Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

Social Media Intelligence - SOCMINT: Προκλήσεις και Προοπτικές για τις Υπηρεσίες Πληροφοριών

Βασιλική Πουλάκη

Επιβλέπουσα Καθηγήτρια
Δρ. Στυλιανή Κλεάνθους

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Κοινωνικά Πληροφοριακά Συστήματα

Μεταπτυχιακή Διατριβή

Social Media Intelligence - SOCMINT: Προκλήσεις και Προοπτικές για τις Υπηρεσίες Πληροφοριών

Βασιλική Πουλάκη

Επιβλέπουσα Καθηγήτρια
Δρ. Στυλιανή Κλεάνθους

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Κοινωνικά Πληροφοριακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2021

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Η εντυπωσιακή ανάπτυξη των Μέσων Κοινωνικής Δικτύωσης (ΜΚΔ) ως συμπληρωματικής πηγής πληροφοριών, έχει αναδειχθεί σε επικουρικό εργαλείο πληροφόρησης "Social Media Intelligence – SOCMINT", το οποίο είναι αρωγός στη σχηματιζόμενη νέα πραγματικότητα πληροφοριακών αναγκών για τις Υπηρεσίες Πληροφοριών (ΥΠ). Στην εποχή της πληροφόρησης μέσω διαδικτύου, η αξιοποίηση των δυνατοτήτων που προσφέρει η τεχνολογία κρίνεται απαραίτητη. Τα δεδομένα που μπορεί να προκύψουν από τα ΜΚΔ συνιστούν προστιθέμενη αξία στη ροή πληροφοριών για τις υπηρεσίες οι οποίες πλέον προσαρμόζονται στις νέες συνθήκες, προκειμένου να προβλέπουν και να αντιμετωπίζουν υβριδικές απειλές και να εποπτεύουν διαμορφούμενες αλλαγές.

Τα ΜΚΔ έχουν αυξήσει κατακόρυφα τον όγκο πληροφοριών για τους αναλυτές, αλλά παράλληλα έχουν θέσει και νέες προκλήσεις. Η διάχυση της παραπληροφόρησης σε κλίμακα, ταχύτητα και ακρίβεια στόχευσης, μέσω υπολογιστικής προπαγάνδας, δημιουργίας εξατομικευμένων σφαιρών ενημέρωσης (filter bubble) και χώρων αλληλεπίδρασης ομονοούντων χρηστών (echo chamber), είναι πλέον άνευ προηγούμενου. Η παρούσα διατριβή καταγράφει τα είδη παραπληροφόρησης και τους μηχανισμούς που τα αναπαράγουν και τα οποία καλείται να αντιμετωπίσει η κοινότητα των ΥΠ. Στη συνέχεια, για την αντιμετώπιση της παραπληροφόρησης και της χειραγώγησης ΜΚΔ, παρουσιάζονται κάποιες ενδεικτικές ενέργειες σε επίπεδο αναλυτή, ΥΠ και κράτους, που προέκυψαν από την επεξεργασία αποτελεσμάτων διενεργηθείσας έρευνας με ερωτηματολόγιο.

Λέξεις κλειδιά: Μέσα Κοινωνικής Δικτύωσης, SOCMINT, OSINT, Information Disorder, Computational Propaganda, Παραπληροφόρηση.

Summary

The remarkable evolution of Social Network Sites (SNS) as a prolific information source, has become an add-on information tool (Social Media Intelligence - SOCMINT), which supports the emerging new order for agencies in the intelligence community. In the digital information age, it is essential to take full advantage of the available technological potential. The data that can be collated from the SNS are added value to the information flow across agencies, which adapt to a digitally changing environment, in order to identify hybrid threats and monitor emerging trends.

SNS have not only vastly increased the volume of information available to intelligence officers but have also posed new challenges. The dissemination of disinformation is unprecedented on a scale and with speed and precision of targeting through the media of computational propaganda, filter bubbles and echo chambers. This dissertation lists the types of disinformation types and the mechanisms that reproduce them, which the intelligence community is called upon to deal with. In order to deal with the disinformation and Social Media manipulation, some indicative proposals are presented at the level of intelligence analyst, agency and state, supported also by the results of a questionnaire-based survey.

Keywords: Social Media, SOCMINT, OSINT, Information Disorder, Computational Propaganda, Disinformation.

Ευχαριστίες

Πέρασαν κάποια χρόνια από εκείνο το καλοκαίρι που με τον Dr. P. προσπαθούσαμε να καταλάβουμε τι σημαίνει Κοινωνικά Πληροφοριακά Συστήματα. Ήμασταν και οι δύο πολύ μακριά από το επιστημονικό πεδίο των Information Systems, όχι όμως του Social. Είχε κλείσει ένας μεγάλος κύκλος με την κ. Κατεχάκη, απ' όπου κράτησα φίλους, γνώσεις, εμπειρία και την αγάπη για τη Μεγαλόνησο και τους Ανθρώπους της. Από το σημείο εκείνο ξεκίνησε ένας νέος κύκλος με τη Jahna, τη Στέλλα και το Κέντρο Αλγοριθμικής Διαφάνειας, που σήμαινε έρευνα, συγγραφή και μεράκι. Δεν ανακάλυψα έναν καινούριο κόσμο, βρήκα όμως ένα νέο τρόπο αντίληψης της πραγματικότητας, διαφανή μεν, με πολλά μαύρα κουτιά δε. Κι εκεί διαπίστωσα ότι οι δύο κύκλοι είναι ομόκεντροι. Σ' αυτό το πλαίσιο λοιπόν η επιλογή του θέματος SOCMINT δεν θα μπορούσε να ήταν διαφορετική και να ξεφύγει από το προσφιλές OSINT. Για καλή μου τύχη η Δρ. Στυλιανή Κλεάνθους με σεβασμό στην ερευνητική μου επιλογή και με διακριτική εποπτεία, με καθοδήγησε επιστημονικά και με ενθάρρυνε να ασχοληθώ μ' αυτό που με προκαλεί και με κεντρίζει, την αναζήτηση πληροφορίας.

Παραθέτω λοιπόν τις ευχαριστίες μου προς όλους εκείνους που στάθηκαν στο πλάι μου, αλλά και σ' εκείνους που με έμαθαν με αγάπη να κολυμπώ μεσοπέλαγα του Μυρτώου, στα δύσκολα.

Έφη και Τάσο†

Για «τα πιο ωραία λαϊκά» Ανωγείων, πανελλήνιες και μέχρι τώρα,

Μιχάλη aka Dr. P και Lisa,

Για την πρωτοπορία, το μένω εκτός, το πείσμα επιτυχίας παρά τους φόβους με «όλα τα έθνη»,

Γιώργο και Τάσσο,

Για τις αγκαλιές, τα χαμόγελα, τις ποδηλατάδες, τις ερωτήσεις, το «μαμά μπορώ να βοηθήσω;»

Σωτήρη,

Για την αγάπη, τη διαρκή συμπαράσταση, τη στωική υπομονή, για την πίστη ότι σ' όλα τα ταξίδια

«μαζί θα τα καταφέρουμε».

Κεφάλαιο 1
Γενικά

1.1. Εισαγωγή

Η ανάπτυξη της τεχνολογίας των επικοινωνιών είναι το κύριο χαρακτηριστικό μιας εποχής που έχει ξεκινήσει από τα μέσα του 20ου αιώνα, αλλάζοντας δραστικά το περιβάλλον σ' όλες τις πτυχές της ανθρώπινης δραστηριότητας, από την εκπαίδευση, τις επιστήμες, την καθημερινή ζωή έως και τον εργασιακό τομέα. Με το διαδίκτυο επήλθαν αλλαγές στη συμπεριφορά και τον τρόπο σκέψης του ατόμου και δόθηκαν αυξημένες δυνατότητες πρόσβασης σε μεγάλο όγκο πληροφοριών από καινούριες πηγές πληροφόρησης που διαμορφώθηκαν σ' όλους τους τομείς, επιστημονικούς και μη.

Μέχρι πρότινος οι πηγές πληροφόρησης πρωτογενείς, δευτερογενείς, τριτογενείς ήταν κυρίως έντυπες, με την πλειονότητα των πληροφοριών να προέρχεται κυρίως από τα έντυπα ΜΜΕ, επιστημονικά περιοδικά, αρχειακό υλικό, στατιστικές έρευνες κ.ο.κ. Οι Υπηρεσίες Πληροφοριών, εφεξής ΥΠ, δεν αποτελούν εξαίρεση στις αλλαγές που επέφερε η τεχνολογία, με την ηλεκτρονική αναζήτηση σε Μηχανές Αναζήτησης και τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ) να καθιστούν τη διαδικασία εντοπισμού και επεξεργασίας πληροφοριών απρόσκοπτη και ευκολότερη σε σύγκριση με τις πρακτικές του παρελθόντος. Τα ηλεκτρονικά περιοδικά και ΜΜΕ, οι online βάσεις δεδομένων, το Διαδίκτυο και τα ΜΚΔ δίνουν πλέον δυνατότητα πρόσβασης σε μια πανσπερμία πληροφοριών. Ο επιτελής σε λιγότερο από έναν αιώνα από την έλλειψη πληροφοριών βρίσκεται πλέον αντιμέτωπος με ενημερωτική αφθονία ή ακόμη και με «υπερφόρτωση» πληροφοριών (Keane, 2013).

1.2. Social Media Intelligence – SOCMINT

Τα τελευταία χρόνια σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο έχει αναπτυχθεί μια νέα τάση στη συλλογή δεδομένων και πληροφοριών από την πλευρά της πολιτείας και δη των αρμόδιων φορέων (ΥΠ, Ένοπλες Δυνάμεις, Σώματα Ασφαλείας, ΥπΕξ), υπέρ της συμπερίληψης των ΜΚΔ ως νέας πηγής πληροφοριών οι οποίες σε σύνθεση με διαβαθμισμένες θα μπορούσαν να παράγουν ένα ίσως πιο διαφορετικό πληροφοριακό προϊόν, προσαρμοσμένο στις ανάγκες και τις απαιτήσεις των κέντρων λήψης αποφάσεων.

Οι τάσεις αυτές στον εντοπισμό και την επεξεργασία πληροφοριών από τα ΜΚΔ (Social Media Intelligence – SOCMINT), επηρέασαν τις ΥΠ και συγκεκριμένα τις Διευθύνσεις Συλλογής και Ανάλυσης Πληροφοριών. Οι τελευταίες πλέον σε μεταβατικό στάδιο υιοθετούν νέες τεχνικές εντοπισμού, συλλογής, επεξεργασίας και ανάλυσης πληροφοριών από τα ΜΚΔ, προκειμένου έχοντας εκσυγχρονίσει την ηλεκτρονική πρόσβαση στις πλατφόρμες να φιλτράρουν έγκαιρα την πληροφορία – κλειδί από ένα τεράστιο όγκο δεδομένων.

Παράλληλα, οι ΥΠ καλούνται να αντιμετωπίσουν τις σύγχρονες προκλήσεις μ’ ένα κατάλληλο μοντέλο συλλογής πληροφοριών με διαδικασίες ελέγχου και ανάλυσης πληροφοριών από ΜΚΔ, σ’ ένα περιβάλλον διευρυμένης συνεργασίας με συναρμόδιους φορείς σε εθνικό και διεθνές επίπεδο, όπου το τελικό πληροφοριακό προϊόν αξιολογείται κυρίως σε επίπεδο συναρμόδιων φορέων και ασφαλώς ενδοϋπηρεσιακά. Ως εκ τούτου, η αξιολόγηση πληροφοριών από ΜΚΔ συνιστά μια αναγκαία επιτελική δραστηριότητα συνεπή με την ιδέα της έγκυρης και έγκαιρης πληροφόρησης συνεργαζόμενων φορέων και του οικοσυστήματος ανταλλαγής διαβαθμισμένων πληροφοριών, η οποία συμβάλλει στην αντιμετώπιση κινδύνων και απειλών και στη διαφύλαξη ενός περιβάλλοντος εθνικής, ευρωπαϊκής και διεθνούς ασφαλείας. Παράλληλα η επεξεργασία και αξιολόγηση του υλικού από ΜΚΔ λειτουργεί και ως μηχανισμός εισαγωγής αλλαγών στην πληροφοριακή ροή, καθώς δίνει τη δυνατότητα στους αναλυτές πληροφοριών να διαμορφώνουν μια συνολική εικόνα για το πληροφοριακό ζητούμενο, συμβάλλει στη σύγκριση και σύνθεση μ’ άλλες πληροφορίες και θέτει τις βάσεις για ένα συνεχώς βελτιούμενο πληροφοριακό

περιβάλλον.

Αρκετά συχνά όμως αναδύονται προκλήσεις σε εθνικό και διεθνές επίπεδο ως αποτέλεσμα κακόβουλης εκμετάλλευσης τεχνολογιών επικοινωνίας μέσω ΜΚΔ, από απολυταρχικά καθεστώτα, παράνομες ομάδες και οργανώσεις, μεμονωμένους πραγματικούς, ψευδείς ή και εικονικούς χρήστες. Ως αποτέλεσμα οι ΥΠ καλούνται να αντιμετωπίσουν μια σειρά προκλήσεων - κινδύνων όπως τις ψευδείς ειδήσεις, παραπληροφόρηση, social bots, trolls, filter bubble, κ.ο.κ. Ανεξάρτητα με τις δυνατότητες εντοπισμού και αντιμετώπισης, το μεγαλύτερο μέρος ανάδειξης τέτοιων φαινομένων επαφίεται στην κριτική αντίληψη, τη γνώση και την εμπειρία του επιτελή. Στο πλαίσιο αυτό, η αναλυτική καταγραφή των προκλήσεων – κινδύνων και οι τεχνικές αντιμετώπισης των φαινομένων παραπληροφόρησης, είναι θέμα υπό διερεύνηση, με την όποια πρόοδο στο SOCMINT να βρίσκεται ακόμη σε πρώιμο στάδιο, τουλάχιστον σε εθνικό επίπεδο.

Πληροφορίες για υπό διερεύνηση πρόσωπα, διεθνείς εξελίξεις, στρατιωτικές συρράξεις, τρομοκρατικά δίκτυα, ομάδες οργανωμένου εγκλήματος, ιδεολογικά ακραίες οργανώσεις δύναται να εντοπιστούν σε διάφορες πλατφόρμες ΜΚΔ και κάθε φορά να αντιμετωπίζονται υπό διαφορετική οπτική γωνία. Υπ’ αυτή την έννοια, η αναζήτηση πληροφοριών συνιστά μια πολυπτυχή επιτελική δραστηριότητα, καθώς η πληροφοριακή έρευνα μπορεί να επεκταθεί σε πηγές-λογαριασμούς ΜΚΔ που εξυπηρετούν διαφορετικές σκοπιμότητες. Επ’ αυτού χρήζει επισήμανσης ότι ο επιτελής αναμένεται να είναι σε θέση να κρίνει το βαθμό αξιοπιστίας πηγής, την ακρίβεια της πληροφορίας, τα μέσα μετάδοσής της και τυχόν σκοπιμότητες που εξυπηρετεί. Στο πλαίσιο αυτό, οι επιτελείς θεωρούνται “Information literates”, καθώς *«έχουν εκπαιδευτεί στην εφαρμογή πηγών πληροφοριών στην εργασία τους, όπου έχουν μάθει τεχνικές και δεξιότητες για τη χρήση ενός ευρέους φάσματος εργαλείων πληροφόρησης και πρωτογενών πηγών για τη διαμόρφωση λύσεων πληροφοριών στα προβλήματά τους»* (Zurkowski, 1974).

Μολονότι οι πληροφοριακές ανάγκες των ΥΠ μπορεί να διαφέρουν από κράτος σε κράτος, οι προκλήσεις που προβάλλονται από τη χρήση ΜΚΔ ως εργαλείο άντλησης πληροφοριών είναι κοινές. Συνήθως οι απαιτήσεις για πληροφορία προσδιορίζονται

από τη σκοπιμότητα απόκτησης της πληροφορίας, σε κάποιες περιπτώσεις δε απαιτείται και η συνέργεια μεταξύ ΥΠ, όταν τα υπό διερεύνηση ζητήματα άπτονται διασυνοριακής - διαπεριφερειακής (λ.χ. προσφυγικό, τρομοκρατία, λαθρεμπόριο) ή και διεθνούς συνεργασίας (επιδημίες, συγκρούσεις). Στο πλαίσιο αυτό, η πληροφοριακή διαχείριση ενός τεράστιου όγκου δεδομένων (Big Data) για να εξαχθεί αξιοποιήσιμη πληροφορία, προϋποθέτει εξοικείωση με τις νέες προκλήσεις.

Σε κάθε περίπτωση, εξυπακούεται ότι η απόκτηση εξειδικευμένων δεξιοτήτων για την αντιμετώπιση πιθανών κινδύνων κατά τη συλλογή και επεξεργασία, διαφοροποιείται ανάλογα με το οικονομικό επίπεδο των χωρών. Ως εκ τούτου, ΥΠ χωρών όπως Η.Π.Α. (IC)[1], Η.Β. (SIS ή MI6), Γαλλίας (DGSE), Γερμανίας (BND), Ρωσίας (SVR & GRU), Κίνας (MSS), Τουρκίας (MIT), Ισραήλ (MOSSAD), έχουν σημαντικό προβάδισμα σε σύγκριση με εκείνες, μικρότερων χωρών όπως Ελλάδας και Κύπρου, οι οποίες παρά το μικρότερο βαθμό εξοικείωσης, φαίνεται να κινούνται προς την ίδια κατεύθυνση. Σε κάθε περίπτωση, η αξιοποίηση των νέων τεχνολογιών επικοινωνίας μπορεί να είναι ενδεικτικές του βαθμού εξοικείωσης των ΥΠ, ωστόσο τα τελευταία χρόνια η αξιοποίηση έχει μετεξελιχθεί σε εκμετάλλευση των ΜΚΔ προς ίδιον όφελος με στόχους είτε στο εσωτερικό, είτε σε βάρος τρίτων χωρών, όπως την επιβεβαιωμένη ρωσική ανάμειξη στις προεδρικές εκλογές στις ΗΠΑ (2016, 2020), τις γαλλικές προεδρικές εκλογές (2017) και την πανδημία παραπληροφόρησης ή «infodemic».[2]

Το SOCMINT σε αντίθεση με τις υπόλοιπες πηγές πληροφοριών[3] δεν προϋποθέτει

---

[1] Η Κοινότητα Πληροφοριών των ΗΠΑ (US Intelligence Community - IC) είναι ομοσπονδία 17 υπηρεσιών, μεταξύ των οποίων CIA, NSA, DIA, I&A, TFI, INR, MIC, IB, ONSI κι άλλες.

[2] Infodemic είναι η παραπληροφόρηση επί θεμάτων δημόσιας υγείας. Ο όρος εμφανίστηκε κατά την επιδημία SARS-CoV-1 2013 και εκ νέου το 2020 λόγω SARS-CoV-2. https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19 (Ανάκτηση 05.04.2021).

[3] Το οικοσύστημα πληροφόρησης στις ΥΠ κατηγοριοποιείται βάσει μεθόδου συλλογής πληροφοριών και της πηγής προέλευσης. Πέρα από το OSINT που αφορά μη διαβαθμισμένες πληροφορίες ανοικτών πηγών, οι υπόλοιπες κατηγορίες είναι απόρρητες και αφορούν: 1) Ανθρώπινες Πηγές (**Human Intelligence – HUMINT**) 2) Μεταδόσεις Σημάτων (**Signals Intelligence – SIGINT**) προερχόμενες από πλοία, α/φ, δορυφόρους. Στην κατηγορία υπάγονται και οι Πληροφορίες Επικοινωνιών (**Communication Intelligence - COMINT**), οι Πληροφορίες Τηλεμετρίας (**Telemetry Intelligence - TELINT**) και οι Ηλεκτρονικές Πληροφορίες (**Electronic Intelligence - ELINT**), οι οποίες συνεισφέρουν στο MASINT. 3) Εικόνες (**Imagery Intelligence – IMINT** ή αλλιώς **Photo Intelligence - PHOTINT**). Σ' αυτή την κατηγορία

προϋπολογισμό μυστικών κονδυλίων και αποδέσμευση για το σχεδιασμό και την υλοποίησή του, ωστόσο οι προκλήσεις του SOCMINT συνδέονται κατά κύριο λόγο με την αξιολόγηση πηγών και πληροφοριών. Το ζητούμενο κατά την αναζήτηση πληροφοριών στα ΜΚΔ, δεν είναι ο εντοπισμός πολυάριθμων πληροφοριών, αλλά ο εντοπισμός στοιχείων συναφών με απόρρητες πληροφορίες. Στο πλαίσιο αυτό, ο επιτελής με δεξιότητα ελέγχου οφείλει να διακρίνει τα ποιοτικά εκείνα χαρακτηριστικά, αλλά και τις ενδείξεις που αφορούν στην πηγή και την πληροφορία αυτή καθ' αυτή.

1.3. Σκοπός Μεταπτυχιακής Διατριβής

Σκοπός της εργασίας είναι ο καθορισμός, η παρουσίαση και η ανάλυση μιας διαδικασίας με τα στάδια που πρέπει να ακολουθηθούν προκειμένου οι επιτελείς πληροφοριών να είναι σε θέση να εντοπίζουν, να επεξεργάζονται και να αξιοποιούν την πληροφορία από ΜΚΔ. Για να καταστεί αποτελεσματική η διαδικασία, πρέπει να γίνει μια μοντελοποίηση των δεδομένων εκείνων που διαχέονται στις πλατφόρμες με σκοπό την πρόκληση "information disorder" ως αποτέλεσμα της παραπληροφόρησης (disinformation, misinformation, malinformation) σε συνδυασμό με τα φαινόμενα του Filter Bubble και Echo Chamber. Η μοντελοποίηση των πληροφοριακών φαινομένων και ο καθορισμός μιας διαδικασίας, που αφορά στον τρόπο εντοπισμού αξιοποιήσιμων πληροφοριών από τα ΜΚΔ, θα βοηθήσει τους αναλυτές σε αποτελεσματική και ασφαλή ανάλυση στοιχείων και σύνθεσής τους με πληροφορίες από διαβαθμισμένες πηγές.

1.3.1. Αναγκαιότητα και σπουδαιότητα της έρευνας

Η μελέτη της τεχνολογίας και της πληροφορίας διασυνδέεται και με το επιστημονικό πεδίο των Διεθνών Σχέσεων. Ερευνητές διερευνούν κατά πόσο και με ποιους τρόπους η τεχνολογία δύναται να διαταράξει τη δημοκρατία, ενισχύοντας ή περιορίζοντας τα ανθρώπινα δικαιώματα, να καθορίσει πολιτικές αλληλεπιδράσεις, καθιστώντας το διαδίκτυο ψηφιακό μέτωπο επιχειρήσεων. Υποστηρίζεται δε ότι η απρόσκοπτη πρόσβαση στα ΜΚΔ με μηδενικό κόστος, έχει αλλάξει την ισορροπία ισχύος υπέρ

υπάγονται και οι Γεωχωρικές Πληροφορίες (**Geospatial Intelligence** - **GEOINT**), που συλλέγονται από δορυφόρους. 4) Πληροφορίες Μετρήσεων **(Measurement and Signatures Intelligence - MASINT)**, που προκύπτουν από μετρήσεις ηλεκτρομαγνητικού φάσματος. Intelligence Studies: Types of Intelligence Collection, https://usnwc.libguides.com/c.php?g=494120&p=3381426 (Ανάκτηση 24.01.2021).

μικρών παραγόντων όπως τρομοκρατικών ομάδων, κοινωνικών κινημάτων και ανεξάρτητων μεμονωμένων ατόμων, αποκομίζοντας πολιτικά οφέλη όπως λ.χ. κατάληψη εξουσίας σε αραβικά κράτη.

Στον αντίποδα, υπάρχουν και παραδείγματα κυβερνήσεων χωρών που αξιοποιούν τα ΜΚΔ για χειραγώγηση της κοινής γνώμης, αναθέτοντας σε εξειδικευμένο προσωπικό το σχεδιασμό και τη διενέργεια εκστρατειών παραπληροφόρησης και προπαγάνδας στο διαδίκτυο, υπό την έννοια της ήπιας ισχύος. Δηλαδή του όρου Soft Power που εισήγαγε ο Joseph Nye, δηλαδή της «*προπαγάνδας που δεν είναι προπαγάνδα*», της δυνατότητας να *«φτάσεις τους στόχους σου χωρίς κανένα εξαναγκασμό, χωρίς μάλιστα να το γνωρίζει το άλλο κράτος.»* (Nye, 1990).

Αυτός ο αναδυόμενος τομέας έρευνας καθίσταται κεντρικός στο επιστημονικό πεδίο των Διεθνών Σχέσεων και συγκεκριμένα στο πεδίο ασφάλειας και Intelligence Studies, που θεωρείται η «χαμένη διάσταση» στις διεθνείς σχέσεις, καθώς ο απόρρητος χαρακτήρας δραστηριοτήτων ΥΠ καθιστά τις «επιτυχίες» άγνωστες,[4] όχι όμως πλέον. Το συγκεκριμένο πεδίο συνυφασμένο με τις νέες εκφάνσεις των Διεθνών Σχέσεων στο διαδίκτυο, προσφέρει ευκαιρία μελέτης και κατανόησης των δυνατοτήτων μετάλλαξης και άσκησης «κυβερνοδύναμης» στην ψηφιακή εποχή.

Σ' αυτό το πλαίσιο, οι ΥΠ συμπεριλαμβάνουν το SOCMINT ως πρακτική συλλογής πληροφοριών από ανοικτές πηγές, είτε αφορά σε δημόσιο ή ιδιωτικό λογαριασμό. Για τους αρμόδιους επιτελείς Συλλογής και Ανάλυσης των ΥΠ ή των συναρμοδίων αρχών, φαίνεται να συνιστά πλέον κύρια ή και συμπληρωματική πηγή πληροφοριών και σπανιότερα μια δευτερεύουσας σημασίας πηγή. Η επιστράτευση των ΜΚΔ στον πόλεμο παραπληροφόρησης μπορεί να σχεδιαστεί και να επιτύχει το στρατηγικό στόχο, παράλληλα όμως καταδεικνύει τις αδυναμίες αντιμετώπισης των φαινομένων, ακόμη και από εξειδικευμένες ομάδες κρούσης σε προηγμένες σε υλικοτεχνικό επίπεδο ΥΠ.

Το πολιτικό κόστος από την αδυναμία πλήρους αξιοποίησης του SOCMINT για τη διαφύλαξη και προάσπιση ενός περιβάλλοντος διεθνούς πληροφοριακής ασφάλειας,

[4] Intelligence Studies. (20 Ιουλίου 2020). *Wikipedia*. https://en.wikipedia.org/wiki/Intelligence_studies#cite_note-1

φαίνεται να είναι αρκετά υψηλό. Στη πλαίσιο αυτό κρίνεται ως επιτακτική η ανάγκη για παραμετροποίηση: να τεθούν δηλαδή ορισμένες παράμετροι, προκειμένου οι Διευθύνσεις Συλλογής και Ανάλυσης να στραφούν στις σύγχρονες προκλήσεις που διαμορφώνονται στα ΜΚΔ για να αντιμετωπιστούν κίνδυνοι και απειλές ως απόρροια κακόβουλης και υστερόβουλης χρήσης τους. Αυτές οι ρυθμίσεις είναι μείζονος σημασίας για την πλήρη αξιοποίηση του SOCMINT, καθώς θα έχουν καθοριστικό ρόλο ώστε να φτάσουν στο μέγιστο δυνατό οι δυνατότητες έρευνας και εντοπισμού πληροφοριών στις πλατφόρμες των ΜΚΔ. Προσδοκώμενα αποτελέσματα αυτής της διατριβής είναι η καταγραφή των φαινομένων και η συγγραφή προτάσεων βελτίωσης των σταδίων επεξεργασίας και αξιολόγησης πληροφοριών από ΜΚΔ, στοχεύοντας στην αποτροπή ή αντιμετώπιση των φαινομένων.

Η καινοτομία της διατριβής εστιάζει στη μοντελοποίηση των πληροφοριών που διαχέονται στα ΜΚΔ και είναι ενδιαφέροντος ΥΠ, καθώς και στον καθορισμό συγκεκριμένων σταδίων συλλογής, επεξεργασίας κι αξιολόγησης πληροφοριών, τα οποία θα εξοικονομούν χρόνο αυτοματοποιώντας τη διαδικασία. Στη βάση αυτή θα είναι πιο αποτελεσματική και η ανάκτηση συναφών στοιχείων από το σύστημα συλλογής δεδομένων (Data Management System) της ΥΠ. Συμπεριλαμβάνονται δε και εμπειρικά δεδομένα από στελέχη των ΥΠ, Σωμάτων Ασφαλείας κ.ο.κ. σε εθνικό, περιφερειακό και διεθνές επίπεδο, η συμπερίληψη των οποίων κρίθηκε χρήσιμη, καθώς εξάγονται συμπεράσματα από την πρακτική ενασχόληση με το SOCMINT.

1.4. Μεθοδολογία

Η μεθοδολογία της παρούσας διατριβής παρουσιάζεται ακολούθως:

1.4.1. Βιβλιογραφική Ανασκόπηση

Στη βιβλιογραφική ανασκόπηση συμπεριλαμβάνονται οι κυριότερες ερμηνευτικές προσεγγίσεις της επιστημονικής κοινότητας στο πεδίο των ΜΚΔ με χρήση της σχετικής αρθρογραφίας αναφοράς, που περιλαμβάνουν βιβλία, επιστημονικά άρθρα, εκθέσεις Ευρωπαϊκών Θεσμών (Ευρωπαϊκή Επιτροπή και Κοινοβούλιο) ή Διεθνών Οργανισμών (Συμβούλιο της Ευρώπης), σχετικά με την παραπληροφόρηση, αλλά και αδιαβάθμητες αναφορές ΥΠ των Η.Π.Α. ή επιτροπών της αμερικανικής Γερουσίας.

Τα ερευνητικά ερωτήματα στα οποία η παρούσα μελέτη επιδιώκει να απαντήσει και τα οποία συμβάλλουν στον καλύτερο σχεδιασμό της δομής της παρούσας διατριβής, διαμορφώνονται ως εξής:

1. Ποιες οι πληροφορίες είναι ενδιαφέροντος για τις ΥΠ στα ΜΚΔ και τι είδους;
2. Ποια είναι οι κύριες υποκατηγορίες του Information Disorder, που μπορεί να επηρεάσουν το στάδιο επεξεργασίας και αξιολόγησης μιας πληροφορίας;
3. Ποιες είναι ο ρόλος των social bots, trolls κ.ά. στη χειραγώγηση της κοινής γνώμης και σε τυχόν αποπροσανατολισμό του επιτελή από τη ζητούμενη πληροφορία;
4. Τι ρόλο μπορούν να διαδραματίσουν τα Echo Chambers, Filter Bubbles και σειρά προκαταλήψεων όπως της επιβεβαίωσης, στην ευθυκρισία του επιτελή;
5. Τι παρατηρείται στην περίπτωση της Τουρκίας σε σχέση με τα ανωτέρω;
6. Ποια τα βήματα που οφείλει να ακολουθήσει ο επιτελής προκειμένου να μειώσει το ενδεχόμενο προσωρινού αποπροσανατολισμού από τον όγκο δεδομένων και του περιεχομένου τους;
7. Σε ποιο βαθμό και με ποιο τρόπο μπορούν να ανταποκριθούν οι ΥΠ, στις νέες προκλήσεις των ΜΚΔ.

1.4.2. Επιπρόσθετες πηγές δεδομένων

Επιπρόσθετα της βιβλιογραφίας, χρησιμοποιήθηκε μια επιπλέον μέθοδος για τη συμπερίληψη στοιχείων και πληροφοριών σχετικά με τις προκλήσεις του SOCMINT. Μέρος των ερευνητικών ερωτημάτων συμπεριελήφθησαν σε ερωτηματολόγιο (ΠΑΡΑΡΤΗΜΑ Α) το οποίο διακινήθηκε σε Ευρώπη, Β. Αμερική και Μ. Ανατολή σε περιορισμένο αριθμό αποδεκτών, πάραυτα εξειδικευμένο προσωπικό σε OSINT και SOCMINT. Οι πληροφορίες που προέκυψαν από τις απαντήσεις που συνελέγησαν μέσω του ερωτηματολογίου, αξιολογούνται και ερμηνεύονται στο Κεφάλαιο 6 της παρούσας διατριβής.

1.4.3. Επιλογή Δείγματος

Λόγω της ιδιαιτερότητας του συγκεκριμένου αντικειμένου μελέτης, το μέγεθος του δείγματος μπορεί να είναι μικρό, ωστόσο είναι αντιπροσωπευτικό δεδομένου ότι τα

στελέχη έχουν εξοικείωση με το αντικείμενο ή εποπτεία για το τελικό παραγόμενο πληροφοριακό υλικό από τα ΜΚΔ. Πλέον συγκεκριμένα συμπεριελήφθησαν στοιχεία από στελέχη σε:

- ΥΠ Κρατών-μελών Ε.Ε.
- Αρμόδιες Ευρωπαϊκές Υπηρεσίες.
- ΥΠ Η.Π.Α.

1.5. Δομή Μεταπτυχιακής Διατριβής

Η εργασία θα αποτελείται από 7 βασικά κεφάλαια, η οποία μετά το εισαγωγικό (Κεφάλαιο 1), έχει την ακόλουθη δομή:

- Στο Κεφάλαιο 2 γίνεται αναφορά στη θεωρία και τις βασικές έννοιες των ΜΚΔ. Επιπρόσθετα, παρουσιάζονται οι τύποι των δεδομένων και των πληροφοριών που εντοπίζονται στα ΜΚΔ και τις κατηγορίες των χρηστών.

- Στο Κεφάλαιο 3 γίνεται ειδική αναφορά στη συλλογή πληροφοριών από Ανοικτές Πηγές (OSINT) και στην υποκατηγορία του SOCMINT.

- Στο Κεφάλαιο 4 δίδεται έμφαση στο Information Disorder, τα είδη που απαντούν κατά την άντληση πληροφοριών από τα ΜΚΔ, καθώς και στα φαινόμενα του Filter Bubble και Echo Chambers.

- Στο Κεφάλαιο 5 μελετάται η περίπτωση της Τουρκίας όσον αφορά τη χειραγώγηση των ΜΚΔ από την κυβέρνηση του ΑΚΡ.

- Στο Κεφάλαιο 6 παρουσιάζονται οι απαντήσεις που συλλέχθηκαν από το ερωτηματολόγιο και μια συγκριτική παρουσίαση των αποτελεσμάτων με βάση τα δημογραφικά χαρακτηριστικά.

- Το Κεφάλαιο 7 ολοκληρώνεται με την καταγραφή συμπερασμάτων και προτάσεων.

Κεφάλαιο 2
ΜΚΔ:Έννοιες – Θεωρία

2.1. Social Media - Ορισμός

Στους επικρατέστερους ορισμούς που απαντούν σε σχετικά συγγράμματα για ΜΚΔ, δύναται να συμπεριληφθεί των Kaplan και Haenlein (2010) σύμφωνα με τον οποίο «*τα μέσα κοινωνικής δικτύωσης είναι ένα σύνολο από διαδικτυακές εφαρμογές που βασίζονται στα ιδεολογικά και τεχνολογικά θεμέλια του Web 2.0 και επιτρέπουν τη δημιουργία και την ανταλλαγή περιεχομένου User Generated Content*».[5] Ωστόσο συνιστά μια σημαντική υπενθύμιση για τον τρόπο που τα ΜΚΔ έχουν μετεξελιχθεί από τεχνολογικά σε εμπορικά πλέον εγχειρήματα που μπορεί αφενός να προσπορίζουν ίδιο όφελος, ταυτόχρονα όμως κομίζουν προστιθέμενη αξία στη ροή πληροφοριών προς ΥΠ, που μέχρι πρότινος στηρίζονταν αποκλειστικά σ' άλλες πηγές πληροφοριών.

Συμπληρωματικά, χαρακτηριστικός είναι και ο ορισμός που δίδεται από τους Kwon & Wen (2010) όπου ορίζουν «*τα online κοινωνικά δίκτυα είναι δικτυακοί τόποι που επιτρέπουν την οικοδόμηση σχέσεων μεταξύ προσώπων σε απευθείας σύνδεση μέσω της συλλογής χρήσιμων πληροφοριών και του διαμοιρασμού αυτών με άλλους ανθρώπους. Επίσης, μπορούν να δημιουργήσουν ομάδες, οι οποίες επιτρέπουν την αλληλεπίδραση μεταξύ των χρηστών με παρόμοια ενδιαφέροντα*».

Σε επίπεδο κοινωνικής αλληλεπίδρασης μεταξύ των χρηστών, ο ορισμός των Boyd &

[5] Το User Created/ή Generated Content (UCC ή UGC) είναι οποιαδήποτε μορφή περιεχομένου (εικόνα, βίντεο, κείμενο, ήχος) αναρτημένο σε διαδικτυακές πλατφόρμες όπως ΜΚΔ. Ως UGC θεωρείται το περιεχόμενο εφόσον (α) είναι δημοσιευμένο σε ιστοσελίδα ή πλατφόρμα (β) συνιστά αποτέλεσμα δημιουργικής προσπάθειας, επομένως αναδημοσίευση περιεχομένου δεν θεωρείται UGC και (γ) έχει δημιουργηθεί από απλούς χρήστες. OECD, DSTI/ICCP/IE(2006)7/FINAL, 12-Apr-2007, σελ. 8.

Ellison προσδίδει μια κοινωνιολογική οπτική στον ορισμό τους, σύμφωνα με τον οποίο «*Τα online κοινωνικά δίκτυα ορίζονται ως web-based (διαδικτυακές) υπηρεσίες που επιτρέπουν σε άτομα (1) να δημιουργήσουν ένα δημόσιο ή ημι-δημόσιο προφίλ μέσα σε ένα οριοθετημένο σύστημα, (2) να επικοινωνήσουν με μια λίστα από άλλους χρήστες με τους οποίους μοιράζονται μια μορφή σύνδεσης και (3) να δουν και να διανείμουν τη δική τους λίστα συνδέσεων και αυτών που φτιάχτηκαν από άλλους μέσα στο σύστημα*» (Boyd & Ellison, 2008).

2.2. ΜΚΔ: Βασικά Χαρακτηριστικά

Μολονότι ο όρος ΜΚΔ μπορεί να είναι γενικός και να καλύπτει διαφορετικές διαδικτυακές πλατφόρμες με πληθώρα χαρακτηριστικών σε ό,τι αφορά τους τρόπους επικοινωνίας ή τις εγγενείς τους λειτουργίες, υφίστανται λειτουργικά χαρακτηριστικά τα οποία συνιστούν κοινό τόπο σ' όλα τα ΜΚΔ και συνοψίζονται, κατά Mayfield (2008), στα ακόλουθα:

Συμμετοχή: παροτρύνουν τον ενδιαφερόμενο να συνεισφέρει και να προσφέρει ανατροφοδότηση και συμμετοχή. Τα ΜΚΔ ενθαρρύνουν τη συμμετοχή των χρηστών υπό τη μορφή νέων αναρτήσεων, σχολίων, κοινοποιήσεων, likes.

Διαφάνεια (openness): οι περισσότερες πλατφόρμες είναι ανοικτές για ανατροφοδότηση, καθώς ενθαρρύνονται σχόλια και κοινοποιήσεις, χωρίς να εμφανίζονται εμπόδια κατά την πρόσβαση και τη χρήση του περιεχομένου.

Συνομιλία: παρέχεται η δυνατότητα αμφίδρομης επικοινωνίας, σε αντίθεση με τη μονόδρομη ροή πληροφοριών από τα παραδοσιακά ΜΜΕ.

Κοινότητα: διευκολύνουν τη γρήγορη διαμόρφωση κοινοτήτων και την αποτελεσματική επικοινωνία μεταξύ των χρηστών. Το χαρακτηριστικό αυτό εξυπηρετεί την ανάγκη κοινωνικοποίησης και της συνεπακόλουθης δημιουργίας κοινοτήτων, ανάγκη που λήφθηκε υπόψη κατά το σχεδιασμό των ΜΚΔ.

Συνεκτικότητα (connectedness): αναπτύσσουν τη συνεκτικότητά τους, δημιουργώντας συνδέσεις μ' άλλες ιστοσελίδες, πηγές και ανθρώπους. Στο πλαίσιο αυτό διευρύνεται έτι περαιτέρω το εύρος του κάθε ΜΚΔ.

2.3. Κατηγορίες ΜΚΔ

2.3.1. Συνεργατικής Συγγραφής (Collaborative Authoring)

Στα συνεργατικής συγγραφής οι χρήστες συμπράττουν για τον εμπλουτισμό περιεχομένου σε ένα συγκεκριμένο θέμα (Allen, 2011). Η συνέργεια αυτή αποδεικνύει ότι τα συνεργατικά έργα συνιστούν το πλέον δημοκρατικό παράδειγμα δημοκρατικής εκδήλωσης του UGC για τους Kaplan & Heinlein (2010), ενώ όπως το Wikipedia ή το Quora, μπορεί να αποτελεί μια σημαντική πηγή πληροφόρησης για το ευρύ κοινό (Kaplan & Heinlein, 2010). Ωστόσο αυτό δεν ισχύει για τους χρήστες που αναζητούν πληροφορίες στη γλώσσα τους, είτε και για τις ΥΠ. Ενδεικτικά αναφέρεται ότι στην πολύγλωσση online εγκυκλοπαίδεια Wikipedia, τα λήμματα που φιλοξενούνται σ' άλλες γλώσσες πλην της αγγλικής, μπορούν να έχουν διαφορετικό περιεχόμενο είτε κι ακόμη αντίθετο, με χαρακτηριστικά παραδείγματα να υπάρχουν σε περιπτώσεις που αφορούν λ.χ. ιστορικά γεγονότα ή πολεμικές συγκρούσεις.

