

ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES



ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΔΙΕΘΝΕΙΣ, ΕΥΡΩΠΑΪΚΕΣ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΕΣ ΣΠΟΥΔΕΣ»
ΚΑΤΕΥΘΥΝΣΗ: ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ

Οι πληροφοριακές επιχειρήσεις ως εργαλείο υψηλής στρατηγικής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Βαΐτσης

Αθήνα, 2018

Τριμελής Επιτροπή

Χαράλαμπος Παπασωτηρίου, Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Κωνσταντίνος Αρβανιτόπουλος, Καθηγητής Παντείου Πανεπιστημίου

Κωνσταντίνος Κολιόπουλος, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου



Copyright © Γεώργιος Βαΐτσης, 2018

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω υπεύθυνα ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Ακόμα δηλώνω ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα προσωπικά και αποκλειστικά και ειδικά για τη συγκεκριμένη διπλωματική εργασία και ότι θα αναλάβω πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχθεί ότι δε μου ανήκει.

Όνοματεπώνυμο

Γεώργιος Βαΐτσης

A.M.

1217M018

Υπογραφή

Περιεχόμενα

Περίληψη – Λέξεις Κλειδιά.....	9
Abstract – Keywords	10
1. Εισαγωγή	11
1.1 Εισαγωγή.....	11
1.2 Σκοπός.....	12
1.3 Μεθοδολογία ανάλυσης.....	12
ΜΕΡΟΣ Α΄	
2. Οι Πληροφοριακές Επιχειρήσεις	15
2.1 Περί πληροφοριακών επιχειρήσεων	15
2.1.1 Το πληροφοριακό περιβάλλον	15
2.1.2 Οι πληροφοριακές επιχειρήσεις	16
2.1.3 Επίπεδα απειλής και μέθοδοι επιθέσεων στο πληροφοριακό περιβάλλον....	19
2.2 Είδη πληροφοριακών επιχειρήσεων	21
2.2.1 Οι ΠΕ ως συντελεστές επαύξησης της ισχύος	21
2.2.2 Τύποι πληροφοριακών επιχειρήσεων.....	22
2.3 Προπαγάνδα και παραπληροφόρηση	24
2.3.1 Προπαγάνδα, μια παλιά ιστορία.....	24
2.3.2 Παραπληροφόρηση, η μαύρη προπαγάνδα με άλλο όνομα	26
2.3.3 Η προπαγάνδα κομμάτι του «υβριδικού πολέμου».....	27
2.4 Ο κυβερνοχώρος και η εργαλειοποίηση των ΜΚΔ και του διαδικτύου.....	28
2.4.1 Ο κυβερνοχώρος ως διάσταση	28
2.4.2 Η φύση του Κυβερνοχώρου	29
2.4.3 Επιχειρήσεις στον Κυβερνοχώρο.....	30
2.4.4 Τα Μέσα Κοινωνικής Δικτύωσης και το διαδίκτυο ως όπλο	32
3. Υψηλή Στρατηγική	35
3.1 Θεωρία της Υψηλής Στρατηγικής.....	35
3.2 Οι διαστάσεις υψηλής στρατηγικής.....	36

3.3 Στον 21 ^ο αιώνα.....	37
-------------------------------------	----

ΜΕΡΟΣ Β΄

4. Περιπτωσιολογική Μελέτη: Ο πόλεμος των 34 ημερών.	41
4.1 Το χρονικό της σύγκρουσης.....	41
4.2 Ποιοι ήταν οι σκοποί που έθεσαν οι δρώντες.....	43
4.3 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν	45
4.4 Επιτευχθέντα αποτελέσματα.....	50
5. Περιπτωσιολογική Μελέτη: Ο Ρωσικός παράγοντας στη ε-σθονία	53
5.1 Το χρονικό της σύγκρουσης.....	53
5.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν	55
5.3 Τι σκοπούς εξυπηρετούσαν	58
5.4 Επιτευχθέντα αποτελέσματα.....	59
6. Περιπτωσιολογική Μελέτη: Το «Ισλαμικό Χαλιφάτο»	61
6.1 Πηγαίνοντας πίσω στο χρόνο.....	61
6.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν	62
6.3 Τι σκοπούς εξυπηρετούσαν	67
6.4 Επιτευχθέντα αποτελέσματα.....	68
7. Περιπτωσιολογική Μελέτη: Η σύγκρουση Ρωσίας – Ουκρανίας	71
7.1 Το χρονικό της σύγκρουσης.....	71
7.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν	72
7.3 Τι σκοπούς εξυπηρετούσαν	77
7.4 Επιτευχθέντα αποτελέσματα.....	78
8. Επίμετρο – Συμπεράσματα	79
Βιβλιογραφία – Πηγές	83

Εικόνες

Εικόνα 2.1: Οι τρεις τομείς του Κυβερνοχώρου.....	29
Εικόνα 2.2: Μοναδικοί χρήστες του διαδικτύου (% του παγκόσμιου πληθυσμού) ...	33
Εικόνα 4.1: Περιοχές του Λιβάνου που επλήγησαν από τις Ισραηλινές αεροπορικές δυνάμεις	42
Εικόνα 4.2: Απεικόνιση των δυνάμεων που είχε αναπτύξει η Χεζμπολαχ στο Λίβανο το 2006.....	44
Εικόνα 4.3: Δείχνοντας τον Nasrallah ως την πηγή του κακού.....	45
Εικόνα 4.4: Δείχνοντας τον Nasrallah ως μαριονέτα Συρίας, Ιράν και Παλαιστίνης	45
Εικόνα 4.5: Προκήρυξη με την οποία προειδοποιεί του πολίτες του Λιβάνου για τις περιοχές τις οποίες θα επιχειρήσει ο Ισραηλινός στρατός.....	46
Εικόνα 4.6: Η ενημέρωση που ερχόταν στα κινητά τηλέφωνα όλων των συνδρομητών που βρίσκονταν στην περιοχή.....	46
Εικόνα 4.7: Από την ιστοσελίδα All4Lebanon.org	47
Εικόνα 4.8: Εικόνες που απεικόνιζαν τον Ισραηλινό Πρόεδρο ως NAZI.....	49
Εικόνα 4.9: Η Θεϊκή Νίκη	50
Εικόνα 5.1: Ρώσος στρατιώτης από την Ημέρα της Νίκης.....	57
Εικόνα 5.2: Ιστοσελίδα η οποία είχε χακαριστεί από τους Ρώσους	57
Εικόνα 5.3: Οδηγίες και εργαλεία για επιθέσεις DDoS.....	57
Εικόνα 6.1: Τα δίκτυα προπαγάνδας του ISIS ανά τον κόσμο	63
Εικόνα 6.2: Πολιτικοστρατιωτική συνεργασία ISIS στην αστυνόμευση και στη φορολόγηση	64
Εικόνα 6.3: Media Center του ISIS	64
Εικόνα 6.4: Διαδικτυακές πλατφόρμες που χρησιμοποιεί το ISIS	65
Εικόνα 6.5: Εξώφυλλα των περιοδικών Rumiya και Dabiq	66
Εικόνα 6.6: Οι Σκοποί των Πληροφοριακών Επιχειρήσεων του ISIS.....	67
Εικόνα 7.1: Φωτογραφία που διανεμήθηκε από το διαδίκτυο για να ενισχύσει το προφίλ του Προέδρου Putin.....	73
Εικόνα 7.2: Φωτογραφίες που διανεμήθηκαν μέσω Facebook μετά το δημοψήφισμα και την προσάρτηση της Κριμαίας	74
Εικόνα 7.3: Φωτογραφία για την υπονόμευση του Ουκρανικού Στρατού	75
Εικόνα 7.4: Τα «Μικρά Πράσινα Ανθρωπάκια»	76

Πίνακες

Πίνακας 1. Δραστηριότητες πληροφοριακών επιχειρήσεων και τομείς επιρροής19

Περίληψη – Λέξεις Κλειδιά

Η πολυπλοκότητα διαχείρισης του πληροφοριακού περιβάλλοντος και οι επιδράσεις που αυτό δέχεται από διάφορες στρατιωτικές και μη δραστηριότητες, η εμφάνιση νέων φορέων και μορφών απειλών οδήγησαν στην ανάγκη αντιμετώπισης τέτοιων δραστηριοτήτων που εμπλέκονται με την πληροφορία, μέσω μιας ευρύτερης συντονιστικής στρατηγικής. Εξαιτίας όμως της φύσης του πληροφοριακού περιβάλλοντος οι επιθέσεις είναι πολύ δύσκολο να ανιχνευθούν, καθώς είναι δυνατό να σχεδιασθούν με τέτοιο τρόπο ώστε τα αποτελέσματα να είναι ορατά μετά από καθορισμένο χρόνο. Στρατηγική, είναι εκείνη η τέχνη χρησιμοποίησης πολιτικών, οικονομικών, ψυχολογικών και στρατιωτικών μέσων, τόσο στην ειρήνη όσο και στον πόλεμο, ώστε να παρέχεται η μέγιστη δυνατή υποστήριξη στην εθνική πολιτική. Ως εκ τούτου αποτελεί εργαλείο της πολιτικής για την επίτευξη των σκοπών της, διαμορφώνεται τόσο στην ειρήνη όσο και στον πόλεμο, ενώ είναι δυνατό να επιτύχει τους πολιτικούς σκοπούς της, χωρίς να προστρέξει σε πολεμικές επιχειρήσεις, δημιουργώντας στον αντίπαλο μια τέτοια ψυχολογική κατάσταση ώστε να πειστεί ότι είναι ανώφελο να επιδιώξει μια σύγκρουση. Στο επίπεδο της Υψηλής Στρατηγικής, οι Πληροφοριακές Επιχειρήσεις εντάσσονται στο όλο πλαίσιο των δραστηριοτήτων που αποσκοπούν στην επίτευξη των εθνικών στόχων, μέσω της προσβολής, αποδιοργάνωσης ή εξουδετέρωσης εκείνων των στοιχείων που συγκροτούν το αντίπαλο δυναμικό και απειλούν τα φίλια συμφέροντα. Οι πόλεμοι σήμερα δεν έχουν καθορισμένα μέτωπα και πλέον δεν μπορούμε να συζητάμε για σαφή στρατιωτικά μέτωπα και μέτωπα μετόπισθεν, δεν είναι μονάχα μεταξύ κρατικών δρώντων, αλλά αντάρτικων ομάδων, τρομοκρατικών δικτύων, πολιτοφυλακών οι οποίες συνδέονται άμεσα ή όχι, φανερά ή όχι πιθανόν και με κρατικούς δρώντες. Αυτό οδηγεί πλέον στη χρησιμοποίηση μέσων τα οποία δεν διαθέτουν όλα δύναμη πυρός, ενώ συνήθως τις περισσότερες φορές δεν προκαλούν και θύματα. Στην παρούσα διπλωματική εργασία θα εξεταστούν ως περιπτώσιολογικές μελέτες οι πληροφοριακές επιχειρήσεις που έλαβαν χώρα στις συγκρούσεις Ισραήλ – Hezbollah το 2006, η περίπτωση της Εσθονίας το 2007, καθώς και οι πληροφοριακές επιχειρήσεις του ISIS και της Ρωσίας στην Ουκρανία από το 2014 και μετά.

Λέξεις Κλειδιά: Πληροφοριακές Επιχειρήσεις, Υψηλή Στρατηγική, Προπαγάνδα, Παραπληροφόρηση, Κυβερνοχώρος

Abstract – Keywords

The complexity on management of the information environment the impacts on that from various military and non-military activities, the emergence of new carriers and threats, have led to the need to address such information-related activities through a broader coordination strategy. However, due to the nature of the information environment, attacks are extremely difficult to be detected, as they can be designed in such way that the results are visible after a set of time. Strategy is the art of using political, economic, psychological and military means, both in peace and war, in order to provide the maximum possible support for national politics. It is therefore, a policy tool for achieving its goal, shaped not only during peace but also on war, and it is possible to achieve its political goals without going to war, creating a psychological condition to the opponent that will convince him that is useless to seek a conflict. As for Grand Strategy, information operations are part of the whole framework of activities aimed at achieving national goals, by inflicting, disrupting or eliminating those elements that constitute the opponent and threaten the friendly interests. The contemporary wars have no definite frontline and so we can no longer discuss for clear military fronts and backwards, for state and non-state actors which might be from guerilla groups, to terrorist networks and militias directly or not connected, disguised or not with state actors. This leads to the use of means that they may not all have the firepower that others have and usually they do not cause victims as well. In this diploma thesis, will be considered as case studies the information operations that took place during the Israeli-Hezbollah conflict in 2006, the Estonian case in 2007, as well as ISIS's and Russia's information operations in Ukraine from 2014 and beyond.

Keywords: Information Operations, Grand Strategy, Propaganda, Disinformation, Cyberspace

1. Εισαγωγή

1.1 Εισαγωγή

Ο Joseph Nye Jr. στο βιβλίο του *Soft Power: The means to success in world politics* αναφέρει ότι «κερδίζοντας την καρδιά και το μυαλό ήταν πάντοτε πολύ σημαντικό, στη σύγχρονη όμως εποχή της παγκόσμιας πληροφόρησης, είναι ακόμα σημαντικότερο» ενώ σχετικά με το τι είναι ισχύς, συνεχίζει ότι «...ισχύς είναι η δυνατότητα [κάποιος] να επηρεάζει τη συμπεριφορά των άλλων, ώστε να επιτυγχάνει το αποτέλεσμα που επιθυμεί». (Nye Jr., 2004, σ. 1-2) Γίνεται πλέον αντιληπτή η ψυχολογική διάσταση που λαμβάνουν οι συγκρούσεις και ότι πέρα από τη στρατιωτική στρατηγική πρέπει να λαμβάνεται υπόψη και το πως θα επηρεαστεί και η βούληση του αντιπάλου και όχι μόνο.

Οι οικονομικές και κοινωνικές συνθήκες στις οποίες διαβιώνουμε στο πλαίσιο της παγκοσμιοποίησης, έχουν καταστήσει τη γνώμη της μάζας σημαντική για τον επηρεασμό της πολιτικής και τη λήψη αποφάσεων. Η τεχνολογία σήμερα επιτρέπει τους πολίτες να ενημερώνονται με πολλούς τρόπους, την τηλεόραση, το ραδιόφωνο το διαδίκτυο. Οπότε και τα μέσα επιρροής ως εργαλείο για την επίτευξη των πολιτικών σκοπών ενός δρώντα πρέπει να εναρμονίζονται ταυτόχρονα. Η απλή ρίψη φυλλαδίων και η ανάρτηση αφισών με τα ανάλογα προπαγανδιστικά μηνύματα δεν είναι πλέον αρκετή.

Πλέον παρατηρείται μια πιο εξελιγμένη μορφή προπαγάνδας, αυτή της παραπληροφόρησης και της διάδοσης κατασκευασμένων ψευδών ειδήσεων οι οποίες αποσκοπούν στον αποπροσανατολισμό του ακροατηρίου ή στον βομβαρδισμό του με πληθώρα ανούσιων ειδήσεων που το ωθούν να χάνει στο τέλος την ουσία της είδησης. Βέβαια σε αυτό συνεπικουρείται και από τα Μέσα Κοινωνικής Δικτύωσης τα οποία έχουν τη δυνατότητα πλέον να μεταφέρουν την πληροφορία, ακόμα και σαν εικόνα ή βίντεο σε όλο τον κόσμο μέσω του διαδικτύου και σε εκατομμύρια χρήστες ταυτόχρονα.

Όμως και στον οικονομικό τομέα η διασύνδεση όλων των δραστηριοτήτων μέσω του διαδικτύου, μπορεί μεν να εξασφαλίζει ταχύτητα και ευελιξία, όμως αφήνει παράθυρο κακόβουλης εκμετάλλευσης από επίδοξους δρώντες οι οποίοι όντας κράτη, μπορεί να μην αποβλέπουν σε οικονομικά οφέλη τα ίδια, αλλά στο να προκαλέσουν μια απώλεια στην οικονομία της χώρας που στοχεύουν και κυρίως στο να πλήξουν την ίδια την αξιοπιστία της στο εσωτερικό, στους ίδιους τους πολίτες της, προκαλώντας πανικό ειδικά εάν συντονίζεται με κάποια άλλη μορφή πληροφοριακής επιχείρησης,

και στο εξωτερικό, παρουσιάζοντας στη διεθνή κοινότητα τη χώρα στόχο ως ένα failed state.

Βέβαια τα αποτελέσματα που μέχρι σήμερα έχουν καταγραφεί από τις πληροφοριακές επιχειρήσεις που έχουν λάβει χώρα είναι αρκετά πρώιμα. Όμως η πρακτική που ακολουθείται δείχνει ότι όλο και περισσότερο θα αξιοποιούνται αυτής της μορφής επιχειρήσεις, ενώ ισχυροί δρώντες στη διεθνή σφαίρα ενσωματώνουν στα δόγματά τους και στις στρατηγικές τους όλο και περισσότερες αυτής της μορφής επιχειρήσεις.

1.2 Σκοπός

Σκοπός της παρούσας εργασίας είναι να γίνει μία αναφορά σε πληροφοριακές επιχειρήσεις που έχουν λάβει χώρα τα τελευταία δεκαπέντε χρόνια και οι οποίες εξυπηρέτησαν έως ένα βαθμό τους πολιτικούς στόχους που είχαν θέσει οι δρώντες. Δεν θα επικεντρωθεί στις στρατιωτικές επιχειρήσεις που έλαβαν οι στρατιωτικές δυνάμεις, καθώς αποσκοπεί στη μελέτη των επιχειρήσεων στο πληροφοριακό περιβάλλον και στην προσπάθεια επηρεασμού.

1.3 Μεθοδολογία ανάλυσης

Στο πρώτο μέρος της εργασίας θα επιχειρηθεί η ανάπτυξη του θεωρητικού πλαισίου. Αρχικά θα προσδιοριστεί η έννοια των πληροφοριακών επιχειρήσεων και θα αναλυθεί η μορφή που αυτές μπορούν να λάβουν, ενώ από το όλο φάσμα που καλύπτουν, θα επικεντρωθούμε στην προπαγάνδα, την παραπληροφόρηση, τη χρήση του κυβερνοχώρου και την εργαλειοποίηση των Μέσων Κοινωνικής Δικτύωσης. Ως προς την υψηλή στρατηγική θα γίνει μια αποτύπωση θεωριών που έχουν αναπτυχθεί ενώ στο δεύτερο μέρος της εργασίας θα ακολουθήσει μια περιπτωσιολογική μελέτη στην οποία παρουσιάζονται σε ποιες διαστάσεις της υψηλής στρατηγικής αποσκοπούσαν οι πληροφοριακές επιχειρήσεις που έλαβαν χώρα και κατά πόσον επέτυχαν ή όχι τους πολιτικούς σκοπούς που ετέθησαν.

Θα ξεκινήσει με την μελέτη της σύγκρουσης Ισραήλ – Hezbollah το 2006, ενώ θα συνεχίσει στη μελέτη της Εσθονίας το 2007 καθώς οι δύο αυτές περιπτώσεις αποτελούν τις πρώτες καταγεγραμμένες μορφές πληροφοριακών επιχειρήσεων, με τη διαχείριση της πληροφορία στην πρώτη περίπτωση και με την μεγαλύτερη έως τότε, στην περίπτωση της δεύτερης κλίμακας κυβερνοεπίθεση η οποία χάραξε και την πολιτική των περισσότερων χωρών στον κυβερνοχώρο. Θα συνεχίσει με την μελέτη

των πληροφοριακών επιχειρήσεων του ISIS και της Ρωσίας στην Κριμαία και την Ανατολική Ουκρανία οι οποίες ξεκίνησαν το 2014, ενός μη κρατικού και ενός κρατικού δρώντα αντίστοιχα και μαίνονται μέχρι σήμερα και οι οποίες αποτελούν την πιο ολοκληρωμένη μορφή τέτοιων επιχειρήσεων.

ΜΕΡΟΣ Α΄

2. Οι Πληροφοριακές Επιχειρήσεις

«Αν η αυτοπεποίθηση είναι όντως η μισή μάχη, τότε η υπονόμηση της αυτοπεποίθησης του εχθρού είναι περισσότερο από την άλλη μισή - επειδή αποφέρει καρπούς χωρίς να απαιτεί να πολεμήσεις με όλες σου τις δυνάμεις.»

Sir Basil Henry Liddell Hart

2.1 Περί πληροφοριακών επιχειρήσεων

2.1.1 Το πληροφοριακό περιβάλλον

Από το 1440 οπότε και τέθηκε σε λειτουργία η πρώτη εκτυπωτική μηχανή του Gutenberg, η οποία συνέβαλε οριστικά στην διάδοση της πληροφορίας σε μεγάλη κλίμακα (γεωγραφική και όγκου), μέχρι και σήμερα έχουν υπάρξει πολύ μεγάλες αλλαγές στο πληροφορικό περιβάλλον. Η ανακάλυψη του τηλέγραφου το 1844 είχε σαν αποτέλεσμα να μειώσει το χρόνο ενημέρωσης του κοινού, καθώς μπορούσε να μεταφέρει ειδήσεις και κυρίως τις πολεμικές ανταποκρίσεις σε μεγάλες αποστάσεις σε λίγα μόνο λεπτά μετά την εξέλιξή τους. Στην προ-ίντερνετ εποχή, ο έντυπος τύπος, η τηλεόραση και το ραδιόφωνο έπαιζαν το σημαντικότερο ρόλο στη διακίνηση της πληροφορίας. Η τεχνολογική έκρηξη όμως που έχει λάβει χώρα κυρίως τα τελευταία 20 χρόνια, είχε σαν αποτέλεσμα ο οποιοσδήποτε να μπορεί να αποκτήσει φωνή, με την ποιότητα της πληροφορίας να αμφισβητείται ακόμα περισσότερο. Όμως πριν μιλήσουμε για το πληροφοριακό περιβάλλον και τις διάφορες μορφές επιχειρήσεων που μπορούν να λάβουν χώρα εντός του, ας προσπαθήσουμε πρώτα να ορίσουμε τι είναι πληροφοριακό περιβάλλον.

Σύμφωνα με το λεξικό του Υπουργείου Άμυνας της Αμερικής ορίζει ως πληροφοριακό περιβάλλον «Το σύνολο των ατόμων, οργανισμών και συστημάτων που συλλέγουν, επεξεργάζονται, διανέμουν ή ενεργούν στην πληροφορία.» (U.S. Joint Chief of Staff, 2010 όπως τροποποιήθηκε το 2016, σ. 110) Στο δόγμα Πληροφοριακών Επιχειρήσεων των ΗΠΑ (U.S. Joint Chief of Staff, 2012 όπως τροποποιήθηκε το 2014) γίνεται μια πιο λεπτομερής ανάλυση του παραπάνω ορισμού προσθέτοντας ότι:

Αυτό το περιβάλλον αποτελείται από τρεις αλληλένδετες διαστάσεις, οι οποίες συνεχώς αλληλεπιδρούν με άτομα, οργανισμούς και συστήματα. Αυτές οι διαστάσεις είναι γνωστές ως φυσικές, πληροφοριακές και γνωστικές. Η φυσική διάσταση αποτελείται από συστήματα διοίκησης και ελέγχου, βασικούς φορείς

λήψης αποφάσεων και υποστηρικτική υποδομή που επιτρέπει σε άτομα και οργανισμούς να παράγουν αποτελέσματα. Η πληροφοριακή διάσταση προσδιορίζει πού και πώς συλλέγονται, επεξεργάζονται, αποθηκεύονται, διαδίδονται και προστατεύονται οι πληροφορίες. Η γνωστική διάσταση συμπεριλαμβάνει το νοητικό μέρος εκείνων που μεταδίδουν, λαμβάνουν και ανταποκρίνονται ή ενεργούν σε πληροφορίες.

Το αποτύπωμα του παραπάνω ορισμού, ενσωματώθηκε και στο δόγμα των αμερικανικών χερσαίων δυνάμεων (U.S. Army TRADOC, 2009), όπου καταδεικνύονται οι δυνατότητες τις οποίες πρέπει να αναπτύξουν κατά την περίοδο 2016-2020 ώστε να αντιμετωπίσουν τις αναδυόμενες απειλές, και αναφέρει συγκεκριμένα ότι :

Επειδή ο πόλεμος παραμένει θεμελιωδώς ένας διαγωνισμός θέλησης, που επικρατεί στη μελλοντική ένοπλη σύγκρουση, θα απαιτήσει από τις στρατιωτικές δυνάμεις να ασκήσουν ψυχολογική και τεχνολογική επιρροή. Οι προσπάθειες ψυχολογικής επιρροής χρησιμοποιούν συνδυασμούς συνεργατικών, πειστικών και καταναγκαστικών μέσων για να βοηθήσουν και να υποστηρίξουν συμμάχους και εταίρους, να προστατεύσουν και να καθησυχάσουν τους πληθυσμούς και να απομονώσουν και νικήσουν τους εχθρούς. Η άσκηση τεχνολογικής επιρροής συνεπάγεται την προστασία φίλων πληροφοριών και επικοινωνιών και τη παρεμπόδιση της ικανότητας του εχθρού να διαδίδει και να χειρίζεται πληροφορίες.

Στην ελληνική βιβλιογραφία «το παγκόσμιο πληροφοριακό περιβάλλον περιλαμβάνει πρόσωπα, οργανισμούς ή συστήματα επικοινωνιών και πληροφορικής τα οποία συλλέγουν, επεξεργάζονται και διανέμουν πληροφορίες σε εθνικούς και διεθνείς αποδέκτες.» (ΓΕΣ, 2012, σ. 5) και σύμφωνα με το Δόγμα Πληροφοριακών Επιχειρήσεων του ΓΕΕΘΑ (ΓΕΕΘΑ, ΔΕ 3.2 «Διακλαδικό Δόγμα Πληροφοριακών Επιχειρήσεων», 2016, σσ. 1-2) περιλαμβάνει:

- την πληροφορία σε οποιαδήποτε μορφή και χρόνο
- τις υποδομές, δηλαδή τα επικοινωνιακά-πληροφοριακά συστήματα, μέσα από τα οποία διακινείται, επεξεργάζεται και αποθηκεύεται η πληροφορία
- το λογισμικό, το οποίο πιθανώς να συνδέεται με οποιοδήποτε τρόπο αναπαραγωγής, διακίνησης ή αποθήκευσής της
- οργανισμούς, πρόσωπα, υποδομές, υπηρεσίες, οργανώσεις σχετιζόμενες με την πληροφορία, τα περισσότερα των οποίων συλλέγουν, επεξεργάζονται και διανέμουν πληροφορίες σε εθνικούς και διεθνείς αποδέκτες ή παίζουν αποφασιστικό ρόλο στο μηχανισμό λήψης αποφάσεων.

2.1.2 Οι πληροφοριακές επιχειρήσεις

Παρατηρώντας πίσω στο χρόνο, θα δούμε ότι στις αρχές του 20^{ου} αιώνα, οι συγκρούσεις διεξάγονταν σε δύο διαστάσεις – στην ξηρά και στη θάλασσα. Με την είσοδο του αεροσκάφους, προστέθηκε και μια τρίτη διάσταση, αυτή του αέρα. Στα μέσα της δεκαετίας του 1950, μια τέταρτη διάσταση ήρθε στο προσκήνιο, αυτή του διαστήματος, οδηγώντας κυρίως τις μεγάλες δυνάμεις της εποχής, να προσπαθούν να εγκαθιδρύσουν την κυριαρχία τους στο διάστημα με την εκτόξευση δορυφόρων (επικοινωνιών, χαρτογράφησης, κατασκοπευτικών κλπ.) καθώς και επανδρωμένων και μη αποστολών, φθάνοντας μέχρι και το σημείο ο Πρόεδρος των ΗΠΑ Ronald Reagan να ανακοινώνει στις 23 Μαρτίου 1983 την ίδρυση του συστήματος Strategic Defense Initiative (SDI)¹.

Το 1990 όμως το διαδίκτυο άρχισε να απλώνεται παγκοσμίως και χάρη στα μοναδικά χαρακτηριστικά του (1) να κινητοποιεί τους χρήστες με τη βοήθεια συμβατικών μέσων να συμμετέχουν στο πολιτικό σύστημα, (2) να διανέμει μεγάλο όγκο πληροφοριών αμφιβόλου όμως ποιότητας και ακρίβειας καθώς και (3) να διασπείρει την πληροφορία σε όλο τον κόσμο, άμεσα με αποτέλεσμα να μην τίθενται πλέον γεωγραφικά εμπόδια, κατάφερε πλέον να κυριαρχεί στη ζωή μας, σε πολιτικό, οικονομικό και στρατιωτικό επίπεδο. Εύλογα επομένως μπορεί να θεωρηθεί ως η πέμπτη διάσταση στην οποία λαμβάνουν χώρα πλέον οι συγκρούσεις.

Βέβαια το πληροφοριακό περιβάλλον, όπως αναφέρθηκε παραπάνω είναι το πλαίσιο στο οποίο άνθρωποι και αυτοματοποιημένα συστήματα παρατηρούν, εστιάζουν, επεξεργάζονται και ενεργούν ανάλογα με τις διατιθέμενες πληροφορίες. Βεβαίως ανατρέχοντας στην ιστορία θα δούμε την ύπαρξη μορφών πληροφοριακών επιχειρήσεων και πριν την ανάπτυξη του διαδικτύου, όπως η μεταβολή της ανθρώπινης στάσης και συμπεριφοράς με την χρήση της προπαγάνδας, την αποκρυπτογράφηση των μηνυμάτων του εχθρού και τη χρήση της παραγόμενης πληροφορίας καθώς και με την παραπλάνηση και την προσβολή φυσικών μέσων που ασκούσαν επιρροή στις δυνάμεις του εχθρού. Πλέον όλα τα συστήματα διοίκησης και ελέγχου, C4I², κάνουν ευρεία χρήση της τεχνολογίας για τη διαχείριση (παραγωγή, διακίνηση και αποθήκευση) της πληροφορίας.

¹ Το SDI αφορούσε την ανάπτυξη αμερικανικών συστημάτων τόσο στο έδαφος όσο και στο διάστημα, έτσι ώστε να δύναται να αποφευχθεί οποιαδήποτε ρωσική επίθεση με βαλλιστικούς διηπειρωτικούς πυραύλους. Πήρε μάλιστα το προσωνύμιο «STAR WARS», από τη δημοφιλή ομότιτλη σειρά ταινιών της εποχής. (President Reagan's Remarks on the Strategic Defense Initiative (SDI) to High Level Defense Officials and Staff in the Blue Room , 23 Μαρτίου 1983)

² C4I: Command, Control, Communications, Computers and Intelligence

Σύμφωνα με το Dictionary of Military and Associated Terms των ΗΠΑ δυνατότητα σχετιζόμενη με την πληροφορία ορίζεται « κάθε εργαλείο, τεχνική ή δραστηριότητα που χρησιμοποιείται σε μια διάσταση του πληροφοριακού περιβάλλοντος και που μπορεί να χρησιμοποιηθεί για τη δημιουργία αποτελεσμάτων και λειτουργικά επιθυμητών συνθηκών.» (U.S. Joint Chief of Staff, 2010 όπως τροποποιήθηκε το 2016, σ. 111). Αντλώντας λοιπόν επιπλέον στοιχεία από το Νατοϊκό Δόγμα Πληροφοριακών Επιχειρήσεων (AJP 3.10, 2015), το Αμερικανικό Δόγμα Πληροφοριακών Επιχειρήσεων (JP 3-13, 2014), το Βρετανικό Δόγμα Πληροφοριακών Επιχειρήσεων (JWP 3-80, 2002) καθώς και το Ελληνικό Δόγμα Πληροφοριακών Επιχειρήσεων (ΔΕ 3.2, 2016) μπορούμε να ορίσουμε τις πληροφοριακές επιχειρήσεις ως εκείνη τη λειτουργία με την οποία αναλύονται, σχεδιάζονται, εκτιμώνται και αλληλοεπιδρούν οι οποιεσδήποτε πληροφοριακές δραστηριότητες με σκοπό την επίτευξη των επιθυμητών αποτελεσμάτων στη θέληση, κατανόηση ικανότητα των αντιπάλων ή πιθανών αντιπάλων για την υποστήριξη των τιθέμενων αντικειμενικών σκοπών.

Και από ρωσικής πλευράς όμως υπάρχει έντονο ενδιαφέρον. Η Ρωσία επενδύει πάρα πολύ στην ασφάλεια των πληροφοριών και στον πληροφοριακό πόλεμο καθώς και στα εργαλεία και στην έρευνα γύρω από αυτόν. Η μακροχρόνια εμπειρία της στην προπαγάνδα, σε συνδυασμό με μεγάλες επενδύσεις στον τομέα των μέσων ενημέρωσης, καθιστούν τις πληροφοριακές επιχειρήσεις την πιο επικίνδυνη απειλή που καλούνται να αντιμετωπίσουν σήμερα τα κράτη μέλη της ΕΕ και του ΝΑΤΟ. Το πιο σημαντικό σχετικό έγγραφο που ασχολείται με την ρωσική κατανόηση του πληροφοριακού πολέμου είναι το Δόγμα Πληροφοριακής Ασφάλειας της Ρωσικής Ομοσπονδίας, το οποίο έχει εγκριθεί από τον ίδιο τον Vladimir Putin στις 5 Δεκεμβρίου 2016 και είναι αναρτημένο στην ιστοσελίδα του Υπουργείου Εξωτερικών της Ρωσικής Ομοσπονδίας. Το όλο έγγραφο επικεντρώνεται αποκλειστικά στην πληροφοριακή ασφάλεια της χώρας και ορίζει ποια είναι η πληροφοριακή ασφάλεια, το περιβάλλον, τις απειλές και τις υποδομές³.

