ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ
Τμήμα Στρατιωτικών Επιστημών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2017-18
ΣΧΕΔΙΑΣΗ ΚΑΙ ΕΠΕΞΕΡΓΑΣΙΑ
ΣΥΣΤΗΜΑΤΩΝ (SYSTEMS ENGINEERING)
(ΠΔ 96 /2015/ΦΕΚ 163Α'/20.08.2014)

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
Σχολή Μηχανικών Παραγωγής & Διοίκησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΠΛΗΡΟΦΟΡΙΑΚΟΣ ΠΟΛΕΜΟΣ ΚΑΙ ΔΙΚΤΥΟΚΕΝΤΡΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Διατριβή που υπεβλήθη για την μερική ικανοποίηση των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης

Υπό:

ΧΑΣΑΠΗ ΒΑΣΙΛΕΙΟΥ- ΡΑΦΑΗΛ

Α.Μ.: 2017018049

2021

Η Μεταπτυχιακή Διατριβή του Χασάπη Βασίλειου- Ραφαήλ εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Καθηγητής Δάρας Νικόλαος (Επιβλέπων),…

Καθηγητής Ματσατσίνης Νικόλαος,……

Nikolaos Matsatsinis
Digitally signed by Nikolaos Matsatsinis
Date: 2021.04.27 08:07:59 +03'00'

Καθηγητής Μπάρδης Νικόλαος,……..

Nikos Bardis
Digitally signed by Nikos Bardis
DN: cn=Nikos Bardis, o=Hellenic Army Academy, ou=Hellenic Army Academy, email=nbardis@sse.gr, c=GR
Date: 2021.04.29 15:00:42 +03'00'

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Έτος 2021

''Οι πληροφορίες είναι η βάση κάθε σχεδίου δράσης''

Carl von Clausewitz

(1780-1831)

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

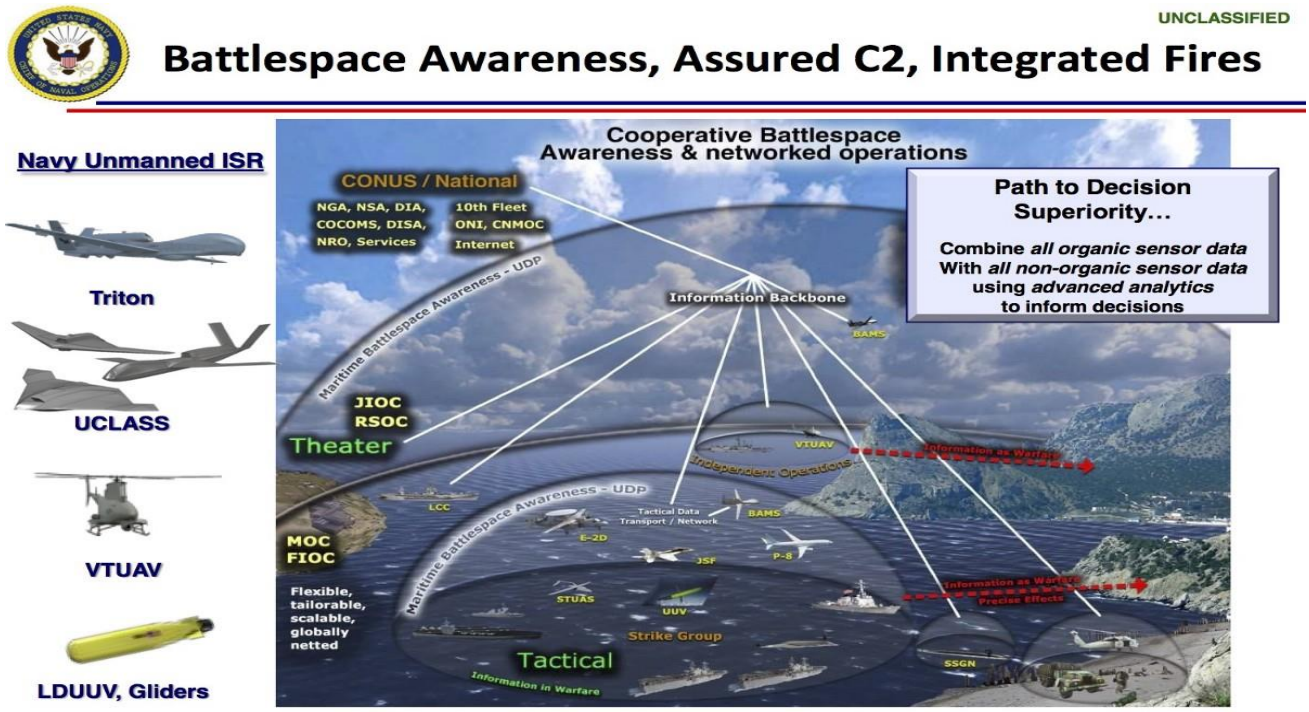
ΠΕΡΙΛΗΨΗ

Στο σημερινό ταχέως εξελισσόμενο θέατρο επιχειρήσεων τα οπλικά συστήματα είναι ικανά να πλήξουν στόχους με εξαιρετική ακρίβεια και διάφορα συστήματα επιτήρησης/αναγνώρισης παρέχουν εξαιρετικά λεπτομερείς πληροφορίες σχετικά με τις εχθρικές δυνάμεις. Πρόκειται σύμφωνα με πολλούς στρατηγικούς αναλυτές για μια επανάσταση στις στρατιωτικές υποθέσεις, η οποία αναδύθηκε στα τέλη του προηγούμενου αιώνα και αφορά στην εναρμόνιση των όπλων με την τεχνολογία, από τον μεγαλύτερο σχηματισμό μέχρι τον τελευταίο στρατιώτη, καθ' όλο το χάος και την αταξία που επικρατούν στην μάχη. Στη συγκεκριμένη εργασία, αρχικά γίνεται ανάπτυξη του δόγματος του πληροφοριακού πολέμου. Αναφέρονται τα χαρακτηριστικά, οι στόχοι, τα είδη, τα στάδια διεξαγωγής καθώς και τα πλεονεκτήματά του έναντι του «μαζικοκεντρικού» πολέμου. Στη συνέχεια αναλύονται οι λόγοι που οδήγησαν λεγόμενη επανάσταση στις στρατιωτικές υποθέσεις (Revolution in Military Affairs) και στον Δικτυοκεντρικό Πόλεμο (Network Centric Warfare). Προσεγγίζεται θεωρητικά το δόγμα του δικτυοκεντρικού πολέμου , παρουσιάζεται η διεξαγωγή διαφόρων επιχειρήσεων όπου είναι εμφανής, τουλάχιστον μέχρι σήμερα, η εφαρμογή του δικτυοκεντρικού και πληροφοριακού δόγματος και παρατίθενται τα πλεονεκτήματα της δικτύωσης (Networking) στο σύγχρονο θέατρο επιχειρήσεων. Επιπλέον, γίνεται εισαγωγή στη θεωρία Διοίκησης και Ελέγχου (Command & Control). Παράλληλα γίνεται αναφορά στον σκοπό, τις βασικές αρχές, τα πλεονεκτήματα χρήσης των τακτικών δικτύων (Tactical Data Links) καθώς επίσης γίνεται εκτενής αναφορά στις κατηγορίες και τα είδη των τακτικών δικτύων. Τέλος γίνεται προσπάθεια να αποσαφηνιστεί ο ρόλος και η χρησιμότητα των παραπάνω στις Ελληνικές Ένοπλες Δυνάμεις, υπό το πρίσμα της οικονομικής κρίσης και των διάφορων απειλών που αντιμετωπίζει η Ελληνική Εθνική Ασφάλεια.

Εισαγωγή

§1. Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA-Revolution In Military Affairs)

Τα τελευταία χρόνια ότι έχουν γίνει τεράστια άλματα στην οπλική τεχνολογία. Τα οπλικά συστήματα είναι πλέον ικανά να πλήξουν στόχους με εξαιρετική ακρίβεια, συστήματα επιτήρησης/αναγνώρισης έχουν την ικανότητα παροχής εξαιρετικά λεπτομερών πληροφοριών σχετικά με τις εχθρικές δυνάμεις. Επιπρόσθετα, η ανάλυση των δεδομένων που τα παραπάνω συστήματα παρέχουν σε συνδυασμό με τη χρήση των κατάλληλων συστημάτων συλλογής και διανομής πληροφοριών μπορεί να οδηγήσει στην ταχεία αξιοποίηση των πληροφοριών. Πολλοί στρατιωτικοί αναλυτές υποστηρίζουν ότι αυτή η τεράστια πρόοδος στη στρατιωτική τεχνολογία οφείλεται στην αναθεώρηση των επιχειρησιακών αντιλήψεων. Έτσι οδηγηθήκαμε σε ένα είδος επανάστασης στις στρατιωτικές υποθέσεις.



Εικόνα 1: «Το μονοπάτι για την κυριαρχία και πρωτοβουλία στο πεδίο μάχης», Γραφική αναπαράσταση του τρόπου με τον οποίο συνδυάζονται τα οργανικά

Ο Andrew Marshall, διευθυντής του Γραφείου Διαδικτυακών υποθέσεων (Office of Net Assessments) στο αμερικανικό Υπουργείο Άμυνας υποστηρίζει: "Μια επανάσταση στις στρατιωτικές υποθέσεις (RMA-Revolution in Military Affairs) είναι μια σημαντική αλλαγή στη φύση του πολέμου που επέφερε την καινοτόμο εφαρμογή των νέων τεχνολογιών, οι οποίες, σε συνδυασμό με τις δραματικές αλλαγές στο στρατιωτικό δόγμα και την επιχειρησιακή και οργανωτική δομή, μεταβάλλει ριζικά το χαρακτήρα και τη συμπεριφορά των στρατιωτικών επιχειρήσεων.[1]

Αλλαγές τέτοιας κλίμακας στην στρατιωτική τεχνολογία έχουν παρατηρηθεί πολλές φορές στο πέρασμα των αιώνων. Το πιο προφανές αίτιο είναι η τεχνολογική «ώθηση». Η εφεύρεση της πυρίτιδας, το υποβρύχιο, η ατμομηχανή, ο κινητήρας εσωτερικής καύσης, το αεροπλανοφόρο και εν τέλει η πυρηνική βόμβα είναι κάποιες από τις καινοτομίες που οδήγησαν σε αλλαγές. Ορισμένοι αναλυτές υποστηρίζουν ότι υπήρξαν μόνο τρεις «επαναστάσεις στις στρατιωτικές υποθέσεις» και ότι αυτές έχουν συνδεθεί με τη φύση των κοινωνιών: **αγροτική**, **βιομηχανική** και **κοινωνία των πληροφοριών**. Αυτό όμως που είναι κοινώς αποδεκτό είναι ότι η τεχνολογία από μόνη της δεν επαρκεί για να επιφέρει μια πραγματική επανάσταση στις στρατιωτικές υποθέσεις και εξαρτάται από τον ανθρώπινο παράγοντα. Για παράδειγμα, σχεδόν πέντε αιώνες μεσολάβησαν από την εφεύρεση της πυρίτιδας και την χρήση της σε μεγάλη κλίμακα για στρατιωτικούς σκοπούς. Στην αρχή του Δευτέρου παγκοσμίου πολέμου, η γερμανική διοίκηση εφήρμοσε καινοτόμες τακτικές που βασίστηκαν στο συνδυασμό αεροπορικών και επίγειων δυνάμεων και είχαν ως αποτέλεσμα να συντρίψουν τις γαλλικές και βρετανικές δυνάμεις που ήταν παρόμοια εξοπλισμένες.

Η κύρια αφορμή που οδήγησε στην λεγόμενη «επανάσταση στις στρατιωτικές υποθέσεις» ήταν ότι παρά την ποιοτική ανωτερότητα των αμερικανικών οπλικών συστημάτων ήταν αδύνατο να εξισωθούν οι πολυπληθέστερες σοβιετικές δυνάμεις οι οποίες βέβαια υστερούσαν τεχνολογικά. Αυτό είχε ως αποτέλεσμα την ανάπτυξη μιας θεωρίας που δίνει έμφαση στην υψηλή κινητικότητα, κυρίως μέσω της αερομεταφοράς, της υπερκέρασης, της πρώτης γραμμής του πεδίου της μάχης και την προσβολή σε βάθος, με τη χρήση πυρομαχικών ακριβείας μεγάλου βεληνεκούς. Επειδή οι Αμερικάνοι δεν μπορούσαν να αυξήσουν ποσοτικά το σύνολο των στρατιωτικών συμβατικών

1 "The Battlefield of the Future" - 21st Century Warfare Issues", Air University, Chapter 3, p. 1, Jeffrey McKitrick, James Blackwell, Fred Littlepage, Georges Kraus, Richard Blanchfield and Dale Hill

δυνάμεων προσπάθησαν να αυξήσουν τη κινητικότητά τους και την ικανότητα να προσβάλλουν με ακρίβεια στόχους σεμεγάλες αποστάσεις.[2] Η αντίληψη αυτή εκφραζόταν κυρίως από την Συνδυασμένη Μάχη Αεροπορικών και Χερσαίων Δυνάμεων (Airland Battle). Έτσι υιοθετήθηκε το «μη γραμμικό πεδίο μάχης», όπου η προσβολή του εχθρού δεν γινόταν σε μια γραμμή επαφής, αλλά σε μεγάλου βάθος και σε όλες τις διαστάσεις, αξιοποιώντας ταχεία μετακινούμενες δυνάμεις και όπλα προσβολής ακριβείας από μεγάλες αποστάσεις. Οι Σοβιετικοί στρατιωτικοί ηγέτες αντελήφθησαν τα νέα αυτά δεδομένα και πρώτοι έκαναν λόγο για μια επανάσταση στις Στρατιωτικές Υποθέσεις, η οποία μπορεί, χοντρικώς, να χωριστεί εννοιολογικά στην «επανάσταση της ακρίβειας», στους προηγμένους αισθητήρες και στις πληροφορικές/επικοινωνιακές τεχνολογίες δικτύου.

Η απαρχή των συζητήσεων όμως σχετικά με την Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA) στις ΗΠΑ ξεκίνησε κατά τον Ψυχρό Πόλεμο, επανήλθε στο προσκήνιο μετά τη λήξη του πολέμου στο Βιετνάμ στον πόλεμο της Νικαράγουα το 1980, μελετήθηκε εκτενώς μετά το τέλος του Ψυχρού Πολέμου. Μέλημα της RMA σε όλες τις φάσεις της είναι η βέλτιστη χρήση των τεχνολογιών πολέμου με σκοπό τα πλήγματα ακριβείας και την ελαχιστοποίηση των θυμάτων του επιτιθέμενου στρατού. Συνδυάζει, παράλληλα, ένα ευρύ σύνολο τεχνικών, αντιλήψεων και στρατηγικών σχετικά με τον εκσυγχρονισμό του στρατού, την επαγγελματοποίηση και την προσαρμογή του μέσα από τη χρήση υψηλών τεχνολογιών σε νέες μορφές πολεμικών «ευέλικτων», στοχευμένων και δικτυακών επιχειρήσεων, στον «ασύμμετρο» και τον «προληπτικό πόλεμο», αλλά κατ' επέκταση και στο αντάρτικο πόλεων και ευρύτερα στην επιτήρηση του αστικού χώρου.[3]

Κατά την διάρκεια του Ψυχρού Πόλεμο, η γεωπολιτική θέση των ΗΠΑ και η ιδέα ότι δεν θα μπορούσαν να αντιτάξουν ικανές χερσαίες και αεροπορικές δυνάμεις στην Ευρώπη, συνέβαλε στην ανάπτυξη μιας στρατηγικής βασισμένης λιγότερο στο έμψυχο χερσαίο στράτευμα και περισσότερο στις δυνάμεις αέρος και τη γνώση μέσω της πληροφορίας[4]. Μετά τη λήξη του πολέμου στο Βιετνάμ, οι προσπάθειες των αμερικανικών επιτελείων επικεντρώθηκαν στην εύρεση τρόπων που θα μείωναν τις απώλειες σε ανθρώπινο δυναμικό, όπως διαφαίνεται και από το

[2] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ.34
[3] Μαρία Μαρκαντωνάτου, «Επανάσταση στις στρατιωτικές υποθέσεις: Από τον πόλεμο χωρίς απώλειες στο πόλεμο κατά της τρομοκρατίας » ,Απρίλιος – Ιούνιος 2010, Τεύχος 111
[4] Γρίβας, Κωνσταντίνος, Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής, Λιβάνης, Αθήνα, 2008,σελ.158

δόγμα Πάουελ περί «πολέμου χωρίς απώλειες». Αυτό πρέσβευε ότι, βάση της εμπειρίας του Βιετνάμ, οι ΗΠΑ δεν θα προχωρούσαν σε πόλεμο στο εξωτερικό αν δεν διατηρούσαν ορθολογικές προσδοκίες νίκης και ότι επίσης και δεν θα διακινδύνευαν τις ανθρώπινες ζωές αν δεν υπήρχε κρίσιμος στρατηγικός λόγος.[5]

Όπως αναφέραμε η πρώτη φορά που αναφέρθηκε ο όρος είναι κατά τη δεκαετία του 1980, από τους Αμερικανούς, στον πόλεμο ενάντια στη Νικαράγουα[6]. Σύμφωνα με τον Chomsky, η περίπτωση της Νικαράγουα είναι από τις πρώτες που εφαρμόστηκε το RMA, καθώς εκεί εισάγεται για πρώτη φορά η έννοια του «πολέμου χαμηλής έντασης». Οι Αμερικανικές στρατιωτικές δυνάμεις εκτέλεσαν «πόλεμο χαμηλής έντασης», δηλαδή ο μισθοφορικός στρατός των ΗΠΑ έλαβε την εντολή να επιτεθεί σε μη-στρατιωτικούς, «μαλακούς στόχους (Soft Targets)».[7]

Στον Πόλεμο του Κόλπου το 1991 η στρατιωτική χρήση της τεχνολογίας των πληροφοριών έφτασε στο ζενίθ της. Μέσω των νέων τεχνολογιών ενισχύθηκε η ικανότητα των συμμαχικών δυνάμεων να ανταλλάσσουν και να χρησιμοποιούν πληροφορίες. Οι νέες τεχνολογίες καθοδήγησης των οπλικών συστημάτων οδήγησαν στην ανάπτυξη των πυρομαχικών που μπορούσαν να πλήξουν στόχους με εκπληκτική ακρίβεια, όπως πυρομαχικά που εκτοξεύονται από αεροσκάφη, τους πυραύλους Cruise, ακόμη και μέσα του πυροβολικού. Η ικανότητα καταστροφής στόχων χρησιμοποιώντας ένα ή δύο κατευθυνόμενα πυρομαχικά ακριβείας και όχι με τη χρήση βομβαρδιστικών για βομβαρδισμούς μεγάλης κλίμακας συνέβαλαν καθοριστικά στην οικονομία υλικών και μέσων. Για παράδειγμα, κατά τη διάρκεια του Πολέμου του Κόλπου, 6.250 τόνους κατευθυνόμενων πυρομαχικών ακριβείας χρησιμοποιήθηκαν σε σύγκριση με 81.980 τόνους συμβατικών βομβών. Το ποσοστό επιτυχίας ήταν μεταξύ του 80 και 90 τοις εκατό για τα κατευθυνόμενα πυρομαχικά ακριβείας (PGMs) σε σύγκριση με περίπου 25 τοις εκατό των συμβατικών βομβών. Η χρήση των κατευθυνόμενων πυρομαχικών ακριβείας επέτρεψε στις συμμαχικές δυνάμεις να ελαχιστοποιήσουν τις παράπλευρες απώλειες.

Εξίσου σημαντικός, αλλά λιγότερο προφανής ήταν ο ρόλος που διαδραμάτισαν τα εξελιγμένα συστήματα επιτήρησης, αναγνώρισης και συλλογής

[5] Sennett, Richard «Αυτή τη φορά μια χώρα αδιαίρετη», στο Σαϊντ, Έντουαρντ (κ.ά.): Η Τρομοκρατία και η Κοινωνία των Πολιτών, Μεταίχμιο, Αθήνα, 2002, σελ.154
[6] Chomsky, Noam, «Ο νέος πόλεμος ενάντια στην Τρομοκρατία», Μεταίχμιο, Αθήνα, 2002, σελ 96
[7] Chomsky, Noam, «Ο νέος πόλεμος ενάντια στην Τρομοκρατία», Μεταίχμιο, Αθήνα, 2002, σελ 105

πληροφοριών. Αυτά περιλαμβάνουν συστήματα επίγεια, εναέρια ή ακόμη και μέσα που αναπτύσσονται στο διάστημα. Τέτοια συστήματα είναι το E-3 Sentry που είναι ένα αεροπλάνο προειδοποίησης και ελέγχου (AWACS) που παρέχει επιτήρηση, διευκρίνιση, διοίκηση και έλεγχο αεροσκαφών. Το RC-135 Rivet σύστημα συλλογής πληροφοριών (JSTARS), καθώς και μια μεγάλη ποικιλία αεροσκαφών φωτο-αναγνώρισης. Ένα άλλο χαρακτηριστικό του πολέμου του Κόλπου ήταν, φυσικά, η χρήση των πυραύλων Patriot με σκοπό την αναχαίτιση των ιρακινών πυραύλων Scud,δηλαδή την αντιμετώπιση βαλλιστικών απειλών.

Ομοίως, κατά την επέμβαση του ΝΑΤΟ στη Γιουγκοσλαβία το 1999 έγινε ευρεία χρήση των λεγόμενων «έξυπνων όπλων», όπως πύραυλοι τύπου Κρουζ που μπορούν να εκτελούν πτήση σε χαμηλό ύψος παραπλανώντας το ραντάρ του αντιπάλου, αλλά και οι βόμβες γραφίτη που έχουν την ικανότητα να βραχυκυκλώνουν τα συστήματα ηλεκτροδότησης.[8]

Περαιτέρω, παρότι στο Αφγανιστάν μετά την πρώτη επίθεση το 2001 οι προσπάθειες «διατήρησης της ειρήνης» (Peace Keeping), «δημιουργίας κράτους» (state-building) και «ανασυγκρότησης» δεν ευδοκίμησαν, οι RMA-τακτικές παραμένουν το βασικό μοτίβο δράσης:

«Η πραγματοποιούμενη μέσα σε μια δεκαετία πρόοδος των ΗΠΑ – 1991 Κόλπος, 2001 Αφγανιστάν – χρήζει προσοχής. (…) Η ικανότητα πρόσβασης στην πληροφορία, η ποιότητα των αποστολών (από την Τάμπα της Φλόριντα μέχρι τις χερσαίες μονάδες στην καρδιά του Αφγανιστάν και τα ιπτάμενα βομβαρδιστικά πάνω από τον Ινδικό ωκεανό), η ακρίβεια των βομβαρδισμών, συνιστούν κατορθώματα τεχνικής, αδιανόητα ακόμη στη δεκαετία του 1970, όταν άρχιζε να διαγράφεται η RMA»[9]

Μετά την 11η Σεπτέμβρη του 2001 ορίστηκε μια νέα μορφή απειλής που ονομάστηκε «νέα τρομοκρατία», η οποία βασιζόταν στον αιφνιδιασμό. Πλέον δεν υπήρχε επαρκής επίγνωση της χρονικής και γεωγραφικής κατάστασης, δυνατότητα υπολογισμού των επιχειρήσεων με βάση τη σχέση κόστους-ωφέλειας. Βασισμένη στον αιφνιδιασμό και τη διαρκή μετατόπιση των χώρων δράσης και των καίριων στόχων, αποστέρησε τη δυνατότητα προετοιμασίας των ΗΠΑ για πόλεμο. Οι ΗΠΑ πλέον, επιδιώκουν την ανάπτυξη νέων στρατηγικών που συμβάλουν στην ανάπτυξη ενός ξέφρενου ρυθμού μάχης (Ferocious combat pace). Δηλαδή αποσκοπούσε στην διάσπαση των στρατιωτικών δυνάμεων σε «ψηφίδες ισχύος», οι

[8] Θεοφίλου, Ανδρέας, «Τα Έξυπνα Όπλα του ΝΑΤΟ και η ανθρωπιστική τους δράση στη Γιουγκοσλαβία», στο: Ουτοπία, τεύχ. 34, 1999,σελ 45
[9] Géré, Francois, «Γιατί οι Πόλεμοι; Ένας αιώνας Γεωπολιτικής», Παπαζήσης, Αθήνα, 2005, σελ. 40

οποίες θα βρίσκονταν διασπαρμένες μέσα στο χώρο. Αυτές οι «ψηφίδες» αναμειγνύονται στο φυσικό χώρο των αντιπάλων σαν «κηλίδες» με φαινομενικά χαοτικό τρόπο, οι οποίες όμως βρίσκονται σε επικοινωνία μεταξύ τους και συντονίζονται μέσω ενός δικτύου συλλογής ανάλυσης και μετάδοσης πληροφοριών.[10]

Όπως αναφέρει η κ. Μαρκαντωνάτου: «Η ανάγκη των Αμερικανών να ανταποκριθούν στον αιφνιδιαστικό χαρακτήρα των πλέον χαρακτηριζόμενων ως «ασύμμετρων απειλών» (π.χ. στο Αφγανιστάν οι Αμερικανοί κλήθηκαν να βρουν στρατηγικές ενάντια σε επιθέσεις αυτοκτονίας, επιθέσεις σε φάλαγγες οχημάτων με εκρηκτικά, κατάληψη δημόσιων κτιρίων όπου μέσα βρίσκονται άμαχοι Αφγανοί αλλά και Ταλιμπάν), υιοθετούν τη μορφή του πληροφοριοκεντρικού και δικτυοκεντρικού πολέμου του RMA, με βασικές προϋποθέσεις «την εντολή, τον έλεγχο, τις επικοινωνίες και την πληροφορία», το επονομαζόμενο «C3I» (Command, Control, Communications, Intelligence) και με τον στρατό να οργανώνεται σε μικρές-ευέλικτες μονάδες όσο το δυνατόν.

Μπορούμε να υποστηρίξουμε ότι τα μέσα και οι δυνατότητες που παρέχει το RMA είναι τα εξής:[11]

- Εναέριες δυνάμεις (π.χ. «ευέλικτα» ελικόπτερα ή ρομποτικά αεροπλάνα) επιδιώκουν να καταλάβουν ένα στρατηγικό για τον εχθρό χώρο, σταθμίζοντας παράλληλα τις δυνατότητές του, με τη δυνατότητα χρήσης «πυρομαχικών ακριβείας», με «έξυπνες βόμβες» και βομβαρδιστικά με λέιζερ μεγάλης ακτίνας, ενώ οι στρατιωτικές υποδομές, τα τεθωρακισμένα, τα φορτηγά του πεζικού, οι κονσόλες των πλοίων, τα πυροβολικά συστήματα, οι εκτοξευτήρες πυραύλων κ.ά. μετατρέπονται, με τη βοήθεια υψηλών ψηφιακών τεχνολογιών και ενσωματωμένων υπολογιστών, σε «ευέλικτα μέσα» του «εκσυγχρονισμένου» στρατού του RMA.

- Δορυφόροι με πολύ μεγάλη ακτίνα ανίχνευσης, σύνθετες τεχνολογίες τηλεκατεύθυνσης, αεροσκάφη με ενσωματωμένους πυραύλους και μη επανδρωμένα αεροσκάφη (drones) των οποίων το στίγμα δεν ανιχνεύεται από εχθρικά ραντάρ, λειτουργούν για την αεροφωτογράφηση, τη χαρτογράφηση, την περιφρούρηση, την κατασκοπεία και τη συλλογή δεδομένων.

[10] Γρίβας, Κωνσταντίνος, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, 2008,σελ.100
[11] Μαρία Μαρκαντωνάτου, «Επανάσταση στις στρατιωτικές υποθέσεις: Από τον πόλεμο χωρίς απώλειες στο πόλεμο κατά της τρομοκρατίας» ,Απρίλιος – Ιούνιος 2010, Τεύχος 111

- Σε συνεργασία με το σύστημα συλλογής πληροφοριών και μέσα από την εγκατάσταση ειδικών διαδικτύων καθίσταται δυνατό να εποπτευθούν όλες οι στρατηγικές θέσεις του εχθρού για τις διαφορετικές επιτιθέμενες δυνάμεις (χερσαίες, θαλάσσιες και εναέριες). Έτσι, μπορούν να συντονίζονται χωρίς να έχουν κοινό οπτικό πεδίο ή να παρατάσσονται ομαδικά.

- Στο «ψηφιακό πεδίο μάχης» παρέχεται η δυνατότητα της εικονικής διάτρησης όλου του πεδίου κρούσης και οι «ψηφιακοί στρατιώτες» μπορούν να χρησιμοποιούν όπλα και τεχνικές ακριβείας με τις θέσεις τους να παραμένουν κρυφές και με τη δυνατότητα να αλλάζουν το σχεδιασμό τους ανά πάσα στιγμή. Με τον ίδιο τρόπο αποκτούν πλεονεκτήματα τόσο στην επισκόπηση του στρατηγικού χώρου, στις μετακινήσεις και την ευέλικτη αναδιάρθρωση των σχεδιασμών, όσο και στην ταχύτητα των επιχειρήσεων.

§1. Πληροφοριακός Πόλεμος

§1.1 Η φύση του Πληροφοριακού Πολέμου

Είναι ο Πληροφοριοκεντρικός Πόλεμος μια νέα εκκολαπτόμενη μορφή τέχνης, ή μια νέα έκδοση του ήδη καθιερωμένου πολέμου; Είναι μια νέα μορφή της σύγκρουσης που οφείλει την ύπαρξή της στην έκρηξη της παγκόσμιας πληροφόρησης ή είναι κάτι παλιό του οποίου η προέλευση υφίσταται από τις απαρχές του ανθρώπου αλλά έχει επαναπροσδιορισθεί από την εποχή της πληροφορίας; Αποτελεί ενοποιημένο πεδίο ή ευκαιριακή συνάθροιση;

Η πληροφορία, είναι η πρωτεύουσα της ψυχικής και πνευματικής σφαίρας. Οι μηχανές μπορούν να χρησιμοποιούν πληροφορίες εντατικά, αλλά μόνο επειδή έχουν σχεδιαστεί για την προσομοίωση μιας διευρυμένης, επιταχυνόμενης – αυξημένης μα ουσιαστικά παρόμοιας ανθρώπινης λειτουργίας. Η ανθρώπινη διανοητική λειτουργία προσπαθεί να μετατρέψει τις ακατέργαστες πληροφορίες σε γνώση και στη συνέχεια, σε

ένα «συνεχή πομπό πληροφοριών». Μηχανικά συστήματα που βασίζονται στην πληροφορία, είναι απλώς επεκτάσεις και τις βοηθούν στις λειτουργίες τους.

Όλοι οι άνθρωποι που ασχολούνται με τον πόλεμο ατομικά ή συλλογικά σε οργανισμούς, χωρίς βοήθεια ή που ενισχύονται από μηχανές αποτελούν αυτό που μπορεί να ονομαστεί και να μοντελοποιηθεί ως "οργανισμός πολέμου". Οι πληροφορίες ρέουν, και υποβάλλονται σε επεξεργασία από το πνευματικό υποσύστημα, αλλά ο «οργανισμός πολέμου» είναι ένα ολιστικό, διαδραστικό, συνυφασμένο σύστημα των υποσυστημάτων. Υπάρχει σε όλα τα επίπεδα, από τα μικρά στα πιο μεγάλα, η οποία πολλαπλασιάζει τις δυνατότητες διαδραστικής πολυπλοκότητας σε μεγαλύτερους και συλλογικότερους οργανισμούς.