2.3.2. Ιστολόγια/Μικροϊστολόγια (Blogs/Microblogging)

Τα ιστολόγια είναι από τις πρώτες μορφές κοινωνικών δικτύων, όπου αναρτώνται κείμενα, απόψεις με πλέον χαρακτηριστικό και δημοφιλές παράδειγμα blog αυτό του Twitter (TW). Το τελευταίο ανήκει στην κατηγορία του microblogging, όπου με συγκεκριμένο αριθμό χαρακτήρων γίνεται συνοπτική καταγραφή των σκέψεων και συναισθημάτων χρήστη ή και περιγραφή καταστάσεων. Εκτός από το TW, γενικά η χρήση των ιστολογίων είναι σχετικά περιορισμένη, ωστόσο για τις ΥΠ είναι προστιθέμενης αξίας λόγω της άμεσης πληροφοριακής ροής και έχει συμπυκνωμένη μορφή.

2.3.3. Κοινότητες περιεχομένου (Content Communities)

Οι κοινότητες περιεχομένου είναι διαδικτυακές βάσεις δεδομένων με περιεχόμενο πολυμέσων, όπου οι χρήστες μπορούν να αναρτήσουν υλικό πολυμέσων κατόπιν εγγραφής. Οι κοινότητες περιεχομένου μπορεί να φιλοξενούν βίντεο (YouTube, Vimeo), φωτογραφίες (Pinterest, Picasa, Flickr), podcasts (iTunes), παρουσιάσεις (SlideShare).

Από τις πλέον δημοφιλείς κοινότητες αναδεικνύεται το YouTube, το οποίο αφενός έχει καταστεί μέσο επικοινωνίας για τους χρήστες-κατόχους λογαριασμών, αλλά και εργαλείο πληροφόρησης. Το γεγονός δε ότι οι χρήστες δεν είναι υποχρεωμένοι να δημιουργήσουν κάποιο προφίλ (Kaplan & Heinlein, 2010), διευκολύνει την αναζήτηση πληροφοριών με μια απλή αναζήτηση με λέξη-κλειδί για τον επιτελή πληροφοριών.

2.3.4. Ιστοσελίδες Κοινωνικής Δικτύωσης[6]

Μέσα από τις πλατφόρμες αυτές, ο χρήστης έχοντας δημιουργήσει ένα προσωπικό προφίλ, μπορεί να αλληλοεπιδρά μ' άλλους χρήστες ή να συμμετέχει σε ομάδες με κοινά ενδιαφέροντα. Το πιο δημοφιλές στη συγκεκριμένη κατηγορία είναι το Facebook (FB) με περισσότερους από 2,74 δισεκατομμύρια ενεργούς χρήστες μηνιαίως.[7]

2.3.5. Εικονικοί Κόσμοι (Virtual Worlds)

Οι Εικονικοί Κόσμοι είναι τρισδιάστατα περιβάλλοντα στα οποία πολλαπλοί χρήστες που εμφανίζονται ως avatars επικοινωνούν μεταξύ τους ή μ' άλλες ομάδες, εξερευνούν και αλληλοεπιδρούν με το περιβάλλον και κατασκευάζουν νέο περιεχόμενο, όπως θα έκαναν και στην πραγματική ζωή. Αποτελούν την πλέον διαδεδομένη υλοποίηση των θεωριών και τεχνικών της εικονικής πραγματικότητας με εφαρμογές στην εκπαίδευση, τον πολιτισμό, αλλά και σε παράνομες δραστηριότητες. Οι εφαρμογές των εικονικών κόσμων διαχωρίζονται σε δύο κύριες κατηγορίες σε α) παιχνίδια εικονικής πραγματικότητας (virtual games world) όπως το World of Warcraft και β) εικονικούς κοινωνικούς κόσμους όπως το Second Life.

Μολονότι εξ ορισμού φαίνεται να είναι «εικονικοί κόσμοι», ΥΠ ΗΠΑ και Βρετανίας σύμφωνα με διαβαθμισμένα έγγραφα που έχουν διαρρεύσει[8], παρακολουθούσαν τους

[6] Η αγγλική ορολογία περιλαμβάνει τους όρους "Social Networks Sites" και "Social Networking Service" με ακρωνύμιο και για τις δύο περιπτώσεις το "SNSs".

[7] Η εταιρεία διαθέτει επίσης τέσσερις από τις μεγαλύτερες πλατφόρμες κοινωνικών μέσων, όλες με πάνω από ένα δισεκατομμύριο μηνιαίους ενεργούς χρήστες: Facebook (βασική πλατφόρμα), WhatsApp, Facebook Messenger και Instagram. H. Tankovska, Most popular social networks worldwide as of January 2021, ranked by number of active users, *Statista*, 9 February 2021. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Ανάκτηση 11.03.2021).

[8] MHS and GCHQ "Get in the Game" with Target Development for World of Warcraft Online Gaming. https://www.documentcloud.org/documents/889134-games (Ανάκτηση 11.3.2021).

φανταστικούς κόσμους του World of Warcraft και SecondLife, συγκεντρώνοντας δεδομένα στα διαδικτυακά παιχνίδια που συμμετέχουν εκατομμύρια άνθρωποι απ' ολόκληρο τον κόσμο. Υπό το φόβο ότι τρομοκρατικά ή εγκληματικά δίκτυα μπορούν να χρησιμοποιούν παιχνίδια για επικοινωνία, μεταφορά χρημάτων ή σχεδιασμό επιθέσεων, οι ΥΠ έχουν παρεισφρήσει και στους εικονικούς κόσμους.

2.4. Κατηγοριοποίηση Χρηστών

Κατά καιρούς έχουν αναπτυχθεί ποικίλες προσεγγίσεις σχετικά με την τυπολογία των χρηστών, οι οποίες καταχωρίζουν επί παραδείγματι τη χρήση των ΜΚΔ για λόγους ψυχαγωγίας, κοινωνικοποίησης, πληροφόρησης, κ.ο.κ. Μια σχετική κατηγοριοποίηση αναφέρεται σε:

- **σποραδικούς χρήστες**,
- **«παρακολουθητές»** (lurker) οι οποίοι παρακολουθούν χωρίς συνεισφορά ή αλληλεπίδραση,
- **«κοινωνικοποιητές»**, άτομα που χρησιμοποιούν ΜΚΔ με στόχο την κοινωνική αλληλεπίδραση,
- **συζητητές (debaters)** και
- **προχωρημένους χρήστες** που χρησιμοποιούν ΜΚΔ για όλους τους παραπάνω λόγους δηλαδή συζήτησης, κοινωνικοποίησης, αλληλεπίδρασης (Brandtzæg and Heim, 2010).

Μολονότι στην τυποποίηση αυτή, υπάρχουν σημαντικές διαφορές, υπάρχει ένας βαθμός αλληλοεπικάλυψης, καθώς λ.χ. οι προχωρημένοι χρήστες μπορούν να συμμετέχουν σε δραστηριότητες που συμμετέχουν κοινωνικοποιητές και συζητητές. Μια άλλη τυποποίηση χρηστών διακρίνει τους χρήστες σε 6 κατηγορίες (Li et al., 2007), οι οποίες συνοπτικά περιλαμβάνουν:

- **δημιουργός** (creator) συμμετέχει ενεργά, δημοσιεύει περιεχόμενο, αναρτά υλικό πολυμέσων, συμμετέχει σε φόρουμ και συνήθως είναι νέοι,
- **κριτής** (critic) ανταποκρίνεται και αντιδρά σε περιεχόμενο άλλων χρηστών, σχολιάζοντας ή δημοσιεύει απόψεις του, συνήθως μεγαλύτερης ηλικίας από την προηγούμενη κατηγορία,
- **συλλέκτης** (collector) οργανώνει το περιεχόμενο που τον ενδιαφέρει με τη

χρήση RSS[9] ή σελιδοδεικτών (bookmarking),

- **joiner** συνδέεται στα ΜΚΔ και πρόκειται για τους νεότερους χρήστες απ' όλες τις κατηγορίες,
- **θεατής** (spectator), η πλέον διαδεδομένη κατηγορία χρηστών που διαβάζει blogs, απόψεις, συζητήσεις και σχόλια άλλων χρηστών ή επισκεπτών και τέλος
- **αδρανής - ανενεργός** χρήστης (inactivate), που δεν χρησιμοποιεί τα ΜΚΔ παρά μόνο το διαδίκτυο.

2.5. Κοινωνική Δικτύωση - Social Networking

Πολλές φορές οι όροι Social Media - Μέσα Κοινωνικής Δικτύωσης και Social Networking - Κοινωνική Δικτύωση χρησιμοποιούνται εκ περιτροπής, θεωρώντας ότι είναι εννοιολογικά ταυτόσημοι. Ωστόσο, υπάρχει μια σημαντική διαφοροποίηση καθώς ο όρος «μέσο κοινωνικής δικτύωσης» αναφέρεται στα μέσα-εργαλεία διαμοιρασμού πληροφορίας, δεδομένων και επικοινωνίας, ενώ ο όρος «κοινωνική δικτύωση» αναφέρεται σε δημιουργία και αξιοποίηση των κοινοτήτων για τη διασύνδεση ανθρώπων με κοινά ενδιαφέροντα, χρησιμοποιούνται δηλαδή κοινότητες κοινού ενδιαφέροντος για να συνδεθούν τα άτομα μεταξύ τους. Επί της ουσίας, ο όρος «μέσα κοινωνικής δικτύωσης» αναφέρεται στα εργαλεία ενημέρωσης,[10] ενώ ο όρος «κοινωνική δικτύωση» στη διαδικασία της δικτύωσης μέσω ηλεκτρονικών πλέον μέσων (διαδικτυακές εφαρμογές). Βέβαια τα κοινωνικά δίκτυα ως έννοια προϋπήρχαν του διαδικτύου, αλλά σήμερα αυτή η μορφή αλληλεπίδρασης λαμβάνει τη μορφή της μέσα από τα ΜΚΔ.

Στην περίπτωση αξιοποίησης της ανάλυσης της κοινωνικής δικτύωσης από τις ΥΠ, η ραγδαία εξάπλωση και χρήση των ΜΚΔ από χρήστες-στόχους έχει επιτρέψει τη μελέτη των δικτύων και της εσωτερικής τους δυναμικής σε πολύ μεγαλύτερη κλίμακα απ' ό,τι στο παρελθόν. Ως αποτέλεσμα οι αλληλεπιδράσεις μεταξύ των ατόμων που ενδιαφέρουν τις υπηρεσίες δύνανται να αποσαφηνιστούν και να μοντελοποιηθούν,

[9] Το RSS είναι format μεταφοράς δεδομένων στο διαδίκτυο, μέσω του οποίου ο χρήστης μπορεί να λαμβάνει νέες πληροφορίες από διάφορες ιστοσελίδες ενδιαφέροντος, τη στιγμή που δημοσιεύονται, χωρίς να χρειάζεται να τις επισκεφτεί.

[10] Τα κοινωνικά δίκτυα αναφέρονται ουσιαστικά στις κοινωνικές σχέσεις του ατόμου, στον τρόπο με τον οποίο αυτά αντιλαμβάνονται και αξιολογούν τις εν λόγω σχέσεις (Christakis, Fowler, 2009).

στοιχείο που συνιστά επικουρικό εργαλείο ανάλυσης για τον χειριστή. Στο πλαίσιο αυτό και με δεδομένο τη δημοφιλία των ΜΚΔ, ο όγκος δεδομένων προς εκμετάλλευση είναι τεράστιος. Η δυνατότητα αξιοποίησης των κοινωνικών δικτύων σε πολύ μεγαλύτερη κλίμακα από ό,τι στο παρελθόν, έχει δώσει νέα ώθηση αφενός στη διαδικασία αναζήτησης της πληροφορίας, αφετέρου στις πιθανές διασυνδέσεις μεταξύ των χρηστών, ακολούθων, ομάδων που συμμετέχουν.

Κεφάλαιο 3
Συλλογή Πληροφοριών Ανοικτών Πηγών

3.1. Open Source Intelligence - OSINT

Το Open-Source Intelligence (OSINT) αφορά την πληροφόρηση που δημοσιεύεται ή μεταδίδεται δημοσίως, προέρχεται από διαθέσιμες στο ευρύ κοινό πληροφορίες, δηλαδή ανοικτές πηγές, η συλλογή από τις οποίες είναι νόμιμη για κάθε απλό χρήστη ή αναλυτή στους τομείς α) επιχειρήσεων, β) αρχών επιβολής νόμου γ) κυβερνητικό δ) στρατιωτικό ε) εγκλήματος και στ) Υπηρεσιών Πληροφοριών. Στην περίπτωση των ΥΠ, το πληροφοριακό υλικό συλλέγεται συστηματικά, αξιοποιείται σε συνδυασμό με πληροφορίες άλλων πηγών και διακινείται έγκαιρα σε συγκεκριμένους αποδέκτες με σκοπό την κάλυψη πληροφοριακών αναγκών ή αιτημάτων. Επί της ουσίας συνεπικουρεί άλλες μορφές διαβαθμισμένης πληροφόρησης (Shulsky & Schmitt, 2002) που μπορεί να ενισχύσουν την αξιοπιστία της πηγής και να επιβεβαιώνουν την ακρίβεια της πληροφορίας.

Στην εποχή του διαδικτύου, το OSINT συνιστά πλέον τη βασικότερη πηγή πληροφοριών[11] καθώς η ροή πληροφόρησης είναι άμεση και προσβάσιμη, ενώ η σημασία της πληροφορίας δεν περιορίζεται μόνο σ' αυτό καθ' αυτό το γεγονός στο οποίο αναφέρεται, αλλά και σε μεταδεδομένα αλληλεπίδρασης που προκύπτουν

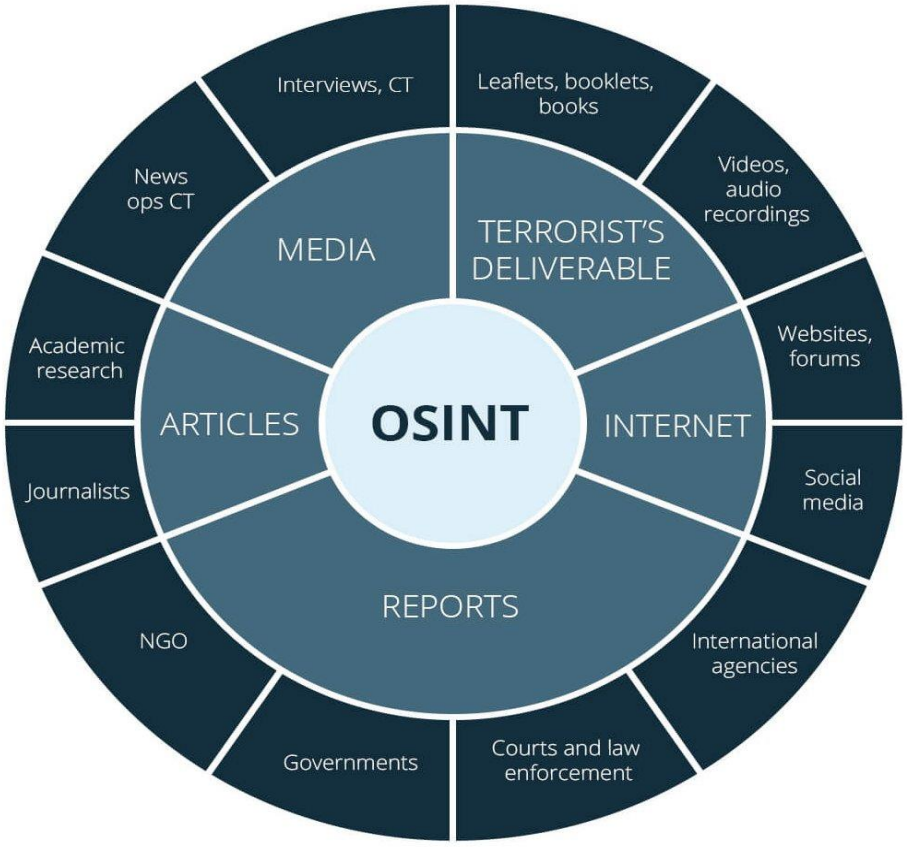
[11] Classification of Intelligence Information, https://fas.org/sgp/library/quist2/app_e.html ανακτήθηκε 24/01/2021.

μεταξύ των χρηστών αναφορικά με το γεγονός, στοιχεία αξιοποιήσιμα όσον αφορά τη δικτύωση χρηστών ενδιαφέροντος, ειδικά στην ανάλυση δεδομένων από λογαριασμούς δημόσιους ή και ιδιωτικούς.

Η διαφοροποίηση του OSINT σε σχέση με τις άλλες πηγές πληροφόρησης έγκειται στο γεγονός ότι οι πληροφορίες είναι δημόσιες χωρίς να παραβιάζονται νόμοι περί πνευματικών ή άλλων συγγενών δικαιωμάτων. Ως εκ τούτου, το OSINT ως διαδικασία «ανοικτή» σπανίως τελεί υπό τον έλεγχο και την αδειοδότηση χρήσης τους από τις αρμόδιες αρχές, σε αντίθεση με τις άλλες πηγές πληροφόρησης που εξ ορισμού είναι κεκαλυμμένης μορφής και επομένως απόρρητες (classified) όπως το HUMINT, SIGINT, κ.ά. Σε κάθε περίπτωση οι πληροφορίες που δημοσιεύονται πέραν από το πληροφοριακό και ενημερωτικό ενδιαφέρον, δύνανται να εξυπηρετούν σκοπιμότητες μονάδων, οργανώσεων ή και υπηρεσιών κρατών και μπορεί να σχετίζονται με διάδοση ψευδών ειδήσεων, θεωριών συνωμοσίας, προπαγάνδα, κ.ο.κ., με αποτέλεσμα να συνιστούν αντικείμενο έγκαιρου εντοπισμού, λεπτομερούς διερεύνησης και περαιτέρω διαχείρισης από τον επιτελή πληροφοριών. Στα ζητήματα – προκλήσεις που αναφέρονται ανωτέρω θα γίνει εκτενής αναφορά στη συνέχεια.

Στον πίνακα που ακολουθεί (Πίνακας 1) περιλαμβάνονται ενδεικτικά τα κύρια μέσα διάδοσης πληροφοριών δημοσίως διαθέσιμα, που συνιστούν τις κύριες ανοικτές πηγές πληροφόρησης οι οποίες μπορεί να είναι φυσικά πρόσωπα, κυβερνήσεις, διεθνείς οργανισμοί και οργανώσεις, ΜΜΕ, ιστοσελίδες, μέλη επιστημονικής κοινότητας, ΜΚΔ ή ακόμη και παράνομες οργανώσεις.

Πίνακας 1 OSINT: Μέσα και Φορείς Διάδοσης Πληροφοριών[12]



3.2. Ο Κύκλος της Πληροφορίας

Οι επιτελείς πληροφοριών που επεξεργάζονται υλικό προερχόμενο από ανοικτές πηγές (OSINT) δίνουν ιδιαίτερη προσοχή στο χρονοδιάγραμμα εμφάνισης πληροφοριών στα Μέσα Μαζικής Ενημέρωσης (ΜΜΕ), καθώς οι πληροφορίες αυτές εντάσσονται σε έναν ευρύτερο κύκλο ειδήσεων. Στη θεωρία των ΜΜΕ ο κύκλος ειδήσεων αναφέρεται στη διαδικασία και το χρόνο κατά τον οποίο αρθρογράφοι (ΜΜΕ) ή άλλοι χρήστες (ΜΚΔ) λαμβάνουν πληροφορίες, τις ενσωματώνουν ή τις μετατρέπουν σ' ένα άρθρο ή ανάρτηση που δημοσιοποιείται στο κοινό. Επί της ουσίας δηλαδή σχετίζεται με τη διαδικασία κάλυψης ενός γεγονότος από τα ΜΜΕ.

[12] https://www.7wdata.be/apache-hadoop/graph-based-intelligence-analysis/ (Ανάκτηση 24.01.2021).

Πίνακας 2 Κύκλος Πληροφορίας[13]

ΚΥΚΛΟΣ ΠΛΗΡΟΦΟΡΙΑΣ – ΜΜΕ				
ΧΡΟΝΙΚΗ ΑΚΟΛΟΥΘΙΑ ΚΑΛΥΨΗΣ ΓΕΓΟΝΟΤΟΣ	**ΗΜΕΡΑ ΔΗΜΟΣΙΕΥΣΗΣ**	**ΕΠΟΜΕΝΗ ΗΜΕΡΑ**	**ΕΠΟΜΕΝΗ ΕΒΔΟΜΑΔΑ**	**ΜΗΝΕΣ/ΕΤΗ ΜΕΤΑ**
Συντάκτης (Χρήστης – ΜΚΔ, Δημοσιογράφος)	ΜΚΔ (TW, FB) Ηλεκτρονικά ΜΜΕ (web)	ΜΚΔ, Έντυπα ΜΜΕ - εφημερίδες	Περιοδικά Ειδικής Ύλης/Εβδομαδιαίες Εφημερίδες, Ινστιτούτα, Δεξαμενές Σκέψεις, ΜΚΟ	Περιοδικά, Κυβερνητικές Εκδόσεις, Πανεπιστημιακά Ιδρύματα, Εκθέσεις
Περιεχόμενο	Βασική Καταγραφή Γεγονότος	Απόψεις, Συνεντεύξεις, Βασική Ανάλυση	Εκτενής Καταγραφή, Αναλύσεις, Επιπλέον Στοιχεία, Συνεντεύξεις	Προϊόν Ακαδημαϊκής ή Δημοσιογραφικής Έρευνας, Βιβλιογραφικές Αναφορές
Αποδέκτης	Κοινό	Κοινό	Ειδικές ομάδες Ακαδημαϊκοί, Εμπειρογνώμονες, Ερευνητές	Ευρύ Κοινό που μπορεί να περιλαμβάνει έναν απλό αναγνώστη ή επιστήμονα

Στο χώρο των ΥΠ, ο επιτελής πληροφοριών ασχολείται σε (α) πρώτο στάδιο με τον Κύκλο Πληροφοριών (Information Cycle) των ΜΜΕ (Πίνακας 2), προκειμένου να εξάγει

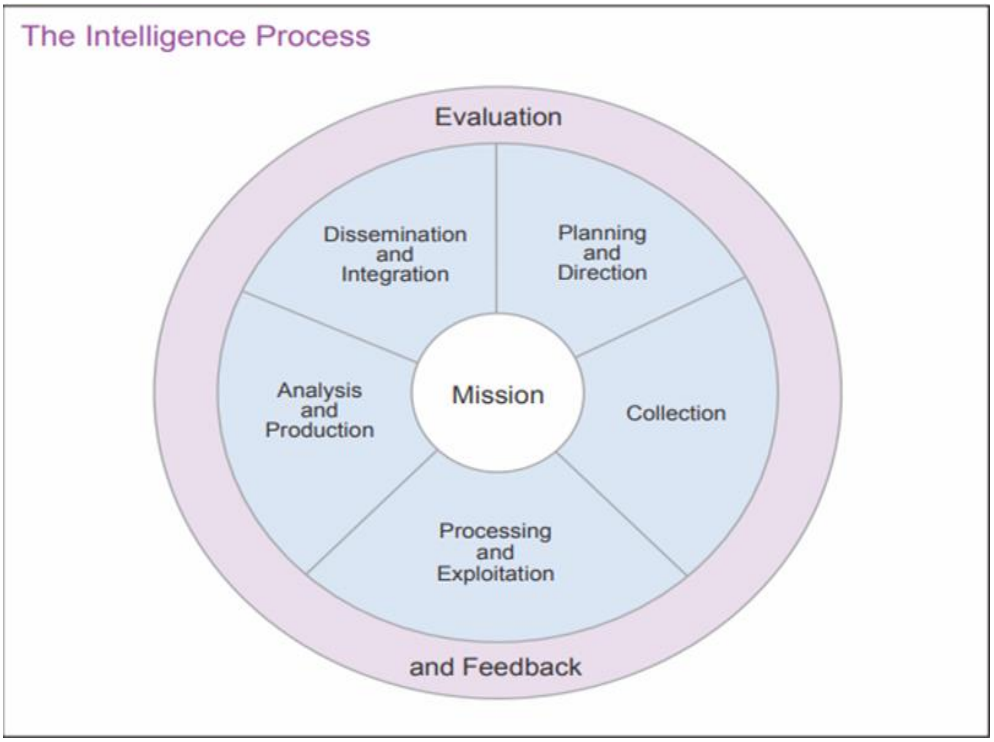
[13] https://www.library.illinois.edu/ugl/howdoi/informationcycle/#Text%20Information%20Cycle (Ανάκτηση 12.01.2021).

συμπεράσματα για την ακρίβεια πληροφορίας και αξιοπιστία πηγής και σε (β) στάδιο μετέχει του Κύκλου Πληροφοριών (Intelligence / Information Cycle) (Πίνακας 3) που αφορά στη διαδικασία εντοπισμού, αξιολόγησης, σύνταξης και κοινοποίησης του τελικού προϊόντος.

Το Intelligence Cycle ή Intelligence Process συνίσταται από πέντε ή περισσότερες αλληλένδετες κατηγορίες επιχειρησιακών δράσεων που αναλαμβάνει ο χειριστής πληροφοριών. Η διαδικασία αυτή διαχωρίζεται στα εξής βήματα: α) σχεδιασμού και καθορισμού πληροφοριακής ανάγκης β) συλλογής υλικού γ) επεξεργασίας δεδομένων και δ) ανάλυσης και διάδοσης του τελικού πληροφοριακού προϊόντος στους αρμόδιους φορείς προς ενέργεια. Στην απεικόνιση του κύκλου που ακολουθεί (Πίνακας 3), επί παραδείγματι για τις ΥΠ των ΗΠΑ η διαδικασία αποτελείται από πέντε βήματα, χωρίς ωστόσο να αποκλείονται περισσότερα στάδια απ' άλλες υπηρεσίες χωρών, επί της ουσίας όμως η διαδικασία παραμένει σε μεγάλο βαθμό η ίδια.

Επίσης, πολλά στάδια στον κύκλο πληροφοριών μπορεί να συμπίπτουν χρονικά ή και να παρακάμπτονται, όπως επί παραδείγματι όταν υπάρχουν συγκεχυμένες πληροφορίες οι οποίες μπορεί να διακινηθούν στον επιτελή χωρίς να έχουν διασταυρωθεί προκειμένου να χρησιμοποιηθούν επικουρικά στην επεξεργασία ενός άλλου στοιχείου. Η παράκαμψη σταδίων συνήθως συμβαίνει σε πληροφορίες, η άμεση αξιοποίηση των οποίων είναι κρίσιμη, όπως σε περιπτώσεις εξάρθρωσης παράνομων κυκλωμάτων ή στρατιωτικές συρράξεις, όπου η λεπτομερής ανάλυση και επαλήθευση δεν αποκλείεται να έπεται της ενημέρωσης της ιεραρχίας. Μάλιστα σε αυτές τις περιπτώσεις, οι πληροφορίες ανάλογα με τη διαβάθμισή τους, μπορεί να είναι ταυτόχρονα διαθέσιμες στην ιεραρχία μιας υπηρεσίας και σε αναλυτές επιτελείς.

Πίνακας 3 Intelligence Process/Cycle – Κύκλος Πληροφορίας



Πηγή: https://web.archive.org/web/20160613010839/http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Σε ό,τι αφορά την εφαρμογή του κύκλου πληροφοριών από ΜΚΔ ισχύει ό,τι και στις υπόλοιπες πηγές. Μερικές ίσως ποιοτικές διαφορές που θα μπορούσαν να επισημανθούν είναι η ενημέρωση σε πραγματικό χρόνο δηλαδή γεγονότων που δημοσιοποιούνται εν τη γενέσει τους. Επίσης σ' ό,τι αφορά την εξόρυξη δεδομένων από τα ΜΚΔ (στάδιο συλλογής), πολλές φορές ο επιτελής χρειάζεται τη συνδρομή εξειδικευμένων στελεχών της πληροφορικής προκειμένου να έχει πρόσβαση σε δεδομένα που δεν μπορούν να προκύψουν από μια απλή προσπέλαση του λογαριασμού-στόχου. Το ίδιο ισχύει και για το στάδιο της επεξεργασίας, όπου επί παραδείγματι μπορεί να χρειάζεται καταγραφή ή οπτικοποίηση των ατόμων-στόχων και των επαφών-σχέσεις τους με χρήση σχετικών λογισμικών. Στο σημείο αυτό κρίνεται σκόπιμο να διευκρινιστεί ότι το αντικείμενο της παρούσας μελέτης δίνει έμφαση στην ανάλυση πληροφοριών από τα ΜΚΔ (SOCMINT), αλλά δεν εμβαθύνει στην επιστήμη της ανάλυσης δεδομένων ή κοινωνικών δικτύων, η οποία αφορά στη θεωρία δικτύων που μετρά και απεικονίζει τους χρήστες (ως κόμβους) και τις σχέσεις-αλληλεπιδράσεις

τους (ως ακμές).[14] Αναλυτικότερα και ανά στάδιο διαδικασίας, θα μπορούσαν να καταγραφούν τα ακόλουθα:

3.2.1. Σχεδιασμός

Στο στάδιο του σχεδιασμού, ουσιαστικά αποσαφηνίζονται οι πληροφοριακές ανάγκες, τα διαθέσιμα μέσα συλλογής πληροφοριών και οι πιθανές εναλλακτικές σε περίπτωση που το αντικείμενο διερεύνησης έχει δυναμικά χαρακτηριστικά, δηλαδή η κατάσταση του στόχου μπορεί να αλλάξει. Είθισται το βήμα αυτό να μην παρακάμπτεται, καθώς στην αντίθετη περίπτωση δύναται να προκύψουν ζητήματα όπως παρατεταμένη διάρκεια αναζήτησης πληροφοριών, μη διαθέσιμοι πόροι (ανθρώπινοι και τεχνικοί). Στην περίπτωση των ΜΚΔ που εξετάζονται, μια ενδεικτική λίστα ερωτήσεων που υποβοηθούν τον αρχικό σχεδιασμό της πληροφοριακής ανάγκης μπορεί να περιλαμβάνει:

- ποιος προβάλλεται **ως κάτοχος** του συγκεκριμένου λογαριασμού,
- ποια **ονόματα** χρησιμοποιεί ή έχει χρησιμοποιήσει κατά το παρελθόν στα ΜΚΔ,
- σε ποια **χώρα** εμφανίζεται να δραστηριοποιείται,
- ποια είναι η **ηλικία** του κατά προσέγγιση,
- ποια **άλλα ΜΚΔ** χρησιμοποιεί (λ.χ. βάσει στοιχείων τηλεφώνου ή email).

Στην περίπτωση συλλογής πληροφοριών από ΜΚΔ, ο επιτελής χρειάζεται να έχει λογαριασμό για να αποκτήσει πρόσβαση σε λογαριασμούς στόχων ή ομάδων, ενώ στην περίπτωση ιδιωτικών λογαριασμών ή αυξημένων τεχνολογικών δεξιοτήτων χρήστη-στόχου απαιτείται μεγαλύτερη προετοιμασία. Στο στάδιο του σχεδιασμού, συνήθως ορίζεται και το αναμενόμενο προϊόν της έρευνας, δηλαδή εάν θα συνταχθεί κάποια αναφορά εσωτερικής χρήσης ή πρόκειται για ενημερωτικό έγγραφο που θα κοινοποιηθεί σε αρμόδιες αρχές με επιπλέον στοιχεία από άλλες πηγές.

[14] Βάσει της Θεωρίας Δικτύων τα ΜΚΔ συνιστούν μια δομή που αποτελείται από κόμβους και συνδέσεις, όπου κάθε κόμβος αντιπροσωπεύει ένα άτομο ή μια ομάδα, ενώ οι συνδέσεις αναπαριστούν τις σχέσεις μεταξύ των ατόμων. Οι κόμβοι που είναι συνδεδεμένοι αποτελούν τις κοινωνικές επαφές του. Σε πολλές περιπτώσεις που εξετάζονται λογαριασμοί-στόχων, επιτελείς πληροφορικής καλούνται να καταγράψουν ή να οπτικοποιήσουν με γραφήματα το άτομο, τις επαφές του, τυχόν επικοινωνίες και μεταξύ τους αλληλεπιδράσεις. Βάσει των δεδομένων που προκύπτουν και ανάλογα με τα εργαλεία – λογισμικά ανάλυσης κοινωνικών δικτύων που θα χρησιμοποιηθούν, παρέχονται δυνατότητες για κατηγοριοποίηση, ταξινόμηση, ομαδοποίηση των ατόμων (κόμβων) και των σχέσεων (ακμών) ενός γραφήματος μέσω χρωματικών διαβαθμίσεων ή και μεταβολής της κλίμακάς τους κ.ά.

3.2.2. Συλλογή

Στο στάδιο συλλογής, ο επιτελής έχει προσπελάσει όλες εκείνες τις πηγές πληροφοριών και έχει συγκρατήσει στοιχεία ενδιαφέροντος που σχετίζονται με την έρευνά του. Διευρύνοντας την αναζήτηση στο ευρύ φάσμα των διαθέσιμων πληροφοριών από τις πλατφόρμες ΜΚΔ, ο επιτελής αφενός μειώνει τις πιθανότητες να προκύψουν ελλείψεις στις επόμενες φάσεις, αφετέρου εξασφαλίζει ότι στο τελικό προϊόν έχουν συμπεριληφθεί όλες οι σχετικές με την έρευνα διαθέσιμες πληροφορίες.

Εξαιτίας του όγκου δεδομένων από την επεξεργασία πληροφοριών στα ΜΚΔ και της σημασίας του χρόνου όπου οι πληροφορίες δημοσιεύονται, ο επιτελής τις καταγράφει χωρίς να τις επεξεργάζεται περαιτέρω. Πολλές φορές περιεχόμενο από αναρτήσεις χρηστών-στόχων αναρτάται και μπορεί να αφαιρεθεί εκ των υστέρων ή και να τροποποιηθεί από τον ίδιο όταν κριθεί απαραίτητο. Επίσης, το στάδιο της συλλογής μπορεί να επαναλαμβάνεται καθ’ όλη τη διαδικασία του πληροφοριακού κύκλου καθώς προκύπτουν νέα ερωτήματα που χρήζουν απαντήσεων. Η πληροφοριακή επίσης ροή σε συμβάντα που είναι υπό εξέλιξη, καθιστούν τη συλλογή δεδομένων συνεχή προκειμένου το υλικό που προκύπτει να είναι έγκυρο για το επόμενο στάδιο της επεξεργασίας.

3.2.3. Επεξεργασία

Στο στάδιο της επεξεργασίας η ακατέργαστη πληροφορία που έχει συλλεχθεί, διαμορφώνεται στη συνέχεια προκειμένου να καταστεί κατάλληλη στο στάδιο της ανάλυσης. Όταν γίνεται αναφορά σε επεξεργασία της πληροφορίας, αυτή μπορεί να συνίσταται σε μετάφραση στη γλώσσα του επιτελή, σε ταξινόμηση με συναφείς πληροφορίες, σε απομαγνητοφώνηση ή μετατροπή των δεδομένων σε μορφή πληροφοριών που μπορεί να επεξεργαστούν από τον αναλυτή.

Στην περίπτωση των πληροφοριών από ΜΚΔ, οι πληροφορίες μπορεί να έχουν περιεχόμενο οπτικο-ακουστικό (λ.χ. βίντεο, εικόνα, podcast) το οποίο πρέπει να μεταφραστεί, να απομαγνητοφωνηθεί ή να περιγραφεί λεπτομερώς ή και να μεταγραφεί. Σε αρκετές περιπτώσεις για τη μετάφραση της πληροφορίας από γλώσσες

ενδιαφέροντος από ΥΠ (αραβικά, περσικά, τουρκικά, ρωσικά, κινεζικά, κ.ά.), μπορεί να μεσολαβεί μεταφραστής, ωστόσο με τα προηγμένα εργαλεία αυτοματοποιημένων μεταφράσεων πολλές φορές ο επιτελής που συλλέγει πληροφορίες από τα ΜΚΔ είναι και ο αναλυτής της πληροφορίας.

Μια σημαντική συνιστώσα κατά την επεξεργασία των πληροφοριών είναι το χρονικό πλαίσιο κατά το οποίο ο επιτελής μπορεί να παρακολουθεί αλληλένδετα με την πληροφορία γεγονότα και βάσει αυτών να αποκτήσει μια πιο συνολική εικόνα για μια δραστηριότητα ή ένα γεγονός. Δεν αποκλείεται δε κατά το στάδιο της επεξεργασίας να προκύψουν συναφείς προς το συμβάν πληροφορίες, οι οποίες μπορεί να μην είχαν αρχικά συμπεριληφθεί στο στάδιο της συλλογής. Στο στάδιο της επεξεργασίας οι ακατέργαστες πληροφορίες φιλτράρονται προκειμένου να συρρικνωθεί ο μεγάλος όγκος δεδομένων για να καταστεί ένα αξιοποιήσιμο προϊόν πληροφοριών.

3.2.4. Ανάλυση

Στο στάδιο της ανάλυσης ο επιτελής καλείται να συνθέσει τα επεξεργασμένα δεδομένα πληροφορίες και να συμπυκνώσει το περιεχόμενο τους. Η ανάλυση των δεδομένων μπορεί να έχει τη μορφή αναφοράς, εσωτερικής ενημέρωσης και εξαρτάται κυρίως από την ιδιότητα του αποδέκτη. Ως επί το πλείστον οι αναλύσεις με αποδέκτες σε εθνικό επίπεδο, είναι πιο αναλυτικές και εξαντλούν όλες τις παραμέτρους που μπορεί να απασχολούν τις αρμόδιες αρχές. Στο πλαίσιο αυτό, η ανάλυση των πληροφοριών δύναται να συμπεριλαμβάνει συστάσεις ή να θέτει ζητήματα για περαιτέρω διερεύνηση. Η τελική μορφοποίηση ενός πληροφοριακού προϊόντος εξαρτάται από τις κατευθυντήριες οδηγίες και το σχεδιασμό που έχουν προηγηθεί.

Δεδομένου ότι ο εντοπισμός πληροφοριών από τα ΜΚΔ μπορεί να αποφέρει στον επιτελή ένα χαοτικό όγκο δεδομένων, το πρώτο στάδιο του σχεδιασμού είναι αυτό που έχει προκαθορίσει το πλαίσιο ανάλυσης και τα υπό διερεύνηση σημεία. Στο στάδιο αυτό ο αναλυτής οφείλει να συνθέσει και να παρουσιάσει τις πληροφορίες εκείνες που διαμορφώνουν μια εικόνα και προσδίδουν προστιθέμενη αξία στη διαδικασία λήψης αποφάσεων από τους αρμοδίους. Σε ό,τι αφορά πληροφορίες ΜΚΔ σημειώνεται ότι το περιεχόμενο και η σημασία τους μπορούν να διακινηθεί στην ιεραρχία για ενημέρωση, ωστόσο δεν είναι απαραίτητο ο «κύκλος της πληροφορίας» να ολοκληρωθεί καθώς τα

στοιχεία μπορεί να κριθούν ανεπαρκή και ως εκ τούτου να αρχειοθετηθούν για μελλοντική χρήση.

3.3. Social Media Intelligence - SOCMINT

Μετά τις ταραχές του 2011 στο Λονδίνο, ο Sir David Omand, πρώην διευθυντής στο Government Communications Headquarters του Ηνωμένου Βασιλείου, όρισε ένα νέο τομέα ο οποίος αποτελείται από ένα σύνολο εφαρμογών, τεχνικών και δυνατοτήτων που αποκτήθηκαν μέσω της συλλογής και χρήσης των ΜΚΔ (Omand, 2012). Μολονότι συνιστά υποκατηγορία του OSINT, διαφέρει ως προς τις πηγές πληροφόρησης καθώς αυτές προέρχονται αποκλειστικά από τα ΜΚΔ, ενώ του OSINT εντοπίζονται στα παραδοσιακά μέσα πληροφόρησης (εφημερίδες, ραδιόφωνο, τηλεόραση, κλπ.), δημόσια δεδομένα (εκθέσεις, επίσημα δεδομένα), καθώς και το διαδίκτυο.

Βέβαια, αρκετοί ερευνητές σημειώνουν ότι η κατηγοριοποίηση του SOCMINT ως υποκατηγορία του OSINT δεν είναι απόλυτα ευσταθής, καθώς οι πληροφορίες δεν είναι απαραίτητα δημόσιες, αλλά μπορούν να αλιευθούν και μέσα από κλειστούς, ιδιωτικούς λογαριασμούς. Όπως επισημαίνεται το SOCMINT δεν καθορίζεται τόσο από τη δημόσια πληροφορία που προσφέρει, αλλά κυρίως στο ό,τι η δημιουργία του ως νέα πηγή πληροφόρησης οφείλεται στα ΜΚΔ. Σε κάθε περίπτωση, ανεξάρτητα με το είδος του λογαριασμού (ιδιωτικός/δημόσιος), το SOCMINT απαιτεί πολύ συγκεκριμένους χειρισμούς όσον αφορά την εκτίμηση της εγκυρότητας και της ερμηνείας των πληροφοριών που προσφέρει (Bartlett & Reynolds, 2015).

