Αλγόριθμοι Επιχειρησιακής Έρευνας και Εφαρμογές τους στις Ένοπλες Δυνάμεις

των **κ. Παπαρρίζου Κωνσταντίνου & Σιφαλέρα Άγγελου**

Πανεπιστήμιο Μακεδονίας, Οικονομικών και Κοινωνικών Επιστημών,
Τμήμα Εφαρμοσμένης Πληροφορικής,
Εγνατίας 156, Θεσσαλονίκη Τ.Κ. 540 06,
E-mail: paparriz@uom.gr, sifalera@uom.gr

Περίληψη

Η εργασία αυτή έχει ως στόχο μια σύντομη ενημέρωση στο επιστημονικό πεδίο των Αλγορίθμων και της Επιχειρησιακής Έρευνας (Ε.Ε.). Εφαρμογές της Ε.Ε. συναντώνται σε μια πληθώρα τομέων, όπως είναι η Πληροφορική, οι Τηλεπικοινωνίες, ο Κατασκευαστικός τομέας κ.α. Στην παρούσα εργασία όμως θα εστιάσουμε σε εφαρμογές της Ε.Ε. στο χώρο των Ενόπλων Δυνάμεων. Ακόμη, θα γίνει μια καταγραφή φορέων που ασχολούνται με την Ε.Ε. στο χώρο των στρατιωτικών εφαρμογών και θα τονιστεί η συνεργασία μεταξύ ερευνητικών κέντρων και στρατιωτικών φορέων. Επίσης θα τονιστεί ο σημαντικός ρόλος της μαθηματικής μοντελοποίησης ενός προβλήματος. Τέλος, θα παρατεθούν πολλές πηγές ενημέρωσης σχετικά με την Επιχειρησιακή Έρευνα τόσο σε διεθνή περιοδικά και συνέδρια όσο και σε βιβλία αλλά και φυσικά στο Διαδίκτυο.

Λέξεις κλειδιά: *Αλγοριθμική Επιχειρησιακή Έρευνα, Συνδυαστική Βελτιστοποίηση, Στρατιωτικές Εφαρμογές.*

1. Εισαγωγή

1.1 Εισαγωγή στους αλγορίθμους

Ο άνθρωπος στην καθημερινή του ζωή παίρνει διάφορες αποφάσεις, οι οποίες είτε αφορούν στη δικιά του προσωπική επιχείρηση, είτε σε κάποιο μεγαλύτερο οργανισμό. Για παράδειγμα, ενδιαφέρεται κανείς να βρει την συμφερότερη προσφορά σε αεροπορικά ναύλα, να προσδιορίσει πόσο χώρο υποδοχής χρειάζεται στην επιχείρηση του, να μειώσει τους χρόνους αναμονής σε τηλεφωνικά κέντρα: Πρώτα κάποιος πρέπει να ασχοληθεί με τα μαθηματικά του αντίστοιχου προβλήματος. Το μυστικό για την εύρεση της βέλτιστης λύσης σε κάθε πραγματικό πρόβλημα βρίσκεται στη χρήση αλγορίθμων. Οι αλγόριθμοι βρίσκονται σήμερα παντού, πίσω από οποιαδήποτε απλή ή σύνθετη εφαρμογή. Πίσω από αυτούς, βρίσκονται οι απαντήσεις σχεδόν στα πάντα, από σχεδίαση κυκλωμάτων για μικροεπεξεργαστές μέχρι και τη σχεδίαση βελτιωμένων αεροσκαφών.

Αυτό που οι υπολογιστικές επιστήμες, οι αλγόριθμοι ειδικότερα, προσφέρουν είναι η σημαντική βελτίωση της ακρίβειας των υπολογισμών. Εάν έχουμε αρκετά δεδομένα, οι σημερινοί υπολογιστές είναι αρκετά ισχυροί και γρήγοροι ούτως ώστε να εφαρμόσουμε μαθηματικούς υπολογισμούς για να βρούμε καλύτερους τρόπους για να κάνουμε σχεδόν οτιδήποτε μπορούμε να σκεφτούμε. Οι αλγόριθμοι αποτελούν μια μαθηματική διαδικασία, ένα σύνολο κανόνων που χρησιμοποιούνται για να υπολογίσει κανείς ένα αποτέλεσμα. Υπάρχουν για παράδειγμα επαναληπτικοί αλγόριθμοι, οι οποίοι είναι σε θέση να εκτελούν εκατοντάδες χιλιάδες μικρών βελτιώσεων, έτσι ώστε ο κάθε ένας να βελτιώνει την ακρίβεια του τελικού αποτελέσματος.

Εδώ και πολλά χρόνια συνεργάζονται διάφορες επιχειρήσεις / οργανισμοί με ερευνητικά κέντρα για να επιλύσουν διάφορα δύσκολα προβλήματα από κάθε κλάδο, με τη βοήθεια αλγορίθμων. Ένα πρόσφατο παράδειγμα είναι με δύο ερευνητικές ομάδες από τα Πανεπιστημία McMaster και Waterloo στον Καναδά, τα οποία συνεργάζονται με ογκολόγους ιατρούς του νοσοκομείου Princess Margaret στο Τορόντο, ώστε να υπολογίσουν την βέλτιστη ποσότητα ακτινοβολίας η οποία πρέπει να χρησιμοποιηθεί για τη θεραπεία του καρκίνου στο ήπαρ. Ο στόχος αυτής της

ερευνητικής προσπάθειας είναι να προσδιοριστεί η ακριβής ποσότητα ακτινοβολίας, η οποία είναι η πλέον αποτελεσματική. Είναι αξιοσημείωτο το γεγονός ότι οι ιατροί που συνεργάζονται σε αυτήν την ερευνητική προσπάθεια, δεν κατανοούν τα μαθηματικά που χρησιμοποιούνται, αλλά αυτό δεν είναι απαραίτητο. Οι ιατροί συνεισφέρουν με τις γνώσεις τους στην θεραπεία, ενώ οι επιστήμονες μαθηματικοί συνεισφέρουν με τις γνώσεις τους στα μαθηματικά.

