ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

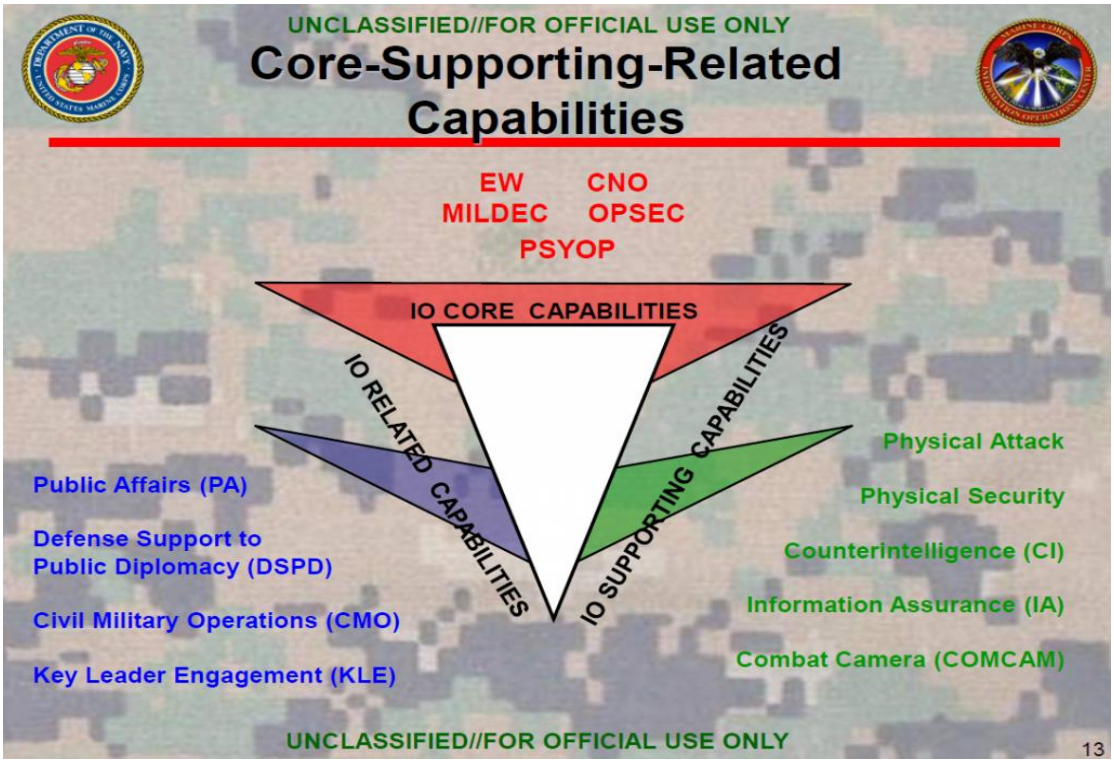
ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ & ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΙΔΙΚΕΥΣΗ : ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ

# ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ. ΔΟΓΜΑ- ΠΡΟΣΕΓΓΙΣΕΙΣ- ΣΥΓΧΡΟΝΕΣ ΤΑΚΤΙΚΕΣ.




**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**ΔΙΤΣΟΥ ΒΑΣΙΛΕΙΟΥ**

*(Α.Μ.: 1212Μ035)*

**ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΧΑΡΑΛΑΜΠΟΣ ΠΑΠΑΣΩΤΗΡΙΟΥ**

**ΑΘΗΝΑ**

**ΣΕΠΤΕΜΒΡΙΟΣ 2014**

# ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

# ΕΙΣΑΓΩΓΗ

Ο κόσμος που ζούμε σήμερα βρίσκεται σε μία μεταβατική φάση. Από τη βιομηχανική επανάσταση που κυριάρχησε στους 2 προηγούμενους αιώνες έχουμε εισέλθει και διανύουμε εδώ και 3 περίπου δεκαετίες την εποχή όπου πρωτεύοντα ρόλο διαδραματίζει η πληροφορία. Για αυτό το λόγο η εποχή μας συχνά χαρακτηρίζεται ως εποχή των δικτύων ή πληροφοριακή εποχή. Η μετάβαση αυτή ριζοσπαστικοποιεί και ανατρέπει σε ένα μεγάλο βαθμό και τον τρόπο με τον οποίο μέχρι σήμερα έβρισκαν στη διεθνή σκακιέρα πεδίο εφαρμογής έννοιες διαχρονικές όπως η πολιτική, ο πόλεμος και η διπλωματία. Οι παραδοσιακές μορφές ισχύος, κατεξοχήν η στρατιωτική και η οικονομική, και οι παράγοντες που τις δημιουργούν, (ενέργεια, ανθρώπινο δυναμικό, τεχνολογία, καινοτομία, φυσικοί πόροι) σίγουρα έχουν και θα συνεχίσουν να έχουν κυρίαρχο ρόλο στη διαμόρφωση του χάρτη του διεθνούς καταμερισμού ισχύος. Ωστόσο, στο νέο πληροφοριακό περιβάλλον που σταδιακά εξελίσσεται και διαμορφώνεται, η ικανότητα πρόσκτησης και σωστής διαχείρισης της πληροφορίας συνιστά ένα κρίσιμο συγκριτικό πλεονέκτημα γι αυτόν που αναγνωρίζει την αξία της, λειτουργώντας ουσιαστικά ως πολλαπλασιαστής ισχύος. Όπως εύστοχα παρατηρεί ο Nye, η ισχύς της πληροφορίας δεν είναι εύκολο να κατηγοριοποιηθεί, διότι τέμνει κάθετα όλους τους οικονομικούς, στρατιωτικούς, κοινωνικούς και πολιτικούς πόρους που δημιουργούν την ισχύ, απομειώνοντας ή πολλαπλασιάζοντας τη δύναμή τους ανάλογα με την περίπτωση.[1] Κάτι τέτοιο καθίσταται ολοένα και περισσότερο προφανές στις μέρες μας, ιδιαίτερα αν αναλογιστούμε πρόσφατα ιστορικά γεγονότα όπως το τρομοκρατικό χτύπημα της 9/11 στις ΗΠΑ και την κλιμακούμενη αδυναμία της υπερδύναμης να καθορίσει τις πολιτικές και οικονομικές εξελίξεις με βάση τα συμφέροντά της σε πολλά σημεία του πλανήτη. Η πολιτική και κοινωνική αστάθεια που επικρατεί σε αρκετές χώρες όπου υπήρξε συντονισμένη στρατιωτική δράση και επέμβαση των ΗΠΑ στο πρόσφατο παρελθόν (Ιράκ, Λιβυή, Αφγανιστάν), το διαφαινόμενο αδιέξοδο στην εξελισσόμενη ουκρανική κρίση και η παρατεινόμενη βία στην Συρία, όλα αυτά τα γεγονότα αλληλοσυνδεόμενα και αλληλοσυμπληρούμενα, αποτελούν ενδείξεις ότι ένα κράτος ακόμη και αν υπερέχει συντριπτικά σε σχέση με τους αντιπάλους του σε όρους <<σκληρής ισχύος>>, δεν είναι δυνατό να κερδίσει έναν πόλεμο μόνο με τη δύναμη των όπλων. Αυτό συμβαίνει διότι ταυτόχρονα με τον συμβατικό διεξάγεται σχεδόν ταυτόχρονα και ένας πόλεμος ιδεών, μία μάχη για <<τις καρδιές και το μυαλό του αντιπάλου>>, η έκβαση του οποίου καθορίζει σε μεγάλο βαθμό και το τελικό αποτέλεσμα της σύγκρουσης. Σε έναν τέτοιου είδος πόλεμο, η πληροφορία και η δυνατότητα ή η αδυναμία εποικοδομητικής χρήσης της, αποτελεί το κρίσιμο εκείνο μέγεθος που σε μεγάλο βαθμό καθορίζει το νικητή και τον ηττημένο. Ο πρώην υπουργός άμυνας των ΗΠΑ Donald Rumsfeld σε μια αποστροφή του λόγου του φωτίζει και επεξηγεί επαρκώς τις παραπάνω αποτυχίες παρατηρώντας πολύ εύστοχα: <<Διεξάγουμε έναν πόλεμο του 21$^{ου}$ αιώνα με ένα υπουργείο άμυνας που ήταν σχεδιασμένο να ανταποκριθεί στις προκλήσεις του 20$^{ου}$. Διαθέτουμε έναν οργανισμό της βιομηχανικής εποχής όμως ζούμε σε μία εποχή της πληροφορίας όπου οι απειλές αναδύονται ξαφνικά, συχνά χωρίς προειδοποίηση, και μας ξαφνιάζουν. Εάν δεν αλλάξουμε γρήγορα τη νοοτροπία μας, οι ελπίδες να επιβιώσουμε σε αυτόν τον κόσμο

[1] Nye and Owens "America's Information Edge". Foreign Affairs 75 (April 1996) 20-36.

είναι ελάχιστες. >>[2]

Ενώ λοιπόν οι όροι και το περιεχόμενο της στρατηγικής επιρροής και επικοινωνίας και των πληροφοριακών επιχειρήσεων είναι σχετικά ασαφείς και δυσνόητοι στο ευρύ κοινό, είναι ξεκάθαρο το γεγονός ότι η επιτυχία πολλών πολιτικών συναρτάται από το μήνυμα που οι παραπάνω δράσεις εκπέμπουν σε διαφορετικά ακροατήρια-τόσο ξένα όσο και εγχώρια- και συνεπακόλουθα από τη δυνατότητα επηρεασμού μίας κρίσιμης μάζας ανθρώπων με την αποτελεσματική μετάδοση μηνυμάτων, εικόνων και παραστάσεων. Ο παράγοντας αυτός είναι καθοριστικός στις διεθνείς σχέσεις, ιδιαίτερα δε στο κομμάτι εκείνο που άπτεται της εθνικής-ασφάλειας των κρατών. Ειδικά στην εποχή μας, όπου πέρα από το συμβατικό τρόπο πολέμου νέες ασύμμετρες απειλές κάνουν την εμφάνιση τους, η διαμόρφωση θετικής στάσης του πληθυσμού απέναντι στις ένοπλες δυνάμεις και γενικότερα την εφαρμοζόμενη στρατηγική μίας χώρας, αποτελεί κύριο και καθοριστικό παράγοντα επιτυχίας σε μία ενδεχόμενη πολεμική αναμέτρηση.

Παρακολουθώντας τη διαχρονική τους εξέλιξη και με αφετηριακό σημείο τις ιστορικές καταβολές τους, η παρούσα εργασία διαπραγματεύεται τα δόγματα και τις πρακτικές των **«πληροφοριακών επιχειρήσεων»** οι οποίες περιλαμβάνουν τον **Ηλεκτρονικό Πόλεμο (Electronic Warfare EW)**, **τις Επιχειρήσεις σε Δίκτυα Υπολογιστών (Computer Network Operations CNO**), **τις Ψυχολογικές Επιχειρήσεις (Psychological Operations PSYOP)**, **την Στρατιωτική Εξαπάτηση (Military Deception MILDEC) και την Ασφάλεια των Επιχειρήσεων (Operation Security OPSEC)** και αποτελούν κομμάτι των **Επιχειρήσεων Επιρροής** που δύναται να διεξάγει ένα κράτος. Παρακολουθηματικές και υποβοηθητικές των παραπάνω αλλά όχι ελάσσονος σημασίας είναι και άλλες δραστηριότητες όπως η **πολιτικοστρατιωτική συνεργασία και οι δημόσιες σχέσεις** που συμπληρώνουν και συμβάλλουν αποφασιστικά στην εδραίωση του κεντρικού σκοπού των πληροφοριακών επιχειρήσεων. Η επιτυχής άσκηση όλων αυτών εξαρτάται από ένα πλήθος παραγόντων που αναλύονται διεξοδικά στην εργασία, ενώ ταυτόχρονα φωτίζονται κρίσιμες παράμετροι που σχετίζονται με την ηθική διάσταση του πληροφοριακού πολέμου και τους νομικούς περιορισμούς που υφίστανται κατά τη διεξαγωγή των συγκεκριμένων επιχειρήσεων. Σε κάθε περίπτωση, οι πληροφοριακές επιχειρήσεις πρέπει να εναρμονίζονται με το γενικότερο πλαίσιο της **Στρατηγικής Επικοινωνίας** που καθορίζεται σε ανώτατο επίπεδο από την στρατιωτική και πολιτική ηγεσία, έτσι ώστε το μήνυμα που εκπέμπουν να είναι ενιαίο και συντονισμένο από ένα κεντρικό όργανο. Τι έχει άραγε όμως να καταδείξει η σύγχρονη εμπειρία όσον αφορά την αποτελεσματικότητα των παραπάνω επιχειρήσεων στο πεδίο της μάχης? Η αλήθεια είναι ότι είναι αρκετά δύσκολο ακόμη και στις μέρες μας να αποτιμηθεί σε ποσοτικούς όρους η συνεισφορά τους στην έκβαση μίας αναμέτρησης. Η αποτελεσματικότητα τους συχνά είναι συνάρτηση της τεχνολογίας που έχουν στα χέρια τους οι αντίπαλες δυνάμεις, ιδιαίτερα όσον αφορά τις τεχνολογίες αιχμής που συνδέονται στενά με τον ηλεκτρονικό πόλεμο και τα δίκτυα υπολογιστών. Επίσης, οι πρακτικές που έχουν επικρατήσει τα τελευταία χρόνια να δανείζονται οι ψυχολογικές επιχειρήσεις στοιχεία από τις τεχνικές του marketing, η να διεξάγονται με όρους πολιτικής

[2] Rumsfeld D. USS CONGRESS, House Armed Service Committee February 5, 2003

επικοινωνίας που χρησιμοποιούνται στις προεκλογικές εκστρατείες προεδρικών υποψηφίων, δε φαίνεται να αποδίδουν πάντα τα αναμενόμενα αποτελέσματα, ειδικότερα όταν τέτοιες προσπάθειες προσκρούουν σε <<σκληρά εχθρικά ακροατήρια>>, όταν πχ έχουν ως αποδέκτες ριζοσπαστικές μουσουλμανικές κοινότητες. Με βάση πάντως και την συσσωρευθείσα εμπειρία των αμερικανικών ενόπλων δυνάμεων από την εφαρμογή πληροφοριακών επιχειρήσεων σε σύγχρονα πεδία μάχης όπως αυτό του Αφγανιστάν και του Ιράκ, και την αξιολόγησή τους με συγκεκριμένους δείκτες αποτελεσματικότητας, προκύπτει το συμπέρασμα ότι η από κοινού σχεδίαση με τις συμβατικές επιχειρήσεις, αποτελεί ένα απαραίτητο προαπαιτούμενο για να έχουν αθροιστική συνεισφορά στο τελικό αποτέλεσμα. Σε ένα διαφορετικό ενδεχόμενο, είναι πολύ πιθανό οι δράσεις που αναπτύσσονται σε τακτικό επίπεδο από τμήματα των ενόπλων δυνάμεων να εκπέμψουν αλληλοσυγκρουόμενα και αλληλοαναιρούμενα μηνύματα και να ζημιώσουν σε βάθος χρόνου τους απώτερους στρατηγικούς σκοπούς ενός πολέμου.

Τέλος, στην εργασία επιχειρείται η ανατομία της στρατηγικής σκέψης που έχουν αναπτύξει μη δυτικοί στρατοί σχετικά με τις επιχειρήσεις επιρροής στο πεδίο της μάχης, όπως ο Ρώσικος και ο Κινέζικος και προβάλλεται ιδιαίτερα το συστατικό στοιχείο της εξαπάτησης που είναι κυρίαρχο στην κουλτούρα αυτών των στρατιωτικών οργανισμών. Η θεωρία συμπληρώνεται με την παράθεση παραδειγμάτων από τα πιο πρόσφατα πολεμικά γεγονότα της Τσετσενίας και της Γεωργίας και παρουσιάζεται εκτενώς ο κρίσιμος ρόλος που είχαν οι επιχειρήσεις αυτές στον γενικότερο σχεδιασμό των ενόπλων δυνάμεων των εμπλεκόμενων κρατών, για την υλοποίηση των αντικειμενικών τους σκοπών.

# ΚΕΦΑΛΑΙΟ 1$^{Ο}$
# Η ΓΕΝΝΗΣΗ ΚΑΙ Η ΕΞΕΛΙΞΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ο ρόλος της πληροφορίας υπήρξε πάντα κρίσιμος στο πεδίο της μάχης. Στην πρώιμη ιστορική καταγραφή αρχαίων πολιτισμών ανευρίσκουμε τα πρώτα ψήγματα στρατιωτικών τακτικών που ενσωματώνουν πολλά από τα στοιχεία που θα μπορούσαν σήμερα να χαρακτηριστούν ως ψυχολογικός πόλεμος, κατασκοπεία για συλλογή πληροφοριών, εξαπάτηση του αντιπάλου, κλπ. χρήση δηλαδή γενικά μεθόδων πέρα το συμβατικό παραδοσιακό τρόπο

πολέμου. Σε ένα π.χ. από τα πιο αρχέγονα έργα στη ιστορία την στρατηγικής σκέψης, << την Τέχνη του Πολέμου>>, ο Σουν Τσου ισχυρίζεται ότι <<*όλος ο πόλεμος βασίζεται στην εξαπάτηση*>> και ότι κύριο συστατικό της στρατιωτικής επιτυχίας είναι το << να γνωρίζεις καλά τόσο τον εαυτό σου όσο και τον εχθρό >>. [3] Επίσης, ο <<δούρειος ίππος>>, το γνωστό τέχνασμα με το οποίο οι έλληνες κατάφεραν να κατακτήσουν την Τροία, συνιστά το πρώτο και ίσως το τελειότερο ιστορικό παράδειγμα στρατιωτικής εξαπάτησης, που υλοποιήθηκε πολλά χρόνια πριν την σχηματοποίηση των σύγχρονων πληροφοριακών επιχειρήσεων. Ωστόσο, παρά το γεγονός ότι παρόμοιες τακτικές χρησιμοποιήθηκαν διαχρονικά από πολλούς στρατούς από την αρχαιότητα μέχρι και τις μέρες μας, οι πληροφοριακές επιχειρήσεις αποτελούν έναν νεολογισμό που έχει εισαχθεί στην στρατιωτική ορολογία από τα μέσα περίπου της δεκαετίας του 90 και αποτελούν ουσιαστικά την εξέλιξη του **<<πληροφοριακού πολέμου>>** ή **<<του πολέμου διοίκησης και ελέγχου>> (C2W),** ο οποίος βρήκε πεδίο εφαρμογής στον πρώτο πόλεμο του Κόλπου, στο Ιράκ. Σε αυτό το χρονικό διάστημα υπήρξε μεγάλη ανησυχία και αβεβαιότητα σχετικά με την επίδραση των νέων τεχνολογιών σε μία σύγκρουση. Τις συνέπειες του πληροφοριακού πολέμου, μπορούμε μερικώς ίσως να τις κατανοήσουμε, αν αναλογιστούμε την επίδραση που είχε στο πεδίο της μάχης ο κεραυνοβόλος πόλεμος, το λεγόμενο <<blitzkrieg>> που εφάρμοσαν οι Γερμανικές δυνάμεις κατά τη διάρκεια του Β΄ Παγκοσμίου Πολέμου και του οποίου οι επιπτώσεις φάνηκαν μετά τις τραγικές αποτυχίες των συμμάχων, κατά τα πρώτα στάδια της σύγκρουσης. Οι σύγχρονες επιστημονικές εφαρμογές όπως το διαδίκτυο, οι δορυφορικές επικοινωνίες και η τηλεόραση, αποτελούν εκτός από τα μέσα ενημέρωσης του κοινού και τα κανάλια ροής στρατιωτικών πληροφοριών και επομένως μία πιθανή επίθεση σε αυτά τα συστήματα, θα νέκρωνε ή θα παρεμπόδιζε τη λειτουργία τους και θα είχε ως αποτέλεσμα τη διακοπή της επικοινωνίας με ό,τι αυτό συνεπάγεται για την ορθή και έγκαιρη λήψη αποφάσεων από τον εκάστοτε διοικητή στο πεδίο της μάχης. Ένα επικοινωνιακό Περλ Χάρμπορ, που θα παρέλυε τις δυνατότητες λήψης και εκπομπής μηνυμάτων και θα επέτρεπε αντίστοιχα την εχθρική πληροφοριακή υπεροχή, θα είχε καταστρεπτικές συνέπειες, πολύ πιο άμεσες ίσως από αυτές του κεραυνοβόλου πολέμου που προαναφέρθηκε. Στο πλαίσιο αυτό, νέες επιστημονικές ανακαλύψεις τις δύο τελευταίες δεκαετίες έκαναν πολύ πιο προσιτή την ιδέα επίθεσης στα πληροφοριακά συστήματα του αντιπάλου και ευνόησαν εξίσου την δυνατότητα παρεμβολής στο σύστημα διοίκησης και ελέγχου. Εισήχθησαν έννοιες όπως ο κυβερνοπόλεμος και ο δικτυοκεντρικός πόλεμος για να περιγράψουν ανεπιθύμητες ενέργειες που στοχεύουν στο να προκαλέσουν δυσλειτουργίες σε υπολογιστικά συστήματα και δίκτυα τόσο σε περίοδο ειρήνης όσο και επιχειρήσεων ή πολέμου χαμηλής εντάσεως. Έτσι, αν και οι βασικές ικανότητες που συνθέτουν τις πληροφοριακές επιχειρήσεις είναι ιστορικά πολύ προγενέστερες του πληροφοριακού πολέμου, η βασική καινοτομία είναι η αναγνώριση ότι ζούμε πλέον σε μία εποχή όπου τα συστήματα διακίνησης πληροφοριών (φίλια ή εχθρικά) είναι ευάλωτα σε προσβολές και γι' αυτό το λόγο απαιτείται μία **ενοποιημένη και συνδυασμένη προσπάθεια που θα αφορά τόσο τα δεδομένα όσο και τα μέσα που τα διακινούν.** Πριν όμως εξετάσουμε αυτές τις διαδικασίες και το πως σχηματοποιήθηκαν στο πέρασμα του χρόνου,

[3] Sun Tzu, The Art Of War (Oxford University Press, 1963). Pages 66, 84.

κρίνεται χρήσιμο και σκόπιμο να γίνει μία μικρή ιστορική αναδρομή και επεξήγηση κάθε μίας από τις θεμελιώδεις ικανότητες που συνθέτουν το μωσαϊκό των πληροφοριακών επιχειρήσεων.

## Ψυχολογικές Επιχειρήσεις και η Ιστορία του Ψυχολογικού Πολέμου.(PSYOP)

Ενώ η ιδέα εκτέλεσης ασύμμετρων επιχειρήσεων με ψυχολογικό αντίκτυπο ανάγεται στην αρχαιότητα, ο όρος ψυχολογικές επιχειρήσεις πρωτοεμφανίστηκε μόλις το 1945 και επικράτησε τελικά τη δεκαετία του 60.[4] Κατά τη διάρκεια του Β΄ ΠΠ ο τρόπος με τον οποίο χρησιμοποιήθηκε ο ψυχολογικός πόλεμος από τους Αμερικάνους αποτέλεσε στην ουσία έναν ευφημισμό για τις εκστρατείες προπαγάνδας που οργάνωσαν όλο αυτό το διάστημα. Οι εκστρατείες αυτές κάλυπταν ένα ευρύ φάσμα δραστηριοτήτων επιρροής και παραπληροφόρησης του αντιπάλου, ασκώντας στην κυριολεξία πολλές φορές <<μαύρη και γκρίζα προπαγάνδα>> καθώς δε διαφαινόταν η πραγματική πηγή προέλευσης του προπαγανδιστικού υλικού ή αποδιδόταν σε πηγή διαφορετική από την πραγματική. Πολλές από τις τεχνικές που χρησιμοποιήθηκαν κατά το Β΄ ΠΠ ήταν παρόμοιες με αυτές που εφαρμόζονται ακόμη και σήμερα, όπως π.χ. η ρίψη φυλλαδίων, και η ραδιοφωνική μετάδοση εκπομπών. Σε αντίθεση όμως με τον σύγχρονο ψυχολογικό πόλεμο, τέτοιου είδους ενέργειες δεν ήταν αποκλειστική αρμοδιότητα του εκάστοτε υπουργείου εθνικής άμυνας. Στην Αμερική π.χ. συστάθηκαν δύο οντότητες με σκοπό τη διενέργεια ΨΕΠ, καμία από τις οποίες δεν είχε στρατιωτική υπαγωγή. : Το γραφείο στρατηγικών υπηρεσιών (Office of Strategic Services OSS) που ασχολούνταν καθαρά με τη μαύρη προπαγάνδα και το γραφείο των πληροφοριών πολέμου (Office of War Information OWI) που είχε σαν αποκλειστικό τομέα ευθύνης τη λευκή.[5]

Ο ψυχολογικός πόλεμος είχε επίσης ευρεία εφαρμογή και κατά τη διάρκεια της στρατιωτικής αντιπαράθεσης στην Κορέα και στο Βιετνάμ. Η αεροπορική ρίψη φυλλαδίων που ενθάρρυναν την παράδοση του εχθρού και η μετάδοση μηνυμάτων από ραδιόφωνα, μεγάφωνα και αφίσες, ήταν μερικές από τις κύριες μεθόδους που χρησιμοποιήθηκαν στην προσπάθεια να επηρεαστεί ο αντίπαλος. Ωστόσο, λίγες αποδείξεις υπάρχουν ότι οι επιχειρήσεις αυτές ήταν ιδιαίτερα αποτελεσματικές.[6] Ο διαχωρισμός της επίδρασης μίας ψυχολογικής επιχείρησης από την επίδραση άλλων παραγόντων που μπορούν να επηρεάσουν την ανθρώπινη συμπεριφορά στο πεδίο της μάχης, παραμένει μία πρόκληση για τον σύγχρονο ψυχολογικό πόλεμο και αναλύεται διεξοδικότερα στα επόμενα κεφάλαια.

## Η Ιστορία της Στρατιωτικής Εξαπάτησης (Military Deception MILDEC).

Η παραπλάνηση του αντιπάλου στον πόλεμο είναι τόσο παλιά όσο και η ιστορία του ανθρωπίνου είδους. Αναφορές για την στρατιωτική εξαπάτηση ανευρίσκονται σε αρκετά κείμενα αρχαίων πολιτισμών. Για παράδειγμα, στο κλασσικό έργο «η Τέχνη του Πολέμου», ο κινέζος στρατηγός Σουν Τζου φέρεται να ισχυρίζεται: << Στον πόλεμο εφαρμόστε την προσποίηση και θα

---

[4] William E. Daugherty. "An account of the Origin of the Terms PsyWar and PsyOp" PSYWAR ORG. (March 29,2007)

[5] Philip M. Taylor, ''Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day''. (Manchester University Press, 2003)

[6] Stephen T. Hosmer, Psychological Effects of U.S. Air Operations in Four Wars 1941-1991: Lessons from U.S. Commanders MR-576-AF (Santa Monica, CA: Rand Corporation, 1996).

πετύχετε>>.[7] Στην σύγχρονη εποχή, μία από τις πιο διάσημες και ταυτόχρονα καταπληκτικές ενέργειες παραπλάνησης του εχθρού, είναι η επιχείρηση που οργάνωσαν οι δυτικοί σύμμαχοι το 1944, με σκοπό να πείσουν τους Γερμανούς ότι επρόκειτο να αποβιβαστούν πλησίον της πόλης *Pas-de-Calais*. (Operation Fortitude)[8]. Για να πετύχουν τον σκοπό τους χρησιμοποίησαν μία πληθώρα μέσων, όπως ομοιώματα φουσκωτών αρμάτων, ανδρείκελα πυροβόλων και οχημάτων. Ταυτόχρονα έδωσαν την ψευδή εντύπωση στους Γερμανούς ότι επρόκειτο να ενεργήσει μία τεράστια στρατιά που αριθμούσε 2 σώματα στρατού και 6 μεραρχίες. Αυτό το πέτυχαν μέσω της δημιουργίας μονάδων ειδικού σκοπού που χαρακτηρίζονταν από ασύμμετρη για το πραγματικό τους μέγεθος ηλεκτρονική και ραδιοφωνική εκπομπή καθώς επίσης και με την αυξημένη κινητικότητα μονάδων υποστηρίξεως. (στην πραγματικότητα επρόκειτο μόνο για 2 ταξιαρχίες που εξέπεμπαν σήματα σε μία αναλογία 20:1 με βάση την πραγματική τους δύναμη). Όλα αυτά, σε συνδυασμό με την εσκεμμένη διαρροή πλαστών πληροφοριών σε γερμανούς πράκτορες, είχαν εξαιρετικά αποτελέσματα. Από την ιστορία πλέον γνωρίζουμε ότι οι Γερμανοί όχι μόνο δεν επάνδρωσαν επαρκώς την πραγματική ακτή αποβάσεως, αλλά και όταν ακόμη εκδηλώθηκε η ενέργεια των συμμάχων, καθυστέρησαν να μετακινήσουν τις δυνάμεις τους, πιστεύοντας ότι επρόκειτο για μία παραπλανητική επίθεση. Τέλος, μία εξαιρετική τεχνική παραπλάνησης χρησιμοποιήθηκε από τους Αμερικανούς στο Βιετνάμ, με σκοπό να διασωθούν οι πιλότοι που θα έπεφταν σε εχθρικό έδαφος, εάν και εφόσον καταρριπτόταν το αεροσκάφος τους. Κομμάτια πάγου που περιείχαν αίμα ζώου ρίπτονταν από αεροσκάφη της Αμερικάνικης αεροπορίας τα οποία έλιωναν και παραπλανούσαν τους αντιπάλους σχετικά με το πραγματικό σημείο πτώσης και τον τραυματισμό του πιλότου.[9]

**Επιχειρήσεις Στρατιωτικής Ασφάλειας. (OPSEC)**

Ενώ ο όρος στρατιωτική ασφάλεια εμφανίζεται επίσημα στην στρατιωτική επιστήμη μόλις το 1988, (ο πρώτος που χρησιμοποίησε τον όρο ήταν ο πρόεδρος Reagan) γνωρίζουμε ότι η προσπάθεια περιορισμού συλλογής πληροφοριών από τον εχθρό, μέσω παρατήρησης ή άλλων μεθόδων, είναι πολύ παλαιότερη. Η απόβαση π.χ. που οργάνωσαν οι σύμμαχοι στη Νορμανδία (Operation Bodyguard), βασίστηκε σε μεγάλο βαθμό στην προστασία των πηγών και οργάνων απ' όπου θα μπορούσαν να διαρρεύσουν πληροφορίες κρίσιμες στον εχθρό που θα έθεταν σε κίνδυνο την όλη επιχείρηση. Για αυτόν ακριβώς το λόγο, η πραγματική ακτή της απόβασης κρατήθηκε μυστική από τους ίδιους τους συμμετέχοντες, ενώ όταν πλησίασε η ημερομηνία που θα ξεκινούσε η επιχείρηση, δόθηκε διαταγή παραμονής των μονάδων που επρόκειτο να εμπλακούν στα στρατόπεδα τους, ώστε να ελαχιστοποιηθεί ο κίνδυνος οποιασδήποτε διαρροής.

Η στρατιωτική ασφάλεια συνδέεται στενά με την στρατιωτική παραπλάνηση διότι πολλές φορές η διαχωριστική γραμμή μεταξύ της απόκρυψης πληροφοριών ή της σκόπιμης παραπληροφόρησης του εχθρού είναι πολύ λεπτή. Στις μέρες μας, όπου τα

[7] Sun Tzu, the Art of War (Oxford University Press, 1963). Pages 47

[8] James P. Pinkerton**,** "Covering the News with Deception'' Long Island Newsday (December 16, 2004).

[9] Philip M. Taylor, "Munitions of the Mind", 267.

κανάλια της πληροφορίας έχουν πολλαπλασιαστεί αριθμητικά και αναβαθμιστεί ποιοτικά (διαδίκτυο, κινητά τηλέφωνα, e-mail), παραμένει ένας μεγάλος και κρίσιμος παράγοντας στη διεξαγωγή επιχειρήσεων.

**Ο Ηλεκτρονικός Πόλεμος και η Ιστορία του.**

Ο ηλεκτρονικός πόλεμος αποτελεί δημιούργημα του Β΄ Παγκοσμίου Πολέμου όπου ουσιαστικά εγκαινιάστηκε η χρήση του ηλεκτρομαγνητικού φάσματος για καθαρά στρατιωτικούς σκοπούς. Οι πρωτόλιες εφαρμογές του αφορούσαν στη λειτουργία ραντάρ για εντοπισμό αεροσκαφών και στις προσπάθειες τόσο των Γερμανών όσο και των συμμάχων να «τυφλώσουν» και να παρεμβάλλουν τα συστήματα ηλεκτρονικού εντοπισμού των αντιπάλων τους αντίστοιχα. Στον Ειρηνικό Ωκεανό ο ηλεκτρονικός πόλεμος είχε πρωτεύοντα ρόλο στις ναυμαχίες που έλαβαν χώρα μεταξύ του ιαπωνικού και του αμερικάνικου ναυτικού. Ο αμερικάνικος στόλος είχε τη δυνατότητα να εντοπίσει τη θέση των ιαπωνικών πλοίων και να αναγνωρίσει την ακριβή ταυτότητά τους λόγω του μοναδικού ηλεκτρονικού σήματος που εξέπεμπαν. [10]

Κατά τη διάρκεια του Ψυχρού Πολέμου χρησιμοποιήθηκαν κατά κόρον εφαρμογές ηλεκτρονικού πολέμου που είχαν ως στόχο να παρεμβάλλουν ή να παραπλανήσουν τα συστήματα του αντιπάλου. Τυπικά, ένα βαρύ βομβαρδιστικό μακράς ακτίνας δράσης της δεκαετίας του 60 έφερε μαζί του συσκευές ικανές να παρεμβάλλουν τα ραντάρ άλλων αεροσκαφών και τους επίγειους σταθμούς ελέγχου του εχθρού.[11] Ο ηλεκτρονικός πόλεμος έφτασε στο απόγειο του κατά τη διάρκεια της σύγκρουσης στο Βιετνάμ όπου χρησιμοποιήθηκε ποικιλία ηλεκτρονικών αντιμέτρων. Για πρώτη φορά εξειδικευμένα αεροσκάφη ανέλαβαν ως αποστολή την καταστολή της εχθρικής αεράμυνας και πέτυχαν την καταστροφή των σταθμών ελέγχου μέσω ειδικών τεχνικών. Οι σημερινές βελτιώσεις στον συγκεκριμένο τομέα επιτρέπουν σε ένα βλήμα να καταστρέψει το ραντάρ εντοπισμού ακόμη και μετά την παύση της λειτουργίας του, ακολουθώντας την τελευταία γνωστή πορεία προς τον στόχο.