Το SOCMINT ορίζεται ως η αναλυτική διαδικασία αναγνώρισης, συλλογής, επεξεργασίας και ανάλυσης δεδομένων, τα οποία αντλούνται από δημόσιους και ιδιωτικούς λογαριασμούς (ατόμων, ομάδων, οργανισμών, οργανώσεων) σε πλατφόρμες ΜΚΔ, η αξιοποίηση των οποίων περιορίζει τις συνθήκες αβεβαιότητας και συμβάλλει στη διαδικασία λήψης αποφάσεων. Οι πληροφορίες αυτές μπορεί να αφορούν προσωπικά δεδομένα, πληροφορίες που προέρχονται και απευθύνονται από χρήστη σ' άλλο χρήστη, από χρήστη σ' ομάδα και από ομάδα σ' ομάδα και περιλαμβάνουν τις αλληλεπιδράσεις των χρηστών μεταξύ τους είτε αυτές γίνονται δημόσια, είτε ιδιωτικά. Οι πληροφορίες αυτές διακρίνονται σε:

- **Αρχικά δημοσιευμένο περιεχόμενο** που αναρτά ο χρήστης για πρώτη φορά, λ.χ.

μια ανάρτηση κειμένου, μια φωτογραφία, ή ένα βίντεο και τα

- **Μεταδεδομένα**, που σχετίζονται με το αρχικό περιεχόμενο και μπορεί να αφορούν ημερομηνία, ώρα, γεωγραφική τοποθεσία.

Στην περίπτωση του SOCMINT ο επιτελής μπορεί να έχει πρόσβαση σε ΜΚΔ:

- **Ως μη χρήστης**, χρησιμοποιώντας ένα πρόγραμμα περιήγησης για αναζήτηση περιεχομένου χωρίς σύνδεση σε ΜΚΔ,
- **Ως χρήστης με ψεύτικο προφίλ**, ακολουθώντας λ.χ. το @fahrettinaltun[15]
- **Ως παράλληλα συνδεδεμένος τρίτος χρήστης** στη συσκευή του χρήστη, ώστε να παρακολουθεί διεξαγόμενες επικοινωνίες και να λαμβάνει περιεχόμενο και τα στοιχεία αυτής σε πραγματικό χρόνο, διαδεδομένη πρακτική ως «επισύνδεση»,
- **Ως αιτών για άρση απορρήτου επικοινωνιών** προς την αρμόδια αρχή και σε συνεργασία με τον πάροχο υπηρεσιών επικοινωνιών και εξαιρετικά σπάνια
- **Ως επικυρωμένος χρήστης** λ.χ. @ChiefMI6 ακολουθεί @frkkymkc.[16]

Οι πληροφορίες στα ΜΚΔ συνιστούν ένα επιπλέον πεδίο έρευνας – αναζήτησης για τον επιτελή, ο οποίος καλείται να εντοπίσει και να αξιολογήσει πληροφορίες[17] από λογαριασμούς χρηστών ενδιαφέροντος. Για την εξόρυξη πληροφοριών από ένα τεράστιο όγκο δεδομένων, μπορεί να χρησιμοποιηθούν εργαλεία και τεχνικές, που δύναται να συμπεριλαμβάνουν από μια συστηματική παρακολούθηση συγκεκριμένου χρήστη χωρίς τη χρήση ειδικών εφαρμογών, μέχρι μεθόδους ανάλυσης κειμένου (text analysis) και λογισμικό για συλλογή δεδομένων από τα ΜΚΔ. Η επεξεργασία των δεδομένων μπορεί να υπόκειται σε περιορισμούς από την κείμενη νομοθεσία, ωστόσο είναι εφικτή υπό όρους και προϋποθέσεις από τις αρμόδιες και εξουσιοδοτημένες αρχές και υπό την διαρκή εποπτεία και τον έλεγχο των δικαστικών αρχών και τη συνδρομή των εταιριών των ΜΚΔ.

[15] Fahrettin Altun, Διευθυντή Επικοινωνίας της Τουρκικής Προεδρίας.

[16] Ο επικεφαλής της SIS ή αλλιώς MI6, Richard Moore ακολουθεί στο Twitter τον Faruk Kaymakcı @frkkymkc, Αναπληρωτή ΥΠΕΞ και Διευθυντή Ευρωπαϊκών Υποθέσεων του τ/ΥΠΕΞ.

[17] Οι πληροφορίες που συνήθως φιλοξενούνται στα προσωπικά προφίλ των χρηστών και μπορούν να αξιοποιηθούν αφορούν ημερομηνία γέννησης, αποφοίτησης, σχέσης, έναρξης ή διακοπής εργασίας, πολιτικές απόψεις, θρησκεία, εθνικότητα, χώρα προέλευσης, χώρα και διευθύνσεις διαμονής και εργασίας, προσωπικές εικόνες και βίντεο, οικογενειακή κατάσταση, κοινωνικές δραστηριότητες, τοποθεσίες όπου ο χρήστης επισκέπτεται, κοινωνικές αλληλεπιδράσεις, κ.ο.κ.

3.3.1. Τρόποι Συλλογής SOCMINT

Οι τρόποι συλλογής στο SOCMINT ποικίλουν και κυμαίνονται από καθαρά τεχνικές μεθόδους έως αρκετά γενικές προσεγγίσεις, στις οποίες κατά Bartlett & Reynolds (2015) συμπεριλαμβάνονται οι ακόλουθες:

- **Επεξεργασία φυσικής γλώσσας** (Natural Language Processing – NLP). Συνιστά κλάδο της Τεχνητής Νοημοσύνης και περιλαμβάνει την υπολογιστική ανάλυση και sentiment analysis χρησιμοποιώντας συχνά μεθόδους μηχανικής μάθησης ή «φυσική» γλώσσα όπως απαντά στα ΜΚΔ.
- **Ανίχνευση συμβάντων** (Event Detection). Η διερεύνηση με στατιστικούς δείκτες των ροών στα ΜΚΔ, όπου καταδεικνύουν offline γεγονότα, όπως πολιτικά, φυσικά ή και έκτακτης ανάγκης, με σκοπό την παροχή στοιχείων σε ραγδαίες εξελίξεις με δυναμικά χαρακτηριστικά. Στον τομέα της αντιτρομοκρατίας, αυτό είναι ιδιαίτερα σημαντικό μετά από ένα τρομοκρατικό συμβάν.
- **Εξόρυξη Δεδομένων και Προγνωστική ανάλυση** (Data Mining & Predictive Analytics). Η στατιστική ανάλυση της εξόρυξης μεγάλων δεδομένων (Big Data) όπως των ΜΚΔ γίνεται μέσω Διεπαφής Προγραμματισμού Εφαρμογών (Application Programming Interface - API) με σκοπό τον εντοπισμό αλληλεπιδράσεων, κυκλωμάτων ανατροφοδότησης (feedback loops) και των αιτιωδών σχέσεων μεταξύ τους.
- **Ανάλυση κοινωνικού δικτύου** (Social Network Analysis). Η εφαρμογή μιας σειράς μαθηματικών τεχνικών προκειμένου να βρεθεί η δομή του δικτύου των χρηστών στα ΜΚΔ που χρησιμοποιούν. Αυτά τα δίκτυα αναλύονται και εξάγονται συμπεράσματα και προβλέψεις βάσει των χαρακτηριστικών της δομής και του τύπου του δικτύου.
- **Δια χειρός ανάλυση / "netnography**" (Manual analysis/netnography). Προκύπτει από την ποιοτική κοινωνιολογία και εθνογραφία, συνίσταται από πολυάριθμες προσεγγίσεις συλλογής και ανάλυσης δεδομένων από τα ΜΚΔ. Στοχεύει στην ανάδειξη συγκεκαλλυμένων σημείων ή ενδείξεων από την εμπειρία των χρηστών στα ΜΚΔ.

3.3.2. Τυπολογία Πληροφοριών σε ΜΚΔ

Η διευρυμένη χρήση των ΜΚΔ κατέστησε αναγκαία την εποπτεία των ΜΚΔ ως μέσο συλλογής πληροφοριών για τις ΥΠ. Τα δεδομένα αυτά διαμορφώνουν μια ροή πληροφόρησης στους αναλυτές, που διαμορφώνεται σ' ένα δυναμικό πληροφοριακό περιβάλλον από:

- **Δημοσίευση - σχόλιο**: Οι χρήστες με πρόσβαση σε ΜΚΔ αναρτούν δημοσιεύσεις ή σχόλια που μπορούν να δουν άλλοι χρήστες.
- **Απάντηση**: Συνιστά μήνυμα κειμένου, μπορεί να έχει μορφή εικόνας, βίντεο που απαντά σε ανάρτηση, κατάσταση ενημέρωσης ή σχόλιο άλλου χρήστη.
- **Οπτικοακουστικό υλικό**: Βίντεο ή φωτογραφίες που αναρτώνται από τον χρήστη.
- **Κοινωνικές αλληλεπιδράσεις** και
- **Μεταδεδομένα**: Τα αποτελέσματα από το άθροισμα των αλληλεπιδράσεων χρηστών με την πλατφόρμα, όπως ημερομηνίες ανταλλαγής μηνυμάτων, ιστορικό αιτημάτων φιλίας, δεδομένα γεωγραφικής τοποθεσίας, κλπ.

3.3.3. Περιεχόμενο Πληροφοριών σε ΜΚΔ για τις Υπηρεσίες

Τα μεγάλα δεδομένα (Big Data) συνδέονται με το SOCMINT, δηλαδή με συλλογή και επεξεργασία-ανάλυση δεδομένων. Στο πλαίσιο αυτό η επεξεργασία των δεδομένων αντιπροσωπεύει επίσης μια αλλαγή στην ανάλυση πληροφοριών (Schönberger and Cukier, 2014), οι οποίες παράγονται συνεχώς και αποκτούν νόημα μόνο όταν παρουσιάζονται ως ένα ουσιαστικό σύνολο στην κατανόησή τους. Με την κοινωνική εξέλιξη και την υιοθέτηση νέων μεθόδων επικοινωνίας, οι ΥΠ προσαρμόζονται προκειμένου να λειτουργούν αποτελεσματικά σ' έναν επιχειρησιακό σχεδιασμό ή στην αντιμετώπιση μιας κρίσης. Επιχειρώντας μια θεματική ταξινόμηση των πεδίων έρευνας που απασχολούν τους αρμόδιους φορείς, αυτές θα μπορούσαν να καταγραφούν ως ακολούθως:

3.3.3.1. Πολιτικό-οικονομικές εξελίξεις

Η εικόνα με στοίβες εφημερίδων και ανοικτούς τηλεοπτικούς δέκτες στις διευθύνσεις συλλογής πληροφοριών από ανοικτές πηγές πλέον ανήκει στο μακρινό παρελθόν. Οι

δημοσιογράφοι δεν είναι οι μόνοι που κομίζουν την πληροφορία στη δημόσια σφαίρα. Οι ψηφιακές πλατφόρμες διευρύνουν το πληροφοριακό πανόραμα, καθώς πληροφορίες μπορούν να διοχετεύσουν και οι απλοί χρήστες, μέχρι πολιτικά πρόσωπα, δημοσιογράφοι, διπλωμάτες, θεσμικοί παράγοντες, ακόμη και troll με αποτέλεσμα το πλαίσιο να διευρύνεται, αλλά και να αποκεντρώνεται παράλληλα. Αυτό έχει ως αποτέλεσμα αφενός να εξασφαλίζεται μια πληθώρα πληροφοριών για τις ΥΠ, ωστόσο η πρόκληση για τον επιτελή πληροφοριών είναι να εντοπίσει ανάμεσα στον όγκο πληροφοριών, εκείνες τις πληροφορίες που συνθέτουν τη μεγαλύτερη εικόνα ανεξάρτητα από το εάν η πηγή είναι εγνωσμένου κύρους ή ένας απλός χρήστης που έτυχε να έχει πρόσβαση σε μια πληροφορία.[18]

3.3.3.2. Στρατιωτικές πληροφορίες

Οι αναρτήσεις αυτές αφορούν συνήθως περιεχόμενο πολυμέσων σε πραγματικό χρόνο από περιοχές-τοποθεσίες όπου είναι σε εξέλιξη κάποιο συμβάν ή κρίση. Το συγκεκριμένο υλικό σε συνδυασμό με δεδομένα από άλλες πηγές πληροφοριών (SIGINT, IMINT) προσφέρει προστιθέμενη αξία στην ανάλυση των δεδομένων που έχει στην κατοχή του ο επιτελής. Στην περίπτωση χωρών όπως οι ΗΠΑ μάλιστα με στρατεύματα σε στρατιωτικές επιχειρήσεις εκτός επικράτειάς τους, η εποπτεία ΜΚΔ για οργανώσεις, ομάδες, μεμονωμένους χρήστες θεωρείται εκ των ων ουκ άνευ για τη διαμόρφωση ενός πιο ολοκληρωμένου επιχειρησιακού σχεδιασμού. Η εικόνα που μπορεί να σχηματιστεί για τις ένοπλες ομάδες (κυβερνητικές, παραστρατιωτικές, αντιπολιτευόμενες), που δραστηριοποιούνται σε μια περιοχή, η οργανωτική τους δομή, οι τομείς δράσης, οι προσφιλείς τους πρακτικές, οι ενέργειες ή και οι διακηρυγμένες προθέσεις, μπορούν να συνθέτουν μια πληρέστερη εικόνα για τις δυνατότητες και τις αδυναμίες του συμμάχου ή του αντιπάλου.

[18] Πλέον χαρακτηριστική είναι η περίπτωση του Sohaib Athar @ReallyVirtual, ο οποίος είχε αναρτήσει στο λογαριασμό του στο Twitter εν αγνοία του μια πληροφορία σχετικά με την επιχείρηση – επιδρομή των ειδικών δυνάμεων ΗΠΑ στο κρησφύγετο του Bin Laden (2011) στο Abbottabad του Πακιστάν.

3.3.3.3. Λευκή, Γκρι, Μαύρη Προπαγάνδα / Cyber Propaganda[19]

Το φαινόμενο της προπαγάνδας ή Ψυχολογικών Επιχειρήσεων (ΨΕΠ) ορίζεται ως το σύνολο των επιχειρήσεων ή τακτικών που σχεδιάζονται από κέντρα λήψης αποφάσεων και εφαρμόζονται από φορείς με στόχο τη χειραγώγηση της λογικής και των συναισθημάτων του ατόμου και ευρύτερα της κοινής γνώμης εν καιρώ πολέμου ή και ειρήνης. Ως όρος είχε αρχίσει να αντικαθίσταται στα μέσα του προηγούμενου αιώνα με τους όρους «επικοινωνιακή εκστρατεία ή πολιτική» ή και «δημόσιες σχέσεις», προκειμένου οι τακτικές επηρεασμού της κοινής γνώμης να αποκτήσουν ένα ουδέτερο ή και θετικό πρόσημο και να προλειάνουν ένα πιο εύφορο έδαφος για την αποτελεσματική επικοινωνία και εμπέδωση μηνυμάτων και ιδεών προς και από την κοινή γνώμη.

Στην ψηφιακή εποχή όμως παραδοσιακά εργαλεία επικοινωνίας, όπως οι έντυπες και ραδιο-τηλεοπτικές διαφημίσεις, άρθρα σε έντυπα ΜΜΕ, ερευνητικές εκδόσεις, ανακοινώσεις Τύπου, έχουν αντικατασταθεί από τα σύγχρονα εργαλεία επικοινωνίας τα ΜΚΔ. Η «επικοινωνιακή πολιτική» είναι πλέον ψηφιακή, επικοινωνείται και υλοποιείται μέσω διάδοσης μηνυμάτων, ιδεών και συναισθημάτων με στόχο το μυαλό του χρήστη. Οι ΥΠ μετέχουν στην εξελιγμένη μορφή «πολέμου», ενός «πολέμου της πληροφορίας/πληροφόρησης» (Boyd, 2017) που είναι πλέον ψηφιακή και μεταλλαγμένη και ξεπερνά κλασσικές αντιπαραθέσεις σε πεδία οικονομίας, πολιτικής – διπλωματίας και στρατιωτικό. Την ιδέα του πολέμου πληροφοριών συρρικνώνει το δόγμα Gerasimov «ο *ρόλος των μη στρατιωτικών μέσων για την επίτευξη πολιτικών και στρατηγικών στόχων έχει αυξηθεί και, σε πολλές περιπτώσεις, υπερέβαινε τη δύναμη της δύναμης των όπλων στην αποτελεσματικότητά τους*».[20]

Η νέα μορφή πολέμου ονομάζεται υπολογιστική ή προγραμματιστική προπαγάνδα (computational ή cyber propaganda) και ορίζεται ως *«ο τρόπος με τον οποίο*

[19] Σε θεωρητικό επίπεδο, τα είδη που συμπεριλαμβάνει η computational propaganda, ανήκουν κυρίως στη Λευκή και τη Γκρι Προπαγάνδα. Λευκή καλείται εκείνη της οποίας η πηγή προελεύσεως είναι γνωστή, σε αντίθεση με τη δεύτερη η οποία έχει μια ασαφή ή μη αποκαλυπτόμενη πηγή ή πρόθεση. Επιπλέον υπάρχει η Μαύρη Προπαγάνδα που παρουσιάζεται με διαφορετική πηγή προελεύσεως από την πραγματική.

[20] Alexander Giles. (2020). 'Valery Gerasimov's Doctrine'. DOI: 10.13140/RG.2.2.10944.35848

χρησιμοποιούνται οι αλγόριθμοι, οι αυτοματισμοί και οι ανθρώπινες παρεμβάσεις για τη σκόπιμη διάδοση παραπληροφόρησης στα Μέσα Κοινωνικής Δικτύωσης» (Woolley, 2017: σ.3) ενώ «*συνιστά πλέον ένα από τα ισχυρότερα εργαλεία κατά της δημοκρατίας*» (Woolley, 2017: σ.7). Στην περίπτωση δε των αμερικανικών εκλογών το 2016, η ανάλυση των δικτύων κατέδειξε ότι τα «bots» στο πλαίσιο της υπολογιστικής προπαγάνδας κατέλαβαν «*θέσεις μετρήσιμης επιρροής*» ασκώντας «*σημαντική επίδραση στην ψηφιακή επικοινωνία*» (Wooley, 2017).

Για τον αναλυτή πληροφοριών τα είδη τα οποία πληροφοριών τα οποία συνιστούν αντικείμενο περαιτέρω έρευνας, καταγράφονται ακολούθως (Πίνακας 4):

Πίνακας 4 Υπολογιστική Προπαγάνδα – Οικοσύστημα Πληροφοριών

ΥΠΟΓΟΛΟΓΙΣΤΙΚΗ ΠΡΟΠΑΓΑΝΔΑ – ΟΙΚΟΣΥΣΤΗΜΑ ΠΛΗΡΟΦΟΡΙΩΝ[21]		
Α/Α	**ΕΙΔΟΣ**	**ΕΝΝΟΙΑ**
1.	**Προπαγάνδα**	Διάδοση κατασκευασμένων πληροφοριών με σκοπό τον επηρεασμό της κοινής γνώμης.
2.	**Fake News - Disinformation**	Εσκεμμένα λανθασμένες ή παραπλανητικές πληροφορίες, διακινούμενες μέσω κυρίως ηλεκτρονικών ΜΜΕ.
3.	**Misinformation** Παραπληροφόρηση	Ακούσια συνήθως ανταλλαγή ψευδών πληροφοριών.
4.	**Θεωρία Συνωμοσίας** (conspiracy theory théorie du complot)	Ένα γεγονός εξηγείται ως αποτέλεσμα μυστικής συνωμοσίας μιας μικρής ομάδας που δρα για ίδιον όφελος και αντίθετα στο δημόσιο συμφέρον.
5.	**Πληρωμένη Καταχώρηση/Άρθρο** Sponsored Content	Δημοσίευμα που εμφανίζεται ως άρθρο της συντακτικής ομάδας εντύπου, αλλά έχει διοχετευτεί από εταιρεία lobby για προβολή σε ΜΜΕ.
6.	**Ψευδοεπιστήμη Scienceploitation**	Επιστημονικοφανείς ισχυρισμοί που έρχονται σε αντίθεση με την επιστημονική μέθοδο.
7.	**Απάτη (Hoax)**	Εσκεμμένη απάτη για εξαπάτηση ή παραπλάνηση.

[21] Η βασική κατηγοριοποίηση προέκυψε από το "European Association for Viewers Interests – EAVI" το οποίο προσδιόρισε κάποια βασικά είδη τύπων δυνητικά παραπλανητικών ειδήσεων. https://eavi.eu/beyond-fake-news-10-types-misleading-info/ (Ανάκτηση 29.03.2021).

8.	**Οπαδισμός -** (Partisan)	Κομματικό περιεχόμενο με μονοδιάστατη ερμηνεία γεγονότων, που εμφανίζεται αμερόληπτο αλλά πλήττει αξιοπιστία αντιπάλου.
9.	**Clickbait** Δόλωμα	Τίτλος με περιεχόμενο που επιχειρεί να προσελκύσει προσοχή και να ενθαρρύνει χρήστη να κάνει κλικ σε έναν σύνδεσμο προς μια συγκεκριμένη ιστοσελίδα.
10.	**Λάθη (Error)**	ΜΜΕ υποπίπτουν σε λάθη, για τα οποία απολογούνται δημοσίως.
11.	**Λανθασμένη αναφορά ή παραπομπή**	Αυθεντικές εικόνες, βίντεο ή φράσεις αποδίδονται σε λάθος γεγονότα ή άτομα
12.	**Πλαστό περιεχόμενο**	Ιστοσελίδες και λογαριασμοί TW και FB παριστάνουν ότι είναι μια γνωστή μάρκα ή πρόσωπο
13.	**Παραπλανητικό περιεχόμενο**	Περιεχόμενο που δεν συνάδει με τον τίτλο και τις λεζάντες.
14.	**Παραποιημένο περιεχόμενο**	Περιεχόμενο που έχει παραποιηθεί ή τροποποιηθεί (στατιστικά στοιχεία, γραφήματα, υλικό πολυμέσων).

Πηγή: Beyond Fake News, Eavi Media Literacy for Citizenship.

Πλέον χαρακτηριστική εκστρατεία υπολογιστικής προπαγάνδας ήταν η περίπτωση των αμερικανικών προεδρικών εκλογών. Ο σχεδιασμός της εκστρατείας από τη Ρωσική Υπηρεσία Πληροφοριών Εξωτερικού (SVR) και η υλοποίησή της από τον Οργανισμό Έρευνας Διαδικτύου (IRA) πέτυχε να ελέγξει το εκλογικό αποτέλεσμα στις προεδρικές εκλογές των ΗΠΑ το 2016, κάτι που επιχείρησε να επαναλάβει και στην εκλογική αναμέτρηση του 2020. Ο IRA αξιοποίησε τα ΜΚΔ για τη διεξαγωγή ενός «πολέμου πληροφοριών» με στόχο την παραπληροφόρηση (disinformation) της κοινής γνώμης μέσω ψευδών ειδησεογραφικών άρθρων, διαφημίσεων, κατασκευασμένων πληροφορίες από «Αμερικανούς» χρήστες, trolls και θεωριών συνωμοσίας. Κατ' αυτή τη μεθόδευση το IRA πέτυχε να εμβαθύνει τη φυλετική, ιδεολογική και κοινωνική πόλωση της αμερικανικής κοινωνίας, χειραγωγώντας δεκάδες εκατομμύρια χρήστες στις ΗΠΑ να ταχθούν στην κάλπη υπέρ του υποψηφίου του ρεπουμπλικανικού κόμματος.

Το σημαντικό ρόλο που διαδραμάτισαν στη χειραγώγηση της αμερικανικής κοινής γνώμης ως ισχυρό εργαλείο για άσκηση πολιτικής επιρροής[22], ανέδειξαν πέντε εκθέσεις της Senate Select Committee on Intelligence (SSCI) των ΗΠΑ, η μια εκ των οποίων αφορά αποκλειστικά τα ΜΚΔ και την αξιοποίησή τους από τη Ρωσία με στόχο την εκλογή του Trump. Η έκθεση διαπίστωσε ότι στόχοι του IRA ήταν αφενός να δυσφημίσει και να αποδυναμώσει την υποψηφιότητα Clinton, αφετέρου να διασαλεύσει την πίστη της αμερικανικής κοινωνίας στις δημοκρατικές διαδικασίες. Η συγκεκριμένη έκθεση συνιστά την πρώτη μεγάλη ανάλυση αυτού του φαινομένου, βάσει δεδομένων που παρείχαν εταιρείες ΜΚΔ στην εν λόγω Επιτροπή (SSCI).[23]

Το ίδιο *modus operandi* υιοθέτησε η Ρωσία και το 2020 γεγονός που αποκαλύπτεται μέσα από προσφάτως αποχαρακτηρισμένα έγγραφα πληροφοριών που καταδεικνύουν ότι ο πρόεδρος της Ρωσίας ενέκρινε επιχειρήσεις με σκοπό να υποσκάψουν και την υποψηφιότητα Biden.[24] Η πλέον πρόσφατη δήλωση του Ρώσου προέδρου σύμφωνα με την οποία η *«απάντηση της Ρωσίας θα είναι ασύμμετρη, γρήγορη και σκληρή»*[25], φαίνεται να αποτυπώνει το ενδεχόμενο επανάληψης μιας προσφιλούς τακτικής, ενώ δεν παρέλειψε να επισημάνει ότι *«οι δυτικοί συνάδελφοί μας αρνούνται επίμονα τις πολυάριθμες ρωσικές προτάσεις να αναπτυχθεί ένας διεθνής διάλογος στον τομέα της πληροφοριακής και κυβερνητικής ασφάλειας»*.[26]

Αντίθετα με τις επικρατούσες απόψεις σχετικά με την πόλωση και την πολιτικοποίηση των ειδησεογραφικών πρακτορείων, καθώς και την αυξανόμενη τάση των ψηφοφόρων να εμπλέκονται σε «κομματικά κίνητρα», οι πληροφορίες αυτές καθ' αυτές

---

[22] United States Department of Justice, United States of America v. Internet Research Agency (18 U.S.C. 2,371,1349,1028A), 2018. https://www.justice.gov/file/1035477/download (Ανάκτηση 19.04.2021).

[23] Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf (Ανάκτηση 19.04.2021).

[24] National Intelligence Council, Foreign Threats to the 2020 US Federal Elections, 10 March 2021. https://int.nyt.com/data/documenttools/2021-intelligence-community-election-interference-assessment/abd0346ebdd93e1e/full.pdf (Ανάκτηση 19.3.2021).

[25] Max Seddon & Henry Foy, Putin threatens 'asymmetric' and 'tough' response to US sanctions, 21 April 2021, Financial Times. https://www.ft.com/content/724560a3-5b8e-483d-8262-e62053247366 (Ανάκτηση 24.04.2021).

[26] Presidential Address to the Federal Assembly, 21 April 2021, http://en.kremlin.ru/events/president/news/65418 (Ανάκτηση 24.04.2021).

εκλαμβάνονται ως πιο σημαντικές σε σχέση με την πηγή τους, κοινή διαπίστωση που αφορά στους ψηφοφόρους και των δύο αμερικανικών κομμάτων (Clayton, et al., 2019).

3.3.3.4. Στρατολόγηση - Ριζοσπαστικοποίηση

Η χρήση των ΜΚΔ στο σύγχρονο πόλεμο, συμπεριλαμβανομένης και της έννοιας του περιβάλλοντος των ασύμμετρων απειλών που αποτελεί βασικό χαρακτηριστικό της διεθνούς κατάστασης ασφαλείας, συνιστά πλέον αντικείμενο εντατικής μελέτης. Το διεθνές οργανωμένο έγκλημα, τρομοκρατικές οργανώσεις μετέρχονται πλέον ψηφιακών τακτικών που προκαλούν δυσανάλογα ασύμμετρο κόστος στον αντίπαλο όχι μόνο σε ανθρώπινες ζωές, αλλά σε ψυχολογικό και κοινωνικό κόστος. Αξιοσημείωτη είναι η περίπτωση της Al Shabaab και DAESH και της εκστρατείας προβολής και στρατολόγησης με την οποία πλαισίωσε την επιχειρησιακή της δράση, προκαλώντας έκπληξη για την πολυπλοκότητα και την έκτασή της.

Η IS/DAESH είχε αναπτύξει έναν αποτελεσματικό μηχανισμό προπαγάνδας μέσω δημοφιλών ΜΚΔ όπως το TW, FB, Telegram, YouTube στα οποία ανέβαζαν «επαγγελματικού» χαρακτήρα βίντεο, η δημοφιλία των οποίων έκαναν το γύρο του διαδικτυακού κόσμου λόγω των οπτικών μηνυμάτων αντί κειμένου και της χρήσης κυρίως της αγγλικής γλώσσας. Η εκστρατεία προβολής και στρατολόγησης με την οποία πλαισίωσε την προέλαση και τις στρατιωτικές της επιχειρήσεις, αποδείχθηκε αποτελεσματική. Η ισλαμιστική οργάνωση απευθυνόμενη στο θυμικό των δεκτών μουσουλμάνων και μη, επιχείρησε να το ενεργοποιήσει μέσω μηνυμάτων νομιμοποίησης των ενεργειών της και ιδεολογικής παρότρυνσης για αντίποινα «απονομής δικαίου» ως απόρροια των «αδικιών» του δυτικού κόσμου σε βάρος των μουσουλμάνων. Η ψηφιακή στρατολόγηση φάνηκε να αποφέρει μεγαλύτερο αριθμό στρατολογημένων απ’ όλο τον κόσμο, από ό,τι η ίδια η οργάνωση θα μπορούσε να προσεγγίσει με ίδια μέσα στην περιφέρεια δράσης της.

Η Αραβική Άνοιξη, η κρίση στην Ουκρανία, αλλά κυρίως η περίπτωση της IS, θα μπορούσε να χαρακτηριστεί ως μια δοκιμασία των ΜΚΔ ως εργαλεία-ασύμμετρων απειλών που εξυπηρετούν «επιχειρησιακούς» σκοπούς με μηδενικό λειτουργικό κόστος.

3.3.3.5. Οργανωμένο Έγκλημα και Τρομοκρατία

Τα δίκτυα οργανωμένου εγκλήματος και τρομοκρατίας με διασυνοριακό χαρακτήρα δράσης, έχουν στραφεί στα ΜΚΔ όπου η επικοινωνία είναι άμεση, αποτελεσματική, ανώνυμη και κρυπτογραφημένη. Ως αποτέλεσμα οι αρμόδιες αρχές επιβολής του νόμου, οι ΥΠ και οι φορείς της δικαιοσύνης καλούνται να αντιμετωπίσουν υποθέσεις κυκλωμάτων εμπορίας ναρκωτικών ουσιών, εμπορίου όπλων, διακίνησης υλικού παιδικής πορνογραφίας, κυκλωμάτων πορνείας και σωματεμπορίας (κυρίως στο darknet), νεοναζιστικών οργανώσεων, ισλαμιστικών δικτύων και γενικότερα ένα διευρυμένο πλέον ψηφιακό φάσμα εγκληματικότητας και παράνομου περιεχομένου στον κυβερνοχώρο.

Το SOCMINT παρέχοντας πληροφορίες σε πραγματικό χρόνο για τρέχουσες δραστηριότητες, καθίσταται χρήσιμο για την παρακολούθηση εγκληματικών πράξεων, τη συλλογή αποδεικτικών στοιχείων και την πρόβλεψη μελλοντικών γεγονότων. Ως μέσο επικοινωνίας στοιχεία ή λεκτικά σήματα που συνδέονται με τη δράση των συγκεκριμένων ομάδων, δύνανται να εντοπιστούν από τις αρχές καταστολής και να τεθούν υπό παρακολούθηση. Συνήθως οι περισσότερες πληροφορίες εξάγονται από μεγάλα δεδομένα στη βάση ανάλυσης της δικτύωσης των μελών των ομάδων και σ’ αυτή προστίθενται επιπλέον πληροφορίες που μπορεί να σχετίζονται με την τοποθεσία – παρουσία μελών μιας οργάνωσης, ιστοτόπους που επισκέφθηκαν, υπηρεσίες που χρησιμοποιήθηκαν και τα μοτίβα συμπεριφορών (Andrews & Brewster, 2018). Τα ανωτέρω δύνανται να συμβάλουν στην περαιτέρω κατανόηση των σύνθετων σχέσεων μεταξύ μελών οργανώσεων, στον εντοπισμό απάτης, συναλλαγών και κυριότερα να αποκωδικοποιήσουν τους στόχους της οργάνωσης ή του δικτύου.

Κεφάλαιο 4

Προκλήσεις Συλλογής Πληροφοριών από ΜΚΔ

Τα δεδομένα για να ενταχθούν σ' ένα πλαίσιο ανάλυσης πρέπει αρχικά να καταστούν πληροφορίες. Το πλαίσιο αυτό ανάλυσης ξεκινά να διαμορφώνεται από τη στιγμή όπου η ηγεσία των ΥΠ διατυπώνει κάποιο αίτημα αναζήτησης πληροφοριών, συνεχίζει με τη συνακόλουθη έρευνα από τη Διεύθυνση Συλλογής και ολοκληρώνεται εφόσον ικανοποιηθεί η πληροφοριακή ανάγκη που προέκυψε από το αρχικό ζητούμενο με τη συνδρομή της Διεύθυνσης Ανάλυσης. Η πληροφορία όμως εξάγεται και σε συνδυασμό με παραμέτρους όπως η εμπειρία του κάθε αναλυτή επί των πηγών-λογαριασμών στα ΜΚΔ, η γνώση επί θεμάτων αρμοδιότητάς του, αλλά και η κριτική του σκέψη που υποδηλώνει ότι είναι σε θέση να αξιολογήσει σειρά κριτηρίων (λ.χ. αξιοπιστία πηγής, ακρίβεια πληροφορίας, σχετικότητα, προθέσεις και σκοπιμότητες συντάκτη, αναπαραγόμενες προκαταλήψεις ή διαστρεβλωμένα στοιχεία κ.ο.κ.). Η πληροφορία από ΜΚΔ είτε ενσωματώνεται τις περισσότερες φορές μ' άλλο υλικό, είτε διακινείται ως έχει προς την ιεραρχία ανάλογα με την αξιοπιστία της πηγής και λιγότερο με την ακρίβεια της πληροφορίας.

Σε κάθε περίπτωση, το SOCMINT ως επικουρική πηγή πληροφόρησης εμπεριέχει κινδύνους στα στάδιο επεξεργασίας και ανάλυσης. Η φύση των κινδύνων με δυναμικά χαρακτηριστικά, δεν έχει προηγούμενο αντιμετώπισης σε σχέση με τις υπόλοιπες πηγές πληροφοριών. Η εναλλαγή λοιπών στην αξιοποίηση πηγών πληροφόρησης μπορεί να κομίζει προστιθέμενη αξία, παράλληλα όμως θέτει υπό αμφισβήτηση τη γνώση και την

εμπειρία του αναλυτή, με αποτέλεσμα να αναδύεται η ανάγκη για έναν νέο ίσως πιο ευέλικτό τεχνολογικά τρόπο σκέψης. Σ’ αυτό το κεφάλαιο λοιπόν θα γίνει αναφορά στις περισσότερες προκλήσεις με τις οποίες έρχεται αντιμέτωπος ο επιτελής κατά την επεξεργασία και ανάλυση της πληροφορίας.

4.1. Information Disorder

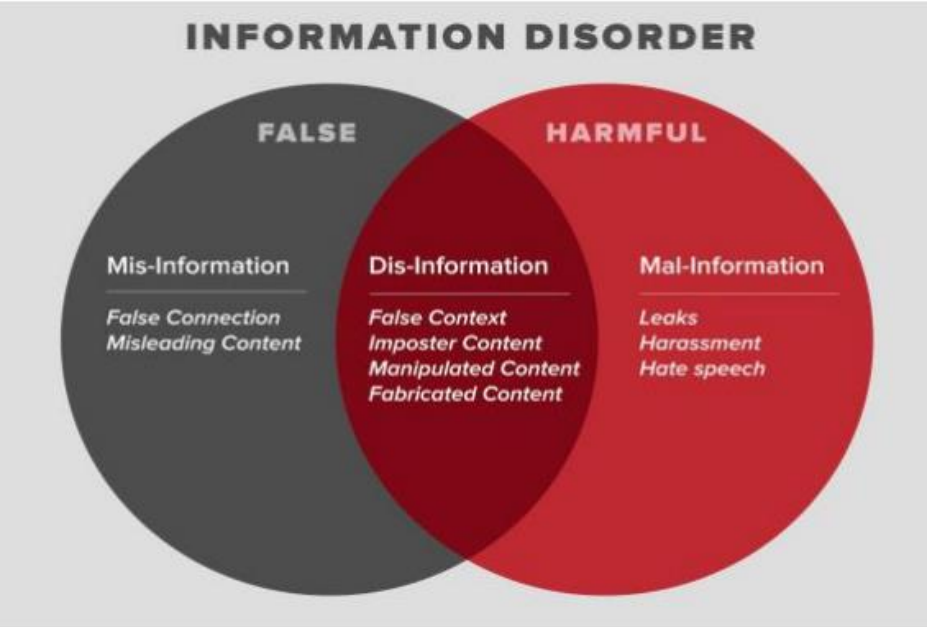
Η εκούσια καθοδηγούμενη παραπληροφόρηση (Disinformation), η ακούσια παραπληροφόρηση (Misinformation) και το Mal-information, δηλαδή πραγματικές πληροφορίες που διαρρέουν (λ.χ. διαβαθμισμένα αρχεία της υπόθεσης Snowden ή το doxxing[27]), συνιστούν υποκατηγορίες παραπληροφόρησης και εντάσσονται σ’ ένα ευρύτερο πλαίσιο φαινομένου που ορίζεται ως Information Disorder (

[27] Doxxing ή docxing αφορά σε διαρροές προσωπικών δεδομένων, λ.χ. ασθενών σε κλινικές δοκιμές.

Πίνακας 5) ή πληροφοριακή διαταραχή σύμφωνα με Wardle & Derakshan (2017). Το information disorder φαίνεται να αναδεικνύει ταυτόχρονα την αδυναμία του όρου "fake news" να αποτυπώσει τη νέα πληροφοριακή πραγματικότητα, η οποία μπορεί να συμπεριλαμβάνει και αληθινές ειδήσεις, αλλά κυρίως λόγω του γεγονότος ότι ως όρος έχει χρησιμοποιηθεί από πολιτικούς σε παγκόσμια κλίμακα για να απομειώσει ακόμη και την έγκυρη δημοσιογραφία (Wardle, 2019). Πλέον αντιπροσωπευτικό το tweet του πρώην Αμερικανού προέδρου «*Μεγάλα ειδησεογραφικά πρακτορεία, όπως CNN, The New York Times, ABC News, MSNBC και WAPO διαδίδουν 24/7 «ψεύτικες ειδήσεις» για πολιτικούς σκοπούς».*[28]

[28] Ο Trump επανειλημμένα ισχυριζόταν ότι συγκεκριμένα ΜΜΕ μεταδίδουν ψευδείς ειδήσεις. Τα σχετικά tweets όπως το "Hard to believe that with 24/7 #Fake News on CNN, ABC, NBC, CBS, NYTIMES & WAPO, the Trump base is getting stronger!" δεν είναι πλέον διαθέσιμο, λόγω αναστολής του λογαριασμού από το Twitter. Steve Coll, Donald Trump's 'Fake News' tactics. 11 Δεκεμβρίου 2017. Διαθέσιμο στο https://www.newyorker.com/magazine/2017/12/11/donald-trumps-fake-news-tactics The New Yorker. (Ανάκτηση 29.03.2021), Louis Nelson, Trump claims his base is 'Getting Stronger' despite 'Fake News'. 7 Αυγούστου 2017. http://www.politico.co/tor/01///rump-new-york-times-criticism-241378 Politico (Ανάκτηση 23.3.2021).

Πίνακας 5 Information Disorder



Πηγή: Wardle & Derakhshan 2019

Στο πλαίσιο αυτό, κρίνεται σκόπιμο να επισημανθεί ότι σε πρόσφατες μελέτες προτείνεται ο όρος «παραπληροφόρηση», σε αντικατάσταση του δημοφιλούς όρου “fake news” ή ψευδών ειδήσεων. Η Ευρωπαϊκή Επιτροπή μάλιστα σε εισήγηση της υποστηρίζοντας την υιοθέτηση της λέξης παραπληροφόρησης, επισημαίνει ότι το πρόβλημα είναι το φαινόμενο της παραπληροφόρησης και όχι οι ψευδείς ειδήσεις (European Commission, 2018a). Σε σχετική μελέτη αναφέρεται στην ασάφεια και σύγχυση που προκαλείται ως αποτέλεσμα κατάχρησης του όρου, με συνέπεια η μελέτη της παραπληροφόρησης να περιπλέκεται περαιτέρω με την αλληλοεπικάλυψη όρων όπως disinformation, misinformation, propaganda, κ.ο.κ. Στο ίδιο πνεύμα, φαίνεται να κινείται και έκθεση της Βρετανίας επί της καθοδηγούμενης εκστρατείας υπέρ του Brexit, σύμφωνα με απόσπασμα της οποίας η έλλειψη ενός κοινά αποδεκτού ορισμού για τον όρο fake news, καθώς και η καταχρηστική του χρήση, καθιστά απαραίτητη τη χρήση των όρων disinformation και misinformation (Waterson, 2018).