Η ισχύς και η ταχύτητα των σημερινών υπολογιστών βοηθάει έτσι ώστε κάποιες επίπονες από υπολογιστικής απόψεως δουλειές, οι οποίες θα έπαιρναν εξαιρετικά πολύ χρόνο παλαιότερα, σήμερα να είναι θέμα μόνο ορισμένων λεπτών. Σήμερα, χάρην στις υπολογιστικές επιστήμες μπορούμε να εξοικονομήσουμε τεράστια ποσά στη βιομηχανία, να κάνουμε πολύ πιο αποτελεσματική διάγνωση και θεραπεία στην Ιατρική, να σχεδιάσουμε καλύτερα προϊόντα ή να κάνουμε καλύτερη διαχείριση των διαθέσιμων πόρων. Η χρήση μαθηματικών μοντέλων ήδη παίζει σημαντικό ρόλο στις επιχειρήσεις ακόμη και στην στήριξη προσωπικών αποφάσεων. Επιπλέον δε, ένα από τα ωραία χαρακτηριστικά των αλγορίθμων είναι η ευρεία τους εφαρμογή σε ποικίλλους κλάδους όπως ταξιδιωτικές ιστοσελίδες στο διαδίκτυο (π.χ. ο ιστοχώρος www.expedia.ca). Ένας άλλο παράδειγμα δημοφιλή ιστοχώρου είναι και ο http://www.mapquest.com, ο οποίος χρησιμοποιεί αλγορίθμους για να προσδιορίσει τα βέλτιστα δρομολόγια για οδηγούς.

Εν συντομία, ένας αλγόριθμος είναι κάτι παραπάνω από μια μαθηματική εξίσωση. Είναι μια συνταγή ή ένα σύνολο βημάτων ή κανόνων που χρησιμοποιούνται για την επίλυση ενός προβλήματος. Μπορεί να είναι από μία απλή συνταγή μαγειρικής (όσο παράξενο και αν φαίνεται) έως κάτι τόσο περίπλοκο όσο και οι διαδικασίες που ακολουθούνται για την προσγείωση ενός οχήματος σε άλλον πλανήτη. Κάθε αλγόριθμος έχει κάποιες ιδιότητες. Σε γενικές γραμμές, δέχεται κάποια δεδομένα εισόδου και παράγει κάποια δεδομένα εξόδου. Εκτελείται με κάποια σειρά πεπερασμένων βημάτων, με τα αποτελέσματα κάθε βήματος να καθορίζονται μόνο από τα δεδομένα εισόδου και εξόδου κάποιου προηγούμενου βήματος. Πρέπει ακόμη να σημειωθεί, ότι κάθε αλγόριθμος έχει ένα σαφή τρόπο για να σταματάει τους υπολογισμούς. Επιπρόσθετα δε, η χρήση των αλγορίθμων ποικίλλει από την ανάλυση των τάσεων στο χρηματιστήριο μέχρι την δημιουργία των γνωστών Sudoku πάζλ, κ.α. Το λογισμικό των υπολογιστών είναι στην ουσία κάποιοι σύνθετοι αλγόριθμοι. Για παράδειγμα για να οξυνθούν τα χρώματα σε μια ψηφιακή φωτογραφία, εφαρμόζεται ένας αλγόριθμος σε κάθε εικονοστοιχείο της για να προσδιορίσει τον τρόπο αλλαγής του κάθε εικονοστοιχείου ώστε να γίνει πιο κρυστάλλινη η εικόνα. Αξίζει να αναφερθεί ότι, η λέξη αλγόριθμος προέρχεται από το όνομα ενός Πέρση Μαθηματικού Al-Khwarizmi, που έζησε στη Βαγδάτη τον 9ο αιώνα. Τέλος, πολύ καλές πηγές για τη μελέτη σε θέματα αλγορίθμων είναι τα βιβλία [1] και [2].

1.2 Εισαγωγή στην Επιχειρησιακή Έρευνα

Η Επιχειρησιακή Έρευνα (Operations research, Operational research, ή εν συντομία OR) αποτελεί ένα επιστημονικό πεδίο στο οποίο εφαρμόζουμε προχωρημένες αναλυτικές μεθόδους για να πάρουμε τις καλύτερες αποφάσεις. Για να πάρουμε τις βέλτιστες αποφάσεις γίνεται χρήση πολλών άλλων επιστημονικών πεδίων και μεθόδων, όπως τα παρακάτω:

- *Βελτιστοποίηση*. Περιορίζονται οι επιλογές μόνο στις καλύτερες εξ' αυτών όταν υπάρχουν αναρίθμητες εφικτές επιλογές και η σύγκριση όλων των περιπτώσεων είναι δύσκολη,
- *Προσομοίωση*. Δίνει τη δυνατότητα να δοκιμαστούν διάφορες προσεγγίσεις και ιδέες για βελτίωση,
- *Πιθανότητες και Στατιστική*. Βοηθάνε

στην εκτίμηση του ρίσκου, στην εξόρυξη δεδομένων για την εύρεση χρήσιμων σχέσεων και πληροφοριών, έλεγχο συμπερασμάτων, καθώς και χρήσιμων προβλέψεων.

Ιστορικά, ο όρος "Επιχειρησιακή Έρευνα" προέρχεται από την έρευνα των πολεμικών επιχειρήσεων κατά τον Β΄ Παγκόσμιο Πόλεμο. Διάφορα κράτη ερίζουν για την "πατρότητα" αυτής της Επιστήμης. Η εκδοχή της Μ. Βρετανίας αναφέρει την μάχη της Αγγλίας ως την πρώτη ευρεία εφαρμογή της Ε.Ε. Ένας από τους πιο γνωστούς Βρετανούς επιστήμονες κατά τη διάρκεια του Β' Παγκόσμιου Πολέμου ήταν ο Alan Turing, ο οποίος εκείνη την εποχή, μαζί και με άλλους Μαθηματικούς, εργάζονταν στο ερευνητικό κέντρο Bletchley Park. Ο Alan Turing έγινε μετέπειτα διάσημος για την αποκρυπτογράφηση της μηχανής "ΑΙΝΙΓΜΑ" των Γερμανών και την τεράστια συμβολή αυτής της αποκρυπτογράφησης στη νίκη των Συμμάχων.

