ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«*Παγκόσμιες Προκλήσεις και Συστήματα Αναλύσεων*»

Η παραπλάνηση και η διάχυση της πληροφόρησης μέσω της ραγδαίας ανάπτυξης της τεχνολογίας της Τουρκίας και ο αντίκτυπος για την Ελλάδα.

Μελέτη του προϋπολογισμού και των μέσων πληροφόρησης της Τουρκίας τα τελευταία 20 χρόνια.

Μεταπτυχιακή Διπλωματική Εργασία Ειδίκευσης
«Διοικητική της διακινδύνευσης στην παγκόσμια πολιτική»

Ηλίας Τσαλαμιδάς

Τριμελής επιτροπή:
Διδάκτωρ Ιωάννης Κωνσταντόπουλος
Επίκουρος Καθηγητής Ευστράτιος Φακιολάς
Αναπληρωτής Καθηγητής Αντώνιος Κάργας

(ε) – Επιβλέπων/ουσα: Ιωάννης Κωνσταντόπουλος

Τελική έκδοση

Κόρινθος, 2023

UNIVERSITY OF THE PELOPONNESE
SCHOOL OF SOCIAL & POLITICAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCE &INTERNATIONAL RELATIONS

MASTER'S PROGRAMME IN
"GLOBAL RISKS AND ANALYTICS"

The deception and dissemination of information through the rapid development of Turkey's technology and the impact on Greece.
Study of Turkey's information budget and media in the last 20 years.

Master's dissertation specializing in
"Risk management in global politics"

Ilias Tsalamidas

Committee:
Dr. Ioannis konstantopoulos
Assistant Professor Eustratios Fakiolas
Associate Professor Antonios Kargas

(s) – Supervisor: Ioannis konstantopoulos

Final version

Corinth, Greece, 2023

Abstract

The use of information through technological development gives Turkey a huge advantage over our country in designing a tactical and operational deception. This dissertation aims to highlight the rapid development of technology by the neighboring country and the impact it has on Greece. For this reason, an analysis of some individual categories is carried out to help understand the context under investigation. Initially, the tactics of deception will be analysed and emphasis will be placed on the conditions of its success in the context of technology development and information dissemination. Subsequently, data on Turkey's technological development in the last 20 years will be collected, studied and analysed, especially some of the means related to intelligence such as UAV satellites as well as the whole of its defence industry. Finally in this dissertation an attempt will be made to determine and analyze the most important risks that Greece may face in the context of this technological development of Turkey and by using Decision Trees, decisions will be made and conclusions will be drawn.

Περίληψη

Η χρησιμοποίηση της πληροφόρησης μέσω της τεχνολογικής ανάπτυξης δίνει στην Τουρκία ένα τεράστιο πλεονέκτημα έναντι της χώρας μας στην σχεδίαση μιας τακτικής και επιχειρησιακής παραπλάνησης. Η παρούσα εργασία στοχεύει στην ανάδειξη της ραγδαίας ανάπτυξη της τεχνολογίας από την γείτονα χώρα καθώς και στον αντίκτυπο που απορρέει από αυτήν για την Ελλάδα. Για το λόγο αυτό πραγματοποιείται ανάλυση κάποιον επιμέρους κατηγοριών που θα βοηθήσουν στην κατανόηση του πλαισίου που ερευνάται. Αρχικά θα γίνει ανάλυση της τακτικής της παραπλάνησης και θα δοθεί έμφαση στις προϋποθέσεις της επιτυχίας της, στο πλαίσιο της ανάπτυξης της τεχνολογίας και τη διάχυση της πληροφόρησης. Στη συνεχεία θα γίνει συλλογή, μελέτη και ανάλυση στοιχείων της τεχνολογικής ανάπτυξης της Τουρκιάς τα τελευταία 20 χρόνια κυρίως κάποιων μέσων που αφορούν την πληροφόρηση όπως UAV δορυφόροι καθώς και το σύνολο της αμυντικής της βιομηχανίας. Τέλος σε αυτήν την εργασία θα γίνει μια προσπάθεια να καθοριστούν και να αναλυθούν οι σημαντικότεροι κίνδυνοι που ενδέχεται να αντιμετωπίσει η Ελλάδα στο πλαίσιο αυτής της τεχνολογικής ανάπτυξης της Τουρκιάς και με την χρήση δένδρων αποφάσεων (Decision Trees) θα παρθούν αποφάσεις και θα προκύψουν συμπεράσματα.

Πρόλογος

Καθώς πλησιάζω στην ολοκλήρωση του μεταπτυχιακού μου ταξιδιού, είμαι υποχρεωμένος να εκφράσω την εγκάρδια εκτίμησή μου για το προνόμιο να φοιτήσω στο Πανεπιστήμιο Πελοποννήσου στο Τμήμα Πολιτικής Επιστήμης και Διεθνών Σχέσεων.

Θα ήθελα να μεταφέρω τη βαθιά μου ευγνωμοσύνη στον καθηγητή μου Ιωάννη Κωνσταντόπουλο για την εξαιρετική συνεργασία και την ανεκτίμητη καθοδήγησή του. Είναι αδιαμφισβήτητο ότι η ουσιαστική συμβολή του υπήρξε απαραίτητη για την ολοκλήρωση αυτής της έρευνας.

Θέλω επίσης να ευχαριστήσω θερμά τους κυρίους Ευστάθιο Φακιολά, Πάνο Χουντάλα και Γεώργιο Φαράντο καθηγητές των βασικών μαθημάτων του μεταπτυχιακού προγράμματος "Παγκόσμιες προκλήσεις και συστήματα ανάλυσης", για τη διαρκή δέσμευσή τους στην προώθηση της εκπαίδευσης και την ανεκτίμητη καθοδήγησή τους καθ' όλη τη διάρκεια αυτού του εξειδικευμένου προγράμματος.

Σεπτέμβριος, 2023

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Γραφημάτων

Εισαγωγή

Είναι σαφές πως η έννοια της παραπλάνησης δεν είναι σταθερή στον χρόνο. Παρότι μπορούμε να την ανιχνεύσουμε σε διαφορετικές περιόδους, είναι απολύτως προφανές ότι αυτή κάθε φορά επανεφευρίσκεται από τα υποκείμενα της δράσης, τόσο με βάση την στοχοθεσία που θέτουν όσο και με τα τεχνικά – τεχνολογικά χαρακτηριστικά της κάθε εποχής.

Είναι επίσης φανερό ότι η παραπλάνηση εξακολουθεί να ασκείται, τόσο από ιδιώτες όσο και από οργανωμένος δομές. Είναι εξαιρετικά ενδιαφέρον ως ερώτημα η μορφή που θα λάβει μέσα στον 21ο αιώνα, τα όριά της αλλά και την δυνατότητα όσων στοχεύουν να αμυνθούν απέναντί της. Μπορεί σε πρώτη ματιά οι στόχοι να μοιάζουν προφανείς, ήτοι στρατιωτικοί και κυβερνητικοί στόχοι, όμως η πολυπλοκότητα της πραγματικότητας έχει μεταφέρει την παραπλάνηση (ως έννοια και με τα διεσταλμένα όρια που μπορεί στο σημερινό πεδίο να έχει) εκτός αυτών των κλασσικών αντικειμένων δράσης της. Αυτό θα επιχειρήσουμε να αναλύσουμε στο παρόν κείμενο, την πολυπλοκότητα της έννοιας, τις διαστάσεις της και την μετάφρασή τους στο πεδίο, αλλά και ειδικότερα την Τουρκική τεχνολογική ανάπτυξη, τις δυνατότητες που αυτή δίνει στην γείτονα χώρα, αλλά και τους κινδύνους που ελλοχεύουν για την Ελλάδα.

1 Μεθοδολογία, Ερευνητικά ερωτήματα και ορισμοί

1.1 Μεθοδολογία και Ερευνητικά Ερωτήματα

Η βιβλιογραφική ανασκόπηση θα χρησιμεύσει ως βασική μεθοδολογική προσέγγιση. Στην παρούσα μελέτη, θα πραγματοποιηθεί μια ενδελεχής βιβλιογραφική ανασκόπηση, η οποία θα περιλαμβάνει ένα ευρύ φάσμα βιβλίων και άρθρων γραμμένων τόσο στην ελληνική όσο και σε ξένες γλώσσες. Στόχος είναι να διασφαλιστεί μια ολοκληρωμένη κάλυψη της σχετικής βιβλιογραφίας.

Αυτή η μελέτη της βιβλιογραφίας αποσκοπεί στην εξακρίβωση της συνάφειας διαφόρων ερευνητικών εργασιών, άρθρων και βιβλίων σε σχέση με το υπό εξέταση θέμα, ενισχύοντας έτσι τη συνολική κατανόηση του θέματος. Πρακτικά, αυτό συνεπάγεται μια διαδικασία που περιλαμβάνει την εξέταση των τίτλων και των περιλήψεων για τον εντοπισμό των καταλληλότερων που αφορούν τα κύρια ερευνητικά ερωτήματα και ενισχύουν την κατανόηση του θέματος. Τα επιλεγμένα κείμενα θα υποβληθούν στη συνέχεια σε ολοκληρωμένη έρευνα για να δώσουν ολοκληρωμένες απαντήσεις στα ερωτήματα. Είναι σημαντικό να αναγνωρίσουμε ότι κατά τη διαδικασία διεξαγωγής μιας μελέτης μέσω της αξιοποίησης μιας βιβλιογραφικής ανασκόπησης, προκύπτει μια δυναμική αλληλεπίδραση μεταξύ του υπάρχοντος σώματος της βιβλιογραφίας και του γραπτού κειμένου. Αυτή η αλληλεπίδραση λειτουργεί ουσιαστικά ως κατευθυντήρια δύναμη, επηρεάζοντας διάφορες πτυχές του κειμένου, όπως η διατύπωση ερευνητικών ερωτημάτων και ο εντοπισμός κενών στη βιβλιογραφία (Creswell, 2021).

Η αποτελεσματικότητα μιας βιβλιογραφικής ανασκόπησης επηρεάζεται από διάφορους παράγοντες (Ζαφειρόπουλος, 2015). Στους παράγοντες αυτούς περιλαμβάνονται: (α) η πληρότητα της διαδικασίας αναζήτησης και εντοπισμού της σχετικής βιβλιογραφίας, (β) η αυθεντικότητα και η συνέπεια στην παρουσίαση των συλλεχθέντων στοιχείων, (γ) η επάρκεια του ερευνητή στη σύνθεση και την ερμηνεία της βιβλιογραφίας μέσω της συγγραφής και (δ) η ακρίβεια και η πληρότητα της ίδιας της βιβλιογραφίας.

Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα που πρόκειται να μας απασχολήσουν κινούνται γύρω από τον πυρήνα της εξέλιξης της τεχνολογίας στην Τουρκία, ιδίως σε σχέση με τα uav, την εξέλιξη των τεχνολογιών πληροφορίας και της διάχυσής της καθώς επίσης και γύρω από τις έννοιες της παραπλάνησης . Αναλύοντας αυτά τα ερωτήματα, θα επιχειρήσουμε να ενσωματώσουμε τις εξελίξεις (που θα περιγράφουν) σε ένα Risk Matrix. Εν συνεχεία θα δημιουργήσουμε ένα

δενδροδιάγραμμα αποφάσεων για την αντιμετώπιση των απειλών που θα έχουν από την παραπάνω ανάλυση.

1.2 Έννοιες και ορισμοί

Στις μελέτες που έχουν πραγματοποιηθεί για την ερμηνεία της παραπλάνησης , διαφαίνεται ότι την παρουσιάζουν παράλληλα με την έννοια της άρνησης - αποφυγής. Οι δύο έννοιες παρουσιάζονται συχνά στην περιγραφή διεξαγωγής πληροφοριακών επιχειρήσεων ενός κράτους που έχει ως στόχο την επίτευξη του επιθυμητού αποτελέσματος. Σύμφωνα με τους Bruce και Bennett(2008) οι δύο όροι συνδέονται άρρηκτα με τους αρμόδιους που επηρεάζουν τις εθνικές αποφάσεις αλλά και τους στρατιωτικούς ενώ ερμηνεύονται ως εγχείρημα ή δραστηριότητα από την πλευρά των κρατικών η μη αντιπάλων με στόχο την επιρροή ή την παραπλάνηση των αντίπαλων σε θέματα λήψης αποφάσεων ή και συλλογής πληροφοριών. Με την παραπλάνηση ελαχιστοποιείται η αποτελεσματικότητα της συλλογής πληροφοριών και γίνεται αναφορά για ασύμμετρο πόλεμο. Επιπλέον θεωρείται πως η άρνηση είναι περισσότερο συνηθισμένη από την παραπλάνηση , όπου η δεύτερη χρησιμοποιείται σε σπάνιες περιπτώσεις.

Από την πλευρά τους οι Shulsky, et al (2002)αναφέρουν ως άρνηση την παρεμπόδιση των καναλιών επικοινωνίας στους αντιπάλους με στόχο την αποτροπή της άμεσης αντίδρασής του. Σε μελέτη που πραγματοποιήθηκε από τους (Godson & Wirtz,2005) η άρνηση ορίζεται ως η ικανότητα αποτροπής ή εξασθένισης της συγκέντρωσης πληροφοριών από τους αντιπάλους και τις δραστηριότητες που είναι σχεδιασμένες με στόχο την εξασθένιση και την υποβάθμιση της συγκέντρωσης πληροφοριών διαμέσου των τεχνολογικών και ανθρώπινων μέσων.

Η παραπλάνηση αφορά την εσκεμμένη προσπάθεια του αντιπάλου να χειραγωγήσει την αντίληψη των ατόμων που διαμορφώνουν και λαμβάνουν αποφάσεις , με στόχο την επίτευξη ενός ανταγωνιστικού πλεονεκτήματος.»(Daniel et al, 1981)και προσθέτουν ότι αφορά την εσκεμμένα λανθασμένη παρουσίαση των γεγονότων προκειμένου να επιτευχθεί ο στόχος. Οι παραπάνω ερευνητές δίνουν έμφαση στην βασική ιδιότητα της παραπλάνησης ως εσκεμένη με στόχο την επίτευξη του επιθυμητού αποτελέσματος.

Οι Shulsky και Schmitt(2002) περιγράφουν την παραπλάνηση ως μια προσπάθεια εξαπάτησης της ανάλυσης πληροφοριών των αντιπάλων, σε θέματα που αφορούν την στρατηγική, την στρατιωτική, την πολιτική και την οικονομική κατάσταση που αντιμετωπίζουν. Έτσι οι αντίπαλοι αρκετές φορές διαμορφώνουν μια λανθασμένη αντίληψη για τα γεγονότα και δρουν αναποτελεσματικά.

Η στρατηγική και το στρατηγικό σύστημα πολέμου ενδέχεται να εμπεριέχουν την παραπλάνηση. Οι ερευνητές στης στρατηγικής έχουν διαμορφώσει διάφορες απόψεις . Από την πλευρά του ο Σουν Τζου υποστηρίζει την παραπλάνηση ως μέσω στρατηγικής, ενώ ο Jomini θεωρεί πως ένας σοφός διοικητής δεν θα πρέπει να τη χρησιμοποιεί. Ο Θουκυδίδης από την πλευρά του αναφέρει ότι ο στόχος επιτυγχάνεται όταν κάποιος καταφέρνει να εξαπατήσει τον εχθρό του και να ωφελήσει τους φίλους του.

Με τον όρο στρατηγική αναφερόμαστε στην στρατιωτική στρατηγική, δηλαδή στον τρόπο που κινούνται οι στρατηγικές δυνάμεις προκειμένου να επιτευχθεί ένας στρατιωτικός σκοπός. Επίσης στρατηγική μπορεί να είναι η μέθοδος που σχεδιάζεται από τα κράτη προκειμένου να ασκήσουν εξωτερική πολιτική και να επιτύχουν ένα στόχο (Κολιόπουλος, 2010)

2 Η τακτική της παραπλάνησης σε ειρήνη και πόλεμο

2.1 Η Παραπλάνηση ως έννοια και ιστορικά παραδείγματα

Η διαχείριση της διακυβέρνησης σε καιρό πολέμου αποτελεί θέμα μελέτης στη διεθνή βιβλιογραφία. Ιδιαίτερα έχει δοθεί έμφαση στην τακτική της παραπλάνησης. Έτσι αρκετοί ερευνητές έχουν καταλήξει σε ένα κοινό συμπέρασμα. Η τακτική της παραπλάνησης εφαρμόζεται για να αναγκασθεί ο αντίπαλος να συγκεντρώσει τις δυνάμεις του σε λανθασμένη τοποθεσία. Έτσι ο αντίπαλος ενδέχεται να παραβιάσει την αρχή της συγκέντρωσης δυνάμεων, όπως για παράδειγμα συνέβη κατά τη διάρκεια του Β Παγκοσμίου Πολέμου. Επίσης ο αντίπαλος ενδέχεται να σπαταλήσει πολύτιμο χρόνο και πόρους . Τέλος η τακτική της παραπλάνησης εμπεριέχει τον αιφνιδιασμό, όπου ο αντίπαλος μπορεί να πιαστεί απροετοίμαστος. Την τακτική της παραπλάνησης και της άρνησης μπορεί να αξιοποιήσουν τα απολυταρχικά καθεστώτα, οι δημοκρατίες, οι μη- κρατικοί δρώντες καθώς και τα καθεστώτα που βρίσκονται σε μεταβατικό στάδιο από την δημοκρατία στον αυταρχισμό και το αντίθετο. Η τακτική της παραπλάνησης, ωστόσο μπορεί να εφαρμοσθεί σε καιρό πολέμου σε δημοκρατικά πολιτεύματα, ενώ σε απολυταρχικά καθεστώτα η άρνηση και η παραπλάνηση αποτελούν πάγια τακτική της εσωτερικής διακυβέρνησης και της εξωτερικής τους πολιτικής.(Bell, Bowyer 2005).

Στη διεθνή βιβλιογραφία τίθεται ένα βασικό ερώτημα που αφορά τους φορείς ή τους αρμόδιους που επιλέγουν αυτή την τακτική, ιδιαίτερα στον πόλεμο. Πρόκειται για ισχυρές κυβερνήσεις ή αδύναμες; Σύμφωνα με τους (Bennett, et al,2007) οι αδύναμες κυβερνήσεις ενδέχεται να εφαρμόσουν την παραπλάνηση λόγω της έλλειψης επιλογών , έτσι ώστε να μπορέσουν να αντισταθμίσουν την ανισορροπία. Ωστόσο οι (Andrew, et al,1990), υποστηρίζουν πως αποτελεί μέρος της τακτικής των ισχυρών , οι οποίοι στοχεύουν στην εξοικονόμιση πόρων και στον περιορισμό των απωλειών.

Σύμφωνα με τον Mearsheimer J. (2011) η παραπλάνηση διακρίνεται ανάλογα με το κίνητρο και τις ικανότητες. Στην πρώτη περίπτωση ο παραπλανών , δείχνει πως επιτίθεται ενώ στην πραγματικότητα δεν το κάνει. Ο στόχος του είναι να εκβιάσει τους αντιπάλους προκειμένου να συλλέξει πληροφορίες και να επιτύχει κάποιες παραχωρήσεις. Ωστόσο σε αυτή την περίπτωση μπορεί να διεξαχθεί πόλεμος. Στη δεύτερη περίπτωση , ο παραπλανών δεν αποκαλύπτει το σχέδιο στρατηγικής και στην πραγματικότητα προετοιμάζεται για επίθεση. Ο στόχος είναι ο αιφνιδιασμός. Μπορούμε ιστορικά να αναφέρουμε πολλά «περιστατικά» παραπλάνησης. Από τους Αιγός Ποταμούς στην αρχαιότητα, έως την D-Day στον 2ο Παγκόσμιο Πόλεμο, το Yom Kippur .

Στους Αιγός Ποταμούς

Σε όλη τη διάρκεια της ιστορίας, στρατηγοί και ηγέτες έχουν χρησιμοποιήσει την παραπλάνηση ως τακτική προσέγγιση στις μάχες. Η στρατηγική αυτή βασίζεται στην εκμετάλλευση του αιφνιδιασμού και της έλλειψης ετοιμότητας του εχθρού, ιδίως όταν μια ασθενέστερη παράταξη προσπαθεί να αντισταθμίσει τη δύναμη του αντιπάλου. Με τον τρόπο αυτό, η μειονεκτούσα πλευρά ενισχύει τις πιθανότητές της να ελαχιστοποιήσει τις απώλειες και να επιτύχει ένα ευνοϊκό αποτέλεσμα. Μια ενδεικτική περίπτωση του κομβικού ρόλου αυτής της τεχνικής είναι εμφανής στη μάχη στους Αιγός Ποταμούς, σημείο καμπής στον Πελοποννησιακό Πόλεμο (431-404 π.Χ.) μεταξύ της Αθήνας και της Σπάρτης ,ο ιστορικός Θουκυδίδης αναγνώρισε τη σύγκρουση αυτή ως ένα κορυφαίο γεγονός, που σηματοδότησε την ήττα της Αθήνας από τη Σπάρτη καθορίζοντας έτσι σε σημαντικό βαθμό την πορεία της Ελληνικής ιστορίας (Prosser, 2009).

Το 408 π.Χ., ο Λύσανδρος ανέλαβε την ηγεσία του σπαρτιατικού στόλου, μετά από σημαντικές ήττες σε κομβικές μάχες όπως η Κύζικος, η Χαλκηδόνα και το Βυζάντιο, οι οποίες είχαν διαβρώσει σοβαρά την επιρροή της Σπάρτης στον Ελλήσποντο. Το 407 π.Χ., εγκατέστησε έξυπνα στην Έφεσο το στρατηγείο του, καλλιεργώντας συμμαχίες με διάφορες φιλοσπαρτιατικές παρατάξεις και δεσμεύοντάς τες. Ο Λύσανδρος συγκέντρωσε επιδέξια την κρίσιμη οικονομική υποστήριξη του ισχυρού Πέρση πρίγκιπα Κύρου, ο οποίος ασκούσε σημαντική εξουσία στη Μικρά Ασία, απέφυγε τις άμεσες ναυτικές συγκρούσεις με την Αθήνα, επιλέγοντας μια έμμεση στρατηγική για να ενισχύσει τη θέση του. Ταυτόχρονα, σε μια υπολογισμένη κίνηση, ο Αλκιβιάδης χώρισε τον αθηναϊκό στόλο σε τμήματα για να αντιμετωπίσει τη σπαρτιατική επιρροή γύρω από τον Ελλήσποντο. Ωστόσο, το σχέδιο αυτό απέτυχε, όταν ο Αντίοχος, στον οποίο ο Αλκιβιάδης είχε αναθέσει να αποφύγει την αντιπαράθεση, αψήφησε τις εντολές και συγκρούστηκε με τον Λύσανδρο (Ζάχος, 2003).

Ο κύριος στόχος του Λύσανδρου επικεντρώθηκε στην αποκοπή των οδών ανεφοδιασμού της Αθήνας και στην απόκτηση της κυριαρχίας σε πόλεις-κλειδιά στο ανατολικό Αιγαίο. Η σοφή εφαρμογή της τακτικής εξαπάτησης από τον Λύσανδρο ήρθε στο προσκήνιο κατά τη διάρκεια της μάχης της Αιγός, όπου χειραγώγησε επιδέξια τις αθηναϊκές προσδοκίες. Οργανώνοντας ένα σενάριο προσποιητής ετοιμότητας, ο Λύσανδρος δημιούργησε μια «εικονική» τετραήμερη αναμέτρηση, παγιδεύοντας τους Αθηναίους στην διαρκή αναμονή. Μέσα σε αυτό το τέχνασμα, οι Αθηναίοι παρέμειναν σταθεροί στις θέσεις, παγιδευμένοι από τον Λύσανδρο. Αυτό το στρατηγικό τέχνασμα κορυφώθηκε σε μια κρίσιμη πέμπτη ημέρα, κατά την οποία οι Σπαρτιάτες επανατοποθετήθηκαν σε προφανή ετοιμότητα, αλλά απείχαν από την άμεση μάχη, αποστέλλοντας αντ' αυτού κρυφά σκάφη. Αυτοί οι κατάσκοποι παρατήρησαν κρυφά τους Αθηναίους να εγκαταλείπουν τη θέση τους, προτρέποντας τους Σπαρτιάτες να εκμεταλλευτούν τη στιγμή και να εξαπολύσουν μια απρόβλεπτη επίθεση. Αιφνιδιασμένοι, οι Αθηναίοι έμειναν ανίσχυροι να αντιδράσουν, παγιδευμένοι από την τακτική του Λύσανδρου. Αυτό το πανούργο στρατήγημα ανέδειξε την ικανότητα του Λύσανδρου να χειραγωγεί τις προσδοκίες και να εκμεταλλεύεται τα τρωτά σημεία, τοποθετώντας τον ως έναν τρομερό αρχιτέκτονα της στρατηγικής καινοτομίας στο πεδίο της μάχης. (Ζάχος, 2003)

Χρησιμοποιώντας αυτό το στρατήγημα η Σπάρτη πέτυχε έναν θρίαμβο. Εκμηδενίζοντας ουσιαστικά τον αθηναϊκό στόλο, εκτός από 8 διαφεύγοντα σκάφη. Τα στρατεύματα που επέζησαν είτε διέφυγαν σε συμμαχικές πόλεις είτε γνώρισαν την αιχμαλωσία από τους Σπαρτιάτες.Η νίκη των Σπαρτιατών στο Αίγος άλλαξε οριστικά την πορεία του Πελοποννησιακού Πολέμου. Μέσα σε λίγους μήνες, η Αθήνα, στερημένη από το στόλο και τις οδούς ανεφοδιασμού της, υπέκυψε στην πολιορκία των Σπαρτιατών, σηματοδοτώντας το τέλος του σχεδόν 30ετούς Πελοποννησιακού Πολέμου. Ένα κεφάλαιο έκλεισε, αναδεικνύοντας ότι ανάμεσα στην ικανότητα των έμπειρων στρατηγών, η εξαπάτηση έπαιζε τον καθοριστικό ρόλο.