Με δεδομένα τα παραπάνω, στη συγκεκριμένη υποενότητα θα γίνει αναφορά στα διάφορα είδη της καθοδηγούμενης παραπληροφόρησης (disinformation), καθώς τα συγκεκριμένα -σε αντίθεση με τη μη-καθοδηγούμενη παραπληροφόρηση (misinformation)- προϋποθέτουν και υποδηλώνουν σχεδιασμό, προβολή και σκόπιμη διάχυση στην κοινή γνώμη, μέσω των «ΜΚΔ οι πλατφόρμες των οποίων συνιστούν ένα

ιδιαίτερα ευνοϊκό περιβάλλον για τη διάχυσή τους».[29] Προς επίρρωση των ανωτέρω, χαρακτηριστικά είναι τα αποτελέσματα έρευνας των Allcott and Gentzkow για τα fake news μέσω ΜΚΔ κατά τις αμερικανικές προεδρικές εκλογές του 2016, τα οποία κατέδειξαν ότι το μεγαλύτερο μερίδιο περιήγησης των χρηστών σε ψευδείς ειδήσεις ανά πηγή πληροφόρησης κατέχουν τα ΜΚΔ με ποσοστό 41.8%, με τα ΜΚΔ των επίσημων ΜΜΕ να καταλαμβάνουν μόλις το 10.1% στην ενημέρωση τους.

Στην περίπτωση του OSINT, με τις μηχανές αναζήτησης να αναδεικνύονται σε κύρια πηγή πληροφοριών για τις ΥΠ, ιδιαίτερο ενδιαφέρον παρουσιάζει το γεγονός ότι η μηχανή αναζήτησης Google Search, σε αναζήτηση με λέξεις-κλειδιά επί συγκεκριμένου πολιτικού ζητήματος εμφάνισε στην πρώτη σελίδα αποτελεσμάτων ακραίες απόψεις από Blogs, με τις αξιόπιστες πληροφορίες των ΜΜΕ να μην εμφανίζονται στην πρώτη σελίδα αποτελεσμάτων (Solon, 2016). Η Google παραδέχθηκε ακολούθως ότι «*παλεύει με ανθρώπους που επιχειρούν να παίξουν με το σύστημα, προκειμένου να ενισχύσουν το περιεχόμενο χαμηλής ποιότητας και τις ψευδείς ειδήσεις*».[30]

Με βάση τα ανωτέρω κρίνεται σκόπιμο να γίνει μια ενδεικτική απεικόνιση των ειδών παραπληροφόρησης που απαντούν στα ΜΚΔ (Πίνακας 6), με ιδιαίτερη έμφαση να δίδεται σε εκείνα που είναι καθοδηγούμενα και απασχολούν κυρίως τις ΥΠ, η οποία διαμορφώνεται πλέον ως εξής:

Πίνακας 6 Είδη Παραπληροφόρησης

Καθοδηγούμενη Παραπληροφόρηση	Propaganda Disinformation Conspiracy Theory Sponsored Content Pseudoscience Hoax Clickbait Counterfeit ή Fabricated Content ή Imposter Content

[29] Allcott H. and Gentzkow M., Social media and fake news in the 2016 election. Stanford University, *Journal of Economic Perspectives* 31(2): 211-236, 2017, σελ. 221.
[30] https://blog.google/products/search/our-latest-quality-improvements-search/ (Ανάκτηση 14/4/2021).

	Misleading Doctored Content
Malinformation	Διαρροή Hacked Emails Διαρροή Προσωπικών Δεδομένων Διαρροή Διαβαθμισμένων Εγγράφων
Μη-καθοδηγούμενη Παραπληροφόρηση	Misinformation Partisan False Attribution Error

Πηγή: Συντάκτης

Επιχειρώντας την αποτύπωση ειδών του information disorder και συγκεκριμένα της καθοδηγούμενης παραπληροφόρησης, μερικά χαρακτηριστικά θα μπορούσαν να συνοψιστούν στα ακόλουθα:

(α) είναι σκοπίμως κατασκευασμένα

(β) είναι ψευδή

(γ) εξαπατούν ψηφιακά

(δ) παραποιούν περιεχόμενο και

(ε) είναι παραπλανητικά.

4.1.1. Προπαγάνδα

«Η προπαγάνδα ορίζεται ως επικοινωνιακή μέθοδος που χρησιμοποιείται για την προώθηση ή τη δημοσιοποίηση μιας πολιτικής επιδίωξης, μιας ιδεολογικής θέσης, ή μιας ατζέντας. Βασίζεται σε μια σκόπιμη, συστηματική έμφαση σε πληροφορίες, συχνά μεροληπτικές ή παραπλανητικές, με σκοπό την προώθηση της επιθυμητής πρόθεσης του αποστολέα» (Ţuţui, 2017). Δεδομένου ότι η προπαγάνδα συνιστά επί της ουσίας μια μέθοδο επικοινωνίας, η αξιοποίησή των ΜΚΔ για προπαγανδιστικούς λόγους αποδεικνύεται αποτελεσματική, λόγω πρόσβασης σε πολυάριθμους κόμβους (χρήστες) μέσω των ακμών τους (συνδέσεις) και της ταχύτητας διάδοσης μηνυμάτων. Το συγκεκριμένος είδος συνιστά την επονομαζόμενη και «λευκή προπαγάνδα» και αφορά σε επίσημη (Πίνακας 7) ή απροκάλυπτη επικοινωνιακή πολιτική ενός κράτους (Vilmer et al., 2018).

Πίνακας 7 Λευκή ή Επίσημη Προπαγάνδα

Είδος	Παράδειγμα
Προπαγάνδα	**ΠΟΛΙΤΙΚΗ: ΤΟΥΡΚΙΑ - ΕΛΛΑΔΑ**: «Η Ελλάδα υποθάλπει τρομοκρατικές οργανώσεις, συμπεριλαμβανομένου του ΡΚΚ. Σε μία δήθεν δομή φιλοξενίας προσφύγων εντός της ΕΕ, οι τρομοκράτες σχεδιάζουν επιθέσεις (συμπεριλαμβανομένων επιθέσεων αυτοκτονίας) εναντίον της Τουρκίας, συμμάχου του ΝΑΤΟ – τη στιγμή που πραγματικοί πρόσφυγες εγκαταλείπονται να πεθάνουν στο Αιγαίο. Είναι ώρα να σταματήσει η ατιμωρησία της Ελλάδας!»[31]

4.1.2. Παραπληροφόρηση

«Η παραπληροφόρηση νοείται ως επαληθεύσιμα ψευδής ή παραπλανητική πληροφορία που δημιουργείται, παρουσιάζεται και διαδίδεται για οικονομικό όφελος ή για την εσκεμμένη εξαπάτηση του κοινού και μπορεί να προκαλέσει δημόσια ζημία. Η δημόσια ζημία περιλαμβάνει τις απειλές για τις δημοκρατικές πολιτικές και τις διαδικασίες χάραξης πολιτικής, καθώς και για τα δημόσια αγαθά, όπως η προστασία της υγείας των πολιτών της ΕΕ, του περιβάλλοντος ή της ασφάλειας. Η παραπληροφόρηση δεν περιλαμβάνει την αναφορά λαθών, τη σάτιρα και την παρωδία ή τις σαφώς προσδιορισμένες κομματικές απόψεις και τον σχολιασμό» (European Commission, 2018b).

Στην ίδια έκθεση της ΕΕ, χρήζει επισήμανσης ότι η «σκόπιμη παραπληροφόρηση με στόχο τον επηρεασμό των εκλογών και των μεταναστευτικών πολιτικών ήταν οι δύο κορυφαίες κατηγορίες που θεωρήθηκαν πιθανές να βλάψουν την κοινωνία», σύμφωνα με ερωτηθέντες σε δημόσια διαβούλευση που διεξήγαγε η Επιτροπή (European Commission, 2018b). Στο πλαίσιο αυτό, πέραν του επηρεασμού του εκλογικού σώματος και σ' ότι αφορά την Ελλάδα, χαρακτηριστικό παράδειγμα συστηματικής παραπληροφόρησης από τουρκικής πλευράς είναι αναρτήσεις από λογαριασμούς

[31] Ο επικεφαλής της Διεύθυνσης Επικοινωνιών της Προεδρίας της Τουρκίας, Fahrettin Altun, δημοσίευσε (09/04) στο λογαριασμό του στο Twitter ανάρτηση γραμμένη στην αγγλική γλώσσα, λίγα 24ωρα πριν τη συνάντηση του Τούρκου ΥπΕξ με τον Έλληνα ομόλογό του στην Τουρκία (15/04) https://twitter.com/fahrettinaltun/status/1380620185011433475.

χρηστών (Πίνακας 8) ή και κυβερνητικών αξιωματούχων σε FB και TW που κάνουν λόγο για απάνθρωπη μεταχείριση μεταναστών στο Αιγαίο από τις ελληνικές αρχές, μηνύματα που επικοινωνούνται σε διάφορες γλώσσες μεταξύ των οποίων και τα ελληνικά.

Πίνακας 8 Παραπληροφόρηση

Είδος	**Παράδειγμα**
Παρα-πληροφόρηση	**ΠΡΟΣΦΥΓΙΚΟ – ΕΛΛΑΔΑ – ΤΟΥΡΚΙΑ**: «Άνδρες του ελληνικού Λιμενικού λήστεψαν μια ομάδα μεταναστών που είχαν φτάσει στη Χίο και στη συνέχεια αφού τους έδεσαν με πλαστικές χειροπέδες τους πέταξαν στη θάλασσα χωρίς βάρκα και σωσίβιο».[32]

4.1.3. Θεωρία Συνωμοσίας

Η πανδημία του Covid-19 (Πίνακας 9) και ο Bill Gates, το ολοκαύτωμα που δεν συνέβη, η επινόηση του τουρκικού ÜST AKIL (Ιθύνων Νους)[33] από τον Erdoğan για μια δύναμη που κρύβεται πίσω από τις εξελίξεις στη Μέση Ανατολή και στην Τουρκία, είναι χαρακτηριστικές παραπλανητικές θεωρίες συνωμοσίας, που εξαπλώνονται μέσω ΜΚΔ. Στην περίπτωση δε της Τουρκίας, ο αρχηγός ενός κράτους ισχυρίζεται ότι υφίσταται μια υποτιθέμενη μυστική πλεκτάνη μιας ισχυρής δύναμης (Σ.Σ. υπαινίσσεται τις ΗΠΑ) που επιβουλεύεται με παρασκηνιακούς και μυστικούς χειρισμούς να επιφέρει αλλαγή στη δημόσια πολιτική σφαίρα, «*ενώ έχει προκαλέσει τις υφιστάμενες συνθήκες στις όμορες χώρες*». Η διάχυση της συγκεκριμένης θεωρίας, συνιστά ένα μοτίβο διαχρονικά προσφιλές στις περισσότερες πολιτικές δυνάμεις της Τουρκίας με στόχο την ενεργοποίηση ενός μηχανισμού νομιμοποίησης του καθεστώτος και απονομιμοποίησης του αντιπολιτευτικού λόγου, για διαφύλαξη του *status quo* και την ευρεία αποδοχή της θεωρίας συνωμοσίας στην τουρκική κοινή γνώμη (Karaosmanoğlu, 2021).

[32] Ο Τούρκος υπουργός Εσωτερικών Süleyman Soylu ανάρτησε βίντεο στο Twitter με τη διάσωση προσφύγων, στο οποίο διασωθείς ισχυρίζεται ότι οι ελληνικές αρχές τους έριξαν δεμένους στη θάλασσα https://twitter.com/suleymansoylu/status/1372839570421776385

[33] Από το 2014 γίνεται λόγος για «ιθύνων νου» που απεργάζεται σχέδια παγίδευσης της Τουρκίας.

Δεδομένου ότι οι θεωρίες συνωμοσίας μέσω ΜΚΔ εξαπλώνονται ταχύτητα και εμπεδώνονται άκριτα, είναι εξαιρετικά δύσκολο να τις αντικρούσει κάποιος, καθώς δύναται να θεωρηθεί συμμέτοχος της συνωμοσίας.[34]

Πίνακας 9 Θεωρία Συνωμοσίας - Γκρι Προπαγάνδα

Είδος	Παράδειγμα
Θεωρία Συνωμοσίας	**COVID – 5G:** «Τα δίκτυα 5G βοηθούν στην εξάπλωση του SARS-CoV-2, ενώ εκπέμπουν ένα είδος ακτινοβολίας που αποδυναμώνει το ανοσοποιητικό σύστημα, καθιστώντας τους ανθρώπους πιο ευαίσθητους σε μολύνσεις».

4.1.4. Sponsored Content

Φιλικά προσκείμενα προς κυβερνήσεις ΜΜΕ στο εσωτερικό αλλά και εξωτερικό, αλλοδαποί αξιωματούχοι, λειτουργούν ως φερέφωνα στη χειραγώγηση της κοινής γνώμης ή στον επηρεασμό των τοπικών αρχών.

Είδος	Παράδειγμα
Πληρωμένη Καταχώρηση	**ΗΠΑ – ΤΟΥΡΚΙΑ:** «Η σύμμαχος Τουρκία βρίσκεται σε κρίση και χρειάζεται την υποστήριξή μας».[35]

4.1.5. Pseudoscience

Η συζήτηση για το ρόλο λ.χ. των εμβολίων στην υγεία έχει επεκταθεί και στο χώρο των ΜΚΔ, μ' έναν αυξανόμενο αριθμό χρηστών να αμφισβητούν τα οφέλη του εμβολιασμού και το κατά πόσο υπερτερούν των κινδύνων, προβάλλοντας μια επιστημονικοφανή επιχειρηματολογία με σκοπό να επηρεάζουν την αντίληψη, τη σκέψη και τη

[34] https://ec.europa.eu/info/identifying-conspiracy-theories_en

[35] Ανήμερα των προεδρικών εκλογών στις ΗΠΑ (08.11.2016), η εφημερίδα The Hill είχε δημοσιεύσει άρθρο του σύμβουλου Εθνικής Ασφαλείας του Trump, το οποίο καλούσε τις ΗΠΑ να υποστηρίξουν τον Erdoğan, εξαπολύοντας ταυτόχρονα κατηγορίες εναντίον του Fethullah Gülen τον οποίο χαρακτήρισε αρχηγό «διεθνούς τρομοκρατικού δικτύου». Ο Flynn εισέπραξε για τις υπηρεσίες lobby χιλιάδες δολάρια μέσω ολλανδικής εταιρείας, χωρίς ωστόσο να δηλώσει το ποσό ως όφειλε στις αμερικανικές αρχές. https://www.nytimes.com/2017/03/10/us/politics/michael-flynn-turkey.html

συμπεριφορά των αποδεκτών.

Είδος	Παράδειγμα
Pseudoscience	**COVID – ΧΡΗΣΗ ΜΑΣΚΑΣ**: «Η συνεχής χρήση μάσκας για την προστασία από τη μόλυνση και τη λοίμωξη που προκαλεί ο Covid-19, προκαλούν δηλητηρίαση από διοξείδιο του άνθρακα».[36]

4.1.6. Hoax, Clickbait, Counterfeit, Misleading, Doctored Content

Είδος	Παράδειγμα
Hoax	**ΤΟΥΡΚΙΑ – ΚΑΤΕΧΟΜΕΝΑ:** «Ορίστε η γέφυρα ΤΔΒΚ – ΤΟΥΡΚΙΑΣ: οδική και σιδηροδρομική σύνδεση των δύο κρατών και υποδομή μεταφοράς φυσικού αερίου, ηλεκτρικής ενέργειας, νερού».[37]
Clickbait	**ΓΑΛΛΙΑ – ΝΙΓΗΡΙΑ – ΕΞΟΠΛΙΣΜΟΙ:** «Ο Μακρόν εξοπλίζει την Μπόκο Χαράμ».[38]
Counterfeit	**Ψευδείς λογαριασμοί σε ΜΚΔ με λογότυπα ΜΜΕ** όπως Associated Press, CNN, WSJ, αναμετάδιδαν ειδήσεις για τις Προεδρικές Εκλογές στις ΗΠΑ.
Misleading	Πάνω από ¼ βίντεο στο YouTube με τις περισσότερες προβολές για COVID-19 περιείχαν παραπλανητικές πληροφορίες.[39]
Doctored Content	Λογισμικό από το Stanford University μπορεί να παραποιεί βίντεο με δηλώσεις δημοσίων προσώπων σε πραγματικό χρόνο.[40]

[36] Το Twitter σε ανακοίνωσή του ανέφερε ότι από το Δεκέμβριο 2020 πλέον αφαιρεί παραπλανητικές πληροφορίες που σχετίζονται με το εμβόλιο, διαγράφοντας πάνω από 8.400 σχετικά tweets και θέτοντας υπό έλεγχο πάνω από 11,5 εκατομμύρια λογαριασμούς παγκοσμίως. https://blog.twitter.com/en_us/topics/company/2020/covid19-vaccine.html

[37] Η καθηγήτρια Emete Gözügüzelli στο «Bahçeşehir Cyprus University» των κατεχομένων, ανήρτησε tweet συνοδευόμενο με σχετικές εικόνες, συγκεντρώνοντας πάνω από 4χιλιάδες likes. https://twitter.com/e_gozuguzelli/status/1255126121646964736

[38] https://factcheck.afp.com/no-these-pictures-do-not-show-weapons-france-going-boko-haram-insurgents-nigeria

[39] Li HO, Bailey A, Huynh D, *et a*l, YouTube as a source of information on COVID-19: *a pandemic of misinformation*? BMJ Global Health 2020.

[40] Solon, O. (2017). The future of fake news: Don't believe everything you see, hear or read, The Guardian https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content

4.2. Μαύρη Προπαγάνδα - Μηχανισμοί

Στη Μαύρη Προπαγάνδα συγκαταλέγονται ως εργαλεία χειραγώγησης πληροφοριών τα Social Bots, Trolls και Hackers[41], τα οποία αναλύονται ακολούθως.

4.2.1. Social – Political Bots

Τα social bots είναι "fake" λογαριασμοί σε ΜΚΔ που προγραμματίζονται και λειτουργούν μέσω ενός υπολογιστικού αλγορίθμου με σκοπό να παράγονται αυτόματα ή και ημι-αυτόματα[42] αναρτήσεις που προσομοιάζουν στην ανθρώπινη επικοινωνία και συμπεριφορά, ούτως ώστε να δίδεται η εντύπωση ότι πίσω το λογαριασμό βρίσκεται υπαρκτό άτομο. Στο πλαίσιο αυτό, μπορούν επί παραδείγματι να αναδημοσιεύουν νέα, να κοινοποιούν την κατάστασή τους, να διαδίδουν πληροφορίες, με σκοπό την εξαπάτηση (Social Media Fraud -SMF), χρησιμοποιώντας λ.χ. τεχνητά retweets και likes (Stieglitz et al., 2017). Κατ' αυτή τη μεθόδευση αυξάνεται η ψηφιακή επιρροή του social bot, καθώς εμφανίζεται να έχει υπερβολικά μεγάλη αποδοχή απ' άλλους χρήστες με αποτέλεσμα οτιδήποτε διατυπώνεται στο λογαριασμό να εκλαμβάνεται ως καθολικά αποδεκτό και σωστό.

Το μοτίβο επικοινωνίας και δραστηριότητας ενός bot λογαριασμού σε συνδυασμό με ορισμένους στατιστικούς δείκτες, όπως ο αριθμός δημοσιεύσεων, ακολούθων και οπαδών, συνιστούν προειδοποιητικούς ενδείξεις. Επίσης, μια άλλη επιστημονική διαπίστωση αναφέρει ότι το μοτίβο συμπεριφοράς των bot παραβιάζει συνεχώς το νόμο του Benford, σε αντίθεση με τους κανονικούς χρήστες οι οποίοι επιβεβαιώνουν τη σχετική θεωρία.[43]

---

[41] Σύμφωνα με την έρευνα του "Institut de recherche stratégique de l'École militaire (IRSEM)" και του "Centre d'analyse, de prévision et de stratégie (CAPS)" για λογαριασμό του γαλλικού Υπουργείου Εξωτερικών. Jeangène Vilmer, et al. (2018), "Les manipulations de l'information: un défi pour nos démocraties", σελ. 73. https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf

[42] Σε ημι-αυτόματη λειτουργία έχουν οι λογαριασμοί "Cyborg", όπου ένας χρήστης αξιοποιώντας τη τεχνολογία των bots, μπορεί να ελέγξει την παραγωγή αναρτήσεων σε σχέση με την ταχύτητα, τη συχνότητα και το απαιτούμενο χρονικό εύρος εμφάνισής τους στα ΜΚΔ.

[43] Σύμφωνα με το νόμο Benford τα σημαντικά ψηφία των αριθμών των διαφόρων φυσικών δεδομένων δεν κατανέμονται ισοπίθανα, αλλά ευνοούνται οι μικρότεροι αριθμοί. Η διασύνδεση νόμου Benford με bots έγινε στα πλαίσια της έρευνας από Golbeck, J. (2019). Benford's Law can detect malicious social bots. First Monday, 24(8). https://doi.org/10.5210/fm.v24i8.10163

Τα bots στο σύγχρονο πόλεμο πληροφοριών ως ψηφιακό «πεζικό» αναδεικνύονται σ' ένα «από τα ισχυρότερα εργαλεία κατά της δημοκρατίας» (Wooley & Howard, 2017), που μεταφέρουν μηνύματα, εισάγουν #HateSpeech, εκφοβίζουν ή «μπλοκάρουν» τον αντίπαλο (Vilmer et al. 2018). Πρόσφατο αποδεικτικό πλήρους επιχειρησιακής ετοιμότητας και δραστηριότητας των bots ήταν η αύξηση bot traffic κατά 372% εν μέσω πανδημίας και μόνο κατά την περίοδο Σεπτεμβρίου 2019 – Μαρτίου 2021 όπου στοχοποιήθηκαν όλοι οι τομείς δημόσιας υγείας.[44]

4.2.2. Trolls

Εάν η διπλωματία είναι ο επίσημος μηχανισμός προβολής της χώρας στη διεθνή κοινή γνώμη και προώθησης των συμφερόντων της στο εξωτερικό, στον ανεπίσημο αντίποδα θα μπορούσαν να ενταχθούν τα trolls, μια συγκεκαλλυμένης μορφής νεωτερική και εξειδικευμένη τεχνική επικοινωνίας μηνυμάτων στα ΜΚΔ. Τα trolls είναι διαδικτυακά «πρόσωπα» που έχουν δημιουργήσει χρήστες με σκοπό τη διάχυση πληροφοριών, την πρόκληση κορεσμού με πολυάριθμα σχόλια ή να προβοκάρουν άλλους χρήστες με τις τοποθετήσεις τους. Επί της ουσίας, επιχειρούν αποδυνάμωση του στόχου με δημιουργία επίπλαστων αντιπαραθέσεων και σπορά διχόνοιας με αμφιλεγόμενα θέματα. Ο συγκεκριμένος μηχανισμός μπορεί να είναι άτυπα θεσμοθετημένος από μια κρατική οντότητα, όπως στην περίπτωση της Ρωσίας με το Internet Research Institute (IRA)[45], ή να λειτουργεί αυτόνομα από μεμονωμένους χρήστες. Στην πρώτη περίπτωση απαντά και ο όρος sockpuppet[46] αντί troll, όπου ο χρήστης ελέγχεται και τελεί υπό τις οδηγίες κάποιας ξένης δύναμης ή φορέα ως μαριονέτα.

Τα trolls πέραν από το ρόλο του κομιστή μηνυμάτων, μπορεί να αναπτύξουν πιο ενεργές και επιθετικές τακτικές. Τα στάδια του trolling παρομοιάζουν με εκείνα της αλιείας, δηλαδή τη διαδικασία τριών σταδίων: α) δόλωμα β) τσίμπημα γ) ανάσυρση του

[44] Edward Roberts, Bad Bot Traffic on Healthcare Websites Rises 372% As Vaccines Become Available Globally, 4 Μαρτίου 2021, https://www.imperva.com/blog/bad-bot-traffic-on-healthcare-websites-rises-372-as-vaccines-become-available-globally/ (Ανάκτηση 25.04.2021).

[45] Στην περίπτωση της Ρωσίας απαντούν επίσης οι όροι: troll farms, troll factory, troll army, lakhta trolls, ρωσικά bots, Putinbots, Kremlinbots ή web brigades. Russian web brigades (17 Απριλίου 2021). *Wikipedia* https://en.wikipedia.org/wiki/Russian_web_brigades (Ανάκτηση 25.04.2021).

[46] Stevel Poole, What's the difference between a troll and a sockpuppet? *The Guardian,* 23 Φεβρουαρίου 2018, https://www.theguardian.com/books/2018/feb/23/troll-steven-poole-word-of-week (Ανάκτηση 25.04.2021).

αλιεύματος (Szwed, 2016). Στη βάση αυτή, το troll δημοσιεύει αρχικά ένα μήνυμα για να προκαλέσει μια αντίδραση. Σε περίπτωση μη αντίδρασης, το troll εμφανίζεται ως άλλος χρήστης συμφωνώντας ή διαφωνώντας με υπερβολικό τρόπο στην αρχική ανάρτηση προκειμένου να προκαλέσει αντιδράσεις. Όταν ένας άλλος χρήστης «τσιμπήσει» το δόλωμα-ανάρτηση, τότε το troll επιχειρεί να συνεχίσει και να διατηρήσει τη «συζήτηση» με κυρίως προσβλητικά και ειρωνικά σχόλια.

Ο αυξημένος αριθμός σχολίων επί συγκεκριμένου θέματος συζήτησης που έχει υποκινηθεί από trolls, δύναται να αξιοποιηθεί για την υποκίνηση «πολιτικού και κοινωνικού ανταγωνισμού», μερικές εκφάνσεις του οποίου είναι η εκδήλωση λαϊκής δυσαρέσκειας, οι πορείες διαμαρτυρίας για καταπάτηση νόμων και οι εθνοτικές συγκρούσεις (Szwed, 2016). Σε κάθε περίπτωση, οι οργανωμένες στρατιές trolls λειτουργούν συνήθως επί πληρωμή, χωρίς βέβαια να αποκλείονται οι περιπτώσεις των χρηστών εκείνων που μετέχουν εθελοντικά, επιθυμώντας να αναπαράγουν ιδέες και θεωρίες με τις οποίες συμφωνούν.

4.2.3. Account/ID Cloning

Το Account cloning ή κλωνοποίηση λογαριασμών[47] αφορά ένα ψεύτικο προφίλ που δημιουργείται με την υποκλοπή προσωπικών στοιχείων και φωτογραφιών, όπως αυτά προβάλλονται σε πραγματικούς λογαριασμούς χρηστών. Πρόκειται για μια τεχνική κοινωνικής μηχανικής[48] όπου ο «εισβολέας» αντιγράφει την παρουσία του χρήστη είτε στην ίδια πλατφόρμα ΜΚΔ είτε σε διαφορετική, μέσω της οποίας επιχειρεί να διαμορφώσει μια σχέση εμπιστοσύνης με τους φίλους του κλωνοποιημένου προφίλ, με σκοπό την απόσπαση εμπιστευτικών πληροφοριών και την εξαπάτηση. Η μεγαλύτερη συχνότητα λειτουργίας λογαριασμών κλώνων εντοπίζονται κυρίως σε FB, αλλά και σε TW, Instagram και LinkedIn.

Ένα από τα πιο ενδιαφέροντα και απτά παραδείγματα αυτής της μορφής επίθεσης ήταν η περίπτωση του πρώην Διοικητή των ΝΑΤΟϊκών δυνάμεων στην Ευρώπη (SACEUR). Ο

[47] Επίσης αναφέρεται ως impersonation account και λογαριασμός πλαστοπροσωπίας.
[48] Ως κοινωνική μηχανική (social engineering) ορίζεται ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων που ολοκληρώνονται μέσω ανθρώπινων αλληλεπιδράσεων. Διαδεδομένες μορφές ψηφιακών επιθέσεων κοινωνικής μηχανικής είναι το baiting, scareware μέσω spam email, pretexting και phishing.

κλωνοποιημένος λογαριασμός του Αμερικανού Ναυάρχου, απετέλεσε το μέσο συλλογής προσωπικών δεδομένων πολλών υψηλόβαθμων αξιωματούχων του ΝΑΤΟ μέσω ενός λογαριασμού-κλώνου που δημιουργήθηκε από κακόβουλο λογισμικό[49] και στον οποίο, πολλοί από τα θύματα απέστειλαν σημαντικά ευαίσθητα δεδομένα, φωτογραφίες, διευθύνσεις e-mail και προσωπικούς αριθμούς κινητών τηλεφώνων. Η ανωτέρω περίπτωση καθώς κι άλλων εντός του ΝΑΤΟ, επιβεβαίωσαν τους φόβους ΗΠΑ και Ηνωμένου Βασιλείου περί κλιμακούμενης κατασκοπείας στον κυβερνοχώρο από πλευράς Κίνας σε βάρος της Δύσης και ειδικά στον ευαίσθητο χώρο της άμυνας και της αμυντικής βιομηχανίας,[50] με τη Ρωσία, το Ιράν και τη Β. Κορέα να εμπλέκονται επίσης σε κυβερνοεπιθέσεις.[51]

4.2.4. Astroturfing

Μια παρεμφερής κατηγορία λογαριασμού με τα trolls, είναι αυτή των astroturfers[52] ή shills, με μοτίβο συμπεριφοράς που προσομοιάζει σ' αυτό ενός απλού χρήστη. Το astroturfing ή shilling είναι η πρακτική δημιουργίας ενός κατ' επίφαση λαϊκού κινήματος στο διαδίκτυο, το οποίο εμφανίζεται να απηχεί απόψεις μερίδας της κοινής γνώμης. Στόχος είναι να παραπλανήσουν το κοινό, δίνοντας την εντύπωση ότι υπάρχει πραγματική λαϊκή υποστήριξη ή αντίθεση για μια συγκεκριμένη ομάδα ή πολιτική. Το astroturfing όπως και στην περίπτωση των trolls, είναι συγκεκαλυμμένο και εμφανίζει έναν υπολογίσιμο αριθμός «χρηστών» να τάσσεται υπέρ ενός ζητήματος ή μιας κυβερνητικής πολιτικής, όταν η δραστηριότητά αφορά σε εθνικό επίπεδο.

Με τη συστηματική συμμετοχή σε συζητήσεις και προφίλ μέσου πολίτη, τα μηνύματα διαχέονται σε ανυποψίαστους χρήστες, προσδίδοντας μια ευρύτητα αποδοχής και αξιοπιστίας μηνύματος σε λαϊκή βάση. Οι astroturfers μπορούν να παρεισφρήσουν σε συζητήσεις, όπου διαφαίνεται η ανάπτυξη μιας διαφορετικής άποψης ανάμεσα σε

[49] Αναφέρεται χωρίς να μπορεί να επιβεβαιωθεί το κακόβουλο λογισμικό koobface.
[50] Nick Hopkins, China suspected of Facebook attack on Nato's supreme allied commander, 11 Μαρτίου 2012. The Guardian. https://www.theguardian.com/world/2012/mar/11/china-spies-facebook-attack-nato (Ανάκτηση 28.04.2021).
[51] European Parliament, Computational Propaganda techniques. 12 Σεπτεμβρίου 2018. https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf (Ανάκτηση 28.04.2021).
[52] Ο όρος προέρχεται από το "AstroTurf" αμερικανική εταιρεία για συνθετικό γρασίδι. Έτσι γίνεται λογοπαίγνιο με κάτι που προσομοιάζει με πραγματικό και είναι στη βάση – grassroots.

χρήστες, με σκοπό να αντιτείνουν μια αντίθετη θέση με «λαϊκό» έρεισμα, ενώ στην πραγματικότητα εξυπηρετούνται κάποια ιδιοτελή ή και εθνικά συμφέροντα. Οι astroturfers επιχειρούν να μεταθέτουν τη συζήτηση από τη λογική στο θυμικό για να μετατρέψουν μερίδα χρηστών σε οργισμένη μάζα, να αποσπάσουν την προσοχή δημοσιογράφων με σκοπό την καθοδήγησή τους σε συγκεκριμένες ροές πληροφόρησης[53] ή και την υποβάθμιση της αξιοπιστίας τους. Οι astroturfers μπορούν επίσης να εκφράσουν έντονη αγανάκτηση για το κατεστημένο προκειμένου να κερδίσουν εύνοια από το διαδικτυακό περίγυρο.[54]

4.2.5. Fake Profile/Account

Ένα Fake Profile ή Account, είναι ένα ψεύτικο προφίλ στα ΜΚΔ, όπου αναπαριστά ένα άτομο, έναν οργανισμό ή μια εταιρεία που δεν υφίσταται πραγματικά στα ΜΚΔ. Πάγια πρακτική συνιστά η χρησιμοποίηση ονομάτων που φαίνονται πραγματικά και έχουν σχεδιαστεί με τέτοιο τρόπο για να έχουν πρόσβαση σε συγκεκριμένα άτομα. Μερικά από τα χαρακτηριστικά των ψεύτικων προφίλ προβάλλουν μια επιμελημένη φωτογραφία προφίλ, έχουν δημιουργηθεί πρόσφατα, διαθέτουν εκατοντάδες φίλους και το περιεχόμενο των αναρτήσεων είναι προϊόν παραποίησης ή και κλοπής απ' άλλους χρήστες. Το πόσο ισχυρό μπορεί να αποδειχθεί ένα ψεύτικό προφίλ είναι σε συνάρτηση με το χρόνο που δραστηριοποιείται, το δίκτυο φίλων του και τις μεταξύ τους αλληλεπιδράσεις. Στόχος δημιουργίας ενός ψεύτικου προφίλ είναι η δημιουργία συνδέσμων που ανακατευθύνουν σε sites με κακόβουλο λογισμικό, η διάδοση ψευδών ειδήσεων, η χειραγώγηση της κοινής γνώμης, η παρενόχληση ή και ο εκβιασμός άλλων χρηστών.

Εταιρείες όπως το FB και TW *«για τη διατήρηση ενός ασφαλούς περιβάλλοντος και την*

[53] Επί παραδείγματι η κυβέρνηση Duterte στις Φιλιππίνες εφαρμόζει εξελιγμένες πρακτικές Astroturfing που στοχεύουν δημοσιογράφους και ΜΜΕ. (Wardle, 2017).

[54] Τη σημασία που αποδίδεται στο astroturfing από χώρες όπως οι ΗΠΑ, επιβεβαιώνουν πληροφορίες του Τύπου, στις οποίες γίνεται αναφορά στον τρόπο λειτουργίας τους: α) δημιουργία πολυάριθμων προσωπικοτήτων ανά χρήστη με στοιχεία και ιστορικό που είναι τεχνικά, πολιτισμικά και γεωγραφικά συνεπή, β) παροχή «τυχαίων επιλεγμένων διευθύνσεων IP οι οποίες πρέπει να αλλάζουν καθημερινά για να αποκρύπτεται η συγκεκριμένη λειτουργία γ) ειδικό λογισμικό – προκάλυμμα που θα συνδυάζει το web traffic των astroturfers με το traffic πλήθους χρηστών. George Monbiot, The need to protect the internet from 'astroturfing' grows ever more urgent, 23 Φεβρουαρίου 2011, The *Guardian.* https://www.theguardian.com/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing (Ανάκτηση, 25.04.2021)

ενίσχυση της ελεύθερης έκφρασης, διαγράφουν λογαριασμούς που είναι επιβλαβείς για την κοινότητα (false amplifiers), συμπεριλαμβανομένων αυτών που θέτουν σε κίνδυνο την ασφάλεια άλλων λογαριασμών και των υπηρεσιών τους».[55] Στο πλαίσιο αυτό έχει δημιουργηθεί ένα αυτοματοποιημένο σύστημα για τον αποκλεισμό και τη διαγραφή που λογαριασμών που χρησιμοποιούνται για κατ' επανάληψη ή κατάφωρη κατάχρηση των όρων που θέτουν τα ΜΚΔ για τις κοινότητές τους.

Το FB στον απόηχο των εκλογών του 2016, εξέδωσε ένα εγχειρίδιο με τίτλο "Information Operations and FB" στην οποία αναφέρθηκαν στα fake profiles ως false amplifiers, μέσω των οποίων οργανωμένοι φορείς, όπως κυβερνήσεις και μη, διαχέουν ψευδείς ειδήσεις ή παραπληροφόρηση για τη διαστρέβλωση του κλίματος εμπιστοσύνης στο εσωτερικό ή εξωτερικό μιας χώρας, αποσκοπώντας στην επίτευξη στρατηγικών ή γεωπολιτικών στόχων (Wardle, 2017).

4.3. Αυτοπροπαγάνδα

«Ένας κόσμος κατασκευασμένος από το γνωστό είναι ένας κόσμος στον οποίο δεν υπάρχει τίποτα να μάθει κάποιος … (αφού υπάρχει) αόρατη αυτοπροπαγάνδα, που μας καθοδηγεί μέσω των δικών μας ιδεών».[56]

4.3.1. Filter Bubble

Το φαινόμενο "Filter Bubble" ή εξατομικευμένων σφαιρών ενημέρωσης, διατυπώθηκε στην επιστημονική κοινότητα από τον ερευνητή Eli Pariser και περιγράφει την κατάσταση στην οποία περιέρχεται ο χρήστης όταν λαμβάνει προσωποποιημένες πληροφορίες, ως αποτέλεσμα εξελιγμένων και απολύτως μυστικών αλγορίθμων εξατομίκευσης (personalization) που χρησιμοποιούνται από εταιρείες παροχής περιεχομένου, όπως μηχανές αναζήτησης (Google), ΜΚΔ, ΜΜΕ, με αποτέλεσμα τον αποκλεισμό του από την αντικειμενική πληροφόρηση.

[55] Μεταξύ των πρακτικών αντιμετώπισης Fake Profiles, το FB απαιτεί επαλήθευση μέσω email ή αριθμού κινητού τηλεφώνου, ενώ περιορίζει τον αριθμό λογαριασμών ανά διεύθυνση email σ' ένα μόνο. https://www.facebook.com/communitystandards/misrepresentation (Ανάκτηση 28.04.2021).

[56] Eli Pariser "Invisible Sieve: Hidden, Specially for You", *The Economist,* 30 Ιουνίου 2011. (Ανάκτηση 25.04.2021).

«Η νέα γενιά φίλτρων του διαδικτύου κοιτάει τα πράγματα που μοιάζει να σου αρέσουν – τα πράγματα που έχεις κάνει ή τα πράγματα που αρέσουν σε ανθρώπους σαν κι εσένα – και προσπαθεί να βγάλει συμπεράσματα. Είναι μηχανές πρόβλεψης, διαρκώς δημιουργώντας και βελτιστοποιώντας μία θεωρία του ποιος είσαι και τι θα κάνεις και θα θελήσεις αργότερα. Μαζί, αυτές οι μηχανές δημιουργούν ένα μοναδικό σύμπαν πληροφοριών για τον καθένα μας – αυτό που αποκαλώ filter bubble – το οποίο αλλάζει ουσιαστικά τον τρόπο με τον οποίο συναντούμε ιδέες και πληροφορίες» (Pariser, 2011).

Τα τρία ιδιαίτερα χαρακτηριστικά, σύμφωνα με τον Pariser (2011), είναι τα εξής: α) ο καθένας είναι μόνος εντός του filter bubble. Παρ' ό,τι μπορεί να υπάρχουν αρκετά κοινά στοιχεία ή ενδιαφέροντα με άλλους, το filter bubble του καθενός είναι απόλυτα προσωποποιημένη και ατομική, β) το filter bubble είναι αόρατη. Εντός του, το άτομο δεν γνωρίζει ότι οι πληροφορίες τις οποίες λαμβάνει φιλτράρονται ή στη βάση ποιων υποτιθέμενων χαρακτηριστικών του ατόμου μπορεί να συμβαίνει αυτό το φιλτράρισμα και γ) το άτομο δεν επιλέγει να εισέλθει στη φούσκα αυτή.

Όταν η ενημέρωση του χρήστη γίνεται από επίσημους ιστοτόπους των ΜΜΕ, σε κάποιο βαθμό επαφίεται στον ίδιο το χρήστη να επιλέξει ένα συγκεκριμένο τρόπο ενημέρωσης, που αποτυπώνει μια συγκεκριμένη ειδησεογραφική πραγματικότητα, βάσει του ιδεολογικού χώρου που εκπροσωπεί το ΜΜΕ. Στην αναζήτηση όμως στα ΜΚΔ, τα αποτελέσματα αναδεικνύουν πληροφορίες μέσα από αδιαφανή αλγοριθμική διαδικασία, ωστόσο καθορίζουν την πρόσβαση του χρήστη στην πληροφορία και ως εκ τούτου επηρεάζουν τις αντιλήψεις του.

4.3.2. Echo Chambers

Το Echo Chamber (χώρος αλληλεπίδρασης ομονοούντων χρηστών - αντηχείο) είναι ένα περιβάλλον στο οποίο το άτομο συναντά μόνο πληροφορίες ή απόψεις που αντανακλούν και ενισχύουν τη δική τους. Στη βάση αυτή το echo chamber μπορεί να προκαλέσει και να διαστρεβλώσει την οπτική ενός ατόμου για ένα θέμα, με αποτέλεσμα να έχει δυσκολία να εξετάσει αντίθετες απόψεις ή να συζητήσει θέματα υπό διαφορετικές οπτικές. Ισχυρός παράγοντας ενίσχυσης ενός περιβάλλοντος echo chamber είναι η προκατάληψη επιβεβαίωσης (confirmation bias) του χρήστη, που αφορά την τάση του ατόμου να συντάσσεται με πληροφορίες που ταυτίζονται με τις

υπάρχουσες ατομικές πεποιθήσεις.