Σύμφωνα με μια άλλη εκδοχή, αυτή των Ηνωμένων Πολιτειών Αμερικής (Η.Π.Α.), η απόβαση στην Νορμανδία (ή αλλιώς η D-Day όπως έμεινε στην ιστορία) την 06/06/1944, αναφέρεται ως η πρώτη ευρεία εφαρμογή της Ε.Ε. Ένας από τους πιο γνωστούς Αμερικανούς επιστήμονες κατά τη διάρκεια του Β' Παγκόσμιου Πολέμου ήταν ο George B. Dantzig, ο οποίος εκείνη την εποχή εργαζόνταν στην εταιρία RAND Corporation. Σήμερα, ολόκληρη η επιστημονική κοινότητα της Ε.Ε. αναγνωρίζει τον George B. Dantzig ως τον "Πατέρα" της Ε.Ε. για την μεγάλη του συνεισφορά και ειδικότερα για την ανακάλυψη του αλγόριθμου Simplex για το Γραμμικό Προγραμματισμό το 1947. Είναι αξιοσημείωτο το γεγονός ότι ο αλγόριθμος Simplex κρατήθηκε αρχικά ως στρατιωτικό μυστικό και δημοσιεύτηκε σε περιοδικό δύο χρόνια αργότερα με την εργασία [3]. Μία εξήγηση του γεγονότος αυτού που υιοθετείται από πολλούς είναι η εξής. Την εποχή εκείνη υπήρχε έντονος ανταγωνισμός μεταξύ Η.Π.Α. και Ε.Σ.Σ.Δ. και όταν οι Η.Π.Α. είχαν πληροφορίες ότι και η Ε.Σ.Σ.Δ. πλησίαζε στην ανακάλυψη ενός τέτοιου επιστημονικού επιτεύγματος δημοσιοποιήσαν στην επιστημονική κοινότητα τον αλγόριθμο Simplex για να τους αναγνωριστεί αυτή η ανακάλυψη.

Ο αλγόριθμος του Dantzig θεωρείται ότι είναι από τους πιο επιτυχημένους όλων των εποχών. Συγκεκριμένα ο αλγόριθμος Simplex επιλύει προβλήματα Γραμμικού Προγραμματισμού τα οποία εμφανίζονται σε όλους σχεδόν τους τομείς, στους οποίους η οικονομική επιβίωση εξαρτάται από την ικανότητα βελτιστοποίησης υπο κάποιους περιορισμούς στο κεφάλαιο ή στο εργατικό δυναμικό ή στους διαθέσιμους πόρους. Η μέθοδος Simplex είναι ένας απλός τρόπος για τον υπολογισμό της βέλτιστης λύσης με ενδιαφέρουσα γεωμετρική απόδειξη ορθότητας. Παρ' όλο που θεωρητικά είναι επιρρεπής σε εκθετική συμπεριφορά, δηλαδή υπάρχει πιθανότητα να καθυστερήσει υπερβολικά να δώσει τη λύση, ο αλγόριθμος είναι αρκετά αποτελεσματικός (ταχύς) στην πράξη. Αξίζει να αναφερθεί ότι ο αλγόριθμος Simplex θεωρείται σήμερα ως μια από τις δέκα πιο σημαντικές ανακαλύψεις στο χώρο της Επιστήμης των Υπολογιστών, όπως φαίνεται και στη μελέτη που δημοσιεύθηκε στο τεύχος Ιανουαρίου/Φεβρουαρίου 2000 του περιοδικού Computing in Science & Engineering [4], μια κοινή έκδοση του Αμερικανικού Ινστιτούτου Φυσικής και της Επιστημονικής Ένωσης Μηχανικών Υπολογιστών IEEE.

Πολύ περιληπτικά κάποιοι από τους πιο σημαντικούς σταθμούς στην Επιχειρησιακή Έρευνα και συγκεκριμένα τον Γραμμικό Προγραμματισμό είναι οι εξής. Τις δεκαετίες '50 και '60 δημοσιεύτηκαν εργασίες με υπολογιστικά αποτελέσματα και η έρευνα είχε στραφεί προς τον υπολογισμό της πρακτικής αποτελεσματικότητας του αλγορίθμου Simplex. Είχε φανεί ότι ο αλγόριθμος Simplex παρουσίαζε προβλήματα χρόνου στην επίλυση μεγάλων προβλημάτων. Ένα ανοιχτό ερευνητικό πρόβλημα της εποχής εκείνης σχετικά με την ανάλυση πολυπλοκότητας του αλγορίθμου simplex απαντήθηκε από τους Klee-Minty το 1972 [5], οι οποίοι απέδειξαν

ότι ο αλγόριθμος έχει εκθετική συμπεριφορά στη χειρότερη περίπτωση. Έτσι η έρευνα στράφηκε προς την κατεύθυνση της ανάπτυξης ενός πολυωνυμικού αλγορίθμου. Ένα πρώτο σημαντικό βήμα προς αυτήν την κατεύθυνση, ήταν και η ανακάλυψη του ελλειψοειδής ή ρωσικού αλγορίθμου το 1979 από τον Khachian [6]. Μερικά χρόνια αργότερα, το 1984, ένας άλλος ερευνητής ονόματι Karmarkar ανεκάλυψε έναν πολυωνυμικό αλγόριθμο εσωτερικών σημείων (ΑΕΣ), βλέπε εργασία [7]. Μάλιστα, είχε υπολογίσει ότι σε συγκεκριμένου τύπου προβλήματα μεγάλης διάστασης, ο αλγόριθμος του ήταν περίπου 50 φορές ταχύτερος του αλγορίθμου Simplex. Αξίζει να αναφερθεί το γεγονός ότι, τα εργαστήρια Bell Labs, όπου δούλευε εκείνη την εποχή ο Karmakar, υλοποίησαν τον (ΑΕΣ) στο λύτη KORBX (μια υπολογιστική πλατφόρμα εκείνης της εποχής) και πούλησαν τρείς άδειες χρήσης του λογισμικού το 1989, προς 8.900.000$ στο Αμερικανικό Ναυτικό, στην Αμερικανική Αεροπορία και στην Αμερικανική αεροπορική εταιρία US Delta Airlines. Παρ' όλα αυτά ο αλγόριθμος Simplex παραμένει μέχρι και σήμερα η πρώτη επιλογή για επίλυση προβλημάτων γραμμικού προγραμματισμού και αυτό διότι ενώ εχει κακή θεωρητική πολυπλοκότητα παρουσιάζει καλή υπολογιστική συμπεριφορά. Μάλιστα, το 1982 ο ερευνητής Borgwardt στην εργασία [8] απέδειξε ότι ο αλγορίθμος Simplex είναι πολυωνυμικός ως προς το πλήθος των επαναλήψεων, στη μέση περίπτωση.

Τέλος πρέπει να σημειωθεί ότι το 1991 ανακαλύφθηκε και μια νέα κατηγορία αλγόριθμων τύπου Simplex Εξωτερικών Σημείων από τον Καθ. κ. Παπαρρίζο Κ., για το πρόβλημα της αντιστοίχισης με την εργασία [9]. Οι αλγόριθμοι εξωτερικών σημείων αποδίδουν καλύτερα από τον κλασικό αλγόριθμο Simplex σε τυχαία γραμμικά προβλήματα μεγάλης διάστασης. Επίσης, αλγόριθμοι εξωτερικών σημείων έχουν κατασκευαστεί και για άλλου τύπου προβλήματα της Συνδυαστικής Βελτιστοποίησης, όπως είναι το Πρόβλημα Ροής Ελαχίστου Κόστους, βλέπε [10].