**Δικτυοκεντρικές Επιχειρήσεις μέσω Η/Υ.**

Οι δικτυοκεντρικές επιχειρήσεις αποτελούν στην ουσία την συγχώνευση δύο τεχνικών δυνατοτήτων που έχουν να κάνουν τόσο με την προστασία των φίλιων Η/Υ από αντίπαλες προσβολές όσο και με τις δυνατότητες επίθεσης σε ξένα υπολογιστικά συστήματα, διαμέσου ασύρματων ή ενσύρματων δικτύων. Οι περισσότερες λεπτομέρειες σχετικά με αυτές τις τεχνικές παραμένουν στις μέρες μας διαβαθμισμένες με αποτέλεσμα ελάχιστες πληροφορίες να έχουν διαρρεύσει στη δημόσια σφαίρα για την επιχειρησιακή τους χρήση. Σχετικές εκθέσεις που ήρθαν στο φως της δημοσιότητας αναφέρουν ότι για πρώτη φορά αμερικάνικοι υπολογιστές κυβερνητικών υπηρεσιών δέχθηκαν τέτοιου είδους προσβολές στα τέλη της δεκαετίας του 90, χωρίς όμως να αποδεσμεύονται και πληροφορίες σχετικά με την τρωτότητα των Η/Υ και τις επιπτώσεις που είχαν πάνω στα δίκτυα οι επιθέσεις. Είναι πάντως γνωστό πως κυβερνοεπίθεση που διενεργήθηκε από άγνωστους χάκερς με την κωδική ονομασία << Ο Λαβύρινθος του Σεληνόφωτος>> (Moonlight Maze) είχε ως αποτέλεσμα ένα σημαντικό ποσό τεχνικών δεδομένων γύρω από ερευνητικά αμυντικά προγράμματα να καταλήξει σε άγνωστα μέρη στη

[10] United States Air Force, Electronic Warfare, Air Force Doctrine Document, 2-5.1 (November 5, 2002).

[11] Alfred Price, Instruments of Darkness: The History of Electronic Warfare (New York 1978), 251

Ρωσία.[12] Στις μέρες μας, η ασφάλεια του κυβερνοχώρου παραμένει ένα κρίσιμο ζήτημα σε παγκόσμια κλίμακα.

# ΚΕΦΑΛΑΙΟ 2$^{Ο}$
# ΣΥΓΧΡΟΝΕΣ ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

## 2.1 ΟΡΙΣΜΟΣ ΤΩΝ ΣΥΓΧΡΟΝΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ.

Κατά τα τελευταία δέκα χρόνια, οι Ηνωμένες Πολιτείες, η Ρωσία και η Κίνα έχουν αναπτύξει τις δικές τους έννοιες του **πολέμου πληροφοριών** (IW), των **πληροφοριακών επιχειρήσεων** (IO) και της **πληροφοριακής υπεροχής** (IS). Είναι σχετικά εύκολο να εξακριβωθεί η προσέγγιση των ΗΠΑ σε σχέση με τις έννοιες αυτές, επειδή αποτελούν τη μοναδική χώρα όπου δημοσιεύεται χωρίς κάποια διαβάθμιση ασφαλείας μεγάλο μέρος της παραπάνω θεωρίας υπό τη μορφή Διακλαδικών Εκδόσεων (Joint Publications) ή Εγχειριδίων Εκστρατείας (Field Manuals). Αντίθετα, ούτε η Ρωσία ούτε η Κίνα δημοσιεύουν τέτοια έγγραφα και ως εκ τούτου η περιγραφή των πληροφοριακών επιχειρήσεων θα βασιστεί αποκλειστικά στην ανάγνωση των δυτικών επίσημων ακαδημαϊκών και στρατιωτικών απόψεων.

Σύμφωνα λοιπόν με τη διακλαδική έκδοση 1-02 (JP 1-02) που αποτελεί στο λεξικό στρατιωτικής ορολογίας του Αμερικάνικου υπουργείου Εθνικής Άμυνας, οι πληροφοριακές επιχειρήσεις ορίζονται ως **οι βασικές ικανότητες του ηλεκτρονικού πολέμου (EW), των δικτυοκεντρικών επιχειρήσεων μέσω υπολογιστών (CNO), των ψυχολογικών επιχειρήσεων (PSYOP), της στρατιωτικής εξαπάτησης (MILDEC) και της ασφάλειας των επιχειρήσεων (OPSEC), σε συνεργασία με άλλες σχετιζόμενες και εξειδικευμένες υποστηρικτικές δυνατότητες που στοχεύουν στο να επηρεάσουν και να υπονομεύσουν τις αντίπαλες διαδικασίες λήψης αποφάσεων και παράλληλα να προστατεύσουν τις αντίστοιχες φίλιες.[13] Οι δυνατότητες που σχετίζονται με τις πληροφοριακές επιχειρήσεις αναφέρονται σε τεχνικές και εργαλεία που αφορούν την ενημέρωση και την επιρροή και περιλαμβάνουν τις δημόσιες**

[12] Leigh Armistead, "Information Operations: Warfare and the Hard Reality of Soft Power" (Washington D.C. 2004), 74

[13] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, as amended through March 22, 2007 (Washington, DC, April 12, 2001)

**σχέσεις (public affairs), την πολιτικοστρατιωτική συνεργασία (civil-military operations) και την αμυντική υποστήριξη στη διπλωματία κοινού (defense support to public diplomacy).[14] Τέλος, οι υποστηρικτικές δυνατότητες των πληροφοριακών επιχειρήσεων περιλαμβάνουν την φυσική ασφάλεια και επίθεση (physical security, physical attack), την καταγραφή γεγονότων στο πεδίο της μάχης μέσω κάμερας (combat camera), την ασφάλεια πληροφοριών (information assurance) και την αντικατασκοπεία (counterintelligence). Επομένως, οι πληροφοριακές επιχειρήσεις δε χαρακτηρίζονται από κυριότητα τεχνικών και δυνατοτήτων αλλά από την ολοκληρωμένη εφαρμογή, συνεργασία και συντονισμό προυπαρχουσών δράστηριοτήτων, η οποία κρίνεται ως απαραίτητη για να επιτευχθούν πληροφοριακοί αντικειμενικοί σκοποί.**

## 2.2 ΤΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ

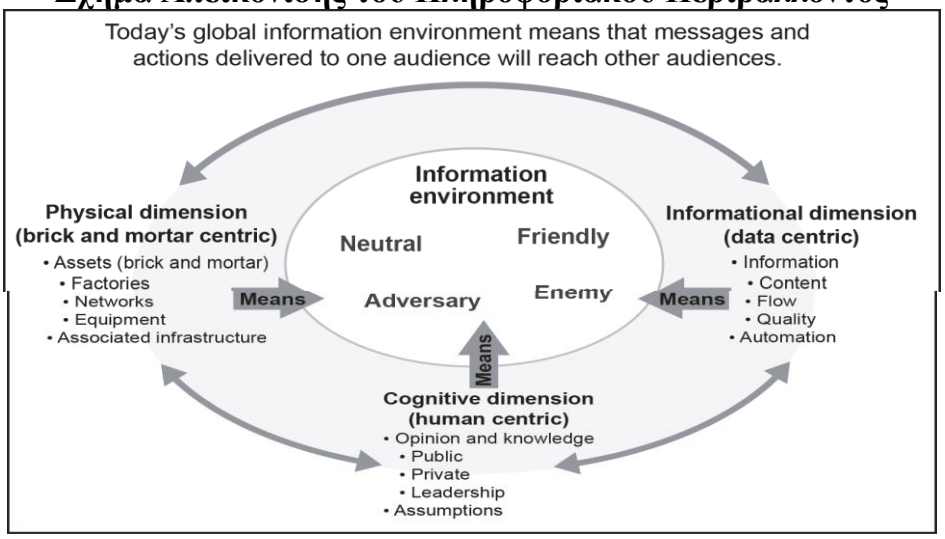
Πριν γίνει οποιαδήποτε αναφορά στο Νατοϊκό Δόγμα για τις Πληροφοριακές επιχειρήσεις, κρίνεται σκόπιμο να επισημανθεί, ότι σε όλα σχεδόν τα επίσημα έγγραφα του Αμερικάνικου Πενταγώνου, είτε πρόκειται για διακλαδικές εκδόσεις είτε για απλά εγχειρίδια πεδίου μάχης, γίνεται ιδιαίτερη μνεία στην περιγραφή του πληροφοριακού περιβάλλοντος μέσα στο οποίο εξελίσσονται οι συγκεκριμένες δράσεις, καθώς και στη γενικότερη αξία της πληροφορίας που χρησιμεύει ως πολλαπλασιαστής ισχύος όταν χρησιμοποιηθεί αποτελεσματικά. ***Σύμφωνα με τον διακλαδικό κανονισμό 3-13, (JP 3-13) το πληροφοριακό περιβάλλον ορίζεται σαν το άθροισμα ατόμων, οργανώσεων, και συστημάτων που συλλέγουν, επεξεργάζονται και διαχέουν πληροφορίες και λειτουργεί σε τρεις αλληλένδετες διαστάσεις, οι οποίες συνεχώς αλληλεπιδρούν με τα άτομα, τις οργανώσεις, και τα συστήματα. Οι διαστάσεις αυτές είναι γνωστές ως φυσική, ενημερωτική και γνωστική***. **Η φυσική διάσταση αποτελείται από τα συστήματα διοίκησης και ελέγχου, τους βασικούς φορείς λήψης αποφάσεων και τις υποστηρικτικές υποδομές που επιτρέπουν σε άτομα και οργανισμούς να παράξουν συγκεκριμένα αποτελέσματα. Η ενημερωτική/πληροφοριακή διάσταση καθορίζει το πού και το πώς οι πληροφορίες συλλέγονται, υποβάλλονται σε επεξεργασία, αποθηκεύονται, διαδίδονται και προστατεύονται. Η γνωστική τέλος διάσταση περιλαμβάνει το νου εκείνων που μεταδίδουν, λαμβάνουν και απαντούν σε μία πληροφορία.**[15]

Με την έλευση του Διαδικτύου και την ευρεία διαθεσιμότητα των ασύρματων επικοινωνιών και της τεχνολογίας των πληροφοριών, το περιβάλλον αυτό έχει γίνει ακόμη πιο σημαντικός παράγοντας για το στρατιωτικό σχεδιασμό και τις επιχειρήσεις από ό, τι τα προηγούμενα χρόνια. Η αυξανόμενη διαφάνεια και η αλληλεξάρτηση των δικτύων, συσκευών και δεδομένων, καθιστούν δυνατή την ταχεία, αποτελεσματική και συχνά απεριόριστη κίνηση των πληροφοριών σε όλο τον κόσμο και τα στρατιωτικά συστήματα διοίκησης και ελέγχου εξαρτώνται όλο και περισσότερο από αυτό το φαινόμενο. Επομένως, οι δραστηριότητες που συμβαίνουν μέσα, μέσω ή με τη βοήθεια του περιβάλλοντος των πληροφοριών, έχουν συνέπειες και στο επιχειρησιακό περιβάλλον και μπορούν να επηρεάσουν τις στρατιωτικές δράσεις και τα

[14] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington, DC, February 13, 2006)
[15] Ibid., I-1.

αποτελέσματα τους. Αφού μάλιστα οι πληροφοριακές επιχειρήσεις διεξάγονται πέρα από τα όρια του φυσικού χώρου, διευρύνουν τα όρια και τη δυναμική των πραγμάτων που μπορεί να επηρεάσει ένας διοικητής. Οι πεζοναύτες για παράδειγμα πιστεύουν ότι βελτιώνουν τις δράσεις τους επηρεάζοντας στόχους από απόσταση ασφαλείας, μειώνοντας έτσι τη φυσική τους παρουσία στο πεδίο της μάχης.[16] Παρόμοια, όταν ένας αντίπαλος κάνει χρήση των πλεονεκτημάτων των πληροφοριακών επιχειρήσεων μπορεί να υπερβεί δυσκολίες που επιβάλλονται από γεωγραφικούς περιορισμούς και πολιτικά σύνορα. Συνεπώς, κάθε κράτος θα πρέπει να διαθέτει την ικανότητα να μεταδώσει, να λάβει, να αποθηκεύσει και να επεξεργαστεί με ασφάλεια πληροφορίες, σε σχεδόν πραγματικό χρόνο.

**Σχήμα Απεικόνισης του Πληροφοριακού Περιβάλλοντος**




## 2.3 ΤΟ ΔΟΓΜΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Σύμφωνα με τη Νατοϊκή Στρατιωτική Σκέψη, το δόγμα αντιπροσωπεύει τις θεμελιώδεις αρχές με τις οποίες οι στρατιωτικές δυνάμεις κατευθύνουν τις δράσεις τους στην υποστήριξη των στόχων τους. Ο διακλαδικός κανονισμός 3-13***(JP 3-13)*** περιγράφει το δόγμα των αμερικανικών πληροφοριακών επιχειρήσεων ως εξής: *«Σκοπός του δόγματος είναι να παράσχει στους διοικητές διακλαδικών δυνάμεων και στο επιτελείο τους την καθοδήγηση για την προετοιμασία, τον σχεδιασμό, την εκτέλεση πληροφοριακών επιχειρήσεων σε υποστήριξη πάντα των διακλαδικών ενεργειών. Για να εφαρμοστούν οι πληροφοριακές επιχειρήσεις σε όλο το φάσμα των στρατιωτικών επιχειρήσεων, η διακλαδική διοίκηση ενοποιεί όλες τις στρατιωτικές ενέργειες, δυνάμεις και δυνατότητες στις τέσσερεις διαστάσεις (του αέρα, της γης, της θάλασσας, και του διαστήματος), προκειμένου να δημιουργήσει ή / και να διατηρήσει επιθυμητά και μετρήσιμα αποτελέσματα σε αντίπαλους ηγέτες, δυνάμεις (κανονικές και μη), πληροφορίες, συστήματα πληροφοριών, και άλλων ακροατήρια προστατεύοντας και υπερασπίζοντας ταυτόχρονα τις δικές της δράσεις,*

[16] Edward Waltz, *Information Warfare: Principles and Operation*. (Boston: Artech House, 1998), p.27.

*δυνάμεις, πληροφορίες, και πληροφοριακά συστήματα.»*[17] Επίσης το δόγμα δεν παραλείπει να αναφερθεί και στο γενικότερο πλαίσιο κάτω από το οποίο διεξάγονται και εκτελούνται πληροφοριακές επιχειρήσεις. Τόσο στο διακλαδικό κανονισμό, όσο και στο εγχειρίδιο εκστρατείας του στρατού, αναφέρεται ρητά, ότι *οι πληροφοριακές επιχειρήσεις πρέπει να χρησιμοποιούνται για να αποτρέψουν μελλοντικούς ή τωρινούς αντιπάλους από την ανάληψη δράσεων που θα απειλούν τα εθνικά συμφέροντα των ΗΠΑ*[18]. Με βάση το παραπάνω κείμενο προκύπτουν δύο βασικά συμπεράσματα: α) Στην στρατιωτική φιλοσοφία των χωρών του ΝΑΤΟ οι πληροφοριακές επιχειρήσεις δε λειτουργούν αυτόνομα εξυπηρετώντας στενά στρατιωτικούς σκοπούς σε ένα τακτικό πεδίο μάχης, αλλά επεκτείνονται και σε άλλα ακροατήρια. Στο πνεύμα αυτό, οι στόχοι τους μπορεί να είναι στρατηγικοί, επιχειρησιακοί ή τακτικοί ανάλογα με την περίσταση. Γενικά, εντάσσονται στο πλαίσιο διεξαγωγής ευρύτερων κυβερνητικών πληροφοριακών δραστηριοτήτων και χρησιμοποιούνται για να παράξουν αποτελέσματα σε όλα τα επίπεδα του πολέμου και σε όλο το φάσμα των στρατιωτικών επιχειρήσεων. β) Στον πυρήνα της φιλοσοφίας των πληροφοριακών επιχειρήσεων βρίσκεται είτε ο επηρεασμός της ροής των πληροφοριών, είτε η προσβολή των πληροφοριακών συστημάτων του αντιπάλου και η δημιουργία προϋποθέσεων για την προστασία των αντίστοιχων φίλιων. Σε όποιο δηλαδή από τα τρία επίπεδα και αν διεξάγονται, συναρτούν σχεδόν πάντα την ύπαρξή τους, με την παρουσία κάποιου ανταγωνιστή. Μία τέτοια λογική αποτελεί κληροδότημα του πληροφοριακού πολέμου που αποτελεί τον άμεσο πρόγονο των πληροφοριακών επιχειρήσεων. Ωστόσο, η τάση που παρουσιάζεται τα τελευταία χρόνια οι ένοπλες δυνάμεις διαφόρων χωρών να εμπλουτίζουν το πλαίσιο δράσης τους, αναλαμβάνοντας καινούργιες αποστολές που δεν έχουν αμιγώς στρατιωτικό χαραχτήρα (π.χ. ανθρωπιστική βοήθεια), μεταβάλλει σταδιακά και την παγιωμένη αντίληψη για το παραδοσιακό ρόλο των πληροφοριακών επιχειρήσεων και είναι ένα ζήτημα που θα αναλυθεί πιο διεξοδικά παρακάτω.

## 2.4 ΔΥΝΑΤΟΤΗΤΕΣ ΚΑΙ ΑΠΟΣΤΟΛΕΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Βασική αποστολή των πληροφοριακών επιχειρήσεων, σύμφωνα με το διακλαδικό κανονισμό 3-13 του Αμερικάνικου Πενταγώνου, είναι η **εξασφάλιση πληροφοριακής υπεροχής**[19] **η οποία ορίζεται ως** *«το επιχειρησιακό πλεονέκτημα που πηγάζει από την ικανότητα της συλλογής, επεξεργασίας και διασποράς μη διακοπτόμενης ροής πληροφοριών και*

[17] Joint Doctrine for Information Operations, Joint Publication 3-13 , I-1.
[18] Ibid, I-8.
[19] Ibid., I-1.

*ταυτόχρονη εκμετάλλευση ή απαγόρευση της εχθρικής ικανότητας να υλοποιήσει το ίδιο».*[20] Οι όροι και οι συνθήκες που εξασφαλίζουν την πληροφοριακή υπεροχή δημιουργούνται από τον συγχρονισμό και το συντονισμό των **πέντε βασικών δυνατοτήτων των πληροφοριακών επιχειρήσεων**, δηλαδή του ηλεκτρονικού πολέμου (EW), των δικτυοκεντρικών επιχειρήσεων μέσω υπολογιστών (CNO), των ψυχολογικών επιχειρήσεων (PSYOP), της στρατιωτικής εξαπάτησης (MILDEC) και της ασφάλειας των επιχειρήσεων. Από αυτές τις δυνατότητες οι δύο πρώτες επικεντρώνονται στα πληροφοριακά συστήματα, ενώ οι τρεις επόμενες αφορούν τις πληροφορίες. Οι πληροφορίες έχουν σχέση με το περιεχόμενο: τα ακατέργαστα ή επεξεργασμένα στοιχεία, τα δεδομένα ή τις ιδέες, ανεξάρτητα από το πού είναι αποθηκευμένα, ή τον τρόπο που ανακοινώνονται. Τα συστήματα πληροφοριών είναι στην ουσία τα μέσα με τα οποία γίνεται ο χειρισμός των πληροφοριών: το hardware, οι άνθρωποι, οι οργανώσεις, τα μέσα, κ.λπ. Ο κύριος λόγος συγχρονισμού των παραπάνω δυνατοτήτων είναι *ο επηρεασμός των αποφάσεων και των διαδικασιών λήψης αποφάσεων του αντιπάλου και η υπεράσπιση αντίστοιχα των φίλιων διαδικασιών λήψης αποφάσεων.*[21] Στη βάση αυτής της λογικής οι πληροφοριακές επιχειρήσεις χωρίζονται σε: α) **Αμυντικές Πληροφοριακές Επιχειρήσεις** οι οποίες αποσκοπούν στην προστασία των φίλιων πληροφοριών και πληροφοριακών συστημάτων, από αντίστοιχες επιθετικές ενέργειες των αντιπάλων και β) **Επιθετικές Πληροφοριακές Επιχειρήσεις** που αποσκοπούν στην προσβολή πληροφοριών και πληροφοριακών συστημάτων των αντιπάλων. Ο κανονισμός παραθέτει 11 μεθόδους με τις οποίες μπορούν να συνδυαστούν και να εφαρμοστούν οι δυνατότητες των πληροφοριακών επιχειρήσεων, λαμβάνοντας είτε αμυντική είτε επιθετική μορφή. Σε αυτές συγκαταλέγονται η καταστροφή και η υποβάθμιση των πληροφοριακών συστημάτων του αντιπάλου, η εξαπάτηση που επιδιώκει να παραπλανήσει τους αντίπαλους φορείς λήψης αποφάσεων , η επιρροή με στόχο τη δημιουργία ευνοϊκών στάσεων για τα συμφέροντα των ΗΠΑ κα.

Όλες οι παραπάνω ενέργειες συνδέονται βέβαια με αμιγώς στρατιωτικές δράσεις και αποτελούν προτεραιότητα για κάθε στρατιωτικό οργανισμό που εκτελεί συμβατικές επιχειρήσεις. Τι συμβαίνει όμως στις περιπτώσεις εκείνες όπου οι ένοπλες δυνάμεις μίας χώρας εμπλέκονται σε αποστολές που δεν ανήκουν στο καθαρά στρατιωτικό φάσμα και αφορούν μη πολεμικές ενέργειες; Είναι άραγε εφικτό να υπάρξει πεδίο εφαρμογής για τις πληροφοριακές επιχειρήσεις χωρίς να υφίσταται αντίπαλος;

Όσον αφορά το κομμάτι εκείνο των πληροφοριακών επιχειρήσεων που στοχεύει τα συστήματα πληροφοριών του αντιπάλου, δηλαδή τον ηλεκτρονικό πόλεμο και τον κυβερνοπόλεμο, η απάντηση σίγουρα είναι αρνητική. Τέτοιου είδες ενέργειες αποκτούν νόημα μόνο με την ύπαρξη ενός ξεκάθαρου ανταγωνιστή. Αντίθετα, οι ικανότητες εκείνες που συνδέονται με το πληροφοριακό περιεχόμενο, είναι εφικτό να συνδυαστούν με επιχειρήσεις σταθεροποίησης και ανοικοδόμησης της ειρήνης, όπου το κύριο διακύβευμα είναι ο επηρεασμός του άμαχου πληθυσμού. Όπως υποστηρίζει ο αμερικάνος ταγματάρχης Joseph Cox στο βιβλίο του «Πληροφοριακές Επιχειρήσεις στο Ιράκ, τι Πήγε Λάθος», «*οι επιχειρήσεις επιρροής είναι εκείνες που σχεδιάζονται για να αλλάξουν την*

[20] Ibid., GL-9.
[21] Ibid. , I-6.

*συμπεριφορά ενός επιλεγμένου ακροατηρίου. Στις συμβατικές επιχειρήσεις η επιρροή κατευθύνεται εναντίον των εχθρικών δυνάμεων. Στις επιχειρήσεις όμως σταθεροποίησης, ο κύριος στόχος είναι ο επηρεασμός ατόμων που δεν έχουν την στρατιωτική ιδιότητα ώστε να συμμορφώνονται με τις οδηγίες της συμμαχίας ή να υποστηρίζουν τον αγώνα εναντίον των ανταρτών.»*[22] Στο επιλεγμένο ακροατήριο επομένως περιλαμβάνονται τόσο εχθρικές δυνάμεις όσο και μη μάχιμο τοπικό στοιχείο. Τόσο στο Ιράκ όσο και στο Αφγανιστάν όπου η επίδραση του παράγοντα του άμαχου πληθυσμού υπήρξε καθοριστική, οι επιχειρήσεις πληροφοριακού περιεχομένου ήταν κατάλληλες για να εφαρμοστούν σε πολιτικούς στόχους.

# ΚΕΦΑΛΑΙΟ 3ο

# ΟΙ ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΣΤΗΝ ΠΡΑΞΗ

Παρά το ότι οι πληροφοριακές επιχειρήσεις αντιμετωπίζονται στο δόγμα των ενόπλων δυνάμεων των ΗΠΑ σαν μία επιχειρησιακή ολότητα με στόχο την εξασφάλιση πληροφοριακής υπεροχής, ωστόσο, δεν παύουν ταυτόχρονα να αποτελούν το σύνολο επιμέρους διακριτών δραστηριοτήτων που χαρακτηρίζονται από ανομοιογένεια, στόχων, αντικειμένου, μεθόδων και τεχνικών. Υπό αυτό το πρίσμα, απαιτείται μία εμβάθυνση στο δόγμα και τον τρόπο λειτουργίας κάθε μίας βασικής ικανότητας ξεχωριστά, ώστε να γίνει κατανοητή η εφαρμογή των πληροφοριακών επιχειρήσεων στην πράξη.

## 3.1 ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΠΕΡΙΕΧΟΜΕΝΟΥ

### Ψυχολογικές Επιχειρήσεις

Οι ψυχολογικές επιχειρήσεις έχουν πρωτεύοντα ρόλο στις σύγχρονες πληροφοριακές επιχειρήσεις. Η αποστολή τους απορρέει από το δόγμα των ψυχολογικών επιχειρήσεων που είναι σαφώς διατυπωμένο τόσο στο διακλαδικό κανονισμό 3-13 όσο και στο εγχειρίδιο εκστρατείας 3-05.30 και συνίσταται στον επηρεασμό της συμπεριφοράς ξένων ακροατηρίων, με απώτερο σκοπό την εξυπηρέτηση των εθνικών συμφερόντων των ΗΠΑ.[23] Επίσης το εγχειρίδιο πεδίου μάχης 3-.05.301 που εστιάζει σε σύγχρονες τακτικές, τεχνικές και διαδικασίες επισημαίνει ότι *ο σκοπός των Ψυχολογικών Επιχειρήσεων είναι να δημιουργήσουν σε φιλικά, ουδέτερα ή εχθρικά κοινά, συναισθήματα και συμπεριφορές που θα υποστηρίζουν την επιτυχία των στρατιωτικών αποστολών και των εθνικών συμφερόντων των ΗΠΑ.*[24] Είναι πολύ βασικό να επισημανθεί ότι ο επηρεασμός της κοινής γνώμης που

[22] Major Joseph L. Cox, "Information Operations in Operations Enduring Freedom in Iraqi Freedom-What Went Wrong?" School of Advanced Military Studies, United States Army Command and General Staff College (AY 05-06) p.67.
[23] Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.30, (Washington D.C., April 2005).
[24] Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.301, (Washington D.C., December 31, 2003), 1-I

περιγράφεται παραπάνω, συνιστά μία διαδικασία που μπορεί να λάβει χώρα τόσο κατά τη διάρκεια της ειρήνης όσο και του πολέμου, μέσω της χρήσης του ραδιοφώνου, του τύπου και άλλων μέσων ενημέρωσης.[25] Επιπλέον, στις αποστολές των ψυχολογικών επιχειρήσεων συγκαταλέγονται τέσσερις ακόμα δράσεις που αφορούν στην παροχή συμβουλών και την υποστήριξη του διοικητή, στη διακίνηση πληροφοριών για ενημέρωση του κοινού, και στην αντιμετώπιση της εχθρικής προπαγάνδας, κατασκοπείας και παραπληροφόρησης.[26]

Σύμφωνα πάντα με το δόγμα των Αμερικανικών Ενόπλων Δυνάμεων, οι ψυχολογικές επιχειρήσεις βρίσκουν πεδίο εφαρμογής στο τακτικό και επιχειρησιακό επίπεδο του πολέμου.[27] Αντίστοιχες ενέργειες στο στρατηγικό επίπεδο αποτελούν αντικείμενο ενασχόλησης της στρατηγικής επικοινωνίας και της διπλωματίας με το κοινό και δεν καθοδηγούνται από το υπουργείο εθνικής άμυνας. Όσον αφορά το επιχειρησιακό επίπεδο, οι ψυχολογικές επιχειρήσεις περιλαμβάνουν προσπάθειες επηρεασμού της κοινής γνώμης που σκοπεύουν στο να αλλάξουν καθημερινές νοοτροπίες, σαν πρελούδιο μίας αλλαγής της γενικής συμπεριφοράς του πληθυσμού. Ο χρονικός ορίζοντας ωρίμανσης τέτοιων δράσεων είναι μακροπρόθεσμος και απαιτείται επίμονη εκπαίδευση και χρόνια ανταλλαγή μηνυμάτων με το επιλεγμένο στόχο-ακροατήριο για να παραχθούν τα επιθυμητά αποτελέσματα. Αντίθετα, στο τακτικό επίπεδο, οι ψυχολογικές επιχειρήσεις βρίσκονται υπό τον έλεγχο ενός διοικητή δυνάμεων ελιγμού, κατευθύνονται εναντίον συγκεκριμένων ακροατηρίων και εκτελούνται στη βάση ενός σχεδιασμού που απαιτεί βραχυπρόθεσμες αλλαγές στην συμπεριφορά του επιλεγμένου κοινού-στόχου, όπως πχ. τη μείωση του ηθικού του αντιπάλου στο πεδίο της μάχης. Στα μέσα που χρησιμοποιούνται για την υλοποίηση των στόχων των ψυχολογικών επιχειρήσεων, τόσο σε επιχειρησιακό όσο και τακτικό επίπεδο, συμπεριλαμβάνεται μία μεγάλη γκάμα προϊόντων. Τα πιο κοινά από αυτά παραμένουν τα φυλλάδια και οι κάθε είδους αναμεταδόσεις( ραδιοφωνικές, τηλεφωνικές κλπ), ωστόσο είναι εφικτό να επιστρατευτούν και άλλα μέσα, όπως το θέατρο, το διαδίκτυο, τα γκράφιτι, και οι εφημερίδες.

Το πιο σύνθετο κομμάτι των ψυχολογικών επιχειρήσεων έχει σχέση με τις διεργασίες που συντελούνται στο εσωτερικό τους. Το προσωπικό των ενόπλων δυνάμεων το οποίο είναι επιφορτισμένο με τις ψυχολογικές επιχειρήσεις, εκτελεί στο πλαίσιο αυτό έξι κύριες εργασίες, που στον κανονισμό περιγράφονται ως ανάπτυξη, σχεδιασμός, παραγωγή, διάδοση, διανομή και αξιολόγηση. [28] Η όλη διαδικασία ξεκινά με τη διατύπωση αντικειμενικών σκοπών και στόχων. Η ιδέα ενεργείας ενός διοικητή συμπεριλαμβάνει την πρόθεση του σχετικά με τους αντικειμενικούς σκοπούς μίας επιχείρησης στους οποίους βασίζεται το αρμόδιο προσωπικό, για να σχεδιάσει τις αποστολές των ψυχολογικών επιχειρήσεων. Σε αυτό το στάδιο γίνεται ο διαχωρισμός *μεταξύ* ***σκοπών ψυχολογικών επιχειρήσεων (Psychological Operations Objectives)*** *και* ***σκοπών ή στόχων που υποστηρίζουν τις ψυχολογικές επιχειρήσεις (Supporting Psychological Operations Objectives)***. Σύμφωνα με το δόγμα, *ένας στόχος ψυχολογικών*

[25] Joint Chiefs of Staff, Doctrine for Joint Psychological Operations, Joint Publication 3-53 (September 5, 2003), ix
[26] Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.30, 1-3.
[27] Ibid., 1-2.
[28] Ibid., 1-5.

*επιχειρήσεων αντιστοιχεί στο σχήμα ρήμα-αντικείμενο,*[29] *το αντικείμενο ταυτίζεται με την αλλαγή που πρέπει να συντελεσθεί και το ρήμα καταδεικνύει την κατεύθυνση της αλλαγής.* Ρήματα όπως το μειώνω, αυξάνω, κερδίζω, διατηρώ περιλαμβάνονται στη λίστα των επιθυμητών ψυχολογικών δράσεων. Οι αντικειμενικοί σκοποί των ψυχολογικών επιχειρήσεων για να γίνουν κατανοητοί πρέπει να επαναπροσδιοριστούν στη βάση του συγκεκριμένου σχήματος ρήμα-αντικείμενο. Για παράδειγμα η φράση «αυξάνω την ασφάλεια» θα μπορούσε να μεταφραστεί σαν «μειώνω (ρήμα) τις τρομοκρατικές επιθέσεις (αντικείμενο, συμπεριφορά) και «διατηρώ (ρήμα) την εμπιστοσύνη (αντικείμενο) στις δυνάμεις ασφαλείας.» Κάθε φορά τώρα που ένας στόχος ψυχολογικών επιχειρήσεων πλαισιώνεται σωστά, παράγεται ένας στόχος που υποστηρίζει τις ψυχολογικές επιχειρήσεις και περιγράφεται στον κανονισμό *σαν την επιθυμητή συμπεριφορική αντίδραση του κοινού στόχου στην διενέργεια ψυχολογικών επιχειρήσεων.* [30]

## Αναγνώριση και Ανάλυση του Ακροατηρίου (Target Audience Identification and Analysis)

Ένα άλλο κρίσιμο στάδιο στη διεξαγωγή ψυχολογικών επιχειρήσεων, είναι η επιλογή του κατάλληλου ακροατηρίου το οποίο θα γίνει αποδέκτης του εκπεμπόμενου ψυχολογικού μηνύματος. Για να γίνει αυτό εφικτό, πρέπει να προηγηθεί μία διαδικασία η οποία είναι γνωστή ως **ανάλυση του ακροατηρίου-στόχου (Target Audience Analysis)**. Η ανάλυση του ακροατηρίου-στόχου αποτελεί μία πολύ σημαντική και κρίσιμη παράμετρο για τον επηρεασμό της συμπεριφοράς και της στάσης ενός κοινού. Συνιστά μία εμπειρική διαδικασία κατά την οποία αναλύονται τα κίνητρα της συμπεριφοράς μίας ομάδας ανθρώπων χρησιμοποιώντας ποιοτικές ή ποσοτικές ερευνητικές μεθόδους και υλοποιείται από μία λογική αλληλουχία δράσεων που εξελίσσονται σε τέσσερα διαδοχικά βήματα-στάδια. Τα στάδια αυτά είναι τα παρακάτω: α) Ποια ακροατήρια-στόχοι αναμένεται ότι πρόκειται να ανταποκριθούν καλύτερα και είναι πιο «επιρρεπή» στο εκπεμπόμενο ψυχολογικό μήνυμα. β) Ποιες στρατηγικές επηρεασμού του κοινού θα επιλεγούν ώστε να υλοποιηθούν οι αντικειμενικοί σκοποί της ψυχολογικής επιχείρησης. γ) Ποια μέσα ενημέρωσης θα μεταφέρουν πιο αποτελεσματικά την επιλεχθείσα στρατηγική επηρεασμού και δ) Ποια είναι εκείνα τα γεγονότα που θα χρησιμεύσουν ως ενδείκτες επιτυχίας ή αποτυχίας της ψυχολογικής επιχείρησης.[31] Για να υλοποιηθεί ο παραπάνω σκοπός, είναι απαραίτητο να προηγηθεί η **αναγνώριση του ακροατήριου στόχου** (**Target Audience Identification),** η οποία συνίσταται στη ενδελεχή γνώση των ιδιαίτερων κοινωνικών, θρησκευτικών, πολιτικό-οικονομικών χαρακτηριστικών των πληθυσμιακών ομάδων που συνυπάρχουν σε μία κοινωνία ή ένα κράτος. Προς την κατεύθυνση αυτή τα τελευταία έτη αντιγράφονται μέθοδοι και τεχνικές που χρησιμοποιεί το εμπορικό μάρκετινγκ, όπως π.χ. η **κατάτμηση (segmentation)** του ακροατηρίου-στόχου σε υποομάδες, με βάση ηλικιακά, δημογραφικά και οικονομικά κριτήρια. Στη μελέτη που δημοσίευσαν το 2007 οι συγγραφείς

[29] Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.301, 4-9.
[30] Ibid.,4-10.
[31] Ibid., 5-1.