D-Day

Η κρίσιμη εισβολή στη Νορμανδία, που ονομάστηκε D-Day (6 Ιουνίου 1944), ήταν ένα γεγονός-ορόσημο του Β' Παγκοσμίου Πολέμου. Οι παραπλανητικές τακτικές οδήγησαν τους Γερμανούς να αναγνωρίσουν λανθασμένα το Pas de Calais ως το σημείο για την πραγματική απόβαση στη Νορμανδία και να πιστέψουν πως θα γινόταν τον Ιούλιο αντί για την πραγματική ημερομηνία, τον Ιούνιο (Rankin, 2008)

Κατά τη διάρκεια του 1943, οι ΗΠΑ και η Μεγάλη Βρετανία ξεκίνησαν μια αποστολή εναντίον της ναζιστικής Γερμανίας, με απώτατο στόχο το άνοιγμα ενός νέου μετώπου. Μετά τις επιχειρήσεις στην Αφρική, ο Χίτλερ ενίσχυσε τον στρατό του ενάντια σε πιθανές συμμαχικές απειλές. Σε απάντηση, οι Σύμμαχοι, τροφοδοτούμενοι από τις επιτυχίες της Βόρειας Αφρικής, επινόησαν ένα περίπλοκο σχέδιο για τη δημιουργία ενός ισχυρού προγεφυρώματος, μιας «γέφυρας» μεταξύ της Βρετανίας και της Ευρώπης (Masterman, 2000).

Στη διάσκεψη της Καζαμπλάνκα, οι ΗΠΑ και η Βρετανία δημιούργησαν το Κοινό Επιτελείο του Ανώτατου Συμμαχικού Διοικητή-COSSAC, με επικεφαλής τον Φρέντερικ Μόργκαν (Barton, 2007). Ο Μόργκαν εκτέλεσε το Σχέδιο Cockade, ένα σχέδιο για τη δημιουργία σύγχυσης στην πλευρά των γερμανικών μυστικών υπηρεσιών, επιτυγχάνοντας αξιοσημείωτη επιτυχία. Αργότερα, το SHAEF αντικατέστησε το COSSAC και σχεδιάστηκαν οι επιχειρήσεις "FORTITUDE I" και "FORTITUDE II" για στρατηγική παραπλάνηση, αφήνοντας να «γίνει γνωστή» μια επίθεση τον Ιούλιο και δίνοντας έμφαση στο Pas de Calais (Barton, 2007).

Το αποκορύφωμα της παραπλάνησης ήταν το σχέδιο "BODYGUARD", υπό την εποπτεία του συνταγματάρχη John Bevan και υπό την καθοδήγηση του Churchill. Αυτό το τριμερές σχέδιο περιελάμβανε τη διάδοση παραπληροφόρησης, την εμπλοκή διπλών πρακτόρων μέσω του συστήματος διπλής διασταύρωσης της MI5 και την παραπλάνηση των γερμανικών μυστικών υπηρεσιών, με επιτομή τον ρόλο του διπλού πράκτορα του Harry Williamson (Masterman, 2000). Ακολούθησαν γερμανικοί εσφαλμένοι υπολογισμοί, καθώς η πραγματική ημερομηνία της επίθεσης (6 Ιουνίου 1944) αποκρύφθηκε επιτυχώς.

Yom Kippur

Yom Kippur ή αλλιώς «γιορτή του εξιλασμού» ονομάζεται η μεγαλύτερη θρησκευτική γιορτή των Εβραίων, κατά την οποία σύμφωνα με την εβραϊκή παράδοση εξιλεώνονται οι άνθρωποι από τις αμαρτίες τους και αποκαθίσταται η σχέση τους με το Θεό. Με αφορμή,

λοιπόν, τις επιθετικές επιχειρήσεις με πρωταγωνιστές την Αίγυπτο και την Συρία σε βάρος του Ισραήλ ανήμερα της γιορτής του εξιλασμού, ονομάστηκε η τέταρτη κατά σειρά Αραβοϊσραηλινή σύρραξη «πόλεμος του Yom Kippur» στις 6-24 Οκτωβρίου 1973.

Οι κρίσιμοι παράγοντες που επηρέασαν την πορεία και την έκβαση της σύγκρουσης ήταν το στοιχείο του αιφνιδιασμού και η ελλιπής ετοιμότητα του Ισραήλ (Godson, 2000). Η αποτελεσματικότητα της παραπλάνησης στην εθνική στρατηγική στηρίζεται σε δύο πυλώνες: είτε αποκρύπτοντας βασικές πληροφορίες που είναι επωφελείς για τον εχθρό, είτε κατακλύζοντάς τον με εκτεταμένα ψευδή δεδομένα. Η αδυναμία του Ισραήλ να προβλέψει τα γεγονότα προερχόταν από την υπερεμπιστοσύνη της άμυνας και την εσφαλμένη εκτίμηση των προθέσεων του αντιπάλου (Farr, 1999).

Οι λανθασμένες υποθέσεις σχετικά με τις προθέσεις των αραβικών δυνάμεων οδήγησαν το Ισραήλ σε διστακτικότητα και περιορισμένη ικανότητα άμεσης αντίδρασης. Ενώ η εμπιστοσύνη στην αεράμυνα συνέβαλε στην πεποίθηση ότι η συριακή εισβολή ήταν απίθανη, καθώς αμφισβητήθηκαν οι δυνατότητες εναέριων ελιγμών της Συριακής αεροπορίας. Επιπλέον, οι εκτιμήσεις για την εξάρτηση της Συρίας από την αιγυπτιακή συμμετοχή αποδείχθηκαν εσφαλμένες (Shlaim, 1976).

Αν και παρατηρήθηκαν ενδείξεις αραβικής στρατιωτικής κινητοποίησης μέσω της τεχνολογίας και των πληροφοριών από τις ΗΠΑ, το Ισραήλ παρερμήνευσε την κατάσταση ως ασκήσεις ρουτίνας. Η Αίγυπτος μετέφερε αποτελεσματικά 90.000 στρατιώτες και 850 άρματα μάχης μέσω της διώρυγας του Σουέζ μέσα σε λίγες ώρες, εγκαθιστώντας οχυρωμένες θέσεις (Pollack, 2002). Παρά τις αρχικές προκλήσεις της Συρίας, κατάφερε να παραβιάσει την ισραηλινή άμυνα και να καταλάβει τμήματα των υψωμάτων του Γκολάν (Zisser, 2013).

Το αποτέλεσμα υπογράμμιζε τον κομβικό ρόλο της παραπλάνησης και της παρερμηνείας στη διαμόρφωση της δυναμικής μιας σύγκρουσης. Αν και οι αρχικές προοπτικές της σύγκρουσης ευνοούσαν τα αραβικά έθνη, η μεταβολή των γεγονότων έδωσε τον έλεγχο στο Ισραήλ. Η δυναμική αυτή υπογραμμίζει τη ρευστότητα του πολέμου και των παραγόντων που τον επηρεάζουν. Στο βορρά, οι ισχυρές αμυντικές θέσεις του Ισραήλ και οι ακριβείς αεροπορικές επιδρομές άλλαξαν τις πολεμικές προτεραιότητες της Συρίας, επιτρέποντας την εστίαση του Ισραήλ σε χερσαίες και αεροπορικές επιχειρήσεις. Ομοίως, στο νότο, το Ισραήλ εκμεταλλεύτηκε τα αιγυπτιακά τρωτά σημεία. Προβλέποντας μια διάβαση της διώρυγας του Σουέζ χωρίς αεροπορική προστασία, προσάρμοσαν οι αντίστοιχες στρατηγικές του για πλεονέκτημα στο πεδίο της μάχης. Παρέσυραν τα αραβικά στρατεύματα βαθύτερα στο ισραηλινό έδαφος, ξεφεύγοντας από την εμβέλεια των πυραύλων, και έστησαν ενέδρες για να εξουδετερώσουν τα εχθρικά άρματα μάχης. Η Αίγυπτος, καταπονημένη από την επιτυχή αντίδραση του Ισραήλ, επιδίωξε διαπραγματεύσεις. Μέχρι το τέλος του έτους, επιτεύχθηκε μια συμφωνία. Αυτό υπογραμμίζει την ευμετάβλητη δυναμική των συγκρούσεων και τη στρατηγική οξυδέρκεια του Ισραήλ για την κατάληψη του ελέγχου, παρά την επιτυχή παραπλάνηση του από Αραβικής πλευράς.

2.2 Οι Ένοπλες δυνάμεις και η Παραπλάνηση

Στόχος μας είναι να τοποθετήσουμε την έννοια της παραπλάνησης στο πλαίσιο των επιχειρήσεων πληροφοριών, ενός όρου που εισήχθη γύρω στα μέσα της δεκαετίας του 1990, εξελισσόμενος από τον "Πόλεμο Πληροφοριών" ή "Πόλεμο Διοίκησης και Ελέγχου", ο οποίος έγινε γνωστός κατά τη διάρκεια του πρώτου πολέμου του Κόλπου στο Ιράκ (Molander, Riddile, Wilson, 1996). Εδώ εστιάζουμε στη διερεύνηση του ρόλου της παραπλάνησης, ιδίως της στρατιωτικής παραπλάνησης, ως εργαλείου στο πλαίσιο των επιχειρήσεων πληροφοριών.

Οι σύγχρονες πλατφόρμες επικοινωνίας και πληροφόρησης διαθέτουν την αξιοσημείωτη ικανότητα να εμπλέκονται άμεσα με το φάσμα των πολιτικοστρατιωτικών δραστηριοτήτων. Η επιρροή αυτή επεκτείνεται πέρα από τους εμπλεκόμενους πληθυσμούς και περιλαμβάνει την παγκόσμια κοινή γνώμη. Είναι σημαντικό ότι η επιρροή στη συμπεριφορά και τις αντιδράσεις, ιδίως σε περιόδους κρίσεων και συγκρούσεων, υπογραμμίζει τον κρίσιμο ρόλο της διαχείρισης των πληροφοριών στη διαμόρφωση της διεθνούς λήψης αποφάσεων και της δυναμικής της κατάστασης (Bergowitz, 2001).

Είναι σκόπιμο να αναγνωρίσουμε ότι ο συγκερασμός της παγκοσμιοποίησης και η διασύνδεση των συστημάτων επικοινωνίας και πληροφοριών, σε συνδυασμό με την απεριόριστη πρόσβαση στην πληροφοριακή υποδομή ενός έθνους, εισάγει νέους τρόπους για επιχειρησιακή εκμετάλλευση. Ταυτόχρονα, αυτή η διασύνδεση ενισχύει την ευπάθεια της υποδομής πληροφοριών. Επιπλέον, η υποδομή που στηρίζει τη ροή πληροφοριών - η οποία περιλαμβάνει προσωπικό, εξοπλισμό και διαδικασίες - έχει πλέον αναδειχθεί σε στόχο υψηλής αξίας, τόσο σε στρατιωτικό όσο και σε μη στρατιωτικό πλαίσιο. Αυτό το εξελισσόμενο τοπίο αναδεικνύει τη σημασία των αποτελεσματικών και συνεχών σύγχρονων Επιχειρήσεων Πληροφοριών, που χαρακτηρίζονται από: α) αξιολόγηση του Πληροφοριακού Περιβάλλοντος, β) έγκαιρο εντοπισμό και επιδέξια διαχείριση των προκλήσεων, γ) συντονισμένες ενέργειες που αξιοποιούν τις εγγενείς δυνατότητες για να σμιλεύσουν το Πληροφοριακό Περιβάλλον και να επηρεάσουν τη βούληση του αντιπάλου. Αυτές οι Επιχειρήσεις Πληροφοριών διαδραματίζουν καθοριστικό ρόλο στον επηρεασμό των αντιλήψεων, των στάσεων και της συμπεριφοράς συγκεκριμένων ακροατηρίων (JP 3-13, 2012). Η σφαίρα των επιχειρήσεων πληροφοριών περιλαμβάνει τόσο επιθετικές όσο και αμυντικές πτυχές. Είναι ζωτικής σημασίας να σημειωθεί ότι οι πτυχές αυτές δεν συμβαίνουν απαραίτητα ταυτόχρονα με άλλες επιχειρήσεις, παρότι ένα κράτος μπορεί να συμμετέχει σε αμυντικές επιχειρήσεις ενώ διεξάγει επίσης επιθετικές επιχειρήσεις πληροφοριών (JP 3-13, 2012). Για τη διευκόλυνση των επιθετικών και αμυντικών επιχειρήσεων, υπεισέρχονται συγκεκριμένες στρατιωτικές δραστηριότητες. Για τις επιθετικές επιχειρήσεις πληροφοριών, οι δραστηριότητες αυτές περιλαμβάνουν: 1) παραπλάνηση, 2) ασφάλεια επιχειρήσεων, 3) ηλεκτρονικός πόλεμος (EW), 4) φυσική επίθεση, 5) ψυχολογικές επιχειρήσεις (PSO) και 6) επιθετικές επιχειρήσεις δικτύου (NO). Αξίζει να σημειωθεί ότι η κύρια εστίαση εδώ έγκειται στην πρώτη δραστηριότητα, την παραπλάνηση(JP 3-13, 2012).

Αντίθετα, οι Επιχειρήσεις Πληροφοριών Άμυνας (DIO) περιλαμβάνουν τις ακόλουθες στρατιωτικές δραστηριότητες: 1) Αντικατασκοπεία (COI), 2) Ασφάλεια επιχειρήσεων, 3)

Ηλεκτρονικός πόλεμος (EW), 4) Ασφάλεια δεδομένων, 5) Αντιπροπαγάνδα και 6) Αμυντικές επιχειρήσεις δικτύου (DNO). Μια αξιοσημείωτη διάκριση είναι εμφανής στις αμυντικές επιχειρήσεις πληροφοριών σε σύγκριση με τις αντίστοιχες επιθετικές: Η «Απάτη» μετατρέπεται σε «Αντι-Απάτη», οι Ψυχολογικές Επιχειρήσεις μετατοπίζονται σε Αντι-Προπαγάνδα και οι Επιχειρήσεις Δικτύου ευθυγραμμίζονται με την αντίστοιχη επιχειρησιακή κατεύθυνση (JP 3-13, 2012).

Οι υπεύθυνοι για τη διαμόρφωση του Δόγματος των Ενόπλων Δυνάμεων σε κάθε έθνος έχουν ενσωματώσει τις θεωρητικές αρχές της παραπλάνησης σε απτά επιχειρησιακά σχέδια. Η στρατιωτική παραπλάνηση χρησιμεύει ως στρατηγικό μέσο που χρησιμοποιείται για να συσκοτίσει την επί του πεδίου στρατιωτική ικανότητα, τις προθέσεις και τις επιχειρησιακές στρατηγικές, προκαλώντας έτσι σύγχυση στους αντίπαλους φορείς λήψης αποφάσεων. Η διαδικασία αυτή συνεπάγεται την κατασκευή μιας τεχνητής εικόνας, μιας -ουσιαστικά- ψευδαίσθησης που ευθυγραμμίζεται αποτελεσματικά με τις πεποιθήσεις του αποδέκτη, επηρεάζοντας αποτελεσματικά τη συμπεριφορά του σε κρίσιμες αντιπαραθέσεις, είτε σε περιόδους πολέμου, είτε σε περιόδους αυξημένης έντασης, είτε ακόμη και σε περιόδους ειρήνης (JP 3-58, 1996).

Μπορεί έτσι να υποστηριχθεί, πως μια σημαντική αρχή της παραπλάνησης έγκειται στην ικανότητα ακριβούς πρόβλεψης των ενεργειών του αντιπάλου. Παρά τη σημαντική πρόοδο στις τεχνολογικές εξελίξεις και το ευρύ φάσμα των πόρων που διαθέτουμε, ο βασικός στόχος της παραπλάνησης παραμένει εστιασμένος στη χειραγώγηση της ανθρώπινης νόησης και απόφασης. Ο ανθρώπινος νους, ως η κεντρική οντότητα που είναι υπεύθυνη για τη λήψη αποφάσεων, παρουσιάζει εγγενείς αδυναμίες που τον καθιστούν ευάλωτο στη χειραγώγηση (JP 3-13, 2012).

Η χρήση της στρατιωτικής παραπλάνησης έχει ευρεία εφαρμογή σε διάφορους τύπους στρατιωτικών επιχειρήσεων. Οι διοικητές χρησιμοποιούν αυτό το στρατήγημα για να χειραγωγήσουν -με τρόπο επωφελή- περιστάσεις, ειδικά όταν πρόκειται να ακολουθήσει κάποια ανάπτυξη δυνάμεων. Οι στόχοι της παραπλάνησης μπορούν να προσαρμοστούν στρατηγικά ώστε να ευθυγραμμιστούν με κάθε φάση των επιχειρήσεων. Είναι προφανές λοιπόν, πως υπάρχει μεγαλύτερη πιθανότητα επιτυχίας όταν οι διοικητές ενσωματώνουν την παραπλάνηση στη διαδικασία λήψης αποφάσεων σε πρώιμο στάδιο (JP 3-58, 1996).

Η στρατιωτική παραπλάνηση διαδραματίζει κρίσιμο ρόλο τόσο στις επιθετικές όσο και στις αμυντικές επιχειρήσεις πληροφοριών. Η αξιοποίηση αυτού του εργαλείου αναγνωρίζεται όλο και περισσότερο ως ένα ισχυρό πλεονέκτημα για τους διοικητές σε διάφορα επίπεδα ιεραρχίας, καθώς δημιουργεί προβλήματα στις διαδικασίες λήψης αποφάσεων των αντιπάλων, ενώ μπορεί ακόμα και να τις οδηγήσει σε λάθη (JP 3-13.1, 2002).

Η παραπλάνηση , σε αδρές γραμμές, έχει προσδιοριστεί ως μια ιεραρχική διαδικασία πολλαπλών διαστάσεων από τον Handel (1989) δηλαδή την στρατηγική, την επιχειρησιακή τέχνη, την τακτική και τα οπλικά συστήματα, η αμιγώς στρατιωτική παραπλάνηση, περιλαμβάνει -και αυτή- διακριτούς τομείς ή διαστάσεις.

Πρώτον, η Στρατηγική Στρατιωτική Παραπλάνηση , η οποία ενορχηστρώνεται υπό την αιγίδα των Ανώτατων Στρατιωτικών Διοικητών, είναι στρατηγικά προσανατολισμένη προς την

υπονόμευση των στρατιωτικών και πολιτικών ελιγμών των αντιπάλων που προωθούν τους γενικότερους στρατηγικούς στρατιωτικούς στόχους, τις πολιτικές και τις επιχειρήσεις στο πλαίσιο των Ενόπλων Δυνάμεων (JP 3-58, 1996).

Δεύτερον, η Επιχειρησιακή Στρατιωτική Παραπλάνηση λειτουργεί εντός διακριτών θεάτρων επιχειρήσεων για να συμβάλει σημαντικά στις γενικότερες στρατιωτικές προσπάθειες. Η αποτελεσματική επιρροή της στις ενέργειες των αντιπάλων ευθυγραμμίζεται στενά με τους στόχους και τις επιχειρήσεις που οριοθετούνται από ανώτερες αρχές, λειτουργώντας έτσι ως δευτερεύουσα πτυχή της στρατιωτικής παραπλάνησης εντός των Ενόπλων Δυνάμεων (JP 3-58, 1996).

Η τρίτη πτυχή, η Τακτική Στρατιωτική Παραπλάνηση, έχει σχεδιαστεί για «να σπέρνει διχόνοια και σύγχυση» στις διαδικασίες λήψης αποφάσεων των αντιπάλων διοικητών σε διάφορα κλιμάκια διοίκησης. Εποπτευόμενη από ανώτερα κλιμάκια διοίκησης, η κατηγορία αυτή επιδιώκει να παρακινήσει τους αντίπαλους διοικητές να ενεργήσουν με τρόπο που να εξυπηρετεί τους τακτικούς στόχους της παραπλανητικής κατάστασης (JP 3-58, 1996,).

Τέταρτον, η Στρατιωτική Παραπλάνηση για την Υποστήριξη της Επιχειρησιακής Ασφάλειας προσπαθεί να θέσει όρια ή και να υπονομεύσει ολικά την ικανότητα του αντιπάλου να εντοπίσει τα ευάλωτα στοιχεία που είναι απαραίτητα για την επιχειρησιακή ασφάλεια. Αυτή η μορφή παραπλάνησης στρέφεται κατά των επιχειρήσεων πληροφοριών του αντιπάλου και εναρμονίζεται απρόσκοπτα με όλες σχεδόν τις προσπάθειες αναγνώρισης, επιτήρησης και πληροφοριών (JP 3-58, 1996).

Η ενίσχυση της αξιοπιστίας της παραπλάνησης απαιτεί την εφαρμογή των παραπάνω όχι αυστηρά, αλλά με μια δόση εφευρετικότητας, ενορχηστρωμένη από τον διοικητή, προκειμένου να βελτιστοποιηθεί η προσπάθεια σε κάθε διαφορετικό περιβάλλον. Ας σημειωθεί εξάλλου ότι η επιτυχία μιας επιχείρησης παραπλάνησης μπορεί να μην γίνει γνωστή για μεγάλο χρονικό διάστημα. Για παράδειγμα, αποχαρακτηρισμένα αρχεία του Β' Παγκοσμίου Πολέμου για τις επιχειρήσεις παραπλάνησης των Ηνωμένων Πολιτειών και της Βρετανίας εμφανίστηκαν μετά από πολλά χρόνια και τότε έγιναν γνωστές οι επιχειρήσεις που διεξήχθησαν την περίοδο εκείνη (Daniel, Herbig, 1980).

Η ουσία των επιχειρήσεων παραπλάνησης εξαρτάται από τον εντοπισμό του στόχου παραπλάνησης - του κεντρικού λήπτη αποφάσεων του αντιπάλου δηλαδή - οι επιλογές του οποίου καθορίζουν το αποτέλεσμα και την επίτευξη της παραπλάνησης. Είναι ζωτικής σημασίας να υπογραμμιστεί ότι ο στόχος δεν είναι πάντα απευθείας ο ίδιος, αλλά το πληροφοριακό σύστημα που χρησιμοποιεί, δηλαδή ο αγωγός μέσω του οποίου το «αφήγημα» της παραπλάνησης θα φτάσει στον στόχο. (JP 3-58, 1996).

Το κριτήριο για μια επιτυχημένη επιχείρηση Στρατιωτικής παραπλάνησης είναι αν ο στόχος αναγκάζεται να ενεργήσει ή να απέχει από ορισμένες ενέργειες που ευνοούν τις φίλιες επιχειρήσεις. Στην ουσία, η παραπλάνηση αποσκοπεί στη διαμόρφωση των αποφάσεων και των ενεργειών του αντιπάλου σε καίριες στιγμές και τοποθεσίες. Αυτή η προσπάθεια απαιτεί συγκεκριμένους πόρους, υλικά και φυσικά στοιχεία για την πραγματοποίηση των επιθυμητών αποτελεσμάτων (JP 3-58, 1996). Ταυτόχρονα απαιτεί την

βέλτιστη δυνατή χρήση τους, συνδυαστικά ή μη και την αποτελεσματική εσωτερική επικοινωνία του οργανισμού που είναι φορέας της δράσης.

Με βάση αυτό, γίνεται απολυτός προφανής, ο ρόλος της Κεντρικής διοίκησης. Ο κεντρικός έλεγχος στις στρατιωτικές επιχειρήσεις παραπλάνησης είναι πράγματι υψίστης σημασίας, η ανάθεση αρμοδιοτήτων εποπτείας σε ένα μέλος της ευρύτερης ομάδας επιχειρήσεων πληροφοριών εξασφαλίζει τον συντονισμό και τον έλεγχο στα υψηλότερα κλιμάκια της επιχείρησης. Αυτό εγγυάται τη αναγκαία γνώση και πληροφόρηση μεταξύ όλων των συμμετεχόντων (FM 6-0, 2014).

Ας σημειωθεί ότι τα μέσα παραπλάνησης περιλαμβάνουν τεχνικές, μεθόδους και πόρους που μεταδίδουν πληροφορίες στον στόχο της παραπλάνησης. Ο στόχος είναι να εξαναγκαστεί ο στόχος να υιοθετήσει την επιδιωκόμενη αντίληψη που διακινεί η επιχείρηση της παραπλάνησης (JP 3-58, 1996).

Οι επιχειρήσεις παραπλάνησης αναπαράγουν ενδείξεις που περιγράφουν προθέσεις ή ικανότητες που δεν διαθέτει ο διοικητής των φίλιων δυνάμεων. Το σύστημα πληροφοριών του αντιπάλου μπορεί να απορρίψει κρίσιμες ενδείξεις εάν προέρχονται από μια μοναχική πηγή. Η αξιοπιστία της αφήγησης παραπλάνησης εξαρτάται από την παρουσίαση ενδείξεων, αληθινών και ψευδών, από μυριάδες πηγές. Αυτό ενισχύει την αυθεντικότητα, δημιουργώντας μια αύρα επαλήθευσης και αυξάνοντας την πιθανότητα ο στόχος να αντιληφθεί την εξαπάτηση ως γνήσια. Ωστόσο, ανεπαρκή στοιχεία ή υποψίες σχετικά με τις πηγές μπορεί να αποκαλύψουν το τέχνασμα (JP 3-58, 1996).