Το πληροφοριακό περιβάλλον περιλαμβάνει στις τρεις διαστάσεις που αναφέρθηκαν παραπάνω (φυσική, πληροφοριακή και γνωστική) τα εξής πεδία:

- το φυσικό χώρο

³ Για περισσότερες πληροφορίες σχετικά με το Δόγμα Πληροφοριακής Ασφάλειας της Ρωσικής Ομοσπονδίας: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICk6BZ29/content/id/2563163 (πρόσβαση στις 7/10/2018)

- τον κυβερνοχώρο
- το ηλεκτρομαγνητικό φάσμα
- την ανθρώπινη στάση και συμπεριφορά
- τις δημόσιες σχέσεις, το περιβάλλον των σύγχρονων ΜΜΕ

Επακόλουθο είναι και οι πληροφοριακές επιχειρήσεις να δραστηριοποιούνται σε τομείς οι οποίοι με οιονδήποτε τρόπο να επηρεάζουν στα ανωτέρω πεδία. Στον πίνακα 3.1 γίνεται μια συνοπτική παρουσίαση των δραστηριοτήτων αυτών και του τομέα τον οποίο επηρεάζουν.

Πίνακας 1. Δραστηριότητες πληροφοριακών επιχειρήσεων και τομείς επιρροής

Δραστηριότητα πληροφοριακών επιχειρήσεων	Τομέας στον οποίο επηρεάζουν
Ηλεκτρονικός Πόλεμος	Ηλεκτρονική Επίθεση Ηλεκτρονική Άμυνα
Επιχειρήσεις Κυβερνοχώρου	Επιτήρηση του Ηλεκτρονικού Φάσματος Επιθέσεις σε δίκτυα Η/Υ Εκμετάλλευση δικτύων Η/Υ Προστασία δικτύων Η/Υ – Κυβερνοάμυνα
Υποστήριξη Πληροφοριακών Επιχειρήσεων (Ψυχολογικές Επιχειρήσεις)	Επιρροή σε συγκεκριμένα ακροατήρια των αντιλήψεων, της στάσης και τη συμπεριφοράς τους για την επίτευξη των ημετέρων αντικειμενικών σκοπών
Ασφάλεια Επιχειρήσεων	Η χρήση παθητικών ή ενεργητικών μέτρων για την αποφυγή διαρροής πληροφοριών στον αντίπαλο
Φυσική Προσβολή	Φυσική προσβολή η οποία θα έχει σημαντικό Ψυχολογικό αντίκτυπο
Επιχειρήσεις Παραπλάνησης	Εξαπάτηση του αντιπάλου με κατάλληλους χειρισμούς
Επιχειρήσεις ΜΜΕ – Δημοσίων Σχέσεων	Σχετίζονται με τις πληροφοριακές επιχειρήσεις και κυρίως τις ψυχολογικές, παραμένοντας όμως ξεχωριστές και αποσκοπούν στην έγκαιρη, έγκυρη και αντικειμενική δημόσια πληροφόρηση αντικρούοντας την αντίπαλη παραπληροφόρηση
Πολιτικοστρατιωτική Συνεργασία	Αυτού του είδους οι επιχειρήσεις μπορούν να αποτελέσουν το συνδετικό κρίκο στρατιωτικών και πολιτικών αρχών (Κυβερνητικών και Μη Οργανώσεων), παρέχοντας πολλές πληροφορίες καθώς και λειτουργώντας ως γέφυρα επικοινωνίας

2.1.3 Επίπεδα απειλής και μέθοδοι επιθέσεων στο πληροφοριακό περιβάλλον

Μπορούμε να ορίσουμε τέσσερα επίπεδα απειλής μέσα στο πληροφοριακό περιβάλλον, τα οποία κατηγοριοποιούνται ως εξής:

- Πρώτο επίπεδο απειλής: αφορά πρόσωπα ή μικρές ομάδες ερασιτεχνών οι οποίοι χρησιμοποιούν απλές μεθόδους και τεχνικές κακόβουλης εισβολής, χωρίς σημαντική υποστήριξη.
- Δεύτερο επίπεδο απειλής: αφορά πρόσωπα ή μικρές ομάδες οι οποίες υποστηρίζονται από εμπορικές εταιρείες, εγκληματικές οργανώσεις ή άλλες διεθνείς ομάδες και χρησιμοποιούν εξελιγμένες μεθόδους διεξαγωγής επιθετικών ΠΕ. Στο επίπεδο αυτό περιλαμβάνονται και οι τρομοκρατικές ομάδες. Οι δε δραστηριότητές τους περιλαμβάνουν κατασκοπεία, συλλογή δεδομένων, δικτυακή χαρτογράφηση ή αναγνώριση και κλοπή δεδομένων.
- Τρίτο επίπεδο απειλής: αφορά πρόσωπα ή μικρές ομάδες οι οποίες υποστηρίζονται από κρατικούς οργανισμούς (στρατιωτικούς ή πολιτικούς) με σημαντικούς πόρους και χρησιμοποιούν υψηλής τεχνολογίας μέσα ή άτομα στρατολογημένα ή φιλικά διακείμενα προς τον αντίπαλο που διαθέτουν νομικά κατοχυρωμένη πρόσβαση στα ημέτερα συστήματα και πληροφορίες. Οι δραστηριότητές τους περιλαμβάνουν τις ενέργειες που αναφέρθηκαν και στο προηγούμενο επίπεδο απειλής.
- Τέταρτο επίπεδο απειλής: αφορά επιθετικές ενέργειες κρατών, ειδικά στον τομέα του κυβερνοχώρου με τη χρήση εργαλείων τεχνολογίας αιχμής και κεκαλυμμένων τεχνικών σε συντονισμό με άλλες μορφές επιχειρήσεων.

Όπως υποδεικνύεται στο Δόγμα Πληροφοριακών Επιχειρήσεων του ΓΕΕΘΑ «Σε στρατηγικό επίπεδο, οι ΠΕ εντάσσονται στο πλαίσιο της πληροφοριακή εκστρατείας της χώρας, που αποσκοπεί στην επίτευξη των εθνικών στόχων, μέσω της προσβολής, αποδιοργάνωσης ή εξουδετέρωσης εκείνων των στοιχείων (πολιτικών, στρατιωτικών, οικονομικών κλπ.) που συγκροτούν το αντίπαλο εθνικό δυναμικό και απειλούν τα εθνικά μας συμφέροντα.» (ΓΕΕΘΑ, ΔΕ 3.2 «Διακλαδικό Δόγμα Πληροφοριακών Επιχειρήσεων», 2016) Ο αντίπαλος δύναται να χρησιμοποιήσει διάφορες μεθόδους προκειμένου να επιτεθεί στο φίλιο σύστημα διοίκησης κι ελέγχου ή να διαμορφώσει το πληροφοριακό περιβάλλον προς όφελός του. Εξαιτίας όμως της φύσης του πληροφοριακού περιβάλλοντος οι επιθέσεις είναι πολύ δύσκολο να ανιχνευθούν, καθώς είναι δυνατό να σχεδιασθούν με τέτοιο τρόπο ώστε τα αποτελέσματα να είναι ορατά μετά από καθορισμένο χρόνο. Οι ενέργειες με τις οποίες

δύναται να υλοποιηθούν τέτοιες επιθέσεις μπορεί να είναι: (1) ενέργειες κυβερνοπολέμου⁴ (2) χρήση προπαγάνδας και παραπληροφόρησης⁵ και (3) φυσική προσβολή με σημαντική επιρροή επί του αντιπάλου⁶.

2.2 Είδη πληροφοριακών επιχειρήσεων

2.2.1 Οι ΠΕ ως συντελεστές επαύξησης της ισχύος

Η πληροφορία ήταν πάντοτε ένα σημαντικό στοιχείο στις στρατιωτικές επιχειρήσεις. Η δυνατότητα συλλογής πληροφοριών έγκαιρα και με ακρίβεια έχει αναδειχθεί σε κρίσιμο παράγοντα της διοίκησης και ελέγχου, της στρατηγικής ευελιξίας και του επιχειρησιακού ελιγμού. Όποιος ελέγχει, προστατεύει και χρησιμοποιεί την πληροφορία, αλλά και τα πληροφοριακά συστήματα, με τον καλύτερο δυνατό τρόπο, διαθέτει αποφασιστικό πλεονέκτημα.

Μια από τις πιο δύσκολες πτυχές του ραγδαία εξελισσόμενου πληροφοριακού περιβάλλοντος, είναι ο αυξανόμενος αντίκτυπος που έχει ο στρατηγικός έλεγχος του αφηγήματος γύρω από τις δραστηριότητές τους από κρατικούς και μη δρώντες. Χρησιμοποιώντας συχνά εμπορικά μέσα, σύγχρονες και ψηφιακές τεχνολογίες οι δρώντες αποκτούν πρόσβαση σε παγκόσμιο ακροατήριο και διαδίδουν αληθείς, προκατειλημμένες αλλά και ψευδείς πληροφορίες προκειμένου να στρατολογήσουν οπαδούς, να κερδίσουν αποδοχή και υποστήριξη, να εκμεταλλευτούν ή να απονομιμοποιήσουν ενέργειες του αντιπάλου τους. Σήμερα περισσότερο από ποτέ οι ενέργειες των δρώντων στοχεύουν σε μη στρατιωτικό ακροατήριο, με μια ισχυρή σε συμβολισμούς στρατηγική επικοινωνία, δημιουργώντας ένα σημαντικό βαθμό επιρροής.

Η συνδυασμένη χρησιμοποίηση πληροφοριακών δραστηριοτήτων και προσβολών «σκληρών» και «μαλακών» στόχων, είναι απαραίτητη για την επίτευξη του αντικειμενικού σκοπού. Τα μέσα στοχοποίησης είναι δευτερεύουσας σημασίας για την επίτευξη των επιθυμητών αποτελεσμάτων, ειδικά καθώς οι στόχοι δεν εμπίπτουν μόνο στο φυσικό επίπεδο, αλλά περιλαμβάνουν τις αντιλήψεις και ενέργειες πολιτών, ηγετικών μορφών της πολιτικής και της στρατιωτικής ηγεσίας του αντιπάλου.

⁴ Επίθεση της Ρωσικής Ομοσπονδίας στα πληροφοριακά συστήματα της Εσθονίας τον Απρίλιο του 2007 και αμερικανο-ισραηλινή επίθεση στο πυρηνικό πρόγραμμα του Ιράν με τον ιό STUXNET.

⁵ Ενέργειες που χρησιμοποιήθηκαν πρόσφατα ευρέως από το DAESH αλλά και τη Ρωσία στην Ουκρανία

⁶ Η πιο γνωστή πρόσφατη ενέργεια τέτοιου είδους είναι τα «Πράσινα Ανθρωπάκια» (little green men) που έκαναν την εμφάνισή τους και συνέβαλαν καθοριστικά στην περιοχή της Κριμαίας το 2014.

2.2.2 Τύποι πληροφοριακών επιχειρήσεων

2.2.2.1 Επιθετικές πληροφοριακές επιχειρήσεις είναι ενέργειες οι οποίες αναλαμβάνονται προκειμένου να επηρεάσουν πληροφορίες, διαδικασίες παραγωγής πληροφοριών, τα συστήματα C4I του αντιπάλου καθώς και τα συστήματα επικοινωνιών και πληροφορικής που χρησιμοποιεί σε περίοδο ειρήνης, κρίσης ή πολέμου, για την επίτευξη συγκεκριμένων αντικειμενικών σκοπών. Στόχος είναι να καταστρέψουν, υποβαθμίσουν, διασπάσουν, απαγορεύσουν, παραπλανήσουν, εκμεταλλευτούν και επηρεάσουν τα κέντρα λήψης αποφάσεων του αντιπάλου. Έχουν γενικά δύο αντικειμενικούς σκοπούς, (1) να επηρεασθεί η αντίληψη και η εικόνα του αντιπάλου για την κατάσταση, να υπονομευθεί η θέλησή του, να μειωθεί η αποφασιστικότητά του, να εμφανισθεί η ήττα ως αναπόφευκτη, προσφέροντας παράλληλα εναλλακτικούς τρόπους ενέργειας και (2) να περιοριστεί στο ελάχιστο η δυνατότητα αποτελεσματικής διοίκησης και ελέγχου καθώς και ανάληψη οποιαδήποτε πρωτοβουλίας.

2.2.2.2 Αμυντικές πληροφοριακές επιχειρήσεις είναι οι ενέργειες οι οποίες λαμβάνονται με σκοπό να προστατεύσουν τη φίλια διαδικασία λήψης αποφάσεων, εξασφαλίζοντας τη πρόσβαση και την αποτελεσματική χρησιμοποίηση των πληροφοριών, των φίλιων C4I επικοινωνιών και συστημάτων πληροφορικής σε περιόδους ειρήνης, κρίσης ή πολέμου. Στόχος είναι η εξασφάλιση, σε όλα τα επίπεδα λήψης αποφάσεων, της συνεχόμενης ροής αξιόπιστων πληροφοριών οι οποίες μπορούν να επηρεάσουν την κατάσταση. Αποσκοπούν (1) στη μείωση της ικανότητας του αντιπάλου να επιδράσει στα φίλια συστήματα διοίκησης και ελέγχου και (2) στη μείωση της τρωτότητας των φίλιων συστημάτων σε περίπτωση ανάληψης τέτοιων πρωτοβουλιών από τον αντίπαλο, διασφαλίζοντας την έγκαιρη, ακριβή και εγγυημένη πρόσβαση στην πληροφορία, ενώ ταυτόχρονα αποτρέπουν την πρόσβαση του αντιπάλου στις φίλιες πληροφορίες και πληροφοριακά συστήματα.

2.2.2.3 Μορφές πληροφοριακών επιχειρήσεων μπορούμε να βρούμε τόσο στο στρατιωτικό όσο και στον πολιτικό/εμπορικό τομέα. Σύμφωνα με τη ΝΑΤΟϊκή και ελληνική βιβλιογραφία οι στρατιωτικές δραστηριότητες που εμπλέκονται στη διεξαγωγή πληροφοριακών επιχειρήσεων είναι: ο ηλεκτρονικός πόλεμος, οι επιχειρήσεις κυβερνοχώρου, οι ψυχολογικές επιχειρήσεις (προπαγάνδα/αντιπροπαγάνδα), η στρατιωτική παραπλάνηση, η ασφάλεια επιχειρήσεων, η φυσική προσβολή και οι επιχειρήσεις μέσων ενημέρωσης. Σύμφωνα

με τον Martin Libicki⁷ υπάρχουν επτά δραστηριότητες πληροφοριακών επιχειρήσεων οι οποίες δύναται αλληλοϋποστηριζόμενες να επιτύχουν στρατηγικά αποτελέσματα και τις οποίες όρισε ως εξής: επιχειρήσεις διοίκησης και ελέγχου, πληροφοριών, ηλεκτρονικού πολέμου, ψυχολογικές, πληροφοριακό πόλεμο στον οικονομικό τομέα, επιχειρήσεις χάκερ και επιχειρήσεις κυβερνοχώρου. (Libicki M. , 1995)

Ο πληροφοριακός πόλεμος και οι πληροφοριακές επιχειρήσεις δεν αποτελούν νέο φαινόμενο, αντιθέτως απαντώνται στο βάθος της ιστορίας της ανθρώπινης κοινωνίας, καθώς το διακύβευμα δεν είναι μόνο φυσικό, αλλά και ψυχολογικό. Τα τελευταία βέβαια χρόνια απέκτησε μεγαλύτερη δυναμική, καθώς η τεχνολογική ανάπτυξη που γνώρισε ο κόσμος και η αυξανόμενη αλληλεξάρτηση όλων των συστημάτων είχε σαν αποτέλεσμα να μπορεί πλέον να κινητοποιεί μεγαλύτερες μερίδες πληθυσμού. Μα αυτόν τον τρόπο, κάνοντας ευρεία χρήση και εκμετάλλευση πληροφοριακών συστημάτων και της σχετικά νέας διάστασης του κυβερνοχώρου μπορεί κάποιος τόσο σε περίοδο ειρήνης, αλλά και σε περιόδους κρίσης και πολέμου, να κατευθύνει συνειδήσεις, αντιλήψεις και να καθοδηγήσει κοινωνίες προς όποια κατεύθυνση εκείνος επιθυμεί, προϋπόθεση βέβαια, να πετύχει κυριαρχία πάνω στην πληροφορία έναντι του αντιπάλου του.

Η διοίκηση και ο έλεγχος αποτελούν ένα πολύ σημαντικό κομμάτι τόσο σε πολιτικό επίπεδο, αλλά κυρίως στις στρατιωτικές επιχειρήσεις. Τα συστήματα συλλογής πληροφοριών και εγκαίρου προειδοποιήσεως είναι πολύ σημαντικά για οποιοδήποτε επίπεδο διοίκησης, προκειμένου τα κέντρα αποφάσεων να δύναται να λάβουν έγκαιρα τις σωστές εκείνες αποφάσεις για την αντιμετώπιση μιας κρίσιμης κατάστασης. Η αποτυχία συγκέντρωσης πληροφοριών και μετάδοσης των αντίστοιχων οδηγιών ενεργειών θα αποτελεί μια πρόκληση τόσο στη φυσική διάσταση όσο και στην πληροφοριακή διάσταση. Είναι σημαντικό τα όργανα λήψης αποφάσεων του αντιπάλου να λαμβάνουν παραποιημένες πληροφορίες (παραπλάνηση, ηλεκτρονικός πόλεμος) και να μη μπορούν να μεταφέρουν τις εντολές τους στα υφιστάμενα κλιμάκια (ηλεκτρονικός πόλεμος, φυσική προσβολή) αλλά και να προστατευθούν τα ημέτερα συστήματα διοίκησης και ελέγχου.

Ο έλεγχος του ηλεκτρομαγνητικού φάσματος αποτελεί το πεδίο στο οποίο δραστηριοποιείται ο ηλεκτρονικός πόλεμος και αποσκοπεί είτε στην εξεύρεση της

⁷ Αμερικανός καθηγητής και ερευνητής στη Ναυτική Ακαδημία των ΗΠΑ όπου εκτός από το ακαδημαϊκό του έργο, ασχολείται και με την έρευνα στον κυβερνοπόλεμο και στην τεχνολογία πληροφοριακών συστημάτων.

θέσης του αντίπαλου μέσω των ηλεκτρομαγνητικών κυμάτων που εκπέμπει, είτε με την παρεμπόδιση των ηλεκτρομαγνητικών σημάτων που εκπέμπει, αφαιρώντας του έτσι τη δυνατότητα να ασκεί τον έλεγχο των τμημάτων του.

Στις ψυχολογικές επιχειρήσεις ο κύριος σκοπός είναι η επιρροή του αντιπάλου. Η προπαγάνδα (όρος ο οποίος χρησιμοποιήθηκε ευρέως τα προηγούμενα χρόνια) ή παραπληροφόρηση (όρος ο οποίος εισήχθη κυρίως από τη Σοβιετική Ένωση στα τέλη της δεκαετίας του 1940) αποσκοπεί να αλλοιώσει μια υπάρχουσα πληροφορία ή να δημιουργήσει μια ψευδή πληροφορία, ώστε να οδηγήσει τα κέντρα λήψης αποφάσεων στην κατεύθυνση εκείνου που επεμβαίνει επί της πληροφορίας. Η τηλεόραση, το ραδιόφωνο και πολύ περισσότερο πλέον το διαδίκτυο παίζουν πολύ σημαντικό ρόλο στις ψυχολογικές επιχειρήσεις. Στις ψυχολογικές επιχειρήσεις η αλήθεια δεν έχει ιδιαίτερη σημασία, αρκεί να επιτευχθεί ο σκοπός. Κάτι το οποίο παρουσιάζεται «άσπρο» σήμερα, μπορεί αύριο να θεωρείται «μαύρο».

Στον οικονομικό/εμπορικό τομέα οι πληροφοριακές επιχειρήσεις στοχεύουν κυρίως στα πληροφοριακά συστήματα μιας χώρας, οδηγώντας την ουσιαστικά σε ένα “ηλεκτρονικό μεσαίωνα”. Τα σύγχρονα οικονομικά και εμπορικά συστήματα είναι διασυνδεδεμένα στο διαδίκτυο, με αποτέλεσμα μια τέτοια επίθεση θα είχε σαν αποτέλεσμα να προσβληθεί η αξιοπιστία μιας χώρας τόσο στα εσωτερικά όσο και στα εξωτερικά κοινά, προκαλώντας μεγάλες απώλειες στον οικονομικό τομέα.

Οι επιχειρήσεις hacking και κυβερνοπολέμου είναι κάτι σχετικά καινούργιο με ολοένα αυξανόμενο πεδίο δράσης. Αποτελεί πλέον συνήθη είδηση η παραβίαση και το μπλοκάρισμα ή παραποίηση μιας ιστοσελίδας ή ενός λογαριασμού στα Μέσα Κοινωνικής Δικτύωσης, η συλλογή πληροφοριών για ένα πρόσωπο ή ομάδα προσώπων. Η ταυτοποίηση πλέον του αντιπάλου γίνεται ακόμα πιο δύσκολη, καθώς μέσα στον παγκόσμιο ιστό όπου λαμβάνουν χώρα οι παραπάνω επιχειρήσεις δεν μπορείς να εντοπίσεις το ποιος ή από που ενεργεί.

2.3 Προπαγάνδα και παραπληροφόρηση

2.3.1 Προπαγάνδα, μια παλιά ιστορία

Αρχικά η λέξη προπαγάνδα σήμαινε τη διάδοση ή προώθηση ιδεών και αποτυπώθηκε για πρώτη φορά στο λατινικό κείμενο που εξέδωσε η Ρωμαιοκαθολική εκκλησία το 1622 υπό τον πάπα Γρηγόριο τον XV με τίτλο *Sacra Congregatio de Propaganda Fide* και αφορούσε μια ομάδα καθολικών ιερέων και τις ενέργειές τους για τη διάδοση της

καθολική θρησκείας σε άλλες χώρες. Αργότερα όμως η λέξη απέκτησε μια πιο πολιτική χροιά και έτσι σύμφωνα με το Oxford English Dictionary προπαγάνδα κατέληξε να σημαίνει «Η συστηματική διάδοση πληροφοριών, με προκατειλημμένο ή παραπλανητικό τρόπο για την προώθηση πολιτικών σκοπών». (OED, 2007) Το NATO ορίζει σαν προπαγάνδα «Πληροφορίες, ειδικά προκατειλημμένης ή παραπλανημένης φύσεως, για την προώθηση πολιτικών σκοπών ή απόψεων». (NATO, 2017)

Η προπαγάνδα μπορεί να χρησιμοποιηθεί τόσο από τα κράτη, προκειμένου να επιτύχουν τους αντικειμενικούς τους σκοπούς αλλά και από μη κρατικούς δρώντες (επαναστατικές ή τρομοκρατικές ομάδες) οι οποίοι μέσω της προπαγάνδας προσπαθούν να επιτύχουν είτε διεθνή νομιμοποίηση είτε ενίσχυση των πόρων τους (οικονομικών ή ανθρώπινων) για την επίτευξη της δικής τους ατζέντας. Όπως όμως μεταλλάχθηκε η προπαγάνδα στο πέρασμα του χρόνου και από εργαλείο κρατικών κυρίως δρώντων πέρασε να αποτελεί εργαλείο πολλών μη κρατικών δρώντων, έτσι και τα μέσα διάδοσής της εξελίχθηκαν, από απλές αφίσες, στο ραδιόφωνο, στην τηλεόραση, στο διαδίκτυο και ευρύτερα πλέον στα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ).

Η χρήση της προπαγάνδας ως μέσο διαχείρισης της ροής της πληροφορίας, επηρεασμού της κοινής γνώμης ή συμπεριφοράς μιας ομάδας ατόμων, οδήγησε να θεωρείται κυρίαρχο στοιχείο στις ψυχολογικές επιχειρήσεις. Κατά NATO λοιπόν ψυχολογικές επιχειρήσεις ορίζονται «Οι σχεδιασμένες εκείνες ενέργειες οι οποίες χρησιμοποιούν μεθόδους επικοινωνίας και άλλα μέσα, κατευθύνονται εναντίον εγκεκριμένων ακροατηρίων προκειμένου να επηρεάσουν αντιλήψεις, τάσεις και συμπεριφορές, και επηρεάζουν την επίτευξη πολιτικών και στρατιωτικών σκοπών». (NATO, 2017) Διακρίνει τρεις μορφές προπαγάνδας τις οποίες κατηγοριοποιεί ως εξής: (1) *Λευκή προπαγάνδα* όταν η πηγή εκπομπής της είναι γνωστή και χρησιμοποιεί πραγματικά γεγονότα και αληθή μηνύματα με πειστικό όμως τρόπο. Αν και βασίζεται σε πραγματικά στοιχεία, παρουσιάζει το μήνυμα προκατειλημμένα οδηγώντας προς εκείνη την κατεύθυνση που επιθυμεί. (2) *Γκρίζα προπαγάνδα* όταν δεν υπάρχει συγκεκριμένα προσδιορισμένη πηγή και με αυτόν τον τρόπο κρύβεται ο δημιουργός της και (3) *Μαύρη προπαγάνδα* όταν αποδίδεται λανθασμένα σε άλλη πηγή από την πραγματική. Η Τρίτη μορφή της μπορεί επίσης να περιγράψει τη χρήση παραπληροφόρησης, η οποία απλώνει ψευδείς πληροφορίες παρουσιάζοντάς τες ως αληθείς με σκοπό το ακροατήριο να μην συνειδητοποιεί ότι προπαγανδίζεται.

2.3.2 Παραπληροφόρηση, η μαύρη προπαγάνδα με άλλο όνομα

Σύμφωνα πάλι με το Oxford English Dictionary παραπληροφόρηση ορίζεται «Η διάδοση σκόπιμα αναληθών πληροφοριών, ιδίως όταν παρέχεται από μία κυβέρνηση ή όργανό της σε μια ξένη δύναμη ή στα μέσα ενημέρωσης, αποσκοπώντας να επηρεάσει την πολιτική ή την άποψη όσων λαμβάνουν αυτές τις πληροφορίες». Στο ίδιο βρίσκουμε επίσης ότι η πρώτη αναφορά στη λέξη γίνεται στις 3 Ιουνίου 1955 στο περιοδικό *The Times* και έκτοτε είχε συσχετιστεί και αναφέρονταν στη μαύρη προπαγάνδα που αποδίδονταν στη Σοβιετική Ένωση και στη μετέπειτα διάδοχό της Ρωσία.

Στην αγγλική ορολογία η λέξη παραπληροφόρηση αποδίδεται τόσο ως *disinformation* αλλά και ως *misinformation*. Η Ευρωπαϊκή Ένωση όμως σύμφωνα με το IATE (InterActive Terminology of Europe), ξεκαθαρίζει ότι ο όρος *disinformation* δεν θα πρέπει να συγχέεται με τον όρο *misinformation*, καθώς ο πρώτος εμπλέκει δόλο. (Ευρωπαϊκό Κοινοβούλιο, 2015) Το NATO από την άλλη δεν αναφέρει καθόλου τον όρο παραπληροφόρηση, όμως κρατά μια επαμφοτερίζουσα στάση καθώς ακόμα και ο ίδιος ο γ.γ. Jens Stoltenberg σε δηλώσεις του χρησιμοποίησε και τους δύο όρους^{8,9}. Ο όρος όμως παραπληροφόρηση αποδίδεται μόνο για τις δραστηριότητες της Ρωσίας, αφήνοντας για τις δραστηριότητες άλλων δρώντων τον όρο προπαγάνδα. Σε μια προσπάθεια της Ε.Ε. να αντισταχθεί στις δραστηριότητες παραπληροφόρησης της Ρωσίας, ιδιαίτερα μετά την κατάληψη της Κριμαίας το 2014, όπου και εμφανίστηκε η έκταση του προβλήματος, δημιουργήθηκε ένα όργανο υπό της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης το οποίο έχει αναλάβει να εκδίδει το εβδομαδιαίο περιοδικό *Disinformation Review* για την ενημέρωση των ευρωπαίων πολιτών και μηχανισμών λήψης απόφασης.¹⁰

Σήμερα όμως, το παγκόσμιο πληροφοριακό περιβάλλον είναι πολυσύνθετο και ραγδαία μεταβαλλόμενο, απαιτεί επομένως συνεργασία και συντονισμό όλων εκείνων των δραστηριοτήτων που πρέπει να λάβει ένας δρών προκειμένου να επιτύχει τον

⁸ NATO. (2015, Μάιος 18). Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the meeting of the EU Foreign Affairs Council in the format of Ministers of Defense and Ministers of Foreign Affairs. Ανάκτηση Οκτώβριος 14, 2018, από https://www.nato.int/cps/en/natohq/opinions_119822.htm?selectedLocale=en

⁹ NATO. (2015, Ιούνιος 25). Press Conference by NATO Secretary General Jens Stoltenberg following the meeting of the NATO-Ukraine Commission at the level of Defense Ministers - Secretary General's opening remarks. Ανάκτηση Οκτώβριος 14, 2018, από https://www.nato.int/cps/en/natohq/opinions_120971.htm?selectedLocale=en

¹⁰ Περισσότερα για το *Disinformation Review* στην ιστοσελίδα <https://euvsdisinfo.eu/> (πρόσβαση στις 14/10/2018)

αντικειμενικό του σκοπό. Οι αμερικανικές ΕΔ το 2010 αποφάσισαν όπως τροποποιήσουν τον όρο ψυχολογικές επιχειρήσεις, χρησιμοποιώντας πλέον τον όρο *στρατιωτικές επιχειρήσεις υποστήριξης των πληροφοριακών (Military Information Support Operations – MISO)* και δίνοντας τον ορισμό «Σχεδιασμένες επιχειρήσεις για τη μετάδοση επιλεγμένων πληροφοριών και ενδεικτών σε ξένα ακροατήρια προκειμένου να επηρεάσουν τα συναισθήματά τους, τα κίνητρά τους, τον αντικειμενικό συλλογισμό τους και τελικά τη συμπεριφορά ξένων κυβερνήσεων, οργανώσεων, ομάδων και ατόμων με τρόπο ευνοϊκό για τους αντικειμενικούς τους σκοπούς». (U.S. Joint Chief of Staff, 2010 όπως τροποποιήθηκε το 2016) Στον παραπάνω ορισμό φαίνεται ξεκάθαρα τη σημασία που έχει λάβει πλέον η προπαγάνδα/παραπληροφόρηση στο ευρύτερο παιχνίδι της επικοινωνίας και της προσπάθειας επιρροής των μαζών.

2.3.3 Η προπαγάνδα κομμάτι του «υβριδικού πολέμου»

Πολλοί είναι πλέον αυτοί που πιστεύουν ότι η φύση των πολεμικών συγκρούσεων έχει αλλάξει δραστικά και θα αλλάξει ακόμα περισσότερο. Όπως αναφέρεται στο άρθρο του Steve Abrams *Beyond Propaganda Soviet Active Measures in Putin's Russia* ο Thomas Nissen επισημαίνει ότι «Ο πόλεμος δεν θα είναι πλέον μεταξύ κρατών Οι σύγχρονοι πόλεμοι θα γίνονται περισσότερο για την απόκτηση ελέγχου πάνω σε πληθυσμούς και στα όργανα λήψης απόφασης, παρά ελέγχου πάνω σε εδαφικές περιοχές». (Abrams, 2016) Ο όρος υβριδικός πόλεμος άρχισε να εμφανίζεται το 2005 και χαρακτηρίσε κυρίως τις δραστηριότητες της Χεζμπολάχ το 2006 στη σύγκρουση Λιβάνου – Ισραήλ. Όμως ακόμα το NATO δεν μπορεί να δώσει ένα σαφή ορισμό του υβριδικού πολέμου, αν και αναγνωρίζει τη σημασία της επικοινωνίας στις συγκρούσεις. (NATO Review, 2015)

Την παραπάνω ιδέα φαίνεται να έχουν ενστερνιστεί τόσο η Ρωσία όσο και η Κίνα, οι οποίες κινούνται προς αυτήν την οδό, τόσο του πολέμου της παραπληροφόρησης και της επιρροής, όσο και της προσπάθειας μέσω αυτών ακριβώς των ενεργειών να λάβουν τη διεθνή νομιμοποίηση στις οποιοσδήποτε ενέργειές τους. Έχοντας αυτό κατά νου, μπορούμε να θεωρήσουμε βέβαιο ότι στο μέλλον τέτοιου είδους δραστηριότητες θα αυξηθούν, και θα απαιτηθεί μεγάλη προσπάθεια να αναγνωριστούν αυτές οι ενέργειες και να αντιμετωπιστούν.