Todd Helmus, Christopher Paul και Russell Glenn με τίτλο «*Enlisting Madison Avenue»*, υποστηρίζουν ότι «*η προσέγγιση μάρκετινγκ γίνεται όλο και πιο δημοφιλής στα θέατρα επιχειρήσεων»*[32] και ότι *«οι πρακτικές του εμπορικού μάρκετινγκ παρέχουν ένα χρήσιμο πλαίσιο εργασίας στην προσπάθεια των ΗΠΑ να διαμορφώσουν τις στάσεις και τις συμπεριφορές των τοπικών πληθυσμών. Ειδικότερα, η προσοχή θα πρέπει να δοθεί στις τεχνικές του branding, της ικανοποίησης των πελατών, και της κατάτμησης του ακροατηρίου»*. Η κατάτμηση του ακροατηρίου εφαρμόζεται με το σκεπτικό ότι τα μέλη μίας υπό-ομάδας είναι πιο επιρρεπή σε μια συγκεκριμένη εκστρατεία μάρκετινγκ. Ωστόσο, η συγκεκριμένη μέθοδος δε φαίνεται να αποδίδει τα επιθυμητά αποτελέσματα, ειδικά όταν εφαρμόζεται σε κοινά με παγιωμένες αντιλήψεις και σχηματοποιημένη εικόνα για το ρόλο που διαδραματίζουν οι ένοπλες δυνάμεις μίας χώρας σε ένα θέατρο επιχειρήσεων. Όπως σημειώνει και ο Steve Tatham σε μελέτη που δημοσιεύτηκε για την Αμερικάνικη Σχολή Πολέμου,[33] η κατάτμηση του ακροατηρίου συνιστά ένα τεχνητό κατασκεύασμα που υφίσταται μόνο στο πλάνο του υπεύθυνου πωλήσεων των εταιριών. Σε ένα όμως θέατρο επιχειρήσεων οι υποομάδες αποτελούν μία πραγματική οντότητα που επηρεάζεται από μία πλειάδα ανεξέλεγκτων παραγόντων. Θα ήταν εξάλλου θαυμάσιο εάν υπήρχε η δυνατότητα σε μία περιοχή που διεξάγονται επιχειρήσεις, να στοχοποιηθούν π.χ. μόνο οι μεσήλικες η οι γυναίκες. Φυσικά, όπως είναι εύκολα κατανοητό, αυτή η πολυτέλεια δεν υφίσταται σε μία πολεμική σύγκρουση όπου ομάδες ανθρώπων έχουν προαποφασίσει να στοιχηθούν σε ένα συγκεκριμένο στρατόπεδο. Επομένως, το έργο του επιτελείου των πληροφοριακών επιχειρήσεων είναι να κατανοήσει τους κανόνες λειτουργίας αυτών των ομάδων όπως ακριβώς υφίστανται-όχι να επινοήσει νέες-και να αποκρυπτογραφήσει τις συνθήκες κάτω από τις οποίες πρόκειται να εκδηλώσουν τις συγκεκριμένες συμπεριφορές που τις χαρακτηρίζουν. Αυτή είναι η πραγματική τεχνική της κατάτμησης του ακροατηρίου και διαφέρει σημαντικά από τις μεθόδους του μάρκετινγκ που χρησιμοποιούνται στη διαφήμιση. Επιπλέον, στο δυτικό κόσμο υπάρχει μία σιωπηρή συναίνεση μεταξύ του δυνητικού καταναλωτή και του διαφημιστή. Πολλές τηλεοπτικές σειρές περιέχουν διαφημίσεις οι οποίες προσπαθούν να πείσουν τον τηλεθεατή για την αγορά ενός προϊόντος και ο τηλεθεατής τις παρακολουθεί, συγκαταβαίνοντας έστω και παθητικά με αυτόν τον τρόπο στη διαφημιστική καμπάνια. Το «συμβόλαιο» αυτό όμως δεν υφίσταται στο πεδίο της μάχης. Οι αρνητικές για παράδειγμα αντιλήψεις για τους Αμερικάνους είναι βαθιά ριζωμένες στις Μουσουλμανικές κοινωνίες και δεν μπορούν να μεταβληθούν με απλές διαφημιστικές εκστρατείες.

Αντί της προσέγγισης του μάρκετινγκ, ο ταγματάρχης του Αμερικάνικου στρατού Baldwin προτείνει μία εντελώς διαφορετική διαχείριση του κοινού-στόχου, κατηγοριοποιώντας το σε πέντε υποσύνολα, ανάλογα με το πόσο «ανθεκτικό» ή «επιρρεπές» είναι το καθένα από αυτά σε ένα ψυχολογικό μήνυμα.[34] Η κατηγοριοποίηση προκύπτει από ανάλυση της

[32] See *www.rand.org/pubs/monographs/MG607.html.*

[33]Steve Tatham, "U.S. GOVERNMENTAL INFORMATION OPERATIONS AND STRATEGIC COMMUNICATIONS: A DISCREDITED TOOL OR USER FAILURE? IMPLICATIONS FOR FUTURE CONFLICT", Strategic Studies Institute and U.S. Army War College Press, December, 2013.

[34]Robert F. Baldwin, " A New Military Strategic Communication System", Advanced Military Studies Program, Fort Leavenworth, May 24, 2009

συμπεριφοράς των εμπλεκομένων στο πεδίο των επιχειρήσεων, που προσδιορίζει το κοινό-ακροατήριο, τοποθετώντας το ουσιαστικά σε ένα συνεχές συμπεριφοράς. Δανειζόμενος πολιτική ορολογία, ο ταγματάρχης χαρακτηρίζει τις πέντε διαφορετικές ομάδες –στόχους ως σκληρή αντιπολίτευση, μετριοπαθή αντιπολίτευση, αναποφάσιστους ή μετακινούμενους, μετριοπαθή και σκληρή υποστήριξη. Κατά τη διάρκεια της ανάπτυξης του ψυχολογικού μηνύματος, κάθε μήνυμα είναι προσαρμοσμένο στα χαρακτηριστικά του κοινού-στόχου. Για παράδειγμα, η σκληρή υποστήριξη απαιτεί ενίσχυση. Η μαλακή στήριξη και οι αναποφάσιστοι απαιτούν τη χρήση πειθούς. Η μαλακή αντιπολίτευση απαιτεί μετατροπή. Τέλος η σκληρή αντιπολίτευση απαιτεί εκπομπή αντίθετων μηνυμάτων. Προτεραιότητα για τις ψυχολογικές επιχειρήσεις έχουν οι αναποφάσιστοι και οι όσοι ανήκουν στη μετριοπαθή υποστήριξη. Μεταξύ δε των δύο, η μετριοπαθής υποστήριξη είναι πιο σημαντική διότι είναι 6 φορές ευκολότερο να μετακινηθεί ένα μέλος από αυτή την ομάδα στην σκληρή υποστήριξη, απ' ότι ένας αναποφάσιστος στη μετριοπαθή υποστήριξη.

Σε κάθε περίπτωση, η ανάλυση του ακροατηρίου είναι μία επίπονη και ιδιαίτερα πολύπλοκη διαδικασία που απαιτεί υποστήριξη από εξειδικευμένο επιστημονικό δυναμικό (επικοινωνιολόγους, ψυχολόγους, δημοσκόπους) και βρίσκεται συνεχώς υπό αναθεώρηση ακόμη και στις πιο προηγμένες στρατιωτικά χώρες.

## Στρατιωτική Εξαπάτηση.

Η στρατιωτική εξαπάτηση παρουσιάζει μία σημαντική ιδιαιτερότητα. Ενώ δεν υφίσταται στελεχωμένη στρατιωτική υπηρεσία στον κόσμο που να είναι αποκλειστικά προσανατολισμένη στη διεξαγωγή επιχειρήσεων αυτού του είδους, ωστόσο είναι γνωστό ότι η παραπλάνηση αποτελεί αναπόσπαστο μέρος σχεδόν κάθε επιχείρησης. Η στρατιωτική ιστορία βρίθει από παραδείγματα εξαπάτησης και ο στρατιωτικός μελετητής Jon Latimer ταξινομεί όλες τις ενέργειες που αποσκοπούν στην παραπλάνηση του αντιπάλου σε δύο μεγάλες κατηγορίες: σε αυτές που αυξάνουν την αμφιβολία σχετικά με τις προθέσεις των φίλιων δυνάμεων και σε εκείνες που σκόπιμα παραπληροφορούν τον εχθρό ώστε να επιλέξει λάθος τρόπο ενεργείας. [35] Το δόγμα των ενόπλων δυνάμεων των ΗΠΑ δε κάνει διάκριση ανάμεσα στις δύο αυτές κατηγορίες αλλά εστιάζει στον γενικό σκοπό της εξαπάτησης που συνίσταται στην καλλιέργεια και προώθηση ψευδών εντυπώσεων σχετικά με τις προθέσεις των φίλιων δυνάμεων. Ένα παράδειγμα ξεκάθαρου στόχου στρατιωτικής εξαπάτησης που περιγράφεται στον κανονισμό 3-13.4 είναι το παρακάτω: «*Κάνε τον εχθρό να κατευθύνει λανθασμένα τις δυνάμεις αναγνώρισης και επιτήρησης που διαθέτει, ώστε να υπερασπιστεί λανθασμένο τομέα στην άμυνα.*»[36] Σε αυτή τη λογική προκρίνεται μία μεθοδολογία που υλοποιείται σε τρία στάδια και βασίζεται στο τρίπτυχο των λέξεων «βλέπω» (τι παρατηρεί ο εχθρός από τις δικές μας επιχειρήσεις), «σκέφτομαι» (Σε ποια συμπεράσματα καταλήγει από την παρατήρησή του), «ενεργώ» (ποιες δράσεις είναι πιθανό να αναλάβει με βάση τα συμπεράσματα που έβγαλε από την

[35] Latimer, Deception in War, p.60.
[36] Joint Chiefs of Staff, Military Deception, Joint Publication 3-13.4(July 13, 2006), viii.

παρατήρηση).[37] Η συγκεκριμένη μέθοδος σύμφωνα πάντα με τον κανονισμό βασίζεται σε ιστορικά μαθήματα στρατιωτικής εξαπάτησης που είχαν επιτυχία από την αρχαιότητα μέχρι και την επιχείρηση «Καταιγίδα της Ερήμου.»

Οι επιχειρήσεις εξαπάτησης υλοποιούνται στη βάση τεσσάρων βασικών τεχνικών οι οποίες είναι γνωστές ως προσποίηση, επίδειξη, τέχνασμα και έκθεση. Η προσποίηση αποτελεί μία επιθετική πράξη που επιδιώκει την επαφή με τον εχθρό ώστε να τον παραπλανήσει για την τοποθεσία ή/και το χρόνο της πραγματικής επίθεσης. Στην επίδειξη εκτίθενται οι φίλιες δυνάμεις στον εχθρό χωρίς να υπάρχει πρόθεση εμπλοκής και με στόχο να παρασυρθεί ο αντίπαλος σε μία δυσμενή γι αυτόν σειρά δράσεων. Το τέχνασμα αποτελεί ένα πονηρό κόλπο που χαρακτηρίζεται από την εσκεμμένη έκθεση ψευδών ή συγκεχυμένων πληροφοριών για συλλογή και επεξεργασία από τον εχθρό. Τέλος, η έκθεση αφορά την εξομοίωση, μεταμφίεση και απεικόνιση αντικειμένων, μονάδων ή ικανοτήτων με στόχο να προωθηθεί το σχέδιο παραπλάνησης της φίλιας διοίκησης.[38] Επίσης, ανάλογα με τα εργαλεία και τα μέσα που χρησιμοποιούνται κάθε φορά, η στρατιωτική παραπλάνηση μπορεί να εφαρμοστεί με τρεις διαφορετικούς τρόπους, το φυσικό, τον τεχνικό και το διοικητικό. Στο φυσικό τρόπο περιλαμβάνονται ενέργειες όπως μετακινήσεις δυνάμεων, ασκήσεις, δραστηριότητες αναγνώρισης και επιτήρησης, επισκευές και συντήρηση εγκαταστάσεων, και τακτικές κινήσεις στρατευμάτων. Ο τεχνικός τρόπος αφορά την και εκπομπή και αναμετάδοση οποιουδήποτε είδους. Τέλος, στα διοικητικά μέσα ανήκουν οι τεχνικές που έχουν ως στόχο να διαρρεύσουν εσκεμμένα πληροφορίες ή αποδείξεις που βασίζονται σε έγγραφα ή προφορικές διαταγές. [39]

## Ασφάλεια Επιχειρήσεων.

Σύμφωνα με το δόγμα των Αμερικανικών Ενόπλων Δυνάμεων, *η στρατιωτική ασφάλεια είναι μία διαδικασία σχεδιασμένη έτσι ώστε να προλαμβάνεται η διαρροή κρίσιμων πληροφοριών στον εχθρό*[40]. Μία τέτοια δραστηριότητα όμως δεν αφορά μόνο πληροφορίες οι οποίες περιέχονται σε διαβαθμισμένα έγγραφα ή συστήματα (που χαρακτηρίζονται δηλαδή από την ένδειξη απόρρητο, άκρως απόρρητο κλπ) και υπακούουν σε δικούς τους αυστηρούς κανόνες χειρισμού και αποδέσμευσης. Κύρια μέριμνα της στρατιωτικής ασφάλειας είναι και η προστασία πληροφοριών ή ενδείξεων που συνδέονται με ευαίσθητες επιχειρήσεις και δραστηριότητες. Ο διακλαδικός Αμερικάνικος κανονισμός 3-13.3 (Ασφάλεια Επιχειρήσεων) επισημαίνει ότι πιθανοί αντίπαλοι- ανάμεσα στους οποίους συγκαταλέγονται και τρομοκρατικοί οργανισμοί- θα μπορούσαν να συλλέξουν αρκετές πληροφορίες από την παρατήρηση και από ανοικτές πηγές ενημέρωσης όπως το Ιντερνέτ, την τηλεόραση κλπ. [41] Από τον ορισμό απορρέει και η βασική αποστολή της στρατιωτική ασφάλειας, η οποία συνίσταται στη μείωση της τρωτότητας των ενόπλων δυνάμεων από την

[37] Ibid., IV-1.
[38] Ibid., 1-7.
[39] Ibid., 1-6.
[40] Joint Chiefs of Staff, Operation Security, Joint Publication 3-13.3(June 29, 2006), vii.
[41] Ibid., III-1.

επιτυχημένη εκμετάλλευση κρίσιμων πληροφοριών που πέφτουν στα χέρια του αντιπάλου. Οι επιχειρήσεις ασφάλειας βρίσκουν εφαρμογή σε όλες τις φάσεις μίας επιχείρησης που διεξάγουν οι ένοπλες δυνάμεις, τόσο κατά το στάδιο της προετοιμασίας, όσο και αυτό της εκτέλεσης.[42]

Το διακλαδικό δόγμα του Αμερικάνικου Πενταγώνου υπογραμμίζει συνεχώς ότι πρόκειται για μία συνεχόμενη διαδικασία και όχι για μία απλή τήρηση κανόνων (όπως την τήρηση π.χ. κανόνων στο χειρισμό εγγράφων). Στην ουσία αποτελεί μία μέθοδο η οποία μπορεί να εφαρμοστεί σε κάθε επιχείρηση ή δραστηριότητα με σκοπό την αποφυγή διαρροής κρίσιμων πληροφοριών στον αντίπαλο[43] και περιλαμβάνει πέντε στάδια: α) Την αναγνώριση των κρίσιμων πληροφοριών. Είναι πολύ σπουδαία διότι επικεντρώνεται στην προστασία πληροφοριών ζωτικής σημασίας παρά στο σύνολο διαβαθμισμένων και ευαίσθητων δεδομένων. β) Την ανάλυση της απειλής. Σε αυτό το στάδιο υλοποιείται η ανάλυση των πληροφοριών με συλλέγονται με ποικίλους τρόπους ώστε να προσδιοριστούν οι δυνητικοί αντίπαλοι κατά τη διάρκεια μίας επιχείρησης. γ) Την ανάλυση των ευαίσθητων σημείων. Γι αυτόν τον σκοπό χρησιμοποιούνται ενδείκτες ασφαλείας που αποκαλύπτουν τα τρωτά σημεία μίας επιχείρησης με βάση τις δυνατότητες που διαθέτει ο αντίπαλος στην συλλογή πληροφοριών. δ) Την αξιολόγηση του κινδύνου. Αφορά την ανάλυση των τρωτών σημείων που αναγνωρίστηκαν στο προηγούμενο στάδιο και την υιοθέτηση συγκεκριμένων μέτρων ασφαλείας που πρέπει να εκτελεστούν σε συνάρτηση με το βαθμό κινδύνου της επιχείρησης. ε) Την Εφαρμογή των Κατάλληλων Μέτρων Ασφαλείας.[44] Το πιο δύσκολο και κρίσιμο από όλα τα στάδια είναι η ανάλυση των τρωτών σημείων κατά το οποίο το επιτελείο που σχεδιάζει την επιχείρηση πρέπει να φανταστεί ποιοι ενδείκτες ασφαλείας ταιριάζουν περισσότερο στην κάθε επιχείρηση. Οι πιο συνηθισμένες ενδείξεις αφορούν την άφιξη και αναχώρηση μεγάλου αριθμού στρατευμάτων και υλικού, την κινητοποίηση ιατρικού προσωπικού και την αποθήκευση φαρμακευτικού υλικού, την αποστολή σημειωμάτων σε προσωπικό του στρατού που βρίσκεται σε άδεια να επιστρέψει όμως θέσεις του κα.[45] Είναι τέλος πολύ σημαντικό να τονισθεί ότι η στρατιωτική ασφάλεια υπόκειται συνεχώς σε αναθεώρηση, όσο οι απειλές μεταβάλλονται με την πάροδο του χρόνου, κάθε φορά δηλαδή που οι αντίπαλοι αλλάζουν και επανακαθορίζουν τα σχέδια συλλογής πληροφοριών.

## 3.2 ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

### Ηλεκτρονικός Πόλεμος

Σύμφωνα με το διακλαδικό δόγμα των ενόπλων δυνάμεων των ΗΠΑ, ο ηλεκτρονικός πόλεμος αναφέρεται σε κάθε στρατιωτική δράση που περιλαμβάνει τη χρήση ηλεκτρομαγνητικής ενέργειας με σκοπό τον έλεγχο του ηλεκτρομαγνητικού φάσματος ή την επίθεση στον εχθρό.[46] Η αποστολή του ηλεκτρονικού πολέμου συνίσταται στο να εξασφαλίσει και να διατηρήσει τον έλεγχο του ηλεκτρομαγνητικού φάσματος υπό τις φίλιες δυνάμεις και να

[42] Ibid., 1-2.
[43] Ibid., 1-2.
[44] Ibid., ix.
[45] Ibid., B-6.
[46] Joint Chiefs of Staff, Joint Doctrine for Electronic Warfare, Joint Publication 3-51 (Washington D.C. April 7, 2007), vii.

απαγορεύσει τη χρήση του από τον εχθρό, μέσω καταστροφής, εξαπάτησης και αποδιοργάνωσης.[47] Οι δραστηριότητες ηλεκτρονικού πολέμου διακρίνονται σε τρεις κατηγορίες: Την ηλεκτρονική επίθεση κατά την οποία χρησιμοποιείται ενέργεια ή όπλα που λειτουργούν με ηλεκτρομαγνητικά σήματα για να προσβληθούν εχθρικά στρατεύματα, εγκαταστάσεις ή εξοπλισμός.[48] Την ηλεκτρονική άμυνα που περιλαμβάνει ενεργητικά και παθητικά μέτρα προστασίας της φίλιας δύναμης από την ηλεκτρονική επίθεση του αντιπάλου. Την υποστήριξη του ηλεκτρονικού πολέμου που είναι πιο περίπλοκη διαδικασία και εξειδικεύεται σε δράσεις ανίχνευσης, προσδιορισμού και εντοπισμού θέσης των πηγών εκπομπής ηλεκτρομαγνητικής ενέργειας.[49] Ενώ όπως φαίνεται από την παραπάνω κατηγοριοποίηση ο ηλεκτρονικός πόλεμος έχει ένα τεράστιο εύρος δραστηριοτήτων, η έμφαση στις σύγχρονες επιχειρήσεις δίνεται στα αντίμετρα που αφορούν τη διοίκηση, τον έλεγχο και τις επικοινωνίες του αντιπάλου. Στην πολεμική αεροπορία τα συγκεκριμένα αντίμετρα χρησιμοποιούνται για την καταστολή της εχθρικής αεράμυνας.

Ο ηλεκτρονικός πόλεμος σε πολλά σημεία είναι ευθυγραμμισμένος με τις επιχείρησης εξαπάτησης, καθώς αρκετές τεχνικές του προσπαθούν να παραπλανήσουν τους εχθρικούς αισθητήρες σχετικά με τις πραγματικές προθέσεις της φίλιας δύναμης. Επίσης, συνεργάζεται και με την στρατιωτική ασφάλεια στον τομέα του ελέγχου των ηλεκτρομαγνητικών εκπομπών. Όπως χαρακτηριστικά αναφέρει το δόγμα, *«Ο Ηλεκτρονικός πόλεμος αποτελεί έναν πολλαπλασιαστή ισχύος. Λειτουργεί σε διάφορα επίπεδα της σύγκρουσης, από την αυτοπροστασία μέχρι και τα επιχειρησιακά σχέδια επίθεσης. Όταν οι εφαρμογές του συνδυάζονται με στρατιωτικές ενέργειες, επιτυγχάνεται ένα διαδραστικό αποτέλεσμα, μειώνονται οι απώλειες και βελτιώνεται η αποτελεσματικότητα.»*[50]

**Επιχειρήσεις σε Δίκτυα Υπολογιστών**

Οι συγκεκριμένες επιχειρήσεις περιβάλλονται με ένα πέπλο μυστικότητας καθώς το δόγμα είναι διαβαθμισμένο και δεν επιτρέπεται η δημόσια δημοσίευσή του. Έτσι, ενώ ο οδικός χάρτης για τις πληροφοριακές επιχειρήσεις του 2003 χαρακτηρίστηκε ως αδιαβάθμητος το 2006, τα τμήματα του εκείνα που αναφέρονται στις δικτυοκεντρικές επιχειρήσεις, παραμένουν ακόμη και σήμερα διαβαθμισμένα. Μία μικρή αναφορά γίνεται μόνο στο διακλαδικό κανονισμό 3-13, όπου περιγράφονται πολύ συνοπτικά οι τρείς μορφές των συγκεκριμένων επιχειρήσεων που είναι: Η επίθεση σε δίκτυα υπολογιστών, η άμυνα των δικτύων υπολογιστών και η εκμετάλλευση των δικτύων πληροφοριών. Η επίθεση σε δίκτυα υπολογιστών αποτελείται από ενέργειες που αναλαμβάνονται με σκοπό να απαγορεύσουν, να υποβαθμίσουν και να καταστρέψουν πληροφοριακό περιεχόμενο υπολογιστών και δικτύων ή τους υπολογιστές και τα δίκτυα. Η άμυνα των δικτύων υπολογιστών περιλαμβάνει ενέργειες μέσω των δικτύων που έχουν ως στόχο να προστατεύσουν, παρακολουθήσουν, αναλύσουν, εντοπίσουν και αμυνθούν σε μη εξουσιοδοτημένες δραστηριότητες που κατευθύνονται εναντίον των πληροφοριακών συστημάτων του υπουργείου εθνικής άμυνας. Η

[47] Ibid. I-3.
[48] United States Air Force, Electronic Warfare, Air Force Doctrine Document 2-5.1 (November 5, 2002), p.7.
[49] Ibid. I-2.
[50] Ibid. vii.

εκμετάλλευση των δικτύων πληροφοριών στοχεύει όχι μόνο στην προστασία των πληροφοριακών συστημάτων από εξωτερικούς εισβολείς αλλά και στην εκμετάλλευση που μπορεί να προέλθει από εσωτερικές ενέργειες και αποτελεί απαραίτητη διαδικασία κάθε στρατιωτικής επιχείρησης.[51]

Τα δημοσιευμένα στοιχεία σχετικά με αυτές τις επιχειρήσεις είναι σχετικά λίγα. Κατά τη διάρκεια όμως Καταιγίδας όμως Ερήμου είναι γνωστό π.χ. ότι οι συμμαχικές δυνάμεις προέβησαν στην εκμετάλλευση των δικτύων για να παραδώσουν μηνύματα ψυχολογικού περιεχομένου σε Ιρακινούς διοικητές μέσω αποστολής e-mail, κλήσεων κινητής τηλεφωνίας και φαξ.[52] Γενικά όμως η επίθεση σε δίκτυα υπολογιστών υπήρξε περιορισμένη λόγω και του γεγονότος ότι τα ιρακινά πληροφοριακά συστήματα δεν ήταν διασυνδεμένα με την παγκόσμια διαδικτυακή τράπεζα.

## 3.3 ΠΕΡΙΟΡΙΣΜΟΙ-ΠΡΟΚΛΗΣΕΙΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

### Το Ζήτημα Της Αξιοπιστίας

Τα ζήτημα της αξιοπιστίας έχει κομβικό χαρακτήρα σε όλο το φάσμα των επιχειρήσεων επιρροής που διεξάγει ένα κράτος. Στις πληροφοριακές επιχειρήσεις αφορά κυρίως τη θεμελιώδη ικανότητα της στρατιωτικής παραπλάνησης του αντιπάλου. Οι τεχνικές εξαπάτησης μπορεί να αποδώσουν βραχυπρόθεσμα οφέλη, αλλά όταν αποκαλυφθούν, ζημιώνουν σε μεγάλο βαθμό την εικόνα αξιοπιστίας ενός έθνους διεθνώς, με ό,τι αυτό συνεπάγεται για τη δυνατότητα που έχει μελλοντικά να συμπήξει συμμαχίες με άλλα κράτη και να επηρεάσει πληθυσμούς που βρίσκονται εκτός των φυσικών του συνόρων. Ένα ιστορικό παράδειγμα εσφαλμένου χειρισμού που ζημίωσε τη φήμη και την αξιοπιστία της νατοϊκής συμμαχίας αφορά τον βομβαρδισμό ενός τρένου από τις νατοϊκές δυνάμεις στην Σερβία το 1999. Το αεροπλάνο στόχευε στην πραγματικότητα τη γέφυρα και επρόκειτο για ένα τραγικό περιστατικό, αλλά το φιλμ που παρουσίασε το NATO δεν ανταποκρινόταν πλήρως στην πραγματικότητα. Έδειχνε το τρένο να κινείται πολύ γρήγορα και να εισέρχεται ξαφνικά στην ακτίνα δράσης της βόμβας, χωρίς να είναι εφικτό για τον πιλότο να ακυρώσει ή να αλλάξει την πορεία της. Στην πραγματικότητα όμως το φιλμ είχε αλλοιωθεί και «έτρεχε πιο γρήγορα από το κανονικό», κάτι που έγινε αντιληπτό από τους δημοσιογράφους. Το έλλειμμα αξιοπιστίας που προκλήθηκε από αυτό το περιστατικό ταλάνισε για αρκετό χρονικό διάστημα το NATO και θα μπορούσε να είχε αποφευχθεί αν δεν γινόταν προσπάθεια χειραγώγησης της κοινής γνώμης και παρουσιαζόταν εξαρχής όχι η πλαστή αλλά η πραγματική εικόνα.[53]

Επίσης το ζήτημα της αξιοπιστίας συνδέεται και με τις ψυχολογικές επιχειρήσεις. Οποιαδήποτε προσπάθεια ανάμιξης αληθινών και πλαστών γεγονότων συνεπάγεται την ταύτιση των πληροφοριακών επιχειρήσεων με την προπαγάνδα η οποία γεννά αυτομάτως αρνητικούς συνειρμούς και καταστρέφει τη φήμη τους. Όσον αφορά το θέμα αυτό, ο ιστορικός και πρώην αξιωματικός του βρετανικού στρατού Jon Latimer, παρατηρεί: «Μία βασική

---

[51] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington, DC, February 13, 2006) II-4-II-5.

[52] Leigh Armistead, "Information Operations: Warfare and the Hard Reality of Soft Power" p.158

[53] Jon Latimer, Deception in War: The Art of the Buff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military Histories, from the Trojan Horse to the Gulf War(New York: The Overlook Press, 2001) p.296-297.

αρχή που εξασφαλίζει την αποτελεσματικότητα των ψυχολογικών επιχειρήσεων είναι ότι πρέπει να ασχολούνται με την αλήθεια και με τίποτα περισσότερο από αυτήν, αν και μπορούν ασφαλώς να μην την παρουσιάζουν στο σύνολό της. Η εξαπάτηση φυσικά συνδέεται με ψέματα και επομένως οι στόχοι της βρίσκονται ριζικά σε αντίθεση με αυτούς των ψυχολογικών επιχειρήσεων.»[54]

## Το Ζήτημα των Νομικών Περιορισμών.

Το σύνολο σχεδόν των πληροφοριακών επιχειρήσεων αφορά ανορθόδοξες ενέργειες που διενεργούνται μυστικά και επομένως είναι αρκετά δύσκολο να καθοριστεί ένα νομικό πλαίσιο που να περιγράφει ποιες από αυτές τις δράσεις είναι νόμιμες και ποιες όχι. Επιπλέον, οι περισσότερες χώρες «δυσφορούν» με την ιδέα επιβολής νομικών περιορισμών καθότι μία τέτοια προοπτική θα ακύρωνε ή θα παρεμπόδιζε σε σημαντικό βαθμό πολλές από τις ασύμμετρες πληροφοριακές δραστηριότητες που αναπτύσσουν από τον καιρό της ειρήνης και κινούνται στο όριο της νομιμότητας. Για τους παραπάνω λόγους δεν έχει καταστεί δυνατό μέχρι τις μέρες μας να υπάρξει μία συλλογική ομοφωνία για τον καθορισμό ενός νομικού πλαισίου που να περιγράφει ποιες από αυτές τις δράσεις είναι ανεκτές και ποιες παραβιάζουν το δίκαιο του πολέμου.

Σε αρκετά βέβαια κράτη-μέλη της διεθνούς κοινότητας υπάρχουν νόμοι που θέτουν φραγμούς στην οποιαδήποτε απόπειρα επηρεασμού του εγχώριου πληθυσμού από την εκάστοτε κυβερνητική εξουσία. Για παράδειγμα, ο νόμος υπ' αριθμ 402, γνωστός και ως πράξη Smith-Munds που θεσπίστηκε το 1948 στις ΗΠΑ, απαγορεύει στην Πληροφοριακή Υπηρεσία των Ηνωμένων Πολιτειών να διαχέει πληροφοριακό υλικό στο Αμερικάνικο ακροατήριο.[55] Η συγκεκριμένη νομική διάταξη σχεδιάστηκε έτσι ώστε να προστατεύονται οι πολίτες από την προπαγάνδα της δικιάς τους κυβέρνησης και το σκεπτικό της παραμένει σε γενικές γραμμές ικανοποιητικό, ακόμη και στις μέρες μας. Ωστόσο η εφαρμογή του νόμου σήμερα, εξαρτάται σε μεγάλο βαθμό από έναν σημαντικό αστάθμητο παράγοντα που δεν υπολόγισαν οι νομοθέτες το 1948 όταν τον πρωτοσυνέταξαν: Το σύγχρονο πληροφοριακό περιβάλλον του οποίου η φύση και η έκταση καθιστά δύσκολη, αν όχι αδύνατη, την οποιαδήποτε διάκριση μεταξύ εσωτερικού και ξένου ακροατηρίου. Για παράδειγμα, μία δημοσίευση στον τοπικό τύπο που απευθύνεται στον ντόπιο πληθυσμό, και καταχωρείται από ένα δημοσιογράφο ηλεκτρονικά, αναπαράγεται σχεδόν αυτόματα σε όλα τα διεθνή μέσα ενημέρωσης. Η πληροφορία δεν γίνεται επομένως να στεγανοποιηθεί και γι αυτό η συμμόρφωση με το νόμο του 1948 αποτελεί μία πρόκληση για τα μέσα ενημέρωσης. Το υπουργείο εθνικής άμυνας των ΗΠΑ, σε πλήρη ευθυγράμμιση με την συγκεκριμένη νομοθεσία και έχοντας αντίληψη των υπαρκτών κινδύνων παραβίασης τους νόμου που ενέχει η διεξαγωγή πληροφοριακών δραστηριοτήτων, απαγορεύει τη χρήση του ιντερνέτ σαν μέσου διάδοσης «προϊόντων ψυχολογικών επιχειρήσεων», πριν αυτά πάρουν έγκριση από τον αρμόδιο γραμματέα. Επίσης, οι ψυχολογικές επιχειρήσεις εμπίπτουν και σε νομικές διατάξεις σχετικές με το χειρισμό και την

[54] Ibid. 79
[55] Armistead, Information Operations, p.132.