Οι ενέργειες που απεικονίζονται στην παραπλανητική αφήγηση ενσωματώνουν γεγονότα παραπλάνησης. Ένα γεγονός παραπλάνησης χρησιμεύει ως αγωγός παραπλάνησης, που τίθεται σε εφαρμογή σε συγκεκριμένες περιπτώσεις και τοποθεσίες για να στηρίξει μια επιχείρηση παραπλάνησης. Τα στοιχεία που απεικονίζουν τα μέσα παραπλάνησης, τα οποία περιλαμβάνουν τεχνικές, μεθόδους και πόρους που μεταφέρουν πληροφορίες στον στόχο, ενσωματώνονται στο γεγονός παραπλάνησης. Τα μέσα που χρησιμοποιούνται για τον σκοπό αυτό, μπορεί κάποιος να τα περιγράψει σε αδρές γραμμές ως φυσικά, τεχνητά και διοικητικά/ διαχειριστικά (JP 3-58, 1996).

Όσον αφορά τα φυσικά μέσα, αυτά περιλαμβάνουν κατά κύριο λόγο τις επιχειρήσεις των μονάδων αναγνώρισης, παράλληλα με την επιτήρηση και την κίνηση των δυνάμεων. Επιπλέον, τα φυσικά μέσα περιλαμβάνουν τον εξοπλισμό προσομοιώσεων, καθώς και τη χρήση τακτικών όπως ο καπνός, η συσκότιση, ο ήχος κλπ για την παραπλάνηση των ανθρώπινων και τεχνικών αισθητήρων (JP 3-58, 1996). Επιχειρούν έτσι εμπράκτως να περιορίσουν τις δυνατότητες πληροφοριών του αντιπάλου, είτε είναι εναέριες, είτε επίγειες, είτε διαστημικές .

Τα τεχνητά μέσα περικλείουν διάφορα στρατιωτικά υλικά και επιχειρησιακές τεχνικές σχεδιασμένες να μεταφέρουν ή να αποκρύπτουν επιλεγμένες πληροφορίες από τον στόχο παραπλάνησης. Αυτό περιλαμβάνει την απορρόφηση ή ανάκλαση ενέργειας, την εκπομπή ή απορρόφηση βιολογικών ουσιών και πυρηνικών σωματιδίων. Στην ουσία, η ηλεκτρονική παραπλάνηση ευθυγραμμίζεται με αυτό το πλαίσιο μέσω της χρήσης τεχνολογικών μέσων (JP 3-58, 1996).

Τα διοικητικά/διαχειριστικά μέσα περιλαμβάνουν μια σειρά μεθόδων, τεχνικών και πόρων που χρησιμοποιούνται για τη μεταφορά ή τον περιορισμό προφορικών και οπτικών πληροφοριών που στοχεύουν στον αποδέκτη της παραπλάνησης, συχνά με τη χρήση κατασκευασμένων πληροφοριών (JP 3-58, 1996).

Δεν μπορεί κάποιος παρά να παρατηρήσει πως ένα μεγάλο μέρος αυτών των προσπαθειών κατατείνει στην εκμετάλλευση των προκαταλήψεων του στόχου. Η ανθρώπινη φύση, εξελικτικά μας ωθεί να σκεφτόμαστε μέσα από μοτίβα εξήγησης της συμπεριφοράς ή των φαινομένων, αυτή η ψυχολογική προδιάθεση παραμένει ισχυρή, επηρεάζοντας βαθιά τις αντιλήψεις και τις αποφάσεις. Αναγνωρίζοντας το γεγονός αυτό, η αποκρυπτογράφηση των προκαταλήψεων του επιδιωκόμενου στόχου παραπλάνησης γίνεται ένα ισχυρό εργαλείο για όσους επιχειρούν ή σχεδιάζουν μια επιχείρηση Στρατιωτικής παραπλάνησης (JP 3-58, 1996).

Συμπερασματικά, ένα επιτυχημένο σχέδιο παραπλάνησης δεν πρέπει να αποκλίνει δραστικά από τις προκαταλήψεις του στόχου, καθώς οι έντονες αποκλίσεις μπορεί να προκαλέσουν υποψίες και να αποκαλύψουν την αλήθεια. Τα βέλτιστα αποτελέσματα προκύπτουν από ένα σενάριο που είναι απόλυτα αληθοφανές από τον στόχο στο σύνολό του, με τα επιμέρους στοιχεία να ευθυγραμμίζονται άψογα. Η παραπλάνηση θα πρέπει να εναρμονίζεται με τις προϋπάρχουσες πεποιθήσεις του στόχου, περιλαμβάνοντας το φιλικό δόγμα, τη στρατηγική προσέγγιση, τις αξίες και τους γενικότερους στόχους του (JP 3-13.4, 2012).

2.3 Πόλεμος και Παραπλάνηση

Οι θεμελιώδεις αρχές του πολέμου, της δύναμης και της παραπλάνησης, αποτέλεσαν το θεμέλιο των αρχαίων στρατιωτικών θεωριών του Σουν Τζου ο οποίος γύρω στο 550 π.Χ. έδωσε έμφαση στην υπονόμευση, τη σύγχυση, την αποδιοργάνωση και το χτύπημα του ηθικού του εχθρού για να εξασφαλίσει τη νίκη (Breuer, 2002).

Αιώνες αργότερα, κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, και οι δύο πλευρές επεδίωξαν οικονομικά, πολιτικά και ψυχολογικά πλεονεκτήματα μέσω μιας σύνθετης σειράς ίντριγκας, εξαπάτησης και πλαστογραφίας - μέθοδοι που θα έλεγε κανείς πως «ξεπήδησαν» από τις πρακτικές του Σουν Τζου, προσαρμοσμένες στο σύγχρονο πλαίσιο. Οι Δυτικοί Σύμμαχοι, ιδίως οι Βρετανοί και αργότερα οι Αμερικανοί, εφάρμοσαν έξυπνα αυτές τις αρχές για να αποκτήσουν καίρια πλεονεκτήματα που θα μπορούσαν να γείρουν τη ζυγαριά της νίκης (Breuer, 2002).

Ενώ έχουν καταγραφεί πολυάριθμες μαρτυρίες για συμβατικές συγκρούσεις στο πεδίο της μάχης, στρατηγικούς ελιγμούς και πράξεις γενναιότητας σε σχέση με τον Β' Παγκόσμιο Πόλεμο, είναι επιτακτική ανάγκη να αναγνωριστεί ο κρίσιμος ρόλος που έπαιξε συχνά η παραπλάνηση στη διαμόρφωση των αποτελεσμάτων και στην αλλαγή της πορείας της σύγκρουσης. Λαμβάνοντας υπόψη ότι οι επιχειρήσεις παραπλάνησης σε καιρό ειρήνης έχουν γίνει κοινός τόπος μεταξύ των κρατών με βάση ιστορικές περιπτώσεις, είναι προφανές ότι το πεδίο της παραπλάνησης διευρύνεται σημαντικά σε περιόδους πολέμου. Καθώς οι

ηθικοί φραγμοί υποχωρούν και η επιβίωση ενός έθνους καθίσταται υψίστης σημασίας, η στρατηγική χρήση τακτικών που μπορεί να ακροβατούν στα όρια της «νομιμότητας» κατά τη διάρκεια της ειρήνης βρίσκει αυξημένη εφαρμογή στο πλαίσιο του πολέμου (Breuer, 2002).

Ιδιαίτερο ενδιαφέρον έχει η αναπτυσσόμενη συζήτηση γύρω από τα ηθικά όρια της εξαπάτησης όπως την περιγράφει ο Kohen (2016). Το ηθικό δίλημμα που περιβάλλει τη στρατιωτική παραπλάνησης είναι περίπλοκο, με τρεις πιθανές στάσεις που η καθεμία θέτει εγγενείς προκλήσεις. Η μία άποψη υποστηρίζει ότι οι ηθικές αρχές που διέπουν τις ανθρώπινες αλληλεπιδράσεις πρέπει να επεκτείνονται στο πεδίο της μάχης, αποφασίζοντας ότι οι συμβατικές απαγορεύσεις κατά της εξαπάτησης και της παραπλάνησης πρέπει να ισχύουν ακόμη και στον πόλεμο. Αντίθετα, η αντίθετη άποψη υποστηρίζει ότι ο πόλεμος αποτελεί μια μοναδική σφαίρα που εξαιρείται από τους γενικούς ηθικούς περιορισμούς για την εξαπάτηση. Η τρίτη άποψη που επιχειρεί να ισορροπήση ανάμεσα στις άλλες δύο, επιτρέπει ορισμένες μορφές εξαπάτησης στον πόλεμο, ενώ απορρίπτει άλλες.

Είναι προφανές ότι καμία από αυτές τις απόψεις δεν φαίνεται απολύτως ικανοποιητική με την πρώτη ματιά. Η αρχική προοπτική υπεραπλουστεύει, καθώς κάποιος βαθμός παραπλάνησης αναγνωρίζεται ευρέως ως ηθικά επιτρεπτός στη μάχη. Η δεύτερη άποψη, που συγχωρεί την αχαλίνωτη απάτη στον πόλεμο, έρχεται σε έντονη αντίθεση με τους εξελισσόμενους διεθνείς κανόνες που προωθούν τις ηθικές αξίες και τις ειρηνικές λύσεις. Η τρίτη θέση, που διακρίνει την αποδεκτή από την απαράδεκτη εξαπάτηση κατά τη διάρκεια του πολέμου, είναι διαφοροποιημένη. Ωστόσο, η διαφοροποίηση αυτή γίνεται πολύπλοκη με μια πιο προσεκτική εξέταση. Η εξαπάτηση, ακόμη και όταν είναι ηθικά δικαιολογημένη για τη διάσωση ζωών, θα μπορούσε να συγκρουστεί με την πράξη της θανάτωσης στον πόλεμο, εγείροντας ερωτήματα σχετικά με την ηθική σημασία των διαφόρων μορφών εξαπάτησης.

Ας σημειωθεί βέβαια ότι η επιτακτική ανάγκη διατήρησης, μιας έστω ελάχιστης εμπιστοσύνης, μεταξύ των αντιμαχόμενων προκειμένου σε κάποιο στάδιο να επιτευχθεί ειρήνευση δικαιολογεί ορισμένους περιορισμούς στη στρατιωτική εξαπάτηση, αυτή η πολιτική λογική δεν είναι καθολική. Επιπλέον, η συσχέτιση μεταξύ αυτών των ορίων και της προθυμίας των αντιπάλων να τερματίσουν τις εχθροπραξίες είναι αβέβαιη. Τελικά, τα ηθικά θεμέλια αλλά και τα όρια της στρατιωτικής παραπλάνησης παραμένουν ασαφή, περιλαμβάνοντας εκτιμήσεις για τη βασική ανθρώπινη αξιοπρέπεια, την επιδίωξη της ειρήνης και τις περιπλοκές της συμπεριφοράς σε καιρό πολέμου.

2.4 Ειρήνη και Παραπλάνηση-Προπαγάνδα και Κοινή γνώμη

Η σκόπιμη και έξυπνη χειραγώγηση των κοινωνικών συνηθειών και πεποιθήσεων του γενικού πληθυσμού μπορεί να είναι εξαιρετικά αποτελεσματικό μέσο. Αυτή η χειραγώγηση είναι ζωτικής σημασίας λόγω της πρόκλησης που αντιμετωπίζουν οι πολίτες να διαμορφώσουν καλά ενημερωμένες απόψεις για περίπλοκα οικονομικά, πολιτικά και ηθικά ζητήματα, ειδικά στην σημερινή εποχή που οι σημαντικές πληροφορίες μπορούν να «χαθούν

στο θόρυβο» που παράγουν τα πολλαπλάσια μέσα ενημέρωσης αλλά και διαδραστικό web2.0. Κατά συνέπεια, η επιρροή πάνω στους πυλωρούς της δημοσιογραφίας από την μια και εν γένει στους διαμορφωτές της κοινής γνώμης από την άλλη, καθίσταται ζωτικής σημασίας (Bernays, 2015).

Η διεθνής προπαγάνδα υπό την μορφή συστηματικού εργαλείου στην παγκόσμια πολιτική χρησιμοποιήθηκε σε μεγάλη κλίμακα, επιτυχία και για μεγάλο χρόνο από τη Σοβιετική Ρωσία, η οποία ισχυριζόταν ότι υπερασπίζεται την παγκόσμια αλήθεια μέσω της Κομμουνιστικής Διεθνούς. Αυτό σηματοδότησε την περίπτωση ενός σύγχρονου κράτους που δημιούργησε έναν μηχανισμό διεθνούς προπαγάνδας μεγάλης κλίμακας. (Carr, 2011).

Υπήρξαν βέβαια και παραδείγματα όπου εμφανίστηκαν προσπάθειες για τον περιορισμό της εχθρικής προπαγάνδας, με παράδειγμα τη συμφωνία των ραδιοφωνικών εταιρειών Γερμανίας-Πολωνίας να μην προσβάλλουν τα εθνικά αισθήματα. Ωστόσο, όπως και η αναποτελεσματικότητα του περιορισμού των στρατιωτικών όπλων, οι περιορισμοί αυτοί αποδείχθηκαν μάταιοι (Carr, 2011).

Στην πράξη, η προπαγάνδα εξαρτάται από την κατανόηση και την επίκληση των επιθυμιών των μαζών για να διαμορφώσει στάσεις εντός μιας χώρας, δηλαδή τις σκέψεις, θέσεις, ακόμα και υποτιθέμενα γεγονότα που είναι εκ των προτέρων έτοιμοι να αποδεχθούν ως πραγματικότητα ή που συμπίπτουν με προηγούμενες αντιλήψεις τους (Hetherington, 2006). Έτσι, μέσα σε αυτό το πλαίσιο και όντας μια μορφή πειστικής επικοινωνίας, η προπαγάνδα επιδιώκει να διαμορφώσει τις συμπεριφορές και τις απόψεις των αποδεκτών σύμφωνα με τις προτιμήσεις των προπαγανδιστών (Gestrlé, 2014). Η αποτελεσματικότητά της έγκειται στην προσαρμογή στις μεταβαλλόμενες συνθήκες και αντιλήψεις, επιτυγχάνοντας εξοικείωση μέσω της επανάληψης (Hetherington, 2006). Ειδικότερα, η αποτελεσματική προπαγάνδα αποκρύπτει τη φύση της, χρησιμοποιώντας ως μέσο για την διάδοσή της εκείνα τα κανάλια που δεν θα δημιουργήσουν κάποια υποψία ως προς την αυθεντικότητα και την αλήθεια του μηνύματος (Gestrlé, 2014).

Παρά τους αρνητικούς συνειρμούς της, η ηθική αξιολόγηση της προπαγάνδας εξαρτάται από το πλαίσιο, τον σκοπό και την ακεραιότητα της πληροφορίας. Χρησιμεύει ως μέσο για τη διάδοση ιδεών, την κατασκευή καταστάσεων και την επανανοηματοδότηση γεγονότων, επηρεάζοντας και οργανώνοντας τελικά ένα χάος (Bernays, 2015).

Δεν θα ήταν μακριά από την πραγματικότητα μια επιχειρηματολογία στην οποία ένα από τα κεντρικά σημεία για την αξία της προπαγάνδας θα ήταν πως το πιο ισχυρό όπλο δεν είναι το στρατιωτικό ή το οικονομικό, αλλά η (χειραγωγημένη) κοινή γνώμη (Carr, 2011). Η χειραγώγηση, μια τεχνική με μακρά ιστορία , μακρά όσο και η ρητορεία και ο δημόσιος λόγος, καταγράφεται ήδη στον Όμηρο όταν κατά τη διάρκεια του Τρωικού Πολέμου, ο Οδυσσέας επηρέασε διακριτικά το ηθικό των Ελλήνων για να παρατείνει την πολιορκία (Κουσκουβέλης, 2015).

Ο επηρεασμός της κοινής γνώμης εκτείνεται πέρα από τους απλούς αριθμούς και απαιτεί χειραγώγηση για τη διαμόρφωση των αντιλήψεων (Bok, 1999). Οι περιστάσεις διαμορφώνουν τις απόψεις των ανθρώπων και, συνεπώς, ο χειρισμός αυτών των περιστάσεων μπορεί να επηρεάσει το δημόσιο αίσθημα. Από την πλευρά του, ο Edward H.

Carr υποστηρίζει ότι η «δύναμη της πειθούς» δεν πρέπει να υποτιμάται, καθώς είναι άρρηκτα συνδεδεμένη με άλλες μορφές εξουσίας, πράγματι θεσμοί όπως η Καθολική Εκκλησία αναγνώρισαν και αξιοποίησαν τη μαζική επιρροή, καθιερώνοντας έναν πρόδρομο της λογοκρισίας στον Μεσαίωνα (Carr, 2011).

Η επιρροή επί της σκέψης λειτουργεί υποσυνείδητα, με στόχο την επίτευξη συγκεκριμένων στόχων (Tilly, 2005). Οι διαδικασίες σκέψης καθοδηγούνται από το τρίπτυχο Συνθήκες (περιβάλλον) - Συμφέροντα - Σκοπός, εξυπηρετώντας τελικά έναν στόχο (Carr, 2011). Οι θεωρίες που διασπείρονται για να υπονομεύσουν το κύρος ενός εχθρού είναι μια εκδήλωση της σκέψης με γνώμονα τον σκοπό. Η κοινή γνώμη αναμφισβήτητα διαμορφώνεται από την κοινωνική θέση και τα συμφέροντα, επιτρέποντας στις κυρίαρχες ομάδες να προπαγανδίζουν τις απόψεις τους. Ενώ οι δημοκρατίες και τα ολοκληρωτικά καθεστώτα διαφέρουν ως προς την επιβολή, και τα δύο αναγνωρίζουν τη σημασία της προπαγάνδας και της εσωτερικής νομιμότητας (Carr, 2011). Η αλήθεια ή έστω η ύπαρξη εμφανών τμημάτων αλήθειας αποτελεί προϋπόθεση και θεμέλιο της αποτελεσματικής προπαγάνδας, καθώς δημιουργεί την αίσθηση της αξιοπιστίας (Ραγιές, 2014). Η εμπλοκή των μέσων ενημέρωσης-στην σημερινή εποχή- καθίσταται κρίσιμη, καθιστώντας την ύπαρξη (και) αλήθειας μονόδρομη στρατηγική.

Είναι αυτονόητο πλέον, σε κάθε θεωρητικό ρεύμα της επιστήμης των Διεθνών Σχέσεων, πόσο αυξημένης σημασίας είναι ο ρόλος της επικοινωνίας στη διαμόρφωση μιας «Διεθνούς κοινής γνώμης» και πόσο απαραίτητες οι στρατηγικές δυνατότητες της παραπληροφόρησης, που περιλαμβάνουν τη διαστρέβλωση της αντικειμενικής πληροφόρησης (Gestrlé, 2014). Βέβαια, ο βαθμός στον οποίο μπορεί να ελεγχθεί η κοινή γνώμη αντιμετωπίζει εγγενή όρια. Αυτός ο περιορισμός προκύπτει κυρίως από την ανάγκη να ευθυγραμμιστεί, σε κάποιο βαθμό, με τα πραγματικά γεγονότα.

Ορισμένα αντικειμενικά γεγονότα δεν μπορούν -πέρα από έναν βαθμό- να υπόκεινται διαστρέβλωση (ή Τραμπικού χαρακτήρα εναλλακτικές πραγματικότητες). Ουσιαστικά, ο κίνδυνος αποκάλυψης της αλήθειας λειτουργεί ως βασικός παράγοντας που περιορίζει την αποτελεσματικότητα των προσπαθειών πειθούς. Επιπλέον, η παρουσία της εκπαίδευσης και της κατάρτισης, συμβάλλει στη μείωση της δυνητικής επιρροής του δημόσιου αισθήματος (Mearsheimer, 2012). Τελικά, η προπαγάνδα, καθώς χειραγωγεί και ερμηνεύει τα γεγονότα για την εξυπηρέτηση συγκεκριμένων στόχων, κρύβει εγγενώς μια αυτο-υπονομευτική πτυχή (Carr, 2011)

Στο πεδίο της διεθνούς πολιτικής, μια υπαρκτή τάση συμπεριφοράς περιλαμβάνει την παραβίαση των καθιερωμένων κανόνων με πολλές φορές ελάχιστες επιπτώσεις. Αυτή η δυναμική αναγκάζει τα κράτη να υιοθετούν κάθε αναγκαίο μέσο για τη διαφύλαξη της ασφάλειάς τους, ακόμη και αν αυτό συνεπάγεται την προσφυγή σε παραπλανητικές πρακτικές. Η χειραγώγηση της κοινής γνώμης αναδεικνύεται σε ισχυρό εργαλείο στην προσπάθεια αυτή, που διευκολύνεται ιδιαίτερα από την άνιση πρόσβαση στην πληροφόρηση και τη δυνατότητα ελέγχου της ροής της (Mearsheimer, 2012).

Στον πυρήνα αυτού του τοπίου βρίσκεται η έννοια του ψεύδους - ένα υπολογισμένο ψέμα με σκοπό την εξαπάτηση. Το ψέμα ενσαρκώνει μια ενεργητική μορφή παραπλάνησης,

που περιλαμβάνει την κατασκευή, την άρνηση και την επιλεκτική αντιπαράθεση γεγονότων ώστε να οδηγηθούμε σε ένα ψευδές συμπέρασμα χωρίς να το δηλώσουμε ανοιχτά. Ωστόσο, η χάραξη μιας σαφούς γραμμής μεταξύ του ψεύδους και της διαστρέβλωσης, της στρατηγικής έμφασης ή παράλειψης γεγονότων, είναι ένα πολύπλοκο εγχείρημα. Αυτή η ασάφεια υπογραμμίζει τη δαιδαλώδη φύση της πολιτικής αρένας, που δημιουργεί πρόσφορο έδαφος για χειραγώγηση που πολλές φορές είναι προσαρμοσμένη στην επίτευξη διακριτών στρατηγικών στόχων (Mearsheimer, 2012). Η επιτυχής προσπάθεια για την υλοποίηση δεδομένων στόχων εξωτερικής πολιτικής μπορεί να χρησιμεύσει στην άμβλυνση των ηθικών διλημμάτων που περιβάλλουν την παραπλάνηση, καθιστώντας την πιο αποδεκτή (Mearsheimer, 2012).

Τα που χρησιμοποιούνται για την παραπλάνηση των κρατών στις μεταξύ τους σχέσεις, δηλαδή τα τρόπον τινά διακρατικά ψέματα , αποτελούν μια εξέχουσα πτυχή αυτού του πολύπλοκου τοπίου. Στοχεύουν σε άλλα έθνη, εξυπηρετώντας είτε την εξασφάλιση στρατηγικού πλεονεκτήματος είτε την παρεμπόδιση των αντιπάλων από την εξασφάλιση ενός ή την εν γένει υποχώρησή τους. Η στρατηγική αυτή συχνά απευθύνεται σε αντίπαλα κράτη, αν και ακόμη και οι σύμμαχοι μπορεί να μην εξαιρούνται. Η διεθνής ψευδολογία είναι ιδιαίτερα εμφανής σε περιβάλλοντα που χαρακτηρίζονται από υψηλό κίνδυνο και έντονο ανταγωνισμό στον τομέα της ασφάλειας, κατά τη διάρκεια κρίσεων και κυρίως σε περιόδους πολέμου. Οι καταστάσεις αυτές παρέχουν τα απαραίτητα κίνητρα για τη διακρατική εξαπάτηση (Hetherington, 2006).

Η επικράτηση του ψεύδους είναι συχνά πιο έντονη στο πλαίσιο χωρών που είναι εμπλεκόμενες σε υψηλό ανταγωνισμό. Τέτοια κράτη, που αισθάνονται διαρκώς ευάλωτα, τείνουν να υιοθετούν στρατηγικές που αποσκοπούν στην ενίσχυση της αίσθησης της ασφάλειάς τους. Έτσι, η πράξη της παραπλάνησης γίνεται συνυφασμένη με τις προσπάθειες να διέλθουν ασφαλώς μέσα από «θάλασσες αβεβαιότητας και κινδύνων» (Mearsheimer, 2012).

Σε περιόδους κρίσεων, ένα κράτος που οδηγείται από μια πολιτική επιδίωξη αποφυγής συγκρούσεων έχει κίνητρο να διαδίδει ψεύδη, αν πιστεύει ότι αυτό θα μπορούσε να συμβάλει στην επίλυση της κρίσης. Ωστόσο, ένα πλαίσιο κρίσης γεννά αμοιβαίο σκεπτικισμό μεταξύ των αντιμαχόμενων πλευρών, καθιστώντας σημαντικά δύσκολη την πειστική διάδοση ψεμάτων . Από την άλλη πλευρά, το θέατρο ενός πολέμου παρέχει πρόσφορο έδαφος για τη διάδοση ψευδών γεγονότων, η πιεστική ανάγκη να διασφαλιστεί η ύπαρξη ενός έθνους απέναντι σε υπαρξιακές απειλές ανοίγει το δρόμο για την εμφάνιση παραπλανητικών πρακτικών (Mearsheimer, 2012).

