2026-01

þÿ — ¨ µ Å ´ ± ¯ Ã ¸ · Ã · ¤ · Â Á ± ³ ¼ ± Ä ¹ º Ì

þÿ Î Â — Ä µ Ç ½ · Ä ® • ¿ · ¼ ¿ Ã Í ½ · ‘ » »

þÿ ¤ ¹ Â £ Ä Á ± Ä · ³ ¹ º - Â ‘ À ¿ Æ ¬ Ã µ ¹ Â £

þÿ µ Á ¯ ¿ ´ ¿ ¨ · Æ ¹ ± º ¿ Í ¿ » - ¼ ¿ Å .

þÿ ± ½ Ä ± ¶ ® , œ ± Á ¯ ½ ±

Μεταπτυχιακό στις Διεθνείς Σχέσεις, τη Στρατηγική και την Ασφάλεια

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η Ψευδαίσθηση Της Πραγματικότητας: Πώς Η τεχνητή Νοημοσύνη Αλλάζει Τις Στρατηγικές Αποφάσεις Σε Περίοδο Ψηφιακού Πολέμου.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ Πανταζή Μαρίνα
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΕΠΙΒΛΕΠΟΝΤΑ Μικέλης Κυριάκος

ΙΑΝΟΥΑΡΙΟΣ/2026

Πανεπιστήμιο Νεάπολις Πάφος

Μεταπτυχιακό στις Διεθνείς Σχέσεις, τη Στρατηγική και την Ασφάλεια

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η Ψευδαίσθηση Της Πραγματικότητας: Πώς Η τεχνητή Νοημοσύνη Αλλάζει Τις Στρατηγικές Αποφάσεις Σε Περίοδο Ψηφιακού Πολέμου.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ Πανταζή Μαρίνα
ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ Μικέλης Κυριάκος, Φλούρος Φλώρος, Δερμετζής Ιωσήφ

ΙΑΝΟΥΑΡΙΟΣ/2026

Πνευματικά δικαιώματα

Σελίδα Εγκυρότητας

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Πανταζή Μαρίνα

Τίτλος Διπλωματικής Εργασίας: Η Ψευδαίσθηση Της Πραγματικότητας: Πώς Η τεχνητή Νοημοσύνη Αλλάζει Τις Στρατηγικές Αποφάσεις Σε Περίοδο Ψηφιακού Πολέμου

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …… [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:
Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)……[Μικέλης Κυριάκος, Επίκουρος Καθηγητής]

Μέλος Εξεταστικής Επιτροπής: ……[Φλούρος Φλώρος, Επίκουρος Καθηγητής]

Μέλος Εξεταστικής Επιτροπής: ……[Δεμερτζής Ιωσήφ, Επίκουρος Καθηγητής]

Ή ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Η Μαρίνα Πανταζή , γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «**Τίτλος Διπλωματικής Εργασίας: Η Ψευδαίσθηση Της Πραγματικότητας: Πώς Η τεχνητή Νοημοσύνη Αλλάζει Τις Στρατηγικές Αποφάσεις Σε Περίοδο Ψηφιακού Πολέμου**», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Η Δηλούσα

Πίνακας περιεχομένων

Περίληψη

Η παρούσα διατριβή εξετάζει τον τρόπο με τον οποίο η τεχνητή νοημοσύνη μεταβάλλει το σύγχρονο στρατηγικό περιβάλλον, μέσω της παραγωγής και διάδοσης κατασκευασμένης πληροφορίας σε συνθήκες ψηφιακού και υβριδικού πολέμου. Ιδιαίτερη έμφαση δίνεται στη στρατηγική παραπληροφόρηση ως εργαλείο επιρροής που επηρεάζει όχι μόνο τη δημόσια αντίληψη, αλλά και τη διαδικασία λήψης αποφάσεων από κρατικούς και μη κρατικούς δρώντες. Η ανάλυση ξεκινά με την εξέλιξη της τεχνητής νοημοσύνης ως στρατηγικού μέσου και συνεχίζει με την ανάδειξη τεχνολογιών όπως τα deepfakes, τα αυτοματοποιημένα bots και οι αλγόριθμοι περιεχομένου, που συμβάλλουν στη δημιουργία μιας «ψευδούς πραγματικότητας». Στη συνέχεια, διερευνάται ο ρόλος της αντίληψης ως κρίσιμης μεταβλητής στην ασφάλεια, μέσα από θεωρητικά σχήματα όπως το perception–reaction–decision και μέσα από τις γνωστικές παραμορφώσεις που καθιστούν τους λήπτες αποφάσεων ευάλωτους σε πληροφοριακές πιέσεις. Η εργασία ενσωματώνει τη στρατηγική παραπληροφόρηση στο πλαίσιο των υβριδικών απειλών και εξετάζει χαρακτηριστικές μελέτες περίπτωσης, όπως ο πόλεμος Ρωσίας–Ουκρανίας, οι επιχειρήσεις επιρροής της Κίνας στην Ταϊβάν και οι παρεμβάσεις μέσω AI σε ευρωπαϊκές εκλογικές διαδικασίες. Τέλος, αναλύονται οι προκλήσεις για κράτη και διεθνείς θεσμούς και προτείνονται πολιτικές ανθεκτικότητας, θεσμικού συντονισμού και κοινωνικής προστασίας απέναντι στην ψηφιακή απειλή.

Λέξεις κλειδιά: Τεχνητή νοημοσύνη, στρατηγική παραπληροφόρηση, υβριδικός πόλεμος, στρατηγική λήψη αποφάσεων, ψηφιακή ανθεκτικότητα

Abstract

This dissertation examines how artificial intelligence is reshaping the contemporary strategic environment through the production and dissemination of fabricated information in conditions of digital and hybrid warfare. Special emphasis is placed on AI-enabled strategic disinformation as an instrument of influence that affects not only public perception but also decision-making processes by both state and non-state actors. The analysis begins by outlining the evolution of artificial intelligence as a strategic tool and proceeds to highlight key technologies such as deepfakes, automated bots, and content algorithms, which contribute to the construction of a "false reality" within the information domain. The study then explores perception as a crucial variable in security dynamics, drawing on theoretical models such as the perception–reaction–decision cycle and examining cognitive distortions that increase vulnerability to informational pressure. The dissertation further integrates strategic disinformation into the broader framework of hybrid threats and presents selected case studies, including the Russia–Ukraine war, China's digital influence operations targeting Taiwan, and AI-driven interference in European electoral processes. Finally, it discusses the challenges faced by states and international institutions and proposes resilience-oriented strategies focused on institutional coordination, verification mechanisms, and societal digital literacy.

Keywords: Artificial intelligence, strategic disinformation, hybrid warfare, strategic decision-making, digital resilience

Εισαγωγή

Η τεχνητή νοημοσύνη έχει εξελιχθεί τα τελευταία χρόνια σε καθοριστικό παράγοντα του σύγχρονου στρατηγικού περιβάλλοντος, επηρεάζοντας ουσιαστικά τον τρόπο με τον οποίο παράγεται, διακινείται και αξιολογείται η πληροφορία. Η δυνατότητα δημιουργίας συνθετικού αλλά ιδιαίτερα πειστικού περιεχομένου, όπως αλλοιωμένα οπτικοακουστικά αρχεία, αυτοματοποιημένες αφηγήσεις και στοχευμένες εκστρατείες παραπληροφόρησης, μεταβάλλει τις συνθήκες μέσα στις οποίες λαμβάνονται πολιτικές και στρατηγικές αποφάσεις, ιδίως σε περιόδους αυξημένης έντασης ή σύγκρουσης (Heath, 2019). Στο πλαίσιο του ψηφιακού και υβριδικού πολέμου, η πληροφορία δεν λειτουργεί πλέον αποκλειστικά ως μέσο κατανόησης της πραγματικότητας, αλλά αποκτά χαρακτηριστικά εργαλείου ισχύος. Η στρατηγική παραπληροφόρηση που παράγεται ή ενισχύεται μέσω τεχνητής νοημοσύνης δύναται να αλλοιώσει την αντίληψη της απειλής, να επηρεάσει την εκτίμηση της κατάστασης και να οδηγήσει σε αποφάσεις βασισμένες σε εσφαλμένα ή κατασκευασμένα δεδομένα. Υπό αυτή την έννοια, η παραπληροφόρηση συνιστά πλέον δομικό στοιχείο των σύγχρονων υβριδικών απειλών και όχι απλώς επικοινωνιακή πρακτική (Mallick 2024, 30–70). Η δυναμική αυτή καθιστά την πληροφορία όχι μόνο αντικείμενο ανάλυσης, αλλά και πεδίο στρατηγικού ανταγωνισμού. Η αλλοίωση της πληροφορίας επηρεάζει άμεσα τη συγκρότηση της αντίληψης και, κατ' επέκταση, τη διαδικασία λήψης αποφάσεων, καθώς οι στρατηγικοί δρώντες καλούνται να ενεργήσουν σε περιβάλλοντα αυξημένης αβεβαιότητας και γνωστικής πίεσης. Σε τέτοιες συνθήκες, η διάκριση μεταξύ αξιόπιστης πληροφορίας και κατασκευασμένης πραγματικότητας καθίσταται ολοένα και πιο δυσχερής, με άμεσες επιπτώσεις στη στρατηγική κρίση.

Ιδιαίτερο προβληματισμό εγείρει το ζήτημα της κατεύθυνσης και της προέλευσης των επιχειρήσεων αυτών. Αν και η στρατηγική παραπληροφόρηση έχει ιστορικά συνδεθεί με κρατικές πρακτικές επιρροής προς την κοινωνία, η ευρεία διάδοση εργαλείων τεχνητής νοημοσύνης έχει ενισχύσει τον ρόλο μη κρατικών δρώντων, κοινωνικών δικτύων και αποκεντρωμένων πρωτοβουλιών. Το αποτέλεσμα είναι η διαμόρφωση ενός υβριδικού πεδίου επιρροής, όπου συνυπάρχουν μηχανισμοί «από τα πάνω προς τα κάτω» και δυναμικές «από τη βάση προς το κράτος», οι οποίες μπορούν να επηρεάσουν τόσο τη δημόσια σφαίρα όσο και τους θεσμικούς μηχανισμούς λήψης αποφάσεων (Anagnostakis2023, 425-441). Η παρούσα διατριβή εξετάζει πώς η τεχνητή νοημοσύνη, μέσω μηχανισμών παραπληροφόρησης και ψηφιακής

αλλοίωσης της πληροφορίας, επηρεάζει τη στρατηγική λήψη αποφάσεων σε συνθήκες ψηφιακού πολέμου. Το ενδιαφέρον εστιάζεται στη σχέση μεταξύ αντίληψης, πληροφορίας και απόφασης, καθώς και στον τρόπο με τον οποίο η κατασκευή μιας «ψευδούς πραγματικότητας» μπορεί να διαμορφώσει τη συμπεριφορά κρατικών και μη κρατικών δρώντων σε κρίσιμα στρατηγικά συμφραζόμενα.

Επιπλέον η παρούσα διατριβή καθοδηγείται από μια σειρά ερευνητικών ερωτημάτων, τα οποία αποσκοπούν στη συστηματική διερεύνηση της επίδρασης της τεχνητής νοημοσύνης στη στρατηγική παραπληροφόρηση και, κατ' επέκταση, στη διαδικασία λήψης αποφάσεων σε συνθήκες ψηφιακού και υβριδικού πολέμου. Ειδικότερα, η μελέτη επιχειρεί να απαντήσει στα ακόλουθα επιμέρους ερευνητικά ερωτήματα:

- Ποιες είναι οι βασικές τεχνικές και εφαρμογές της τεχνητής νοημοσύνης στη στρατηγική παραπληροφόρηση;
- Πώς επηρεάζεται η αντίληψη του κινδύνου και της απειλής στους λήπτες αποφάσεων;
- Ποια είναι τα πιο χαρακτηριστικά παραδείγματα παραπληροφόρησης μέσω AI σε διεθνές και εθνικό επίπεδο;
- Πώς ανταποκρίνονται οι θεσμοί ασφάλειας στις σύγχρονες μορφές ψηφιακής παραπληροφόρησης και ποιοι είναι οι βασικοί περιορισμοί τους;
- Ποιες στρατηγικές ή πολιτικές μπορούν να ενισχύσουν τη θεσμική και επιχειρησιακή ανθεκτικότητα;
- Η παραπληροφόρηση μέσω AI λειτουργεί κυρίως ως εργαλείο κρατικής επιρροής («top-down») ή ως φαινόμενο μη κρατικών δρώντων που στοχεύουν το κράτος («bottom-up»);

Στο πλαίσιο αυτό, η εργασία προσεγγίζει αρχικά θεωρητικά τον ρόλο της τεχνητής νοημοσύνης στο σύγχρονο στρατηγικό περιβάλλον και τη σύνδεσή της με την ασφάλεια και τη λήψη αποφάσεων. Στη συνέχεια, αναλύονται οι βασικοί μηχανισμοί παραπληροφόρησης και ψηφιακής αλλοίωσης της πραγματικότητας, καθώς και η επίδρασή τους στην αντίληψη της απειλής και στις γνωστικές διαδικασίες των στρατηγικών δρώντων. Η θεωρητική ανάλυση συμπληρώνεται από την εξέταση επιλεγμένων περιπτώσεων ψηφιακής παραπληροφόρησης σε διεθνές επίπεδο, μέσα από τις οποίες αναδεικνύεται ο τρόπος λειτουργίας των επιχειρήσεων

επιρροής σε διαφορετικά γεωπολιτικά συμφραζόμενα. Τέλος, η διατριβή καταλήγει σε συμπεράσματα και προτάσεις που αφορούν την ενίσχυση της θεσμικής και στρατηγικής ανθεκτικότητας απέναντι στις σύγχρονες ψηφιακές απειλές.

Η τεχνητή νοημοσύνη δεν αποτελεί απλώς ένα νέο τεχνολογικό μέσο στο πεδίο της ασφάλειας, αλλά έναν παράγοντα που επηρεάζει ουσιαστικά τον τρόπο με τον οποίο διαμορφώνεται η αντίληψη, η στρατηγική κρίση και η διαδικασία λήψης αποφάσεων. Η στρατηγική παραπληροφόρηση μέσω AI αναδεικνύεται ως πολυδιάστατο φαινόμενο, το οποίο δεν περιορίζεται αποκλειστικά σε κρατικές πρακτικές επιρροής, αλλά διαχέεται σε ένα ευρύτερο οικοσύστημα δρώντων και αφηγημάτων. Τα ευρήματα της διατριβής υποδεικνύουν την ανάγκη ενίσχυσης της θεσμικής ανθεκτικότητας και της κριτικής διαχείρισης της πληροφορίας, προκειμένου η λήψη αποφάσεων σε συνθήκες ψηφιακής έντασης να παραμένει σταθερή και ορθολογική.

Κεφάλαιο 1ο Εννοιολογικό και θεωρητικό πλαίσιο

1.1 Τεχνητή Νοημοσύνη (AI)

Η έννοια της Τεχνητής Νοημοσύνης (ArtificialIntelligence – AI) χρησιμοποιείται συχνά με τρόπο γενικευμένο και ασαφή, γεγονός που καθιστά αναγκαία τη σαφή εννοιολογική της οριοθέτηση, ιδίως όταν εντάσσεται στο πεδίο των στρατηγικών και των σπουδών ασφάλειας. Στο πλαίσιο της παρούσας διατριβής, η τεχνητή νοημοσύνη δεν προσεγγίζεται ως τεχνικό ή υπολογιστικό επίτευγμα καθαυτό, αλλά ως σύνολο συστημάτων ικανών να επεξεργάζονται πληροφορία, να εξάγουν συμπεράσματα και να επηρεάζουν διαδικασίες κρίσης και απόφασης σε περιβάλλοντα αβεβαιότητας (Jaboobetal. 2024, 3–22). Λειτουργικά, η AI ορίζεται ως η ικανότητα τεχνητών συστημάτων να εκτελούν γνωστικές λειτουργίες που προσομοιάζουν ανθρώπινες διαδικασίες, όπως η αναγνώριση προτύπων, η αξιολόγηση εναλλακτικών σεναρίων και η προσαρμογή σε μεταβαλλόμενα δεδομένα. Για τις στρατηγικές σπουδές, η σημασία της τεχνητής νοημοσύνης δεν έγκειται στην ακρίβεια των αλγορίθμων, αλλά στον τρόπο με τον οποίο τα παραγόμενα αποτελέσματα εντάσσονται στη διαδικασία λήψης αποφάσεων και επηρεάζουν την αντίληψη της απειλής, της ισχύος και του κινδύνου (Erskine and Miller 2024, 135–147).

Ιδιαίτερη σημασία έχει η διάκριση μεταξύ τεχνητής νοημοσύνης και απλής αυτοματοποίησης. Τα αυτοματοποιημένα συστήματα λειτουργούν βάσει προκαθορισμένων

κανόνων και προβλέψιμων ακολουθιών ενεργειών, χωρίς να διαθέτουν ικανότητα προσαρμογής ή ερμηνείας νέων δεδομένων. Αντιθέτως, τα συστήματα τεχνητής νοημοσύνης χαρακτηρίζονται από τη δυνατότητα μάθησης και δυναμικής αναπροσαρμογής, στοιχείο που τους επιτρέπει να λειτουργούν σε σύνθετα και αβέβαια περιβάλλοντα. Η διάκριση αυτή είναι κρίσιμη, καθώς η στρατηγική σημασία της AI προκύπτει ακριβώς από αυτή τη σχετική αυτονομία στην επεξεργασία της πληροφορίας (Csaszar, Ketkar, and Kim 2024, 322-345).

Στο πεδίο της ασφάλειας και της στρατηγικής, η τεχνητή νοημοσύνη δεν αντικαθιστά τον άνθρωπο που αποφασίζει, αλλά παρεμβάλλεται μεταξύ πληροφορίας και απόφασης, επηρεάζοντας τον τρόπο με τον οποίο η πραγματικότητα αναπαρίσταται και ερμηνεύεται. Η παρέμβαση αυτή μπορεί να ενισχύσει την αναλυτική ικανότητα των δρώντων, αλλά ταυτόχρονα ενδέχεται να εισαγάγει νέες μορφές γνωστικής εξάρτησης και στρατηγικού ρίσκου, ιδίως όταν τα αλγοριθμικά αποτελέσματα αντιμετωπίζονται ως ουδέτερα ή αντικειμενικά.

1.2 Πληροφορία, παραπληροφόρηση και στρατηγική επιρροή

Η πληροφορία αποτελεί διαχρονικά βασικό στοιχείο της ισχύος στις διεθνείς σχέσεις και στη στρατηγική σκέψη. Η δυνατότητα συλλογής, ελέγχου και αξιοποίησής της επηρεάζει άμεσα την ικανότητα των δρώντων να αντιλαμβάνονται το περιβάλλον τους, να εκτιμούν απειλές και να διαμορφώνουν αποτελεσματικές στρατηγικές επιλογές. Στο πλαίσιο αυτό, η πληροφορία δεν λειτουργεί απλώς ως ουδέτερη αντανάκλαση της πραγματικότητας, αλλά ως μέσο που μπορεί να ενισχύσει ή να περιορίσει την ισχύ ενός δρώντα, ανάλογα με τον τρόπο χρήσης της. Στη σύγχρονη στρατηγική ανάλυση, η πληροφορία συνδέεται στενά με την έννοια της επιρροής, καθώς η ικανότητα διαμόρφωσης αφηγημάτων, πλαισίων ερμηνείας και συλλογικών αντιλήψεων καθίσταται εξίσου σημαντική με την κατοχή υλικών μέσων ισχύος. Η επιρροή, ως μορφή ισχύος, δεν προϋποθέτει απαραίτητα εξαναγκασμό ή άμεση βία, αλλά βασίζεται στην πειθώ, στη νομιμοποίηση και στη διαμόρφωση της αντίληψης των άλλων δρώντων. Υπό αυτή την έννοια, η πληροφορία λειτουργεί ως στρατηγικός πόρος που επιτρέπει την έμμεση άσκηση ισχύος (Nye 2020, 143–145).

Η παραπληροφόρηση συνιστά ειδική και ιδιαίτερα αποτελεσματική μορφή αξιοποίησης της πληροφορίας για στρατηγικούς σκοπούς. Δεν περιορίζεται στη διάδοση ψευδών ειδήσεων, αλλά περιλαμβάνει ένα ευρύτερο φάσμα πρακτικών που στοχεύουν στη σύγχυση, στην αποδόμηση της εμπιστοσύνης και στην αλλοίωση της αντίληψης της πραγματικότητας. Μέσω της επιλεκτικής παρουσίασης γεγονότων, της αποσπασματικής πληροφόρησης ή της

κατασκευής πειστικών αφηγημάτων, η παραπληροφόρηση μπορεί να επηρεάσει τόσο την κοινή γνώμη όσο και τους θεσμικούς μηχανισμούς λήψης αποφάσεων. Σε στρατηγικό επίπεδο, λειτουργεί ως εργαλείο που επιτρέπει την επίτευξη στόχων χωρίς άμεση αντιπαράθεση, επιδιώκοντας τη μεταβολή της συμπεριφοράς του αντιπάλου μέσω της αλλοίωσης της αντίληψής του. Η στρατηγική της αξία έγκειται ακριβώς στην έμμεση φύση της, καθώς επιτρέπει την άσκηση πίεσης και την πρόκληση αποσταθεροποίησης χωρίς το κόστος που συνεπάγεται η χρήση σκληρών μέσων ισχύος (Bennett and Livingston 2018, 122–139). Η σύνδεση της παραπληροφόρησης με τη στρατηγική επιρροή καθίσταται ιδιαίτερα έντονη σε περιβάλλοντα υψηλής αβεβαιότητας και πολιτικής έντασης, όπου η δυσκολία επαλήθευσης της πληροφορίας και η πίεση του χρόνου ενισχύουν την αποτελεσματικότητα των επιχειρήσεων επιρροής. Σε τέτοιες συνθήκες, η παραπληροφόρηση μπορεί να εντείνει υφιστάμενες κοινωνικές ή πολιτικές διαιρέσεις, να υπονομεύσει την εμπιστοσύνη στους θεσμούς και να περιορίσει την ικανότητα συλλογικής αντίδρασης (Chesney and Citron 2019, 147–155; Hartmann and Giles 2020, 233–250).

1.3 Ψηφιακός και υβριδικός πόλεμος

Ο όρος «ψηφιακός πόλεμος» χρησιμοποιείται συχνά για να περιγράψει συγκρούσεις που εκτυλίσσονται στον κυβερνοχώρο, όπως επιθέσεις σε δίκτυα, πληροφοριακά συστήματα ή κρίσιμες υποδομές. Παρότι οι πρακτικές αυτές αποτελούν αναπόσπαστο μέρος των σύγχρονων συγκρούσεων, η ταύτιση του ψηφιακού πολέμου με τον κυβερνοπόλεμο είναι εννοιολογικά περιοριστική και ανεπαρκής. Ο ψηφιακός πόλεμος δεν αφορά μόνο την τεχνική διάσταση της σύγκρουσης, αλλά περιλαμβάνει το σύνολο των ενεργειών που αξιοποιούν τον ψηφιακό χώρο για την άσκηση επιρροής, την αποσταθεροποίηση και τη διαμόρφωση στρατηγικών αποτελεσμάτων (Hoffman 2018, 30–47). Σε αυτό το ευρύτερο πλαίσιο, ο ψηφιακός πόλεμος συνδέεται άμεσα με την έννοια του υβριδικού πολέμου. Ο υβριδικός πόλεμος χαρακτηρίζεται από τον συνδυασμό συμβατικών και μη συμβατικών μέσων, στρατιωτικών και μη στρατιωτικών πρακτικών, με στόχο την επίτευξη πολιτικών και στρατηγικών σκοπών χωρίς την κήρυξη ανοιχτής σύγκρουσης. Η ψηφιακή διάσταση λειτουργεί ως καταλύτης αυτής της στρατηγικής, επιτρέποντας την ταυτόχρονη δράση σε πολλαπλά επίπεδα: πληροφοριακό, γνωστικό, πολιτικό και κοινωνικό (Rid 2020, 112–114).

Η κρίσιμη διαφορά μεταξύ κυβερνοπολέμου και ψηφιακού ή υβριδικού πολέμου έγκειται στο αντικείμενο της επίθεσης. Ενώ ο κυβερνοπόλεμος στοχεύει κυρίως τεχνικές

υποδομές και συστήματα, ο ψηφιακός και υβριδικός πόλεμος εστιάζει στην αντίληψη, στη συμπεριφορά και στη συνοχή των κοινωνιών και των θεσμών. Η πληροφορία και η παραπληροφόρηση, η διαχείριση αφηγημάτων και η χειραγώγηση της δημόσιας σφαίρας αποτελούν βασικά εργαλεία αυτής της μορφής σύγκρουσης (Kello 2017, 84–86). Ιδιαίτερη σημασία έχει το γεγονός ότι ο ψηφιακός και υβριδικός πόλεμος λειτουργεί συχνά κάτω από το κατώφλι της ένοπλης σύγκρουσης. Οι ενέργειες που τον συγκροτούν είναι σχεδιασμένες ώστε να παραμένουν αμφίσημες, δυσδιάκριτες και δύσκολα αποδοτέες σε συγκεκριμένους δρώντες. Η αμφισημία αυτή περιορίζει τη δυνατότητα άμεσης αντίδρασης και αποτροπής, ενώ ταυτόχρονα επιτρέπει τη σταδιακή φθορά της εμπιστοσύνης στους θεσμούς και της κοινωνικής συνοχής (Libicki 2016, 47–49).

Στο πλαίσιο αυτό, η ψηφιακή τεχνολογία, και ιδίως τα εργαλεία ανάλυσης και παραγωγής πληροφορίας, αποκτούν στρατηγική σημασία. Η σύγκρουση δεν εκτυλίσσεται μόνο στο πεδίο της μάχης ή στον κυβερνοχώρο, αλλά και στο επίπεδο της αντίληψης και της ερμηνείας της πραγματικότητας. Ο ψηφιακός και υβριδικός πόλεμος επιδιώκει να επηρεάσει το πώς οι δρώντες αντιλαμβάνονται την κατάσταση, ποιες απειλές θεωρούν κρίσιμες και ποιες επιλογές θεωρούν αποδεκτές.