αναπαραγωγή κειμένων, γεγονός που δυσχεραίνει περισσότερο τη διεξαγωγή τους. Ειδικά πάνω σε αυτό το ζήτημα ο αμερικάνικος κανονισμός 3-05.30 επισημαίνει: Στο *νόμο για τα πνευματικά δικαιώματα υπόκεινται και οι ψυχολογικές επιχειρήσεις. Κανένα προϊόν δε θα πρέπει να περιέχει υλικό αντιγραφής αν δεν έχει λάβει πρώτα την συγκατάθεση του συντάκτη. Εικόνες, ηχητικοί φάκελοι, κείμενα και όλα τα θέματα που σχετίζονται με τα μέσα ενημέρωσης πρέπει να έχουν διευθετηθεί πριν την παραγωγή τους.*[56] Οι συγκεκριμένοι περιορισμοί φυσικά είναι κατανοητό ότι έχουν επίδραση τόσο στο χρόνο όσο και στην ποιότητα του παραγόμενου προϊόντος. Η μεγαλύτερη δυσκολία έγκειται στα ραδιοτηλεοπτικά μέσα εκεί όπου ο νόμος για τα πνευματικά δικαιώματα απαγορεύει να χρησιμοποιούνται αντιγραμμένα κινούμενα σχέδια, εμπορικές ραδιοφωνικές και τηλεοπτικές μεταδόσεις και φωτογραφίες.[57] Το θέμα της νομιμότητας όμως δεν περιορίζεται μόνο στις ψυχολογικές επιχειρήσεις, αλλά «αγγίζει» και κάθε δραστηριότητα που συνδέεται με την στρατιωτική εξαπάτηση. Το δόγμα των αμερικάνικων ενόπλων δυνάμεων είναι πολύ κατηγορηματικό σε αυτήν την περίπτωση επισημαίνοντας ότι: «Ιδιαίτερη προσοχή θα πρέπει να δίνεται ώστε να προστατεύεται η ποιότητα των πληροφοριών που είναι διαθέσιμες σε δημόσιο ακροατήριο».[58] Γι' αυτόν το λόγο απαιτείται πολύ διακριτική διαχείριση του πληροφοριακού υλικού ώστε να μη μεταφέρονται ψευδείς ειδήσεις στο φίλιο κοινό που παραβιάζουν το νόμο και δοκιμάζουν την εμπιστοσύνη του. Αναμφίβολα πρόκειται για μία δύσκολη άσκηση ισορροπίας που αποτελεί ένα από τα κεντρικά ζητήματα της στρατιωτικής εξαπάτησης. Στην ίδια τέλος κατηγορία μη επιτρεπτών ενεργειών ανήκουν και επιχειρήσεις παραπλάνησης που μετέρχονται παράνομων μεθόδων για να υλοποιήσουν τους σκοπούς τους. Στις μεθόδους αυτές συγκαταλέγονται αρκετές πράξεις όπως: Η προσποίηση παράδοσης στον εχθρό με χρήση λευκή σημαίας που σκοπεύει στο να παγιδέψει τον αντίπαλο, η κατάχρηση προστατευτικών σημάτων και συμβόλων με πρόθεση να τραυματίσει, σκοτώσει ή συλλάβει το εχθρικό προσωπικό, η χρήση ασθενοφόρων ή οχημάτων με τον ερυθρό σταυρό για μεταφορά οπλισμού πυρομαχικών και στρατιωτών, η αμφίεση του στρατιωτικού προσωπικού με παραπλανητικά διακριτικά και στολές κατά τη διάρκεια της μάχης κ.α.

## Το Ζήτημα της Αξιολόγησης.

Η κύρια πρόκληση που αντιμετωπίζουν οι πληροφοριακές επιχειρήσεις έγκειται στη δυσκολία που υφίσταται να αξιολογηθεί και να αποτιμηθεί σε πραγματικούς όρους η συνεισφορά τους σε μία στρατιωτική επιχείρηση. Η παράδοση π.χ. χιλιάδων στρατιωτών στον πόλεμο του Ιράκ δε μπορεί να θεωρηθεί αποκλειστικά αποτέλεσμα συντονισμένων ψυχολογικών δραστηριοτήτων διότι σε αυτό ενδέχεται να συνετέλεσαν και άλλοι παράγοντες όπως π.χ. η συντριπτική στρατιωτική και υλική υπεροχή των συμμάχων, η απέχθεια για το καθεστώς του Σαντάμ Χουσεΐν κλπ. Επομένως, ενώ η συμπεριφορά σε αυτό το παράδειγμα είναι ορατή και αφορά την παράδοση των

[56] Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.30, 1-13.
[57] Christopher Lamb, Review of Psychological Operations Lessons Learned from Recent Operational Experience (Washington D.C.: National Defense University Press, September 2005), p.9.
[58] Joint Chiefs of Staff, Military Deception, 1-6.

στρατιωτών, οι πιθανοί λόγοι που την προκάλεσαν είναι αρκετά συγκεχυμένοι.

Στο νατοϊκό δόγμα η αξιολόγηση αποτελεί μία λειτουργία που ενσωματώνεται σε όλες τις φάσεις του σχεδιασμού και του κύκλου εκτέλεσης των πληροφοριακών επιχειρήσεων και περιλαμβάνει δραστηριότητες που σχετίζονται με καθήκοντα, γεγονότα, ή προγράμματα για την υποστήριξη διακλαδικών στρατιωτικών επιχειρήσεων.[59] Σχεδιάζεται στην αρχή κάθε επιχείρησης με πρόθεση να παράσχει ανατροφοδότηση στους υπεύθυνους λήψης αποφάσεων, προκειμένου να προχωρήσουν σε ενέργειες που θα φέρουν τα επιθυμητά αποτελέσματα. Η αξιολόγηση επίσης επιδιώκει να αναλύσει και να πληροφορήσει για την απόδοση και τη αποτελεσματικότητα των πληροφοριακών δραστηριοτήτων. Η νατοϊκή συμμαχία για να υλοποιήσει τον παραπάνω σκοπό έχει ενσωματώσει και υιοθετήσει στα δόγματά της τους όρους **μέτρα αποδοτικότητας (measures of performance MOPs) και μέτρα αποτελεσματικότητας (measures of effectiveness MOEs).[60] Τα μέτρα αποδοτικότητας είναι κριτήρια που χρησιμοποιούνται για την εκτίμηση της εκπλήρωσης καθηκόντων και εργασιών που σχετίζονται με την εκτέλεση της αποστολής των φίλιων δυνάμεων. Αντίθετα, τα μέτρα αποτελεσματικότητας αποτελούν τα κριτήρια που χρησιμοποιούνται για την αξιολογήσουν τις αλλαγές που συντελούνται στην συμπεριφορά του συστήματος και του επιχειρησιακού περιβάλλοντος και καθορίζουν το εάν οι ενέργειες που εκτελούνται, συμβάλλουν τελικά στους αντικειμενικούς σκοπούς του σχεδιασμού μίας επιχείρησης. Ουσιαστικά, σκοπός των μέτρων αποτελεσματικότητας είναι να συνεισφέρουν στην αξιολόγηση των πληροφοριακών επιχειρήσεων με την ποσοτικοποίηση άυλων χαρακτηριστικών μέσα στο πληροφοριακό περιβάλλον, προκειμένου να εκτιμηθεί η αποτελεσματικότητα των πληροφοριακών δραστηριοτήτων κατά ενός υφιστάμενου ή δυνητικού αντιπάλου.** Γι' αυτό το λόγο πρέπει να είναι συγκεκριμένα, μετρήσιμα και παρατηρήσιμα. Η αποτελεσματικότητα και η απόδοση μετριέται είτε ποσοτικά (π.χ., μετρώντας αριθμό επιθέσεων) ή ποιοτικά (π.χ. αξιολογώντας υποκειμενικά το βαθμό εμπιστοσύνης στις δυνάμεις ασφαλείας). Παραδείγματα μέτρων αποδοτικότητας και αποτελεσματικότητας φαίνονται στους πίνακες που ακολουθούν.

**Παραδείγματα Μέτρων Αποδοτικότητας.**

| |
|---|
| Αριθμός ανθρώπων που ακούει εκπομπές που αναφέρονται σε δράσεις στήριξης των πληροφοριακών επιχειρήσεων |
| Ποσοστό των εγκαταστάσεων διοίκησης και ελέγχου του αντιπάλου που δέχτηκε επίθεση |
| Αριθμός σχεδίων επιχειρήσεων πολιτικό-στρατιωτικής συνεργασίας που έχουν ξεκινήσει / αριθμός των έργων που ολοκληρώθηκε. |

**Πιθανές Πηγές Μέτρων Αποτελεσματικότητας**

| |
|---|
| Αξιολογήσεις από πληροφορίες (ανθρώπινες πηγές, κλπ) |
| Ανοικτές πηγές πληροφοριών |

[59] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington, DC, November 27, 2012), IV-8.

[60] Ibid., IV-

| |
|---|
| Ίντερνετ |
| Επικοινωνία με το κοινό |
| Έρευνες Τύπου και σχόλια. |
| Δημοσκοπήσεις, εκθέσεις και έρευνες. |
| Μη κυβερνητικές οργανώσεις, διακυβερνητικοί οργανισμοί, διεθνείς οργανώσεις. |
| Συναντήσεις συμβούλων εξωτερικής πολιτικής. |
| Εμπορικές δημοσκοπήσεις. |

Η ποσοτικοποίηση των μέτρων αποτελεσματικότητας υλοποιείται με κατάλληλους ενδείκτες που ονομάζονται **ενδείκτες μέτρων αποτελεσματικότητας**.[61] **Ο ενδείκτης μέτρων αποτελεσματικότητας είναι μια μονάδα, τοποθεσία ή γεγονός, μετρήσιμο και παρατηρήσιμο, που δύναται να χρησιμοποιηθεί για την εκτίμηση ενός μέτρου αποτελεσματικότητας.** Οι ενδείκτες βοηθούν το επιτελείο των πληροφοριακών επιχειρήσεων να αναγνωρίσει και καθορίσει μέτρα αποτελεσματικότητας μέσα στο πληροφοριακό περιβάλλον. Σε μία επιχείρηση μεγάλης κλίμακας μπορεί να χρειαστεί να χρησιμοποιηθούν εκατοντάδες ενδείκτες. Παράδειγμα του πώς τα αποτελέσματα μεταφράζονται σε ενδείκτες φαίνεται παρακάτω:

**Αποτέλεσμα**: Η ηγεσία των ανταρτών δεν ενορχηστρώσει τρομοκρατικές ενέργειες στις δυτικές περιοχές.

**Μέτρο Αποτελεσματικότητας**: (Ποιοτικό) Μείωση της λαϊκής υποστήριξης προς τους εξτρεμιστές και τους αντάρτες.

**Ενδείκτες Μέτρου Αποτελεσματικότητας**:

α. Αύξηση του αριθμού των ανταρτών που έχουν μεταστραφεί / εντοπιστεί από τις 1η Οκτώβριου.

β. Αύξηση του ποσού των χρημάτων που καταβλήθηκαν στους πολίτες από το «πρόγραμμα ανταμοιβής» από την 1η Οκτωβρίου.

γ. Περισσότερα μπλογκ υποστηρίζουν τους τοπικούς αξιωματούχους.

## 3.4 ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΜΕ ΒΑΣΗ ΤΗ ΜΕΘΟΛΟΓΙΑ ΤΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Σύμφωνα με το διακλαδικό νατοϊκό κανονισμό 3-10, οι πληροφοριακές επιχειρήσεις μπορούν να εκτελεσθούν πιο αποτελεσματικά με την υιοθέτηση ενός μοντέλου που ονομάζεται μέθοδος βασισμένη στα αποτελέσματα (*Effect's Based Approach* ο Αγγλικός όρος).[62] Το συγκεκριμένο μοντέλο παρέχει έναν αυστηρό και ορθολογικό μηχανισμό για την ανάπτυξη στρατηγικής στον τομέα των πληροφοριακών επιχειρήσεων. Εξηγεί λογικά τους συσχετισμούς μεταξύ των δράσεων των πληροφοριακών επιχειρήσεων, τα έμμεσα ή άμεσα αποτελέσματα που αναμένεται να προκληθούν από τις δράσεις αυτές και το πώς τα παραγόμενα αποτελέσματα συμβάλλουν στην επίτευξη των στόχων ενός διοικητή.[63] Με βάση δηλαδή τη προσέγγιση αυτή, κάθε ενέργεια εναντίον του εχθρού έχει σχεδιαστεί έτσι ώστε να παράγει επιπτώσεις που υλοποιούν

[61] Ibid., IV-10.

[62] NATO Allied Joint Doctrine for Information Operations, Joint Publication 3-10, November 2009, xii.

[63] Edward C. Mann, Gary Enders and Thomas R. Searle. *Thinking Effects: Effects-Based Methodology for Joint Operations* (Maxwell AFB, AL: Air University Press, 2002), p. 2.

συγκεκριμένους στρατιωτικούς και πολιτικούς αντικειμενικούς σκοπούς. Πρέπει δε να επισημανθεί ότι οι πληροφοριακές δράσεις παράγουν διαφορετικούς τύπους αποτελεσμάτων, ωστόσο αυτό που έχει σημασία δεν είναι ο χαρακτήρας και η μορφή των επιπτώσεων αλλά η ορθή χρησιμοποίησή τους με στόχο την υλοποίηση των αντικειμενικών σκοπών του εκάστοτε διοικητή. Στο πλαίσιο αυτό, υπάρχει η πιθανότητα να δημιουργηθούν και παράπλευρες επιπτώσεις που βλάπτουν παρά ωφελούν τους αντικειμενικούς σκοπούς. Ωστόσο, ένας καλός σχεδιασμός επιδιώκει να ελαχιστοποιεί τις παραπάνω πιθανότητες. Ένα υποθετικό απλό σενάριο που μπορεί να εξηγήσει τη δράση των αποτελεσμάτων αυτών έχει ως εξής: Μια στρατιωτική δύναμη προσπαθεί μέσω διεξαγωγής πληροφοριακών επιχειρήσεων να εξαπατήσει τον αντίπαλο διοικητή ως προς την κατεύθυνση διενέργειας μίας επίθεσης. Για να το επιτύχει, η φίλια δύναμη θα μπορούσε να κατασκευάσει ομοιώματα αρμάτων και να τα εκθέσει σκόπιμα στην εχθρική παρατήρηση δορυφόρων και μη επανδρωμένων αεροσκαφών. Οι φωτογραφίες που θα έφταναν στο διοικητή του εχθρού, θα οδηγούσαν σε αλυσιδωτές αντιδράσεις. Αν επιπλέον οι φίλιες δυνάμεις είχαν τη δυνατότητα να παρεμβάλλουν τις επικοινωνίες των μονάδων αναγνώρισης του εχθρού ώστε να μην είναι ικανές να στείλουν τις αναφορές τους στο διοικητή τους, τότε θα δημιουργούνταν μεγαλύτερη ασάφεια στο αντίπαλο στρατόπεδο σχετικά με τις φίλιες προθέσεις. Τέλος, με την εισαγωγή ψευδών πληροφοριών στα Η/Υ του αντίπαλου διοικητή η πληροφοριακή δράση θα παρήγαγε ένα άμεσο αποτέλεσμα που θα εξασφάλιζε την επίτευξη του επιθυμητού στόχου: την εξαπάτηση του διοικητή του εχθρού σχετικά με την κατεύθυνση της φίλιας επίθεσης.

# ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ
# ΣΤΡΑΤΗΓΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ

## 5.1 ΣΥΝΤΟΜΟ ΙΣΤΟΡΙΚΟ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

Ο όρος <<στρατηγική επικοινωνία>> παρουσιάζεται για πρώτη φορά στη διεθνή βιβλιογραφία μόλις στις αρχές της νέας χιλιετίας. Προγενέστεροι ωστόσο όροι που περιγράφουν συναφείς με το αντικείμενο της στρατηγικής επικοινωνίας δραστηριότητες, εντοπίζονται στα μέσα της δεκαετίας του 60. Ο πιο γνωστός από αυτούς είναι η διπλωματία κοινού (public diplomacy) και σύμφωνα με τις ιστορικές πηγές η πρώτη διατύπωση της συγκεκριμένης φράσης έγινε το 1965 από τον Πρέσβη Edmund Gullion, ο οποίος διετέλεσε επί μακρόν καθηγητής στη διπλωματική σχολή του Fletcher, στο

Πανεπιστήμιο Tufts.[64] Οι κεντρικές πρακτικές της διπλωματίας κοινού ανάγονται στην αρχαιότητα και εμφανίζονται περιοδικά στην παγκόσμια ιστορία. Για παράδειγμα, η δημοκρατία της Ρώμης προσκαλούσε τα παιδιά γειτονικών κρατών να σπουδάσουν και να μορφωθούν στην πρωτεύουσα της αυτοκρατορίας, η μεγάλη αλεξανδρινή βιβλιοθήκη που ανεγέρθηκε από τους Έλληνες προσέφερε ειδικά προγράμματα επιμόρφωσης σε ξένους σπουδαστές από όλο τον αρχαίο γνωστό κόσμο και ο Ναπολέοντας όταν εισέβαλε στην Αίγυπτο είχε στις προθέσεις του να ασπαστεί όλος ο Γαλλικός στρατός την Ισλαμική πίστη ώστε να εδραιωθεί ευκολότερα ο Γαλλικός Νόμος. [65] Η αμερικάνικη επίσης διπλωματία κοινού έχει να επιδείξει μία μακρά γενεαλογία. Είναι γενικό αποδεκτό ότι η πρώτη πράξη της Αμερικάνικης Επανάστασης, η διακήρυξη της Ανεξαρτησίας, ήταν αναμφίβολα μία άσκηση διπλωματίας κοινού που είχε ως στόχο να διαφημίσει το νέο έθνος που γεννιόταν στους πολίτες των άλλων κρατών. Όσον αφορά την πιο σύγχρονη ιστορία, ανάλογες δραστηριότητες -αλλά πιο συστηματοποιημένες και θεσμικά κατοχυρωμένες αυτή τη φορά- υλοποιούνται κατά τη διάρκεια των δύο παγκοσμίων πολέμων με κύριους φορείς και εκφραστές τέτοιων πρακτικών την αμερικάνικη και την αγγλική κυβέρνηση. Ο πρόεδρος Woodrow Wilson συνέστησε κατά τον Α΄ ΠΠ την **επιτροπή της πληροφόρησης του κοινού *(The creel Committee[66])***. Αυτή η επιτροπή αποτέλεσε την πρώτη σημαντική προσπάθεια των Ηνωμένων Πολιτειών να διαδώσουν ευρέως πληροφοριακό υλικό τόσο σε εσωτερικά όσο και ξένα ακροατήρια και να αντιμετωπίσουν αποτελεσματικά τη γερμανική προπαγάνδα. Με βάση την συγκεκριμένη εμπειρία δημιουργήθηκε και το γραφείο πληροφοριών πολέμου από τον πρόεδρο Φραγκλίνο Ρούσβελτ το Ιούνιο του 1942. Η υπηρεσία αυτή χρησιμοποιούσε φωτογραφίες με σκοπό να προμηθεύει φίλια και εχθρικά ακροατήρια με πολεμικά νέα και πληροφορίες σχετικές με τις πολιτικές των ΗΠΑ και να ενσπείρει τον πατριωτικό ζήλο στις τάξεις του Αμερικάνικου κοινού. Στα προϊόντα της συγκεκριμένης επιτροπής συγκαταλέγονταν αφίσες, ανακοινώσεις τύπου, ραδιοφωνικές εκπομπές ακόμη και κινηματογραφικές ταινίες. Επίσης, μία από τις πιο καταλυτικές και διαρκείς δράσεις του συγκεκριμένου γραφείου ήταν και η σύσταση της <<*Φωνής της Αμερικής*>> το 1942. Η Φωνή της Αμερικής συνεχίζει να μεταδίδει νέα απ' όλο τον κόσμο ακόμη και σήμερα. Οι πρώτες της εκπομπές αφορούσαν πολεμικές ανταποκρίσεις που αναμεταδίδονταν μέχρι τον Ειρηνικό Ωκεανό, την κατεχόμενη Ευρώπη και τη Νότια Αφρική.

Κατά την περίοδο του Ψυχρού Πολέμου η στρατηγική επικοινωνία των ΗΠΑ είναι εναρμονισμένη με τη μεταβατική πορεία που συνοδεύει το διεθνές σύστημα και τις αλλαγές στις ισορροπίες ισχύος που συντελούνται όλο αυτό το διάστημα. Σύμφωνα με τον ειδικό σε θέματα πολιτικών συγκρούσεων, Lowell Schwartz, οι πληροφοριακές προσπάθειες των ΗΠΑ υπό την καθοδήγηση του προέδρου Τρούμαν μπορούν να ταξινομηθούν σε τρεις διακριτές κατηγορίες-στάδια. Καταρχάς, αμέσως μετά τη λήξη του Β΄ ΠΠ υπήρξαν αποφάσεις που απονεύρωσαν βασικές

[64] Nicholas J. Cull "Public Diplomacy before Gull ion: The Evolution of a Phrase" , New York : Routledge, 2009, p.19

[65] Stefanie Babst, Public Diplomacy-The Art of Engaging and Influencing, Speech at NATO PfP Symposium, January 22, 2009.

[66] Kennon H. Nakamura and Matthew C. Weed, U.S. Public Diplomacy: Background and Current Issues, December 18, 2009, p. 9.

ικανότητες των ΗΠΑ να διεξάγουν ουσιαστικές επιχειρήσεις επηρεασμού του αντιπάλου.[67] Το δεύτερο στάδιο συνέπεσε με το ξεκίνημα του Ψυχρού Πολέμου και περιέλαβε την ανάπτυξη νέων ικανοτήτων στη βάση της υλοποίησης του σχεδιασμού του George Kennan για αντιμετώπιση της Σοβιετικής προπαγάνδας. [68]Για να είναι πιο αποτελεσματικό αυτό το σχέδιο ο Kennan απαίτησε να αναπτύξουν οι ΗΠΑ όλα τα διαθέσιμα μέσα για να πετύχουν τους εθνικούς τους σκοπούς, τόσο φανερές ενέργειες(π.χ. πολιτικές συμμαχίες, οικονομικά μέτρα, <<λευκή προπαγάνδα>>) όσο και συγκεκαλυμμένες δραστηριότητες (μαύρο ψυχολογικό πόλεμο) που στόχευαν στο να υποκινήσουν και ενθαρρύνουν εξεγέρσεις σε εχθρικές χώρες. Τέλος στο τρίτο στάδιο έλαβε χώρα <<μία προπαγανδιστική εκστρατεία αλήθειας>> που συνιστούσε μία πραγματική σταυροφορία εναντίον του κομμουνισμού.[69]

Ένας βασικός οργανισμός που γεννήθηκε και ανδρώθηκε κατά τη διάρκεια του Ψυχρού Πολέμου και ήταν υπεύθυνος για την εκτέλεση και των συντονισμό ενεργειών που σήμερα θα τις αποκαλούσαμε διπλωματία με το κοινό, ήταν η Υπηρεσία Ενημέρωσης των ΗΠΑ. (United States Information Agency). Δημιουργήθηκε από τον πρόεδρο Αϊζενχάουερ το 1953 με σκοπό να διεξάγει διεθνείς πληροφοριακές δραστηριότητες προς υποστήριξη της εξωτερικής πολιτικής των ΗΠΑ. Σύμφωνα με το ιδρυτικό καταστατικό της υπηρεσίας, αποστολή της ήταν να *<<κατανοήσει, πληροφορήσει και επηρεάσει ξένα ακροατήρια με σκοπό την προώθηση του εθνικού συμφέροντος και να διευρύνει το διάλογο μεταξύ των Αμερικάνων και των συνεταίρων τους στο εξωτερικό.>>*[70] *Η* Υπηρεσία Ενημέρωσης ανέλαβε σε αυτό το πλαίσιο δράσης τη διαχείριση της <<Φωνής της Αμερικής>> αλλά χρησιμοποίησε επίσης και άλλα μέσα επικοινωνίας όπως συναισθηματικές εικόνες, τηλεοπτικά προγράμματα, διανομή φυλλαδίων κλπ. Πολλές από τις παραπάνω δραστηριότητες αποτέλεσαν στην ουσία το θεμέλιο λίθο γι' αυτό που στις μέρες μας ονομάζεται διπλωματία με το κοινό.

Με το τέλος του Ψυχρού Πολέμου και την πτώση του υπαρκτού Κομμουνισμού δημιουργείται ένα κλίμα ευφορίας για επικράτηση της ειρήνης σε πλανητική κλίμακα, γεγονός που καθιστά αυτόματα πολύ λιγότερο απαραίτητες για τον κρατικό μηχανισμό τις συγκεκριμένες υπηρεσίες οι οποίες χάνουν την διοικητική τους αυτονομία και μεταβιβάζουν σταδιακά πολλές από τις αρμοδιότητες τους σε άλλους φορείς. Παράλληλα, συρρικνώνεται δραστικά ο οικονομικός τους προϋπολογισμός και περιορίζεται συνολικά ο ρόλος τους στο κεντρικό κυβερνητικό σχεδιασμό . Ωστόσο, τα γεγονότα της 9/11 σύντομα θα έρθουν να διαψεύσουν τις όποιες προσδοκίες καλλιεργήθηκαν τα μεταβατικά αυτά χρόνια και να δώσουν νέα ώθηση στο αντικείμενο της στρατηγικής επικοινωνίας.

## 5.2 ΟΡΙΣΜΟΣ ΚΑΙ ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

Μία από τις πιο σημαντικές προκλήσεις που εμφανίζει το αντικείμενο της στρατηγικής επικοινωνίας είναι η αδυναμία ή η ασυμφωνία να υπάρξει ένας κοινός ορισμός μεταξύ των ειδικών που να περιγράφει με ακρίβεια και ευκρίνεια το αντικείμενο και τον σκοπό της. Ενώ φαίνεται να υφίσταται μία

[67] Lowell H. Schwartz Political Warfare against the Kremlin: US and British Propaganda Policy at the Beginning of the Cold War, Hampshire UK : Palgrave, Macmillan, 2009, p. 96
[68] Lowell H. Schwartz Political Warfare against the Kremlin, p.96
[69] Lowell H. Schwartz Political Warfare against the Kremlin, p.97
[70] U.S. Information Agency (USIA), "Overview: 1998".

ευρεία αποδοχή σχετικά με τον πυρήνα της έννοιας, υπάρχουν ωστόσο αρκετές λεπτομέρειες στη δομή της που γίνονται αντιληπτές με διαφορετικό τρόπο από διαφορετικά κοινά, με αποτέλεσμα να προκύπτει αρκετές φορές σύγχυση σχετικά με τους ρόλους που της ανατίθενται και την αποστολή που έχει και πρέπει να εκτελέσει. Για παράδειγμα, είναι πολύ συνηθισμένο να θεωρείται η στρατηγική επικοινωνία ταυτόσημη έννοια με τη διπλωματία κοινού ή με τις πληροφοριακές επιχειρήσεις, ενώ στην πραγματικότητα οι παραπάνω δραστηριότητες αποτελούν υποσύνολα της και συνιστούν διακριτές εννοιολογικές οντότητες με συμπληρωματικό αλλά όχι το ίδιο ακριβώς περιεχόμενο. Πάντως σε γενικές γραμμές και ανεξάρτητα από τις επί μέρους διαφορετικές ερμηνευτικές αντιλήψεις, όλοι οι ορισμοί οι οποίοι έχουν κατά καιρούς διατυπωθεί μπορούν να ταξινομηθούν σε δύο γενικές κατηγορίες: Σε εκείνους που προέρχονται από επίσημους κυβερνητικούς οργανισμούς και υπηρεσίες και σε εκείνους που έχουν κατατεθεί από ανεπίσημους φορείς ή ιδιώτες ακαδημαϊκούς και ερευνητές που είναι εξειδικευμένοι σε θέματα επικοινωνίας και δημοσιών σχέσεων.

Αναφορικά με την πρώτη πηγή προέλευσης, μπορούν να σταχυολογηθούν ως σημαντικότεροι και πιο αντιπροσωπευτικοί οι ορισμοί του ανευρίσκονται σε ειδικές εκδόσεις τόσο του υπουργείου Άμυνας των ΗΠΑ και όσο και του γραφείου του Λευκού Οίκου που ασχολείται με το υπό συζήτηση θέμα. Στη διακλαδική έκδοση 1-02 του στρατιωτικού λεξικού του υπουργείου άμυνας, η στρατηγική επικοινωνία ορίζεται ως *«η εστιασμένη προσπάθεια της κυβέρνησης των ΗΠΑ στην κατανόηση και ενασχόληση με συγκεκριμένα ακροατήρια-κοινά με απώτερο στόχο την δημιουργία, ενδυνάμωση και συντήρηση των συνθηκών εκείνων που είναι απαραίτητες για την προώθηση των συμφερόντων και των πολιτικών της Αμερικής, διαμέσου συντονισμένων προγραμμάτων, σχεδίων, μηνυμάτων και προϊόντων συγχρονισμένων με ενέργειες όπου εμπλέκονται όλα τα όργανα της εθνικής ισχύος.»* [71] Επίσης, σύμφωνα με το εθνικό πλαίσιο του Λευκού Οίκου για την στρατηγική επικοινωνία που συντάχθηκε το 2010 με σκοπό να ξεδιαλύνει τις ασάφειες γύρω από τον όρο, *«η στρατηγική επικοινωνία αναφέρεται στον συγχρονισμό λέξεων και πράξεων και στον τρόπο που οι παραπάνω γίνονται αντιληπτές από επιλεγμένα ακροατήρια, όπως επίσης σε προγράμματα και δραστηριότητες σκόπιμα στοχευμένες στην επικοινωνία και την προσέγγιση με συγκεκριμένα κοινά που συμπεριλαμβάνουν τις δημόσιες σχέσεις, τη διπλωματία με το κοινό και τις πληροφοριακές επιχειρήσεις που διεξάγονται από εξειδικευμένο προσωπικό.»* [72] Ένας παρόμοιος αλλά σαφώς και πιο επεξηγηματικός ορισμός με προέλευση τη διακλαδική ενοποιημένη πρόταση του υπουργείου εθνικής άμυνας των ΗΠΑ που κατατέθηκε το 2009 δίνει το δικό του στίγμα, εξηγώντας την στρατηγική επικοινωνία *«ως τη διάχυση μηνυμάτων με σκοπό την εξυπηρέτηση στρατηγικών εθνικών αντικειμενικών σκοπών. Μία τέτοια ενέργεια είναι αμφίδρομη, δηλαδή περιέχει τόσο την ακρόαση όσο και τη μετάδοση των μηνυμάτων. «Βρίσκει εφαρμογή όχι μόνο στο επίπεδο των πληροφοριών αλλά επίσης και στη φυσική επικοινωνία η οποία από μόνη της μεταφέρει νοήματα.»*[73] Στο ίδιο τέλος μήκος κύματος κινούνται και οι ερμηνευτικές προσεγγίσεις

[71] Department of Defense, Dictionary of Military and Associated Terms, Washington, D.C., Joint Publication 1-02, April 12, 2001, p.448.
[72] The White House, National Framework for Strategic Communication, Washington, D.C., March 2010, p. 2.
[73] United States Department of Defense, Strategic Communication Joint Integrating Concept, p. 2.

ειδικών που χρημάτισαν κατά καιρούς σε κομβικές θέσεις στο κυβερνητικό μηχανισμό των ΗΠΑ όπως π.χ. του υφυπουργού άμυνας για τις πληροφορίες Steve Cambone ο οποίος χαρακτηρίζει την στρατηγική επικοινωνία σαν *«μία διαδικασία, συγκεκριμένα τον συντονισμό ανόμοιων επιχειρήσεων, δραστηριοτήτων και άλλων προσπαθειών για να επιτευχθούν οι εθνικοί και πολιτικοί αντικειμενικοί σκοποί.»*[74] .

Το πρώτο κοινό στοιχείο που παρατηρούμε με μία πρώτη ανάγνωση σε όλους τους παραπάνω ορισμούς είναι ***η σημασία που αποδίδεται στον επηρεασμό ή πιο γενικά στη διαδραστική επικοινωνία με την κοινή γνώμη, στα πλαίσια πάντα επιδίωξης και εξυπηρέτησης του γενικότερου εθνικού συμφέροντος. Θα μπορούσαμε να πούμε ότι η δυνατότητα εποικοδομητικής επικοινωνίας με συγκεκριμένα ακροατήρια ανθρώπων και η ικανότητα επηρεασμού τους, σε βαθμό τέτοιο που να μετριάζει τις αρνητικές εικόνες που παράγονται από εσφαλμένες και άστοχες πολιτικές ενέργειες, να ουδετεροποιεί στο μέτρο του δυνατού εχθρικές στάσεις και να προδιαθέτει έτσι πιο φιλικά για τις δικές μας δράσεις όπου και όταν αυτές αναπτύσσονται, είναι πολύ σημαντική και βρίσκεται στον πυρήνα λειτουργίας αυτής της διαδικασίας. Ο σχεδιασμός αυτός όμως πρέπει να απορρέει από διαυγείς και κεντρικούς αντικειμενικούς πολιτικούς σκοπούς και αυτό είναι το στοιχείο που καθιστά αυτομάτως την στρατηγική επικοινωνία «στρατηγική». Η πληροφόρηση, ο επηρεασμός και η προσπάθεια πειθούς συγκεκριμένων κοινών, ενεργειών δηλαδή που περιγράφονται με παρόμοιες φράσεις στους παραπάνω ορισμούς και αποτελούν την ουσιαστική λειτουργία της στρατηγικής επικοινωνίας, απαιτούν κάθε φορά έναν κεντρικό στρατηγικό σχεδιασμό σε κυβερνητικό επίπεδο ώστε να αποδώσουν τα προσδοκώμενα οφέλη.***

Τα οφέλη αυτά είναι πολλαπλά και ιδιαίτερα σημαντικά ιδιαίτερα στο ψηφιακό κόσμο που ζούμε σήμερα και συνδέονται στενά και με τις στρατιωτικές επιχειρήσεις. Σε ένα συμπόσιο που διοργανώθηκε το 2008 στη Στρατιωτική Βάση Συνδυασμένων Όπλων στην τοποθεσία Leavenworth των ΗΠΑ με θέμα τις πληροφορίες και τον κυβερνοχώρο, διατυπώθηκε η άποψη ότι *«η αποτυχία ή η επιτυχία των επιχειρήσεων στο έδαφος βρίσκεται σε άμεση συνάφεια με την εικόνα που σχηματίζουν οι αντίπαλες πληθυσμιακές ομάδες ανθρώπων που διαβιούν στις περιοχές όπου αυτές λαμβάνουν χώρα».* [75] Ο στρατηγός Peter Chiarreli αναπαράγοντας και συνοψίζοντας τις γνώμες που αναπτύχθηκαν στο εν λόγω συνέδριο, έγραψε σε ένα άρθρο της Στρατιωτικής Επιθεώρησης τα παρακάτω : *« Ενώ η απόφαση να αναπτυχθούν στρατιωτικές δυνάμεις έχει ληφθεί, για όλους εμάς που φοράμε στολή πρέπει να γίνει κατανοητό πως το πιο αποφασιστικό στοιχείο για την τελική επικράτηση, πιο συχνά ίσως από ποτέ, στις περισσότερες μοντέρνες συγκρούσεις, δεν είναι οι δυνάμεις ελιγμού. Ενώ πρέπει να διατηρήσουμε την ανταγωνιστικότητά μας να επιβληθούμε στον εχθρό με τις συμβατικές δυνάμεις, πρέπει επίσης να είμαστε ικανοί να προσφέρουμε στους πληθυσμούς των χωρών που επηρεάζονται από τον πόλεμο την ελπίδα ότι η ζωή τους και η ζωή των παιδιών τους, θα γίνει καλύτερη εξαιτίας της παρουσίας μας.*

---

[74] Dennis Murphy, "Strategic Communication", in Department of Military Strategy, Planning and Operations Center for Strategic Leadership, Information Operations Primer, Carlisle, Pa.: U.S. Army War College, November 2009, p.29.