§1.2 Η έννοια Πληροφοριακού Πολέμου

Όσον αφορά την προσέγγιση της έννοιας του πληροφοριακού πολέμου, υπάρχουν πολλές δυσκολίες. Πολλοί θεωρητικοί του πολέμου λογίζουν ως σταθμό στην ιστορία του πολέμου, τον Πόλεμο του Περσικού Κόλπου, ο οποίος έφερε επανάσταση στις στρατιωτικές υποθέσεις, συνιστά μια νέα στρατηγική αντίληψη στην οποία δόθηκαν διάφορες ονομασίες όπως π.χ Πόλεμος των υπολογιστών, τεχνολογικός ή πληροφοριοκεντρικός.

Με το πέρασμα των χρόνων, επικράτησε ο όρος «πληροφοριοκεντρικός ή πληροφοριακός πόλεμος» και μπήκε σε διαδικασία η συστηματική μελέτη του. Με αυτή την ονομασία δίνεται ιδιαίτερη έμφαση στην έννοια πληροφορία κάτι το οποίο ίσχυε από παλιά, καθώς η διεξαγωγή του πολέμου ήταν ανέκαθεν συνδεδεμένη με τη διαχείριση της πληροφορίας. Φυσικά, η στρατηγική προσέγγιση του Πληροφοριακού πολέμου, διαφέρει από εκείνη του παρελθόντος κυρίως λόγω ενός καινοφανούς χαρακτηριστικού που δεν είναι άλλο από το είδος της αντιπαράθεσης που προωθείται μέσω αυτής της στρατηγικής. Βασικοί πυλώνες της, θεωρούνται οι ταχείες, ακριβείς, φθηνές μα πολύ αποτελεσματικές

επιχειρήσεις, που βασίζονται στη γνώση. Για την επιτυχή διεξαγωγή πληροφοριοκεντρικών επιχειρήσεων όμως, καθίσταται υψίστης σημασίας ο έλεγχος και η αξιοποίηση της κάθε κρίσιμης πληροφορίας. Συμπεραίνοντας λοιπόν, η λογική του πληροφοριοκεντρικού πολέμου θέτει σαν κυρίαρχο στοιχείο για την επιτυχή έκβαση των αντιπαραθέσεων την ορθή χρήση της πληροφορίας αντί άλλων παραγόντων που ανέκαθεν καθόριζαν την πολεμική ισχύ.

Όσες προσπάθειες και αν έχουν γίνει ως τώρα ώστε να γίνει κατανοητή πλήρως η έννοια του πληροφοριακού πολέμου δεν έχουν καρποφορήσει καθώς δεν έχει αποκρυσταλλωθεί η πλήρης προοπτική και δυναμική του. Το μόνο σίγουρο, είναι το ότι στο παρασκήνιο μιας τέτοιας στρατηγικής φαίνεται μια συγκεκριμένη **επιδίωξη για πληροφοριακή κυριαρχία των φίλιων δυνάμεων επί των δυνάμεων του αντιπάλου**.

§1.3 Τα χαρακτηριστικά, οι στόχοι και τα είδη του Πληροφοριακού Πολέμου

Βασικό χαρακτηριστικό αυτής της νέας στρατηγικής του πληροφοριακού πολέμου, αποτελεί η ενίσχυση και επικράτηση της αντίληψης ότι η έκβαση μιας αντιπαράθεσης εξαρτάται σε πολύ μεγάλο βαθμό απ τον έλεγχο και ορθή εκμετάλλευση των πληροφοριών που διαθέτουν οι κάθε πλευρές.

Για να πετύχουμε το απόλυτο πλεονέκτημα επί του αντιπάλου στον πληροφοριοκεντρικό πόλεμο, πρέπει να υλοποιηθούν κάποιοι αν όχι όλοι από τους παρακάτω στόχους, όπως η απόκτηση και εκμετάλλευση κρίσιμων πληροφοριών έναντι του εχθρού και ταυτόχρονη προστασία των πληροφοριών που μας αφορούν από εχθρικές επιθέσεις, ή τον επηρεασμό των πληροφοριών που κατέχει ο εχθρός και την προσβολή των συστημάτων του.

Η νέα αυτή στρατηγική αντίληψη, διακρίνεται σε δυο επιμέρους φάσεις αναλόγως με τους επιδιωκόμενους σκοπούς. Η πρώτη φάση είναι ο πόλεμος 1^{ης} γενιάς, όπου

στοχεύεται ο εκσυγχρονισμός των οπλικών συστημάτων για την διεξαγωγή αποτελεσματικών επιχειρήσεων σύντομης διάρκειας, την συλλογή όσο το δυνατόν περισσότερων πληροφοριών για τον εχθρό αλλά και την διασφάλιση της μυστικότητας των δικών μας πληροφοριών. Η δεύτερη φάση, είναι ο πόλεμος 2ης γενιάς όπου κυρίαρχη δύναμη προσδίδει ο έλεγχος των μέσων ενημέρωσης με σκοπό την σε βάθος χρόνου αποτελεσματική επιρροή του κοινού βασιζόμενη στη δημοσιοποίηση των πιο κατάλληλων πληροφοριών.

Η στρατηγική του Πληροφοριακού Πολέμου διαφέρει από τις πραγματικές ένοπλες συγκρούσεις που διαδραματίζονται μέχρι στιγμής στα γνωστά πεδία της μάχης (στεριά, θάλασσα, αέρα). Σε τέτοιου είδους συγκρούσεις οι αντιμαχόμενοι επιδιώκουν την πληροφοριακή υπεροχή έναντι του αντιπάλου όσον αφορά στρατιωτικά ζητήματα (π.χ τα αριθμητικά δεδομένα σχετικά με την μαχητική ισχύ του αντιπάλου ή την τοποθεσία που βρίσκονται οι εχθρικές δυνάμεις). Αυτό στοχεύει σε δυο κατευθύνσεις, πρώτον με την ορθή – έγκαιρη αξιοποίηση των πληροφοριών να εξασφαλίζεται η νίκη και η επιτυχία σε κάθε εμπλοκή και δεύτερον να εξασφαλισθεί υπεροχή στην μετάδοση και αναπαραγωγή από τα μέσα μαζικής επικοινωνίας των πληροφοριών εκείνων, που θα εξασφαλίσουν την απαιτουμένη υποστήριξη εκ μέρους της κοινής γνώμης των επιδιωκόμενων δια της συγκρούσεως στόχων.[12]

Οι παραπάνω στόχοι επιτυγχάνονται με διαφόρου είδους δραστηριότητες, οι οποίες συντελούν στην διαμόρφωση των επιμέρους μορφών μέσω των οποίων εκδηλώνεται ο Πληροφοριοκεντρικός Πόλεμος, ο οποίος εξειδικεύεται σε επτά επιμέρους κατηγορίες. Τον πόλεμο διοίκησης και ελέγχου, τον πόλεμο βασισμένο στην πληροφορία, τον ηλεκτρονικό πόλεμο, τις ψυχολογικές επιχειρήσεις, τον πόλεμο με χάκερς, τον πληροφοριακό – οικονομικό πόλεμο και τον κυβερνοπόλεμο.

[12] Μάρθα Ε. Παπαδούλη, «Οι επιθέσεις στον κυβερνοχώρο: Τι είναι και ποιους προβληματισμούς δημιουργούν», 2011, σελ. 9

§1.4 Τι είναι Πληροφοριακός Πόλεμος

Εικόνα 2 Ο Πρώσσος Υποστράτηγος Καρλ Φον Κλαούζεβιτς θεμελίωσε τις αρχές για την θεωρία και την φύση του πολέμου και οι απόψεις του αποτέλεσαν βάση για τους στρατηγιστές μέχρι και σήμερα.

Πληροφοριοκεντρικός πόλεμος ή Information Warfare (IW) ή ακόμη πιο σύντομα "Infowar" όπως παρουσιάζεται στη διεθνή στρατιωτική κοινότητα, είναι το σύνολο των δραστηριοτήτων στο οποίο χρησιμοποιούνται όλα τα εργαλεία της εθνικής άμυνας μιας χώρας, ώστε να δημιουργηθεί ένα πληροφοριακό κενό στον αντίπαλο, με αποτέλεσμα **την επίτευξη της πληροφοριακής υπεροχής** (Information superiority) και του στρατιωτικού πλεονεκτήματος.[13]

Πληροφοριακή υπεροχή ονομάζεται ο βαθμός κυριαρχίας στο πληροφοριακό πεδίο, στον οποίο είναι δυνατή η διεξαγωγή των επιχειρήσεων από τις φίλιες δυνάμεις χωρίς αποτελεσματική αντίσταση από τον αντίπαλο.

[13] Ανχης (ΠΖ) Κωνσταντίνος Χαμεζόπουλος, «Πληροφοριακός πόλεμος και οι στρατιωτικές του εφαρμογές στην αυγή του 21ου αιώνα» ,2010, σελ 129

Ο πληροφοριοκεντρικός πόλεμος έχει ως αποστολή του να ανιχνεύσει, υποκλέψει τόσο τις πληροφορίες του εχθρού όσο και το σύστημα πληροφοριών του αντίπαλου ενώ ταυτόχρονα επιδιώκει να προστατέψει τα φίλια αντίστοιχα από ανάλογες ενέργειες του εχθρού. Θεωρείται ως ο πυρήνας της RMA (Revolution in Military Affairs). Έχει ως σκοπό την προσβολή του αντιπάλου σε μηδενικό χρόνο, από μεγάλες αποστάσεις χωρίς εκείνος να αποκτά κανένα περιθώριο άμυνας ή αντεπίθεσης.

Η ιστορία μας έχει αποδείξει πως η σχέση μεταξύ των παρακάτω τριών παραγόντων, δηλαδή της πληροφορία,της κινητικότητας και της ποσότητας των οπλικών μέσων είναι αλληλοεξαρτώμενη, η μια συμπληρώνει την άλλη, καθώς μπορούμε να χρησιμοποιήσουμε τον έναν ως υποκατάστατο του άλλου εφόσον ένας από τους παραπάνω παράγοντες λείπει.

Εάν καθίσουμε να αναλύσουμε την ισχύ μιας πολεμικής δύναμης σε μια τυχαία ιστορική περίοδο, θα δούμε ότι βασίζεται σε δυο κύρια συστατικά στοιχεία τα οποία είναι η **πληροφορία** και η **μάζα των καταστροφικών μέσων**. Τα δυο αυτά συστατικά λειτουργούν αντιστρόφως ανάλογα, δηλαδή, όσο πιο πολλές ακριβείς, ευκολονόητες και πρόσφατες πληροφορίες διαθέτουμε και όσο καλύτερες ικανότητες αξιοποίησης αυτών των πληροφοριών μέσω πυρών ακριβείας, τόσο λιγότερη μάζα καταστροφικών μέσων (π.χ πυρών) θα χρειαστούμε. Από την άλλη μεριά, στην περίπτωση που διαθέτουμε λίγες πληροφορίες οι οποίες παραμένουν αναξιοποίητες λόγω έλλειψης ικανότητας προσβολής ακριβείας, τόσο περισσότερη μάζα καταστροφικών μέσων (π.χ ανθρώπινο δυναμικό) θα χρειαστούμε.

Χρησιμοποιώντας τον όρο Πληροφοριοκεντρικός Πόλεμος, αναφερόμαστε πρωτίστως στην διεξαγωγή πολεμικών επιχειρήσεων από ένα στράτευμα, η δομή του οποίου και το είδος της ισχύος που ασκεί στον εχθρό, βασίζονται κυρίως στην άριστη αξιοποίηση και χειρισμό της πληροφορίας και όχι στον μαζικό όγκο πυρός ή την κινητικότητα. Από τις πιο βασικές προϋποθέσεις ώστε να οριστεί ο εννοιολογικός προσδιορισμός του πληροφοριοκεντρικού πολέμου, είναι η κατανόηση της έννοιας «πληροφορία» στην πολεμική ορολογία.

Σαν αρχική μορφή, η έννοια της πολεμικής πληροφορίας περιορίζεται στη γνώση της θέσης του εχθρού και της ακριβής θέσης των φίλιων τμημάτων, από όλα όμως τα επίπεδα του τακτικού και στρατηγικού περιβάλλοντος. Όλη αυτή την έννοια συμπυκνώνεται από αμερικανούς αναλυτές στο εξής σλόγκαν: ***«που είμαι εγώ, που είναι ο εχθρός, που είναι οι φίλοι μου»***[14] (where am I, where is the enemy, where are my buddies). Σε αυτή την φράση, αποτυπώνεται η ουσία αυτού του νέου ψηφιακού πεδίου μάχης. Δεν αρκεί όμως να γνωρίζουμε μόνο το «που», αυτομάτως πρέπει να απαντάμε και στην ερώτηση «πότε» στην οποία όμως δεν είναι καμιά απάντηση αποδεκτή πλην του «τώρα». Μια πληροφορία η οποία φτάνει στα χέρια μας καθυστερημένη δεν έχει καμία ουσιαστική αξία. Φανταστείτε μια πληροφορία που φτάνει σε ένα άρμα, η οποία αφορά την θέση άλλων εχθρικών αρμάτων πριν από κάποια ελάχιστα λεπτά σε μια θέση έστω Α. Μια τέτοιου είδους πληροφορία είναι θεωρητικά άχρηστη διότι τα εχθρικά άρματα πιθανόν να έχουν προχωρήσει σε μια θέση Β η οποία ακόμη δεν έχει αναφερθεί σαν πληροφορία, με αποτέλεσμα, τα πυρά των φίλιων αρμάτων να αποδειχθούν αναποτελεσματικά ή ακόμη σε χειρότερη περίπτωση, να προκληθούν καταστροφές σε φίλια τμήματα. Επίσης, σε αυτό το επίπεδο της πληροφοριοκεντρικής διαδικασίας, οφείλεται να απαντάται και το ερώτημα «τι», δηλαδή το είδος των εχθρικών και των φίλιων δυνάμεων στο πεδίο της μάχης. Σε ένα ψηφιοποιημένο χάρτη, πρέπει να εμφανίζονται όχι σε γενικά πλαίσια μπλε και κόκκινες κουκίδες αλλά πιο συγκεκριμένα συστήματα με περισσότερες πληροφορίες που θα περιγράφουν το τι απεικονίζεται (π.χ άρμα μάχης, σταθμός διοικήσεως, φίλιο αεροσκάφος, εχθρικό αεροσκάφος, φίλιο πολεμικό πλοίο, κ.λπ).

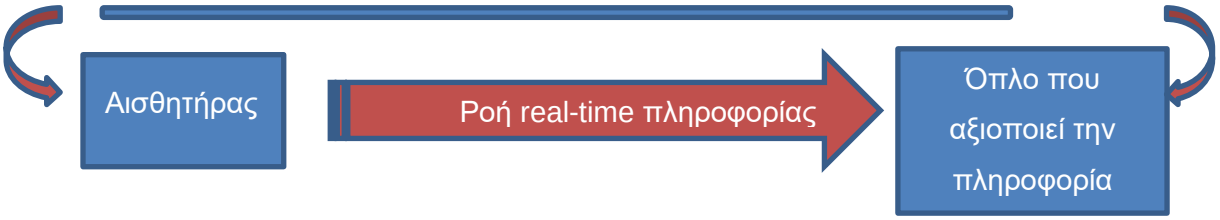
Ένα ακόμη στάδιο μεγάλης σημασίας του πληροφοριοκεντρικού πολέμου, αφορά τις Πληροφορίες Περιβάλλοντος. Αυτό αφορά κυρίως την γνώση του πεδίου της μάχης δηλαδή οτιδήποτε αφορά οπλικά συστήματα, ατμοσφαιρικές συνθήκες και τις επιδράσεις

[14] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής» , Λιβάνης, Αθήνα, σελ 253

τους (π.χ η βατότητα του εδάφους, η ανάλυση της πυκνότητας της βλάστησης, η ικανότητα κίνησης ενός οχήματος πάνω στο έδαφος κλπ). Άλλο εξίσου σημαντικό στάδιο της πληροφοριοκεντρικής διαδικασίας, αποτελεί η «γνώση ισχύος» των ημετέρων δυνάμεων κάτι το οποίο βοηθά σε πολύ μεγάλο βαθμό τον διοικητή να γνωρίζει την κατάσταση που διαχειρίζεται και να διευκολύνεται το έργο του. Παραδείγματα αυτού του σταδίου του πληροφοριοκεντρικού πολέμου είναι, τα αποθέματα πυρομαχικών – καυσίμων, τυχόν βλάβες και η επίδραση τους στην εξέλιξη του αγώνα. Τέλος, θα ήταν σφάλμα να μην αναφέρουμε την προέκταση των επιχειρήσεων στο μέλλον σαν επιπλέον στάδιο του πληροφοριοκεντρικού πολέμου. Όταν γνωρίζουμε απόλυτα την δύναμη και τα μέσα που έχουμε στα χέρια μας, τότε μπορούμε να κάνουμε σχέδια για το μέλλον διαμορφώνοντας αντίστοιχα και την στρατηγική μας. Κοινώς, σκεφτόμαστε πλέον ως εξής, «τί μπορούμε να κάνουμε» και «τί ενδέχεται να κάνει ο εχθρός».

Μια πολύ απλή παρομοίωση που μπορεί να περιγράψει την πληροφοριοκεντρική πολεμική διαδικασία είναι η εξής. Ας υποθέσουμε πως η παραπάνω διαδικασία, είναι ένας σωλήνας στον οποίο πρόκειται να κινηθεί η πληροφορία. Θεωρούμε την είσοδο του σωλήνα ως τον αισθητήρα που εντοπίζει την πληροφορία και την έξοδο του σωλήνα, ως το όπλο που την αξιοποιεί[15]. Αυτός ο υποθετικός σωλήνας θα πρέπει να είναι σχετικά μικρού μήκους ώστε να έχουμε ταχεία μετάδοση πληροφορίας και ταυτόχρονα θα πρέπει να είναι στενός αποσκοπώντας στο να διέρχονται μονάχα οι χρήσιμες και όχι οι ανούσιες πληροφορίες, οι οποίες χρειάζονται επιπρόσθετο χρόνο για ανάλυση-απόρριψη τους. Τέλος, θα πρέπει να διαθέτει παχιά τοιχώματα έτσι ώστε η πληροφορία να μη μπορεί να δεχθεί αλλοίωση αλλά και να μην διακοπεί η ροή της από τον εχθρό. Σχηματικά φαίνεται στο ακόλουθο διάγραμμα.

[15] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ 254



Εικόνα 3: Διαγραμματική ροή της πληροφορίας.

§1.5 Πλεονεκτήματα του Πληροφοριακού Πολέμου έναντι του «Μαζικοκεντρικού» Πολέμου

Στην εποχή που διανύουμε, η νοοτροπία όσον αφορά τον πόλεμο έχει αλλάξει και το σύγχρονο πεδίο μάχης έχει διαμορφωθεί έτσι ώστε να επιζητά την ικανότητα να ασκείται «φτηνός πόλεμος», κάτι το οποίο φιλοδοξεί να καλύψει η RMA. Η έννοια του φτηνού πολέμου αποτελείται από δυο συνιστώσες:

α. Την μείωση της δαπάνης χρημάτων, συναρτήσει του σήμερα, όσον αφορά την απόκτηση και επιχειρησιακή χρησιμοποίηση μιας πολεμικής δύναμης.

β. Την μείωση των ανθρωπίνων απωλειών στο πεδίο της μάχης, όχι απαραίτητα στις φίλιες δυνάμεις, αλλά και στον άμαχο πληθυσμό και τον εχθρό.

Μέσω της πληροφοριοκεντρικής φιλοσοφίας στην πολεμική διαδικασία, επιτυγχάνεται οι δυο παραπάνω στόχοι. Εφόσον ασχοληθούμε με την πληροφοριακή πολεμική διαδικασία και αποκτήσουμε εκτός από αξιόλογες πληροφορίες και μέσα για την αξιοποίηση τους, τότε θα βρισκόμαστε σε θέση να μειώσουμε τον όγκο των οπλικών συστημάτων για την εξόντωση του εχθρού.

Το πιο σημαντικό θετικό και ουσιώδη στοιχείο του Πληροφοριοκεντρικού πολέμου, είναι η μείωση του κινδύνου που εκτίθενται τα φίλια τμήματα. Αυτό συμβαίνει διότι από τη στιγμή που με την ορθή επεξεργασία της πληροφορίας και τον ελάχιστον δυνατό κόπο μπορούμε να έχουμε τα επιθυμητά αποτελέσματα έναντι του εχθρού, το

βάρος πλέον της ενέργειας δε το επωμίζονται σε τόσο μεγάλο βαθμό το ανθρώπινο δυναμικό στην πρώτη γραμμή του πεδίου μάχης. Επίσης, ένα τέτοιο πεδίο μάχης, συνδυασμένο με τα πυρομαχικά προσβολής ακριβείας, μας δίνει την δυνατότητα να πλήττουμε μόνο τα εχθρικά τμήματα και να μην έχουμε παράπλευρες φίλιες απώλειες. Εξίσου θετικό στοιχείο του πληροφοριοκεντρικού πολέμου είναι το γεγονός ότι μπορείς να καταστρέψεις «κεντρικούς» στόχους υψηλής σημασίας για τον εχθρό, αδιαφορώντας έτσι για το σύνολο του προσωπικού, επιζητώντας κυρίως την αποδιοργάνωση αντί της εξολοκλήρου καταστροφής του.

Η παραπάνω μέθοδος, θεωρείται ως οικονομική τόσο ως προς το χρηματικό κόστος, όσο και ως την καταβαλλόμενη προσπάθεια. Αυτό γίνεται ξεκάθαρο στο παρακάτω απλό παράδειγμα. Από την στιγμή που γίνεται χρήση λιγότερων βλημάτων ενάντια στον εχθρό, τότε ως φυσικό επακόλουθο απαιτούνται και λιγότερα μέσα για την εκτόξευση των βλημάτων. Άρα και λιγότερο ανθρώπινο δυναμικό και λιγότεροι συντελεστές διοικητικής μερίμνης και λιγότερα χρήματα. Συμπερασματικά λοιπόν, **ο πληροφοριοκεντρικός πόλεμος δημιουργεί ένα θετικό βρόχο ανάδρασης, ο οποίος βελτιώνει συνεχώς τα περιθώρια άσκησης του «φτηνού πολέμου»**[16].

Το προαναφερθέν όμως είδος πολέμου, δεν είναι το μοναδικό θετικό στοιχείο του πληροφοριοκεντρικού πολέμου. Είναι κοινώς αποδεκτό πως ο πληροφοριοκεντρικός πόλεμος είναι και πολύ αποτελεσματικός. Αυτό συμβαίνει κατά κύριο λόγο διότι αυξάνεται σημαντικά η ταχύτητα της διεξαγωγής του πολέμου και μας δίνεται η δυνατότητα να ενεργούμε ταχύτερα από τον εχθρού. Αυτή λοιπόν η αυξημένη ταχύτητα, προκαλεί παντελή αποπροσανατολισμό στην αλυσίδα διοίκησης του εχθρού και εν συνεχεία κατάρρευση στο εχθρικό στράτευμα.

[16] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ. 259

Σύμφωνα με την ορολογία του Λίντελ Χαρτ (Άγγλος στρατιωτικός ιστορικός) η βελτίωση της ταχύτητας της διεξαγωγής του πολέμου είναι μια νέα μέθοδος στρατηγικής προσέγγισης η οποία ανταποκρίνεται στο σύγχρονο πεδίο μάχης. Μιλάμε για κάτι αντίστοιχο του «Blitzkrieg» (κεραυνοβόλος πόλεμος, ο οποίος επινοήθηκε από τον Γερμανό Χάιντς Γκουντεριαν στις αρχές του Β' Παγκοσμίου Πόλεμο) στην πληροφοριακή εποχή. Το Blitzkrieg θεμελιώνεται στην συνεχή κινητικότητα καθιστώντας τον εχθρό ανίκανο να ακολουθήσει στο πεδίο της μάχης. Αντίστοιχα εφόσον γνωρίζουμε ακριβώς τη θέση μιας εχθρικής δύναμης μέσω κάποιου UAV και διαθέτουμε βλήματα ακριβούς προσβολής, μπορούμε να τους εξουδετερώσουμε σε μικρό χρονικό διάστημα. Εάν όμως δεν είχαμε τις κατάλληλες πληροφορίες και τα μέσα προσβολής, τότε απαιτείται άμεση εμπλοκή των τμημάτων 1ης γραμμής με δεδομένο ένα ποσοστό απωλειών των φίλιων δυνάμεων.

Εν κατακλείδι, στο σύγχρονο επιχειρησιακό περιβάλλον και στις μεταβολές που αυτό έχει υποστεί, ο πληροφοριοκεντρικός πόλεμος ταιριάζει απόλυτα. Αυτό οφείλεται κυρίως στα χρόνια του Β' Παγκοσμίου Πολέμου λόγω της αύξησης της κινητικότητας των στρατευμάτων έχουν δημιουργηθεί πολύ ρευστά πεδία μαχών. Αυτή η κατάσταση ενισχύεται περισσότερο από την αύξηση της ικανότητας μηχανοκίνησης και αεροκίνησης των σύγχρονων στρατών.

Εικόνα 4. Άρμα μάχης LEO 2 A6 HEL.

Η εξέλιξη της τεχνολογίας, αναμένεται να προκαλέσει μελλοντικά πολύ ανεπτυγμένα πεδία μαχών με πολύ ασαφή όρια. Οι αντιμαχόμενες δυνάμεις θα αναμειγνύονται σε μεγάλο βαθμό δημιουργώντας ένα «χυλό μάχης»[17]. Εκτός των μεγάλων μονάδων μάχης,

[17] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ. 260

θα υπάρχει ανάμειξη και στις βασικές μονάδες. Όλη αυτή η αύξηση του «ορίζοντα ανάμειξης» αποτελεί κυρίως αποτέλεσμα της αύξησης των μαχητικών ικανοτήτων μικρών μονάδων.

Ισχύει σε μεγάλο βαθμό, ότι η μείωση του βάρους και του όγκου των οπλικών συστημάτων προσβολής, μέσω της εξάπλωσης της χρήσης μικροηλεκτρομηχανικών συστημάτων (Micro Electronic Mechanic Systems [MEMS]), βελτιώνει σε πολύ μεγάλο βαθμό την εμβέλεια, την ακρίβεια πυρός και την καταστρεπτική ικανότητα ενός οπλικού συστήματος μεγάλου βεληνεκούς ή μιας ομάδας πεζικού με «υπερευφυείς» (brilliant)[18] όλμους, για παράδειγμα. Παρόλα αυτά, σε περίπτωση μάχης που διεξάγεται από μικρές διασπασμένες ομάδες, οι δύο αντίπαλες δυνάμεις μπορούν πολύ πιο εύκολα να «χωνευτούν» η μία μέσα στην άλλη από ότι αν η μάχη αυτή διεξαγόταν από συμβατικές σημερινές δυνάμεις μεγαλύτερου μεγέθους. Αυτό όμως μετουσιώνει το μελλοντικό πεδίο της μάχης σε έναν άναρχο χαώδη χώρο, απόλυτα ασαφή, ασταθή και ταχύτατα ευμετάβλητο. Αυτό έχει σαν αποτέλεσμα να υπάρχει επιστάμενος κίνδυνος για αδελφοκτόνα γεγονότα, δηλαδή για κατά λάθος εμπλοκές μεταξύ φίλιων δυνάμεων (κοινώς blue on blue incidents). Όλο αυτό έχει σαν αποτέλεσμα να καθίσταται ακόμη περισσότερο **επιτακτική η δημιουργία ενός πληροφοριοκεντρικού στρατεύματος**.

Για παράδειγμα, σε μια υποτιθέμενη ελληνοτουρκική σφοδρή ένοπλη αντιπαράθεση, υπάρχει μεγάλη πιθανότητα σύγχυσης των φίλιων με των εχθρικών δυνάμεων διότι και οι δυο χώρες έχουμε πολλά κοινά οπλικά συστήματα.

[18] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ. 261

§1.6 Στάδια διεξαγωγής Πληροφοριακού Πολέμου

Μια πληροφοριοκεντρική πολεμική ενέργεια μπορεί να διαχωριστεί στα εξής στάδια:

α. Απόκτηση της πληροφορίας (ποιος είναι, πόσος είναι και πού είναι ο εχθρός).

β. Ασφαλής, αξιόπιστη και ταχεία μετάδοση της πληροφορίας (ει δυνατόν σε πραγματικό χρόνο) στο επικοινωνιακό δίκτυο (σε οπτικοποιημένη ψηφιακή μορφή και όχι ακουστικά).

γ. Διαχείριση της πληροφορίας (ποιο είναι το καταλληλότερο μέσο από τη μαχητική δύναμη για να την αξιοποιήσει).

δ. Αξιοποίηση της πληροφορίας (Εξόντωση του εχθρού).

Για να γίνει ορθή αξιοποίηση πληροφοριών, τα οπλικά συστήματα που θα την αναλάβουν οφείλουν να πληρούν ορισμένες προϋποθέσεις – χαρακτηριστικά, όπως τα παρακάτω. Ικανότητα προσβολής ακριβείας (καθώς δε φτάνει μόνο η γνώση της θέσης εφόσον δεν υπάρχει κάποιο όπλο που να φτάσει στη ζητούμενη θέση), υψηλή καταστροφική ικανότητα, ταχεία αξιοποίηση της πληροφορίας μέσω ακριαίου προγραμματισμού δεδομένων και αυτόνομης καθοδήγησης στο χώρο. Εξίσου σημαντικές προϋποθέσεις που πρέπει να πληρούν τα νέα οπλικά συστήματα, είναι η αυτοάμυνα έναντι εχθρικών θέσεων, η μη προειδοποίηση του εχθρού για την έλευση του βλήματος, χαμηλό κόστος (ώστε τα συστήματα προσβολής να μπορούν να διατίθενται σε μεγάλα αποθέματα), επίσης θα πρέπει τα οπλικά αυτά συστήματα να μην χρειάζονται ιδιαίτερες απαιτήσεις συντήρησης ή αποθήκευσης και ταυτόχρονα να μην επηρεάζονται από κλιματολογικά

Εικόνα 5:Πολλαπλός Εκτοξευτής Πυραύλων MLRS M271.

φαινόμενα. Τέλος, τα οπλικά συστήματα θα πρέπει να διατίθενται σε ευρεία γκάμα, ώστε να προσβάλουν πολλούς στόχους και να χρησιμοποιείται το κατάλληλο όπλο εναντίον του κατάλληλου στόχου επιτυγχάνοντας την καλύτερη δυνατή σχέση κόστους – απόδοσης.

Άξιο αναφοράς, είναι το γεγονός ότι στον πληροφοριοκεντρικό πόλεμο ίσως και να υπάρχει σύγχυση και συγχώνευση των διαφόρων τακτικών και στρατηγικών επιπέδων. Για παράδειγμα, ένα μεμονωμένο οπλικό σύστημα προσβολής ακριβείας (π.χ MLRS) συνδυαστικά με ένα σύστημα παροχής πληροφοριών (π.χ UAV) μπορεί να διαδραματίσει ένα στρατηγικής σημασίας ρόλο στην εξέλιξη των πολεμικών επιχειρήσεων. Ως επακόλουθο, το να γνωρίζουμε τη θέση ενός συστήματος που θεωρητικά ανήκει στο τακτικό επίπεδο, ίσως αποτελεί χρήσιμη πληροφορία και για την ανώτατη ηγεσία.