1.4 Αντίληψη και λήψη αποφάσεων στην ασφάλεια

Η λήψη αποφάσεων στον τομέα της ασφάλειας δεν αποτελεί μια καθαρά τεχνική ή ορθολογική διαδικασία, αλλά διαμορφώνεται σε μεγάλο βαθμό από τον τρόπο με τον οποίο οι δρώντες αντιλαμβάνονται την πραγματικότητα και τις απειλές που αντιμετωπίζουν. Οι στρατηγικές επιλογές δεν βασίζονται αποκλειστικά σε αντικειμενικά δεδομένα, αλλά σε ερμηνείες, προσδοκίες και εκτιμήσεις, οι οποίες συχνά επηρεάζονται από περιορισμούς πληροφόρησης, γνωστικές προκαταλήψεις και θεσμικά φίλτρα. (Klasche and Selg 2020, 544–564). Στο πλαίσιο αυτό, η συμβολή του Robert Jervis υπήρξε καθοριστική, καθώς ανέδειξε ότι οι αποφάσεις στην εξωτερική πολιτική και την ασφάλεια διαμορφώνονται μέσα από την αντίληψη των δρώντων και όχι απαραιτήτως μέσα από την αντικειμενική πραγματικότητα. Οι ηγεσίες και οι θεσμοί τείνουν να ερμηνεύουν τις πληροφορίες βάσει υφιστάμενων προσδοκιών και προϋπαρχόντων αντιλήψεων, γεγονός που μπορεί να οδηγήσει σε σφάλματα εκτίμησης και σε στρατηγικές επιλογές με απρόβλεπτες συνέπειες (Jervis 2020, 47–81).

Η αντίληψη λειτουργεί, επομένως, ως ενδιάμεσος μηχανισμός μεταξύ πληροφορίας και απόφασης. Η πληροφορία δεν μεταφράζεται αυτόματα σε γνώση, αλλά φιλτράρεται και

αποκωδικοποιείται μέσα από γνωστικά και οργανωτικά πλαίσια. Σε περιβάλλοντα υψηλής αβεβαιότητας, όπως εκείνα που χαρακτηρίζουν τις κρίσεις και τις συγκρούσεις, η διαδικασία αυτή καθίσταται ακόμη πιο ευάλωτη σε παραμορφώσεις, καθώς η πίεση του χρόνου και ο φόρτος πληροφορίας περιορίζουν την ικανότητα επαλήθευσης και αναστοχασμού (Johnson 2019, 147–169). Η σημασία της αντίληψης για τη στρατηγική ασφάλεια εντείνεται στο σύγχρονο ψηφιακό περιβάλλον. Η πληθώρα πληροφοριών και η ταχύτητα διάδοσής τους αυξάνουν τον κίνδυνο σύγχυσης και επιλεκτικής ερμηνείας. Η λήψη αποφάσεων επηρεάζεται όχι μόνο από το περιεχόμενο της πληροφορίας, αλλά και από τον τρόπο παρουσίασής της, τη συχνότητα επανάληψης και το πλαίσιο μέσα στο οποίο εντάσσεται. Οι παράγοντες αυτοί μπορούν να ενισχύσουν υφιστάμενες αντιλήψεις ή να δημιουργήσουν ψευδή αίσθηση βεβαιότητας(Paul and Matthews 2016, 2–4).

Στο πεδίο της ασφάλειας, οι επιπτώσεις των γνωστικών στρεβλώσεων είναι ιδιαίτερα κρίσιμες, καθώς οι αποφάσεις αφορούν ζητήματα υψηλού ρίσκου και δυνητικά μη αναστρέψιμων συνεπειών. Η εσφαλμένη αντίληψη της απειλής μπορεί να οδηγήσει είτε σε υπερβολική αντίδραση είτε σε επικίνδυνη υποεκτίμηση κινδύνων. Η στρατηγική σταθερότητα εξαρτάται, συνεπώς, όχι μόνο από την ισορροπία ισχύος, αλλά και από την ακρίβεια με την οποία οι δρώντες αντιλαμβάνονται τις προθέσεις και τις δυνατότητες των άλλων.

1.5 Σύνοψη Κεφαλαίου

Το παρόν κεφάλαιο ανέδειξε την τεχνητή νοημοσύνη ως δομικό παράγοντα του σύγχρονου στρατηγικού περιβάλλοντος, εξετάζοντας τόσο την εξέλιξή της όσο και τη μετατόπιση του ρόλου της από τεχνολογικό εργαλείο σε μέσο στρατηγικής επιρροής. Η ανάλυση κατέδειξε ότι η αξία της AI δεν περιορίζεται στις τεχνικές της δυνατότητες, αλλά συνδέεται άμεσα με τον τρόπο επεξεργασίας της πληροφορίας και τη διαμόρφωση της αντίληψης. Παράλληλα, αναδείχθηκε η αλληλεξάρτηση μεταξύ τεχνητής νοημοσύνης, λήψης αποφάσεων και ασφάλειας, υπογραμμίζοντας ότι οι αλγοριθμικές εφαρμογές επηρεάζουν το πλαίσιο εντός του οποίου διαμορφώνονται στρατηγικές επιλογές. Το κεφάλαιο αυτό θέτει έτσι το απαραίτητο θεωρητικό υπόβαθρο για την ανάλυση της παραπληροφόρησης και της ψηφιακής αλλοίωσης της πραγματικότητας που ακολουθεί.

Κεφάλαιο 2ο Η Τεχνητή Νοημοσύνη στο Στρατηγικό Περιβάλλον

2.1 Εξέλιξη της AI στον 21ο αιώνα

Η Τεχνητή Νοημοσύνη (ArtificialIntelligence – AI) αποτελεί έναν από τους πλέον σύνθετους και δυναμικά εξελισσόμενους τομείς της σύγχρονης τεχνολογίας, με άμεσες και έμμεσες επιπτώσεις στο στρατηγικό, πολιτικό και ασφαλείας περιβάλλον. Σε γενικές γραμμές, ο όρος αναφέρεται στην ικανότητα τεχνητών συστημάτων να εκτελούν λειτουργίες που παραδοσιακά συνδέονται με την ανθρώπινη νοημοσύνη, όπως η μάθηση, η ανάλυση δεδομένων, η αναγνώριση προτύπων, η λήψη αποφάσεων και η παραγωγή λόγου ή εικόνας. Ωστόσο, ο ορισμός της AI δεν είναι ενιαίος ούτε στατικός, καθώς μεταβάλλεται ανάλογα με τις τεχνολογικές δυνατότητες και τα πεδία εφαρμογής της (Jiangetal. 2022, 4).

Κατά τον 21ο αιώνα, η τεχνητή νοημοσύνη απομακρύνεται από τα πρώιμα θεωρητικά και πειραματικά της στάδια και μετατρέπεται σε λειτουργικό και ευρέως διαδεδομένο εργαλείο. Η εξέλιξη αυτή συνδέεται άμεσα με τρεις βασικούς παράγοντες. Τη ραγδαία αύξηση της υπολογιστικής ισχύος, τη διαθεσιμότητα τεράστιων όγκων δεδομένων (bigdata) και την ανάπτυξη προηγμένων αλγοριθμικών μεθόδων, ιδίως στον τομέα της μηχανικής μάθησης (machinelearning) και της βαθιάς μάθησης (deeplearning). Οι τεχνολογίες αυτές επιτρέπουν στα συστήματα AI να μην περιορίζονται στην εκτέλεση προκαθορισμένων εντολών, αλλά να προσαρμόζονται δυναμικά στο περιβάλλον τους, αναθεωρώντας τις λειτουργίες τους βάσει νέων πληροφοριών (Rasheedetal. 2024, 15–46). Στο πλαίσιο αυτό, η AI του 21ου αιώνα διαφοροποιείται ουσιωδώς από προηγούμενες μορφές αυτοματοποίησης. Ενώ τα παλαιότερα υπολογιστικά συστήματα λειτουργούσαν βάσει αυστηρά καθορισμένων κανόνων, τα σύγχρονα συστήματα τεχνητής νοημοσύνης χαρακτηρίζονται από σχετική αυτονομία στη διαδικασία επεξεργασίας και ερμηνείας της πληροφορίας. Η δυνατότητα αυτή καθιστά την AI ιδιαίτερα ελκυστική για εφαρμογές που αφορούν πολύπλοκα και αβέβαια περιβάλλοντα, όπως αυτά της ασφάλειας, της άμυνας και της στρατηγικής ανάλυσης(Muthukrishnanetal. 2020, 393–399).

Παράλληλα, η εξέλιξη της τεχνητής νοημοσύνης συνοδεύεται από τη διεύρυνση των πεδίων χρήσης της πέρα από τον τεχνικό ή επιστημονικό χώρο. Στον 21ο αιώνα, η AI ενσωματώνεται στη δημόσια σφαίρα, στα μέσα ενημέρωσης, στα κοινωνικά δίκτυα και στους μηχανισμούς πολιτικής επικοινωνίας. Ιδιαίτερη σημασία αποκτά η ικανότητά της να παράγει και να διαχειρίζεται πληροφορία σε μαζική κλίμακα, επηρεάζοντας τον τρόπο με τον οποίο διαμορφώνονται αφηγήσεις, αντιλήψεις και συλλογικές στάσεις. Η μετάβαση αυτή

σηματοδοτεί μια ποιοτική αλλαγή: η τεχνητή νοημοσύνη δεν λειτουργεί πλέον μόνο ως εργαλείο υποστήριξης αποφάσεων, αλλά ως ενεργός παράγοντας διαμόρφωσης του πληροφοριακού περιβάλλοντος (Haenlein and Kaplan 2019, 5–14). Η στρατηγική σημασία της AI ενισχύεται περαιτέρω από το γεγονός ότι οι εφαρμογές της δεν περιορίζονται σε κρατικούς φορείς. Η διάχυση της τεχνολογίας σε ιδιωτικές εταιρείες, οργανώσεις και μεμονωμένους χρήστες δημιουργεί ένα πολυεπίπεδο και αποκεντρωμένο οικοσύστημα, στο οποίο η ισχύς δεν απορρέει αποκλειστικά από την κατοχή υλικών μέσων, αλλά από την ικανότητα επεξεργασίας και χειραγώγησης της πληροφορίας. Στο νέο αυτό περιβάλλον, η τεχνητή νοημοσύνη λειτουργεί ως επιταχυντής στρατηγικών δυναμικών, επιτρέποντας ταχεία προσαρμογή, στοχευμένη επιρροή και εκμετάλλευση γνωστικών αδυναμιών (Toosietal. 2021, 449–469).

2.2 Η Τεχνητή Νοημοσύνη ως στρατηγικό εργαλείο

Η αρχική ανάπτυξη της τεχνητής νοημοσύνης συνδέθηκε κυρίως με τεχνικά ζητήματα υπολογιστικής απόδοσης και αυτοματοποίησης διαδικασιών. Στο πλαίσιο αυτό, η AI αντιμετωπιζόταν ως εργαλείο υποστήριξης της ανθρώπινης εργασίας, με περιορισμένη επίδραση πέρα από τον λειτουργικό και τεχνοκρατικό της ρόλο. Ωστόσο, κατά τον 21ο αιώνα, η σταδιακή ενσωμάτωσή της σε τομείς που άπτονται της πληροφορίας, της επικοινωνίας και της ανάλυσης δεδομένων οδήγησε σε μια ουσιαστική μετατόπιση: η τεχνητή νοημοσύνη παύει να αποτελεί απλώς τεχνολογικό μέσο και μετατρέπεται σε εργαλείο επιρροής με σαφές στρατηγικό αποτύπωμα (Puttaraju 2023, 2242–2247). Η μετάβαση αυτή οφείλεται πρωτίστως στην ικανότητα της AI να επεξεργάζεται, να αναλύει και να αναδιαμορφώνει πληροφορία σε μεγάλη κλίμακα και με ταχύτητα που υπερβαίνει τις ανθρώπινες δυνατότητες. Η δυνατότητα αυτή δεν αφορά μόνο τη συλλογή δεδομένων, αλλά κυρίως τη διαμόρφωση αφηγημάτων, την πρόβλεψη συμπεριφορών και τη στοχευμένη προσαρμογή μηνυμάτων σε συγκεκριμένα ακροατήρια. Στο στρατηγικό περιβάλλον, όπου η αντίληψη της πραγματικότητας συχνά καθορίζει την αντίδραση των δρώντων, η AI αποκτά ιδιαίτερη σημασία ως μηχανισμός επηρεασμού της κρίσης και της απόφασης (Jafarietal. 2025, 258–276).

Σε αντίθεση με τις παραδοσιακές μορφές πληροφοριακής ισχύος, η τεχνητή νοημοσύνη επιτρέπει την εξατομίκευση της επιρροής. Μέσω αλγοριθμικών συστημάτων, η πληροφορία δεν διαχέεται πλέον ομοιόμορφα, αλλά προσαρμόζεται δυναμικά στις γνωστικές προδιαθέσεις, τις κοινωνικές ταυτότητες και τα συναισθηματικά χαρακτηριστικά των αποδεκτών της. Η εξέλιξη αυτή ενισχύει την αποτελεσματικότητα των επιχειρήσεων επιρροής, καθιστώντας δυσδιάκριτα

τα όρια μεταξύ πληροφόρησης, πειθούς και χειραγώγησης (Selvarajan 2023, 2121–2132). Η στρατηγική αξία της AI εντείνεται περαιτέρω από τη δυνατότητά της να λειτουργεί σε περιβάλλοντα αβεβαιότητας και πολυπλοκότητας. Σε καταστάσεις κρίσης, όπου ο χρόνος είναι περιορισμένος και οι πληροφορίες συχνά αντιφατικές, τα συστήματα τεχνητής νοημοσύνης μπορούν να επηρεάσουν καθοριστικά την εκτίμηση της κατάστασης, είτε υποστηρίζοντας τη λήψη αποφάσεων είτε, αντιθέτως, ενισχύοντας τη σύγχυση και την αβεβαιότητα. Η διττή αυτή λειτουργία καθιστά την AI στρατηγικό εργαλείο με δυνητικά αποσταθεροποιητικές συνέπειες (Serwar 2024, 77–85). Παράλληλα, η χρήση της τεχνητής νοημοσύνης ως εργαλείου επιρροής δεν περιορίζεται αποκλειστικά στα κράτη. Η διάδοση σχετικών τεχνολογιών σε μη κρατικούς δρώντες, ιδιωτικούς οργανισμούς και άτυπα δίκτυα δημιουργεί ένα αποκεντρωμένο πεδίο στρατηγικής δράσης, στο οποίο η ισχύς δεν απορρέει από την κατοχή υλικών μέσων, αλλά από την ικανότητα διαχείρισης της πληροφορίας και της αντίληψης. Το γεγονός αυτό μεταβάλλει τις παραδοσιακές αντιλήψεις περί στρατηγικού ανταγωνισμού και καθιστά δυσκολότερη την ανίχνευση, την απόδοση ευθύνης και την αποτροπή(Ashritha and Reddy 2023, 10–18).

2.3 Η σχέση Τεχνητής Νοημοσύνης, λήψης αποφάσεων και ασφάλειας

Η λήψη στρατηγικών αποφάσεων στον τομέα της ασφάλειας βασίζεται διαχρονικά στην ικανότητα των δρώντων να συλλέγουν, να αξιολογούν και να ερμηνεύουν πληροφορίες σε περιβάλλοντα αβεβαιότητας. Η είσοδος της τεχνητής νοημοσύνης στη διαδικασία αυτή δεν μεταβάλλει απλώς τα τεχνικά μέσα της ανάλυσης, αλλά επηρεάζει βαθύτερα τον τρόπο με τον οποίο διαμορφώνεται η ίδια η κρίση και η αντίληψη της απειλής. Η σχέση μεταξύ AI, απόφασης και ασφάλειας είναι συνεπώς πολυεπίπεδη και δεν μπορεί να περιοριστεί σε έναν γραμμικό μηχανισμό υποστήριξης (Keding 2021, 91–134). Στον 21ο αιώνα, τα συστήματα τεχνητής νοημοσύνης χρησιμοποιούνται όλο και περισσότερο για την επεξεργασία μεγάλων όγκων δεδομένων, την πρόβλεψη εξελίξεων και την αξιολόγηση πιθανών σεναρίων. Η συμβολή τους στη διαδικασία λήψης αποφάσεων είναι ιδιαίτερα εμφανής σε τομείς όπου ο χρόνος αντίδρασης είναι κρίσιμος και η πληροφόρηση κατακερματισμένη. Ωστόσο, η αυξανόμενη εξάρτηση από αλγοριθμικά συστήματα δημιουργεί νέες μορφές ευαλωτότητας, καθώς η απόφαση αρχίζει να βασίζεται όχι μόνο στην ανθρώπινη κρίση, αλλά και σε υποθέσεις, μοντέλα και δεδομένα των οποίων η εγκυρότητα δεν είναι πάντοτε διαφανής (Dear 2019, 18–25).

Η έννοια της ασφάλειας, όπως έχει αναδειχθεί στη θεωρία των διεθνών σχέσεων, δεν περιορίζεται σε αντικειμενικές απειλές, αλλά συνδέεται άμεσα με την αντίληψή τους. Η τεχνητή

νοημοσύνη παρεμβαίνει σε αυτό το επίπεδο, επηρεάζοντας τον τρόπο με τον οποίο οι δρώντες αντιλαμβάνονται κινδύνους και ευκαιρίες. Μέσω της επιλογής, της ιεράρχησης και της παρουσίασης της πληροφορίας, τα συστήματα AI μπορούν να ενισχύσουν συγκεκριμένες εκτιμήσεις εις βάρος άλλων, διαμορφώνοντας ένα πλαίσιο εντός του οποίου η απόφαση εμφανίζεται ως «ορθολογική», ακόμη και όταν βασίζεται σε μερικά ή παραπλανητικά δεδομένα (Radulov 2019, 3–5). Η σύνδεση της τεχνητής νοημοσύνης με τη στρατηγική ασφάλεια γίνεται ιδιαίτερα προβληματική σε συνθήκες κρίσης ή σύγκρουσης. Σε τέτοιες καταστάσεις, η πίεση του χρόνου, η ασάφεια της πληροφορίας και η πολιτική ή στρατιωτική ένταση περιορίζουν τα περιθώρια ελέγχου και επαλήθευσης. Η χρήση αλγοριθμικών εργαλείων μπορεί να επιταχύνει τη διαδικασία λήψης αποφάσεων, αλλά ταυτόχρονα ενδέχεται να μειώσει τον χώρο για κριτική σκέψη και αναστοχασμό, αυξάνοντας τον κίνδυνο σφαλμάτων ή υπερβολικών αντιδράσεων (Dear 2019, 18–25).Παράλληλα, η ενσωμάτωση της τεχνητής νοημοσύνης στη διαδικασία ασφάλειας μεταβάλλει τη σχέση μεταξύ κρατικών και μη κρατικών δρώντων. Η πρόσβαση σε εργαλεία ανάλυσης, πρόβλεψης και επιρροής δεν αποτελεί πλέον αποκλειστικό προνόμιο των κρατών, γεγονός που περιπλέκει το στρατηγικό περιβάλλον και καθιστά δυσκολότερη τη διάκριση μεταξύ εσωτερικών και εξωτερικών απειλών. Η απόφαση, σε αυτό το πλαίσιο, δεν αφορά μόνο την επιλογή στρατηγικής δράσης, αλλά και την ερμηνεία της ίδιας της πραγματικότητας μέσα στην οποία λαμβάνεται (HorowitzandLin-Greenberg, 2022).

2.4 Σύνοψη Κεφαλαίου

Το δεύτερο κεφάλαιο ανέλυσε τη στρατηγική παραπληροφόρηση ως βασική συνιστώσα του σύγχρονου ψηφιακού περιβάλλοντος, με έμφαση στον ρόλο της τεχνητής νοημοσύνης στην παραγωγή και διάδοση παραπλανητικού περιεχομένου. Εξετάστηκαν οι βασικές τεχνολογίες και πρακτικές που συμβάλλουν στη δημιουργία ψευδών ή αλλοιωμένων αναπαραστάσεων της πραγματικότητας, καθώς και οι επιπτώσεις τους στη διαμόρφωση της αντίληψης. Η ανάλυση ανέδειξε ότι η παραπληροφόρηση δεν λειτουργεί αποσπασματικά, αλλά εντάσσεται σε ευρύτερα πλαίσια πληροφοριακής ισχύος και ψυχολογικής πίεσης. Το κεφάλαιο αυτό θέτει τις βάσεις για την κατανόηση της αντίληψης ως στρατηγικής μεταβλητής, η οποία εξετάζεται αναλυτικότερα στο επόμενο κεφάλαιο.

Κεφάλαιο 3ο Η Αντίληψη ως Στρατηγική Μεταβλητή

3.1. Θεωρία Perception–Reaction–Decision

Η αντίληψη αποτελεί έναν από τους πιο κρίσιμους αλλά συχνά υποτιμημένους παράγοντες στη στρατηγική ανάλυση. Σε περιβάλλοντα ασφάλειας, όπου οι αποφάσεις λαμβάνονται υπό συνθήκες αβεβαιότητας, η πραγματικότητα δεν γίνεται αντιληπτή άμεσα και αντικειμενικά, αλλά μέσα από ερμηνευτικά φίλτρα, γνωστικά σχήματα και προσδοκίες. Η θεωρία Perception–Reaction–Decision προσφέρει ένα χρήσιμο πλαίσιο για την κατανόηση του τρόπου με τον οποίο οι στρατηγικοί δρώντες μεταβαίνουν από την πρόσληψη πληροφοριών στην επιλογή δράσης, αναδεικνύοντας ότι η απόφαση δεν προκύπτει ως αυτόματη αντίδραση στα γεγονότα, αλλά ως αποτέλεσμα μιας διαμεσολαβούμενης διαδικασίας αντίληψης και ερμηνείας (Andradeetal. 2022).

Στην καρδιά της θεωρίας βρίσκεται η παραδοχή ότι η αντίληψη προηγείται της αντίδρασης και καθορίζει το είδος της απόφασης που τελικά λαμβάνεται. Οι δρώντες δεν ανταποκρίνονται σε μια «αντικειμενική» πραγματικότητα, αλλά σε εκείνη την εκδοχή της πραγματικότητας που έχουν σχηματίσει μέσα από τις πληροφορίες που διαθέτουν και τους τρόπους με τους οποίους τις κατανοούν. Η στρατηγική συμπεριφορά, επομένως, δεν εξαρτάται μόνο από υλικούς συσχετισμούς ισχύος, αλλά και από το πώς οι απειλές και οι προθέσεις του αντιπάλου γίνονται αντιληπτές (Casino 2025).Το στάδιο της αντίληψης περιλαμβάνει τη συλλογή και την αρχική επεξεργασία πληροφοριών. Ωστόσο, ακόμη και σε αυτό το πρώτο επίπεδο, η πληροφόρηση δεν είναι ποτέ πλήρης ούτε ουδέτερη. Οι στρατηγικοί δρώντες επιλέγουν τι θα θεωρήσουν σημαντικό, τι θα αγνοήσουν και πώς θα εντάξουν νέα δεδομένα σε ήδη υπάρχοντα ερμηνευτικά πλαίσια. Η επιλογή αυτή δεν γίνεται μόνο συνειδητά, αλλά επηρεάζεται από θεσμικές ρουτίνες, πολιτικές προτεραιότητες και γνωστικές προκαταλήψεις. Έτσι, η αντίληψη διαμορφώνει το πεδίο των πιθανών επιλογών πριν ακόμη ξεκινήσει η διαδικασία λήψης απόφασης (Grahn and Taipalus 2025, 41–43).

Ακολουθεί το στάδιο της αντίδρασης, το οποίο δεν ταυτίζεται με άμεση δράση, αλλά με τη διαμόρφωση στρατηγικής στάσης απέναντι σε ένα ερέθισμα. Η αντίδραση αποτελεί το μεταβατικό επίπεδο όπου ο δρών προσπαθεί να αποδώσει νόημα στην πληροφορία: να αξιολογήσει αν πρόκειται για απειλή, για πρόκληση, για παραπλάνηση ή για ευκαιρία. Σε αυτό το σημείο, η αντίληψη επηρεάζει καθοριστικά τη φύση της στρατηγικής ανταπόκρισης. Δύο δρώντες μπορεί να αντιμετωπίζουν το ίδιο γεγονός, αλλά να αντιδρούν με εντελώς διαφορετικό

τρόπο, επειδή το ερμηνεύουν διαφορετικά (Doherty 2023).

Το τρίτο στάδιο, αυτό της απόφασης, συνιστά το αποτέλεσμα της διαδικασίας. Η απόφαση εμφανίζεται συχνά ως προϊόν ορθολογικής στάθμισης, στην πράξη όμως αποτελεί επιλογή εντός ενός περιορισμένου πλαισίου, το οποίο έχει ήδη διαμορφωθεί από την αντίληψη και την αντίδραση. Οι στρατηγικές αποφάσεις δεν λαμβάνονται σε κενό, αλλά μέσα σε περιβάλλοντα πίεσης, ατελούς πληροφόρησης και πολιτικών περιορισμών. Επομένως, το μοντέλο Perception–Reaction–Decision υπογραμμίζει ότι η στρατηγική επιλογή δεν είναι μόνο ζήτημα ισχύος ή δυνατοτήτων, αλλά και ζήτημα ερμηνείας της κατάστασης (Marjanović and Smiljanić 2025, 84–114).

Η χρησιμότητα του συγκεκριμένου πλαισίου γίνεται ιδιαίτερα εμφανής στο σύγχρονο πληροφοριακό περιβάλλον. Στον ψηφιακό πόλεμο, η πληροφορία δεν αποτελεί απλώς μέσο κατανόησης, αλλά εργαλείο παρέμβασης στο στάδιο της αντίληψης. Η στρατηγική παραπληροφόρηση, ιδίως όταν ενισχύεται από τεχνολογίες τεχνητής νοημοσύνης, στοχεύει ακριβώς στην αλλοίωση του πρώτου σταδίου της διαδικασίας: στην κατασκευή μιας διαφορετικής εκδοχής της πραγματικότητας. Όταν η αντίληψη διαστρεβλώνεται, οι αντιδράσεις και οι αποφάσεις που ακολουθούν μπορεί να οδηγήσουν σε στρατηγικά λάθη, υπερβολικές κλιμακώσεις ή αποσταθεροποιητικές επιλογές (Nawaz 2025, 21–30).