[75] U.S. Army Combined Arms Center, Information & Cyberspace Symposium, Fort Leavenworth, April 15-18, p. 5

*Με άλλα λόγια, σε αντίθεση με την ιδέα ότι η βία πάντα νικά στο τέλος, πρέπει να κατανοήσουμε ότι όλα τα προβλήματα δεν λύνονται τελικά με την κάνη ενός όπλου.»*[76] Στο ίδιο μήκος κύματος, το επιφορτισμένο με τις πληροφοριακές δραστηριότητες τμήμα του υπουργείου άμυνας των ΗΠΑ προέβη το 2009 σε μία εκτίμηση σχετικά με το ρόλο που θα έχει η στρατηγική επικοινωνία στο ολοένα και πιο περίπλοκο πληροφοριακό περιβάλλον του 21ου αιώνα, καταλήγοντας επιγραμματικά στα ακόλουθα συμπεράσματα: <<*Η μορφή του πολέμου συνεχώς αλλάζει. Ενώ αυτή η ιδέα έχει αποδείξει την επαληθευσιμότητά της κατά το ρου της ιστορίας και η διατύπωσή της δεν αποτελεί παρά μία κοινοτυπία, ωστόσο υπάρχει μία έντονη φιλολογία ότι η εικόνα που σχηματίζει το κοινό για τις στρατιωτικές δράσεις, θα εκτοπίσει προοδευτικά τα ορατά οφέλη που μπορούν να αποκομίσουν πρακτικά οι ένοπλες δυνάμεις από πραγματικές συγκρούσεις στο πεδίο της μάχης*>>.[77] Η τελευταία φράση είναι ιδιαίτερα σημαντική και αναδεικνύει την αξία και το ρόλο που έχει να επιτελέσει η στρατηγική επικοινωνία στο σύγχρονο πεδίο της μάχης. Η δυνατότητα ενός κράτους να οργανώνει και να διευθύνει αποτελεσματικά επιχειρήσεις επιρροής συνιστά πρόκριμα εθνικής υπεροχής μέσα στο διεθνές σύστημα το οποίο διαμορφώνεται όπως γνωρίζουμε κυρίως από τις δράσεις των κυρίαρχων και ανεξάρτητων κρατών-μελών. Αποτελεί πχ ιστορικό κεκτημένο και χωρίς να υποτιμόνται οι συσχετισμοί ένοπλης ισχύος, πως οι αποτελεσματικές πληροφοριακές επιχειρήσεις που εκτέλεσαν οι ΗΠΑ κατά τη διάρκεια του Ψυχρού Πολέμου, συνεισέφεραν σε μεγάλο βαθμό στη τελική τους νίκη. Επίσης, σε μία έκθεση του Rand Corporation που δημοσιεύτηκε το 2010 εξετάστηκε η συνεισφορά της στρατηγικής επικοινωνίας σε 30 επιχειρήσεις εναντίον ανταρτών που έλαβαν χώρα μεταξύ των ετών 1978-2008 . Η έρευνα κατέληξε στο συμπέρασμα ότι η επιτυχία σε τέτοιου είδες ενέργειες εξαρτάται από παράγοντες που συνδέονται με τις δραστηριότητες στρατηγικής επικοινωνίες που διεξάγουν οι δυνάμεις κατά των ανταρτών.[78] Αντίθετα, καμιά στρατιωτική νίκη δεν είναι εφικτή αν δεν συνδυάζεται και με το όραμα μίας μεταπολεμικής ανοικοδόμησης και κυρίως αν δεν κατευνάζει τα εχθρικά αισθήματα του ντόπιου πληθυσμού. Οι συμπεριφορές που δημιουργούν την «αίσθηση του κατακτητή» γενούν αντανακλαστικά αντιδράσεις και ριζοσπαστικοποιούν τα πιο ενεργά τμήματα της κοινωνίας, γεγονός που στο τέλος μεγενθύνει το κόστος του πολέμου υπέρμετρα και καθιστά ασύμφορη την όποια στρατιωτική δράση. Τα λόγια του στρατηγού Chiarreli αντικατοπτρίζουν σε μεγάλο βαθμό μία βασική αρχή της στρατηγικής επικοινωνίας, που συνοψίζεται στη φράση ότι ***«οι πράξεις μιλάνε πολύ πιο δυνατά από τις λέξεις».*** Κάτι τέτοιο εξάλλου αναφέρεται ρητά και στον ορισμό που προέρχεται από το κείμενο που συντάχθηκε από το Λευκό Οίκο το 2010, ότι δηλαδή η στρατηγική επικοινωνία αναφέρεται στον **συγχρονισμό λέξεων και πράξεων** και στον τρόπο που οι παραπάνω γίνονται αντιληπτές από επιλεγμένα ακροατήρια. Επίσης, στο ίδιο κείμενο τονίζεται εμφατικά ότι *«Κάθε ενέργεια που εκτελείται από την*

---

[76] Peter M. Chiarreli, "Learning from Our Modern Wars: The Imperatives of Preparing for a Dangerous Future," Military Review, September-October 2007, p. 6.

[77] Bruce Gregory, "Public Diplomacy and National Security :Lessons from the U.S. Experience", Small Wars Journal, August 14, 2008, p.6

[78] Christopher Paul, "Strategic Communication, Origins, Concepts and Current Debates" (Santa Barbara, California) page 79.

*κυβέρνηση των ΗΠΑ στέλνει ένα αντίστοιχο μήνυμα».*[79] Οι εφαρμογές στρατηγικής επικοινωνίας επομένως που περιλαμβάνουν μόνο τα παραδοσιακά μέσα επικοινωνίας, όπως τις ανακοινώσεις τύπου, τις αποστολές μηνυμάτων, τις σχέσεις με τα ΜΜΕ κλπ είναι καταδικασμένες σε αποτυχία. Αυτή η παραδοχή ισχύει ακόμη και στην περίπτωση που χρησιμοποιούνται μη παραδοσιακά μέσα όπως π.χ. το διαδίκτυο, οι νέες τεχνολογίες κοινωνικής δικτύωσης και η προσωπική επαφή. Αντίθετα, μία επιτυχημένη εκστρατεία βασίζεται σε όλο το επικοινωνιακό περιεχόμενο, δηλαδή σε πράξεις, πολιτικές, μηνύματα και εικόνες. Οι πράξεις δεν περιορίζονται σε συγκεκριμένες πολιτικές δράσεις που κατευθύνονται μόνο από επίσημους κυβερνητικούς φορείς αλλά περιλαμβάνουν προσωπικές συμπεριφορές και ενέργειες μελών και αντιπροσώπων της κυβέρνησης και φυσικά το προσωπικό των ενόπλων δυνάμεων. Κάθε ενέργεια, μήνυμα, και κίνηση των ενόπλων δυνάμεων ενός έθνους διαμορφώνει τις αντιλήψεις και τις γνώμες τόσο του πληθυσμού που διαβιεί στη περιοχή των επιχειρήσεων όσο και του ευρύτερου κόσμου. Επομένως, η εικόνα που έχουν σχηματίσει κάποιοι να θεωρούν την στρατηγική επικοινωνία σαν μία απλή διάδραση με τα μέσα επικοινωνίας που εξαντλείται σε ανακοινώσεις τύπου και επίσημες δηλώσεις αξιωματούχων της κυβέρνησης, είναι εντελώς εσφαλμένη.

Μία δεύτερη βασική αρχή που πρέπει να επισημανθεί, είναι ότι η στρατηγική επικοινωνία αποτελεί μία αμφίδρομη διαδικασία που δεν εξαντλείται μόνο στη μετάδοση μηνυμάτων, αλλά αφουγκράζεται και τον τρόπο που αυτά μεταφράζονται και προσλαμβάνονται από τα ακροατήρια στα οποία καταλήγουν. Αυτό οφείλεται στο γεγονός ότι όλα σχεδόν τα μηνύματα που μεταφέρονται, έχουν σαν κύριο χαρακτηριστικό τους την αποσπασματικότητα, επειδή οι πληροφορίες που περιέχονται σε αυτά είναι ανοικτές σε ποικίλες πολιτιστικές και πολιτικές ερμηνείες, ανάλογα με το πολιτιστικό, θρησκευτικό και κοινωνικό υπόβαθρο του κοινού που τα υποδέχεται. Σε αντίθεση έτσι με τα γραμμικά επικοινωνιακά μοντέλα του περασμένου αιώνα που προϋποθέτουν απλά την ύπαρξη ενός πομπού, ενός μέσου που θα διαχύσει το μήνυμα και ενός παθητικού δέκτη, η αληθινή πρόκληση για την στρατηγική επικοινωνία είναι όχι να αναπτύξει το σωστό μήνυμα για ένα ακροατήριο, αλλά να δημιουργήσει ένα καλύτερο γνωστικό υπόβαθρο για το κάθε κοινό, βασισμένο σε θρησκευτικά, κοινωνικά, πολιτικά, πολιτιστικά και τοπικά κριτήρια, έτσι ώστε να είναι στο μέτρο του δυνατού προβλέψιμο το πώς πρόκειται να μεταφραστεί το κάθε μήνυμα όταν παραληφθεί από τους αποδέκτες του, σε έναν ολοένα μεταβαλλόμενο και εξελισσόμενο κόσμο.

Για να ανταποκριθεί στον σύνθετό της ρόλο η στρατηγική επικοινωνία βασίζεται σε μία πλειάδα άλλων **υποστηρικτικών ικανοτήτων** που σχετίζονται με δραστηριότητες επικοινωνίας, πληροφόρησης και επηρεασμού μίας ομάδας ανθρώπων όπως π.χ. δημοσίων σχέσεων, σχέσεων με τον τύπο, διπλωματίας με το κοινό, ψυχολογικών επιχειρήσεων κλπ. Οι παραπάνω ικανότητες προσδίδουν **στην στρατηγική επικοινωνία το χαρακτήρα περισσότερο μίας διαδικασίας παρά μίας αυτόνομης υπηρεσίας με δικό της στελεχιακό δυναμικό, προϋπολογισμό, τμήμα σχεδιασμού κλπ.** Η αποστολή της δηλαδή έγκειται στο συγχρονισμό και συντονισμό όλων

[79] The White House, National Framework for Strategic Communication, Washington, D.C., March 2010, p. 3.

αυτών των «εξαρτημάτων» αφού οι υποδομές για να μεταφερθεί το μήνυμα ήδη υπάρχουν και αυτό που πραγματικά χρειάζεται είναι μία διαδικασία ενοποίησης τους με στόχο πάντα την εξυπηρέτηση του γενικότερου εθνικού συμφέροντος. Κάτι τέτοιο αναφέρεται και στην έκθεση του υπουργείου Εθνικής Άμυνας των ΗΠΑ του 2009 όπου τονίζεται ότι η στρατηγική επικοινωνία *«θα πρέπει να θεωρείται μάλλον μια διαδικασία παρά μία ομάδα οργανισμών, διακριτών δραστηριοτήτων και ικανοτήτων. Σε μία ευρύτερη σύλληψη είναι η μετατροπή των θεμάτων που απασχολούν το ακροατήριο και την κοινή γνώμη σε αποτελεσματικό σχεδιασμό και υλοποίηση πολιτικών αποφάσεων σε κάθε επίπεδο.»*[80]

## 5.3 ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ ΣΚΟΠΟΙ ΣΤΡΑΤΗΓΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

Ένας από τους κύριους λόγους διαφωνίας σχετικά με τον ακριβή ορισμό της στρατηγικής επικοινωνίας είναι η αδυναμία να χαραχτεί μία κοινή συνισταμένη που να καθορίζει επακριβώς τις αποστολές που έχει να εκπληρώσει. Όπως διατείνεται ο ακαδημαϊκός John Robert Kelley, «η στρατηγική επικοινωνία περιπλέκεται από την ύπαρξη ανταγωνιστικών στόχων».[81] Υπάρχουν αρκετές διχογνωμίες σχετικά με τους πρωταρχικά επιδιωκόμενους σκοπούς, τα χρονοδιαγράμματα και τους τρόπους υλοποίησης τους. Επιπλέον, η σύγχυση αυτή επεκτείνεται από το γεγονός ότι πολλοί από τους σκοπούς δεν αποτελούν αποκλειστικό αντικείμενο ενασχόλησης της στρατηγικής επικοινωνίας. Παρακάτω αναλύονται οι σημαντικότεροι από αυτούς.

**Εθνικοί Αντικειμενικοί Σκοποί.**

Πολλοί μελετητές θεωρούν ότι αποκλειστική στόχευση της στρατηγικής επικοινωνίας είναι οι εθνικοί αντικειμενικοί σκοποί, η εθνική στρατηγική και το εθνικό πολιτικό συμφέρον. Αυτό είναι που την καθιστά πραγματικά «στρατηγική». Σύμφωνα με την επίσημη θέση του υπουργείου εθνικής άμυνας των ΗΠΑ, *«Οι προτεραιότητες της στρατηγικής επικοινωνίας δεν είναι ούτε ξεχωριστές, ούτε διακριτές από τους εθνικούς πολιτικούς στόχους. Η διαδικασία αυτή είναι σχεδιασμένη για να υποστηρίξει την κυβέρνηση των ΗΠΑ και τους πολιτικούς σκοπούς του υπουργείου εθνικής άμυνας: δηλαδή την εθνική στρατηγική ασφαλείας, την εθνική στρατηγική άμυνας, την εθνική στρατιωτική στρατηγική και την καθοδήγηση των δυνάμεων που αναπτύσσονται για να εξυπηρετήσουν πρωταρχικούς πολιτικούς σκοπούς».*[82]

**Επιχειρησιακοί Αντικειμενικοί Σκοποί.**

Σύμφωνα με την επιθυμία ορισμένων μελετητών, η στρατηγική επικοινωνία πρέπει να εξυπηρετεί εθνικούς στόχους αλλά οι στόχοι αυτοί είναι δυνατόν να συνδέονται με υποδεέστερες ή ένθετες αποστολές που εντοπίζονται στο επιχειρησιακό ή ακόμη και τακτικό επίπεδο. Εάν για παράδειγμα ο εθνικός σκοπός των επιχειρήσεων που εκτέλεσαν οι ΗΠΑ στο Αφγανιστάν ήταν η ήττα των ανταρτών Ταλιμπάν και η σταθεροποίηση της νέας κυβέρνησης, τότε η στρατηγική επικοινωνία θα μπορούσε να χρησιμοποιηθεί σαν εργαλείο για να υποστηριχθούν δευτερεύοντες επιχειρησιακοί σκοποί σε περιοχές όπως την Κανταχάρ. Μία τέτοια άποψη φιλοξενείται και στο αμερικάνικο εγχειρίδιο του διοικητή για την στρατηγική επικοινωνία όπου ρητά αναφέρεται ότι: *«Η χρήση του όρου "στρατηγική" επικοινωνία συχνά*

---

[80] Department of Defense, Report on Strategic Communication, Washington, D.C., December 2009, p. 1.

[81] John Robert Kelley " Between Take-Offs and Crash Landings", p.2.

[82] Department of Defense, Report on Strategic Communication, p.5.

*δημιουργεί λανθασμένους συνειρμούς ότι η συγκεκριμένη διαδικασία βρίσκει εφαρμογή μόνο στο στρατηγικό επίπεδο. Παρά ταύτα, κάθε επίπεδο διοίκησης χρειάζεται μία στρατηγική για τον συντονισμό και τον συγχρονισμό θεμάτων, μηνυμάτων, εικόνων και δράσεων για την υποστήριξη σκοπών που σχετίζονται με την επικοινωνία και την εξασφάλιση της ενότητας μηνυμάτων και θεμάτων στο κατώτατο τακτικό επίπεδο. Αυτή η στρατηγική πρέπει να συντονίζεται με τις παρόμοιες δράσεις που υπόκεινται, υπέρκεινται ή βρίσκονται στο ίδιο με αυτήν επίπεδο ώστε να μεταφέρεται ένα αμοιβαία υποστηριζόμενο «επικοινωνιακό πακέτο» στα στοχευόμενα ακροατήρια.»* [83]

**Υποστήριξη Συγκεκριμένων Ρόλων/Σκοπών/Πολιτικών.**

Η χρήση της στρατηγικής επικοινωνίας για την υποστήριξη συγκεκριμένων πολιτικών αποτελεί πάγια τακτική που διακατέχει τη φιλοσοφία του Ηνωμένου Βασιλείου. Αυτή η προσέγγιση αναγνωρίζει ότι οι συγκεκριμένες πολιτικές συνήθως εμπεριέχονται μέσα σε ευρύτερους εθνικούς σκοπούς αλλά ταυτόχρονα λαμβάνει υπ' όψη ότι οι πόροι για την επικοινωνία είναι περιορισμένοι και επομένως απαιτείται πολύ καλός συντονισμός ώστε να υπάρξουν τα επιθυμητά επικοινωνιακά αποτελέσματα με τη χρήση μίας λελογισμένης δαπάνης.[84]

**Δημιουργία Θετικών Στάσεων σε Βάθος Χρόνου.**

Πέρα από στόχους που είναι αποκλειστικά συνδεδεμένοι με σκοπούς εθνικούς, επιχειρησιακούς και τακτικούς, η στρατηγική επικοινωνία μπορεί να χρησιμοποιηθεί για να πραγματωθούν πιο μακροπρόθεσμες επιδιώξεις που σχετίζονται με τη δημιουργία θετικών στάσεων της κοινής γνώμης απέναντι στην εικόνα, την αξιοπιστία και τις εφαρμοζόμενες πολιτικές ενός κράτους διεθνώς. Το ζήτημα της απόκτησης και της διατήρησης της αξιοπιστίας ενός κράτους στο διεθνή στίβο είναι εξαιρετικά σημαντικό και αφορά τόσο την εσωτερική όσο και εξωτερική νομιμοποίηση των πολιτικών του δράσεων. Η σφυρηλάτηση και η οικοδόμηση εμπιστοσύνης με το ξένο ακροατήριο στην παγκοσμιοποιημένη εποχή που διανύουμε είναι μία μακροχρόνια και επίπονη διαδικασία και δεν εξασφαλίζεται με την απλή μετάδοση μηνυμάτων και εικόνων. Οι οργανωμένες πολιτικές δράσεις είναι κυρίως αυτές που διαμορφώνουν την εικόνα ενός κράτους στα μάτια της κοινής γνώμης. Οι δράσεις αυτές, ανάλογα και με τα αποτελέσματα που παράγουν, καταχωρούνται με αρνητικό ή θετικό πρόσημο στο συλλογικό υποσυνείδητο μίας κοινωνίας, διαμορφώνοντας αντίληψη και εικόνα για το ρόλο που διαδραματίζει κάθε έθνος διεθνώς και σε βάθος χρόνου συχνά μετουσιώνονται σε εχθρικές ή φιλικές αντίστοιχα στάσεις. Κάτι τέτοιο φυσικά βρίσκει πεδίο εφαρμογής στο μέγιστο βαθμό και στις στρατιωτικές επιχειρήσεις. Σύμφωνα με τον ταγματάρχη Cliff Gilmore *«σε συγκρούσεις όπου οι τοπικοί πληθυσμοί καθορίζουν το αποτέλεσμα, τόσο η εμπιστοσύνη όσο και η αξιοπιστία, είναι ζωτικές για την στρατιωτική επιτυχία. Αν μία από τις δύο καταρρεύσει, τότε πιθανότατα η επιχείρηση θα αποτύχει.»*[85] Υπό αυτό το πρίσμα, εξηγείται πολλές φορές και η αδυναμία των ΗΠΑ να εξαργυρώσουν

[83] United States Joint Forces Command, Commander's Handbook for Strategic Communication and Communication Strategy, Suffolk Va.: United States Joint Forces Command Warfighting Center, Version 3.0, June 24, 2010. p. II-11.
[84] Defense Academy of the United Kingdom, Cranfield University, UK, March 2009.
[85] R.S. Zaharma, "The U.S. Credibility Deficit", Foreign Policy in Focus, December 13, 2006.

την συμβατική τους υπεροχή σε οπλικά συστήματα σε ουσιαστική νίκη στο πεδίο της μάχης. Το έλλειμμα αξιοπιστίας που ταλανίζει τα τελευταία χρόνια τις πολιτικές των ΗΠΑ σε πλανητικό επίπεδο στις οποίες συχνά παρατηρείται ανακολουθία και χάσμα μεταξύ λόγων και πράξεων, προθέσεων και τετελεσμένων γεγονότων, έχει αρνητικά αποτελέσματα που αντανακλούν σε μερικό βαθμό και στην εχθρότητα με την οποία αντιμετωπίζονται τα αμερικάνικα στρατεύματα στις περιοχές όπου αναπτύσσονται και στις δυσκολίες που συναντάνε για να ανοικοδομήσουν την σταθερότητα και την ειρήνη σε εμπόλεμες ζώνες.

Μεγάλη βοήθεια στο θέμα της απόκτησης και διατήρησης της αξιοπιστίας ενός κράτους μπορεί να προσφέρει η προβολή και η προώθηση κοινών αξιών. Οι κοινές αξίες πράγματι αποτελούν το ενδιάμεσο βήμα για την επιτυχία άλλων πιο μακροπρόθεσμων σκοπών. Αυξάνουν τη δυνατότητα αμοιβαίας κατανόησης διεθνώς και δημιουργούν αισθήματα συμπάθειας σε άλλες ομάδες ανθρώπων. Σύμφωνα με μία αναφορά της καθηγήτριας Kristin Lord για το ινστιτούτο Brookings το 2008, υπάρχουν δύο στρατηγικοί σκοποί που μπορεί να εξυπηρετήσει η στρατηγική επικοινωνία σε αυτό το πλαίσιο: α) η δημιουργία ενός κλίματος αμοιβαίας κατανόησης, σεβασμού και αλήθειας μέσα στο οποίο η συνεργασία φαντάζει πιο εφικτή και β) η προώθηση κοινών αξιών όπως η προστασία του περιβάλλοντος, η υποστήριξη της ελεύθερης αγοράς, το κράτος δικαίου κλπ που υποστηρίζουν διεθνώς τα Αμερικάνικα συμφέροντα.[86] Το ζήτημα των κοινών αξιών φαίνεται να είναι τόσο σπουδαίο που καταγράφεται ως ένας από τους τρεις θεμελιώδεις σκοπούς στην Εθνική Στρατηγική των ΗΠΑ για την Στρατηγική Επικοινωνία και τη Διπλωματία με το Κοινό. Σε αυτό το κείμενο επισημαίνεται ότι *«η Αμερική οφείλει να εργαστεί για να καλλιεργήσει κοινά ιδανικά και αξίες μεταξύ των Αμερικανών και ανθρώπων από διαφορετικές χώρες και διαφορετικό πολιτισμό και θρησκεία σε όλο τον κόσμο.»*[87]

Βέβαια, δε πρέπει να παραγνωριστεί το γεγονός, πως ανάμεσα στα μέλη της ακαδημαϊκής κοινότητας και με βάση και τις προηγούμενες αναφορές, το συγκεκριμένο θέμα παραμένει ανοικτό σε ποικίλες ερμηνείες και είναι εν πολλοίς αμφιλεγόμενο. Στον αντίποδα της παραπάνω θεώρησης, που τοποθετεί την στρατηγική επικοινωνία ουσιαστικά «οδηγό σε ένα όχημα ιδεολογικής διασποράς» βρίσκεται η άποψη όσων αμφισβητούν μία τέτοια προσέγγιση, προκρίνοντας την εφαρμογή της για την παραγωγή μόνο συγκεκριμένων στρατηγικών αποτελεσμάτων. Αντίθετα, ορισμένοι θα ήταν εξαιρετικά ευτυχείς αν η στρατηγική επικοινωνία χρησιμοποιούνταν για τη διάδοση και διάχυση κοινών αξιών οι οποίες μετά με την κατάλληλη μόχλευση από την παραδοσιακή διπλωματία θα μπορούσαν να μετατραπούν σε πιο απτά αποτελέσματα όπως τη μείωση της αντιπάθειας ή της αντίστασης στις εφαρμοζόμενες πολιτικές ενός κράτους.

**Πληροφοριακή Υπεροχή και Κυριαρχία.**

Ένας ακόμη πιθανός σκοπός της στρατηγικής επικοινωνίας συναρτά την ύπαρξή του με την στρατιωτική παρακαταθήκη των πληροφοριακών επιχειρήσεων που έχουν τις ρίζες τους στο πόλεμο διοίκησης και ελέγχου που πρωτοεμφανίστηκε στα τέλη του περασμένου αιώνα. Ο σκοπός αυτός είναι η

[86] Kristin M. Lord, Voices of America: U.S. Public Diplomacy for the 21st Century, Washington D.C.: The Foreign Policy Program at Brookings, 2008, p.14

[87] Strategic Communication and Public Diplomacy Policy Coordinating Committee, U.S. National Strategy for Public Diplomacy and Strategic Communication, p.3.

«πληροφοριακή υπεροχή» ή «πληροφοριακή κυριαρχία».

Η πληροφοριακή υπεροχή ορίζεται στο διακλαδικό δόγμα των αμερικανικών ενόπλων δυνάμεων σαν *«το επιχειρησιακό πλεονέκτημα που πηγάζει από την ικανότητα της συλλογής, επεξεργασίας και διασποράς μη διακοπτόμενης ροής πληροφοριών και ταυτόχρονη εκμετάλλευση ή απαγόρευση της εχθρικής ικανότητας να υλοποιήσει το ίδιο.»*[88] Για να επιτευχθεί αυτή η υπεροχή απαιτείται στο ελάχιστο να διαθέτουν οι φίλιες δυνάμεις ένα επιχειρησιακό πληροφοριακό πλεόνασμα 51% έναντι 49% του αντιπάλου. Αντίθετα, ο εναλλακτικός όρος της πληροφοριακής κυριαρχίας-και αυτό συνιστά την ουσιαστική διαφορά από την πληροφοριακή υπεροχή- αναφέρεται στην εξασφάλιση ενός αδιαμφισβητήτου πλεονεκτήματος στο πληροφοριακό περιβάλλον σε κάθε περίπτωση.

Με βάση τους παραπάνω ορισμούς, η σχέση μεταξύ στρατηγικής επικοινωνίας και πληροφοριακής υπεροχής φαίνεται να είναι αμφίδρομη. Αφενός η στρατηγική επικοινωνία χρειάζεται την απρόσκοπτη ροή πληροφοριών ώστε να σχεδιαστούν και υλοποιηθούν αποτελεσματικές επιχειρήσεις επιρροής στο θέατρο των επιχειρήσεων και να αντιμετωπισθούν αντίστοιχες ενέργειες του αντιπάλου, αφετέρου η πληροφοριακή κυριαρχία από μόνη της δεν εξασφαλίζει κάποιο πλεονέκτημα στις φίλιες δυνάμεις αν όλες οι πληροφορίες που συλλέγονται δεν καταλήγουν βάση ενός κεντρικού σχεδιασμού στους κατάλληλους αποδέκτες.

Βέβαια, η στρατηγική επικοινωνία και η πληροφοριακή υπεροχή αποτελούν διακριτές έννοιες που έχουν δύο κύριες διαφορές. Πρώτον, η πληροφοριακή κυριαρχία στοχεύει στην εξασφάλιση επιχειρησιακού πλεονεκτήματος μέσω της ικανότητας της συλλογής και ροής πληροφοριών. Αντίθετα η στρατηγική επικοινωνία επικεντρώνεται στο πλεονέκτημα που εξασφαλίζουν οι συγκεκριμένες πληροφορίες στις φίλιες δυνάμεις και στην επίδραση που έχει το περιεχόμενό τους. Επιγραμματικά, μπορούμε να ισχυριστούμε ότι η πρώτη αναφέρεται στο «μέσο» ενώ η δεύτερη στο «μήνυμα». Δεύτερον, η πληροφοριακή υπεροχή είναι μία έννοια που εξετάζεται πάντα σε συνάρτηση με την ύπαρξη ενός ανταγωνιστικού αντιπάλου ενώ η στρατηγική επικοινωνία είναι μία διαδικασία που δεν μπαίνει στη λογική ενός παιγνίου μηδενικού αθροίσματος και μπορεί να εφαρμοστεί και χωρίς αντίπαλο.

## 5.4 ΣΧΕΣΗ ΜΕΤΑΞΥ ΣΤΡΑΤΗΓΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ – ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ-ΔΙΠΛΩΜΑΤΙΑΣ ΚΟΙΝΟΥ

Μέχρι τώρα αναλύθηκαν τόσο όσο προς το περιεχόμενο όσο και ως προς τον σκοπό τους οι **έννοιες της Στρατηγικής Επικοινωνίας, των Πληροφοριακών Επιχειρήσεων και της Διπλωματίας Κοινού που συνθέτουν το βασικό τρίπτυχο των Επιχειρήσεων Επιρροής που διεξάγει ένα κράτος.** Ποια είναι όμως άραγε η συνάφεια μεταξύ των τριών αυτών δραστηριοτήτων και πως αυτές αλληλεπιδρούν μεταξύ τους ; Ένας σημαντικός αριθμός μελετητών ενστερνίζεται την άποψη ότι πρόκειται για ταυτόσημες έννοιες που έχουν ανεπαίσθητες ως ανύπαρκτες διαφορές. Αποτελούν δηλαδή στην ουσία ίδιες ακριβώς δράσεις που περιγράφονται από συνώνυμες λέξεις. Για παράδειγμα, οι συγγραφείς του αμερικάνικου

[88] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Washington, D.C., Joint Publications 1-02, April 12, 2001.

κυβερνητικού γραφείου αξιολόγησης ομολόγησαν ότι χρησιμοποίησαν τους τρεις όρους πανομοιότυπα σε μία αναφορά που συνέταξαν το 2009[89]. Παρόμοια, ο καθηγητής Bruce Gregory θεωρεί την στρατηγική επικοινωνία και τη διπλωματία κοινού ανάλογες[90] ενώ και ο Leigh Armistead στο βιβλίο του Ζητήματα Πληροφοριακών Επιχειρήσεων αρνείται να κάνει την οποιαδήποτε διάκριση μεταξύ των τριών εννοιών.[91] Όσοι ταυτίζονται με την παραπάνω προσέγγιση, πιστεύουν απλά ότι ο όρος στρατηγική επικοινωνία χρησιμοποιείται για να περιγράψει ενέργειες που υλοποιούνται από το υπουργείο εθνικής άμυνας ενώ ο όρος διπλωματία κοινού από το υπουργείο εξωτερικών. Αντίθετα, μία άλλη μερίδα ερευνητών θεωρεί ότι οι παραπάνω έννοιες αντικατοπτρίζουν διακριτές δραστηριότητες. Μπορεί να ταυτίζονται σε αρκετά σημεία, όπως πχ. να συγκλίνουν οι σκοποί που εξυπηρετούν, να ομοιάζουν σε μεγάλο βαθμό τα επιστημονικά εργαλεία και οι τεχνικές που μεταχειρίζονται για να εκπληρώσουν τους στόχους τους ή και να απευθύνονται πολλές φορές σε κοινά ακροατήρια ανθρώπων, ωστόσο, η ιεραρχική τους κατάταξη στο πληροφοριακό χάρτη με κριτήριο την ευρύτητα των λειτουργιών τους, συνιστά μία σημαντική διαφορά που καθιστά απαγορευτική την απόλυτη εξομοίωσή τους. Επίσης, μία άλλη διαφορά εντοπίζεται στο γεγονός ότι ο χρονικός ορίζοντας ωρίμανσης των δράσεων τους με βάση τα προσδοκώμενα οφέλη είναι εντελώς διαφορετικός. Για παράδειγμα, στους διπλωματικούς κύκλους είναι ευρέως διαδεδομένη η άποψη ότι οι πληροφοριακές επιχειρήσεις αποτελούν μία αμιγώς στρατιωτική δραστηριότητα που στοχεύει σε βραχύβια αποτελέσματα και ορισμένες φορές μάλιστα είναι πιθανό οι επιχειρήσεις αυτές να θέσουν σε κίνδυνο την παραδοσιακή διπλωματία κοινού. Στο σημείο αυτό ο ειδικός σε θέματα διπλωματίας κοινού Phil Seib επισημαίνει: « *Η επικοινωνία υπό την στρατιωτική οπτική γωνία-η στρατηγική επικοινωνία, ο ψυχολογικός πόλεμος και οι πληροφοριακές επιχειρήσεις-λειτουργεί σε ένα περιβάλλον συγγενικό με αυτό της διπλωματίας κοινού και αντιπροσωπεύει μία πρόκληση για την ακεραιότητα της μη στρατιωτικής διαδικασίας. Η διατήρηση ενός τείχους προστασίας μεταξύ των φανερών πολιτικών δράσεων και των μυστικών στρατιωτικών ενεργειών αποτελεί μία ουσιαστική προϋπόθεση για την επιτυχή οικοδόμηση διπλωματίας κοινού για κάθε έθνος.»*[92] Αν θέλαμε τώρα σχηματικά να απεικονίσουμε τη θέση που καταλαμβάνει κάθε δραστηριότητα στον πληροφοριακό χάρτη, θα μπορούσαμε να ισχυριστούμε ότι η ανώτερη ιεραρχικά διαδικασία που ενσωματώνει όλες ή μέρος από τις λειτουργίες των άλλων δραστηριοτήτων είναι η στρατηγική επικοινωνία. Η στρατηγική επικοινωνία συνιστά μια σύνθετη διαδικασία που εκφράζει την ολότητα των επιχειρήσεων επιρροής που διεξάγει ένα κράτος και στηρίζεται για τη λειτουργία της σε δευτερεύουσες και υποδεέστερες ικανότητες τις οποίες έχει την ευθύνη και την αρμοδιότητα να συντονίζει και να συγχρονίζει με σκοπό πάντα την εξυπηρέτηση εθνικών πολιτικών σκοπών. Αυτή την άποψη ενστερνίζεται και ο ακαδημαϊκός καθηγητής Phil Taylor ο οποίος

[89] U.S. Government Accountability Office, U.S. Public Diplomacy Key Issues for Congressional Oversight, footnote 1.