Στα πλαίσια των επιχειρήσεων, το **κάθε οπλικό σύστημα**, νοείται ως **οργανικό μέρος μιας συλλογικότερης πολεμικής οντότητας** το οποίο δε μπορεί να κατανεμηθεί ότι ανήκει σε στρατηγικό ή τακτικό επίπεδο (πχ στην εικόνα 5 το MLRS M271). **Το τακτικό με το στρατηγικό επίπεδο, στα πλαίσια του πληροφοριοκεντρικού πολέμου εμπλέκονται** και αυτό είναι κάτι το οποίο πρέπει να ληφθεί σοβαρά υπόψη από τους σχεδιαστές των πολυστρωματικών συστημάτων διοίκησης και ελέγχου, τα οποία θα παρουσιάζουν στους διοικητές την ζωντανή εικόνα του περιβάλλοντος που θέλουν να ενεργήσουν. Θα ήταν σωστό και χρήσιμο λοιπόν, να υπάρχει μια τέτοια διαμόρφωση, η οποία να προσφέρει αναλόγως των επιχειρησιακών απαιτήσεων, τη δυνατότητα μετακίνησης επιπέδου στα συστήματα της απεικόνισης δεδομένων.

Ως επακόλουθο, δεν αρκεί μονάχα η δυνατότητα της ανώτατης διοίκησης να λαμβάνει γνώση της τοποθεσίας και των ενεργειών των μικρών μονάδων, καθώς και οι μικρές μονάδες οφείλουν να αποκτούν γνώση της κατάστασης σε γενικότερα πλαίσια εκτός των στενών γεωγραφικών ορίων που ως σήμερα όριζαν τον τρόπο ενεργεία τους. Δεδομένης της συνεχώς βελτιούμενης αύξησης της εμβέλειας και της ακρίβειας πυρός μικρών βλημάτων, όπως είναι ένα βλήμα πυροβόλου των 155 mm, δεν νοείται ο

περιορισμός της γνωστικής σφαίρας των φορέων τους στο μέχρι σήμερα στενό πλαίσιο. Στο κοντινό μέλλον αναμένεται η ανάπτυξη οβίδων των 155 mm με υπερσμικρυμένα συστήματα κατεύθυνσης. Αυτές οι οβίδες θα επιτυγχάνουν πλήγμα ακρίβειας μέτρου σε αποστάσεις μεγαλύτερες των 100 χλμ. Τα δύο αυτά στοιχεία προσφέρουν ικανότητες στρατηγικών οπλικών συστημάτων. Κατά συνέπεια, και οι φορείς τους θα πρέπει να τροφοδοτούνται από πληροφορίες στρατηγικού επιπέδου.[19]

§1.7 Τα συστατικά- εργαλεία του Πληροφοριακού Πολέμου

Παρακάτω θα γίνει μια μικρή αναφορά-ανάλυση των πέντε συστατικών των στρατιωτικών εφαρμογών του Πληροφοριοκεντρικού Πολέμου.

α. Φυσική Καταστροφή

Φυσική καταστροφή μιας διαδικασίας ή εγκατάστασης (π.χ στρατηγείου, αισθητήρων, Η/Υ) σημαίνει πως δεν μπορούν να επιχειρούν μόνιμα ή για ένα μικρό χρονικό διάστημα.[20]

β. Ηλεκτρονικός Πόλεμος(Η/Π)

Ο Η/Ν πόλεμος, αποτελεί μια στρατιωτική δραστηριότητα που περιγράφει το φάσμα ενεργειών για: α) προσδιορισμό, αναγνώριση, εκμετάλλευση των εκπομπών, β) χρήση ηλεκτρομαγνητικής και κατευθυνόμενης ενέργειας με σκοπό τη μείωση ή παρεμπόδιση εκμετάλλευσης του Η/Μ φάσματος από τον εχθρό και μέσω αυτού, την επίθεση εναντίον του, γ) επιβεβαίωση αποτελεσματικής χρήσης του Η/Μ φάσματος απο τις φίλιες δυνάμεις.[21]

[19]Κωνσταντίνος Γρίβας,2003, «Η Πολεμική Τεχνολογία & η Γεωπολιτική Σκέψη στην αυγή της 3ης Χιλιετίας», σελ 48

[20]Ανχης (ΠΖ) Κωνσταντίνος Χαμεζόπουλος, 2010 , «Πληροφοριακός πόλεμος και οι στρατιωτικές του εφαρμογές στην αυγή του 21ου αιώνα», σελ 137-144.

[21] Ανχης (ΠΖ) Κωνσταντίνος Χαμεζόπουλος, 2010, «Πληροφοριακός πόλεμος και οι στρατιωτικές του εφαρμογές στην αυγή του 21ου αιώνα», σελ. 146

γ. Ασφάλεια Επιχειρήσεων

Ασφάλεια επιχειρήσεων (Operations Security- OPSEC) είναι η διαδικασία προσδιορισμού της ταυτότητας κρίσιμων πληροφοριών και στη συνέχεια ανάλυσης των φίλιων ενεργειών που σχετίζονται με στρατιωτικές επιχειρήσεις αλλά και άλλες δραστηριότητες ώστε να εκτελεστούν μέτρα εξάλειψης των τρωτών σημείων των φίλιων ως προς εκμετάλλευση από τον εχθρό.[22]

δ. Ψυχολογικές Επιχειρήσεις

Είναι προσχεδιασμένες ενέργειες μετάδοσης επιλεγμένων πληροφοριών και μηνυμάτων σε συγκεκριμένα ακροατήρια, για επίδραση στα συναισθήματα, τα κίνητρα, την αντικειμενική λογική και τελικά στη συμπεριφορά αντιπάλων κυβερνήσεων, οργανισμών, στρατιωτικών σχηματισμών ή ομάδων. Ο σκοπός των ψυχολογικών επιχειρήσεων, είναι να παρακινήσουν ή να ενδυναμώσουν τη στάση και συμπεριφορά του στόχου τους, έτσι ώστε αυτές να είναι ευνοϊκές για εκείνο που τις προκαλεί.[23]

ε. Στρατιωτική Παραπλάνηση

Είναι τα μέτρα που σχεδιάζονται και λαμβάνονται για να παραπλανήσουν σκόπιμα τον αντίπαλο ηγέτη στη λήψη αποφάσεων. Εκτελείται με την παραποίηση, διαστρέβλωση ή απόκρυψη, πληροφοριών, θέσεων, σχηματισμών, δυνατοτήτων των φίλιων δυνάμεων, με σκοπό την παρακίνησή του να εκτιμήσει λανθασμένα την κατάσταση και κατά συνέπεια να δράσει λανθασμένα και επιζήμια για τα συμφέροντά του. Η στρατιωτική παραπλάνηση, μπορεί να διαιρεθεί σε πέντε κατηγορίες:[24]

(1). Στρατηγική

(2). Επιχειρησιακή

---

[22] Γρίβας Κωνσταντίνος, «,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής» , Λιβάνης, Αθήνα, Σελ 274

[23] Γρίβας Κωνσταντίνος, «,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής» , Λιβάνης, Αθήνα, Σελ 272-276

[24]Congressional Research Service, 'Network Centric Operations: Background and Oversight Issues for Congress' (Washington DC: Congressional Research Service, 2007), Summary

(3). Τακτική

(4). Υπηρεσιών

(5). Προς υποστήριξη της Ασφάλειας Επιχειρήσεων.

§1.8 Από τον Πληροφοριακό στον Δικτυοκεντρικό Πολεμο

Μια αναμενόμενη συνέπεια του πληροφοριοκεντρικού πολέμου αποτελεί, ο διαχωρισμός των στοιχείων που αποτελούν μια μαχητική δύναμη και η «διασπορά» της στο πεδίο της μάχης, αφού **οι πληροφορίες συγκροτούν έναν ισχυρό ενοποιητικό ιστό ώστε να μην είναι απαραίτητη η φυσική επαφή των μονάδων**.

Διάφορα τεχνολογικά μέσα όπως ραντάρ μεγάλης εμβέλειας, ή ένα επικοινωνιακό δίκτυο «αραχνωτού – χαοτικού» τύπου, στα πρότυπα του διαδικτύου και διαφόρου τύπου πυρομαχικά ακρίβειας μεγάλου βεληνεκούς, που είναι δυνατόν να προσβάλλουν σημειακούς στόχους σε μεσαίες ή μεγάλες αποστάσεις. Τέτοιου είδους τεχνολογικά μέσα επιβάλουν την υπαγωγή των μονάδων μιας μαχητικής δύναμης σε μια δικτυακή «οντότητα» μάχης, πολύ ανώτερη από την απλή άθροιση των μέσων.

Μια δύναμη δικτυοκεντρικού – πληροφοριοκεντρικού τύπου, δεν είναι απαραίτητο να κρατάει την φυσική συνοχή της. Πλέον χωρίζεται σε τμήματα μάχης τα οποία εισέρχονται στην εχθρική διάταξη και μέσω του δικτύου πληροφοριών και πυρών ακριβείας που αξιοποιούν τις δοθείσες πληροφορίες, τα τμήματα αποκτούν μια ουσιαστική μαχητική συνοχή. Για παράδειγμα, ένα όχημα τεχνολογικά ανεπτυγμένο με ψηφιακά συστήματα ή ένα σύνολο οχημάτων που έρχεται κοντά με τον εχθρό, δεν θα στηρίζεται απλά στα δικά του μέσα για την αντιμετώπιση του. Σε αυτή την περίπτωση, κοινοποιεί μέσω δικτύου τα στοιχεία στοχοποίησης και αυτομάτως πυρομαχικά ακριβείας δικά του (βλέπε εικόνα 6 οπλισμένο αερόχημα), ή που προέρχονται από φίλιες δυνάμεις εξοντώνουν τον εχθρό. Έτσι λοιπόν δημιουργείται μια ενότητα ισχύος την οποία δε μπορούμε να την σχετίσουμε με την φυσική συνοχή. Είναι αλήθεια πως για να

μπορέσει να δημιουργηθεί αυτή η δικτυακή δύναμη μάχης δεν επαρκεί το να γίνεται απλή ανταλλαγή πληροφοριών και πυρών υποστήριξης. Πολύ χρήσιμο σε αυτή την περίπτωση είναι η ενεργειακή αυτονομία των καθαυτών δυνάμεων της. Όσο δυνατό και επαρκές όμως είναι το δίκτυο συλλογής, ανάλυσης και μετάδοσης πληροφοριών και όσο ανεπτυγμένα πυρομαχικά ακριβείας μεγάλου βεληνεκούς και αν έχουμε, μια υποτυπώδης ψηφιοποιημένη δύναμη οχημάτων ή άλλων μέσων, δε μπορεί σε καμία περίπτωση να είναι λειτουργική σε αυτό το αποκεντρωτικό μοντέλο αν βασίζεται στα πολύ μικρής αυτονομίας πετρελαιοκίνητα οχήματα του σήμερα. Είναι δηλαδή ανούσιο τα πάντα να λειτουργούν δικτυοκεντρικά και εμείς να χρειαζόμαστε συνεχή ροή ενέργειας ώστε να λειτουργούν τα οχήματα μας. Στην παραπάνω περίπτωση, οι δυνατές επιλογές που μπορούμε να επιλέξουμε είναι δυο.

Εικόνα 6: Μη επανδρωμένο οπλισμένο αερόχημα RQ-1 / MQ-1 Predator.

α. Είτε επιστρέφουμε στην κλασσική «παραδοσιακή» συνοχή των δυνάμεων, αδιαφορώντας για διαδικτυακή λειτουργία.

β. Είτε διασκορπίζουμε τις ευαίσθητες γραμμές ανεφοδιασμού μέσα στις αντίπαλες γραμμές με κίνδυνο φυσικά ο εχθρός να τις καταστρέψει με μεγάλη ευκολία.

Είναι δεδομένο πως η κατάσταση, καθίσταται ακόμη χειρότερη κυρίως λόγω του πολλαπλασιασμού του αριθμού των οχημάτων που δύναται να χρησιμοποιηθούν από τις σημερινές δικτυοκεντρικές δυνάμεις όπως για παράδειγμα το πολυπλατφορμικό (multiplatform) σύστημα FCS το οποίο, αποτελεί σύστημα που επιδιώκει την αντικατάσταση μεγάλου μεγέθους πλατφορμών όπως π.χ. τα άρματα μάχης από νέες πλατφόρμες πιο εξελιγμένες τεχνολογικά. Αυτό οδηγεί σε εκθετική αύξηση των ενεργειακών αναγκών των οχημάτων. Τέτοιου είδους συστήματα, απαιτούν την εύρεση

νέου είδους ενεργειακών πηγών κάτι το οποίο μπορεί να εξελιχθεί μέσω μιας ενεργειακής επανάστασης σε μεγάλη κλίμακα, αντίστοιχη της βιομηχανικής επανάστασης.

Αυτές οι νέες ενεργειακές δυνάμεις είναι απαραίτητες για το «μοντέρνο» στράτευμα που αναπτύσσεται, σύμφωνα με το οποίο χρησιμοποιούνται διασπασμένες δυνάμεις κυρίως εντός της εχθρικής διάταξης που συνδέονται μέσω δικτυοκεντρικών τεχνολογιών. Εξίσου σημαντικό, το γεγονός ότι τέτοιου είδους δυνάμεις, είναι δυνατό να δράσουν και στο πιο απόμερο σημείο του πλανήτη, με μηδαμινό χρόνο προετοιμασίας χωρίς ουδεμία προειδοποίηση, κάτι που μέχρι πρότινος ήταν πρακτικά αδύνατο. Ιδιαίτερα σημαντικό ρόλο ως προς τον εκμηδενισμό του χρόνου προετοιμασίας, παίζει η ανάπτυξη ευέλικτων και οικονομικών υποκατάστατων συστημάτων για δορυφόρους καθώς οι «μοντέρνοι» στρατοί βασίζονται σε αυτούς. Επειδή όμως ο χρόνος για την δημιουργία ενός δορυφόρου και ο χρόνος για να τεθεί σε τροχιά είναι υπερβολικά μεγάλος, γίνονται έρευνες ώστε να βρεθούν νέα μέσα – μέθοδοι (υποκατάστατα) δορυφόρων. Εξαιτίας αυτού λοιπόν και λόγω της τεχνολογικής ανάπτυξης των τελευταίων ετών, με πρωτεργάτες τους Αμερικάνους, επιδιώκεται η ανάπτυξη μη επανδρωμένων αεροχημάτων (τύπου UAV [Unmanned Aerial Vehicles]) πολύ μεγάλου ύψους και εμβέλειας που θα υποκαθιστούν τους δορυφόρους σε «αιφνίδιες» εκστρατείες.

Ακόμη και με αυτή την προοπτική όμως, αυτά τα ρομποτικά αεροσκάφη οφείλουν να έχουν την δυνατότητα να διατηρούνται στον αέρα για μεγαλύτερο διάστημα της μιας εβδομάδας χωρίς αναχορηγία καυσίμου, κάτι το οποίο είναι πολύ δύσκολο εάν δεν εφευρεθεί μια νέα ενεργειακή πηγή. Ήδη οι Ισραηλινοί παρουσιάζουν ανάλογα αεροχήματα τα οποία ίπτανται για διάστημα δύο ημερών.

Ακόμη όμως και στην περίπτωση που δε χρειαζόταν να αναπτυχτούν τα UAV, οι σύγχρονοι στρατοί οφείλουν να αναπτύξουν νέου είδους ενεργειακές τεχνολογίες οι οποίες θα προσφέρουν υψηλή αυτονομία στις δυνάμεις εκστρατείας. Αυτό πρέπει να πραγματοποιηθεί κυρίως διότι ο ρυθμός μάχης γίνεται όλο και πιο γρήγορος κάτι το οποίο φυσικά δε μπορεί να συνδυαστεί με το αργό και παντελώς αναξιόπιστο σύστημα

τροφοδοσίας των σημερινών «πετρελαιοκίνητων» στρατευμάτων εκστρατείας διότι το πετρέλαιο αποτελεί τροχοπέδη στα πόδια των σύγχρονων στρατευμάτων. Ιδιαίτερα, θα πρέπει να αναφέρουμε την ακόρεστη δίψα των ψηφιακών δυνάμεων η οποία φαίνεται με την υπερκατανάλωση μπαταριών. Μια δίψα η οποία δε μπορεί να καλυφθεί από το πετρέλαιο που σημαίνει πως επιβάλλεται η ανάπτυξη νέων ενεργειακών συστημάτων που συνδυάζεται με τις μπαταρίες.

Υπάρχουν φυσικά πολλά περισσότερα τακτικά πλεονεκτήματα των νέων ενεργειακών τεχνολογιών για τους σύγχρονους στρατούς, όπως για παράδειγμα τα stealth χαρακτηριστικά που προσδίδουν οι κινητήρες υδρογόνου σε οχήματα και αεροχήματα ή τα υψηλά περιθώρια επιβίωσης μετά το πλήγμα[25]. Τέλος, άξια αναφοράς θεωρείται και η δυνατότητα σύζευξης αεροχημάτων (υψηλής αυτονομίας που κινούνται με κινητήρες υδρογόνου ή ηλεκτρικής ενέργειας τύπου stealth) με διάφορα όπλα κατευθυνόμενης ενέργειας όπως για παράδειγμα πυροβόλα laser ή μικροκυμάτων. Ένας τέτοιος συνδυασμός τεχνολογιών και μέσων, μπορεί να αποφέρει τεράστια τακτικά πλεονεκτήματα στον κάτοχο τους αλλά και να βρει στρατηγικές επιλογές κρίσιμης σημασίας όπως, για παράδειγμα, στο πλαίσιο της περικύκλωσης της Ρωσίας από συστήματα ικανά να επιφέρουν δραστικό πλήγμα στο Ρώσικο βαλλιστικό οπλοστάσιο και στη Ρώσικη αεράμυνα αποσταθεροποιώντας έτσι το διεθνές σύστημα.

[25] Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής», Λιβάνης, Αθήνα, σελ. 260

§2 Δικτυοκεντρικός Πόλεμος- Network Centric Warfare(NCW)

§2.1 Εισαγωγή στον Δικτυοκεντρικό Πόλεμο

Με την είσοδο μας σε αυτή τη νέα χιλιετία ο στρατός μας εισήλθε σε μια νέα εποχή του τρόπου διεξαγωγής του πολέμου. Βρισκόμαστε στην εποχή όπου ο πόλεμος επηρεάζεται από τις αλλαγές στο στρατηγικό περιβάλλον και την ταχεία τεχνολογική αλλαγή. Βιώνουμε μια μετάβαση από την βιομηχανική εποχή στην εποχή της πληροφορίας. Ταυτόχρονα η Ευρώπη στην οποία ανήκουμε έχει εμπλακεί σε έναν ολοκληρωτικό πόλεμο ενάντια στην τρομοκρατία (επιθέσεις στο Παρίσι, στις Βρυξέλλες, κλπ). Αυτές οι μεταβολές σε συνδυασμό με τις εμπειρίες που αποκτήθηκαν από τις πρόσφατες πολεμικές επιχειρήσεις είχε ως αποτέλεσμα τη δημιουργία της έννοιας του δικτυοκεντρικού πολέμου (NCW).

Ο δικτυοκεντρικός πόλεμος είναι μια αναδυόμενη θεωρία που προέκυψε από τη μετάβαση στον πόλεμο της πληροφορίας. Ο όρος δικτυοκεντρικός πόλεμος περιλαμβάνει τον συνδυασμό των στρατηγικών, των αναδυόμενων τακτικών, των τεχνικών, των διαδικασιών, και των οργανώσεων που μια δικτυωμένη δύναμη εξ ολοκλήρου ή ένα κομμάτι μιας «δικτυωμένης δύναμης» (Networked Force) μπορεί να χρησιμοποιήσει για να επιτευχθεί ένα αποφασιστικό αποτέλεσμα.

Η εφαρμογή του NCW βασίζεται πρώτα από όλα στην ανθρώπινη συμπεριφορά σε αντίθεση με την τεχνολογία των πληροφοριών. Όταν εξετάζουμε το βαθμό στον οποίο μια στρατιωτική οργάνωση, ένα τμήμα της ή το σύνολο της, εκμεταλλεύεται τα μέσα του δικτυοκεντρικού πολέμου θα πρέπει να εστιάσουμε στην ανθρώπινη συμπεριφορά στο «δικτυωμένο» περιβάλλον. Πώς όμως είναι εφικτό οι στρατιωτικές δυνάμεις να συμπεριφέρονται και οργανώνονται αποτελεσματικά όταν είναι «συνδεδεμένες»;

Η θεωρία του δικτυοκεντρικού πολέμου έχει εφαρμογή και στα τρία επίπεδα του πολέμου, δηλαδή στο στρατηγικό, επιχειρησιακό και τακτικό και σε όλο το φάσμα των στρατιωτικών επιχειρήσεων. Μια «δικτυωμένη» δύναμη η οποία διεξάγει δικτυοκεντρικές επιχειρήσεις (Network Centric Operation, NCO) δεν κάνει κάτι καινούργιο ή κάτι διαφορετικό από τις ήδη αναγνωρισμένες μορφές πολέμου. Στο πέρασμα της ιστορίας τα πρόσωπα τα οποία λαμβάνουν αποφάσεις επιδιώκουν να διαμορφώσουν τις συνθήκες ώστε να επιτύχουν τους στόχους τους. Οι σχεδιαστές των επιχειρήσεων από την άλλη επιδιώκουν να δημιουργήσουν αυτές τις συνθήκες ώστε να επιτύχουν τους στόχους τους. Αυτές τις δυνατότητες όμως που παρέχουν τα μέσα του δικτυοκεντρικού πόλεμου δεν επιθυμούν να εκμεταλλευτούν μόνο τακτικοί στρατοί αλλά και διεθνείς τρομοκρατικές και παραστρατιωτικές οργανώσεις όπως η Αλ Κάιντα.

Ο δικτυοκεντρικός πόλεμος (NCW) παρέχει αυξημένες δυνατότητες διεξαγωγής της μάχης λόγω της δικτύωσης που επιτυγχάνεται από τους αισθητήρες, τους φορείς λήψης αποφάσεων και τους μαχητές, ώστε να επιτευχθεί η αύξηση στη ταχύτητα λήψης αποφάσεων και έκδοσης διαταγών, αύξηση του ρυθμού των διαδικασιών, αύξηση της επιβιωσιμότητας και να επιτευχθεί ένας βαθμός αυτό-συγχρονισμού. Ειδικότερα μετατρέπει το πλεονέκτημα των πληροφοριών μάχης συνδέοντας τις φίλιες δυνάμεις μέσα στη ζώνη επιχειρήσεων παρέχοντας πολύ βελτιωμένη αντίληψη της τακτικής κατάστασης, επιτρέποντας την ταχεία και αποτελεσματική δράση με ρυθμό που ο αντίπαλος δεν μπορεί να ακολουθήσει.

Υπάρχουν διαφορετικές προσεγγίσεις ως προς τον ορισμό του Δικτυοκεντρικού Πολέμου (NCW). Ωστόσο όλες συγκλίνουν στην έννοια της διαδικτυακής τεχνολογίας ως πρόσημου στην απόκτηση του πλεονεκτήματος και της πρωτοβουλίας στα πεδία της μάχης. Η Ομοσπονδιακή Υπηρεσία Έρευνας των ΗΠΑ, σε έκθεσή της[26], ορίζει τις δικτυοκεντρικές επιχειρήσεις (όρο που θεωρεί στενά συνδεδεμένο με τον δικτυοκεντρικό

[26] Congressional Research Service, 'Network Centric Operations: Background and Oversight Issues for Congress' (Washington DC: Congressional Research Service, 2007), Summary.

πόλεμο), ως επιχειρήσεις, η διεξαγωγή των οποίων βασίζεται στον υπολογιστικό εξοπλισμό και τις διαδικτυακές επικοινωνίες για την παροχή κοινής αντίληψης(Shared Awareness) του πεδίου της μάχης για τις ένοπλες δυνάμεις. Παρόλα αυτά, άλλα κράτη προσεγγίζουν την έννοιά του με διαφορετικό τρόπο. Οι ένοπλες δυνάμεις της Βρετανίας για παράδειγμα, κάνουν λόγο για την Δικτυοκεντρική Ικανότητα (Network Enabled Capability). Σύμφωνα με έκθεση[27], η βελτίωση της μαχητικής ικανότητας των ένοπλων δυνάμεων και η αύξηση της πιθανότητας επιτυχίας τους στις πολεμικές επιχειρήσεις απαιτούν μια Δικτυοκεντρική προσέγγιση.

§2.2 Θεωρητική Προσέγγιση

Για την καλύτερη αντίληψη του θέματος όμως, είναι σκόπιμο να γίνει μία ιστορική αναδρομή για την εξέλιξη της έννοιας, ιδιαίτερα από πλευράς των Η.Π.Α., καθώς το δικτυοκεντρικό δόγμα αποτελεί μεγάλο κεφάλαιο προς ανάπτυξη του τομέα της διοίκησης και ελέγχου(Command and Control/ C2) αλλά και άλλων τομέων για την ηγεσία των ενόπλων δυνάμεων τους. Η λογική του Δικτυοκεντρικού Πολέμου που αρχικά αποτελούσε μία πιο αυθαίρετη και θεωρητική έννοια, θεμελιώνεται για πρώτη φορά σε βιβλιογραφία το 1996, όταν ο Αμερικανός Ναύαρχος Γουίλλιαμ Όουενς (Admiral William Owens) εισήγαγε την έννοια του «Συστήματος των Συστημάτων» στο ομώνυμο βιβλίο του.

Σύμφωνα με τον Όουενς, υπάρχει η επιτακτική ανάγκη για την ανάπτυξη ενός συστήματος με:

- αισθητήρες συλλογής πληροφοριών
- συστήματα διοίκησης και ελέγχου

[27] Ministry of Defence Joint Service Publication 777 Edn 1, 'Network Enabled Capability' (London: Ministry of Defence UK, 2005).

- όπλων ακριβείας

το οποίο θα είναι ικανό να βελτιώσει την αντίληψη της επιχειρησιακής κατάστασης, την γρήγορη και βέλτιστη στοχοποίηση καθώς και την ορθότερη ανάθεση αποστολών στις Ένοπλες Δυνάμεις.

Το 1996 επίσης το Συμβούλιο Αρχηγών των Η.Π.Α. (Joint Chiefs of Staff) στην έκθεση που εκδίδει ανά δεκαετία (Joint Vision) σχετικά με τις προβλέψεις του περί της εξέλιξης της διεξαγωγής των επιχειρήσεων, κάνει λόγο επίσης για το «**Σύστημα των Συστημάτων**», το οποίο, ως «διαδραστική εικόνα» με την διοίκηση θα αποδίδει άμεσα και με ακρίβεια τα στοιχεία των φίλιων και εχθρικών επιχειρήσεων εντός της περιοχής ενδιαφέροντος, επιτυγχάνοντας την επικρατούσα αντίληψη της τακτικής κατάστασης στο πεδίο των επιχειρήσεων (Dominant Battlespace Awareness)[28], ενώ προσθέτει ότι, παρότι αυτό δεν θα εξαλείψει την λεγόμενη «Ομίχλη του Πολέμου (Fog of War), η αντίληψη της τακτικής κατάστασης, θα βελτιώσει ποιοτικά στην επίγνωση της επιχειρησιακής κατάστασης και θα μειώσει την απαιτούμενη χρονική διάρκεια για αντίδραση, κερδίζοντας έτσι το επιχειρησιακό πλεονέκτημα (Εικόνα 7).

[28] John M. Shalikashvili Chairman of the Joint Chiefs of Staff , «Joint Vision 2010» , Pentagon, Washington, έκδοση 1996, σελ.12

Εικόνα 7: Σχηματική αναπαράσταση της αμερικανικής οπτικής επιχειρήσεων στον κόσμο πριν 15 χρόνια.

Ο όρος όμως του Δικτυοκεντρικού Πόλεμου, πρώτη φορά αναγράφεται σε άρθρο που δημοσιεύτηκε το 1998 από το Πολεμικό Ναυτικό των ΗΠΑ. Οι Αντιναύαρχος Arthur K. Cebrowski και ο απόφοιτος της Ακαδημίας της Πολεμικής Αεροπορίας John Garstka ήταν οι θεμελιωτές του, με το βιβλίο τους «Network Centric Warfare: Developing and Leveraging Information Superiority». Σύμφωνα με το βιβλίο[29] στον εμπορικό τομέα, οι πιο ισχυρές και ανταγωνιστικές επιχειρήσεις είναι οι πρώτες που ανέπτυξαν την πληροφοριακή υπεροχή και την μετάφρασαν σε ανταγωνιστικό πλεονέκτημα δίνοντας κατεύθυνση στις δικτυοκεντρικές επιχειρήσεις. Αυτό το κατάφεραν εκμεταλλευόμενες την πληροφορική τεχνολογία και την ομοιόμορφη ανάπτυξη της οργάνωσης τους. Παρόμοιες θεωρίες έχουν αρχίσει και γεννιούνται στα στρατιωτικά

[29] David S. Alberts, John J. Garstka, «Network Centric Warfare»,2η εκδ.2000,σελ 1

επιτελεία διάφορων χωρών και για αυτό είναι επείγον να μελετηθεί και να απορροφηθεί το δόγμα αυτό στις στρατιωτικές επιχειρήσεις.

Εικόνα 8: Σχηματική Αναπαράσταση του «Κυρίαρχου Ελιγμού» όπως είχαν πρωτοερμηνεύσει τις εφαρμογές του Δικτυοκεντρικού Δόγματος οι David S. Alberts, John J. Garstka και Frederick P. Stein. Στην εικόνα παρουσιάζεται πως η δύναμη που διαθέτει «ζωντανές» πληροφορίες και είναι ικανή να εκτελέσει ταχή ελιγμό, μπορεί να κερδίσει μια ασύμμετρη αναμέτρηση στην οποία ο εχθρός πρέπει είτε να την αντιμετωπίσει από μειονεκτική θέση, είτε να αποσυρθεί από τον αγώνα.

Το 2001 γράφεται το «Understanding Information Age Warfare (UIAW)», με κοινή συγγραφή από τους Alberts, Garstka, Richard Hayes και David S. Signori στο οποίο η γενική θεωρία του προηγούμενου βιβλίου πλέον επεκτείνεται στην εφαρμογή στο επιχειρησιακό πλαίσιο. Συμφώνα με το βιβλίο, το επιχειρησιακό περιβάλλον μπορεί να

αναλυθεί σε τρία domains (πεδία). Το φυσικό πεδίο είναι εκεί όπου πραγματοποιούνται γεγονότα και γίνονται αντιληπτά από αισθητήρες και το προσωπικό. Τα δεδομένα που απορρέουν από το φυσικό πεδίο εκπέμπονται μέσω του πληροφοριακού πεδίου και τελικά λαμβάνονται και επεξεργάζονται από το γνωστικό πεδίο(Cognitive Domain) από όπου αξιολογούνται και αντιμετωπίζονται ανάλογα(Assessed and Acted Upon). Η διαδικασία αντιγράφει τον βρόγχο παρατήρηση, κατεύθυνση, απόφαση και δράση που πρώτος διατύπωσε ο Ταγματάρχης John Boyd της Πολεμικής Αεροπορίας των ΗΠΑ(USAF).