Επιπλέον, η θεωρία Perception–Reaction–Decision αναδεικνύει ότι το πεδίο της στρατηγικής σύγκρουσης δεν περιορίζεται στη στρατιωτική διάσταση, αλλά επεκτείνεται στο γνωστικό επίπεδο. Η επιτυχία μιας επιχείρησης δεν εξαρτάται μόνο από την υλική της αποτελεσματικότητα, αλλά και από το πώς γίνεται αντιληπτή από τον αντίπαλο, το κοινό ή τους θεσμούς. Η αντίληψη μετατρέπεται έτσι σε στρατηγική μεταβλητή, η οποία μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης, χειραγώγησης ή προστασίας (Kin 2025, 22–29).

3.2. Γνωστικές παραμορφώσεις και λήψη αποφάσεων

Η διαδικασία λήψης αποφάσεων στον τομέα της ασφάλειας δεν διεξάγεται σε ένα περιβάλλον πλήρους πληροφόρησης και ουδέτερης κρίσης. Αντιθέτως, χαρακτηρίζεται από αβεβαιότητα, πίεση χρόνου και υψηλό διακύβευμα, στοιχεία που καθιστούν την ανθρώπινη αντίληψη ιδιαίτερα ευάλωτη σε γνωστικές παραμορφώσεις. Οι γνωστικές παραμορφώσεις δεν αποτελούν απλώς ατομικά σφάλματα σκέψης, αλλά δομικά χαρακτηριστικά της ανθρώπινης επεξεργασίας πληροφορίας, τα οποία επηρεάζουν την αξιολόγηση απειλών, την εκτίμηση προθέσεων και, τελικά, την ίδια τη στρατηγική επιλογή (Cristofaro et al. 2022, 2–3, 12–13). Στο

πεδίο της στρατηγικής, οι αποφασίζοντες καλούνται να ερμηνεύσουν συχνά αντιφατικές ή αποσπασματικές πληροφορίες, να προβλέψουν τη συμπεριφορά αντιπάλων και να ενεργήσουν υπό συνθήκες όπου η πλήρης επαλήθευση είναι αδύνατη. Η ανάγκη ταχείας κρίσης οδηγεί συχνά σε γνωστικές συντομεύσεις, μέσα από τις οποίες η πολύπλοκη πραγματικότητα απλοποιείται σε πιο διαχειρίσιμα σχήματα. Ωστόσο, η απλοποίηση αυτή μπορεί να δημιουργήσει στρεβλές ερμηνείες, καθώς οι αποφάσεις δεν βασίζονται σε αντικειμενική αποτίμηση, αλλά σε αντιλήψεις διαμορφωμένες από προκαταλήψεις, εμπειρία και προσδοκίες (Fenget.al., 2022).

Μία από τις πλέον χαρακτηριστικές παραμορφώσεις στη στρατηγική λήψη αποφάσεων είναι η τάση επιβεβαίωσης προϋπαρχόντων αντιλήψεων. Οι δρώντες τείνουν να αναζητούν και να ερμηνεύουν πληροφορίες με τρόπο που ενισχύει τις ήδη διαμορφωμένες εκτιμήσεις τους, ενώ παράλληλα υποβαθμίζουν στοιχεία που θα μπορούσαν να τις αμφισβητήσουν. Σε περιβάλλοντα κρίσης, όπου η ανάγκη σταθερότητας είναι έντονη, η συγκεκριμένη γνωστική τάση μπορεί να ενισχύσει την εσφαλμένη εκτίμηση μιας απειλής ή να οδηγήσει σε υπερβολικά βεβαιωμένες αποφάσεις (Zhou and Shen, 2024).

Εξίσου σημαντική είναι η υπερεκτίμηση της συνοχής και της πρόθεσης του αντιπάλου. Οι στρατηγικοί δρώντες συχνά αποδίδουν στον αντίπαλο μεγαλύτερη ορθολογικότητα, ενιαίο σχεδιασμό και πρόθεση από όση πραγματικά υπάρχει. Το αποτέλεσμα είναι η δημιουργία μιας εικόνας απειλής πιο συμπαγούς και επικίνδυνης από την πραγματική, γεγονός που μπορεί να οδηγήσει σε προληπτικές ή δυσανάλογες αντιδράσεις. Σε αυτό το πλαίσιο, η λήψη απόφασης δεν αντανακλά απαραίτητα την αντικειμενική ισορροπία ισχύος, αλλά την αντιληπτή πρόθεση και ικανότητα του άλλου (Kortelingetal. 2023). Οι γνωστικές παραμορφώσεις ενισχύονται περαιτέρω από θεσμικούς και οργανωτικούς παράγοντες. Οι αποφάσεις στην ασφάλεια λαμβάνονται εντός γραφειοκρατικών μηχανισμών, όπου η πληροφορία φιλτράρεται, ιεραρχείται και μεταφέρεται μέσω συγκεκριμένων διαδικασιών. Αυτό σημαίνει ότι οι ηγεσίες δεν έχουν άμεση πρόσβαση στην «πρώτη ύλη» της πραγματικότητας, αλλά σε ήδη επεξεργασμένες αναπαραστάσεις της. Ο τρόπος με τον οποίο οργανισμοί ασφαλείας δομούν την πληροφόρηση μπορεί να παγιώσει συγκεκριμένες αντιλήψεις και να περιορίσει την ικανότητα αναθεώρησης μιας στρατηγικής εκτίμησης (Kertzeret.al., 2022).

Στο σύγχρονο ψηφιακό περιβάλλον, οι γνωστικές παραμορφώσεις αποκτούν ακόμη μεγαλύτερη σημασία, καθώς η πληροφορία δεν είναι απλώς ατελής, αλλά συχνά εσκεμμένα

διαμορφωμένη. Η στρατηγική παραπληροφόρηση και η κατασκευή ψευδούς περιεχομένου ενισχύουν την αβεβαιότητα και δυσχεραίνουν τη διάκριση μεταξύ αξιόπιστων και παραποιημένων δεδομένων. Όταν οι αποφασίζοντες λειτουργούν σε ένα περιβάλλον όπου η πληροφορία μπορεί να είναι προϊόν χειραγώγησης, οι γνωστικές αδυναμίες δεν αποτελούν απλώς περιορισμό, αλλά δυνητικό πεδίο εκμετάλλευσης από τον αντίπαλο (Milshteinetal. 2024, 277–298). Η τεχνητή νοημοσύνη επιτείνει αυτή τη συνθήκη, καθώς επιτρέπει την παραγωγή πειστικών αναπαραστάσεων που μπορούν να ενεργοποιήσουν συναισθηματικές αντιδράσεις, να ενισχύσουν προκαταλήψεις και να δημιουργήσουν ψευδή αίσθηση επαλήθευσης. Η γνωστική διαδικασία, αντί να λειτουργεί ως φραγμός απέναντι στην παραπλάνηση, μπορεί υπό ορισμένες συνθήκες να καταστεί μηχανισμός αναπαραγωγής της. Έτσι, η λήψη αποφάσεων επηρεάζεται όχι μόνο από στρατιωτικά ή πολιτικά δεδομένα, αλλά και από την κατασκευή της αντιληπτής πραγματικότητας (Horowitz and Kahn 2024, 1-14).

Συνεπώς, η μελέτη των γνωστικών παραμορφώσεων είναι κρίσιμη για την κατανόηση της στρατηγικής συμπεριφοράς σε περιβάλλοντα ψηφιακού πολέμου. Οι αποφάσεις δεν αποτελούν απλή λογική κατάληξη της πληροφόρησης, αλλά προϊόν σύνθετων διαδικασιών αντίληψης, ερμηνείας και ψυχολογικής επεξεργασίας. Η στρατηγική παραπληροφόρηση, ιδιαίτερα όταν υποστηρίζεται από τεχνητή νοημοσύνη, δεν στοχεύει μόνο στην πληροφορία ως περιεχόμενο, αλλά στην ανθρώπινη γνωστική λειτουργία ως πεδίο στρατηγικής παρέμβασης (Sopranoet.al., 2024).

3.3. Η πληροφορία ως απειλή και ως εργαλείο στρατηγικής

Η πληροφορία αποτελεί θεμελιώδη συνιστώσα της στρατηγικής σκέψης και της ασφάλειας, καθώς συνδέεται άμεσα με την ικανότητα ενός δρώντα να κατανοεί το περιβάλλον του, να προβλέπει εξελίξεις και να διαμορφώνει αποφάσεις. Ωστόσο, στο σύγχρονο διεθνές σύστημα, η πληροφορία δεν λειτουργεί μόνο ως μέσο κατανόησης της πραγματικότητας, αλλά και ως πεδίο ανταγωνισμού. Η ίδια μπορεί να αξιοποιηθεί τόσο για την ενίσχυση της στρατηγικής αποτελεσματικότητας όσο και για την αποσταθεροποίηση αντιπάλων, γεγονός που αναδεικνύει τη διττή της φύση: εργαλείο ισχύος αλλά και πηγή απειλής (Thomas 2020, 125–144). Στην παραδοσιακή στρατηγική αντίληψη, η πληροφορία αποτελούσε κυρίως πόρο υποστήριξης της απόφασης. Η συλλογή πληροφοριών μέσω διπλωματικών δικτύων, υπηρεσιών πληροφοριών ή στρατιωτικής αναγνώρισης εξυπηρετούσε τον περιορισμό της αβεβαιότητας και τη βελτίωση της εκτίμησης της κατάστασης. Παρά το γεγονός ότι οι πληροφορίες ήταν

πάντοτε ατελείς, η βασική τους λειτουργία παρέμενε η ενίσχυση της γνώσης και η υποστήριξη της ορθολογικής στρατηγικής επιλογής (Saressalo and Huhtinen 2022, 41–66).

Ωστόσο, η εξέλιξη του ψηφιακού περιβάλλοντος μεταβάλλει ριζικά τη θέση της πληροφορίας στη στρατηγική σύγκρουση. Η πληροφορία δεν αποτελεί πλέον ουδέτερο αγαθό, αλλά πεδίο δράσης, όπου η παραγωγή, η επιλογή και η διανομή της μπορούν να επηρεάσουν άμεσα τη συμπεριφορά κρατών και κοινωνιών. Η στρατηγική αντιπαράθεση δεν διεξάγεται αποκλειστικά με στρατιωτικά μέσα, αλλά και μέσω της διαμόρφωσης της αντίληψης, της αξιοπιστίας και της εμπιστοσύνης (Asmolov, 2018). Σε αυτό το πλαίσιο, η πληροφορία μπορεί να καταστεί απειλή όταν χρησιμοποιείται για την αλλοίωση της πραγματικότητας και τη διαστρέβλωση της αντίληψης. Η παραπληροφόρηση, η επιλεκτική παρουσίαση δεδομένων και η κατασκευή αφηγημάτων αποτελούν πρακτικές που στοχεύουν όχι στη φυσική καταστροφή, αλλά στη γνωστική αποσταθεροποίηση. Η απειλή εδώ δεν προκύπτει από την άμεση βία, αλλά από την υπονόμευση της ικανότητας του αντιπάλου να ερμηνεύει σωστά την κατάσταση και να λαμβάνει συνεκτικές αποφάσεις (Deppe and Schaal 2024, 5–6).

Η στρατηγική χρήση της πληροφορίας αποκτά ιδιαίτερη σημασία σε συνθήκες υβριδικού πολέμου. Σε τέτοια περιβάλλοντα, οι ενέργειες επιρροής λειτουργούν κάτω από το κατώφλι της ανοιχτής σύγκρουσης, επιδιώκοντας να προκαλέσουν πολιτική φθορά, κοινωνική πόλωση ή θεσμική δυσπιστία χωρίς τη χρήση συμβατικών στρατιωτικών μέσων. Η πληροφορία, σε αυτή τη λογική, μετατρέπεται σε εργαλείο έμμεσης ισχύος, ικανό να μεταβάλλει τα στρατηγικά δεδομένα χωρίς εμφανή αντιπαράθεση (Marangione 2021). Παράλληλα, η ίδια η υπερπληθώρα πληροφορίας μπορεί να λειτουργήσει ως μορφή απειλής. Στο σύγχρονο ψηφιακό περιβάλλον, οι δρώντες δεν αντιμετωπίζουν έλλειψη δεδομένων αλλά υπερφόρτωση, γεγονός που δυσχεραίνει τη διάκριση μεταξύ σημαντικού και ασήμαντου, αξιόπιστου και παραποιημένου. Η πληροφοριακή υπεραφθονία δημιουργεί συνθήκες σύγχυσης, όπου η αβεβαιότητα δεν μειώνεται αλλά εντείνεται, περιορίζοντας τη δυνατότητα στρατηγικής καθαρότητας (Papadogiannakisetal. 2025, 1577–1587).

Η τεχνητή νοημοσύνη ενισχύει περαιτέρω αυτή τη δυναμική, καθώς επιτρέπει την ταχεία παραγωγή πειστικού περιεχομένου και τη στοχευμένη προσαρμογή του σε διαφορετικά ακροατήρια. Η πληροφορία μπορεί πλέον να κατασκευαστεί με τρόπο που να φαίνεται αξιόπιστος, ακόμη και όταν είναι πλήρως ψευδής. Το αποτέλεσμα είναι η δημιουργία ενός περιβάλλοντος όπου η διάκριση ανάμεσα στην πραγματικότητα και την αναπαράστασή της

γίνεται όλο και πιο ασαφής. Σε αυτό το πλαίσιο, η πληροφορία δεν είναι μόνο μέσο επικοινωνίας, αλλά μηχανισμός διαμόρφωσης της στρατηγικής πραγματικότητας (Kertysova 2018, 55–81). Επιπλέον, η πληροφορία ως εργαλείο στρατηγικής δεν περιορίζεται στην επικοινωνία προς την κοινωνία, αλλά αφορά και τη λειτουργία των ίδιων των θεσμών. Οι μηχανισμοί ασφαλείας και λήψης αποφάσεων εξαρτώνται από την εγκυρότητα των πληροφοριών που λαμβάνουν. Όταν το πληροφοριακό περιβάλλον καθίσταται πεδίο χειραγώγησης, οι θεσμοί αυτοί μπορεί να οδηγηθούν σε εσφαλμένες εκτιμήσεις ή σε στρατηγικές επιλογές που βασίζονται σε αλλοιωμένα δεδομένα (de Lima-Santos and Ceron 2023, 165–184).

Κατά συνέπεια, η πληροφορία αποτελεί ταυτόχρονα στρατηγικό πόρο και πεδίο απειλής. Η ισχύς στον σύγχρονο κόσμο δεν συνδέεται αποκλειστικά με υλικές δυνατότητες, αλλά με την ικανότητα διαμόρφωσης της αντίληψης και της ερμηνείας της πραγματικότητας. Η πληροφοριακή διάσταση της σύγκρουσης αναδεικνύει ότι ο στρατηγικός ανταγωνισμός εκτυλίσσεται πλέον και στο γνωστικό επίπεδο, όπου η επιτυχία εξαρτάται από το ποιος ελέγχει τα αφηγήματα, την αξιοπιστία και την εμπιστοσύνη (Fenstermacheretal. 2023, 172–187).

3.4 Σύνοψη Κεφαλαίου

Το τρίτο κεφάλαιο ανέδειξε την αντίληψη ως κρίσιμη στρατηγική μεταβλητή στη διαδικασία λήψης αποφάσεων σε ζητήματα ασφάλειας. Μέσα από το σχήμα Perception–Reaction–Decision, εξετάστηκε ο τρόπος με τον οποίο οι δρώντες δεν ανταποκρίνονται άμεσα στα γεγονότα, αλλά στις ερμηνείες που διαμορφώνουν για αυτά. Η ανάλυση των γνωστικών παραμορφώσεων κατέδειξε ότι οι στρατηγικές αποφάσεις επηρεάζονται συχνά από προκαταλήψεις, θεσμικούς περιορισμούς και ατελή πληροφόρηση, ιδιαίτερα σε περιβάλλοντα κρίσης και αβεβαιότητας. Τέλος, το κεφάλαιο ανέδειξε τη διττή φύση της πληροφορίας, τόσο ως εργαλείου στρατηγικής ισχύος όσο και ως πεδίου απειλής, ιδίως στο σύγχρονο ψηφιακό πλαίσιο όπου η διαχείριση της αντίληψης αποκτά κεντρική σημασία.

Κεφάλαιο 4ο Υβριδικές Απειλές και Ψηφιακός Πόλεμος

4.1 Ο επαναπροσδιορισμός της ασφάλειας στον ψηφιακό χώρο

Η έννοια της ασφάλειας έχει υποστεί σημαντική μεταβολή τις τελευταίες δεκαετίες, όχι μόνο ως προς το τι θεωρείται απειλή, αλλά και ως προς το πού και πώς εκδηλώνονται οι απειλές. Η ψηφιακή στροφή δεν πρόσθεσε απλώς ένα ακόμη πεδίο κινδύνου δίπλα στα παραδοσιακά.

Δημιούργησε ένα περιβάλλον στο οποίο η ασφάλεια συνδέεται στενά με ροές δεδομένων, πληροφοριακές υποδομές, πλατφόρμες επικοινωνίας και γνωστικές διαδικασίες. Κατά συνέπεια, η ασφάλεια στον ψηφιακό χώρο δεν μπορεί να αντιμετωπιστεί αποκλειστικά ως τεχνικό ζήτημα προστασίας δικτύων· αφορά την ανθεκτικότητα θεσμών, κοινωνιών και διαδικασιών λήψης αποφάσεων απέναντι σε νέες μορφές επιρροής και αποσταθεροποίησης (Marrone, 2022).

Στο παραδοσιακό στρατηγικό πλαίσιο, η ασφάλεια συνδεόταν κυρίως με την προστασία της εδαφικής ακεραιότητας, την αποτροπή στρατιωτικής επίθεσης και τη διαχείριση υλικών απειλών. Η ψηφιακή διάσταση μετατοπίζει το κέντρο βάρους: η στοχοποίηση δεν αφορά μόνο φυσικές υποδομές, αλλά και πληροφοριακές αλυσίδες, συστήματα επικοινωνίας, κρίσιμες υπηρεσίες και, συχνά, την ίδια τη νομιμοποίηση της κρατικής εξουσίας. Σε αυτό το πλαίσιο, η ασφάλεια αποκτά χαρακτηριστικά διαρκούς διαχείρισης κινδύνων, καθώς οι ψηφιακές απειλές δεν εμφανίζονται μόνο σε περιόδους κρίσης, αλλά λειτουργούν συνεχώς, με διαφορετικές εντάσεις και μορφές (IANCU, 2024).

Η ιδιαιτερότητα του ψηφιακού χώρου έγκειται στη φύση του: πρόκειται για πεδίο υψηλής διασύνδεσης, όπου η πληροφορία κυκλοφορεί με ταχύτητα, οι δρώντες μπορούν να δράσουν από μεγάλη απόσταση και τα όρια μεταξύ εσωτερικού και εξωτερικού αμφισβητούνται. Η επίθεση σε μια χώρα δεν προϋποθέτει απαραίτητα φυσική παρουσία ή συμβατικά μέσα. Μπορεί να εκδηλωθεί μέσω διαρροών δεδομένων, παραβίασης συστημάτων, παρεμβάσεων στις επικοινωνίες ή στοχευμένων επιχειρήσεων επιρροής. Έτσι, ο ψηφιακός χώρος μετατρέπεται σε πεδίο όπου η ασφάλεια δεν εξαρτάται μόνο από στρατιωτικές δυνατότητες, αλλά από την ικανότητα πρόληψης, ανίχνευσης και γρήγορης αποκατάστασης (Cîrdei and Ispas 2017, 71–78). Σε αυτό το σημείο καθίσταται αναγκαία η διάκριση μεταξύ κυβερνοασφάλειας και ευρύτερης ψηφιακής ασφάλειας. Η κυβερνοασφάλεια επικεντρώνεται κυρίως στην προστασία συστημάτων, δικτύων και δεδομένων από παραβιάσεις, επιθέσεις και τεχνικές καταστροφές. Αντίθετα, η ψηφιακή ασφάλεια περιλαμβάνει και τη διαχείριση κινδύνων που σχετίζονται με το πληροφοριακό περιβάλλον, την κοινωνική συνοχή και την αξιοπιστία των θεσμών. Ένα κράτος μπορεί να διαθέτει ισχυρά τεχνικά μέτρα κυβερνοασφάλειας και, παρ' όλα αυτά, να παραμένει ευάλωτο σε επιχειρήσεις παραπληροφόρησης ή σε στοχευμένη υπονόμευση της εμπιστοσύνης. Η διαφορά αυτή είναι κρίσιμη, διότι η ασφάλεια στον ψηφιακό χώρο δεν κρίνεται μόνο από την τεχνική αντοχή των συστημάτων, αλλά και από την ικανότητα του κράτους και της κοινωνίας να διατηρούν

σταθερές διαδικασίες αντίληψης και απόφασης (Deppe and Schaal 2024, 1–2; 5–6). Η μετατόπιση αυτή οδηγεί σε έναν επαναπροσδιορισμό του τι σημαίνει «απειλή». Οι ψηφιακές απειλές συχνά δεν προκαλούν άμεση, ορατή ζημία με τον τρόπο που το κάνει μια συμβατική επίθεση. Μπορούν να λειτουργούν σταδιακά, με μικρά, συσσωρευτικά αποτελέσματα: αποδόμηση εμπιστοσύνης, καλλιέργεια αβεβαιότητας, πόλωση, δυσλειτουργία θεσμών ή υπονόμευση της αξιοπιστίας της πληροφόρησης. Η ασφάλεια, συνεπώς, δεν αφορά μόνο την αποτροπή καταστροφής, αλλά και την αποτροπή διάβρωσης της θεσμικής και κοινωνικής σταθερότητας (DunnCavelty&Wenger, 2020).

Επιπλέον, ο ψηφιακός χώρος καθιστά δυσκολότερη τη διάκριση ανάμεσα σε ειρήνη και σύγκρουση. Πολλές ενέργειες που έχουν στρατηγικό αποτέλεσμα δεν υπάγονται εύκολα σε κατηγορίες πολέμου, ούτε ενεργοποιούν αυτόματα μηχανισμούς άμυνας. Αυτή η αμφισημία δημιουργεί ένα περιβάλλον «χαμηλής έντασης» στο οποίο οι δρώντες μπορούν να δοκιμάζουν, να πιέζουν και να αποσταθεροποιούν χωρίς το κόστος και τους κινδύνους μιας ανοιχτής στρατιωτικής σύγκρουσης. Κατ’ επέκταση, η ασφάλεια στον ψηφιακό χώρο συνδέεται με τη διαχείριση μιας μόνιμης στρατηγικής τριβής, όπου το διακύβευμα είναι συχνά η ανθεκτικότητα και η συνοχή, όχι η άμεση επιβίωση (Barguésetal. 2023, 2281–2299). Στο νέο αυτό πλαίσιο, η απόδοση ευθύνης αποτελεί επιπλέον πρόκληση. Οι ψηφιακές επιθέσεις, αλλά και οι επιχειρήσεις επιρροής, μπορούν να σχεδιαστούν έτσι ώστε να αφήνουν ασαφή ίχνη, να πραγματοποιούνται μέσω ενδιάμεσων δικτύων ή να εμφανίζονται ως «αυθόρμητες» κοινωνικές εκδηλώσεις. Η δυσκολία απόδοσης ευθύνης περιορίζει την αποτελεσματικότητα της αποτροπής, καθώς η αποτροπή προϋποθέτει σαφή αντίπαλο και καθαρό μηχανισμό ανταπόδοσης. Όταν ο δρών παραμένει αόρατος ή αμφίσημος, η στρατηγική αντίδραση γίνεται πιο περίπλοκη και συχνά πολιτικά ευαίσθητη (Lin and Kerr 2017, 4–22). Ο επαναπροσδιορισμός της ασφάλειας στον ψηφιακό χώρο επηρεάζει και τον ρόλο των κρατικών θεσμών. Η προστασία δεν μπορεί να βασίζεται αποκλειστικά σε στρατιωτικούς ή τεχνικούς μηχανισμούς· απαιτεί διατομεακή συνεργασία, θεσμικό συντονισμό και συνεχή προσαρμογή. Παράλληλα, ο ιδιωτικός τομέας καθίσταται συχνά κρίσιμος εταίρος, καθώς πολλές ψηφιακές υποδομές και πλατφόρμες ανήκουν ή λειτουργούν υπό ιδιωτική διαχείριση. Η ασφάλεια παύει έτσι να είναι αποκλειστική αρμοδιότητα κρατικών μηχανισμών και αποκτά χαρακτηριστικά σύνθετης διακυβέρνησης (MikhaylovskayaandRouméas, 2024).

Τέλος, η ψηφιακή ασφάλεια συνδέεται άμεσα με το επίπεδο της αντίληψης και της πληροφορίας. Σε περιβάλλοντα όπου η πληροφορία μπορεί να παραποιηθεί, να κατασκευαστεί

ή να παρουσιαστεί επιλεκτικά, η διαχείριση της αλήθειας και της αξιοπιστίας αποκτά στρατηγική διάσταση. Η ασφάλεια δεν εξαρτάται μόνο από το τι συμβαίνει, αλλά και από το τι γίνεται πιστευτό, πώς ερμηνεύεται και πώς επηρεάζει αποφάσεις. Αυτή η διάσταση είναι ιδιαίτερα κρίσιμη για την παρούσα διατριβή, καθώς συνδέει τον ψηφιακό χώρο με τη λήψη στρατηγικών αποφάσεων και εξηγεί γιατί η παραπληροφόρηση μέσω τεχνητής νοημοσύνης μπορεί να λειτουργήσει ως απειλή με ευρύτερες συνέπειες από μια μεμονωμένη τεχνική επίθεση (Sliwa&Antczak, 2018).