2.4 Ο κυβερνοχώρος και η εργαλειοποίηση των ΜΚΔ και του διαδικτύου

2.4.1 Ο κυβερνοχώρος ως διάσταση

Σύμφωνα με το Oxford English Dictionary κυβερνοχώρος ορίζεται «το πλασματικό περιβάλλον μέσα στο οποίο λαμβάνει χώρα η ηλεκτρονική επικοινωνία, ειδικά όταν αντιπροσωπεύεται ως το εσωτερικό ενός συστήματος ηλεκτρονικών υπολογιστών· χώρος ο οποίος γίνεται αντιληπτός ως τέτοιος από έναν παρατηρητή, παράγεται όμως από ένα σύστημα υπολογιστών και δεν έχει απτή ύπαρξη· ο χώρος της εικονικής πραγματικότητας». Ο κυβερνοχώρος είναι μια διάσταση η οποία άρχισε να αναπτύσσεται τόσο ποσοτικά όσο και ποιοτικά τα τελευταία 30 χρόνια και κυρίως μετά τη δημιουργία του παγκόσμιου ιστού *World Wide Web* το 1991. Έτσι το διαδίκτυο άρχισε πλέον να συστήνει στο ευρύτερο κοινό την έννοια ενός νέου “χώρου”, ο οποίος είναι διασυνδεδεμένος έχοντας μια τεράστια επίδραση σε όλα τα τμήματα της κοινωνίας. Στο πλαίσιο που έχει ορίσει η Ευρωπαϊκή Επιτροπή, στην προσπάθεια χάραξης της στρατηγικής της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο (Ευρωπαϊκή Επιτροπή, 2013), αποτυπώνει ξεκάθαρα την επίδραση που έχει σε όλα τα τμήματα της κοινωνίας, αναφέροντας:

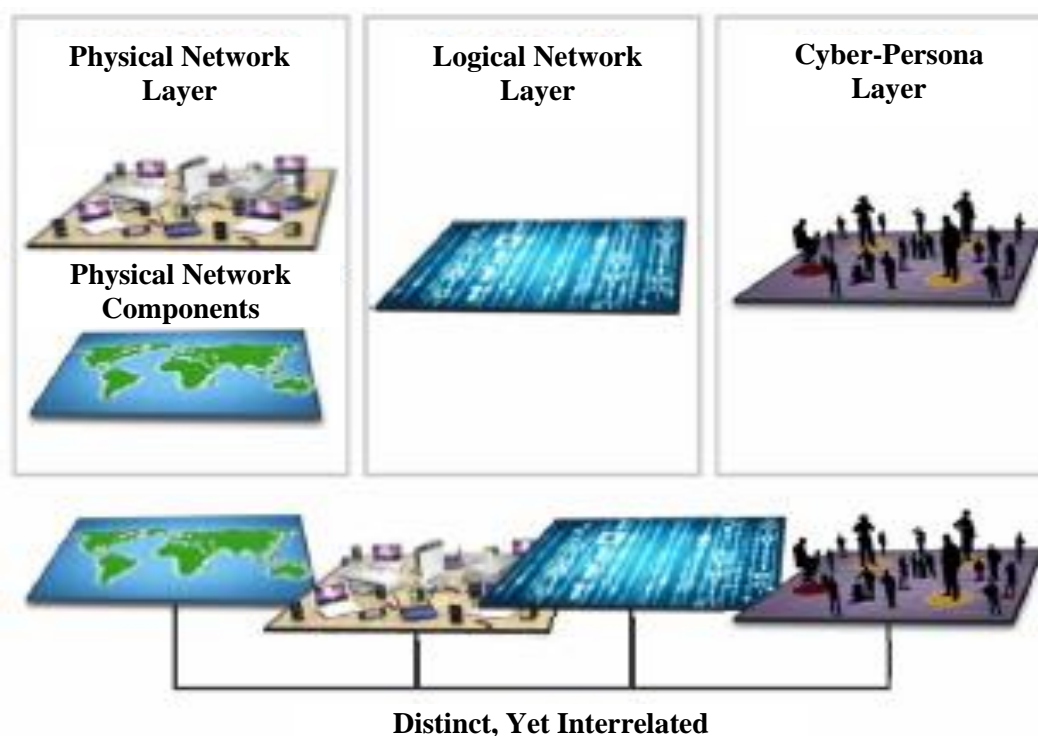
Η καθημερινή μας ζωή, τα θεμελιώδη δικαιώματα, οι κοινωνικές αλληλεπιδράσεις και οι οικονομίες εξαρτώνται από την ομαλή λειτουργία της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ανοικτός και ελεύθερος κυβερνοχώρος προώθησε την πολιτική και κοινωνική ένταξη παγκοσμίως, κατάργησε τα σύνορα μεταξύ χωρών, κοινοτήτων και πολιτών και κατέστησε δυνατή την αλληλεπίδραση και την κοινή χρήση πληροφοριών και ιδεών ανά την υφήλιο, εξασφάλισε ένα βήμα ελευθερίας της έκφρασης και άσκησης των θεμελιωδών δικαιωμάτων και ενδυνάμωσε τους λαϊκούς αγώνες για δημοκρατικότερες και δικαιότερες κοινωνίες...

Έγινε πλέον αντιληπτό ότι με την κατάλυση πλέον των γεωγραφικών συνόρων μέσα στον κυβερνοχώρο, είχαμε και την τροποποίηση του όρου (αν και δεν έχει αποτυπωθεί, τουλάχιστον ακόμα, επίσημα) πολίτη (citizen) σε πολίτη του διαδικτύου (netizen), αναγνωρίζοντας τη δυνατότητα που έχει αποκτήσει πλέον το διαδίκτυο για κινητοποίηση, αλλά και στοχοποίηση όχι μόνο πολιτικών και οικονομικών μηχανισμών αλλά όλων εκείνων που εμπλέκονται στη λειτουργία της κοινωνίας.

2.4.2 Η φύση του Κυβερνοχώρου

Ο κυβερνοχώρος αποτελεί μια διάσταση η οποία είναι ανθρώπινο κατασκεύασμα, σε αντίθεση με τις άλλες τέσσερις διαστάσεις (ξηρά, αέρα, θάλασσα, διάστημα), εξαρτάται όμως άμεσα από αυτές. Ο κυβερνοχώρος αποτελείται από τρία επίπεδα (1) το φυσικό/υλικοτεχνικό, (2) το λογικό/δικτυακό και (3) το κοινωνικό. Όπως φαίνεται και στην παρακάτω εικόνα 2.1 αυτά τα τρία επίπεδα είναι ναί μεν διακριτά, παρόλα αυτά όμως διασυνδέονται.

Εικόνα 2.1: Οι τρεις τομείς του Κυβερνοχώρου



Πηγή: Joint Publication 3-12 «Cyberspace Operations» (2018)

Στο φυσικό/υλικοτεχνικό επίπεδο, συμπεριλαμβάνονται όλες εκείνες οι υποδομές και υπολογιστικά συστήματα τα οποία χρησιμοποιούνται για τη λειτουργία των δικτύων. Είναι εκείνα τα οποία είτε αποτελούν το μέσο είτε και το στόχο μιας κυβερνοεπίθεσης. Είναι, τα μόνα μέσα στον κυβερνοχώρο, που μπορούν να προστατευτούν από κάποια φυσική προσβολή, ενώ είναι και τα μόνα τα οποία έχουν κάποια γεωγραφική υπόσταση αλλά και ένα νομικό πλαίσιο προστασίας, καθώς στο φάσμα του κυβερνοχώρου, μονάχα στα φυσικά/υλικά μέσα μπορεί ένα κράτος να έχει απόλυτη κυριαρχία, επιτρέποντας ή απαγορεύοντας τη χρήση τους σε ομάδες.

Το λογικό/δικτυακό επίπεδο εμπεριέχονται όλοι εκείνοι κώδικες, εφαρμογές, δεδομένα και τα οποία λειτουργούν μέσα στον κυβερνοχώρο και διασυνδέουν όλα τα ανωτέρω υπολογιστικά συστήματα (πχ. πρωτόκολλα επικοινωνίας (IP), url κλπ.) Είναι εκείνο το επίπεδο το οποίο δεν δύναται να προσβληθεί συμβατικά, παρά μόνο μέσω ηλεκτρονικών συστημάτων και αντίστοιχων εφαρμογών.

Το κοινωνικό επίπεδο αφορά όλες εκείνες τις διαδικτυακές προσωπικότητες και τα δεδομένα τα οποία διακινούν μέσα στον κυβερνοχώρο. Ένας άνθρωπος μπορεί να διαθέτει παραπάνω από μια διαδικτυακές προσωπικότητες καθώς μπορεί να συμμετέχει σε περισσότερα του ενός διαδικτυακά φόρα. Η ταυτότητα επομένως ενός ατόμου μπορεί να έχει πολλά ίχνη μέσα στον κυβερνοχώρο, αντίστροφα όμως και μια διαδικτυακή ταυτότητα μπορεί να αντιστοιχεί σε περισσότερα του ενός ατόμου. Η πολυπλοκότητα αυτών των διαδικτυακών προσωπικοτήτων και η αδυναμία ταυτοποίησή τους στο φυσικό περιβάλλον απαιτεί ενδελεχή συγκέντρωση και ανάλυση πληροφοριών, πληροφορίες όμως που το συνεχώς μεταβαλλόμενο πληροφοριακό περιβάλλον κάνει δύσκολο να εντοπιστούν έγκαιρα για εκμετάλλευση.

2.4.3 Επιχειρήσεις στον Κυβερνοχώρο

Η τεχνολογία αναπτύσσεται και αλλάζει ραγδαία επηρεάζοντας όχι μόνο την υλικοτεχνική οπτική του κυβερνοχώρου, αλλά και τη δυναμική της πληροφορίας που διακινείται μέσα στα δικτυοκεντρικά ηλεκτρονικά συστήματα και όχι μόνο στους τομείς της συλλογής, επεξεργασίας, εκμετάλλευσης και διάχυσης της πληροφορίας, παραμετροποιώντας τόσο την τεχνολογία όσο και την πληροφορία την ίδια ώστε να χρησιμοποιείται ως όπλο για τη διεξαγωγή επιχειρήσεων μέσα στον ψηφιακό κόσμο του κυβερνοχώρου. Η χρήση της τεχνολογίας σε κάθε μορφή της καθημερινότητας, στη διασύνδεση υπηρεσιών, στη διασύνδεση των μέσων και συστημάτων λήψης αποφάσεων και διοίκησης και ελέγχου, οδήγησε σε αυτό που σήμερα είναι γνωστό ως επιχειρήσεις κυβερνοχώρου. (ΓΕΕΘΑ, 2013)

Οι κυβερνοεπιθέσεις έχουν γίνει πλέον αντικείμενο άσκησης εξωτερικής πολιτικής¹¹. Η δυσκολία που εντοπίζεται όμως στην αντιμετώπιση τέτοιων επιθέσεων

¹¹ Από την περίοδο 2001 και μετά έχουν καταγραφεί κυβερνοεπιθέσεις μικρής κλίμακας, οι οποίες στόχευαν κυρίως στη συλλογή πληροφοριών, κυρίως μεταξύ Κίνας και Αμερικής. Όμως από το 2007 και έπειτα παρατηρείται διόγκωση τέτοιων επιχειρήσεων. Η επίθεση στα πληροφοριακά συστήματα της Εσθονίας το 2007, η κατάρρευση όλων των κυβερνητικών ΜΜΕ και ηλεκτρονικών σελίδων της Γεωργία στον Ρωσο-γεωργιανό πόλεμο του 2008, ο ιός STUXNET το 2010, ο οποίος θεωρείται το πιο εξελιγμένο κυβερνοόπλο σήμερα και ο οποίος σχεδιάστηκε από τις ΗΠΑ προκειμένου να «χτυπήσει» τα φυγόκεντρικά συστήματα στο πυρηνικό πρόγραμμα του Ιράν καθώς και η πρόσφατη εμπλοκή στις

έγκειται στο γεγονός ότι όπως προείπαμε ο κυβερνοχώρος δεν έχει απτή ύπαρξη. Αυτό έχει σαν αποτέλεσμα να μην καθίσταται δυνατή, τις περισσότερες φορές, η εξεύρεση της ταυτότητας του δράντα, καθώς μπορεί να γίνεται χρήση μέσων και συστημάτων οι φυσικές υποδομές των οποίων να βρίσκονται σε τρίτες χώρες. Επίσης οι καταγεγραμμένες κυβερνοεπιθέσεις, τουλάχιστον οι γνωστές μέχρι τώρα, δεν έχουν προκαλέσει ανθρώπινες απώλειες, ενώ μόλις αυτές γίνουν αντιληπτές, οδηγούν σε αντικατάσταση της υλικοτεχνικής υποδομής του στόχου. Επίσης, ακριβώς επειδή δεν εμπεριέχεται κινητικότητα μεγάλων δυνάμεων, έχει οδηγήσει την πλειονότητα κρατικών και μη δράντων να προσανατολίζονται πλέον στη χρησιμοποίηση του κυβερνοχώρου για την επίτευξη των στόχων τους.

Τα περισσότερα πλέον κράτη μέλη των Ηνωμένων Εθνών έχουν εντάξει πλέον την κυβερνοασφάλεια στην αμυντική στρατηγική τους. Σύμφωνα με έρευνα που διεξήγαγε το 2013 το UNIDIR¹² με τίτλο *The Cyber Index. International Security Trends and Realities*, γίνεται εμφανές ότι τα περισσότερα κράτη έχουν εντάξει την κυβερνοασφάλεια στη στρατηγική τους, ενώ ένας μεγάλος αριθμός εξ αυτών έχουν εμπλέξει και τις ένοπλες δυνάμεις, με την Αμερική, την Κίνα, τη Ρωσία και τη Μεγάλη Βρετανία να λαμβάνουν πρωταγωνιστικό ρόλο. Όμως αυτό που γίνεται επίσης εύκολα αντιληπτό είναι ότι και μικρότερα κράτη προσπαθούν να εμπλακούν όλο και περισσότερο ενεργά. Όμως και παγκόσμιοι και περιφερειακοί οργανισμοί όπως το NATO και η ΕΕ την τελευταία δεκαετία δραστηριοποιούνται όλο και περισσότερο στον τομέα συγκροτώντας όργανα τόσο για την αντιμετώπιση κυβερνοεπιθέσεων όσο και για την εκπαίδευση και τη χάραξη πολιτικής από τα κράτη μέλη τους.^{13,14}

Το μεγαλύτερο μέρος των επιχειρήσεων που παρατηρούνται μέσα στον κυβερνοχώρο, ποικίλουν από μια απλή εισβολή σε κάποιο σύστημα και τον έλεγχο του για λόγους επίδειξης ισχύος ή για λόγους αντεκδίκησης, συλλογής πληροφοριών, πρόκλησης εσκεμμένης βλάβης στα υπολογιστικά συστήματα ή πιο βαθιά στις υποδομές μιας χώρας είτε ακόμα και στην υπεξαίρεση χρημάτων από λογαριασμούς.

Αμερικανικές εκλογές του 2016, είναι ορισμένα μόνο παραδείγματα που καταδεικνύουν τη μεγάλη σημασία του κυβερνοχώρου στην εξωτερική πολιτική και στις διεθνείς σχέσεις. (Geers, 2014)

¹² United Nations Institute for Disarmament Research

¹³ NATO Cooperative Cyber Defence Centre of Excellence στο Τάλλιν της Εσθονίας από τον Οκτώβριο του 2008 <https://ccdcoc.org/> (πρόσβαση στις 21/10/2018)

¹⁴ European Union Agency for Network and Information Security στο Ηράκλειο Κρήτης στην Ελλάδα από το Σεπτέμβριο του 2005 <https://www.enisa.europa.eu/> (πρόσβαση στις 21/10/2018)

2.4.4 Τα Μέσα Κοινωνικής Δικτύωσης και το διαδίκτυο ως όπλο

Όπως αναφέρθηκε και προηγουμένως, η ραγδαία ανάπτυξη της τεχνολογίας και του διαδικτύου είχε σαν αποτέλεσμα τα γεωγραφικά σύνορα να εκμηδενιστούν. Πλέον μία είδηση που λαμβάνει χώρα σε μια περιοχή του πλανήτη έχει μεταφερθεί σε ελάχιστα μόλις λεπτά σε ολόκληρο τον κόσμο. Βέβαια αυτό αποτελεί την «καλή» πλευρά της χρήσης του διαδικτύου. Όμως αυτή την ταχύτητα διακίνησης της πληροφορίας αλλά και την αδυναμία, που προαναφέραμε παραπάνω, εξακρίβωσης των στοιχείων εκείνου που τη διαδίδει, έχει σαν αποτέλεσμα κρατικοί και μη δρώντες να εκμεταλλεύονται την κατάσταση και με αυτόν τον τρόπο να εγραιοποιούν και να οπλοποιούν το διαδίκτυο για την επίτευξη των αντικειμενικών τους σκοπών.

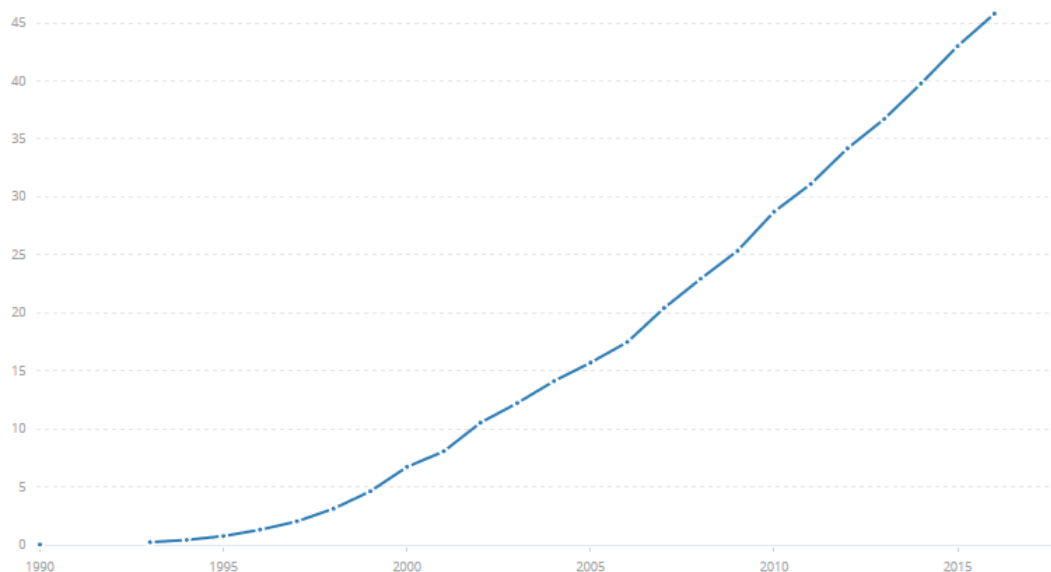
Τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ) θα μπορούσαμε να πούμε ότι ξεκίνησαν από το 1997 με την πρώτη πλατφόρμα δικτύωσης το *SixDegrees.com* όμως είναι το 2004 και μετά όπου η εμφάνιση του *Facebook* και του *Twitter* εκτόξευσαν τον αριθμό χρηστών τους σε εκατομμύρια. Όμως τα ΜΚΔ έχουν χάσει πλέον το σκοπό για τον οποίο αρχικά δημιουργήθηκαν, την άμεση σε φιλικό ή μη επίπεδο επικοινωνία μεταξύ των χρηστών τους. Καθώς η πρόσβαση σε αυτά καθίσταται πολύ εύκολη από ένα υπολογιστή ή από τα έξυπνα κινητά (smartphones), ο καθένας μας μπορεί να κάνει χρήση των ΜΚΔ και αυτό οδήγησε στην εργαλειοποίηση τους τόσο από εταιρείες για εμπορικούς και διαφημιστικούς σκοπούς ενώ οδήγησε και στην μετατροπή του από οργανωμένες ομάδες ή ακόμα και κράτη σε ένα πανίσχυρο όπλο.

Καθώς η χρήση των ΜΚΔ και η δραστηριοποίηση σε αυτά των εμπλεκόμενων σε μια σύγκρουση αυξάνεται, το πλεονέκτημα θα περάσει σε εκείνους οι οποίοι επενδύουν χρόνο και πόρους σε αυτά και τα εντάσσουν στην ευρύτερη πολιτική τους στη σχεδίαση πληροφοριακών επιχειρήσεων. Χαρακτηρίζονται από την εύκολη πρόσβαση, την παγκόσμια εμβέλεια και την ταχεία ροή πληροφοριών και πολυμέσων σε σχεδόν πραγματικό χρόνο. Αυτό έχει σαν αποτέλεσμα μεγάλος αριθμός χρηστών με κοινά ενδιαφέροντα να είναι σε θέση να ανταλλάσσουν απόψεις και πολύ περισσότερο εικόνες και βίντεο. Το παραπάνω ώθησε το φαινόμενο των «fake news», καθώς η παραμετροποίηση των λογαριασμών των χρηστών στα ΜΚΔ και η ανάλυση τους έδωσε την ευκαιρία σε όσους τα παρήγαγαν να κάνουν μια πιο στοχευμένη χρησιμοποίησή τους.

Καθώς τα ΜΚΔ κάνουν ευρεία χρήση εμπορικών τεχνολογιών, αυτό έχει σαν αποτέλεσμα να κάνει ιδιαίτερα φθηνή την ανάπτυξη και διατήρηση μιας ηλεκτρονικής παρουσίας σε αυτά, μειώνοντας έτσι τυχόν εμπόδια από τη μη διάδοση τεχνολογίας.

Η πρόσβαση σε αυτά είναι αρκετά εύκολη χωρίς να απαιτείται κάποιος εξειδικευμένος εξοπλισμός, όπως ηλεκτρονικοί υπολογιστές και κινητά τηλέφωνα, ο οποίος είναι προσβάσιμος από μεγάλες ομάδες ατόμων ακόμα και σε περιοχές με περιορισμένους πόρους. Σύμφωνα με στοιχεία από τη Παγκόσμια Τράπεζα και όπως φαίνεται στην εικόνα 2.2 ο αριθμός χρηστών στον κόσμο αυξάνεται με ταχείς ρυθμούς φθάνοντας για το 2016 το 45,79% του παγκόσμιου πληθυσμού να κάνει χρήση του διαδικτύου.

Εικόνα 2.2: Μοναδικοί χρήστες του διαδικτύου (% του παγκόσμιου πληθυσμού)



Πηγή: The World Bank data <https://data.worldbank.org/indicator/it.net.user.zs?end=2017&start=1990&view=chart> (πρόσβαση στις 21/10/2018)

Έτσι τα ΜΚΔ επιτρέπουν την ανταλλαγή της πληροφορίας σε ένα ευρύτερο κοινό χωρίς γεωγραφικούς περιορισμούς, καθιστώντας τα ένα από τα πιο διαπεραστικά μέσα του παγκόσμιου πληροφοριακού περιβάλλοντος. Ένα ακόμα χαρακτηριστικό τους είναι η δυνατότητα αυτοματοποίησης επανάληψης της πληροφορίας και ταυτόχρονης ενσωμάτωσης οποιαδήποτε σχολίου κάθε χρήστη, ενώ σε αυτό συντελεί και η συμβατότητα όλων των χρησιμοποιηθέντων μέσων. Επίσης παρέχεται και η δυνατότητα της ανωνυμίας και της πλαστοπροσωπίας καθώς επίσης και η διαστρέβλωση του περιεχομένου σε όσο βαθμό επιθυμεί κάποιος δρώντας να παραπλανήσει. Τα σύγχρονα μέσα έχουν καταστήσει δυνατή την επεξεργασία ήχου και εικόνας κάνοντας με αυτόν το τρόπο πιο εύκολη την υποστήριξη μιας θέσης η οποία διαστρεβλώνει την αλήθεια. Η χαμηλή ανάλυση των πολυμέσων που διακινούνται μέσω των ΜΚΔ, καθώς δεν είναι δυνατή η μεταφορά μεγάλων όγκων δεδομένων,

προσφέρει τη δυνατότητα σε εκείνους που θέλουν να χρησιμοποιήσουν τα ΜΚΔ για τη διάδοση ψευδών ειδήσεων να υποστηρίξουν τη θέση με χαλκευμένα στοιχεία προς υποστήριξή των.

Καταλήγουμε επομένως στο συμπέρασμα ότι χρησιμοποιώντας κατάλληλα περισσότερες από μια πλατφόρμες των ΜΚΔ, αναλόγως του τι μπορεί να διακινήσει η κάθε μια, δημιουργούμε μια ιστορία η οποία εξαπλώνεται στο διαδίκτυο και προσεγγίζει τα επιλεγμένα κοινά με ποικίλους τρόπους, προσδίδοντας με αυτόν τον τρόπο και ένα βαθμό αξιοπιστίας, καθώς οι περισσότεροι χρήστες πείθονται για την ακρίβεια της πληροφορίας όχι τόσο εξετάζοντας την αξιοπιστία της πηγής, αλλά την επανάληψή της στο διαδίκτυο. Σύμφωνα με έρευνα που διεξήχθη το 2016 αποδείχτηκε ότι μόλις το 41% των χρηστών διαβάζει πλήρως το κείμενο που επαναπροωθεί, ενώ το 59% προωθεί χωρίς καν να διαβάζει το σύνδεσμο που το συνοδεύει¹⁵. Τέλος τα ΜΚΔ αποδείχτηκαν, ειδικά μετά το 2014 και την τρομοκρατική οργάνωση DAESH, ένα χρήσιμο εργαλείο στρατολόγησης και μετάδοσης των εξτρεμιστικών μηνυμάτων του. Το Ισλαμικό χαλιφάτο κάνοντας ευρεία χρήση του διαδικτύου και των ΜΚΔ κατάφερε να κερδίσει πόρους, οικονομικούς και ανθρώπινους, ενώ και μέσω του «dark web» κατάφερε να κερδίσει μεγάλα χρηματικά ποσά αλλά και να προμηθευτεί μεγάλες ποσότητες οπλισμού.

¹⁵ Maksym Gabielkov, Arthi Ramachandran, Augustin Chaintreau, Arnaud Legout. Social Clicks: What and Who Gets Read on Twitter?. ACM SIGMETRICS / IFIP Performance 2016, Jun 2016, Antibes Juan-les-Pins, France. 2016. <hal-01281190>

3. Υψηλή Στρατηγική

«Το αποκορύφωμα της στρατηγικής ικανότητας δεν είναι να δώσεις εκατό μάχες και να κερδίσεις και τις εκατό. Αποκορύφωμα είναι να υποτάξεις τον εχθρό, χωρίς να δώσεις ούτε μια μάχη.»

Η Τέχνη του Πολέμου, Sun Tzu

3.1 Θεωρία της Υψηλής Στρατηγικής

Ο Carl von Clausewitz στο έργο του *Περί Πολέμου*, όρισε ότι η στρατηγική «είναι η χρήση των συμπλοκών για την επίτευξη των σκοπών του πολέμου». (von Clausewitz, 2007) διαχωρίζοντας με αυτόν τον τρόπο την έννοια της στρατηγικής από την τακτική, την οποία την τοποθετεί στον τρόπο χρήσης των μέσων σε μια συμπλοκή. Ο André Beaufre στο έργο του *Introduction à la stratégie* προσπάθησε να δώσει ένα πιο αφηρημένο ορισμό και πολύ πιο γενικό ορισμό περί της στρατηγικής ορίζοντας ως «την τέχνη της διαλεκτικής της ισχύος ή, ακριβέστερα, η τέχνη της διαλεκτικής των βουλήσεων που χρησιμοποιούν την ισχύ για την επίλυση της διένεξής τους». (Beaufre, 2015). Όπως αναφέρει ο Sir Michael Howard στο άρθρο του *Grand Strategy in the Twentieth Century*, ήδη από το 1929 ο Sir Basil H. Liddell Hart είχε γράψει ότι «Ενώ ο ορίζοντας της στρατηγικής περιορίζεται στον πόλεμο, η υψηλή στρατηγική προσβλέπει στη συνέχιση της ειρήνης. Δεν θα πρέπει να προσβλέπει μονάχα στο συνδυασμό των διαφόρων μέσων, αλλά και στη ρύθμιση της χρήσης αυτών, ώστε να αποφευχθεί οποιαδήποτε βλάβη στη μελλοντική κατάσταση της ειρήνης, ασφάλειας και ευημερίας»¹⁶. (Howard, 2001)

Η παραδοσιακή στρατηγική ανάλυση επικεντρώνονταν μόνο στο καθαρά συγκρουσιακό στοιχείο της διεθνούς πολιτικής. Στο επίπεδο όπως στη υψηλής στρατηγικής, όπως αναφέρει και ο καθηγητής Χαράλαμπος Παπασωτηρίου στο βιβλίο του *Βυζαντινή Υψηλή Στρατηγική: 6^{ος}-11^{ος} αιώνας*, διευρύνεται το γνωστικό αντικείμενο με δύο τρόπους (α) στα πλαίσια της ανάλυσης των πολέμων συμπεριλαμβάνει πέρα από τη στρατιωτική στρατηγική, τους μη στρατιωτικούς παράγοντες που καθορίζουν την πορεία και έκβαση ενός πολέμου και (β) επεκτείνεται στις μακροσκοπικές υψηλές στρατηγικές των κρατών σε περιόδους τόσο ειρήνης όσο και πολέμου. (Παπασωτηρίου, 2011) Καταλήγουμε λοιπόν στο συμπέρασμα ότι

¹⁶ Το παραπάνω αποτελεί αναφορά του Sir Michael Howard στα γραφόμενα από τον Sir Basil H. Liddell Hart το 1929 στο βιβλίο του *The Decisive Wars of History: A Study in Strategy* (Λονδίνο: G. Bell).

σήμερα, στρατηγική είναι εκείνη η τέχνη χρησιμοποίησης πολιτικών, οικονομικών, ψυχικών και στρατιωτικών δυνάμεων, τόσο στην ειρήνη όσο και στον πόλεμο, ώστε να παρέχεται η μέγιστη δυνατή υποστήριξη στην εθνική πολιτική. Ως εκ τούτου αποτελεί εργαλείο της πολιτικής για την επίτευξη των σκοπών της, διαμορφώνεται τόσο στην ειρήνη όσο και στον πόλεμο, ενώ είναι δυνατό να επιτύχει τους πολιτικούς σκοπούς της, χωρίς να προστρέξει σε πολεμικές επιχειρήσεις, δημιουργώντας στον αντίπαλο μια τέτοια ψυχολογική κατάσταση ώστε να πειστεί ότι είναι ανώφελο να επιδιώξει μια σύγκρουση. Στο υψηλότερο επίπεδο της, η υψηλή στρατηγική συνδέεται με την πολιτική και τη διπλωματία, ενώ πρέπει να λαμβάνεται υπόψη πέρα από τη μαχητική, στρατιωτική ισχύ και η ισχύς της οικονομίας, της διπλωματίας, των εμπορικών συναλλαγών καθώς επίσης και του ηθικού και της θέλησης του αντιπάλου να αντισταχθεί στους σκοπούς μας.

Όπως αναφέρει και ο Beaufré «η στρατηγική, για την επίτευξη του επιδιωκόμενου σκοπού, έχει στη διάθεση της μια ποικιλία υλικών και ηθικών μέσων, τα οποία ποικίλουν από τον βομβαρδισμό με πυρηνικά όπλα μέχρι και την προπαγάνδα και τις εμπορικές συμφωνίες.» (Beaufre, 2015) Στο σύγχρονο περιβάλλον πρέπει να κατανοήσουμε ότι η ανάλυση μόνο των στρατιωτικών στρατηγικών δεν επαρκεί να ερμηνευθούν τα αποτελέσματα μιας σύγκρουσης. Ο αντικειμενικός σκοπός των περισσότερων δρώντων (κρατών ή ομάδων) τις περισσότερες φορές είναι να διατηρήσουν την ανεξαρτησία τους ή να ενισχύσουν την επιρροή τους ή και καμιά φορά την εδαφική τους κυριαρχία. Η επιλογή επομένως των μέσων που θα χρησιμοποιηθούν, έχει να κάνει με τα τρωτά σημεία του αντιπάλου, αλλά και με τις δικές μας δυνατότητες. Ο πόλεμος όμως δεν είναι ένα αποκλειστικό στρατιωτικό φαινόμενο.