Η πιο πρόσφατη έκδοση (μέχρι τη στιγμή που γράφεται το παρόν) που να πραγματεύεται την θεωρία του δικτυοκεντρικού πολέμου, εκδόθηκε το 2003 με τον τίτλο «Power to the Edge» συγγεγραμμένο από τους David S. Alberts και Richard E. Hayes. Πρόκειται για την ωρίμανση του έργου των δύο συγγραφέων και υποστηρίζει ότι τα σύγχρονα στρατιωτικά περιβάλλοντα είναι περίπλοκα και μάλιστα σε τέτοιο βαθμό ώστε να μην δύνανται να γίνουν πλήρως και εγκαίρως αντιληπτά από έναν μοναδικό μηχανισμό (κέντρο αποφάσεων).

Το επίπεδο όμως της σύγχρονης πληροφοριακής τεχνολογίας είναι σε θέση να επιτρέψει την ταχύτατη και αποτελεσματική διασπορά των δεδομένων σε όλο το δίκτυο και μάλιστα σε τέτοιο βαθμό, ώστε **οι μονάδες που μάχονται, να συλλέγουν** άμεσα **πληροφορίες που τις ενδιαφέρουν**, από μία πηγή πληροφοριών, **παρακάμπτοντας την ιεραρχία.** Έτσι **ισοπεδώνονται οι σχέσεις ροής πληροφοριών και διαταγών της παραδοσιακής ιεραρχίας.**

Αυτές οι «επαναστατικές» ιδέες προκάλεσαν το ενδιαφέρον του Πενταγώνου το οποίο ξεκίνησε έρευνες για την εφαρμογή της ιδέας, καταλήγοντας στην Peer-To-Peer δραστηριότητα σε συνδυασμό με τον παραδοσιακό διαμοιρασμό πληροφοριών. Η αρχή είχε γίνει και είχε έρθει η ώρα για την εφαρμογή.

Ο τότε υπουργός άμυνας Ντόναλντ Ράμσφιλντ (Donald Rumsfeld)[30] ξεκίνησε σοβαρές αλλαγές στην διαδικασία εξέλιξης των ένοπλων δυνάμεων με ακρογωνιαίο λίθο πλέον το Δικτυοκεντρικό Δόγμα.

Στις 29 Οκτώβρη 2001, δημιουργήθηκε το Γραφείο Μετασχηματισμού των Ένοπλων Δυνάμεων (Office of Force Transformation) στο Υπουργείο Άμυνας των ΗΠΑ. Σκοπός του γραφείου αυτού ήταν να φέρει στο προσκήνιο νέες ιδέες και δόγματα, να ανακατευθύνει και να εξασφαλίσει την πρωτοκαθεδρία των ΕΔ της ΗΠΑ παγκοσμίως.

Ως υπεύθυνος του γραφείου αυτού δεν θα μπορούσε να είναι άλλος παρά αυτός που διάρθρωσε το δόγμα του Δικτυοκεντρικού Πολέμου, ο Arthur K. Cebrowski[31]. Ο ίδιος τότε θα δηλώσει ότι «**Ο μετασχηματισμός είναι πάνω από όλα μια συνεχής διαδικασία που δεν έχει τέλος αλλά και έχει ως στόχο να δημιουργήσει ή να προβλέψει το μέλλον**. Επίσης έχει ως στόχο να ασχοληθεί με την συν εξέλιξη των εννοιών, των διαδικασιών, των οργανισμών και την τεχνολογία. Μία αλλαγή σε οποιαδήποτε από αυτές τις περιοχές απαιτεί αλλαγή σε όλα.

Έχει ακόμα ως στόχο να εντοπίσει, να βελτιώσει και να δημιουργήσει νέες βασικές αρχές καθώς και να εντοπίσει και να αξιοποιήσει νέες πηγές ισχύος. Ο γενικός στόχος αυτών των αλλαγών είναι να δημιουργηθεί ένα βιώσιμο και ανταγωνιστικό πλεονέκτημα που θα κατέχουν οι Αμερικανοί στο πεδίο της μάχης.[32]

[30]Ο Ντόναλντ Ράμσφιλντ διατέλεσε υπουργός άμυνας των ΗΠΑ επί προεδρίας Τζορτζ Μπους το διάστημα 20 Ιαν 2001-18 Δεκ 2006

[31] Διατέλεσε διευθυντής του Γραφείου Εκσυγχρονισμού στο Υπουργείο Άμυνας το διάστημα 29 Οκτ 2001- 2 Φεβ 2005.

[32] Defense Science Board 2005 Summer Study on Transformation: A Progress Assessment, April 2006,Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, D.C. 20301-3140,Available from : http://www.oft.osd.mil/what_is_transformation.cfm

§2.3 Το δόγμα των ΗΠΑ

Για τις ΕΔ των ΗΠΑ, όπως υπογραμμίζεται και στις εκθέσεις των γενικών τους επιτελείων (Joint Vision 2010 και 2020), η πληροφορία είναι ο πολλαπλασιαστής της μαχητικής ισχύος. Ο Δικτυοκεντρικός Πόλεμος είναι ένα πακέτο ιδεών, σχεδιασμένων να δημιουργήσουν και να εκμεταλλευτούν την πληροφορία αυτή. Το πακέτο αυτό ακόμα, είναι η οργανωτική αρχή για την απορρόφηση των πληροφοριακών τεχνολογιών από τις ένοπλες δυνάμεις, αλλά και για την προσαρμογή των δεύτερων στο τεχνολογικό περιβάλλον.

Τα αξιώματα του δόγματος του δικτυοκεντρικού πόλεμου σύμφωνα με τον Άλμπερτς[33] είναι :

- Μία ισχυρά δικτυωμένη δύναμη βελτιώνει την ανταλλαγή πληροφοριών.
- Η ανταλλαγή πληροφοριών και η συνεργασία ενισχύουν την ποιότητα των πληροφοριών και την κοινή αντίληψη της επιχειρησιακή κατάστασης.
- Η κοινή αντίληψη της επιχειρησιακής κατάστασης επιτρέπει τον αυτοσυγχρονισμό των εμπλεκόμενων δυνάμεων.

Τα παραπάνω, με την σειρά τους, αυξάνουν δραματικά την αποτελεσματικότητα της αποστολής. Για αυτό το λόγο ο Δικτυοκεντρικός Πόλεμος περιλαμβάνει τόσο την παροχή πληροφοριών σε όλα τα κλιμάκια όσο και τον επαναπροσδιορισμό των σχέσεων όλων των συμμετεχόντων στην αποστολή διοικητών και υφισταμένων.

Το Υπουργείο Άμυνας των ΗΠΑ έχει αποφασίσει ότι το κύριο τεχνικό πλαίσιο για την εφαρμογή του δικτυοκεντρικού πολέμου θα είναι το Παγκόσμιο Πλέγμα Πληροφοριών (ΠΠΠ) (Global Information Grid GIG). Το ΠΠΠ αποτελεί την πιο πιστή υλοποίηση του «Συστήματος των Συστημάτων» (όπως το είχε περιγράψει ο Ναύαρχος Όουενς) μέχρι σήμερα και εξελίσσεται-διευρύνεται με ραγδαίους ρυθμούς.

[33] Information Age Transformation: Getting to a 21st Century Military, Washington, DC, CCRP Publications, Πρώτη έκδοση 1996, σελ. 7-8.

Περιλαμβάνει όσα συστήματα πληροφοριών, υπολογιστικά συστήματα, λογισμικό, δεδομένα, υπηρεσίες ασφάλειας καθώς και τα συστήματα εθνικής ασφαλείας και σχετικές υπηρεσίες κατέχει ή εκμεταλλεύεται η Αμερικανική κυβέρνηση. Το ΠΠΠ διαχειρίζεται από μία επιχειρησιακή δικτύωση, γνωστή ως Net Ops[34] το οποίο ορίζεται ως το επιχειρησιακό πλαίσιο που υποστηρίζει τις αποστολές διαμοιράζοντας διαβαθμισμένες πληροφορίες σε όσους συμμετέχουν σε αυτές, ενώ φροντίζει οι δεύτεροι να έχουν πρόσβαση σε αυτές έγκαιρα και από οποιοδήποτε σημείο. Το Net Ops έχει τρεις βασικές αποστολές:

- Την Επιχειρησιακή Διαχείριση ΠΠΠ (GIG Enterprise Management/GEM)
- Την Εξασφάλιση Δικτύου ΠΠΠ (GIG Net Assurance/GNA)
- Τη Διαχείριση Περιεχομένου ΠΠΠ (GIG Content Management/GCM)[35]

Έτσι η διαχείριση, η βιωσιμότητα και η λειτουργία του ΠΠΠ αρχικά βασιζόταν στην Επιχειρησιακή Επίγνωση και στην Διοίκηση και Έλεγχο που ασκείται από τον Διοικητή της Στρατηγικής Διοίκησης των ΗΠΑ (US STRAT COM), σε συνεργασία με το Υπουργείο Άμυνας των ΗΠΑ και την παγκόσμια κοινότητα του Net Ops. Η ομάδα αυτή (Joint Task Force-Global Network Operations (JTF-GNO))[36] θα εξασφάλιζε την πληροφορική υπεροχή των ΗΠΑ σε παγκόσμιο επίπεδο. Μετά από μερικές αλλαγές στην σύνθεση και στις διοικήσεις που υπαγόταν η ομάδα καταργήθηκε[37] ενώ η αποστολή της

[34] Department of Defense INSTRUCTION, «NetOps for the Global Information Grid (GIG)», December 2008, No. 8410.02, σελ.2 Available from: http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf

[35] NetOps for the Global Information Grid (GIG), DoD(Department of Defence) No. 8410.02, 19 Dec 2008, σελ. 2, Available from: http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf

[36] NetOps for the Global Information Grid (GIG), DoD(Department of Defence) No. 8410.02, 19 Dec 2008, σελ. 11-12 , Available from: http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf

[37]Ο χρόνος που λειτούργησε επιχειρησιακά ήταν 1998-2010 μέχρι την ανακοίνωση διάλυσης της από τον τότε Διοικητή της Στρατηγικής Διοίκησης, Στρατηγό Αεροπορίας Kevin P. Chilton. Ο ίδιος θα δηλώσει ότι ο πληροφοριακός πόλεμος πλέον είναι ένα νέο πεδίο μάχης αναβαθμίζοντας έτσι τον ρόλο του δικτυοκεντρικού δόγματος
Army Sgt. 1st Class Michael J. Carden, «Cyber Task Force Passes Mission to Cyber Command», American Forces Press Service, 2010.

αναβαθμίστηκε, διευρύνθηκε και ανατέθηκε στην Διοίκηση Διαδικτύου (US Cyber Command).

§2.4 Επιχειρησιακές εφαρμογές Δικτυοκεντρικού Πολέμου

Στο κεφάλαιο αυτό, γίνεται ανάλυση του τρόπου με τον οποίο οι ΗΠΑ χρησιμοποίησαν την θεωρία και την οργάνωση που επιβάλλει το Δικτυοκεντρικό δόγμα καθώς και διάφορα τακτικά συστήματα που χρησιμοποίησαν στο πεδίο της μάχης, κυρίως την εποχή 1990-2000.

1991: Επιχείρηση Desert Storm

Εικόνα 9: Αεροσκάφος F-14 Tomcat του Αμερικανικού Ναυτικού σε πτήση πάνω από τις κατεστραμένες πετρελαιοπηγές του Κουβέιτ από τον Ιρακινό στρατό. Η υποστήριξη με πυρά ακριβείας και αποστολές επιτήρησης που προσέφερε η συμμαχική αεροπορία μείωσαν δραματικά τις απώλειες των δυνάμεων στο έδαφος από το εχθρικό πυρ.

Στην επιχείρηση Καταιγίδα της Ερήμου[38] ο αμερικανικός στρατός μόλις είχε ξεκινήσει να εκμεταλλεύεται τις πληροφοριακές τεχνολογίες στον βαθμό που πρόσταζε το δικτυοκεντρικό δόγμα. Τα συστήματα επικοινωνιών ήταν αρκετά ελλιπή, σε βαθμό μάλιστα που αρκετές φορές οι μονάδες στο πεδίο της μάχης θα έπρεπε να χρησιμοποιούν τα πολιτικά δίκτυα επικοινωνιών. Οι επικοινωνίες επίσης μεταξύ συστημάτων διοίκησης και ελέγχου και μεταξύ αισθητήρων (όπως για παράδειγμα μεταξύ AWACS και των πλοίων με το σύστημα Aegis) ήταν επίσης περιορισμένες ή αναξιόπιστες ενώ στο πεδίο της μάχης οι τακτικές επικοινωνίες γίνονταν με ασύρματους AM και FM που ήταν ο πλέον «παραδοσιακός» τρόπος επικοινωνιών αλλά δημιουργούσε μεγάλα κενά πληροφοριών.

Ωστόσο υπάρχουν παραδείγματα όπου αισθητήρες προσέφεραν πληροφορίες ταυτόχρονα σε διάφορους διοικητές. Η αεροπορία έκανε αναγνωρίσεις με δορυφόρους και αεροσκάφη στο έδαφος, με ραντάρ και AWACS στον αέρα. Στο έδαφος επίσης οι μονάδες παραλάμβαναν πληροφορίες από UAV. Ενώ το σύστημα JSTARS συμμετείχε για πρώτη φορά σε πόλεμο τροφοδοτώντας με πληροφορίες τα διοικητικά κέντρα σε αέρα και έδαφος.[39] Η εκμετάλλευση των συστημάτων έγινε η βάση στην οποία θα αναδειχθεί ο δικτυοκεντρικός πόλεμος.

[38] Η επιχείρηση Desert Storm πραγματοποιήθηκε σε χώρες της Μέσης Ανατολής (Ιράκ, Σαουδική Αραβία, Κουβέιτ) το διάστημα 2 Αυγ 1990 με 28 Φεβ 1991 με αντιμαχόμενες τις δυνάμεις των ΗΠΑ και της συμμαχία τους έναντι του Ιράκ.

[39] U. S. News and World Report, Triumph without Victory, σελ. 275-277.

1995-1998: Επιχειρήσεις Deliberate Force & Joint Endeavor

Εικόνα 10: Βομβαρδιστικό Αεροσκάφος τύπου Stealth F-117 NightHawk. Αποτέλεσε ένα από τα πλέον προηγμένης τεχνολογίας αεροσκάφη που χρησιμοποίησε η συμμαχική αεροπορία κατα τις επιχειρήσεις στην Γιουγκοσλαβία. Καθώς και το μοναδικό αεροσκάφος τεχνολογίας Stealth που καταρρίφθηκε ποτέ.

Η επιχείρηση Deliberate Force[40] περιλάμβανε τον συγχρονισμό των νατοϊκών δυνάμεων που επιχειρούσαν από βάσεις στην Αλβανία, Γερμανία, Ιταλία, Γαλλία και ναυτικό στην Αδριατική θάλασσα. Σύγχρονα συστήματα διοίκησης, ελέγχου και επικοινωνιών (ακόμα και στο επίπεδο συμβουλίων μεταξύ διοικητών και πολιτικών αρχηγών) υποστήριξαν τις επιχειρήσεις. Επίσης αναβαθμίστηκε ο ρόλος των UAV σε αποστολές αναγνώρισης και επιτήρησης, ενώ σε ορισμένες περιπτώσεις αισθητήρες είχαν

[40] Πρόκειται για αεροναυτική επιχείρηση που διήρκησε από τον Αυγ 1995 με Σεπ 1995 στην Βαλκανική χερσόνησο και πιο συγκεκριμένα στα εδάφη της τότε Γιουγκοσλαβικής Δημοκρατίας με αντιμαχόμενες δυνάμεις τη συμμαχία του ΝΑΤΟ έναντι της Σερβικής Δημοκρατίας.

συνδεθεί με αναλυτές οι οποίοι έκαναν εκτιμήσεις σχετικά με την στόχευση και καταστροφή στόχων[41].

Στις αρχές Δεκέμβρη του 1995 η επιχείρηση Joint Endeavor ξεκίνησε στην Βοσνία. Καθ'όλη τη διάρκεια της αποστολής γίνονταν συνεχείς τεχνολογικές βελτιώσεις στα συστήματα που χρησιμοποιούσαν οι επίγειες δυνάμεις (γνωστές ως IFOR/ Implementation Force). Ένα δίκτυο πληροφοριών βασισμένο στο διαδίκτυο χρησιμοποιήθηκε για την συνεργασία μεταξύ των IFOR και των μονάδων υποστήριξης. Τα UAV απέκτησαν ακόμα πιο σημαντικό επιχειρησιακό ρόλο στις αποστολές πληροφοριών, προβάλλοντας εικόνα near real time, δηλαδή σχεδόν ζωντανή σύνδεση, στα κέντρα διοίκησης ένα σημαντικό νέο χαρακτηριστικό στοιχείο τους. Σημαντικό είναι επίσης ότι γίνεται η υπαγωγή όλων των κέντρων ανάλυσης, που μέχρι τότε ήταν διαφορετικό για κάθε κατηγορία αισθητήρων (διάστημα, αέρας, ξηρά), στο κέντρο ανάλυσης του θεάτρου επιχειρήσεων. Συμπερασματικά βελτιώθηκε το επίπεδο των αισθητήρων, με την καλύτερη προβολή του πεδίου επιχειρήσεων στα κέντρα διοίκησης. Μόνο οι πληροφορίες που ενδιέφεραν το κάθε κέντρο θα μεταδίδονταν σε αυτό, ενώ αυτές οι πληροφορίες θα προέρχονταν από αισθητήρες από όλο το πεδίο επιχειρήσεων[42].

1998-1999: Επιχείρηση Allied Force

Στην επιχείρηση αυτή[43], έχουμε ακόμα μεγαλύτερη διασύνδεση μεταξύ εδάφους, θάλασσας και αέρα από ότι στην Deliberate Force χάρη στην περαιτέρω ανάπτυξη της τεχνολογίας του C4I. Βελτιώσεις στις επικοινωνίες επέτρεψαν την επιτάχυνση της

[41] Owen, Robert C , «Deliberate Force: A Case Study in Effective Air Campaigning», Maxwell AFB έκδοση 2000 , σελ. 54, 160-163, 180-182.,

[42]. Wentz & Larry K, «Lessons From Bosnia: The IFOR Experience» , Contributing Editor Larry Wentz, 2007, σελ.111, 137, 227-228

[43] Η επιχείρηση Allied Force διήρκησε από τα τέλη 1998 μέχρι αρχές 1999, αποστολή είχε τη δημιουργία συνθηκών για ειρήνη στην περιοχή του Κόσσοβου.

διάδοσης πληροφοριών και την εμπλοκή στόχων με χρονικό περιορισμό, μέσω μιας διαδικασίας που ενέπλεκε επιτελεία που βρίσκονταν στην Ιταλία, στο Βέλγιο, στην Αγγλία ή ακόμα και στις ΗΠΑ. Ο χώρος δηλαδή που βρίσκονταν μια υπηρεσία η ένα επιτελείο που συμμετείχε στην διαδικασία δεν έπαιζε πλέον ρόλο.[44] Στην επιχείρηση αυτή επίσης μετείχε το TF HAWK[45], ένα αμφιλεγόμενο πρόγραμμα της συμμαχικής αεροπορίας για την συνεργασία και τον αυτοσυγχρονισμό της Αεροπορίας και του Στρατού Ξηράς σε αποστολές κρούσης σε στόχους εις βάθος. Όσο αναφορά την αποστολή του μάλλον απέτυχε (διότι δεν ανέλαβε τελικά ούτε μια αποστολή κρούσης) αλλά οι ISR (Intelligence- Surveilance- Reconnaisance) ικανότητες του εκτιμήθηκαν. Αυτό γιατί η διασύνδεση των συστημάτων αεροπορίας-στρατού ήταν άμεση από το ενιαίο αυτό κέντρο διοίκησης και ενώ η φυσική του παρουσία να περιέχεται σε έναν μικρό τομέα στην Αλβανία, τα συστήματα αισθητήρων του να φτάνουν αρκετά μέσα στο Κόσσοβο.

Το Κόσσοβο ήταν μια μεγάλη δοκιμασία για την Συμμαχική Αεροπορία. Ο Σέρβικος στρατός, όντας πιο έμπειρος στην τεχνική της παραλλαγής και της παραπλάνησης, σε συνδυασμό με την καλά οργανωμένη αεράμυνά του κατάφερε και παρέσυρε τους Νατοϊκούς σε μεγάλη σπατάλη πυρομαχικών ενώ κατάφερε και προκάλεσε απώλειες σε συστήματα UAV αλλά και 2 αεροπλάνων.

2001-Σήμερα: Επιχείρηση Enduring Freedom

Πρόκειται για μέρος του Πολέμου έναντι στην Τρομοκρατία, η επιχείρηση αυτή τερματίστηκε μερικώς τον Δεκέμβριο του 2014 μετά από σχετικό διάγγελμα του Προέδρου της Αμερικής Μπαράκ Ομπάμα. Ωστόσο συνεχίζει να εξελίσσεται υπό το όνομα «Operation Freedom's Sentinel» σε όλα τα πεδία επιχειρήσεων (όπως Κέρας Αφρικής- Σομαλία). Ωστόσο οι καινοτομίες και οι εφαρμογές στο πλαίσιο της Διοίκησης

[44] Michael Ignatieff , «Virtual War: Kosovo and Beyond» Metropolitan Books, Henry Holt and Co., έκδοση 2000, σελ 99-101

[45] Επιχειρησιακό από 5 Απρ 1999 – 24 Ιουν 1999

και Ελέγχου θα μπορούσαν να κάνουν τους μελλοντικούς ιστορικούς να αναφέρονται στην επιχείρηση αυτή ως την πρώτη στρατιωτική επιχείρηση όπου εφαρμόστηκε πλήρως το δικτυοκεντρικό δόγμα αλλά και οι «ψηφιακές δυνάμεις».

Το πιο ενδιαφέρον είναι ότι πριν ακόμα ξεκινήσει η επιχείρηση αυτή ο Αμερικάνικός Στρατός είχε πραγματοποιήσει την άσκηση (The Division Capstone Exercise) όπου δοκιμάστηκε σε πολεμικά παίγνια η πρώτη ψηφιακή μεραρχία (4η M/K Μεραρχία, έδρα Fort Hood Texas). Οι μονάδες που συμμετείχαν στην άσκηση χρησιμοποίησαν ολοκληρωμένα συστήματα C4I και δίκτυα πληροφοριών μέχρι και στο επίπεδο διμοιριών αλλά και κάθε οχήματος. Το αποτέλεσμα ήταν η πλήρης επιχειρησιακή επίγνωση του πεδίου επιχειρήσεων (η οποία προήλθε από αισθητήρες τόσο εξωτερικούς όπως δορυφόροι, JSTAR, Radar και αεροσκάφη όσο και οργανικούς όπως UAV μεραρχίας, παρατηρητές, οπτικά οχημάτων και ελικόπτερα), καθ' ύψος και πλάτος της Ζώνης Ενεργείας (ZEN) της Μεραρχίας[46]. Η επιτυχία αυτής της άσκησης και τα συμπεράσματα που διεξήχθησαν θα ήταν καθοριστικά για τις επιχειρήσεις του Στρατού Ξηράς ειδικά στο Αφγανιστάν.

Με την έναρξη της Enduring Freedom το στοίχημα για τις Ένοπλες Δυνάμεις των Αμερικάνων δεν ήταν η κυριαρχία στο πεδίο της μάχης (η οποία θα λέγαμε ότι μάλλον ήταν δεδομένη), αλλά η βιωσιμότητα των τακτικών δικτύων και των ψηφιακών μονάδων και η έγκαιρη προσαρμογή τους σε κάθε επιχειρησιακό περιβάλλον.

Ένα περίπολο καταδρομών των Η αυξημένη χρήση των UAV και άλλων πλατφόρμων αισθητήρων όπως τα P3 Orion και των νεοφερμένων UAV Globan Hawk βοήθησε στην δημιουργία ενός συμπαγούς συστήματος ISR που, ως σύνολο συστημάτων, θα μπορούσε να επιτηρεί συνεχώς οποιαδήποτε περιοχή επιχειρήσεων του δοθεί, συμβάλλοντας καταλυτικά στην επιτυχία του εγχειρήματος. Σημειώνεται ότι για πρώτη

[46] Η άσκηση αποτελούταν από δύο φάσεις. Η πρώτη σχετίζονταν με τους ελιγμούς και το πυρ μιας ταξιαρχίας σε περιβάλλον μάχης έναντι δυνάμεων, συμβατικών και μη, με αυτοματοποιημένα συστήματα διοίκησης πυρός. Η δεύτερη αφορούσε την διοίκηση και τον έλεγχο της μεραρχίας, με την χρήση αισθητήρων σε όλα τα επίπεδα διοίκησης και την σύνθεση της επιχειρησιακής αυτής εικόνας καθώς και την επικοινωνία των προηγουμένων με τακτικά δίκτυα.

φορά δόθηκε σημασία στα συστήματα επιτήρησης, για την διεξαγωγή μιας επιχείρησης, αντάξια της σημασίας και της προσοχής που δίνεται στα οπλικά συστήματα, ενώ η επικοινωνία μεταξύ συστημάτων εξασφαλίστηκε μέσω του τακτικού δικτύου Link-16. Έτσι η συνεργασία αέρα-εδάφους εδραιώθηκε στις ΗΠΑ, σήμερα έχει διαρκή εγγύς αεροπορική υποστήριξη, η οποία θα προσβάλλει άμεσα στόχους με την κατεύθυνση του πρώτου, ενώ και τα δύο στοιχεία βρίσκονται σε περιοχές αρκετές εκατοντάδες χιλιόμετρα από τις μονάδες που εδρεύουν (πιθανόν σε διαφορετικές χώρες), αλλά παρά την φυσική απόσταση, έχουν υποστήριξη, διοικητική μέριμνα από αυτές καθώς και επικοινωνία μεταξύ τους, ενώ βασικό στοιχείο της δράσης τους είναι ο αυτοσυγχρονισμός.

2018-2020: Τουρκική εισβολή στο Αφρίν (Zeytin Dalı Harekâtı)

Η στρατιωτική αυτή επιχείρηση αποτελεί ένα ακόμη μέρος της μακροχρόνιας Κουρδοτουρκικής σύγκρουσης που επικρατεί από το 1978 και του Συριακού Εμφύλιου πολέμου. Το συγκρότημα καντονίων της λεγόμενης Ροζάβα περίπου από τα μέσα του πολέμου έχει επεκταθεί, καταφέρνοντας να έχουν τον έλεγχο όλων των περιοχών που ξεκινούν από τα επίσημα σύνορα της Συρίας με την Τουρκία και καταλήγουν παράλληλα με τον ποταμό Ευφράτη. Η απόκτηση των εδαφών αυτών, έγινε κάτα την διάρκεια πολεμικών συγκρούσεων των Κούρδων με τους στρατιώτες του Ισλαμικού κράτους, οδηγώντας έτσι στην εδαφική παρακμή των δεύτερων. Επίσης, έχουν ύπο την κατοχή τους μια συνοικία της πόλης του Χαλεπίου. Ο Τούρκικος στρατός ωστόσο, έχει εισβάλει μέσω της αποστολής "Η Ασπίδα του Ευφράτη", έχει κατακτήσει και αποκόψει τον έλεγχο από τους Κούρδους ανάμεσα στα καντόνια του Αφρίν και του Κομπανίου, ανατολικά του καντονίου του Αφρίν. Μάλιστα, εντός των πρώτων δεκαπέντε ημερών κατάφερε να αιχμαλωτίσει με την βοήθεια Σύριων ανταρτών 15 χωριά.

Κατά την περίοδο των επιχειρήσεων στο Αφρίν τα Τουρκικά UAV τύπου BayraktarTB2 και τα νεότευκτα ANKA-S περιπολούσαν σε 24ωρη βάση και μετέδιδαν συνεχώς την εικόνα από το πεδίο των συγκρούσεων στα κέντρα επιχειρήσεων. Μέσω της

κεραίας SATCOM μεταφέρονταν η εικόνα στο δορυφόρο Türksat 4B. Ο δορυφόρος αναμετέδιδε την εικόνα στην Άγκυρα και λαμβάνονταν εγκαίρως οι κατάλληλες αποφάσεις, ενώ παράλληλα αεροσκάφη με αρτηρίες μεταφοράς δεδομένων λάμβαναν συντεταγμένες των στόχων για να τους προσβάλλουν άμεσα. Παράλληλα τα UAV τύπου Togan πραγματοποιούσαν παρεμβολές στο H/M φάσμα λαμβάνοντας εικόνα για τις θέσεις τυχόν εχθρικών «αισθητήρων» στο καντόνι. Είχαμε δηλαδή μια συνεχή ροή πληροφοριών μεταξύ αισθητήρων και οπλικών συστημάτων, ανάλυση και επεξεργασία από τα κέντρα λήψης αποφάσεων, συνεχείς και ασφαλείς επικοινωνίες μεταξύ των εμπλεκόμενων μονάδων-μέσων, και υψηλό βαθμό διακλαδικότητας. Η ένταξη του ψηφιακού διακλαδικού δικτύου επικοινωνιών TAFICS11, και η περαιτέρω ανάπτυξη του δορυφορικού προγράμματος, θα συμβάλει καθοριστικά στην ολοκληρωμένη ικανότητα των Τουρκικών ενόπλων δυνάμεων να δημιουργήσουν περιβάλλον δικτυοκεντρικού πολέμου.

Σεπτέμβριος 2020: Πόλεμος στο Ναγκόρνο- Καραμπάχ

Η σύγκρουση του Ναγκόρνο- Καραμπάχ το 2020 είναι ένα επεισόδιο στην ένοπλη σύγκρουση μεταξύ της Αρμενίας και του Αζερμπαϊτζάν για τον έλεγχο του Ναγκόρνο-Καραμπάχ (Αρτσάχ) ενός μη αναγνωρισμένου κράτους, το οποίο ανακήρυξε την ανεξαρτησία του από το Αζερμπαϊτζάν το 1991. Κατά την διάρκεια των επιχειρήσεων έγινε εκτενής χρήση δικτυοκεντρικών συστημάτων τόσο για την αναγνώριση όσο και για την πλήξη στόχων ευκαιρίας και μη. Ο στρατός του Αζερμπαιτσάν χρησιμοποιείσαι αποτελεσματικά τα UAS, ειδικά το Bayraktar TB-2, τα οποία επιτηρούσαν επί 24ώρου βάσεως την περιοχή ενδιαφέροντας και απέστειλαν πληροφορίες σε πραγματικό χρόνο στα κέντρα επιχειρήσεων. Επίσης η χρήση «έξυπνων πυρομαχικών» τύπου MAM-L[47]

[47] Το MAM-L (Mini Akıllı Mühimmat, Smart Micro Munition) είναι ένα σύστημα έξυπνων πυρομαχικών που καθοδηγείται από λέιζερ και παράγεται από τον τουρκικό κατασκευαστή αμυντικής βιομηχανίας ROKETSAN. Το MAM έχει αναπτυχθεί για μη επανδρωμένα εναέρια οχήματα (UAV), ελαφρά αεροσκάφη και αποστολές εδάφους-εδάφους για πλατφόρμες αέρα χαμηλής χωρητικότητας. Η Roketsan ισχυρίζεται ότι το MAM μπορεί να εμπλέξει σταθερούς και κινούμενους στόχους με υψηλή ακρίβεια.