4.2 Η στρατηγική παραπληροφόρηση ως μέθοδος επιβολής

Η στρατηγική παραπληροφόρηση αποτελεί μία από τις πλέον χαρακτηριστικές μορφές άσκησης ισχύος στο σύγχρονο ψηφιακό περιβάλλον. Σε αντίθεση με τις παραδοσιακές μεθόδους επιβολής, που στηρίζονται κυρίως στη χρήση στρατιωτικής ισχύος ή οικονομικού εξαναγκασμού, η παραπληροφόρηση λειτουργεί έμμεσα, διαμορφώνοντας το πλαίσιο μέσα στο οποίο οι κοινωνίες και οι θεσμοί αντιλαμβάνονται την πραγματικότητα. Η επιβολή, σε αυτή την περίπτωση, δεν προκύπτει από την άμεση καταναγκαστική δύναμη, αλλά από την ικανότητα ελέγχου της πληροφορίας, της αντίληψης και, τελικά, της συμπεριφοράς (Pace and Coelho 2022, 707–722).

Στη στρατηγική της διάσταση, η παραπληροφόρηση δεν περιορίζεται στη διάδοση ψευδών ειδήσεων ή ανακριβών δεδομένων. Πρόκειται για ένα ευρύτερο σύνολο πρακτικών που αποσκοπούν στη χειραγώγηση της αντίληψης, στη δημιουργία σύγχυσης και στη σταδιακή υπονόμευση της εμπιστοσύνης. Η στρατηγική παραπληροφόρηση δεν στοχεύει απαραίτητα να γίνει αποδεκτή ως απόλυτη αλήθεια· συχνά αρκεί να καταστήσει ασαφή τη διάκριση μεταξύ αληθούς και ψευδούς, να αποδυναμώσει την αξιοπιστία θεσμών ή να καλλιεργήσει ένα περιβάλλον αβεβαιότητας που ευνοεί τον δρώντα που την παράγει (SaressaloandHuhtinen, 2022). Η λειτουργία της ως μέθοδος επιβολής εδράζεται στο γεγονός ότι η στρατηγική ισχύς δεν ασκείται μόνο μέσω υλικών μέσων, αλλά και μέσω της διαμόρφωσης προτιμήσεων, αντιλήψεων και πλαισίων ερμηνείας. Σε αυτό το πλαίσιο, η πληροφορία μετατρέπεται σε πεδίο αντιπαράθεσης, όπου ο στόχος δεν είναι απλώς η επικράτηση στο στρατιωτικό επίπεδο, αλλά η διαμόρφωση πολιτικών και κοινωνικών συνθηκών που περιορίζουν τις επιλογές του αντιπάλου. Η παραπληροφόρηση μπορεί να επηρεάσει τις πολιτικές αποφάσεις ενός κράτους, να ενισχύσει εσωτερικές διαιρέσεις ή να αποσταθεροποιήσει τη δημόσια σφαίρα, επιτυγχάνοντας στρατηγικά αποτελέσματα χωρίς άμεση σύγκρουση(Levinger 2018, 125–134).

Ιδιαίτερη σημασία αποκτά ο ρόλος της παραπληροφόρησης στον υβριδικό πόλεμο, όπου τα όρια μεταξύ ειρήνης και σύγκρουσης καθίστανται δυσδιάκριτα. Οι επιχειρήσεις παραπληροφόρησης επιτρέπουν την άσκηση πίεσης κάτω από το κατώφλι της ανοιχτής στρατιωτικής αντιπαράθεσης, δημιουργώντας σταδιακές αλλά ουσιαστικές μεταβολές στο πολιτικό και κοινωνικό περιβάλλον του αντιπάλου. Η επιβολή εδώ λειτουργεί μέσω φθοράς: όχι μέσω άμεσης καταστροφής, αλλά μέσω διάβρωσης της συνοχής, της εμπιστοσύνης και της στρατηγικής ικανότητας αντίδρασης (Whiteaker and Valkonen 2022, 11-1). Η στρατηγική παραπληροφόρηση αποκτά επιπλέον ισχύ στο ψηφιακό περιβάλλον λόγω της ταχύτητας διάδοσης και της δυνατότητας μαζικής αναπαραγωγής περιεχομένου. Τα κοινωνικά δίκτυα, οι αλγόριθμοι προώθησης και οι ψηφιακές πλατφόρμες δημιουργούν συνθήκες όπου μια αφήγηση μπορεί να εξαπλωθεί ταχύτατα και να αποκτήσει δυσανάλογη επιρροή. Η επιβολή δεν χρειάζεται πλέον να προέρχεται από έναν κεντρικό μηχανισμό προπαγάνδας· μπορεί να λειτουργήσει μέσα από αποκεντρωμένα δίκτυα, όπου η παραπληροφόρηση παρουσιάζεται ως «αυθόρμητη» κοινωνική δυναμική (Can 2020, 271–286).Σε αυτό το πλαίσιο, η παραπληροφόρηση δεν στοχεύει μόνο την κοινή γνώμη, αλλά και τους ίδιους τους θεσμούς λήψης αποφάσεων. Η επιβολή επιτυγχάνεται όταν η στρατηγική κρίση διαμορφώνεται σε περιβάλλον αβεβαιότητας και γνωστικής πίεσης. Εάν οι πολιτικοί ή στρατιωτικοί δρώντες λαμβάνουν αποφάσεις στηριγμένοι σε εσφαλμένες ή αλλοιωμένες πληροφορίες, τότε η παραπληροφόρηση έχει ήδη παράξει στρατηγικό αποτέλεσμα. Η επιβολή εδώ είναι γνωστική: αφορά την αλλοίωση του πλαισίου απόφασης και όχι την άμεση επιβολή φυσικής ισχύος (Casero-Ripollésetal. 2023)

Η χρήση τεχνητής νοημοσύνης ενισχύει περαιτέρω τη στρατηγική αποτελεσματικότητα της παραπληροφόρησης. Η παραγωγή πειστικών συνθετικών εικόνων, η αυτοματοποίηση αφηγημάτων και η στοχευμένη προσαρμογή μηνυμάτων σε διαφορετικά ακροατήρια αυξάνουν την ικανότητα χειραγώγησης. Η παραπληροφόρηση παύει να είναι περιστασιακή και αποκτά χαρακτηριστικά συστηματικής στρατηγικής πρακτικής, με δυνατότητα κλιμάκωσης και προσαρμογής. Η εξέλιξη αυτή καθιστά δυσκολότερη την ανίχνευση και την αντιμετώπισή της, καθώς οι ψευδείς αναπαραστάσεις μπορούν να εμφανίζονται ως απολύτως αυθεντικές (Bradshawetal. 2021, 5–7). Παράλληλα, η στρατηγική παραπληροφόρηση λειτουργεί ως μέθοδος επιβολής και στο επίπεδο της διεθνούς νομιμοποίησης. Η διαμόρφωση αφηγημάτων σχετικά με συγκρούσεις, επεμβάσεις ή κρίσεις μπορεί να επηρεάσει τη στάση τρίτων κρατών, διεθνών οργανισμών και παγκόσμιας κοινής γνώμης. Η ισχύς δεν ασκείται μόνο έναντι του

άμεσου αντιπάλου, αλλά και μέσω της διαμόρφωσης του διεθνούς περιβάλλοντος μέσα στο οποίο αυτός δρα. Κατ' αυτόν τον τρόπο, η παραπληροφόρηση μπορεί να περιορίσει τη διπλωματική ελευθερία κινήσεων ενός κράτους ή να ενισχύσει τη θέση του επιτιθέμενου δρώντα (Kertysova, 2018).

4.3 Θεωρητική ενσωμάτωση της παραπληροφόρησης στη στρατηγική ανάλυση

Η παραπληροφόρηση δεν αποτελεί ένα περιφερειακό επικοινωνιακό φαινόμενο, αλλά ένα πεδίο στρατηγικής δράσης που επηρεάζει τον τρόπο με τον οποίο διαμορφώνονται συμφέροντα, αντιλήψεις και επιλογές. Για να ενσωματωθεί θεωρητικά στη στρατηγική ανάλυση, δεν αρκεί να περιγραφεί ως «ψευδές περιεχόμενο» ή ως πρακτική προπαγάνδας. Χρειάζεται να αντιμετωπιστεί ως μηχανισμός που παρεμβαίνει στη σχέση ανάμεσα σε πληροφορία, αντίληψη και απόφαση, μεταβάλλοντας το πλαίσιο μέσα στο οποίο λειτουργούν οι δρώντες. Η στρατηγική σημασία της παραπληροφόρησης προκύπτει ακριβώς από το ότι επιδρά στο γνωστικό και πολιτικό επίπεδο της σύγκρουσης, συχνά χωρίς να υπερβαίνει το κατώφλι της ανοιχτής αντιπαράθεσης (Bryczek-Wróbel and Moszczyński 2022, 48–62).

Στη στρατηγική θεωρία, η ανάλυση των συγκρούσεων στηρίζεται συνήθως σε μεταβλητές όπως οι δυνατότητες, οι προθέσεις, η αποτροπή και οι συσχετισμοί ισχύος. Η παραπληροφόρηση εισάγει μια πρόσθετη διάσταση: επηρεάζει την πρόσβαση στη γνώση για τις δυνατότητες και τις προθέσεις, αλλοιώνει την αξιολόγηση της κατάστασης και μπορεί να μεταβάλει την αντίληψη της απειλής. Όταν οι πληροφορίες που τροφοδοτούν τη στρατηγική κρίση είναι αμφίβολης αξιοπιστίας ή σκόπιμα παραποιημένες, οι κλασικές μεταβλητές εξακολουθούν να ισχύουν, αλλά η σημασία τους εξαρτάται από το πώς γίνονται αντιληπτές. Έτσι, η παραπληροφόρηση ενσωματώνεται στη στρατηγική ανάλυση ως παράγοντας που μετασχηματίζει την ίδια τη διαδικασία εκτίμησης (Iosifidis 2024, 21–36). Η ενσωμάτωση αυτή προϋποθέτει, πρώτον, να θεωρηθεί η πληροφορία ως πεδίο ισχύος. Η ισχύς δεν ασκείται μόνο μέσω της υλικής υπεροχής ή της απειλής χρήσης βίας, αλλά και μέσω της ικανότητας καθορισμού του πλαισίου μέσα στο οποίο οι άλλοι ερμηνεύουν τα γεγονότα. Η παραπληροφόρηση λειτουργεί, συνεπώς, ως μέσο στρατηγικής επιρροής: διαμορφώνει προτεραιότητες, προκαλεί αμφιβολία, ενισχύει φόβους ή επιθυμίες, και τελικά περιορίζει ή κατευθύνει τις διαθέσιμες επιλογές του αντιπάλου. Σε ένα τέτοιο σχήμα, η στρατηγική επιτυχία δεν μετριέται μόνο από το αποτέλεσμα στο πεδίο, αλλά και από τη διαμόρφωση αντιληπτικών και πολιτικών συνθηκών που ευνοούν τον δρώντα (Hedling and Ördén 2025, 967-986).

Δεύτερον, η παραπληροφόρηση πρέπει να ενταχθεί στη λογική της αποτροπής και της κλιμάκωσης. Η αποτροπή βασίζεται στην αξιοπιστία: στην πεποίθηση ότι ένας δρών διαθέτει δυνατότητες και βούληση να τις χρησιμοποιήσει. Η παραπληροφόρηση μπορεί να αποδυναμώσει ή να διαστρεβλώσει αυτή την αξιοπιστία, είτε υπερβάλλοντας είτε υποβαθμίζοντας τις πραγματικές δυνατότητες και προθέσεις. Εάν ο αντίπαλος πειστεί ότι μια απειλή είναι μπλόφα ή ότι μια ικανότητα δεν υπάρχει, η αποτροπή αποδυναμώνεται. Αντίστροφα, η καλλιέργεια υπερβολικού φόβου μπορεί να οδηγήσει σε πρόωρη κλιμάκωση ή σε πολιτικές αποφάσεις που υπό άλλες συνθήκες θα θεωρούνταν δυσανάλογες. Έτσι, η παραπληροφόρηση ενσωματώνεται στη στρατηγική ανάλυση ως μηχανισμός που επηρεάζει την ισορροπία κινδύνου, το κατώφλι αντίδρασης και τη δυναμική της κρίσης (Miller, 2023).

Τρίτον, η παραπληροφόρηση πρέπει να θεωρηθεί εργαλείο που στοχεύει τόσο στην κοινωνία όσο και στους θεσμούς. Στο κοινωνικό επίπεδο, μπορεί να επηρεάσει την κοινή γνώμη, να ενισχύσει πολώσεις, να διαμορφώσει συλλογικές πεποιθήσεις και να υπονομεύσει την εμπιστοσύνη σε θεσμούς. Στο θεσμικό επίπεδο, μπορεί να αλλοιώσει την πληροφόρηση που φτάνει στους αποφασίζοντες ή να περιορίσει τον χώρο πολιτικής επιλογής μέσω της πίεσης που δημιουργεί η δημόσια αντίδραση. Η στρατηγική ανάλυση οφείλει να λαμβάνει υπόψη αυτή τη διπλή κατεύθυνση, επειδή η κρατική ισχύς δεν ασκείται σε κενό: εξαρτάται από κοινωνική νομιμοποίηση και από την αποτελεσματικότητα των θεσμών. Όταν η παραπληροφόρηση διαβρώνει αυτούς τους πυλώνες, επιτυγχάνει αποτελέσματα στρατηγικής επιβολής χωρίς να απαιτείται συμβατική αντιπαράθεση (Romanishynetal. 2025).

Τέταρτον, η θεωρητική ενσωμάτωση απαιτεί να αντιμετωπιστεί η παραπληροφόρηση ως πρακτική που λειτουργεί σε επίπεδο «γνωστικής ασφάλειας». Η έννοια αυτή δεν αναφέρεται σε ψυχολογικούς όρους με στενή έννοια, αλλά στη σταθερότητα των διαδικασιών αντίληψης και κρίσης που επιτρέπουν σε μια κοινωνία και σε ένα κράτος να αξιολογούν απειλές και να λαμβάνουν αποφάσεις. Όταν ο πληροφοριακός χώρος κατακλύζεται από κατασκευασμένο περιεχόμενο, όταν μειώνεται η εμπιστοσύνη σε αξιόπιστες πηγές και όταν η επαλήθευση γίνεται δυσκολότερη, η γνωστική σταθερότητα κλονίζεται. Αυτό έχει άμεσες συνέπειες στη στρατηγική ικανότητα, διότι η αποτελεσματική δράση προϋποθέτει ένα ελάχιστο επίπεδο κοινής κατανόησης της πραγματικότητας (Karinshak and Jin 2023, 539–562).

Ιδιαίτερα στο σύγχρονο ψηφιακό περιβάλλον, η παραπληροφόρηση δεν λειτουργεί μόνο με το περιεχόμενο, αλλά και με τη δομή της διάδοσης. Η στρατηγική ανάλυση οφείλει να

λαμβάνει υπόψη ότι η επιρροή δεν παράγεται μόνο από «ισχυρά» μηνύματα, αλλά και από τις συνθήκες αναπαραγωγής τους: τον ρυθμό διάχυσης, την ενίσχυση μέσω πλατφορμών, την επανάληψη, την αξιοποίηση δικτύων και την εκμετάλλευση συναισθηματικών αντιδράσεων. Έτσι, η παραπληροφόρηση ενσωματώνεται ως δυναμική διαδικασία που αλληλεπιδρά με τεχνολογικές υποδομές και κοινωνικές προδιαθέσεις (Angwald and Wagnsson 2024, 1527–1538). Η τεχνητή νοημοσύνη προσθέτει σε αυτή τη συζήτηση μια κρίσιμη ποιοτική μεταβολή, καθώς διευκολύνει την κλιμάκωση και την πειστικότητα των επιχειρήσεων παραπληροφόρησης. Το ζήτημα δεν είναι μόνο η παραγωγή μεγαλύτερου όγκου περιεχομένου, αλλά η δυνατότητα ταχείας προσαρμογής αφηγημάτων και η δημιουργία υλικού που δυσκολεύει την επαλήθευση. Η στρατηγική ανάλυση, συνεπώς, καλείται να συνδέσει την παραπληροφόρηση με την τεχνολογική ικανότητα παραγωγής «πραγματοφανών» αναπαραστάσεων, οι οποίες επηρεάζουν την αντίληψη και μπορούν να πυροδοτήσουν αντιδράσεις πριν υπάρξει επαρκής έλεγχος της εγκυρότητάς τους (Vasistetal. 2024, 663–688).

4.4 Σύνοψη Κεφαλαίου

Το τέταρτο κεφάλαιο εξέτασε τον τρόπο με τον οποίο η ασφάλεια επαναπροσδιορίζεται στον ψηφιακό χώρο, όπου οι απειλές δεν εκδηλώνονται πλέον μόνο με στρατιωτικά μέσα αλλά και μέσω της πληροφορίας και της επιρροής. Αναλύθηκε η στρατηγική παραπληροφόρηση ως μέθοδος επιβολής που στοχεύει στη διαμόρφωση αντιλήψεων, στη δημιουργία σύγχυσης και στη διάβρωση θεσμικής εμπιστοσύνης. Ιδιαίτερη έμφαση δόθηκε στη θεωρητική ενσωμάτωση της παραπληροφόρησης στη στρατηγική ανάλυση, ως παράγοντα που επηρεάζει την αποτροπή, τη λήψη αποφάσεων και τη συνοχή των κοινωνιών. Συνολικά, το κεφάλαιο ανέδειξε ότι στο σύγχρονο υβριδικό περιβάλλον η πληροφορία λειτουργεί ως κεντρικό εργαλείο ισχύος και πεδίο αντιπαράθεσης.

Κεφάλαιο 5ο Μελέτες Περίπτωσης Ψηφιακής Παραπληροφόρησης

5.1 Η χρήση deepfakes και bots στον πόλεμο Ρωσίας–Ουκρανίας

Ο πόλεμος Ρωσίας–Ουκρανίας ανέδειξε με ιδιαίτερα καθαρό τρόπο ότι το ψηφιακό πεδίο δεν λειτουργεί απλώς ως «κανάλι ενημέρωσης», αλλά ως χώρος όπου παράγονται στρατηγικά αποτελέσματα. Στο πλαίσιο αυτό, τα deepfakes και τα bots δεν είναι μεμονωμένες τεχνολογικές «ακρότητες». Εντάσσονται σε ένα ευρύτερο φάσμα πληροφοριακών επιχειρήσεων που στοχεύουν στη σύγχυση, στη διάβρωση εμπιστοσύνης και στη διαμόρφωση αντιλήψεων σε κοινωνίες, θεσμούς και διεθνές ακροατήριο (Briggs and Tusor 2025, 177–185).

5.1.1 Deepfakes

Τα deepfakes αποτελούν μία από τις πιο χαρακτηριστικές εφαρμογές της σύγχρονης τεχνολογίας στη σφαίρα της παραπληροφόρησης, καθώς συνδυάζουν την οπτικοακουστική πειστικότητα με τη δυνατότητα κατασκευής γεγονότων που δεν συνέβησαν ποτέ. Η ιδιαιτερότητά τους δεν έγκειται μόνο στο ότι παράγουν ψευδές περιεχόμενο, αλλά στο ότι επιχειρούν να μιμηθούν με ακρίβεια πρόσωπα, φωνές και δηλώσεις, δημιουργώντας υλικό που μπορεί να λειτουργήσει ως υποκατάστατο της πραγματικότητας. Σε ένα περιβάλλον όπου η εικόνα και το βίντεο θεωρούνται συχνά αδιάψευστα τεκμήρια, η εμφάνιση των deepfakes εισάγει μια κρίσιμη αβεβαιότητα σχετικά με το τι είναι αυθεντικό και τι κατασκευασμένο (Boháček and Farid 2022).

Στο πλαίσιο του πολέμου Ρωσίας–Ουκρανίας, τα deepfakes απέκτησαν ιδιαίτερη σημασία ως εργαλείο πληροφοριακής πίεσης. Ένα από τα πιο γνωστά περιστατικά ήταν η διακίνηση βίντεο που εμφάνιζε τον Ουκρανό πρόεδρο να καλεί τον πληθυσμό να παραδοθεί. Παρότι το περιεχόμενο αποδομήθηκε σχετικά γρήγορα και η τεχνική του ποιότητα δεν ήταν ιδιαίτερα υψηλή, το περιστατικό ανέδειξε τη στρατηγική στόχευση των deepfakes, όχι απαραίτητα να πείσουν πλήρως, αλλά να δημιουργήσουν στιγμιαία σύγχυση, να δοκιμάσουν την εμπιστοσύνη του κοινού και να ενεργοποιήσουν μηχανισμούς αμφιβολίας (George and George 2023, 58–74). Η στρατηγική αξία των deepfakes δεν περιορίζεται στην επιτυχία μιας εξαπάτησης. Ακόμη και όταν αποκαλύπτονται, μπορούν να παράγουν δευτερογενείς συνέπειες. Η διάδοση ενός deepfake σε συνθήκες κρίσης προκαλεί αναστάτωση, επιβραδύνει τη διαδικασία επαλήθευσης και επιβαρύνει την επικοινωνιακή διαχείριση των θεσμών. Η ανάγκη διάψευσης και αποκατάστασης της αλήθειας απορροφά χρόνο και πόρους, ενώ ταυτόχρονα η αρχική εντύπωση μπορεί να έχει ήδη επιδράσει σε συναισθηματικό επίπεδο. Έτσι, το deepfake λειτουργεί ως εργαλείο γνωστικής πίεσης, ακόμη και όταν δεν γίνεται τελικά πιστευτό (Twomeyetal. 2023). Επιπλέον, τα deepfakes συμβάλλουν στη διάβρωση της εμπιστοσύνης στο ίδιο το πληροφοριακό περιβάλλον. Όσο περισσότερο καθίσταται γνωστό ότι ένα βίντεο ή μια δήλωση μπορεί να είναι προϊόν κατασκευής, τόσο δυσκολότερη γίνεται η αποδοχή οποιουδήποτε οπτικοακουστικού τεκμηρίου. Αυτό δημιουργεί μια συνθήκη όπου η αβεβαιότητα δεν αφορά μόνο το ψευδές περιεχόμενο, αλλά και την πιθανότητα αμφισβήτησης της αλήθειας. Πρόκειται για ένα φαινόμενο που έχει ιδιαίτερη στρατηγική σημασία, καθώς επιτρέπει στους δρώντες να αρνούνται πραγματικά γεγονότα ή να καθυστερούν την απόδοση ευθύνης, επικαλούμενοι την πιθανότητα αλλοίωσης (Westerlund 2019, 39–52).

Η λειτουργία των deepfakes στο ψηφιακό πεδίο συνδέεται επίσης με τη δυναμική της ταχύτητας. Σε περιόδους πολέμου, το πληροφοριακό περιβάλλον χαρακτηρίζεται από συνεχή ροή ειδήσεων, έντονη συναισθηματική φόρτιση και περιορισμένο χρόνο επαλήθευσης. Ένα deepfake δεν χρειάζεται να διατηρηθεί για μεγάλο διάστημα· αρκεί να διαδοθεί γρήγορα και να δημιουργήσει ένα αρχικό κύμα αμφιβολίας ή πανικού. Η στρατηγική αποτελεσματικότητα, συνεπώς, βασίζεται περισσότερο στην ταχύτητα και στην εμβέλεια παρά στη μακροπρόθεσμη πειθώ (VaccariandChadwick, 2020). Παράλληλα, η ανάπτυξη deepfakes εντάσσεται σε μια ευρύτερη μεταβολή της πληροφοριακής σύγκρουσης, όπου η εικόνα της πραγματικότητας γίνεται πεδίο χειραγώγησης. Στον πόλεμο Ρωσίας–Ουκρανίας, η σύγκρουση δεν περιορίστηκε σε στρατιωτικές επιχειρήσεις, αλλά επεκτάθηκε στη διεθνή κοινή γνώμη και στη νομιμοποίηση των εμπλεκόμενων πλευρών. Τα deepfakes, ως τεχνολογία που μπορεί να αλλοιώσει συμβολικά κρίσιμες στιγμές, ενισχύουν αυτή την τάση και καθιστούν δυσκολότερη τη διατήρηση ενός σταθερού πλαισίου ενημέρωσης (Nasiri and Hashemzadeh 2025, 229–250).

5.1.2 Bots

Η χρήση αυτοματοποιημένων λογαριασμών, γνωστών ως bots, αποτελεί μία από τις πιο διαδεδομένες πρακτικές στο πεδίο της ψηφιακής παραπληροφόρησης. Σε αντίθεση με τα deepfakes, τα οποία στηρίζονται κυρίως στη δημιουργία εντυπωσιακού ψευδούς υλικού, τα bots λειτουργούν μέσω της μαζικής αναπαραγωγής, της συνεχούς επανάληψης και της συστηματικής ενίσχυσης συγκεκριμένων αφηγημάτων. Η στρατηγική τους αξία δεν έγκειται τόσο στο περιεχόμενο αυτό καθαυτό, αλλά στην ικανότητά τους να επηρεάζουν την ορατότητα και την πρόσληψη της πληροφορίας σε μεγάλη κλίμακα (Smart etal. 2022, 34–53).

Στον πόλεμο Ρωσίας–Ουκρανίας, τα bots αξιοποιήθηκαν εκτενώς ως μέσο πληροφορικής πίεσης και επιρροής. Μέσα από δικτυωμένες δραστηριότητες σε πλατφόρμες κοινωνικής δικτύωσης, αυτοματοποιημένοι λογαριασμοί συνέβαλαν στη διάδοση συγκεκριμένων μηνυμάτων, στην ενίσχυση επιλεγμένων θεμάτων και στη δημιουργία ενός περιβάλλοντος όπου ορισμένες αφηγήσεις εμφανίζονταν ως κυρίαρχες. Η στρατηγική αυτή επιτρέπει σε έναν δρών να δημιουργήσει την εντύπωση ότι μια θέση υποστηρίζεται ευρέως, ακόμη και όταν πρόκειται για κατασκευασμένη εικόνα συναίνεσης (Geissleretal. 2023). Ο όρος «ψευδαίσθηση συναίνεσης» περιγράφει ακριβώς αυτή τη λειτουργία. Όταν ένα μήνυμα επαναλαμβάνεται συνεχώς από πολλούς λογαριασμούς, όταν εμφανίζεται ως δημοφιλές ή όταν κατακλύζει τον δημόσιο διάλογο, οι χρήστες τείνουν να το αντιλαμβάνονται ως κοινωνικά ισχυρό ή ως ευρέως αποδεκτό. Η αντίληψη αυτή μπορεί να επηρεάσει τη στάση του κοινού, όχι

επειδή το περιεχόμενο είναι απαραίτητα πειστικό, αλλά επειδή παρουσιάζεται ως κυρίαρχο. Σε αυτό το πλαίσιο, η ισχύς των bots δεν είναι πρωτίστως επιχειρηματολογική, αλλά αντιληπτική, αφορά το πώς διαμορφώνεται το κλίμα μέσα στο οποίο αξιολογείται η πληροφορία (Mariglianoetal. 2024).

