IJAEML) A Refereed International Journal of Srinivas University*, 5(2), pp. 2581–7000. doi:10.5281/zenodo.5171580.

Parachini, J. v., Williams, J.D. and Roberts, A.C. (2021) *An Early Policy Victory for DNI Haines: Boost the Priority of Open Sources Information*, *RAND*. Available at: https://www.rand.org/blog/2021/03/an-early-policy-victory-for-dni-haines-boost-the-priority.html (Accessed: January 5, 2022).

Peterson, M. (2005) *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC 20531: U.S. Department of Justice. Available at: www.ojp.usdoj.gov/BJA (Accessed: February 17, 2022).

Phythian, M. (2014) "Cultures of National Intelligence," in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge Companion to Intelligence Studies*. First Edition. London and New York: Routledge, pp. 33–41.

Quiggin, T. (2006) *CO06105 | It Sure is Dark in Those Classified Caves Open Source Intelligence for National Security - RSIS*. Available at: https://www.rsis.edu.sg/rsis-publication/cens/860-it-sure-is-dark-in-those-class/#.YcBMKWhByMo (Accessed: December 20, 2021).

Quiggin, T. (2007) *Seeing the Invisible National Security Intelligence in an Uncertain Age*. Singapore: World Sicentific.

Qusef, A. and Alkilani, H. (2022) "The effect of ISO/IEC 27001 standard over open-source intelligence," *PeerJ Computer Science*, 8, p. e810. doi:10.7717/peerj-cs.810.

Richards, J. (2014) "Signals Intelligence," in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge Companion to Intelligence Studies*. First Edition. London and New York: Routledge.

Richey, M.K. and Binz, M. (2015) "Open source collection methods for identifying radical extremists using social media," *International Journal of Intelligence and CounterIntelligence*, 28(2), pp. 347–364. doi:10.1080/08850607.2014.962374.

RIEAS (2018) *INTELLIGENCE JOURNAL*, *Research Institute for European and American Studies*. Available at: https://www.rieas.gr/intelligence-journal (Accessed: December 31, 2021).

Sands, A. (2005) "Integrating Open Sources into Transnational Threat Assessments," in Sims, J. and Gerber, B. (eds) *Transforming U.S. Intelligence*. First. Washington, D.C.: Georgetown University Press, pp. 63–73.

Shulsky, A.N. and Schmitt, G.J. (2002) *Silent Warfare*. Third edition. Washington, D.C.: Potomac Books, Inc.

Signorini, A., Segre, A.M. and Polgreen, P.M. (2011) "The Use of Twitter to Track Levels of Disease Activity and Public Concern in the U.S. during the Influenza a H1N1 Pandemic," *PLos ONE*, 6(5). doi:10.1371/journal.pone.0019467.

Steele, R.D. (1995) "The importance of open source intelligence to the military," *International Journal of Intelligence and CounterIntelligence*, 8(4), pp. 457–470. doi:10.1080/08850609508435298.

Steele, R.D. (2001) *On Intelligence: Spies and Secrecy in an Open World*. Oakton, Virginia: OSS International Press.

Steele, R.D. (2002) *The New Craft of Intelligence: Personal, Public, & Political*. Oakton, Virginia: OSS International Press.

Steele, R.D. (2010) *Intelligence for Earth: Clarity, Diversity, Integrity, & Sustainability*. Oakton, Virginia: Earth Intelligence Network.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005). WASHINGTON, D.C. 20503 . Available at: https://www.govinfo.gov/content/pkg/GPO-WMD/pdf/GPO-WMD.pdf (Accessed: May 21, 2022).

The Defence Committee (2016) *Open Source Stupidity: The Threat to the BBC Monitoring Service Fifth Report of Session 2016-17 Report, together with formal minutes relating to the report The Defence Committee HC 748*. London. Available at: www.parliament.uk. (Accessed: May 21, 2022).

Treverton, G.F. (2004) *Reshaping National Intelligence for an Age of Information*. Cambridge: Cambridge University Press.

Tropotei, T.O. (2018) "CRITICISM AGAINST THE INTELLIGENCE CYCLE," *SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE*, 20, pp. 77–88. doi:10.19062/2247-3173.2018.20.9.

Warner, M. (2014) “Theories of intelligence: the state of play,” in Dover, R., Goodman, M.S., and Hillebrand, C. (eds) *Routledge Companion to Intelligence Studies*. First Edition. London and New York: Routledge, pp. 25–32.

Weaver, G.S. (2008) “Open Source Intelligence (OSINT),” *The Police and the Military: Future Challenges and Opportunities in Public Safety*, 4. Available at: https://sciences.ucf.edu/fwg/wp-content/uploads/sites/24/2016/11/vol4Weaver.pdf (Accessed: February 17, 2022).

Weinbaum, C., Chan, A., *et al*. (2018) *Moving to the Unclassified: How the Intelligence Community Can Work from Unclassified Facilities*, *Moving to the Unclassified: How the Intelligence Community Can Work from Unclassified Facilities*. RAND Corporation. doi:10.7249/RR2024.