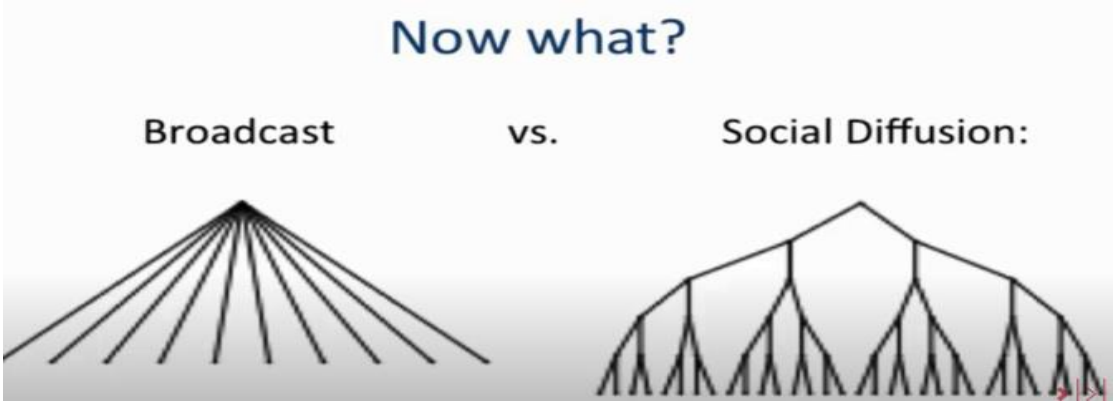
Το echo chamber σε αντίθεση με το filter bubble, προϋπήρχε του διαδικτύου, καθώς μπορεί να διαμορφωθεί ως περιβάλλον οπουδήποτε ανταλλάσσονται πληροφορίες δια ζώσης ή online. Αυτή η συνθήκη του ομόηχου περιβάλλοντος ευνοείται στα ΜΚΔ, καθώς οι χρήστες μπορούν να εντοπίσουν ιδέες που τους αντιπροσωπεύουν ή άτομα με ταυτόσημες απόψεις με αποτέλεσμα τα echo chambers λόγω του εύρους της διάχυσης της πληροφορίας στο διαδίκτυο να διευρύνονται αριθμητικά κι αυτά. Ως αποτέλεσμα των echo chambers αντηχείται μία άποψη αληθής ή ψευδής ως η επικρατούσα[57] και η πιο ευρέως αποδεκτή, ενώ η διαφορετική άποψη λογοκρίνεται ή υποβαθμίζεται με mute, unfollow ή και block.

Επί της ουσίας επιβεβαιώνεται ότι:

(α) η πληροφορία υπερνικά την πηγή από την οποία προέρχεται (Clayton, et al., 2019) και

(β) τα likes, comments, shares, δηλαδή οι κοινωνικές αποδείξεις (social proof) διαδραματίζουν πιο βαρύνοντα ρόλο σε ό,τι αφορά τη διάχυση της πληροφορίας ή της παραπληροφόρησης στο ψηφιακό οικοσύστημα, σε σύγκριση με τις πληροφορίες που στηρίζονται σε επιστημονικές αποδείξεις (Gyenes & Seymour, 2017). Ενδεικτικός ο κάτωθι πίνακας, που απεικονίζει τη σύγκριση στο εύρος της κοινωνικής διάχυσης μιας πληροφορίας μέσα από τα ΜΚΔ και τα ΜΜΕ.

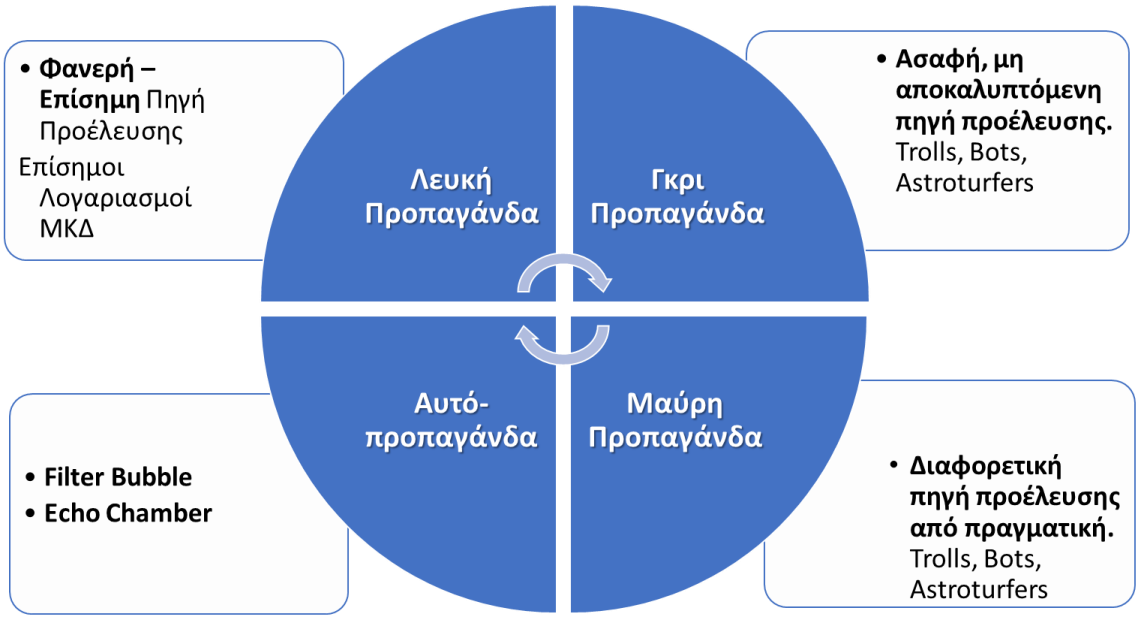
Πίνακας 10 Διάχυση μέσω Μετάδοσης και ΜΚΔ



Πηγή: Gyenes & Seymour (2017). Public Health Echo Chambers in a Time of Mistrust & Misinformation

[57] Βάσει της αρχής της ομοφιλίας οι όμοιοι χρήστες στα ΜΚΔ τείνουν να συνδέονται μεταξύ τους και ως εκ τούτου η διάχυση της πληροφορίας να καθίσταται πιο εύκολη.

Τέλος, επιχειρώντας μια οπτικοποίηση των όσων καταγράφηκαν ανωτέρω, φαίνεται να προκύπτουν τέσσερις βασικές κατηγορίες προπαγάνδας:



Κεφάλαιο 5

Μελέτη Περίπτωσης: Τουρκία

Οι εξελίξεις στις τεχνολογίες πληροφοριών και επικοινωνιών αναμενόταν, μεταξύ άλλων, να διευκολύνουν τη διαδικασία εκδημοκρατισμού σε αυταρχικά καθεστώτα. Ωστόσο, οι κυβερνήσεις των χωρών αυτών προσαρμόστηκαν στο μεταβαλλόμενο περιβάλλον των νέων τεχνολογιών, χωρίς όμως η προσαρμογή αυτή να συνεπάγεται και ανάλογη μεταστροφή προς μια δημοκρατική διακυβέρνηση. Τα καθεστώτα αυτά προσαρμόστηκαν στις προκλήσεις των ΜΚΔ με στόχο την περαιτέρω εδραίωση της κυριαρχίας τους μέσω ενός «Δικτυωμένου Αυταρχισμού» (”Networked Authoritarianism”, MacKinnon, 2011), όπως στις περιπτώσεις Κίνας και Ρωσίας. Αντίστοιχες μεθοδεύσεις υιοθετήθηκαν και από την Τουρκία, όταν αντιλήφθηκε τη δύναμη των πολιτών μέσω των ΜΚΔ και την αδυναμία της να την καταστείλει.

Όπως θα διαφανεί από τη μελέτη διαφόρων ερευνών για τη χρήση των ΜΚΔ από το τουρκικό κυβερνών κόμμα ΑΚΡ, η πρακτική που έχει υιοθετήσει και εφαρμόζει εντάσσεται σ’ αυτό που ορίζεται ως «*τρίτης γενιάς έλεγχος του κυβερνοχώρου»* των Deibert και Rohozinksi (2010). Σε αντίθεση με τις άλλες «γενιές ελέγχου»[58] που έχουν αμυντικό χαρακτήρα, ο έλεγχος είναι επιθετικός, εξελιγμένος και πολυδιάστατος, αυξάνοντας την «ανταγωνιστικότητα» έναντι αντιπάλων, καθώς είναι εξαιρετικά δύσκολο να εντοπίσουν από ποιόν και από που προέρχεται, με τις κυβερνήσεις χωρών

[58] Βάσει της κατηγοριοποίησης του Deibert α) το φιλτράρισμα «πρώτης γενιάς», τύπου Κίνας, συνίσταται σε αποκλεισμό πρόσβασης σε συγκεκριμένους ιστοτόπους, αποκλεισμό εύρεσης με λέξεις-κλειδιά και διευθύνσεις IP β) ο έλεγχος «δεύτερης γενιάς» αφορά στη συγκρότηση ενός κανονιστικού πλαισίου με το οποίο νομιμοποιούνται οι αποφάσεις του κράτους. .

ΗΠΑ, Γαλλίας, Ηνωμένου Βασιλείου να διερευνούν τον ενορχηστρωτή πίσω από τις εκστρατείες παραπληροφόρησης σε βάρος τους.[59] Για την «εξημέρωση» των ΜΚΔ, το ΑΚΡ δεν περιορίστηκε σε αναθεωρημένα νομοθετικά πλαίσια, συλλήψεις, κ.ο.κ. Η λύση στο ζήτημα της «κατακερματισμένης» ψηφιακής κοινωνίας ήταν η συγκρότηση μιας ψηφιακής στρατηγικής στα ΜΚΔ, με κύριες δράσεις «ελέγχου»:

- *Στοχοθετημένης κυβερνοκατασκοπείας* δηλαδή της παρακολούθησης ακτιβιστών και αντιφρονούντων,
- *Astroturfing* και
- *Trolling.*

[59] Western intelligence services tackle challenge of attributing foreign influence operations, 12.05.2021, *Intelligence Online.* https://www.intelligenceonline.com/government-intelligence/2021/05/12/western-intelligence-services-tackle-challenge-of-attributing-foreign-influence-operations,109665127-art

5.1. Χειραγώγηση ΜΚΔ – Θεωρητικό Πλαίσιο

Σε ό,τι αφορά τη χειραγώγηση των ΜΚΔ στην Τουρκία, από την επεξεργασία των δεδομένων κατά την έρευνα του Computational Propaganda Project (Bradshaw & Howard, 2018 & 2019), προέκυψαν για τα έτη 2017 και 2018 ανά θεματική κατηγορία, τα κάτωθι συμπεράσματα:

(1) Οργανωτική Μορφή Χειραγώγησης ΜΚΔ

ΕΤΟΣ	**Κυβερνητικές Υπηρεσίες**	**Πολιτικοί & Κόμματα**	**Εξωτερικοί Συνεργάτες**	**ΜΚΟ**	**Πολίτες & Influencers**
2017	√ (1)	√ (1)	X	X	√
2018	√ (1)	√ (1)	X	X	√

Μία κυβερνητική υπηρεσία, πολιτικοί, ένα κόμμα (ΑΚΡ) και πολίτες, χρησιμοποιούν τα ΜΚΔ ως μέσο χειραγώγησης. Στην κατηγορία εξωτερικών συνεργατών δεν προκύπτουν στοιχεία που να καταδεικνύουν ανάθεση έργου σε τρίτους. Όπως και στη Ρωσία και Ισραήλ, αντίστοιχα και στην Τουρκία, εξειδικευμένοι νέοι στα ΜΚΔ στρατολογούνται από “Cyber Troops” για να συνδράμουν στις δραστηριότητες του κράτους.

(2) Στρατηγικές Χειραγώγησης στα ΜΚΔ: Μηνύματα και Valence[60]

Έτος	*Είδος Ψεύτικου Λογαριασμού*	*Υπέρ Κυβέρνησης*	*Κατά Αντιπολίτευσης*	*Μηνύματα διασπαστικά*	*Trolling ή Harassment*	*Suppressing*
‘17	Human & Automated Accounts	√	√	X	√	-
‘18	Human & Automated Accounts	√	√	X	√	√

[60] Στα ΜΚΔ το Valence καταδεικνύει σε ποιο βαθμό οι πληροφορίες που κοινοποιούνται είναι θετικές, ουδέτερες ή αρνητικές.

Με δύο είδη "fake" λογαριασμών, human και automated, χωρίς χρήση cyborg accounts, προβάλλονται μηνύματα υπέρ της κυβέρνησης και κατά των κομμάτων της αντιπολίτευσης, τα οποία πέρα από trolling ή harassment αποκτούν και κατασταλτικό χαρακτήρα.

(3) Στρατηγικές για χειραγώγηση των ΜΚΔ

Η Τουρκία μέσω ΜΚΔ επικοινωνεί μηνύματα «στρατηγικού περιεχομένου». Η ψηφιακή της παρουσία όπως αυτή καθορίζεται από το εύρος παρουσίας και συμμετοχής cyber troops στις πλατφόρμες, την εντάσσει στη *μεσαία κατηγορία* χωρών, κύρια χαρακτηριστικά της οποίας είναι:

(α) **συνεπής στρατηγική**,

(β) **πλήρης απασχόληση εργαζομένων**,

(γ) **συνεχής εναλλαγή εργαλείων χειραγώγησης**.

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά τα ευρήματα της μελέτης:

Πίνακας 11 Συγκριτική Μελέτη Χειραγώγησης ΜΚΔ από Κράτη

Συγκριτική Μελέτη Χειραγώγησης Μέσων Κοινωνικής Δικτύωσης από Κυβερνήσεις χωρών σε παγκόσμια κλίμακα				
Πολίτευμα (κρατών υπό μελέτη)	**Δρών** (Modal Actor)	**Επίπεδο Οργάνωσης**	**Επίπεδο Ικανότητας**	**Στόχος**
Δημοκρατία Αργεντινή, Αυστραλία, Βραζιλία, Τσεχία, Ισημερινός, **Γερμανία**, Ινδία, **Ισραήλ,** Μεξικό, Φιλιππίνες, Πολωνία, Σερβία, Ν. Κορέα, Ταϊβάν, **Η. Β., Η.Π.Α.**	Πολιτικό Κόμμα	Μεσαίο	4.63	Εσωτερικό
Αυταρχικό Αζερμπαϊτζάν, Μπαχρέιν, Κίνα, Ιράν, Β. Κορέα, Ρωσία, Σαουδική Αραβία, **Τουρκία** Βενεζουέλα, Βιετνάμ	Κυβέρνηση	Υψηλό	4.4	Εσωτερικό
Κράτος υπό κρίση Ουκρανία, Συρία	Κυβέρνηση	Χαμηλό	3.5	Εσωτερικό

Πηγή: Bradshaw & Howard (2018b).

(4) Modal Actors

Στα αυταρχικά καθεστώτα συντονιστικό ρόλο διαδραματίζουν τα υπουργεία ή συναρμόδιες υπηρεσίες, τα οποία λειτουργούν παράλληλα ως κέντρα λήψης αποφάσεων για επιβολή λογοκρισίας ή για άσκηση ελέγχου και εποπτείας στον κυβερνοχώρο. Στην περίπτωση της Τουρκίας, αρμόδιος φορέας είναι η Αρχή Τεχνολογιών Πληροφοριών και Επικοινωνιών - ΒΤΚ[61] (Oğuz & Demirkol, 2019).

(5) Επίπεδο οργάνωσης

Η Τουρκία εμφανίζει το υψηλότερο επίπεδο επίσημης οργάνωσης, με τις επιφορτισμένες ομάδες να εργάζονται σε δομημένο περιβάλλον με διαχειριστές και δομές αναφοράς.[62] Cyber troops αναλαμβάνουν καθημερινά να κάνουν αναρτήσεις ή να προσεγγίζουν πραγματικούς χρήστες. Η επαγγελματική κατάρτιση του προσωπικού είναι συνεχής, το οποίο λαμβάνει υποτροφίες ως αναγνώριση αλλά και ως κίνητρο για να καταστεί η δραστηριοποίησή τους στα ΜΚΔ περαιτέρω συστηματική, τακτική ιδιαίτερα προσφιλής σε απολυταρχικά καθεστώτα, όπως σημειώνει σχετικά η έρευνα.

(6) Επίπεδο ικανότητας

Στην κατηγορία των απολυταρχικών καθεστώτων όπου ανήκει, οι συνήθεις πρακτικές περιλαμβάνουν εξελιγμένα εργαλεία φίμωσης ελευθερίας λόγου, όπως trolling, παρενόχληση, ρητορική μίσους ή απειλών εναντίον πολιτικών αντιφρονούντων. Η στοχοποίηση δημοσιογράφων με ρεκόρ φυλακίσεων[63], συνιστά πλέον μια

---

[61] Το χαρτοφυλάκιό της ΒΤΚ - Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı συμπεριλαμβάνει και τις αρμοδιότητες της καταργηθείσας «Προεδρίας Επικοινωνιών Τηλεπικοινωνιών» (Telekomünikasyon İletişim Başkanlığı - TİB), που είχε σε συνεργασία με τη MİT και τα σώματα ασφαλείας, την ευθύνη υποκλοπών, εποπτείας διαδικτυακού περιεχομένου και μπλοκάρισμα ιστοτόπων. Telekomünikasyon İletişim Başkanlığı, Vikipedi, 10 Φεβρουαρίου 2021. Τουρκική έκδοση Wikipedia, https://tr.wikipedia.org/wiki/Telekom%C3%BCnikasyon_%C4%B0leti%C5%9Fim_Ba%C5%9Fkanl%C4%B1%C4%9F%C4%B1 (Ανάκτηση, 01.05.2021).

[62] Σύμφωνα με τουρκικά δημοσιεύματα ειδικές εκπαιδεύσεις πραγματοποιήθηκαν και στις 81 τουρκικές επαρχίες της τουρκικής επικράτειας. https://www.hurriyet.com.tr/gundem/ak-partiden-6-bin-kisilik-sosyal-medya-ordusu-25115336 (Ανάκτηση 24.04.2021).

[63] Σύμφωνα με έρευνας της οργάνωσης «Δημοσιογράφοι Χωρίς Σύνορα (RSF)», το 90% του τουρκικού Τύπου ελέγχεται από φιλοκυβερνητικούς επιχειρηματίες. 160 ΜΜΕ υποχρεώθηκαν να κλείσουν μετά την απόπειρα πραξικοπήματος, 200 δημοσιογράφοι βρίσκονται κρατούμενοι σε τουρκικές φυλακές κατά την τελευταία πενταετία, 139 εκπρόσωποι του Τύπου υπήρξαν στόχοι επιθέσεων τα τελευταία πέντε έτη, 3,436 έχουν απολυθεί, ενώ 1,358 άρθρα στο διαδίκτυο έχουν διαγραφεί μετά από εντολή του Erdoğan ή συγγενών και συνεργατών του. Turkey – press freedom in figures. 28 Ιανουαρίου 2021. RSF. https://rsf.org/en/news/turkey-press-freedom-figures (Ανάκτηση, 30.04.2021).

διαδεδομένη απειλή για την ελευθερία του Τύπου σε διεθνές επίπεδο (Bradshaw & Howard 2018b). Το hashtag #ΥπάρχειΠίεσησταΜΜΕ (#MedyayaBaskıVar), συνιστά ένδειξη της διευρυμένης αποδοχής και απήχησής του, με περισσότερα από 500.000 tweets σε 24 ώρες στην Τουρκία μετά τη δημοσιοποίηση ηχογραφημένης τηλεφωνικής συνομιλίας του Erdoğan.[64] Σε αντίθεση με τουρκική έρευνα που υποστηρίζει ότι το trolling στην Τουρκία δεν είναι θεσμοθετημένο από κάποια αρχή, αλλά συνιστά *ad hoc* αντίδραση ομάδων στο διαδίκτυο (Saka, 2018), η έρευνα των Bradshaw και Howard (2019) αποδεικνύει ότι το trolling στην Τουρκία χρηματοδοτείται από κράτος, το οποίο διεξάγει εκστρατείες παραπληροφόρησης μέσω εφαρμογής υπολογιστικής προπαγάνδας σε TW και FB.

(7) Στοχοποίηση

Σ' ό,τι αφορά τους στόχους χειραγώγησης μέσω ΜΚΔ, η έρευνα καταλήγει ότι αυτοί εντοπίζονται στο εσωτερικό ανεξάρτητα με το είδος πολιτεύματος. Στις δημοκρατικές χώρες, η εκστρατεία παραπληροφόρησης συνήθως λαμβάνει χώρα πριν τη διεξαγωγή εκλογών. Στην περίπτωση της Τουρκίας οι εκστρατείας παραπληροφόρησης συνιστούν ένα επιπρόσθετο εργαλείο εφαρμογής λογοκρισίας και καταστολής.

5.2. Πρακτική Εφαρμογή

Τα ευρήματα της έρευνας των Bradshaw και Howard, επιβεβαιώνουν δηλώσεις αξιωματούχων του ΑΚΡ περί στρατολόγησης 6 χιλιάδων ατόμων – κομματικών μελών, που θα επάνδρωναν ομάδες ελέγχου και εποπτείας των ΜΚΔ, ως αποτέλεσμα των γεγονότων στο Gezi Park το 2013. Η επίσημη έστω και αποσπασματική αναγνώριση της δράσης ομάδων στα ΜΚΔ εκ μέρους της κυβέρνησης, δεν προέκυψε ως ανάγκη ενημέρωσης της κοινής γνώμης, αλλά ως αποτέλεσμα πιέσεων από δημοσιογραφικούς κύκλους για επιβεβαίωση ή διάψευση δημοσιεύματος της αμερικανικής ε/φ Wall Street Journal που προηγήθηκε των δηλώσεων (09/13).

Με τα γεγονότα στο Gezi Park, το ΑΚΡ συνειδητοποιεί τη δύναμη της κοινωνίας πολιτών να αντιδράσουν μέσω ΜΚΔ, αλλά και την αδυναμία του να τα ελέγξει. Η πρώτη

[64] #BBCtrending: Turkish PM's private call goes viral, 13 Φεβρουαρίου 2013, https://www.bbc.com/news/blogs-trending-26174287 (Ανάκτηση, 29.04.2021).

εκδήλωση αντίδρασης του λαού εναντίον της κυβέρνησης του ΑΚΡ από την ανάληψη της εξουσίας το 2002, αποτελεί και το σημείο καμπής για την πορεία της Τουρκίας προς το «δικτυωμένο αυταρχισμό».[65] Οι ομάδες κρούσης με πλατφόρμα ευθύνης κυρίως το «ταραχοποιό» TW[66], FB, Instagram και YouTube, ήταν επιφορτισμένες με αρμοδιότητες «*δημιουργίας περιεχομένου, ανταλλαγής οπτικού και γραπτού περιεχομένου, προβολής πολιτικών του ΑΚΡ και εξάλειψης «ρυπαντογόνων πληροφοριών» (bilgi kirliliğinin) που στόχο έχουν την καθοδήγηση της κοινής γνώμης*».[67]

Σε κάθε περίπτωση αυτό που χρήζει επισήμανσης είναι ότι ο σχεδιασμός και η υλοποίηση του, σύμφωνα με δημοσιεύματα του τουρκικού Τύπου, προήλθε από σχετική εισήγηση της Διεύθυνσης Στρατηγικής Ανάπτυξης του τουρκικού Υπουργείου Εσωτερικών σύμφωνα με την οποία «*τα ΜΚΔ πρέπει να «αξιοποιούνται ενεργά λόγω της αποτελεσματικότητας τους ιδιαίτερα κατά τις προεκλογικές περιόδους*».[68]

5.2.1. Social Bots

Η μελέτη των social bots ως game changer σε διεθνές και εθνικό επίπεδο αποτελεί ένα νέο σχετικά πεδίο έρευνας, με την Τουρκία να προσελκύει το επιστημονικό ενδιαφέρον ειδικά κατά τις περιόδους σοβαρών εσωτερικών πολιτικών εξελίξεων. Στο πλαίσιο αυτό, μια έρευνα μελέτησε τις αλληλεπιδράσεις των Social Bots συγκρίνοντας τις περιπτώσεις της Τουρκίας μετά την απόπειρα πραξικοπήματος, της Ουκρανίας κατά την αναζωπύρωση της ρωσο-ουκρανικής κρίσης και των ΗΠΑ κατά την προεκλογική περίοδο του 2016. Μια *«υπερ-κοινωνική φύση»* των bots διαπιστώνεται και στις τρεις περιπτώσεις, καθώς καταγράφεται υπεραυξημένος αριθμό tweets και retweets, σε

[65] Mustafa Cem Oğuz και Ozhan Demirkol, Networked Authoritarianism in Turkey: Jdp's Political Trolling and Astroturfing. (235-256) Στο συλλογικό βιβλίο των Chiluwa, I., & Bourvier, G. (2019). Activism, campaigning and political discourse on Twitter. https://paromitapain.com/wp-content/uploads/2019/12/Activsim-Twitter-discorse.pdf (Ανάκτηση, 30.04.2021).

[66] Ο Erdoğan κατηγόρησε ως υπεύθυνο ένα «λόμπι ρομπότ» ότι στοχεύει την κυβέρνηση μέσω Tweets, ενώ παράλληλα αρνήθηκε την αυθεντικότητα τηλεφωνικών διαρροών που αναπαρήχθησαν στην «ταραχοποιό» πλατφόρμα. Turkish PM accuses 'robot lobby' of conducting plot against the gov't, 25 Φεβρουαρίου 2014, τουρκική ε/φ Hürriyet, https://www.hurriyetdailynews.com/turkish-pm-accuses-robot-lobby-of-conducting-plot-against-the-govt-62928 (Ανάκτηση 29.04.2021).

[67] "AK Parti'den 6 bin kişilik sosyal medya ordusu" (μτφ.«Στρατός 6 χιλ. ανθρώπων από το ΑΚΡ για τα ΜΚΔ), 14 Νοεμβρίου 2013, τουρκική ε/φ Hürriyet, https://www.hurriyet.com.tr/gundem/ak-partiden-6-bin-kisilik-sosyal-medya-ordusu-25115336 (Ανάκτηση 24.04.2021).

[68] Η εισήγηση ανήκει στο Τμήμα Έρευνας και Ανάπτυξης ("Ar-Ge") της Διεύθυνσης Στρατηγικής Ανάπτυξης (Strateji Geliştirme Başkanliği) του τ/ΥΠΕΣ (İçişleri Bakanlığı).

σύγκριση με συμπεριφορά ενός πραγματικού χρήστη στα ΜΚΔ.

Τα ευρήματα της έρευνας (Schuchard et al. 2019) κατέδειξαν ότι μολονότι τα bots συνιστούν λιγότερο από το 0,3% του συνολικού πληθυσμού χρηστών, εμφανίζουν ένα δυσανάλογο υψηλό επίπεδο επιρροής στα ΜΚΔ, συγκρίσιμο ακόμη και με λογαριασμούς των πλέον ενεργών χρηστών. Η έρευνα των μελετά την περίοδο του Δεκεμβρίου 2016, μετά δηλαδή την απόπειρα πραξικοπήματος κατά της κυβέρνησης[69] όπου απαγορεύεται η χρήση του TW μετά από δύο γεγονότα α) τη δημόσια δολοφονία του Ρώσου Πρέσβη στην Τουρκία (19.12.16) και β) την κυκλοφορία ενός βίντεο που δείχνει δύο Τούρκους στρατιώτες να καίγονται ζωντανοί (23.12.16). Ο πίνακας που ακολουθεί (Πίνακας 12) καταδεικνύει ότι τα bots σημειώνουν σχεδόν πενταπλάσια δραστηριότητα μέσω tweets/retweets σε σχέση με τους πραγματικούς χρήστες.
Δηλαδή κατά μέσο όρο και σε χρονική περίοδο τριάντα ημερών:

- ένας πραγματικός χρήστης έκανε 7,36 tweets και ένα 1,46 retweet, ενώ
- ένας λογαριασμός bot παρήγαγε 33,88 tweets και 6,81 retweets.

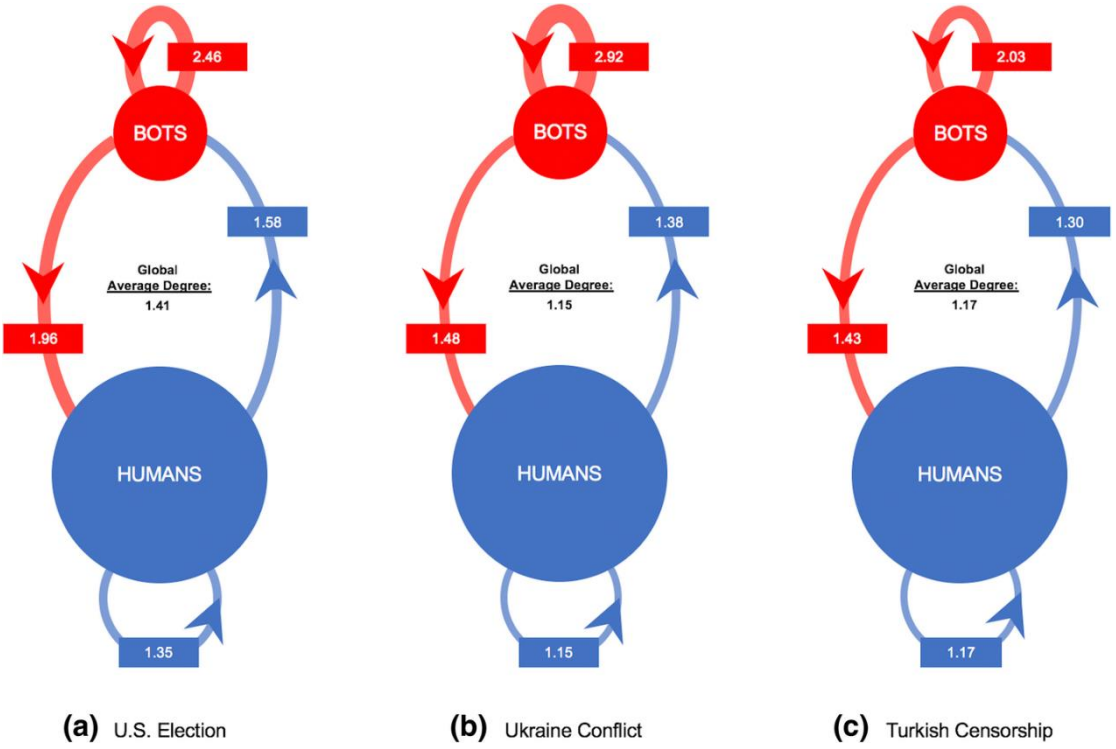
Πίνακας 12 Αναλογία Tweets & Retweets/ανά χρήστη και Bot

Χρονικό Διάστημα (1-31/12/2016) **Αναλογία Tweets/χρήστη Retweets/χρήστη ≠ Tweets/Bot Retweets/Bot**			
Εβδομάδες		**Tweets/χρήστη**	**Retweets/χρήστη**
1η εβδ.	Πραγματικός χρήστης	**2,32**	**1,44**
	BOTS	**9,64**	**6,32**
2η εβδ.	Πραγματικός χρήστης	**2,18**	**1,44**
	BOTS	**10,11**	**6,72**
3η εβδ.	Πραγματικός χρήστης	**2,33**	**1,63**
	BOTS	**11,77**	**7,80**
4η εβδ.	Πραγματικός χρήστης	**2,15**	**1,34**
	BOTS	**9,46**	**6,43**
Επί συνόλου Πραγμ. Χρηστών		**3,03**	**1,99**
Επί συνόλου Bots		**22,41**	**14,92**

Πηγή: Συντάκτης (από επεξεργασία στοιχείων έρευνας Schuchard et al. 2019)

[69] Λέξεις-κλειδιά για tweets με Turkey, Türkiye, Turkish, Erdogan, Erdoğan, Turkeycoup, Erdoganblockedtwitter Erdoganblockstwitter, Twitterisblockedinturkey, Resisttwitter.

Οι ερευνητές επίσης συγκρίνοντας τις αμερικανικές εκλογές, την ουκρανική κρίση και την τουρκική λογοκρισία, κατέληξαν ότι τα bots εμφανίζουν μεγαλύτερη αλληλεπίδραση (Γράφημα 1) εντός ομάδων bots (in-group) και μεταξύ bot με πραγματικούς χρήστες (cross-group). Επίσης, η δραστηριότητα των bots καθ' όλη την περίοδο, παρέμεινε συστηματική και στις περισσότερες περιπτώσεις παρά το μικρό αριθμό τους, συνέβαλε εξίσου ή και περισσότερο με τη δραστηριότητα των πραγματικών χρηστών:

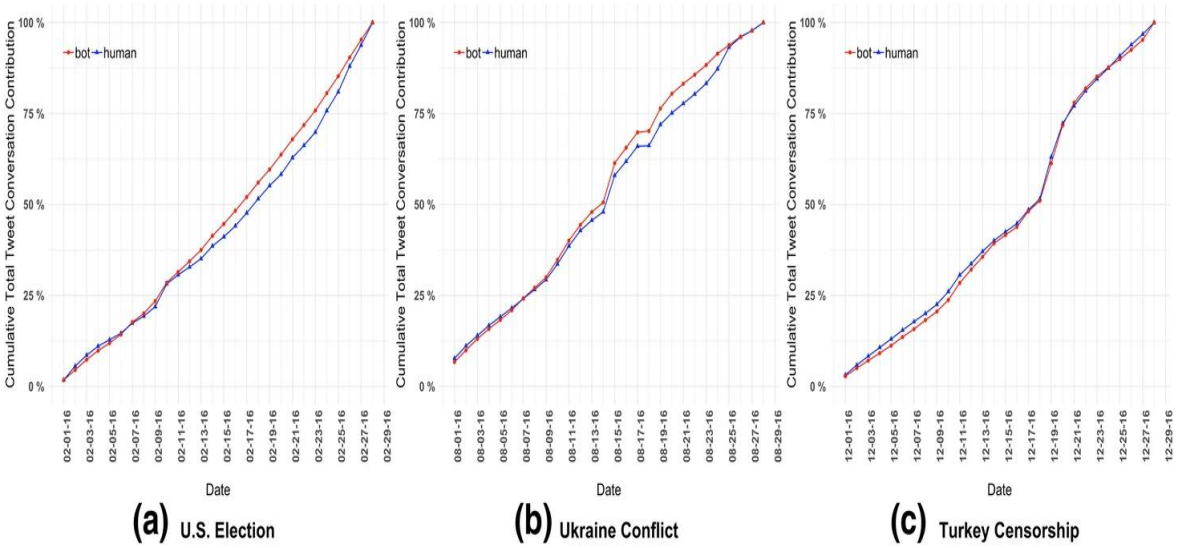


Γράφημα 1 In-group and cross-group retweet communication

Πηγή: Schuchard et al. 2019

Τέλος, σε σχέση με τα αθροιστικά ποσοστά συνεισφοράς των tweets από πραγματικούς ανθρώπους και bot, στην περίπτωση των ΗΠΑ και της Ουκρανίας Γράφημα 2) απεικονίζεται ένα χάσμα μεταξύ ποσοστών συνεισφοράς bot και χρήστη που αρχίζει να διευρύνεται περίπου στις 2 εβδομάδες, ενώ τείνει να κλείσει στις τελευταίες ημέρες. Ωστόσο, στην περίπτωση της τουρκικής λογοκρισίας δεν εντοπίζεται αυτό το χάσμα (Γράφημα 2), ενώ η αρχική της πορεία συνομιλίας είναι πολύ πιο ρηχή έως ότου πραγματοποιηθεί μια αύξηση των συνεισφορών των bots που αντιστοιχεί στην έναρξη του πρώτου γεγονότος λογοκρισίας στην Τουρκία (19.12.2016).

Αυτή η τελευταία αύξηση της συνεισφοράς, σε συνδυασμό με χαμηλότερους συνολικούς όγκους tweet/retweet από τα bots μπορεί να είναι ενδεικτική των συζητήσεων καταγγελιών περί τουρκικής λογοκρισίας από την τουρκική κυβέρνηση κατά την περίοδο της έρευνας, σε αντίθεση με την ήδη καθιερωμένη συζήτηση για τις εκλογές ή για την Ουκρανία (Schuchard et al. 2019). Επιχειρώντας μια πολιτική ερμηνεία, η αυτοσυγκράτηση (μη-χάσμα) σε ό,τι αφορά τα bot/χρήστες μπορεί να είναι ενδεικτική της ετοιμότητας της τουρκικής κυβέρνησης να «ελέγχει» άμεσα την όποια μυστική δραστηριότητα των bots, ιδιαίτερα όταν αυτή μπορεί να είναι μετρήσιμη από εξωτερικούς παράγοντες λόγω επικαιρότητας.

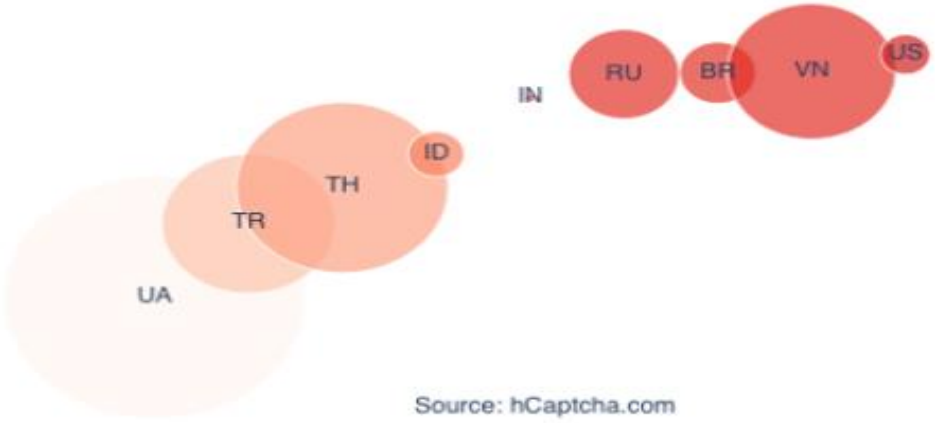


Γράφημα 2 Cumulative total tweet contributions over Twitter conversation span

Πηγή: Schuchard et al. 2019.

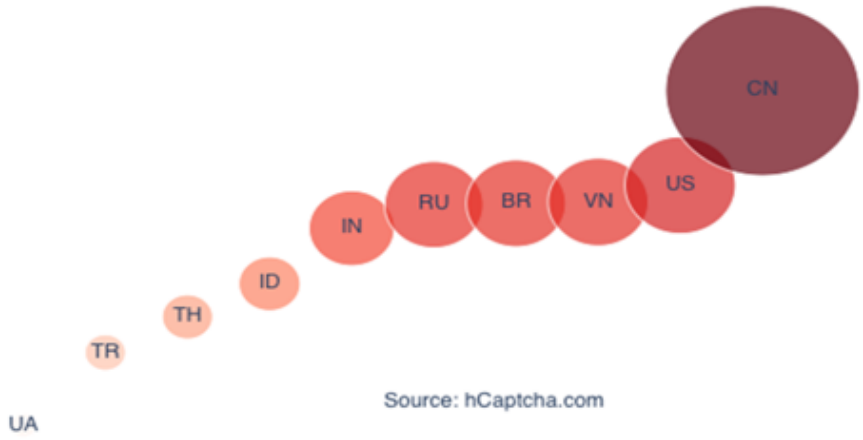
Η ανωτέρω μελέτη αν και καλύπτει μια συγκεκριμένη περίοδο είναι ενδεικτική του ρόλου των social bots στη ψηφιακή εκστρατεία επικοινωνίας της Τουρκίας μέσω ΜΚΔ, την οποία εφαρμόζει συστηματικά με αποτέλεσμα να συγκαταλέγεται για το 2019[70] στη δεύτερη θέση παγκοσμίως μετά την Ταϊλάνδη (Γράφημα 3) σε σχέση με τον πληθυσμό της, ενώ καταλαμβάνει την ένατη θέση παγκοσμίως μετά από Κίνα, ΗΠΑ, Ρωσία (Γράφημα 4).

[70] Το 2019 ήταν έτος τοπικών εκλογών, παρεμβάσεων στη δικαστική εξουσία, εισβολής τουρκικών στρατευμάτων στη Συρία, «δικαστικών μεταρρυθμίσεων», αποκλεισμού ιστοτόπων και διαγραφής διαδικτυακού περιεχομένου, διεξαγωγής ποινικών ερευνών, διώξεων χιλιάδων χρηστών λόγω αναρτήσεων στα ΜΚΔ. World Report 2020, Human Rights Watch, https://www.hrw.org/world-report/2020/country-chapters/turkey (Ανάκτηση, 30.04.2021).



Γράφημα 3 December 2019 Top Bad Actor Countries (Normalized by Population)

Εικ. (Πηγή: hCaptcha.com)



Γράφημα 4 December 2019 Top Bad Actor Countries

Πηγη: hCaptcha "Which countries have the most bot traffic? (2019)" [71]

5.2.2. AK Trolls - Astroturfers

Το ΑΚΡ φέρεται να ξεκίνησε να χρησιμοποιεί τα "AK Trolls"[72] και το astroturfing ήδη

[71] https://medium.com/@hCaptcha/which-countries-have-the-most-bot-traffic-2019-dcb399f2c333 (Ανάκτηση 29.04.2021).

[72] Στην τουρκική γλώσσα AK Troller, Aktroller.