Ιδιαίτερη σημασία έχει και η ταχύτητα που προσφέρουν τα bots στις επιχειρήσεις επιρροής. Σε περιόδους πολέμου, όπου η πληροφορία εξελίσσεται διαρκώς και η ανάγκη για άμεση ενημέρωση είναι υψηλή, η δυνατότητα μαζικής διάδοσης σε σύντομο χρονικό διάστημα δημιουργεί στρατηγικό πλεονέκτημα. Τα bots μπορούν να ενεργοποιηθούν σχεδόν στιγμιαία, να κατακλύσουν τον διάλογο με συγκεκριμένες ερμηνείες και να προηγηθούν των μηχανισμών επαλήθευσης. Έτσι, ακόμη και μια παραπλανητική αφήγηση μπορεί να αποκτήσει προσωρινή δυναμική πριν υπάρξει θεσμική ή δημοσιογραφική αντίδραση (Bradshawetal. 2020). Επιπλέον, η λειτουργία των bots δεν περιορίζεται στη διάδοση ψευδών πληροφοριών. Συχνά συμβάλλουν στη δημιουργία σύγχυσης μέσω πληθώρας αντικρουόμενων μηνυμάτων, εντείνοντας την πληροφοριακή υπερφόρτωση. Η τεχνική αυτή δεν στοχεύει απαραίτητα στην πειθώ, αλλά στη διάβρωση της δυνατότητας του κοινού να διακρίνει αξιόπιστες πηγές. Όταν η δημόσια σφαίρα κατακλύζεται από συνεχείς, αντιφατικές και επαναλαμβανόμενες αναρτήσεις, η αβεβαιότητα ενισχύεται και η εμπιστοσύνη στην ενημέρωση μειώνεται (Teperiketal. 2022, 21–23).

Στον πόλεμο Ρωσίας–Ουκρανίας, η στρατηγική χρήση bots συνδέθηκε επίσης με την προσπάθεια επηρεασμού διεθνών ακροατηρίων. Οι πληροφοριακές επιχειρήσεις δεν περιορίστηκαν στο εσωτερικό πεδίο της σύγκρουσης, αλλά στόχευσαν και την παγκόσμια κοινή γνώμη, επιδιώκοντας να ενισχύσουν την κόπωση, να αποδυναμώσουν τη στήριξη προς την Ουκρανία ή να μεταβάλουν τις πολιτικές ισορροπίες σε τρίτες χώρες. Σε αυτό το επίπεδο, τα bots λειτουργούν ως εργαλείο διάχυσης αφηγημάτων πέρα από τα εθνικά σύνορα, προσφέροντας τη δυνατότητα μαζικής επιρροής με χαμηλό κόστος (Alsmadi, Rice, and O'Brien 2024, 190–193). Η στρατηγική διάσταση των bots γίνεται ακόμη πιο σύνθετη όταν αυτά εντάσσονται σε ευρύτερα δίκτυα συντονισμένης συμπεριφοράς, όπου αυτοματοποιημένοι λογαριασμοί συνεργάζονται με ανθρώπινους φορείς, τρολ ή οργανωμένες ομάδες επιρροής. Σε τέτοιες περιπτώσεις, η διάκριση ανάμεσα σε «αυθεντική» κοινωνική αντίδραση και σε οργανωμένη κατασκευή γίνεται δυσκολότερη. Η δημόσια σφαίρα μετατρέπεται έτσι σε πεδίο όπου η κοινωνική πραγματικότητα μπορεί να αλλοιωθεί τεχνητά, όχι με την κατασκευή ενός μεμονωμένου ψέματος, αλλά με τη δημιουργία ενός παραμορφωμένου περιβάλλοντος συζήτησης (Bryant 2023, 49).

5.1.3 Συνδυασμός deepfakes και bots

Η αποτελεσματικότητα της σύγχρονης στρατηγικής παραπληροφόρησης δεν στηρίζεται απαραίτητα σε ένα μεμονωμένο εργαλείο, αλλά στη συνδυαστική χρήση διαφορετικών τεχνολογικών μέσων που λειτουργούν συμπληρωματικά. Στον πόλεμο Ρωσίας–Ουκρανίας, η παράλληλη αξιοποίηση deepfakes και bots ανέδειξε μια νέα μορφή «πακέτου» επιρροής, όπου η κατασκευή περιεχομένου και η μαζική διάδοσή του αποτελούν ενιαία στρατηγική διαδικασία. Το κρίσιμο στοιχείο δεν είναι μόνο η παραγωγή ενός ψευδούς μηνύματος, αλλά η δυνατότητα να αποκτήσει άμεση εμβέλεια, να ενισχυθεί τεχνητά και να επιδράσει στο πληροφοριακό περιβάλλον πριν υπάρξει οργανωμένη αντίδραση (Chesney and Citron, 2019).

Τα deepfakes λειτουργούν κυρίως ως περιεχόμενο υψηλού συμβολικού φορτίου. Ένα πειστικό συνθετικό βίντεο ή μια αλλοιωμένη δήλωση μπορεί να προκαλέσει ισχυρή εντύπωση, επειδή αξιοποιεί την οπτικοακουστική διάσταση της επικοινωνίας. Σε περιόδους κρίσης, η εικόνα συχνά αποκτά αυξημένο βάρος, καθώς γίνεται αντιληπτή ως άμεση απόδειξη ενός γεγονότος. Ωστόσο, ακόμη και το πιο εντυπωσιακό deepfake έχει περιορισμένη στρατηγική αξία εάν παραμείνει απομονωμένο ή εάν η διάδοσή του είναι αργή και ελεγχόμενη. Εδώ ακριβώς παρεμβαίνουν τα bots, τα οποία προσφέρουν το στοιχείο της κλίμακας και του ρυθμού (Twomeyetal 2023). Τα bots λειτουργούν ως μηχανισμός πολλαπλασιασμού. Μέσα από αυτοματοποιημένη αναπαραγωγή, διαμοιρασμό και ενίσχυση συγκεκριμένου υλικού, μπορούν να μετατρέψουν ένα deepfake από μεμονωμένο περιστατικό σε ευρύτερο πληροφοριακό γεγονός. Η στρατηγική αξία του συνδυασμού έγκειται στο ότι η τεχνητή διάδοση δημιουργεί την αίσθηση ότι το περιεχόμενο αποτελεί κεντρικό σημείο δημόσιας συζήτησης. Έτσι, το deepfake δεν παρουσιάζεται απλώς ως ψευδής εικόνα, αλλά ως αφήγημα που φαίνεται να επιβεβαιώνεται από την ίδια τη δυναμική της πλατφόρμας (Mariglianoetal 2024).

Η συνδυαστική αυτή πρακτική ενισχύει και το φαινόμενο της χρονικής πίεσης. Σε ένα ψηφιακό περιβάλλον όπου η πληροφορία κυκλοφορεί με ταχύτητα, οι πρώτες ώρες διάδοσης ενός μηνύματος είναι συχνά καθοριστικές. Τα bots μπορούν να επιταχύνουν τη διάχυση ενός deepfake τόσο γρήγορα, ώστε οι μηχανισμοί επαλήθευσης να ακολουθούν εκ των υστέρων. Ακόμη και αν το περιεχόμενο αποκαλυφθεί ως κατασκευασμένο, η αρχική εντύπωση μπορεί να έχει ήδη προκαλέσει σύγχυση ή να έχει συμβάλει στη διαμόρφωση προσωρινών αντιλήψεων (Geisslеretal.2023). Επιπλέον, ο συνδυασμός deepfakes και bots επιτρέπει την προσαρμογή της επιρροής σε διαφορετικά ακροατήρια. Ένα συνθετικό βίντεο μπορεί να σχεδιαστεί με στόχο ένα συγκεκριμένο μήνυμα, ενώ τα δίκτυα αυτοματοποιημένης διάδοσης μπορούν να το

κατευθύνουν σε ομάδες με διαφορετικές πολιτισμικές ή πολιτικές ευαισθησίες. Η στρατηγική παραπληροφόρηση αποκτά έτσι χαρακτηριστικά στοχευμένης επιχείρησης, όπου το ίδιο περιεχόμενο μπορεί να πλαισιωθεί με διαφορετικούς τρόπους ανάλογα με το κοινό στο οποίο απευθύνεται (Shenetal. 2023).

Η χρήση αυτών των εργαλείων ως «πακέτο» επιρροής έχει επίσης σημαντικές επιπτώσεις στο επίπεδο της εμπιστοσύνης. Όταν ένα deepfake διακινείται ευρέως μέσω αυτοματοποιημένων δικτύων, δεν στοχεύει μόνο στη διάδοση ενός ψεύδους, αλλά στη δημιουργία ενός ευρύτερου κλίματος αμφιβολίας. Η συνεχής παρουσία συνθετικού περιεχομένου ενισχύει την αντίληψη ότι η πληροφορία είναι αναξιόπιστη, γεγονός που μπορεί να οδηγήσει σε γενικευμένη δυσπιστία προς τα μέσα ενημέρωσης, τους θεσμούς ή ακόμη και προς αυθεντικά τεκμήρια. Με αυτόν τον τρόπο, η επιρροή δεν περιορίζεται στο ψευδές περιεχόμενο, αλλά επεκτείνεται στη σταδιακή διάβρωση της ίδιας της δυνατότητας συλλογικής διάκρισης του πραγματικού (Tsotniashvili 2024, 54–65). Στον πόλεμο Ρωσίας–Ουκρανίας, η στρατηγική σημασία του συνδυασμού deepfakes και bots συνδέεται και με τη διεθνή διάσταση της σύγκρουσης. Οι επιχειρήσεις παραπληροφόρησης δεν αποσκοπούν αποκλειστικά στην εσωτερική αποσταθεροποίηση, αλλά και στη διαμόρφωση διεθνών αφηγημάτων, τα οποία επηρεάζουν συμμαχίες, πολιτικές αποφάσεις και τη στήριξη τρίτων κρατών. Η ικανότητα δημιουργίας και μαζικής διάχυσης περιεχομένου επιτρέπει σε έναν δρών να παρέμβει στο παγκόσμιο πληροφοριακό πεδίο, επιχειρώντας να καθορίσει τον τρόπο με τον οποίο η σύγκρουση γίνεται αντιληπτή (Littell and Starck, 2023).

5.1.4 Στρατηγικές επιπτώσεις

Η χρήση deepfakes και bots στον πόλεμο Ρωσίας–Ουκρανίας δεν αποτελεί απλώς ένα τεχνολογικό φαινόμενο της ψηφιακής εποχής, αλλά συνιστά εργαλείο με σαφείς στρατηγικές επιπτώσεις. Η σημασία τους δεν περιορίζεται στο επίπεδο της επικοινωνίας ή της ενημέρωσης, αλλά επεκτείνεται σε κρίσιμες παραμέτρους της σύγκρουσης, όπως το ηθικό των κοινωνιών, η θεσμική σταθερότητα και η ίδια η διαδικασία λήψης αποφάσεων. Η παραπληροφόρηση μέσω τέτοιων μέσων λειτουργεί ως μορφή πίεσης που διαμορφώνει το πληροφοριακό περιβάλλον μέσα στο οποίο εξελίσσεται ο πόλεμος (Ahmed 2023, 1108–1129).

Μία από τις πρώτες και πιο άμεσες στρατηγικές συνέπειες αφορά το ηθικό και την ψυχολογική ανθεκτικότητα των κοινωνιών. Σε συνθήκες πολέμου, η εμπιστοσύνη σε θεσμούς, η αίσθηση συνοχής και η αντίληψη της πραγματικότητας αποτελούν κρίσιμους παράγοντες

επιβίωσης και αντίστασης. Ένα deepfake που παρουσιάζει έναν ηγέτη να καλεί σε παράδοση ή ένα κύμα αυτοματοποιημένων μηνυμάτων που ενισχύουν την αίσθηση ήττας μπορεί να στοχεύσει ακριβώς σε αυτό το επίπεδο: στη δημιουργία στιγμιαίας αποδιοργάνωσης και συναισθηματικής αβεβαιότητας. Ακόμη και αν τέτοιες προσπάθειες δεν είναι διαρκώς επιτυχημένες, η πρόθεσή τους είναι να διαβρώσουν την ψυχική σταθερότητα και να ενισχύσουν το αίσθημα φόβου ή σύγχυσης (Kloo, Cruickshank, and Carley 2024, 839–850). Παράλληλα, οι στρατηγικές επιπτώσεις επεκτείνονται στη δημόσια σφαίρα και στη συνοχή της κοινωνικής πληροφόρησης. Η μαζική κυκλοφορία παραπλανητικού υλικού μπορεί να οδηγήσει σε ένα περιβάλλον όπου πολλαπλές, αντικρουόμενες εκδοχές της πραγματικότητας συνυπάρχουν ταυτόχρονα. Η συνέπεια δεν είναι μόνο η παραπλάνηση, αλλά η δυσκολία συλλογικής συμφωνίας γύρω από το τι συμβαίνει. Σε τέτοιες συνθήκες, η κοινωνία δεν αποσταθεροποιείται μόνο από το ψέμα, αλλά από την απώλεια ενός κοινού πλαισίου ερμηνείας. Η πληροφοριακή σύγχυση λειτουργεί έτσι ως μέσο στρατηγικής φθοράς (Geisslеretal 2023).

Ιδιαίτερη βαρύτητα αποκτούν οι επιπτώσεις στο θεσμικό επίπεδο. Οι κρατικοί μηχανισμοί ασφαλείας και λήψης αποφάσεων βασίζονται στην αξιοπιστία της πληροφόρησης που λαμβάνουν. Όταν το πληροφοριακό περιβάλλον κατακλύζεται από συνθετικό περιεχόμενο ή από οργανωμένα δίκτυα διάδοσης παραπλάνησης, η διαδικασία αξιολόγησης απειλών καθίσταται δυσχερέστερη. Η ανάγκη συνεχούς επαλήθευσης επιβραδύνει τις αντιδράσεις, ενώ η πιθανότητα εξαπάτησης μπορεί να δημιουργήσει υπερβολική επιφυλακτικότητα απέναντι ακόμη και σε αυθεντικές πληροφορίες. Έτσι, η παραπληροφόρηση δεν στοχεύει απλώς την κοινωνία, αλλά τον ίδιο τον μηχανισμό στρατηγικής κρίσης (Krawczyk and Wiśnicki 2022, 278–286)

Οι στρατηγικές επιπτώσεις είναι εμφανείς και στο επίπεδο της διεθνούς πολιτικής και της νομιμοποίησης. Ο πόλεμος Ρωσίας–Ουκρανίας δεν διεξάγεται μόνο στο στρατιωτικό πεδίο, αλλά και στο πεδίο της διεθνούς κοινής γνώμης, όπου η υποστήριξη ή η κόπωση τρίτων κρατών μπορεί να επηρεάσει τις εξελίξεις. Η διάδοση deepfakes ή η αυτοματοποιημένη προώθηση αφηγημάτων μπορεί να στοχεύσει στη διαμόρφωση διεθνών αντιλήψεων, στην αποδυνάμωση της συμπάθειας προς την Ουκρανία ή στη δημιουργία αμφιβολιών σχετικά με την αξιοπιστία των πηγών ενημέρωσης. Η πληροφοριακή επιρροή αποκτά έτσι διπλωματική σημασία, καθώς τα αφηγήματα μπορούν να επηρεάσουν πολιτικές αποφάσεις σε παγκόσμιο επίπεδο (Horowitz and Kahn 2024, 1-14). Επιπλέον, η στρατηγική χρήση αυτών των εργαλείων επιδρά στη δυναμική της αποτροπής και της κλιμάκωσης. Σε ένα περιβάλλον όπου η πληροφορία μπορεί

να παραποιηθεί, ο υπολογισμός του κινδύνου γίνεται πιο περίπλοκος. Ένα ψευδές ή αλλοιωμένο γεγονός μπορεί να ερμηνευθεί ως πραγματική πρόκληση, οδηγώντας σε βιαστικές αντιδράσεις ή σε απρόβλεπτη κλιμάκωση. Αντίστοιχα, η αμφιβολία σχετικά με το τι είναι αυθεντικό μπορεί να επιβραδύνει την ανταπόκριση σε πραγματικές απειλές. Κατ' αυτόν τον τρόπο, η παραπληροφόρηση ενσωματώνεται στη στρατηγική αβεβαιότητα, επηρεάζοντας την ισορροπία αποφάσεων σε κρίσιμες στιγμές (Au, Ho, and Chiu 2022, 1331–1354).

Τέλος, οι επιπτώσεις αυτές δεν εξαντλούνται στη διάρκεια της σύγκρουσης, αλλά αφήνουν μακροπρόθεσμο αποτύπωμα. Η σταδιακή διάβρωση της εμπιστοσύνης σε πληροφορίες, θεσμούς και δημόσιο διάλογο μπορεί να επιβιώσει μετά το τέλος των επιχειρήσεων, δημιουργώντας βαθύτερα ρήγματα στη συλλογική αντίληψη και στην πολιτική σταθερότητα. Η παραπληροφόρηση μέσω τεχνολογιών όπως τα deepfakes και τα bots, επομένως, δεν λειτουργεί μόνο ως τακτικό εργαλείο στιγμιαίας πίεσης, αλλά ως στρατηγικός μηχανισμός που μπορεί να επηρεάσει θεσμούς, κοινωνίες και αποφάσεις σε βάθος χρόνου (Tyushka 2022, 115–135).

5.1.5 Όρια και αντιδράσεις

Παρότι οι τεχνολογίες παραπληροφόρησης, όπως τα deepfakes και τα αυτοματοποιημένα δίκτυα bots, ενισχύουν σημαντικά τις δυνατότητες επιρροής στο ψηφιακό πεδίο, η αποτελεσματικότητά τους δεν είναι απόλυτη ούτε δεδομένη. Η παραπληροφόρηση δεν λειτουργεί σε κενό· συναντά θεσμικές αντιδράσεις, κοινωνικές άμυνες και τεχνολογικούς περιορισμούς που μπορούν να μειώσουν την επιρροή της. Ο πόλεμος Ρωσίας–Ουκρανίας προσφέρει χαρακτηριστικά παραδείγματα όπου, παρά την ένταση των πληροφοριακών επιχειρήσεων, η στρατηγική τους απόδοση δεν υπήρξε πάντα αντίστοιχη των προσδοκιών (Moon and Kahlor 2025).

Ένα πρώτο όριο αφορά την ίδια την αξιοπιστία του περιεχομένου. Τα deepfakes, όσο εντυπωσιακά και αν είναι ως τεχνολογία, δεν επιτυγχάνουν πάντοτε υψηλή πειστικότητα. Σε πολλές περιπτώσεις, η τεχνική ατέλεια ή η ασυνέπεια του υλικού καθιστά το ψεύδος εμφανές, ιδιαίτερα όταν πρόκειται για πρόσωπα υψηλής δημοσιότητας ή για γεγονότα που παρακολουθούνται στενά. Στον πόλεμο Ρωσίας–Ουκρανίας, το γνωστό παράδειγμα του πλαστού βίντεο με τον πρόεδρο Ζελένσκι αποδομήθηκε σχετικά γρήγορα, γεγονός που δείχνει ότι η επιτυχία ενός deepfake δεν εξαρτάται μόνο από την παραγωγή του, αλλά και από το πόσο εύκολα μπορεί να εντοπιστεί και να διαψευστεί (Kandari, Tripathi, and Pant 2023, 392–395).

Ένα δεύτερο όριο σχετίζεται με την αυξανόμενη θεσμική εγρήγορση. Η εμπειρία των τελευταίων ετών έχει οδηγήσει κυβερνήσεις, μέσα ενημέρωσης και οργανισμούς ασφαλείας στην ανάπτυξη μηχανισμών ανίχνευσης και αντιμετώπισης ψηφιακής παραπληροφόρησης. Στην ουκρανική περίπτωση, η ύπαρξη προϋπάρχουσας εμπειρίας από προηγούμενες ρωσικές επιχειρήσεις επιρροής συνέβαλε στην ταχύτερη αναγνώριση ψευδών αφηγημάτων και στην πιο άμεση αντίδραση. Η ανθεκτικότητα δεν προκύπτει μόνο από τεχνολογία, αλλά από θεσμική προετοιμασία και συντονισμό επικοινωνιακών μηχανισμών (Borzetal. 2024, 709–729). Παράλληλα, οι ίδιες οι πλατφόρμες κοινωνικής δικτύωσης έχουν αρχίσει να παίζουν πιο ενεργό ρόλο στη διαχείριση συντονισμένων επιχειρήσεων. Αν και οι περιορισμοί είναι εμφανείς, η απομάκρυνση δικτύων bots, η επισήμανση παραπλανητικού περιεχομένου και οι πολιτικές κατά της συντονισμένης μη αυθεντικής συμπεριφοράς αποτελούν μορφές αντίδρασης που περιορίζουν την ανεξέλεγκτη διάδοση. Αυτό δεν σημαίνει ότι η παραπληροφόρηση εξαφανίζεται, αλλά ότι η αποτελεσματικότητά της μπορεί να μειωθεί όταν ενεργοποιούνται μηχανισμοί επιτήρησης και παρέμβασης (Borzetal. 2024; Moon and Kahlor 2025).

Ένα ακόμη κρίσιμο στοιχείο είναι η κοινωνική προσαρμογή. Όσο περισσότερο οι πολίτες εξοικειώνονται με την πιθανότητα εξαπάτησης, τόσο περισσότερο αναπτύσσουν επιφυλακτικότητα απέναντι σε εντυπωσιακά ή ακραία μηνύματα. Η παραπληροφόρηση μπορεί να λειτουργήσει ισχυρά σε περιβάλλοντα αιφνιδιασμού, όμως με την πάροδο του χρόνου δημιουργείται μια μορφή συλλογικής ανοσίας, ιδιαίτερα όταν υπάρχουν ισχυρές εναλλακτικές πηγές ενημέρωσης και αξιόπιστοι θεσμοί επαλήθευσης. Στην ουκρανική κοινωνία, η εμπειρία συνεχούς πληροφοριακής πίεσης φαίνεται να ενίσχυσε βαθμιαία την κριτική στάση απέναντι σε ύποπτο περιεχόμενο (Luetal. 2023). Τα όρια αυτά, ωστόσο, δεν συνεπάγονται ότι η παραπληροφόρηση παύει να αποτελεί απειλή. Αντιθέτως, αναδεικνύουν ότι πρόκειται για πεδίο διαρκούς αλληλεπίδρασης ανάμεσα σε επιτιθέμενους και αμυνόμενους μηχανισμούς. Η επιτυχία της παραπληροφόρησης εξαρτάται από τη συγκυρία, την ποιότητα της εκτέλεσης, το επίπεδο κοινωνικής εμπιστοσύνης και τη θεσμική ανθεκτικότητα. Σε ορισμένες περιπτώσεις, ακόμη και αποτυχημένες προσπάθειες μπορούν να παράγουν έμμεσες συνέπειες, όπως τη γενικότερη καλλιέργεια δυσπιστίας ή την ενίσχυση της σύγχυσης (Nabilaetal. 2025, 916–923).

Ιδιαίτερα σημαντικό είναι το γεγονός ότι η ύπαρξη deepfakes μπορεί να δημιουργήσει ένα νέο είδος αμφισβήτησης: όχι μόνο του ψεύδους, αλλά και της αλήθειας. Όταν η κοινωνία γνωρίζει ότι οπτικοακουστικό υλικό μπορεί να είναι κατασκευασμένο, καθίσταται ευκολότερο για δρώντες να αρνούνται πραγματικά γεγονότα ή να καθυστερούν την απόδοση ευθύνης,

επικαλούμενοι πιθανή αλλοίωση. Έτσι, ακόμη και όταν η παραπληροφόρηση δεν πείθει, μπορεί να λειτουργεί ως μηχανισμός αποσταθεροποίησης της εμπιστοσύνης στο αποδεικτικό υλικό (Janzen 2024, 211–214).

5.2 Ψηφιακές επιχειρήσεις επιρροής της Κίνας στην Ταϊβάν

Η Ταϊβάν αποτελεί ένα από τα πλέον χαρακτηριστικά παραδείγματα σύγχρονου πεδίου ψηφιακών επιχειρήσεων επιρροής, καθώς βρίσκεται στο επίκεντρο μιας μακροχρόνιας στρατηγικής αντιπαράθεσης με την Κίνα. Σε αντίθεση με περιπτώσεις όπου η παραπληροφόρηση εμφανίζεται αποσπασματικά, στο ταϊβανέζικο πλαίσιο παρατηρείται μια συστηματική και πολυεπίπεδη προσπάθεια διαμόρφωσης του πληροφοριακού περιβάλλοντος, η οποία συνδέεται άμεσα με ευρύτερους πολιτικούς στόχους. Οι επιχειρήσεις αυτές δεν περιορίζονται στη διάδοση ψευδών ειδήσεων, αλλά λειτουργούν ως μορφή γνωστικής και πολιτικής πίεσης, επιδιώκοντας να επηρεάσουν αντιλήψεις, θεσμική εμπιστοσύνη και κοινωνική συνοχή (Jaw-Nian 2023, 143–170). Η στρατηγική σημασία της Ταϊβάν για την Κίνα καθιστά το νησί ένα ιδιαίτερα ευαίσθητο πεδίο επιρροής. Οι ψηφιακές επιχειρήσεις που στοχεύουν την Ταϊβάν εντάσσονται σε μια λογική υβριδικής αντιπαράθεσης, όπου η χρήση στρατιωτικής ισχύος συνυπάρχει με πληροφοριακές και ψυχολογικές μεθόδους. Το ζητούμενο δεν είναι απαραίτητα η άμεση αλλαγή πολιτικής κατεύθυνσης, αλλά η σταδιακή δημιουργία ενός περιβάλλοντος αβεβαιότητας, πόλωσης και δυσπιστίας προς τους θεσμούς, το οποίο διευκολύνει την άσκηση πίεσης σε βάθος χρόνου (Huang 2024, 121–136).