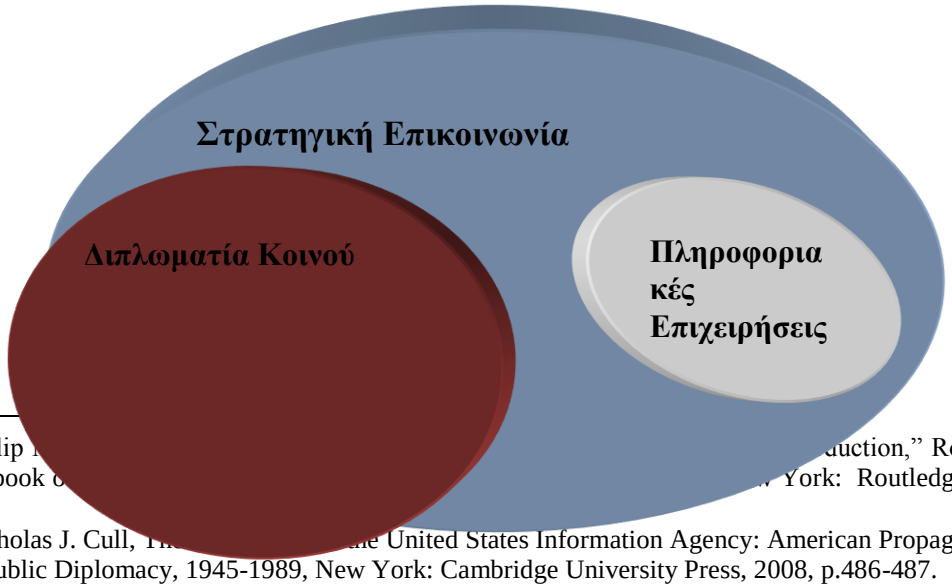
[90] Bruce Gregory, Mapping Smart Power in Multi Stakeholder Public Diplomacy/Strategic Communication, transcript from "New Approached to U.S. Outreach " forum, George Washington University, The Institute for Public Diplomacy and Global Communication, October 5, 2009, p. 1.

[91] Leigh Armistead "Information Operations Matters": Best Practices, Washington, D.C.: Potomac Books, 2010.

[92] Seib, Toward a New Public Diplomacy, p.24.

διατείνεται ότι *«η στρατηγική επικοινωνία ακουμπάει σε τέσσερα μαξιλάρια που είναι οι πληροφοριακές και ψυχολογικές επιχειρήσεις, η διπλωματία κοινού και οι δημόσιες σχέσεις»*[93]. Επομένως, υπό αυτήν την οπτική γωνία, οι πληροφοριακές επιχειρήσεις είναι σαφώς υποδεέστερες της στρατηγικής επικοινωνίας και αποτελούν οργανωμένο υποσύνολο της, εξυπηρετώντας κυρίως επιχειρησιακούς επικοινωνιακούς σκοπούς στο στρατιωτικό πεδίο δράσης. Ιδιαίτερη μνεία οφείλει να γίνει στην σχέση μεταξύ στρατηγικής επικοινωνίας και διπλωματίας με το κοινό η οποία δεν είναι και τόσο ξεκάθαρη. Καταρχήν πρέπει να διευκρινιστεί ότι το αντικείμενο τους δεν είναι απολύτως το ίδιο. Η διπλωματία κοινού περιλαμβάνει δραστηριότητες που εντοπίζονται στην προσπάθεια μίας κυβέρνησης να προσεγγίσει και να αναπτύξει σταδιακά δεσμούς με ξένα κοινά. Για να το επιτύχει αυτό μεταχειρίζεται μία σειρά εργαλείων όπως εκπαιδευτικά σεμινάρια ανταλλαγής φοιτητών και μαθητών, πολιτιστικά γεγονότα, ραδιοφωνικές εκπομπές και τηλεοπτικές αναμεταδόσεις και προγράμματα εκμάθησης γλωσσών. Ο καθηγητής Nick Cull αποφεύγει να καταγράψει ξεχωριστά κάθε μία από αυτές τις δράσεις και στη θέση τους τοποθετεί τα πέντε κύρια στοιχεία της διπλωματίας κοινού: την ικανότητα ακρόασης, την συνηγορία, τη διεθνή αναμετάδοση προγραμμάτων, τον πολιτισμό, και τις διπλωματικές συναλλαγές.»[94] Η στρατηγική επικοινωνία συμπεριλαμβάνει σαφώς όλα τα ανωτέρω αλλά εσωκλείει και επιπλέον ικανότητες όπως αυτές που διαθέτουν πχ οι πληροφοριακές επιχειρήσεις. Κυρίως όμως αυτό που την χαρακτηρίζει και την καθιστά ξεχωριστή είναι ότι η φιλοσοφία της εστιάζει στην επικοινωνιακής αξία που έχουν όλες οι πράξεις και πολιτικές δράσεις. Η διπλωματία κοινού αντίθετα δεν περιέχει κάποιο τέτοιο στοιχείο. Παρά ταύτα δεν μπορεί να θεωρηθεί κατώτερη συνολικά επειδή ένα κομμάτι των λειτουργιών της δεν εξυπηρετεί κανέναν από τους αντικειμενικούς σκοπούς της στρατηγικής επικοινωνίας όπως αναλύθηκαν παραπάνω. Κάποιες δηλαδή από τις δράσεις της διπλωματίας κοινού δεν εντάσσονται στη λογική της εξυπηρέτησης εθνικών πολιτικών σκοπών. Στο παρακάτω διάγραμμα αναπαρίσταται γραφικά η σχέση μεταξύ της στρατηγικής επικοινωνίας και των υπολοίπων πληροφοριακών ικανοτήτων.

**Διάγραμμα Απεικόνισης της Σχέσης Μεταξύ Στρατηγικής Επικοινωνίας, Πληροφοριακών Επιχειρήσεων και Διπλωματίας Κοινού.**




[93] Philip [illegible] duction," Routledge Handbook o[illegible] York: Routledge, 2009, p.14.

[94] Nicholas J. Cull, Th[illegible]e United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989, New York: Cambridge University Press, 2008, p.486-487.

# ΚΕΦΑΛΑΙΟ 6$^{Ο}$
# ΑΜΕΡΙΚΑΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

*. . . Σας λέω: ότι είμαστε σε μια μάχη, και ότι πάνω από το ήμισυ της μάχης λαμβάνει χώρα στο πεδίο των μέσων μαζικής ενημέρωσης. Και ότι είμαστε σε μια κούρσα για τις καρδιές και τα μυαλά των Ούμα.*

*-Αιμάν Αλ-Ζαουάχρι στον Αμπού Μουσάμπ αλ-Ζαρκάουι, 9 Ιουλίου 2005*[95]

## ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ ΙΡΑΚ

Τον Απρίλιο του 2004, σε απάντηση της δολοφονίας και της βεβήλωσης εργολάβων της Blackwater στη Φαλούτζα, οι συμμαχικές δυνάμεις υπό την ηγεσία του 1$^{ου}$ εκστρατευτικού σώματος των πεζοναυτών, εξαπέλυσαν επιχείρηση με την κωδική ονομασία *«Vigilant Resolve»*[96] που ήταν στην ουσία μια επίθεση για να αποκαταστήσουν τον έλεγχο της πόλης. Παρά την ανωτερότητα των συμμαχικών στρατευμάτων σε θέματα ηγεσίας, ελιγμών και υποστήριξης πυρών, η επιχείρηση απέτυχε, διότι δεν είχε συμπεριληφθεί η πληροφοριακή διάσταση στο επιχειρησιακό σχέδιο που καταρτίσθηκε. Στην πραγματικότητα δεν είχε εκτελεστεί καμία προεργασία συναφής με την προετοιμασία του πληροφοριακού πεδίου μάχης, όπως προσέγγιση των Ιρακινών ηγετών, συγκέντρωση στοιχείων σχετικά με τα κέντρα πληροφόρησης του εχθρού, και δυνατότητα διάδοσης πληροφοριών από το πεδίο της μάχης με τα μέσα μαζικής ενημέρωσης, σε όλο τον υπόλοιπο κόσμο. Υπό αυτές τις συνθήκες, οι δυνάμεις των ΗΠΑ περιορίστηκαν μετά από λίγες ημέρες μονομερώς σε πολεμικές επιχειρήσεις, λόγω της έλλειψης υποστήριξης από την προσωρινή ιρακινή κυβέρνηση και πιέσεων από τα διεθνή φόρα που αναμετέδιδαν αβάσιμες αναφορές του εχθρού για παράπλευρες απώλειες και υπερβολική χρήση βίας. Αντίθετα, οι δυνάμεις των ανταρτών δημιούργησαν κανάλια επικοινωνίας με περιφερειακά και παγκόσμια μέσα μαζικής ενημέρωσης που είχαν τις δικές τους ατζέντες. Έτσι, παρά τη νικηφόρα έκβαση που είχαν όλες σχεδόν οι μάχες που έδωσαν οι Πεζοναύτες εντός των καθορισμένων κανόνων εμπλοκής, το σχέδιο στο σύνολό του είχε μειωμένη αποτελεσματικότητα. Η αποτυχία στην παραγωγή μαζικών αποτελεσμάτων στην παγκόσμια πληροφοριακή σφαίρα αποδείχθηκε καθοριστική για το πεδίο μάχης στη Φαλούτζα.[97] Με το πέρας του θέρους του 2004 και έχοντας κατανοήσει και αφομοιώσει τα μαθήματα από την επιχείρηση Vigilant Resolve, οι συμμαχικές δυνάμεις άρχισαν να προετοιμάζονται εκ νέου για την κατάληψη της πόλης, ενσωματώνοντας αυτή τη φορά και τη πληροφοριακή διάσταση στο καινούργιο σχέδιο που

---

[95] Ayman al-Zawahiri, intercepted letter to Abu Musab al-Zarqawi, 9 July 2005, on-line at <www.dni.gov/letter_in_english.pdf>, accessed 26 April 2006.

[96] Operation Vigilant Resolve, GlobalSecurity.org.

[97] Ralph Peters, "The Counterrevolution in Military Affairs—Fashionable thinking about defense ignores the great threats of our time," *The Weekly Standard*, Volume 11, 2, 6 February 2006.

κατήρτισαν. Στην επιχείρηση Al-Fajr[98]-όπως ονομάστηκε η δεύτερη μάχη της Φαλούτζα- αυτό σήμαινε την ακριβή και επίπονη εκτέλεση όλων των βασικών στοιχείων των παραδοσιακών πληροφοριακών επιχειρήσεων καθώς και άλλων υποστηρικτικών δράσεων, όπως την ενεργοποίηση της στρατιωτικής διπλωματίας και της διπλωματίας κοινού. Καταρχάς έγιναν ενέργειες παραπλάνησης των Ιρακινών ανταρτών που είχαν ως στόχο να αποκρύψουν συσσώρευση των συμμαχικών δυνάμεων βόρεια της Φαλούτζα. Ταυτόχρονα επιχειρήθηκε να εστιαστεί η προσοχή των ανταρτών προς νότο με επιθετικές περιπολίες, προσποιήσεις και επιλεκτικά χτυπήματα από τα νότια της πόλης. Η κίνηση της Βρετανικής Ομάδας Μάχης «Black Watch»[99] και η ανάπτυξη μίας ευέλικτης ταξιαρχίας σε ένα δυναμικό κλοιό βοήθησε επίσης στην προσπάθεια αυτή. Στον τομέα των ψυχολογικών επιχειρήσεων πάρθηκαν πολύ ικανοποιητικές πρωτοβουλίες που ενεθάρρυναν τους άμαχους να εγκαταλείψουν την πόλη και έπεισαν τους αντάρτες να παραδοθούν. Ορισμένες μάλιστα εκτιμήσεις έδειξαν ότι το 90% περίπου των αμάχων, 300.00 κάτοικοι,[100] εγκατέλειψαν την πόλη δίνοντας κατ' αυτό τον τρόπο ένα αποφασιστικό πλεονέκτημα στις στρατιωτικές δυνάμεις των ΗΠΑ. Ο ηλεκτρονικός πόλεμος επίσης έπαιξε σημαντικότατο ρόλο είτε περιορίζοντας είτε παρακολουθώντας τις επικοινωνίες των Ιρακινών.

Η μαζικότητα των πληροφοριακών αποτελεσμάτων στην επιχείρηση Al-Fajr ενισχύθηκε επιπλέον και από την ενσωμάτωση άλλων δράσεων από στοιχεία των δυνάμεων ελιγμού. Η κατάληψη για παράδειγμα του νοσοκομείου στη Φαλούτζα από Ιρακινούς καταδρομείς κατά τα πρώτα στάδια της μάχης ήταν ένα εξαιρετικό δείγμα εκτέλεσης πληροφοριακών επιχειρήσεων για την υποστήριξη των γενικών στόχων της εκστρατείας. Κατά τη διάρκεια της διαδικασίας λήψης αποφάσεων, το συμμαχικό επιτελείο προσδιόρισε ένα κομμάτι εδάφους που έπρεπε να εξασφαλιστεί από νωρίς ώστε να εξαλειφθεί η ικανότητα των ανταρτών για παραπληροφόρηση και προπαγάνδα. Το νοσοκομείο της Φαλούτζα είχε από καιρό χρησιμοποιηθεί ως όργανο προπαγάνδας από τις αντάρτικες δυνάμεις και ήταν μία από τις πιο σημαντικές πηγές πληροφοριών τους κατά τη διάρκεια της επιχείρησης Vigilant Resolve. Με την εξασφάλιση επομένως αυτού του κρίσιμου πληροφοριακού πεδίου, οι δυνάμεις των ΗΠΑ μπόρεσαν να υπονομεύσουν σημαντικά τη δυνατότητα του εχθρού για διάδοση πληροφοριών.

Η κύρια δύναμη που εισήλθε στη Φαλούτζα από το βορρά είχε λάβει συγκεκριμένες οδηγίες να τεκμηριώσει φωτογραφικά τις δραστηριότητες των ανταρτών και να μεταβιβάσει γρήγορα όποιες πληροφορίες συνέλεγε στο επιτελείο ώστε αυτές να επεξεργαστούν και να μεταδοθούν από την Ιρακινή κυβέρνηση και την ομάδα των δημοσίων σχέσεων. Ειδικές οδηγίες εκδόθηκαν ώστε να δημιουργηθούν γραφικά με σαφείς ιστορίες.[101] Σε αυτό το πλαίσιο κατασκευάστηκαν έγγραφα που περιέγραφαν τις αγριότητες των ανταρτών

---

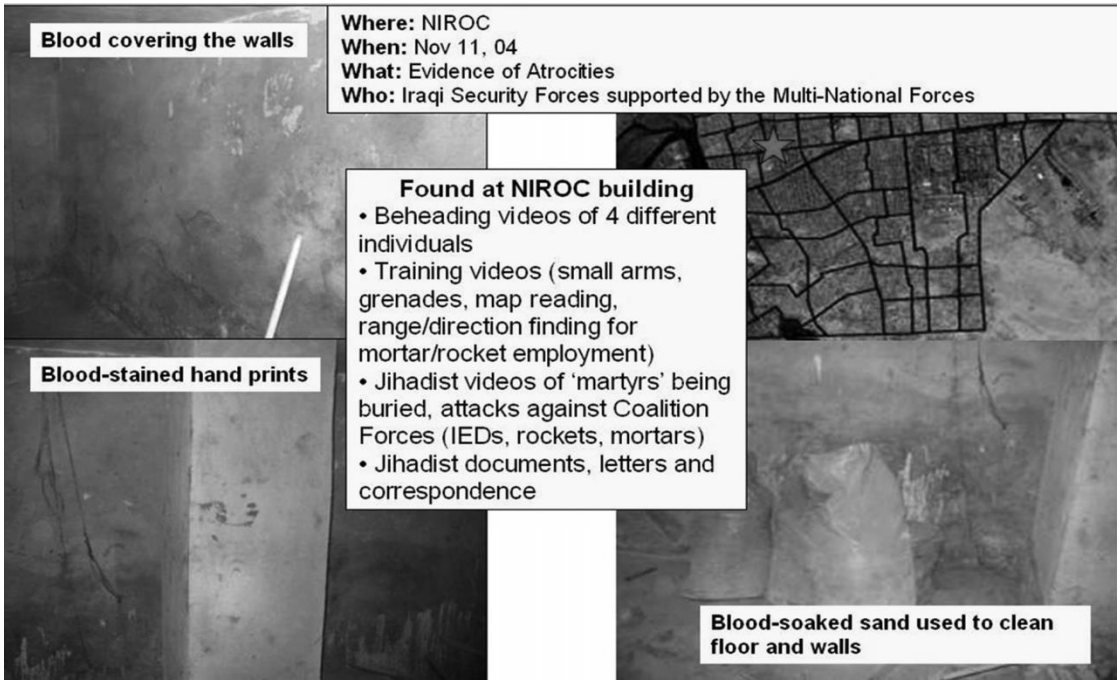
[98] Ricks, Thomas E. (2007). *Fiasco: The American Military Adventure in Iraq, 2003–2005*. Penguin. p. 399. ISBN 0-14-303891-5.

[99] "Black Watch ordered to join US cordon for assault on Fallujah". *The Independent* (London). 22 October 2004. Retrieved 1 July 2011.

[100] Filkins, Dexter; James Glanz (8 November 2004). "With Airpower and Armor, Troops Enter Rebel-Held City". *The New York Times*. Retrieved 27 December 2008.

[101] LTG Thomas F. Metz, "The Battle of Fallujah: A Case Study for Warfare in the Information Age," briefing to the Capitol Bohemian Club, 26 October 2005, Washington, D.C.

που ανακαλύφθηκαν στη Φαλούτζα και διανεμήθηκαν στα μέσα μαζικής ενημέρωσης για δικιά τους χρήση. Παράδειγμα τέτοιου γραφικού φαίνεται στην εικόνα.




Το γενικό συμπέρασμα που προκύπτει σε σχέση με την επιχείρηση Al-Fajr είναι ότι υπήρξε επιτυχημένη για δύο λόγους που συνδέονται με τις μαζικές επιπτώσεις των πληροφοριακών επιχειρήσεων: Σχεδιάστηκε ένας εφικτός τελικός αντικειμενικός σκοπός που φρόντισε να ενσωματώσει όλα τα στοιχεία της δύναμης μάχης (ηγεσία, κίνηση και ελιγμός, νοημοσύνη) και τα εργαλεία του πληροφοριακού πολέμου και γεφυρώθηκε αποτελεσματικά το κενό μεταξύ πληροφοριακών επιχειρήσεων και δημοσίων σχέσεων για να επιτευχθεί το επιθυμητό αποτέλεσμα, χωρίς να παραβιάζονται οι εσωτερικοί κανόνες λειτουργίας τους.

## ΠΑΡΑΔΕΙΓΜΑ 2 - ΠΑΚΙΣΤΑΝ

Τον Σεπτέμβριο του 2012, η κυβέρνηση των ΗΠΑ προέβαλλε διαφημιστικά spot στην δημόσια τηλεόραση του Πακιστάν για να καταγγείλει το αμφιλεγόμενο και προσβλητικό αντί-ισλαμικό βίντεο υπό την ονομασία *«Η αθωότητα των μουσουλμάνων»* που απεικόνιζε τον προφήτη Μωάμεθ. Η πρωτοβουλία αυτή συνοδεύτηκε από τεράστιες διαδηλώσεις κοντά στην αμερικανική πρεσβεία του Ισλαμαμπάντ στο Πακιστάν και κρούσματα βίας που στράφηκαν εναντίον αμερικανικών στόχων, με αποκορύφωμα τη δολοφονία του πρέσβη των ΗΠΑ στη Λιβύη, Christopher Stevens. Η διαφήμιση που περιελάμβανε δηλώσεις του πρόεδρου Μπαράκ Ομπάμα και της τότε υπουργού Εξωτερικών Χίλαρι Κλίντον, επέκρινε την ταινία και παρουσίαζε εντυπωσιακή ομοιότητα με μία προηγούμενη επικοινωνιακή εκστρατεία των ΗΠΑ, υπεύθυνη για την οποία ήταν η εμπορική εταιρία Charlotte Beers. Η Beers υπήρξε ο εμπνευστής μίας εκστρατείας μάρκετινγκ με κόστος 15.000.000 δολάρια υπό τον τίτλο «*κοινές αξίες»,* η οποία μετά τις επιθέσεις της 11ης Σεπτεμβρίου 2001 παρήγαγε μια σειρά από τηλεοπτικές διαφημίσεις που απεικόνιζαν την καθημερινή ζωή των μουσουλμάνων στις ΗΠΑ. Το πρόγραμμα ξεκίνησε στην Ινδονησία, την πολυπληθέστερη μουσουλμανική χώρα του κόσμου, αλλά απέτυχε να βρει ανταπόκριση στη Μέση Ανατολή. Πολλοί στον αραβικό κόσμο υποτίμησαν την εκστρατεία και τη θεώρησαν απλοϊκή στην σύλληψή της. Οι αναφορές των

μέσων ενημέρωσης τόσο στο εξωτερικό όσο και στις Ηνωμένες Πολιτείες ήταν σε γενικές γραμμές αρνητικές και το προϊόν της εκλήφθηκε ως ακατέργαστη προπαγάνδα. Τόσο το CNN και η Wall Street Journal ανέφεραν ότι η εκστρατεία απέτυχε στον αρχικό στόχο της που ήταν η επαφή και η γνωριμία με το μουσουλμανικό κοινό. Η Beers σε μία πιο αισιόδοξη προσέγγιση υποστήριξε ότι ήταν επιτυχής διότι είχε αρχίσει ένα διάλογος με τους μουσουλμάνους. Τον Μάρτιο του 2003, η Beers παραιτήθηκε από το State Department και το σχέδιο κατέρρευσε. Δεδομένης της ομοιότητας μεταξύ των τηλεοπτικών σποτ του 2012 και της εκστρατεία της Beers φαίνεται ότι αυτό που είχε προηγηθεί της κατάρρευσης της εταιρίας, ήταν η αποτυχία των ιδεών της. Πράγματι, κατά την αξιολόγηση των τηλεοπτικών διαφημίσεων του Πακιστάν, ανακύπτει μία σειρά από ερωτήματα σχετικά με την προσβασιμότητα και την ικανότητά τους να φτάσουν στο ακροατήριο. Από το μεγάλο σώμα των ανθρώπων που ενεπλάκησαν στις ταραχές, μόνο ένα πολύ μικρό ποσοστό είχε δει πραγματικά το προσβλητικό βίντεο. Το βίντεο ήταν διάρκειας 74 λεπτών, λίγο πάνω από 400 megabyte (MB) και θα μπορούσε επομένως να αναπαραχθεί μέσω των smart phones, εάν φυσικά υπήρχε πρόσβαση στο διαδίκτυο. Ενώ η διείσδυση του Internet στο Πακιστάν αναμφισβήτητα αυξάνεται, το επίπεδο μόρφωσης εξακολουθεί να είναι πολύ χαμηλό και περίπου 30% με 40% του πληθυσμού ζει κάτω από το όριο της φτώχειας, το οποίο παραπέμπει σε περιορισμένη πρόσβαση στο Internet μέσω υπολογιστή. Την ίδια στιγμή, η παρακολούθηση των τηλεοπτικών σποτ των ΗΠΑ απαιτούσε τόσο την δυνατότητα πρόσβασης σε τηλεόραση όσο και την ικανότητα κατανόησης της αγγλικής γλώσσας. Ως εκ τούτου, πολλοί από τους στασιαστές δεν είχαν πιθανώς δει ποτέ ούτε το αρχικό βίντεο, ούτε την προεδρική ομιλία που ακολούθησε, και η γνώση τους προερχόταν από τοπικούς θρησκευτικούς ηγέτες που μιλούσαν σε τόπους θρησκευτικής συνάθροισης όπως τα τζαμιά.

Δεύτερον, η οργή για το βίντεο ήταν ακόμη πιο έντονη, επειδή ευθυγραμμιζόταν με το αφήγημα του μίσους των ΗΠΑ εναντίον των μουσουλμάνων. Έτσι προστέθηκε στην ήδη μεγάλη λίστα αδικιών, συμπεριλαμβανομένων των συγκρούσεων της Παλαιστίνης, του Ιράκ, του Αφγανιστάν, καθώς και της βεβήλωσης του Κορανίου. Στο πλαίσιο αυτό, φαίνεται υπερβολικά αισιόδοξος ο στόχος ότι μερικές λέξεις σε μια τηλεοπτική διαφήμιση από τον πρόεδρο των ΗΠΑ θα μπορούσαν να κατευνάσουν έναν εξοργισμένο όχλο.

Τρίτον, ο υποτιθέμενος στόχος των διαφημίσεων ήταν να μειώσει την ανεπιθύμητη συμπεριφορά των μουσουλμάνων. Ο Πρόεδρος Ομπάμα γι' αυτό το λόγο δήλωσε στην διαφήμιση ότι το βίντεο δεν αντανακλά τις απόψεις ή την πολιτική των ΗΠΑ. Δήλωσε, επίσης, ότι οι Ηνωμένες Πολιτείες σεβάστηκαν την ισλαμική θρησκεία και τους μουσουλμάνους. Εν ολίγοις, ζήτησε να αλλάξει η στάση των ανθρώπων αυτών απέναντι στις Ηνωμένες Πολιτείες, με την ελπίδα ότι η εξέγερση θα σταματήσει. Δεδομένης της ευρείας αποδοχής της ιδέας που διακατέχει τον ισλαμικό κόσμο ότι «η Αμερική μισεί τους μουσουλμάνους» μία τέτοια προσπάθεια αποδείχτηκε υπερβολικά φιλόδοξη. Στην πραγματικότητα, ο Ομπάμα αγνόησε ένα σημαντικό κομμάτι της έρευνας των κοινωνικών επιστημών παρελθόντων ετών, οι οποίες κατέδειξαν ότι η αλλαγή στην καθημερινή συμπεριφορά δεν συνιστά απαραίτητα πρόδρομη κατάσταση της συνολικής αλλαγής στάσης ενός ακροατηρίου. Οι διαφημίσεις δεν ήταν

φυσικά η μόνη απάντηση των ΗΠΑ στο βίντεο. Από την ομιλία του προέδρου Ομπάμα το 2009 στο Κάιρο στην Αίγυπτο, οι Ηνωμένες Πολιτείες είχαν προσπαθήσει να ξαναχτίσουν την εικόνα τους στον αραβικό και μουσουλμανικό κόσμο. Ωστόσο, η διαφημιστική εκστρατεία είχε κοστίσει στον φορολογούμενο των ΗΠΑ σημαντικά χρηματικά ποσά αν και οι πιθανότητες επιτυχίας του εγχειρήματος ήταν από την αρχή ελάχιστες. Επαληθεύοντας την αναποτελεσματικότητα της διαφημιστικής καμπάνιας, το τηλεοπτικό δίκτυο ABC μετέδωσε στις 21 Σεπτέμβρη του 2012 ότι *«Θανατηφόρες διαδηλώσεις κατά των ΗΠΑ ξέσπασαν στο Πακιστάν παρά τη διαφημιστική καμπάνια στην πακιστανική τηλεόραση από τον Πρόεδρο Ομπάμα και την υπουργό Εξωτερικών Χίλαρι Κλίντον που κατήγγειλαν την ταινία «η αθωότητα των μουσουλμάνων». Οι διαφημίσεις έχουν αναμεταδοθεί αυτή την εβδομάδα σε επτά διαφορετικούς πακιστανικούς τηλεοπτικούς σταθμούς, σε μια προσπάθεια να μετριάσουν τις αντιδράσεις που έχει προκαλέσει η ταινία, αλλά οι σημερινές διαμαρτυρίες υπήρξαν οι μεγαλύτερες που έχουν συμβεί μέχρι σήμερα, δεδομένου ότι η διαμάχη ξεκίνησε στο Πακιστάν την περασμένη εβδομάδα με την επιχειρούμενη κατάληψη της πρεσβείας των ΗΠΑ.»*[102]

Το παραπάνω περιστατικό αντικατοπτρίζει τη λάθος πολιτική που επέλεξαν οι Ηνωμένες Πολιτείες σε σχέση με τις ψυχολογικές επιχειρήσεις τα τελευταία χρόνια: εμπιστοσύνη σε φιλόδοξους εργολάβους, και απουσία «ευφυών πελατών» σε συνδυασμό με μία προφανή έλλειψη κατανόησης του πώς η επικοινωνία μπορεί ή δεν μπορεί να κατευνάσει μία κρίση ή σύγκρουση.

# ΚΕΦΑΛΑΙΟ 6$^{Ο}$
# ΟΙ ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΣΤΟ ΡΩΣΙΚΟ ΣΤΡΑΤΟ

Οι πληροφοριακές επιχειρήσεις έχουν κατά καιρούς οριστεί με διάφορους τρόπους από τους Ρώσους συγγραφείς. Χωρίς ωστόσο να υπάρχουν έγκυρες δημοσιεύσεις όπως αυτές των αμερικάνικων διακλαδικών κανονισμών, είναι σχεδόν αδύνατο να διατυπωθεί επίσημος ορισμός του κάθε όρου. Γενικά, η Ρωσική πολιτική και πολιτιστική ιστορία, η οικονομική και τεχνολογική κατάσταση, η γεωγραφική θέση και η στρατιωτική εμπειρία, αποτελούν παράγοντες που δημιουργούν μια διαφορετική βάση για τον τρόπο σκέψης των Ρώσων Στοχαστών. Η ανάλυσή τους διαμορφώνεται κάτω από το πρίσμα Ρωσικών επιδιώξεων και ηθικών αρχών τελείως διαφορετικών από αυτών της Δύσης.

Στους επιφανέστερους Ρώσους θεωρητικούς συναριθμείται ο

[102] See *abcnews.go.com/International/deadly-anti-us-riots-pakistan-obamas-ad-denouncing/story?id=17291751*.

εμπειρογνώμονας Rastorguyev του οποίου οι απόψεις έχουν βαρύνουσα σημασία. (Δεν είναι τυχαίο ότι του ανατέθηκε να γράψει βιβλίο που ονομάζεται Πληροφορικός πόλεμος για λογαριασμό του Συμβουλίου Ασφαλείας της Ρωσικής Ομοσπονδίας.) Στο βιβλίο του που κυκλοφόρησε το 2003 με τίτλο *Εισαγωγή στην Επίσημη Θεωρία του Πληροφοριακού Πολέμου*, ορίζει την έννοια του Πληροφοριακού Πολέμου ως *«μια μάχη μεταξύ των κρατών που διεξάγεται αποκλειστικά με τη χρήση πληροφοριακών όπλων στην σφαίρα ενός πληροφοριακού μοντέλου»* και την πληροφοριακή επιχείρηση ως *«μια σειρά από ενέργειες όπου χρησιμοποιούνται πληροφοριακά όπλα για την επιτυχία ενός έργου.»* Το πληροφοριακό όπλο μπορεί να είναι οποιοδήποτε τεχνικό, βιολογικό, ή κοινωνικό μέσο ή σύστημα που χρησιμοποιείται για την σκόπιμη παραγωγή, επεξεργασία, μετάδοση, εμφάνιση ή κλείδωμα δεδομένων και διαδικασιών που λειτουργούν με δεδομένα»[103] Σύμφωνα με τον Rastorguyev, τα όπλα πληροφοριών είναι τα πιο σημαντικά όπλα στην σύγχρονη εποχή για τέσσερις λόγους: προσφέρουν μια πολύ φθηνότερη παραγωγή δεδομένων λόγω της ανάδυσης των τεχνολογιών της πληροφορίας, παρέχουν αυτοματοποιημένα μέσα για την απόκτηση γνώσης από τα δεδομένα που έχουν ήδη δημιουργηθεί, παρέχουν μία μεγάλη μείωση του κόστους και του χρόνου για την παροχή πληροφοριών σε σχεδόν οποιοδήποτε σημείο του πλανήτη λόγω της ανάπτυξης των τηλεπικοινωνιών και προσφέρουν μια μεγάλη αύξηση της αποτελεσματικότητας των πληροφοριών.[104]

Η έννοια του πληροφοριακού όπλου δεν αποτελεί τη μοναδική διαφορά μεταξύ της δυτικής και ρωσικής στρατιωτικής σκέψης στον τομέα των πληροφοριακών επιχειρήσεων. Στη Ρώσικη βιβλιογραφία, οι πληροφοριακές επιχειρήσεις δεν περιγράφονται ως ένα άθροισμα επιμέρους ικανοτήτων αλλά διαιρούνται σε δύο μεγάλες κατηγορίες. Στο έργο του Rastorguyev γίνεται αναφορά σε δύο βασικές πτυχές των ρώσικων πληροφοριακών επιχειρήσεων: την τεχνική-πληροφοριακή και τη ψυχολογική-πληροφοριακή. Η ίδια διάκριση καταγράφεται και σε μία έρευνα που διενεργήθηκε από το Γραφείο Στρατιωτικών Σπουδών Εξωτερικού των ΗΠΑ, όπου επιπλέον τονίζεται ότι η Ρωσία αντιμετωπίζει το θέμα της πληροφοριακής υπεροχής υπό διαφορετική οπτική γωνία. Οι Ρώσοι θεωρητικοί δίνουν μεγάλη έμφαση στην «αποδιοργάνωση» του εχθρού, αντί στην επίτευξη πληροφοριακής υπεροχής».[105] Παρόμοιες απόψεις αντηχεί και ένα άρθρο του λοχαγού R. Bikkenin που δημοσιεύθηκε στη **Ναυτική Εφημερίδα (Morskoy Sbornik)** τον Οκτώβριο του 2003. Σε αυτό το άρθρο ο Bikkenin τονίζει ότι προτιμά να χρησιμοποιεί τον όρο αποδιοργάνωση αντί πληροφοριακή υπεροχή και στην συνέχεια απαριθμεί τα συστατικά στοιχεία των δύο μεγάλων κατηγοριών των πληροφοριακών επιχειρήσεων. Στις συνιστώσες της τεχνικής-πληροφοριακής πλευράς περιλαμβάνει την παραπληροφόρηση, την στρατιωτική εξαπάτηση-*Maskirovka*, την συλλογή πληροφοριών, την επιστήμη της κρυπτογράφησης, και τη στενογραφία. Η Maskirovka είναι ένας όρος που δεν έχει άμεσο ισοδύναμο στη Δύση, αλλά περικλείει ταυτόχρονα τις τέχνες της απόκρυψης, της χρήσης ανδρεικέλων και δολωμάτων, της παραπληροφόρησης ακόμα και την εκτέλεση πολύπλοκων

---

[103] S. P. Rastorguyev, An Introduction to the Formal Theory of Information Warfare, Moscow 2003, p. 6, 7.
[104] Ibid., p 9.
[105] Timothy Thomas, "*Comparing US, Russian and Chinese IO Concepts*," Ft. Leavenworth, KS: Foreign Military Studies Office, 2004.