από το 2013 (Saka, 2018 & Irak, 2016), επιχειρώντας αφενός παγίωση της πολυετούς διακυβέρνησης από το 2003 και αφετέρου εποπτεία αντιπολιτευτικών δράσεων. Η Τουρκία, σε αντίθεση μ' άλλα καθεστώτα που απαγορεύουν πλήρως την πρόσβαση των πολιτών στα ΜΚΔ:

(α) *προσδίδει στη χρήση των ΜΚΔ μια επίφαση ελευθερίας έκφρασης και συζήτησης* θεμάτων στις πλατφόρμες, ωστόσο οι συνομιλίες παρακολουθούνται ή «ακολουθούνται» και ελέγχονται από trolls ή astroturfers υπό την ιδιότητα followers ή φίλων,

(β) *χρησιμοποιεί τα trolls ως μέσο προώθησης της πολιτικής ατζέντας,* με ένα ενδεικτικό παράδειγμα τη συνομιλία της θυγατέρας Erdoğan με τον τότε σύμβουλο του Προέδρου και νυν υπουργό Βιομηχανίας και Τεχνολογίας Mustafa Varank, από τον οποίο ζητείται υποστήριξη *από «τα troll μας»* ("trollerimize"),[73]

(γ) *ασκεί πιέσεις στις πλατφόρμες,* όποτε κρίνει απαραίτητο *λ.χ. στο TW για να καταργήσει λογαριασμούς* (Oğuz & Demirkol, 2019), οι οποίοι αναπαρήγαγαν υλικό από υποκλαπείσες τηλεφωνικές συνομιλίες που αποδείκνυαν κυβερνητική διαπλοκή σε σκάνδαλα διαφθοράς.[74]

Σταδιακά καθιερώνεται ο όρος "AKTrolls" με μισθούς να κυμαίνονται από 800 και 4000 TL. Παράλληλα, και σύμφωνα με δημοσιεύματα του Τύπου, φέρεται να ιδρύεται πριν τις εκλογές του 2015 το «Ψηφιακό Γραφείο Νέας Τουρκίας (Yeni Türkiye Digital Ofisi – YTDO)», του οποίου η στελέχωση αριθμεί 200 υπαλλήλους με αρμοδιότητα δημιουργίας και ελέγχου περιεχομένου σε ΜΚΔ στο πλαίσιο υλοποίησης σχεδιασμού που αφορούσε σε «περιεχόμενο με δεκάδες χιλιάδες tweets, αναρτήσεις στο FB και blog», τα οποία εντάσσονται στην επικοινωνιακή στρατηγική «*αυτοί μιλούν* (Σ.Σ.: εννοεί αντιπάλους), *το ΑΚΡ πράττει*».[75] Στον αντίποδα μιας «εξευγενισμένης» επικοινωνιακής πολιτικής όπως προβάλλεται από το ΑΚΡ, οι Bulut & Yörük αναφέρονται στο trolling στην Τουρκία ως εργαλείο πολιτικού λιντσαρίσματος και δη *«χειραγώγησης, προσβολής, συκοφαντίας και πόλωσης»* (Bulut & Yörük, 2017).

---

[73] Başbakanın Kızı Sümeyye Mustafa Varank Ses Kaydı Çıktı https://www.youtube.com/watch?v=c0MYM_KK33Y (Ανάκτηση 05.05.2021).

[74] Αφορούν ηχογραφημένες συνομιλίες του Erdoğan με τον υιό του, στον οποίο δίνει εντολές για τη φύλαξη χρημάτων κατά τη διάρκεια ελέγχου σκανδάλου διαφθοράς της κυβέρνησης.

[75] "AK Party founded New Turkey Digital Office for the general elections on June 7". 11 Μαΐου 2015. The Daily Sabah. https://www.dailysabah.com/elections/2015/05/11/ak-party-founded-new-turkey-digital-office-for-the-general-elections-on-june-7 (Ανάκτηση 03.05.2021).

Πέραν των δημοσιευμάτων και μεμονωμένων δηλώσεων Τούρκων αξιωματούχων, επίσημα στοιχεία σχετικά με τις ψηφιακές στρατηγικές του ΑΚΡ και τυχόν διασυνδέσεών του με τα AK Trolls δεν υφίστανται. Ωστόσο έχουν διεξαχθεί έρευνες και από τις αναλύσεις δικτύων με λογαριασμούς AKTrolls, έχει εξεταστεί ο βαθμός της μεταξύ τους διασύνδεσης και οι αλληλεπιδράσεις με κομματικά στελέχη. Ο λογαριασμός που διερευνήθηκε -πλέον παυθείς- ανήκει στο χρήστη Esad Ç @esatreis ο οποίος βρισκόταν στο κέντρο των αλληλεπιδράσεων.[76] Από την ανάλυση του δικτύου προέκυψαν δύο διαφορετικές ομάδες:

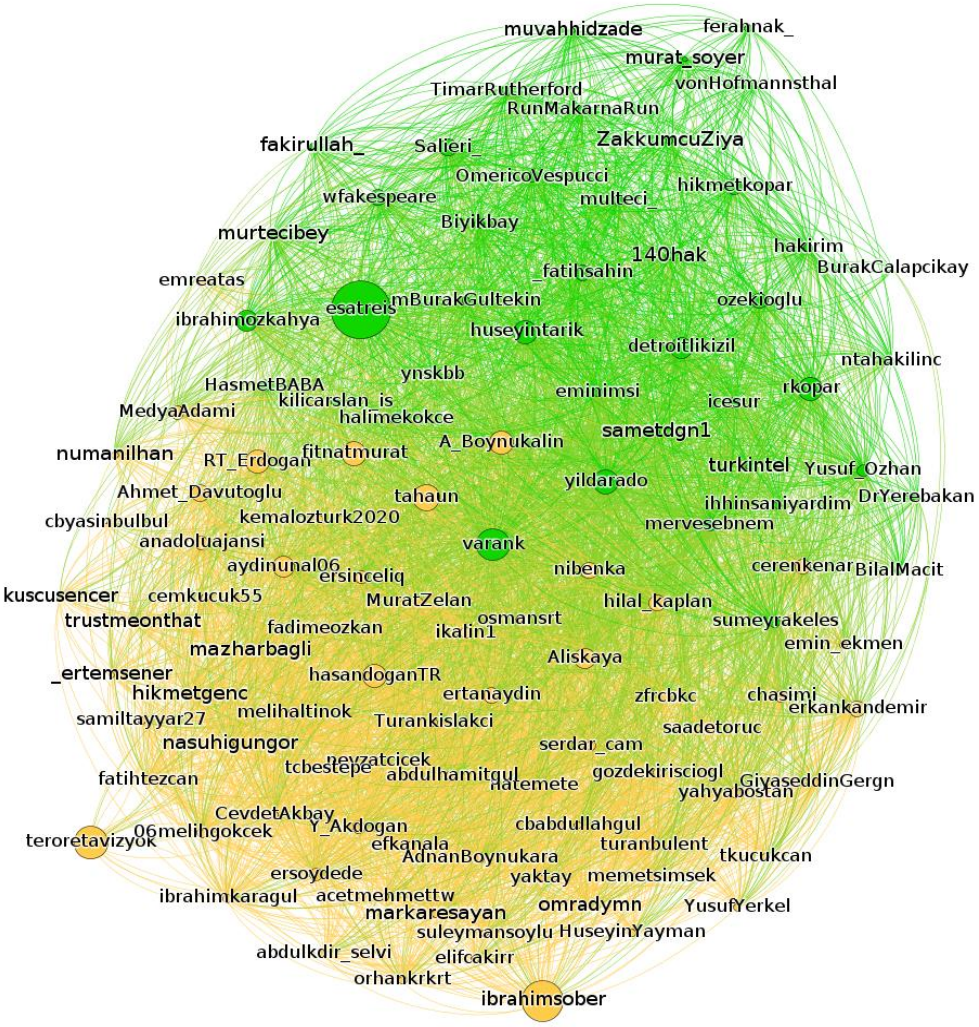
(α) Πραγματικοί λογαριασμοί πολιτικών ΑΚΡ, υπουργών, φιλοκυβερνητικών δημοσιογράφων, συμβούλων και του Mustafa Varank @varank, ο κόμβος του οποίου εμφανίζεται ως γέφυρα[77] μεταξύ των επισήμων λογαριασμών μελών του ΑΚΡ και των

(β) Trolls που παράγουν περιεχόμενο για το ΑΚΡ.

Από το γράφο που απεικονίζεται παρακάτω, το σημαντικότερο για τους ερευνητές εύρημα δεν συνδέεται με την ταυτοποίηση των κόμβων, αλλά με τη διαπίστωση δεσμών μεταξύ κόμβων-λογαριασμών AK Trolls με επίσημους χρήστες -κόμβους του ΑΚΡ.

[76] Η μελέτη της οργάνωσης Hafıza Kolektifi δεν κατέστη δυνατό να εντοπιστεί, παρά μόνο αποσπασματικά σε δημοσιεύματα της εποχής. «Τα AK trolls χαρτογραφήθηκαν: ο σύμβουλος του Erdoğan Varank βρίσκεται στο κέντρο» (“Ak Trol’lerin haritası çıkarıldı: Merkezde Erdoğan’ın danışmanı Varank var”. https://www.diken.com.tr/ak-trollerin-haritasi-cikarildi-merkezde-erdoganin-danismani-varank-var/ (Ανάκτηση 03.05.2021).

[77] Στη θεωρία των γράφων με τη μετρική του closeness centrality του κόμβου, φαίνεται πόσο σημαντικός είναι ο κόμβος του Varank από τον οποίο ξεκινούν μονοπάτια προς τους υπόλοιπους κόμβους μέσα στο συνδεδεμένο γράφο με τα μέλη του ΑΚΡ – Trolls.



Γράφημα 5 Γράφος Δικτύου AKTrolls και Επίσημων Λογαριασμών στελεχών ΑΚΡ

Πηγή: https://www.diken.com.tr/ak-trollerin-haritasi-cikarildi-merkezde-erdoganin-danismani-varank-var/

Modus operandi: **#hashtags, memes και posts** χρησιμοποιούνται για τη δημιουργία περιεχομένου. Τις περισσότερες φορές τα hashtags είναι γεωγραφικά στοχευμένα, δηλαδή ανάλογα με την επαρχία της Τουρκίας και των έργων που έχουν πραγματοποιηθεί ή σχεδιάζονται να υλοποιηθούν από το ΑΚΡ στην περιοχή, προκειμένου να εξασφαλίσουν λαϊκή βάση (Oğuz & Demirkol, 2019). Επίσης, τα trolls επιχειρούν να καθιερώσουν trending topics, ειδικά όταν αυτά σχετίζονται είτε με την προβολή του Erdoğan σε εθνικό και διεθνές επίπεδο ή την προώθηση τουρκικών θέσεων ή αντιδράσεων στις διεθνείς εξελίξεις με πλέον πρόσφατο παράδειγμα την αναγνώριση της αρμενικής γενοκτονίας από τον Αμερικανό Πρόεδρο (24.04.2021) και τη δημιουργία συναφών #hashtags όπως #ArmenianLies #ErmeniSoykırımıYalandır (Η γενοκτονία των Αρμενίων είναι ψέμα) #1915Olayları (Γεγονότα του 1915, 1η θέση) #OttomanEmpire #Ermeni #StopArmenianLies.

Στοχοποίηση δημοσιογράφων: Τούρκων ή αλλοδαπών. Τα trolls χρησιμοποιούν προσβλητικά hashtag ή ρητορική μίσους (hate speech), χαρακτηρίζοντας τους αντιφρονούντες δημοσιογράφους ως προδότες, τρομοκράτες, σιωνιστές ή συνεργάτες ξένων υπηρεσιών, με πλέον χαρακτηριστική την περίπτωση του Τούρκου αυτοεξόριστου δημοσιογράφου Abdullah Bozkurt, ο οποίος έχει κατηγορηθεί επανειλημμένως για συνεργασία με τη CIA, MOSSAD, FSB[78] ή του Αμερικανού Διεθνολόγου στο Council on Foreign Relations - CFR, Steven A. Cook.[79] Στη συγκεκριμένη πρακτική φέρεται εμπλεκόμενη και η τουρκική Υπηρεσία Πληροφοριών (MİT), υπό την καθοδήγησή της οποίας φαίνεται να λειτουργούσε ομάδα troll για εκφοβισμό ξένων και Τούρκων δημοσιογράφων.[80]

Wikipedia & Ιστότοποι: Η συγκεκριμένη ομάδα φαίνεται επίσης να διευρύνει τις δραστηριότητες σε πλατφόρμες συνεργατικής συγγραφής όπως το Wikipedia, δημοσιεύοντας παραποιημένες πληροφορίες. Επίσης, στα AKTrolls αποδίδεται και η κατασκευή ιστοσελίδων, συνήθως προσώπων που δεν ανήκουν στο χώρο του AKP, προκειμένου να παραπλανούν τους επισκέπτες και να συγκεντρώνουν στοιχεία από την επικοινωνία τους με τον κλωνοποιημένο – αποδέκτη ιδιοκτήτη της ιστοσελίδας.[81]

Hacking λογαριασμών ΜΚΔ η τουρκική ομάδα χάκερ "Ayyildiz Tim" που συνδέεται με το βαθύ κράτος, έχει κατά καιρούς στοχοποιήσει λογαριασμούς ΜΚΔ Αμερικανών δημοσιογράφων έγκριτων ΜΜΕ όπως Bloomberg, NYT και Fox News, προκειμένου να αναρτηθούν μηνύματα υπέρ της Τουρκίας ή του Erdoğan.[82] Η πρακτική αυτή εφαρμόζεται και στο εσωτερικό της χώρας, όπου μέσω λογαριασμών με κοσμικό χαρακτήρα και κοινό, σε αντίθεση με του AKP, επιχειρούν προσέγγιση εκλογικής βάσης άλλων κομμάτων (Saka, 2018).

Πολυγλωσσία για κινητοποίηση και «ενημέρωση» χρηστών εκτός Τουρκίας (Saka,

[78] https://twitter.com/abdbozkurt/status/1013818694399651840 (Ανάκτηση 05.05.2021).
[79] https://twitter.com/stevenacook/status/759009022376681472 (Ανάκτηση 05.05.2021).
[80] Abdullah Bozkurt, Exposing the generals in Erdoğan's troll army. 24 Ιανουαρίου 2019. Nordic Monitor. https://nrdc.wpengine.com/2019/01/exposing-generals-in-erdogans-troll-army/ (Ανάκτηση 03.05.2021)
[81] Ο ιστότοπος www.abdullahbozkurt.eu ξεκίνησε να λειτουργεί από το 2019 εμφανίζοντας τον φερώνυμο δημοσιογράφο ως διαχειριστή, ωστόσο ο ιστότοπος ελέγχεται από τρίτους. Abdullah Bozkurt, Turkey's disinformation campaign through trolls and bots in the assassination of Russian ambassador exposed. 9 Ιανουαρίου 2021. Nordic Monitor. https://nordicmonitor.com/2020/06/11796/ (03.05.2021).
[82] https://cisomag.eccouncil.org/turkish-hacktivists-take-over-twitter-accounts-of-u-s-journalists/

2018). Τα μηνύματα των AKTrolls στην αγγλική, αποσκοπούν στη «νομιμοποίηση» των τουρκικών ενεργειών και την προβολή των θέσεων της στο διεθνές προσκήνιο, με πλέον πρόσφατα παραδείγματα (Πίνακας 13) την εισβολή στη Συρία («Πηγή της Ειρήνης» - Barış Pınarı Harekâtı), την εργαλειοποίηση του προσφυγικού (03/2020) και την προβολή της Ελλάδας ως «θύτη» με το δημοφιλές #GreeceAttacksRefugees, στη χρήση του οποίου κατέφυγε και ο Τούρκος ΥπΕΞ στο λογαριασμό του (Πίνακας 14).[83]

Πίνακας 13 Tweets με trending hashtags επί θεμάτων Εξωτερικής Πολιτικής

ΘΕΜΑ	#hashtags	Tweets
Συρία	**#TurkeyJustKilledTerrorists** #TurkishArmyForThePeace #NoOneCanDivideTurkey #kurdssidewithturkey #OurVoiceErdogan #TurkeyisnotAlone	Our country is determined to clean the areas that are adjacent to our borders from Deash and YPG/PKK, which is exactly the same as the former.[84]
Ελλάδα	**#GreeceKillingRefugees** **#GreeceAttacksRefugees** #IStandWithTheSyrianRefugees #OpenBorders2Refugees #MassacreInGreekBorder #EuropeTheBarbarian	Greek refugees who took refuge in Syria in 1942! Shame on you Greece...[85] After July 2016 coup attempt, Greece opened their borders fully and welcomed #Fetö/#Gulen terrorists and took them in. And now Greece is killing refugees who are running away from Assad's murder.[86]

Πηγή: Συντάκτης

[83] https://twitter.com/MevlutCavusoglu/status/1235633777365393413 (Ανάκτηση, 08.05.2021).
[84] https://twitter.com/metinarpac04/status/1194704618103721986 (Ανάκτηση, 08.05.2021).
[85] https://twitter.com/eserekli61/status/1234949992646877190 (Ανάκτηση, 08.05.2021).
[86] https://twitter.com/DenizUcin/status/1235437996557709312 (Ανάκτηση, 08.05.2021).

Πίνακας 14 Tweet Τούρκου ΥπΕξ με χρήση #GreeceAttacksRefugees

Ψηφιακός λαϊκισμός: Η γλώσσα επικοινωνίας των trolls χαρακτηρίζεται από δυναμικά χαρακτηριστικά λαϊκισμού, τα οποία προκαλούν διάσπαση στις πολιτικές συζητήσεις και παγιώνουν την εξουσία του ΑΚΡ πετυχαίνοντας να «δικτυώσουν» διάσπαρτες μάζες ψηφοφόρων από την φιλελεύθερη αριστερά (CHP) μέχρι την κεμαλική ακροδεξιά (MHP) (Bulut & Yörük, 2017).

TW vs FB: η διαφορά μεταξύ των δύο για τα trolls έγκειται στο γεγονός ότι στο TW μπορούν να επηρεάσουν την εθνική ατζέντα, θέτοντας ακόμη και θέματα που δεν υπάρχουν (astroturfing), προκειμένου να ανταποκριθεί το κόμμα στην υποτιθέμενη λαϊκή βούληση, σε αντίθεση με το FB όπου απλώς μπορούν να σχολιάσουν.

Νομοθετικό πλαίσιο: Με τροποποιητική διάταξη αναθεώρησε το ν.5651 που αφορά τέλεση εγκλημάτων μέσω διαδικτύου. Ο αναθεωρημένος νόμος διευρύνει το πεδίο κρατικής παρέμβασης στα ΜΚΔ, υποχρεώνοντας τις πλατφόρμες που έχουν πάνω από ένα εκατομμύριο χρήστες να ανοίξουν υποκαταστήματα στη χώρα, ενώ σε περίπτωση άρνησής τους προβλέπεται μείωση έως και 95% του εύρους διάδοσης του περιεχομένου ή και επιβολή προστίμων για «αμφιλεγόμενες» πληροφορίες.

Καταληκτικά, τα ανωτέρω επιβεβαιώνουν ότι τα ΜΚΔ συνιστούν ένα πεδίο άσκησης

πολιτικής για το ΑΚΡ, μέσω του οποίου δύναται να διαδίδει ψευδείς ειδήσεις που αφορούν εξελίξεις με αποδέκτες στο εσωτερικό ή εξωτερικό και να αναπαράγει περιεχόμενο υπέρ του Erdoğan και κατά των αντιπάλων του. Στην επικοινωνιακή αυτή εκστρατεία έχει εξαναγκάσει σε «συστράτευση» τις εταιρείες ΜΚΔ με πρόσχημα την «προσβολή προσωπικότητας», κ.ά. Σε επίπεδο χρηστών μέσω του εκφοβισμού έχει επιτύχει την αυτολογοκρισία τους. Από την άλλη πλευρά, bots, trolls και astroturfers έχουν διαμορφώσει μια ψευδαίσθηση δημοτικότητας του Τούρκου Προέδρου ή μιας επίπλαστης «κατασκευαστικής συναίνεσης» (Wooley, 2019), παράλληλα όμως η λειτουργία τους αποδεικνύει το μέγεθος χειραγώγησης της κοινής γνώμης μέσω ΜΚΔ στην Τουρκία.

Σε κάθε περίπτωση, είναι προφανές ότι η άσκηση προπαγάνδας μέσω ΜΚΔ επιφέροντας σημαντικά και υπολογίσιμα αποτελέσματα στην πολιτική διακυβέρνηση του ΑΚΡ, καταδεικνύει περίτρανα ότι η δυνατότητα εκδήλωσης αντίδρασης από την κοινωνία πολιτών μέσω των ΜΚΔ με σκοπό να παρακαμφθεί η κρατική λογοκρισία, έχει πλέον εξαλειφθεί.

Κεφάλαιο 6
Ερωτηματολόγιο: Παρουσίαση Αποτελεσμάτων

Σκοπός εργασίας είναι η κατάρτιση μιας τυποποιημένης διαδικασία λειτουργίας SOP η οποία θα διευκολύνει τους αναλυτές πληροφοριών ΥΠ στη συλλογή, επεξεργασία, αξιολόγηση και επαλήθευση πληροφοριών που προέρχονται από τα ΜΚΔ. Στο πλαίσιο αυτό στα προηγούμενα κεφάλαια έγινε μια σύντομη παρουσίαση των ΜΚΔ, των ειδών παραπληροφόρησης και ακολούθησε μια μελέτη περίπτωσης για την Τουρκιά, ως χώρα ενδιαφέροντος για Ελλάδα και Κύπρο, που επιδεικνύει συστηματική και θεσμοθετημένη δραστηριοποίηση στα ΜΚΔ. Η μελέτη περίπτωσης έγινε με σκοπό να χαρτογραφηθούν οι βασικές παράμετροι που η διαδικασία πρέπει να συμπεριλάβει. Στο κεφάλαιο αυτό, κρίθηκε σκόπιμη η χρήση ενός ερωτηματολογίου για να καταγράψει τις απόψεις των αναλυτών πληροφοριών σε σχέση με τις προτιμήσεις ΜΚΔ, την αξιολόγηση κριτηρίων, το βαθμό εμπιστοσύνης, την καταγραφή προβλημάτων και τις λύσεις που οι ίδιοι προτείνουν για τη χρήση του SOCMINT.

Η δειγματοληψία και η ανάλυση λαμβάνουν υπόψη τις απαντήσεις σε ανώνυμο ερωτηματολόγιο (ΠΑΡΑΡΤΗΜΑ Α') στην αγγλική γλώσσα με τίτλο "Social Media Intelligence (SOCMINT) | Usage Questionnaire", που δημιουργήθηκε με ειδικό λογισμικό διαχείρισης ερευνών (Google Forms) και διανεμήθηκε με κοινοποίηση συνδέσμου σε ορισμένο αριθμό αποδεκτών σε Ευρώπη, Β. Αμερική και Μ. Ανατολή, οι οποίοι έχουν εξοικείωση με τη συλλογή πληροφοριών από ανοικτές πηγές OSINT και συγκεκριμένα από το SOCMINT. Λόγω της ιδιαιτερότητας του υπό διερεύνηση θέματος, το τελικό δείγμα αριθμεί συνολικά 17 συμμετέχοντες, άνδρες και γυναίκες από Ευρώπη και Β. Αμερική, οι οποίοι συμπλήρωσαν το ερωτηματολόγιο κατά το διάστημα 28.4-

7.5.2021.

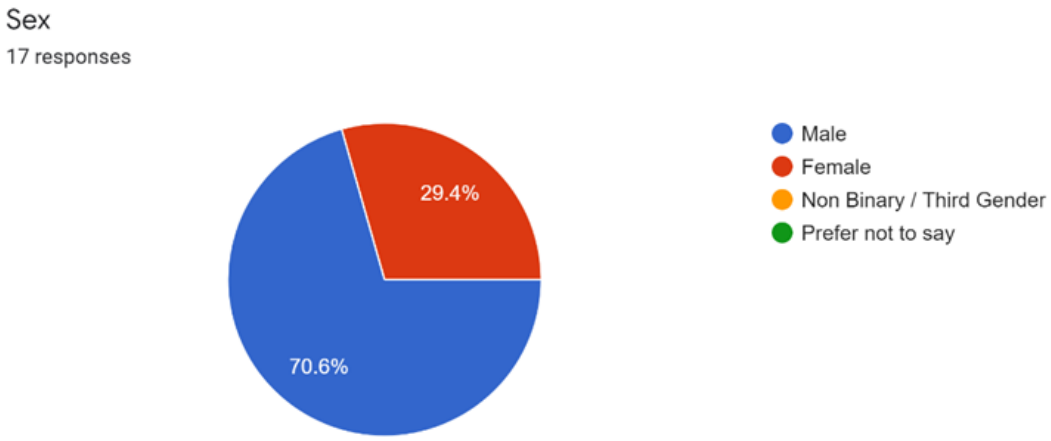
Στόχος του ερωτηματολογίου είναι η συλλογή δεδομένων σχετικά με το SOCMINT ως μέσο εξόρυξης πληροφοριών από επιτελείς πληροφοριών σε ΥΠ και διακρίνεται σε τέσσερα (4) μέρη:

(1) Δημογραφικά Δεδομένα,
(2) Συλλογή Πληροφοριών,
(3) Συμπεριφορά Χρήστη κατά τη διάρκεια συλλογής και αξιοποίησης πληροφοριών (πληροφοριακά κενά, προβλήματα, αισθήματα),
(4) Αξιολόγηση Εμπειρίας Χρήστη με το SOCMINT.

Η παρουσίαση των αποτελεσμάτων από τη συμπλήρωση του ερωτηματολογίου, παρουσιάζονται με γραφήματα, τα οποία φιλοξενούνται στην υποενότητα που ακολουθεί (6.1).

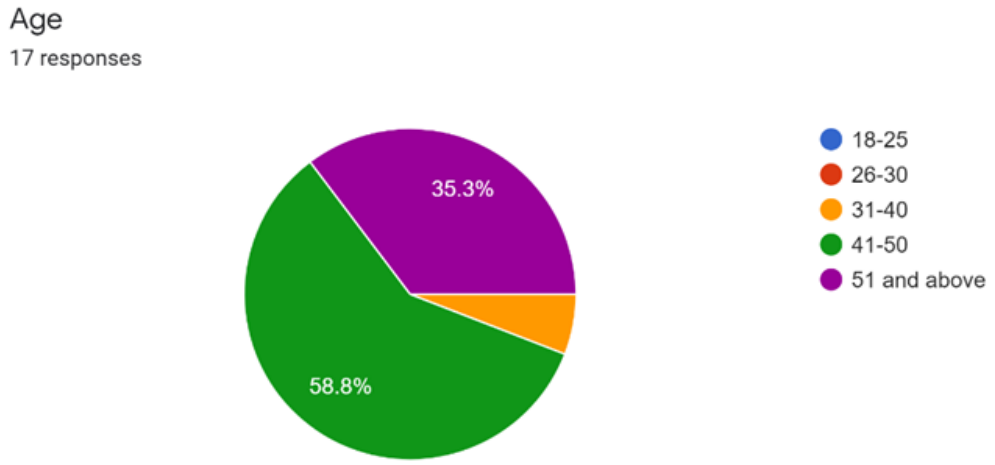
6.1. Παρουσίαση Αποτελεσμάτων

Το δείγμα των συμμετεχόντων στην παρούσα έρευνα λόγω του αντικειμένου που εξετάζεται είναι συγκεκριμένο και αποτελείται από 17 άτομα. Ακολούθως, παρουσιάζονται τα αποτελέσματα σε γραφήματα και πίνακες, με σκοπό να εξαχθούν συμπεράσματα και να επιλυθούν τα ερευνητικά ερωτήματα της παρούσας μεταπτυχιακής διατριβής.



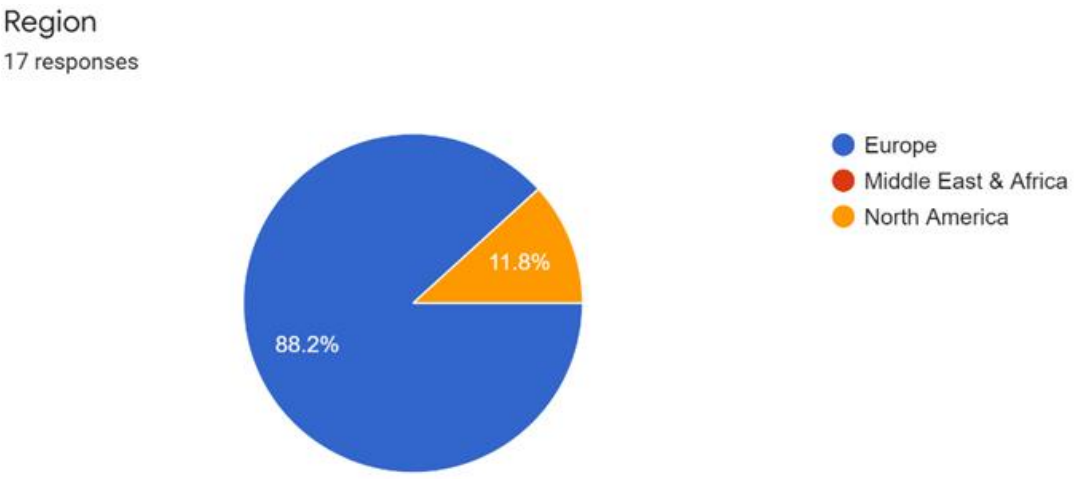
Γράφημα 6 Κατανομή Φύλων

Όσον αφορά στο φύλο των συμμετεχόντων, οι άνδρες ήταν περισσότεροι από τις γυναίκες με ποσοστό 70.6% και 29.4% αντίστοιχα (12 άνδρες και 5 γυναίκες).



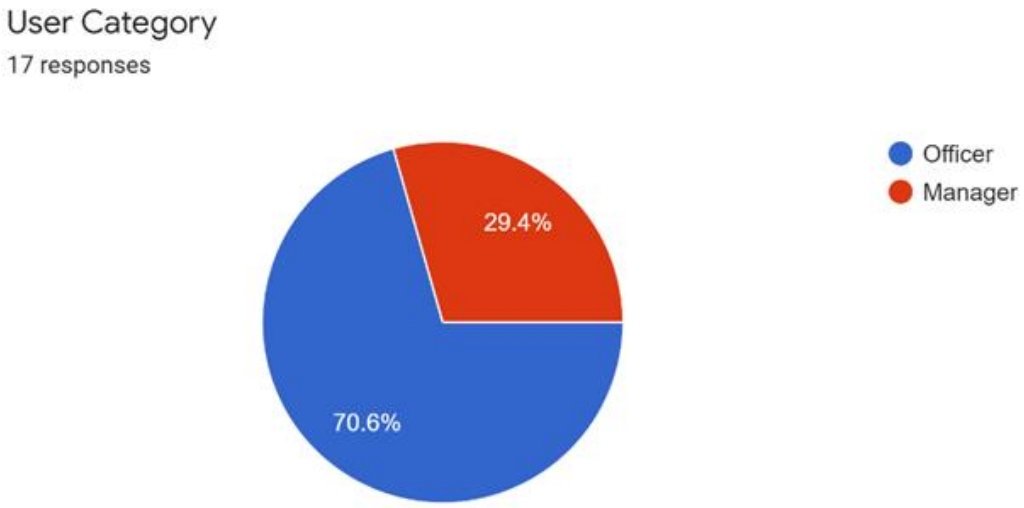
Γράφημα 7 Ηλικιακή Ομάδα

Από το ανωτέρω γράφημα, διαφαίνεται ότι η ηλικιακή ομάδα 41-50 ετών, είναι η πλειοψηφία του δείγματος, με ποσοστό 58.8% (10 άτομα). Ακολουθεί η ηλικιακή ομάδα 51 και άνω με ποσοστό 35.3% (6 άτομα) και τέλος η ηλικιακή ομάδα μεταξύ 31-40 ετών (1 άτομο).



Γράφημα 8 Γεωγραφική Κατανομή

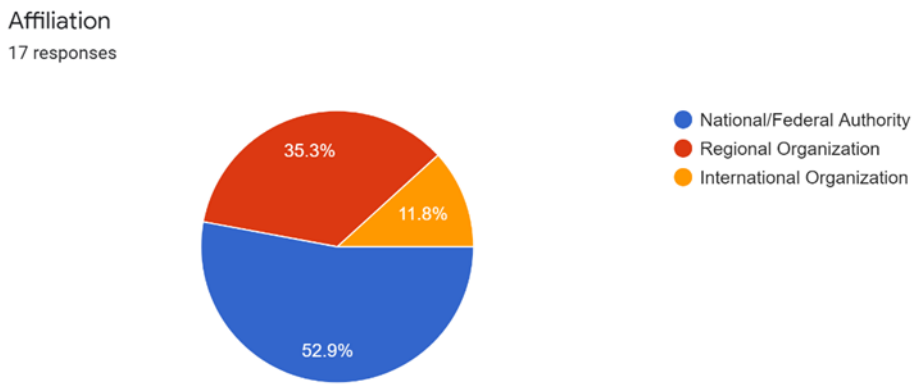
Αναφορικά με τη γεωγραφική κατανομή του δείγματος, η πλειοψηφία του δείγματος προέρχεται από την Ευρώπη με ποσοστό 88.2% (15 άτομα) και ακολουθεί η Β. Αμερική με 11.8% ποσοστό συμμετοχής (2 άτομα). Το ερωτηματολόγιο διακινήθηκε και σε αποδέκτες χωρών στη Μ. Ανατολή, ωστόσο δεν συμπληρώθηκε.



Γράφημα 9 Ιδιότητα Χρήστη

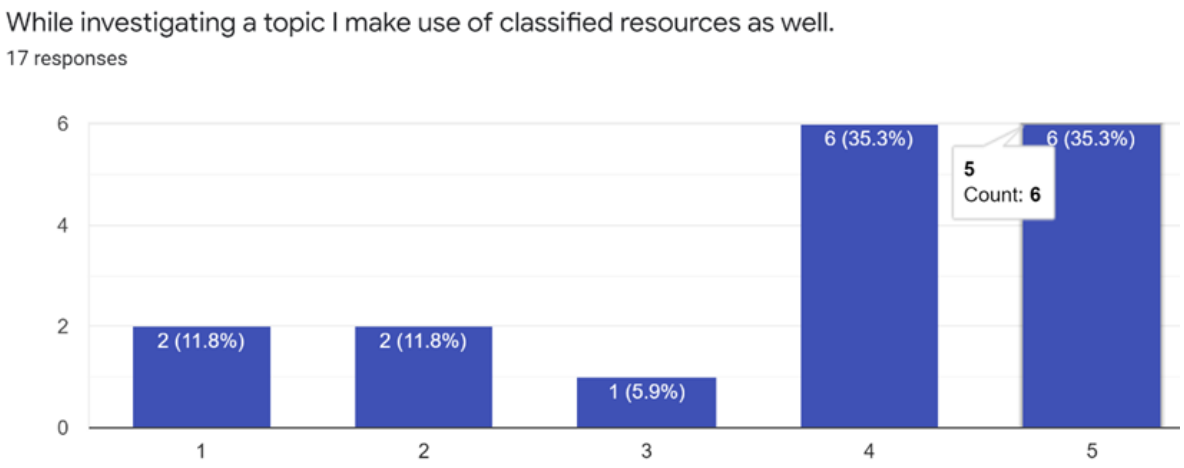
Αναφορικά με την ιδιότητα των συμμετεχόντων στην έρευνα, το 70.6% (12 άτομα)

απάντησαν ότι είναι επιτελείς πληροφοριών (intelligence officer), ενώ το 29.4%, (5 άτομα) κατέχουν θέση ευθύνης (προϊστάμενος – manager).



Γράφημα 10 Affiliation

Από το ανωτέρω γράφημα προκύπτει ότι η πλειοψηφία των συμμετεχόντων δηλαδή το 52.9% (9 άτομα) ανήκει σε εθνικές ή ομοσπονδιακές υπηρεσίες, με τους υπηρετούντες σε περιφερειακούς και διεθνείς οργανισμούς να καταλαμβάνουν το 35.3% (6 άτομα) και 11.8% (2 άτομα) αντίστοιχα.



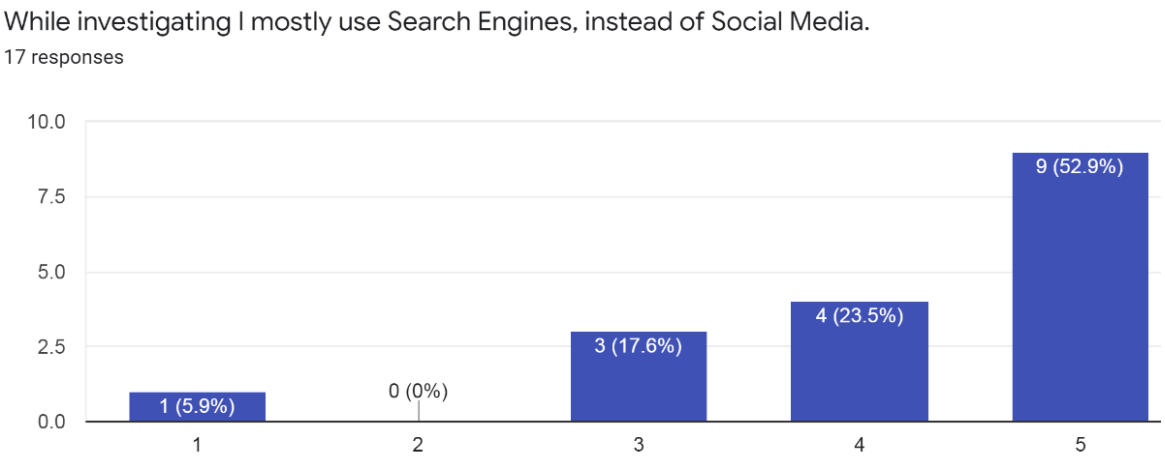
Γράφημα 11 Βαθμός Χρήσης Απόρρητων Πηγών

Αναφορικά με το βαθμό χρήσης απόρρητων πηγών, η πλειοψηφία των χρηστών δήλωσε ότι κατά τη διερεύνηση ενός θέματος, χρησιμοποιεί πάντοτε διαβαθμισμένες πηγές πληροφόρησης (12 άτομα), ενώ 4 εκ των ερωτηθέντων δήλωσαν ότι σχεδόν ποτέ δεν χρησιμοποιούν διαβαθμισμένες πηγές (κλίμακα 1 και 2).

Τα στελέχη φαίνεται να χρησιμοποιούν περισσότερο διαβαθμισμένες πηγές με μ.ό 3,83, απ' ό,τι οι προϊστάμενοι που εμφανίζουν μ.ό. 3,4.

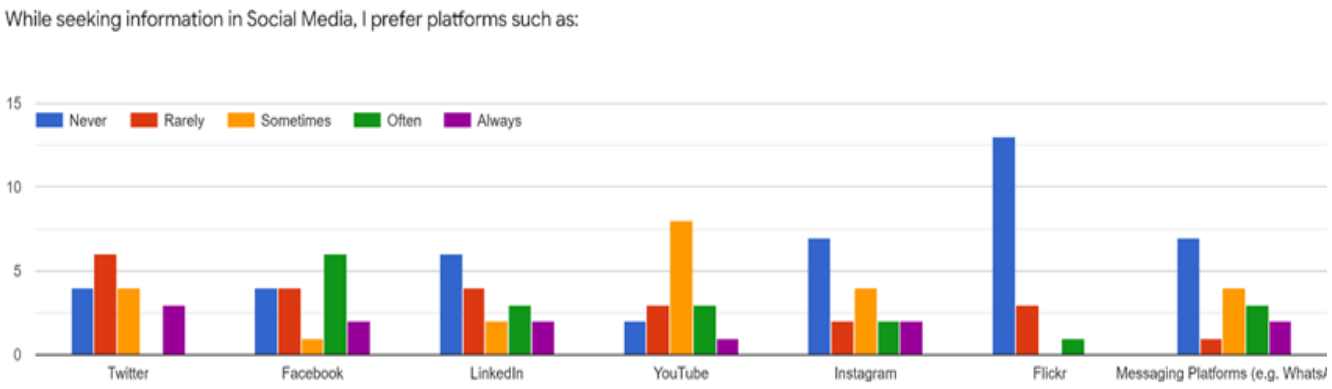
Οι εθνικές αρχές φαίνεται επίσης να χρησιμοποιούν περισσότερο τις διαβαθμισμένες πληροφορίες με μ.ό. 4 ενώ οι περιφερειακοί και Διεθνείς οργανισμοί 3,38.

Για τους συμμετέχοντες από την Β. Αμερική ο μ.ό. είναι 4, ενώ στην Ευρώπη ο μ.ό. είναι 3.67. Ωστόσο, λόγω του ό,τι το δείγμα από Αμερική είναι εξαιρετικά μικρό, δεν μπορεί να εξαχθεί κάποιο συμπέρασμα από τον μ.ό.



Γράφημα 12 Χρήση Search Engines vs Social Networking Services

Η πλειοψηφία των χρηστών (52.9% & 23.5%), δηλαδή 13 άτομα χρησιμοποιούν Μηχανές Αναζήτησης (OSINT), αντί του SOCMINT.



Γράφημα 13 Επιλογή Πλατφόρμας ΜΚΔ

Σχετικά με την πλατφόρμα ΜΚΔ που επιλέγουν οι επιτελείς πληροφοριών, ανά πλατφόρμα διαπιστώνονται τα ακόλουθα στοιχεία:

TW - η πλειοψηφία των χρηστών φαίνεται να κάνει χρήση σπάνια (6) ή ποτέ (4), ή μερικές φορές (4). Μόνο 3 άτομα κάνουν πάντα χρήση του TW.

FB - Σε αντίθεση με το TW, το FB φαίνεται να χρησιμοποιείται πάντα (2), συχνά (6), μερικές φορές (1), σπάνια (4), ποτέ (4).