έπαιξαν πρωταγωνιστικό ρόλο στην καταστολή της αεράμυνας των Αρμενίων. Αξιοσημείωτο είναι ότι εντός των δυο πρώτων εβδομάδων της σύρραξης τα Drone των Αζέρων κατέστρεψαν περίπου 60 αρμένικα συστήματα Αεράμυνας όπως το 9K33 OSA[48] και το 9K35 Strela[49]. Η συνεχής ροή πληροφοριών μεταξύ αισθητήρων και οπλικών συστημάτων, η τάχιστη ανάλυση και επεξεργασία από τα κέντρα λήψης αποφάσεων είχαν ως αποτέλεσμα την στρατιωτική υπεροχή των Αζέρων.

§2.5 Πλεονεκτήματα Δικτύωση (Networking)

Πολλά έχουν γραφτεί και ειπωθεί κατά την τελευταία δεκαετία ως προς το γιατί η δικτύωση είναι απαραίτητη, και πως βελτιώνει την ικανότητα των επιχειρήσεων. Η δικτύωση αποσκοπεί στην επιτάχυνση του ρυθμού των επιχειρήσεων σε όλα τα επίπεδα. Αυτό επιτυγχάνεται με την παροχή ενός μηχανισμού για την ταχεία συγκέντρωση και διανομή πληροφοριών στόχευσης και ταχύτατης έκδοσης οδηγιών εμπλοκής

Σε μια πιο τεχνική έννοια του όρου, η δικτύωση βελτιώνει την ρυθμό των επιχειρήσεων (op- tempo) επιταχύνοντας τις φάσεις Παρατήρησης-Προσανατολισμού (Observation-Orientation) της θεωρίας του Boyd, η οποία ονομάστηκε OODA (Observation-Orientation-Decision-Action). Διατυπώθηκε πρώτη φορά κατά τη διάρκεια της δεκαετίας του 1970 από τον στρατηγό John Boyd της πολεμικής αεροπορίας των ΗΠΑ. Η OODA είναι μια αφηρημένη έννοια που περιγράφει την ακολουθία των γεγονότων που λαμβάνουν χώρα σε οποιαδήποτε στρατιωτική εμπλοκή. Οι αντίπαλοι πρέπει συνεχώς να συγκεντρώνουν πληροφορίες, η επιτιθέμενη δύναμη θα

[48] Το 9K33 Osa είναι ένα αυτοκινούμενο, χαμηλού υψομέτρου, τακτικό σύστημα πυραύλων επιφανείας-αέρος μικρής εμβέλειας που αναπτύχθηκε στη Σοβιετική Ένωση τη δεκαετία του 1960.

[49] Το 9K35 Strela είναι ένα σύστημα πυραύλων επιφανείας-αέρος μικρής εμβέλειας, οπτικής / υπέρυθρης καθοδήγησης, χαμηλού υψομέτρου που αναπτύχθηκε στη Σοβιετική Ένωση τη δεκαετία του 1970.

πρέπει η ίδια να προσανατολίσει την κατάσταση, στη συνέχεια να παίρνει αποφάσεις και να ενεργεί προς επίτευξη των στρατηγικών σκοπών της.

Σε φιλοσοφικό και πρακτικό επίπεδο αυτό που παρέχει ένα βασικό πλεονέκτημα στις επιχειρήσεις είναι η δυνατότητα μιας δύναμης να καθορίζει το ρυθμό της εμπλοκής και να διατηρεί την πρωτοβουλία. Στην πραγματικότητα, ο επιτιθέμενος αναγκάζει τον αντίπαλό του σε μια αμυντική στάση και δεν επιτρέπει στον αμυνόμενο να αποκτήσει πλεονέκτημα στη σύγκρουση.

Τα τέσσερα συστατικά στοιχεία της OODA μπορεί να κατηγοριοποιηθούν σε 3 κατηγορίες οι οποίες σχετίζονται με την επεξεργασία πληροφοριών, την κίνηση των στρατευμάτων και την εκμετάλλευση της δύναμης πυρός. Η θεωρία της «Παρατήρηση-Προσανατολισμός-Απόφασης», που ήδη αναφέραμε, βασίζονται στις πληροφορίες ενώ η «δράση» του πεδίου της μάχης βασίζεται στην κίνηση των δυνάμεων, τη θέση και τη δύναμη πυρός.

Η θεωρία της «Παρατήρησης-Προσανατολισμού-Απόφασης» αφορά τη συλλογή πληροφοριών, τη διάδοση πληροφοριών, την ανάλυση πληροφοριών, την κατανόηση των πληροφοριών και την απόφαση του τρόπου ενεργείας μια στρατιωτικής δύναμης με βάση αυτές τις πληροφορίες. Όσο πιο γρήγορα μπορεί μια δύναμη να συγκεντρώσει, να διανείμει, να αναλύει, και να κατανοεί τις πληροφορίες, τόσο πιο γρήγορα μπορεί να αποφασίζει πώς και πότε να δράσει κατά τη διάρκεια της μάχης. Η δικτύωση είναι ένας μηχανισμός μέσω του οποίου μπορεί να επιτευχθεί η επιτάχυνση των φάσεων της Παρατήρησης-Προσανατολισμού της OODA, και λόγω αυτού διευκολύνεται η φάση της απόφασης.

Η σωστή εφαρμογή της δικτύωσης μπορεί να συμβάλει στη βελτίωση της αποτελεσματικότητας και με άλλους τρόπους. Μια τέτοια τεχνική είναι ο «αυτό-συγχρονισμός», ο οποίος επιτρέπει τον «απευθείας έλεγχο». Για παράδειγμα ένας πιλότος που λαμβάνει συνεχείς ενημερώσεις από ένα αεροσκάφος AEW & C μέσω ενός δικτύου, μπορεί να λάβει τις δικές του τακτικής σημασίας αποφάσεις, αξιοποιώντας την εικόνα της κατάστασης που μεταδίδεται από το αεροσκάφος AEW & C. Αυτό δεν αποτελεί βέβαια

ένα νέο μοντέλο μάχης, αλλά η δικτύωση διευκολύνει των συνδυασμό των πληροφοριών. Συγκρίνετε αυτό το παράδειγμα με τις ραδιοφωνικές εκπομπές που εξέπεμπαν οι κόμβοι αεράμυνας της γερμανικής αεροπορίας σε συχνότητα ΑΜ προς τα μαχητικά της Luftwaffe κατά τον Β' Παγκόσμιο. Οι εκπομπές αυτές παρείχαν την δυνατότητα στους χειριστές των μαχητικών να εντοπίσουν και να καταρρίψουν τα συμμαχικά βομβαρδιστικά.

Μέχρι πρόσφατα, τα μαθηματικά μοντέλα που υπολογίζουν τα κέρδη που προκύπτουν από τις δυνατότητες των μεγάλων πολεμικών «δικτυοκεντρικών» συστημάτων δεν έχουν μελετηθεί προσεκτικά. Πολλοί μελετητές του NCW απλά δανείστηκαν το καθιερωμένο νόμο Metcalfe που ισχύει στον πολιτικό εμπόριο και τον υιοθέτησαν και στα στρατιωτικά συστήματα. Ο νόμος Metcalfe αναφέρει ότι η «χρησιμότητα» ενός δικτύου αυξάνεται με το τετράγωνο του αριθμού των κόμβων του δικτύου - δέκα κόμβοι (πλατφόρμες) επιτρέπουν εκατό πιθανές συνδέσεις, εκατό κόμβοι επιτρέπουν δέκα χιλιάδες. Ο νόμος Metcalfe παρουσιάζει πιθανόν, ένα καλύτερο σενάριο για τη διανομή των πληροφοριών που συλλέγονται από αισθητήρες σε ένα στρατιωτικό σύστημα.

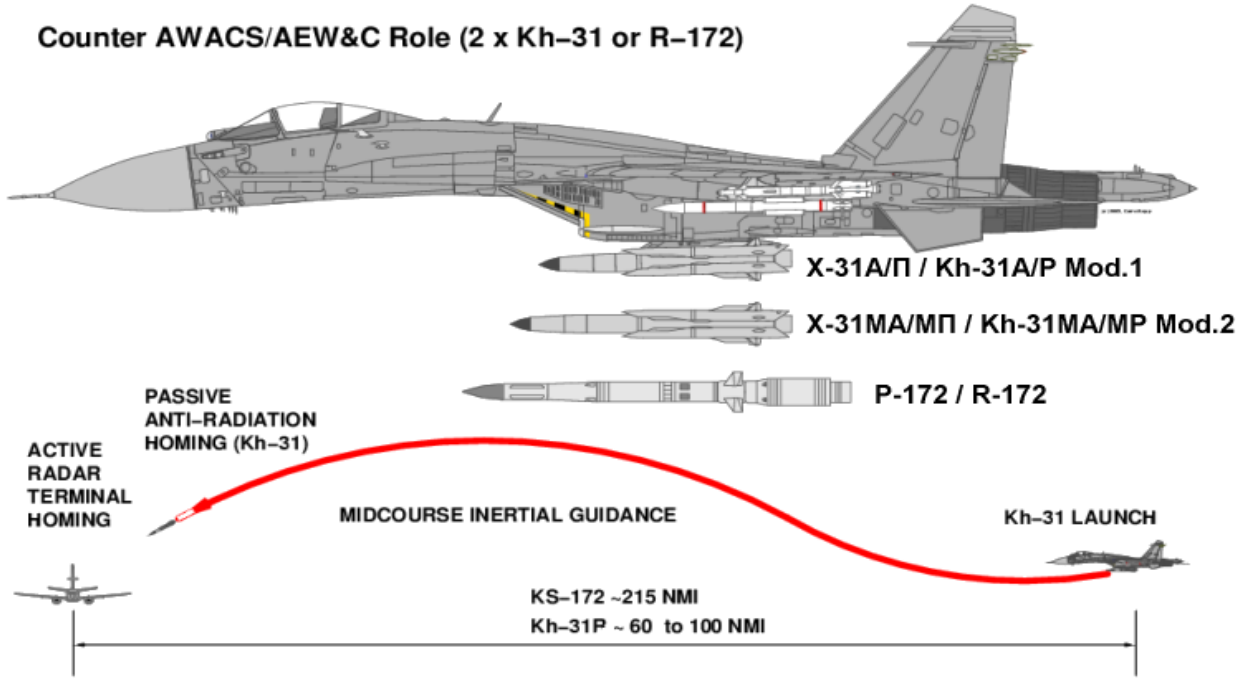
Στη φάση της απόφασης ο διοικητής αξιοποιεί τις γνώσεις που έχουν αποκτηθεί από τις προηγούμενες φάσεις «Παρατήρηση- Προσανατολισμό». Στη φάση της Δράσης ο διοικητής θα πρέπει να αναπτύξει τα στρατιωτικά του μέσα και να πραγματοποιήσει την εμπλοκή.

Η δικτύωση μπορεί να επιταχύνει τον επιχειρησιακό ρυθμό μέσω της επιτάχυνσης των φάσεων Παρατήρηση - Προσανατολισμός του OODA. Τα όρια για την ικανότητα του «συστήματος των συστημάτων (system of systems)» επιβάλλονται από τις φάσεις της απόφασης και ιδιαίτερα της δράσης των βρόγχων. Κατά συνέπεια παρατηρούμε ότι η δικτύωση συμβάλει καθοριστικά στην εξισορρόπηση της ισχύος του αντιπάλου κατά τη διάρκεια των επιχειρήσεων. Αξιοσημείωτη είναι η επίδραση στη ζήτηση συγκεκριμένω Βτύπων εξοπλισμών για την υποστήριξη του δικτυοκεντρικών επιχειρήσεων. [50]Η

[50] Kopp Carlo, NCW101 : an introduction to network centric warfare, 1st Edition, Air Power Australia, 2008

«Δικτύωση» έχει επιφέρει και άλλα χρήσιμα οφέλη. Μία είναι η διευκρίνιση μάχης, όπου το σύστημα JTIDS Link-16 έχει χρησιμοποιηθεί πολύ αποτελεσματικά ως ένα πιο ικανό υποκατάστατο των συμβατικών συστημάτων διευκρίνησης, ικανό να υποστηρίξει τα επίγεια, εναέρια και θαλάσσια συστήματα.

Ένα βασικό ζήτημα στις δικτυοκεντρικές επιχειρήσεις είναι η ικανότητα για Πληροφορίες-Επιτήρηση-Αναγνώριση (Intelligence-Surveillance- Reconnaissance).



Εικόνα 11: Αναπαράσταση λειτουργίας Ρωσικού συστήματος αντιμετώπισης ιπτάμενων radar. Στην εικόνα διαφαίνεται ένα Su-27 Flanker να εκτοξεύει έναν A/A πύραυλο τύπου Kh-31 Krypton γνωστό και ως AWACS killer.

Η διάχυση των εμπορικών συστημάτων πληροφορικής και δικτύωσης σε παγκόσμιο επίπεδο έχει συμβάλει στην αυξανόμενη εστίαση σε αυτόν το τομέα από διάφορους στρατούς. Η Ρωσία έχει επικεντρωθεί σε αυτό τον τομέα υιοθετώντας μια πολιτική μάρκετινγκ για αγορά πλατφόρμων ISR όπως τα A-50 AWACS και ψηφιακά προϊόντα datalinking. Οι Ρώσοι ενδιαφέρονταν πάντα για την αγορά ψηφιακών δικτύων αεράμυνας και αντι-ISR συστημάτων. Το τελευταίο περιλαμβάνει ένα μεγάλο φάσμα AAMs, όπως ο

R-172, R-37 ο Kh-31[51] (εικόνα 11) και παραλλαγές τους, καθώς και μια πληθώρα και από εναέριους και επίγειους κινητούς εξοπλισμούς ηλεκτρονικών παρεμβολών υψηλής ισχύος[52]. Τέλος περιλαμβάνει και μεγάλης εμβέλειας πυραύλους εδάφους-αέρος όπως το σύστημα S-400.

§2.6 Η τεχνολογική Προοπτική

Η προϋπόθεση για την εφαρμογή του NCW είναι η «ψηφιοποίηση» της μάχης σε πλατφόρμες. Ένα μαχητικό αεροσκάφος που διαθέτει ψηφιακά οπλικά συστήματα μπορεί επιτυχώς να ενσωματωθεί σε ένα περιβάλλον NCW παρέχοντας τη δυνατότητα ψηφιακής διασύνδεσης με άλλες πλατφόρμες. Χωρίς την ύπαρξη ενός ψηφιακού οπλικού συστήματος και των υπολογιστών που επιτυγχάνουν τη δικτύωση με άλλες πλατφόρμες ο NCW δεν μπορεί να εφαρμοστεί.

Η ύπαρξη ψηφιακής ασύρματης συνδεσιμότητας και η τυποποίηση της, μεταξύ πλατφόρμων μάχης, είναι πολύ σημαντική[53]. Τα πολιτικά συστήματα δικτύωσης των υπολογιστών βασίζονται σε μεγάλο βαθμό στην χρήση ενσύρματων μέσων (όπως καλώδια που είναι κατασκευασμένα από χαλκό ή οπτικές ίνες), ενώ η συνδεσιμότητα με ασύρματα μέσα χρησιμοποιείται συμπληρωματικά. Στο στρατιωτικό περιβάλλον όπου χρησιμοποιούνται κινούμενες πλατφόρμες η ασύρματη συνδεσιμότητα είναι απαραίτητη για τη συλλογή και διανομή των πληροφοριών μεταξύ των συστημάτων.

[51] Πύραυλοι anti-radar

[52] Υπάρχουν, για παράδειγμα, πληροφορίες ότι στη Συρία από το 2015 έχουν τοποθετηθεί συστήματα Krasukha-2 EW από την Ρωσική Αεροπορία, συστήματα με δυνατότητες παρεμβολής συστημάτων ραντάρ καθώς και συστημάτων επικοινωνιών.

[53] Στο πλαίσιο του NATO υπάρχουν τα STANAG (Standardization Agreement). Πρόκειται για συμφωνίες τυποποίησης στις διαδικασίες, στους όρους και στις συνθήκες όσο αφορά τους νατοϊκούς στρατούς , κυρίως σε θέματα λογιστικής. Έτσι ένα σύστημα που χρησιμοποιείται από μία χώρα-μέλος, μπορεί να συνδεθεί στο δίκτυο μίας άλλης χώρας-μέλους καθώς αυτά έχουν τυποποιηθεί σε βαθμό ομοιότητας.

Τα προβλήματα που εμφανίζονται στη στρατιωτική δικτύωση μπορεί να συνοψιστούν στα παρακάτω:

α. Ασφάλεια της μετάδοσης (Security of transmission). Οι στρατιωτικές δυνάμεις προσπαθούν να εκμεταλλευτούν με το καλύτερο δυνατό τρόπο τις ψηφιακές συνδέσεις. Οι ψηφιακές συνδέσεις και ιδιαίτερα αυτές που είναι ασύρματες απαιτούν υψηλή κρυπτογράφηση ώστε να μη μπορούν να υποκλαπούν. Ακόμα και αν ένα σήμα δεν μπορεί να αποκρυπτογραφηθεί με επιτυχία, η ανίχνευση του παρέχει στον αντίπαλο πολύτιμες πληροφορίες σχετικά με την παρουσία, τη θέση ή ακόμη και τη δραστηριότητα της πλατφόρμας ή μονάδας.

β. Ευρωστία της μετάδοσης (Robustness of transmission). Πολλές φορές η μετάδοση επηρεάζεται από τις εκάστοτε συνθήκες. Οι ηλιακές εκλάμψεις, οι κακές καιρικές συνθήκες και οι εχθρικές παρεμβολές, μπορούν να επηρεάσουν τη λειτουργία των δικτύων. Εάν ένα σήμα δεν έχει ικανή ισχύ λόγω καταιγίδας ή υπέστη εχθρική παρεμβολή , διακόπτεται η σύνδεση καθώς και τερματίζεται το μοντέλο NCW.

γ. Δυνατότητα όγκου μεταφοράς (Transmission capacity). Η ταχύτητα διάδοσης των δεδομένων είναι ζωτικής σημασίας, ειδικά όταν πρέπει να αποσταλούν ψηφιοποιημένες εικόνες. Εάν πρέπει να αποσταλεί μια εικόνα μεγέθους 10mb ένα κανάλι που θα έχει την ικανότητα να μεταδίδει σε συχνότητα 9600 bit/sec θα ήταν άχρηστο. Πολλοί υποστηρίζουν ότι η συμπίεση των δεδομένων λύνει αυτό το πρόβλημα όμως η πραγματική θεωρία επικοινωνίας του Shannon[54] απορρίπτει αυτή τη θεώρηση.

δ. Μήνυμα και δρομολόγηση σήματος (Message and signal routing). Οι πλατφόρμες και τα διάφορα οπλικά συστήματα να μπορούν να επικοινωνούν μεταξύ τους

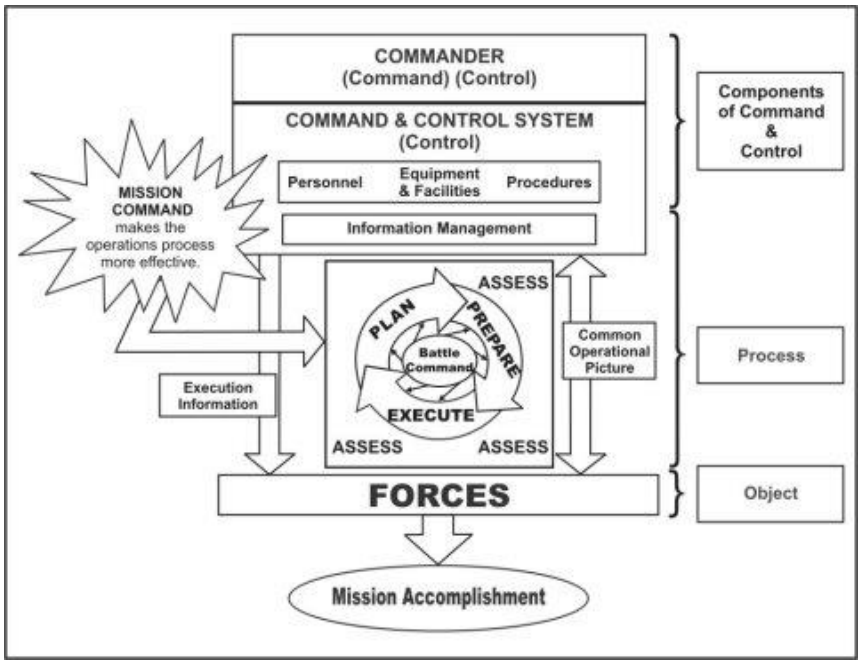
[54] Το μοντέλο επικοινωνίας των Shannon και Weaver είναι ένα ξεκάθαρο παράδειγμα γραμμικής εφαρμογής της επικοινωνίας, ως μεταφοράς μηνυμάτων. Αναπτύχθηκε κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου στα εργαστήρια της Bell Telephone και κύριος στόχος τους ήταν να βρουν ποια κανάλια επικοινωνίας μπορούσαν να χρησιμοποιηθούν πιο αποτελεσματικά. Στο μοντέλο αυτό η πηγή είναι που αποφασίζει ποιο μήνυμα θα σταλεί. Το επιλεγμένο μήνυμα μετατρέπεται από έναν μετασχηματιστή σε σήμα το οποίο στη συνέχεια αποστέλλεται μέσω του καναλιού στον αποδέκτη..

σε ένα δικτυοκεντρικό περιβάλλον. Ακριβώς όπως ένα email σε ένα πολιτικό δίκτυο πρέπει να έχει μια διεύθυνση, έτσι και ένα στρατιωτικό σύστημα ανταλλαγής μηνυμάτων

ε. Μορφή σήματος και συμβατότητα πρωτοκόλλου επικοινωνίας (Signal format and communications protocol compatibility). Είναι απαραίτητο οι πλατφόρμες και τα συστήματα να μπορούν να επικοινωνούν μεταξύ τους σε ένα περιβάλλον NCW. Αυτό το πρόβλημα δεν αφορά μόνο στη χρήση διαφορετικής διαμόρφωσης στα σήματα αλλά και στα ψηφιακά πρωτόκολλα, αλλά και στη χρήση μη συμβατών διαμορφώσεων οι οποίες φαινομενικά έχουν το ίδιο πρωτόκολλο διαμόρφωση σήματος ή επικοινωνίας. Αυτή η ασυμβατότητα στις διαμορφώσεις προκαλεί πολλά προβλήματα στην εμπορική τεχνολογία των υπολογιστών και ακόμη μεγαλύτερα προβλήματα στους υπολογιστικά συστήματα που χρησιμοποιούνται από τον στρατό.

Την παρούσα στιγμή σχεδόν όλα τα στρατιωτικά συστήματα ζεύξης δεδομένων που χρησιμοποιούνται στον NCW λειτουργούν σε ταχύτητες που θα μπορούσαν να θεωρηθούν μικρές στο πολιτικό / εμπορικό κόσμο των υπολογιστών, γεγονός που αντανακλά την πραγματική κατάσταση που επικρατεί στις ασύρματες επικοινωνίες. Επιπλέον, στην στρατιωτική τεχνολογία παρατηρείται ασυμβατότητα όσον αφορά τις διαμορφώσεις των σημάτων, των συχνοτήτων, και των πρωτοκόλλων των ψηφιακών επικοινωνιών. Για να αντιμετωπιστεί το παραπάνω πρόβλημα οι δυτικές ένοπλες δυνάμεις και κυρίως οι ΗΠΑ και οι χώρες του ΝΑΤΟ αναπτύσσουν σήμερα συστήματα που χρησιμοποιούν ένα ευρύ φάσμα κωδικοποιημένων σημάτων και πρωτοκόλλων. Για παράδειγμα, σε μια συνομιλία το στόμα είναι ο μετασχηματιστής, το σήμα είναι τα ηχητικά κύματα που περνούν μέσα από το κανάλι του αέρα και το αυτί είναι ο αποδέκτης

§3. Εισαγωγή στη θεωρία Διοίκησης και Ελέγχου



Εικόνα 12: Γραφική αναπαράσταση της λογικής της Διοίκησης και Ελέγχου.

Για την ανάλυση των δικτύων και πρωτοκόλλων που αναφέρθηκαν προηγουμένως είναι απαραίτητη η ανάλυση της φιλοσοφίας στην οποία στηρίχτηκαν, η διοίκηση και έλεγχος (command and control). Τα συστήματα C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance & Reconnaissance) αποτελούν απαραίτητο στοιχείο των συγχρόνων στρατών προκειμένου να είναι δυνατή η λειτουργία τους στο σύγχρονο επιχειρησιακό περιβάλλον και η άμεση αντίδρασή τους στις σύγχρονες απειλές και απαιτήσεις. Η εξέλιξη των συστημάτων C4ISR αποτελεί μια συνεχή διαδικασία η οποία έχει επιφέρει σημαντικές αλλαγές κατά τις δύο τελευταίες δεκαετίες. Η **Διοίκηση** και ο **Έλεγχος** (C2) αποτελούσαν ανέκαθεν τις διαδικασίες ηγεσίας, οι οποίες σταδιακά απέκτησαν υψηλού επιπέδου **Επικοινωνίες** (C3). Στα μέσα της δεκαετίας του 1980 στις τρεις παραπάνω λειτουργίες προστέθηκε ο τομέας των Πληροφοριών (C3I). Η ανάπτυξη των Υπολογιστών εισήγαγε νέα δεδομένα και δυνατότητες στην ενάσκηση της διοίκησης και ελέγχου (C4I). Τελευταία, άρχισαν να

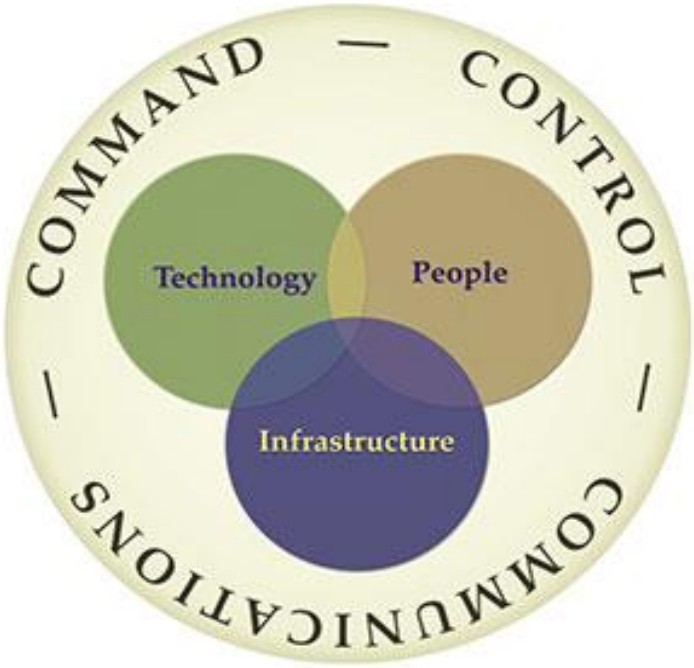
ενσωματώνονται η **Επιτήρηση** και η **Αναγνώριση** (C4ISR). Οι δύο τελευταίες λειτουργίες υλοποιούνται κυρίως με επίγεια ραντάρ, μη επανδρωμένα εναέρια οχήματα, γνωστά ως UAV, αερομεταφερόμενα συστήματα επιτήρησης εδάφους (airborne ground surveillance – AGS) και δορυφόρους παρατήρησης-αναγνώρισης.

§3.1 Διοίκηση και Έλεγχος- Command And Control (C2)

Το σύστημα διοίκησης και ελέγχου παρέχει τη δυνατότητα άσκησης εξουσίας και παροχής κατευθύνσεων, από έναν διοικητή προς τις δυνάμεις του σε δεδομένο χρόνο και χώρο. Το επίκεντρο του της διοίκησης και ελέγχου είναι ο διοικητής (εικόνα 12). Οι διοικητές είναι υπεύθυνοι να κάνουν εκτίμηση κατάστασης, να λαμβάνουν αποφάσεις και να ελέγχουν την εκτέλεση τους.

Ο σκοπός της διοίκησης και ελέγχου είναι η επιτυχής ολοκλήρωση μιας αποστολής. Το βασικό κριτήριο της επιτυχίας του C2 είναι ο τρόπος με τον οποίο συμβάλλει στην εκπλήρωση αυτού του στόχου. Αυτό μπορεί να περιλαμβάνει την κατάλληλη τοποθέτηση δυνάμεων και την αποτελεσματική εκμετάλλευση πόρων για μελλοντικές επιχειρήσεις. Οι διοικητές οφείλουν να οργανώνουν τους πόρους για την άσκηση διοίκησης και ελέγχου. Μέσω της διοίκησης και ελέγχου ο διοικητής, διαχειρίζεται πληροφορίες για την παραγωγή και διάδοση μιας κοινής επιχειρησιακής εικόνας για τον κυβερνήτη, το προσωπικό και δευτερεύουσες δυνάμεις. Το σύστημα διοίκησης και ελέγχου βοηθά τον διοικητή στην κατεύθυνση των δυνάμεων, μέσω της διαβίβασης των πληροφοριών εκτέλεσης. Η διοίκηση και ο έλεγχος, διακρίνεται από τα εξής χαρακτηριστικά:

- Ικανότητα αναγνώρισης και αντίδρασης σε πιθανή αλλαγή τακτικής κατάστασης.
- Δυνατότητα παροχής μια συνεχούς, αμφίδρομης διαδικασίας αμοιβαίας επιρροής μεταξύ του διοικητή , του προσωπικού, και των διαθέσιμων δυνάμεων.
- Ικανότητα μείωσης του «χάους και της αβεβαιότητας» στο πεδίο της μάχης.



Εικόνα 13: Η λογική της Διοίκησης και Ελέγχου και Επικοινωνιών προϋποθέτουν την ισοροπημένη εκμετάλλευση της τεχνολογίας, του ανθρώπινου

Ωστόσο, ακόμη και οι διοικητές που ασκούν την πιο αποτελεσματική διοίκηση και έλεγχο, δεν μπορούν να εξαλείψουν την αβεβαιότητα και να δημιουργήσουν με ακρίβεια μια μηχανιστική, προβλέψιμη σειρά.

Συνοψίζοντας, ένα σύστημα διοίκησης & ελέγχου, είναι η ρύθμιση του προσωπικού, η διαχείριση πληροφοριών, διαδικασιών, εξοπλισμού και εγκαταστάσεων απαραίτητων για την διεξαγωγή επιχειρήσεων από τον διοικητή[55].