Για μια πολύ πιο αναλυτική μελέτη της ιστορίας της Επιχειρησιακής Έρευνας, μπορεί κανείς να ανατρέξει στο βιβλίο [11]. Τέλος, πολύ καλή πηγή για μελέτη θεμάτων Επιχειρησιακής Έρευνας αποτελεί το βιβλίο [12].

2. *Εφαρμογές της Επιχειρησιακής Έρευνας στις Ένοπλες Δυνάμεις*

Υπάρχει μια μεγάλη πληθώρα εφαρμογών της Επιχειρησιακής Έρευνας, αλλά και των αλγορίθμων γενικότερα, στο χώρο των Ενόπλων Δυνάμεων και ενδεικτικά μπορούν να αναφερθούν οι παρακάτω εφαρμογές.

- Βέλτιστη Κατανομή Περιορισμένων Πόρων, *(Γραμμικό Πρόβλημα)*
- Διαχείριση Ανθρώπινου Δυναμικού, *(Πρόβλημα Αντιστοίχισης)*
- Πρόβλημα Μεταφοράς Υλικών και Εφοδίων, *(Πρόβλημα Μεταφοράς, Ροής Ελάχιστου Κόστους, Ελάχιστων Δρόμων)*
- Κρυπτογράφηση/Αποκρυπτογράφηση, *(χρήση της Θεωρίας Αριθμών)*,
- Παρακολούθηση Στόχων,
- κ.α.

Όλες οι παραπάνω εφαρμογές, αρχικά μοντελοποιούνται με τη βοήθεια μαθηματικών μοντέλων και έπειτα επιλύονται. Στη παρούσα εργασία δεν θα επεκταθούμε στην μοντελοποίηση, αφού στόχος είναι κυρίως να γίνει μια καταγραφή των στρατιωτικών εφαρμογών Επιχειρησιακής Έρευνας. Παρ' όλα αυτά, στην παρακάτω λίστα μέσα σε παρένθεση αναγράφεται το αντίστοιχο μαθηματικό μοντέλο που χρησιμοποιείται σε κάθε περίπτωση.

Ειδικά στο χώρο των Ενόπλων Δυνάμεων η ασφάλεια της μετάδοσης πληροφοριών έχει βαρύνουσα σημασία. Άλλωστε είναι γνωστή η καταλυτικής σημασία στον Β' παγκόσμιο πόλεμο, συνεισφορά του Alan Turing στην αποκρυπτογράφηση της συσκευής "Αίνιγμα". Ως εκ τούτου θα δοθεί ένα

παράδειγμα από το χώρο της εφαρμογής αλγορίθμων στην κρυπτογραφία και συγκεκριμένα ο γνωστός αλγόριθμος RSA.

Έστω ότι το ΓΕΣ θέλει να στείλει το μήνυμα Χ στο Δ' Σώμα Στρατού (ή εν συντομία Δ' Σ.Σ.). Για λόγους απλούστευσης, ας θεωρήσουμε ότι το μήνυμα αποτελείται μόνο από τον ένα χαρακτήρα Χ. Αντί του χαρακτήρα Χ θα στείλει την αντίστοιχη συμβολοσειρά ASCII, δηλαδή τον αριθμό 1011000 του δυαδικού συστήματος αρίθμησης. Αυτός ο αριθμός του δυαδικού συστήματος, είναι ο αριθμός M = 88 στο δεκαδικό σύστημα αρίθμησης. Το Δ' Σ.Σ. έχει δημοσιοποιήσει το δημόσιο κλειδί του, το οποίο αποτελείται από τους δυο αριθμούς e = 7 και N = 187. Το Δ' Σ.Σ. γνωρίζει και δυο πρώτους αριθμούς p = 17 και q = 11, για τους οποίους ισχύει N = p*q. Οι αριθμοί p και q είναι μυστικοί και τους γνωρίζει μόνο το Δ'Σ.Σ., ούτε καν το ΓΕΣ. Το ΓΕΣ λοιπόν, παίρνει τους αριθμούς e και N (δημόσιο κλειδί του Δ'Σ.Σ.) και υπολογίζει τον αριθμό:

$$C = Me(\text{mod } N) = 11$$

Το ΓΕΣ στέλνει τον αριθμό C = 11, το οποίο είναι το κρυπτογραφημένο μήνυμα, στο Δ'Σ.Σ. Εννοείται ότι το 11 μπορεί να το υποκλέψει οποιοσδήποτε. Το ζητούμενο είναι για το Δ'Σ.Σ. πως να αποκρυπτογραφήσει το μήνυμα. Μόλις το Δ'Σ.Σ. λάβει το μήνυμα, για να το αποκρυπτογραφήσει χρησιμοποιεί το ιδιωτικό του κλειδί d (κρυφό) το οποίο προκύπτει από την παρακάτω σχέση:

$$e*d = 1 \text{ mod}((p - 1)*(q - 1)) \quad \text{ή}$$

$$e*d = 1 \text{ mod } 160,$$

οπότε παίρνουμε ότι d = 23. Τώρα λοιπόν υπολογίζει τον αριθμό:

$$C^d(\text{mod } N) = 88$$

και χρησιμοποιώντας την ASCII κωδικοποίηση γνωρίζει ότι το 88 είναι ο χαρακτήρας Χ. Προκύπτει όμως ένα ενδιαφέρον ερώτημα. Γιατί κανένας άλλος, εκτός από το Δ'Σ.Σ. δεν μπορεί να αποκρυπτογραφήσει το μήνυμα του ΓΕΣ ακόμα και αν το υποκλέψει; Η απάντηση είναι η εξής. Αν κάποιος δεν γνωρίζει τους πρώτους αριθμούς p και q είναι πολύ δύσκολο (χρονοβόρο) να τους υπολογίσει. Στην πράξη το δημόσιο κλειδί N έχει τουλάχιστον 1000 ψηφία. Ένα άλλο ερώτημα είναι το κατά πόσο είναι σίγουρο ότι το Δ'Σ.Σ. θα αποκρυπτογραφεί πάντοτε σωστά το μήνυμα. Η απάντηση στο ερώτημα αυτό στηρίζεται στο παρακάτω αποτέλεσμα που απέδειξαν οι ερευνητές Rivest, Shamir και Adleman το 1978, στην εργασία [13]:

Θεώρημα 1. Έστω p, q, e πρώτοι αριθμοί και d, N αριθμοί τέτοιοι ώστε να ισχύει:

$$e * d = 1[\text{mod } (p-1) * (q-1)] \text{ και } N = p * q$$

Τότε θα ισχύει:

$$M^e \text{ mod } N = C^d \text{ mod } N$$

όπου M, N, C είναι θετικοί ακέραιοι αριθμοί.