3.2 Οι διαστάσεις υψηλής στρατηγικής

Οι ένοπλες συρράξεις μεταξύ κρατών έχουν πλέον μειωθεί, και οι αντίπαλες πλευρές (κρατικοί ή μη δρώντες) χρησιμοποιούν πλέον και άλλα μέσα, πέρα από την ένοπλη βία, για να κάμψουν τη θέληση του αντιπάλου και να επιτύχουν τους αντικειμενικούς τους σκοπούς. Όπως αναφέρει και ο καθηγητής Χαράλαμπος Παπασωτηρίου η υψηλή στρατηγική περιλαμβάνει το σύνολο των μέσων που χρησιμοποιούν οι αντίπαλες πλευρές για την προώθηση των στόχων τους και ορίζει ότι υπάρχουν πέντε βασικές

διαστάσεις μέσα στις οποίες κινούνται οι εμπόλεμοι. (Παπασωτηρίου, 2011) Έτσι διακρίνονται οι εξής:

1. Στρατιωτική στρατηγική με τον όρο να αναφέρεται σε αυτό ακριβώς που λέει η λέξη στρατιωτική, δηλαδή τη χρήση ένοπλης βίας από στρατιωτικές μονάδες για την επίτευξη του πολιτικού σκοπού.

2. Οικονομική διάσταση των επιχειρήσεων με τις προσπάθειες των εμπόλεμων να προσπαθούν να πλήξουν την οικονομία του αντιπάλου και τις υποδομές αυτού ώστε να επιτύχουν τους σκοπούς τους. Βέβαια όταν ο στόχος που τίθεται είναι μια γενική αποδυνάμωση της αντίπαλης οικονομίας, η οποία θα αποσκοπεί στην πρόκληση εσωτερικών αναταραχών (κυβερνοεπιθέσεις στην Εσθονία 2007) λίγα αποτελέσματα μπορεί να παρουσιάσει, καθώς τέτοιες ενέργειες μόλις αποκαλυφθούν αντιμετωπίζονται σχετικά γρήγορα.

3. Εσωτερική πολιτική με τον όρο να αναφέρεται στη νομιμοποίηση που προσπαθούν να βρουν οι πολιτικοί δρώντες τόσο στα εσωτερικά κοινά τους, στην προσπάθειά τους να στρατολογήσουν κόσμο (προπαγάνδα και στρατολόγηση από το ISIS) όσο και στην προσπάθειά τους να κάμψουν τη λαϊκή βούληση και την εσωτερική νομιμοποίηση των αντιπάλων τους. (Εσθονία 2007, Ουκρανία 2014)

4. Διεθνής νομιμοποίηση με τη διάσταση αυτή να αφορά την προσπάθεια των εμπλεκομένων να δώσουν μια μορφή νομιμότητας στις πράξεις τους, πατώντας συνήθως στους κανόνες του διεθνούς δικαίου ή προσπαθώντας να αποδείξουν ότι οι ενέργειες τους είναι δικαιολογημένες επιζητώντας τον επηρεασμό της κοινής γνώμης μέσω μεθοδευμένων και στοχευμένων ενεργειών παραπληροφόρησης και προβολής της προσπάθειάς τους με ένα μανδύα νομιμότητας από μια ευνοϊκή σκοπιά. (Ουκρανία 2014, Hezbollah-Λίβανος 2006)

5. Διπλωματία κατά την οποία γίνεται προσπάθεια εξασφάλισης της σύμπραξης τρίτων δυνάμεων ή έστω την έμμεση υποστήριξή τους, καθώς διαφαίνεται ότι τα συμφέροντά τους συγκλίνουν ή συμπίπτουν με εκείνα ενός εκ των εμπλεκομένων ή και τον πολιτικό συντονισμό μεταξύ των συμμάχων.

3.3 Στον 21^ο αιώνα

Όπως περιγράφηκε παραπάνω, η υψηλή στρατηγική ορίζει τους απώτερους στόχους ενός κράτους και καθορίζει τα μέσα για την επιδίωξή των, με τα μέσα αυτά να μην είναι αυστηρά στρατιωτικά, αλλά να περιλαμβάνουν και οικονομικά, διπλωματικά,

κοινωνικά και πολιτικά εργαλεία για την επίτευξη των εθνικών πολιτικών σκοπών. Με τη ραγδαία ανάπτυξη της τεχνολογίας, μια τέτοια πολυπληθής και πολύπλοκη σειρά ενεργειών, μπορεί να συνδυαστεί με πολλούς τρόπους.

Σε άρθρο του ο Joseph Nye Jr το οποίο δημοσιεύθηκε και στην εφημερίδα *Το Βήμα* το 2015¹⁷ αναφέρει ότι οι πόλεμοι σήμερα δεν έχουν καθορισμένα μέτωπα και πλέον δεν μπορούμε να συζητάμε για σαφή στρατιωτικά μέτωπα και μέτωπα μετόπισθεν. Οι ένοπλες συγκρούσεις πλέον δεν είναι μεταξύ κρατικών δρώντων, αλλά αντάρτικων ομάδων, τρομοκρατικών δικτύων, πολιτοφυλακών οι οποίες συνδέονται άμεσα ή όχι, φανερά ή όχι πιθανόν και με κρατικούς δρώντες. Αυτό οδηγεί πλέον στη χρησιμοποίηση μέσων τα οποία δεν διαθέτουν όλα δύναμη πυρός, ενώ συνήθως τις περισσότερες φορές δεν προκαλούν και θύματα. Η κάμερα ενός κινητού, το διαδίκτυο, μια ανάρτηση σε κάποιο Μέσο Κοινωνικής Δικτύωσης και ο ανταγωνισμός για τη διαχείριση της πληροφορίας έχουν σαν αποτέλεσμα να αναδεικνύονται σε τρωτά σημεία αλλά και σε πυλώνες ισχύος στις σύγχρονες συγκρούσεις.

Οι μορφές συγκρούσεων που αναφέρθηκαν στο 2^ο κεφάλαιο ξεκίνησαν σαν απάντηση στην υπεροπλία των ισχυρότερων στρατιωτικά δυνάμεων από τους ασθενέστερους σε μια συμπλοκή, καθώς οι περισσότεροι κρατικοί και μη κρατικοί δρώντες δεν δύναται να συγκεντρώσουν ισχυρές στρατιωτικές δυνάμεις λόγω των υψηλών κυρίως οικονομικών και δευτερευόντως ανθρωπίνων πόρων. Όμως, σύντομα οι ισχυροί στο παγκόσμιο στερέωμα, είτε διότι αντιμετώπισαν τέτοιες ενέργειες είτε κατόπιν ανάλυσης και εξαγωγής συμπερασμάτων από ενέργειες που έλαβαν χώρα αλλού, αποφάσισαν να ενσωματώσουν στα δόγματά τους τρόπους αντιμετώπισης αρχικά τέτοιων ενεργειών αλλά και υιοθετώντας στρατηγικές πολέμου χωρίς περιορισμούς, συνδυάζοντας κάθε μορφής εργαλεία στρατιωτικά ή πολιτικά, σε όλες τις φυσικές και μη διαστάσεις (ξηρά, θάλασσα, αέρα, διάστημα και κυβερνοχώρο), με τρομοκρατικές ή συμβατικές επιχειρήσεις και αποσκοπώντας είτε στην πληροφόρηση (αμυντική φύση) είτε στην προπαγάνδα και την παραπληροφόρηση (επιθετική φύση) για την προστασία είτε την εξαπάτηση και εξουθένωση του κοινωνικού συνόλου.

Στα επόμενα κεφάλαια θα ακολουθήσει μια περιπτωσιολογική μελέτη ορισμένων μορφών πληροφοριακών επιχειρήσεων που έλαβαν χώρα, προσπαθώντας να καταδειχθεί η μορφή των επιχειρήσεων που έλαβαν χώρα καθώς και ποιοι ήταν οι

¹⁷ Nye Jr, J. (2015). Ο Πόλεμος στον 21ο αιώνα. Το Βήμα. Ανάκτηση Οκτώβριος 28, 2018, από <https://www.tovima.gr/2015/02/09/world/o-polemos-ston-21o-aiwna/>

στρατηγικοί στόχοι που είχαν θέσει οι δρώντες και κατά πόσο μπόρεσαν να τους υλοποιήσουν. Θα γίνει μια προσπάθεια ανάλυσης της σύγκρουσης Ισραήλ-Hezbollah το 2006 η οποία θεωρείται ότι ξεκίνησε και τη συζήτηση για τον υβριδικό πόλεμο, το Ρωσικό παράγοντα στην Εσθονία το 2007 καθώς και από το 2014 και μετά τις δραστηριότητες του αυτοαποκαλούμενου Ισλαμικού Κράτους και της Ρωσίας στην Ουκρανία.

ΜΕΡΟΣ Β΄

4. Περιπτωσιολογική Μελέτη: Ο πόλεμος των 34 ημερών.

Η σύγκρουση Ισραήλ – Χεζμπολάχ

«ΠΑΡΑΔΟΣΙΑΚΑ στις διεθνείς συγκρούσεις, η πλευρά με την ισχυρότερη στρατιωτική δύναμη τείνει να κερδίζει. Στη σημερινή εποχή της πληροφορίας, η πλευρά με την πιο ισχυρή ιστορία να είναι εκείνη που κερδίζει.»

The Boston Globe, Joseph S. Nye¹⁸

4.1 Το χρονικό της σύγκρουσης

Ήδη από τη γέννηση του κράτους του Ισραήλ το 1948, η περιοχή ταλανίζεται από συνεχόμενες συγκρούσεις με γειτονικά αραβικά κράτη και μουσουλμανικές θρησκευτικές ομάδες. Στα βόρεια σύνορα του Ισραήλ βρίσκεται το κράτος του Λιβάνου, του οποίου οι δημογραφικές εντάσεις οδήγησαν σε ένα εμφύλιο πόλεμο που διήρκησε πάνω από μία δεκαετία και εγκαθίδρυσε ένα ιδιότυπο σύστημα διακυβέρνησης. Από το 1982 και την εισβολή του Ισραήλ στο νότιο τμήμα της χώρας και με την χρηματοδότηση του σιιτικού θεοκρατικού Ιράν, εμφανίζεται στην περιοχή μια σιιτική στρατιωτική ομάδα η Χεζμπολάχ, η οποία εδραιώνεται δυναμικά συσπειρώνοντας του σίιτες μουσουλμάνους γύρω της. Παράλληλα εξοπλίζεται από Συρία και Ιράν και εξαπολύει επιθέσεις εναντίον του Ισραήλ. Το 2000 το Ισραήλ αποχωρεί από την περιοχή και η Χεζμπολάχ ενισχύει την παρουσία της στην περιοχή με τον ηγέτη της Σεΐχη Hassan Nasrallah να ανακοινώνει ότι « υπόσχομαι ότι όλοι οι αιχμάλωτοι και οι φάρμες στις Shebaa θα επιστρέψουν στο Λίβανο». ¹⁹ Έτσι το 2004 χρησιμοποίησε τη σύλληψη τριών ισραηλινών στρατιωτών ως μοχλό πίεσης και πέτυχε την ανταλλαγή τους με αριθμό Λιβανέζων πολιτών οι οποίοι κρατούνταν στις φυλακές του Ισραήλ, με τη διαμεσολάβηση της Γερμανίας. ²⁰

Έτσι λοιπόν οδηγούμαστε στο καλοκαίρι του 2006 και στη σύγκρουση μεταξύ Χεζμπολάχ – Ισραήλ, που έμεινε γνωστή ως ο δεύτερος πόλεμος του Λιβάνου διάρκειας 34 ημερών. Στις 12 Ιουλίου 2006 η Χεζμπολάχ εξαπέλυσε μια αιφνιδιαστική

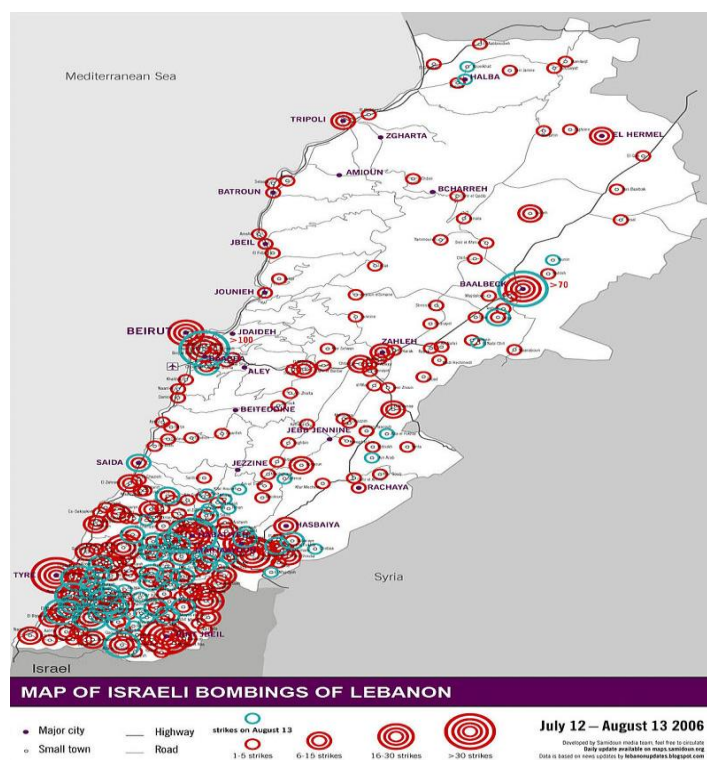
¹⁸ Nye, J. (2006, Αύγουστος 19). In Mideast, the Goal is 'Smart Power'. The Boston Globe. Ανάκτηση Οκτώβριος 31, 2018, από <https://www.belfercenter.org/publication/mideast-goal-smart-power>

¹⁹ 2000: *Hezbollah celebrates Israeli retreat* (2000, Μάιος 26) από BBCHome http://news.bbc.co.uk/onthisday/hi/dates/stories/may/26/newsid_2496000/2496423.stm (πρόσβαση στις 4/11/2018)

²⁰ Από τη μεριά της Χεζμπολάχ επεστράφησαν οι σωροί των 3 στρατιωτών που είχαν συλληφθεί καθώς και ένας Ισραηλινός επιχειρηματίας, ενώ από το Ισραήλ απελευθερώθηκαν πάνω από είκοσι κρατούμενοι συμπεριλαμβανομένου και δύο ηγετών της Χεζμπολάχ. Περισσότερα στο *Israel, Hezbollah swap prisoners* (2004, Ιανουάριος 29) από CCN International.com <http://edition.cnn.com/2004/WORLD/meast/01/29/prisoner.exchange/> (πρόσβαση 4/11/2018)

επίθεση στα λιβανο-ισραηλινά σύνορα εναντίον ενός ισραηλινού περιπόλου, σκοτώνοντας οκτώ στρατιώτες και συλλαμβάνοντας άλλους δύο. Η απάντηση του Ισραήλ υπήρξε άμεση. Τεθωρακισμένες δυνάμεις εισήλθαν στα νότια της χώρας του Λιβάνου, εφεδρικές δυνάμεις κινήθηκαν προς τα σύνορα Ισραήλ – Λιβάνου, ενώ η αεροπορία ξεκίνησε μπαράζ βομβαρδισμών εναντίον των νότιων περιοχών του Λιβάνου όπου βρίσκονταν οι δυνάμεις της Χεζμπολάχ όμως και εναντίον συιτικών περιοχών στα περίχωρα της Βηρυτού, καταστρέφοντας παράλληλα διάφορες υποδομές τις χώρας σε αυτές τις περιοχές. Η Χεζμπολάχ είχε κρύψει το οπλοστάσιο της και τα κέντρα διοίκησης της μέσα στις πόλεις και στα χωριά του νοτίου Λιβάνου, και αυτό είχε σαν αποτέλεσμα οι επιθέσεις που εξαπέλυσε η Ισραηλινή αεροπορία και το πυροβολικό να προκαλούν πολλές παράπλευρες απώλειες. Όπως απεικονίζεται και στην εικόνα 4.1 υπήρξε πρωτοφανής αριθμός αεροπορικών επιθέσεων εναντίον του Λιβάνου στην περίοδο των 34 ημερών και όχι μόνο εναντίον των περιοχών που δραστηριοποιούνταν η Χεζμπολάχ, καθώς το Ισραήλ δίστασε να εκτοξεύσει μια μεγάλης κλίμακας επίθεση στο Λίβανο, προκειμένου να αποφύγει μεγάλες απώλειες.

Εικόνα 4.1: Περιοχές του Λιβάνου που επλήγησαν από τις Ισραηλινές αεροπορικές δυνάμεις



Πηγή: maps.samidoun.org (πρόσβαση στις 4/11/2018)

Από την αρχή του πολέμου η διεθνής κοινότητα ζητούσε την κατάπαυση του πυρός μεταξύ των εμπλεκομένων Χεζμπολάχ – Ισραήλ, δικαιολογώντας όμως την ανταπόδοση του Ισραήλ, τουλάχιστον αρχικά, ως “νόμιμη άμυνα”. Όμως σύντομα η κατάσταση αναστράφηκε. Μόλις μια εβδομάδα μετά την έναρξη των επιχειρήσεων, άρχισαν να κάνουν το γύρω του κόσμου φωτογραφίες και αναμεταδόσεις από τις περιοχές του νοτίου Λιβάνου δείχνοντας νεκρούς αθώους Λιβανέζους πολίτες και καταστροφές εγκαταστάσεων οι οποίες δεν ήταν στρατιωτικές. Ενδεικτικό είναι το γεγονός πως αναφέρονται ότι από τις ισραηλινές επιδρομές εκτιμάται ότι σκοτώθηκαν 1.500 άνθρωποι με το 1/3 αυτών να είναι μικρά παιδιά. Άρχισε επομένως να τίθεται το ερώτημα εάν τα αντίποινα για την αιχμαλωσία των δύο Ισραηλινών στρατιωτών ήταν δυσανάλογα. Έτσι σύντομα η διεθνής κοινότητα έφθασε στο σημείο να κατηγορεί το Ισραήλ για εγκλήματα πολέμου.²¹ Τελικά η σύγκρουση έληξε στις 14 Αυγούστου 2006, με την ψήφιση από το από το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών της απόφασης 1701 με την οποία τίθονταν τερματισμός των εχθροπραξιών και δημιουργία μιας ουδέτερης ζώνης από τον Ποταμό Λιτάνι στο νότιο μέρος της χώρας ως την μπλε γραμμή η οποία θα έπρεπε να είναι τελειώς απελευθερωμένη από ένοπλο προσωπικό και όπλα εκτός από αυτά που ανήκουν στον Στρατό του Λιβάνου και των ειρηνευτικών δυνάμεων του ΟΗΕ στο Λίβανο (UNIFIL), το προσωπικό των οποίων αυξήθηκε στα 15.000 άτομα.

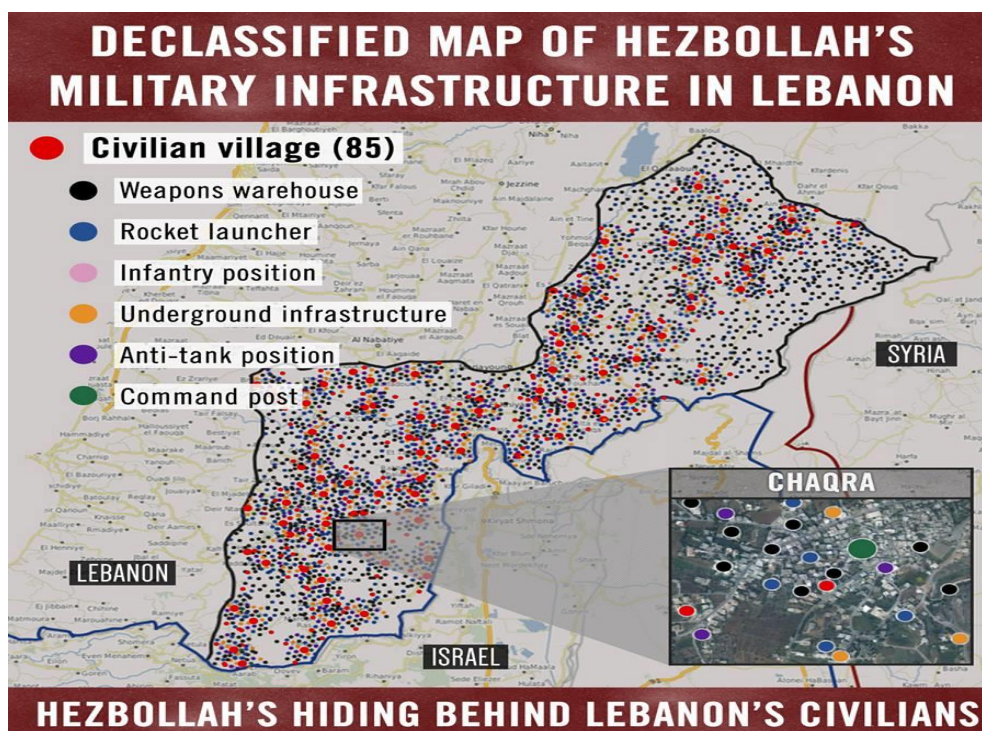
4.2 Ποιοι ήταν οι σκοποί που έθεσαν οι δρώντες

Το Ισραήλ, με την εκδήλωση μιας τόσο δυσανάλογης στρατηγικής, φαίνεται ότι είχε θέσει ως σκοπό (1) να κάνει επίδειξη της αποτρεπτικής του δύναμης στην περιοχή και (2) να πιέσει, μέσω της καταστροφής των υποδομών και της πρόκλησης απωλειών αμάχων, την επίσημη κυβέρνηση της Βηρυτού να στραφεί εναντίον της Χεζμπολάχ. (Fayutkin, 2008) Το Ισραήλ γνώριζε ότι η Χεζμπολάχ είχε αναπτύξει τις δυνάμεις του εντός των πόλεων του νοτίου Λιβάνου όπως φαίνεται και στην εικόνα 4.2. Με τις δύο επιχειρήσεις που εξαπέλυσε το Ισραήλ «Operation Accountability» και «Operation Grapes of Wrath», το Ισραήλ προσπάθησε να καταστήσει σαφές ότι τιμωρεί την

²¹ *Israel/Lebanon: Israel Responsible for Qana Attack Indiscriminate Bombing in Lebanon a War Crime* από Human Rights Watch <https://www.hrw.org/news/2006/07/29/israel/lebanon-israel-responsible-qana-attack> (πρόσβαση 4/11/2018)

κυβέρνηση του Λιβάνου για την απόφασή της να μην περιορίζει την Χεζμπολάχ στην επικράτειά της και να την πείσει να λάβει μέτρα εναντίον της.

Εικόνα 4.2: Απεικόνιση των δυνάμεων που είχε αναπτύξει η Χεζμπολάχ στο Λίβανο το 2006



Πηγή: Jewish Virtual Library (πρόσβαση στις 4/11/2018)

Από την πλευρά της, η Χεζμπολάχ έχοντας χτίσει γερούς δεσμούς με την τοπική σιιτική κοινωνία, της οποίας εξασφάλιζε τρόφιμα και άλλες παροχές, είχε καταφέρει να κρύψει τους πόρους της μέσα στις πόλεις του Λιβάνου. Με επιτυχημένη προπαγάνδα είχε καταφέρει να πείσει του Λιβανέζους της περιοχής ότι η κεντρική κυβέρνηση²² δεν νοιάζονταν για εκείνους και η Χεζμπολάχ αποτελούσε τη μοναδική πηγή σταθερότητας στην περιοχή. Οπότε σκοπός του ήταν να μπορέσουν να κρυφτούν μέσα στον αστικό ιστό και να μπορέσουν με τις ρίψεις πυραύλων εναντίον των Ισραηλινών πόλεων να πείσουν το Ισραήλ σε μία εκχειρία, καθώς η προσβολή Ισραηλινών πόλεων και η απώλεια αμάχων ήταν ένα πολιτικό κόστος το οποίο η Χεζμπολάχ πίστευε ότι δεν θα μπορούσε να το διαχειριστεί η κυβέρνηση του Ehud Olmert. Γνώριζε ότι στρατιωτικά δεν μπορούσε να νικήσει σε μια συμβατική μάχη το

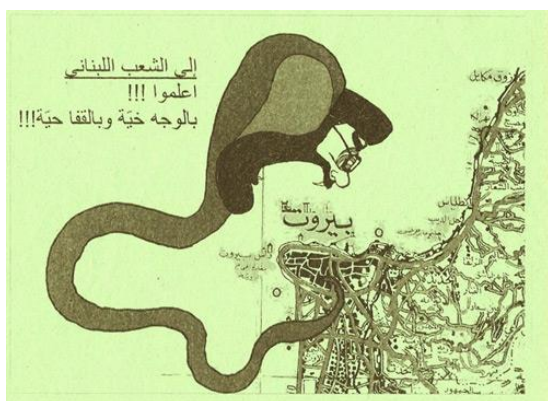
²² Στο Λίβανο όπου επικρατούν τρεις μεγάλες θρησκευτικές ομάδες Χριστιανοί, Σουνίτες Μουσουλμάνοι και Σίτες Μουσουλμάνοι οι τελευταίοι νιώθουν να υπο-αντιπροσωπεύονται στο οικονομικό, κοινωνικό και πολιτικό σκηνικό της χώρας.

Ισραήλ, όμως ήλπιζε μέσω της προπαγάνδας να μπορέσει να επιτύχει μια συμβολική νίκη, τόσο στα εσωτερικά (τοπικό Λιβανέζικό πληθυσμό και μουσουλμανικό στοιχείο της περιοχής) όσο και στα εξωτερικά κοινά (διεθνή κοινότητα, καθώς χαρακτηρίζεται ως τρομοκρατική οργάνωση). Ήθελε επομένως με την ενέργειά της στις 12 Ιουλίου 2006 να προκαλέσει το Ισραήλ, δεν πίστευε όμως ότι η αντίδραση του Ισραήλ θα ήταν τόσο βίαιη και αυτό φαίνεται και από τη συνέντευξη που έδωσε επικεφαλής της Σειχης Hassan Nasrallah σε τηλεοπτική του συνέντευξη στις 27 Αυγούστου 2006²³.

4.3 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν

Οι επιχειρήσεις προσβολής του Ισραήλ στο νότιο Λίβανο υποστηρίχτηκαν και από μία εκστρατεία προπαγάνδας με την οποία προσπάθησε να στρέψει τον τοπικό πληθυσμό απέναντι της Χεζμπολάχ και να αποσταθεροποιήσει την ηγεσία της. Από την αρχή των επιχειρήσεων υπήρξε ρίψη προκηρύξεων, σχεδόν καθημερινά, με τις οποίες ωθούσε τους Λιβανέζους να ξεσηκωθούν ενάντια της Χεζμπολάχ και του ηγέτη της Σειχη Nasrallah, τον οποίο τον χαρακτήριζε σαν μαριονέτα της Συρίας και του Ιράν και ο οποίος δεν νοιαζόταν για τους Λιβανέζους πολίτες εικόνες 4.3 και 4.4, προειδοποιώντας τους όμως και για τις επικείμενες επιθέσεις που θα εξαπολούσε εικόνα 4.5.

Εικόνα 4.3: Δείχνοντας τον Nasrallah ως την πηγή του κακού.



To the Lebanese people,
Beware!!!

He appears to be a brother, but he is a snake.

Πηγή: PSYWAR.ORG (πρόσβαση στις 5/11/2018)

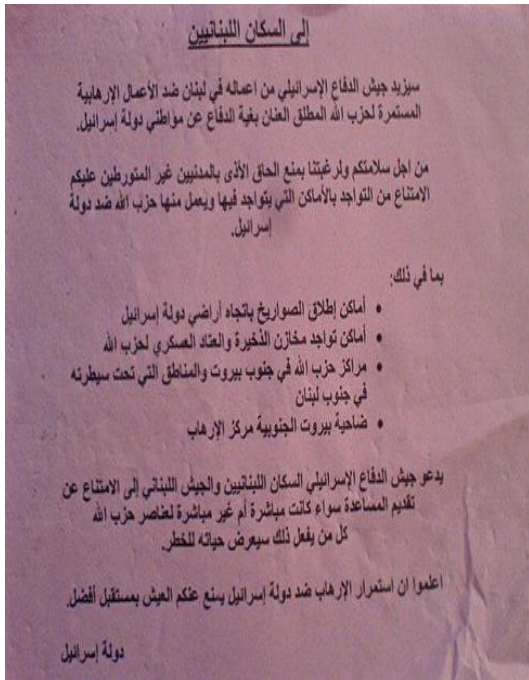
Εικόνα 4.4: Δείχνοντας τον Nasrallah ως μαριονέτα Συρίας, Ιράν και Παλαιστίνης



Need any favors?

²³ Στη συνέντευξη που έδωσε δήλωσε ότι «εάν ήξερα στις 11 Ιουλίου ότι η ενέργεια αυτή προκαλούσε πόλεμο δεν θα την προκαλούσα» περισσότερα στο Nasrallah: *We Wouldn't Have Snatched Soldiers if We Thought it Would Spark War* στο HAARETZ <https://www.haaretz.com/1.4870294> (πρόσβαση 4/11/2018)

Εικόνα 4.5: Προκήρυξη με την οποία προειδοποιεί του πολίτες του Λιβάνου για τις περιοχές τις οποίες θα επιχειρήσει ο Ισραηλινός στρατός.



To the Residents of Lebanon

The Israeli army will increase its actions in Lebanon against the continuing terrorist actions of Hezbollah to defend the citizens of the state of Israel.

For the sake of your own safety, and in our wish not to harm any civilians that are not implicated, you must keep away from the locations where Hezbollah is present and acting against the state of Israel. Including:

- Locations where missiles are fired in the direction of the state of Israel.
- Locations of Hezbollah's arsenals and military equipment.
- Hezbollah's centers south of Beirut and areas under its control in the south of Lebanon.
- Beirut's southern suburb, the center of terrorism.

The Israeli defense army calls on the Lebanese residents and Lebanese army to refrain from aiding, either directly or indirectly, elements of Hezbollah. Anyone who does will be putting their life in danger.

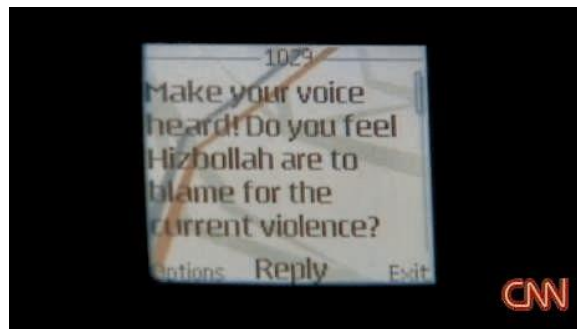
Know that the persistence of terrorism against the state of Israel is keeping you from a better future.

The State of Israel

Πηγή: PSYWAR.ORG (πρόσβαση στις 5/11/2018)

Υπήρξε και προσπάθεια επηρεασμού με την αποστολή μηνυμάτων στα κινητά τηλέφωνα των Λιβανέζων πολιτών με τα οποία καλούσε ουσιαστικά σε εξέγερση τους Λιβανέζους πολίτες εναντίον της Χεζμπολάχ, την οποία κατηγορούσε για την αγριότητα του πολέμου που βίωναν, με τα μηνύματα να εμφανίζονται σαν ενημέρωση των πολιτών εικόνα 4.6.

Εικόνα 4.6: Η ενημέρωση που ερχόταν στα κινητά τηλέφωνα όλων των συνδρομητών που βρισκόταν στην περιοχή.



Πηγή: PSYWAR.ORG (πρόσβαση στις 5/11/2018)

Ταυτόχρονα στο διαδίκτυο εμφανίσε μια ιστοσελίδα με την επωνυμία All4Lebanon.org στην οποία στα πλαίσια μια γκρίζας προπαγάνδας, καθώς όλα τα στοιχεία της ιστοσελίδας παρέπεμπαν σε ιστοσελίδα του Λιβάνου, με τηλέφωνο όμως δορυφορικό και διακομιστή της ιστοσελίδας με έδρα το Ισραήλ, προσκαλούσε τον κόσμο στην παροχή πληροφοριών σχετικά με ενέργειες και εγκαταστάσεις της Χεζμπολάχ, με αντάλλαγμα προστασία και οικονομικές παροχές εικόνα 4.7. Επίσης υπήρξαν και πολλές περιπτώσεις όπου το Ισραήλ είχε επέμβει σε ιστοσελίδες που ανήκαν σε Λιβανέζικους ιστοχώρους με την προσθήκη συνδέσμων με τους οποίους τους ανακατεύθυνε σε ιστοσελίδες με προπαγανδιστικό υλικό εναντίον της Χεζμπολάχ.