§3.2 Επικοινωνίες, Διοίκηση και Έλεγχος-Communications, Command And Control (C3)

Η C3 τεχνολογία, περιλαμβάνει την δυνατότητα απόκτησης και διάδοσης πληροφοριών σε όλες τις εμπλεκόμενες φίλιες δυνάμεις (εικόνα 13). Η ικανότητα πρέπει

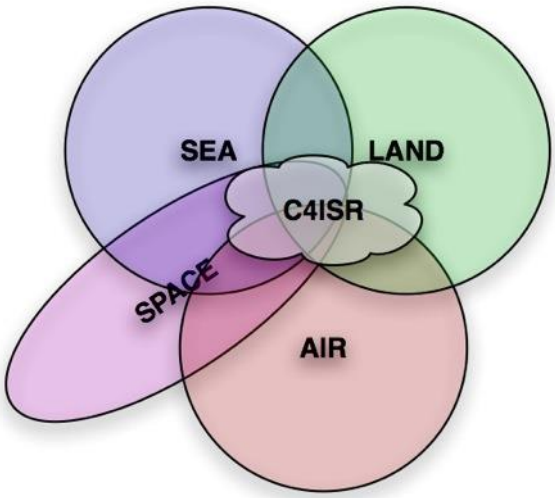
[55] David S. Alberts, Richard E. Hayes , «UNDERSTANDING COMMAND AND CONTROL», 2014

να είναι αξιόπιστη και να παρέχει ασφαλή πολυεπίπεδη πρόσβαση προστατευμένη από τις επιθέσεις του εχθρού. Αυτό απαιτεί εξέλιξη όχι μόνο σε λογισμικό υπολογιστών αλλά και στη διασύνδεση του ιστού των επικοινωνιών. Ο σκοπός είναι η απρόσκοπτη και αποτελεσματική ενσωμάτωση των ικανοτήτων για το σχεδιασμό, την ολοκληρωμένη διαχείριση δύναμης και την αποτελεσματική χρησιμοποίηση των συστημάτων πληροφοριών και σκόπευσης

Αυτή η τεχνολογία, είναι το κλειδί για τη διαχείριση της μάχης και την αξιοποίηση της πληροφοριακής ανωτερότητας ως έναυσμα όλων των αποστολών υποστήριξης και ελιγμού. Η αποτελεσματική C3 διαβεβαιώνει την επίγνωση της τακτικής κατάστασης και παρέχει την δυνατότητα να ελέγχονται οι επίγειες και αεροδιαστημικές – πυραυλικές δυνάμεις σε όλα τα επίπεδα διοίκησης. Επικεντρώνεται στο να παρέχει τις σωστές πληροφορίες στους σωστούς χρήστες την κατάλληλη στιγμή. Η τεχνολογία C3 υποστηρίζει την άσκηση διοίκησης και ελέγχου (C2) που προαναφέρθηκε και περιλαμβάνει επεξεργασία, ανάλυση, χρήση και διάδοση πληροφοριών για την κυριαρχία στη μάχη. Με την τεχνολογία C3 μέσω δορυφορικών επικοινωνιών και άλλων συνδέσεων, παρέχονται στις στρατιωτικές δυνάμεις δεδομένα σε πραγματικό χρόνο (real-time data). Αυτά τα συστήματα, παρέχουν πληροφορίες ζωτικής σημασίας σε όλο το φάσμα των επιτυχημένων στρατιωτικών επιχειρήσεων. Για παράδειγμα, το δίκτυο SATCOM (Satellite Communications) παρέχει σχεδόν σε παγκόσμια κάλυψη πρόσβαση σε πληροφορίες που σχετίζονται με οποιαδήποτε αποστολή και μας επιτρέπει να λαμβάνουμε αποφάσεις (σε σχεδόν πραγματικό χρόνο) ζωτικής σημασίας για την επιτυχή έκβαση των αποστολών[56].

[56] Communications, Command, and Control (C3). Available from: http://www.globalsecurity.org/military/systems/ground/c3.htm

§3.3 Διοίκηση και Έλεγχος, Επικοινωνίες, Υπολογιστές και Πληροφορία- Command,Control,Communications, Computers & Intelligence(C4I & C4ISR)



Εικόνα 14: Το C4ISR ενοποιεί τις τέσσερεις διαστάσεις των επιχειρήσεων, το έδαφος, τη θάλασσα, τον αέρα και το διάστημα.

Η διοίκηση και ο έλεγχος, αφορά την λήψη αποφάσεων ενός διοικητή για την επιτυχή έκβαση μιας αποστολής η οποία υποστηρίζεται από πληροφοριακή τεχνολογία (μέσω υπολογιστών και επικοινωνιών, μέρος του C4I). Οι ΗΠΑ, αξιοποιούν ενεργά τέτοιες τεχνολογίες προκειμένου να επιτύχουν πληροφοριακή υπεροχή με σκοπό να καταφέρουν να λαμβάνουν καλύτερες και πιο γρήγορες αποφάσεις.

Μια σημαντική δυνατότητα που παρέχουν τα συστήματα C4I στους διοικητές, εκτός από την επίγνωση της κατάστασης στο πεδίο της μάχης, είναι και οι πληροφορίες για την τοποθεσία και την κατάσταση τόσο του εχθρού όσο και των φίλιων. Κάτι το οποίο είναι απαραίτητο για την διατήρηση της πρωτοβουλίας κατά τη διάρκεια των επιχειρήσεων. Οι διοικητές, οφείλουν να λαμβάνουν σχετική γνώση και να την συνδυάζουν με την κρίση τους, συμπεριλαμβανομένων των πτυχών της ανθρώπινης συμπεριφοράς, (ασχέτως αν είναι δύσκολο να ποσοτικοποιηθούν για παράδειγμα

κόπωση, άγχος, εμπειρία), την αβεβαιότητα των δεδομένων και της πιθανές μελλοντικές ενέργειες του εχθρού.

Επιπλέον, η αυξανόμενη αλληλεπίδραση και αλληλεξάρτηση των C3 και ISR μέσω της αυξανόμενης εξάρτησης από υπολογιστές έχουν αναγνωριστεί ως λειτουργική συνέχεια διοίκησης, ελέγχου, επικοινωνιών, Η/Π, νοημοσύνης, επιτήρησης και αναγνώρισης ή C4ISR (εικόνα 14). Στο στρατιωτικό τομέα, το C4ISR συνδυάζει όλα τα συστήματα που επιτρέπουν στους στρατιωτικούς διοικητές να κατανοήσουν το περιβάλλον επιχειρήσεων τους, τον εντοπισμό κρίσιμων παραγόντων για διεξαγωγή αποστολών, και τον έλεγχο των μέσων.

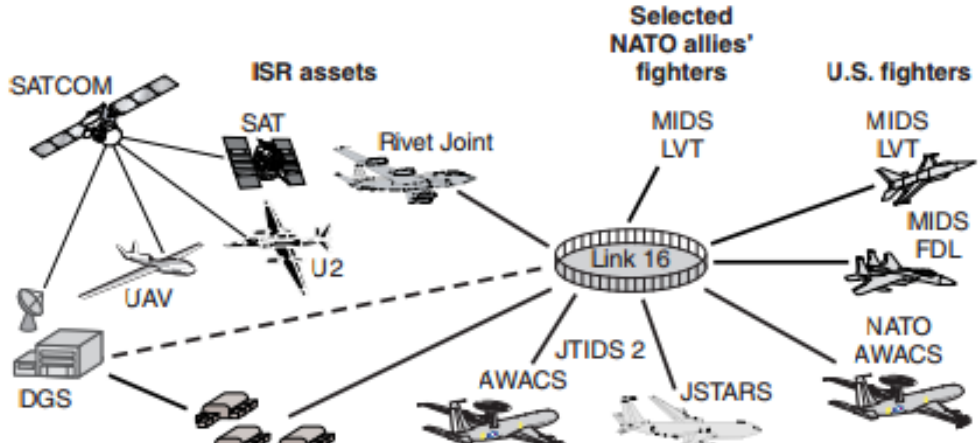
Μελλοντικά, τεχνολογικά προγράμματα είναι έτοιμα να αποδώσουν δυνατότητες της επόμενης γενιάς, τα οποία βασίζονται στην ανάπτυξη των ήδη υπαρχόντων συστημάτων.

§4 Τακτικά Δίκτυα- Tactical Data Links(TDLs)

Πλέον στο σύγχρονο επιχειρησιακό περιβάλλον είναι απαραίτητη η έγκαιρη και έγκυρη δημιουργία μιας κοινής επιχειρησιακής εικόνας (COP[57] / Common Operational Picture) καθώς και η ασφαλής και ταχεία διαβίβαση της εικόνας αυτής προς τα άνω και πλάγια. Τα TDLs συμβάλουν καθοριστικά στη σύνθεση της «διευκρινισμένης εικόνας Αέρος – Επιφανείας» (RASP[58] / Recognized Air Surface Picture, βλέπε εικόνα 15).

[57] COP: είναι η ενιαία εικόνα των επιχειρησιακών πληροφοριών (πχ. Γεωγραφική θέση των στρατευμάτων μας, θέση και κατάσταση διαφόρων υποδομών όπως γέφυρες και εργοστάσια) η οποία διαμοιράζεται μεταξύ των διαφόρων κέντρων ελέγχου των επιχειρήσεων. Η COP διευκολύνει τον σχεδιασμό των επιχειρήσεων και τη συνεργασία μεταξύ των μονάδων καθώς επίσης συμβάλει καθοριστικά στην επίγνωση της τακτικής κατάστασης (situational awareness). www.kforcegov.com/Solutions/DataKM/COP_Solution

[58] RASP: Θεωρητικά είναι μια λίστα η οποία περιέχει όλα τα αεροσκάφη που εκτελούν πτήση εντός ενός συγκεκριμένου εναέριου χώρου. Αυτή η λίστα παρέχει διάφορα δεδομένα όπως αν τα αεροσκάφη είναι φίλια ή εχθρικά και περιλαμβάνει λεπτομέρειες σχετικά με τον τύπο του αεροσκάφους, τον αριθμό της πτήσης ή ακόμη και το σχέδιο πτήσης. Οι παραπάνω



Εικόνα 25: Το τακτικό δίκτυο Link-16 έχοντας τερματικούς σταθμούς σε αεροσκάφη, κέντρα αποφάσεων και αισθητήρες καθιστά εφικτή την σύνθεση της «ζωντανής» επιχειρησιακής εικόνας.

§4.1 Σκοπός και Βασικές Αρχές Τακτικών Δικτύων

Σκοπός όλων των τακτικών δικτύων είναι να εξασφαλίσουν πρόσβαση στη κατάλληλη πληροφορία, την κατάλληλη στιγμή, παρέχοντας τη δυνατότητα στις στρατιωτικές δυνάμεις να διαθέσουν την απαιτούμενη προσπάθεια στο κατάλληλο γεωγραφικό σημείο, για να επιτύχουν τον αντικειμενικό τους σκοπό. Μερικά από τα οφέλη χρήσης των τακτικών δικτύων είναι η άμεση προειδοποίηση, η άμεση εκτέλεση διαταγών σε συνδυασμένες επιχειρήσεις και η τυποποιημένη απόδοση και παρουσίαση των εμπλεκόμενων δυνάμεων.

Η χρήση τυποποιημένων TDLs παρέχει τη δυνατότητα ανάλυσης των δεδομένων και εξαλείφει επιχειρησιακά προβλήματα επικοινωνίας, εξασφαλίζοντας παράλληλα

πληροφορίες μπορούν να αντληθούν από τα στρατιωτικά ραντάρ, από τους ελεγκτές αεράμυνας των αεροδρομίων ή ακόμη και από συμμαχικά κράτη η στρατιωτικούς οργανισμούς όπως το NATO. www.fas.org

διαλειτουργικότητα μεταξύ των στρατιωτικών δυνάμεων. Τα βασικά στοιχεία υλοποίησης μιας εφαρμογής TDL είναι τα εξής:[59]

α. Ο κεντρικός επεξεργαστής δεδομένων (Data Link Interface Processor/ DLIP)

β. Το hardware/τερματικό διασύνδεσης(Data Link Interface/ Terminal /DTS /MIDS)

γ. Η Μονάδα κωδικοποίησης πληροφοριών (Encryption Unit) όπως για παράδειγμα το KG-40, KG84, KV-7, MIDS

δ. Το DLM (Data Link Management/ Διαχειριστής τακτικού δικτύου), εργαλείο για τη διαχείριση και απεικόνιση των πληροφοριών μέσω του δικτύου

ε. Το μέσο/σύστημα μετάδοσης (π.χ. HF-UHF-SATCOM).

§4.2 Γενικοί κανόνες εφαρμογής των Τακτικών Δικτύων

«Η υλοποίηση των TDL στηρίζεται στους εξής πέντε βασικούς κανόνες εφαρμογής:[60]

- Τα TDLs είναι συστήματα επικοινωνιών που χρησιμοποιούν τυποποιημένη μορφή μηνυμάτων και επιτρέπουν την ηλεκτρονική μετάδοση δεδομένων.
- Το μέγεθος των μηνυμάτων και του εύρους ζώνης μετάδοσης εν χρήση, είναι πολύ σημαντικά.
- Ο δίαυλος επικοινωνίας ποικίλει ανάλογα με την απόσταση και το μέγεθος των δεδομένων.

[59] Northtropp Grumman, «Understanding Voice and Data Link Communication», December 2014 , σελ. 23

[60] ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΤΑΚΤΙΚΩΝ ΔΙΚΥΩΝ - TACTICAL DATA LINKS (TDLs), Ιούλιος 2015, Available from: www.iknowgr.blogspot.de.

- Πολύ συχνά υπάρχουν πολύ περισσότερα δεδομένα προς μετάδοση, από αυτά που είναι δυνατόν να μεταδοθούν έγκαιρα.
- Η ευθύνη του Διαχειριστή Δικτύων [DATA LINK MANAGER (DLM)] είναι να τοποθετεί κατά σειρά προτεραιότητας τις πληροφορίες προς μετάδοση.»

Με τον όρο DATA LINK MANAGEMENT, χαρακτηρίζονται οι διαδικασίες εκείνες που εφαρμόζονται για την σύνθεση μιας αναγνωρισμένης επιχειρησιακής εικόνας, χρησιμοποιώντας τις δυνατότητες και γνωρίζοντας τους περιορισμούς των δικτύων DATA LINK που χρησιμοποιούνται.

§4.3 Πλεονεκτήματα Χρήσης των Τακτικών Δικτύων

Τα πλεονεκτήματα που απορρέουν από τη χρήση των τακτικών δικτύων βελτιώνουν την ταχύτητα, ευελιξία και αποτελεσματικότητα των επιχειρήσεων:[61] [62]

α. Κάθε μέλος της ομάδας που επιχειρεί τη ζεύξη γνωρίζει την πραγματική μαχητική ισχύ κάθε άλλου μέλους της ομάδας, πληροφορία που προσφέρεται για σωστή σχεδίαση της αποστολής σε κάθε περίοδο της επιχείρησης.

β. Υπάρχει συνεχής επίγνωση της διάταξης μάχης του συνόλου των φίλιων δυνάμεων, σε οποιαδήποτε κατάσταση ηλεκτρομαγνητικών παρεμβολών.

γ. Υπάρχει διαβίβαση ολοκληρωμένης τακτικής εικόνας σε όλους τους συμμετέχοντες στα Δίκτυα TDL με δυνατότητα «ενημέρωσης» σε σχεδόν πραγματικό χρόνο.

δ. Υπάρχει διατήρηση της συνοχής ενός σχηματισμού και δυνατότητα συνεχούς τροποποίησης της στρατηγικής του.

ε. Υπάρχει περιορισμός των εκπομπών από τον ασύρματο, με αποτέλεσμα να γίνεται ευκολότερος ο έλεγχος της εναέριας κυκλοφορίας και κυρίως να αυξάνεται η

[61] ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΤΑΚΤΙΚΩΝ ΔΙΚΥΩΝ - TACTICAL DATA LINKS (TDLs) , Ιούλιος 2016, Available from: www.iknowgr.blogspot.de

[62] «Understanding Voice and Data Link Communication», Northtropp Grumman, December 2014, σελ.23

αντίσταση των φίλιων συστημάτων στις παρεμβολές και υποκλοπές του εχθρού, χωρίς να υπάρξει παράλληλη υποβάθμιση των πληροφοριών που διανέμονται μεταξύ αυτών.

στ. Υπάρχει μεταφορά της εικόνας του ραντάρ από το ένα σύστημα στο άλλο. Από αυτή τη δυνατότητα απορρέουν τα δύο παρακάτω ειδικότερα πλεονεκτήματα :

ζ. Επίγνωση ολόκληρου του θεάτρου επιχειρήσεων ή εναλλακτικά της περιοχής στην οποία το σύστημα εμπλέκεται άμεσα .

η.Δύναται, μόνο ένα σύστημα του σχηματισμού να έχει ανοιχτό το ραντάρ του και τα υπόλοιπα να λαμβάνουν την εικόνα του ραντάρ και στοιχεία που αφορούν στους στόχους από το σύστημα αυτό.

§4.4 Κατηγορίες των Τακτικών Δικτύων

Γενικά, τα TDL διακρίνονται σε κατηγορίες ανάλογα με το είδος της σύνδεσης, την διαμόρφωση λειτουργίας και το είδος των κεραιών που χρησιμοποιούνται. Έτσι λοιπόν διακρίνονται σε:[63]

α. Από σημείο σε σημείο (POINT-TO-POINT) : Στη σύνδεση από σημείο σε σημείο οι συμμετέχοντες συνδέονται απευθείας μεταξύ τους, ενώ οι μονάδες κατά τεκμήριο είναι σταθερές σε κάποιο σημείο. Εφαρμογή μιας POINT-TO-POINT σύνδεσης αποτελεί το Link 1.

β. Εκπομπής (BROADCAST) : Μόνο μια μονάδα κάθε φορά έχει τη δυνατότητα εκπομπής των δεδομένων της προς όλα τα μέλη που συμμετέχουν στο τηλεπικοινωνιακό δίκτυο.

γ. Δικτυωμένες (NETTED) : Οι μονάδες μπορούν να ανταλλάσσουν δεδομένα μεταξύ τους στα πλαίσια ενός ευέλικτου δικτύου. Εφαρμογή ενός NETTED TDL αποτελεί το Link 16.

[63] «Understanding Voice and Data Link Communication», Northtropp Grumman, December 2014

§4.5 Είδη των Τακτικών Δικτύων

Τα είδη των τακτικών δικτύων είναι τα εξης:

α. Link-1 είναι ένα σύστημα αμφίδρομης ζεύξης δεδομένων που σχεδιάστηκε στα τέλη της δεκαετίας του 1950 και χρησιμοποιήθηκε στα συστήματα αεράμυνας (NADGE)[64] του NATO. Το Link-1 και χρησιμοποιείται για επικοινωνία εδάφους - εδάφους (Point to Point[65]), μεταξύ μονάδων ΣΑΕ (Σύστημα Αεροπορικού Ελέγχου). Η σύνδεση είναι χαμηλής ποιότητας, με ταχύτητες μετάδοσης δεδομένων 600, 1200 και 2400 Bps. Ουσιαστικά χρησιμοποιείται στην ανταλλαγή συνθετικής αεροπορικής εικόνας. Οι δυνατότητες ασφαλείας που έχει είναι χαμηλές. Επίσης η αντίσταση που παρέχει σε ηλεκτρονικά αντίμετρα ή ασφάλεια σε υποκλοπές, είναι χαμηλή. Τα χαρακτηριστικά εκπομπών - λήψεων καθώς και τα standards των μηνυμάτων του LINK-1, περιγράφονται στη STANAG 5501 , ενώ η επιχειρησιακή εκμετάλλευση του, καθορίζεται στην ADatP-31.[66]

β. TADIL A / Link-11A / Link-11B αναπτύχθηκε ως ένα σύστημα ζεύξης δεδομένων για το ναυτικό τη δεκαετία του 1960 και έχει ενσωματωθεί στο επίγειο C2 σύστημα του NATO μέσω του SSSB (Ship-Shore-Ship Buffer)[67]. Το Link-11A είναι ένα αυτόματο, υψηλής ταχύτητας HF/UHF, που υποστηρίζει την ανταλλαγή αεροπορικής

[64] NATO Air Defence Ground Environment (NADGE): είναι ένα σύστημα το οποίο αναπτύχθηκε από κοινού από τα κράτη-μέλη του NATO. Μέσω του NADGE δημιουργείται ένα δίκτυο στο οποίο συνδέονται τα συστήματα αεράμυνας αλλά και τα εθνικά radar κάθε κράτους-μέλους με σκοπό την επιτήρηση του συνόλου του εναερίου χώρου του NATO. http://www.nspa.nato.int/en/organization/Logistics/WSES/nadge

[65] Είναι η απλούστερη σύνδεση μεταξύ δύο τερματικών / υπολογιστικών σημείων και επιτυγχάνεται με απ'ευθείας σύνδεση. Στην περίπτωση αυτή μια πόρτα εισόδου-εξόδου (I/O port) ενός και μόνο τερματικού (ή υπολογιστή) είναι συνδεδεμένη είτε μόνιμα με αφιερωμένη γραμμή, είτε παροδικά μέσω του επιλεγμένου τηλεφωνικού δικτύου, με μια αντίστοιχη πόρτα εισόδου-εξόδου ενός άλλου υπολογιστή (ή τερματικού). http://fluidmesh.com/point-to-multipoint-wireless

[66] NATO Link 1 STANA 5501

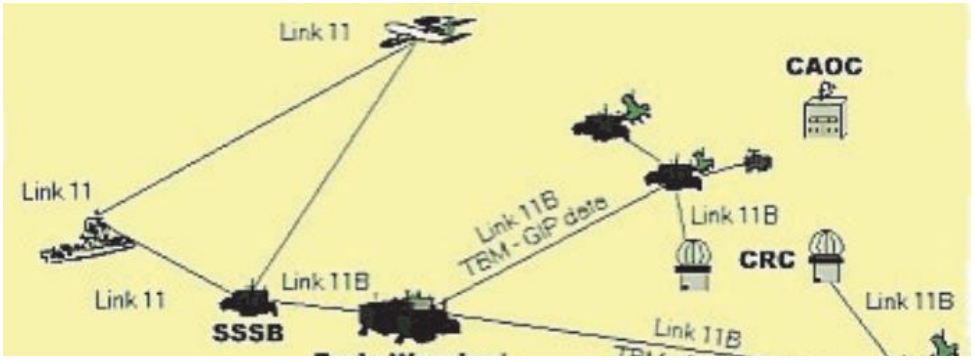
[67] Ship-Shore-Ship Buffer (SSSB) είναι ένα σύστημα ζεύξης σε πραγματικό χρόνο (real time) το οποίο υποστηρίζει την ανταλλαγή δεδομένων μεταξύ των ναυτικών δυνάμεων, συμπεριλαμβανομένων των αερομεταφερόμενων μέσων και των associated air defence ground environment units. http://www.nato.int

εικόνας, εντολών, καταστάσεως και πληροφοριών ελέγχου, μεταξύ των ναυτικών μονάδων, αλλά και με τους επίγειους σταθμούς C2. Βασίζεται σε τεχνολογία της δεκαετίας του '60 και είναι μια σχετικά αργή σύνδεση (ταχύτητες 1364 ή 2250 Bps). Το Link 11 μπορεί να χρησιμοποιηθεί και με τρόπους ραδιοφωνικής μετάδοσης (BROADCAST) στους οποίους μια ενιαία μετάδοση στοιχείων, ή μια σειρά ενιαίων μεταδόσεων, γίνεται από έναν συμμετέχοντα που ορίζεται σαν NET CONTROL STATION (NCS). Είναι ασφαλές, αλλά μη ανθεκτικό σε ηλεκτρονικά αντίμετρα.

Το LINK 11^{A} (ασύρματη έκδοση) λειτουργεί σε υψηλές συχνότητες (HF) και έχει ικανότητα μετάδοσης πέρα από τον ορίζοντα (Beyond Line Of Sight.). Επομένως δεν απαιτείται οπτική επαφή μεταξύ των χρηστών. Προσφέρει την δυνατότητα λειτουργίας στη UHF ζώνη αλλά περιορίζεται σε αποστάσεις οπτικής επαφής, LOS (περίπου 25 ναυτικά μίλια εδάφους-εδάφους ή 150 ναυτικά μίλια εδάφους-αέρος).

Το Link-11B (ενσύρματη έκδοση) είναι μια Point-To-Point εφαρμογή του Link-11 με τη διαφορά ότι ενώ το Link-11 λειτουργεί με χαρακτηριστικά ταυτόχρονης μετάδοσης σε πολλούς συμμετέχοντες (εικόνα 16) στα πλαίσιο ενός δικτύου, το Link-11B είναι ένα point-to-point σύστημα που χρησιμοποιεί τμηματική διαβίβαση των στοιχείων σε μια ταχύτητα 1.200 Bps και εφεδρική στα 600 Bps. Τα χαρακτηριστικά εκπομπών – λήψεων του Link-11 περιγράφονται στη STANAG 5511, ενώ η επιχειρησιακή εκμετάλλευση του, καθορίζεται στις ADatP-11 και ADatP-33 .[68]

[68] INK-11 Tactical Data Link, Advanced Protocols, WAVECOM ELEKTRONIK AG. Available from: http://www.wavecom.ch/content/pdf/advanced_protocol_link-11.pdf.



Εικόνα 36: Το κέντρο άμεσης προειδοποίησης Early Warning/TMD Centre συνθέτει την επιχειρησιακή εικόνα από δεδομένα που προέρχονται από διάφορα τακτικά δίκτυα και την μεταφράζει σε πληροφορίες επιχειρήσεων για το κέντρο λήψης αποφάσεων CAOC.

γ. TADIL C/Link-4 είναι ένα σύστημα ζεύξης δεδομένων που χρησιμοποιείται για την παροχή εντολών σε πραγματικό χρόνο στα αεροσκάφη της USAF αλλά και σε άλλα μαχητικά αεροσκάφη του NATO. Λειτουργεί στη ζώνη UHF στα 5.000 bps. Διαχωρίζεται σε δύο εκδόσεις, στην Link-4A και Link-4C.

Το Link-4A/ TADIL C είναι ένα από τα πολλά τακτικά δίκτυα που χρησιμοποιούνται από τις Αμερικανικές ένοπλες δυνάμεις αλλά και από τις δυνάμεις του NATO. Χρησιμοποιείται για την παροχή ψηφιακών δεδομένων επικοινωνιών εδάφους-αέρος, αέρος-εδάφους και αέρος-αέρος. Το link-4A είχε αρχικά σχεδιαστεί να αντικαταστήσει το υπάρχων σύστημα φωνητικών επικοινωνιών για τον έλεγχο των μαχητικών αεροσκαφών. Η χρήση του Link-4^{A} έκτοτε έχει επεκταθεί για να συμπεριλάβει και τις επικοινωνίες ψηφιακών δεδομένων μεταξύ επίγειων και εναέριων πλατφόρμων . Εγκαταστάθηκε για πρώτη φορά στα τέλη της δεκαετίας του 1950. Παρά τη φήμη ότι το Link-4A θεωρείται αξιόπιστο, στην πραγματικότητα δεν είναι ούτε ασφαλές σαν δίκτυο ούτε είναι ανθεκτικό σε παρεμβολές.

Τα χαρακτηριστικά εκπομπών - λήψεων καθώς και τα Standards των μηνυμάτων του LINK-4C, περιγράφονται στη STANAG 5504 , ενώ η επιχειρησιακή εκμετάλλευση του, καθορίζεται στην ADatP-4.[69]

δ. Link-14 είναι ένα παλαιό σύστημα ζεύξης δεδομένων το οποίο λειτουργεί σε υψηλές συχνότητες HF και χρησιμοποιείται για την μεταφορά πληροφοριών επιτήρησης (surveillance information) μεταξύ των θαλάσσιων μονάδων. Το Link-14 παρέχει τη δυνατότητα μετάδοσης εικόνων και πληροφοριών σε μονάδες που δεν έχουν την δυνατότητα να λάβουν τα δεδομένα αυτά μέσω του Link-11 είτε άμεσα είτε μέσω διεπαφής. Τα χαρακτηριστικά εκπομπών - λήψεων του LINK-14, περιγράφονται στη STANAG 5514, ενώ η επιχειρησιακή εκμετάλλευση του, καθορίζεται στην ADatP-14.[70]

ε. TADIL J / MIDS / JTIDS / Link-16. Το Link-16 είναι το πιο σύγχρονο σύστημα ψηφιακής ζεύξης δεδομένων το οποίο χρησιμοποιείται από τη χώρα μας, τις ΗΠΑ, τον ΟΗΕ (Οργανισμός Ηνωμένων Εθνών) και από τις περισσότερες χώρες της Βόρειο-Ατλαντικής συμμαχίας (NATO). Το Link 16 χρησιμοποιεί το σύστημα διανομής JTIDS (Joint Tactical Information Distribution System), το οποίο είναι το πρωτόκολλο επικοινωνιών του. Είναι ένα σύστημα που αναπτύχθηκε τη δεκαετία του 1970 με σκοπό να βελτιστοποιήσει τη χρήση της αρχιτεκτονικής MIDS/JTIDS και μπορεί πλέον να φέρει τουλάχιστον τέσσερις φορές μεγαλύτερο όγκο πληροφοριών επιτήρησης σε σχέση με τον πρόγονο του IJMS και καλύπτει τις απαιτήσεις για τη λειτουργία του C2 , τον έλεγχο αεροσκαφών, αναθέσεις αποστολών και επικοινωνίες σε περιβάλλον τακτικών επιχειρήσεων. Το Link-16 παρέχει τεχνικές και λειτουργικές βελτιώσεις στα υπάρχοντα συστήματα (Link-11,Link-14). Παρέχει σημαντικές

[69] John Pike, « Tactical Digital Information Links (TADIL)» , updated Sunday, April 23, 2000. Available from: http://fas.org/irp/program/disseminate/tadil

[70] Rolald Proersch, «Technical Handbook for Radio Monitoring HF» , Edition 2015, σελ. 315

βελτιώσεις όπως υψηλό βαθμό προστασίας έναντι παρεμβολών, αυξημένο ρυθμό μετάδοσης δεδομένων, μειωμένο μέγεθος τερματικού σταθμού δεδομένων, λόγω του μικρού μεγέθους του τερματικού σταθμού είναι δυνατή η εγκατάσταση και σε αεροσκάφη. Ο τερματικός σταθμός JTIDS είναι ένας από τους δύο σταθμούς που παρέχουν σε στρατιώτες και ναύτες τη δυνατότητα διασύνδεσης μέσω του Link-16. Τα JTIDS είναι πολύ-πλατφορμικά (multi-platform) συστήματα που χρησιμοποιούνται ευρέως για τη μετάδοση δεδομένων σχετικά με τη θέση της μονάδας. Μέσω αυτών των συστημάτων επιτυγχάνεται η παροχή οδηγιών και συμβουλών, καθώς επίσης αποστέλλονται δεδομένα που διευκολύνουν την αναγνώριση των φίλιων αλλά και εχθρικών δυνάμεων.