Η "κινδυνολογία", ένα φαινόμενο που συνεπάγεται τη διάδοση ψεμάτων στους πολίτες μιας χώρας σχετικά με τις αντιληπτές εξωτερικές απειλές, χρησιμεύει ως μηχανισμός για την εξασφάλιση υποστήριξης των εθνικών συμφερόντων. Η πρακτική αυτή υλοποιείται όταν οι ηγέτες αντιλαμβάνονται μια αναδυόμενη απειλή και θεωρούν την εξαπάτηση ως μέσο διαμόρφωσης των αντιλήψεων του κοινού. Ο στόχος επεκτείνεται πέρα από τον επηρεασμό του γενικού πληθυσμού, περιλαμβάνοντας ακόμη και μορφωμένες ελίτ και κυβερνητικούς γραφειοκράτες. Η κινδυνολογία επιδιώκει να δημιουργήσει την απαραίτητη

υποστήριξη για μια συγκεκριμένη πολιτική πορεία, θυσιάζοντας συχνά τις δημοκρατικές αρχές για στρατηγικά οφέλη (Mearsheimer, 2012).

Οι στρατηγικές συγκάλυψης, που συνιστούν μια μορφή παραπλάνησης, χρησιμοποιούνται συχνά για τη συγκάλυψη αμφιλεγόμενων πολιτικών ή δράσεων. Η πρόθεση δεν είναι να πάντα προστατευθούν τα ίδια τα άτομα από την ευθύνη, αλλά μάλλον να διασφαλιστούν τα συμφέροντα του ίδιου του έθνους. Οι στρατηγικές αυτές μπορούν να λάβουν πολλαπλές μορφές, όπως η υποβάθμιση των αποτυχιών της πολιτικής ή η συγκάλυψη προκλητικών στρατηγικών. Ενώ οι συγκαλύψεις μπορεί να ευθυγραμμίζονται με τους στρατηγικούς στόχους, ενέχουν επίσης εγγενείς κινδύνους, οδηγώντας ενδεχομένως σε απρόβλεπτες συνέπειες (Mearsheimer, 2012).

Ας σημειωθεί πως και οι εθνικιστικοί μύθοι αντιπροσωπεύουν μια ακόμη διάσταση παραπλάνησης, η οποία περιστρέφεται γύρω από τη δημιουργία ψευδών αφηγήσεων σχετικά με την ιστορία ενός έθνους. Αυτοί οι μύθοι χρησιμεύουν για την κατασκευή μιας συλλογικής ταυτότητας που είναι απαραίτητη για την οικοδόμηση του έθνους (αφηγήσεις για nation building) . Σε αυτό το πλαίσιο, οι ιστορικές αφηγήσεις αναλαμβάνουν κεντρικό ρόλο στην προώθηση της ενότητας και στη διαμόρφωση του δημόσιου αισθήματος και την σφυρηλάτηση μιας ταυτότητας (Mearsheimer, 2012). Σε περιόδους ανασφάλειας, οι ηγέτες μπορεί να καταφεύγουν στην εθνικιστική-πατριωτική ρητορική, μετατρέποντας ουσιαστικά την πειθώ σε προπαγάνδα και πολιτική κατήχηση. Η πρακτική αυτή εκμεταλλεύεται τα τρωτά σημεία των πολιτών και αξιοποιεί τα εθνικιστικά τους αισθήματα (Nye, 2009). Ο περίπλοκος ιστός των ψεμάτων και της χειραγώγησης στο πλαίσιο της διεθνούς πολιτικής υπογραμμίζει την πολύπλευρη φύση της παραπλάνησης ως στρατηγικού εργαλείου.

3 Ψηφιακή τεχνολογία και η διάχυση της πληροφόρησης

3.1 Η εξέλιξη του πολέμου πληροφορίας από το ’90 ως την εποχή της Μετά- αλήθειας

Ο 21ος αιώνας έχει εγκαινιάσει μια αλλαγή παραδείγματος που χαρακτηρίζεται από τεχνολογικές εξελίξεις, επικοινωνιακά εργαλεία και ευρεία πρόσβαση στο Διαδίκτυο. Στις δυτικές φιλελεύθερες δημοκρατίες, ο σύγχρονος πολίτης έχει εξελιχθεί σε κάτοικο τόσο της κοινωνίας της πληροφορίας όσο και της κοινωνίας των δικτύων. Αυτή η δυναμική δηλώνει την τεχνική ικανότητα του πολίτη να δημιουργεί συνδέσεις με σχεδόν οποιοδήποτε άτομο (Castells, 2008). Η γνώση και η πληροφόρηση έχουν αναδειχθεί ως πρωταρχικές αξίες στην κοινωνία της πληροφορίας, ενώ η κοινωνία των δικτύων, μια πτυχή της κοινωνίας της πληροφορίας, μετατρέπει τους πολίτες σε κόμβους μέσα σε ένα παγκοσμιοποιημένο δίκτυο. Αυτή η μεταμόρφωση επιτρέπει τη σφυρηλάτηση απεριόριστων σχέσεων μέσω μέσων όπως το Διαδίκτυο και το τηλέφωνο (Castells, 2008).

Στη ρουτίνα του "δικτυωμένου πολίτη", μια πληθώρα πληροφοριών όχι μόνο λαμβάνεται αλλά και παράγεται και διαδίδεται μεταξύ των κοινωνικών του κύκλων. Παρά το γεγονός ότι απολαμβάνει σχεδόν απεριόριστη πρόσβαση σε πηγές και κανάλια πληροφόρησης, το άτομο αυτό βρίσκει τον εαυτό του περιορισμένο από το χρόνο και την απουσία δεξιοτήτων για να «κοσκινίσει» τον κατακλυσμό των ψηφιακών πληροφοριών(Cronin & Crawford, 1999). Μέσα σε αυτή τη χιονοστιβάδα δεδομένων, τα όρια μεταξύ αλήθειας και ψεύδους γίνονται όλο και πιο δυσδιάκριτα. Αυτή η δυσχερής θέση αναγνωρίζεται καλά όχι μόνο από πολιτικά πρόσωπα, από τα ΜΜΕ και ιδιωτικές εταιρείες, αλλά και από κράτη. Αυτοί οι παράγοντες αναγνωρίζουν τη λανθάνουσα δυνατότητα ή επιτακτική ανάγκη (ανάλογα με την οπτική τους) να εμπλακούν σε έναν διαρκή πληροφοριακό πόλεμο είτε για να διαταράξουν είτε για να περιχαρακώσουν (στον βαθμό που κάτι τέτοιο είναι πράγματι εφικτό) την κοινωνία της πληροφορίας, επιτυγχάνοντας έτσι τους επιθυμητούς πολιτικούς, οικονομικούς, ακόμη και στρατιωτικούς στόχους τους (Cronin & Crawford, 2006).

Στις δεκαετίες του 1980 και του 1990, τοποθετείται χρονικά η γέννηση της ίδιας της έννοιας (και φυσικά της δυνατότητας) του πληροφοριακού πολέμου (ΠΚ) στα δυτικά φιλελεύθερα δημοκρατικά έθνη. Αρχικά περιοριζόμενος στον στρατιωτικό τομέα, ο πληροφοριακός πόλεμος ήταν απόρροια του ηλεκτρονικού πολέμου, των ψυχολογικών επιχειρήσεων, της στρατιωτικής παραπλάνησης και της επιχειρησιακής ασφάλειας πληροφοριών (Hutchinson, 2006). Η κύρια εστίασή του ήταν η χρήση της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) για την παραβίαση των δομών ΤΠΕ του αντιπάλου με

σκοπό τη διατάραξη ή την απόκτηση δεδομένων που σχετίζονται με τους πόρους ή τις στρατιωτικές στρατηγικές του αντιπάλου (Endsley & Jones, 1997).

Αυτή η ερμηνεία του πληροφοριακού πολέμου εξυπηρετούσε κυρίως την απόκτηση ανταγωνιστικού πλεονεκτήματος στο πεδίο της μάχης, ενισχύοντας τις δυνατότητες πληροφοριών, στόχευσης, διοίκησης και ελέγχου. Ενδεικτικό παράδειγμα ήταν ο πόλεμος του Κόλπου το 1991, όπου τα στρατεύματα του διεθνούς συνασπισμού χρησιμοποίησαν την τεχνολογική υπεροχή για να εξουδετερώσουν τον ιρακινό στρατό, διαταράσσοντας τα δίκτυα επικοινωνίας του, κυριαρχώντας στις επιχειρήσεις πληροφοριών και διαλύοντας το πλαίσιο ΤΠΕ του (Hutchinson, 2006).

Ωστόσο, ο Πόλεμος του Κόλπου αποκάλυψε την ανάδυση μιας άλλης πτυχής στο πλαίσιο του πληροφοριακού πολέμου: τη διαχείριση των μέσων ενημέρωσης. Η πτυχή αυτή προέκυψε ως απάντηση στα διδάγματα που αντλήθηκαν από την «ήττα στο εσωτερικό μέτωπο» κατά τη διάρκεια του πολέμου του Βιετνάμ, όπου η κάλυψη από τα μέσα ενημέρωσης συνέβαλε στην απώλεια του πολέμου λόγω και των μαζικών διαμαρτυριών των πολιτών. Ο πόλεμος του Κόλπου έδειξε ότι ο έλεγχος των αφηγημάτων που προέρχονταν από τα μέσα ενημέρωσης ήταν ζωτικής σημασίας για τη διαμόρφωση της κοινής γνώμης (Carruthers, 2000). Κατά τη διάρκεια του Πολέμου του Κόλπου, ασκήθηκε αυστηρός έλεγχος στους εκπροσώπους των μέσων ενημέρωσης, οι οποίοι κατευθύνθηκαν να διαδίδουν μόνο εγκεκριμένες πληροφορίες, προωθώντας μια συνεκτική αφήγηση που παρουσίαζε τη σύγκρουση ως δίκαιη και ανθρωπιστική (Knightley, 2000).

Αν και η διαχείριση των μέσων ενημέρωσης αναγνωρίστηκε ως συστατικό στοιχείο του πολέμου, δεν υπήρξε συναίνεση σχετικά με την ένταξή της στο πλαίσιο του πληροφοριακού πολέμου. Για παράδειγμα, ο ορισμός του πολέμου των πληροφοριών από την Αεροπορία των ΗΠΑ το 1995 κάλυπτε δραστηριότητες που αποσκοπούσαν στη διατάραξη ή την εκμετάλλευση των πληροφοριών του εχθρού, την προστασία από τέτοιες δραστηριότητες και την αξιοποίηση των δικών μας δυνατοτήτων πληροφόρησης. Μια ευρύτερη προοπτική υποστηρίχθηκε από τον Martin Libicki, που περιλαμβάνει τις ακόλουθες δραστηριότητες (Libicki, 1996):

- Πόλεμος διοίκησης και ελέγχου με στόχο τις δομές διοίκησης του εχθρού.
- Πόλεμος βασισμένος στις πληροφορίες που χρησιμοποιεί έξυπνους αισθητήρες και όπλα για τη λήψη αποφάσεων σε πραγματικό χρόνο, παρεμποδίζοντας παράλληλα τις δυνατότητες του αντιπάλου.
- Ηλεκτρονικός πόλεμος που διακόπτει τη μετάδοση πληροφοριών του αντιπάλου και διασφαλίζει τις δικές του.
- Ψυχολογικός πόλεμος με την επεξεργασία πληροφοριών για τον άμεσο επηρεασμό της κοινής γνώμης, του στρατιωτικού προσωπικού ή των διοικητών του εχθρού.
- Πόλεμος hacking που περιλαμβάνει επιθέσεις σε συστήματα πληροφοριών και ελέγχου υπολογιστών.

- Οικονομικός πόλεμος πληροφοριών που περιλαμβάνει την παρεμπόδιση της ροής οικονομικών πληροφοριών για τον έλεγχο των αγορών.
- Κυβερνοπόλεμος που καλύπτει δραστηριότητες από την ηλεκτρονική τρομοκρατία έως την προσομοίωση πολεμικών σεναρίων.

Επιπλέον, η δεκαετία του 1990 σηματοδότησε μια θεμελιώδη αλλαγή στο παράδειγμα της διαχείρισης πληροφοριών: τον επαναπροσδιορισμό της ίδιας της πληροφορίας. Η μετάβαση από τη βιομηχανική εποχή στην οικονομία της πληροφορίας και της γνώσης οδήγησε στη θεώρηση της πληροφορίας όχι απλώς ως περιεχομένου αλλά ως ανεξάρτητου, και άκρως πολύτιμου πόρου. Οι οργανισμοί μετατοπίστηκαν από μοντέλα με επίκεντρο την εργασία, τις πρώτες ύλες και το κεφάλαιο σε δομές βασισμένες στη γνώση (Drucker, 1994). Αυτός ο μετασχηματισμός τοποθέτησε την πληροφορία ως έναν κεντρικό πόρο στις οικονομικές και κοινωνικές αρένες (Drucker, 1999), προκαλώντας τη συνειδητοποίηση ότι η ελεγχόμενη διάδοση της πληροφορίας ήταν ζωτικής σημασίας όχι μόνο σε περιόδους συγκρούσεων αλλά και σε καιρό ειρήνης.

Ο δυναμικός μετασχηματισμός της διαχείρισης και της επεξεργασίας πληροφοριών πυροδοτήθηκε από την εξάπλωση του Διαδικτύου και την έλευση των μέσων κοινωνικής δικτύωσης στον 21ο αιώνα. Η μετάβαση αυτή διευκόλυνε την εξέλιξη της κοινωνίας της πληροφορίας σε μια δικτυωμένη κοινωνία, όπου τα άτομα, ως πολίτες του δικτύου, έγιναν κόμβοι μέσα σε ένα παγκόσμιο δίκτυο, υπογραμμίζοντας την πληροφορία ως ύψιστη αξία (Castells, 2008). Η πρόοδος του Διαδικτύου έδωσε τη δυνατότητα στους πολίτες του δικτύου να λαμβάνουν, να παράγουν και να μεταδίδουν γρήγορα πληροφορίες, υπερβαίνοντας τα γεωγραφικά όρια και δημιουργώντας ένα "www χωριό" που υπερβαίνει το «παγκόσμιο χωριό του McLuhan , γεμάτο με ανώνυμες κοινωνικές αλληλεπιδράσεις και διαδικτυακές ομαδικές σχέσεις που βασίζονται σε κοινά ενδιαφέροντα και αξίες (Wagner, 1999).

Αυτή η μνημειώδης αλλαγή στην επικοινωνία, την επεξεργασία και τη δημιουργία πληροφοριών κατέστησε αναγκαία μια αντίστοιχη αλλαγή στον τομέα του πληροφοριακού πολέμου (ΠΚ), προωθώντας τη μετάβασή του στο διαδικτυακό πεδίο. Η μετεγκατάσταση του πληροφοριακού πολέμου στο διαδίκτυο αντανακλούσε την ταχεία επέκταση του Διαδικτύου. Κατά τη διάρκεια του δεύτερου πολέμου στο Ιράκ, προέκυψαν οι πρώτες ενδείξεις ότι το Διαδίκτυο θα μπορούσε να συμπληρώσει τα μέσα μαζικής ενημέρωσης, αλλά σύντομα έγινε φανερό ότι θα μπορούσε να ξεπεράσει την αποτελεσματικότητα των παραδοσιακών μέσων ενημέρωσης (Tkeshelashvili, 2021).

Ο πληροφοριακός πόλεμος αναγνωρίστηκε ως η αξιοποίηση των τεχνολογιών πληροφοριών και επικοινωνιών για επιθετικούς ή αμυντικούς σκοπούς με σκοπό την άμεση διείσδυση, τη διατάραξη ή τον έλεγχο των πόρων ενός αντιπάλου. Αυτό περιελάμβανε τρεις κεντρικές πτυχές: την ανάπτυξη ρομποτικών όπλων, την εκτέλεση κυβερνοεπιθέσεων και την ενορχήστρωση της επικοινωνίας μέσω της τεχνολογίας πληροφοριών και επικοινωνιών (Tkeshelashvili, 2021). Ο τομέας του πληροφοριακού πολέμου επεκτάθηκε πέρα από τη στρατιωτική σφαίρα για να συμπεριλάβει ένα ευρύτερο φάσμα μη διαπροσωπικών

συγκρούσεων, αποτελώντας μια ολοκληρωμένη έννοια που ξεπερνά την απλή προπαγάνδα. (Taddeo, 2012).

Η σύγκρουση της Γεωργίας με τη Ρωσία το 2008 κατέδειξε την πολύπλευρη φύση του πληροφοριακού πολέμου, με τις κυβερνοεπιθέσεις να ενισχύουν την εχθρική κάλυψη από τα μέσα ενημέρωσης. Εν μέσω των ανταγωνιστικών αφηγήσεων των φιλορωσικών μέσων ενημέρωσης, η γεωργιανή κυβέρνηση αντιμετώπισε κυβερνοεπιθέσεις που στόχευαν επίσημους ιστότοπους, με χαρακτηριστικό παράδειγμα τη χειραγώγηση και παραποίηση εικόνων στον ιστότοπο του γεωργιανού κοινοβουλίου. Οι ενέργειες της Ρωσίας δεν αποσκοπούσαν μόνο στη βραχυπρόθεσμη παραπληροφόρηση, αλλά είχαν επίσης ως στόχο να διαμορφώσουν τις μεταπολεμικές αντιλήψεις, απαξιώνοντας τις φιλοδοξίες ένταξης της Γεωργίας στις Ατλαντικές δομές, κάτι που απαίτησε και την δημιουργία αρνητικών συναισθημάτων προς (και από) τους στρατηγικούς συμμάχους και προωθώντας ένα ορθόδοξο αντίβαρο στις δυτικές αξίες. Αντίστοιχες εικόνες υπήρξαν κατά την διάρκεια της Ρωσικής εισβολής στην Κριμαία (Lelonek, 2016).

Αναγνωρίζοντας το ευρύτερο φάσμα του πληροφοριακού πολέμου, δίνεται έμφαση όχι μόνο στις πτυχές της υψηλής τεχνολογίας και του κυβερνοχώρου, αλλά και στον ρόλο των δημοσιογράφων και των μέσων ενημέρωσης. Αυτό υπογραμμίστηκε από την εκτεταμένη εκστρατεία παραπληροφόρησης που ενορχήστρωσε η Ρωσία κατά τη διάρκεια της σύγκρουσης του 2014, χρησιμοποιώντας κρατικά ελεγχόμενα μέσα και διαδικτυακά τρολ για να προπαγανδίσει μια αφήγηση που απομάκρυνε τη Ρωσία από κάθε πρόθεση κατοχής της Ουκρανίας. Η επακόλουθη σύγχυση στη δυτική κοινή γνώμη αποδυνάμωσε τη νομιμότητα των δυτικών αντιδράσεων κατά της Ρωσίας, υποδηλώνοντας τον κομβικό ρόλο των μέσων ενημέρωσης στον σύγχρονο πληροφοριακό πόλεμο (Golovchenko et al., 2018). Την ίδια στρατηγική είδαμε πως χρησιμοποίησε -η Ρωσία- και στην εισβολή που πραγματοποίησε τον Φεβρουάριο του 2022 στην Ουκρανία, παρότι τότε ήταν πολύ λιγότερο αποτελεσματική εξαιτίας της στρατηγικής των ΗΠΑ (πχ αποκάλυψη πιθανών ημερομηνιών εισβολής και εξαναγκασμό Ρωσίας σε διαψεύσεις που αποδείχθηκαν ψευδείς).

Σε αυτή την ψηφιακή εποχή, η τακτική του πληροφοριακού πολέμου επεκτείνεται πέρα από τους κρατικούς φορείς και περιλαμβάνει μη κρατικές οντότητες, κυρίως τους χρήστες του διαδικτύου. Τα άτομα αυτά, οπλισμένα με εκτεταμένα δίκτυα κοινωνικών μέσων, συμβάλλουν στην αρένα του του πληροφοριακού πολέμου, χρησιμεύοντας τόσο ως στόχοι όσο και ως ενεργοί παράγοντες εκστρατειών παραπληροφόρησης (Golovchenko et al., 2018). Η εκρηκτική επιρροή των χρηστών του διαδικτύου υπογραμμίζει τον «εκδημοκρατισμό» του πληροφοριακού πολέμου, αντανακλώντας τη μεταμόρφωση αυτής της δυναμικής αρένας στο πλαίσιο του σύγχρονου πληροφοριακού τοπίου.

3.2 Η Παραπλάνηση στο πλαίσιο του πληροφοριακού πολέμου

Οι ρίζες του πληροφοριακού πολέμου είναι βαθιά προερχόμενες από ένα πολεμικό πλαίσιο, ωστόσο το περίγραμμά του έχει επεκταθεί πολύ πέρα από το πεδίο των

συγκρούσεων, διεισδύοντας στις σφαίρες των πολιτικών υποθέσεων. Η επέκταση αυτή έχει προωθηθεί από τη συγχώνευση των μέσων ενημέρωσης, του στρατού και κατασκευών (με αναμφίβολο πολιτικό, ιδεολογικό και στρατηγικό περιεχόμενο) όπως ο «πόλεμος με την τρομοκρατία», αυτά δημιουργούν μια συνθήκη λεπτής αλληλεπίδρασης μεταξύ πολέμου και ειρήνης, πραγματικού και εικονικού, σαφούς και διαχεόμενου στον θόρυβο της πληροφορίας, που συχνά αψηφά σαφείς τις οριοθετήσεις. Μέσα σε αυτό το περίπλοκο μωσαϊκό αποκτά σημασία η έννοια της παραπλάνησης στο πλαίσιο στρατιωτικών «επιχειρήσεων», αν και τα όρια μεταξύ στρατιωτικών και πολιτικών τομέων δεν μπορούν παρά να παραμένουν θολά.

Η παραπλάνηση, -όπως είδαμε- είναι μια διαχρονική πτυχή της ανθρώπινης αλληλεπίδρασης, έχει μια διαρκή ιστορική κληρονομιά που εκτείνεται σε διάφορες πτυχές της κοινωνίας, συμπεριλαμβανομένου του πολέμου. Ο σύγχρονος πληροφοριακός πόλεμος περιλαμβάνει ένα φάσμα λειτουργιών, που κυμαίνονται από αμυντικές δραστηριότητες, όπως η ασφάλεια των επιχειρήσεων και η αντιπαρακολούθηση, έως επιθετικούς ελιγμούς, συμπεριλαμβανομένων των ψυχολογικών επιχειρήσεων και της στρατιωτικής παραπλάνησης (U.S. Air Force, 2005). Η έννοια των επιχειρήσεων επιρροής αναδεικνύεται ως κεντρικό στοιχείο σε αυτό το πλαίσιο, περικλείοντας τις ψυχολογικές επιχειρήσεις, τη στρατιωτική παραπλάνηση, την αντικατασκοπεία, την ασφάλεια επιχειρήσεων, τις δημόσιες σχέσεις και την αντιπροπαγάνδα.

Η παραπλάνηση, στο πλαίσιο αυτό, χρησιμεύει ως τακτικό μέσο ενσωματωμένο στην ευρύτερη παλέτα του πληροφοριακού πολέμου, στρατηγικά σχεδιασμένο για την επίτευξη «πληροφοριακής υπεροχής». Αυτή η υπεροχή ορίζεται από την ικανότητα να αξιοποιείται μια πλεονεκτική θέση πληροφόρησης, εκμεταλλευόμενοι αυτήν για την απόκτηση ανταγωνιστικού πλεονεκτήματος (Alberts, Gartska, & Stein, 1999). Στον πυρήνα της, η παραπλάνηση επιδιώκει να εξαναγκάσει τους αντιπάλους να υιοθετήσουν τις επιθυμητές πεποιθήσεις, οπλοποιώντας ουσιαστικά τις πληροφορίες ως εργαλείο χειραγώγησης.

Έχουν διατυπωθεί δομημένα μοντέλα σχεδιασμού παραπλάνησης για να παρέχουν ένα ορθολογικό πλαίσιο για την ενορχήστρωση αποτελεσματικών εκστρατειών. Το μοντέλο RAND, το οποίο παρουσιάζεται στα κείμενα των Gerwehr και Glenn (2000), υπογραμμίζει τα βασικά συστατικά στοιχεία: έναν στόχο, ένα στοχευόμενο κοινό, μια αφήγηση και τα μέσα διάδοσης. Ομοίως, ο Hall (2003) τονίζει την ανάγκη να λαμβάνεται υπόψη η προοπτική του στόχου και η ταυτότητα του επιτιθέμενου, ενισχύοντας έτσι την ακρίβεια των τακτικών εξαπάτησης. Εξάλλου είναι σημαντικό να θυμόμαστε πως αυτή εντάσσεται στην ανάλυση του Mitchell (1986) που υποστηρίζει ότι η εξαπάτηση συμβαίνει όταν μια οντότητα μεταδίδει ένα μήνυμα που ευθυγραμμίζεται με τα συμφέροντά της, οδηγώντας τον παραλήπτη να υιοθετήσει μια παραποιημένη πεποίθηση. Στο πλαίσιο του πληροφοριακού πολέμου, η παραπλάνηση αναλαμβάνει διττό ρόλο τόσο σε επιθετικό όσο και σε αμυντικό επίπεδο. Οι αμυντικές στρατηγικές περιλαμβάνουν την ασφάλεια των επιχειρήσεων, την αντιπαραπληροφόρηση και την αντιπροπαγάνδα, ενώ οι επιθετικοί ελιγμοί περιλαμβάνουν τη στρατιωτική παραπλάνηση και τις ψυχολογικές επιχειρήσεις (Joint Pub 3-13, 1998). Στην

εποχή της πληροφορίας, ο πληροφοριακός πόλεμος ξεπερνά τη στρατιωτική σφαίρα και περιλαμβάνει τον έλεγχο της λεγόμενης «infosphere», περικλείοντας ροές πληροφοριών σε διάφορα επίπεδα και πλαίσια. Η προσπάθεια αυτή περιλαμβάνει τη χειραγώγηση των πηγών και τη διάδοση των πληροφοριών για τη δημιουργία αντιλήψεων που ευθυγραμμίζονται με τα συμφέροντα του κυρίαρχου μέρους. Αυτή η ικανότητα χειραγώγησης των αντιλήψεων με τη δημιουργία υποσυνόλων της "πραγματικότητας" ή ακόμη και "τεχνητών πραγματικοτήτων" συνιστά ένα τύπο παραπλάνησης.