ελιγμών των συμβατικών δυνάμεων, στην πραγματικότητα οτιδήποτε είναι ικανό να μπερδέψει και να αποδυναμώσει τον εχθρό.[106] Η «πληροφοριακή-ψυχολογική» διάσταση συνίσταται στη χρήση των μέσων μαζικής ενημέρωσης (τύπος, ραδιόφωνο, τηλεόραση), σε διανομή φυλλαδίων σε θρησκευτική προπαγάνδα, στα δίκτυα υπολογιστών, και ειδικά στο Διαδίκτυο .[107]

Αναφορικά με πληροφοριακή- ψυχολογική» διάσταση των πληροφοριακών επιχειρήσεων, ο Αμερικάνος Συνταγματάρχης Timothy Tomas σημειώνει ό η Ρωσία αρέσκεται στο χειρισμό των γνωστικών διεργασιών του αντιπάλου, με τον οποίο επιδιώκει να επηρεάσει τις διαδικασίες λήψης αποφάσεων του εχθρού ώστε να παράγει αποτελέσματα ευνοϊκά για τους Ρωσικούς στόχους, χωρίς να το συνειδητοποιεί ο εχθρός. Κάτι τέτοιο μπορεί να περιλαμβάνει μέσα που θεωρούνται ιδιαίτερα ασυνήθιστα στις ΗΠΑ, όπως η χρήση της παραψυχολογίας, η βιοενέργεια, και η ακουστική.[108] Επιπλέον, σε αντίθεση με τη δυτική προσέγγιση, οι Ρώσοι αναλυτές αντιλαμβάνονται την πληροφοριακή-ψυχολογική πτυχή των πληροφοριακών επιχειρήσεων με όρους προστασίας της κοινωνίας από τον πληροφοριακό επηρεασμό του αντιπάλου.[109] Στην προκειμένη περίπτωση, ο έλεγχος της πληροφορίας δεν αποσκοπεί μόνο στην ασφάλεια του κράτους αλλά και στην σταθερότητα του εκάστοτε καθεστώτος και των ηγετών του. Η σταθερότητα αυτή επιτυγχάνεται ελέγχοντας την πληροφοριακή ροή μέσω της εποπτείας των διαφόρων μέσων ενημέρωσης, όπως του τύπου, της τηλεόρασης, του ραδιοφώνου, του διαδικτύου κλπ. Η Ρωσική αντίληψη σχετικά με τον σταθεροποιητικό ρόλο που διαδραματίζει ο πληροφοριακός έλεγχος, μπορεί να γίνει κατανοητή μόνο υπό το πρίσμα προγενεστέρων τραυματικών εμπειριών, που συνδέονται με τη διάλυση της πρώην Σοβιετικής ένωσης. Οι παραπάνω εμπειρίες γαλούχησαν και ενίσχυσαν σε σημαντικό βαθμό τα αισθήματα καχυποψίας και εχθρότητας απέναντι σε κάθε ξένη προσπάθεια επηρεασμού της Ρωσικής κοινής γνώμης. Σε αυτό το πλαίσιο, η Ρωσία διενεργεί πληροφοριακές επιχειρήσεις από τον καιρό της ειρήνης που κατευθύνονται τόσο προς τον εγχώριο πληθυσμό της όσο σε ξένα ακροατήρια. Στο εσωτερικό επίπεδο οι επιχειρήσεις αυτές αποσκοπούν στην κατάλληλη διαμόρφωση της κοινής γνώμης έτσι ώστε να εξασφαλίζεται η σταθερότητα της πολιτείας και να προλαμβάνονται ανατρεπτικές ενέργειες από ξένες δυνάμεις ενώ στο διακρατικό επίπεδο προβλέπεται η λήψη οικονομικών και διπλωματικών μέτρων και η εκτέλεση επιχειρήσεων επιρροής. Στον καιρό του πολέμου, οι πληροφοριακές επιχειρήσεις της Ρωσίας έχουν ως αντικειμενικό σκοπό την απόκτηση και διατήρηση πληροφοριακού πλεονεκτήματος και την προστασία των φίλιων πληροφοριακών συστημάτων. Είναι σημαντικό επίσης να επισημανθεί ότι παρόμοια με το δόγμα των Ενόπλων Δυνάμεων των ΗΠΑ, η Ρωσία διεξάγει τις παραπάνω επιχειρήσεις και στα τρία επίπεδα, δηλαδή στο στρατηγικό, στο επιχειρησιακό και στο τακτικό. Σύμφωνα με τον Bikkenin, στο στρατηγικό επίπεδο εμπλέκονται διάφορα τμήματα και υπουργεία που σε καιρό πολέμου μπορούν να εκτελέσουν δύο ή περισσότερες στρατηγικές αποστολές. Σε

---

[106] Mark Lloyd, *The Art of Military Deception*, London, UK: Pen and Sword Books, 1997, p. 115.

[107] R. Bikkenin, "Information Conflict in the Military Sphere: Basic Elements and Concepts," Morskoy, No 10, 2003, pp 38-40 as translated and downloaded from the FBIS web site on 6 February 2004.

[109] Thomas T. (1998a), "Dialectical versus Empirical Thinking Ten Key Elements of Russian Understanding of Information Operations", FMSO Special Study Center for Army Lesson Learned. Fort Leavenworth, KS 66027-1327.

επιχειρησιακό επίπεδο εμπλέκονται ο ναυτικός στόλος και τα σώματα στρατού και τέλος στο τακτικό επίπεδο οι πληροφοριακές επιχειρήσεις διεξάγονται από σχηματισμούς, μονάδες και υπομονάδες του στρατού και μεμονωμένα πλοία.[110]

Στενά συνδεδεμένη με την πληροφοριακή-ψυχολογική πτυχή των πληροφοριακών επιχειρήσεων είναι η θεωρία του **«ανακλαστικού ελέγχου» (reflexive control),** μία εξελιγμένη ρωσική εκδοχή στη διαχείριση της ανθρώπινης αντίληψης.[111] Αν και η θεωρία αυτή αναπτύχθηκε πριν από αρκετό καιρό στη Ρωσία, εξακολουθεί να υφίσταται περαιτέρω επεξεργασία. Πρόσφατη απόδειξη αυτού του γεγονότος είναι η κυκλοφορία τον Φεβρουάριο του 2001, ενός νέου ρωσικού περιοδικού, γνωστού ως *«Αντανακλαστικές Διεργασίες και Έλεγχος»*. Στο περιοδικό, που είναι το προϊόν συνεργασία μιας ομάδας επιστημόνων από τα κορυφαία εθνικά ιδρύματα ασφάλειας της Ρωσίας, ο αντανακλαστικός έλεγχος ορίζεται ως ένα μέσο που μεταφέρει σε έναν εταίρο ή έναν αντίπαλο ειδικά προετοιμασμένες πληροφορίες, τέτοιες που θα τον ωθήσουν να λάβει προκαθορισμένες αποφάσεις σε αντιστοιχία με την βούληση του δημιουργού τους. [112]

Ο ανακλαστικός έλεγχος αποτελεί εφεύρημα του Ρώσου Vladimir Lefebvre, ο οποίος χρησιμοποιώντας το 1950 τη νεοαποκτηθείσα τεχνολογία των υπολογιστών, προσπάθησε να εξετάσει και να ερμηνεύσει τις διαδικασίες λήψης στρατιωτικών αποφάσεων. Γι' αυτόν τον λόγο, δημιούργησε ένα σύστημα μοντελοποίησης που αποτελείτο από τρία υποσυστήματα: ένα μοντέλο για την προσομοίωση των φίλιων αποφάσεων, ένα μοντέλο για την προσομοίωση των συστημάτων του αντιπάλου, και ένα μοντέλο που θα υλοποιούσε τις αποφάσεις. Στο τέλος, κατέληξε στο συμπέρασμα ότι το μοντέλο αυτό θα μπορούσε να χρησιμοποιηθεί για να επηρεάσει έναν αντίπαλο στην παραγωγή αποφάσεων που θα ήταν ευνοϊκές για την Σοβιετική Ένωση. Πιο συγκεκριμένα ο Lefebvre υποστήριξε ότι: Κατά τη λήψη των αποφάσεών του, ο αντίπαλος χρησιμοποιεί πληροφορίες σχετικά με την περιοχή της σύγκρουσης, για τα στρατεύματά του και τα δικά μας, σχετικά με την ικανότητά τους να πολεμήσουν, κ.λπ. Μπορούμε να επηρεάσουμε τα κανάλια των πληροφοριών του και να στείλουμε μηνύματα που μετατοπίζουν τη ροή των πληροφοριών με τρόπο ευνοϊκό για εμάς.[113]Στην ουσία, αυτό που υποδηλώνει ο Lefebvre ήταν ότι αν η Σοβιετική Ένωση μπορούσε να εισβάλλει στο εσωτερικό της διαδικασίας λήψης αποφάσεων του αντιπάλου και να κατανοήσει τη διαδικασία αυτή, θα ήταν εφικτό να διοχετευθούν στον αντίπαλο πληροφορίες και δεδομένα τέτοια ώστε να τον οδηγήσουν σε προκαθορισμένες αποφάσεις. Ο Ρώσος θεωρητικός A.E. Komov προσφέρει μια σειρά από θεωρητικά παραδείγματα εφαρμογής του ανακλαστικού ελέγχου όπως:

• Τη διάσπαση της προσοχής κατά τις προπαρασκευαστικές φάσεις των πολεμικών επιχειρήσεων. Δημιουργώντας μια πραγματική ή φανταστική απειλή εναντίον ενός από τα πιο ζωτικά σημεία της εχθρικής διάταξης, όπως τα

---

[110] R. Bikkenin, "Information Conflict in the Military Sphere: Basic Elements and Concepts,"

[111]Timothy L. Thomas, "Human Network Attacks," *Military Review* (September-October 1999): <http://fmso.leavenworth.army.mil/fmsopubs/issues/humannet/humannet.htm> (August 30, 2002).

[112] Timothy Thomas, "Russia's Reflexive Control Theory & The Military," *The Journal of Slavic & Military Studies*, Vol. 17, London, UK: Frank Cass, 2004, pp. 237–256.

[113] Brian Daily and Patrick Parker, "*Soviet Strategic Deception,"* London, UK: The Free Press, 1987, p. 294.

πλευρά και τα νώτα, τον εξαναγκάζεις να επανεκτιμήσει τον τρόπο ενεργείας του.

• Την Υπερφόρτωση-συχνά εκδηλώνεται με την αποστολή στον εχθρό ενός μεγάλου όγκου αντικρουόμενων πληροφοριών.

• Την Παράλυση δημιουργώντας την πεποίθηση συγκεκριμένης απειλής για ένα ζωτικό συμφέρον ή αδύνατο σημείο.[114]

Όσον αφορά την πληροφοριακή-τεχνολογική πτυχή του πληροφοριακού πολέμου, σε ένα άρθρο που δημοσίευσε το 1999 ο τότε Ρώσος υπουργός Άμυνας Ιγκόρ Σεργκιέβεφ, περιέγραψε ως προτεραιότητες για τις ένοπλες δυνάμεις της Ρωσίας τα επόμενα χρόνια τα παρακάτω συστήματα: Όπλα καθοδηγούμενα με ηλεκτρομαγνητική ενέργεια, κυβερνοόπλα, μη ανιχνεύσιμες και μη επανδρωμένες πλατφόρμες μάχης και όπλα ακριβείας μεγάλου βεληνεκούς.[115] Το ρωσικό στρατιωτικό περιοδικό Στρατιωτική Παρέλαση ανέλυσε κατά διαστήματα το πώς εφαρμόστηκε στην πράξη το σχέδιο του Σεργκιέβεφ. Για παράδειγμα, στο πρώτο τεύχος του 2003, είχε άρθρα για μη επανδρωμένα αεροσκάφη αναγνώρισης, για συσκευές επικοινωνίας, για ραντάρ με ηλεκτρονικό σύστημα ελέγχου πορείας, τεχνολογίες λέιζερ για συλλογή πληροφοριών, υψηλής ακρίβειας πυραύλους cruise, ψηφιακές τεχνολογίες χαρτογράφησης, συστήματα αυτόματου ελέγχου, και έξυπνα συστήματα καθοδήγησης.

## ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΗΣ ΤΣΕΤΣΕΝΙΑΣ

Η πρόσφατη σύγκρουση στην Τσετσενία έχει προσφέρει παραδείγματα τόσο της τεχνολογικής όσο και της ψυχολογικής διάστασης των πληροφοριακών επιχειρήσεων. Ο Ρώσος συγγραφέας Panchenkov εξηγεί την πληροφοριακή-ψυχολογική ήττα των ρωσικών ενόπλων δυνάμεων στην πρώτη (1994-1996) σύγκρουση στην Τσετσενία και τα μέτρα που ελήφθησαν για τη διόρθωση της κατάστασης στη δεύτερη σύγκρουση. Στην πρώτη σύγκρουση, τα ρωσικά μέσα ενημέρωσης δεν ήταν υπό τον έλεγχο του κράτους και συχνά χρηματοδοτούνταν από Τσετσένους. Επίσης το Ρωσικό Υπουργείο Άμυνας δεν είχε στη διάθεση του διαπιστευμένους δημοσιογράφους ώστε να ενημερώνουν με φιλτραρισμένες πληροφορίες τη Ρώσικη κοινή γνώμη. Όπως σημείωσε ο Γενικός Γραμματέας του Στρατού Makhmut Gareyev, κανένας στρατός δεν μπορεί να λειτουργήσει με επιτυχία εάν ... είναι ηθικά αποδιοργανωμένος και χτυπημένος από τους συμπατριώτες του και τα μέσα μαζικής ενημέρωσης.[116] Αντίθετα, στη δεύτερη σύγκρουση, ιδρύθηκαν κέντρα πληροφόρησης σε δύο δημοκρατίες που γειτνιάζουν με την Τσετσενία, αυτές του Νταγκεστάν και της Βόρειας Οσσετίας. Οι δημοσιογράφοι ήταν εξοπλισμένοι με βίντεο και ενημερωτικό υλικό, και συνοδεύονταν σε συγκεκριμένες τοποθεσίες από επίσημους αντιπροσώπους. Με τον τρόπο αυτό, τα κέντρα πληροφοριών ήταν σε θέση να ασκήσουν καλύτερο πληροφοριακό έλεγχο στα δεδομένα των συγκρούσεων.[117] Ο Panchenkov επίσης σημείωσε ότι κατά την έναρξη της δεύτερης σύγκρουσης

---

[114] See *www.au.af.mil/info-ops/perception.htm#reflexive*

[115] Igor Sergeyev, "The Main Factors which Determine Russia's Military-Technical Policy on the Eve of the 21st Century," Krasnaya Zvezda, 9 December 1999, as translated and downloaded from the FBIS web site on 6 February 2004.

[116] V. V. Panchenkov, "Lessons from the Information War in the North Caucasus," Vooruzhenie, Politika, Konversiia, No 4 2002, downloaded from the FBIS web site on 5 February 2004.

[117] Ibid.

στην Τσετσενία, το 1999, ανευρέθηκαν περισσότερα από 150 σημεία ελέγχου και ράδιο-ηλεκτρονικές εγκαταστάσεις που λειτουργούσαν προς το συμφέρον των παράνομων ένοπλων σχηματισμών. Μέχρι το τέλος του Σεπτέμβριου, 77 από αυτούς είχαν καταστραφεί από άμεσα πυρά, συμπεριλαμβανομένων 22 σε σύνολο 38 ραδιοφωνικών σταθμών. Τέλος, περίπου το 90% των σταθμών βάσης των ανταρτών που χρησιμοποιούνταν για ραδιοεπικοινωνία και άλλους τύπους επικοινωνιών, είτε κατασχέθηκαν είτε τέθηκαν εκτός λειτουργίας.[118]

## ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΗΣ ΓΕΩΡΓΙΑΣ

Ο πόλεμος στη Γεωργία το 2008 αποτέλεσε μεταξύ άλλων και το προνομιακό πεδίο εφαρμογής της διαδικασίας του ανακλαστικού ελέγχου από τις Ρώσικες Ένοπλες Δυνάμεις. Αυτήν την άποψη ενστερνίζεται ο απόστρατος Αντισυνταγματάρχης Charles Blandy που υπηρέτησε ως κορυφαίος ειδικός στο Κέντρο Ερευνών της Ακαδημίας Άμυνας του Ηνωμένου Βασιλείου. Ο Blandy πιστεύει ότι μπορεί να βρει αποδείξεις του αντανακλαστικού έλεγχου στην πορεία της εισβολή της Ρωσίας στη Γεωργία το 2008, επισημαίνοντας ότι: οι Σοβιετικοί και τα Ρώσικα γενικά επιτελεία, για ένα μεγάλο χρονικό διάστημα, έχουν μελετήσει την εφαρμογή της ανακλαστικής θεωρίας ελέγχου. . . προκειμένου να επηρεάσουν τη διαδικασίας λήψης αποφάσεων του εχθρού.[119]

Ο Blandy θεωρεί ότι ο χαρακτήρας και η προσωπικότητα του Προέδρου της Γεωργίας Μιχαήλ Σαακασβίλι, ωρίμασαν τις σκέψεις για την εφαρμογή αυτής της θεωρίας. Ο Σαακασβίλι ήταν από φύσεως θερμόαιμος, βιαστικός στις αποφάσεις του και μέθυσος. Κατά την άποψή του, οι Ρώσοι ήξεραν πώς να αυξήσουν την πολιτική πίεση πάνω του, αλλά και το πώς θα ενεργήσει, όταν η πίεση γινόταν ανυπόφορη. Η πίεση ήταν σταδιακή και προέβαλλε σκόπιμα στη διεθνή πολιτική τις απειλές της Ρωσίας για το θέμα των ημι-αυτόνομων Δημοκρατιών της Νότιας Οσετίας και της Αμπχαζίας για μερικά χρόνια. Ωστόσο, αυτό που ενέτεινε την κρίση και εξόργισε τον Πρόεδρο Σαακασβίλι οδηγώντας τον σε λανθασμένες αποφάσεις, ήταν η ανάπτυξη των ρωσικών στρατευμάτων την άνοιξη του 2008 στην Αμπχαζία. Ο Blandy αναφέρεται ενδεικτικά, στο ψυχολογικό προφίλ του Σαακασβίλι που είχε δημοσιευτεί στην ρωσική στρατιωτική εφημερίδα Krasnaya Zvezda, και που σύμφωνα με εκτιμήσεις και μελέτες, είχε δημιουργήσει ένα χρήσιμο πρότυπο για τον τρόπο με τον οποίο λαμβάνει αποφάσεις ο γεωργιανός πρόεδρος.[120] Παράλληλα, ο πόλεμος της Γεωργίας υπήρξε η πρώτη ιστορική περίπτωση όπου μία επίθεση στο κυβερνοχώρο συντονίσθηκε με σημαντικές συμβατικές δράσεις μάχης. Οι «Ρώσοι εισβολείς» πραγματοποίησαν μια πρόβα τζενεράλε για την συγχρονισμένη κυβερνοεπίθεση τους στις αρχές Ιουλίου του 2008. Ο ερευνητής ασφαλείας της εταιρίας Arbor Networks, Jose Nazario, παρατήρησε από το Λέξινγκτον της Μασαχουσέτης στις αρχές Ιουλίου, μια ροή δεδομένων που απευθυνόταν σε κυβερνητικούς δικτυακούς τόπους της Γεωργίας και περιείχε το μήνυμα: «win+love+in+Russia.» Στις 20 Ιουλίου, το ίδρυμα Shadowserver που είναι ένα ιντερνετικό παρατηρητήριο στελεχωμένο με ειδικούς σε θέματα διακίνησης κακόβουλου λογισμικού στο διαδίκτυο, εντόπισε συντονισμένες αποστολές εκατομμυρίων αιτήσεων που

---

[118] Ibid.

[119] Charles Blandy, "*Provocation, Deception, Entrapment: The Russo-Georgian Five Day War,"* ARAG Paper 09/01, Swindon, UK: UK Defense Academy, 2009.

[120] Charles Blandy, "Georgia & Russia: A Further Deterioration in Relations,*"* ARAG paper, Swindon, UK: UK Defense Academy, August 22, 2008.

υπερφόρτωσαν και γκρέμισαν τους γεωργιανούς servers και είναι γνωστές ως **επιθέσεις άρνησης εξυπηρέτησης (Denial-of-service attack, DoS attack)**. Οι επιθέσεις κατευθύνονταν και εναντίον της επίσημης ιστοσελίδας του Γεωργιανού προέδρου που αναγκάστηκε να κλείσει για 24 ώρες. Μετέπειτα αναλύσεις απέδειξαν ότι οι επιθέσεις αυτές εκπορεύονταν από ένα σύστημα διοίκησης και ελέγχου που είχε την έδρα του στις ΗΠΑ.[121]

Παρά τις επίσημες διαψεύσεις από τη Μόσχα, η ρωσική επίθεση κατά των στρατιωτικών στόχων της Γεωργίας και των δικτύων της κυβέρνησης ήταν άκρως επιτυχημένη. Φαίνεται ότι 54 web sites στη Γεωργία που σχετίζονται με την επικοινωνία, την ενημέρωση, την οικονομία και τις κυβερνητικές αρχές δέχθηκαν επίθεση από κακοποιά στοιχεία εντός της Ρωσίας. Έτσι, όταν στις 8 Αυγούστου τα άρματα μάχης και τα στρατεύματα διέσχιζαν τα σύνορα και τα βομβαρδιστικά πραγματοποιούσαν εξόδους, οι γεωργιανοί πολίτες δεν μπορούσαν να έχουν πρόσβαση σε ιστοσελίδες για πληροφορίες και οδηγίες.[122] Οι επιθέσεις περιελάμβαναν επίσης επεμβάσεις σε ιστοσελίδες για να εξυπηρετηθούν Ρώσικοι σκοποί προπαγάνδας.[123] Στο πλαίσιο αυτό, η εικόνα του Γεωργιανού προέδρου Σαακασβίλι που ήταν αναρτημένη στην προσωπική του ιστοσελίδα παραμορφώθηκε και παραλληλίστηκε με πορτραίτα του Αδόλφου Χίτλερ.

Το κέντρο βάρους της Ρωσικής επίθεσης υπήρξε η Γεωργιανή κυβέρνηση. Εργασίες που εκτελέστηκαν από Ρώσους χάκερ στον κυβερνοχώρο υποστήριξαν αυτή την προσπάθεια υποβαθμίζοντας την ικανότητα της γεωργιανής κυβέρνησης να επικοινωνεί τόσο εσωτερικά όσο και με τον έξω κόσμο. Στο τακτικό και επιχειρησιακό επίπεδο, στοχοποιήθηκαν συγκεκριμένες γεωγραφικές περιοχές πριν την έναρξη των συμβατικών επιχειρήσεων. Για παράδειγμα, τόσο επίσημες ιστοσελίδες, όσο και τοπικές ειδησεογραφικές ιστοσελίδες στο Γκόρι κατέρρευσαν δεχόμενες επιθέσεις άρνησης εξυπηρέτησης, πολύ πριν τα ρωσικά αεροπλάνα φτάσουν στην περιοχή.[124] Ένα σημαντικό στρατηγικό ζήτημα στον πόλεμο της Γεωργίας είναι το ότι οι κυβερνοεπιθέσεις των Ρώσων ιδιωτών χάκερ, ήταν στενά συντονισμένες με τους γενικούς στρατηγικούς στόχους της ρωσικής κυβέρνησης: «Για παράδειγμα, δεν επιχείρησαν να υπονομεύσουν εγκαταστάσεις που αν κατέρρεαν θα επέφεραν χάος ή τραυματισμούς, όπως εκείνες που συνδέονται π.χ. με σταθμούς παραγωγής ηλεκτρικής ενέργειας ή τερματικούς σταθμούς πετρελαίου, αλλά μόνο όσες που θα μπορούσαν να προκαλέσουν μια συγκριτική «ταλαιπωρία». Αυτό αντικατοπτρίζεται στις ρωσικές ενέργειες εναντίον του υψίστης στρατηγικής σημασίας πετρελαιαγωγού Μπακού-Τσεϊχάν της Γεωργίας. Η Ρωσία βομβάρδισε όλες τις περιοχές γύρω από τον αγωγό, χωρίς όμως να πλήξει τον ίδιο, στέλνοντας ένα σαφές μήνυμα ότι θα μπορούσε να το πράξει, αν το επιθυμούσε. Η επίθεση στον κυβερνοχώρο ήταν απόλυτα ευθυγραμμισμένη με την συνολική

---

[121] Markoff J. 2008 "Before the Gunfire, Cyber attacks" International Herald Tribune, 3 August. On the Internet: http://www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html

[122] Jon Oltsik "Russian Cyber Attack on Georgia: Lessons Learned?" Network World, (17 August 2009), found at: http://www.networkworld.com/community/node/44448.

[123] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government" LA Times, (13 August 2008), found at: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html and Associated Press "Russian Hackers Attack Georgia in Cyberspace" Fox News (13 August 2008), found at: http://www.foxnews.com/story/0,2933,402406,00.html

[124] Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government" LA Times, (13 August 2008), found at: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

στρατηγική της Ρωσίας όσον αφορά το θέμα της πετρελαϊκής υποδομής της Γεωργίας.[125] Εν κατακλείδι, το Νορβηγικό Υπουργείο Άμυνας σε μία έκθεση που συνέταξε το 2010, αποτύπωσε με τον καλύτερο τρόπο το περίγραμμα των πληροφοριακών επιχειρήσεων του πολέμου της Γεωργίας. Στην ενημέρωση που έλαβε χώρα στα πλαίσια του ΝΑΤΟ, επεσήμανε ότι η ρωσική πληροφοριακή εκστρατεία επικεντρώθηκε σε τέσσερις στρατηγικούς στόχους: (1) τη δυσφήμιση και την ποινικοποίηση της Γεωργίας ως υπόλογου χώρας σε επιχειρήσεις γενοκτονίας (2) την υπονόμευση της αξιοπιστίας του Προέδρου Σαακασβίλι (3) τη νομιμοποίηση της δικής της εισβολή στη Νότια Οσετία και (4) τη διεξαγωγή δικτυοκεντρικών επιχειρήσεων μέσω Η/Υ για να αποκοπούν οι γεωργιανές επικοινωνίες στα κρίσιμα πρώτα στάδια της εκστρατείας. Ο επιθυμητός τελικός στόχος, σύμφωνα με τους Νορβηγούς, ήταν διττός: να αποτραπεί η επέμβαση του ΝΑΤΟ και η υποστήριξη στη Γεωργία, και ενισχυθεί η εσωτερική εγχώρια υποστήριξη.[126]

# ΚΕΦΑΛΑΙΟ 7$^{Ο}$
# ΚΙΝΕΖΙΚΕΣ ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Όπως οι Ρώσοι, έτσι και οι Κινέζοι συγγραφείς προσεγγίζουν τις πληροφοριακές επιχειρήσεις από τη δική τους οπτική γωνία. Ποικίλοι πολιτιστικοί, κοινωνικοί και ιστορικοί παράγοντες διαμορφώνουν τον Κινέζικο τρόπο σκέψης, δημιουργώντας μία ιδιαίτερη στρατιωτική κουλτούρα στον τρόπο διεξαγωγής του πληροφοριακού πολέμου. Το κοινό πχ. αίσθημα που είναι διάχυτο στην Κινέζικη κοινωνία ότι το έθνος τους βρίσκεται διαρκώς σε πόλεμο με ανώτερους τεχνολογικά αντιπάλους, αντανακλά σε μεγάλο βαθμό στην άποψη, ότι δεδομένης της κατώτερης θέσης της Κίνας, κάθε μέσο που θα προσφέρει στη νίκη είναι αποδεκτό. Επίσης ο τρόπος διεξαγωγής των πληροφοριακών επιχειρήσεων επηρεάζεται από τη Μαοϊκή παράδοση που ενθαρρύνει κατά κάποιο τρόπο τη συμμετοχή κάθε προσώπου στην ένοπλη πάλη.[127] Τέλος, η αρχαία επιρροή του Sun Tzu είναι συχνά εκ διαμέτρου εμφανής, τόσο ρητά όσο και με υπαινιγμούς.[128] Αυτό αποδεικνύεται από την ενσωμάτωση ιδεών όπως η έμμεση προσέγγιση, η ασυμμετρία, η ισορροπία

[125]US Cyber Consequences Unit, "The US-CCU Report on the Georgian Cyber Campaign," (August 2008) found at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf A

[126] "Russian Strategic/Operational Influence Activities in Georgia 2008," Briefing to NATO Senior Officers Info Ops Orientation Course, September 23, 2010.

[127] Mao Tse Tung, "The Struggle in the Chingkang Mountains, November 25, 1928" reprinted in *Selected Writing of Mao Tse Tung*, (Ft. Leavenworth: Command and General Staff College Combat Studies Institute, undated), pp 94-97.

[128]Yoshihara, Toshi. *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?* Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA: November 200, p. 26.

μεταξύ θετικών και αρνητικών, η αδυναμία έναντι της ισχύος, η δύναμη εναντίον της πονηριάς κλπ. Όλα τα στοιχεία που αφορούν το Κινέζικο δόγμα των πληροφοριακών επιχειρήσεων είναι διαβαθμισμένα ως απόρρητα και δεν διατίθενται ελεύθερα στο διαδίκτυο. Γενικά, οι Κινέζικες Πληροφοριακές Επιχειρήσεις βασίζονται σε έννοιες παρόμοιες με εκείνες που χρησιμοποιούνται από τις Ηνωμένες Πολιτείες. Επιπρόσθετα, οι Κινέζοι τις έχουν εξελίξει, για να ταιριάζουν καλυτέρα με την κινεζική κουλτούρα και το κομμουνιστικό δόγμα. Ο πατέρας του κινεζικού πληροφοριακού πολέμου, Υποστράτηγος Wang Pufeng, γράφει σχετικά ότι ο «Πληροφοριακός πόλεμος είναι ένα κρίσιμο στάδιο του πολέμου υψηλής τεχνολογίας....Στην καρδιά του βρίσκονται οι πληροφοριακές τεχνολογίες συνδυάζοντας τον στρατηγικό πόλεμο, τον ηλεκτρονικό πόλεμο, τον πόλεμο με κατευθυνόμενα βλήματα, τον πόλεμο της «μηχανοκίνησης» [Jidong zhan]. Πρόκειται ουσιαστικά για ένα νέο είδος πολέμου».[129] Ένας ακόμη ορισμός έχει δοθεί από τον πρώην υφυπουργό Επιστήμης & Τεχνολογίας και Βιομηχανίας για την Εθνική Άμυνα, Xie Guang, ο οποίος σημειώνει ότι: *«Οι Πληροφοριακές επιχειρήσεις αφορούν τη συνολική χρήση των διαφόρων τύπων πληροφοριών, του εξοπλισμού και των συστημάτων, ιδιαίτερα των συστημάτων διοίκησης, με σκοπό να επηρεάσουν τη δυνατότητα του εχθρού να λαμβάνει αποφάσεις και την ίδια στιγμή τη χρήση όλων των δυνατών μέσων για να διασφαλιστεί ότι τα φίλια συστήματα δεν έχουν καταστραφεί ή επηρεαστεί».* [130]

Οι Κινέζικες πληροφοριακές επιχειρήσεις έχουν έξι υποδιαιρέσεις τις οποίες έχει περιγράψει ο διευθυντής του τμήματος Πληροφοριακού Πολέμου του Γενικού Επιτελείου του Λαϊκού Στρατού της Κίνας, Στρατηγός Dai Qingmin, σε μία συνέντευξη που έδωσε το 2002 στο Κινέζικο περιοδικό *«Κινέζικη Στρατιωτική Σκέψη»*. Αυτές αναλυτικά είναι η επιχειρησιακή ασφάλεια, η εξαπάτηση, οι επιθέσεις εναντίον δικτύων, τα συστήματα ηλεκτρονικού πολέμου, η συλλογή πληροφοριών και η φυσική καταστροφή. Στις στρατιωτικές προτεραιότητες της Κίνας, δύο από τις έξι αυτές διαστάσεις του πληροφοριακού πολέμου έχουν ένα αισθητό προβάδισμα: ο ηλεκτρονικός πόλεμος και ο δικτυοκεντρικός πόλεμος. Ειδικότερα, μεγάλη σημασία αποδίδεται στην έννοια του «ολοκληρωμένου δικτυοκεντρικού ηλεκτρονικού πολέμου» που αναφέρεται σε μια σειρά από ενέργειες μάχης σε συνεργασία με την ολοκληρωμένη χρήση ηλεκτρονικών αντιμέτρων στο πληροφοριακό πεδίο, με σκοπό να διαταραχθεί η κανονική λειτουργία των δικτυοκεντρικών πληροφοριακών συστημάτων μάχης του εχθρού, και να προστατευθούν τα αντίστοιχα φίλια. Ο στόχος του ολοκληρωμένου δικτυοκεντρικού ηλεκτρονικού πολέμου είναι η απόκτηση πληροφοριακής υπεροχής, σύμφωνα με τον Dai.[131] Τα χαρακτηριστικά γνωρίσματα της πληροφοριακής υπεροχής είναι τρία: Επιτρέπει ελευθερία κινήσεων στην πληροφοριακή σφαίρα, διεξάγεται σε τρεις περιοχές (ηλεκτρομαγνητισμός, δίκτυα υπολογιστών, γνωστικές διεργασίες) και δύο επίπεδα (επίθεση κατά των συστημάτων πληροφοριών, επίθεση κατά της ανθρώπινης νόησης) και

[129]Wang Pufeng, "Xinxi zhanzheng yu junshi geming" (Information Warfare and the Revolution in Military Affairs), Beijing: Junshi kexueyuan, 1995. Quoted in Mulveron, 1999, "The PLA and Information Warfare"

[130] Anand, Vinod. "Chinese Concepts and Capabilities of Information Warfare." Strategic Analysis, Indian Institute for Defence Studies and Analyses, Vol: 30, Issue:4, October 2006. (Accessed 15 April 2011).

[131]Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002, pp 112-117 as translated and downloaded from the FBIS web site.