Ειδικά κατά τον Β' Παγκόσμιο Πόλεμο υπήρξαν πολλές εφαρμογές αλγορίθμων της Επιχειρησιακής Έρευνας. Μία από αυτές ξεκινά το 1935, μετά την ανακάλυψη του ραντάρ. Η Βρετανική Αεροπορία είχε την ανάγκη να σχεδιάσει τη στρατηγική της σχετικά με τον εντοπισμό των Γερμανικών αεροπλάνων μέχρι και την αναχαίτιση τους. Για την ακρίβεια, το πρόβλημα που έπρεπε να επιλύσει ήταν ο υπολογισμός του ελάχιστου αριθμού ραντάρ καθώς και της βέλτιστης τοποθέτησης τους σε φίλιο έδαφος, για τη μεγιστοποίηση του εύρους που σαρώνεται για την ύπαρξη εχθρικών αεροσκαφών, αλλά και με την ελαχιστοποίηση του κόστους.

Μία ακόμη εφαρμογή ήταν ο έγκαιρος εντοπισμός και καταστροφή των εχθρικών υποβρυχίων, όπου φαίνεται από διάφορες πηγές [14] ότι η αποτελεσματικότητα στην αρχή του πολέμου ήταν 1% ενώ αργότερα με την εφαρμογή μεθόδων Ε.Ε. υπήρχε

αποτελεσματικότητα (lethality per attack) σε ποσοστό 40%. Άλλες εφαρμογές ήταν ο προσδιορισμός του βέλτιστου μεγέθους των νηοπομπών, η βέλτιστη κατανομή στρατιωτικών μονάδων, κ.α. Πολύ γνωστή είναι και η ομάδα που αναπτύχθηκε από τον επιστήμονα Φυσικό Blacket P.M.S. (ο οποίος τιμήθηκε και με βραβείο Nobel) για τις ανάγκες του νυχτερινού πολέμου κατά το φθινόπωρο του 1940, η οποία έμεινε γνωστή ως "το τσίρκο του Blackett". Για περισσότερες πληροφορίες όσον αφορά την συνεισφορά του Blacket P.M.S. στην Επιχειρησιακή Έρευνα, μπορεί κανείς να μελετήσει το άρθρο [15].

Οι πρώτες ομάδες Επιχειρησιακής Έρευνας εμφανίστηκαν στον Αμερικανικό και Καναδικό Στρατό τον Οκτώβριο του 1942. Εκτιμάται ότι οι τρείς στρατοί (Βρετανικός, Αμερικανικός και Καναδικός) απασχολούσαν περίπου 700 άτομα επιστημονικού προσωπικού στις ομάδες επιχειρησιακής έρευνας τους. Πρέπει να αναφερθεί ότι, δεν υπάρχουν ενδείξεις μέχρι σήμερα, για ύπαρξη τέτοιων εξειδικευμένων επιστημονικών ομάδων. Οι τεχνικές της Επιχειρησιακής Έρευνας βοήθησαν σημαντικά τους Συμμάχους να αντιμετωπίσουν τις δυνάμεις του Άξονα στις αρχές της δεκαετίας του 1940. Μια ενδιαφέρουσα πηγή ενημέρωσης για την εφαρμογή μεθόδων Επιχειρησιακής Έρευνας σε πολεμικές επιχειρήσεις, ειδικά στην Μεγάλη Βρετανία είναι και το βιβλίο του Kirby [16], ενώ αρκετά αναλυτικό είναι και το άρθρο του Rau [17].

Επίσης κάποιες πιο σύγχρονες εφαρμογές είναι η εύρεση βέλτιστου τρόπου ρίψης ειδικών συσκευών - αισθητήρων σε εχθρικό έδαφος για την επικάλυψη περιοχής μεγίστου εμβαδού, όπου θα διεξαχθούν πιθανώς μάχες. Το ζητούμενο είναι με ποια σειρά πρέπει να ενεργοποιούνται οι αισθητήρες, ώστε όταν θα απενεργοποιούνται κάποιοι, ταυτόχρονα να ενεργοποιούνται κάποιοι άλλοι και να εξακολουθούν να καλύπτουν για το μέγιστο χρονικό διάστημα κάποια περιοχή.

3. Επιστημονικοί φορείς Στρατιωτικής Επιχειρησιακής Έρευνας

3.1. Διεθνείς

Ένας από τους πιο γνωστούς διεθνείς επιστημονικούς φορείς Στρατιωτικής Επιχειρησιακής Έρευνας, είναι η Military Applications Society (ή εν συντομία MAS). Η MAS είναι μια ομάδα ειδικού ενδιαφέροντος της επιστημονικής κοινότητας Institute for Operations Research and the Management Sciences (ή εν συντομία INFORMS), των ΗΠΑ.

Ένας άλλος επίσης γνωστός διεθνής επιστημονικός φορέας Στρατιωτικής Επιχειρησιακής Έρευνας, είναι η Military Operations Research Society (ή εν συντομία MORS) η οποία βοήθησε σημαντικά το Υπουργείο Αμύνης των ΗΠΑ για περισσότερο από σαράντα χρόνια. Η συγκεκριμένη επιστημονική κοινότητα έλαβε πολλές επιχορηγήσεις από τον Αμερικανικό Στρατό, Ναυτικό, Αεροπορία, Σώμα Πεζοναυτών, και άλλους φορείς για τη διεξαγωγή έρευνας αιχμής. Ο στόχος της MORS είναι η προώθηση της ποιότητας και αποτελεσματικότητας της Στρατιωτικής Επιχειρησιακής Έρευνας. Στα μέλη της MORS συμπεριλαμβάνονται στρατιωτικοί αναλυτές και διευθύνοντα στελέχη από την κυβέρνηση, βιομηχανία και ακαδημαϊκά ιδρύματα. Η ενασχόληση τους βοηθάει στην ανταλλαγή τεχνογνωσίας και πληροφοριών με την στρατιωτική κοινότητα.

Επιχειρησιακής Έρευνας σε ενδιαφέροντα θέματα εθνικής ασφάλειας και στήριξης αποφάσεων σε πολλούς οργανισμούς Τέλος, πρέπει να σημειωθεί το γεγονός ότι η MORS διοργανώνει σε τακτά χρονικά διαστήματα συνέδρια, όπως επίσης εκδίδει διάφορα βιβλία και περιοδικά, ούτως ώστε να ενημερώνονται τα μέλη της στο ευρύ φάσμα των σταρτιωτικών εφαρμογών από εξέχοντες στρατιωτικούς αναλυτές και επιστήμονες επιχειρησιακούς ερευνητές.