Εικόνα 4.7: Από την ιστοσελίδα All4Lebanon.org



Πηγή: PSYWAR.ORG (πρόσβαση στις 5/11//2018)

Επίσης οι Ισραηλινές δυνάμεις κατάφεραν να επέμβουν και στο ηλεκτρομαγνητικό φάσμα, καθώς επενέβησαν στη συχνότητα του τηλεοπτικού σταθμού al-Manar και κατάφεραν να ενσωματώσουν ένα βίντεο ενενήντα δευτερολέπτων στο οποίο φαινόταν ο ηγέτης της Χεζμπολάχ Σεΐχης Nasrallah να αναγνωρίζει την ανωτερότητα των Ισραηλινών Ενόπλων Δυνάμεων ενώ ακολουθούσαν εικόνες από νεκρούς μαχητές της οργάνωσης και κυριευμένο υλικό αυτής.²⁴ Προσπάθησε και να καταστρέψει τις εγκαταστάσεις του σταθμού,

²⁴ Περισσότερα στο Friedman, H. (2006, Αύγουστος 14). *Psychological Operations during the Israel-Lebanon War 2006*. Ανάκτηση Νοέμβριος 5, 2018, από PSYWAR.ORG: <https://www.psywar.org/>

αποτυχημένα όμως, ενώ θα πρέπει να σημειωθεί ότι αντιμετώπισε επιτυχώς την αντίπαλη προπαγάνδα διαγράφοντας τις περισσότερες ιστοσελίδες που χρησιμοποίησε η Χεζμπολάχ στο πλαίσιο της δικής της εκστρατείας. (Pahlavi, 2007)

Από τη μεριά της η Χεζμπολάχ χρησιμοποίησε κυρίως τον τηλεοπτικό σταθμό που ήλεγχε al-Manar προκειμένου να διασπείρει τα μηνύματά της, καθώς και αριθμό ιστοσελίδων που διαχειρίζονταν. Στα εσωτερικά της κοινά (χριστιανούς και σουνίτες μουσουλμάνους πολίτες του Λιβάνου καθώς και σίιτες μουσουλμάνους που δεν είχαν στρατευτεί με την οργάνωση) εμφανιζόταν σαν προστάτης τους διακηρύσσοντας ακόμη και αποζημιώσεις σε όσους τα σπίτια καταστράφηκαν από τους Ισραηλινούς βομβαρδισμούς.²⁵ Επίσης από το 1982 οπότε και δημιουργήθηκε η οργάνωση και κυρίως μετά την αποχώρηση των Ισραηλινών δυνάμεων το 2000, είχε καταφέρει να αποτελεί τον κυριότερο, εάν όχι μοναδικό πάροχο υπηρεσιών κοινής ωφέλειας στην περιοχή, χτίζοντας σχολεία, νοσοκομεία, τζαμιά σε μία προσπάθεια να κερδίσει και την εύνοια του τοπικού στοιχείου, ανεξαρτήτως θρησκευτικής ή εθνοτικής ταυτότητας, μέσα από τα οποία όμως προσπαθούσε να περάσει και την προπαγάνδα της. Οπότε κατά την περίοδο του πολέμου αυτό που έπρεπε να κάνει ήταν να κατηγορεί συνεχώς το Ισραήλ για τις θηριωδίες που προκαλούσε με τους συνεχείς βομβαρδισμούς αμάχων. Επίσης προσπαθούσε μέχρι το τέλος του πολέμου και για αρκετό καιρό αργότερα, να ορίζει ότι αυτός δεν ήταν ένας πόλεμος εναντίον της Χεζμπολάχ μόνο, αλλά εναντίον ολόκληρου του Λιβάνου, χωρίς όμως να εμπλέκει την επίσημη κυβέρνηση του Λιβάνου ή τις επίσημες Ένοπλες Δυνάμεις. Δεν δίστασε να κατηγορήσει τον Ισραηλινό Πρόεδρο Ehud Olmert ως συνεχιστή των NAZI εικόνα 4.8. και πολλές από τις πράξεις των Ισραηλινών Ενόπλων Δυνάμεων να τις παρουσιάζει και να τις συσχετίζει με πράξεις των NAZI.

Στην προσπάθεια της να εκφοβίσει του Ισραηλινούς, η Χεζμπολάχ, παρουσίαζε βίντεο που έδειχνε καταστροφές που προκαλούσαν οι πύραυλοι που εξαπέλυε στο Ισραηλινό έδαφος, ενώ ταυτόχρονα ο σείχης Nasrallah σε συνεχείς εξαγγελίες του από τον τηλεοπτικό σταθμό al-Manar απειλούσε με περισσότερους βομβαρδισμούς οι

israellebanon.php και Israeli Propaganda Video (2006). [Ταινία]. Ανάκτηση Νοέμβριος 5, 2018, από https://www.youtube.com/watch?v=E7x15o_jIoY

²⁵ Από την ομιλία του Σείχη Hasan Nasrallah στον τηλεοπτικό σταθμό al-Manar με τη λήξη του πολέμου στις 14 Αυγούστου 2006 <https://arabist.net/blog/2006/8/16/nasrallahs-speech-full-text.html> (πρόσβαση 5/11/2018).

οποίοι θα έφταναν μέχρι και το Τελ-Αβίδ προκειμένου να στρέψει την κοινή γνώμη του Ισραήλ ενάντια στην κυβέρνησή της. (Pahlavi, 2007)

Εικόνα 4.8: Εικόνες που απεικόνιζαν τον Ισραηλινό Πρόεδρο ως NAZI



Πηγή: https://elainemeinelsupkis.typepad.com/war_and_peace/2006/07/elaine_meinel_s_9.html (πρόσβαση στις 5/11/2018)



Η παραπάνω φωτογραφία δημοσιεύθηκε σε Νορβηγική εφημερίδα
Πηγή: <https://www.jpost.com/Jewish-World/Jewish-News/Cartoonist-likens-Olmert-to-Nazi> (πρόσβαση στις 5/11/2018)

Επίσης το μεγαλύτερο κατόρθωμα της προπαγάνδας της Χεζμπολάχ ήταν ο έλεγχος που κατάφερε να εφαρμόσει πάνω στους δημοσιογράφους που κάλυπταν τον πόλεμο. Ήθελε να περάσει το μήνυμα ότι εκείνοι είναι οι προστάτες του Λιβάνου και το Ισραήλ ο «κακός» που επιτίθεται στους αθώους πολίτες. Οδηγούσαν τους δημοσιογράφους στις περιοχές που είχε βομβαρδίσει το Ισραήλ, ενώ συχνά, ενδεχομένως και σκοπίμως, εμφάνιζαν ασθενοφόρα να περνούν συνέχεια προσπαθώντας να εμφανίζουν μεγαλύτερο από τον ήδη υπάρχοντα αριθμό αμάχων θυμάτων, προκειμένου να κερδίσουν την κοινή γνώμη και να πιέσουν τη διεθνή κοινότητα να αναγκάσει το Ισραήλ να κηρύξει εκεχειρία. Επίσης τους απαγορεύτηκε να κινηματογραφούν τις εκτοξεύσεις πυραύλων και των έργων οχύρωσης που είχαν φτιάξει καθώς και τις ανθρώπινες ασπίδες που χρησιμοποιούσαν. (Pahlavi, 2007) Ήταν τέτοια η επιτυχία τους που ενώ στα μηνύματά τους καταφέρονταν και εναντίον της Αμερικής υπήρξαν και εφημερίδες στις ΗΠΑ οι οποίες υποστήριζαν την προπαγάνδα τους, δείχνοντας την Χεζμπολάχ όχι σαν μια τρομοκρατική οργάνωση, αλλά σαν μια απελευθερωτική.²⁶

²⁶ Από άρθρο των Erlanger, S. Oppel Jr., R.A. *A Disciplined Hezbollah Surprises Israel With Its Training, Tactics and Weapon* στις *The New York Times* (2006, Αύγουστος 7) <https://www.nytimes.com/2006/08/07/world/middleeast/07hezbollah.html> (πρόσβαση 5/11/2018)

Τέλος, η Χεζμπολάχ εξ' αρχής διεκδίκησε και κατάφερε μέσω κυρίως του τηλεοπτικού σταθμού al-Manar να αποτελεί το δίαυλο επικοινωνίας με τον έξω κόσμο, καθώς ήταν ο ίδιος ο Σεΐχης Nasrallah ο οποίος ανέφερε την απαγωγή των δύο στρατιωτών ενώ και με τη λήξη του πολέμου παρέμεινε στο ίδιο μοτίβο, διεκδικώντας τις δάφνες της νίκης. Επίσης κινηματογραφούσε αρκετά βίντεο των επιχειρήσεων και τα οποία μετά από την ανάλογη επεξεργασία και λογοκρισία, χρησιμοποιούνταν από τους ίδιους ή και αποστέλλονταν για διασπορά σε διάφορους τηλεοπτικούς σταθμούς ανά τον κόσμο. (Friedman, 2006) Η ικανότητα όμως της Χεζμπολάχ να διαχειριστεί το παιχνίδι της επικοινωνίας και της ενημέρωσης φαίνεται και από το γεγονός ότι ακόμα και μετά τη λήξη του πολέμου συνέχισε την προπαγάνδα με προκηρύξεις αλλά και με αφίσες στις οποίες αναφέρονταν στη θεϊκή νίκη *The Divine Victory* εικόνα 4.9.

Εικόνα 4.9: Η Θεϊκή Νίκη



Στην αριστερή φωτογραφία φαίνεται ένα αγόρι να κρατάει μία προκήρυξη που διέσπειρε η Χεζμπολάχ στις 14 Αυγούστου 2006 στην παραλιακή πόλη της Zahrani του Λιβάνου, με την οποία συγχαίρει το Λίβανο για τη νίκη του επί του Ισραήλ, ενώ ευχαριστεί και τους πολίτες για την υπομονή τους στον 34 ημερών πόλεμο.

Πηγή: PSYWAR.ORG (πρόσβαση στις 5/11/2018)

4.4 Επιτευχθέντα αποτελέσματα

Η πρωτοφανής δυσανάλογη αεροπορική εκστρατεία που διεξήγαγε η Ισραηλινή αεροπορία στη διάρκεια του πολέμου, είχε σαν αποτέλεσμα να προκαλέσει μεγάλο αριθμό απωλειών στον άμαχο πληθυσμό και καταστροφή μεγάλου αριθμού υποδομών του Λιβάνου, συμπεριλαμβανομένου και του αεροδρομίου της Βηρυτού. Παρόλο που η Χεζμπολάχ ήταν εκείνη η οποία ξεκίνησε ουσιαστικά τον πόλεμο με την επίθεση δυνάμεών της στο Ισραηλινό έδαφος, το θάνατο οκτώ και την απαγωγή άλλων δύο στρατιωτών, τελικά βρέθηκε στο τέλος να αντιστρέφει το κλίμα στη διεθνή κοινή

γνώμη, κάνοντας ακόμα και ΜΜΕ της δύσης να μιλούν για εγκλήματα πολέμου από τη μεριά του Ισραήλ.

Κατάφερε επίσης να αντικρούσει την προσπάθεια της Ισραηλινής προπαγάνδας να προκαλέσει πολιτικούς τριγμούς στο εσωτερικό του Λιβάνου, καθώς η επίσημη κυβέρνηση του Λιβάνου τήρησε ουδέτερη ουσιαστικά στάση,²⁷ ενώ ο τοπικός πληθυσμός, παρόλο που βρισκόταν ανάμεσα στις εγκαταστάσεις που τηρούσε η Χεζμπολάχ τον οπλισμό της δεν αντέδρασε, υπομένοντας του βομβαρδισμούς του Ισραήλ. Οπότε από τους στρατηγικούς στόχους που είχε ορίσει, όπως αναφέρθηκε παραπάνω, ενώ μπορούμε να πούμε ότι έδειξε να επιτυγχάνει την αποτροπή -αν και μεγάλος αριθμός πυραύλων κατάφερε να βληθεί ή να παραμείνει άθικτος- την πολιτική κατάσταση στο Λίβανο, δεν μπόρεσε να την ανατρέψει.

Αντίθετα η Χεζμπολάχ κατάφερε να επηρεάσει το «μυαλό και την καρδιά» τόσο των εσωτερικών της κοινών -ο τοπικός πληθυσμός παρέμεινε πιστός ή τουλάχιστον δεν εναντιώθηκε- αλλά και των εξωτερικών της κοινών. Τα υπόλοιπα αραβικά κράτη, αν και σουνιτικά και εχθρικά απέναντι στο σιιτικό Ιράν τα περισσότερα, υποστήριξαν τον Nasrallah διαδηλώνοντας υπέρ του κρατώντας αφίσες του, ενώ υπήρχαν και εφημερίδες οι οποίες τον παρουσίαζαν ως «σύμβολο αντίστασης» πανηγυρίζοντας για την νίκη που πέτυχε με την γνωστοποίηση του συμφώνου του Σ.Α του ΟΗΕ. (Said Aly, 2006) Όμως και η υπόλοιπη διεθνής κοινότητα ενώ αρχικά καταδίκασε την κίνηση της Χεζμπολάχ, στο τέλος βρέθηκε να βομβαρδίζεται από εικόνες καταστροφών που προκαλούσαν οι Ισραηλινές αεροπορικές επιδρομές και να φτάσει στο σημείο να κατηγορεί την κυβέρνηση του Ισραήλ και τις Ισραηλινές Ένοπλες Δυνάμεις για εγκλήματα πολέμου, ειδικά μετά τον βομβαρδισμό της πόλης Qana και το θάνατο ενός μεγάλου αριθμού άμαχων θυμάτων, κυρίως παιδιών. Αυτή η κατακραυγή, ήταν που οδήγησε και το Ισραήλ να απολογείται και να προσπαθεί να αντικρούσει τις ευθύνες που του αποδίδονταν από την προπαγάνδα της Χεζμπολάχ στο διεθνή και όχι μόνο τύπο.

Ο πόλεμος το Λιβάνου θα μπορούσαμε να πούμε ότι θεωρείται από τις πρώτες επιχειρήσεις ευρείας χρήσης πληροφοριακών επιχειρήσεων, καθώς ένας μη-κρατικός δρώντας, η Χεζμπολάχ κατάφερε να ανατρέψει ένα κλίμα εις βάρος της και να επιτύχει τους στρατηγικούς της σκοπούς, απαγορεύοντας το Ισραήλ να πράξει το ίδιο.

²⁷ Αποποιήθηκε ότι γνώριζε για την απαγωγή των δύο στρατιωτών, καλούσε την Χεζμπολάχ και το Ισραήλ σε ηρεμία, παράλληλα όμως δεν αντέδρασε εναντίον της Χεζμπολάχ προκαλώντας ένα εμφύλιο πόλεμο.

5. Περιπτωσιολογική Μελέτη: Ο Ρωσικός παράγοντας στη e-εθονία

The Bronze Nights

«Ήταν μια καταπληκτική άσκηση ασφαλείας. Απλά δεν γνωρίζουμε σε ποιόν να στείλουμε το λογαριασμό.»

Estonia MoD, Tanel Sepp²⁸

5.1 Το χρονικό της σύγκρουσης

Η Εσθονία είναι μια μικρή χώρα της Βαλτικής, η οποία συνορεύει με τη Ρωσία και τη Λετονία και το 70% του πληθυσμού της είναι Εσθονοί, ενώ Ρώσοι το 25%.²⁹ Βέβαια οι σχέσεις των δύο χωρών διακατέχονται από συγκρούσεις που χρονολογούνται πίσω στο 1920 και την υπογραφή της Συνθήκης Ειρήνης του Tartu οπότε και σηματοδοτείται η δημιουργία του κράτους της Εσθονίας. Το 1940 η Εσθονία προσαρτήθηκε στη Σοβιετική Ένωση και το 1945 με την πτώση της Γερμανίας παρέμεινε στη Σοβιετική Ένωση. Το 1991 με την κατάρρευση της Σοβιετικής Ένωσης δημιουργήθηκε η Δημοκρατία της Εσθονίας με τις σχέσεις της χώρας με τη Ρωσία να παραμένουν τεταμένες, διότι παρέμειναν και εδαφικές διαφορές μεταξύ των δύο χωρών καθώς τα σύνορα των δύο χωρών δεν επανήλθαν στα καθοριζόμενα από το 1920. Το 2005 υπήρξε μια προσέγγιση μεταξύ των δύο χωρών,³⁰ όμως τελικά δεν επετεύχθη συμφωνία,³¹ διότι το Riigikogu (Εσθονικό Κοινοβούλιο) ήθελε να προσθέσει ως προοίμιο στο νόμο για κύρωση των συμφωνιών που υπεγράφησαν, μια αναφορά στη Συνθήκη Ειρήνης του Tartu, στην οποία αναφέρονταν και τα εδάφη τα οποία δεν επιστρέφονταν στην Εσθονία. Η Εσθονία από το 2004 είναι χώρα της Ευρωπαϊκής Ένωσης και του NATO, κινήσεις οι οποίες δεν ήταν αρεστές στη Ρωσία, η οποία έβλεπε να χάνει την επιρροή της σε αυτή τη μικρή χώρα. Η Εσθονία επίσης από το

²⁸ Ο Tanel Sepp είναι Αναπληρωτής Διευθυντής του τμήματος Cyber Policy του Υπουργείου Εθνικής Άμυνας της Εσθονίας. Η δήλωση προέρχεται από άρθρο του Damien McGuinness στο BBCNews δέκα χρόνια μετά από τα γεγονότα που έλαβαν χώρα στην Εσθονία το 2007 με τίτλο *How a cyber attack transformed Estonia* <https://www.bbc.com/news/39655415> (πρόσβαση στις 31/10/2018).

²⁹ Στοιχεία απογραφής την 1 Ιανουαρίου 2012 <http://pub.stat.ee/px-web.2001/Dialog/Saveshow.asp> (πρόσβαση 6/11/2018)

³⁰ Στις 18 Μαΐου 2005, ο Εσθονός υπουργός Εξωτερικών Urmas Paet και ο Ρώσος ομόλογός του Sergei Lavron υπέγραψαν στην Μόσχα την «Σύμβαση μεταξύ της Κυβέρνησης της Δημοκρατίας της Εσθονίας και της Κυβέρνησης της Ρωσικής Ομοσπονδίας για τα σύνορα Εσθονίας-Ρωσίας» και τη «Συνθήκη μεταξύ της Κυβέρνησης της Δημοκρατίας της Εσθονίας και της Κυβέρνησης της Ρωσικής Ομοσπονδίας για την Οριοθέτηση των Θαλάσσιων Ζωνών στον Κόλπο της Φινλανδίας και στον Κόλπο της Narva». Περισσότερα στο Republic of Estonia Ministry of Foreign Affairs *Estonian Review: May 16-22, 2005* <https://vm.ee/en/node/35610> (πρόσβαση 5/11/2018).

³¹ Правительство предложило Путину отказаться от пограничного договора с Эстонией (Putin's government has proposed to abandon the border treaty with Estonia) (2005, Αύγουστος 13) στο LENTA.RU (πρόσβαση 6/11/2018).

1991 είδε ότι προκειμένου να μπορέσει να σταθεί στα πόδια της θα έπρεπε να επενδύσει στην τεχνολογία, κάτι το οποίο το πέτυχε και έχει καταφέρει να είναι η πιο ψηφιοποιημένη χώρα στον κόσμο. (Reynolds, 2016)

Στις αρχές του 2007 η κυβέρνηση της Εσθονίας ψήφισε το νόμο περί προστασίας στρατιωτικών ταφών (Military Graves Protection Act), οπότε και ξεκίνησαν συζητήσεις για τη μεταφορά ενός ρωσικού μνημείου του Β΄ Παγκοσμίου Πολέμου και των λειψάνων που βρίσκονταν από κάτω του, του περίφημου *Bronze Soldier*, από το κέντρο της πόλης, στο στρατιωτικό νεκροταφείο στα περίχωρα της πρωτεύουσας Ταλίν. Ήδη η Υπηρεσία πληροφοριών της Εσθονίας είχε ενδείξεις ότι από το 2006 η Ρωσία είχε προσεγγίσει τους ρωσόφωνους πληθυσμούς και είχε βοηθήσει στο να ιδρυθούν ΜΚΟ στην Εσθονία όπως οι *Nochnoi Dozor (Night Watch)* και *Mir bez Natsizma (World without Nazism)* και οι οποίοι δραστηριοποιήθηκαν έντονα στα γεγονότα του Απριλίου 2007. Επίσης ρωσικά μέσα ενημέρωσης προσπαθούν να κινητοποιήσουν τους τοπικούς πληθυσμούς κάνοντας συνεχείς αναφορές στο υπόψη μνημείο, ενώ συχνά εμφανίζονται Ρώσοι διανοούμενοι και πολιτικοί να χαρακτηρίζουν την Εσθονία ως χώρα φίλια προσκείμενη στο ναζισμό και να καλούν το ρωσικό κοινοβούλιο να επέμβει για να προστατέψει τους ρωσόφωνους κατοίκους από τους ρωσοφοβικούς δυτικούς. (Bulakh, Turay, Kaas, Tuohy, & Visnapuu, 2014) και (Lucas & Pomeranzev, 2016) Το μνημείο του *Bronze Soldier* πρέπει να αναφέρουμε ότι διχάζει την κοινωνία της Εσθονίας, καθώς για τους μεν Εσθονούς αποτελεί ένα κατάλοιπο της Σοβιετικής «κατοχής» ενώ για τους δε ρωσόφωνους ένα μνημείο ηρώων του Β΄ Παγκοσμίου Πολέμου.

Τελικά στις 26 Απριλίου 2007 η κυβέρνηση της Εσθονίας ξεκίνησαν τις εργασίες μεταφοράς του μνημείου, με την προστασία της αστυνομίας. Μεγάλος αριθμός ρωσόφωνων πολιτών συγκεντρώθηκαν στην πλατεία και επιτέθηκαν στην αστυνομία προκαλώντας και μεγάλες ζημιές σε δημόσια κτήρια αλλά σε μαγαζιά στην περιοχή, προχωρώντας ακόμα και σε λεηλασίες. Οι αναταραχές συνεχίστηκαν και την επόμενη μέρα, με την αστυνομία να καταφέρνει να επιβάλει την τάξη το βράδυ της 27 Απριλίου.

Τότε είναι που ξεκινάει η δεύτερη φάση των γεγονότων που έλαβαν χώρα, μια πιο εξελιγμένη και φουτουριστική επίθεση, η οποία έμεινε γνωστή ως η πρώτη κυβερνοεπίθεση μεγάλη κλίμακας εναντίον μιας χώρας. Από τις 27 Απριλίου έως και τις 23 Μαΐου 2007 ακολούθησε μια ευρείας κλίμακα επίθεση στα πληροφοριακά συστήματα της χώρας. Όπως αναφέραμε παραπάνω, η Εσθονία είναι μια έντονα

τεχνολογική χώρα, έχοντας ενσωματώσει την πληροφορική και τα δίκτυα σε όλα τα συστήματα συναλλαγών κράτους με πολίτες και πολιτών μεταξύ τους. Το 2007 υπήρξε η πρώτη χώρα που έδωσε το δικαίωμα συμμετοχής στις εκλογές μέσω του διαδικτύου, με το 5,5% του πληθυσμού να κάνει χρήση αυτού του δικαιώματος. Υπήρξε ένας μεγάλος αριθμός επιθέσεων DDoS³² και Botnet³³ τα οποία καθήλωσαν τα συστήματα της χώρας. Οι κυβερνοεπιθέσεις κορυφώθηκαν την 9 Μαΐου, την *Victory Day*³⁴ ημέρα εθνικής εορτής της χώρας και μετά αντιμετωπίστηκε από ενέργειες που έλαβε η Εσθονία με την βοήθεια και άλλων κρατών, συμπεριλαμβανομένου της Ευρωπαϊκής Ένωσης και του NATO.

5.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν

Κατά τη διάρκεια των γεγονότων που έλαβαν χώρα, η Ρωσία αρνήθηκε οποιαδήποτε συμμετοχή της. Όμως αν μη τι άλλο, η εμπλοκή της γινόταν αντιληπτή σε όλες τις ενέργειες. Ξεκίνησε με μια καμπάνια παραπληροφόρησης της τοπικής κοινωνίας, οργάνωσε ομάδες ρωσόφωνων πολιτών τις οποίες και καθοδηγούσε. Επεδίωξε να παρουσιάσει ότι η μετακίνηση ενός μνημείου του Β΄ Παγκοσμίου Πολέμου ήταν εκείνο το οποίο ξεσήκωσε το ρωσόφωνο πληθυσμό. Σκηνοθετήθηκαν διαδηλώσεις από δημοσιογράφους της κρατικής ρωσικής τηλεόρασης ενώ η προσπάθεια πόλωσης είχε ξεκινήσει ήδη από τις αρχές του έτους. Σε άρθρο που δημοσιεύθηκε στο RT³⁵ στις 16 Φεβρουαρίου 2007 φαίνεται αυτή πόλωση που θέλει να σχηματίσει η ρωσική πλευρά, καθώς παρουσιάζεται μέλος από τις ομάδες «φύλαξης» του αγάλματος που είχαν σχηματιστεί να αναφέρει «If we are in Europe, if we want to be polite to everybody, then this has to stay, It is history and not possible to cancel, to garbage it. And

³² DDoS - Distributed Denial of Service. Στα Ελληνικά μεταφράζεται ως "Κατανεμημένη Επίθεση Αρνήσης Εξυπηρέτησης". Μια επίθεση DDoS έχει σαν στόχο ένα σύστημα, συνήθως έναν server ή ένα ολόκληρο κέντρο δεδομένων (datacenter). Η επίθεση "βομβαρδίζει" το σύστημα με ένα τεράστιο όγκο δεδομένων από διαφορετικές πηγές. Το σύστημα, στην προσπάθειά του να ανταποκριθεί, καταλήγει να εξαντλήσει τους πόρους του, όπως CPU, RAM, κτλ, με αποτέλεσμα να υπερφορτώνεται και στο τέλος να καταρρεύσει. περισσότερα στο PC-Steps <https://www.pcsteps.gr/213898-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-%CE%B5%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7-ddos-dos/> (πρόσβαση 6/11/2018).

³³ Ως botnet ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται ζόμπι. περισσότερα στο in.gr <https://www.in.gr/2011/04/13/tech/future/ti-esti-botnet-einai-to-pc-moy-zompi/> (πρόσβαση 6/11/2018).

³⁴ Υπάρχει έντονη συζήτηση στο πολιτικό σκηνικό της χώρας για το εάν θα πρέπει να γιορτάζεται η 9^η Μαΐου ως εθνική εορτή με τα δεδομένα που είχε ορίσει η Σοβιετική Ένωση και ακολουθεί σήμερα η Ρωσία. περισσότερα στο ERR.ee <https://news.err.ee/595177/ratas-no-reason-why-may-9-should-be-celebrated-in-estonia> (πρόσβαση 6/11/2018).

³⁵ Civic organizations to guard Bronze Soldier in Tallinn στο RT <https://www.rt.com/news/civic-organisations-to-guard-bronze-soldier-in-tallinn/> (πρόσβαση 6/11/2018).

in meantime the people want to put [instead], maybe, a Nazis monument, maybe Hitler... and all the world understands, who was right, who was not, how many millions people died for our peace.» (Civic organisations to guard Bronze Soldier in Tallinn, 2007) Σε διεθνές επίπεδο η Ρωσία ζήτησε από την Ευρωπαϊκή Ένωση να πάρει θέση, καθώς μια χώρα η οποία έγινε μέλος της πριν από 3 χρόνια, συμπεριφέρονταν με αυτόν τον τρόπο σε μνημεία του Β΄ παγκοσμίου Πολέμου και της καταπάτησης του ναζισμού. Χαρακτηριστικά ο υφυπουργός Εξωτερικών της Ρωσίας Alexander Yakovenko ανέφερε ότι «Η μεταφορά του μνημείου αποτελεί μια προσβολή της μνήμης εκείνων οι οποίοι υπερασπίστηκαν όλα τα έθνη της Ευρώπης από το φασισμό» ενώ εξέφρασε και την άποψη ότι οι αρχές της Εσθονίας χρησιμοποίησαν εκτεταμένη βία ενάντια στους πολίτες που διαδήλωναν ειρηνικά. (Harding, 2007) Ανάλογη ήταν και οι χαρακτηρισμοί που χρησιμοποίησε και ο υπουργός Εξωτερικών της Ρωσίας Sergei Lavron χαρακτηρίζοντας, κάθε άλλο παρά με διπλωματική αβρότητα, την ενέργεια της Ρωσίας «disgusting» και ότι «αυτή η βλασφημία θα έχει σοβαρές επιπτώσεις στις σχέσεις των δύο χωρών». (Lee Myers, 2007)

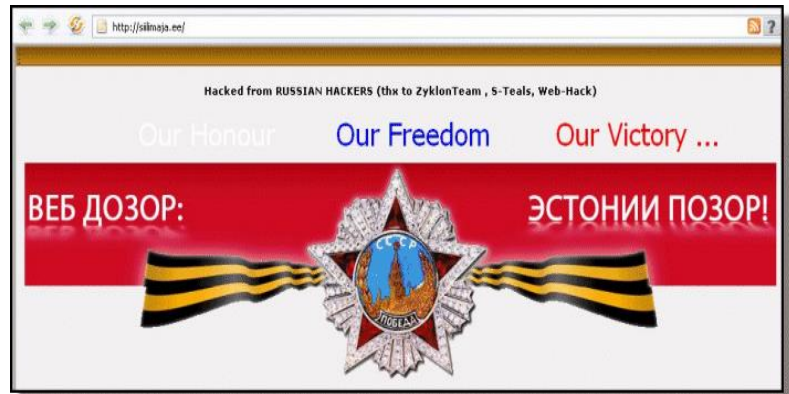
Η δεύτερη φάση αφορούσε τις κυβερνοεπιθέσεις που εκτοξεύτηκαν. Αποτελούσε μια πρωτόγνωρη, σε κλίμακα, ενέργεια. Μεγάλος αριθμός πακέτων δεδομένων ταξίδευαν στο δίκτυο της χώρας. Ομάδες χάκερ επιτέθηκαν σε όλες τις κυβερνητικές σελίδες της χώρας. Οι δύο μεγαλύτερες τράπεζες της χώρας αναγκάστηκαν να καταστείλουν προσωρινά στις δραστηριότητές τους στο διαδίκτυο. Ο mail server του Κοινοβουλίου επλήγη, ενώ ακόμα και τα MME της χώρας δεν μπορούσαν πλέον να ανταλλάσσουν πληροφορίες μεταξύ τους. Σε ορισμένες κρατικές σελίδες εμφανίζονταν ένας ρώσος στρατιώτης εικόνα 5.1 είτε ένα μήνυμα ότι είχαν επέμβει στη σελίδα ρώσοι χάκερ εικόνα 5.2. Υπήρξαν ακόμα και ρωσικές ιστοσελίδες οι οποίες παρείχαν οδηγίες και εργαλεία σε όποιον ήθελε να συμμετάσχει στις DDoS ενέργειες εναντίον της Εσθονίας εικόνα 5.3. Αρχικά η κυβέρνηση, μιας και ο όγκος των επιθέσεων ήταν πρωτόγνωρος, δεν αντελήφθη ότι επρόκειτο για συντονισμένη επίθεση από άλλη χώρα. Όπως επισημαίνει σε συνέντευξή του στο περιοδικό *Foreign Policy* δέκα χρόνια μετά ο τότε Πρόεδρος της Εσθονίας Toomas Hendrik Ilves «Ήταν πρωτάκουστο και κανένας δεν κατάλαβε τι συνέβαινε στην αρχή»³⁶.

³⁶ *Ten Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* (2017, Απρίλιος 27) στο *Foreign Policy* <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/> (πρόσβαση 6/11/2018).

Εικόνα 5.1: Ρώσος στρατιώτης από την Ημέρα της Νίκης



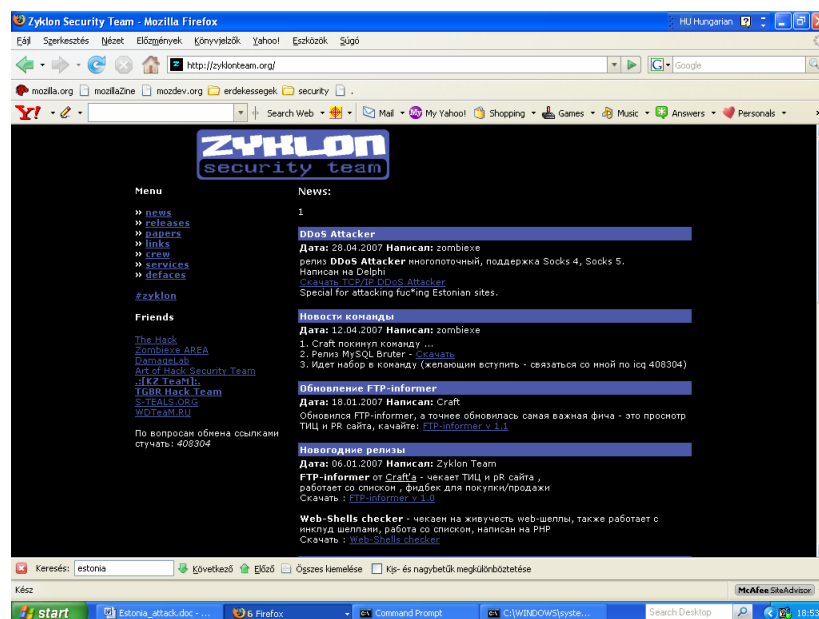
Εικόνα 5.2: Ιστοσελίδα η οποία είχε χακαριστεί από τους Ρώσους



Πηγή: Hungary-CERT (πρόσβαση στις 6/11/2018)

Δεν μπόρεσε βέβαια να αποδειχτεί ποιος ήταν πίσω από αυτές τις επιθέσεις. Όλοι έβλεπαν τη Ρωσία να κρύβεται πίσω από αυτές τις επιθέσεις με εκείνη να αρνείται κάθε συμμετοχή. Αποκόπηκαν όλες οι εξωτερικές IPs και ελέγχθηκε η προέλευσή τους. Αριθμός αυτών διαπιστώθηκε ότι προέρχονταν από τη Ρωσία, μέχρι και ότι μια εξ αυτών προέρχονταν από αξιωματούχο που εργάζονταν στο Κρεμλίνο. Όμως δεν μπορούσε να αποδειχτεί μία εμπλοκή του ρωσικού κράτους στην όλη επίθεση, καθώς πάνω από ένα εκατομμύριο υπολογιστές σε όλο τον κόσμο είχαν χακαριστεί και συμμετείχαν εν αγνοία των χρηστών τους στην επίθεση.