Η ουσία του πληροφοριακού πολέμου επικεντρώνεται στον έλεγχο και τη διαφύλαξη των πληροφοριών, γεγονός που απαιτεί την προστασία των δεδομένων, των ατόμων και των τεχνολογιών που διευκολύνουν τη δημιουργία και την επικοινωνία των πληροφοριών. Ο αμυντικός πληροφοριακός πόλεμος είναι αφιερωμένος στη ματαίωση των προσπαθειών παραβίασης αυτών των στοιχείων, ενώ ο επιθετικός πληροφοριακός πόλεμος αξιοποιεί παρόμοιες τακτικές κατά των αντιπάλων. Μπορεί λοιπόν βάσιμα να υποστηριχθεί πως ο πληροφοριακός πόλεμος συγκλίνει με την παραπλάνηση, καθώς και οι δύο έννοιες περιλαμβάνουν μια δυναμική αλληλεπίδραση στρατηγικών και τακτικών με στόχο τη διαμόρφωση αντιλήψεων, την κατασκευή πλεονεκτικών υποσυνόλων της πραγματικότητας και την καθοδήγηση των αποτελεσμάτων μέσα στον περίπλοκο ιστό της σύγχρονης διασύνδεσης.

Αν δούμε με μια ευρύτερη προοπτική -και ταυτόχρονα με μια μεθοδολογική «χαλαρότητα»- τον Πληροφοριακό Πόλεμο, θα μπορούσαμε να βρούμε κομμάτια του πριν από την εποχή της πληροφορικής. Πρόκειται για εκείνες τις πρακτικές παραπλάνησης και ψυχολογικού πολέμου που είναι εγγενείς στην ίδια την ιστορία του πολέμου και που σήμερα σε συνδυασμό με τις τεχνολογικές εξελίξεις στην τεχνολογία πληροφοριών (ΤΠ) έθεσαν τις βάσεις για τις έννοιες του Πληροφοριακού Πολέμου. Η ενσωμάτωση των προσωπικών υπολογιστών στο πεδίο της μάχης, καταδεικνύει μια πρώιμη υιοθέτηση της τεχνολογίας για τακτικούς σκοπούς (Shaker & Finkelstein, 1987).

Η εισβολή των ιρακινών δυνάμεων στο Κουβέιτ το 1990 και η επακόλουθη εμπλοκή με τις δυτικές συμμαχικές δυνάμεις σηματοδότησε μια κομβική στιγμή που ανέδειξε τις προόδους που σημειώθηκαν στην έννοια της μάχης αέρος-εδάφους. Το σενάριο αυτό έθεσε τις βάσεις για την τακτική του Πληροφοριακού Πολέμου, που χαρακτηρίστηκε από εκστρατείες στα μέσα ενημέρωσης, την εισαγωγή ιών υπολογιστών στα εχθρικά συστήματα, ακόμη και το ενδεχόμενο χρήσης ηλεκτρομαγνητικού παλμού για την απενεργοποίηση ιρακινών ηλεκτρονικών συσκευών (Barry, 1991). Η σύνθεση των τακτικών ψυχολογικού, ηλεκτρονικού και συμβατικού πολέμου κατά τη διάρκεια αυτής της σύγκρουσης ανέδειξε την ενσωμάτωση των στοιχείων του Πολέμου της Πληροφορίας στις σύγχρονες ένοπλες δυνάμεις (Ruhmann, 2003). Η φάση αυτή αντιπροσωπεύει την εμφάνιση αυτού που θα μπορούσαμε να ονομάσουμε (κατ' αναλογία και με την τεχνολογική εξέλιξη) Πληροφοριακό Πόλεμο 1.0.

Καθώς προχωρούσε η δεκαετία του 1990, ο Πληροφοριακός Πόλεμος εξελίχθηκε σε μια πιο δομημένη έννοια που θα μπορούσε να περιγραφεί και ως Πληροφοριακός Πόλεμος 2.0.

Στη φάση αυτή παρατηρήθηκε η σύγκλιση της τεχνολογίας και του δόγματος ως κύρια προσέγγιση του πολέμου. Το αμερικανικό δόγμα έθεσε μια στέρεη βάση, ωστόσο δεν διέθετε μια ενιαία πολιτική σε διάφορους στρατιωτικούς κλάδους. Οι στρατηγικές του Στρατού και της Αεροπορίας διέφεραν από εκείνες του Ναυτικού και του Σώματος Πεζοναυτών, τονίζοντας την ανάγκη για μια ενοποιημένη προοπτική σε τακτικό και στρατηγικό επίπεδο (Bernhardt & Ruhmann, 1997).

Ταυτόχρονα, η Ρωσία ανέπτυξε το δικό της δόγμα με επίκεντρο την κυριαρχία της πληροφορίας. Έχοντας γίνει μάρτυρες του μετασχηματισμού του τοπίου των μέσων μαζικής ενημέρωσης, οι Ρώσοι στρατηγοί αναγνώρισαν την ανάγκη να εισέλθουν σε αυτό το πεδίο τόσο αμυντικά, δηλαδή να προστατεύσουν τους πολιτικούς ηγέτες και τον λαό τους από τις αρνητικές επιρροές της πληροφόρησης, όσο και «επιθετικά» ασκώντας οι ίδιοι επιρροή. Έτσι προέκυψε η έννοια της «πληροφοριακής-ψυχολογικής ασφάλειας», η οποία σχεδιάστηκε για να διασφαλίσει τη σφαίρα της πληροφορίας στο εσωτερικό του κράτους με τον συντονισμό των κρατικών φορέων, των δημόσιων οργανισμών, των πολιτικών κομμάτων και των πολιτών (Panarin, 1998).

Παράλληλα, ο Λαϊκός Απελευθερωτικός Στρατός της Κίνας (PLA) ανέπτυξε σταδιακά το δικό του δόγμα για τον λεγόμενο «πόλεμο πληροφοριών του λαού» όπως έγινε γνωστό, σύμφωνα με τα επίσημα κείμενα , αλλά και την κομματική αργκό. Εισήχθη το 1998και αναγνώριζε τον Πληροφοριακό Πόλεμο ως προϊόν της εποχής της πληροφορίας, αξιοποιώντας την τεχνολογία της πληροφορίας και αντιμετωπίζοντάς τα ως αναπόσπαστα στοιχεία μιας «μάχης». Η «δικτύωση» του πεδίου της μάχης αναδείχθηκε ως βασικό δόγμα, προαναγγέλλοντας ένα νέο μοντέλο που μεταμόρφωνε τη δυναμική του χρόνου και του χώρου. Κεντρικό ρόλο σε αυτή την προσέγγιση έπαιξε η μάχη για τον έλεγχο του πληροφοριακού τοπίου, επιτρέποντας την επιρροή ή τον καθορισμό των αποτελεσμάτων των συγκρούσεων (Pufeng, 1995). Αυτή η έννοια της «δικτύωσης» είχε ομοιότητες με τις δυτικές ιδέες για ένα ολοκληρωμένο πεδίο μάχης υψηλής τεχνολογίας.. Η κατοχή των «βασικών όπλων» του Πολέμου των Πληροφοριών θεωρήθηκε ότι θα παρείχε τη δυνατότητα πρώτου πλήγματος (Weigang, 1998).

Μέσα από αυτές τις δογματικές εξελίξεις, αναδύθηκε ένα κοινό νήμα - μια ολοκληρωμένη προοπτική που αγκάλιαζε ποικίλα μέσα πληροφόρησης, τεχνολογίες πληροφορικής και μια συνέχεια που περιλάμβανε τη σύγκρουση και την ειρήνη. Αυτή η ρευστότητα θόλωσε τα όρια μεταξύ συμβατικού και κυβερνοπολέμου, επεκτεινόμενη ακόμη και πέρα από τα παραδοσιακά πολεμικά σενάρια. Σε όλα τα δόγματα των ΗΠΑ, της Ρωσίας και της Κίνας, ο Κυβερνοπόλεμος αναδείχθηκε ως ένα κρίσιμο συστατικό στοιχείο στο ευρύτερο πλαίσιο του Πληροφοριακού Πολέμου, ξεκλειδώνοντας νέους δρόμους για επιχειρησιακές στρατηγικές, ενώ παρέμεινε υποταγμένος στους γενικούς στόχους που περιγράφονται από τα δόγματα Πληροφοριακού Πολέμου. Εύλογα συμπεραίνει λοιπόν κάποιος πως τα δόγματα των ΗΠΑ, της Ρωσίας και της Κίνας παρουσιάζουν ομοιότητες στην ευρεία προοπτική τους που καλύπτει πολλαπλές διαστάσεις της σύγκρουσης και της εμπλοκής. Εν μέσω της συνεχούς εξέλιξης του Πληροφοριακού Πολέμου, μια σταθερά

παραμένει - ο βαθύς αντίκτυπος της πληροφορίας και της χειραγώγησής της στο σύγχρονο πεδίο της μάχης.

Μετά τη δημιουργία δογματικών βάσεων για τον Πόλεμο των Πληροφοριών από ορισμένες από τις ισχυρότερες ένοπλες δυνάμεις του κόσμου, ακολούθησε μια ταχεία κούρσα εξοπλισμών. Τα δόγματα αυτά έδωσαν έμφαση στη χειραγώγηση των διαφόρων μορφών πληροφοριών από την πλευρά των αντιπάλων, γεγονός που οδήγησε στην ανάγκη ανάπτυξης ισχυρών όπλων που θα μπορούσαν να παρέχουν πρόσβαση σε στοχευμένα συστήματα ΤΠ, να τροποποιούν πληροφορίες και να εξορθολογίζουν επιχειρήσεις και οργανισμούς που σχετίζονται με τους στόχους αυτούς . Η εξέλιξη του Πληροφοριακού Πολέμου επέφερε τη σύγκλιση των δραστηριοτήτων μεταξύ των στρατιωτικών υπηρεσιών και των υπηρεσιών πληροφοριών, οδηγώντας σε ένα μετασχηματισμένο τοπίο. Πριν από αυτό, οι οντότητες αυτές λειτουργούσαν με διακριτούς στρατηγικούς και επιχειρησιακούς στόχους και τακτικές. Κομβικό σημείο αποτέλεσε η επίθεση «9/11» της Αλ Κάιντα το 2001, η οποία αποκάλυψε την έλλειψη συντονισμού στις δυνατότητες πληροφόρησης. Η επακόλουθη αναδιάρθρωση και αναδιατύπωση των δογμάτων οδήγησε σε πιο ολοκληρωμένα πλαίσια και αύξηση στην κατανομή πόρων. Η αναδιάρθρωση αυτή επεκτάθηκε και στους παγκόσμιους στρατιωτικούς οργανισμούς, προωθώντας την εμφάνιση νέων οργανωτικών δομών (Ruhmann & Bernhardt, 2014).

Το 2004, ο Στρατός των ΗΠΑ παρείχε έναν νέο ορισμό για τις επιχειρήσεις Πληροφοριακού Πολέμου, ο οποίος περιελάμβανε τον ηλεκτρονικό πόλεμο, τις επιχειρήσεις δικτύων υπολογιστών, τις ψυχολογικές επιχειρήσεις, τη στρατιωτική παραπλάνηση και την ασφάλεια των επιχειρήσεων, με στόχο να επηρεάσει και να υπερασπιστεί τις πληροφορίες και τα πληροφοριακά συστήματα για να επηρεάσει τη λήψη αποφάσεων (Army, 2004).

Η επέκταση των δραστηριοτήτων του Κυβερνοπολέμου ήταν ένα συνεπακόλουθο βήμα στην εξέλιξη του Πληροφοριακού Πολέμου. Τόσο οι σοβιετικές όσο και οι αμερικανικές δυνάμεις χρησιμοποιούσαν μεθόδους hacking και "φυσικής πρόσβασης" από τη δεκαετία του 1980. Η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA), ο Στρατός και η Αεροπορία δημιούργησαν μονάδες hacking τη δεκαετία του 1990, ενώ στη συνέχεια ακολούθησαν και άλλα έθνη. Περιπτώσεις όπως οι κυβερνοεπιθέσεις των ζαπατιστών ανταρτών στο Μεξικό το 1995, καθώς και συγκρούσεις στις οποίες συμμετείχαν Παλαιστίνιοι-Ισραηλινοί και Ταϊβανέζοι-Κινέζοι παράγοντες, παρουσίασαν την πρώιμη υιοθέτηση τακτικών στον κυβερνοχώρο (Rötzer, 2000a, 2000b).

Οι δυνάμεις της Γερμανίας δημιούργησαν κυρίως το "Kommando Strategische Aufklärung" το 2002, ενσωματώνοντας μονάδες πληροφοριών σημάτων, ηλεκτρονικής μάχης, ψυχολογικού πολέμου, ανάκρισης και άλλα. Η επακόλουθη εστίαση αυτής της διοίκησης στις επιχειρήσεις στον κυβερνοχώρο σηματοδότησε ένα καίριο βήμα προς τη δημιουργία μιας εξορθολογισμένης δύναμης αφιερωμένης στον Πόλεμο Πληροφοριών (Scheuch & Möhle, 2018).

Παρομοίως, οι ΗΠΑ δημιούργησαν το 2010 την ενοποιημένη Διοίκηση Κυβερνοχώρου των ΗΠΑ (U.S. Cyber Command), συνδυάζοντας τις προσπάθειες της NSA και εστιάζοντας σε επιχειρήσεις στον κυβερνοχώρο. Έργα όπως το Stuxnet σηματοδότησαν ορόσημα στον κρατικά χρηματοδοτούμενο κυβερνοπόλεμο, ενώ το σύστημα XKeyScore της NSA παρουσίασε τις δυνατότητες των σύγχρονων εργαλείων κυβερνοπολέμου, επιτρέποντας στους πράκτορες να αναζητούν και να χειρίζονται με ευκολία το περιεχόμενο και τα μεταδεδομένα των επικοινωνιών. Τα αυτοματοποιημένα όπλα στον κυβερνοχώρο συνέχισαν να εξελίσσονται, με πλήθος εργαλείων που αναπτύχθηκαν για σκοπούς επιτήρησης, χειραγώγησης και επίθεσης. Ο τεράστιος αριθμός τεχνολογιών κυβερνοεπιθέσεων που αναπτύχθηκαν και χρησιμοποιήθηκαν από εξειδικευμένες μονάδες κατέδειξε την αδιάκοπη επιδίωξη των κυβερνοδυνατοτήτων .

Η εμφάνιση του "δόγματος Gerasimov" από τον Ρώσο αρχηγό του Γενικού Επιτελείου το 2013 ανέδειξε την ενσωμάτωση των στοιχείων του Πληροφοριακού Πολέμου στη ρωσική στρατηγική ασφάλειας. Η στρατηγική αυτή έδινε έμφαση στη διεξαγωγή πληροφοριακού-ψυχολογικού πολέμου και πληροφοριακού-τεχνολογικού πολέμου, αντανακλώντας μια εξέλιξη στην κατανόηση του Πληροφοριακού Πολέμου (Gerasimov, 2013). Ο Λαϊκός Απελευθερωτικός Στρατός της Κίνας (PLA) ευθυγραμμίστηκε επίσης με αυτές τις εξελίξεις, δημιουργώντας τη Δύναμη Στρατηγικής Υποστήριξης (SSF) ως απάντηση στις προκλήσεις του Πληροφοριακού Πολέμου. Η SSF συνδύασε διάφορες δυνατότητες, συμπεριλαμβανομένης της αναγνώρισης στον κυβερνοχώρο, της επίθεσης και της άμυνας, σε έναν ενιαίο οργανισμό, τονίζοντας περαιτέρω την πολύπλευρη φύση του σύγχρονου Πληροφοριακού Πολέμου (Office of the Secretary of Defense, 2017).

Η άνοδος του υβριδικού πολέμου έφερε μια νέα διάσταση στον Πόλεμο της Πληροφορίας. Χαρακτηριζόμενος από ένα συνδυασμό στρατιωτικών και μη στρατιωτικών μέτρων, ο υβριδικός πόλεμος στόχευε σε τρωτά σημεία σε όλους τους πολιτικούς, στρατιωτικούς, οικονομικούς, κοινωνικούς, πληροφοριακούς τομείς και τους τομείς των υποδομών. Η έννοια αυτή, που περιλαμβάνει τη χειραγώγηση των μέσων ενημέρωσης και την καταπολέμηση στον κυβερνοχώρο, ενώ επέστησε την προσοχή στις προκλήσεις που θέτουν οι σύγχρονες συγκρούσεις που βασίζονται στην πληροφόρηση (Cullen & Reichborn-Kjennerud, 2017).

Συμπερασματικά, ο Πόλεμος Πληροφοριών έχει εισέλθει σε μια νέα φάση που χαρακτηρίζεται από αυτοματοποίηση και εντατικοποίηση των δραστηριοτήτων. Η ενσωμάτωση του πολέμου στον κυβερνοχώρο και η στρατηγική χειραγώγηση των πληροφοριών έχει γίνει μια σταθερή και διάχυτη πτυχή των παγκόσμιων συγκρούσεων. Οι ένοπλες δυνάμεις παγκοσμίως έχουν αναγνωρίσει τις δυνατότητες του Κυβερνοπολέμου και την ικανότητά του να διαταράσσει και να χειραγωγεί τα συστήματα πληροφορικής των αντιπάλων. Η δημιουργία εξειδικευμένων μονάδων, η ανάπτυξη προηγμένων όπλων στον κυβερνοχώρο και η υιοθέτηση σύγχρονων δογμάτων καταδεικνύουν την αυξανόμενη σημασία του Πληροφοριακού Πολέμου στο σύγχρονο τοπίο της ασφάλειας. Καθώς η παγκόσμια κοινότητα παλεύει με τις επιπτώσεις του υβριδικού πολέμου και της

χειραγώγησης των πληροφοριών, οι προσπάθειες για την αντιμετώπιση αυτών των απειλών συνεχίζουν να εξελίσσονται και να προσαρμόζονται.

Στις αρχές της δεκαετίας του 2000, η κυρίαρχη προοπτική της συνδεσιμότητας στο Διαδίκτυο περιστρεφόταν γύρω από την παγκόσμια ανισότητα. Οι νεοφιλελεύθερες απόψεις πλαισίωναν την πρωταρχική πρόκληση για την ασφάλεια ως την ενσωμάτωση των ατόμων στο τεράστιο δίκτυο των παγκόσμιων ροών πληροφοριών (Reid, 2009). Ωστόσο, αυτή η αισιόδοξη προοπτική βασίστηκε στην υπόθεση ότι οι χρήστες του Διαδικτύου θα αξιοποιούσαν τις νέες πηγές πληροφοριών για εποικοδομητικούς σκοπούς, όπως η εκπαίδευση και η ανάπτυξη.

Η τρέχουσα αναταραχή που χαρακτηρίζεται από την παραπληροφόρηση μέσω του Διαδικτύου και την άνοδο του αυταρχικού λαϊκισμού στις δυτικές φιλελεύθερες δημοκρατίες αμφισβητεί αυτή την υπόθεση (Bradshaw & Howard, 2019). Κοιτάζοντας πίσω από το 2016, είναι σαφές ότι η δικτυωμένη πολιτική ξεπέρασε τα πεδία της παγκοσμιοποίησης και των κινημάτων διαμαρτυρίας, αιφνιδιάζοντας τις αρχές ασφαλείας. Εμφανίστηκαν συγκλίνουσες τάσεις που επηρέασαν τις διεθνείς συγκρούσεις και την εξέλιξη των μέσων κοινωνικής δικτύωσης (Singer & Brooking, 2018). Οι μεγάλες εταιρείες έθεσαν ως προτεραιότητα τη δέσμευση των χρηστών και τη δημιουργία εσόδων στο σχεδιασμό των πλατφορμών τους, ενώ ισχυρά κράτη όπως η Ρωσία τελειοποίησαν κυβερνο- και συμβατικές τακτικές για να σπείρουν τη σύγχυση. Η έξαρση της χρήσης των μέσων κοινωνικής δικτύωσης συνέβαλε σε ψυχολογικά ζητήματα μεταξύ των χρηστών, προωθώντας την ομαδική σκέψη και την προκατάληψη επιβεβαίωσης. Πολιτικές εκστρατείες και αντίπαλοι επωφελήθηκαν από αυτές τις τάσεις, διαδίδοντας διχαστική παραπληροφόρηση μέσω μιμιδίων (memes), ψευδών ειδήσεων και bots.

Πολυάριθμες ερευνητικές μελέτες και εκθέσεις υπογραμμίζουν τον τρόπο με τον οποίο οι εξελίξεις αυτές δημιούργησαν μια νέα μορφή ανασφάλειας, η οποία συχνά αναφέρεται ως "υβριδικός πόλεμος" ή "σύγκρουση γκρίζων ζωνών" (Hicks et al., 2019). Η κατάσταση αυτή θολώνει τις παραδοσιακές διακρίσεις στο πλαίσιο των συζητήσεων για την ασφάλεια, συμπεριλαμβανομένων εκείνων μεταξύ της εσωτερικής και της διεθνούς πολιτικής, της πολιτικής και της στρατιωτικής σφαίρας, των πολιτικών και των επίσημων φορέων και των ορίων μεταξύ ειρήνης και πολέμου. Συνδεδεμένη με μεταδημοκρατικά καθεστώτα και πρακτικές μετά την αλήθεια, η κατάσταση αυτή αμφισβητεί τα συμβατικά πλαίσια (Karpf, 2017).

Μια αξιοσημείωτη πτυχή που πρέπει να εξεταστεί είναι η εμφάνιση των deepfakes, μιας τεχνολογίας που έχει συγκεντρώσει σημαντικό ενδιαφέρον και ανησυχία από την έναρξή της το 2017. Τα deepfakes αξιοποιούν την τεχνητή νοημοσύνη, την επεξεργασία πολυμέσων και τα αρχειοθετημένα ψηφιακά δεδομένα για τη χειραγώγηση και τη δημιουργία οπτικοακουστικού περιεχομένου. Τόσο οι ερευνητές όσο και οι πολιτικοί αναγνωρίζουν τα deepfakes ως μια άμεση και ουσιαστική απειλή ικανή να υπονομεύσει την εμπιστοσύνη του κοινού στα οπτικά αποδεικτικά στοιχεία (π.χ. ένα deepfake που απεικονίζει κάποιον να λέει ή

να κάνει κάτι που στην πραγματικότητα δεν είπε ή δεν έκανε ποτέ). Αυτά τα deepfakes έχουν τη δυνατότητα να επιδεινώσουν τις επιστημολογικές κρίσεις, να παρέμβουν στις εκλογές και να χειραγωγήσουν τον πολιτικό λόγο.

Τα Deepfakes, ως παράδειγμα, ρίχνουν φως στη σύνθετη σχέση μεταξύ τεχνολογίας, επικοινωνίας και ασφάλειας. Λειτουργούν με βάση την αρχή της μίμησης, όπου τα Generative Adversarial Networks (GANs) συμμετέχουν σε μια ανταγωνιστική διαδικασία σύνθεσης και αξιολόγησης περιεχομένου πολυμέσων, έως ότου το παραγόμενο υλικό γίνει δυσδιάκριτο από την πραγματικότητα (Taylor, 2017). Επιπλέον, τα deepfakes έχουν τη δυνατότητα να αποτελέσουν κεντρικό στοιχείο του σύγχρονου πληροφοριακού πολέμου, καθώς μπορούν κυριολεκτικά να εξαπατήσουν το κοινό και να χειραγωγήσουν τις αντιλήψεις (Singer & Brooking, 2018).

4 Η ανάπτυξη της τουρκικής τεχνολογίας και των πληροφοριακών δυνατοτήτων

4.1 Η Αμυντική βιομηχανία της Τουρκίας

Η τουρκική αμυντική βιομηχανία μπορεί να κατηγοριοποιηθεί σε τέσσερις κύριες ομάδες (Petrőcz, 2021), καθεμία από τις οποίες συμβάλλει με μοναδικό τρόπο στην υποδομή ασφάλειας της χώρας:

1. Κυβερνητικά ιδρύματα στη στρατιωτική βιομηχανία:

Το Υπουργείο Εθνικής Άμυνας και οι Τουρκικές Ένοπλες Δυνάμεις (TAF) διαδραματίζουν κρίσιμο ρόλο στον αμυντικό τομέα της Τουρκίας. Το Υπουργείο Εθνικής Άμυνας, εποπτεύει όλους τους κυβερνητικούς οργανισμούς που εμπλέκονται άμεσα στην εθνική ασφάλεια, ενώ η TAF δεν είναι μόνο ο εθνικός στρατός αλλά και ο κύριος καταναλωτής των τουρκικών στρατιωτικών προϊόντων. Η Προεδρία των Αμυντικών Βιομηχανιών (SSB), η οποία ιδρύθηκε το 1985 και αναδιαρθρώθηκε το 2017, διαδραματίζει καθοριστικό ρόλο στην απόκτηση στρατηγικών αμυντικών συστημάτων. Στις αρμοδιότητές της περιλαμβάνονται η έρευνα, η ανάπτυξη και η παραγωγή πρωτοτύπων σύγχρονων όπλων, ενώ παράλληλα διευκολύνει τη χρηματοδότηση μέσω διαφόρων μέσων, τόσο εγχώριων όσο και διεθνών.