Ακόμη, υπάρχει και το Defense Technical Information Center (DTIC), ένας φορέας των ΗΠΑ που ασχολείται με την προβολή της έρευνας και ανάπτυξης στον

αμυντικό τομέα. Στο δικτυακό του ιστοχώρο (http://www.dtic.mil), μπορεί κανείς να βρεί τεχνικές αναφορές (ή και μεταπτυχιακές θέσεις φοιτητών της σχολής Naval Postgraduate School στο Monterey της California) για την προώθηση της στρατιωτικής έρευνας.

3.2. *Ελληνικοί*

Στην Ελλάδα, προς το παρόν, δεν υπάρχει κάποια ομάδα Επιχειρησιακής Έρευνας που να ασχολείται αποκλειστικά με στρατιωτικές εφαρμογές. Όμως, υπάρχουν θεσμοθετημένοι φορείς έρευνας και τεχνολογίας εποπτευόμενοι του Υπουργείου Εθνικής Αμύνης. Σε αυτήν την ενότητα θα αναφερθούν κάποιοι Ελληνικοί αντίστοιχοι φορείς, όμως πρώτα πρέπει να περιγραφεί το πλαίσιο στρατιωτικής έρευνας και τεχνολογίας στην Ελλάδα.

Κάποιοι από τους πρωταρχικούς στόχους του Υπουργείου Εθνικής Αμύνης, είναι η διασφάλιση της βιωσιμότητας και η αύξηση της ανταγωνιστικότητας των ελληνικών αμυντικών βιομηχανιών και παράλληλα η ενθάρρυνση της ανάπτυξης και παραγωγής προϊόντων στα οποία ενσωματώνονται και τεχνολογίες διπλής χρήσης (εμπορικού - στρατιωτικού τύπου). Τα αρμόδια όργανα του Υπουργείου Εθνικής Αμύνης, είναι η Γενική Γραμματεία Οικονομικού Σχεδιασμού και Αμυντικών Επενδύσεων και η Γενική Διεύθυνση Αμυντικής Βιομηχανίας και Έρευνας (ΓΓΟΣΑΕ/ΓΔΑΒΕ).

Όπως φαίνεται και στην επίσημη ιστοσελίδα του Υπουργείου [18] σχετικά με την έρευνα και τεχνολογία, κάποιοι από τους κύριους άξονες δράσεις αυτών των αρμοδίων οργάνων του Υπουργείου που υποστηρίζουν τους παραπάνω στόχους του Υπουργείου, είναι οι παρακάτω:

i. Ο συστηματικός σχεδιασμός της έρευνας για την ανάπτυξη αμυντικής τεχνολογίας και η υλοποίηση ερευνητικών - αναπτυξιακών προγραμμάτων που εντάσσονται σε τομείς υψηλής επιχειρησιακής προτεραιότητας καθώς και η αυστηρή τήρηση ενός χρονο-διαγράμματος υλοποίησης για τη διασφάλιση της ανάπτυξης σε βάθος χρόνου.
ii. Η αξιοποίηση των αποτελεσμάτων της έρευνας σε πρώτη φάση για την ανάπτυξη αμυντικού υλικού και τεχνολογιών υποστήριξης σε κρίσιμους τομείς και σε δεύτερη φάση στην προσαρμογή τους σε προϊόντα ή και υπηρεσίες διπλής χρήσης.
iii. Συντονισμός των φορέων σχεδιασμού - προγραμματισμού - έρευνας - ανάπτυξης και παραγωγής και η επίτευξη της μέγιστης δυνατής συνέργιας δράσεων για την ανάπτυξη αμυντικών τεχνολογιών με έγκαιρη διάχυση και εφαρμογή των αποτελεσμάτων της έρευνας στην αμυντική Βιομηχανία.
iv. Η αξιοποίηση καινοτόμων ιδεών ανάπτυξης νέων τεχνικών ή μεθόδων διπλής χρήσεως (στρατιωτικού - εμπορικού τύπου).

Σύμφωνα και με τις τάσεις στον λοιπό εθνικό και διεθνή χώρο, αποφασίστηκε ότι πρέπει να συγχωνευθούν τα ερευνητικά κέντρα του Υπουργείου Εθνικής Αμύνης στο ενιαίο Κέντρο Έρευνας και Τεχνολογίας Εθνικής Αμύνης (ΚΕΤΕΘΑ) και να εναρμονιστεί το θεσμικό πλαίσιο της έρευνας στην αμυντική τεχνολογία. Επιπλέον, επιδιώκεται η συστηματική και στενότερη συνεργασία των εθνικών ερευνητικών κέντρων και των πανεπιστημιακών ιδρυμάτων με τους φορείς διεξαγωγής της έρευνας του ΥΠΕΘΑ. Προς αυτήν την κατεύθυνση, γίνεται προσπάθεια να δοθεί έμφαση στην ανάπτυξη της εγχώριας ερευνητικής και εργαστηριακής υποδομής, σε ανθρώπινο δυναμικό, υλικοτεχνικά μέσα και εξασφάλιση πόρων για την έρευνα.

Επιπλέον δε, το 1996 ιδρύθηκε το Ινστιτούτο Αμυντικών Αναλύσεων (ΙΑΑ) το οποίο είναι εποπτευόμενο από το Υπουργείο Εθνικής Αμύνης και άρχισε να λειτουργεί εντός του 1998. Η χρηματοδότησή του προέρχεται κυρίως από το Υπουργείο Εθνικής Αμύνης, ενώ μέρος των λειτουργικών του εξόδων καλύπτεται από τις εκδόσεις και τη συμμετοχή του σε εθνικά και

ευρωπαϊκά ερευνητικά προγράμματα.

Σύμφωνα και με την επίσημη ιστοσελίδα του ΙΑΑ [19], σκοπός του ΙΑΑ είναι η παροχή, αποκλειστικά στον ΥΕΘΑ, απόψεων ή γνωμών σε θέματα αμυντικής πολιτικής και εξοπλισμών και ειδικότερα η επιστημονική υποβοήθηση και προβολή του έργου του επί θεμάτων εθνικής αμυντικής και στρατηγικής πολιτικής στο πλαίσιο των διεθνών σχέσεων και της γεωπολιτικής. Τέλος το Ινστιτούτο Αμυντικών Αναλύσεων παρέχει στον ΥΕΘΑ αναλύσεις, εκτιμήσεις και γνωμοδοτήσεις επί θεμάτων που άπτονται της εθνικής άμυνας, εκπονεί μελέτες, διεξάγει επιστημονικές έρευνες και συμμετέχει σε εθνικά και ευρωπαϊκά προγράμματα για θέματα αμυντικής πολιτικής και βιομηχανίας, νέων τεχνολογιών, στρατηγικής ανάλυσης, διεθνών σχέσεων και γεωπολιτικής.