Εικόνα 5.3: Οδηγίες και εργαλεία για επιθέσεις DDoS



Πηγή: Hungary-CERT (πρόσβαση στις 6/11/2018)

Ο υπουργός Άμυνας της Εσθονίας δήλωσε ότι «Αποδείχτηκε τελικά ότι ήταν θέμα Εθνικής ασφάλειας...Μπορεί κάλλιστα να συγκριθεί με αποκλεισμό των λιμανιών στη θάλασσα», καθώς κάθε επαφή στο διαδίκτυο με τον εξωτερικό κόσμο αποκλείστηκε προκειμένου να αντιμετωπιστεί η επίθεση. (Landler & Markoff, 2007). Αργότερα όμως ο ίδιος παραδέχτηκε σε συνέντευξή του στον εσθονικό τηλεοπτικό σταθμό KANAL 2, ότι δεν δύναται να αποδειχτεί η σχέση του Κρεμλίνου με τις κυβερνοεπιθέσεις.³⁷ Υπήρξε βέβαια περίπου 2 χρόνια μετά αποδοχή από μια ομάδα Ρώσων ότι ήταν εκείνοι οι οποίοι κατάφεραν τα πλήγματα ενάντια στην Εσθονία αλλά αυτό δεν ήταν αρκετό. Σύμφωνα με δημοσιεύματα τόσο των *The New York Times* όσο και των *Financial Times* ένα μέλος της ομάδας *NASHI (Ours)*, η οποία συνδέεται άμεσα με το Κρεμλίνο παραδέχτηκε ότι ευθύνονταν για τα χτυπήματα στην Εσθονία, σαν ανταπόδοση των παράνομων ενεργειών της το 2007. (Snachtman, 2009)

Από την πλευρά της η Εσθονία, αντιμετώπισε με τις αστυνομικές δυνάμεις τις εξεγέρσεις, προσάγοντας μεγάλο αριθμό διαδηλωτών, ενώ ένα άνθρωπος σκοτώθηκε. Στις κυβερνοεπιθέσεις κατέβαλε μεγάλη προσπάθεια για να τις περιορίσει. Ο αντίκτυπος που είχαν ήταν μεγάλος. Είναι χαρακτηριστική η δήλωση της Tuuli Aug εκδότρια στην εφημερίδα *Eesti Päevaleht* ότι «Προκάλεσε μεγάλο και ανεξέλεγκτο φόβο, διότι δεν ήταν συνηθισμένοι [σαν κοινωνία] να μην έχουν internet όλη την ώρα και ξαφνικά [αυτό] σταμάτησε να υπάρχει. Δεν μπορούσες να λάβεις πληροφορίες, δεν μπορούσες να κάνεις τη δουλειά σου. Δεν μπορούσες να εισέλθεις στον τραπεζικό σου λογαριασμό, δεν μπορούσες να ελέγξεις τα δρομολόγια του λεωφορείου. Προκαλούσε σύγχυση και φόβο, αλλά δεν συνειδητοποιούσαμε ότι ήταν πόλεμος, διότι δεν το είχαμε ξαναδεί ποτέ». Στη συνέχεια απευθύνθηκε σε άλλες χώρες όπως Ισραήλ και Αμερική προκειμένου να τη βοηθήσουν να αντιμετωπίσει την επίθεση. (O'Connell, 2012)

5.3 Τι σκοπούς εξυπηρετούσαν

Θα πρέπει να έχουμε υπόψη μας ότι η Εσθονία είχε γίνει σχετικά πρόσφατα, πριν από 3 χρόνια, κράτος μέλος της Ευρωπαϊκής Ένωσης και του NATO, και η Ρωσία ένιωθε πλέον την παρουσία αυτών των θεσμών στα σύνορά της καθώς και την επιρροή της σε αυτές τις χώρες, όπου υπάρχει και έντονο ρωσικό στοιχείο, να χάνεται. Επίσης ήδη από τις αρχές του έτους, είχε ξεκινήσει και η συζήτηση περί εγκατάστασης αμερικανικών

³⁷ Όπως αναπαράχθηκε από το ρωσικό σταθμό Sputnik Estonia *haw no evidence of Kremlin involvement in Cyber attacks* (2007, Σεπτέμβριος 6) <https://sputniknews.com/world/2007090676959190/> (πρόσβαση 6/11/2018)

πυραύλων στην Τσεχία και την Πολωνία, που εξόργιζε την Ρωσία. Όταν λοιπόν τέθηκε το ζήτημα της μετακίνησης του μνημείου *Bronze Soldier* δόθηκε η ευκαιρία στη Ρωσία να κάνει επίδειξη της ισχύος της, κυρίως επιδεικνύοντας την επιρροή που είχε στην περιοχή. Έθεσε λοιπόν τρεις στόχους (1) να εμποδίσει τη μετακίνηση του αγάλματος, (2) να επιδείξει τις δυνατότητες που είχε στον κυβερνοπόλεμο (3) να εκθέσει την Ευρωπαϊκή Ένωση και το NATO, καθώς δεν περίμενε κάποια αντίδραση ή ακόμα και να μετρήσει τυχόν αντιδράσεις και (4) να προσβάλει τις οικονομικές δραστηριότητες και την αξιοπιστία της Εσθονίας τόσο στους πολίτες της, όσο και στη διεθνή κοινότητα.

Υπήρξαν έντονες συζητήσεις μήπως θα έπρεπε να εκληφθούν οι παραπάνω επιθέσεις στον κυβερνοχώρο, ως επίθεση εναντίον ενός κ-μ του NATO και σύμφωνα με το άρθρο 5 της Συμφωνίας θα έπρεπε η συμμαχία να ανταποδώσει. Όμως εναντίον ποιανού; Δεν υπήρξε στρατιωτική επίθεση εναντίον της Εσθονίας, ούτε μπόρεσε ποτέ να αποδειχθεί ως τέτοια. Αντιθέτως, σε μία επίδειξη θα μπορούσαμε να πούμε δύναμης, το NATO αποφάσισε το 2008 να εγκαταστήσει στην Εσθονία το Κέντρο Αριστείας για την Αντιμετώπιση Κυβερνοεπιθέσεων (CCDCOE).

5.4 Επιτευχθέντα αποτελέσματα

Η Ρωσία ποτέ δεν αποδέχτηκε την εμπλοκή της στις κυβερνοεπιθέσεις εναντίον της Εσθονίας. Το μνημείο τελικά μετακινήθηκε, με τις εξεγέρσεις απλά επιτάχυνε τις διαδικασίες. Βέβαια στη χώρα ακόμα γίνεται συζήτηση μεταξύ των κομμάτων περί της χρησιμότητας του παραπάνω εγχειρήματος, όμως δεν διαφαίνεται ότι θα επιστρέψει ποτέ στην πρότερη θέση. Οι επιπτώσεις στην οικονομία της Εσθονίας δεν ήταν τελικά τόσο μεγάλες. Στις πληροφοριακές υποδομές της χώρας η ζημιά ήταν πολύ μικρή καθώς η μορφή των επιθέσεων (DDoS) ήταν τέτοια η οποία δεν προκάλεσε ζημιές σε server και router, οπότε με το που ανακαλύφθηκε η απειλή και αντιμετωπίστηκε, επανήλθαν όλα τα συστήματα, χωρίς να έχουν εκτεθεί σε κάποιον κίνδυνο.

Η Ρωσική καμπάνια παραπληροφόρησης βασίστηκε στο έντονο ρωσόφωνο στοιχείο της περιοχής, το οποίο παρακολουθούσε κυρίως τα ρωσικά μέσα ενημέρωσης για την ενημέρωσή του. Υπήρξε βέβαια μια πρωτοφανής επίδειξη δύναμης στον κυβερνοχώρο, η οποία συνδέθηκε με τη Ρωσία, αν και αυτή δεν το αποδέχτηκε ποτέ. Αυτό όμως ταρακούνησε όλες τις χώρες, οι οποίες μέχρι τότε γνώριζαν μόνο για το κυβερνοέγκλημα και δεν μπορούσαν να συνειδητοποιήσουν ενδεχομένως ότι ένα υπολογιστής και το διαδίκτυο μπορούν να γίνουν ένα ισχυρό όπλο. Βέβαια τα

αποτελέσματά του είναι μικρής διάρκειας και σχετικά εύκολα ανατρέψιμα (Herzog, 2011) και (Joubert, 2012).

Όλοι οι πολιτικοί στόχοι που είχε θέσει η Ρωσία απέτυχαν, έδειξαν όμως ότι δεν χρειάζεται άρματα για να επιτεθεί, κάτι που το απέδειξε και τα επόμενα χρόνια στη Γεωργία και ακόμα περισσότερο στην Ουκρανία. Κατάφεραν να χαλυβδώσουν όμως το ΝΑΤΟ, την Ευρωπαϊκή Ένωση οι οποίες συμπεριέλαβαν πλέον τον κυβερνοπόλεμο στο δόγμα τους, ενώ για την ίδια την Εσθονία, κατάφερε να γίνει η πιο εξελιγμένη και πρωτοπόρος στην ασφάλεια δικτύων και προστασίας από κυβερνοεπιθέσεις. Η παραπάνω κρίση που μελετήθηκε, δεν εξελίχθηκε σε καταστροφή κυρίως λόγω της έγκαιρης επέμβασης των αστυνομικών δυνάμεων της χώρας, της φιλοσοφίας που είχε η χώρα περί ασφάλειας δικτύων και υπολογιστών αλλά και της απόμακρης στάσης που κράτησε η Ρωσία, περιορίζοντας έτσι τα αποτελέσματα της όλης εκστρατείας.

6. Περιπτώσιολογική Μελέτη: Το «Ισλαμικό Χαλιφάτο»

«Δεν είναι αρκετό να νικήσουμε το ISIL στο πεδίο της μάχης. Πρέπει να το εμποδίσουμε να ριζοσπαστικοποιεί, να στρατολογεί και να εμπνέει τους άλλους στη βία. Και αυτό σημαίνει να νικήσουμε την ιδεολογία τους. Οι ιδεολογίες δεν ανατρέπονται με όπλα, αλλά ηττούνται από καλύτερες ιδεολογίες – ένα πιο ελκυστικό και συναρπαστικό όραμα.»

POTUS (2009-2017), Barack Obama³⁸

6.1 Πηγαίνοντας πίσω στο χρόνο

Τον Μάρτιο του 2003 οι ΗΠΑ ρίχνουν τον Saddam Hussein, αφήνοντας ένα κενό εξουσίας το οποίο εκμεταλλευθήκαν τρομοκρατικές ομάδες οι οποίες εγκαταστάθηκαν στην περιοχή. Ο Osama bin Laden βρίσκει την ευκαιρία να επεκτείνει την οργάνωσή του Al-Qaeda στην περιοχή, αποστέλλοντας τον υπαρχηγό του Abu Musab Al-Zarqawi, και δημιουργώντας την Al-Qaeda in Iraq (AQI), η οποία προσπαθεί με βομβιστικές επιθέσεις σε Ιρακινούς σιιτικούς στόχους να δημιουργήσει ένα πολωτικό σεχταριστικό κλίμα. Το 2006 ο al-Zarqawi σκοτώνεται από αμερικανική επίθεση, οπότε η AQI αποδυναμώνεται και συνασπίζεται με άλλες τρομοκρατικές οργανώσεις. Το 2010 αναλαμβάνει ηγέτης της ο Abu Bakr Al-Baghdadi ο οποίος εκμεταλλευόμενος τα αποτελέσματα της «Αραβικής Άνοιξης» στη Συρία και της ολοένα και πιο χαοτικής κατάστασης που δημιουργείται εναντίον του Bashar Al-Assad και απλώνει τα δίκτυα του και στη Συρία. Έτσι το 2013 η AQI βρίσκεται πλέον να δραστηριοποιείται τόσο στο Ιράκ όσο και στη Συρία, και μετονομάζεται πλέον σε Islamic State of Iraq and Syria/Levante (ISIS/ISIL). Το 2014 διαρρηγνύονται οι δεσμοί του ISIS με την Al-Qaeda καθώς ο Abu Bakr Al-Baghdadi αρχίζει να καταλαμβάνει εδάφη, με την δεύτερη στις 2 Φεβρουαρίου 2014 να ανακοινώνει ότι πλέον η ISIS δεν αποτελεί κομμάτι της Al-Qaeda³⁹. Στις 29 Ιουνίου του ίδιου έτους ο Abu Bakr Al-Baghdadi ανακοινώνει την ίδρυση του Ισλαμικού Χαλιφάτου ενώ εκδίδεται και ένα έγγραφο με τίτλο *This is the Promise of Allah* το οποίο μεταφράζεται σε τέσσερις γλώσσες (αγγλικά, ρωσικά,

³⁸ Από την ομιλία του Προέδρου των ΗΠΑ Barack Obama στη Σύνοδο Κορυφής για την καταπολέμηση του ISIL και του βίαιου εξτρεμισμού στην έδρα των Ηνωμένων Εθνών στις 29 Σεπτεμβρίου 2015 <https://obamawhitehouse.archives.gov/the-press-office/2015/09/29/remarks-president-obama-leaders-summit-countering-isil-and-violent> (πρόσβαση 31/10/2018)

³⁹ Ο επικεφαλής της Al-Qaeda Ayman Al-Zawahiri σε ανακοίνωσή του στις 3 Φεβρουαρίου 2014 αναφέρει συγκεκριμένα «[ISIS] is not a branch of the al-Qaeda group . . . does not have an organizational relationship with it and [al-Qaeda] is not the group responsible for their actions» περισσότερο στο Sly,L.(2014, Φεβρουάριος 3) *Al-Qaeda disavows any ties with radical Islamist ISIS group in Syria, Iraq* στην The Washington Post https://www.washingtonpost.com/world/middle_east/al-qaeda-disavows-any-ties-with-radical-islamist-isis-group-in-syria-iraq/2014/02/03/2c9afc3a-8cef-11e3-98ab-fe5228217bd1_story.html?utm_term=.edb29d93323b (πρόσβαση 11/11/2018)

γαλλικά και γερμανικά) και το οποίο αποτελεί ουσιαστικά τη διακήρυξη του Χαλιφάτου και παρουσιάζει τον Al-Baghdadi ως Χαλίφη και επικεφαλής όλων των Μουσουλμάνων του κόσμου⁴⁰. Υπαρχηγός του Al-Baghdadi, εκπρόσωπος τύπου του ISIS και επικεφαλής των επιχειρήσεων εξωτερικού και ουσιαστικά εμπνευστής και κύριος συντονιστής της όλης πληροφοριακής επιχείρησης του ISIS είναι ο Abu Mohammad Al-Adnani.

Το Ισλαμικό Χαλιφάτο εξαπολύει μεγάλης κλίμακας πληροφοριακές επιχειρήσεις οι οποίες, αρχικά τουλάχιστον ήταν εναρμονισμένες και με τις επίγειες επιτυχίες του στη Συρία και στο Ιράκ. Χρησιμοποιεί μια εξελιγμένη μηχανή προπαγάνδας η οποία χωρίζεται σε δυο τμήματα: (1) το Al-Hayat Media το οποίο επικεντρώνεται στη στρατολόγηση και στην παρουσίαση μιας ειδυλλιακής κοινωνίας μέσα στο Χαλιφάτο και το (2) Mu'assassat al-Furqan το οποίο εστιάζει στην διάδοση του φόβου. Πίσω από τα δύο αυτά μέσα, βρίσκονται καλοπληρωμένοι τεχνικοί και δημοσιογράφοι Άραβες και μη, των οποίων καθήκον είναι η παραγωγή βίντεο και γραφικών για την υποστήριξη της όλης προπαγάνδας. (Dylan, 2017) Από το 2016 και μετά το Ισλαμικό Χαλιφάτο έχει γνωρίσει μεγάλες ήττες και πλέον έχει περιοριστεί εδαφικά χάνοντας πάνω από το 95% των εδαφών του. Το «ψηφιακό» όμως Ισλαμικό Χαλιφάτο είναι ακόμα πολύ ενεργό. Μπορεί στρατιωτικά το ISIS να έχει αποδυναμωθεί και να έχει αναγκαστεί να επιστρέψει ξανά σε επιχειρήσεις ανταρτοπολέμου, συνεχίζει όμως να στρατολογεί κόσμο και να διαδίδει την προπαγάνδα του στο διαδίκτυο.

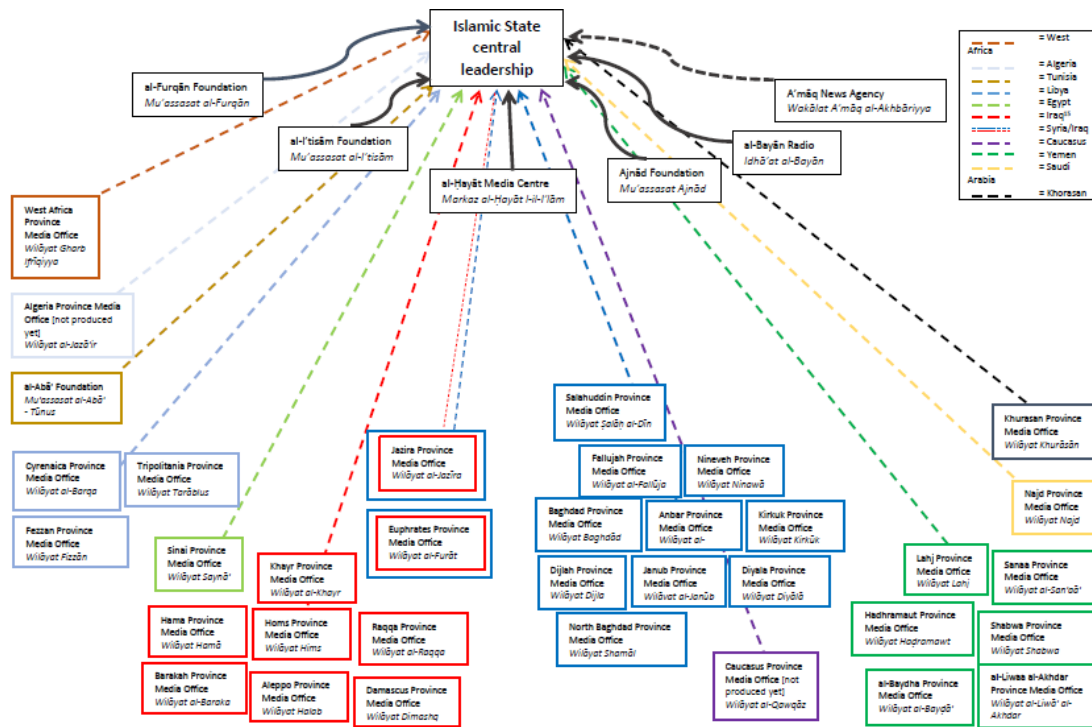
6.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν

Από την 29 Ιουνίου 2014 διαφάνηκε η πορεία που θα ακολουθούσε το ISIS στον τομέα των πληροφοριακών επιχειρήσεων, καθώς την ιδρυτική του διακήρυξη φρόντισε να την μεταφράσει και να τη διαδώσει εκτός από τα αραβικά, που μέχρι τότε ήταν η γλώσσα που χρησιμοποιούσε στην προπαγάνδα του, και σε άλλες τέσσερις γλώσσες. Έκτοτε τα μηνύματα του διαδίδονται σε πολλές γλώσσες, ανάλογα το στοχευμένο ακροατήριο. Με την ίδρυσή του το Ισλαμικό Χαλιφάτο, εφόσον αποτελούσε πέρα από την εδαφική περιοχή που κατείχε και Χαλιφάτο όλου του μουσουλμανικού κόσμου που

⁴⁰ Περισσότερα στο *Sunni rebels declare new 'Islamic caliphate'* (2014, Ιούνιος 30) στο Aljazeera <https://www.aljazeera.com/news/middleeast/2014/06/isil-declares-new-islamic-caliphate-201462917326669749.html> και το έγγραφο *This is the Promise of Allah* κατεβασμένο από το https://ia902505.us.archive.org/28/items/poa_25984/EN.pdf (πρόσβαση 11/11/2018)

επιθυμούσε την εφαρμογή της Σαρία, ανέπτυξε, σε συνεργασία με κατά τόπους μουσουλμανικές τρομοκρατικές ομάδες τα λεγόμενα Wilāyat στα οποία με τις εκεί ομάδες επικοινωνίας προωθούσε μια καλά ενορχηστρωμένη προπαγάνδα με σκοπό την αποκόμιση πόρων, έμψυχων και υλικών, εικόνα 6.1.

Εικόνα 6.1: Τα δίκτυα προπαγάνδας του ISIS ανά τον κόσμο

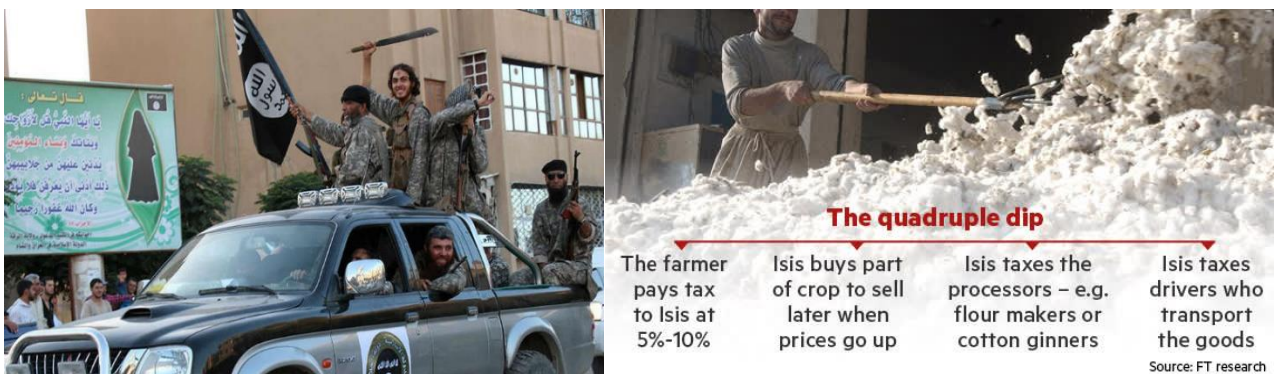


Πηγή: (Winter, The Virtual ‘Caliphate’: Understanding Islamic State’s Propaganda Strategy , 2015, σ. 14)

Στις περιοχές τις οποίες καταλάμβανε, εφάρμοζε πολιτικοστρατιωτική συνεργασία, εγκαθιδρύοντας μονάδες θρησκευτικής αστυνομίας, φορολογίας, εκπαίδευσης εικόνα 6.2. Επίσης ξεκίνησε και την ανάπτυξη υποδομών, σε μια προσπάθεια να κερδίσει νομιμοποίηση ως κράτος εφόσον αυτό πρόσφερε παροχές στον τοπικό πληθυσμό, εξασφαλίζοντας έτσι και μέσω της προπαγάνδας που εξαπέλυε κατευνασμό του τοπικού πληθυσμού, εμπλέκοντας ενεργά και τους τοπικούς επικεφαλής των περιοχών οι οποίοι είτε ήταν ιδεολογικά προσκείμενοι, είτε υπό το καθεστώς φόβου, ενέκυπταν στις απειλές. (Gambhir, 2016) Επίσης γινόταν μια πολύ καλά οργανωμένη επιχείρηση πλουσίματος εγκεφάλου μέσα από τα περίφημα *Media Centers* που αναπτύσσονταν σε κάθε πόλη που καταλάμβανε και που σκοπό είχαν να στρατολογήσουν κόσμο, να αποδείξουν την ισχύ που είχε το Ισλαμικό Χαλιφάτο έναντι

των εχθρών του και να προκαλέσουν όμως και έντονα το αίσθημα του φόβου, με την προβολή αποκεφαλισμών και άλλων φρικαλεοτήτων σε όσους αποφάσιζαν να αντισταθούν εικόνα 6.3. Επίσης απέκοψε κάθε επικοινωνία με τον έξω κόσμο τόσο μέσω διαδικτύου, όσο και μπλοκάροντας το σήμα από ραδιοτηλεοπτικούς σταθμούς που δεν ήλεγχε. Ταυτόχρονα προέβη σε έκδοση μεγάλου αριθμού έντυπου υλικού το οποίο αναπαράγονταν καθημερινά, προσδίδοντας την εντύπωση ότι οι επιτυχίες της ήταν πάρα πολλές. (Winter, Documenting the Virtual 'Caliphate', 2015, σ. 3)

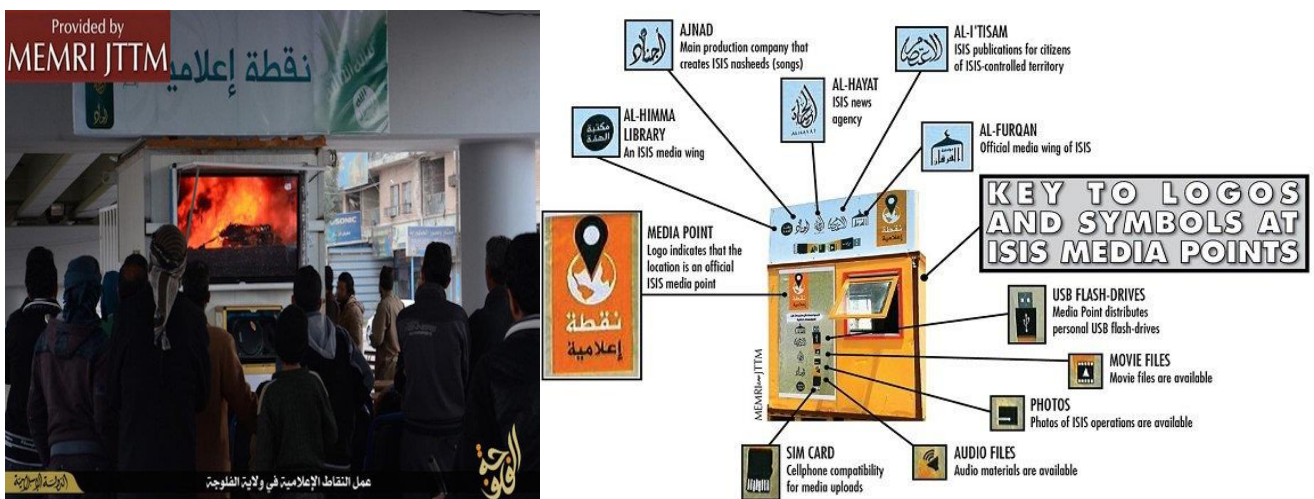
Εικόνα 6.2: Πολιτικοστρατιωτική συνεργασία ISIS στην αστυνόμευση και στη φορολόγηση



Πηγή: <http://www.europe-israel.org/2015/02/la-hisbah-police-religieuse-veille-avec-la-plus-grande-attention-sur-les-restrictions-rigoureuses/> (πρόσβαση 11/11/2018)

Πηγή: Financial Times <https://www.ft.com/content/aee89a00-9ff1-11e5-beba-5e33e2b79e46> (πρόσβαση 11/1/2018)

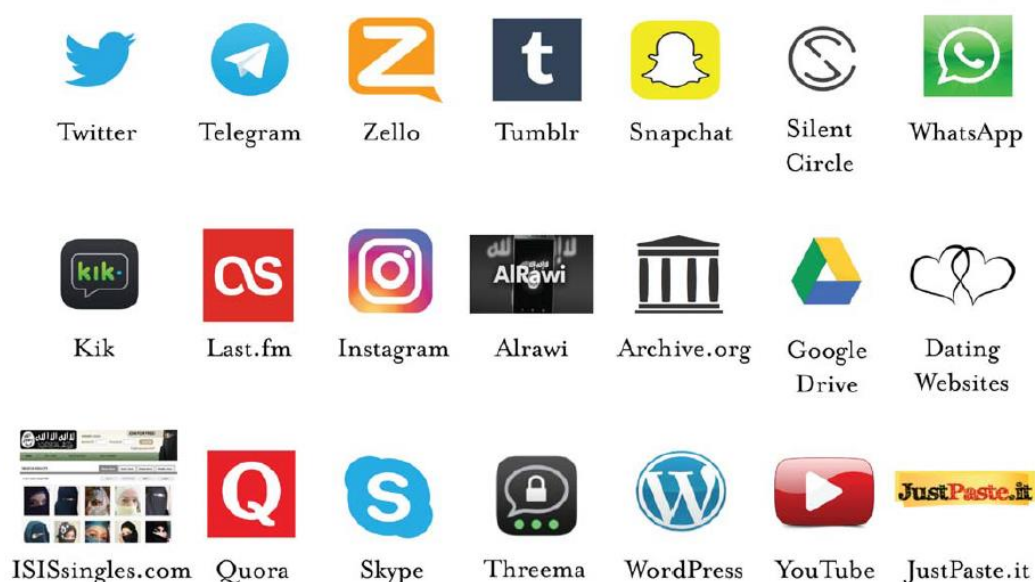
Εικόνα 6.3: Media Center του ISIS



Πηγή: Business Insider <https://www.businessinsider.com/isis-propaganda-strategy-2015-11> (πρόσβαση 11/1/2018)

Αυτό όμως που διαφοροποιεί το ISIS από άλλες τρομοκρατικές οργανώσεις είναι η μεγάλη εκστρατεία που διεξήγαγε μέσω διαδικτύου σε κοινά έξω από τα στενά σύνορα των περιοχών που είχε καταλάβει. Το Ισλαμικό Χαλιφάτο ιδιαίτερα μετά το 2014 έγινε «ψηφιακό». Πέρα από δικές του εφαρμογές που ανέπτυξε, έκανε ευρεία χρήση ήδη διαδεδομένων, εικόνα 6.4, ειδικά στη δύση, εφαρμογών προκειμένου να επιτύχει να στρατολογήσει μαχητές, να συγκεντρώσει χρήματα μέσω δωρεών και να ριζοσπαστικοποιήσει τους μουσουλμάνους υποστηρικτές του σε όλον το κόσμο, ωθώντας τους και συντονίζοντας τρομοκρατικές επιθέσεις σε όλο τον κόσμο. Το Twitter και το You Tube αποδείχτηκαν οι πλατφόρμες στις οποίες διέπρεψε το ISIS.

Εικόνα 6.4: Διαδικτυακές πλατφόρμες που χρησιμοποιεί το ISIS



Πηγή: (Winter, The Virtual ‘Caliphate’: Understanding Islamic State’s Propaganda Strategy , 2015)

Μέσω του Twitter, χρησιμοποιώντας για ίδιους σκοπούς, τα ίδια αναλυτικά εργαλεία, το ISIS κατόρθωσε να στοχοποιήσει καλύτερα τα κοινά του, βάση ηλικίας, μορφωτικού επιπέδου, ενδιαφέροντα και να εκπέμπει στον καθένα τους μηνύματα που να πετύχουν το σκοπό τους. Κάνοντας ευρεία χρήση εμπορικών εφαρμογών οι οποίες αναμετέδιδαν tweets όπως BufferApp, Dawn of good Tidings κ.α. είχαν φτάσει σε σημείο να αναμεταδίδουν, όχι απαραίτητα σε στοχευμένα ακροατήρια, μέχρι και δεκάδες χιλιάδων tweets ημερησίως, κάνοντας τον ISIS να εκπέμπει την προπαγάνδα του σε παγκόσμια κλίμακα. (Berger & Morgan, 2015, σ. 14) Στο You Tube δε, υπήρξε διάδοση μεγάλου αριθμού βίντεο με φρικαλεότητες του ISIS και αποκεφαλισμού συλληφθέντων. Σύμφωνα με την Chistina Pineda σε μια έρευνα που διεξήγαγε η

Homeland Security Digital Library σχετικά με την αναρτήσεις τους ISIS στην περίοδο από 8 Μαρτίου έως 8 Ιουνίου 2018 στο YouTube τα αποτελέσματα ήταν ανησυχητικά καθώς αποδεικνύουν ότι το «ψηφιακό» Ισλαμικό Χαλιφάτο συνεχίζει ακόμα να επιχειρεί. (Pineda, 2018)

- **1.348** βίντεο του ISIS ανέβηκαν στο YouTube, με **163.391** views
- **24%** των βίντεο παρέμειναν για πάνω από δύο ώρες στο YouTube, με **148.590** views
- **76%** των βίντεο παρέμειναν για λιγότερο από δύο ώρες στο YouTube, με **14.801** views
- **278** λογαριασμοί χρηστών ανέβασαν τα **1.348** βίντεο
- **60%** των λογαριασμών παρέμειναν ανοιχτοί ακόμα και όταν η YouTube κατέβασε τα βίντεο λόγω εξτρεμιστικού περιεχομένου.