2. Σημαντικές ενώσεις και ιδρύματα:

Ήδη κατά τη διάρκεια της δεκαετίας του 1960, η Τουρκία αναγνώρισε τη σημασία της ενίσχυσης των αμυντικών της συστημάτων για τη μείωση της εξάρτησης από εισαγόμενα κρίσιμα αμυντικά συστήματα. Εμφανίστηκαν ιδρύματα και ενώσεις για τη μεταρρύθμιση της αμυντικής βιομηχανίας και την παροχή υποστήριξης. Αργότερα, το Ίδρυμα Τουρκικών Ενόπλων Δυνάμεων (TAFF ή TSKGV), που ιδρύθηκε το 1987, έχει ως στόχο να ενισχύσει τις δυνατότητες των τουρκικών ενόπλων δυνάμεων μέσω της ανάπτυξης της εθνικής αμυντικής βιομηχανίας. Εποπτεύει διάφορες θυγατρικές εταιρείες, συμπεριλαμβανομένων των Aselsan Electronics Industry and Trade Inc., Turkish Aerospace Industries Inc. (TAI), Roketsan Missiles Industries Inc., Havelsan - Air Electronics Industry and Trade Inc., ISBIR Electricity Industry Inc. και Aspilsan Energy Industry and Trade Inc. Η Ένωση Κατασκευαστών Αμυντικής και Αεροδιαστημικής Βιομηχανίας (SaSaD), που ιδρύθηκε το 1990, επιδιώκει να εκπροσωπεί και να υποστηρίζει την τουρκική αμυντική και αεροπορική βιομηχανία. Η ένωση συνεργάζεται με τους ενδιαφερόμενους φορείς της βιομηχανίας για την ενίσχυση της συνεργασίας, τη δημιουργία συνεργειών και την ελαχιστοποίηση της εξάρτησης από το εξωτερικό στον τομέα της άμυνας και της ασφάλειας. Ο Σύνδεσμος Εξαγωγέων Αμυντικής και Αεροδιαστημικής Βιομηχανίας της Τουρκίας (SSI), που ιδρύθηκε το 2011, επικεντρώνεται στην ενίσχυση των εξαγωγών των τουρκικών προϊόντων άμυνας και αεροπορίας. Η SSI συντονίζει τις

προσπάθειες για την ενίσχυση της παραγωγής με εξαγωγικό προσανατολισμό, των επενδύσεων σε έρευνα και ανάπτυξη και της ανταλλαγής γνώσεων εντός του τομέα.

3. Ιδιωτικά ινστιτούτα και εταιρείες:

Ενώ αρχικά η κυβέρνηση και τα ιδρύματα στήριξαν τις περισσότερες αμυντικές εταιρείες, η δεκαετία του 1990 σηματοδότησε την άνοδο των αμυντικών εταιρειών που χρηματοδοτούνται από τον ιδιωτικό τομέα. Παραδείγματα περιλαμβάνουν τη Mechanical and Chemical Industry Corporation , γνωστή για την κατασκευή όπλων και πυρομαχικών. Μια άλλη αξιοσημείωτη εταιρεία είναι η ASFAT, που περιλαμβάνει στρατιωτικά εργοστάσια, επιπλέον, η STM, μια εταιρεία σχεδιασμού και παραγωγής, ιδρύθηκε από την Προεδρία Αμυντικών Βιομηχανιών (SSB). Αυτές οι εταιρείες που συνδέονται με την κυβέρνηση ασκούν εμπορικές δραστηριότητες για να συμβάλουν στην ανάπτυξη του τομέα.

4. clusters/οικοσυστήματα αμυντικών βιομηχανιών:

Η αμυντική βιομηχανία της Τουρκίας ευδοκιμεί επίσης στο πλαίσιο διαφόρων συστάδων που διευκολύνουν τη συνεργασία μεταξύ εταιρειών, ερευνητικών ιδρυμάτων και πανεπιστημίων. Αυτές οι συστάδες έχουν ως στόχο την προώθηση της καινοτομίας, της ανταλλαγής γνώσεων και της τεχνολογικής προόδου στον αμυντικό τομέα.

Συμπερασματικά, η αμυντική βιομηχανία της Τουρκίας περιλαμβάνει ένα δυναμικό οικοσύστημα που περιλαμβάνει κυβερνητικά ινστιτούτα, ενώσεις, ιδρύματα, ιδιωτικές εταιρείες και συνεργατικά clusters. Αυτές οι δομές (μέσα από την διαφορετική μορφή τους) συμβάλλουν συλλογικά στην ασφάλεια της Τουρκίας και στην τεχνολογική πρόοδο στον αμυντικό τομέα.

Τα τελευταία χρόνια, η Τουρκία έχει μετατραπεί σε έναν ικανό κατασκευαστή ενός ευρέος φάσματος αμυντικών προϊόντων, σημειώνοντας ένα σημαντικό βήμα προς την (μεγαλύτερη δυνατή εντός του σύγχρονου τεχνολογικού περιβάλλοντος) αυτάρκεια και άρα αυτονομία της. Αξιοσημείωτα επιτεύγματα περιλαμβάνουν την παραγωγή δορυφόρων, μη επανδρωμένων αεροσκαφών (UAV), εκπαιδευτικών αεροσκαφών, ελικοπτέρων, υπηρεσιακών τυφεκίων, πολεμικών πλοίων, τεθωρακισμένων οχημάτων και πυραυλικών συστημάτων. Ο μετασχηματισμός αυτός προωθείται από εξειδικευμένο ανθρώπινο δυναμικό, ισχυρά ερευνητικά ιδρύματα, εργαστήρια E&A, μικρομεσαίες επιχειρήσεις (ΜΜΕ) και συνεργασίες με διεθνείς εταιρείες. Ο αμυντικός τομέας της Τουρκίας διακλαδίζεται επίσης στην προσομοίωση και την ανάπτυξη λογισμικού, δημιουργώντας συνεργασίες σε παγκόσμια έργα, κατασκευάζοντας κέντρα παραγωγής και δοκιμών δορυφόρων, ξεκινώντας εγκαταστάσεις εκτόξευσης δορυφόρων και προωθώντας έργα εγχώριων μαχητικών αεροσκαφών και ελικοπτέρων(Petrőcz, 2021).

Η τουρκική αμυντική βιομηχανία υπερηφανεύεται (και στον βαθμό που οι προδιαγραφές και δυνατότητες που αναφέρονται ανταποκρίνονται στην πραγματικότητα) για αρκετά προϊόντα που ανταγωνίζονται στην παγκόσμια αγορά. Τα προϊόντα αυτά περιλαμβάνουν τα 8x8 PARS, 6x6 PARS, 6X6 ARMA, 4x4 COBRA, EJDER YALCIN, VURAN, ALTAY MBT και KAPLAN Medium Tanks. Τα προϊόντα αυτά έχουν κερδίσει αναγνώριση ς, προωθώντας τη θέση της Τουρκίας στη διεθνή αμυντική αγορά. Το 8x8 PARS ξεχωρίζει με το σύστημα διεύθυνσης όλων των αξόνων, προσφέροντας τη χαμηλότερη ακτίνα στροφής στην κατηγορία του. Σχεδιασμένο για την προστασία του προσωπικού, διαθέτει καθίσματα ανθεκτικά στις νάρκες και μπορεί να υπερπηδήσει με ευκολία εμπόδια και χαρακώματα. Το PARS 6x6, που μοιράζεται παρόμοια χαρακτηριστικά, ενσωματώνει δομή έξι τροχών με σύστημα διεύθυνσης πρώτου και τρίτου άξονα, ενισχύοντας την κινητικότητα και την ευελιξία, ιδιαίτερα σε μαλακά εδάφη. Η έκδοση 6X6 PARS Scout είναι ακόμη και αμφίβια, διευρύνοντας το επιχειρησιακό του πεδίο.Το τεθωρακισμένο όχημα 6X6 ARMA παρουσιάζει ανώτερη κινητικότητα, σημαντική προστασία από νάρκες και βαλλιστική προστασία και ευέλικτες επιλογές ενσωμάτωσης όπλων. Σχεδιασμένο για λειτουργία σε απαιτητικά εδάφη και κλίματα, μπορεί να διαμορφωθεί για διάφορους ρόλους, όπως μεταφορέας προσωπικού, φορέας μάχης πεζικού, κέντρο διοίκησης, ασθενοφόρο, αναγνωριστικό και άλλα. Το 4x4 COBRA, μια πλατφόρμα πολλαπλών χρήσεων, προσαρμόζεται σε ρόλους όπως μεταφορέας προσωπικού, πλατφόρμα όπλων, αναγνώριση, ακόμη και αμφίβια καθήκοντα. Το EJDER YALCIN, ένα τεθωρακισμένο όχημα μάχης 4X4, προσφέρει προσαρμογή για ρόλους όπως επιτήρηση συνόρων, αναγνώριση, διοίκηση, καθήκοντα ασθενοφόρου και άλλα. Ένα άλλο ξεχωριστό όχημα, το VURAN, είναι ένα τεθωρακισμένο όχημα 4 τροχών με αξιοσημείωτη χωρητικότητα πληρώματος και ισχυρή προστασία του προσωπικού από νάρκες και βαλλιστικές απειλές, το MBT ALTAY, αντιπροσωπεύει ένα άρμα μάχης τρίτης γενιάς. Αναπτύχθηκε στο πλαίσιο του Τουρκικού Εθνικού Έργου για το Άρμα Κύριας Μάχης, διατείνεται πως ενσωματώνει χαρακτηριστικά άρματος αιχμής, με σχέδια για μαζική παραγωγή και ανάπτυξη. Η σειρά μεσαίων αρμάτων μάχης KAPLAN, συμπεριλαμβανομένων των αμφίβιων δυνατοτήτων Kaplan 10 και Kaplan 20, επεκτείνει περαιτέρω την γκάμα αμυντικού υλικού που παράγεται και προσφέρεται από την Τουρκία(Petrőcz, 2021).

Οι φιλοδοξίες της τουρκικής αμυντικής βιομηχανίας επεκτείνονται πέρα από την παραγωγή, περιλαμβάνοντας πλήρη «Έρευνα και Ανάπτυξη» πολεμικού υλικού. Η βιομηχανία τους στοχεύει να ανταποκριθεί στα απαιτητικά πρότυπα που θέτουν οι Νατοϊκές προδιαγραφές. Τα τελευταία χρόνια επίσης, διάφορα σχέδια βρίσκονται σε διαφορετικό στάδιο σχεδίασης, εξέλιξης ή παραγωγής1. Ανάμεσα σε αυτά είναι το Εθνικό Πολεμικό Πλοίο MILGEM Project, το Cirit, τα αντιαρματικά, οι πύραυλοι Bora, Tyfon και Kasırga, το εκπαιδευτικό αεροσκάφος (HÜRKUŞ), περιπολικά σκάφη και τα σκάφη ακτοφυλακής, ελαφρά όπλα και σύγχρονα πυρομαχικά.

[1] Έναν εκτενή κατάλογο οπλικών συστημάτων που παράγει και φιλοδοξεί να παράξει η Τουρκία μπορεί κάποιος να βρει στα επίσημα κείμενα του Τουρκικού Υπ.Εξ., ειδικότερα στο https://www.mfa.gov.tr/data/ENFORMASYON/SSB-tanitim-catalog.pdf

4.2 Τα UAVs

Η απόκτηση και η μίσθωση ισραηλινών μη επανδρωμένων αεροσκαφών HERON από την Τουρκία συνάντησε σημαντικά πολιτικά εμπόδια, γεγονός που αντανακλά την τεταμένη σχέση μεταξύ των δύο χωρών. Οι προκλήσεις αυτές είχαν ως αποτέλεσμα σημαντικές καθυστερήσεις στην παράδοση και μετέπειτα επιπλοκές στην ενσωμάτωση των τουρκικών εξαρτημάτων στο σύστημα. Οι αναποδιές αυτές, σε συνδυασμό με την απόρριψη του αιτήματος της Τουρκίας για 4 MQ-1 και 6 MQ-9 Predator από το Κογκρέσο των ΗΠΑ το 2008, υπογράμμισαν την ανάγκη της Τουρκίας για εγχώρια UAV. Η κατάσταση αυτή έδωσε κίνητρο στην τοπική αμυντική βιομηχανία να αναλάβει ηγετικό ρόλο ως κύριος ανάδοχος και κατασκευαστής τέτοιων συστημάτων.Ήδη από το 2001, η τουρκική Επιτροπή Αμυντικής Βιομηχανίας (SSM) προκήρυξε διαγωνισμό για εννέα συστήματα για την κάλυψη των προηγμένων απαιτήσεων αναγνώρισης του τουρκικού στρατού, οδηγώντας τελικά στην προμήθεια 54 εναέριων οχημάτων.

Το 2004, ανακοινώθηκε η ανάπτυξη ενός UAV μεσαίου ύψους μεγάλης αντοχής (MALE) και στις 25 Οκτωβρίου 2013, η SSM ανέθεσε στην Tusas Aerospace Industry (TAI) τη σύμβαση για την ανάπτυξη και παραγωγή δέκα UAV. Αυτά τα νέα UAV ονομάστηκαν ANKA (Phoenix), με τις αρχικές παραδόσεις να ξεκινούν το 2017 μετά από αρκετές καθυστερήσεις. Η TAI παρήγαγε πολλαπλά πρωτότυπα για την ανάπτυξη της ατράκτου και του ωφέλιμου φορτίου και το αεροσκάφος έχει υποβληθεί σε επιτυχείς πτητικές δοκιμές. Οι δυνατότητες του ANKA περιλαμβάνουν αναγνώριση ημέρας και νύχτας, ανίχνευση και αναγνώριση στόχων παντός καιρού και έξυπνες δυνατότητες αποστολής, χάρη στο ηλεκτρο-οπτικό/υπέρυθρο (EO/IR) ραντάρ και τα χαρακτηριστικά αυτόνομης πτήσης, συμπεριλαμβανομένης της αυτόματης απογείωσης και προσγείωσης. Το UAV διαθέτει εντυπωσιακή αντοχή 24 ωρών στα 30.000 πόδια και εμβέλεια 200 χιλιομέτρων. Μια άλλη αξιοσημείωτη τουρκική εξέλιξη UAV είναι το Bayraktar T2B. Στις 20 Δεκεμβρίου 2011 υπεγράφη μια αρχική σύμβαση με την Kalekalip Baykar Makina Industry για την παραγωγή ενός "τακτικού συστήματος UAV" σχεδιασμένου για αναγνώριση, επιτήρηση και συλλογή πληροφοριών για τις τουρκικές ένοπλες δυνάμεις. Βασικό χαρακτηριστικό αυτού του UAV είναι η ικανότητά του να αναπτύσσει αντιαρματικούς πυραύλους. Τον Δεκέμβριο του 2015, η πρώτη επιτυχής πτήση πραγματοποιήθηκε σε ύψος 16.000 ποδών, πλήττοντας στόχο σε απόσταση οκτώ χιλιομέτρων, χρησιμοποιώντας τον πύραυλο μεγάλου βεληνεκούς Roketsan UMTAS, ο οποίος είχε αρχικά σχεδιαστεί για το τουρκικό επιθετικό ελικόπτερο T-129. Αυτό το "έξυπνο μικροπυρομαχικό" επιτρέπει στο μη επανδρωμένο αεροσκάφος να διατηρεί την αντοχή του ακόμη και όταν είναι πλήρως οπλισμένο. Στις αρχικές του εκδόσεις, το UAV διαθέτει αντοχή άνω των 24 ωρών, ταχύτητα 70 κόμβων την ώρα, εμβέλεια περίπου 150 χιλιομέτρων και επιχειρησιακή ικανότητα 24.000 ποδιών. Οι μαζικές παραδόσεις ξεκίνησαν το 2016 και το Bayraktar T2B έχει σημειώσει σημαντική εξαγωγική επιτυχία (Baykar, 2023).

Ένα ακόμη τουρκικής κατασκευής UAV είναι το Karayel, το οποίο κατασκευάζεται από την Vestel Defense Industry Corporation. Μοιράζεται παρόμοιες δυνατότητες με το Bayraktar

και μπορεί να αναλάβει επιχειρήσεις μεγάλης εμβέλειας που διαρκούν έως και 20 ώρες σε υψόμετρο που φτάνει τα 20.000 πόδια. Οι πρωταρχικές του αποστολές επικεντρώνονται στις υπηρεσίες πληροφοριών, επιτήρησης και αναγνώρισης (ISR) μέσω των ηλεκτρο-οπτικών/υπέρυθρων αισθητήρων του. Εκτός από αυτά τα τακτικά UAV και τα μη επανδρωμένα εναέρια οχήματα μάχης (UCAV), η Τουρκία έχει επιτύχει στην παραγωγή μικρότερων αεροσκαφών. Μεταξύ αυτών, ξεχωρίζει το μίνι Bayraktar. Αυτό το UAV μικρού βεληνεκούς υπερέχει σε καθήκοντα αναγνώρισης και επιτήρησης ημέρας και νύχτας και εισήχθη σε υπηρεσία το 2007. Το πιο αξιοσημείωτο επίτευγμά του είναι ότι έγινε το πρώτο τουρκικό όχημα που επιλέχθηκε από ξένο φορέα εκμετάλλευσης. Το 2012, το Κατάρ αγόρασε δέκα από αυτά τα αεροσκάφη έναντι 2,5 εκατομμυρίων δολαρίων (Baykar, 2023).

Η TAI, ή Turkish Aerospace Industries, είναι ο κατασκευαστής πίσω από τη δημιουργία του Anka, μιας κατηγορίας UAV μεσαίου ύψους και μεγάλης αντοχής (MALE) που κατέχει ζωτικό ρόλο ως στρατηγικά μη επανδρωμένα αεροσκάφη για την Τουρκία. Η ανάπτυξή του, σε επίπεδο σχεδιασμού και εν συνεχεία πρωτοτύπου, ξεκίνησε το 2004, και απέφερε τρία πρωτότυπα και συνοδευτικά επίγεια συστήματα. Οι αρχικές δοκιμές πραγματοποιήθηκαν το 2010. Το ντεμπούτο του Anka-A, ωστόσο, αποδείχθηκε κατώτερο του αναμενομένου , καθώς η TAI παρέδωσε μόλις δύο πρωτότυπα στον τουρκικό στρατό σε μια δεκαετία προσπαθειών, ένα εκ των οποίων συνετρίβη το 2013. Το Anka-B, σημείωσε σημαντική βελτίωση το 2015 και πέτυχε αξιοσημείωτα ορόσημα, όπως η επίτευξη υψομέτρων που ξεπερνούν τα 30.000 πόδια, οι δυνατότητες αντοχής έως και 26 ώρες και η επιχειρησιακή ακτίνα των 200 χιλιομέτρων. Αξίζει να σημειωθεί ότι το Anka-B έθεσε επίσης τα θεμέλια για την ενσωμάτωση οπλικών συστημάτων στην πλατφόρμα.Το σύγχρονο Anka-S, που κινείται με έλικες, διαθέτει μήκος περίπου 26 ποδιών και διαθέτει τη δυνατότητα μεταφοράς ωφέλιμου φορτίου περίπου 400 κιλών. Αυτό που το κάνει να ξεχωρίζει είναι η αντοχή, με την ικανότητα να παραμένει στον αέρα για περισσότερες από 24 ώρες συνεχώς. Επιπλέον, είναι εξοπλισμένο για να μεταφέρει μικρούς πυραύλους ακριβείας και διαθέτει ραντάρ συνθετικού διαφράγματος (SAR) μαζί με ραντάρ ένδειξης επίγειου στόχου για τον αποτελεσματικό εντοπισμό και την παρακολούθηση επίγειων στόχων (Rossiter& Cannon, 2022).

Ένα από τα πιο αξιοσημείωτα χαρακτηριστικά του Anka-S είναι η δυνατότητα δορυφορικού ελέγχου, που του επιτρέπει να επιχειρεί πέρα από την οπτική επαφή. Αυτό το προηγμένο χαρακτηριστικό το τοποθετεί ως το πιο εξελιγμένο μη επανδρωμένο αεροσκάφος της Τουρκίας μέχρι σήμερα. Στα μέσα του 2021, οι Τουρκικές Ένοπλες Δυνάμεις (TAF) παρέλαβαν τέσσερα από τα τελευταίας γενιάς μη επανδρωμένα αεροσκάφη Anka-S από την TAI (Rossiter& Cannon, 2022). Αυτά διανεμήθηκαν στη συνέχεια, με δύο να διατίθενται στην Τουρκική Αεροπορία (THK) και δύο στο Τουρκικό Ναυτικό (Türk Deniz Kuvvetleri). Συνοπτικά, ο τουρκικός στρατός έχει συγκεντρώσει ένα στόλο περίπου 130 μη επανδρωμένων αεροσκαφών, που περιλαμβάνει διάφορα σχέδια, αν και τα ακριβή στοιχεία είναι δυσδιάκριτα.

Τα μη επανδρωμένα αεροσκάφη έχουν διαδραματίσει καθοριστικό ρόλο στην ενίσχυση των δυνατοτήτων της Τουρκίας και στην επέκταση της επιρροής της στο ευρύτερο

γεωπολιτικό τοπίο. Αυτά τα μη επανδρωμένα αεροσκάφη έχουν αναπτυχθεί κυρίως για να καλύψουν τις εξελισσόμενες επιχειρησιακές ανάγκες των τουρκικών ενόπλων δυνάμεων και να επιτύχουν μεγαλύτερη αυτάρκεια και αυτονομία στις στρατιωτικές επιχειρήσεις. Η ενσωμάτωση αυτών των προηγμένων τεχνολογιών έχει δρομολογήσει σημαντικούς μετασχηματισμούς στις στρατιωτικές στρατηγικές της Τουρκίας, προσφέροντας αξιοσημείωτα πλεονεκτήματα τόσο όσον αφορά την αποτελεσματικότητα στο πεδίο της μάχης όσο και τη μείωση των απωλειών.

Όπως έχει αναφερθεί, οι σύγχρονες στρατιωτικές επιχειρήσεις εξαρτώνται από την έγκαιρη απόκτηση λεπτομερών πληροφοριών σχετικά με την κατάσταση του εχθρού και την ακριβή απεικόνιση της διάταξης του πεδίου μάχης. Η διαδικασία των αποστολών ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) αποτελείται από διάφορα στάδια: αρχική απόκτηση στόχου (TASK), συλλογή πληροφοριών (COLLECT), επεξεργασία (PROCESS), ανάλυση (EXPLOIT) και ανταλλαγή πληροφοριών (DISSEMINATE). Οι αποστολές αυτές αποσκοπούν στη συλλογή κρίσιμων πληροφοριών για τον αντίπαλο, συμπεριλαμβανομένων των κέντρων διοίκησης και ελέγχου, της δομής των δυνάμεων, των οπλικών συστημάτων, των αποθηκών πυρομαχικών, των μέσων υποστήριξης, των υποδομών, του προσωπικού, των εγκαταστάσεων αποθήκευσης, των επιχειρησιακών χώρων και των δικτύων επικοινωνίας, καθώς και στον εντοπισμό βασικών στόχων, όπως οι εγκαταστάσεις αεράμυνας (Αναδιώτης, 2018).

Η αξιοποίηση από την Τουρκία μη επανδρωμένων αεροσκαφών εξοπλισμένων με κάμερες παρέχει τη δυνατότητα να διεξάγει ημερήσια και νυχτερινή επιτήρηση συγκεκριμένων περιοχών ενδιαφέροντος κοντά στα σύνορά της, παραμένοντας εντός του φιλικού εναέριου χώρου, με μοναδικό περιορισμό τις δυσμενείς καιρικές συνθήκες, όπως η νεφοκάλυψη. Επιπλέον, οι σταθμοί ελέγχου αυτών των μη επανδρωμένων αεροσκαφών μπορούν να τοποθετηθούν σε αποστάσεις έως και 200 ναυτικά μίλια μακριά, εφόσον διατηρείται η δυνατότητα οπτικής επαφής (LOS). Τα μη επανδρωμένα αεροσκάφη που είναι εξοπλισμένα με δυνατότητες SATCOM μπορούν να ελέγχονται από ακόμη μεγαλύτερες αποστάσεις. Η ενσωμάτωση των τεχνολογιών RADAR Synthetic Aperture Radar (SAR) και Ground Moving Target Indicator (GMTI) εξαλείφει τα προβλήματα που σχετίζονται με τις καιρικές συνθήκες και ενισχύει την ακρίβεια των πληροφοριών. Τα μη επανδρωμένα αεροσκάφη μπορούν να παρέχουν συνεχώς σε πραγματικό χρόνο, εξαιρετικά ακριβείς ενημερώσεις σχετικά με τις θέσεις κινητών και σταθερών χερσαίων και θαλάσσιων στόχων, μεταδίδοντας αυτά τα ζωτικής σημασίας δεδομένα στα Κέντρα Επιχειρήσεων, στερώντας έτσι από τον αντίπαλο το στοιχείο του αιφνιδιασμού. Η προσέγγιση αυτή εξοικονομεί πολύτιμους πόρους, μειώνοντας την εξάρτηση από επανδρωμένα μέσα όπως τα αεροσκάφη, μειώνοντας την επιχειρησιακή φθορά και αποτρέποντας τις απώλειες φίλιων δυνάμεων, ενώ διατηρεί σταθερή πίεση στον αντίπαλο. Αξίζει να σημειωθεί ότι σε περιορισμένες περιοχές, όπως τα νησιά, τα μη επανδρωμένα αεροσκάφη με περιορισμένη εμβέλεια ελέγχου μπορούν να παρακολουθούν αποτελεσματικά την πλειονότητα των εχθρικών δυνάμεων και των σχηματισμών μάχης τους (Αναδιώτης, 2018).