Weinbaum, C., Parachini, J. v, *et al*. (2018) *Perspectives and Opportunities in Intelligence for U.S. Leaders*, *RAND* . Available at: www.rand.org/t/PE287. (Accessed: January 9, 2022).

Weinbaum, C. (2021) *The Intelligence Community’s Deadly Bias Toward Classified Sources*. Available at: https://www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html (Accessed: January 5, 2022).

What is Grey Literature? - Grey Literature - LibGuides at University of Exeter (no date). Available at: https://libguides.exeter.ac.uk/c.php?g=670055&p=4756572 (Accessed: April 6, 2022).

WHO (2003) *Consensus document on the epidemiology of severe acute respiratory syndrome (SARS)*.

Wiil, U.K. (ed.) (2011) *Counterterrorism and Open Sources Intelligence*. Vienna: SpringerWienNewYork. Available at: www.springer.com/series/8768.

Williams, H.J. and Blum, I. (2018) *Defining second generation Open Source Intelligence (OSINT) for the defense enterprise*. Santa Monica, Calif.: RAND Corporation.

Wolfers, A. (1952) “‘National security’ as an ambiguous symbol,” *Political Science Quarterly*, 67(4), pp. 481–502. Available at: https://www.jstor.org/stable/2145138?casa_token=vUkGxgzfmHEAAAAA:idCnkwD0AznrlcoIFFroxNQipaInkRjQ98Ffh6G7XVEbjSteYsCzoJwGqJaHE98FxQMZNjp_X1i81b6mUbz_YMvZ9X9Ge3M-tC0TiLshccnfgv5DKWfY (Accessed: May 25, 2022).

Ελληνόγλωσση Βιβλιογραφία

Γκρίζα βιβλιογραφία: Τι είναι; | Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης Βιβλιοθήκη (no date). Available at:

https://www.lib.auth.gr/el/%CE%B3%CE%BA%CF%81%CE%AF%CE%B6%CE%B1-%CE%B2%CE%B9%CE%B2%CE%BB%CE%B9%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9 (Accessed: April 6, 2022).

Καθημερινή (2022) "Ευλογιά των πιθήκων: Πόσο επικίνδυνη είναι, τι θεραπείες υπάρχουν | Η ΚΑΘΗΜΕΡΙΝΗ," 22 May. Available at: https://www.kathimerini.gr/world/561875599/eylogia-ton-pithikon-poso-epikindyni-einai-ti-therapeies-yparchoyn/ (Accessed: May 26, 2022).

Κυρανούδη, Δ. (2015) *10 χρόνια από το τρομοκρατικό χτύπημα*, *DW*. Available at: https://www.dw.com/el/10-%CF%87%CF%81%CF%8C%CE%BD%CE%B9%CE%B1-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-%CF%84%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%B9%CE%BA%CF%8C-%CF%87%CF%84%CF%8D%CF%80%CE%B7%CE%BC%CE%B1/a-18567198 (Accessed: January 4, 2022).

Κωνσταντόπουλος, Ι. (2010) *Οικονομία και Κατασκοπεία: Θεωρία και Πράξη*. Εκδόσεις Ποιότητα. Available at: https://www.politeianet.gr/books/9789607803528-konstantopoulos-ioannis-poiotita-oikonomia-kai-kataskopeia-62707 (Accessed: December 31, 2021).

Κωνσταντόπουλος, Ι. (2018) "Πληροφόρηση και Ασφάλεια: Μία άρρηκτη σχέση," in Κεβόρκ, Η. and Κόλλιας, Χ. (eds) *Κείμενα στην Οικονομική της Άμυνας & της Ασφάλειας*. Βόλος: Πανεπιστημιακές Εκδόσεις Θεσσαλίας.

Κωνσταντόπουλος, Ι.Λ. (2015) "Ο Ρόλος της Παραπλάνησης στην Ειρήνη και στον Πόλεμο (Β΄ Μέρος)," *Αεροπορική Επιθεώρηση*, 104, pp. 127–164.

Μαυραγάνης, Κ. (2019) "Ιωάννης Κωνσταντόπουλος: Στόχοι των υβριδικών απειλών είναι οι κοινωνίες και όχι οι στρατοί | HuffPost Greece," *Huffingtonpost*. Available at: https://www.huffingtonpost.gr/entry/ioannes-konstantopoelos-stochoi-ton-evridikon-apeilon-einai-oi-koinonies-kai-ochi-oi-stratoi_gr_5cbee6ffe4b0f7a84a74b9e2 (Accessed: December 31, 2021).

Παπαγεωργίου, Γ. (no date) *Μέτρηση (ΕΓΚΥΡΟΤΗΤΑ/ ΑΞΙΟΠΙΣΤΙΑ)*, *Τμήμα Κοινωνιολογίας Σχολή Κοινωνικών Επιστημών Πανεπιστήμιο Κρήτης*. Available at: https://sociology.soc.uoc.gr/pegasoc/wp-content/uploads/2014/10/Microsoft-Word-Papageorgiou-Egkyrotita.pdf (Accessed: May 4, 2022).

ΜΗΛΙΑΔΗΣ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ.docx

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		