Επίσης το Ισλαμικό Χαλιφάτο προχώρησε και στην έκδοση δύο περιοδικών τα οποία προσανατολιζόνταν για κοινά εκτός των κατεχόμενων περιοχών. Τα δύο αυτά περιοδικά γραμμένα σε διάφορες γλώσσες, δεν είχαν τίποτα να ζηλέψουν των δυτικών προτύπων έντυπα σε γραφικά. Το *Dabiq* περιείχε φωτογραφικό υλικό και αναφορές από τις επιτυχίες του Ισλαμικού Κράτους ενώ προσπαθούσε να περάσει και μια ρομαντική εικόνα της χρυσής εποχής της ισλαμικής κυριαρχίας. Το *Rumiyah* από την άλλη προσπαθούσε να περάσει τις πολιτικές και θεολογικές αρχές του ISIS, εξηγώντας το ανώφελο της αντίστασης στις διδαχές του εικόνα 6.5.

Εικόνα 6.5: Εξώφυλλα των περιοδικών *Rumiyah* και *Dabiq*



Πηγή: (Clarion Project, 2014)

6.3 Τι σκοπούς εξυπηρετούσαν

Το ISIS είχε θέσει σαν στόχο να εγκαθιδρύσει και να επεκτείνει το Ισλαμικό Χαλιφάτο σε όλο τον μουσουλμανικό κόσμο. Εμμένοντας σε αυτόν τον σκοπό, ακόμα και μετά τις στρατιωτικές ήττες που γνώρισε, προσπάθησε με αφύπνιση πυρήνων στις δυτικές μεγαλουπόλεις και με τρομοκρατικές ενέργειες να αποσταθεροποιήσει και να πολώσει τις δυτικές κυβερνήσεις και φίλια αραβικά κράτη, ελπίζοντας έτσι σε ένα αποκαλυπτικό πόλεμο ο οποίος θα ενώσει όλους τους μουσουλμάνους εναντίον της δύσης.

Προσπάθησε μέσω των πληροφοριακών επιχειρήσεων, τις οποίες τουλάχιστον στην αρχή είχε εναρμονίσει με τις στρατιωτικές επιχειρήσεις που διεξήγαγε, να διατηρήσει τον έλεγχο των περιοχών που κατείχε, να στρατολογήσει υποστηρικτές, τόσο στο εσωτερικό όσο και στο εξωτερικό, να κάνει επίδειξη δύναμης τόσο σε περιοχές στόχους στις οποίες θα ενεργούσε όσο και διεθνώς. Επίσης μέσω του διαδικτύου, προσπάθησε και κατόρθωσε να δημιουργήσει ένα ψηφιακό Ισλαμικό Χαλιφάτο με πολλούς μουσουλμάνους εξτρεμιστές να το ακολουθούν, και να το ενισχύουν τόσο σε προσωπικό όσο και οικονομικά. Επίσης, σε τακτικό κυρίως επίπεδο, έγινε ευρεία χρήση πλατφορμών ΜΚΔ για τη διακίνηση μηνυμάτων και εντολών προς πυρήνες τρομοκρατών οι οποίοι δραστηριοποιούνται στο εξωτερικό. Η Harleen Gambhir στο *The Virtual Caliphate: ISIS's Information Warfare* κάνει μια απεικόνιση των σκοπών που έθεσε το ISIS.

Εικόνα 6.6: Οι Σκοποί των Πληροφοριακών Επιχειρήσεων του ISIS

ISIS's Military Framework	Objective of ISIS's Information Operations
Controlled Terrain	<ul style="list-style-type: none"> > Compel, coopt, and incorporate populations in areas of control > Assert ISIS's success in governing > Convey narrative of endurance to local residents and outside world
Areas of Expansion	<ul style="list-style-type: none"> > Argue for ISIS's superiority over al Qaeda > Recruit fighters and families to support ISIS's entry into new areas > Intimidate potential rivals > Confuse military forces acting against ISIS > Convey narrative of constant expansion to local residents and outside world
International Terror Campaign	<ul style="list-style-type: none"> > Convey narrative of continued operational strength > Intimidate anti-ISIS actors > Encourage and celebrate polarization in the West
Online Recruitment	<ul style="list-style-type: none"> > Convey narrative of global war and ultimate victory > Radicalize populations globally > Encourage international lone actor and small cell attacks in support of ISIS

Πηγή: (Gambhir, 2016)

6.4 Επιτευχθέντα αποτελέσματα

Ως προς την επιτυχία της καμπάνιας του ISIS στο πληροφοριακό περιβάλλον, θα μπορούσαμε να την κρίνουμε ιδιαίτερος επιτυχημένη. Κατόρθωσε να είναι ανθεκτική στο χρόνο. Τοποθετώντας λοιπόν τις ενέργειες του ISIS στις διαστάσεις της υψηλής στρατηγική του, παρατηρούμε ότι πέτυχε τους σκοπούς της. Κατόρθωσε είτε με το φόβο που διέσπειρε είτε κερδίζοντας την καρδιά και το μυαλό του τοπικού πληθυσμού να έχει έσοδα τα οποία για το 2015 έφθασαν να κυμαίνονται στα 2,4 δισεκατομμύρια δολάρια, ο μεγαλύτερος όγκος των οποίων προέρχονταν μεν από εκμετάλλευση πλουτοπαραγωγικών πηγών της περιοχής, κυρίως στη μαύρη αγορά, αλλά και από ιδιαίτερα υψηλή φορολόγηση, επιβολή προστίμων και κατάσχεση περιουσιών. (Binder & Poirot, 2016) Και όλα αυτά, χωρίς να υπάρχει αντίσταση από τον τοπικό πληθυσμό, ο οποίος είτε υποτάσσονταν στη θέληση του καθεστώτος του ISIS, είτε αποφάσιζε να αποχωρήσει πριν ακόμα φθάσουν οι δυνάμεις στην περιοχή. Αξιοσημείωτη είναι και η προσφορά σε μαχητές που εισέρχονταν στις δυνάμεις του.

Στο διεθνές επίπεδο, το Ισλαμικό Χαλιφάτο επεδίωξε να κερδίσει μια μορφή νομιμοποίησης, κυρίως βέβαια προσπαθώντας να παρουσιαστεί ως μια παν-μουσουλμανική οργάνωση. Για αυτό εξ' αρχής έκοψε δεσμούς με την Al-Qaeda και φρόντισε να εμφανίζεται ως η μόνη τζιχαντιστική οργάνωση. Βάση και των εκδόσεων που διένειμε στο εξωτερικό και στα πλαίσια στρατολόγησης, καλούσε τους μαχητές να έρθουν στο Ισλαμικό Χαλιφάτο που αποτελούσε τη μοναδική περιοχή στον κόσμο που εφαρμόζονταν η Σαρία, ο πραγματικός Ισλαμικός νόμος (ερχόμενο έτσι σε κόντρα με τα υπόλοιπα μουσουλμανικά καθεστώτα κρατικά και μη) μια μουσουλμανική ουτοπία την οποία ως "σωστοί μουσουλμάνοι" πρέπει να έρθουν να την υπηρετήσουν. (Gartenstein-Ross, Barr, & Moreng, 2016, σ. 9) Κατάφερε να κινητοποιήσει περίπου 30.000 μαχητές οι οποίοι ταξίδεψαν, πολέμησαν και αρκετοί σκοτώθηκαν υπερασπίζοντας το Ισλαμικό Χαλιφάτο και οι οποίοι επιστρέφοντας πλέον στις χώρες τους και μέσω ενός ευρύτατου δικτύου που έχει στήσει το ψηφιακό Ισλαμικό Χαλιφάτο συνεχίζει τις δράσεις του στο εξωτερικό. (Walker, 2017)

Η χρήση των MKΔ από το ISIS προκειμένου (1) να προωθήσει το διεθνές του προφίλ, (2) να στρατολογήσει μαχητές και (3) να εμπνεύσει και να συντονίσει πυρήνες τρομοκρατών εκτός των στενών συνόρων του (Berger & Morgan, 2015) εξέπληξε τα δυτικά κράτη που προσπαθούσαν να πολεμήσουν το ISIS μόνο στη Συρία και στο Ιράκ, τουλάχιστον αρχικά και να κατανοήσουν ότι πρέπει την ιδεολογία του να πολεμήσουν, την οποία τη διέδιδε μέσω των MKΔ σε μεγάλο αριθμό ευήκοων ώτων ανά την υφήλιο.

Το 2015 στο *Meeting of Ministers of the Global Coalition on the Defeat of ISIS* ο Αμερικανός ΥΠΕΞ Rex Tillerson ζήτησε τη συνεργασία των χωρών και των τεχνολογικών εταιρειών προκειμένου να αντιμετωπίσουν την τρομοκρατία. Τον Ιούνιο του 2017 εταιρείες κολοσσοί στον τομέα της τεχνολογίας, Google, Facebook, Twitter και Microsoft ανακοίνωσαν τη δημιουργία του *Global Internet Forum to Counter Terrorism (GIFCT)* για την καταπολέμηση του φαινομένου, περιορίζοντάς το αρκετά, χωρίς να μπορεί να το εξαλείψει καθώς υπάρχει πληθώρα εναλλακτικών πλατφορμών και μεθόδων που το ψηφιακό Ισλαμικό Χαλιφάτο αναπροσαρμόζεται και αξιοποιεί⁴¹.

⁴¹ περισσότερα στο Macdonald, S. (2018, Σεπτέμβριος 26) *How tech companies are successfully disrupting terrorist social media activity* στο The Conversation <https://theconversation.com/how-tech-companies-are-successfully-disrupting-terrorist-social-media-activity-98594> (πρόσβαση 12/11/2018)

7. Περιπτώσιολογική Μελέτη: Η σύγκρουση Ρωσίας – Ουκρανίας

«Οι ίδιοι οι ‘κανόνες του πολέμου’ έχουν αλλάξει. Ο ρόλος των μη στρατιωτικών μέσων για την επίτευξη πολιτικών και στρατηγικών στόχων έχει αυξηθεί και σε πολλές περιπτώσεις υπερβαίνουν σε αποτελεσματικότητα της ισχύς από τη χρήση των όπλων.»

Russian MoD, General Valery Gerasimov⁴²

7.1 Το χρονικό της σύγκρουσης

Στις 21 Νοεμβρίου του 2013 η Ουκρανική κυβέρνηση του Viktor Yanukovich αποφάσισε να αποσυρθεί από τις διαπραγματεύσεις ένταξης στην Ευρωπαϊκή Ένωση, κίνηση η οποία πυροδότησε ένα μεγάλο αριθμό διαδηλώσεων στην πλατεία Ανεξαρτησίας του Κιέβου με αίτημα αρχικά τη συνέχιση των διαπραγματεύσεων αλλά στη συνέχεια και μετά την επέμβαση των Ουκρανικών αρχών που οδήγησαν και στη σύλληψη διαδηλωτών, στην παραίτηση της Κυβέρνησης. Οι διαδηλώσεις κλιμακώνονταν με τα κύρια αιτήματα των συγκεντρωμένων να είναι (1) η επιστροφή στις ενταξιακές διαπραγματεύσεις και (2) να αλλάξει η πολιτική ζωή στην Ουκρανία κάτι το οποίο θα ερχόταν με την προκήρυξη εκλογών από την κυβέρνηση (Euronews, 2013). Η ορμή των διαδηλωτών ήταν τέτοια, και η Ουκρανική αστυνομία ανήμπορη πλέον να τους εμποδίσει, που οδήγησε στην κατάληψη κυβερνητικών κτηρίων στο Κίεβο και τελικά στις 21 Φεβρουαρίου 2014 τη φυγή του Προέδρου Yanukovich στη Μόσχα και στις 22 Φεβρουαρίου την επίσημη καθαίρεσή του από τη Βουλή.

Στις 25 Φεβρουαρίου, προσωπικό οπλισμένο και ντυμένο με στολές χωρίς διακριτικά και μάσκες στο πρόσωπο και το οποίο δηλώνει ότι είναι αυτονομιστές, καταλαμβάνει δημόσια κτήρια στην Κριμαία, ενώ αποκόπτονται επικοινωνίες σταθερής και κινητής τηλεφωνίας προς την Ουκρανία και δυνάμεις των Ουκρανικών Ενόπλων Δυνάμεων αποκλείονται εντός των στρατοπέδων τους, ενώ πολεμικά πλοία της Ρωσίας λαμβάνουν θέσεις μπροστά από το λιμάνι της Σεβαστούπολης. Τελικά στις 16 Μαρτίου 2014 διεξάγεται δημοψήφισμα στην Κριμαία με το οποίο ο πληθυσμός αποφασίζει να αποχωρήσει από την Ουκρανία και να επιστρέψει στη Ρωσική

⁴² Ο Στρατηγός Valery Gerasimov είναι από το 2012 Αρχηγός του Γενικού Επιτελείου των Ενόπλων Δυνάμεων και πρώτος Αναπληρωτής Υπουργός της Ρωσικής Ομοσπονδίας. Η δήλωση του προέρχεται από άρθρο στο ρωσικό περιοδικό Military-Industrial Kurier την 27 Φεβρουαρίου 2013, όπως παρατέθηκε σε άρθρο του Robert Coalson στην HUFFPOST στις 09 Φεβρουαρίου 2014 με τίτλο *Top Russian General Lays Bare Putin's Plan for Ukraine* https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html?guccounter=1 (πρόσβαση 31/10/2018)

Ομοσπονδία⁴³. Τελικά στις 21 Μαρτίου ο Ρώσος Πρόεδρος Vladimir Putin επικύρωσε την προσάρτηση της περιοχής στη Ρωσική Ομοσπονδία.

Ταυτόχρονα και στην περιοχή του Donetsk και του Luhansk υπήρχαν αντί-διαδηλώσεις ρωσόφωνων οι οποίοι αντιδρούσαν στις EuroMaidan διαδηλώσεις του Κιέβου και συμπεριφέρονταν με περισσότερη βία. Στις 7 Απριλίου Ρωσόφωνοι αυτονομιστές, υποστηριζόμενοι και από τη Ρωσία, διακήρυξαν την αυτοαποκαλούμενη Λαϊκή Δημοκρατία του Donetsk και Luhansk καταλαμβάνοντας κυβερνητικά κτήρια στο Donetsk και στο Luhansk. Η αντίδραση της Ουκρανικής πλευράς ήταν δυναμική και μέχρι το Σεπτέμβρη του ίδιου έτους είχε ανακαταλάβει τις περιοχές, ενώ θύματα υπήρξαν και από τις δύο πλευρές. Πρωτόκολλο κατάπαυσης πυρός υπογράφηκε στις 5 Σεπτεμβρίου, όμως δεν ίσχυσε ποτέ καθώς οι φιλορωσικές αυτονομιστικές δυνάμεις υποβοηθούμενες και από Ρώσους «εθελοντές» πέρασε στην αντεπίθεση, διώχνοντας τις Ουκρανικές Ένοπλες Δυνάμεις από την περιοχή. Από τότε που ανέλαβαν οι αυτονομιστές την εξουσία στην περιοχή του Donbas (οι περιοχές Donetsk και Luhansk μαζί), η Ουκρανική κυβέρνηση σταμάτησε να πληρώσει τις συντάξεις και τους μισθούς των δημοσίων υπαλλήλων στην περιοχή. Στις 11 Μαΐου 2014, διεξάγεται δημοψήφισμα στην περιοχή για αποχώρηση από την Ουκρανία και ανεξαρτητοποίηση της περιοχής με τα αποτελέσματα, αμφισβητούμενα, να δείχνουν 90% υπέρ. (Walker S. , 2014) Στη συνέχεια ο επικεφαλής των αυτονομιστών στην περιοχή Denis Pushilin ζήτησε όπως το αποτέλεσμα του δημοψηφίσματος ληφθεί από την Ρωσική πλευρά ως αίτημα προσάρτησης της περιοχής στη «μητέρα» Ρωσία. Ο Πρόεδρος Putin όμως, χαιρέτησε το αποτέλεσμα, αλλά αρνήθηκε να θέσει θέμα ενσωμάτωσης της περιοχής στην Ρωσική Ομοσπονδία. Έκτοτε στην περιοχή επικρατεί αναβρασμός με πάνω από 20 εκαεχειρίες να έχουν τεθεί σε ισχύ και να παραβιάζονται σχεδόν αμέσως.

7.2 Μορφές πληροφοριακών επιχειρήσεων που χρησιμοποιήθηκαν

Από το 2007, όπου η Ρωσία, αν και δεν το παραδέχτηκε ποτέ αλλά ούτε αποδείχτηκε επαρκώς, εξαπέλυσε μια πληροφοριακή επίθεση στην Εσθονία, έδρασε παρόμοια, εξελίσσοντας τις τεχνικές της στις γειτονικές της χώρες. Έτσι το 2014 βρέθηκε προετοιμασμένη για να δράσει στο πεδίο της Ουκρανίας. Χρησιμοποιήθηκε η

⁴³ Η περιοχή της Κριμαίας στα βάθη των χρόνων μαστίζονταν από πολλές συγκρούσεις. Το 1954 όταν ανέλαβε την εξουσία στη Σοβιετική Ένωση ο Nikita Khrushchev παραχώρησε την Κριμαία στην Ουκρανία. Το έντονο ρωσικό στοιχείο που υπήρχε, μετά τη διάλυση του σοβιετικού μπλόκ πάντοτε έβλεπε θετικά την αποχώρηση της Κριμαίας από την Ουκρανία και την επιστροφή στην αγκαλιά της μητέρας Ρωσίας (Pikulicka-Wilczewska & Sakwa, 2016)

πλειονότητα των μέσων ενημέρωσης της χώρας, ραδιοφωνικοί και τηλεοπτικοί σταθμοί, έντυπα μέσα και το διαδίκτυο για τη διάδοση ενός πολύ μεγάλου όγκου ειδήσεων, πολλών από τις οποίες ήταν χαλκευμένες. Χρησιμοποιήθηκαν επίσης προσωπικότητες του διπλωματικού, πολιτικού και ακαδημαϊκού χώρου προκειμένου να προσδώσουν μια βαρύτητα στο αφήγημα που επιθυμούσε η ρωσική κυβέρνηση να διαδώσει. (Darczewska, 2014)

Εξ' αρχής οι διαδηλώσεις των EuroMaidan παρουσιάστηκαν τόσο στα εσωτερικά κοινά της Ρωσίας όσο και στις ρωσόφωνες περιοχές της Ουκρανίας όπου εξέπεμπαν οι Ρωσικοί σταθμοί και αποτελούσαν το κυριότερο μέσο ενημέρωσης των πολιτών, ως μια παράνομη κατάλυση του καθεστώτος και ότι οι διαδηλώσεις ήταν υποκινούμενες από τη δύση και κυρίως από της Αμερική. Σκοπός της Ρωσικής πλευράς ήταν να παρουσιάσει την Ουκρανία σαν μια χώρα φασιστική, στην οποία υπάρχουν έντονα ναζιστικά και ρωσοφοβικά πρότυπα, μια χώρα μαριονέτα των Αμερικανών. Βέβαια σε μια χώρα όπου είναι αρκετά αυταρχική, όπως η Ρωσία, θα έπρεπε η εικόνα του ηγέτη της να ενισχύεται, έναντι του αντιπάλου του και να φαίνεται ότι τυγχάνει της λαϊκής αποδοχής όχι μόνο του λαού του αλλά και ολόκληρου του ρωσόφωνου στοιχείου της περιοχής, σε μία προσπάθεια να κερδίσει μια μορφή νομιμοποίησης για την επέμβαση της Ρωσίας εικόνα 7.1

Εικόνα 7.1: Φωτογραφία που διανεμήθηκε από το διαδίκτυο για να ενισχύσει το προφίλ του Προέδρου Putin



Πηγή: (Saznov, et al., 2017)

Σύμφωνα με έκθεση του Κέντρου Αριστείας του NATO για τη Στρατηγική Επικοινωνία η Ρωσία χρησιμοποίησε μια πληθώρα μέσων για τη διενέργεια της προπαγάνδας της συμπεριλαμβανομένου κρατικούς και ιδιωτικούς τηλεοπτικούς σταθμούς (Pervyi Kanal, Rossija 1, NTV, Russia Today, LifeNews), ραδιοφωνικούς σταθμούς (Radio Mayak), εταιρείες κινητής τηλεφωνίας (KyivStar), διαδικτυακά μέσα ενημέρωσης (Regnum, TV Zvezda, Komsomolskaya Pravda, Itar Tass, RIA Novosti) καθώς και Μέσα Κοινωνικής Δικτύωσης (YouTube, Facebook, Vk.com, odnoklassniki.ru), ενώ χρησιμοποιήθηκαν και ουκρανικά μέσα τα οποία είτε πρόσκεινταν είτε λειτουργούσαν από ρωσόφωνους, όπως στην περιοχή τους Donbas. (NATO Stratcom, 2016) Αυτό έδινε την ευκαιρία στη Ρωσική πλευρά να βομβαρδίζει τα ακροατήρια με μεγάλο όγκο πληροφορίας, να παρουσιάζει τη σύγκρουση σαν μια σύγκρουση της Ρωσίας με την δύση και κυρίως την Αμερική, να προσπαθεί να δώσει μια νομιμοποίηση στα δημοψηφίσματα που διενεργήθηκαν, κατά παράβαση του Ουκρανικού συντάγματος και στην ενσωμάτωση της Κριμαίας στη Ρωσική Ομοσπονδία εικόνα 7.2.

Εικόνα 7.2: Φωτογραφίες που διανεμήθηκαν μέσω Facebook μετά το δημοψήφισμα και την προσάρτηση της Κριμαίας



[Μετάφραση] Οι ΗΠΑ δεν έφυγαν από τη Βρετανική Αυτοκρατορία εντελώς νόμιμα



[Μετάφραση] Δημοψήφισμα για την απόσχιση των ΗΠΑ από τον πλανήτη Γη. Προωθήστε εάν συμφωνείτε.

Πηγή: (Saznov, et al., 2017)

Καθώς οι δυνάμεις που ενεπλάκησαν στις συγκρούσεις ήταν κυρίως Ουκρανοί φιλορώσοι αυτονομιστές και «εθελοντές» οι οποίοι μετέβησαν στην Ουκρανία, εναντίον ενός εθνικού στρατού, διανεμήθηκαν και εικόνες οι οποίες είχαν σαν στόχο να πλήξουν την αξιοπιστία των Ουκρανικών Ενόπλων Δυνάμεων εικόνα 7.3, σε μια

προσπάθεια να οδηγήσουν τον Ουκρανικό πληθυσμό να αμφισβητήσει την κυβέρνησή του.

Εικόνα 7.3: Φωτογραφία για την υπονόμηση του Ουκρανικού Στρατού



[Μετάφραση] Στο δρόμο για το Donbas

Στο δρόμο από το Donbas

Πηγή: (Saznov, et al., 2017)

Στο διαδίκτυο υπήρχε μια έντονη κινητικότητα τόσο από τη Ρωσία από τις «φάρμες troll» που διαθέτει και των οποίων σκοπός είναι η διάδοση χιλιάδων μηνυμάτων στα ΜΚΔ καθημερινά, για την παραπληροφόρηση των χρηστών, όσο και από τους αυτονομιστές στην περιοχή του Donbas οι οποίοι παρουσίαζαν κατασκευασμένες ειδήσεις τις οποίες προσπαθούσαν να συνδέσουν με ναζιστικά μορφώματα τα οποία δραστηριοποιούνταν στην Ουκρανία. (Soshnikov, 2017) Όπως είπαμε και προηγουμένως κύριο αφήγημα της ρωσικής και φιλορωσικής πλευράς ήταν να εμφανίζεται η κυβέρνηση της Ουκρανίας ως μια φασιστική, φιλοναζιστική χούντα και οι Ουκρανικές Ένοπλες Δυνάμεις να συσχετιστούν με τα τάγματα θανάτου των NAZI. (Saznov, και συν., 2017)

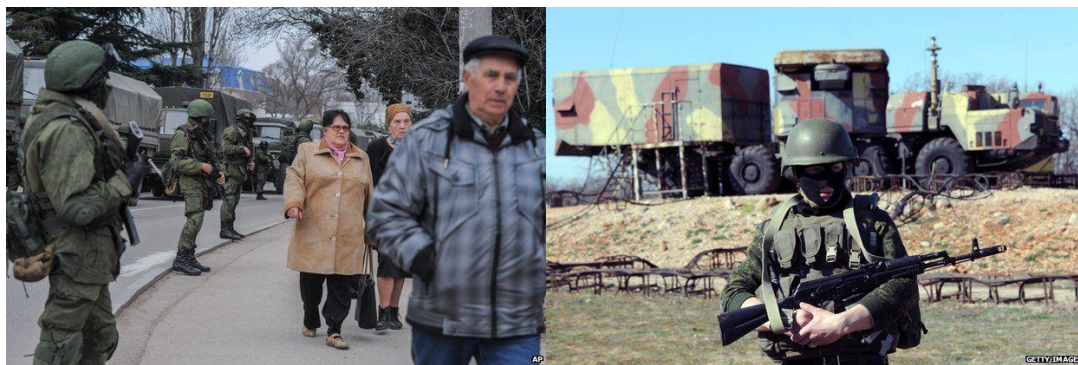
Παράλληλη η Ρωσία προσπάθησε να κερδίσει και τη διεθνή κοινή γνώμη, οργανώνοντας και εκτελώντας ανθρωπιστικές αποστολές στην περιοχή. Στην περίοδο από 2014 έως 2015 εκτέλεσε 50 αποστολές με 100 οχήματα κατά μέσο όρο στην περιοχή του Donbas, προσφέροντας ανθρωπιστική βοήθεια, χωρίς όμως την έγκριση της Ουκρανικής κυβέρνησης ούτε σε συντονισμό με τον Ερυθρό Σταυρό. Αυτή η κίνηση σχολιάστηκε αρνητικά από όλες της χώρες τη δύσης, ενώ η Ουκρανία μιλούσε για καταφανή παραβίαση της κυριαρχίας της από τη Ρωσία. Κυκλοφόρησαν όμως βίντεο και ειδήσεις οι οποίες εκθείαζαν αυτή την ενέργεια, που οι δυτικοί αρνούσαν,

σε μια προσπάθεια παρουσίασης της Ρωσίας ως προστάτιδας των ανθρωπίνων δικαιωμάτων. (The Moscow Times, 2014) και (Saznov, και συν., 2017)

Στον τομέα του κυβερνοχώρου, υπήρξε από την αρχή μια επίθεση στα πληροφοριακά συστήματα της χώρας με επιθέσεις DDoS σε κυβερνητικές ιστοσελίδες, ενώ το Δεκέμβρη του 2015 κατάφερε και άφησε στο σκοτάδι 250.000 Ουκρανούς όταν «επιτέθηκε» ηλεκτρονικά σε μονάδες παραγωγής ενέργειας. Ηλεκτρονικές επιθέσεις δέχτηκε και η Κεντρική Τράπεζα της Ουκρανίας ενώ χαρακτηριστική είναι η ανάληψη ευθύνης από μια ακτιβιστική ομάδα η οποία θεωρείται ότι συνδέεται με το Κρεμλίνο την CyberBerkut, η οποία κατάφερε και επενέβη στην Κεντρική Εκλογική Επιτροπή της χώρας κατά τη διενέργεια των εκλογών το 2014. (Mauere & Janz, 2014) Στο φυσικό/υλικοτεχνικό επίπεδο, πέρα από την καταστροφή των οπτικών ινών που συνέδεαν την Κριμαία με την υπόλοιπη Ουκρανία, αποκόπτοντας έτσι την περιοχή, η Ρωσία είχε και το πλεονέκτημα ότι οι περισσότερες εταιρίες της Ουκρανίας είχαν τον server τους στη Ρωσία, δίνοντας έτσι εύκολη πρόσβαση στους Ρώσους.

Τέλος πρέπει να αναφερθεί και η παραπλάνηση που χρησιμοποίησε η ρωσική πλευρά. Στην Κριμαία, και αργότερα στο Donbas, έκαναν την εμφάνισή τους οι γνωστοί «little green men» ή «polite men», άνδρες οι οποίοι ήταν καλά εξοπλισμένοι, έφεραν πράσινες στολές, ήταν καλά οργανωμένοι, αλλά δεν έφεραν διακριτικά στις στολές τους και ήταν πολύ ευγενικοί απέναντι στους πολίτες. Από την όλη επιχείρηση που έλαβε χώρα, δεν υπάρχει ούτε μια φωτογραφία Ρώσων στρατιωτών, παρά μόνο τέτοιων φιγούρων, να καταλαμβάνουν, δημόσια κτήρια, βάσεις των Ουκρανικών Ενόπλων Δυνάμεων και να κινούνται μεταξύ των πολιτών. (Shevchenko, 2014)

Εικόνα 7.4: Τα «Μικρά Πράσινα Ανθρωπάκια»



Πηγή: BBCNews <https://www.bbc.com/news/world-europe-26532154>

7.3 Τι σκοπούς εξυπηρετούσαν

Η Ρωσία πάντοτε έβλεπε την Ουκρανία ως μια χώρα εντός της σφαίρας επιρροής της και την Κριμαία ως μια περιοχή που προστατεύει την έξοδό της στη Μαύρη θάλασσα και κατ' επέκταση στη Μεσόγειο. Οπότε η κίνηση της Ουκρανίας να ενταχθεί στο ΝΑΤΟ και στην Ευρωπαϊκή Ένωση, ήταν κάτι το οποίο δεν μπορούσε να το δεχτεί. Φυσικό επακόλουθο ήταν να εκμεταλλευτεί την αναστάτωση που δημιουργήθηκε στη χώρα με την παύση από τον φιλορώσο Πρόεδρο Yanukovich των ενταξιακών διαπραγματεύσεων στην Ευρωπαϊκή Ένωση. Σκοπός των πληροφοριακών επιχειρήσεων που διεξήγαγαν ήταν να παρουσιάσουν την κυβέρνηση της Ουκρανίας (μετά την αποχώρηση του Yanukovich) ως μια φασιστική κυβέρνηση, μαριονέτα στα χέρια της Αμερικής, ότι το Σλαβικό Ορθόδοξο στοιχείο δέχεται μια επίθεση από τη δύση και ότι η Ουκρανία είναι ένα failed-state, ανίκανο να προστατεύσει τους πολίτες της. Συχνά κυριαρχούσε ο συσχετισμός των διαδηλωτών EuroMaidan ως NAZI καθώς αποσκοπούσε στην τόνωση του πατριωτικού συναισθήματος των Ρώσων, ενώ επεδίωκε και να συνδέσει και τη διεθνή κοινότητα η οποία υποστήριζε την Ουκρανία ως υποστηρικτή της φασιστικής ιδεολογίας. Η παραπάνω ενέργεια αποσκοπούσε βέβαια κυρίως σε εσωτερική κατανάλωση, προκειμένου να παρουσιάσει την εμπλοκή, την οποία αρνιόταν στο εξωτερικό, ως δίκαιη και αναγκαία.

Η χρήση δυνάμεων χωρίς διακριτικά, έδωσε την ευκαιρία στη ρωσική πλευρά να αρνείται οποιαδήποτε εμπλοκή. Ακόμα και το γεγονός ότι η προπαγάνδα που διεξάγονταν και οι επιχειρήσεις στον κυβερνοχώρο ήταν απόλυτα συντονισμένες με τις επίγειες κινήσεις αυτών των αγνώστης ταυτότητας δυνάμεων, απευθείας σύνδεσή τους με τη ρωσική κυβέρνηση δεν μπόρεσε να αποδειχτεί. Αυτό έδινε τη δυνατότητα να αρνείται ο Πρόεδρος Putin οποιαδήποτε εμπλοκή στην περιοχή, αφήνοντας ΝΑΤΟ, Ευρωπαϊκή Ένωση και διεθνή κοινότητα να αναρωτιέται για το ποιος πραγματικά κρύβεται πίσω από αυτές τις ενέργειες. Επίσης με αυτή τη ενέργεια ο Πρόεδρος Putin μπορούσε να αποκρύψει και στο εσωτερικό της χώρας του την εμπλοκή ρωσικών στρατευμάτων στην περιοχή και να καλύψει με ένα πέπλο μυστικότητας τις απώλειες που προκαλούνταν. (Demirjian, 2015)

Η προπαγάνδα πάντως της Ρωσίας και η παραπληροφόρηση συνεχίζεται ακόμα και σήμερα, σε μια προσπάθεια να δείξει ότι η Ουκρανική κυβέρνηση δεν είναι ικανή να προστατεύσει και να ελέγξει τις περιοχές του Donbas. Για αυτό εμφανίζει δεκάδες Fake news σχετικά με την περιοχή, ακόμα και από παραποιημένους λογαριασμούς στα ΜΚΔ μελών της κυβέρνησης οι οποίοι να παραδέχονται ότι δεν μπορούν να

υποστηρίζουν τους κατοίκους της περιοχής και ότι αυτό είναι ευθύνη της Ρωσίας η οποία ελέγχει την περιοχή. (StopFake, 2018) Στη διεθνή κοινότητα η ρωσική πλευρά προσπάθησε να υποστηρίξει τη νομιμότητα των δημοψηφισμάτων που διεξήχθησαν, όμως έκανε αποδεκτή μόνο την απόφαση στην Κριμαία και όχι στο Donbas.