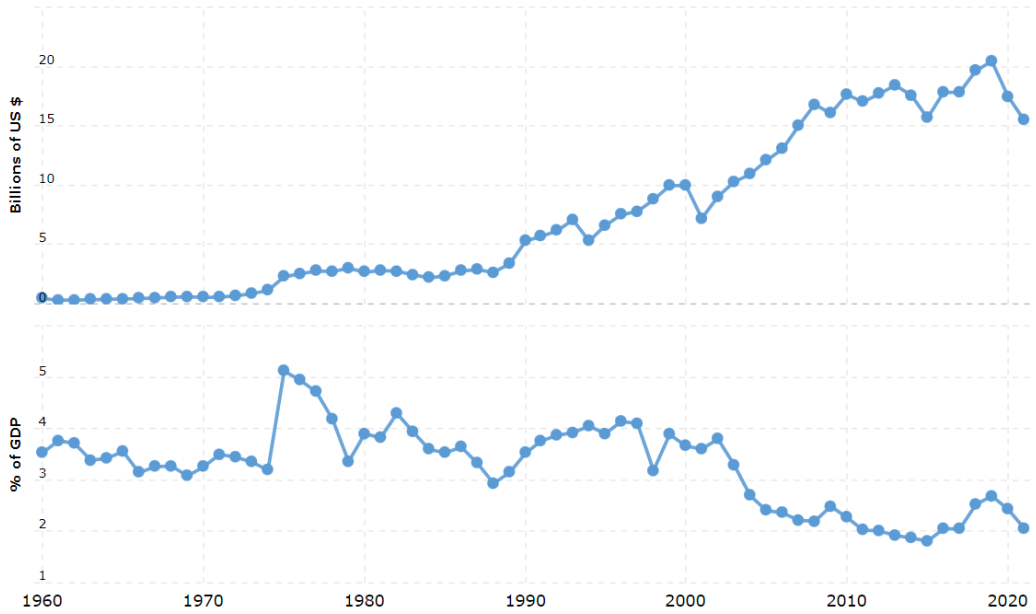
Οι ικανότητες ηλεκτρονικού πολέμου είναι ένα άλλο χαρακτηριστικό (σύμφωνα με τις ανακοινώσεις) των τουρκικών drones, σε πλατφόρμες όπως η ANKA-B και ANKA-S. Αυτά τα μη επανδρωμένα αεροσκάφη είναι εξοπλισμένα με ακροφύλακες ηλεκτρονικών μέτρων υποστήριξης (ESM), σημάτων πληροφοριών (SIGINT) και ηλεκτρονικών πληροφοριών (ELINT) που ειδικεύονται στον ηλεκτρονικό πόλεμο. Μπορούν να ανιχνεύουν ηλεκτρονικά τις θέσεις των ενεργών εχθρικών συστημάτων RADAR από σημαντικές αποστάσεις, ενώ παράλληλα παραμένουν εκτός της εμβέλειας της εχθρικής αεράμυνας.

Εστιάζοντας στις ένοπλες συγκρούσεις στη Συρία και τη Λιβύη, η ανάλυση επικεντρώνεται στη χρήση μη επανδρωμένων αεροσκαφών (UAV) από τις τουρκικές δυνάμεις. Εντός της Συρίας, οι τουρκικές δυνάμεις όχι μόνο χρησιμοποίησαν UAVs για πληροφορίες, επιτήρηση και αναγνώριση, αλλά και ως μαχητικά μέσα ενσωματωμένα στις επιχειρησιακές στρατηγικές τους. Στο πλαίσιο της Συρίας, η επιχειρησιακή σημασία των τουρκικών UAV ήταν εμφανής κατά τη διάρκεια της επιχείρησης «Κλάδος Ελαίας» το 2018, η οποία αποσκοπούσε στη δημιουργία ρυθμιστικής ζώνης και στην εκτόπιση των υποστηριζόμενων από τις ΗΠΑ Κούρδων μαχητών. Ωστόσο, ήταν κατά τη διάρκεια της επιχείρησης «Ασπίδα της Άνοιξης» το 2020 που η Τουρκία εκτέλεσε ανάπτυξη UAV μεγάλης κλίμακας. Η επιχείρηση αυτή απεικόνισε τη στρατηγική ενσωμάτωση των συστημάτων ηλεκτρονικού πολέμου με τις τακτικές δυνατότητες των UAV, επιτρέποντας στην Τουρκία να εκτελέσει τους στόχους της ακόμη και εντός του εναέριου χώρου που περιορίζεται από τη Ρωσία και τη Συρία. Οι επιχειρήσεις αυτές βασίστηκαν κυρίως στα UAV Bayraktar-TB2 και Anka-S, δίνοντας έμφαση στο ρόλο τους στις λειτουργίες αναγνώρισης, επιτήρησης, εξάλειψης στόχων και αναμετάδοσης (Królikowski, 2022).

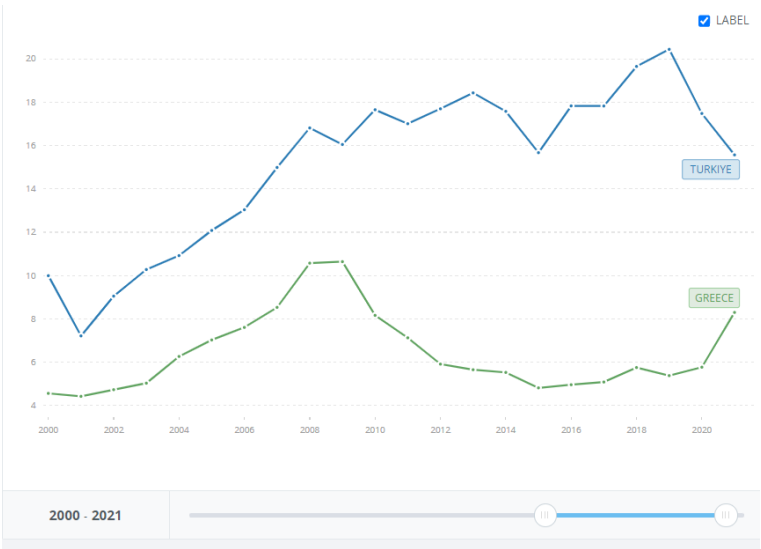
Στη σύγκρουση στη Λιβύη, η Τουρκία επανέλαβε τη στρατηγική της με επίκεντρο τα UAV από τη Συρία.. Η Τουρκία χρησιμοποίησε αποτελεσματικά UAV για συνεχή περιπολία, επιτήρηση και υποστήριξη στο σχετικά επίπεδο και αραιοκατοικημένο έδαφος της Λιβύης. Η δημιουργία ενός δικτύου αεράμυνας γύρω από την Τρίπολη ενίσχυσε περαιτέρω τις εναέριες δυνατότητές της. Ωστόσο, τα τουρκικά UAV αντιμετώπισαν τα ρωσικά αντιαεροπορικά συστήματα Pantsir-S1 (Królikowski, 2022). Στη σύγκρουση του Ναγκόρνο-Καραμπάχ μεταξύ της Αρμενίας και του Αζερμπαϊτζάν το 2020 έγινε εκτεταμένη χρήση UAV, συμπεριλαμβανομένων των τουρκικών Bayraktar TB2 και των ισραηλινών drones, για πλήγματα ακριβείας και αντιαεροπορικές αποστολές. Οι δυνάμεις του Αζερμπαϊτζάν, με την υποστήριξη της Τουρκίας και του Ισραήλ, κατάφεραν να καταστείλουν τα αρμενικά μέσα αεράμυνας. Τα UAV χρησιμοποιήθηκαν ακόμη και για στοχευμένες δολοφονίες, αλλάζοντας ουσιαστικά τη δυναμική του σύγχρονου πολέμου (Królikowski, 2022).

4.3 Η οικονομική παράμετρος

Οι στρατιωτικές και αμυντικές δαπάνες της Τουρκίας έχουν υποστεί σημαντικές αλλαγές με την πάροδο των ετών (γράφημα 1). Αυτές δεν αντικατοπτρίζουν μόνο τις προθέσεις της Τουρκίας στην εξωτερική της πολιτική, αλλά και την οικονομική της κατάσταση, το διεθνές κλίμα και την εσωτερική της κατάσταση (πχ Κουρδικό).



Γράφημα 4-1. Στρατιωτικές δαπάνες/προϋπολογισμός άμυνας της Τουρκίας και ποσοστό του ΑΕΠ

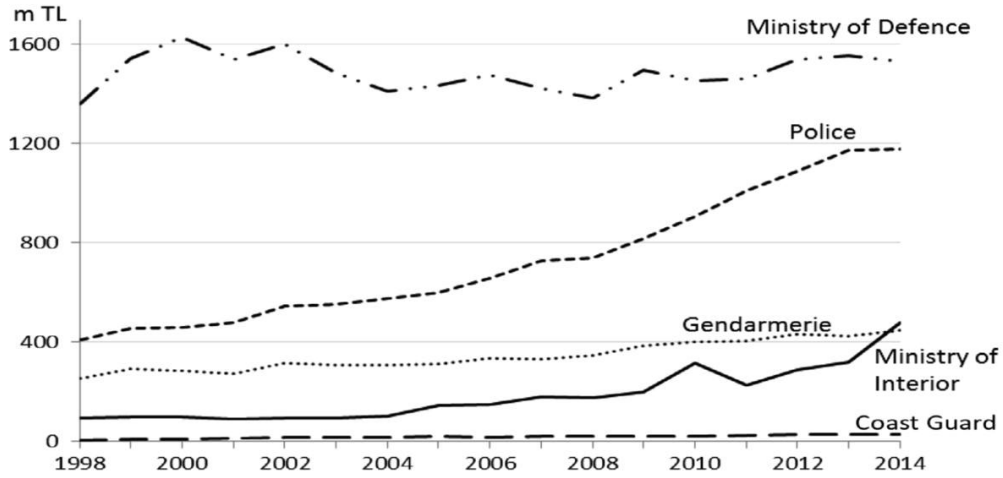


Γράφημα 4-2. Σύγκριση στρατιωτικών δαπανών/προϋπολογισμού άμυνας Τουρκίας/ Ελλάδας

Πηγή: World Bank[2]

Σε αντίθεση με την υπόθεση των σταθερά υψηλών επενδύσεων στον στρατό, ένα σημαντικό μέρος των στρατιωτικών δαπανών της Τουρκίας κατευθύνεται ιστορικά προς τις υπηρεσίες εσωτερικής και συνοριακής ασφάλειας και όχι προς το Υπουργείο Άμυνας. Αυτό είναι εμφανές στο γράφημα 2 , το οποίο δείχνει ότι οι υπηρεσίες ασφαλείας λάμβαναν σταθερά μεγαλύτερο μερίδιο του εθνικού προϋπολογισμού.

Τα πρώτα χρόνια της κυβέρνησης ΑΚΡ, υπήρξε μείωση του προϋπολογισμού του Υπουργείου Άμυνας, η οποία αποδόθηκε στις μεταρρυθμίσεις αποστρατιωτικοποίησης και στις αντιδράσεις για τις ενέργειες του στρατού το 2007. Ωστόσο, η τάση αυτή μεταβλήθηκε κατά τη δεύτερη θητεία του Κόμματος ΑΚΡ, ιδίως μετά τη νίκη στις εκλογές του 2007. Ενώ ο εκδημοκρατισμός συνήθως οδηγεί σε μείωση των στρατιωτικών δαπανών σε ορισμένες χώρες, η εμπειρία της Τουρκίας έχει δει αύξηση των δαπανών για την ασφάλεια και τις στρατιωτικές δαπάνες, εδώ έχουμε μάλλον την αντανάκλαση της «αλλαγής καθεστώτος», από το Τουρκικό βαθύ κράτους με τον πολιτικά πανίσχυρο στρατό, η Τουρκία πέρασε στην πολιτική παντοκρατορία του Ερντογάν. Η σύμπτωση της μετάβασης αυτής και της μεταβολής δαπανών δεν είναι τυχαία. Επιπλέον, η χρηματοδότηση εκτός προϋπολογισμού, συμπεριλαμβανομένου του Ταμείου Υποστήριξης της Αμυντικής Βιομηχανίας, παρουσιάζει προκλήσεις στην ακριβή αξιολόγηση των προϋπολογισμών (Seren, 2020) για την ασφάλεια και την άμυνα (γράφημα 2, πίνακας 1).



Γράφημα 4-3. Κατανομή δαπανών

Οι μυστικές πιστώσεις περιπλέκουν περαιτέρω την ανάλυση του προϋπολογισμού, με τους επικριτές να εκφράζουν ανησυχίες σχετικά με τη διαφάνεια, τις αυξημένες δαπάνες και τη συσχέτισή τους με τα έσοδα του προϋπολογισμού. Συνοπτικά, τα πρότυπα αμυντικών δαπανών της Τουρκίας είναι πολύπλευρα, επηρεαζόμενα από παράγοντες όπως η

[2] https://www.macrotrends.net/countries/TUR/turkey/military-spending-defense-budget'>Turkey Military Spending/Defense Budget 1960-2023. www.macrotrends.net. Retrieved 2023-09-02

χρηματοδότηση εκτός προϋπολογισμού, οι εξελισσόμενες έννοιες ασφάλειας και οι μυστικές πιστώσεις. Αυτές οι πολυπλοκότητες3 καθιστούν δύσκολη τη διαμόρφωση ακριβούς ανάλυσης δεδομένων, αλλά παρέχουν πληροφορίες για τις τάσεις των στρατιωτικών και αμυντικών δαπανών της Τουρκίας (Seren, 2020).

Πίνακας 4-1. Αμυντικός προϋπολογισμός της Τουρκίας ανά έτος

	2013	2014	2015	2016	2017	2018	2019
Defense Services	19,784,158	21,255,644	22,876,604	26,550,460	30,779,685	41,494,933	53,349,228
Military Defense Services	19,476,021	20,895,020	22,155,915	25,564,000	29,422,100	38,779,026	49,659,293
Civil Defense Services	306,688	177,595	81,179	66,754	66,962	25,991	53,660
Foreign Military Assistance Services	0	60,018	39,500	48,750	53,032	152,000	81,750
Non-Classified Defense Services	1,449	123,011	600,010	870,956	1,237,591	2,537,916	3,554,525
Budget Realization	408,224,560	448,752,337	506,305,093	584,071,431	678,269,193	830,809,401	999,489,433
Share in the Budget (%)	4.8%	4.7%	4.5%	4.5%	4.5%	5.0%	5.3%

[3] Ενδιαφέρον έχει ότι μια σειρά επιχειρηματιών που συνεργάζεται το καθεστώς Ερντογάν έχει βρεθεί τόσο στα Panama Papers , κάτι που καθιστά τα μεγέθη δαπανών που εμφανίζει η Τουρκία επισφαλή αν όχι εντελώς αναξιόπιστα πχ https://www.iefimerida.gr/kosmos/pandora-papers-ergolabos-erntogan-palatia-agkyra

5 Κίνδυνοι και αποφάσεις

5.1 Risk Matrix

Risk Matrix: Για την Ελλάδα, από την χρήση UAVs, δορυφόρων και συστημάτων πληροφοριών από μέρους της Τουρκίας.

Ιεράρχηση των κινδύνων:

Επίπεδο 1: Γενικοί κίνδυνοι

1 Κυριαρχία και εδαφική ακεραιότητα:

Μη επανδρωμένα αεροσκάφη (UAV), δορυφόροι και συστήματα πληροφοριών ενδέχεται να αναπτυχθούν για τη συλλογή πληροφοριών που παραβιάζουν την ελληνική κυριαρχία και εδαφική ακεραιότητα.

2 Ασφάλεια και εθνική άμυνα:

Η ανάπτυξη προηγμένης τεχνολογίας από την Τουρκία θα μπορούσε να θέσει σε κίνδυνο την εθνική ασφάλεια και τις αμυντικές δυνατότητες της Ελλάδας.

Επίπεδο 2: Ειδικοί κίνδυνοι

1 Συλλογή στρατηγικών πληροφοριών:

Η ανάπτυξη από την Τουρκία συστημάτων πληροφοριών, δορυφόρων και UAV θα μπορούσε να της παρέχει στρατηγικές πληροφορίες σχετικά με τις ελληνικές στρατιωτικές επιχειρήσεις και εγκαταστάσεις.

2 Επιτήρηση συνόρων και εισβολές:

Τα UAV θα μπορούσαν να χρησιμοποιηθούν για την επιτήρηση των συνόρων, οδηγώντας σε πιθανές παραβιάσεις του εναέριου χώρου και εδαφικές παραβιάσεις.

3 Θαλάσσιες επιχειρήσεις και επιτήρηση (search and rescue):

Η ανάπτυξη δορυφορικών συστημάτων θα μπορούσε να ενισχύσει την ικανότητα της Τουρκίας να παρακολουθεί τις ελληνικές θαλάσσιες δραστηριότητες, επηρεάζοντας τις ναυτικές επιχειρήσεις και τη θαλάσσια ασφάλεια της Ελλάδας.

4 Τρωτά σημεία στην κυβερνοασφάλεια:

Η ενσωμάτωση των συστημάτων πληροφοριών θα μπορούσε να εκθέσει την Ελλάδα σε απειλές και τρωτά σημεία στον κυβερνοχώρο, θέτοντας ενδεχομένως σε κίνδυνο κρίσιμες υποδομές.

Πίνακας 5-1. Λίστα με τους ειδικούς κινδύνους που αναγνωρίστηκαν σχετικά με τα συστήματα πληροφόρησης

ID Κινδύνου	Κίνδυνοι
1	Συλλογή στρατηγικών πληροφοριών
2	Επιτήρηση συνόρων και εισβολές
3	Θαλάσσιες επιχειρήσεις και επιτήρηση (search and rescue)
4	Τρωτά σημεία στην κυβερνοασφάλεια

Risk Analysis/ Ανάλυση κινδύνου:

Κίνδυνος 1: Συλλογή στρατηγικών πληροφοριών

Αντιπροσωπεύει έναν σοβαρό κίνδυνο για την ασφάλεια και τα εθνικά συμφέροντα της Ελλάδας σε σχέση με την τουρκική τεχνολογική ανάπτυξη. Αυτός ο κίνδυνος περιλαμβάνει τη συλλογή ελληνικών στρατηγικών πληροφοριών από την Τουρκία, καθώς μπορεί να αναπτύξει UAVs, δορυφόρους και συστήματα πληροφοριών για τον σκοπό αυτό. Αυτές οι πληροφορίες αφορούν ελληνικές στρατιωτικές επιχειρήσεις, τις στρατιωτικές δομές και τις εγκαταστάσεις, και μπορούν να χρησιμοποιηθούν για την ανάπτυξη αντίμετρων και τακτικών επιθέσεων. Η συλλογή αυτής της πληροφορίας από την Τουρκία αντιπροσωπεύει απειλή για την ελληνική κυριαρχία και εδαφική ακεραιότητα, καθώς οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για να διεκδικήσουν εδάφη ή για να προετοιμαστούν ειδικές επιχειρήσεις ασύμμετρου χαρακτήρα.

Πιθανότητα: Υψηλή

Επιπτώσεις: Υψηλός

Επίπεδο κινδύνου: Υψηλός

Αντιμετώπιση: Ενίσχυση των προσπαθειών αντικατασκοπείας, διασφάλιση των διαύλων επικοινωνίας και διατήρηση της ετοιμότητας για πιθανές απειλές.

Κίνδυνος 2: Επιτήρηση συνόρων και εισβολές

Εδώ επισημαίνεται ο πιθανός κίνδυνος που αντιμετωπίζει η Ελλάδα από την τουρκική τεχνολογική ανάπτυξη, ο οποίος συνίσταται στην δυνατότητα επιβλέψης των συνόρων και πιθανών εισβολών μέσω της χρήσης UAVs. Η Τουρκία μπορεί να εκμεταλλευτεί τα UAVs για την παρακολούθηση των συνόρων, δημιουργώντας έναν αυξημένο κίνδυνο για πιθανές παραβιάσεις του εναέριου χώρου και εδαφικές εισβολές. Αυτό μπορεί να αποτελέσει απειλή για την ελληνική κυριαρχία και εδαφική ακεραιότητα, καθώς η παρακολούθηση των συνόρων από την αεροπορία επιτρέπει στην Τουρκία να αξιολογήσει πιθανά σημεία εισβολής ή παραβίασης του εναέριου χώρου. Επιπλέον, η δυνατότητα των UAVs να παρακολουθούν τα σύνορα αυξάνει τον κίνδυνο της ανατροπής της ελληνικής αεροπορικής

ασφάλειας και την ανάγκη για στρατηγική αντίδραση σε περίπτωση παραβίασης. Επίσης, η παρακολούθηση των συνόρων μπορεί να επηρεάσει τις ναυτικές επιχειρήσεις και τη θαλάσσια ασφάλεια της Ελλάδας, καθώς η πληροφορία για την θαλάσσια δραστηριότητα μπορεί να χρησιμοποιηθεί για στρατηγικούς σκοπούς. Συνολικά, ο "Κίνδυνος 2" αποτελεί μια αυξημένη απειλή για την ελληνική ασφάλεια και απαιτεί στρατηγικές αντιμετώπισης για την διατήρηση της εδαφικής ακεραιότητας και της αεροπορικής ασφάλειας.

Πιθανότητα: Υψηλή

Επιπτώσεις: Μέτριες

Επίπεδο κινδύνου: Υψηλός

Αντιμετώπιση:: Ενίσχυση των δυνατοτήτων εναέριας επιτήρησης, δημιουργία διαύλων επικοινωνίας με την Τουρκία για την πρόληψη παραβιάσεων του εναέριου χώρου και επένδυση σε μηχανισμούς ταχείας αντίδρασης.

Κίνδυνος 3: Θαλάσσιες επιχειρήσεις και επιτήρηση (Search and rescue)

Εδώ αναφερόμαστε σε μια σημαντική απειλή για την Ελλάδα από την τουρκική τεχνολογική ανάπτυξη. Αυτός ο κίνδυνος περιλαμβάνει την δυνατότητα της Τουρκίας να ενισχύσει την ικανότητά της να παρακολουθεί τις ελληνικές θαλάσσιες δραστηριότητες μέσω της ανάπτυξης δορυφορικών συστημάτων. Με αυτά τα συστήματα, η Τουρκία μπορεί να παρακολουθεί τη θαλάσσια κυκλοφορία, τις ναυτικές επιχειρήσεις και τη θαλάσσια ασφάλεια στην περιοχή. Αυτό δημιουργεί μια αυξημένη δυνατότητα της Τουρκίας να παρεμβαίνει σε θαλάσσιες επιχειρήσεις της Ελλάδας και να επηρεάζει την θαλάσσια ασφάλεια, ενδεχομένως να αποκτά και ένα χρονικό πλεονέκτημα για την ενεργή αμφισβήτηση των συνόρων μέσω της αμφισβήτησης (στο πεδίο) του χώρου ευθύνης έρευνας και διάσωσης της κάθε χώρας. Επιπλέον, αυτή η δυνατότητα ενδέχεται να επηρεάσει τη διπλωματική κατάσταση στην περιοχή, καθώς η παρακολούθηση των θαλάσσιων επιχειρήσεων μπορεί να οδηγήσει συνολικά σε εντάσεις και συγκρούσεις. Συνολικά, ο "Κίνδυνος 3" αντιπροσωπεύει μια απειλή για την θαλάσσια ασφάλεια και τις θαλάσσιες επιχειρήσεις της Ελλάδας, καθώς δίνει στην Τουρκία τη δυνατότητα να παρακολουθεί και να επηρεάζει τις θαλάσσιες δραστηριότητες στην περιοχή.

Πιθανότητα: Υψηλή

Επίπτωση: Υψηλός

Επίπεδο κινδύνου: Υψηλός

Αντιμετώπιση:: Ενίσχυση των ναυτικών περιπολιών, καθιέρωση σαφών θαλάσσιων ορίων και συμμετοχή σε διπλωματικές συζητήσεις για την αποτροπή της κλιμάκωσης.