Ιδιαίτερα έντονη ήταν η δραστηριοποίηση πληροφοριακών επιχειρήσεων ενόψει των προεδρικών εκλογών του 2020. Αναλύσεις έχουν επισημάνει ότι κατά την προεκλογική περίοδο παρατηρήθηκε αυξημένη διάδοση αφηγημάτων που αμφισβητούσαν την αξιοπιστία των υποψηφίων, υπονόμευαν τη δημοκρατική διαδικασία και ενίσχυαν την εικόνα αναπόφευκτης σύγκρουσης ή «μοιραίας» επανένωσης. Το περιεχόμενο αυτό συχνά εμφανιζόταν ως προϊόν εσωτερικής κοινωνικής δυσαρέσκειας, ενώ στην πραγματικότητα εντασσόταν σε συντονισμένες πρακτικές χειραγώγησης (Ferenczy 2024, 83–110). Κεντρικό χαρακτηριστικό των κινεζικών επιχειρήσεων επιρροής είναι η αξιοποίηση ενός ευρέος φάσματος τεχνικών που εκτείνονται πέρα από την κλασική παραπληροφόρηση. Δεν πρόκειται μόνο για ψευδή δημοσιεύματα, αλλά για δημιουργία πληροφοριακού «θορύβου», υπερπληθώρα αντιφατικών μηνυμάτων και καλλιέργεια δυσπιστίας. Η στρατηγική αυτή δεν επιδιώκει πάντοτε να πείσει, αλλά να καταστήσει δυσκολότερη τη διάκριση αλήθειας και ψεύδους, δημιουργώντας ένα κλίμα

κόπωσης και αμφιβολίας (Hung and Hung 2022).

Η Ταϊβάν έχει επίσης αναφέρει αυξημένη χρήση πρακτικών όπως η πλαστοπροσωπία και η υποκλοπή ταυτότητας στο ψηφιακό περιβάλλον. Σύμφωνα με εκθέσεις των ταϊβανέζικων αρχών, έχουν εντοπιστεί περιπτώσεις όπου λογαριασμοί ή πλατφόρμες χρησιμοποιήθηκαν για τη διάδοση ψευδών πληροφοριών μέσω υποδυόμενων στρατιωτικών ή κρατικών προσώπων, με στόχο τη δημιουργία δυσπιστίας στο εσωτερικό της κοινωνίας και ιδιαίτερα απέναντι στις ένοπλες δυνάμεις. Αυτού του τύπου οι επιχειρήσεις επιβεβαιώνουν ότι η πληροφορία αξιοποιείται ως εργαλείο αποσταθεροποίησης σε κρίσιμες στιγμές (Kazim 2025, 433–442). Ένα ακόμη στοιχείο που ενισχύει την αποτελεσματικότητα των επιχειρήσεων επιρροής είναι η χρήση αυτοματοποιημένων δικτύων και ψευδών λογαριασμών, τα οποία αναπαράγουν μαζικά συγκεκριμένα αφηγήματα. Με αυτόν τον τρόπο δημιουργείται η αίσθηση κοινωνικής δυναμικής και «συναίνεσης», η οποία μπορεί να επηρεάσει την πρόσληψη της πληροφορίας από τους πολίτες. Η στρατηγική αξία δεν έγκειται μόνο στο περιεχόμενο, αλλά στην τεχνητή ενίσχυση της ορατότητας και στη διαμόρφωση ενός παραμορφωμένου δημόσιου διαλόγου (Lee 2024).

Η κινεζική προσέγγιση στην Ταϊβάν έχει συχνά χαρακτηριστεί ως μορφή «γνωστικού πολέμου», καθώς στοχεύει άμεσα στο επίπεδο της αντίληψης και της ψυχολογικής ανθεκτικότητας. Η προσπάθεια υπονόμευσης της εμπιστοσύνης στους θεσμούς, η διάβρωση της κοινωνικής συνοχής και η ενίσχυση της πολιτικής πόλωσης αποτελούν αποτελέσματα που δεν επιτυγχάνονται μέσω στρατιωτικής ισχύος, αλλά μέσω διαχείρισης της πληροφορίας. Αυτή η λογική αναδεικνύει ότι οι επιχειρήσεις επιρροής λειτουργούν ως μέθοδος επιβολής σε περιβάλλοντα όπου η ανοιχτή σύγκρουση δεν είναι άμεσα επιθυμητή (Lin 2023, 37–54). Παράλληλα, η Ταϊβάν έχει αναπτύξει σημαντικές μορφές αντίδρασης και ανθεκτικότητας. Η εμπειρία της ως στόχος παραπληροφόρησης έχει οδηγήσει σε θεσμικούς μηχανισμούς επαλήθευσης, ενίσχυση της ψηφιακής παιδείας και ταχύτερη δημόσια διάψευση ψευδών αφηγημάτων. Παρότι η απειλή παραμένει, το ταϊβανέζικο παράδειγμα δείχνει ότι η αντιμετώπιση των επιχειρήσεων επιρροής δεν είναι αδύνατη, αλλά απαιτεί συνδυασμό τεχνολογικής ετοιμότητας και κοινωνικής εγρήγορσης (Huang 2024, 121–136).

5.3 Παρεμβάσεις μέσω AI σε ευρωπαϊκές εκλογές

Οι ευρωπαϊκές εκλογικές διαδικασίες των τελευταίων ετών έχουν αναδειχθεί σε ιδιαίτερα ευαίσθητο πεδίο ψηφιακής επιρροής, καθώς η πολιτική νομιμοποίηση και η κοινωνική

συνοχή εξαρτώνται σε μεγάλο βαθμό από την αξιοπιστία της πληροφόρησης. Η τεχνητή νοημοσύνη προσθέτει μια νέα διάσταση σε αυτό το περιβάλλον, διότι επιτρέπει την παραγωγή πειστικών ψευδών δηλώσεων, αλλοιωμένων οπτικοακουστικών τεκμηρίων και στοχευμένων αφηγημάτων που μπορούν να επηρεάσουν την αντίληψη των ψηφοφόρων. Οι παρεμβάσεις αυτές δεν στοχεύουν πάντα στην άμεση μεταβολή του εκλογικού αποτελέσματος, αλλά στη διάβρωση της εμπιστοσύνης, στην ενίσχυση της πόλωσης και στη σταδιακή αποσταθεροποίηση του δημοκρατικού πλαισίου (VaccariandChadwick, 2020).

Η στρατηγική σημασία των εκλογών ως στόχος παραπληροφόρησης είναι προφανής: αποτελούν την κορυφαία στιγμή πολιτικής επιλογής, κατά την οποία η κοινωνία διαμορφώνει την πολιτική της κατεύθυνση. Σε αυτό το πλαίσιο, η παραπληροφόρηση μέσω AI λειτουργεί ως εργαλείο παρέμβασης στη διαδικασία σχηματισμού πολιτικής κρίσης. Η παραγωγή συνθετικών δηλώσεων ή ψευδών βίντεο μπορεί να δημιουργήσει στιγμιαία εντύπωση σκανδάλου, να πλήξει την αξιοπιστία πολιτικών προσώπων ή να ενισχύσει συγκεκριμένες ερμηνείες της πραγματικότητας πριν υπάρξει δυνατότητα επαλήθευσης (Calderón, Sierra, and Bermejo-Casado 2025, 58–83).

Ένα χαρακτηριστικό στοιχείο των παρεμβάσεων μέσω AI είναι η δημιουργία ψευδών δηλώσεων που αποδίδονται σε πολιτικούς ή θεσμικούς φορείς. Τα συνθετικά αυτά μηνύματα δεν χρειάζεται να είναι πλήρως πειστικά για να είναι αποτελεσματικά. Συχνά αρκεί να προκαλέσουν αμφιβολία ή να ενεργοποιήσουν συναισθηματικές αντιδράσεις, ιδιαίτερα όταν διακινούνται σε προεκλογικές περιόδους έντασης. Σε τέτοιες συνθήκες, η διάψευση μπορεί να ακολουθήσει, αλλά το αρχικό επικοινωνιακό αποτύπωμα έχει ήδη παραχθεί (Romanishynetal. 2025). Παράλληλα, η τεχνητή νοημοσύνη επιτρέπει τη μαζική παραγωγή παραπλανητικού περιεχομένου προσαρμοσμένου σε διαφορετικά ακροατήρια. Σε αντίθεση με την παραδοσιακή προπαγάνδα, όπου το μήνυμα ήταν σχετικά ενιαίο, οι σύγχρονες τεχνικές επιτρέπουν μικρο-στοχευμένες παρεμβάσεις που εκμεταλλεύονται πολιτισμικά, ιδεολογικά ή κοινωνικά χαρακτηριστικά. Η χειραγώγηση δεν επιδιώκει να πείσει το σύνολο του εκλογικού σώματος, αλλά να ενισχύσει συγκεκριμένες διαιρέσεις ή να αποθαρρύνει ομάδες ψηφοφόρων, δημιουργώντας ένα πιο κατακερματισμένο πολιτικό περιβάλλον (Tache 2023, 121–132).

Η χειραγώγηση δημόσιας εικόνας αποτελεί επίσης κεντρικό στόχο. Η πολιτική αξιοπιστία και η προσωπική υπόσταση των υποψηφίων μπορούν να πληγούν μέσω συνθετικών βίντεο ή αλλοιωμένων ηχητικών αποσπασμάτων που παρουσιάζουν δηλώσεις εκτός πλαισίου ή

γεγονότα που δεν συνέβησαν ποτέ. Ακόμη και όταν τέτοιο υλικό αποκαλύπτεται ως ψευδές, η ύπαρξή του μπορεί να διαβρώσει την εμπιστοσύνη στην αυθεντικότητα της πολιτικής επικοινωνίας συνολικά. Το αποτέλεσμα δεν είναι μόνο η απαξίωση ενός προσώπου, αλλά η γενικότερη αμφισβήτηση της δυνατότητας διάκρισης του αληθούς (Bradshawetal. 2021). Στο ευρωπαϊκό πλαίσιο, οι παρεμβάσεις αυτές έχουν ιδιαίτερη βαρύτητα λόγω της πολυπλοκότητας των πολιτικών συστημάτων και της σημασίας των υπερεθνικών θεσμών. Εκλογικές διαδικασίες για το Ευρωπαϊκό Κοινοβούλιο ή για κυβερνήσεις κρατών-μελών συνδέονται με κρίσιμες αποφάσεις για την ασφάλεια, την οικονομία και τη γεωπολιτική θέση της Ευρώπης. Συνεπώς, η αποσταθεροποίηση μέσω παραπληροφόρησης δεν αφορά μόνο εσωτερικά πολιτικά ζητήματα, αλλά μπορεί να έχει επιπτώσεις στη συνολική στρατηγική συνοχή της Ένωσης (Farooqetal. 2025). Ένα ακόμη χαρακτηριστικό των AI-υποβοηθούμενων παρεμβάσεων είναι η δυσκολία απόδοσης ευθύνης. Η παραγωγή ψευδούς περιεχομένου μπορεί να πραγματοποιηθεί από κρατικούς ή μη κρατικούς δρώντες, ενώ η διάδοσή του συχνά γίνεται μέσα από αποκεντρωμένα δίκτυα που δυσχεραίνουν την ανίχνευση της προέλευσης. Αυτό καθιστά τις απαντήσεις πιο περίπλοκες, διότι δεν είναι πάντα σαφές ποιος βρίσκεται πίσω από μια εκστρατεία επιρροής και ποιοι είναι οι πολιτικοί της στόχοι (Vasistetal.2024).

Παράλληλα, η ύπαρξη deepfakes και συνθετικού υλικού δημιουργεί μια νέα μορφή πολιτικής αβεβαιότητας: ακόμη και αυθεντικές δηλώσεις μπορούν να αμφισβητηθούν ως πιθανώς κατασκευασμένες. Αυτό ενισχύει μια κατάσταση όπου η αλήθεια γίνεται αντικείμενο πολιτικής διαμάχης και όχι κοινό σημείο αναφοράς. Σε τέτοιες συνθήκες, οι θεσμοί αντιμετωπίζουν όχι μόνο την ανάγκη διάψευσης ψευδών ειδήσεων, αλλά και τη δυσκολία διατήρησης ενός ελάχιστου επιπέδου εμπιστοσύνης στο δημόσιο λόγο (Saeva and Tasheva 2024, 226–234). Η ευρωπαϊκή αντίδραση σε αυτές τις προκλήσεις περιλαμβάνει προσπάθειες κανονιστικής ρύθμισης, μηχανισμούς παρακολούθησης και ενίσχυση της ψηφιακής παιδείας. Ωστόσο, το πρόβλημα παραμένει ιδιαίτερα σύνθετο, καθώς οι τεχνολογίες εξελίσσονται ταχύτερα από τα θεσμικά εργαλεία αντιμετώπισης. Η προστασία των εκλογών δεν αφορά μόνο τεχνικά μέτρα, αλλά και την ενίσχυση της κοινωνικής ανθεκτικότητας απέναντι σε παραπλανητικά αφηγήματα. (AngwaldnandWagnsson, 2024).

5.4 Σύνοψη Κεφαλαίου

Το πέμπτο κεφάλαιο επικεντρώθηκε σε χαρακτηριστικά παραδείγματα σύγχρονων επιχειρήσεων παραπληροφόρησης όπου η τεχνητή νοημοσύνη αξιοποιείται ως εργαλείο

στρατηγικής επιρροής. Αρχικά εξετάστηκε ο πόλεμος Ρωσίας–Ουκρανίας, στον οποίο η χρήση deepfakes και αυτοματοποιημένων δικτύων ανέδειξε τη δυνατότητα πρόκλησης σύγχυσης και ψυχολογικής πίεσης σε κοινωνίες και θεσμούς. Στη συνέχεια αναλύθηκε η περίπτωση της Ταϊβάν, όπου οι ψηφιακές επιχειρήσεις της Κίνας στοχεύουν στη διαμόρφωση αβεβαιότητας και στη σταδιακή υπονόμευση της εμπιστοσύνης στο δημοκρατικό σύστημα. Τέλος, παρουσιάστηκαν παρεμβάσεις σε ευρωπαϊκές εκλογικές διαδικασίες, μέσα από ψευδείς δηλώσεις και συνθετικό περιεχόμενο που επηρεάζουν την πολιτική εικόνα και τη δημόσια κρίση. Συνολικά, το κεφάλαιο ανέδειξε ότι η πληροφορία έχει μετατραπεί σε πεδίο σύγκρουσης, όπου η τεχνολογία ενισχύει τη δυνατότητα χειραγώγησης της αντίληψης σε διεθνές επίπεδο.

Κεφάλαιο 6ο Θεσμικές και Πολιτικές Αντιδράσεις στη Ψηφιακή Απειλή

6.1 Προκλήσεις για κράτη και διεθνείς θεσμούς

Η άνοδος της τεχνητής νοημοσύνης και η ενσωμάτωσή της σε πρακτικές παραπληροφόρησης και επιχειρήσεων επιρροής δημιουργούν ένα σύνολο προκλήσεων που υπερβαίνουν τα στενά όρια της τεχνικής κυβερνοασφάλειας. Τα κράτη και οι διεθνείς θεσμοί καλούνται να αντιμετωπίσουν απειλές που δεν εκδηλώνονται μόνο ως παραβιάσεις συστημάτων, αλλά ως σταδιακή αλλοίωση της αντίληψης, της εμπιστοσύνης και της πολιτικής σταθερότητας. Η δυσκολία έγκειται στο ότι οι επιθέσεις αυτές κινούνται συχνά κάτω από το κατώφλι της παραδοσιακής σύγκρουσης, ενώ ταυτόχρονα μπορούν να παράγουν ουσιαστικά στρατηγικά αποτελέσματα (Mayer 2023, 1–19).

Μία από τις βασικότερες προκλήσεις αφορά την αβεβαιότητα ως προς την προέλευση και την απόδοση ευθύνης. Στο ψηφιακό περιβάλλον, οι επιχειρήσεις παραπληροφόρησης μπορούν να οργανωθούν με τρόπους που αποκρύπτουν τον πραγματικό δρώντα, αξιοποιώντας ενδιάμεσους, ιδιωτικές υποδομές, πλατφόρμες ή δίκτυα λογαριασμών που μιμούνται «αυθόρμητη» κοινωνική συμπεριφορά. Η τεχνητή νοημοσύνη ενισχύει αυτή την αμφισημία, καθώς επιτρέπει την παραγωγή περιεχομένου που φαίνεται οργανικό, πολλαπλό και χρονικά συγχρονισμένο, χωρίς να απαιτεί ανθρώπινη συμμετοχή σε αντίστοιχη κλίμακα. Για τα κράτη, η δυσκολία απόδοσης ευθύνης επηρεάζει άμεσα την αποτροπή, επειδή η αποτροπή προϋποθέτει σαφή αντίπαλο και πειστική δυνατότητα ανταπόδοσης (Collett 2021, 298–317). Συναφής πρόκληση είναι η μεταβολή της έννοιας του «επεισοδίου» στην ασφάλεια. Οι πληροφοριακές επιθέσεις δεν εμφανίζονται πάντα ως μεμονωμένα γεγονότα, αλλά ως συνεχείς και πολυεπίπεδες

παρεμβάσεις. Αυτό οδηγεί σε μια κατάσταση όπου οι θεσμοί αντιμετωπίζουν μια μόνιμη πίεση, χωρίς σαφείς φάσεις έναρξης και λήξης. Η διαχείριση απειλών σε τέτοιο περιβάλλον απαιτεί διαφορετική θεσμική λογική: λιγότερο «έκτακτη», περισσότερο διαρκή και προσαρμοστική (Wigell, Mikkola, and Juntunen 2021, 12–15). Ιδιαίτερα κρίσιμη είναι η πρόκληση της ταχύτητας. Οι μηχανισμοί του κράτους και των διεθνών οργανισμών λειτουργούν συνήθως με διαδικασίες που προϋποθέτουν έλεγχο, αξιολόγηση και διαβούλευση. Αντίθετα, η παραπληροφόρηση που παράγεται ή ενισχύεται μέσω AI μπορεί να διαδοθεί σε ελάχιστο χρόνο, να προσαρμοστεί σε νέα δεδομένα και να αποκτήσει μαζική ορατότητα πριν υπάρξει θεσμική αντίδραση. Αυτό δημιουργεί ένα δομικό χάσμα ανάμεσα στον ρυθμό της απειλής και στον ρυθμό της αντιμετώπισης, με αποτέλεσμα οι αποφάσεις να λαμβάνονται συχνά υπό πίεση και αβεβαιότητα (FloresVivar 2019, 197–212). Μία ακόμη πρόκληση αφορά το ζήτημα της αξιοπιστίας των πληροφοριών ως βάση πολιτικής και επιχειρησιακής δράσης. Οι κρατικοί θεσμοί ασφαλείας στηρίζονται στην εγκυρότητα της πληροφόρησης για να εκτιμήσουν κινδύνους, να αξιολογήσουν προθέσεις και να σχεδιάσουν απαντήσεις. Όταν το πληροφοριακό περιβάλλον κατακλύζεται από συνθετικό ή παραποιημένο υλικό, η διαδικασία εκτίμησης γίνεται πιο επισφαλής. Επιπλέον, η ίδια η ύπαρξη τεχνολογιών που μπορούν να κατασκευάσουν οπτικοακουστικά τεκμήρια επιβαρύνει το αποδεικτικό πεδίο: ακόμη και πραγματικά στοιχεία μπορούν να αμφισβητηθούν, προκαλώντας καθυστέρηση ή αδυναμία λήψης αποφάσεων (DunnCavelty, Eriksen, and Scharte 2023).

Στο επίπεδο της δημοκρατικής διακυβέρνησης, οι προκλήσεις αφορούν τη σχέση ανάμεσα στην ασφάλεια και στα δικαιώματα. Η αντιμετώπιση της παραπληροφόρησης συχνά οδηγεί σε πιέσεις για αυστηρότερη εποπτεία του ψηφιακού χώρου, ενίσχυση της επιτήρησης ή περιορισμούς στην κυκλοφορία περιεχομένου. Ωστόσο, αυτές οι απαντήσεις ενδέχεται να δημιουργήσουν πολιτικό και θεσμικό κόστος, εφόσον μπορούν να εκληφθούν ως περιορισμός της ελευθερίας έκφρασης ή ως επέκταση κρατικού ελέγχου. Οι διεθνείς θεσμοί αντιμετωπίζουν εδώ ένα κλασικό δίλημμα: πώς να θωρακίσουν τη δημοκρατική διαδικασία χωρίς να υπονομεύσουν τις αρχές που την θεμελιώνουν (Holmes and Wheeler 2024, 168–170). Η πολυπλοκότητα αυξάνεται περαιτέρω λόγω του ρόλου του ιδιωτικού τομέα. Πολλές κρίσιμες ψηφιακές υποδομές, καθώς και τα βασικά κανάλια δημόσιας επικοινωνίας, ανήκουν σε ιδιωτικές εταιρείες ή λειτουργούν υπό ιδιωτική διαχείριση. Αυτό σημαίνει ότι η ασφάλεια στον ψηφιακό χώρο δεν είναι αποκλειστικά κρατική υπόθεση, αλλά απαιτεί συνεργασία και συντονισμό με εταιρείες που έχουν δικές τους προτεραιότητες, οικονομικά κίνητρα και

διαφορετικές προσεγγίσεις στη διαχείριση περιεχομένου. Οι διεθνείς θεσμοί καλούνται να δημιουργήσουν πλαίσια συνεργασίας και λογοδοσίας, χωρίς να υποκαθιστούν τις εθνικές αρμοδιότητες ή να συγκρούονται με διαφορετικά νομικά συστήματα (Castelfranchi and Falcone 2018, 70–73). Στο επίπεδο της διεθνούς ασφάλειας, μια πρόσθετη πρόκληση αφορά την έλλειψη κοινά αποδεκτών κανόνων. Ενώ υπάρχουν προσπάθειες διαμόρφωσης διεθνών προτύπων για τη συμπεριφορά στο ψηφιακό πεδίο, η παραπληροφόρηση ως μέθοδος επιρροής παραμένει δυσκολότερο να ρυθμιστεί σε σύγκριση με τις καθαρά τεχνικές επιθέσεις. Η βασική δυσκολία είναι ότι πολλές πρακτικές επιρροής κινούνται στη γκρίζα ζώνη μεταξύ νόμιμης δημόσιας διπλωματίας, πολιτικής επικοινωνίας και εχθρικής παρέμβασης. Η απουσία σαφών ορίων ευνοεί τη χρήση τέτοιων πρακτικών, καθώς το κόστος διεθνούς καταδίκης ή κυρώσεων είναι συχνά περιορισμένο (Araujo, Helberger, Kruikemeier, and de Vreese 2020, 618–620).

Τέλος, η πιο κρίσιμη πρόκληση είναι η ίδια η ανθεκτικότητα της στρατηγικής κρίσης. Η τεχνητή νοημοσύνη και η παραπληροφόρηση δεν απειλούν μόνο την υλική ασφάλεια, αλλά τον τρόπο με τον οποίο οι κοινωνίες και οι θεσμοί κατανοούν την πραγματικότητα. Όταν το πληροφοριακό περιβάλλον γίνεται πεδίο διαρκούς χειραγώγησης, οι αποφάσεις λαμβάνονται σε συνθήκες μειωμένης βεβαιότητας, ενισχυμένης πόλωσης και περιορισμένης εμπιστοσύνης. Η στρατηγική πρόκληση, επομένως, δεν είναι απλώς να αποτραπεί ένα ψεύδος, αλλά να διασφαλιστεί ότι το κράτος και οι διεθνείς θεσμοί διατηρούν την ικανότητα να λειτουργούν αποτελεσματικά σε ένα περιβάλλον αμφισβητούμενης αλήθειας (FloresVivar 2019, 197–212).

6.2 Πολιτικές και στρατηγικές ανθεκτικότητας

Η έννοια της ανθεκτικότητας έχει αποκτήσει κεντρική θέση στη σύγχρονη συζήτηση για την ασφάλεια, ιδιαίτερα σε περιβάλλοντα όπου οι απειλές δεν εκδηλώνονται ως άμεση στρατιωτική επίθεση, αλλά ως σταδιακή διάβρωση θεσμών, εμπιστοσύνης και ικανότητας λήψης αποφάσεων. Στο ψηφιακό πεδίο, η ανθεκτικότητα δεν ταυτίζεται με την απόλυτη «ασφάλεια» ή με την πλήρη εξάλειψη του κινδύνου. Περιγράφει την ικανότητα ενός κράτους, μιας κοινωνίας και των θεσμών τους να αντέχουν σε πιέσεις, να προσαρμόζονται σε επιθέσεις επιρροής και να επανακτούν λειτουργικότητα χωρίς να καταρρέουν πολιτικά ή θεσμικά. Η παραπληροφόρηση που παράγεται ή ενισχύεται μέσω τεχνητής νοημοσύνης καθιστά αυτή την προσέγγιση ιδιαίτερα αναγκαία, διότι μεταφέρει το κέντρο βάρους από την «άμυνα συστημάτων» στην προστασία της αξιοπιστίας του πληροφοριακού περιβάλλοντος (Romanishynetal 2025). Μια αποτελεσματική στρατηγική ανθεκτικότητας ξεκινά από τη σαφή

κατανόηση ότι οι επιχειρήσεις επιρροής δεν αντιμετωπίζονται με ένα μόνο εργαλείο. Απαιτείται πολυεπίπεδη πολιτική που να συνδυάζει θεσμικές διαδικασίες, τεχνολογικές δυνατότητες, κανονιστικά πλαίσια και κοινωνική συμμετοχή. Το ζητούμενο είναι να μειωθεί η πιθανότητα επιτυχίας της παραπληροφόρησης και να περιοριστεί η ζημία όταν αυτή συμβεί, χωρίς να διακυβευθούν θεμελιώδεις δημοκρατικές αρχές (Ruggiero, Piotrowicz, and John 2024).