Αξίζει να αναφερθεί ότι οι εργασίες του ΙΑΑ συντάσσονται από ειδικούς επιστήμονες, αξιωματικούς των Ενόπλων Δυνάμεων και επιστημονικά ιδρύματα από την Ελλάδα και το εξωτερικό. Χαρακτηριστικά αναφέρουμε ότι το ΙΑΑ εκδίδει μια τετραμηνιαία επιστημονική επιθεώρηση "Γεωστρατηγική" ενώ επίσης διοργανώνει και διεθνή συνέδρια, όπως για παράδειγμα το Διεθνές Συνέδριο Χειρισμού Κρίσεων
"Αθηνά ΄07".

4. *Πηγές ενημέρωσης*

Έχουν κυκλοφορήσει κάποια αξιόλογα βιβλία από την επιστημονική κονότητα της MORS, όπως είναι για παράδειγμα το βιβλίο Methods for Conducting Military Operational Analysis με εκδότες τους Andrew G. Loerch και Larry B. Rainey [20] το 2007. Αυτή η συγγραφική προσπάθεια αποτελεί μια συλλογή εργασιών που προωθεί την Επιχειρησιακή Έρευνα σε στρατιωτικές εφαρμογές. Περιλαμβάνει αρκετά πρόσφατες μεθόδους, εφαρμογές και μελέτες περιπτώσεων που αφορούν σε ανοιχτά ερευνητικά προβλήματα της στρατιωτικής Επιχειρησιακής Έρευνας.

Μία ακόμη ενδιαφέρουσα πηγή ενημέρωσης είναι το βιβλίο Predicting Combat Effects από τον Hartley D.S. III το 2001 [21], της σειράς Topics in Operations Research Series (http://topicsinor.pubs.informs.org/titles.htm). Αυτό το βιβλίο αναλύει μια πληθώρα ιστορικών μαχών και προσπαθεί να προσδιορίσει κατά πόσον υπάρχει κάποιος μαθηματικός τύπος βάσει του οποίου να γίνεται πρόγνωση για το αποτέλεσμα κάποιας μάχης. Τα αποτελέσματα που εξάγονται για μαθηματικά μοντέλα μαχών ενσωματώνονται σε λογιστικά φύλλα εργασίας (spreadsheet battle model), τα οποία προσπαθούν να συνυπολογίσουν διάφορες πιθανές παραμέτρους. Πρέπει να αναφερθεί ότι το συγκεκριμένο βιβλίο περιλαμβάνει και συνοδευτικό CD με όλα τα στοιχεία των μαθηματικών μοντέλων που χρησιμοποιούνται καθώς και των δεδομένων.

Τέλος, πάλι από την επιστημονική κονότητα της MORS και την σειρά Topics in Operations Research Series, υπάρχει και το βιβλίο Modern Combat Models: A Critique of Their Foundations των Ancker C.J. και Gafarian Jr. & A.V. το 1992 [22]. Το βιβλίο αυτό εξετάζει διάφορα μοντέλα πολεμικών μαχών, τις υποθέσεις τους, την αποτελεσματικότητά τους, καθώς και τις σχέσεις τους. Συγκεκριμένα ασχολείται με τα μοντέλα (models of combat) Lanchester, Stochastic Lanchester καθώς και με το Generalized Renewal.

Τέλος, το Institute for Operations Research and the Management Sciences, (INFORMS) (www.informs.org) εκδίδει συχνά συγκριτικές αξιολογήσεις για λογισμικά πακέτα στην Επιχειρησιακή Έρευνα. Αυτές οι αξιολογήσεις μπορεί να φανούν πολύ χρήσιμες σε κάποιον ιδιώτη/οργανισμό ο οποίος ενδιαφέρεται να αγοράσει κάποιο εξειδικευμένο λογισμικό Ε.Ε., απο τη στιγμή που τα περισσότερα απο τα εμπορικά λογισμικά πακέτα συνήθως είναι πολύ ακριβά. Συγκεκριμένα το περιοδικό OR/MS Today έχει εκδώσει τις παρακάτω συγκριτικές μελέτες για λογισμικά πακέτα διαφόρων υπο-περιοχών της Επιχειρησιακής Έρευνας:

Ανάλυση Αποφάσεων (Decision Analysis), OR/MS Today, Δεκέμβριος 2006 http://lionhrtpub.com/orms/surveys/das/das.html

Δρομολόγηση Οχημάτων, (Vehicle Routing), OR/MS Today, Ιούνιος 2006. http://lionhrtpub.com/orms/surveys/Vehicle_Routing/vrss.html

Γραμμικό Προγραμματισμό, (Linear Programming), OR/MS Today, Ιούνιος 2005. http://lionhrtpub.com/orms/surveys/LP/LP-survey.html

Στατιστική Ανάλυση, (Statistical Analysis), OR/MS Today, Φεβρουάριος 2007. http://lionhrtpub.com/orms/surveys/sa/sa-survey.html

Πρόβλεψη (Forecasting), OR/MS Today, Αύγουστος 2006. http://lionhrtpub.com/orms/surveys/FSS/FSS.html

Επίσης υπάρχει το περιοδικό Interfaces (http://interfaces.journal.informs.org), της επιστημονικής κονότητας INFORMS. Σε αυτό το περιοδικό δημοσιεύονται συχνά μελέτες περιπτώσεων από το χώρο της επιχειρησιακής Έρευνας και κάποιες απο αυτές αφορούν και σε στρατιωτικές εφαρμογές. Ενδεικτικά μπορεί να αναφερθεί το άρθρο των Brown G.G., Dell R.F. και Newman A.M. το 2004 [23], στο οποίο ερευνάται το πρόβλημα της μεγιστοποίησης των εσόδων του στρατού με κατάλληλη αξιοποίηση των πόρων που διαθέτει. Μάλιστα, το πιό απλό ίσως μαθηματικό μοντέλο που μπορεί να χρησιμοποιηθεί σε αυτήν την περίπτωση, είναι αυτό του προβλήματος του δυαδικού σακκιδίου (binary knapsack). Άλλο ενδιαφέρον άρθρο είναι από τους Trainor T.E., Parnell G.S., Kwinn B., Brence J., Tollefson E. και Downes P. το 2007 [24], στο οποίο περιγράφεται η χρήση μαθηματικών μοντέλων βελτιστοποίησης για την ανάλυση αποφάσεων σχετικά με τη βέλτιστη χωροθέτηση στρατιωτικών μονάδων στην περιφέρεια.