Κίνδυνος 4: Ευπάθειες στην κυβερνοασφάλεια

Αυτός ο κίνδυνος περιλαμβάνει το ενδεχόμενο εισβολής στα κρίσιμα συστήματα και την πληροφορία της Ελλάδας μέσω κυβερνοεπιθέσεων. Η Τουρκία μπορεί να αξιοποιήσει την τεχνολογική ανάπτυξή της για να επιτεθεί στα δίκτυα και τα συστήματα της Ελληνικής κυβέρνησης και των κρίσιμων υποδομών. Αυτό μπορεί να προκαλέσει πολιτική και κοινωνική αναταραχή (ας σκεφτεί κάποιος μια επίθεση σε πολιτικά και όχι στρατιωτικά συστήματα, όπως για παράδειγμα τις μέρες των πανελλαδικών εξετάσεων ή στους ΑΔΜΗΕ και ΔΕΔΔΗΕ), εκτεταμένη οικονομική αστάθεια (σε συγκεκριμένα χρονικά διαστήματα), και απώλεια εμπιστοσύνης στην ασφάλεια των πληροφοριών. Επιπλέον, ο "Κίνδυνος 4" αντιπροσωπεύει τη δυνατότητα ανάκτησης ευαίσθητων πληροφοριών από την Ελλάδα, περιλαμβανομένων πληροφοριών σχετικών με την ασφάλεια, την άμυνα, και την εθνική ασφάλεια. Οι ευπάθειες στην κυβερνοασφάλεια μπορεί να έχουν σοβαρές επιπτώσεις στην εθνική ασφάλεια της Ελλάδας και απαιτούν συνεχή προσοχή και προληπτικά μέτρα για την προστασία των κρίσιμων κυβερνοασφαλειακών συστημάτων και της ευαίσθητης πληροφορίας.

Πιθανότητα: Μέτρια

Επιπτώσεις: Υψηλές

Επίπεδο κινδύνου: Υψηλός

Αντιμετώπιση: Επενδύστε σε ισχυρά μέτρα κυβερνοασφάλειας, διεξάγετε τακτικές αξιολογήσεις των κρίσιμων συστημάτων και αναπτύξτε ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών.

Πίνακας 5-2. Μήτρα κινδύνων (risk matrix) με την κατανομή των κινδύνων αναλόγως πιθανότητας και αντικτύπου τους

Risk	Πιθανότητα	Αντίκτυπος	Επίπεδο κινδύνου
1. Συγκέντρωση στρατηγικών πληροφοριών	Υψηλή	Υψηλός	h/h Υψηλό
2. Επιτήρηση συνόρων και εισβολές	Υψηλή	Μέτριος	h/m Υψηλό
3. Θαλάσσιες επιχειρήσεις και επιτήρηση(SAR)	Υψηλή	Υψηλός	h/h Υψηλό
4.Ευπάθειες στην κυβερνοασφάλεια	Μέτρια	Υψηλός	m/h Υψηλό

Πίνακας 5-3. Μήτρα κινδύνων (risk matrix)

	ΑΝΤΙΚΤΥΠΟΣ			
ΠΙΘΑΝΟΤΗΤΑ		ΧΑΜΗΛΟΣ	ΜΕΤΡΙΟΣ	ΥΨΗΛΟΣ
	ΧΑΜΗΛΗ			
	ΜΕΤΡΙΑ			**4**
	ΥΨΗΛΗ		**2**	**1,3**

5.2 Δενδροδιάγραμμα αποφάσεων

Δενδρόγραμμα αποφάσεων: Στρατηγικές μετριασμού των κινδύνων από την τουρκική ανάπτυξη UAVs, δορυφόρων και συστημάτων πληροφοριών

Το ακόλουθο δενδροδιάγραμμα αποφάσεων αποτελεί μια επεξεργασμένη σύνθεση στρατηγικών μετριασμού των κινδύνων που απορρέουν από την τουρκική ανάπτυξη UAV, δορυφόρων και συστημάτων πληροφοριών στην Ελλάδα. Η διαδικασία δημιουργίας αυτού του δενδροδιαγράμματος αποφάσεων περιελάμβανε μια συστηματική και εμπεριστατωμένη προσέγγιση, με στόχο την παροχή ενός ολοκληρωμένου συνόλου δράσεων για την αντιμετώπιση των εντοπισμένων κινδύνων.

Ξεκινώντας με την ανάλυση του πίνακα κινδύνων, ο οποίος αξιολογούσε την πιθανότητα και τον αντίκτυπο κάθε κινδύνου, δημιουργήθηκε ένα δομημένο πλαίσιο. Το δενδροδιάγραμμα αποφάσεων που προέκυψε παρουσιάζει μια λογική ιεραρχία στρατηγικών και δράσεων, που κυμαίνεται από τα γενικότερα μέτρα έως τις ειδικές παρεμβάσεις. Η μεθοδολογία περιελάμβανε καταιγισμό ιδεών, αξιολόγηση και οργάνωση των πιθανών τρόπων δράσης, λαμβάνοντας υπόψη τη σκοπιμότητα, την αποτελεσματικότητα και τις πιθανές επιπτώσεις.

Αυτό το δενδροδιάγραμμα αποφάσεων συνδυάζει διαφορετικές προσεγγίσεις, περιλαμβάνοντας διπλωματικές προσπάθειες, τεχνολογικές βελτιώσεις και επιχειρησιακές απαντήσεις. Ο στόχος ήταν να επιτευχθεί ισορροπία μεταξύ προληπτικών πρωτοβουλιών και αντιδραστικών τακτικών, ενώ παράλληλα προωθήθηκαν τόσο οι άμεσες αντιδράσεις όσο και τα προληπτικά μέτρα.

Κάθε κατηγορία κινδύνου αντιμετωπίζεται προσεκτικά, παρουσιάζοντας ένα φάσμα στρατηγικών που προσφέρουν στην Ελλάδα μια ολοκληρωμένη εργαλειοθήκη για την αποτελεσματική αντιμετώπιση των προκλήσεων που θέτει η Τουρκική πλευρά. Ο ολιστικός χαρακτήρας του δενδροδιαγράμματος αποφάσεων θα μπορούσε να αποτελεί ένα παράδειγμα της δέσμευσης για τη διαφύλαξη των συμφερόντων, της κυριαρχίας και της ασφάλειας της Ελλάδας απέναντι στις εξελισσόμενες απειλές.

1 Κίνδυνος συγκέντρωσης στρατηγικών πληροφοριών

└─ Ενίσχυση των προσπαθειών αντικατασκοπείας

│ ├─ Ενίσχυση των υπηρεσιών πληροφοριών

│ ├─ Βελτίωση της ανταλλαγής πληροφοριών

│ └─ Ανάπτυξη προγραμμάτων εσωτερικών απειλών

└─ Ασφαλή κανάλια επικοινωνίας

├─ Εφαρμογή κρυπτογραφημένης επικοινωνίας

├─ Αξιοποίηση ασφαλούς δορυφορικής επικοινωνίας

└─ Διεξαγωγή τακτικών ελέγχων επικοινωνίας

2. Κίνδυνος επιτήρησης συνόρων και εισβολών

└─ Ενίσχυση της εναέριας επιτήρησης

│ ├─ Ανάπτυξη προηγμένων συστημάτων ραντάρ

│ ├─ Αύξηση των περιπολιών μη επανδρωμένων αεροσκαφών κατά μήκος των συνόρων

│ └─ Ενίσχυση των συστημάτων έγκαιρης προειδοποίησης

└─ Δημιουργία διαύλων επικοινωνίας με την Τουρκία και Ε.Ε

├─ Κοινή επιτήρηση του εναέριου χώρου με Ε.Ε

├─ Εφαρμογή άμεσης γραμμής επικοινωνίας για παραβιάσεις του εναέριου χώρου

└─ Καθιέρωση πρωτοκόλλων επικοινωνίας για κρίσεις

└─ Επένδυση σε μηχανισμούς ταχείας αντίδρασης

├─ Ενίσχυση αεροπορικών μονάδων ταχείας αντίδρασης

├─ Ενίσχυση των δυνατοτήτων αναχαίτισης

└─ Εφαρμογή πρωτοκόλλων άμεσου κλεισίματος του εναέριου χώρου

3. Κίνδυνος από θαλάσσιες επιχειρήσεις και επιτήρηση (Search and rescue)

└─ Ενίσχυση των ναυτικών περιπολιών

│ ├─ Αύξηση της συχνότητας των θαλάσσιων περιπολιών

- Ανάπτυξη πρόσθετων ναυτικών μέσων (Unmanned surface vehicle ή USV)
- Συνεργασία με διεθνείς ναυτικές δυνάμεις
- Καθιέρωση σαφών θαλάσσιων ορίων
  - Ενίσχυση των συμφωνιών για τα θαλάσσια σύνορα
  - Διεξαγωγή κοινών περιπολιών με Ε.Ε
  - Προώθηση διπλωματικών διαλόγων για συνοριακές διαφορές
- Διπλωματικές συζητήσεις για την πρόληψη της κλιμάκωσης
  - Διεξαγωγή διμερών συνομιλιών με την Τουρκία
  - Αξιοποίηση διεθνών οργανισμών για διαμεσολάβηση
  - Προώθηση μέτρων οικοδόμησης εμπιστοσύνης

4. Κίνδυνος τρωτών σημείων κυβερνοασφάλειας
- Επένδυση σε αξιόπιστα μέτρα κυβερνοασφάλειας
  - Ενίσχυση των πρωτοκόλλων ασφάλειας δικτύου
  - Τακτική ενημέρωση λογισμικού και υλικού
  - Διεξαγωγή συχνών ελέγχων κυβερνοασφάλειας
- Αξιολόγηση σε τακτικά διαστήματα των κρίσιμων συστημάτων
  - Εντοπισμός τρωτών σημείων σε βασικές υποδομές
  - Δημιουργία συστημάτων ανίχνευσης εισβολών
  - Ανάπτυξη σχεδίων αντιμετώπισης περιστατικών στον κυβερνοχώρο
- Ανάπτυξη ολοκληρωμένου σχεδίου αντιμετώπισης περιστατικών
  - Καθορισμός ρόλων και αρμοδιοτήτων
  - Εφαρμογή πρωτοκόλλων επικοινωνίας κατά τη διάρκεια περιστατικών
  - Διεξαγωγή τακτικών εκπαιδεύσεων και προσομοιώσεων

6 Συμπεράσματα

Στην παρούσα εργασία ανιχνεύθηκαν οι διαδρομές τις έννοιας της παραπλάνησης στον χρόνο. Ταυτόχρονα εστιάσαμε στις σύγχρονες διαστάσεις της από ευρέως χρησιμοποιούμενες στο στρατιωτικό πεδίο, στο πεδίο της πληροφορίας των υπηρεσιών και εν τέλει στο πως το ίδιο το σώμα των πολιτών μπορεί να επηρεαστεί από υβριδικές επιχειρήσεις. Το τελευταίο αποτελεί μια εξαιρετικά σημαντική διάσταση καθώς το πολιτικό μπορεί να καθορίσει τα υπόλοιπα, από την απλή κατανομή οικονομικών πόρων (άρα και απόκτησης δυνατοτήτων, καθώς οι πόροι μεταφράζονται σε δομές, τεχνολογία και δυνατότητες) έως συγκεκριμένες αποφάσεις χάραξης πολιτικής που μπορεί εν τέλει να συμπορεύονται με τους στόχους που ένας αντίπαλος θέτει.

Εξίσου σημαντικές όμως είναι δύο ακόμα διαστάσεις που αναδείχθηκαν στο πλαίσιο της εργασίας. Η πρώτη ήταν το πλέγμα δομών, δηλαδή το τεχνολογικό οικοσύστημα, που δημιουργήθηκε στην Τουρκία και με την σειρά του μπόρεσε να παράγει αποτελέσματα σε επίπεδο οπλικών συστημάτων, ιδίως σε ότι αφορά τα uav με τις συγκεκριμένες δυνατότητες που δίνουν τόσο στο καθ’αυτό πεδίο της μάχης όσο και στο επίπεδο συλλογής πληροφοριών. Διερευνήθηκε η πρόοδος -σε τεχνικό επίπεδο- αυτών, αλλά και η οικονομική διάσταση. Παρότι ο χώρος για κάτι τέτοιο ήταν περιορισμένος, έγινε σαφής η σχέση ανάπτυξης και αδιαφάνειας σε μια χώρα με το θεσμικό πλαίσιο της Τουρκίας, ενώ πολλές φορές διατυπώθηκε η αμφιβολία της ακρίβειας των ανακοινώσεων σε ότι αφορά τις πραγματικές δυνατότητες, χωρίς όμως αυτό να σημαίνει ότι θα πρέπει να υποτιμηθούν ως συστήματα.

Η δεύτερη διάσταση περιλαμβάνει την αναγνώριση κινδύνου, την ανάλυση του επιπέδου του αλλά και δημιουργία «δρόμων» αντιμετώπισης αυτών. Κλείνοντας, θα πρέπει να τονιστεί ότι το τεχνολογικό χάσμα που μας χωρίζει από την Τουρκία στον τομέα αυτό, καίτοι υπαρκτό, είναι μικρότερο από αυτό που σκεφτόμαστε ή πιθανολογούμε. Αυτό προκύπτει όχι από μια γενική διαίσθηση ή από έλλειψη αξιοπιστίας των Τουρκικών ανακοινώσεων , αλλά από τον τρόπο που δομείται η κατασκευή τους, καθώς πρόκειται σε ένα πολύ σημαντικό βαθμό για συναρμολόγηση και λιγότερο για πλήρη και αυτοτελή κατασκευή μέσω R&D. Αυτό ακριβώς είναι το «σήμα» πως επείγει η χώρα να συμμετάσχει σε ευρύτερα σχήματα έρευνας και (συμ)παραγωγής, είτε στο Ευρωπαϊκό πλαίσιο, είτε σε συνεργασία με τις ΗΠΑ ή ακόμα (και σκεπτόμενοι πέρα από τις συνήθεις οδούς) με χώρες όπως η Κορέα και η Ιαπωνία.

Κατάλογος Πηγών

Alberts, D.S, Gartska, J.J., & Stein, F.P. (1999). Network centric warfare: Developing and leveraging information superiority. Washington, CCRP

Army, Secretary of the. (2004). Field Manual 1-02 “Operational Terms and Graphics.” Washington D.C. Διαθέσιμο στο https://army.rotc.umich.edu/public/resources/FM1-02OperationalTerms.pdf

Barry, John (1991), The Nuclear Option: Thinking the Unthinkable; Newsweek, 14.1.1991, pp.· 12-13.

Barton, W., (2007), STRATAGEM: Deception and Surprise in War. London, Artech House

Baykar, 2023, İnsansız Hava Aracı Sistemleri/Συστήματα μη επανδρωμένων αεροσκαφών, διαθέσιμο στο https://baykartech.com/tr/insansiz-hava-araci-sistemleri/

Bennett, Michael & Waltz, Edward,(2007) Counterdeception Principles and Applications for National Security ,Boston & London: Artech House

Berkowitz, Br. (2001) “Information Warfare: Time to Prepare.” Issues in Science and Technology 17, no. 2

Bernays, E. (2015). Προπαγάνδα, Αθήνα, Νεφέλη

Bernhardt, Ute, & Ruhmann, Ingo. (1997). Der digitale Feldherrnhügel, Military Systems: Informationstechnik für Führung und Kontrolle. Dossier Nr. 24. Διαθέσιμο στο https://wissenschaft-und-frieden.de/seite.php?dossierID=050

Bok, S. (1999). Lying: Moral Choice in Public and Private Life. New York, Vintage Books

Bradshaw, S., & Howard, P. (2019). The global disinformation order. Διαθέσιμο στο https://comprop.oii.ox.ac.uk/research/cybertroops2019/

Breuer W. (2002) “Deception of World War II”, New York, John Wiley & Sons

Bruce, James B. & Bennett, Michael, “Foreign Denial and Deception: Analytical Imperatives”, στο George, Roger Z. & Bruce, James B., (Επιμέλεια), Analyzing Intelligence: Origins, obstacles, and innovations (Washington D.C.: Georgetown University Press, 2008)

Carr, E. (2011). Η εικοσαετής κρίση 1919-1939. Εισαγωγή στη μελέτη των διεθνών σχέσεων. , Αθήνα, Ποιότητα

Carruthers, S.L. (2000). The media at war. Houndsville: MacMillan Press

Cohen, S. Are There Moral Limits to Military Deception?. Philosophia 44, 1305–1318 (2016).

Creswell W., Creswell D. (2021). Μετ. Βενετσάνου. «Σχεδιασμός Έρευνας». Αθήνα: Προπομπός.

Cronin B., Crawford H. (1999). Information Warfare. Its Application in Military and Civilian Contexts, „The Information Society", Vol. 15, No. 4, Indiana University, Bloomington.

Cronin, B., Crawford H. (2006). Information Warfare: Its Application in Militaryand Civilian Contexts διαθέσιμο στο: https://doi.org/10.1080/019722499128420

Cullen, Dr. Patrick J., & Reichborn-Kjennerud, Erik. (2017). Understanding Hybrid Warfare: A Multinational Capability Development Campaign project. Διαθέσιμο στο https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Daniel D. & Herbig K., (1981) "Strategic Military Deception , New York, Pergamon Press

Drucker, P. F. (1994). The Age of Social Transformation: The Atlantic Monthly 274: 27

Drucker, P. F. (1999). Post-capitalist society: Science Publishing Company PWN

Endsley, M., Jones, W. (1997). Situation Awareness Information Dominance & Information Warfare. 94

Farr, W., (1999), the third temple's holy of holies: israel's nuclear weapons. Future Warfare Series No. 2 , Alabama, Maxwell Air Force Base.

Field Manual 6-0 (2014) "Commander and Staff Organization and Operations". USA: Headquarters Department of the Army. διαθέσιμο στο https://www.milsci.ucsb.edu/sites/default/files/sitefiles/fm6_0.pdf

Gerasimov, Valery. (2013). The value of science in anticipation. New challenges require rethinking the forms and methods of conducting military operations. VPK-News. Διαθέσιμο στο https://www.vpk-news.ru/articles/14632

Gerwehr, S., & Glenn, R.W. (2000). Unweaving the web: Deception and adaptation in future urban operations.Santa Monica, CA

Gestrlé, J. (2014). Η πολιτική επικοινωνία. Αθήνα, Τυπωθητώ - Γ. Δαρδάνος

Godson, R., (2000), Strategic Denial and Deception. Calhoun, The NPS Institutional Archive

Godson, Roy & Wirtz, James J., “Strategic Denial and Deception”, στο Godson, Roy & Wirtz, James J., (Επιμέλεια), Strategic Denial and Deception: The Twenty-First Century Challenge (New Brunswick (U.S.A.) & London (U.K.): Transaction Publishers, 2005)

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. International Affairs, 94(5), 975-994

Hall, W. (2003). Stray voltage. Annapolis, Naval Institute Press

Handel M., (1987) “Strategic and Operational deception in Historical Perspective” διαθέσιμο στο https://doi.org/10.1080/02684528708431904

Hetherington, M. (2006). Why Trust Matters: Declining Political Trust and the Demise of American Liberalism. New Jersey, Princeton University Press.

Hicks, K., Friend, A., Federici, J., Shah, H., Donahoe, M., Conklin, M., Sheppard, L. (2019). By other means: Part I. Rowman & Littlefield

Hutchinson, W., (2006). Information warfare and deception. Informing Science, 9, 213.

Joint Publication 3.13.1 (2012) “Electronic Warfare” USA, Joint Staff, διαθέσιμο στο https://irp.fas.org/doddir/dod/jp3_13.pdf

Joint Publication 3.13.1 (2016) “Operations Security” USA, Joint Staff, διαθέσιμο στο https://media.defense.gov/2020/Oct/28/2002524944/-1/-1/0/JP%203-13.3-OPSEC.PDF

Joint Publication 3-58 (1996) “Joint Doctrine for Military Deception” USA, Joint Staff, διαθέσιμο στο https://irp.fas.org/doddir/dod/jp3_58.pdf

Karpf, D. (2017). Digital politics after Trump. Annals of the International Communication Association, 41(2), 198–207. https://doi.org/10.1080/23808985.2017.1316675

Knightley, P. (2000). The first casualty. Baltimore: John Hopkins University Press

Królikowski, Hubert. (2022). The Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts – Selected Issues. Politeja. 19.

Libicki, M. (2017). The convergence of information warfare. Strategic Studies Quarterly, 11(2)

Masterman, J., (2000), The double-cross system , Guilford, Lyons Press

Mearsheimer, J. (2012). Γιατί οι πολιτικοί λένε ψέματα. Η αλήθεια για το ψέμα στη διεθνή πολιτική σκηνή. Αθήνα, Πατάκη

Mitchell, R.W., & Thompson, N.S. (Eds.). (1986). Deception: Perspectives on human and nonhuman deceit. Albany, State University of New York Press

Molander R., Riddile A.,& Wilson P.,(1996) “Strategic War in Cyberspace” διαθέσιμο στο https://www.rand.org/pubs/research_briefs/RB7106.html

Nye, J. (2009). Ηγεσίες που πρωτοπορούν. Αθήνα, Παπαζήση

Office of the Secretary of Defense. (2017). Annual report to Congress: Military and Security Developments Involving the People’s Republic of China. Washington D.C

Panarin, Igor Nicolaevich. (1998). InfoWar and Authority Διαθέσιμο στο https://archive.aec.at/me-dia/archive/1998/183589/File_03450_AEC_FE_1998.pdf

Petrőcz J., (2021), An insight into today’s Turkish military industry, Safety and Security Sciences Review, Vol 3, No 1 (SI), pp 105-122

Pollack, K., (2002), Arabs at War: Military Effectiveness, 1948–1991. University of Nebraska Press

Prosser, S., (2009), The Battle of Aigos Potamoi. Munich, GRIN Verlag

Reid, J. (2009). Politicizing connectivity. Cambridge Review of International Affairs, 22(4), 607–623. https://doi.org/10.1080/09557570903325520

Rossiter, Ash & Cannon, Brendon. (2022). Turkey's rise as a drone power: trial by fire. Defense & Security Analysis. 38. 1-20.

Rötzer, Florian. (2000a). Israelische Hacker wollen Websites vor pro-palästinensischen Angriffenschützen . Διαθέσιμο στο https://www.telepolis.de/features/Israelische-Hacker-wollen-Websites-vor-pro-palaestinensischen-Angriffen-schuetzen-3442459.html

Rötzer, Florian. (2000b). Taiwans Militär probt Angriffe mit Computerviren Διαθέσιμο στο https://www.telepolis.de/features/Taiwans-Militaer-probt-Angriffe-mit-Computerviren-3447492.html

Ruhmann, Ingo. (2003). Sicherheitspolitische Folgerungen aus dem Golfkrieg. Wissenschaft & Frieden, vol. 3, pp. 27–31. Διαθέσιμο στο https://wissenschaft-und-frieden.de/seite.php?artike-lID=0254

Scheuch, Laszlo, & Möhle, Holger. (2018, January 28). Das eigene System vor Feinden schützen. General-Anzeiger. Bonn. Διαθέσιμο στο https://ga.de/news/politik/deutschland/cyber-zentrum-mit-kommando-in-bonn-soll-ausgebaut-werden_aid-43633923

SEREN, M. (2020). Turkey's Military Spending Trends: A Reflection of Changes in Defense Policy. Insight Turkey, 22(3), 183–214

Shaker, Steven M., & Finkelstein, Robert, (1987), The Bionic Soldier. National Defense, pp. 27–32.

Shlaim, A., (1976), Failures in National Intelligence Estimates: The Case of the Yom Kippur. World Politics, 28(3), pp. 348-380

Shulsky, Abram N. & Schmitt, Garry J., Silent Warfare: Understanding the World of Intelligence (Washington, D.C.: Brassey's Inc., 2002, third edition)

Singer, P. W., & Brooking, E. T. (2018). Likewar. Houghton Mifflin Harcourt.

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective, „Philosophy and Technology" 2012, vol. 25

Taylor, B. C. (2017). Imitation (In) security. Communication Theory, 27(1), 48–69. https://doi.org/10.1111/comt.12104

Tilly, C. (2005). Trust and Rule. New York, Cambridge University Press

U.S. Air Force (2005). Information operations. Air Force Doctrine 2-5, 11 January, 2005 διαθέσιμο στο https://www.globalsecurity.org/military/library/policy/usaf/afdd/3-13/afdd3-13_2011.pdf

Wagner, A. (1999). Life on the Screen: Identity in the Age of the Internet. The Psychohistory Review, 27(2), 113

Weigang, Shen. (1998). Der Informationskrieg – eine Herausforderung. στο G. Stocker & C. Schöpf (Eds.), Information. Macht. Krieg

Zisser, E., (2013), Syria and the October War: The Missed Opportunity. Βρίσκεται στο: The Yom Kippur War: Politics, Legacy, Diplomacy. Oxford, Oxford University Press

Αναδιώτης Σ., (2018), «Η ανάπτυξη drones από την Τουρκία: προβλήματα, αντιμετώπιση, αποτροπή», Πανεπιστήμιο Μακεδονίας, Διπλωματική εργασία

Ζαφειρόπουλος, Κ. (2015). «Πως γίνεται μια επιστημονική εργασία». Εκδόσεις Κριτική:Αθήνα

Ζάχος, Γ., (2003), Μάχη στους Αιγός Ποταμούς, 405 π.Χ.. Αθήνα, Εγκυκλοπαίδεια Μείζονος Ελληνισμού, Μ.Ασία

Κολιόπουλος, Κ. (2010). Η στρατηγική σκέψη από την αρχαιότητα έως σήμερα, Αθήνα, Ποιότητα.

Κουσκουβέλης, Η. (2007). Εισαγωγή στις Διεθνείς Σχέσεις. Αθήνα, Ποιότητα.

Ραγιές, Ι. (2014). Δημόσια Διπλωματία & Στρατηγική Επικοινωνία σε πολυεθνικές στρατιωτικές επιχειρήσεις διαχείρισης κρίσεων. Αθήνα, Σταμούλης

https://cdn.ymaws.com/cicentre.com/resource/resmgr/articles/american_intelligence_journa.pdf