Πρώτη κρίσιμη διάσταση είναι η θεσμική ετοιμότητα και ο συντονισμός. Σε πολλές χώρες, το βασικό πρόβλημα δεν είναι η πλήρης έλλειψη εργαλείων, αλλά η κατακερματισμένη διαχείριση. Υπηρεσίες ασφαλείας, υπουργεία, ανεξάρτητες αρχές και επικοινωνιακοί μηχανισμοί συχνά λειτουργούν με διαφορετικές προτεραιότητες, διαφορετικά πρωτόκολλα και ασύμβατους ρυθμούς απόκρισης. Η ανθεκτικότητα ενισχύεται όταν υπάρχουν σαφείς ρόλοι, ενιαία κανάλια ανταλλαγής πληροφοριών και διαδικασίες που επιτρέπουν γρήγορη αξιολόγηση και κοινή δημόσια τοποθέτηση σε περιστατικά παραπληροφόρησης. Η έλλειψη συντονισμού δημιουργεί κενά που μπορεί να αξιοποιηθούν από αντίπαλους δρώντες, ιδίως σε περιόδους κρίσης (Simchonetal. 2025).

Δεύτερη διάσταση αφορά τη διαχείριση της δημόσιας επικοινωνίας ως εργαλείο άμυνας. Σε επιχειρήσεις επιρροής, το κενό πληροφόρησης λειτουργεί υπέρ του επιτιθέμενου. Όταν οι θεσμοί καθυστερούν να ενημερώσουν, αφήνουν χώρο σε φήμες και κατασκευασμένες αφηγήσεις να παγιωθούν. Η ανθεκτικότητα ενισχύεται μέσω σταθερής, προβλέψιμης και αξιόπιστης ενημέρωσης, χωρίς υπερβολές και χωρίς πολιτική εργαλειοποίηση. Η επικοινωνία δεν πρέπει να στοχεύει μόνο στη διάψευση, αλλά και στην αποκατάσταση της εμπιστοσύνης, δηλαδή να εξηγεί τι γνωρίζεται, τι ερευνάται και ποια είναι τα επόμενα βήματα (DiOrioetal. 2020, 70–78).

Τρίτη διάσταση είναι η τεχνολογική ικανότητα ανίχνευσης και επαλήθευσης. Η παραγωγή συνθετικού περιεχομένου απαιτεί αντίστοιχη ενίσχυση εργαλείων ελέγχου αυθεντικότητας, τόσο για εικόνα και βίντεο όσο και για ηχητικά τεκμήρια. Σε πρακτικό επίπεδο, αυτό σημαίνει ανάπτυξη ή πρόσβαση σε μηχανισμούς ψηφιακής εγκληματολογίας, εκπαίδευση ειδικών ομάδων και συνεργασία με ακαδημαϊκά κέντρα ή φορείς που έχουν τεχνική επάρκεια. Παράλληλα, η τεχνολογία από μόνη της δεν αρκεί αν δεν συνδέεται με πρωτόκολλα αντίδρασης: η ανίχνευση πρέπει να μετατρέπεται γρήγορα σε αξιολόγηση κινδύνου και σε επικοινωνιακή/θεσμική απόκριση (Guessetal. 2020, 15538–15540).

Τέταρτη διάσταση αφορά το ρυθμιστικό και κανονιστικό πεδίο. Η αντιμετώπιση της

παραπληροφόρησης μέσω AI συνδέεται με το ερώτημα ποια είναι η ευθύνη των πλατφορμών, ποια τα όρια της πολιτικής διαφήμισης και ποιοι μηχανισμοί διαφάνειας μπορούν να επιβληθούν χωρίς να οδηγήσουν σε αυθαίρετους περιορισμούς. Οι πολιτικές ανθεκτικότητας εδώ δεν έχουν μόνο τιμωρητικό χαρακτήρα. Στόχος τους είναι να δημιουργήσουν κανόνες διαφάνειας για πολιτικό περιεχόμενο, να περιορίσουν τη χειραγώγηση μέσω ψευδών λογαριασμών και να επιβάλουν σαφέστερη επισήμανση περιεχομένου που παράγεται συνθετικά ή διακινείται με μη αυθεντικό τρόπο. Η αποτελεσματικότητα των κανόνων εξαρτάται από την εφαρμογή τους και από τη δυνατότητα διεθνούς συνεργασίας, αφού οι πλατφόρμες και τα δίκτυα επιρροής λειτουργούν διασυνοριακά (Micallefetal. 2022, 12–14).

Πέμπτη και ίσως πιο καθοριστική διάσταση είναι η κοινωνική ανθεκτικότητα. Σε τελική ανάλυση, οι επιχειρήσεις παραπληροφόρησης ευδοκιμούν όταν υπάρχει δυσπιστία, πόλωση και χαμηλή ικανότητα αξιολόγησης πηγών. Η ενίσχυση της ψηφιακής παιδείας, η ανάπτυξη κριτικού γραμματισμού στα μέσα και η εκπαίδευση σε βασικές πρακτικές επαλήθευσης αποτελούν στρατηγικές με μεσοπρόθεσμη απόδοση, αλλά υψηλή σημασία. Η κοινωνική ανθεκτικότητα δεν σημαίνει ότι οι πολίτες γίνονται ειδικοί, αλλά ότι αποκτούν σταθερές συνήθειες επιφυλακτικότητας απέναντι στο «εντυπωσιακό» και στο συναισθηματικά φορτισμένο περιεχόμενο, ιδίως σε κρίσιμες περιόδους (Goodman 2025, 961).

Έκτη διάσταση αφορά τις εκλογικές διαδικασίες και την προστασία της δημοκρατικής νομιμοποίησης. Οι προεκλογικές περίοδοι είναι ιδιαίτερα ευάλωτες, επειδή ο δημόσιος διάλογος είναι έντονος και η ανάγκη άμεσης πληροφόρησης αυξάνεται. Οι πολιτικές ανθεκτικότητας σε αυτό το επίπεδο περιλαμβάνουν μηχανισμούς ταχείας διάψευσης, αυξημένη διαφάνεια για πολιτική διαφήμιση, συνεργασία με fact-checking οργανισμούς και ειδικά πρωτόκολλα για την αντιμετώπιση συνθετικού περιεχομένου που στοχεύει υποψηφίους ή θεσμικά πρόσωπα. Σημαντικό είναι επίσης να υπάρχει θεσμική ουδετερότητα: η αντιμετώπιση παραπληροφόρησης να μην ταυτίζεται με κομματικά συμφέροντα, διότι αυτό υπονομεύει τον ίδιο τον στόχο της εμπιστοσύνης (Rogers 2021, 90–93).

Τέλος, καθοριστικό στοιχείο αποτελεί η διεθνής συνεργασία. Οι επιχειρήσεις επιρροής υπερβαίνουν τα σύνορα και αξιοποιούν παγκόσμιες πλατφόρμες, άρα οι πολιτικές ανθεκτικότητας χρειάζονται κοινά πρότυπα, ανταλλαγή πληροφοριών και συντονισμό μεταξύ κρατών και θεσμών. Αυτό αφορά τόσο την τεχνική διάσταση (κοινές μέθοδοι ανίχνευσης, ανταλλαγή δεδομένων για δίκτυα επιρροής) όσο και τη στρατηγική διάσταση (κοινή στάση,

συλλογική απόδοση ευθύνης, μέτρα περιορισμού δραστηριοτήτων). Η ανθεκτικότητα, σε αυτό το πλαίσιο, δεν είναι μόνο εθνική υπόθεση, αλλά στοιχείο συλλογικής ασφάλειας (Cesarini 2026, 558–560).

6.3 Προτάσεις για τη διαχείριση της στρατηγικής παραπληροφόρησης

Η διαχείριση της στρατηγικής παραπληροφόρησης, ιδιαίτερα όταν υποστηρίζεται από τεχνητή νοημοσύνη, προϋποθέτει μια προσέγγιση που συνδυάζει πρόληψη, έγκαιρη ανίχνευση, θεσμική αντίδραση και μακροπρόθεσμη ενίσχυση ανθεκτικότητας. Οι προτάσεις που ακολουθούν δεν αντιμετωπίζουν την παραπληροφόρηση ως μεμονωμένο πρόβλημα «ψευδών ειδήσεων», αλλά ως στρατηγικό φαινόμενο που επιδιώκει να αλλοιώσει την αντίληψη, να διαβρώσει την εμπιστοσύνη και να επηρεάσει αποφάσεις. Η αποτελεσματικότητα δεν εξαρτάται από ένα εργαλείο, αλλά από τη συνοχή πολιτικής και τη δυνατότητα εφαρμογής σε συνθήκες κρίσης (Cipers, Meyer, and Lefevere 2023, 3–4; 15–17).

6.3.1 Θεσμική αρχιτεκτονική και συντονισμός

Πρώτη βασική προϋπόθεση είναι η ύπαρξη ξεκάθαρης θεσμικής αρχιτεκτονικής. Σε πολλά κράτη, η παραπληροφόρηση αντιμετωπίζεται αποσπασματικά από διαφορετικούς φορείς, χωρίς ενιαία εικόνα και χωρίς κοινά πρωτόκολλα. Μια λειτουργική πρόταση είναι η δημιουργία μόνιμου μηχανισμού συντονισμού, με σαφή κατανομή αρμοδιοτήτων ανάμεσα σε υπηρεσίες ασφαλείας, υπουργεία, ανεξάρτητες αρχές και επικοινωνιακούς φορείς. Ο μηχανισμός αυτός δεν χρειάζεται να είναι υπερσυγκεντρωτικός, αλλά πρέπει να διαθέτει επιχειρησιακή δυνατότητα: να συγκεντρώνει δεδομένα, να αξιολογεί κίνδυνο και να κινητοποιεί θεσμικές απαντήσεις με ταχύτητα (Ruggieroetal. 2024). Παράλληλα, κρίνεται απαραίτητη η ύπαρξη κοινών πρωτοκόλλων για περιόδους αυξημένης ευαλωτότητας, όπως κρίσεις ασφάλειας, εκλογές ή μεγάλα συμβάντα. Σε τέτοιες περιπτώσεις, η διαχείριση πρέπει να είναι προσχεδιασμένη: ποιος εκδίδει την επίσημη ενημέρωση, ποιος αξιολογεί την αξιοπιστία υλικού, ποιος συνεργάζεται με πλατφόρμες και πότε ενεργοποιούνται ειδικές διαδικασίες (Karinshak and Jin, 2023).

6.3.2 Δυνατότητες επαλήθευσης και τεκμηρίωσης

Η στρατηγική παραπληροφόρηση μέσω AI αξιοποιεί συχνά πειστικό οπτικοακουστικό υλικό, γεγονός που καθιστά κρίσιμη την ενίσχυση των δυνατοτήτων ψηφιακής εγκληματολογίας. Προτείνεται η συγκρότηση εξειδικευμένων ομάδων επαλήθευσης εντός κρατικών δομών ή σε συνεργασία με πανεπιστημιακά/ερευνητικά κέντρα, με αντικείμενο τον

έλεγχο αυθεντικότητας σε βίντεο, ήχο και εικόνες. Η τεχνογνωσία αυτή πρέπει να συνδέεται με γρήγορα κανάλια ενημέρωσης της πολιτικής ηγεσίας, ώστε η τεχνική διάγνωση να μετατρέπεται εγκαίρως σε στρατηγική απόκριση (Mündges and Park 2024, 1-21). Εξίσου σημαντικό είναι το αποδεικτικό επίπεδο. Η ύπαρξη διαδικασιών που διασφαλίζουν την αλυσίδα τεκμηρίωσης, την αποθήκευση και την έγκαιρη δημοσιοποίηση επιλεγμένων στοιχείων μπορεί να λειτουργήσει αποτρεπτικά. Όσο πιο αδύναμο είναι το δημόσιο αποδεικτικό πεδίο, τόσο ευκολότερα ο επιτιθέμενος μπορεί να επιβάλει αμφιβολία (Leiser, 2023).

6.3.3 Στρατηγική δημόσια επικοινωνία και διαχείριση κρίσεων

Η παραπληροφόρηση εκμεταλλεύεται συχνά το κενό ενημέρωσης. Όταν οι θεσμοί σιωπούν ή αντιδρούν αργά, οι ψευδείς αφηγήσεις κερδίζουν χρόνο να παγιωθούν. Προτείνεται, συνεπώς, η ενίσχυση της στρατηγικής δημόσιας επικοινωνίας ως μηχανισμού άμυνας. Αυτό δεν σημαίνει «αντιπροπαγάνδα», αλλά σταθερή, συνετή και προβλέψιμη ενημέρωση που μειώνει τη σύγχυση και αποτρέπει τη διάδοση φημών. Σε πρακτικό επίπεδο, η επικοινωνία πρέπει να βασίζεται σε τρία στοιχεία: ταχύτητα, σαφήνεια και αξιοπιστία. Η διάψευση χωρίς εξήγηση συχνά δεν αρκεί. Χρειάζεται να παρουσιάζεται πώς τεκμηριώνεται η διάψευση, τι ακριβώς είναι ανακριβές και ποια είναι τα επόμενα βήματα. Επιπλέον, η επικοινωνία πρέπει να αποφεύγει υπερβολές, διότι αυτές μπορούν να λειτουργήσουν αντίστροφα, ενισχύοντας την καχυποψία (Gsenger 2025, 1–19).

6.3.4 Ρυθμιστικό πλαίσιο και λογοδοσία πλατφορμών

Η αποτελεσματική διαχείριση της στρατηγικής παραπληροφόρησης απαιτεί κανόνες διαφάνειας στο ψηφιακό οικοσύστημα. Προτείνεται η ενίσχυση ρυθμίσεων που αφορούν πολιτική διαφήμιση, χρηματοδότηση περιεχομένου, χρήση αυτοματοποιημένων λογαριασμών και διάδοση συνθετικού υλικού. Η λογοδοσία των πλατφορμών αποτελεί κρίσιμο στοιχείο, όχι με τη λογική της γενικευμένης λογοκρισίας, αλλά με τη λογική της διαφάνειας και της αποτροπής μη αυθεντικής συμπεριφοράς (Chystoforova and Reviglio 2025, 1-28). Ιδιαίτερα σε εκλογικές περιόδους, προτείνεται η θεσμοθέτηση ειδικών διαδικασιών για την ταχεία απομάκρυνση δικτύων που λειτουργούν συντονισμένα και η υποχρέωση διατήρησης στοιχείων για την προέλευση πολιτικών διαφημίσεων. Η διαφάνεια σε αυτούς τους τομείς περιορίζει τη δυνατότητα χειραγώγησης χωρίς να καταργεί την ελευθερία του λόγου (Heldt and Dreyer 2021, 266–300).

6.3.5 Ενίσχυση κοινωνικής ανθεκτικότητας και ψηφιακής παιδείας

Η παραπληροφόρηση είναι πιο αποτελεσματική όταν βρίσκει πρόσφορο έδαφος: δυσπιστία, πόλωση, χαμηλή κριτική ικανότητα απέναντι στις πηγές. Γι' αυτό, μια ουσιαστική πολιτική διαχείρισης πρέπει να επενδύει στην κοινωνική ανθεκτικότητα. Προτείνεται η συστηματική ενίσχυση της ψηφιακής παιδείας σε σχολεία, πανεπιστήμια και επαγγελματικά περιβάλλοντα, με πρακτικές δεξιότητες: αναγνώριση χειριστικών τίτλων, έλεγχος πηγών, βασική επαλήθευση εικόνας/βίντεο, κατανόηση του τρόπου λειτουργίας αλγορίθμων προώθησης (Guessetal. 2020, 15536–15545). Επιπλέον, η συνεργασία με ανεξάρτητους οργανισμούς επαλήθευσης και η ενίσχυση αξιόπιστων ενημερωτικών δομών λειτουργεί ως προστατευτικός παράγοντας. Η ανθεκτικότητα δεν χτίζεται μόνο με ενημέρωση των πολιτών, αλλά και με ενίσχυση της αξιοπιστίας των φορέων που μπορούν να λειτουργήσουν ως σημεία αναφοράς (Traberg, Roozenbeek, and VanderLinden 2022, 136–151).

6.3.6 Στοχευμένη προστασία κρίσιμων στιγμών και θεσμών

Ορισμένες περίοδοι και θεσμοί είναι πιο ευάλωτοι: εκλογές, δημοψηφίσματα, διαχείριση κρίσεων, ένοπλες δυνάμεις, υπηρεσίες πολιτικής προστασίας. Προτείνεται η θέσπιση ειδικών «πλάνων προστασίας» για αυτές τις περιπτώσεις, με ενισχυμένη επιτήρηση πληροφοριακών ροών, άμεση συνεργασία με πλατφόρμες και σαφείς διαδικασίες διάψευσης. Η λογική εδώ δεν είναι η γενικευμένη επιτήρηση, αλλά η εστιασμένη άμυνα σε σημεία όπου η πληροφορία μπορεί να προκαλέσει άμεσο επιχειρησιακό αποτέλεσμα (DeVerna 2025).

6.3.7 Διεθνής συνεργασία και συλλογική απόκριση

Η στρατηγική παραπληροφόρηση είναι διασυνοριακή. Απαιτείται ανταλλαγή πληροφοριών, κοινές μεθοδολογίες ανίχνευσης και δυνατότητα συντονισμένης δημόσιας στάσης. Η συλλογική απόκριση μπορεί να ενισχύσει την αποτροπή, ιδιαίτερα όταν συνδέεται με σαφή απόδοση ευθύνης και κόστος για δρώντες που διεξάγουν επιχειρήσεις επιρροής. Επιπλέον, κοινά πρότυπα για επισήμανση συνθετικού περιεχομένου και για διαφάνεια πολιτικής διαφήμισης μπορούν να μειώσουν την ασυμμετρία ανάμεσα σε επιτιθέμενους που δρουν γρήγορα και σε θεσμούς που λειτουργούν με βραδύτερους ρυθμούς (Ramašauskaitė, 2023).

6.4 Σύνοψη Κεφαλαίου

Το έκτο κεφάλαιο επικεντρώθηκε στις σύγχρονες προκλήσεις που δημιουργεί η στρατηγική παραπληροφόρηση μέσω τεχνητής νοημοσύνης για τα κράτη και τους διεθνείς θεσμούς. Αναδείχθηκε ότι οι απειλές αυτές δεν περιορίζονται σε τεχνικές επιθέσεις, αλλά

επηρεάζουν την εμπιστοσύνη, τη θεσμική σταθερότητα και τη διαδικασία λήψης αποφάσεων. Παρουσιάστηκαν πολιτικές και στρατηγικές ανθεκτικότητας που βασίζονται στον θεσμικό συντονισμό, στην ανάπτυξη δυνατοτήτων επαλήθευσης και τεκμηρίωσης, καθώς και στη διαμόρφωση ενός πιο αξιόπιστου πληροφοριακού περιβάλλοντος. Συνολικά, το κεφάλαιο υπογράμμισε ότι η αποτελεσματική διαχείριση της παραπληροφόρησης απαιτεί συνδυασμό τεχνολογικών εργαλείων, θεσμικής προετοιμασίας και κοινωνικής ανθεκτικότητας, ώστε να προστατεύεται η στρατηγική κρίση και η δημοκρατική λειτουργία στον ψηφιακό χώρο.

Συμπέρασμα

Η παρούσα διατριβή εξέτασε τον τρόπο με τον οποίο η τεχνητή νοημοσύνη μεταβάλλει το στρατηγικό περιβάλλον μέσα από την παραγωγή και διάδοση παραπληροφόρησης σε συνθήκες ψηφιακού και υβριδικού πολέμου. Η ανάλυση ανέδειξε ότι η πληροφορία δεν λειτουργεί πλέον ως ουδέτερο μέσο ενημέρωσης, αλλά ως κρίσιμο εργαλείο ισχύος, ικανό να επηρεάσει αντιλήψεις, να διαμορφώσει συμπεριφορές και να καθορίσει στρατηγικές επιλογές κρατικών και μη κρατικών δρώντων, επηρεάζοντας άμεσα την απειλή και τη διαδικασία λήψης αποφάσεων. Υπό αυτές τις συνθήκες, η αντίληψη του κινδύνου και της απειλής στους λήπτες αποφάσεων καθίσταται περισσότερο ασταθής και ευάλωτη σε γνωστική χειραγώγηση, γεγονός που επηρεάζει άμεσα την ποιότητα και τον χρόνο των στρατηγικών αποφάσεων.

Ένα βασικό συμπέρασμα της εργασίας είναι ότι οι τεχνολογίες AI ενισχύουν σημαντικά την αποτελεσματικότητα των επιχειρήσεων επιρροής, επιτρέποντας τη μαζική παραγωγή πειστικού περιεχομένου, την ταχεία προσαρμογή αφηγημάτων και τη στοχευμένη χειραγώγηση κοινωνικών ομάδων. Deepfakes, αυτοματοποιημένα δίκτυα και συνθετικές δηλώσεις δεν αποτελούν απλώς τεχνικές καινοτομίες, αλλά μηχανισμούς που μεταφέρουν τη σύγκρουση στο γνωστικό επίπεδο, όπου η αλήθεια, η εμπιστοσύνη και η πολιτική νομιμοποίηση γίνονται αντικείμενο στρατηγικής αντιπαράθεσης και επηρεάζουν τον τρόπο με τον οποίο οι δρώντες εκτιμούν τον κίνδυνο και διαμορφώνουν στρατηγικές επιλογές. Η διατριβή κατέδειξε επίσης ότι η παραπληροφόρηση μέσω AI δεν λειτουργεί αποκλειστικά ως εργαλείο «από τα πάνω» κρατικής επιβολής, αλλά συχνά εμφανίζεται μέσα από αποκεντρωμένα δίκτυα, κοινωνικές δυναμικές και μη κρατικούς δρώντες. Η διάκριση μεταξύ top-down και bottom-up επιρροής παραμένει σημαντική, αλλά στην πράξη οι δύο μορφές αλληλεπιδρούν, δημιουργώντας ένα σύνθετο οικοσύστημα όπου η τεχνολογία επιτρέπει σε πολλούς φορείς να επηρεάζουν το κράτος, τις κοινωνίες και τη διεθνή τάξη.

Παράλληλα, αναδείχθηκε ότι η στρατηγική επίδραση της παραπληροφόρησης δεν περιορίζεται στη στιγμιαία εξαπάτηση. Ακόμη και όταν το ψευδές περιεχόμενο αποκαλύπτεται, μπορεί να προκαλέσει σύγχυση, να διαβρώσει την εμπιστοσύνη στους θεσμούς και να επιβαρύνει τη διαδικασία λήψης αποφάσεων, υπονομεύοντας τη στρατηγική κρίση σε περιβάλλοντα αυξημένης αβεβαιότητας. Η ασφάλεια στον ψηφιακό χώρο συνδέεται έτσι άμεσα με την ικανότητα διατήρησης αξιόπιστης πληροφόρησης και σταθερής στρατηγικής κρίσης. Τα παραδείγματα που εξετάστηκαν, από τον πόλεμο Ρωσίας–Ουκρανίας έως τις επιχειρήσεις επιρροής στην Ταϊβάν και τις παρεμβάσεις σε ευρωπαϊκές εκλογές, επιβεβαίωσαν ότι οι σύγχρονες συγκρούσεις διεξάγονται ταυτόχρονα στο στρατιωτικό, πολιτικό και πληροφοριακό πεδίο με την τεχνητή νοημοσύνη λειτουργεί ως επιταχυντής και πολλαπλασιαστής ισχύος αυτής της μετάβασης, καθιστώντας πιο δύσκολη την ανίχνευση, την απόδοση ευθύνης και την αποτελεσματική θεσμική αντίδραση. Οι θεσμοί ασφάλειας επιχειρούν να ανταποκριθούν μέσω μηχανισμών παρακολούθησης, ρυθμιστικών παρεμβάσεων και διεθνούς συνεργασίας, ωστόσο οι προσπάθειες αυτές συχνά περιορίζονται από την ταχύτητα της τεχνολογικής εξέλιξης και την ασυμμετρία πληροφορίας.

Τέλος, η εργασία υπογράμμισε ότι η αντιμετώπιση της στρατηγικής παραπληροφόρησης απαιτεί συνδυασμό θεσμικού συντονισμού, τεχνολογικών δυνατοτήτων επαλήθευσης, κανονιστικών πλαισίων και κοινωνικής ανθεκτικότητας. Η προστασία της δημοκρατικής λειτουργίας και της στρατηγικής σταθερότητας δεν μπορεί να βασιστεί μόνο σε τεχνικές λύσεις, αλλά προϋποθέτει διαρκή προσαρμογή και ενίσχυση της εμπιστοσύνης στο πληροφοριακό περιβάλλον ώστε η λήψη αποφάσεων να παραμένει ορθολογική και ανθεκτική απέναντι στην κατασκευή μιας ψηφιακά διαμεσολαβημένης «ψευδούς πραγματικότητας».

Βιβλιογραφία

Ahmed, S. 2023. “Navigating the Maze: Deepfakes, Cognitive Ability, and Social Media News Skepticism.” New Media & Society 25 (5): 1108–1129.

Alsmadi, Izzat, Nathan M. Rice, and Michael J. O’Brien. 2024. “Fake or Not? Automated Detection of COVID-19 Misinformation and Disinformation in Social Networks and Digital Media.” Computational and Mathematical Organization Theory 30 (3): 187–205.

Anagnostakis, D. 2023. “Hybrid Threats: A European Response.” In Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies, 425–441. Cham: Springer International Publishing.

Andrade, Roberto O., Walter Fuertes, María Cazares, Iván Ortiz-Garcés, and Gustavo Navas. 2022. “An Exploratory Study of Cognitive Sciences Applied to Cybersecurity.” Electronics 11, no. 11: 1692. https://doi.org/10.3390/electronics11111692.

Angwald, A., and C. Wagnsson. 2024. “Disinformation and Strategic Frames: Introducing the Concept of a Strategic Epistemology towards Media.” Media, Culture & Society 46 (7): 1527–1538.

Araujo, T., N. Helberger, S. Kruikemeier, and C. H. de Vreese. 2020. “In AI We Trust? Perceptions about Automated Decision-Making by Artificial Intelligence.” AI & Society 35 (3): 611–623.