Το JTIDS είναι ένα διακλαδικό σύστημα για τις Αμερικανικές-Νατοϊκές και Ελληνικές ένοπλες δυνάμεις. Ο άλλος τερματικός σταθμός του Link-16 είναι το σύστημα MIDS (Multifunctional Information Distribution System). Το MIDS είναι το πιο προηγμένο σύστημα διοίκησης, ελέγχου, επικοινωνιών, συντονισμού και ενοποίησης (C4I) το οποίο παρέχει στο χρήστη υψηλή χωρητικότητα δεδομένων, ανθεκτικότητα στις παρεμβολές και ψηφιακή ζεύξη δεδομένων για την ανταλλαγή σε πραγματικό χρόνο πληροφοριών αλλά και φωνητικών δεδομένων σε επίγεια, εναέρια και θαλάσσια μέσα. Το σύστημα MIDS προορίζεται για την υποστήριξη βασικών λειτουργιών του θεάτρου των επιχειρήσεων όπως της επιτήρησης, της αναγνώρισης, του ελέγχου του εναέριου χώρου και του συντονισμού εμπλοκής των διατιθέμενων όπλων. Ο Αμερικανικός στόλος χρησιμοποιεί το σύστημα AN/ URC-107 το οποίο παρέχει στα πολεμικά πλοία, αεροπλάνα αλλά και στις επίγειες δυνάμεις της δυνατότητα διασύνδεσης μέσω του link-16. Το πρόγραμμα TADIL J Range Extension (JRE) καλύπτει την απαίτηση ασφαλούς μετάδοσης δεδομένων και πέραν του ορίζοντα χωρίς τη χρήση ενός ειδικού αερομεταφερόμενου αναμεταδότη. Δύο είναι οι λόγοι που οδήγησαν στην ανάπτυξη αυτού του προγράμματος:

α. Η τρέχουσα μέθοδος για την επέκταση της εμβέλειας ενός δικτύου JTIDS είναι να χρησιμοποιήσει εναέρια μέσα ως αναμεταδότες. Αυτό επιτρέπει την ανάπτυξη ενός πολύ μεγάλου (γεωγραφικά), ολοκληρωμένου δικτύου JTIDS που παρέχει δυνατότητα διασύνδεσης μεταξύ όλων των στοιχείων σε ένα θέατρο επιχειρήσεων. Ωστόσο, η χρήση των αερομεταφερόμενων αναμεταδοτών από το JTIDS αποτελεί σπατάλη διότι μειώνει την χωρητικότητα του δικτύου, με αυτόν τον τρόπο μειώνεται η ταχύτητα μετάδοσης άλλων χρήσιμων πληροφοριών.

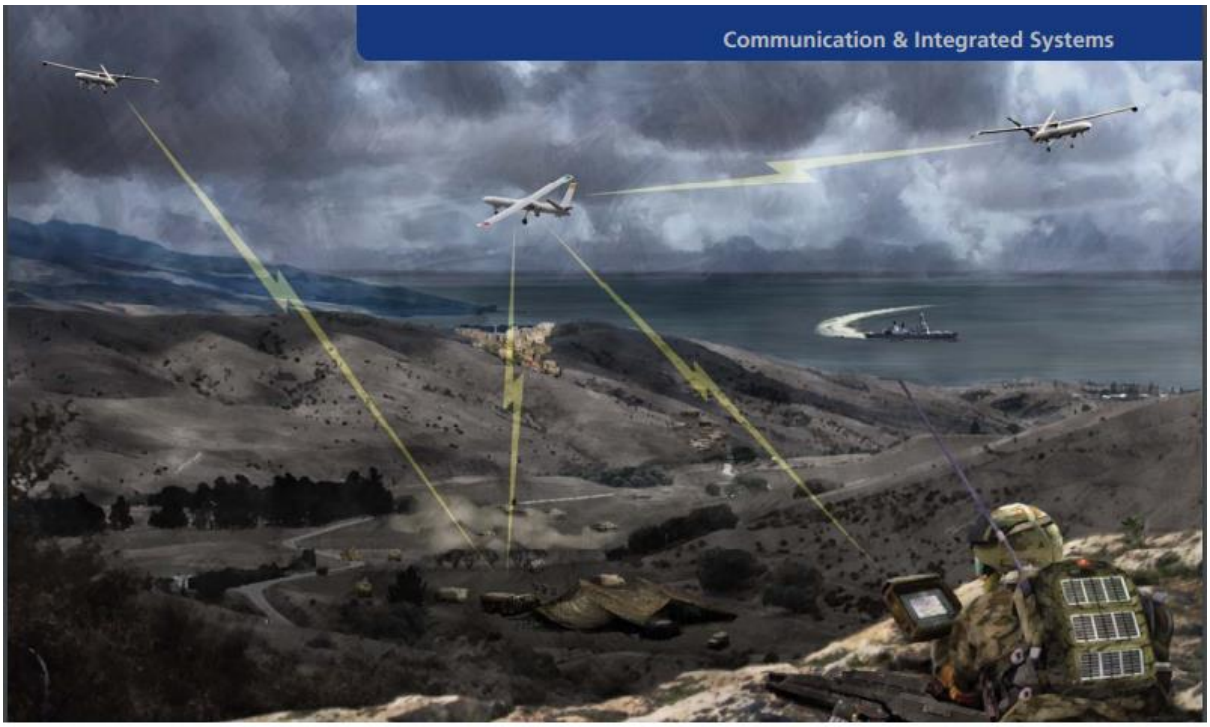
β. Οι μελέτες δείχνουν ότι το JTIDS έχει την τεχνική ικανότητα να υποστηρίξει τις απαιτήσεις των επικοινωνιών τύπου TMDS[71] (Transition Minimized Differential Signalling), οι οποίες θα συμβάλουν στην βελτίωση της απόδοσης του δικτύου. Το σύστημα JRE[72] θα αποτελεί μια πύλη μεταξύ των υφιστάμενων JTIDS και τον δορυφορικών τερματικών. Η εκάστοτε διαμόρφωση της πύλης θα καθορίζεται από τις απαιτήσεις του χρήστη. Θα μπορούσε είτε να ενσωματωθεί πλήρως σε ένα υπάρχον σύστημα υποδοχής ή σε ένα αυτόνομο σύστημα επεξεργαστή.

Το τερματικό JTIDS θα συνδέεται με την πύλη JRE για τη μετάδοση και λήψη TADIL J μηνυμάτων από μια συγκεκριμένη ζώνη JTIDS. Στο άλλο άκρο της πύλης θα είναι συνδεδεμένο το δορυφορικό τερματικό του οποίου η λειτουργία είναι να μεταδίδει και να λαμβάνει μηνύματα. Τρέχουσες μελέτες έχουν επικεντρωθεί σε δύο εφαρμογές της πύλης JRE: Πρώτον στο θέατρο επιχειρήσεων Reachback: Αυτή η εφαρμογή χρησιμοποιείται για τη μετάδοση πληροφοριών εναέριας επιτήρησης και δεδομένων που

[71] TMDS: είναι μια τεχνολογία για τη μετάδοση υψηλής ταχύτητας σειριακών δεδομένων. Ο πομπός ενσωματώνει έναν προχωρημένο αλγορίθμων κωδικοποίησης, ο οποίος μειώνει την Ηλεκτρομαγνητική παρεμβολή πάνω από τα καλώδια χαλκού και έτσι αυξάνεται η ταχύτητα μετάδοσης. www.bicsi.org/pdf/Regions/UnderstandingDVI-HDMand Display Port Signals.pdf

[72] JRE: Είναι ένα σύστημα υλικού(hardware) και λογισμικού(software) που λαμβάνει πληροφορίες από τακτική ζεύξη δεδομένων (link) σε ένα συγκεκριμένο τομέα των επιχειρήσεων και τις μεταδίδει σε ένα άλλο τερματικό ζεύξης δεδομένων πέρα από τη γραμμή της όρασης (Beyond Line Of Sight/ BLOS). www.globalsecurity.org/military/systems/aircraft/systems/jre

προέρχονται από τα κέντρα διευθύνσεως πυρός των βαλλιστικών πυραύλων σε κάποιο απομακρυσμένο κέντρο (μεγάλη απόσταση από τα προκεχωρημένα JTIDS στοιχεία) ελέγχου που βρίσκεται πέρα από τη γραμμή οράσεων. Δεύτερον στην Inter-zone Συνδεσιμότητα: Αυτή η εφαρμογή χρησιμοποιείται για τη μετάδοση πληροφοριών εναέριας επιτήρησης και δεδομένων που προέρχονται από τα κέντρα διευθύνσεως πυρός των **βαλλιστικών πυραύλων** μεταξύ προκαθορισμένων περιοχών ενός θεάτρου επιχειρήσεων.[73] Τέλος, προβλέπεται ότι το Link-16 πρόκειται να αντικαταστήσει το Link-4A σε επιχειρήσεις ATC (Air traffic control) όπως και το Link-4C που χρησιμοποιείται για επιχειρήσεις στο επίπεδο του μαχητή.



Εικόνα 47: Αναπαράσταση του τρόπου με τον οποίο λειτουργούν τα δίκτυα επικοινωνιών και κατάδειξης στόχων.

[73] John Pike, « Tactical Digital Information Links (TADIL)» , updated Sunday, April 23, 2000. Available from: http://fas.org/irp/program/disseminate/tadil

στ. Link-22: Το κύριο σύστημα ανταλλαγής πληροφοριών των αμερικανικών ναυτικών δυνάμεων, είναι το LINK 11 που ενώ είναι σχετικά ένα ασφαλές δίκτυο, το πρωτόκολλο όμως που χρησιμοποιεί δεν καλύπτει πλήρως τις απαιτήσεις ανταλλαγής τακτικών δεδομένων που είναι διαθέσιμα σε ένα σύγχρονο περιβάλλον αεροναυτικών επιχειρήσεων. Πέραν τούτου, η αρχιτεκτονική ανάπτυξης και εκμετάλλευσης του το καθιστά ευάλωτο και είναι ιδιαίτερα ευαίσθητο σε ηλεκτρονικά αντίμετρα (ECM). Για τον παραπάνω λόγο έχει ξεκινήσει η ανάπτυξη του LINK-22, το οποίο σταδιακά θα αντικαταστήσει το ξεπερασμένο LINK 11, με απώτερο σκοπό τη δημιουργία μιας μορφής LINK 16 (με όλες τις δυνατότητες μεταφοράς δεδομένων και ασφαλείας πού έχει το LINK 16) με επιπρόσθετη δυνατότητα διασύνδεσης σε HF, προκειμένου να καλύψει τις απαιτήσεις επικοινωνίας BLOS. Το πρωτόκολλο του LINK 22, που βρίσκεται ακόμα υπό ανάπτυξη στο NATO, περιγράφεται στην NATO STANAG 5522, ενώ στοιχεία σχετικά με την επιχειρησιακή εκμετάλλευση του, δίδονται στην ADatP-22. Μέχρι σήμερα το LINK 22, χρησιμοποιείται σε περιορισμένη επιχειρησιακή μορφή, από το ναυτικό της Ιταλίας και των ΗΠΑ[74].

ζ. CDL (Common Data Link) είναι ένα αμερικανικής προέλευσης πρωτόκολλο στρατιωτικών επικοινωνιών. Δημιουργήθηκε από το Αμερικανικό Υπουργείο άμυνας το 1991 ως το πρωταρχικό πρωτόκολλο που θα χρησιμοποιούσε ο στρατός για την μετάδοση εικόνων και πληροφοριών. Λειτουργεί εντός της ζώνης (Band) K_u [75] με ρυθμό ανταλλαγής δεδομένων (data rate) έως και 254 Mbit / s. Το CDL επιτρέπει την αμφίδρομη ανταλλαγή δεδομένων. Τα σήματα (signals) του CDL μεταδίδονται,

[74] John Pike, « Tactical Digital Information Links (TADIL)» , updated Sunday, April 23, 2000. Available from: http://fas.org/irp/program/disseminate/tadil

[75] Η ζώνη(band) K_u που κυμαίνεται στα 12-18 Ghz του ηλεκτρομαγνητικού φάσματος. Χρησιμοποιείται κυρίως από συστήματα στις δορυφορικές επικοινωνίες.

λαμβάνονται, συγχρονίζονται, δρομολογούνται και προσομοιώνονται από τα κουτιά δεδομένων (interface boxes/CIBs) του CDL.

η. TCDL (Tactical Common Data Link) είναι ένα ασφαλές πρωτόκολλο ζεύξης δεδομένων υψηλής ταχύτητας. Είναι Αμερικανικής κατασκευής και χρησιμοποιείται από τον στρατό των ΗΠΑ για την ασφαλή αποστολή δεδομένων και τη αποστολή βίντεο σε συνεχή ροή (streaming) από τις αερομεταφερόμενες πλατφόρμες (ΜΕΑ, αεροσκάφη, Drone) σε επίγειους σταθμούς (εικόνα 17). Το TCDL έχει τη δυνατότητα να δεχτεί δεδομένα (data) από πολλές διαφορετικές πηγές (sources) και στην συνέχεια να τα κρυπτογραφήσει, κωδικοποιήσει και διαβιβάσει σε υψηλές ταχύτητες στους ενδιαφερόμενους. Το TCDL σχεδιάστηκε για τα UAVs και ειδικά για το MQ-8B Fire Scout.Μεταδίδει ραντάρ, εικόνες, βίντεο και άλλες πληροφορίες σε συχνότητες από 1544 Mbit/s έως 10,7 Mbit/s σε αποστάσεις έως 200 χιλιόμετρα.[76]

Εικόνα 58. Τερματικός Σταθμός τακτικού δικτύου.

θ. HIDL (High Integrity Data Link) είναι αμερικανικής προέλευσης πρωτόκολλα ζεύξης δεδομένων (εικόνα 18).Παρέχει τη δυνατότητα διοίκησης και ελέγχου σε UAV αλλά και στους επίγειους σταθμούς που παρέχουν υποστήριξη στα UAV. Η ευελιξία του συστήματος HIDL προσφέρει επίσης ασφαλή μετάδοση βίντεο σε συνεχή ροή, την ικανότητα αναμετάδοσης δεδομένων ακόμη και εκτός της γραμμής

[76] Η πρώτη του επιχειρησιακή εφαρμογή σε πόλεμο πραγματοποιήθηκε το 1998-1999 στην Επιχείρηση Allied Force. Benjamin S. Lambeth , «NATO's War to Save Kosovo» , Washington, D. C.: Brookings Institution, έκδοση 2000 ,σελ. 236

οράσεως (Line Of Sight/LOS) των οπλικών συστημάτων και τη μεταφορά δεδομένων μέσω ενός ασφαλούς δικτύου. Οι βασικές δυνατότητες που παρέχονται μέσω του HIDL είναι:[77]

- Η δυνατότητα διοίκησης και ελέγχου (Command&control) των UAVs αλλά και διαφόρων οπλικών συστημάτων.
- Ασφαλή δίκτυα τηλεπικοινωνιών από παρεμβολές(jamming).
- Ασφαλή μετάδοση βίντεο σε συνεχής ροή(live).
- Δυνατότητα αναμετάδοσης πέραν της γραμμής οράσεως(line of sight).
- Χαμηλή πιθανότητα ανίχνευσης ή υποκλοπής.
- Υπερβαίνει τις συνέπειες του φαινομένου Doppler έως την ταχύτητα ενός mach.
- Πλήρως Επεκτάσιμο.

ι. **ABIT (Airborne Information Transmission System)** είναι και αυτό σύστημα ζεύξης δεδομένων. Χρησιμοποιείται κατά κύριο λόγο για μετάδοση των εικόνων από δορυφόρους και ΜΕΑ (Μη Επανδρωμένα αεροχήματα). Το ABIT είναι μια εξέλιξη του CDL και λειτουργεί στην συχνότητα των 548 Megabits / s και οι πιθανότητα παρεμβολής του είναι πολύ μικρή. Η μονάδα συλλογής είναι ικανή να εκπέμπει δεδομένα είτε με την μορφή κυματομορφής του ABIT σε μια πλατφόρμα αναμετάδοσης ή με την μορφή κυματομορφής του CDL σε έναν σταθμό εδάφους. Η μονάδα αναμετάδοσης έχει τη δυνατότητα να λειτουργεί όπως ένας κανονικός συλλέκτης δεδομένων και μπορεί ανταλλάζει δεδομένα μέσω ευρείας ζώνης από άλλους συλλέκτες. Το ABIT δεν είναι ένα «απτό» υλικό αλλά αποτελεί software το οποίο μπορεί να εισαχθεί σε συστήματα ζεύξης δεδομένων.[78]

[77] HIDL (High Integrity Data Link), UAV case Study, Ultra Electronics

[78]Airborne Information Transmission System (ABIT) , Available from: http://www.globalsecurity.org/intell/systems/abit

ια. Improved Data Modem (IDM)[79] είναι ένα σύστημα επικοινωνιών και στόχευσης το οποίο παρέχει τη δυνατότητα διασύνδεσης μεταξύ διαφορετικών πλατφόρμων επικοινωνίας το οποίο αναπτύχθηκε από την εταιρία Lynx OS. Χρησιμοποιείται για τη διασύνδεση του στρατού των Αμερικάνων με την πολεμική τους αεροπορία. Έχει χρησιμοποιηθεί ευρέως για τη διαβίβαση των δεδομένων στόχευσης σε μαχητικά F-15E / F-16C και F-16CJ. Στην Ελλάδα χρησιμοποιείται από τα αεροσκάφη F-16 BLOCK 52.

ιβ. PATRIOT Digital Information Link – PADIL[80] είναι ένα ψηφιακό δίκτυο πληροφοριών το οποίο είναι ασφαλές και παρέχει δυνατότητα αμφίδρομης σύνδεσης για την ανταλλαγή πληροφοριών ανάμεσα στα συστήματα εκτόξευσης των πυραύλων Patriot, ανάμεσα στο σύστημα εκτόξευσης και το όχημα που βρίσκεται το ΚΔΠ (Κέντρο Διευθύνσεως πυρός). Το PADIL ανταλλάζει (εικόνα 19) δεδομένα στη συχνότητα UHF ή χρησιμοποιεί σταθερά τηλέφωνα (landlines[81]) .

[79] ICI's IDM (Improved Data Modem), Lynx Software Technologies. Available from: www.lynx.com/icis-idm-improved-data-modem

[80]Army Airspace Command and Control Connectivity . Available from: http://www.globalsecurity.org/military/library/policy/army/fm/3-52/ch5.htm

[81] «Σταθερά» τηλέφωνα(landlines): είναι τύπος τηλεφώνων που μεταδίδουν σήματα μέσω ενσύρματων μέσων (καλωδίων, οπτικών ινών) και όχι χρησιμοποιώντας ασύρματα μέσα όπως γίνεται στα κινητά τηλέφωνα που μεταδίδει σήματα μετατρέπονται από τα δεδομένα ήχου μέσω φυσικά μέσα, όπως σύρμα ή καλώδιο οπτικών ινών, και όχι μέσω ασύρματης μετάδοσης, όπως συμβαίνει με τα κινητά τηλέφωνα. Ο όρος σταθερό τηλέφωνο είναι επίσης μερικές φορές χρησιμοποιείται για να αναφερθεί σε μια ειδική γραμμή, η οποία είναι μια μόνιμη σύνδεση ανάμεσα σε δύο θέσεις. Ωστόσο, τα τελευταία χρόνια, ο όρος χρησιμοποιείται κυρίως για τη διαφοροποίηση της έννοια σταθερού τηλεφώνου στο σπίτι από τα κινητά.

Εικόνα 69: Τερματικός σταθμός τακτικού δικτύου PADIL

ιγ. Tactical Information System Broadcast - TIBS που χρησιμοποιείται για τα συστήματα πυραυλικής άμυνας. Είναι ένα δίκτυο το οποίο έχει την δυνατότητα συνεχούς, ασφαλούς μετάδοσης των δεδομένων μεταξύ των πυραυλικών συστημάτων. Η αρχική του λειτουργία συστήματος ήταν η παροχή σε σχεδόν πραγματικό χρόνο, πληροφορίες τακτικής φύσεως στους διοικητές κατά τη διάρκεια της μάχης σχετικά με την στόχευση των συστημάτων του. Επίσης συμβάλει καθοριστικά στη διοίκηση και έλεγχο (command&control) καθώς και στην επίγνωση της τακτικής κατάστασης από τον διοικητή.[82]

ιδ. PLRS (Position Location and Reporting System)/EPLRS (Enhanced Position Location Reporting System)/SADL (Situation Awareness Data Link) είναι μια οικογένεια τακτικών δικτύων του Αμερικανικού Στρατού / Σώμα των Πεζοναυτών με ζεύξεις δεδομένων που χρησιμοποιούνται για την παρακολούθηση των μονάδων εδάφους και την παροχή οριστικής αναγνώρισης φίλου/εχθρού του εδάφους

[82] Steven Aftergood, Tactical Information Broadcast Service [TIBS], Updated Tuesday, January 19, 1999. Available from: http://fas.org/irp/program/disseminate/tibs.htm

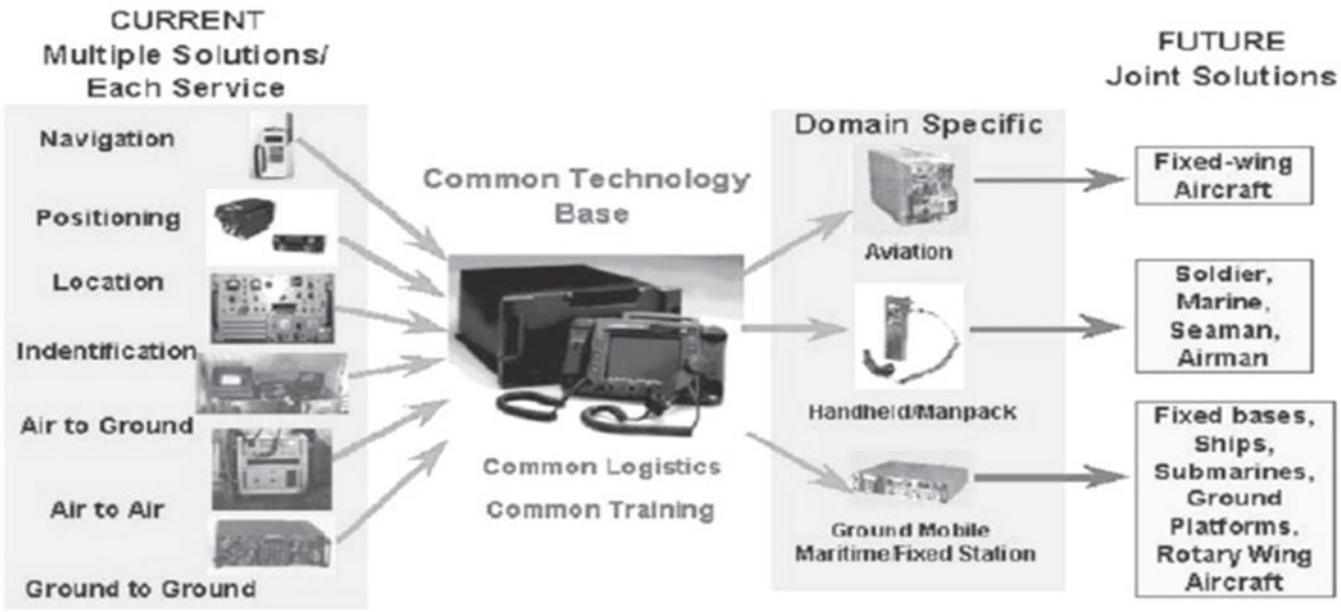
μονάδων. Το EPRLS χρησιμοποιείται επίσης για τη μετάδοση δεδομένων μεταξύ μονάδων εδάφους.

ιε.TCP/IP (Transmission Control Protocol/Internet Protocol) είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων «τρέχει» πάνω από τα άλλα κανάλια, για να παρέχει συνδεσιμότητα μεταξύ των πλατφόρμων και των απομακρυσμένων επίγειων εγκαταστάσεων.[83]

ιστ. Joint Tactical Radio System (JTRS) έχει σκοπό να αντικαταστήσει τα περισσότερα υπάρχοντα συστήματα ραδιοτηλεφωνίας των αμερικανικών ενόπλων δυνάμεων με ένα ενιαίο σύνολο λογισμικού. Το λογισμικό αυτό θα παρέχει μεγάλη ευελιξία καθώς πλέον δεν θα απαιτούνται διαφορετικοί τύποι ραδιοφωνικών συστημάτων στα οχήματα εδάφους για να επιτευχθεί η ενδοεπικοινωνία, θα υπάρχει δηλαδή μόνο ένα κανάλι επικοινωνίας. Το JTRS θα αναπτύξει μια οικογένεια από τακτικά ραδιοφωνικά συστήματα υψηλής χωρητικότητας σε προσιτές τιμές. Τα συστήματα αυτά θα καλύπτουν ένα φάσμα λειτουργίας 2-2000 MHz, θα είναι ικανά να μεταδίδουν φωνή, βίντεο και δεδομένα.[84]

[83] W. Richard Stevens, «The Protocols TCP/IP Illustrated» , Volume 1, σελ. 50

[84] The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress, 17 November 2005

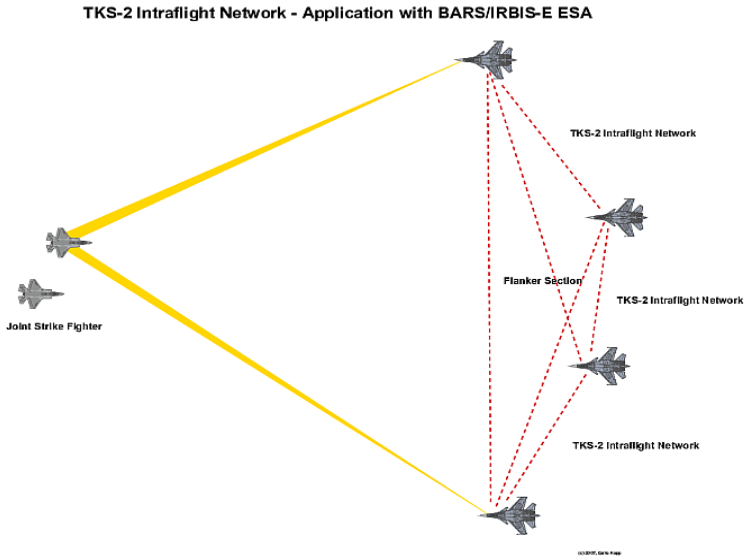


Εικόνα 20: Παρούσα και Μελλοντική διακλαδική δικτύωση.

Οι ικανότητες των παραπάνω συστημάτων που επιτρέπουν τη ζεύξη δεδομένων/πρωτοκόλλων ανταναμλά τις πραγματικές εξελίξεις στην τεχνολογία των υπολογιστών που παρατηρούνται την τελευταία δεκαετία. Νέα πρωτόκολλα όπως το JTRS (Joint Tactical Radio System) προορίζεται να ενσωματώσει μηχανισμούς για τη κωδικοποίηση τέτοιων πρωτοκόλλων σε μορφές που μπορούν να σταλούν σε ένα κοινό κανάλι για διακλαδική εκμετάλλευση (εικόνα 20). Ξεχωριστά από αυτά τα πολύ-πλατφορμικά (multi-platform) πρωτόκολλα και διαμορφώσεις υπάρχουν άλλα συστήματα ζεύξης δεδομένων, όπως οι «intra» (εικόνα 21) και «interflight» ζεύξης δεδομένων που χρησιμοποιούνται από F/A-22A και αργότερα το μαχητικό αεροπλάνα τύπου JSF (Joint Strike Fighter)[85].

[85] Joint Strike Fighter (JSF) είναι ένα πρόγραμμα ανάπτυξης μαχητικών αεροσκαφών το οποίο προορίζεται να αντικαταστήσει κάποιους τύπους μαχητικών αεροσκαφών που ήδη χρησιμοποιούνται (μαχητικών και βομβαρδιστικών). Η ανάπτυξη του προγράμματος γίνεται από κοινού από τις ΗΠΑ, το Ηνωμένο Βασίλειο , την Τουρκία, την Ιταλία, την Ολλανδία, τον Καναδά, την Αυστραλία. Μετά από ένα διαγωνισμό μεταξύ του X-32 της Boing και το X-35 της Lockheed

Μέχρι στιγμής δεν έχει σημειωθεί ικανή προσπάθεια ώστε να επωφεληθούμε από τα νέα ad-hoc[86] πρωτόκολλα δικτύου, τα οποία είναι σχεδιασμένα για την οργάνωση των δικτύων κινητών πλατφορμών, αν και το πρόγραμμα JTRS είναι πολλά υποσχόμενο. Τα συστήματα δικτύωσης Ad-Hoc αποτελούν μια επαναστατική τεχνολογία υπέρ του NCW.



Εικόνα 21: Μελλοντική δικτύωση αεροσκαφών.

Οι παρεμβολές των δικτύων και των πλατφόρμων ISR είναι πολύ σημαντικές για έναν εισβολέα. Οι κεραίες των δικτύων είναι συνήθως κατασκευασμένες από φθηνά υλικά

Martin, το τελικό σχέδιο επιλέχθηκε με βάση το X-35. Αυτό είναι το F-35 Lightning II, το οποίο θα αντικαταστήσει διάφορους τύπους τακτικών αεροσκαφών, συμπεριλαμβανομένων των F-16, A-10, F / A-18, AV-8B Harrier καθώς και των βρετανικών GR 7 & GR9s. Το προβλεπόμενο μέσο ετήσιο κόστος αυτού του προγράμματος είναι 12,5 δισεκατομμύρια δολάρια και το εκτιμώμενο πρόγραμμα κόστους κύκλου ζωής των $ 1.100 δισεκατομμύρια. ***A history of the Joint Strike Fighter Program, Martin-Baker. Retrieved April 2011***

[86] Ad-hoc: Ένα ασύρματο ad-hoc δίκτυο (αυτοοργανωμένο δίκτυο ή δίκτυο κατ' απαίτηση) είναι ένας αποκεντρωμένος τύπος ασύρματου δικτύου. Αυτοί οι τύποι δικτύων δε βασίζονται σε κάποια προϋπάρχουσα υποδομή, όπως δρομολογητές στα ενσύρματα δίκτυα ή ασύρματα access points στα διαχειριζόμενα ασύρματα δίκτυα. Αντίθετα, κάθε κόμβος λαμβάνει μέρος στη δρομολόγηση προωθώντας τα δεδομένα προς τους άλλους κόμβους, κι έτσι ο καθορισμός του ποιοι κόμβοι προωθούν δεδομένα γίνεται δυναμικά με βάση τη συνδεσιμότητα του δικτύου. Πέρα από την κλασσική δρομολόγηση, τα ad hoc δίκτυα μπορούν να χρησιμοποιήσουν την υπερχείλιση για να προωθήσουν τα δεδομένα.

παρόλα αυτά μπορούν να πετύχουν ημισφαιρική κάλυψη και οι πομποί ζεύξης δεδομένων μπορούν να φτάσουν έως εκατοντάδες Watt ισχύ εξόδου.

§5 Δικτυοκεντρικός Πόλεμος- Τακτικά Δίκτυα στο επιχειρησιακό περιβάλλον της Ελλάδας

§5.1 Γενικά

Η χώρα μας ως μέλος του NATO παρακολουθεί και συνδιαμορφώνει-συναποφασίζει τις εξελίξεις στα πλαίσια της Συμμαχίας. Είναι επόμενο η φιλοσοφία, η εκπαίδευση, τα οπλικά συστήματα, αλλά και η γενικότερη δομή των ΕΔ να επηρεάζονται ανάλογα από την εμπειρία του NATO αλλά και των ΗΠΑ.

Ένας τομέας που η Συμμαχία εδώ και δεκαετίες έχει ενοποιήσει στα πλαίσια της καλύτερης αντιμετώπισης αρχικά της Σοβιετικής απειλής και στη συνέχεια των ενδεχόμενων περιφερειακών κινδύνων, είναι η Αεράμυνα των χωρών μελών. Ένα δίκτυο RADAR από την Νορβηγία μέχρι την Τουρκία στήθηκε και συνεχώς ανανεώνεται με τη δημιουργία αντίστοιχων κέντρων επιχειρήσεων για τον έλεγχο των αεροσκαφών αεράμυνας, των κατευθυνόμενων βλημάτων, των Α/Α όπλων, αλλά και το συντονισμό διακλαδικά όπου απαιτείται (πολεμικά πλοία, κλπ).

Το πρώτο DATA LINK 1 στη χώρα μας λειτούργησε το 1971 από το RADAR EARLY WARNING Βιτσίου προς το SOC (SECTOR OPERATION CENTER) Λάρισας. Το 1975 το δίκτυο LINK-1 ολοκληρώθηκε με Ίσμαρο-Χορτιάτη-Πήλιο-Πάρνηθα-Ζήρο.