7.4 Επιτευχθέντα αποτελέσματα

Η στρατηγική που ακολούθησε η Ρωσία στην Ουκρανία, μέχρι στιγμής, φαίνεται να έχει αποδώσει. Η Κριμαία πέρασε στην κατοχή της, με μια αναίμακτη και καλά συντονισμένη επιχείρηση. Στην ανατολική Ουκρανία, η περιοχή μαστιζείται από συγκρούσεις, στις οποίες η ίδια δεν λαμβάνει μέρος επισήμως, αλλά φαίνεται να λειτουργεί ανθρωπιστικά. Η ενταξιακή πορεία της Ουκρανίας στην Ευρωπαϊκή Ένωση και το NATO έχει προς το παρόν παγώσει. Η Ουκρανία, σύμφωνα και με δηλώσεις του Προέδρου της Petro Poroshenko προχωρά σε μια αναδιοργάνωση των δυνάμεών της. Θα μπορούσαμε να πούμε ενδεχομένως ότι η σύγκρουση στην Ουκρανία δεν έχει τελειώσει ακόμα και έχει πολλά να δώσει.

Η απομόνωση πάντως των ανατολικών περιοχών από άλλα πλην ρωσικών μέσα ενημέρωσης και η συνεχή προπαγάνδα που διαδίδεται από τη Ρωσία, διατηρούν μια έκρυθμη κατάσταση στην περιοχή. Σύμφωνα με δημοσκόπηση που διενεργήθηκε τον Αύγουστο του 2018 και αναρτήθηκε και στην ιστοσελίδα CNNgreece, ακόμα και 4 χρόνια μετά, μόλις το 52% επιθυμεί την ένταξη της χώρας στην Ευρωπαϊκή Ένωση και το 15% δεν έχει αποφασίσει ακόμα⁴⁴. (CNN Greece, 2018) Οπότε ενδεχομένως θα μπορούσαμε να πούμε ότι η στρατηγική της Ρωσίας είχε μια επιτυχία ως προς το να δημιουργήσει μια αμφιβολία στον πληθυσμό της Ουκρανίας.

⁴⁴ Ωστόσο τα ποσοστά αυτά ποικίλουν ανάλογα με τις περιοχές της χώρας. Περισσότερο απ' όλους, σε ποσοστό 79%, θέλουν να δουν την Ουκρανία να γίνεται μέλος της ΕΕ οι κάτοικοι της Δυτικής Ουκρανίας αλλά και της Κεντρικής Ουκρανίας σε ποσοστό 58%. Παράλληλα στη Νότια και Ανατολική Ουκρανία, η πλειοψηφία των Ουκρανών δεν συμμερίζεται την προοπτική της ένταξης της χώρας τους στην ΕΕ, σε ποσοστά 58% και 57% αντίστοιχα. Η δημοσκόπηση πραγματοποιήθηκε σε όλες τις περιοχές της Ουκρανίας, εκτός από την Κριμαία και τις περιοχές Λουγκάνσκ και Ντονέτσκ.

8. Επίμετρο – Συμπεράσματα

Κάποιοι ενδεχομένως πλέον να πιστεύουν ότι ο πόλεμος έχει χάσει τα όρια που είχε κάποτε, τα οποία έχουν πλέον διευρυνθεί σημαντικά λόγω της τεχνολογικής προόδου που έχει επιτευχθεί. Όλο και περισσότερο γίνεται συζήτηση στον 21^ο αιώνα για τον πληροφοριακό πόλεμο, ενώ όλο και περισσότεροι δρώντες, ΗΠΑ, Ρωσία, Κίνα αλλά και ΝΑΤΟ και Ευρωπαϊκή Ένωση βλέπουμε να ενσωματώνουν στα δόγματά τους και στην εθνική στρατηγική τους μέσα πληροφοριακών επιχειρήσεων αλλά και μεθόδους αντιμετώπισής τους. Όμως στον τομέα των πληροφοριακών επιχειρήσεων βλέπουμε να δραστηριοποιούνται, με επιτυχία θα έλεγα και μη κρατικοί δρώντες, καθώς η πρόοδος της τεχνολογίας δύναται να προσφέρει τα εμπορικά εκείνα μέσα τα οποία απαιτούνται για να φέρουν εις πέρας την αποστολή τους.

Οι μέθοδοι πλέον των συγκρούσεων έχουν αλλάξει, εμπλέκοντας όλο και περισσότερο τη χρήση πολιτικών, οικονομικών, πληροφοριακών, καθώς και άλλων μη στρατιωτικών μέσων για την επίτευξη των πολιτικών σκοπών των εμπλεκομένων, καθώς σκοπός πλέον δεν ορίζεται η φυσική εξόντωση του αντιπάλου, αλλά ο έλεγχος της καρδιάς και του μυαλού του. Το παιχνίδι της προπαγάνδας είναι παλιό, όμως τα μέσα έχουν εξελιχθεί, όπως επίσης και το επίπεδο των ακροατηρίων που στοχεύει. Πλέον έχουμε περάσει στον έλεγχο της πληροφορίας. Από την προπαγάνδα που πρωταρχικός σκοπός της ήταν να πείσει και να παρακινήσει τις μάζες, πλέον έχουμε περάσει στην παραπληροφόρηση, στην παραγωγή ψευδών ειδήσεων και στη διακίνηση μεγάλου όγκου πληροφορίας ώστε πλέον το ακροατήριο να αποφασίζει να μην εμπλακεί ή να μη γνωρίζει ποια κανάλια πληροφόρησης να εμπιστευθεί. Το μήνυμα πλέον προσαρμόζεται αναλόγως και με τη χρήση σύγχρονων αναλυτικών εργαλείων που προσφέρουν τα ΜΚΔ δίνεται η ευκαιρία αυτό το μήνυμα να κωδικοποιείται και να ανταποκρίνεται διαφορετικά στον καθένα, ενώ αυτοματοποιημένα συστήματα μπορούν να τα αναπαραγάγουν πολλές φορές και χωρίς την άμεση εμπλοκή των παραγωγών τους.

Το διαδίκτυο και τα ΜΚΔ αποτελούν χρήσιμες πλατφόρμες διάδοσης της πληροφορίας. Μπορούν να διαδραματίσουν ένα τόσο θετικό όσο και αρνητικό ρόλο. Τα ΜΚΔ αποτέλεσαν το εργαλείο για την «Αραβική Άνοιξη». Τα ΜΚΔ χρησιμοποιήθηκαν ουσιαστικά τόσο από τρομοκρατικές οργανώσεις (ISIS) όσο και από πολίτες (EuroMaidan) προκειμένου να οργανώσουν τις κινήσεις τους. Μέσα σε λιγότερο από 20 χρόνια, μια πλατφόρμα στο διαδίκτυο, το Twitter, κατόρθωσε να γίνει

ένα από τα κυριότερα μέσα ενημέρωσης, διάδοσης και αναμετάδοσης της πληροφορίας, επηρεάζοντας θετικά ή και παραπλανώντας τις περισσότερες φορές τους λήπτες αποφάσεων. Περνάμε ουσιαστικά από την στρατηγική της άμεσης αντιπαράθεσης δυνάμεων σε μια έμμεση αντιπαράθεση με τη χρήση όλων των δυνατών μέσων, πολιτικών οικονομικών, για την επίτευξη των στόχων που τίθενται τόσο από κρατικούς αλλά και από μη κρατικούς δρώντες. Πεδίο δράσεις πλέον δεν αποτελεί ο χώρος που αναπτύσσονται οι συμβατικές δυνάμεις, αλλά το πεδίο των πληροφοριακών επιχειρήσεων περνάει σε μεγαλύτερο βάθος, στα μεγάλα αστικά κέντρα και απευθύνεται τόσο σε ένοπλους όσο και μη, ενώ μεταφέρεται πλέον και σε μια άλλη διάσταση αυτή του κυβερνοχώρου. Βέβαια, τουλάχιστον ακόμα αν και δεν προβλέπεται μια εύκολη αντιμετώπιση του θέματος, ο κυβερνοχώρος παρουσιάζεται σαν μια χαώδης και χαοτική διάσταση στην οποία δεν μπορεί να επιβληθεί κάποιος εύκολα και στην οποία δραστηριοποιούμαστε όλο και περισσότερο.

Από το κυβερνοέγκλημα, έχουμε περάσει πλέον στον κυβερνοπόλεμο, με κράτη πλέον να στοχοποιούν άλλα κράτη. Τα πλήγματα βέβαια που προκύπτουν έχουν περισσότερο ψυχολογικό αντίκτυπο, παρά οικονομικό καθώς μόλις αναγνωριστούν αντιμετωπίζονται σχετικά εύκολα, και διότι αποσκοπούν περισσότερο στο να παρουσιάσουν τον επιτιθέμενο ως failed state, μειώνοντας τη αξιοπιστία του τόσο μπροστά στους ίδιους τους πολίτες του, όσο και στη διεθνή κοινότητα. Βέβαια από τότε που μια τέτοια ενέργεια έγινε αντιληπτή (Εσθονία 2007) η πλειονότητα των χωρών έχει κάνει σοβαρά βήματα θωράκισης των συστημάτων τους. Η παγκοσμιοποίηση σε μεγάλο βαθμό ωθείται από την επιρροή που ασκεί η τεχνολογική πρόοδος στον οικονομικό, πολιτικό και κοινωνικό τομέα. Η διαχείριση επομένως της πληροφορίας και κυρίως η χειραγώγησή δίνουν μεγάλο πλεονέκτημα καθώς μπορεί να απευθύνεται τόσο στο εσωτερικό, όσο και σε περιφερειακό και παγκόσμιο επίπεδο. Όμως όσο εύκολο και αν μπορεί να αποδειχθεί η αναγνώριση τέτοιων επιθέσεων, το μόνο σίγουρο ότι η απόδειξη των πραγματικών ιθυνόντων είναι πολύ περίπλοκο να αποδειχθεί, προσφέροντας τη δυνατότητα της μη παραδοχής.

Όπως αναφέραμε και στο Κεφάλαιο 3 υψηλή στρατηγική είναι εκείνη η τέχνη χρησιμοποίησης πολιτικών, οικονομικών, ψυχολογικών και στρατιωτικών μέσων, τόσο στην ειρήνη όσο και στον πόλεμο, ώστε να παρέχεται η μέγιστη δυνατή υποστήριξη στην εθνική πολιτική. Είναι εμφανές επομένως ότι εφόσον και στις πληροφοριακές επιχειρήσεις τα μέσα που χρησιμοποιούνται είναι τα ίδια, θα μπορούσαμε ενδεχομένως να υποστηρίξουμε ότι οι πληροφοριακές επιχειρήσεις

μπορούν να χρησιμοποιηθούν ως εργαλείο υψηλής στρατηγικής. Άλλωστε επηρεάζοντας την πληροφορία, επηρεάζονται αντιλήψεις, πεποιθήσεις και τελικά επηρεάζεται και η διαδικασία λήψης απόφασης, η οποία οδηγεί στην υποστήριξη της εθνικής πολιτικής. Από τις περιπτωσιολογικές μελέτες που αναπτύχθηκαν βλέπουμε ότι με τη χρήση των πληροφοριακών επιχειρήσεων οι δρώντες κρατικοί ή μη πέτυχαν έως ένα βαθμό τουλάχιστον τους πολιτικούς τους στόχους. Όμως αυτό το οποίο μπορούμε να διαπιστώσουμε είναι ότι ενώ ξεκίνησε ως ένα εργαλείο αντιστροφής της κοινής γνώμης μεταξύ δύο εμπολέμων (Χεζμπολάχ), σύντομα εξελίχτηκε σε εργαλείο επίτευξης των πολιτικών σκοπών ακόμα και χωρίς την εμφάνιση στρατιωτικών δυνάμεων στη περιοχή (Κριμαία, Ανατολική Ουκρανία), αναβαθμίζονταν την αξία που μπορούν να προσδώσουν αυτού του είδους οι επιχειρήσεις.

Βέβαια πέρα από τις δυνατότητες που προσδίδει η χειραγώγηση της πληροφορίας, τα κράτη και οι θεσμοί θα πρέπει να αναπτύξουν τρόπους αντιμετώπισης τέτοιων μορφών επιθέσεων, τόσο επιθέσεων στον κυβερνοχώρο όσο και επιθέσεων με «ψευδή νέα» που σκοπό έχουν να κατευθύνουν την κοινή γνώμη προς μια αντίληψη που εκείνοι που τα διασπείρουν επιθυμούν. Ο έλεγχος της αξιοπιστίας της πηγής όσο και της ίδιας της πληροφορίας, δεν θα πρέπει να λειτουργεί ως λογοκρισία, αλλά να ενημερώνει τους ίδιους τους πολίτες.

Βιβλιογραφία – Πηγές

Πηγές

- 2000: *Hezbollah celebrates Israeli retreat*. (2000, Μάιος 26). Ανάκτηση Νοέμβριος 4, 2018, από BBCHome: http://news.bbc.co.uk/onthisday/hi/dates/stories/may/26/newsid_2496000/2496423.stm
- Amrani, I. (2006, Αύγουστος 16). *Nasrallah's speech: full text*. Ανάκτηση Νοέμβριος 5, 2018, από The Arabist: <https://arabist.net/blog/2006/8/16/nasrallahs-speech-full-text.html>
- Civic organisations to guard Bronze Soldier in Tallinn. (2007, Φεβρουάριος 16). *RT*.
- Clarion Project. (2014, Σεπτέμβριος 10). *Islamic State's (ISIS, ISIL) Horrific Magazine*. Ανάκτηση Νοέμβριος 11, 2018, από clarionproject.org: <https://clarionproject.org/islamic-state-isis-isil-propaganda-magazine-dabiq-50/>
- CNN Greece. (2018, Σεπτέμβριος 28). *Ουκρανία: Το 52% της χώρας θέλει να ενταχθεί στην Ευρωπαϊκή Ένωση*. Ανάκτηση Νοέμβριος 14, 2018, από CNN Greece: <https://www.cnn.gr/news/kosmos/story/148724/oykrania-to-52-tis-xoras-thelei-na-entaxthei-stin-eyropaiki-enosi>
- Demirjian, K. (2015, Μάιος 28). *Putin denies Russian troops are in Ukraine, decrees certain deaths secret*. Ανάκτηση Νοέμβριος 14, 2018, από The Washington Post: https://www.washingtonpost.com/world/putin-denies-russian-troops-are-in-ukraine-decrees-certain-deaths-secret/2015/05/28/9bb15092-0543-11e5-93f4-f24d4af7f97d_story.html?utm_term=.18c00eeab88d
- EEAS. (χ.χ.). *EU vs Disinfo*. Ανάκτηση Οκτώβριος-Νοέμβριος 2018, από <https://euvsdisinfo.eu/>
- Erlanger, S., & Opiel Jr, R. (2006). A Disciplined Hezbollah Surprises Israel With Its Training, Tactics and Weapons. *The New York Times*. Ανάκτηση Νοέμβριος 5, 2018, από <https://www.nytimes.com/2006/08/07/world/middleeast/07hezbollah.html>
- Estonia has no evidence of Kremlin involvement in cyber attacks*. (2007, Σεπτέμβριος 6). Ανάκτηση Νοέμβριος 6, 2018, από Sputnik: <https://sputniknews.com/world/2007090676959190/>
- Estonian Review: May 16-22, 2005*. (χ.χ.). Ανάκτηση Νοέμβριος 6, 2018, από Republic of Estonia Ministry of Foreign Affairs: <https://vm.ee/en/node/35610>

- Euronews. (2013, Δεκέμβριος 13). *Ukrainian opposition uses polls to bolster cause*. Ανάκτηση Νοέμβριος 13, 2018, από Euronews: <https://www.euronews.com/2013/12/13/ukrainian-opposition-uses-polls-to-bolster-cause>
- Friedman, H. (2006, Αύγουστος 14). *Psychological Operations during the Israel-Lebanon War 2006*. Ανάκτηση Νοέμβριος 5, 2018, από PSYWAR.ORG: <https://www.psywar.org/israellebanon.php>
- Geers, K. (2014). *Pandemonium: National States, National Security, and the Internet. The Tallinn Papers, 1ος(1ο)*. Ανάκτηση Οκτώβριος 21, 2018, από https://www.ccdcoe.org/publications/TP_Vol1No1_Geers.pdf
- Harding, L. (2007, Απρίλιος 29). *Protest by Kremlin as police quell riots in Estonia*. *The Guardian*. Ανάκτηση Νοέμβριος 6, 2018, από <https://www.theguardian.com/world/2007/apr/29/russia.lukeharding>
- Israel, Hezbollah swap prisoners*. (2004, Ιανουάριος 29). Ανάκτηση Νοέμβριος 4, 2018, από CCN International.com: <http://edition.cnn.com/2004/WORLD/meast/01/29/prisoner.exchange/>
- Israeli Propaganda Video* (2006). [Ταινία]. Ανάκτηση Νοέμβριος 5, 2018, από https://www.youtube.com/watch?v=E7x15o_jIoY
- Isral/Lebanon: Israel Responsible for Qana Attack Indiscriminate Bombing in Lebanon a War Crime*. (2006, Ιούλιος 29). Ανάκτηση Νοέμβριος 4, 2018, από Human Rights Watch: <https://www.hrw.org/news/2006/07/29/israel/lebanon-israel-responsible-qana-attack>
- Landler, M., & Markoff, J. (2007, Μάιος 29). *Digital Fears Emerge After Data Siege in Estonia*. *The New York Times*. Ανάκτηση Νοέμβριος 6, 2018, από The New York Times: <https://www.nytimes.com/2007/05/29/technology/29estonia.html>
- Lee Myers, S. (2007, Απρίλιος 27). *Estonia removes Soviet-era war memorial after a night of violence*. *The New York Times*. Ανάκτηση Νοέμβριος 6, 2018, από <https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html>
- Libicki, M. (1995). *What is Information warfare?* Ανάκτηση Οκτωβρίου 13, 2018, από IWS-The Information Warfare Site: <http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html>
- Macdonald, S. (2018, Ιούνιος 26). *How tech companies are successfully disrupting terrorist social media activity*. Ανάκτηση Νοέμβριος 12, 2018, από The

- Conversation: <https://theconversation.com/how-tech-companies-are-successfully-disrupting-terrorist-social-media-activity-98594>
- McGuinness, D. (2017, Απρίλιος 27). How a cyber attack transformed Estonia. *BBCNews*. Ανάκτηση Οκτώβριος 31, 2018, από <https://www.bbc.com/news/39655415>
- Mite, V. (2007, Μάιος 30). *Estonia: Attacks Seen As First Case Of 'Cyberwar'*. Ανάκτηση Νοέμβριος 6, 2018, από RadioFreeEurope RadioLiberty: <https://www.rferl.org/a/1076805.html>
- Nasrallah: We Wouldn't Have Snatched Soldiers if we Thought it Would Spark War*. (2006, Αύγουστος 27). Ανάκτηση Νοέμβριος 4, 2018, από HAARETZ: <https://www.haaretz.com/1.4870294>
- NATO. (2015, Μάιος 18). Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the meeting of the EU Foreign Affairs Council in the format of Ministers of Defence and Ministers of Foreign Affairs. Ανάκτηση Οκτώβριος 14, 2018, από https://www.nato.int/cps/en/natohq/opinions_119822.htm?selectedLocale=en
- NATO. (2015, Ιούνιος 25). Press Conference by NATO Secretary General Jens Stoltenberg following the meeting of the NATO-Ukraine Commission at the level of Defence Ministers - Secretary General's opening remarks. Ανάκτηση Οκτώβριος 14, 2018, από https://www.nato.int/cps/en/natohq/opinions_120971.htm?selectedLocale=en
- NATO Review. (2015). Hybrid war – does it even exist? Ανάκτηση Οκτώβριος 14, 2018, από <https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm>
- Nye Jr, J. (2015). Ο Πόλεμος στον 21ο αιώνα. *Το Βήμα*. Ανάκτηση Οκτώβριος 28, 2018, από <https://www.tovima.gr/2015/02/09/world/o-polemos-ston-21o-aiwna/>
- Nye, J. (2006, Αύγουστος 19). In Mideast, the Goal is 'Smart Power'. *The Boston Globe*. Ανάκτηση Οκτώβριος 31, 2018, από <https://www.belfercenter.org/publication/mideast-goal-smart-power>
- OED. (2007, Ιούνιος). Oxford English Dictionary, 3η. Ανάκτηση Οκτώβριος 14, 2018, από <http://www.oed.com/view/Entry/152605?rskey=WQ9U7W&result=1&isAdvanced=false>

- President Reagan's Remarks on the Strategic Defense Initiative (SDI) to High Level Defense Officials and Staff in the Blue Room* (23 Μαρτίου 1983). [Ταινία].
- Reynolds, M. (2016, Οκτώβριος 20). *Welcome to E-stonia, the world's most digitally advanced society*. Ανάκτηση Νοέμβριος 6, 2018, από WIRED: <https://www.wired.co.uk/article/digital-estonia>
- Russian Federation. (χ.χ.). *The Ministry of Foreign Affairs of the Russian Federation*. Ανάκτηση Οκτώβριος 7, 2018, από Foreign policy/Fundamental documents: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
- Shevchenko, V. (2014, Μάρτιος 14). *"Little green men" or "Russian invaders"?* Ανάκτηση Νοέμβριος 14, 2018, από BBCNews: <https://www.bbc.com/news/world-europe-26532154>
- Sly, L. (2014, Φεβρουάριος 3). *Al-Qaeda disavows any ties with radical Islamist ISIS group in Syria, Iraq*. Ανάκτηση Νοέμβριος 11, 2018, από The Washington Post: https://www.washingtonpost.com/world/middle_east/al-qaeda-disavows-any-ties-with-radical-islamist-isis-group-in-syria-iraq/2014/02/03/2c9afc3a-8cef-11e3-98ab-fe5228217bd1_story.html?utm_term=.edb29d93323b
- Snachtman, B. (2009, Νοέμβριος 3). *Kremlin Kids: We Launched the Estonian Cyber War*. Ανάκτηση Νοέμβριος 6, 2018, από WIRED: <https://www.wired.com/2009/03/pro-kremlin-gro/>
- Soshnikov, A. (2017, Νοέμβριος 13). *BBC Trending: Inside a pro-Russia propaganda machine in Ukraine*. Ανάκτηση Νοέμβριος 14, 2018, από BBCNews: <https://www.bbc.com/news/blogs-trending-41915295>
- StopFake. (2018, Φεβρουάριος 15). *Fake: Europe Denies Donbas Pensions*. Ανάκτηση Νοέμβριος 14, 2018, από StopFake.org: <https://www.stopfake.org/en/fake-europe-denies-donbas-pensions/>
- Sunni rebels declare new 'Islamic caliphate'*. (2014, Ιούνιος 30). Ανάκτηση Νοέμβριος 11, 2018, από aljazeera: <https://www.aljazeera.com/news/middleeast/2014/06/isil-declares-new-islamic-caliphate-201462917326669749.html>
- Tamkin, E. (2017, Απρίλιος 27). *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* Ανάκτηση Νοέμβριος 6, 2018, από Foreign Policy: <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/>

- The Moscow Times. (2014, Αύγουστος 22). *Ukraine Claims 'Direct Invasion' After Russian Convoy Crosses Border*. Ανάκτηση Νοέμβριος 14, 2018, από The Moscow Times: <https://themoscowtimes.com/articles/ukraine-claims-direct-invasion-after-russian-convoy-crosses-border-38626>
- Walker, D. (2017, Οκτώβριος 23). *How real is the threat of returning IS fighters?* Ανάκτηση Νοέμβριος 12, 2018, από BBCNews: <https://www.bbc.com/news/world-41679377>
- Walker, S. (2014, Μάιος 12). *Ukraine: pro-Russia separatists set for victory in eastern region referendum*. Ανάκτηση Νοέμβριος 13, 2018, από The Guardian: <https://www.theguardian.com/world/2014/may/11/eastern-ukraine-referendum-donetsk-luhansk>
- Ευρωπαϊκή Επιτροπή. (2013, Φεβρουάριος). *EUR-Lex*. Ανάκτηση Οκτώβριος 21, 2018, από ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: <https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52013JC0001>
- Ευρωπαϊκό Κοινοβούλιο. (2015, Ιούνιος 16). *IATE*. Ανάκτηση Οκτώβριος 14, 2018, από <http://iate.europa.eu/FindTermsByOtherLanguage.do?lilId=1873368&langId=el&typeOfSearch=s&display=EL>
- Правительство предложило Путину отказаться от пограничного договора с Эстонией. (2005, Αύγουστος 13). *LENТА.RU*. Ανάκτηση Νοέμβριος 6, 2018, από <https://lenta.ru/news/2005/08/13/border/>

Ελληνόγλωσση Βιβλιογραφία

- Beaufre, A. (2015). *Εισαγωγή στη Στρατηγική*. (Π. Μαυρόπουλος, Μεταφρ.) Αθήνα: ΓΕΕΘΑ.
- Sun Tzu. (2003). *Η Τέχνη του Πολέμου*. (Ρ. Λέκκου-Δάντου, Μεταφρ.) Αθήνα: Περίπλους.
- von Clausewitz, K. (2009). *Περί του Πολέμου*. (Ν. Ξεπουλιά, Μεταφρ.) Θεσσαλονίκη: Βάνιας.
- ΓΕΕΘΑ. (2013). *ΔΕ 3.9 «Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου»*.
- ΓΕΕΘΑ. (2016). *ΔΕ 3.2 «Διακλαδικό Δόγμα Πληροφοριακών Επιχειρήσεων»*.
- ΓΕΣ. (2012). *ΕΕ 123-1 «Πληροφοριακές Επιχειρήσεις»*.

Κολιόπουλος, Κ. (2001). *Η Υψηλή Στρατηγική της Αρχαίας Σπάρτης (750-192 π.Χ.)*. Αθήνα: Ποιότητα.

Παπασωτηρίου, Χ. (2011). *Βυζαντινή υψηλή στρατηγική: 6ος-11ος αιώνας* (7η εκδ.). Αθήνα: Ποιότητα.

Ξενόγλωσση Βιβλιογραφία

Abrams, S. (2016, Χειμώνας). Beyond Propaganda Soviet Active Measures in Putin's Russia. *Connections*, 15ος(1ο), σσ. 5-31.

Bentzen, N. (Νοέμβριος 2015). *Understanding propaganda and disinformation*. European Parliamentary Research Service. Ανάκτηση από <http://www.europal.europa.eu/thinktank>

Berger, J., & Morgan, J. (2015). *The ISIS Twitter Census: Defining and describing the population of ISSI supporters on Twitter*. Brookings.

Binder, L., & Poirot, G. (2016). *ISIS Financing in 2015*. Center for the Analysis of Terrorism.

Bulakh, A., Tupay, J., Kaas, K., Tuohy, E., & Visnapuu, K. (2014). *Tools of Destabilization Russian soft Power and Non-military Influence in the Baltic States*. (M. Winnerstig, Επιμ.) Swedish Defence Research Agency.

Cirling, C.-C. (2014). *Cyber defence in the EU. Preparing for Cyber warfare?* European Parliament Research Service.

Čížik, T., Schmidt-Felzmann, A., Amb. Gvineria, S., Pashkov, M., & Šukytė, D. (2017). *Information Warfare - New Security Challenge for Europe*. (T. Čížik, Επιμ.) Bratislava: Centre for European and North Atlantic Affairs (CENAA).

CSIS-Highlights from the Workshop. (2018). *WHO SAID WHAT? The Security Challenges of Modern Disinformation*. Καναδάς: Canadian Security Intelligence Service.

Darczewska, J. (2014). *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*. Βαρσοβία: Center for Eastern Studies.

Dylan, G. (2017). ISIS and Innovative Propaganda: Confronting Extremism in the Digital Age. *Swarthmore International Relations Journal*(1), σσ. 1-9.

Fayutkin, D. (2008, Ιούνιος). The Second Lebanon War: A One-Year Perspective. *Defense & Security Analysis*, 24(2ο), σσ. 213-216. Ανάκτηση Νοέμβριος 4, 2018

- Gambhir, H. (2016). *The Virtual Caliphate: ISIS's Information Warfare*. Washington: Institute for the Study of War.
- Gartenstein-Ross, D., Barr, N., & Moreng, B. (2016). *The Islamic State's Global Propaganda Strategy*. Χάγη: International Centre for Counter-Terrorism.
- Herzog, S. (2011, Καλοκαίρι). Revisiting the Estonian Cyber Attacks: *Journal of Strategic Security*, 4(2ο), σσ. 49-60.
- Howard, M. (2001, Άνοιξη). Grand Strategy in the Twentieth Century. *Defence Studies*, 1(1), σσ. 1-10.
- Joubert, V. (2012). *Five yeras after Estonia's cyber attacks: lessons learned for NATO?* Πώμη: NATO Defence College.
- Libicki, M. C. (2017). The Convergence of Information Warfare. *Strategic Studies Quarterly*, 11, σσ. 49-65.
- Liddell Hart, B. H. (1954). *Strategy* (2η εκδ.). New York.
- Lucas, E., & Pomeranzev, P. (2016). *Winning the Information War Techniques and Counter-Strategies in Russian Propaganda*. Center for European Policy Analysis.
- Manjikian, M. (2010, Ιούνιος). From Global Village to Virtual Battlespace: The Colonizing of the Internet and thw Extension of Realpolitik. *International Studies Quarterly*, 54(2), σσ. 381-401.
- Mauere, T., & Janz, S. (2014). *The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context*. Ζυρίχη: International Relations and Security Network.
- NATO. (2017). *NATO Glossary of Terms and Definitions*. Βρυξέλες: NATO Standarization Office.
- NATO Stratcom. (2016). *Russian Information Campaign Against Ukrianian State and Defence Forces*. Πίγα: NATO Strategic Communications Centre of Excellence.
- Nye Jr., J. (2004) *Soft Power: The Means to Success in World Politics* Νέα Υόρκη:PublicAffairs
- O'Connell, M. (2012). Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 17(2ο), σσ. 187-209.
- Pahlavi, P. (2007, Καλοκαίρι). The 33-Day War: An Example of Psychological Warfare in the Information Age. *Th Canadian Army Journal*, 10(2ο), σσ. 12-24.

- Pikulicka-Wilczewska, A., & Sakwa, R. (2016). *Ukraine and Russia: People, Politics, Propaganda and Perspectives*. Μπρίστολ: E-International Relations.
- Pineda, C. (2018). *ISIS Content on You Tube*. Counter Extremism Project.
- Said Aly, A. (2006). *The Sixth Arab-Israeli War: An Arab Perspective*. Μασσαχουσέτη: Crown Center for Middle East Studies.
- Saznov, V., Mölder, H., Müür, K., Pruulmann-Vengerfeldt, P., Kopötin, I., Ermus, A., . . . Värk, R. (2017). *Russian Information Warfare against Ukrianian State and Defence Forces: April-December 2014*. Ταρτού: Estonian National Defence College.
- Schleifer, R. (2007, Φεβρουάριος 24). Psychological Operations: A New Variation on an Age Old Art: Hezbollah versus Israel. *Studies in Conflict & Terrorism*, 29(1ο), σσ. 1-19.
- The Information Environment and Information Warfare. (2013). Στο I. Porche, C. Paul, M. York, C. Serena, J. Sollinger, E. Axelband, . . . B. Held, *Redefining Information Warfare Boundariew for an Army in Wireless World* (σσ. 11-17). RAND Corporation.
- U.S. Amry TRADOC. (2009). *Pam 5-25-3-0 «The Army Capstone Concept Operational Adaptability—Operating Under Conditions of Uncertainty and Complexity in an Era of Persistent Conflict»*.
- U.S. Joint Chief of Staff. (2010 όπως τροποποιήθηκε το 2016). *JP 1-02 «Dictionary of Military and Associated Terms»*.
- U.S. Joint Chief of Staff. (2012 όπως τροποποιήθηκε το 2014). *JP 3-13 «Information Operations»*.
- U.S. Joint Chief of Staff. (2018). *JP 3-12 «Cyberspace Operations»*.
- von Clausewitz, C. (2007). *On War*. (M. Howard, & P. Paret, Μεταφρ.) New York: Oxford University Press.
- Waxman, D. (2010, Ιανουάριος 5). Between Victory and Defeat: Israel after the War with Hizballah. *The Washington Quarterly*, 30(1ο), σσ. 27-43.
- Winter, C. (2015). *Documenting the Virtual 'Caliphate'*. Quilliam.
- Winter, C. (2015). *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*. Quilliam.