Ashritha, P., and P. S. Reddy. 2023. “Impact of Artificial Intelligence on Management Decision-Making.” International Journal of Advances in Business and Management Research (IJABMR) 1 (2): 10–18.

Asmolov, G. 2018. “The Disconnective Power of Disinformation Campaigns.” Journal of International Affairs 71 (1.5): 69–76.

Au, C. H., K. K. Ho, and D. K. Chiu. 2022. “The Role of Online Misinformation and Fake News in Ideological Polarization: Barriers, Catalysts, and Implications.” Information Systems Frontiers 24 (4): 1331–1354.

Bargués, P., J. Joseph, and A. E. Juncos. 2023. “Rescuing the Liberal International Order: Crisis, Resilience and EU Security Policy.” International Affairs 99 (6): 2281–2299.

Bennett, W. L., and S. Livingston. 2018. “The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions.” European Journal of Communication 33 (2): 122–139.

Boháček, Matyáš, and Hany Farid. 2022.“Protecting President Zelenskyy against Deep Fakes.”arXiv preprint arXiv:2206.12043. https://arxiv.org/abs/2206.12043

Borz, G., F. De Francesco, T. L. Montgomerie, and M. P. Bellis. 2024. “The EU Soft Regulation of Digital Campaigning: Regulatory Effectiveness through Platform Compliance to the Code of Practice on Disinformation.” Policy Studies 45 (5): 709–729.

Bradshaw, S., U. Campbell-Smith, A. Henle, A. Perini, S. Shalev, H. Bailey, and P. N. Howard. 2021. Country Case Studies: Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Oxford: Oxford Internet Institute. Accessed October 24, 2024.

Briggs, Chad M., and Anita Tusor. 2025. “Surveying New Battlegrounds: Ukraine and the Future of Cognitive Warfare.” Journal of Strategic Security 18, no. 4: 177–185. https://doi.org/10.5038/1944-0472.18.4.2587

Bryant, Andrew. 2023. “AI Chatbots: Threat or Opportunity?” Informatics 10 (2): 49.

Bryczek-Wróbel, P., and M. Moszczyński. 2022. “The Evolution of the Concept of Information Warfare in the Modern Information Society of the Post-Truth Era.” PrzeglądNauk o Obronności 7 (13): 48–62.

Calderón, K. K., J. L. P. Sierra, and R. Bermejo-Casado. 2025. “Conceptualizing Information Suppression: A Distinct Strategy within Foreign Information Manipulation and Interference Operations.” In Disinformation and Counternarratives in International Security, 58–83. Routledge.

Can, M. 2020. “Grey Zone Conflicts in Cyber Domain: Nonlocality of Political Reality in the World of ‘Hyperobjects’.” In Encyclopedia of Criminal Activities and the Deep Web, 271–286. IGI Global.

Casero-Ripollés, A., J. Tuñón, and L. Bouza-García. 2023. “The European Approach to Online Disinformation: Geopolitical and Regulatory Dissonance.” Humanities and Social Sciences Communications 10 (1): 1–10.

Casino, Fran. 2025. “Unveiling the Multifaceted Concept of Cognitive Security: Trends, Perspectives, and Future Challenges.” Technology in Society 83 (December): 102956. https://doi.org/10.1016/j.techsoc.2025.102956.

Castelfranchi, C., and R. Falcone. 2018. “The Problematic Relationship between Trust and Democracy; Its Crisis and Web Dangers and Promises.” In The Future of Digital Democracy: An Interdisciplinary Approach, 62–82. Cham: Springer International Publishing.

Cesarini, P. 2026. “The EU Policy Framework to Counter Disinformation: Enabler or Inhibitor of Freedom of Expression?” In Disinformation: A Multi-Disciplinary Analysis, 551–575. Cham: Springer Nature Switzerland.

Chesney, R., and D. Citron. 2019. “Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics.” Foreign Affairs 98: 147-155.

Chystoforova, K., and U. Reviglio. 2025. “Framing the Role of Experts in Platform Governance: Negotiating the Code of Practice on Disinformation as a Case Study.” Internet Policy Review 14 (1): 1–28.

Cipers, Samuel, Trisha Meyer, and Jonas Lefevere. 2023. “Government Responses to Online Disinformation Unpacked.” Internet Policy Review 12 (4): 1–19. https://doi.org/10.14763/2023.4.1736

Cîrdei, I. A., and L. Ispas. 2017. “A Possible Answer of the European Union to Hybrid Threats.” Scientific Bulletin – Nicolae Bălcescu Land Forces Academy 22 (2): 71–78.

Collett, R. 2021. “Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures.” Journal of Cyber Policy 6 (3): 298–317.

Cristofaro, Matteo, Pier Luigi Giardino, Andrea P. Malizia, and Antonio Mastrogiorgio. 2022. “Affect and Cognition in Managerial Decision Making: A Systematic Literature Review of Neuroscience Evidence.”Frontiers in Psychology 13: 1–20. https://doi.org/10.3389/fpsyg.2022.762993

Csaszar, F. A., H. Ketkar, and H. Kim. 2024. “Artificial Intelligence and Strategic Decision-Making: Evidence from Entrepreneurs and Investors.” Strategy Science 9 (4): 322–345.

Dear, K. 2019. “Artificial Intelligence and Decision-Making.” The RUSI Journal 164 (5–6): 18–25.

de-Lima-Santos, M. F., and W. Ceron. 2023. “Coordinated Amplification, Coordinated Inauthentic Behaviour, Orchestrated Campaigns: A Systematic Literature Review of Coordinated Inauthentic Content on Online Social Networks.” In Mapping Lies in the Global Media Sphere, 165–184.

Deppe, Christoph, and Gary S. Schaal. 2024.“Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept.” Frontiers in Big Data 7: 1–13. https://doi.org/10.3389/fdata.2024.1452129

DeVerna, M. R. 2025. Social Media Misinformation: Spread, Impact, and Fact-Checking with Large Language Models. Doctoral dissertation, Indiana University.

Di Orio, Giulia, Gustavo Brito, Pietro Malè, Andrei Sadu, Nicolai Wirtz, and Antonello Monti. 2020. “A Cyber-Physical Approach to Resilience and Robustness by Design.” International Journal of Advanced Computer Science and Applications 11 (7): 70–78.

Doherty, G. 2023. “Cognitive Security: An Architecture Informed Approach from Cognitive Science.” In International Conference on Human-Computer Interaction, 395–415. Cham: Springer Nature Switzerland.

Dunn Cavelty, M., C. Eriksen, and B. Scharte. 2023. “Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes.” Journal of Risk Research 26 (7): 801–814.

Erskine, T., and S. E. Miller. 2024. “AI and the Decision to Go to War: Future Risks and Opportunities.” Australian Journal of International Affairs 78 (2): 135–147.

Ferrara, E., O. Varol, C. Davis, F. Menczer, and A. Flammini. 2016. “The Rise of Social Bots.” Communications of the ACM 59 (7): 96–104.

Farooq, A., E. van den Hoogen, M. Tulin, and C. de Vreese. 2025. “Generative AI Generating Concerns: Citizens’ Perspectives During the 2024 European Elections.” The International Journal of Press/Politics: 19401612251376060.

Feng, J., P. Han, W. Zheng, and A. Kamran. 2022. “Identifying the Factors Affecting Strategic Decision-Making Ability to Boost the Entrepreneurial Performance.” Frontiers in Psychology 13: 1038604.

Fenstermacher, L., D. Uzcha, K. Larson, C. Vitiello, and S. Shellman. 2023. “New Perspectives on Cognitive Warfare.” In Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII, Vol. 12547, 172–187. SPIE.

Ferenczy, Z. A. 2024. “Democratic Resilience: Lessons to Tell, Lessons to Learn.” In Partners in Peace: Why Europe and Taiwan Matter to Each Other, 83–110. Singapore: Springer Nature Singapore.

Flores Vivar, Jesús Miguel. 2019. “Artificial Intelligence and Journalism: Diluting the Impact of Disinformation and Fake News through Bots.” Doxa Comunicación 29: 197–212.

Geissler, D., D. Bär, N. Pröllochs, and S. Feuerriegel. 2023. “Russian Propaganda on

Social Media during the 2022 Invasion of Ukraine." EPJ Data Science 12 (1): 35.

George, A. S., and A. H. George. 2023. "Deepfakes: The Evolution of Hyper Realistic Media Manipulation." Partners Universal Innovative Research Publication 1 (2): 58–74.

Goodman, E. P. 2025. "Symposium Preview: Defending Tomorrow's Democracy—Synthetic Content: Default to Distrust." Case Western Reserve Law Review 75 (3): 961.

Grahn, Henrik, and Tuomas Taipalus. 2025. "Defining Comprehensive Cognitive Security in the Digital Era: Literature Review and Concept Analysis." Journal of Information Warfare 24 (2): 39–59.

Gsenger, R. 2025. "Platform Governance under the Digital Services Act: A Perspective on Disinformation." Information, Communication & Society: 1–19.

Guess, A. M., M. Lerner, B. Lyons, J. M. Montgomery, B. Nyhan, J. Reifler, and N. Sircar. 2020. "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India." Proceedings of the National Academy of Sciences 117 (27): 15536–15545.

Haenlein, M., and A. Kaplan. 2019. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence." California Management Review 61 (4): 5–14.

Hartmann, K., and K. Giles. 2020. "The Next Generation of Cyber-Enabled Information Warfare." In 2020 12th International Conference on Cyber Conflict (CyCon), 233–250. IEEE.

Heath, D. R. 2019. "Prediction Machines: The Simple Economics of Artificial Intelligence: by Ajay Agrawal, Joshua Gans and Avi Goldfarb…" (book review). California Management Review.

Hedling, Erik, and Håkan Ördén. 2025. "Disinformation, Deterrence and the Politics of Attribution." International Affairs 101 (3): 967–986.

Heldt, A., and S. Dreyer. 2021. "Competent Third Parties and Content Moderation on Platforms: Potentials of Independent Decision-Making Bodies from a Governance Structure Perspective." Journal of Information Policy 11: 266–300.

Hoffman, F. G. 2018. "Examining Complex Forms of Conflict." Prism 7 (4): 30–47.

Holmes, M., and N. J. Wheeler. 2024. "The Role of Artificial Intelligence in Nuclear Crisis Decision Making: A Complement, Not a Substitute." Australian Journal of International Affairs 78 (2): 164–174.

Horowitz, Michael C., and Lauren Kahn. 2024. "Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts." International Studies Quarterly 68 (2): sqae020. https://doi.org/10.1093/isq/sqae020

Horowitz, Michael C., Erik Lin-Greenberg, and Lauren Kahn. 2022. "Algorithms and Influence: Artificial Intelligence and Decision Making in Crises." International Studies Quarterly 66 (4): sqac069. https://doi.org/10.1093/isq/sqac069

Huang, A. 2024. "Combatting and Defeating Chinese Propaganda and Disinformation: A Case Study of Taiwan's 2020 Elections." In State-Sponsored Disinformation around the

Globe, 121–136. Routledge.

Hung, T. C., and T. W. Hung. 2022. “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars.” Journal of Global Security Studies 7 (4): ogac016.

IANCU, N. 2024. “A National Security Perspective on Strengthening EU Civilian-Defence Cybersecurity Synergy: A Systemic Approach.” In Proceedings of the International Conference on Cybersecurity and Cybercrime-2024, 22–34. Asociatia Romana pentruAsigurareaSecuritatiiInformatiei.

Iosifidis, P. 2024. “Theoretical Understanding of State-Sponsored Disinformation.” In State-Sponsored Disinformation Around the Globe, 21–36. Routledge.

Jaboob, A., O. Durrah, and A. Chakir. 2024. “Artificial Intelligence: An Overview.” Engineering Applications of Artificial Intelligence: 3–22.

Jafari, M., A. Shahbazi, M. Kawsar, S. P. M. Davoudi, and S. Janani. 2025. “The Role of Artificial Intelligence in Strategic Planning and Competitive Advantage.” International Journal of Advanced Business Studies 4 (4): 258–276.

Janzen, J. 2024. “The Role of Strategic Communication within Contemporary Information Warfare.” The Journal of Intelligence, Conflict, and Warfare 6 (3): 211–214.

Jaw-Nian, H. 2023. “China’s Propaganda and Disinformation Operations in Taiwan: A Sharp Power Perspective.” China: An International Journal 21 (2): 143–170.

Jervis, R. 2020. “Strategic Theory: What’s New and What’s True.” In The Logic of Nuclear Terror, 47–81. Routledge.

Jiang, Yuchen, Xiang Li, Hao Luo, Shen Yin, and Okyay Kaynak. 2022. “Quo vadis Artificial Intelligence?” Discover Artificial Intelligence 2 (1): Article 4. https://doi.org/10.1007/s44163-022-00022-8

Johnson, J. 2019. “Artificial Intelligence & Future Warfare: Implications for International Security.” Defense & Security Analysis 35 (2): 147–169.

Kandari, M., V. Tripathi, and B. Pant. 2023. “A Comprehensive Review of Media Forensics and Deepfake Detection Technique.” In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), 392–395. IEEE.

Karinshak, E., and Y. Jin. 2023. “AI-Driven Disinformation: A Framework for Organizational Preparation and Response.” Journal of Communication Management 27 (4): 539–562.

Kazim, A. 2025. “The Role of AI in Shaping US–China Diplomacy: A Case Study of the Taiwan Strait Crisis.” Journal of Regional Studies Review 4 (1): 433–442.

Keding, C. 2021. “Understanding the Interplay of Artificial Intelligence and Strategic Management: Four Decades of Research in Review.” Management Review Quarterly 71 (1): 91–134.

Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven, CT: Yale University Press.Kertysova, K. 2018. “Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered.” Security and Human Rights 29 (1–4): 55–81.

Kertzer, J. D., M. Holmes, B. L. LeVeck, and C. Wayne. 2022. “Hawkish Biases and Group Decision Making.” International Organization 76 (3): 513–548.

Kin, O. 2025. “The Cognitive Dimension of Modern Hybrid Warfare: Military-Political Analysis.” Political Science and Security Studies Journal 6 (4): 22–29.

Klasche, B., and P. Selg. 2020. “A Pragmatist Defence of Rationalism: Towards a Cognitive Frames–Based Methodology in International Relations.” International Relations 34 (4): 544–564.

Kloo, I., I. J. Cruickshank, and K. M. Carley. 2024. “A Cross-Platform Topic Analysis of the Nazi Narrative on Twitter and Telegram during the 2022 Russian Invasion of Ukraine.” In Proceedings of the International AAAI Conference on Web and Social Media 18: 839–850.

Korteling, J. E., G. L. Paradies, and J. P. Sassen-van Meer. 2023. “Cognitive Bias and How to Improve Sustainable Decision Making.” Frontiers in Psychology 14: 1129835.

Krawczyk, P., and J. Wiśnicki. 2022. “Information Warfare Tools and Techniques in the Context of Information Operations Conducted by the Russian Federation during the 2022 War in Ukraine.” Cybersecurity and Law 8 (2): 278–286.

Lee, L. M. C. 2024. “Decoding China’s Digital Offensive: An Analysis of Information Warfare Tactics in Taiwan’s 2024 Presidential Election.” Yale Journal of International Affairs.

Leiser, M. R. 2023. “Reimagining Digital Governance: The EU’s Digital Service Act and the Fight Against Disinformation.” SSRN 4427493.

Levinger, M. 2018. “Master Narratives of Disinformation Campaigns.” Journal of International Affairs 71 (1.5): 125–134.

Libicki, Martin C. 2016. Cyberspace in Peace and War. Annapolis, MD: Naval Institute Press.Lin, H., and J. Kerr. 2017. “On Cyber-Enabled Information/Influence Warfare and Manipulation.” Center for International Security and Cooperation, Stanford, 4–22.

Lin, Y. Y. 2023. “China’s Cognitive Warfare Against Taiwan and Taiwan’s Countermeasures.” Taiwan Strategists (20): 37–54.

Littell, J., and N. Starck. 2023. “Russian Influence Operations during the Invasion of Ukraine.” In International Conference on Cyber Warfare and Security, 209–XIV. Academic Conferences International Limited.

Lu, C., B. Hu, Q. Li, C. Bi, and X. D. Ju. 2023. “Psychological Inoculation for Credibility Assessment, Sharing Intention, and Discernment of Misinformation: Systematic Review and Meta-Analysis.” Journal of Medical Internet Research 25: e49255.

Mallick, P. K. 2024. “Artificial Intelligence, National Security and the Future of Warfare.” In Artificial Intelligence, Ethics and the Future of Warfare, 30–70. Routledge India.

Marangione, M. S. 2021. “Words as Weapons: The 21st Century Information War.” Security and Intelligence 6 (1).

Marigliano, R., L. H. X. Ng, and K. M. Carley. 2024. “Analyzing Digital Propaganda and Conflict Rhetoric.” Social Network Analysis and Mining 14 (1): 170.

Marjanović, A., and D. Smiljanić. 2025. “Cognitive Warfare—the Human Mind as the New Battlefield.” In Proceedings of the Defense and Security Conference, 84–114. Zagreb.

Marrone, A. 2022. “NATO’s New Strategic Concept: Novelties and Priorities.” IAI

Commentaries 22: 30.

Mayer, S. 2023. “Introduction: NATO as an Object of Research.” In Research Handbook on NATO, 1–19. Edward Elgar Publishing.

Micallef, N., V. Armacost, N. Memon, and S. Patil. 2022. “True or False: Studying the Work Practices of Professional Fact-Checkers.” Proceedings of the ACM on Human-Computer Interaction 6 (CSCW1): 1–44.

Mikhaylovskaya, A., and A. Roum?as. 2024. “Building Trust with Digital Democratic Innovations.” Ethics and Information Technology 26 (1): 1.

Miller, S. 2023. “Cognitive Warfare: An Ethical Analysis.” Ethics and Information Technology 25 (3): 46.

Milshtein, D., A. Henik, E. H. Ben-Zedeff, and U. Milstein. 2024. “Mind on the Battlefield.” Defence Studies 24 (2): 277–298.

Moon, W. K., and L. A. Kahlor. 2025. “Fact-Checking in the Age of AI: Reducing Biases with Non-Human Information Sources.” Technology in Society 80: 102760.

Mündges, S., and K. Park. 2024. “But Did They Really? Platforms’ Compliance with the Code of Practice on Disinformation in Review.” Internet Policy Review 13 (3): 1–21.

Muthukrishnan, N., F. Maleki, K. Ovens, C. Reinhold, B. Forghani, and R. Forghani. 2020. “Brief History of Artificial Intelligence.” Neuroimaging Clinics 30 (4): 393–399.

Nabila, Mohammed Hafiz, Rohany Abdul Shaibu, Glory EdinamAfeti, and Esinu Aku Adza. 2025. “Disinformation as a Driver of Political Polarization: A Strategic Framework for Rebuilding Civic Trust in the U.S.” World Journal of Advanced Research and Reviews 27 (1): 916–925. https://doi.org/10.30574/wjarr.2025.27.1.2564

Nasiri, S., and A. Hashemzadeh. 2025. “The Evolution of Disinformation from Fake News Propaganda to AI-Driven Narratives as Deepfake.” Journal of Cyberspace Studies 9 (1): 229–250.

Nawaz, F. 2025. “Psychological Warfare in the Digital Age: Strategies, Impacts, and Countermeasures.” Journal of Future Building 2 (1): 21–30.

Nye, J. S. 2020. Do Morals Matter?: Presidents and Foreign Policy from FDR to Trump. Oxford University Press.

Pace, R. M., and E. R. Coelho. 2022. “Information as a Weapon of Mass Disruption.” Revista da EGN 28 (3): 707–722.

Papadogiannakis, E., P. Papadopoulos, N. Kourtellis, and E. Markatos. 2025. “Before & After: The Effect of EU’s 2022 Code of Practice on Disinformation.” In Proceedings of the ACM on Web Conference 2025, 1577–1587.

Paul, Christopher, and Miriam Matthews. 2016. The Russian “Firehose of Falsehood” Propaganda Model. Santa Monica, CA: RAND Corporation.Puttaraju, K. H. 2023. “Augmenting Classical Strategic Tools with Artificial Intelligence.” International Journal of Science and Research (IJSR) 12 (11): 2242–2247.

Radulov, N. 2019. “Artificial Intelligence and Security.” Security 4.0. Security & Future 3 (1): 3–5.

Ramašauskaitė, O. 2023. “The Role of Collaborative Networks in Combating Digital Disinformation.” In International Conference on Economics ‘Regional Development–Digital Economy’ (Proceedings Book), 432–437. Liberty Academic Publishers.

Rasheed, K., A. Zaland, S. Saad, S. Ammad, and A. Rostami. 2024. “History of AI.” In AI in Material Science, 15–46. CRC Press.

Rid, T. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. Profile Books.

Rogers, Z. 2021. “The Promise of Strategic Gain in the Digital Information Age.” The Cyber Defense Review 6 (1): 81–106.

Romanishyn, Alexander, Olena Malytska, and Vitaliy Goncharuk. 2025. “AI-Driven Disinformation: Policy Recommendations for Democratic Resilience.” Frontiers in Artificial Intelligence 8: 1569115. https://doi.org/10.3389/frai.2025.1569115

Ruggiero, A., W. D. Piotrowicz, and L. John. 2024. “Enhancing Societal Resilience through the Whole-of-Society Approach to Crisis Preparedness.” International Journal of Disaster Risk Reduction 114: 104944.

Saeva, E., and I. Tasheva. 2024. “The 2024 EU Elections and Cybersecurity: A Retrospective and Lessons Learned.” European View 23 (2): 226–234.

Saressalo, T., and A. M. Huhtinen. 2022. “Information Influence Operations.” Journal of Information Warfare 21 (4): 41–66.

Selvarajan, G. P. 2023. “Augmenting Business Intelligence with AI.” International Journal of All Research Education and Scientific Methods 11 (10): 2121–2132.

Serwar, A. 2024. “The Role of Artificial Intelligence in Management Decision-Making: A Critical Appraisal.” The Journal of Research Review 1 (02): 77–85.

Shen, F., E. Zhang, W. Ren, Y. He, Q. Jia, and H. Zhang. 2023. “Examining the Differences between Human and Bot Social Media Accounts.” First Monday 28 (2).

Simchon, Almog, Tomer Zipori, Louis Teitelbaum, Stephan Lewandowsky, and Sander van der Linden. 2025. “A Signal Detection Theory Meta-Analysis of Psychological Inoculation Against Misinformation.” Current Opinion in Psychology 67: 102194. https://doi.org/10.1016/j.copsyc.2025.102194

Sliwa, Z., and A. Antczak. 2018. “Military Domain as a Component of Information Warfare.” Sõjateadlane: The Estonian Journal of Military Studies (8): 16–47.

Smart, Benjamin, James Watt, Silvia Benedetti, Lewis Mitchell, and Matthew Roughan. 2022. “#IStandWithPutin versus #IStandWithUkraine: The Interaction of Bots and Humans in Discussion of the Russia/Ukraine War.” In International Conference on Social Informatics, 34–53. Cham: Springer International Publishing.

Soprano, Michael, Kevin Roitero, David La Barbera, Davide Ceolin, Damiano Spina, Gianluca Demartini, and Stefano Mizzaro. 2024. “Cognitive Biases in Fact-Checking and Their Countermeasures: A Review.” Information Processing & Management 61 (3): 103672. https://doi.org/10.1016/j.ipm.2024.103672

Tache, C. E. P. 2023. “About the Human Rights and Consumer Protection in the Digital Age of Digital Services Act 2022.” International Investment Law Journal 3 (2): 121–132.

Teperik, Dmitri, Solvita Denisa-Liepniece, Dalia Bankauskaitė, and Kaarel Kullamaa. 2022. Resilience Against Disinformation: A New Baltic Way to Follow?, 21–23. Tallinn: International Centre for Defence and Security.

Thomas, T. L. 2020. “Information Weapons.” The Cyber Defense Review 5 (2): 125–144.

Toosi, A., A. G. Bottino, B. Saboury, E. Siegel, and A. Rahmim. 2021. “A Brief History of AI: How to Prevent Another Winter (a Critical Review).” PET Clinics 16 (4): 449–469.

Traberg, C. S., J. Roozenbeek, and S. Van Der Linden. 2022. “Psychological Inoculation against Misinformation: Current Evidence and Future Directions.” The ANNALS of the American Academy of Political and Social Science 700 (1): 136–151.

Tsotniashvili, Z. 2024. “Silicon Tactics: Unravelling the Role of Artificial Intelligence in the Information Battlefield of the Ukraine Conflict.” Asian Journal of Research 9 (1–3): 54–65.

Twomey, James, Daniel Ching, Maeve P. Aylett, Michael Quayle, Ciara Linehan, and Gerard Murphy. 2023. “Do Deepfake Videos Undermine Our Epistemic Trust?” PLOS ONE 18 (10): e0291668. https://doi.org/10.1371/journal.pone.0291668.

Tyushka, A. 2022. “Weaponizing Narrative: Russia Contesting EUrope’s Liberal Identity, Power and Hegemony.” Journal of Contemporary European Studies 30 (1): 115–135.

Vaccari, C., and A. Chadwick. 2020. “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News.” Social Media + Society 6 (1): 2056305120903408.

Vasist, P. N., D. Chatterjee, and S. Krishnan. 2024. “The Polarizing Impact of Political Disinformation and Hate Speech.” Information Systems Frontiers 26 (2): 663–688.

Westerlund, Mika. 2019. “The Emergence of Deepfake Technology: A Review.” Technology Innovation Management Review 9 (11): 39–52.

Whiteaker, John, and Sami Valkonen. 2022. “Cognitive Warfare: Complexity and Simplicity.” In Cognitive Warfare: The Future of Cognitive Dominance, edited by Bernard Claverie, Baptiste Prébot, Norbou Buchler, and François du Cluzel, 11-1–11-5. NATO Science and Technology Organization (STO).

Wigell, M., H. Mikkola, and T. Juntunen. 2021. Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats. European Parliament, Policy Department for External Relations.

Zhou, Y., and L. Shen. 2024. “Processing of Misinformation as Motivational and Cognitive Biases.” Frontiers in Psychology 15: 1430953.https://doi.org/10.3389/fpsyg.2024.1430953