Σήμερα το νατοϊκό πρόγραμμα ACCS (AIR COMMAND CONTROL SYSTEM), το οποίο για το NATO λογίζεται το σύστημα των συστημάτων σε τακτικό επίπεδο, είναι το κύριο σύστημα διεξαγωγής δικτυοκεντρικών επιχειρήσεων. Η χώρα μας έχει συμβάλλει στην ανάπτυξη του λογισμικού με πάνω από 5 εκατομμύρια ευρώ. Έχει

παραλάβει από το NATO το BUNKER του Κουτσόχερου-Λάρισας, όπου συστεγάζεται το ΕΚΑΕ (Εθνικό Κέντρο Αεροπορικών Επιχειρήσεων), ο εξοπλισμός του CAOC (Combined Air Operation Center) Λάρισας, που δεν ενεργοποιήθηκε λόγω αντίδρασης της Τουρκίας, και το ARS (**A**ir command center-**R**ecognized picture center-**S**ensor fusion post=Κέντρο ελέγχου, παραγωγής διευκρινισμένης εικόνας και ενοποίησης της εικόνας radar). Η Ελλάδα με το CAOC+ARS=CARS Λάρισας απέκτησε ένα σύγχρονο σύστημα ανοιχτής αρχιτεκτονικής, πλήρως δικτυοκεντρικό για εθνική χρήση, πλήρως επιχειρησιακό με όλα τα τακτικά δίκτυα της χώρας (LINK 1, LINK 11, LINK 16).

Σε τακτικό επίπεδο οι Μονάδες Κατευθυνόμενων Βλημάτων μεγάλου, μεσαίου και μικρού βεληνεκούς (πλην μερικών παλαιάς τεχνολογίας), του ΣΞ, ΠΝ και ΠΑ είναι δικτυωμένες.

Στα πλαίσια των νατοϊκών του υποχρεώσεων, ο Σ.Ξ. διαθέτει το AAOCC (ARMY AIR OPERATION COORDINATION CENTER) υπό τις διαταγές του NDC GR σε καιρό ειρήνης, ή υπό εθνική διοίκηση σε περίπτωση εθνικών επιχειρήσεων. Η εν λόγω Μονάδα μπορεί να συντονίσει την ομαλή διεξαγωγή διακλαδικών επιχειρήσεων, χρησιμοποιώντας κοινά πρωτόκολλα από το νατοϊκό πρόγραμμα ACCS (AIR COMMAND CONTROL SYSTEM). Η παραγωγή, η διανομή και η εκμετάλλευση της Κοινής Επιχειρησιακής Εικόνας (ΣΞ-ΠΝ-ΠΑ) είναι το κυριότερο επιδιωκόμενο αποτέλεσμα, όταν το AAOCC είναι δικτυωμένο με το Εθνικό Κέντρο Αεροπορικών Επιχειρήσεων ή το νατοϊκό CAOC (TOREJON-Ισπανία).

Ο δικτυοκεντρικός τρόπος πολέμου αποτελεί την αιχμή του δόρατος στην Πολεμική Αεροπορία μας. Όπως είναι γνωστό ήδη το LINK 16 αποτελεί μέρος του ηλεκτρονικού εξοπλισμού των αεροσκαφών μας F-16 BLOCK 52+ ADV. Αυτή η δυνατότητα επιτρέπει στα εν λόγω Α/Φ να εκτελούν τις πιο απαιτητικές αποστολές αεράμυνας ή βομβαρδισμού ή προσβολής πλοίων ή συνοδείας κλπ.

Η ίδια δυνατότητα έχει πιστοποιηθεί-χρησιμοποιηθεί από το ελληνικό ιπτάμενο radar (ΑΣΕΠΕ) στον έλεγχο των επιχειρήσεων του εναέριου χώρου της Λιβύης. Το

σύστημα PATRIOT χρησιμοποιεί το LINK 16 στα δύο Κέντρα διανομής στόχων (ICC) για τις επιχειρήσεις αεράμυνας.

Τέλος με τη βοήθεια του ΝΑΤΟ τοποθετήθηκαν στα τρία Κέντρα Ελέγχου Περιοχής (Χορτιάτης-Πάρνηθα-Ζήρος) ο απαραίτητος εξοπλισμός (υλικά, διασυνδέσεις) και το αντίστοιχο λογισμικό, ενώ η χώρα δάνεισε στο ΝΑΤΟ τα τερματικά (MIDS TERMINAL μέχρι να τοποθετηθούν τα νατοϊκά από αντίστοιχο πρόγραμμα) για την ολοκλήρωση της δικτύωσης. Έτσι η χώρα μας συγκαταλέγεται στις λίγες χώρες που έχει πραγματικά ολοκληρωμένη δυνατότητα δικτυοκεντρικού πολέμου στις αεροπορικές επιχειρήσεις.

Αν ληφθεί υπόψη και η υπάρχουσα δυνατότητα του LINK 11 στις κυριότερες Μονάδες Διοίκησης και Ελέγχου της ΠΑ (ΕΚΑΕ-CARS Λάρισας-ΚΕΠ-ΑΣΕΠΕ-Κ/Β-SHORAD), του ΠΝ (Πολεμικά πλοία-CROTALE) και του ΣΞ (Μονάδες διασυνδεμένες στο ενοποιημένο σύστημα αεράμυνας, όπως HAWK, TOR M1, κλπ), τότε είναι φανερό ότι τα τακτικά δίκτυα είναι σήμερα-μελλοντικά ο μεγαλύτερος πολλαπλασιαστής ισχύος στις διακλαδικές επιχειρήσεις που αναπόφευκτα, θα εκτελέσουν οι ΕΔ της χώρας μας.

Ειδικά για το ΠΝ η τοποθέτηση του LINK 22 μετά από πολυετείς καθυστερήσεις θα είναι ένα σημαντικό βήμα προόδου. Ταυτόχρονα θα πρέπει να ληφθεί υπόψη, ότι αντίστοιχα χώρες με ισχυρό ναυτικό έχουν ήδη τοποθετήσει το LINK 16 και το χρησιμοποιούν καθημερινά σε ασκήσεις με τις ελληνικές ΕΔ. Το Γερμανικό, το Αγγλικό, το Ολλανδικό, το Αμερικανικό, το Ισπανικό, το Νορβηγικό, το Γαλλικό, το Ιταλικό, κλπ, ναυτικό είναι ήδη χρήστες του LINK 16.

§5.2 Δικτυοκεντρική Δυνατότητα στις ελληνικές ΕΔ

Η Ελλάδα βρίσκεται σε μία σημαντικά στρατηγική γεωγραφική θέση. Συνορεύει με μία χώρα, την Τουρκία, η οποία ευθέως απειλεί την ακεραιότητά της. Τα χαρακτηριστικά της απειλής προσδιορίζονται από μια ισχυρά πληθυσμιακή χώρα 75 εκατ. συνοδευόμενα από ισχυρή οικονομική ανάπτυξη, με παράλληλη βελτίωση της στρατιωτικής της τεχνολογίας και παραγωγής όπλων. Ακριβώς στον αντίποδα η χώρα μας βρίσκεται σε μια μεγάλη οικονομική κρίση που οδηγεί στην αναγκαστική μείωση των αμυντικών της δαπανών. Η χώρα μας μαζί με τις συμμαχίες που πρέπει να κτίζει στην περιοχή (Ισραήλ, Αίγυπτος, κλπ) είναι αναγκαίο να επενδύσει σε έναν **οικονομικό τρόπο αντιμετώπισης της απειλής από τον Έβρο μέχρι το ακρωτήριο Άγιος Ανδρέας της Κύπρου.**

Όπως ήδη αναλύθηκε σε προηγούμενα κεφάλαια ζούμε την εποχή της πληροφορίας. Αυτός που την έχει νωρίτερα, αντιλαμβάνεται την τακτική κατάσταση γρηγορότερα, αποφασίζει και διατάζει γρηγορότερα κλπ., με άλλα λόγια έχει υπεροχή στην άμεση λήψη και υλοποίηση αποφάσεων. Η τεχνολογική αλλαγή είναι τόσο ραγδαία, που επηρεάζει[87] (Gordon Moore's Law of Integrated circuits) τη φιλοσοφία εκτέλεσης επιχειρήσεων, αφού βελτιώνει-αλλάζει τις επιχειρησιακές δυνατότητες των οπλικών συστημάτων, που χρησιμοποιούν ηλεκτρονικούς υπολογιστές ως εξής: *Κάθε 18 μήνες τα νέα chips των υπολογιστών έχουν διπλάσια χωρητικότητα και γίνονται ταυτόχρονα δύο φορές ταχύτερα με ίδιο κόστος, πράγμα που σημαίνει ότι γίνονται 4 φορές δυνατότερα κάθε 18 μήνες.* Η Ελλάδα δεν μπορεί στο άμεσο μέλλον να διαθέσει αρκετούς πόρους για την αγορά οπλικών συστημάτων της συνεχώς εξελισσόμενης στρατιωτικής τεχνολογίας, μπορεί και πρέπει όμως επιλεκτικά να χρησιμοποιεί εμπορική-στρατιωτική τεχνολογία διασύνδεσης στρατιωτικών συστημάτων, επενδύοντας στην ενοποίηση πληροφοριών σε μια κοινή

[87] Network Centric Operations: Background and Oversight Issues for Congress March 15, 2007 Clay Wilson, Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division

επιχειρησιακή εικόνα απαραίτητη και στα τρία όπλα με την ανάλογη ασφάλεια των επικοινωνιών.

Ο χώρος του Αιγαίου αποτελεί ένα ιδιόμορφο ενδεχόμενο θέατρο επιχειρήσεων. Ένας μεγάλος θαλάσσιος χώρος διάσπαρτος από νησιά μεγάλα και μικρά, από νησίδες και βραχονησίδες. Ένας χώρος με ιδιαίτερες αμυντικές απαιτήσεις, αλλά με αυτονόητη την απαίτηση για διεξαγωγή διακλαδικών επιχειρήσεων, για να γίνει δυνατή η προστασία της εδαφικής ακεραιότητας και των συμφερόντων της χώρας μας.

Οι στρατιωτικές δυνάμεις μας στο Αιγαίο είναι διάσπαρτες «ψηφίδες ισχύος» και δεν είναι εφικτό λόγω της γεωγραφίας να αποτελέσουν μία ενιαία γραμμή άμυνας ξηράς όπως πχ. στον Έβρο. Σε περίπτωση επιχειρήσεων οι ψηφίδες ισχύος μας θα αναμειχθούν στο φυσικό χώρο με αντίπαλες δυνάμεις (πλοία, αεροσκάφη, δυνάμεις καταδρομών ή απόβασης), δημιουργώντας μία φαινομενικά χαοτική εικόνα, οι οποίες όμως ευρισκόμενες σε επικοινωνία μεταξύ τους και μέσω ενός δικτύου συλλογής, ανάλυσης, εκτίμησης και μετάδοσης πληροφοριών, θα μπορούν να **συντονίζονται χωρίς να έχουν κοινό οπτικό πεδίο ή να παρατάσσονται ομαδικά**.

Η ισχύς κάθε πολεμικής δύναμης όπως ήδη αναλύθηκε βασίζεται σε δυο κύρια συστατικά στοιχεία, τα οποία είναι η πληροφορία και η μάζα των καταστροφικών μέσων. Τα δυο αυτά συστατικά λειτουργούν αντιστρόφως ανάλογα, δηλαδή, όσο πιο πολλές ακριβείς, ευκολονόητες και πρόσφατες πληροφορίες διαθέτουμε και όσο καλύτερες ικανότητες αξιοποίησης αυτών των πληροφοριών μέσω πυρών ακριβείας, τόσο λιγότερη μάζα καταστροφικών μέσων θα χρειαστούμε.

Η δικτύωση των Μονάδων που θα αμυνθούν της χώρας μας, αλλά ιδιαίτερα στο Αιγαίο είναι ο οικονομικότερος τρόπος άμυνας . Κατά ένα μέρος υπάρχει σήμερα στην ενοποιημένη αεράμυνα, σε μονάδες πυροβολικού, αρμάτων κλπ. Θα πρέπει όμως να επεκταθεί σε κάθε επίπεδο διακλαδικά, περιλαμβάνοντας όχι μόνον επιχειρησιακές παραμέτρους αλλά και την υποστήριξη της πολεμικής προσπάθειας (συντήρηση, ψυχολογικές επιχειρήσεις, διαχείριση μαζικών μέσων ενημέρωσης, κλπ).

Έτσι σήμερα η ύπαρξη αισθητήρων επιτήρησης και των τριών κλάδων (ΣΞ-ΠΝ-ΠΑ), συμφέρει οικονομικά-τεχνολογικά-επιχειρησιακά να ενοποιηθούν-δικτυωθούν **με τη χρήση ενός εθνικού πρωτοκόλλου**. Έτσι είναι δυνατή η εξοικονόμηση πόρων. Για παράδειγμα αν σε ένα νησί σήμερα υπάρχει ένα radar επιτήρησης του ΠΝ, ένα της ΠΑ, και ένα του ΣΞ, με τη σημερινή τεχνολογία είναι δυνατή η κάλυψη της επιχειρησιακής ανάγκης με **ένα σύστημα που να καλύπτει και τους τρεις κλάδους** μοιράζοντας δικτυακά την εικόνα σε κάθε επίπεδο (τοπικά-πλάγια σε τακτικό επίπεδο, προς τα πάνω σε επιχειρησιακό επίπεδο). Προϋπόθεση η καθιέρωση ενός εθνικού πρωτόκολλου επικοινωνίας και για τα τρία όπλα.

Το 1991 στον πόλεμο του Κόλπου οι απώλειες των αμερικανών από φίλια πυρά ήταν το 25% του συνόλου των απωλειών μάχης. Το ποσοστό μειώθηκε στο 11% των απωλειών στο δεύτερο πόλεμο του Κόλπου και στο Αφγανιστάν με τη επέκταση της χρήσης του Ιχνηλάτη Φίλιων Δυνάμεων (Blue Force Tracker), όπως ισχυρίζονται οι Αμερικανοί σε σχετική αναφορά προς το Κογκρέσο. Η δικτύωση όλων των φίλιων μονάδων που δρουν στο Αιγαίο, με τον εφοδιασμό τους με αντίστοιχο Ιχνηλάτη Φίλιων Δυνάμεων θα μειώσει σημαντικά τα αδελφοκτόνα πυρά και θα αυξήσουν τον συντονισμό και την φονικότητα των πυρών μας διακλαδικά.

Σε περίοδο επιχειρήσεων το Αιγαίο θα είναι ένας χώρος με διάσπαρτες χερσαίες δυνάμεις στα νησιά (στατικά οπλισμένες περιοχές) οι Διοικητές των οποίων, θα πρέπει να παρακολουθούν τη διάταξη των δυνάμεων τους αλλά ενδεχομένως και τη θέση των φίλιων αεροσκαφών για να μη τα καταρρίψουν, τη θέση των φίλιων πλοίων για να μη τα βουλιάξουν. Ταυτόχρονα θα πρέπει οπωσδήποτε να ξέρει ο Διοικητής κάθε νησιού, που κάνει ο εχθρός απόβαση ή καταδρομική επιχείρηση, με τι δυνάμεις, αν κινδυνεύει το διπλανό νησί πως θα συνδράμει την κρίσιμη στιγμή του αγώνα, που δρουν τα εχθρικά πλοία και αεροσκάφη. Η σωστή δικτύωση θα δώσει σε όλους τους Διοικητές των νησιών την απαραίτητη αντίληψη της τακτικής κατάστασης και θα μειώσει την αναπόφευκτη «ομίχλη της μάχης».

Ο Ιχνηλάτης Φίλιων Δυνάμεων είναι ένας τεχνητός όρος για φορητούς υπολογιστές που φέρονται από προσωπικό, οχήματα, αεροσκάφη ή πλοία και εκπέμπει πληροφορίες στα κέντρα διεύθυνσης επιχειρήσεων. Η ίδια ακριβώς λειτουργία μπορεί να διεκπεραιωθεί δορυφορικά (ιδανικά) ή μέσα από το δίκτυο κινητής τηλεφωνίας (με κάποια μειονεκτήματα κάλυψης και μη αντοχής σε παρεμβολές). Η θέση κάθε μονάδας υπολογιστή στη συνέχεια αποτυπώνεται ως φίλιο (μπλε) σύμβολο στις οθόνες όλων των συνδεδεμένων μονάδων. Έτσι οι Διοικητές Μονάδων του απειλούμενου νησιού ή περιοχής, θα έχουν άμεση εικόνα της φίλιας διάταξης και την ίδια ακριβώς εικόνα θα έχουν τα κέντρα σχεδίασης και συντονισμού των επιχειρήσεων. Θα μπορούν έχοντας κοινή αντίληψη της επιχειρησιακής κατάστασης, να συντονίσουν τα πυρά τους/δυνάμεις τους σε στόχους που μπαίνουν ανάμεσά τους, την αμοιβαία υποστήριξη κλπ. **Συμπερασματικά θα έχουν λιγότερες ανθρώπινες απώλειες και θα είναι πιο οικονομικοί σε κάθε διάσταση στο πεδίο της μάχης.**

Συμπεράσματα

Σκοπός της διπλωματικής αυτής εργασίας ήταν η παρουσίαση και ανάλυση των θεωριών του πληροφοριοκεντρικού και δικτυοκεντρικού δόγματος και εν συνεχεία η εφαρμογή τους στο ελληνικό επιχειρησιακό περιβάλλον. Συμπερασματικά βλέπουμε πως η πληροφοριακή και κατ' επέκταση Δικτυοκεντρική προσέγγιση των στρατιωτικών επιχειρήσεων, αποτελεί μονόδρομο στο εγγύς μέλλον, κυρίως λόγω τον πλεονεκτημάτων που προσφέρουν έναντι των υπόλοιπων συμβατικών επιχειρήσεων όσον αφορά τόσο την εξοικονόμηση ανθρωπίνου δυναμικού όσο και στα θετικά αποτελέσματα που μπορεί να επιφέρει.

Σημειώνεται ότι ο τομέας αυτός των ΕΔ είναι περιορισμένος όσο αφορά δυνατότητα άντλησης, πόσο μάλλον καταγραφής πληροφοριών επί του θέματος. Αυτό οφείλεται πρώτα από όλα, στο ότι είναι μια διαβαθμισμένης αξίας πληροφορία, αλλά και ένα φαινόμενο στην πρώιμη φάση του. Παρόλα αυτά έγινε εφικτή η πρόσβαση σε περιορισμένες πηγές πληροφοριών κυρίως μέσω διαδικτύου ή συνεντεύξεων και περιορισμένης βιβλιογραφίας.

Υπάρχει η πεποίθηση από πολλούς στρατιωτικούς αναλυτές ότι το δόγμα αυτό θα κυριαρχήσει στην μελέτη των στρατιωτικών υποθέσεων για τις επόμενες δεκαετίες και αυτό γιατί αναδεικνύει την άρρηκτη σχέση μεταξύ του πεδίου της μάχης και των τεχνολογικών εφαρμογών.

Ζούμε την εποχή της πληροφορίας. Όποιος την έχει άμεσα, αντιλαμβάνεται την τακτική κατάσταση γρηγορότερα, αποφασίζει και διατάζει γρηγορότερα, δρα γρηγορότερα, με αποτέλεσμα να επιταχύνει το ρυθμό των επιχειρήσεων και να αναγκάζει τον αντίπαλο να χάνει την πρωτοβουλία των κινήσεων.

Η χώρα μας θα συνεχίσει να αντιμετωπίζει την τουρκική απειλή σε όλο το εύρος των ανατολικών συνόρων μας για τις επόμενες δεκαετίες. Η δικτύωση όλων των φίλιων μονάδων που αντιμετωπίζουν την απειλή, με προτεραιότητα όσων αμύνονται των νησιών μας-δρουν στο Αιγαίο, και ο εφοδιασμός τους με Ιχνηλάτη Φίλιων Δυνάμεων θα μειώσει

σημαντικά τα αδελφοκτόνα πυρά και θα αυξήσουν τον συντονισμό και την φονικότητα των πυρών μας διακλαδικά, μειώνοντας τις απώλειές μας.

Γλωσσάριο

ACCS AIR COMMAND CONTROL SYSTEM (Σύστημα Διοίκησης και Ελέγχου Αεροπορικών Επιχειρήσεων)

AAOCC ARMY AIR OPERATION COORDINATION CENTER (Κέντρο Συντονισμού Αεροπορικών Επιχειρήσεων του Στρατού)

AWACS Airborne Warning And Control System (Αερομεταφερόμενα Συστήματα Έγκαιρης Προειδοποίησης και Ελέγχου – ΑΣΕΠΕ)

Airland Battle Συνδυασμένη Μάχη Αεροπορικών και Χερσαίων Δυνάμεων

Battlespace Το περιβάλλον, οι παράγοντες και οι συνθήκες που πρέπει να γίνουν κατανοητοί για να εφαρμοστεί επιτυχώς η μαχητική ισχύς, να προστατευτεί η δύναμη, ή να ολοκληρωθεί η αποστολή. Αυτό περιλαμβάνει τις αεροπορικές, χερσαίες, θαλάσσιες, διαστημικές και τις συμπεριλαμβανόμενες εχθρικές και φιλικές δυνάμεις, εγκαταστάσεις, καιρό, διαμόρφωση εδάφους, το ηλεκτρομαγνητικό φάσμα και το περιβάλλον πληροφοριών μέσα στις επιχειρησιακές περιοχές και τους τομείς ενδιαφέροντος.

BFT Blue Force Tracker (Ιχνηλάτης Φίλιων Δυνάμεων)

C2 Command and Control (Διοίκηση, Έλεγχος)

C4I Command, Control, Communications, Computers and Intelligence(Διοίκηση, Έλεγχος, Επικοινωνίες, Υπολογιστές, Πληροφορίες)

C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (Διοίκηση, Έλεγχος, Επικοινωνίες, Υπολογιστές, Πληροφορίες, Παρακολούθηση και Αναγνώριση)

DOD Department Of Defense (Υπουργείο Άμυνας)

DoS Denial of Service (Άρνηση Παροχής Υπηρεσιών)

GAO Government Accounting Office (Λογιστικό Γραφείο της Κυβέρνησης Η.Π.Α.)

GIG Global Information Grid (Παγκόσμιο Πλέγμα Πληροφοριών) εμπεριέχει το σύνολο των πληροφοριακών δυνατοτήτων, των σχετικών διαδικασιών και του προσωπικού που είναι διασυνδεδεμένα σε παγκόσμια κλίμακα και συλλέγουν, επεξεργάζονται, αποθηκεύουν και διαχειρίζονται τις πληροφορίες, ανάλογα με τις απαιτήσεις των μαχητών, των αρχηγείων και του προσωπικού υποστήριξης. Στο GIG περιλαμβάνονται όλα τα συστήματα και οι υπηρεσίες επικοινωνιών και ηλεκτρονικών υπολογιστών, τα software, τα δεδομένα, και όλες οι υπηρεσίες που απαιτούνται για την επίτευξη Πληροφοριακής Υπεροχής από τις Ένοπλες Δυνάμεις των Η.Π.Α.

GIG-BE Global Information Grid Bandwidth Expansion (Επέκταση Εύρους Ζώνης του Παγκόσμιου Πλέγματος Πληροφοριών)

JTIDS Joint Tactical Information Distribution System (Σύστημα Διανομής Τακτικών Πληροφοριών)

HTML Hyper Text Markup Language

ICT Information and Communication Technologies (Τεχνολογίες Πληροφοριών και Επικοινωνιών)

IP Internet Protocol (Πρωτόκολλο Διαδικτύου)

JHMCS Joint Helmet Mounted Cueing System (Σύστημα Σκόπευσης και Απεικόνισης στην Κάσκα)

NADGE: NATO Air Defence Ground Environment (Επίγειο σύστημα Αεράμυνας του ΝΑΤΟ)

NRDC-GR NATO Rapid Deployable Corps – Greece (Σώμα Ταχείας Ανάπτυξης του ΝΑΤΟ-Ελλάδας)

NCES Network Centric Enterprise Services (Υπηρεσίες Δικτυοκεντρικών Επιχειρήσεων)

NCN Network Centric Nodes (Δικτυοκεντρικοί Κόμβοι)

NCO Network Centric Operations (Δικτυοκεντρικές Επιχειρήσεις)

NCW Network Centric Warfare (Δικτυοκεντρικός Πόλεμος)

NSA National Security Agency (Υπηρεσία Εθνικής Ασφαλείας)

OODA Observe, Orient, Decide, Act (Παρατήρησε, Προσανατόλισε, Αποφάσισε, Δράσε)

RASP Recognized Air Surface Picture (Διευκρινισμένη Εικόνα Αέρος Επιφανείας)

RMA Revolution in Military Affairs (Επανάσταση στις Στρατιωτικές Υποθέσεις)

SA Situational Awareness (Επίγνωση της (Τακτικής) Κατάστασης)

SATCOM Communication Satellite (Δορυφόρος Επικοινωνιών)

SOC SECTOR OPERATION CENTER (Κέντρο Επιχειρήσεων τομέα)

TCP Transmission Control Protocol (Πρωτόκολλο Ελέγχου Εκπομπών)

WWW World Wide Web (Παγκόσμιος Ιστός)

ΕΚΑΕ Εθνικό Κέντρο Αεροπορικών Επιχειρήσεων.

ΣΑΕ Σύστημα Αεροπορικού Ελέγχου

ΣΞ Στρατός Ξηράς

ΠΝ Πολεμικό Ναυτικό

ΠΑ Πολεμική Αεροπορία

ΒΙΒΛΙΟΓΡΑΦΙΑ

Επιστημονικές Αναφορές

"The Battlefield of the Future" - 21st Century Warfare Issues", Air University, Chapter 3, p. 1, Jeffrey McKitrick, James Blackwell, Fred Littlepage, Georges Kraus, Richard Blanchfield and Dale Hill

Steven Metz, James Kievit. "Strategy and the Revolution in Military Affairs: From Theory to Policy" June 27, 1995

Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής» , Λιβάνης, Αθήνα,

Μαρία Μαρκαντωνάτου, «Επανάσταση στις στρατιωτικές υποθέσεις: Από τον πόλεμο χωρίς απώλειες στο πόλεμο κατά της τρομοκρατίας » ,Απρίλιος – Ιούνιος 2010, Τεύχος 111

Network Centric Operations: Background and Oversight Issues for Congress March 15, 2007 Clay Wilson, Specialist in Technology and National Security Foreign Affairs, defence and Trade Division

Chomsky, Noam, «Ο νέος πόλεμος ενάντια στην Τρομοκρατία», Μεταίχμιο, Αθήνα,2002

Sennett, Richard «Αυτή τη φορά μια χώρα αδιαίρετη», στο Σαϊντ, Έντουαρντ (κ.ά.): Η Τρομοκρατία και η Κοινωνία των Πολιτών, Μεταίχμιο, Αθήνα, 2002

Θεοφίλου, Ανδρέας, «Τα Έξυπνα Όπλα του ΝΑΤΟ και η ανθρωπιστική τους δράση στη Γιουγκοσλαβία», Ουτοπία, τεύχος 34, 1999

Géré, Francois, «Γιατί οι Πόλεμοι; Ένας αιώνας Γεωπολιτικής», Παπαζήσης, Αθήνα, 2005

Μάρθα Ε. Παπαδούλη, «Οι επιθέσεις στον κυβερνοχώρο: Τι είναι και ποιους προβληματισμούς δημιουργούν», 2011

Ανχης (ΠΖ) Κωνσταντίνος Χαμεζόπουλος, «Πληροφοριακός πόλεμος και οι στρατιωτικές του εφαρμογές στην αυγή του 21ου αιώνα» ,2010

Γρίβας Κωνσταντίνος,2008, «Το τέλος του πετρελαίου και η αρχή της νέας Αμερικανικής Γεωστρατηγικής» , Λιβάνης, Αθήνα

Congressional Research Service, 'Network Centric Operations: Background and Oversight Issues for Congress' (Washington DC: Congressional Research Service, 2007), Summary.

Ministry of Defence Joint Service Publication 777 Edn 1, «Network Enabled Capability» (London: Ministry of Defence UK, 2005).

John M. Shalikashvili Chairman of the Joint Chiefs of Staff , «Joint Vision 2010» , Pentagon, Washington, έκδοση 1996

David S. Alberts, John J. Garstka, Frederick P. Stein, «Network Centric Warfare» ,έκδοση 2η, 2000

Information Age Transformation: Getting to a 21st Century Military, Washington, DC, CCRP Publications, Πρώτη έκδοση 1996

Owen, Robert C , «Deliberate Force: A Case Study in Effective Air Campaigning», Maxwell AFB, έκδοση 2000

Wentz & Larry K, «Lessons From Bosnia: The IFOR Experience» , Contributing Editor,Larry Wentz, 2007

Michael Ignatieff , «Virtual War: Kosovo and Beyond» Metropolitan Books, Henry Holt and Co., έκδοση 2000

Carlo Kopp, «Network Centric Warfare Textbook», Air Power Australia, 2008

Northtropp Grumman, «Understanding Voice and Data Link Communication», December 2014

Rolald Proersch, «Technical Handbook for Radio Monitoring HF» , Edition 2015

Benjamin S. Lambeth , «NATO's War to Save Kosovo» , Washington, D. C.: Brookings Institution, έκδοση 2000

W. Richard Stevens, «The Protocols TCP/IP Illustrated» , Volume 1

The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress, 17 November 2005

Martin-Baker. «A history of the Joint Strike Fighter Program» , Retrieved April 2011

«Australia To Develop High-Tech Mine System», Defense News (March 1998)

«Future Combat Systems to enter development», Mark Hewish, IDR, Ιούλιος 2003

Στρατηγός Μιχαήλ Κωσταράκος «Διοίκηση με Βάση την Αποστολή». Έκδοση ΓΕΕΘΑ, 2013

David Potts , «THE BIG ISSUE: COMMAND AND COMBAT IN THE INFORMATION AGE»

0Alberts, D.S., (2002), Information Age Transformation: Getting to a 21st Century Military, Washington, DC, CCRP Publications, First published 1996

United States Army (2003). Mission Command: Command and Control of Army Forces. Washington, D.C.: Headquarters, United States Department of the Army, Field Manual No. 6-0

Vassiliou, Marius, David S. Alberts, and Jonathan R. Agre (2015). "C2 Re-Envisioned: the Future of the Enterprise." New York: CRC Press

Congressional Research Service NCO Background and Oversight Issues for Congress

Department of Defense Dictionary of Military and Associated Terms", Joint Publication 1-02, US Department of Defense, 17 March 2009.

John Gordon, "Transforming for What? Challenges Facing Western Militaries Today", Focus stratégique, Paris, Ifri, November 2008.

Alexander, John B., Future War: Non-Lethal Weapons in Twenty-First-Century Warfare, New York, Thomas Dunne Books/St. Martin's Griffin, 1999 ISBN 0-312-26739-8

ΙΣΤΟΣΕΛΙΔΕΣ

www.ultra-cis.com

www.iknowgr.blogspot.de

www.nspa.nato.int

www.fas.org

www.dodccrp.org

www.globalsecurity.org

www.kforcegov.com

www.dtic.mil

www.stratcom.mil

www.bicsi.org

www.rusi.org