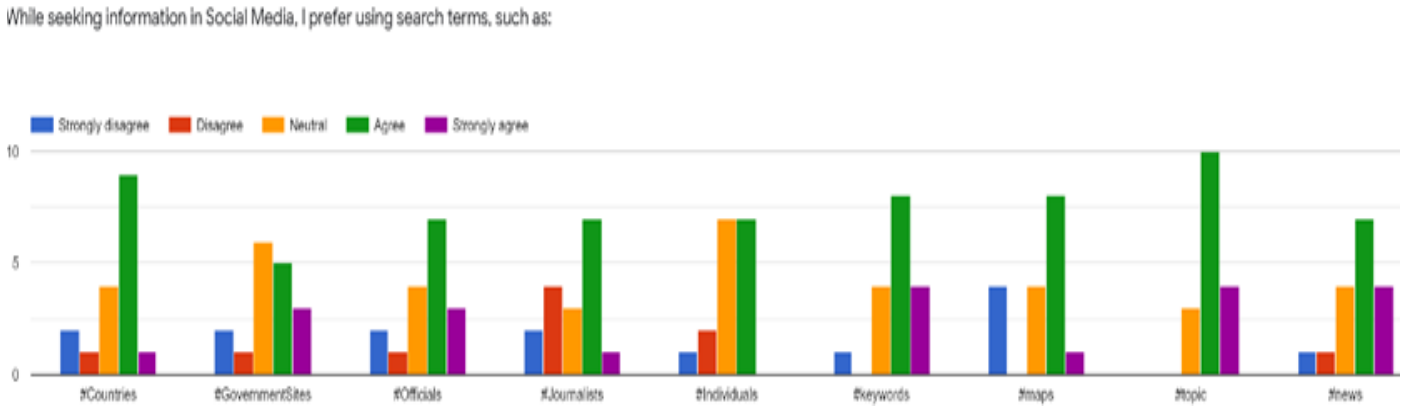
LI – Στο LinkedIn 10 το χρησιμοποιούν σπάνια (4) ή ποτέ (6). Οι υπόλοιποι το χρησιμοποιούν πάντα (2), συχνά (3) ή μερικές φορές (2).

YT – Στο YouTube η πλειοψηφία των χειριστών το χρησιμοποιεί μερικές φορές (8) και συχνά (3), ενώ η μειοψηφία πάντα (1), σπάνια (3) ή ποτέ (2).

IG – Στο Instagram η χρήση του δεν είναι αξιοσημείωτη, δεδομένου 9 χρήστες δεν το χρησιμοποιούν σχεδόν ποτέ (ποτέ 7 και σπάνια 2). Μερικές φορές (4), συχνά (2) και πάντα (2).

Flickr – Η πλειοψηφία των συμμετεχόντων δεν το χρησιμοποιούν ποτέ (13), σπάνια (3) και συχνά (1).

Messaging – 7 απάντησαν ότι δεν το χρησιμοποιούν ποτέ και 1 σπάνια. 4 απάντησαν ότι κάνουν χρήση μερικές φορές, συχνά (2) και πάντα (2).

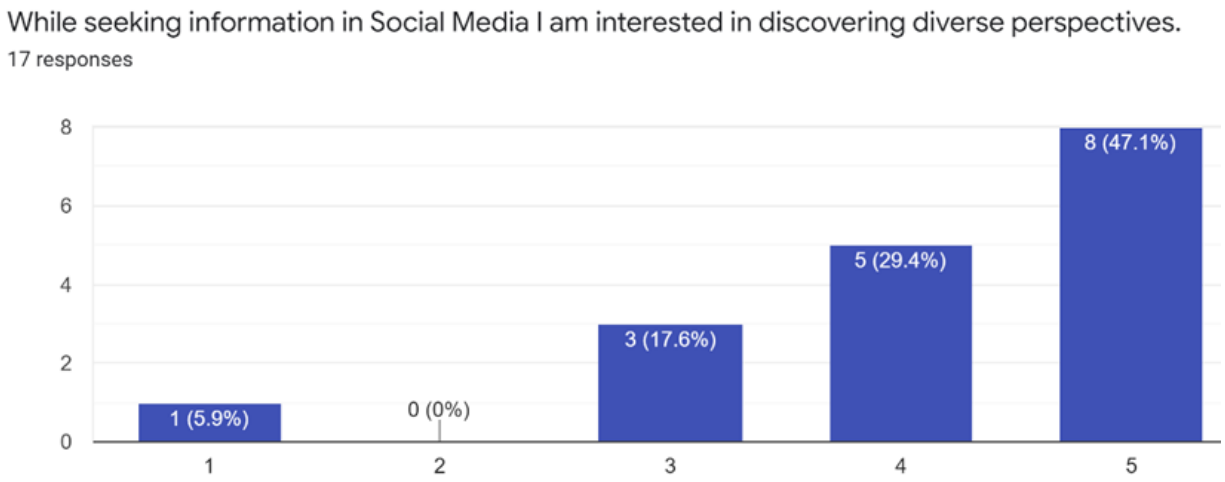


Γράφημα 14 Λέξεις - κλειδιά Αναζήτησης πληροφοριών στα ΜΚΔ

Από το ανωτέρω γράφημα ο μέσος όρος των χρηστών κάνουν χρήση όλων των λέξεων – κλειδιών (#Countries, #Gov, #Officials, #Journalists, #Individuals, #keywords #maps #topics #news) για αναζήτηση πληροφοριών στα ΜΚΔ.

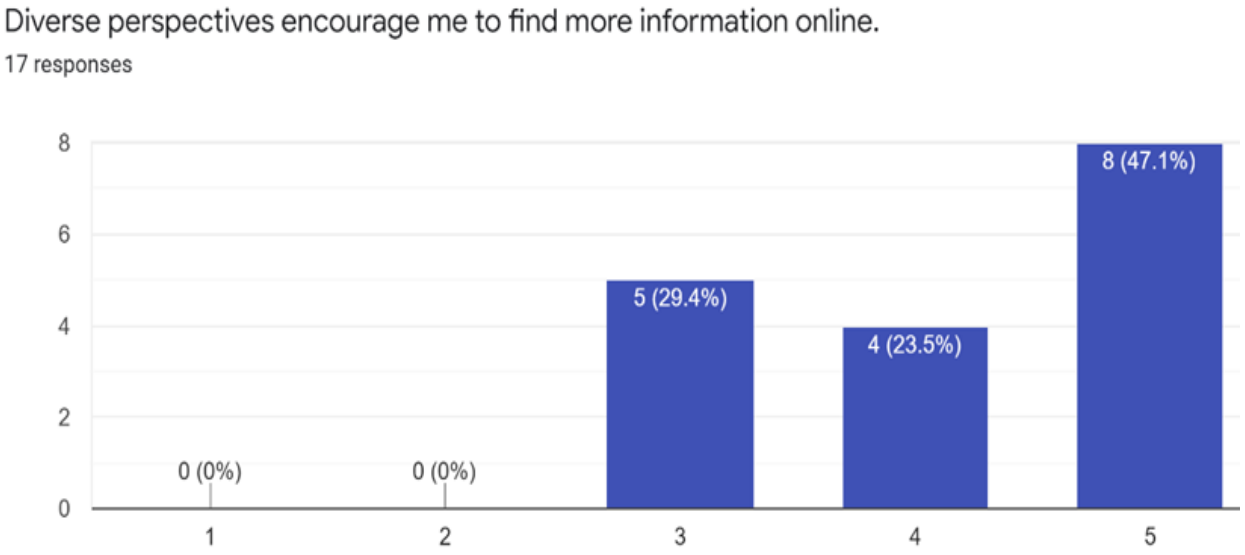
Ενδιάμεση τιμή officers για ανά λέξη-κλειδί είναι η εξής:

1. #Countries 3,5,
2. #Governments 3
3. #Officials 3,5
4. #Journalist 3
5. #Individuals 3
6. #Keywords 4
7. #Maps 4
8. #Topic 4
9. #News 4



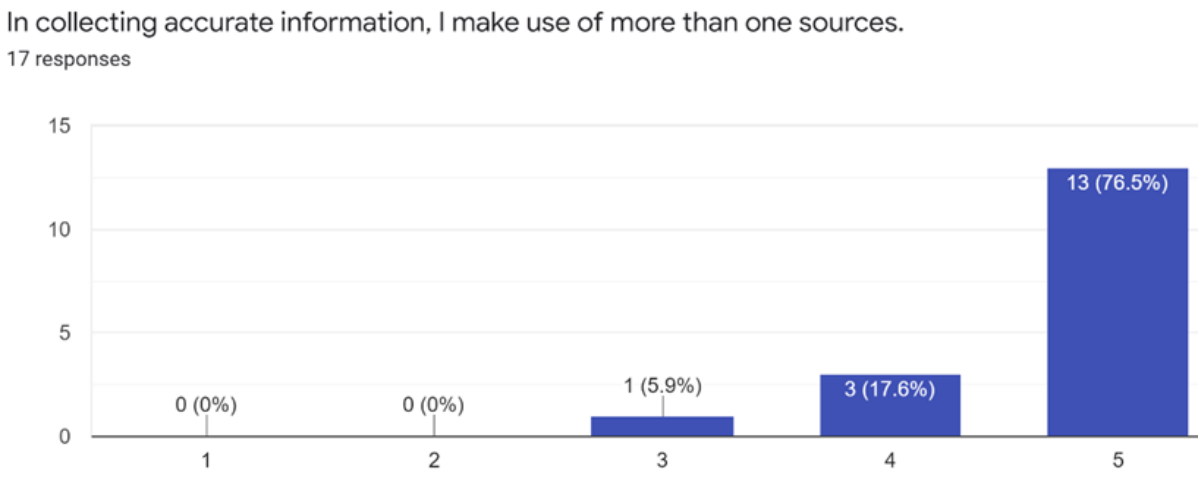
Γράφημα 15 Αναζήτηση Εναλλακτικών Προσεγγίσεων σε θέματα ενδιαφέροντος

Η πλειοψηφία των χρηστών (13) όταν επιλέγουν τα ΜΚΔ, ενδιαφέρονται να διαφορετικές προσεγγίσεις σε θέματα ενδιαφέροντος.



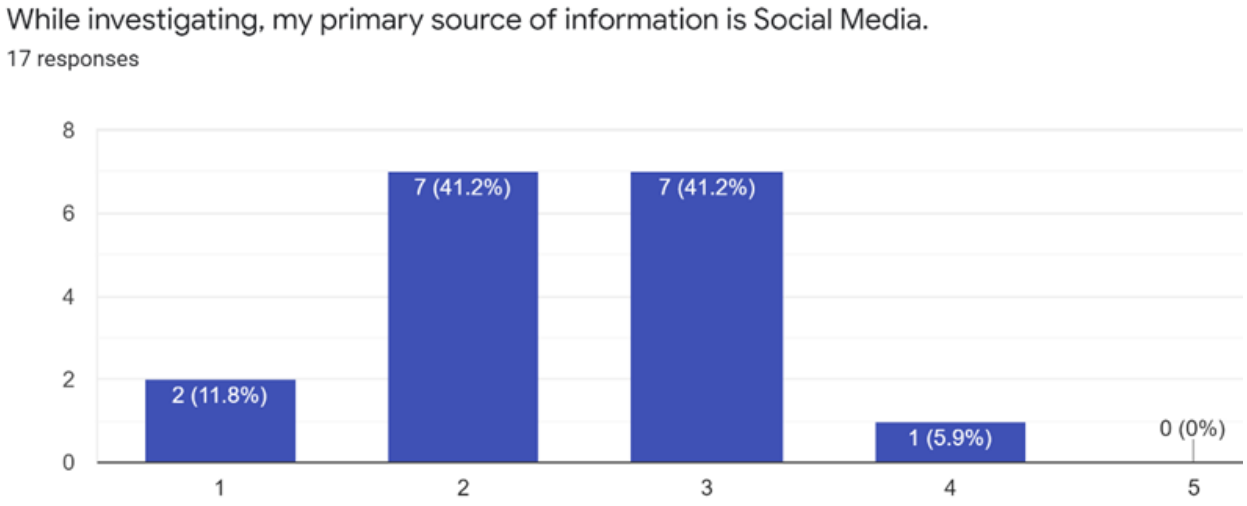
Γράφημα 16 Εναλλακτικές Προσεγγίσεις ενθαρρύνουν περαιτέρω διερεύνηση

Για όλους τους συμμετέχοντες ο εντοπισμός εναλλακτικών απόψεων, τους οδηγεί σε περαιτέρω διερεύνηση.



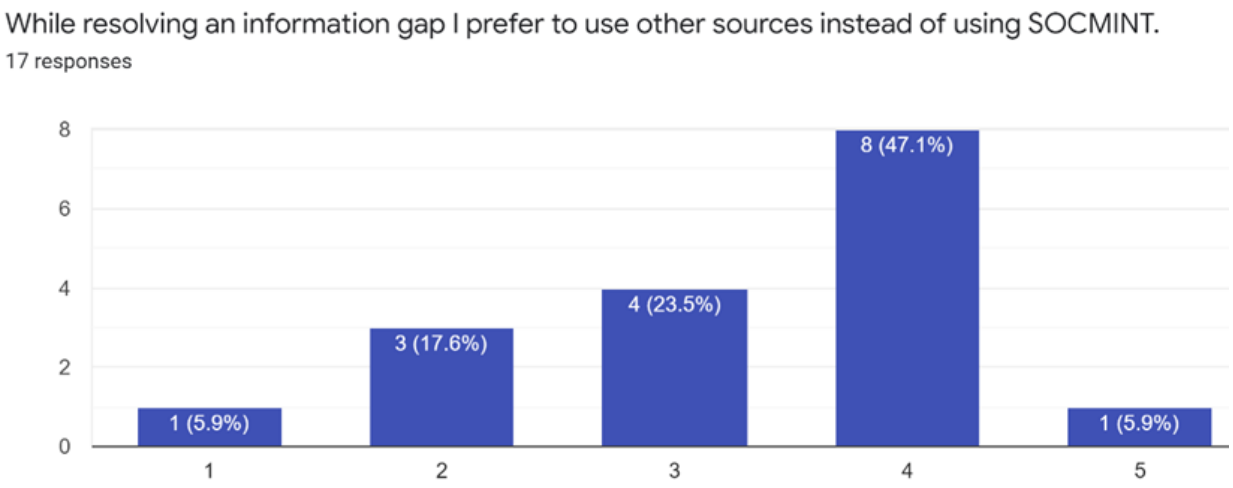
Γράφημα 17 Αριθμός Πηγών που χρησιμοποιεί ο Αναλυτής

Η πλειοψηφία συμμετεχόντων κατατείνει να επιλέγει περισσότερες από μια πηγή πληροφοριών, όταν πρέπει να ελέγξει την ακρίβειά της.



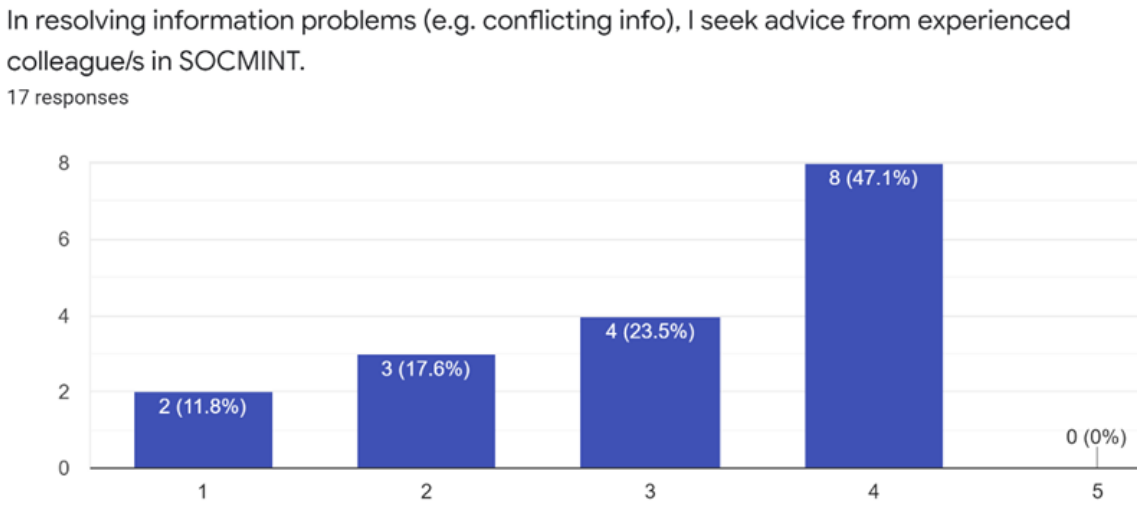
Γράφημα 18 Τα ΜΚΔ ως πρωταρχική πηγή πληροφόρησης

Για τη συλλογή πληροφοριών κανείς από τους επιτελείς πληροφοριών, δεν επιλέγει ως πρωταρχική πηγή πληροφόρησης το SOCMINT.



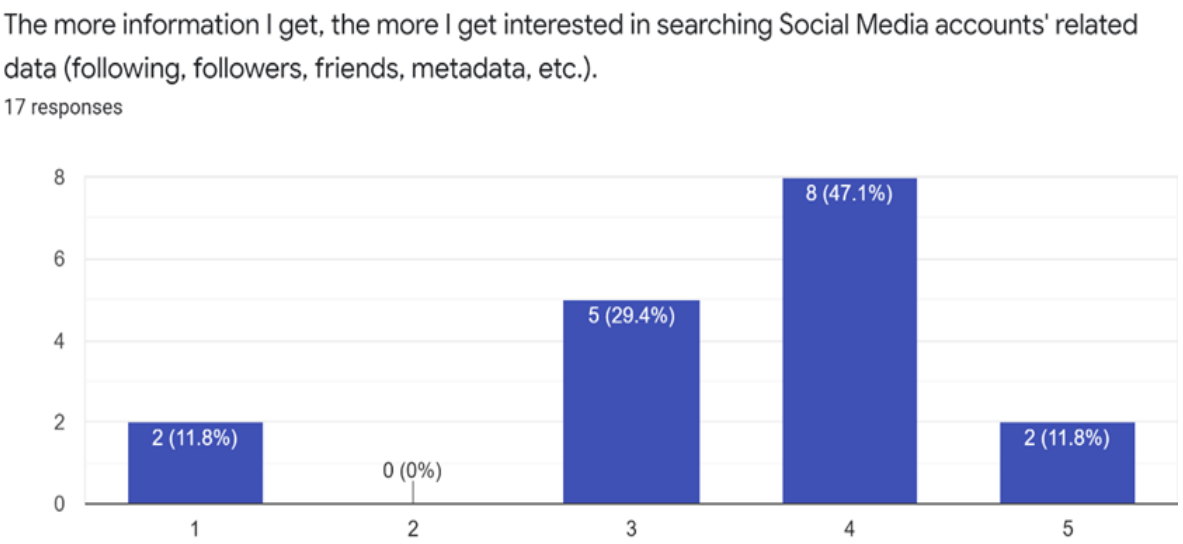
Γράφημα 19 SOCMINT έναντι άλλων πηγών πληροφοριών

Όταν υφίσταται πληροφοριακό κενό, η πλειοψηφία των επιτελών επιλέγουν άλλες πηγές εκτός του SOCMINT.



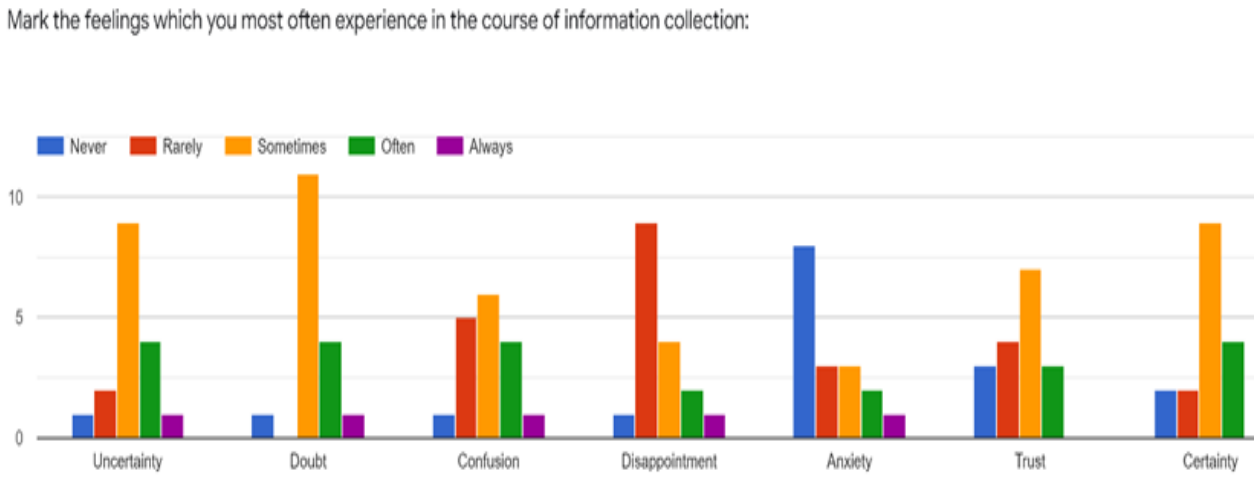
Γράφημα 20 Αντιμετώπιση ζητήματος κατά το SOCMINT – Συμπεριφορά αναλυτή

Στο ανωτέρω γράφημα και όταν ανακύπτουν πληροφοριακά ζητήματα όπως αντιφατικές πληροφορίες, 12 επιτελείς θα ζητήσουν συμβουλή από εξοικειωμένους με το SOCMINT επιτελείς.



Γράφημα 21 Βαθμός ενδιαφέροντος για περαιτέρω αναζήτηση στα ΜΚΔ

Το ανωτέρω γράφημα δεικνύει ότι η πλειοψηφία των αναλυτών, θα διερευνήσει περαιτέρω τα δεδομένα που συνδέονται με τους λογαριασμούς – χρηστών στόχων στα ΜΚΔ.

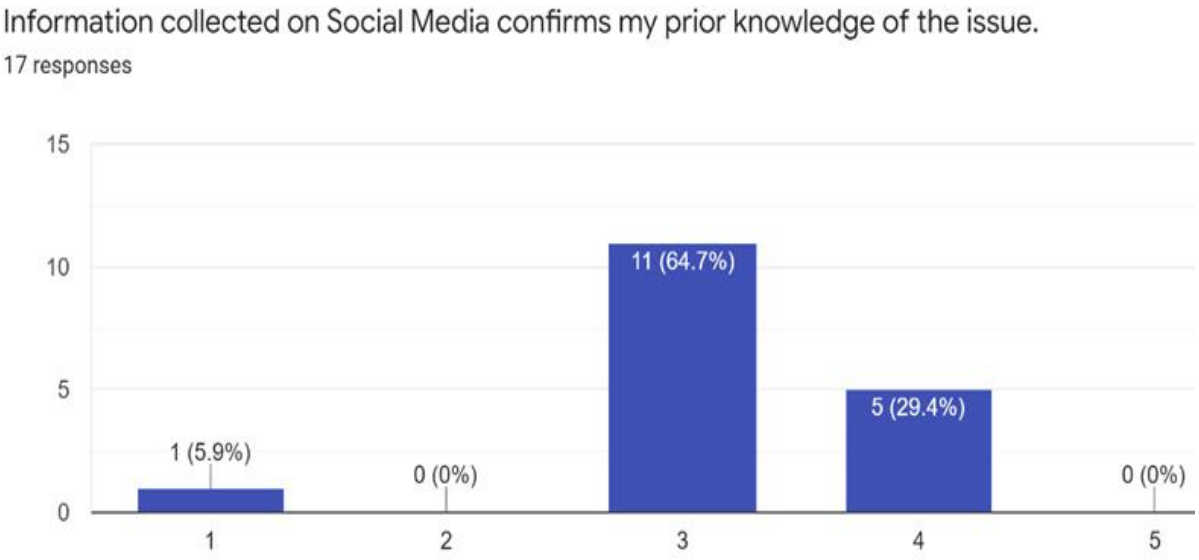


Γράφημα 22 Αντιδράσεις χρήστη κατά τη συλλογή πληροφοριών

Από τους ερωτηθέντες ζητήθηκε να καταγράψουν τη συχνότητα συγκεκριμένων αισθημάτων κατά τη συλλογή πληροφοριών στα ΜΚΔ. Τα αισθήματα αφορούν σε αβεβαιότητα (uncertainty), αμφιβολία (doubt), σύγχυση (confusion), απογοήτευση (disappointment), άγχος (anxiety), εμπιστοσύνη (trust), βεβαιότητα (certainty).

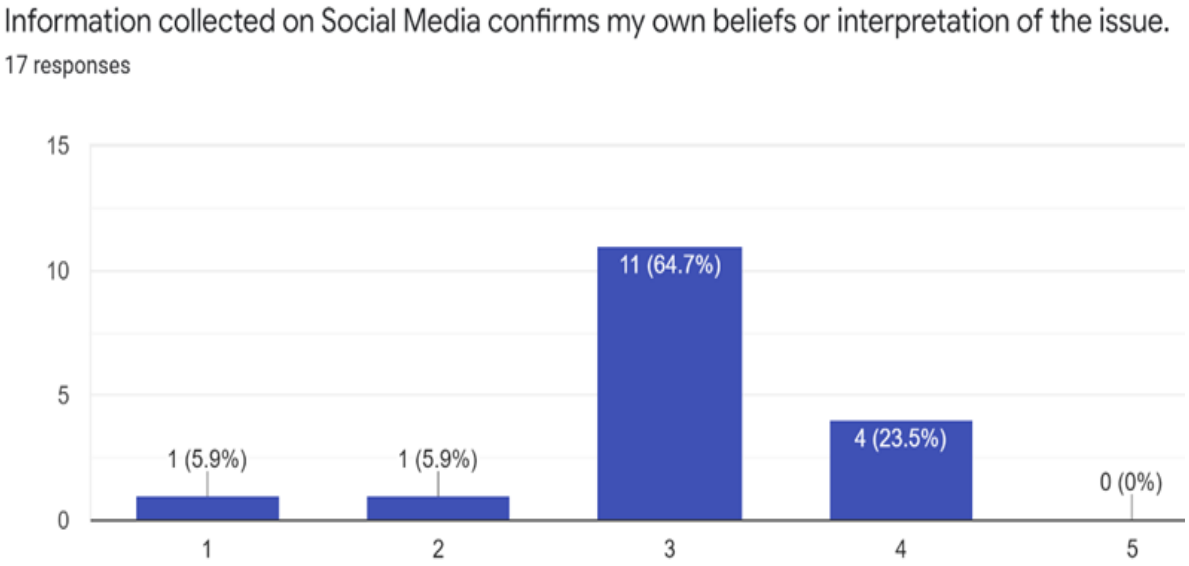
Από το παραπάνω γράφημα προκύπτει ότι κανείς από τους συμμετέχοντες δεν

αισθάνεται σιγουριά και εμπιστοσύνη κατά τη συλλογή πληροφοριών με το SOCMINT.



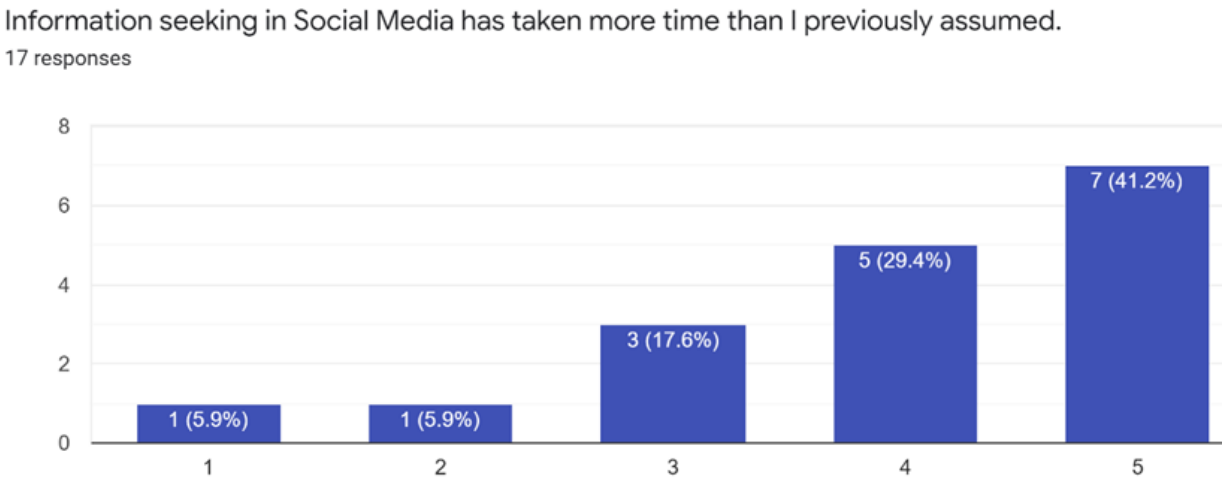
Γράφημα 23 Βαθμός επιβεβαίωσης γνώσης σε σχέση με νέα πληροφορία από SOCMINT

Στη διαπίστωση ότι οι πληροφορίες των ΜΚΔ, επιβεβαιώνουν πρότερη γνώση του θέματος, οι απαντήσεις κινούνται λίγο πάνω από την ουδέτερη στάση.



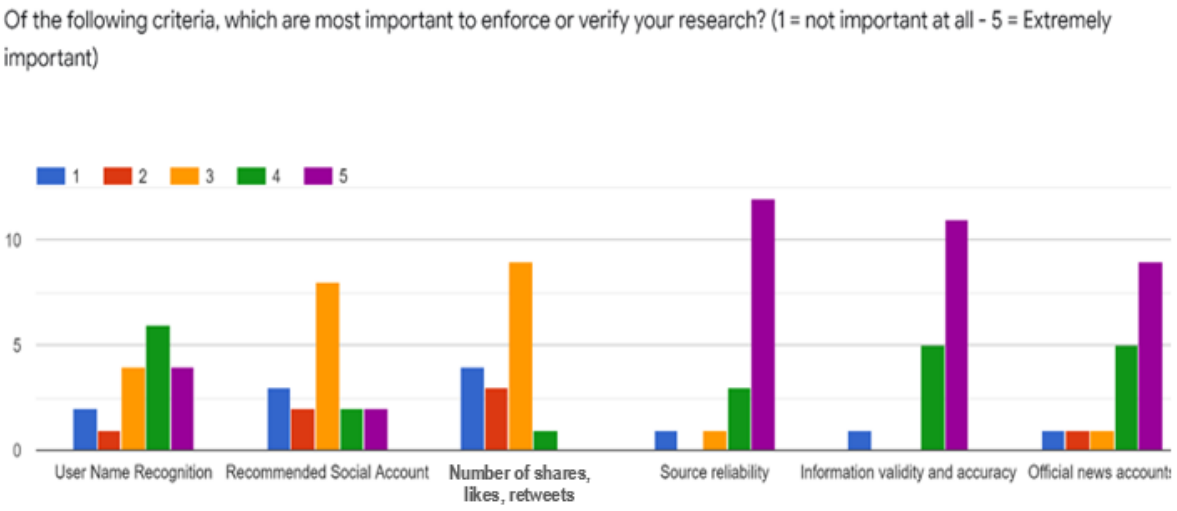
Γράφημα 24 Βαθμός Προκατάληψης Επιβεβαίωσης

Όσον αφορά την επιβεβαίωση απόψεων ή ερμηνειών σχετικά με ένα ζήτημα, η πλειοψηφία του δείγματος φαίνεται να είναι ανεπηρέαστη – ουδέτερη, με 4 άτομα να τείνουν ωστόσο να συμφωνήσουν με τη διαπίστωση.



Γράφημα 25 Διατιθέμενος Χρόνος στα ΜΚΔ

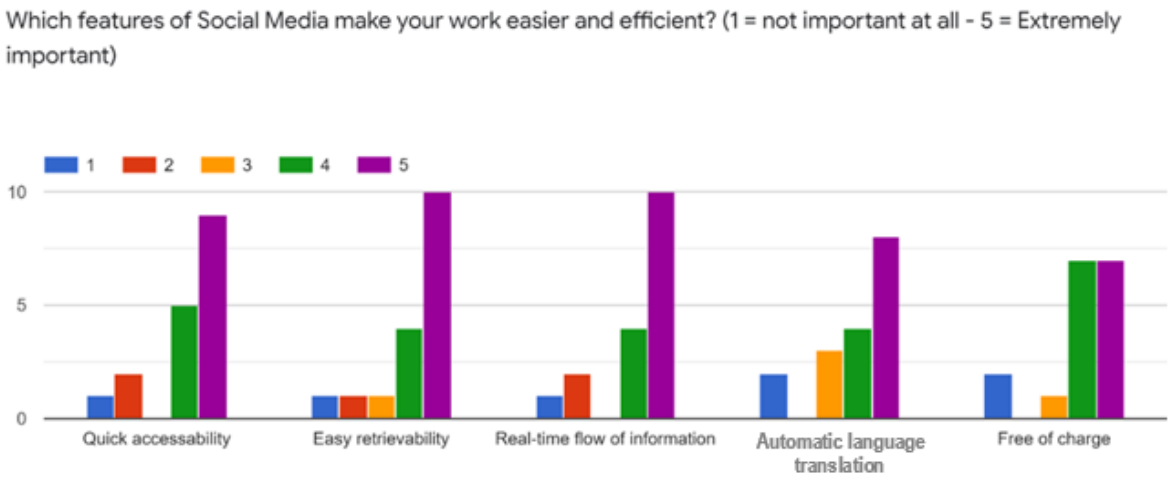
Στη διαπίστωση ότι ο χρόνος που δαπανάται στο SOCMINT από τον επιτελή είναι μεγαλύτερος απ' ό,τι αρχικά είχε προβλεφθεί, η πλειοψηφία του δείγματος απάντησε ότι ταυτίζεται με την πρόταση.



Γράφημα 26 Κριτήρια των ΜΚΔ που ενισχύουν την αξιοπιστία έρευνας

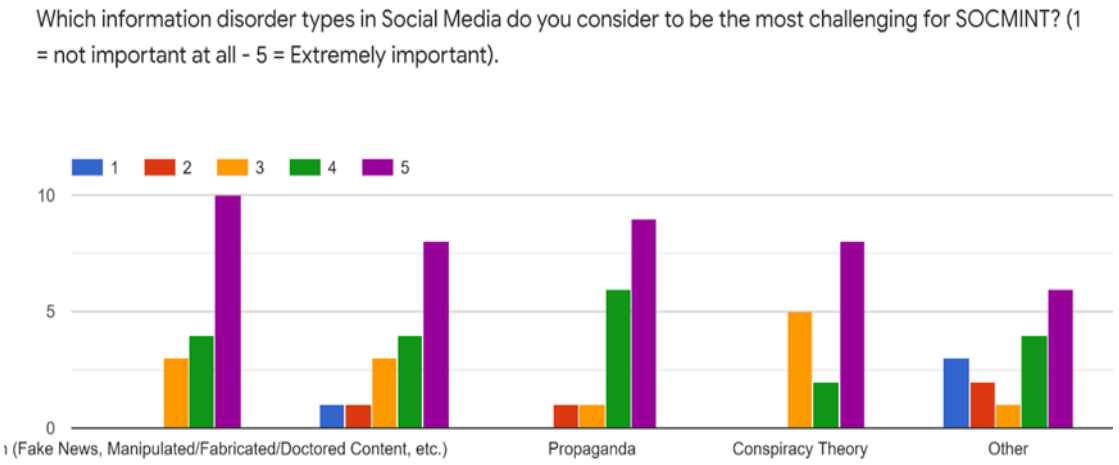
Στα κριτήρια που καθιστούν τη συλλογή πληροφοριών από τα ΜΚΔ αξιόπιστη ή την ενισχύουν περαιτέρω, οι χειριστές κλήθηκαν να επιλέξουν μεταξύ 6 κριτηρίων: 1. User Name Recognition 2. Recommended Social Account 3. Number of shares, likes, retweets 4. Source reliability 5. Information validity and accuracy 6. Official news accounts.

Πάνω από 10 άτομα επέλεξαν την αξιοπιστία της πηγής και την ακρίβεια της πληροφορίας ως τα πιο σημαντικά. Ένα επιπλέον κριτήριο είναι η πηγή πληροφοριών να προέρχεται από επίσημους λογαριασμούς ΜΜΕ. Τα social proof (tweets, retweets, likes), καθώς και τα υπόλοιπα κριτήρια αντιμετωπίζονται από τους αναλυτές σχεδόν ουδέτερα.



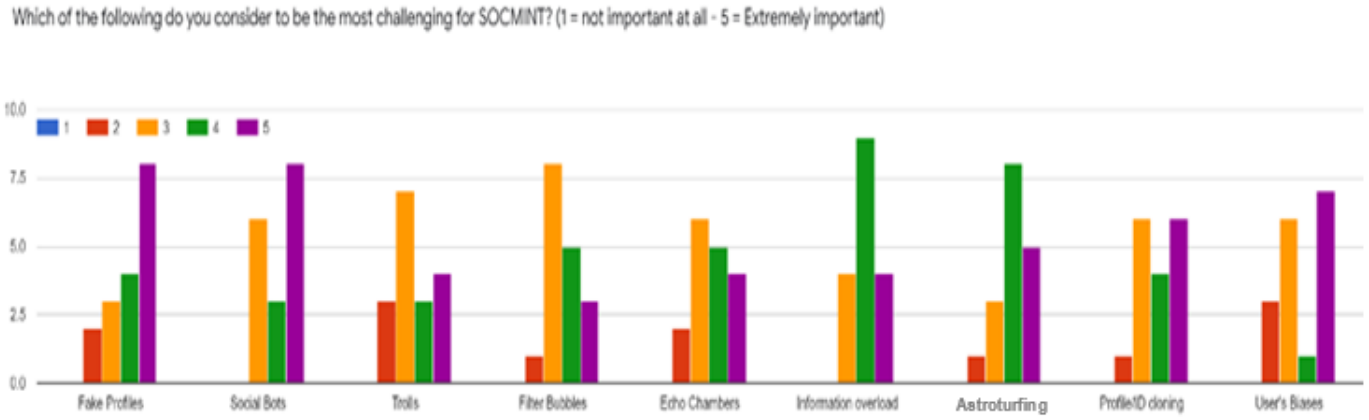
Γράφημα 27 Κριτήρια Χρήσης SOCMINT

Στην ερώτηση ποια χαρακτηριστικά των ΜΚΔ, καθιστούν πιο εύκολη και αποτελεσματική την εργασία του επιτελή, η πλειοψηφία του δείγματος αναδεικνύει την απευθείας μετάδοση πληροφοριών ως το πιο σημαντικό κριτήριο, με την εύκολη δυνατότητα ανάκτησης και τη γρήγορης προσβασιμότητα να είναι επίσης σημαντικά στο SOCMINT.



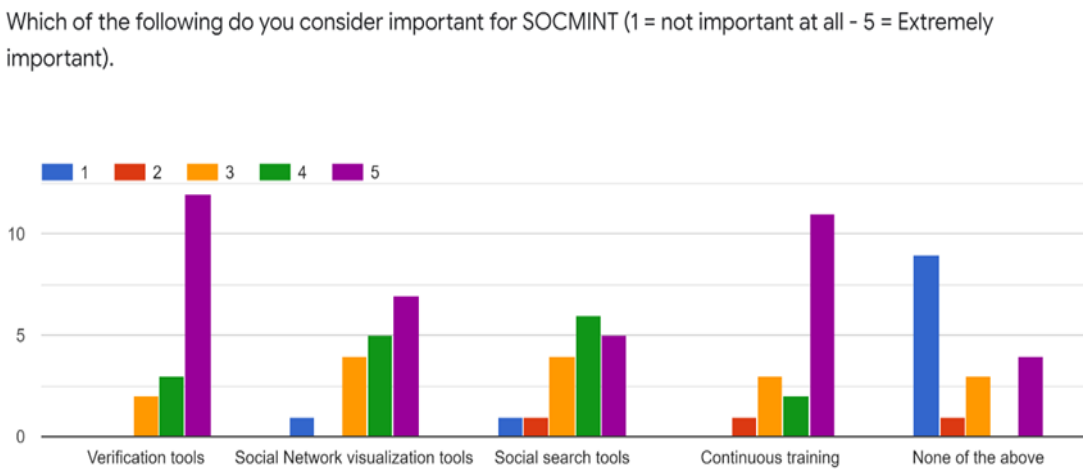
Γράφημα 28 Κίνδυνοι Information Disorder στο SOCMINT

Στο ερώτημα ποιες από τις παρακάτω προκλήσεις θεωρείται κρίσιμες για το SOCMINT, πρώτη σε κατάταξη και κοινή επιλογή του δείγματος ήταν να συμπεριλάβει την παραπληροφόρηση/disinformation ως «εξαιρετικά σημαντική» κατά την αναζήτηση πληροφοριών, με την προπαγάνδα να έπεται και τη θεωρία συνωμοσίας με το malinformation να ακολουθούν.



Γράφημα 29 Προκλήσεις SOCMINT

Fake Profiles, Social Bots, Trolls, Filter Bubbles, Echo Chambers, Information Overload, Astroturfing, Profile/ID Cloning, User's Biases ανάμεσα σ' όλα αυτά, οι περισσότεροι χειριστές διαπιστώνουν ότι το Information Overload, επιλέγεται ως το πιο εξαιρετικά σημαντικό για το SOCMINT, με τα fake profiles και τα Social Bots να ακολουθούν.



Γράφημα 30 Προτάσεις Αντιμετώπισης Κινδύνων

Σύμφωνα με το τελευταίο γράφημα της έρευνας η πλειοψηφία των ερωτηθέντων θα επέλεγαν τα εργαλεία επαλήθευσης και τη συνεχιζόμενη εκπαίδευση, ως εξαιρετικά σημαντικά για τη χρήση του SOCMINT.

6.2. Συσχέτιση Αποτελεσμάτων

Στην υποενότητα αυτή γίνεται ανάλυση των απαντήσεων επιλεγμένων ερωτήσεων στην βάση των δημογραφικών χαρακτηριστικών του δείγματος (φύλο, ηλικία, περιοχή, βαθμός και εμβέλεια του χώρου εργασίας (εθνικός, περιφερειακός ή διεθνής οργανισμός). Λόγω του μικρού αριθμού του δείγματος (17) κρίθηκε αναγκαία η ομαδοποίηση των ηλικιών σε κάτω και άνω των 50 ετών, και της εμβέλειας του φορέα εργασίας σε εθνικό και διεθνή ενσωματώνοντας τους περιφερειακούς φορείς στους διεθνείς.