επηρεάζει τα γεγονότα στην πληροφοριακή διάσταση με τέτοιο τρόπο, έτσι ώστε να παράγει αποτελέσματα στη φυσική διάσταση.[132]

Γνωρίζοντας τον καθοριστικό ρόλο που διαδραματίζει η πληροφοριακή υπεροχή, οι Κινέζοι έχουν επίσης αναπτύξει με δικιά τους πρωτοβουλία μία θεωρία που είναι γνωστή ως «ιδέα των τριών πολέμων» **(*san zhong zhanfa*).**[133] Σε μία ετήσια έκθεσή του το 2011, το Αμερικάνικο Υπουργείο Άμυνας στο Κογκρέσο επισημαίνει σχετικά με την θεωρία αυτή τα παρακάτω: [134] *«Ο Λαϊκός Απελευθερωτικός Στρατός έχει στραφεί στην ανάπτυξη ασύμμετρων στρατηγικών και ικανοτήτων με την επωνυμία «Το Ρόπαλο του Δολοφόνου», που έχουν σχεδιαστεί για να παρέχουν στρατιωτικά πλεονεκτήματα στις κατώτερες τεχνολογικά Κινέζικες δυνάμεις και έτσι να ανακατευθύνουν τη ροή μίας σύγκρουσης.»* Από τα τέλη της δεκαετίας του 1990, ο όρος εμφανίζεται πιο συχνά σε κινεζικές στρατιωτικές εκδόσεις και περιοδικά, ιδίως στο πλαίσιο ενδεχόμενης σύγκρουσης με τις Ηνωμένες Πολιτείες για το θέμα της κυριότητας της Ταϊβάν.[135] Αν και υπάρχει ανεπαρκής πληροφόρηση από ανοικτές πηγές για την στρατηγική «Ρόπαλο του Δολοφόνου», ωστόσο, σε μια χώρα που γέννησε τον Sun Tzu, φαίνεται πιθανό ότι σε αυτήν εμπεριέχονται τεχνικές που παρέχουν οδηγίες για τον επηρεασμό της στάσης και της συμπεριφοράς ενός ακροατηρίου. Ο Timothy Thomas πάνω στο θέμα αυτό αναφέρει τα κάτωθι: «Το *Δόγμα των Ψυχολογικών Επιχειρήσεων στην αρχαία Κίνα περιγράφει σαν κύριο στόχο του πολέμου την νίκη επί του αντιπάλου χωρίς όμως την καταφυγή σε πόλεμο. Η βασική αρχή του πολέμου είναι η μάχη για τον έλεγχο της καρδιάς, το μυαλού και του ηθικού του αντιπάλου.»*[136]

Στο ίδιο πνεύμα ασύμμετρων στρατηγικών οι Κινέζοι έχουν εισαγάγει την έννοια των «στρατηγημάτων πληροφοριακού πολέμου», αντιμετωπίζοντας τις πληροφοριακές επιχειρήσεις όπως και πολλά άλλα είδη του πολέμου, σαν μία στρατηγική μονομαχία μεταξύ δύο διοικητών. *«Τα στρατηγήματα είναι τα συστήματα ή οι μέθοδοι που έχουν επινοηθεί και χρησιμοποιούνται από τους διοικητές για την απόκτηση και διατήρηση πληροφοριακής υπεροχής, με βάση έξυπνες μεθόδους, ώστε να είναι εφικτή η επικράτηση στον πληροφοριακό πόλεμο με ένα σχετικά μικρό κόστος»*[137] Με βάση τον παραπάνω ορισμό, συνάγεται το συμπέρασμα ότι ο αριθμός των στρατηγημάτων των οποίων δύναται να κάνει χρήση ένας διοικητής είναι απεριόριστος και οριοθετείται μόνο από το εύρος της ανθρώπινης επινοητικότητας και φαντασίας. Γενικά όμως και για λόγους τυπολογίας όλα τα στρατηγήματα ταξινομούνται σε τέσσερα μεγάλα υποσύνολα-κατηγορίες. Η πρώτη δέσμη των πληροφοριακών στρατηγημάτων εκμεταλλεύεται τη γνωστική διάσταση του πληροφοριακού περιβάλλοντος στοχεύοντας στη

---

[132] Dai Qingmin, "On Seizing Information Supremacy," China Military Science, April 2003, pp 9-17, as translated and downloaded from the FBIS web site.

[133] Office of the Secretary State for Defense, "*Military Power of the People's Republic of China 2008: Annual Report to Congress,"* Washington, DC: U.S. Department of Defense, 2008.

[134] Office of the Secretary of State for Defense "*Military and Security Developments Involving the People's Republic of China*, *Annual Report to Congress*," Washington, DC: U.S. Department of Defense, 2011.

[135] Timothy A Walton, "*China's Three Warfares,"* Herndon, VA: Delex Consulting, January 18, 2012.

[136] Timothy Thomas, "*Dragon Bytes*," Ft. Leavenworth, KS: Foreign Military Studies Office, 2004, p. 98.

[137] Niu Li, Li Jiangzou and Xu Dehui, "On Information Warfare Stratagems," *China Military Science* in Chinese (August 20, 2000), 115-122. Translated and downloaded from the FBIS website. (February 11, 2003).

διανοητική ικανότητα του εκάστοτε διοικητή και επηρεάζοντας με κατάλληλους χειρισμούς την αντίληψη, τις γνώσεις και τις πεποιθήσεις του, ώστε να τον οδηγήσει στη λήψη λανθασμένων αποφάσεων. Κάτι τέτοιο βέβαια προϋποθέτει την εκ των προτέρων εις βάθος γνώση του χαρακτήρα και της προσωπικότητας του αντιπάλου ηγέτη. Η δεύτερη ομάδα στρατηγημάτων βασίζεται στην τεχνολογία η οποία χρησιμοποιείται για να εξασφαλισθεί υπεροχή έναντι του εχθρού. Η συγκεκριμένη υπεροχή αποκτάται είτε με την ανάπτυξη ανώτερων πληροφοριακών συστημάτων σε σχέση με τα αντίστοιχα του αντιπάλου, είτε με την αποτελεσματικότερη και αποδοτικότερη χρήση των ήδη υπαρχόντων ώστε να υλοποιηθεί ένας καλύτερος σχεδιασμός. Τα στρατηγήματα «πολυδιάστατου περιεχομένου» αποτελούν μία τρίτη διακριτή κατηγορία. Σε αυτήν την περίπτωση γίνεται χρήση και των τριών διαστάσεων του πληροφοριακού περιβάλλοντος, της γνωστικής, της φυσικής και της ενημερωτικής με τέτοιο τρόπο που να εξασφαλίζεται η ενσωμάτωση των στρατηγημάτων σε ένα γενικότερο πλέγμα-πλαίσιο δράσεων που εξυπηρετούν αντικειμενικούς στρατιωτικούς σκοπούς. Τέλος, η τέταρτη κατηγορία αποτελείται από τεχνάσματα που εφαρμόζονται με σκοπό τον έλεγχο της συνολικής πληροφοριακής διαδικασίας στο πέρασμα του χρόνου. Τα στρατηγήματα αυτού του πεδίου διασφαλίζουν την ακεραιότητα της φίλιας πληροφοριακής διαδικασίας και υπονομεύουν την αντίστοιχη διαδικασία του εχθρού. Επίσης, σχετίζονται με την επίθεση ή την άμυνα πληροφοριακών συστημάτων σε περιόδους κρίσης και έντασης. Στην ουσία τα στρατηγήματα αποτελούν ένα απαραίτητο βοήθημα για το διοικητή και το επιτελείο ώστε να είναι σε θέση να κάνουν ισόρροπη χρήση όλων των διαστάσεων του πληροφοριακού περιβάλλοντος, ιδιαίτερα δε του γνωστικού και του ενημερωτικού. Ειδικά οι δύο τελευταίες κατηγορίες αφορούν τον συγχρονισμό όλων των δράσεων τόσο στο χώρο όσο και στο χρόνο. Αυτό είναι ένα θέμα υψηλής προτεραιότητας για τις πληροφοριακές επιχειρήσεις, δεδομένου του ότι η σωστή εκμετάλλευση τόσο του χώρου όσο και του χρόνου, είναι καθοριστικής σημασίας για την παραγωγή μαζικών αποτελεσμάτων. Η προθυμία της Κίνας να εμπλακεί σε ευαίσθητα ζητήματα με μη συμβατικούς στρατιωτικούς τρόπους, αποδεικνύεται από τον «πόλεμο του Twitter» που ξέσπασε το Μάρτιο του 2012, για το θέμα του Θιβέτ.[138] Τότε, οι οθόνες των υπολογιστών πλημμύρισαν με τους λογότυπους #Tibet και #Freetibet, εκτοξεύοντας απειλές εναντίον των ακτιβιστών που υποστηρίζουν την ανεξαρτησία του Θιβέτ. Αν και αυτή ήταν ίσως η πρώτη κινεζική μεγάλη πληροφοριακή εκστρατεία στο εξωτερικό, τα τελευταία χρόνια ακολούθησε μια σειρά από παρόμοια προγράμματα που συνδέονται με συγκεκριμένους οικονομικούς και πολιτικούς στόχους. Το 2013 υπήρξαν αναφορές των μέσων ενημέρωσης για τη δημιουργία μιας ταξιαρχίας, που ενδεχομένως, ονομάζεται waumao και αριθμεί 60.000 ανθρώπους, οι οποίοι πληρώνονται 75 σεντς ανά Tweet από το κυβερνών κινεζικό καθεστώς για να κάνουν θετικά σχόλια σχετικά με το Κομμουνιστικό Κόμμα και το κινεζικό ισοδύναμο του Twitter, το Weibo.[139]

[138] Adam Segal, "China's Twitter War," *Asia Unbound*, March 22, 2012.
[139] See *www.weibo.com*.

# ΚΕΦΑΛΑΙΟ 8$^{Ο}$
# ΠΡΟΤΑΣΕΙΣ-ΣΥΜΠΕΡΑΣΜΑΤΑ ΓΙΑ ΠΙΟ ΑΠΟΔΟΤΙΚΗ ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Έχοντας παρουσιάσει και αναλύσει όλο το φάσμα των πληροφοριακών επιχειρήσεων, όπως τουλάχιστον αυτές διεξάγονται στις προηγμένες στρατιωτικά χώρες, προκύπτουν χρήσιμα συμπεράσματα σχετικά με τους παράγοντες εκείνους που επηρεάζουν θετικά ή αρνητικά την επιτυχή εφαρμογή και διεξαγωγή του πληροφοριακού πολέμου. Στο πλαίσιο αυτό, προτείνονται τρόποι και αναλύονται οι προϋποθέσεις, κάτω από τις οποίες θα ήταν εφικτή η καλύτερη εκμετάλλευση των πληροφοριακών επιχειρήσεων στο σύγχρονο πεδίο της μάχης.

### Απόκτηση και Διατήρηση Αξιοπιστίας.

Η αποκάλυψη σκόπιμης παραπληροφόρησης σε οποιαδήποτε πληροφοριακή δράση βλάπτει την αξιοπιστία των ενόπλων δυνάμεων μίας χώρας και έχει πολλές παράπλευρες συνέπειες και επιπτώσεις. Επομένως, οι προσπάθειες διαμόρφωσης της κοινής γνώμης θα πρέπει να βασίζονται μόνο σε πραγματικά περιστατικά. Η αξιοπιστία των ψυχολογικών και πληροφοριακών επιχειρήσεων εξασφαλίζεται με την απομόνωση των παραπλανητικών από τα αληθινά δεδομένα. Είναι πολύ σημαντικό να επιτευχθεί συντονισμός μεταξύ των δύο αυτών δράσεων αλλά να μην υπάρχει ανάμειξη μεταξύ των ψευδών και πραγματικών τους συστατικών.

### Σφαιρική Γνώση του Περιβάλλοντος των Επιχειρήσεων.

Κατά το στάδιο αξιολόγησης της αποτελεσματικότητας των μηνυμάτων των ψυχολογικών επιχειρήσεων, έχει αποδειχθεί ότι μία από τις μεγαλύτερες ανεπάρκειες είναι η ελλιπής γνώση των κοινωνικών, πολιτικών, θρησκευτικών και πολιτισμικών παραγόντων που συμβάλλουν στη διαμόρφωση της γνώμης μίας κοινωνίας. Γι' αυτό το λόγο, οι υπηρεσίες πληροφοριών θα πρέπει να επικεντρώσουν τις προσπάθειές τους στην απόκτηση μια βαθιάς και εμπεριστατωμένης κατανόησης των ιθαγενών ακροατηρίων. Αυτές οι πληροφορίες θα περιλαμβάνουν γενικά, αν και δεν θα πρέπει να περιορίζονται, σε γεωγραφικά, δημογραφικά, ψυχογραφικά (π.χ., κοινωνική τάξη, τον τρόπο

ζωής, την προσωπικότητα), και συμπεριφοριστικά χαρακτηριστικά όπως επίσης και στις συνήθειες των μέσων ενημέρωσης. Επίσης θα πρέπει να διατεθούν πόροι έτσι ώστε τα στρατεύματα που βρίσκονται στο πεδίο των επιχειρήσεων, να μπορούν να επικοινωνούν με περιφερειακούς εμπειρογνώμονες έξω από αυτό.

**Αποτελεσματική Μόχλευση της Πολιτικό-Στρατιωτικής Συνεργασίας-Ικανοποίηση Τοπικού Πληθυσμού.**

Η ανταπόκριση στις προσδοκίες του γηγενούς πληθυσμού συμβάλλει αναμφίβολα στην εδραίωση των αποτελεσμάτων που αποτελούν παράγωγο πληροφοριακών επιχειρήσεων. Η δημιουργία προσδοκιών για τη βελτίωση του βιοτικού επιπέδου δύναται να εφαρμοστεί σε όλα τα επίπεδα του πολέμου. Χρησιμοποιώντας όρους μάρκετινγκ, αυτό μπορεί να παραλληλιστεί με την αίσθηση ικανοποίησης που έχουν οι καταναλωτές μετά τη χρήση ενός προϊόντος ή μιας υπηρεσίας. Οι άμαχοι που ζουν σε περιοχές όπου διεξάγονται π.χ. επιχειρήσεις σταθεροποίησης, έχουν τη δυνατότητα να επιλέξουν την πλευρά με την οποία θα συμπαραταχθούν. Ο βαθμός στον οποίο είναι ικανοποιημένοι με τις διάφορες πτυχές της δράσης των ενόπλων δυνάμεων, θα αποτελέσει ένας κρίσιμο προσδιοριστικό παράγοντα στη λήψη των αποφάσεων τους. Ανεκπλήρωτες υποσχέσεις δημιουργούν απογοητευμένα κοινά και γι αυτό οι ένοπλες δυνάμεις πρέπει να είναι ιδιαίτερα προσεκτικές στην πολιτική τους απέναντι στους πληθυσμούς.

**Καθιέρωση Δεικτών Συμπεριφοράς**.

Από την αρχή μίας επιχείρησης, είναι απαραίτητο να προσδιοριστούν οι ενδεδειγμένοι δείκτες για τη μέτρηση της αλλαγής της συμπεριφοράς του κοινού-στόχου. Αυτό απαιτεί μια σε βάθος κατανόηση της ομάδας-στόχου και των προτύπων συμπεριφοράς της, και συνειδητοποίηση του ποιες συμπεριφορές είναι πιο πρόσφορες για αλλαγή. Η πραγματική δυσκολία έγκειται στη διάκριση μεταξύ των παραγόντων που προκαλούν την αλλαγή συμπεριφοράς και εκείνων που απλώς συσχετίζονται με την αλλαγή. Γι' αυτό το λόγο είναι απαραίτητη η ανάλυση του ακροατηρίου στόχου μέσω ποιοτικών μεθόδων και η μέτρηση στάσεων, προθέσεων και αντιλήψεων που καθορίζουν τις αλλαγές στα ακροατήρια-στόχους.

**Αποτελεσματική Χρησιμοποίηση των Social Media.**

Σε όλο τον κόσμο, τα μέσα κοινωνικής δικτύωσης είναι όλο και πιο συνηθισμένα εργαλεία για πολιτικό και κοινωνικό ακτιβισμό. Η ταχεία εξάπλωση των blogs, των ιστοσελίδων κοινωνικής δικτύωσης, και η τεχνολογία μέσων επιμερισμού (όπως το YouTube), με τη βοήθεια της διάδοσης της κινητής τεχνολογίας, αλλάζει τις συνθήκες υπό τις οποίες οι ένοπλες δυνάμεις διεξάγουν στρατιωτικές επιχειρήσεις. Οι άνθρωποι μπορούν να χρησιμοποιήσουν την κοινωνική δικτύωση για να κινητοποιήσουν ομάδες με σκοπό την υποστήριξη ενός αντικειμενικού στόχου, χωρίς να εκθέτουν τον εαυτό τους σε κινδύνους και οικονομικά έξοδα. Σε απάντηση, οι κυβερνήσεις και τα θεσμικά όργανα μπορούν να κάνουν ελάχιστα για να αποτρέψουν την υλοποίηση των παραπάνω δράσεων αποτελεσματικά. Αν στρατιωτικοί ηγέτες δεν αντιληφθούν την συγκεκριμένη διάσταση αυτών των εργαλείων, δεν είναι σε θέση να κατανοήσουν και τις σημαντικές επιπτώσεις που έχουν για τις επιχειρήσεις.

Πώς μπορεί μια αποτελεσματική στρατηγική για τα μέσα κοινωνικής δικτύωσης να έχει επιπτώσεις στα αποτελέσματα των στρατιωτικών επιχειρήσεων; Σε ένα πρόσφατο άρθρο στην Αμερικάνικη Στρατιωτική Επιθεώρηση περιγράφεται η χρήση των νέων εργαλείων κοινωνικής δικτύωσης, στο δεύτερο πόλεμο του Λιβάνου το 2006, όπου συνεπλάκησαν οι ισραηλινές δυνάμεις και η οργάνωση Χεζμπολάχ.[140] Στο Λίβανο, η Χεζμπολάχ διεξήγαγε αποτελεσματικά ολοκληρωμένες πληροφοριακές επιχειρήσεις, ενσωματώνοντας τη διάσταση των μέσων κοινωνικής δικτύωση στις τακτικές της ενέργειες. Στο πλαίσιο αυτό, αναπαρήγαγε φωτογραφίες και βίντεο που είχαν τραβηχτεί στο πεδίο της μάχης και τα ανήρτησε σε blogs και στο YouTube, για να παρουσιάσει μια εξωραϊσμένη εικόνα της οργάνωσης και να αναδείξει ταυτόχρονα τις αρνητικές πτυχές δράσης των ισραηλινών ενόπλων δυνάμεων. Χρησιμοποίησε δηλαδή τις πληροφορίες αποτελεσματικά για τον περιορισμό των στρατηγικών επιλογών του Ισραήλ. Ύστερα από 33 μέρες μαχών, και την κήρυξη της κατάπαυσης του πυρός, η Χεζμπολάχ ήταν σε θέση να ισχυριστεί ότι πέτυχε μία νίκη και δημιούργησε μια «αντίληψη αποτυχίας» για το Ισραήλ, το οποίο αγνόησε την πραγματικότητα των νέων μέσων και επέλεξε τις παραδοσιακές πληροφοριακές στρατηγικές. Αντίθετα, στην επιχείρηση Cast Lead, οι ισραηλινές δυνάμεις εφάρμοσαν πιο αποτελεσματικές μεθόδους για τη χρήση των νέων μέσων ενημέρωσης. Ανέπτυξαν μια προληπτική στρατηγική που ενσωμάτωνε τα κοινωνικά μέσα και κινητοποιούσε την υποστήριξη των διαδικτυακά συνδεδεμένων ισραηλινών κοινοτήτων, ώστε να καθορίσουν την ημερήσια διάταξη στα μέσα ενημέρωσης και να διαμορφώσουν την εικόνα των μαχών.[141]

**Βελτίωση των Σχέσεων με τα ΜΜΕ.**

Τα παραδοσιακά μέσα ενημέρωσης παραμένουν ο κυριότερος και πιο αποτελεσματικός δίαυλος για τη διάχυση ενός μηνύματος. Γενικά, οι καλές σχέσεις με τους ρεπόρτερ και τον τύπο παρέχουν σημαντικά πλεονεκτήματα στην στρατηγική επικοινωνία. Ειδικά η πρόσβαση στα τοπικά μέσα ενημέρωσης κρίνεται ως ιδιαίτερα σημαντική επειδή βοηθούν στην αποκρυστάλλωση γνώμης σχετικά με τα επικοινωνιακά γεγονότα που διαδραματίζονται στο θέατρο των επιχειρήσεων και ως τούτου συνεισφέρουν στη λήψη των τελικών αποφάσεων. Σε αυτό το πλαίσιο, θα πρέπει να υπάρχει αγαστή συνεργασία και διάδραση μεταξύ των γραφείων τύπου των Ενόπλων Δυνάμεων και των ΜΜΕ και να δίνεται η δυνατότητα επικοινωνίας μεταξύ των ρεπόρτερ και των τοπικών διοικητών χωρίς να παραβλάπτεται φυσικά η ασφάλεια μίας επιχείρησης.

**Καλύτερη Συνεργασία με τον Ιδιωτικό Τομέα-Χρήση Νέων Τεχνολογιών.**

---

[140] William B. Caldwell, Denis M. Murphy, and Anton Menning, "Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts," *Military Review* (May–June 2009), 2–10.

[141] Ibid.

Οι καλύτεροι και πιο ανεπτυγμένοι στρατιωτικοί οργανισμοί του πλανήτη αδυνατούν να ανταποκριθούν πλήρως από μόνοι τους στις απαιτήσεις που προκύπτουν κατά την εφαρμογή πληροφοριακών σχεδίων και σχετίζονται με κρίσιμες υποδομές, τεχνολογίες αιχμής και εξειδικευμένο στελεχιακό δυναμικό. Γι' αυτό το λόγο απαιτείται εποικοδομητική συνεργασία από τον καιρό της ειρήνης με ιδιωτικούς-δημόσιους φορείς, την ακαδημαϊκή κοινότητα, τα πανεπιστήμια και τη βιομηχανία και η κινητοποίηση όλων των μη κυβερνητικών οργανώσεων και οργανισμών για να παραχθεί ένα ικανοποιητικό πληροφοριακό αποτέλεσμα σε περίοδο επιχειρήσεων, κρίσεως ή έντασης.

# ΕΠΙΛΟΓΟΣ

Η ανάπτυξη των δικτύων επικοινωνίας έχει μειώσει δραστικά τα τελευταία χρόνια τον αριθμό των απομονωμένων πληθυσμών ανά τον κόσμο. Η εμφάνιση της προηγμένης ενσύρματης και ασύρματης τεχνολογίας διευκολύνει την παγκόσμια επικοινωνία. Η δυνατότητα να μοιράζονται οι πληροφορίες σε σχεδόν πραγματικό χρόνο, ανώνυμα ή/ και με ασφάλεια, αποτελεί κοινό περιουσιακό στοιχείο για εταιρείες, ιδιώτες, ακόμη και βίαιες εξτρεμιστικές οργανώσεις. Στο πλαίσιο αυτό η πληροφορία συνιστά ένα ισχυρό εργαλείο τόσο ενημέρωσης όσο και επιρροής. Οι προηγμένες στρατιωτικά οντότητες έχοντας εγκαίρως αντιληφθεί την ανεκτίμητη πολλαπλασιαστική αξία της πληροφορίας στο πεδίο της μάχης, έχουν ενσωματώσει στο οπλοστάσιό τους τις πληροφοριακές επιχειρήσεις, τις οποίες διεξάγουν τόσο σε περιόδους ειρήνης, όσο και κρίσης-έντασης ή πολέμου. Οι πληροφοριακές επιχειρήσεις λαμβάνουν χώρα στο πληροφοριακό περιβάλλον που περιλαμβάνει τη γνωστική, ενημερωτική-πληροφοριακή και φυσική διάσταση. Οποιαδήποτε πληροφοριακή ενέργεια διεξάγεται μέσα στο περιβάλλον αυτό, βρίσκεται ή θα πρέπει να βρίσκεται σε απόλυτη σύμπνοια με το πλαίσιο της στρατηγικής επικοινωνίας που χαράσσεται και καθορίζεται σε ανώτατο επίπεδο ώστε να μην παράγονται αντιθετικά και συγκρουόμενα μηνύματα που βλάπτουν την εικόνα ενός κράτους.

Όπως κατέδειξαν τα πρόσφατα πολεμικά γεγονότα σε Γεωργία και Τσετσενία (και Ουκρανία που είναι σε εξέλιξη), οι πληροφοριακές επιχειρήσεις μεγιστοποιούν τα αποτελέσματα των συμβατικών δράσεων, προσβάλλοντας κύριες πληροφοριακές υποδομές και καθιστώντας δύσκολη έως αδύνατη τη λήψη αποφάσεων στο στρατηγικό αλλά και επιχειρησιακό επίπεδο. Συμβάλλοντας στην απόκτηση πληροφοριακής κυριαρχίας και υπεροχής εξουθενώνουν κατ'

ουσία την οποιαδήποτε δυνατότητα ικανοποιητικής ροής πληροφοριών, παράγοντας ασύμμετρα ψυχολογικά αποτελέσματα στους πληθυσμούς και τις οντότητες που τις υφίστανται. Οποιοσδήποτε επομένως στρατιωτικός οργανισμός παρανοεί ή παραμελεί να αναπτύξει ανάλογες δυνατότητες είναι πολύ πιθανό να εκπλαγεί δυσάρεστα πριν/η και με την έναρξη των επιχειρήσεων. Η ικανότητα διεξαγωγής αποτελεσματικών πληροφοριακών επιχειρήσεων συνδέεται με ένα πλήθος οικονομοτεχνικών παραγόντων αλλά κυρίως επηρεάζεται από την κουλτούρα των ενόπλων δυνάμεων από τη γενική στρατηγική μίας χώρας και από το βαθμό κατανόησης, αφομοίωσης και βούλησης εφαρμογής των παραπάνω δράσεων από τα ανώτατα κλιμάκια της ηγεσίας.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


- Armistead Leigh, "Information Operations: Warfare and the Hard Reality of Soft Power" Washington D.C. 2004.

- Armistead Leigh, "Information Operations Matters": Best Practices, Washington, D.C.: Potomac Books, 2010.

- Babst Stefanie, Public Diplomacy-The Art of Engaging and Influencing, Speech at NATO PfP Symposium, January 22, 2009

- Baldwin Robert, "A New Military Strategic Communication System", Advanced Military Studies Program, Fort Leavenworth, May 24, 2009.

- Bikkenin R., "Information Conflict in the Military Sphere: Basic Elements and Concepts," Morskoy, No 10, 2003 as translated and downloaded from the FBIS web site on 6 February 2004.

- Blandy Charles, "Provocation, Deception, Entrapment: The Russo-Georgian Five Day War," ARAG Paper 09/01, Swindon, UK: UK Defense Academy, 2009.

- Briefing to NATO Senior Officers Info Ops Orientation Course "Russian Strategic/Operational Influence Activities in Georgia 2008," September 23, 2010.

- Chiarreli Peter, "Learning from Our Modern Wars: The Imperatives of Preparing for a Dangerous Future," Military Review, September-October 2007.

- Paul Christopher, "Strategic Communication, Origins, Concepts and Current Debates", Santa Barbara, California, 2006.

- Cox Joseph, "Information Operations in Operations Enduring Freedom in Iraqi Freedom-What Went Wrong" School of Advanced Military Studies, United States Army Command and General Staff College.

- Cull J. Nicholas, "Public Diplomacy before Gull ion: The Evolution of a Phrase", New York: Routledge, 2009.

- Cull Nicholas, The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945-1989, New York: Cambridge University Press, 2008.

- Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," China Military Science, Feb 2002 as translated and downloaded from the FBIS web site.

- Dai Qingmin, "On Seizing Information Supremacy," China Military Science, April 2003 as translated and downloaded from the FBIS web site.

- Daily Brian and Patrick Parker, "Soviet Strategic Deception," London, UK: The Free Press, 1987

- Daugherty E. William, "An account of the Origin of the Terms PsyWar and PsyOp" PSYWAR ORG. March 29, 2007

- Defense Academy of the United Kingdom, Cranfield University, UK, March 2009.

- Department of Defense, Strategic Communication Joint Integrating Concept.

- Department of Defense, Dictionary of Military and Associated Terms, Washington, D.C., Joint Publication 1-02, April 12, 2001

- Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.30, Washington D.C., April 2005.

- Department of the Army, Psychological Operations, Headquarters, Field Manual 3-05.301, Washington D.C., December 31, 2003.

- Dexter Filkins and James Glanz (8 November 2004). "With Airpower and Armor, Troops Enter Rebel-Held City". The New York Times, Retrieved 27 December 2008.

- Gregory Bruce, "Public Diplomacy and National Security Lessons from the U.S. Experience", Small Wars Journal, August 14, 2008.

- Gregory Bruce, Mapping Smart Power in Multi Stakeholder Public Diplomacy/Strategic Communication, transcript from "New Approached to U.S. Outreach " forum, George Washington University, The Institute for Public Diplomacy and Global Communication, October 5, 2009

- Hosmer Stephen, Psychological Effects of U.S. Air Operations in Four Wars 1941-1991: Lessons from U.S. Commanders MR-576-AF Santa Monica, CA: Rand Corporation, 1996.

- Joint Chiefs of Staff, Doctrine for Joint Psychological Operations, Joint Publication 3-53 September 5, 2003.

- Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, as amended through March 22, 2007 Washington, DC, April 12, 2001.

- Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 Washington, DC, February 13, 2006.

- Joint Chiefs of Staff, Military Deception, Joint Publication 3-13.4 July 13, 2006.

- Joint Chiefs of Staff, Operation Security, Joint Publication 3-13.3 June 29, 2006.

- Lamb Christopher, Review of Psychological Operations Lessons Learned from Recent Operational Experience,Washington D.C.: National Defense University Press, September 2005.

- Latimer John, Deception in War: The Art of the Buff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military Histories, from the Trojan Horse to the Gulf War, New York: The Overlook Press, 2001.

- Lloyd Mark, "The Art of Military Deception", London, UK: Pen and Sword Books, 1997.

- Lord M. Kristin, Voices of America: U.S. Public Diplomacy for the 21st Century, Washington D.C.: The Foreign Policy Program at Brookings, 2008.

- Mann Edward, Gary Enders and Thomas R. Searle. Thinking Effects: Effects-Based Methodology for Joint Operations Maxwell AFB, AL: Air University Press, 2002.

- Mao Tse Tung, "The Struggle in the Chingkang Mountains, November 25, 1928" reprinted in Selected Writing of Mao Tse Tung, (Ft. Leavenworth: Command and General Staff College Combat Studies Institute, undated).

- Menn Joseph, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government" LA Times, (13 August 2008), found at: http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html and Associated Press "Russian Hackers Attack Georgia in Cyberspace" Fox News, 3 August 2008, found at: http://www.foxnews.com/story/0,2933,402406,00.html.

- Metz Thomas, "The Battle of Fallujah: A Case Study for Warfare in the Information Age," briefing to the Capitol Bohemian Club, 26 October 2005, Washington, D.C.

- Murphy Dennis, "Strategic Communication", in Department of Military Strategy, Planning and Operations Center for Strategic Leadership, Information Operations Primer, Carlisle, Pa.: U.S. Army War College, November 2009.

- Nakamura H. Kennon and Matthew C. Weed, U.S. Public Diplomacy: Background and Current Issues, December 18, 2009.

- NATO Allied Joint Doctrine for Information Operations, Joint Publication 3-10, November 2009.

- Niu Li, Li Jiangzou and Xu Dehui, "On Information Warfare Stratagems," China Military Science in Chinese August 20, 2000.

- Nye and Owens, "America's Information Edge". Foreign Affairs 75, April 1996.

- Office of the Secretary State for Defense, "Military Power of the People's Republic of China 2008: Annual Report to Congress," Washington, DC: U.S. Department of Defense, 2008.

- Office of the Secretary of State for Defense "Military and Security Developments Involving the People's Republic of China, Annual Report to Congress," Washington, DC: U.S. Department of Defense, 2011.

- Panchenkov V., "Lessons from the Information War in the North Caucasus," Vooruzhenie, Politika, Konversiia, No 4 2002, downloaded from the FBIS web site on 5 February 2004.

- Peters Ralph, "The Counterrevolution in Military Affairs—Fashionable thinking about defense ignores the great threats of our time," The Weekly Standard, Volume 11, 2, 6 February 2006.

- Price Alfred, Instruments of Darkness: The History of Electronic Warfare (New York 1978).

- Pinkerton James, "Covering the News with Deception'' Long Island Newsday (December 16, 2004).

- Rastorguyev S., "An Introduction to the Formal Theory of Information Warfare", Moscow 2003.

- Ricks, Thomas E. (2007). Fiasco: The American Military Adventure in Iraq, 2003–2005.

- Rumsfeld D. USS CONGRESS, House Armed Service Committee February 5, 2003

- Segal, Adam "China's Twitter War," Asia Unbound, March 22, 2012.

- Sergeyev Igor, "The Main Factors which Determine Russia's Military-Technical Policy on the Eve of the 21st Century," Krasnaya Zvezda, 9 December 1999, as translated and downloaded from the FBIS web site on 6 February 2004.

- Sun Tzu, The Art Of War (Oxford University Press, 1963.

- Schwartz H. Lowell Political Warfare against the Kremlin: US and British Propaganda Policy at the Beginning of the Cold War, Hampshire UK: Palgrave, Macmillan, 2009.

- Tatham Steve, "U.S. GOVERNMENTAL INFORMATION OPERATIONS AND STRATEGIC COMMUNICATIONS: A DISCREDITED TOOL OR

USER FAILURE? IMPLICATIONS FOR FUTURE CONFLICT", Strategic Studies Institute and U.S. Army War College Press, December, 2013.

- The White House, National Framework for Strategic Communication, Washington, D.C., March 2010.

- Taylor Philip, "Public Diplomacy and Strategic Communications," in "Introduction," Routledge Handbook of Public Diplomacy, Nancy Snow and Philip M. Taylor eds., New York: Routledge, 2009.

- Taylor Philip, ''Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day''. (Manchester University Press, 2003)

- Thomas Timothy, "Dragon Bytes," Ft. Leavenworth, KS: Foreign Military Studies Office, 2004.

- Thomas Timothy, "Comparing US, Russian and Chinese IO Concepts," Ft. Leavenworth, KS: Foreign Military Studies Office, 2004.

- Thomas Timothy, "Human Network Attacks," Military Review (September-October 1999): <http://fmso.leavenworth.army.mil/fmsopubs/issues/humannet/humannet.htm > (August 30, 2002).

- Thomas Timothy, "Russia's Reflexive Control Theory & The Military," The Journal of Slavic & Military Studies, Vol. 17, London, UK: Frank Cass, 2004.

- Toshi Yoshihara, Chinese Information Warfare: A Phantom Menace Or Emerging Threat? Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA: November 2006.

- U.S. Army Combined Arms Center, Information & Cyberspace Symposium, Fort Leavenworth, April 15-18.

- U.S. Information Agency (USIA), "Overview: 1998".

- U.S. Government Accountability Office, U.S. Public Diplomacy Key Issues for Congressional Oversight, footnote 1.

- US Cyber Consequences Unit, "The US-CCU Report on the Georgian Cyber Campaign," (August 2008) found at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf A.

- United States Joint Forces Command, Commander's Handbook for Strategic Communication and Communication Strategy, Suffolk Va.: United States Joint Forces Command Warfighting Center, Version 3.0, June 24, 2010.

- United States Air Force, Electronic Warfare, Air Force Doctrine Document, 2-5.1 (November 5, 2002).

- Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare." Strategic Analysis, Indian Institute for Defence Studies and Analyses, Vol: 30, Issue:4, October 2006.

- Walton Timothy, “China’s Three Warfares,” Herndon, VA: Delex Consulting, January 18, 2012.

- Waltz Edward, Information Warfare: Principles and Operation. (Boston: Artech House, 1998)

- Wang Pufeng, "Xinxi zhanzheng yu junshi geming" (Information Warfare and the Revolution in Military Affairs), Beijing: Junshi kexueyuan, 1995. Quoted in Mulveron, 1999, "The PLA and Information Warfare.


## Πηγές Ίντερνετ.


www.rand.org/pubs/monographs/MG607.html.

www.nytimes.com/2008/08/13/technology/13iht-13cyber.15227999.html

http://www.au.af.mil/info-ops/perception.htm#reflexive

http://www.independent.co.uk/news/world/middle-east/black-watch-ordered-to-join-us-cordon-for-assault-on-fallujah-6159503.html

www.networkworld.com/community/node/44448