Κλείνοντας την ενότητα αυτή, δεν πρέπει να παραληφθεί και το περιοδικό Naval Research Logistics (NRL) του εκδοτικού οίκου Wiley Periodicals, Inc., (http://www3.interscience.wiley.com/journal/37057/home). Το συγκεκριμένο περιοδικό, μεταξύ και άλλων επιστημονικών θεμάτων, δημοσιεύει εδώ και χρόνια επιστημονικές εργασίες σχετικές με εφαρμογές της Ε.Ε. στο ναυτικό και στο στρατό.

5. *Επίλογος - Προτάσεις*

Μπορεί κανείς πραγματικά να δει μια πληθώρα επιτυχημένων παραδείγματων εφαρμογής μεθόδων Επιχειρησιακής Έρευνας σε πολεμικές επιχειρήσεις. Παραδείγματα που καταδεικνύουν ότι μπορεί να γίνει όχι μόνο εξοικονόμηση πόρων αλλά και ελάττωση των ανθρωπίνων απωλειών σε μάχες. Σκεφτόμενοι αυτά τα παραδείγματα, πιστεύουμε ότι πρέπει να γίνει πιο έντονη η σύνδεση των ερευνητικών κέντρων στην Ελλάδα με στρατιωτικούς φορείς και μεγαλύτερη αξιοποίηση του επιστημονικού μας δυναμικού, ούτως ώστε να επιτευχθούν τα καλύτερα δυνατά αποτελέσματα. Βλέποντας τις χρηματοδοτήσεις που γίνονται απο στρατιωτικούς φορείς σε άλλα κράτη όπως τη Μεγάλη Βρετανία και τις ΗΠΑ για την προώθηση της βασικής έρευνας, αλλά και τα οφέλη που προκύπτουν από αυτήν, πρέπει να παραδειγματιστούμε και να κινηθούμε προς αυτήν την κατεύθυνση. Άλλωστε η Ελλάδα ούτε έχει απεριόριστους διαθέσιμους πόρους για σπατάλη σε περίοδο πολεμικών επιχειρήσεων, αλλά ούτε και μεγάλο σε πλήθος στρατιωτικό έμψυχο δυναμικό.

Επίσης χρήσιμη θα είναι και η δημιουργία μιας ομάδας εργασίας της Ελληνικής Εταιρίας Επιχειρησιακών Ερευνών (Ε.Ε.Ε.Ε.) (http://www.eeee.org.gr), με ειδικό ενδιαφέρον στις στρατιωτικές εφαρμογές. Αντίστοιχες εξειδικευμένες ερευνητικές ομάδες υπάρχουν εδώ και χρόνια σε άλλα κράτη και συνεργάζονται με κρατικές/στρατιωτικές υπηρεσίες.

Αναφορές

[1] Cormen T.H., Leiserson C.E., Rivest R.L. and Stein C. (2001), *Introduction to Algorithms,* 2nd ed., MIR Press.

[2] Levitin A.V. (2003), *Introduction to the Design and Analysis of Algorithms,* Addison Wesley.

[3] Dantzig B.G. (1949), "Programming in a linear structure", *Econometrica,* 17, 73-74.

[4] Dongarra J. and Sullivan F. (2000), "Guest Editors Introduction: The Top 10 Algorithms," *Computing in Science and Engineering,* 2(1), 22-23.

[5] Klee V., Minty G.J. (1972), "How good is the simplex algorithm?", in: *Inequalities III*, (Sisha O., Ed.), Academic Press, New York, 159-175.

[6] Khachian, L. (1979), "A polynomial algorithm in linear programming", *Soviet Mathematics Doklady,* 20, 191-194.

[7] Karmarkar N. (1984), "A new polynomial time algorithm for linear programming", *Combinatorica,* Springer-Verlag, 4, 373-395.

[8] Borgwardt K.H. (1982), "The average number of pivot steps required by the simplex method is polynomial", *Zeitschrift f?r Operations Research,* 26, 157-177.

[9] Paparrizos K. (1991), "An infeasible (exterior point) simplex algorithm for assignment problems", *Mathematical Programming,* Springer-Verlag, 51, 45-54.

[10] Paparrizos K., Samaras N. and Sifaleras A. (2008), "A new exterior Simplex type algorithm for the minimum cost network flow problem", accepted for publication *in Computers & Operations Research,* Elsevier Publications.

[11] Gass S.I. and Assad A.A. (Eds) (2005), "An Annotated Timeline of Operations Research", in *International Series in Operations Research & Management Science,* Kluwer Academic Publishers.

[12] Taha H.A. (1996), Operations Research: An Introduction, 6th ed., Prentice-Hall Publications.

[13] Rivest R.L., Shamir A. and Adleman L.M. (1978), "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM,* 21(2), 120-126.

[14] Waddington C.H. (1973), *OR in World War II - Operational Research against the U-boat,* Paul Elek Ltd., London, England.

[15] IFORS' Operational Research Hall of Fame Patrick Maynard Stuart Blackett, (2003), *International Transactions in Operational Research,* 10, 405-407.

[16] Kirby M.W. (2003), *Operational Research in War and Peace: The British Experience from the 1930s to 1970,* Imperial College Press.

[17] Rau E.P. (2005), "Combat science: the emergence of Operational Research in World War II", *Endeavour*, Elsevier Ltd., 29(4), 156-161.

[18] Ιστοσελίδα Υπουργείου Εθνικής Αμύνης, σχετικά με την Έρευνα και Τεχνολογία, (2008) www.mod.mil.gr/Pages/MainAnalysisPage3.asp?HyperLinkID=3&MainLinkID=48

[19] Ιστοσελίδα Ινστιτούτου Αμυντικών Αναλύσεων, (2008) www.iaa.gr

[20] Loerch A.G. and Rainey L.B. (Eds.) (2007), *Methods for Conducting Military Operational Analysis,* Military Operations Research Society, LMI Research Institute.

[21] Hartley D.S. III (2001), "Predicting Combat Effects", *Topics in Operations Research Series.*

[22] Ancker C.J., and Gafarian Jr. and A.V. (1992), "Modern Combat Models: A Critique of Their Foundations", *Topics in Operations Research Series.*

[23] Brown G.G., Dell R.F. and Newman A.M. (2004), "Optimizing Military Capital Planning", *Interfaces*, INFORMS Publications, 34, 415-425.

[24] Trainor T.E., Parnell G.S., Kwinn B., Brence J., Tollefson E. and Downes P. (2007), "The US Army Uses Decision Analysis in Designing Its US Installation Regions", *Interfaces,* INFORMS Publications, 37, 253-264.