Παρουσιάζονται τα αποτελέσματα στις ερωτήσεις που αφορούν στη συχνότητα προτίμησης των ΜΚΔ, τη συχνότητα βίωσης διαφορετικών συναισθημάτων και την αξιολόγηση της σημασίας διαφορετικών προτεινόμενων λύσεων για τη διευκόλυνση των χρηστών. Στις πρώτες δύο ερωτήσεις η ονομαστική κλίμακα απαντήσεων μετατράπηκε σε αριθμητική. Η ανάλυση βασίζεται στη διάμεση τιμή των απαντήσεων σε κάθε στήλη.

Πίνακας 15 Διάμεση τιμή συχνότητας προτίμησης διαφορετικών ΜΚΔ για διάφορες ομάδες του δείγματος

Παράμετροι	**n**	**Twitter**	**Facebook**	**Youtube**	**Instagram**	**Linkedin**	**Flickr**	**Messaging**
Sex								
Female	5	3	2	2	2	2	2	1
Male	12	2	3,5	3	2	1,5	1	3
Total	**17**	**2**	**3**	**3**	**2**	**2**	**1**	**3**
Age								
<50	11	2	4	3	3	2	1	3
>50	6	2,5	2,5	3	1	1,5	1	1,5
Total	**17**	**2**	**3**	**3**	**2**	**2**	**1**	**3**
Region								
Europe	15	2	2	3	2	2	1	3
North America	2	4	4	2,5	3	3,5	1,5	2
Total	**17**	**2**	**3**	**3**	**2**	**2**	**1**	**3**

Rank								
Manager	5	3	2	2	2	2	1	1
Officer	12	2	4	3	2	2	1	3
Total	**17**	**2**	**3**	**3**	**2**	**2**	**1**	**3**
Affiliation								
International Organization	8	3	3,5	3	3	2,5	1	3
National/Federal Authority	9	2	2	3	2	2	1	1
Total	**17**	**2**	**3**	**3**	**2**	**2**	**1**	**3**

Αντιστοίχιση Κλίμακας: 1:Never, 2: Rarely, 3: Sometimes, 4: Often, 5: Always

- Οι γυναίκες φαίνεται να προτιμούν πρώτα το TW και μετά το FB.
- Οι άντρες προτιμούν πρώτα το FB και μετά το YT και Messaging.
- Οι άνω των 50 προτιμούν κυρίως το YT και έχουν χαμηλή προτίμηση για τα ΜΚΔ.
- Οι κάτω των 50 προτιμούν κυρίως το FB.
- Οι εργαζόμενοι στις ΗΠΑ προτιμούν περισσότερο το TW.

Πίνακας 16 Διάμεση τιμή για τη συχνότητα βίωσης διαφορετικών συναισθημάτων από τους χρήστες κατά την αναζήτηση πληροφορίας στα ΜΚΔ

Παράμετροι	**n**	**Uncertainty**	**Doubt**	**Confusion**	**Disappointment**	**Anxiety**	**Trust**	**Certainty**
Sex								
Female	5	3	3	3	3	3	4	4
Male	12	3	3	3	2	1,5	3	3
Total	**17**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
Age								
<50	11	3	3	3	2	1	3	3
>50	6	3	3,5	3	2,5	3	2	2,5
Total	**17**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
Region								
Europe	15	3	3	3	2	2	3	3
North America	2	2	2	2	1,5	1	3,5	3,5
Total	**17**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
Seniority								

Manager	5	2	3	3	3	1	4	4
Officer	12	3	3	3	2	2	3	3
Total	**17**	**3**	**3**	**3**	**2**	**2**	**3**	**3**
Affiliation								
International Organization	8	3	3	3	2	1	2,5	3
National/Federal Authority	9	3	3	3	2	3	3	3
Total	**17**	**3**	**3**	**3**	**2**	**2**	**3**	**3**

Αντιστοίχιση Κλίμακας: 1:Never, 2: Rarely, 3: Sometimes, 4: Often, 5: Always

- Οι άντρες βιώνουν σπανιότερα στρες, ενώ οι γυναίκες τείνουν να εμπιστεύονται τα ΜΚΔ συχνότερα.
- Οι άνω των 50 βιώνουν συχνότερα στρες ενώ οι κάτω των 50 εμπιστεύονται συχνότερα τα ΜΚΔ.
- Οι εργαζόμενοι σε διεθνείς οργανισμούς εμφανίζου σπανιότερα στρες.

Πίνακας 17 Αξιολόγηση σημασίας διαφορετικών προτεινόμενων λύσεων (διάμεσες τιμές) από τους χρήστες ΜΚΔ

Παράμετροι	n	Verification Tools	Visualization Tools	Search Tools	Continuous Training	Other
Sex						
Female	5	5	4	4	5	3
Male	11	5	4	4	4	1
Total	**16**	**5**	**4**	**4**	**5**	**1**
Age						
<50	11	5	5	4	5	1
>50	5	5	4	4	4	1
Total	**16**	**5**	**4**	**4**	**5**	**1**
Seniority						
Manager	5	5	4	4	5	3
Officer	11	5	4	4	5	1
Total	**16**	**5**	**4**	**4**	**5**	**1**
Region						
Europe	14	5	4	4	5	1,5
North America	2	5	4,5	3,5	3,5	1
Total	**16**	**5**	**4**	**4**	**5**	**1**
Affiliation						
International Organization	8	5	4,5	4	5	1
National/Federal Authority	8	5	4	4	5	3
Total	**16**	**5**	**4**	**4**	**5**	**1**

Εύρος Κλίμακας 1 = not important at all - 5 = Extremely important

- Όλες οι ομάδες θεωρούν σημαντικά ή εξαιρετικά σημαντικά την παροχή βοηθητικών εργαλείων για τα ΜΚΔ.
- Οι κάτω των 50 θεωρούν εξαιρετικά σημαντική τη συνεχιζόμενη εκπαίδευση στα ΜΚΔ ίσως κατανοώντας καλύτερα την πολυπλοκότητα τους.
- Οι περισσότεροι θεωρούν ότι τα προτεινόμενα εργαλεία λύσεις καλύπτουν τις ανάγκες των χρηστών και δεν αναζητούν άλλα εργαλεία (Median 1).
- Τα εργαλεία επαλήθευσης και η συνεχιζόμενη κατάρτιση τα σημαντικότερα βοηθήματα (Median 5).

Κεφάλαιο 7
Εισηγήσεις Συμπεράσματα

Όπως έχει επισημανθεί στο εισαγωγικό Κεφάλαιο 1, η παρούσα έρευνα πέρα από την καταγραφή των προκλήσεων που εντοπίζονται στα ΜΚΔ, αποσκοπεί και στη διαμόρφωση κάποιας τυποποιημένης διαδικασίας λειτουργίας όπου βάσει αυτής ο επιτελής να μπορεί να διαχειρίζεται και να αντιμετωπίζει φαινόμενα που συνδέονται με το information disorder και των μηχανισμών που τα προκαλούν, ενώ παράλληλα να εντοπίζει συναφή στοιχεία με υπό έρευνα θέματα.

Έχοντας λοιπόν καταγράψει τα φαινόμενα και τους μηχανισμούς πρόκλησής τους στο Κεφάλαιο 4, στην παρούσα ενότητα επιχειρείται να διατυπωθεί μια λίστα κατευθυντήριων ενεργειών κατά τα στάδια συλλογής και επεξεργασίας της πληροφορίας.

7.1. Προτεινόμενη Διαδικασία

Σε επίπεδο ΥΠ και συγκεκριμένα Διευθύνσεων Συλλογής και Ανάλυσης, οι επιτελείς ανοικτών πηγών και ειδικότερα SOCMINT οφείλουν να διακρίνουν τον τύπο information disorder και το μηχανισμό που τον αναπαράγει. Σε ενδοϋπηρεσιακό επίπεδο αυτό μπορεί να γίνει σε:

(α) Συνεργασία μ’ άλλους χειριστές, των οποίων τα θέματα μπορεί να συμπίπτουν,

(β) Διαρκή συνεννόηση με τμήματα Πληροφορικής των ΥΠ.

Οι ενέργειες κατηγοριοποιούνται ανάλογα με τον δρώντα και ως εκ τούτου προκύπτουν τρία επίπεδα:

7.1.1. Επίπεδο Αναλυτή Πληροφοριών - Τμήματος

Οι ενέργειες του επιτελή (Πίνακας 18) όσον αφορά σε καταγραφή ζητημάτων που προκύπτουν κατά τη συλλογή και επεξεργασία, υποβολή αιτήματος συνδρομής από αρμόδια στελέχη, συνεχή ανανέωση βάσης δεδομένων με στοιχεία από λογαριασμούς χρηστών (flagging, labeling, κ.ο.κ.).

Πίνακας 18 Διαδικασία Ελέγχου Επιτελή για SOCMINT

Α/Α	*Τεχνικές*	*Στάδιο*	*Στοιχεία Καταγραφής*
1.	**Κατάρτιση Μαύρης Λίστας**	Συλλογή Επεξεργασία Ανάλυση	@TrollAccount, @BotAccount, @CyborgAccount, @Astroturfer, @FakeAccount, @ClonedAccount
2.	**Flagging λογαριασμών – Ειδική Σήμανση**	Συλλογή Επεξεργασία Ανάλυση	Προσθήκη ένδειξης – flag σε ύποπτους λογαριασμούς και καταχώρηση σε κοινή βάση δεδομένων
3.	**Labeling λογαριασμών – Ετικετοποίηση**	Συλλογή Επεξεργασία Ανάλυση	Λογαριασμοί με label περιεχομένου επί information disorder
4.	**Βαθμολόγηση Αξιοπιστίας λογαριασμού**	Ανάλυση Ανατροφοδότηση	Αξιολόγηση ποιότητας υλικού από αναλυτή και τελικό αποδέκτη
5.	**Βαθμολόγηση Ακρίβειας Πληροφορίας**	Ανάλυση Ανατροφοδότηση	Αξιολόγηση ακρίβειας πληροφορίας από αναλυτή και τελικό αποδέκτη.
6.	**Έλεγχος Πηγής (cross-checking)**	Σχεδιασμός Επεξεργασία	-Οπτικοποίηση Δικτύου Χρήστη από ειδικό -Διασταύρωση με διαβαθμισμένη πηγή
7.	**Έλεγχος Πληροφορίας (cross-checking)**	Σχεδιασμός Επεξεργασία	-Οπτικοποίηση διαμοιρασμού πληροφορίας σε ΜΚΔ -Διασταύρωση με διαβαθμισμένη πληροφορία.
8.	**Καταγραφή και υποβολή ζητημάτων κατά την πληροφοριακή διαδικασία**	Συλλογή Επεξεργασία	Καταγραφή εμποδίων, καθυστερήσεων, κλπ.
9.	**Χρήση Εφαρμογών για έλεγχο γεγονότων**	Συλλογή Επεξεργασία	- www.dogrulukpayi.com - https://teyit.org/ για Τουρκία

Πηγή: Συντάκτης

Αναφορικά με τα σημεία 4 και 5 σχετικά με τη βαθμολόγηση αξιοπιστίας λογαριασμού

κι ακρίβειας πληροφορίας, ένας **ενδεικτικός πίνακας ελέγχου σημείων** για τον επιτελή κατά τα στάδια συλλογής, επεξεργασίας, ανάλυσης και ανατροφοδότησης, θα μπορούσε να περιέχει τα εξής:

Πίνακας 19 Πίνακας Ελέγχου Σημείων Πηγής και Πληροφορίας

Α/Α	Χαρακτηρισμός	ΠΗΓΗΣ	ΠΛΗΡΟΦΟΡΙΑΣ
1.	Αληθής ≠ Ψευδής	√	√
2.	Υπαρκτή ≠ Ανύπαρκτη	√	√
3.	Αυθεντική ≠ Πλαστή	√	√
4.	Αντικειμενική ≠ Υποκειμενική	√	√
5.	Αναμφισβήτητη ≠ Διφορούμενη	√	√
6.	Προσβάσιμη ≠ Μη-προσβάσιμη	√	√
7.	Επίκαιρη ≠ Ανεπίκαιρη	√	√
8.	Διαφορετικότητα ≠ Ομοιότητα	√	√
9.	Διαχρονική ≠ Εφήμερη	√	√
10.	Παρατεταμένη ≠ Σύντομη διάρκεια	√	√
11.	Συστηματική ≠ Ανοργάνωτη	√	√
12.	Επαληθεύεται ≠ Διαψεύδεται	√	√
13.	Κινητοποιεί ≠ Αδρανοποιεί	√	√
14.	Ευνοϊκή ≠ Δυσμενής ≠ Ουδέτερη	√	√
15.	Ισορροπημένη ≠ Ασταθής	√	√
16.	Συγκεκριμένη ≠ Γενική	√	√
17.	Σαφής ≠ Ασαφής	√	√
18.	Επίκαιρη ≠ Ανεπίκαιρη	√	√
19.	Πολυσυλλεκτική ≠ Μονοδιάστατη	√	√
21.	Εμβριθής ≠ Επιφανειακή		√
22.	Λογική ≠ Παράλογη		√
23.	Πρόωρη ≠ Όψιμη		√

24.	Συνεχής ≠ Διακεκομμένη	√
25.	Σύνθετη/Πολύπλοκη ≠ Απλή	√
26.	Πραγματική ≠ Φαινομενική	√
27.	Εύλογη ≠ Παράδοξη	√

Πηγή: Συντάκτης

7.1.2. Επίπεδο Υπηρεσίας Πληροφοριών

Σε επίπεδο ΥΠ ο Πίνακας 20 παρουσιάζει κάποιες ενδεικτικές ενέργειες που αφορούν σε ψηφιακό εκσυγχρονισμό, διατύπωση ειδικών διαδικασιών για το SOCMINT, ανάθεση αρμοδιοτήτων σε ειδικό προσωπικό, συνεργασία με ξένες ΥΠ για τεχνογνωσία.

Πίνακας 20 Προτεινόμενες Ενέργειες ΥΠ για SOCMINT

Α/Α	Ενέργειες	Επίπεδο	Μηχανισμός - Συνεργασίες
1.	**Παρατηρητήριο (Watchdog)**	Εθνικό	Computational Propaganda Watchdog. Συντήρηση και ανανέωση κοινής βάσης δεδομένων Δνσεις Συλλογής & Ανάλυσης.
2.	**Σύσταση Ομάδας Έρευνας Αλγορίθμων**	Εθνικό	Δνση Ηλεκτρονικών Πληροφοριών & Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας
3.	**Σύσταση Ομάδας Αντιπροπαγάνδας**	Εθνικό	Αντιμετώπιση παραπληροφόρησης συνεργασία αρμοδίων Δνσεων.
4.	**Καθορισμός Ενδείξεων Computational Propaganda**	Ευρωπαϊκό Εθνικό	Συνεργασία με ΥΠ Ε.Ε., Κέντρα Έρευνας και Πανεπιστήμια
5.	**Θέσπιση Κριτηρίων Βαθμολόγησης Πηγών ΜΚΔ**	Εθνικό Ευρωπαϊκο	Συνεργασία με συναρμόδιους φορείς (Έν. Δυνάμεις, Σώματα Ασφ., ΥπΕξ,)
6.	**Αξιοποίηση υφιστάμενων μεθόδων & εργαλείων SOCMINT**	Εθνικό Ευρωπαϊκό	Αξιοποίηση μεθόδων και εργαλείων κατάρτισης και εκπαίδευσης για SOCMINT σε συνεργασία με ΥΠ και Πανεπιστήμια
7.	**Επικαιροποίηση διαδικασιών OSINT**	Εθνικό Ευρωπαϊκό	Συνεργασία με ΥΠ και Πανεπιστήμια.
8.	**Κοινή Βάση Δεδομένων**	Ευρωπαϊκό	Open source για accounts/χρήστες μεταξύ ΥΠ Ε.Ε.
	Διενέργεια κοινών ασκήσεων	Εθνικό Ευρωπαϊκό	Με φορείς σε εθνικό και ευρωπαϊκό περιβάλλον, για συντονισμένη αντιμετώπιση απειλής
9.	**Ενδυνάμωση**	Εθνικό	Αποτροπή φαινομένων/βελτιστοποίηση

	Μηχανισμών	Ευρωπαϊκό	επιχειρησιακής συνεργασίας
10.	**Επαγγελματική Κατάρτιση**	Εθνικό	Επικαιροποίηση γνώσεων και δεξιοτήτων, συμβατές με εξελίξεις τεχνολογίας – μεταβαλλόμενες απειλές
11.	**Δια βίου μάθηση**	Εθνικό Ευρωπαϊκό	Ειδικά σεμινάρια και προγράμματα σπουδών σε επιτελείς για SOCMINT.

7.1.3. Κρατικό Επίπεδο

Ο Πίνακας 21Πίνακας 21 εμπεριέχει προτεινόμενες δράσεις σε κρατικό επίπεδο και αφορούν μεταξύ άλλων σε διεξαγωγή ειδικών εκπαιδεύσεων για υπαλλήλους συναρμόδιων φορέων, συνεργασία επί θεμάτων παραπληροφόρησης σ' ευρωπαϊκό επίπεδο, κοινή αντιμετώπιση πληροφοριακών φαινομένων.

Πίνακας 21 Πολιτικές Κράτους έναντι Computational Propaganda στα ΜΚΔ

Α/Α	Τεχνικές	Επίπεδο	Στοιχεία Καταγραφής
1.	**Σύσταση Ειδικού Συμβουλευτικού Οργάνου**	Εθνικό, Ευρωπαϊκό	Με εκπροσώπους φορέων από ΥΠ και συναρμόδιες Υπηρεσίες
2.	**Σύσταση Κόμβου Επιστήμης και ΜΚΔ**	Εθνικό	Ανάλογο του European Science - Media Hub (ESMH) και EUvsDisinfo
3.	**Χρηματοδότηση έρευνας**	Εθνικό	Αντιμετώπιση κακόβουλων ενεργειών μέσω ΜΚΔ.
4.	**Αίτημα Διαφάνειας προς εταιρείες ΜΚΔ**	Διεθνές	Απαίτηση για Αλγοριθμική Διαφάνεια από εταιρείες ΜΚΔ.
5.	**Ενίσχυση Επίσημων Φορέων Πληροφόρησης**	Εθνικό, Ευρωπαϊκό	Συνεργασία με ΜΜΕ
6.	**Ενδυνάμωση Συνεργασιών**	Εθνικό, ΕΕ, Διεθνές	Σχεδιασμός αποτίμησης επικινδυνότητας & διαχείρισης πληροφοριακών προκλήσεων.
7.	**Συνεχής Εκπαίδευση**	Εθνικό, Ευρωπαϊκό	Digital Literacy

7.2. Συμπεράσματα

Η μελέτη της υφιστάμενης βιβλιογραφίας οδήγησε στο συμπέρασμα ότι μια σειρά φαινομένων που συνδέονται με την υπολογιστική προπαγάνδα, την παραπληροφόρηση, τη χειραγώγηση της κοινής γνώμης μέσω ΜΚΔ, έχουν θέσει νέες προκλήσεις στις ΥΠ κατά τη συλλογή πληροφοριών από το διαδίκτυο και συγκεκριμένα από τα Μέσα Κοινωνικής Δικτύωσης. Μαζικές διαδικτυακές εκστρατείες

παραπληροφόρησης αποτελούν μορφή υβριδικών απειλών για την ασφάλεια της χώρας, είτε αφορά σε εκλογική διαδικασία, είτε σε διαχείριση διμερών ζητημάτων κ.ο.κ. Αυτές οι προκλήσεις για το SOCMINT, δύναται να αντιμετωπιστούν σε συνεργασία με κρατικούς και ακαδημαϊκούς φορείς και με μεταφορά τεχνογνωσίας σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο μεταξύ ΥΠ.

Στη βάση των προτεινόμενων ενεργειών που παρουσιάστηκαν ανά δρώντα (αναλυτής, υπηρεσία και κράτος) φαίνεται να διαμορφώνεται το επιδιωκόμενο επίπεδο πληροφόρησης προκειμένου το παραγόμενο πληροφοριακό προϊόν να καταστεί χρήσιμο και αποτελεσματικό για τα κέντρα λήψης αποφάσεων.

Έναντι όμως όλων των εισηγήσεων, βασική προϋπόθεση είναι η ευαισθητοποίηση του αναλυτή και η αναγκαιότητα αντίληψης ότι το οικοσύστημα πληροφοριών μεταβάλλεται και οποιαδήποτε απόπειρα άντλησης κι ανάλυσης πληροφοριών απ' αυτό συμπεριλαμβάνει στοιχεία από μεγάλα δεδομένα. Η συμπερίληψη του SOCMINT ως μιας σύγχρονης πηγής πληροφόρησης είναι επιτακτική, όμως η πλήρης αξιοποίησή της συνεπάγεται ειδική κατάρτιση του προσωπικού και περαιτέρω ενδυνάμωση συνεργασίας σε επίπεδο Υπηρεσιών στο συγκεκριμένο τομέα.

Λαμβάνοντας υπόψη τα ανωτέρω, κρίνεται σκόπιμο να μελετηθούν για υιοθέτηση κι εφαρμογή πρακτικές που αφορούν σε περαιτέρω:

1. Ευαισθητοποίηση για το είδος των απειλών που καλούνται να αντιμετωπίσουν οι ΥΠ (υβριδικές απειλές, εκστρατείες παραπληροφόρησης, κ.ο.κ.).
2. Συντονισμό και ανταλλαγή πληροφοριών μεταξύ των ενδιαφερομένων σχετικά με ύποπτη δραστηριότητα λογαριασμών και χρηστών.
3. Προσπάθεια εφάμιλλης αντιμετώπισης υβριδικών απειλών, με σκοπό να εξαλειφθεί το χάσμα στη χρήση των ΜΚΔ, ειδικά όταν αυτό αφορά σε διμερείς σχέσεις και προάσπιση εθνικών συμφερόντων, όπως στην περίπτωση Ελλάδας – Τουρκίας.
4. Καθορισμό προληπτικού σχεδίου για την αντιμετώπιση πιθανών απειλών.
5. Διερεύνηση και εφαρμογή καινοτόμων μεθόδων αντιμετώπισης απειλών όπως μέσω της τεχνολογίας:

(α) τεχνητής νοημοσύνης (AI), κρίσιμη για την επαλήθευση και τον

εντοπισμό της παραπληροφόρησης

(β) της εφαρμογής σειράς καταχωρήσεων “blockchain”, ενός μητρώου για αποθήκευση και επαλήθευση πληροφοριών και πηγών, ώστε να υπάρχει μια συνεχής αλυσίδα πληροφοριών και

(γ) γνωστικών αλγορίθμων που δύναται να διαχειριστούν συναφείς πληροφορίες, συμπεριλαμβανόμενης της ακρίβειας και της ποιότητας των πηγών δεδομένων, βελτιώνοντας συνάφεια και αξιοπιστία αποτελεσμάτων αναζήτησης (Ευρωπαϊκή Επιτροπή 2018b).

Παράρτημα Α
Ερωτηματολόγιο

Social Media Intelligence (SOCMINT) | Anonymous Usage Questionnaire

Welcome and thank you for your participation.

This questionnaire has been designed to gather user experience information related to SOCMINT as a tool for military, security, law enforcement agencies and decision-making bodies. The purpose of this survey is to examine how SOCMINT is used and it's value as a source of Information. The knowledge gained from this questionnaire will be used as part of academic research.

The expected time to complete this survey is 5 minutes.

*Required

1. Sex *

Mark only one oval.

- ◯ Male
- ◯ Female
- ◯ Non Binary / Third Gender
- ◯ Prefer not to say

2. Age *

Mark only one oval.

- ◯ 18-25
- ◯ 26-30
- ◯ 31-40
- ◯ 41-50
- ◯ 51 and above

3. Region *

Mark only one oval.

- ◯ Europe
- ◯ Middle East & Africa
- ◯ North America

4. User Category *

Mark only one oval.

- ◯ Officer
- ◯ Manager

5. Affiliation *

Mark only one oval.

- ◯ National/Federal Authority
- ◯ Regional Organization
- ◯ International Organization

Social Media Intelligence Collection & Use

Mark the extent of your identification with the following statements on the scale 1-5.

6. While investigating a topic I make use of classified resources as well. *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

7. While investigating I mostly use Search Engines, instead of Social Media. *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

8. While seeking information in Social Media, I prefer platforms such as: *

Mark only one oval per row.

	Never	Rarely	Sometimes	Often	Always
Twitter	◯	◯	◯	◯	◯
Facebook	◯	◯	◯	◯	◯
LinkedIn	◯	◯	◯	◯	◯
YouTube	◯	◯	◯	◯	◯
Instagram	◯	◯	◯	◯	◯
Flickr	◯	◯	◯	◯	◯
Messaging Platforms (e.g. WhatsApp)	◯	◯	◯	◯	◯

9. While investigating a topic I prefer well-known Social Media accounts. *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

10. While seeking information in Social Media, I prefer using search terms, such as: *

Mark only one oval per row.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
#Countries					
#GovernmentSites					
#Officials					
#Journalists					
#Individuals					
#keywords					
#maps					
#topic					
#news					

11. While seeking information in Social Media I am interested in discovering diverse perspectives. *

Mark only one oval.

	1	2	3	4	5	
Almost never						Almost always

12. Diverse perspectives encourage me to find more information online. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

13. In collecting accurate information, I make use of more than one sources. *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

14. While investigating, my primary source of information is Social Media. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

15. While resolving an information gap I prefer to use other sources instead of using SOCMINT. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

16. In resolving information problems (e.g. conflicting info), I seek advice from experienced colleague/s in SOCMINT. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

17. The more information I get, the more I get interested in searching Social Media accounts' related data (following, followers, friends, metadata, etc.). *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

18. Mark the feelings which you most often experience in the course of information collection: *

Mark only one oval per row.

	Never	Rarely	Sometimes	Often	Always
Uncertainty	◯	◯	◯	◯	◯
Doubt	◯	◯	◯	◯	◯
Confusion	◯	◯	◯	◯	◯
Disappointment	◯	◯	◯	◯	◯
Anxiety	◯	◯	◯	◯	◯
Trust	◯	◯	◯	◯	◯
Certainty	◯	◯	◯	◯	◯

Skip to question 19

19. Information collected on Social Media confirms my prior knowledge of the issue. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

20. Information collected on Social Media confirms my own beliefs or interpretation of the issue. *

Mark only one oval.

	1	2	3	4	5	
Never	◯	◯	◯	◯	◯	Always

21. Information seeking in Social Media has taken more time than I previously assumed. *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

22. Of the following criteria, which are most important to enforce or verify your research? (1 = not important at all - 5 = Extremely important) *

Mark only one oval per row.

	1	2	3	4	5
User Name Recognition	◯	◯	◯	◯	◯
Recommended Social Account	◯	◯	◯	◯	◯
Total number of shares, likes, retweets	◯	◯	◯	◯	◯
Source reliability	◯	◯	◯	◯	◯
Information validity and accuracy	◯	◯	◯	◯	◯
Official news accounts	◯	◯	◯	◯	◯

23. Which features of Social Media make your work easier and efficient? (1 = not important at all - 5 = Extremely important) *

Mark only one oval per row.

	1	2	3	4	5
Quick accessability	◯	◯	◯	◯	◯
Easy retrievability	◯	◯	◯	◯	◯
Real-time flow of information	◯	◯	◯	◯	◯
Automatic language translation	◯	◯	◯	◯	◯
Free of charge	◯	◯	◯	◯	◯

24. Which information disorder types in Social Media do you consider to be the most challenging for SOCMINT? (1 = not important at all - 5 = Extremely important).

Mark only one oval per row.

	1	2	3	4	5
Disinformation (Fake News, Manipulated/Fabricated/Doctored Content, etc.)	◯	◯	◯	◯	◯
Malinformation (Confidential Information Leak, Disclosures, etc.)	◯	◯	◯	◯	◯
Propaganda	◯	◯	◯	◯	◯
Conspiracy Theory	◯	◯	◯	◯	◯
Other	◯	◯	◯	◯	◯

25. Which of the following do you consider to be the most challenging for SOCMINT? (1 = not important at all - 5 = Extremely important) *

Mark only one oval per row.

	1	2	3	4	5
Fake Profiles	◯	◯	◯	◯	◯
Social Bots	◯	◯	◯	◯	◯
Trolls	◯	◯	◯	◯	◯
Filter Bubbles	◯	◯	◯	◯	◯
Echo Chambers	◯	◯	◯	◯	◯
Information overload	◯	◯	◯	◯	◯
Astroturfing (fake grass-roots movement)	◯	◯	◯	◯	◯
Profile/ID cloning	◯	◯	◯	◯	◯
User's Biases	◯	◯	◯	◯	◯

26. Which of the following do you consider important for SOCMINT (1 = not important at all - 5 = Extremely important). *

Mark only one oval per row.

	1	2	3	4	5
Verification tools	◯	◯	◯	◯	◯
Social Network visualization tools	◯	◯	◯	◯	◯
Social search tools	◯	◯	◯	◯	◯
Continuous training	◯	◯	◯	◯	◯
None of the above	◯	◯	◯	◯	◯

27. Is there anything else that you would like to share with the researchers?

Βιβλιογραφικές Αναφορές

Andrews, S., Brewster, B. & Day, T. (2018). Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online. Secur Inform 7(3) https://doi.org/10.1186/s13388-018-0032-8

Allcott, H., & Gentzkow, M. (March 01, 2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives,* 31 (2): 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf

Bartlett. J., & Reynolds, L. (2015). State of the art 2015: a literature review of social media intelligence capabilities for counter-terrorism. Demos. http://www.demos.co.uk/wp-content/uploads/2015/09/State_of_the_Arts_2015.pdf (Ανάκτηση 26.04.2021).

Boyd, D., Ellison, N., Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, 13(1):210–230, https://doi.org/10.1111/j.1083-6101.2007.00393.x

Boyd, D., The Information War Has Begun, 27 January 2017. http://www.zephoria.org/thoughts/archives/2017/01/27/the-information-war-has-begun.html

Brandtzæg, P. B. (2010). Towards a unified media-user typology (MUT): A meta-analysis and review of the research literature on media-user typologies. *Computers in Human Behavior,* 26(5): 940–956.

Bradshaw, S. & Howard, P. (2018a). "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Computational Propaganda Working Paper (2018). https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf (Ανάκτηση 19.04.2021).

Bradshaw, S. & Howard, P. (2018b). The Global Organization of Social Media Disinformation

Campaigns, 17 Σεπτεμβρίου 2018. Journal of International Affairs. https://jia.sipa.columbia.edu/global-organization-social-media-disinformation-campaigns (Ανάκτηση 29.04.2021).

Bradshaw, S. & Howard, P. (2019). "The global disinformation order: 2019 global inventory of organised social media manipulation". https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf (Ανάκτηση 19.04.2021).

Bulut, E., & Yörük, E. (2017). Mediatized Populisms| Digital Populism: Trolls and Political Polarization of Twitter in Turkey. *International Journal Of Communication,* 11(25).https://ijoc.org/index.php/ijoc/article/view/6702/2158 (Ανάκτηση 07.05.2021).

Christakis, N. A., & Fowler, J. H. (2009). Connected: The surprising power of our social networks and how they shape our lives. New York: Little, Brown and Co. http://connectedthebook.net/pdf/excerpt.pdf (Ανάκτηση 18.04.2021).

Clayton, K., Davis, J., Hinckley, K., & Horiuchi, Y. (2019). Partisan motivated reasoning and misinformation in the media: Is news from ideologically uncongenial sources more suspicious? *Japanese Journal of Political Science*, 20(3): 129-142. doi:10.1017/S1468109919000082.

Coll, S (2017). Donald Trump's 'Fake News' tactics. 11 Δεκεμβρίου 2017. https://www.newyorker.co/agazin/01///onald-trumps-fake-news-tactics. The New Yorker (Ανάκτηση 23.3.2021).

Deibert, R., & Rohozinski, R. (2010). Control and subversion in Russian cyberspace. Στο Ronald Deibert et al. Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace https://library.oapen.org/bitstream/id/983c1e21-331d-4693-8ab4-04fa665a903f/1004009.pdfv (Ανάκτηση, 01.05.2021).

European Commission - Publications Office of the European Union (2018a), A multi-dimensional approach to disinformation: Report of the independent High-level Group on fake news and online disinformation, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en#document-info (Ανάκτηση 11.04.2021).

European Commission (2018b), Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, Tackling online disinformation: a European Approach, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN (Ανάκτηση 12.04.2021).

Golbeck, J. (2019). Benford's Law can detect malicious social bots. *First Monday*, 24(8). https://doi.org/10.5210/fm.v24i8.10163

Gyenes, N., Seymour, B., (2017). Public Health Echo Chambers in a Time of Mistrust & Misinformation - Digital Health. *The Berkman Klein Center for Internet & Society at Harvard University*. https://cyber.harvard.edu/events/digitalhealth/2017/02/GyenesSeymour (Ανάκτηση 27.04.2021)

Irak, D. (2016). A Close-Knit Bunch: Political Concentration in Turkey's Anadolu Agency through Twitter Interactions, *Turkish Studies*, 17(2): 336-360, DOI: 10.1080/14683849.2016.1138287 https://www.researchgate.net/publication/295840859_A_Close-Knit_Bunch_Political_Concentration_in_Turkey's_Anadolu_Agency_through_Twitter_Interactions (Ανάκτηση, 30.04.2021).

Kaplan, A.M. & Haenlein, M. (2010) Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons,* 53(1): 59-68. http://dx.doi.org/10.1016/j.bushor.2009.09.003

Keane, J. (2013). Media decadence. In *Democracy and Media Decadence* (pp. 109-190). Cambridge: Cambridge University Press. doi:10.1017/CBO9781107300767.003.

Kerem Karaosmanoğlu (2021) The discourse of üst akıl: a search for hegemony in the Turkish media, *Southeast European and Black Sea Studies*, 21(1): 77-99, DOI: 10.1080/14683857.2021.1872233.

Kwon, O., & Wen, Y. (2010). An empirical study of the factors affecting social network service

use. *Computers in Human Behavior,* 26(2): 254–263. https://doi.org/10.1016/j.chb.2009.04.011

Li, Charlene, Bernoff, Josh, et al (2007). "Social Technographics. Mapping Participation in Activities Forms the Foundation of a Social Strategy". http://www.tccta.org/links/Committees/pub-archive/Social-Technographics.pdf (Ανάκτηση 13.3.2021)

Li HO, Bailey A, Huynh D, Chan J. YouTube as a source of information on COVID-19: a pandemic of misinformation? *BMJ Glob Health*. 2020 May; 5(5):e002604. doi: 10.1136/bmjgh-2020-002604.

MacKinnon, R. (2011). Liberation Technology: China's "Networked Authoritarianism". *Journal of Democracy* 22(2), 32-46. doi:10.1353/jod.2011.0033.

Mayfield, A. (2008). *What is Social Media?*.iCrossing eBook, διαθέσιμο στον ιστότοπο: http://www.icrossing.co.uk/fileadmin/uploads/eBooks/What_is_Social_Media_iCrossing_ebook.pdf (30.12.2020).

MHS and GCHQ "Get in the Game" with Target Development for World of Warcraft Online Gaming. https://www.documentcloud.org/documents/889134-games (Ανάκτηση 11.3.2021).

National Intelligence Council, Foreign Threats to the 2020 US Federal Elections, 10 March 2021. https://int.nyt.com/data/documenttools/2021-intelligence-community-election-interference-assessment/abd0346ebdd93e1e/full.pdf

Nelson, L (2017), Trump claims his base is 'Getting Stronger' despite 'Fake News'. 7 Αυγούστου 2017. http://www.politico.co/tor/01///rump-new-york-times-criticism-241378 Politico. (Ανάκτηση 23.3.2021).

Nye, J. S. (1990). Bound to lead: The changing nature of American power. New York: Basic Books.

Oğuz, M. C., & Demirkol, O. (2019). Networked Authoritarianism in Turkey: Jdp's Political Trolling and Astroturfing. (235-256) Στο συλλογικό βιβλίο των Chiluwa, I., & Bourvier, G. (2019). Activism, campaigning and political discourse on Twitter. https://paromitapain.com/wp-content/uploads/2019/12/Activsim-Twitter-discorse.pdf (Ανάκτηση, 30.04.2021).

Omand, D., Bartlett, J. & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT), *Intelligence and National Security*, 27(6): 801-823, DOI: 10.1080/02684527.2012.716965

Pariser, E. (2011). The filter bubble: How the new personalized web is changing what we read and how we think. Penguin. https://hci.stanford.edu/courses/cs047n/readings/The_Filter_Bubble.pdf (Ανάκτηση 25.04.2021).

Saka, E. (2018). Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling, *Middle East Critique*, 27(2): 161-177, DOI: 10.1080/19436149.2018.1439271 https://www.researchgate.net/publication/323379843_Social_Media_in_Turkey_as_a_Space_for_Political_Battles_AKTrolls_and_other_Politically_motivated_trolling (Ανάκτηση, 30.04.2021).

Schönberger, V.M. & Cukier, K. (2014). Big Data: A Revolution that Will Transform how We Live, Work, and Think, Houghton Mifflin Harcourt.

Schuchard, R., Crooks, A.T., Stefanidis, A. et al. (2019) Bot stamina: examining the influence and staying power of bots in online social networks. *Appl Netw Sci* 4(55). https://doi.org/10.1007/s41109-019-0164-x (Ανάκτηση 20.04.2021).

Shulsky, A. N., & Schmitt, G. J. (2002). *Silent warfare: Understanding the world of intelligence*. (EBL.) Washington, D.C: Brassey's, Inc. https://books.google.nl/books?printsec=frontcover&vid=LCCN93013181&redir_esc=y#v=onepage&q&f=false (Ανάκτηση 13.04.2021).

Solon, O. & Levin, S. (2016). How Google's search algorithm spreads false information with a rightwing bias. The Guardian: https://www.theguardian.com/technology/2016/dec/16/google-autocomplete-rightwing-bias-algorithm-political-propaganda (Ανάκτηση 13.04.2021).

Solon, O. (2017). The future of fake news: Don't believe everything you see, hear or read, The Guardian: https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content (Ανάκτηση 03.04.2021).

Stieglitz, S., Brachten, F., Berthelé, D., Schlaus, M., Venetopoulou, C., & Veutgen, D. (2017). Do Social Bots (Still) Act Different to Humans? - Comparing Metrics of Social Bots with Those of Humans. HCI.

Szwed, Robert, Framing of the Ukraine-Russia Conflict in Online and Social Media, *NATO Strategic Communications Centre of Excellence*, May 2016. https://www.stratcomcoe.org/framing-ukraine-russia-conflict-online-and-social-media (Ανάκτηση 25.04.2021).

Tsvetkova, M., García-Gavilanes, R., Floridi, L., & Yasseri, T. (2017). Even good bots fight: The case of Wikipedia. *PloS one*, 12(2), e0171774.

Ţuţui, V. (2017, July). Some reflections concerning the problem of defining propaganda. In Argumentum: *Journal of the Seminar of Discursive Logic, Argumentation Theory & Rhetoric*, 15(2): 110-125. https://journals.indexcopernicus.com/api/file/viewByFileId/222890.pdf (Ανάκτηση 13.04.2021).

United Nations, Department of Global Communications, UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis, https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19 (Ανάκτηση 05.04.2021).

U.S. Senate, Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election

https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

United States Department of Justice, United States of America v. Internet Research Agency (18 U.S.C. 2,371,1349,1028A), 2018. https://www.justice.gov/file/1035477/download (Ανάκτηση 19.04.2021).

Vickery, G. & Wunsch-Vincent S. (2007) Participative Web and User Created Content, Web. 2.0, Wikis and Social Networking, Paris: *OECD Publishing*, διαθέσιμο στον ιστότοπο http://www.oecd.org/digital/ieconomy/38393115.pdf

Vilmer, J.-B. Jeangène, Escorcia, A., Guillaume, M., Herrera, J., (2018). Les Manipulations de l'information : un défi pour nos démocraties, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées. https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf

Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (Ανάκτηση 14.04.2021).

Wardle, C. (October 2019), Understanding Information Disorder, Firstdraft. https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701 (Ανάκτηση 14.04.2020).

Waterson, J. (2018) Democracy at risk due to fake news and data misuse, MPs conclude. The Guardian: https://www.theguardian.com/technology/2018/jul/27/fake-news-inquiry-data-misuse-deomcracy-at-risk-mps-conclude (Ανάκτηση 11.04.2021).

Woolley, S. & Howard, P. (2017) "Computational Propaganda Worldwide: Executive Summary," Working Paper, Project on Computational Propaganda, Oxford University.

https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf (Ανάκτηση 20.3.2021).

Woolley S. (2019). United States: Manufacturing Consensus online. In Woolley, S. C., & In Howard, P. N. (2019). Computational propaganda: Political parties, politicians, and political manipulation on social media. https://books.google.nl/books?hl=el&lr=&id=qTpxDwAAQBAJ&oi=fnd&pg=PP1&dq=computational+propaganda+constructive+consent&ots=foI4WpqnLi&sig=GCUdgM-GwkjEXHrclc7zL8IPrVw#v=onepage&q&f=false (Ανάκτηση, 13.05.2021).

Zurkowski, Paul G. & National Commission on Libraries and Information Science, Washington, DC. National Program for Library and Information Services. (1974). *The Information Service Environment Relationships and Priorities*. Related Paper No. 5. ERIC Clearinghouse, https://files.eric.ed.gov/fulltext/ED100391.pdf (Ανάκτηση 05.04.2021).