ΕΛΙΑΜΕΠ

ΕΛΛΗΝΙΚΟ ΙΔΡΥΜΑ ΕΥΡΩΠΑΪΚΗΣ & ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

HELLENIC FOUNDATION FOR EUROPEAN & FOREIGN POLICY

ELIAMEP-NATO Youth Symposium: Why Defense Matters

Η Αντιμετώπιση των Αναδυόμενων Απειλών: Από τις Υβριδικές Προκλήσεις στους Νέους Τεχνολογικούς Μετασχηματισμούς.

Ντάρας Ιγνάτιος

Δεκέμβριος 2025

Εισαγωγή

Το σύγχρονο περιβάλλον ασφαλείας, χαρακτηρίζεται από αστάθεια και πολυπλοκότητα. Η έντονη γεωπολιτική αντιπαλότητα, η ταχεία σύγκλιση παραδοσιακών και μη παραδοσιακών απειλών καθώς και η επιτάχυνση της τεχνολογικής εξέλιξης, συγκροτούν ένα τοπίο όπου τα όρια μεταξύ ειρήνης και σύγκρουσης καθίστανται ολοένα και πιο θολά.

Σε αυτό το πλαίσιο, οι υβριδικές απειλές αμφισβητούν τις παραδοσιακές αντιλήψεις για την ασφάλεια συνδυάζοντας στρατιωτικά ή μη στρατιωτικά μέσα. Η σύγκρουση επεκτάθηκε πέρα από το διακρατικό ή ενδοκρατικό πεδίο αξιοποιώντας στρατιωτικά, οικονομικά, πολιτικά και ψηφιακά μέσα για την επίτευξη στρατηγικών στόχων. Στη «γκρίζα ζώνη» μεταξύ ειρήνης και σύγκρουσης δρουν οι υβριδικοί δρώντες, προσπαθώντας να επιτύχουν τα μέγιστα δυνατά αποτελέσματα με το χαμηλότερο δυνατό κόστος αλλά και ρίσκο. Στοχεύουν κυρίως τις ευάλωτες δομές μίας κοινωνίας υπονομεύοντας την πολιτική σταθερότητα και την κοινωνική συνοχή. Οι απειλές για την άμυνα δεν εκδηλώνονται αποκλειστικά πλέον με συμβατικές στρατιωτικές επιχειρήσεις αλλά μέσα από ένα ευρύ φάσμα υβριδικών ενεργειών που δυσχεραίνουν την άμεση αντίδραση και την απόδοση ευθυνών.

Η ραγδαία ανάπτυξη της τεχνολογίας μετασχημάτισε σημαντικά το πεδίο των υβριδικών επιχειρήσεων. Μέσω της τεχνητής νοημοσύνης, του κυβερνοχώρου καθώς και των αυτόνομων οπλικών συστημάτων δημιουργήθηκαν νέες δυνατότητες πολλαπλασιάζοντας την αποτελεσματικότητα των υβριδικών επιχειρήσεων προσφέροντας μεγαλύτερη ταχύτητα και ακρίβεια. Οι νέες τεχνολογίες μετασχημάτισαν σε σημαντικό βαθμό τη φύση, τα εργαλεία καθώς και τους στόχους των υβριδικών επιχειρήσεων.

Η έννοια των υβριδικών απειλών κατέστη ιδιαίτερα δημοφιλής το 2014 μέσα από τη σύγκρουση Ρωσίας - Ουκρανίας η οποία οδήγησε στην προσάρτηση της Κριμαίας από τη Ρωσία. Η σύγκρουση αυτή απέδειξε πως οι υβριδικές επιχειρήσεις θα αποτελέσουν αναπόσπαστο κομμάτι των διεθνών συγκρούσεων. Για τον λόγο αυτό το ΝΑΤΟ και η ΕΕ ξεκίνησαν έναν διάλογο σχετικά με την αναπροσαρμογή του στρατηγικού τους σχεδιασμού, ώστε να μπορούν να αντιμετωπίσουν αυτού του είδους τις απειλές.

Η παρούσα εργασία επιδιώκει να αναδείξει τη σχέση μεταξύ των υβριδικών προκλήσεων και των νέων τεχνολογικών μετασχηματισμών εστιάζοντας κυρίως στο κομμάτι του πληροφοριακού πολέμου (information warfare) το οποίο λειτουργεί ως κοινός παρονομαστή τους. Μέσω της μελέτης περίπτωσης του Ρωσο-Ουκρανικού πολέμου θα εξεταστεί πως η Ρωσία επεδίωξε να εργαλειοποιήσει την πληροφορία για να ασκήσει πίεση στην ουκρανική πλευρά αλλά και πως η Ουκρανία προσπάθησε να ανταποκριθεί σε αυτό. Η ρωσική στρατηγική συνδύασε τις συμβατικές στρατιωτικές επιχειρήσεις με έναν πολυδιάστατο πληροφοριακό πόλεμο που ως στόχο είχε τόσο να καλλιεργήσει αφηγήματα όσο και να υπονομεύσει την εμπιστοσύνη στους θεσμούς.

Αναφορικά με τη διάρθρωση της εργασίας αρχικά παρουσιάζεται ένα σύντομο θεωρητικό πλαίσιο για τις υβριδικές απειλές και τις μορφές που μπορούν να λάβουν. Ιδιαίτερη έμφαση δίνεται στην περίπτωση του πληροφοριακού πολέμου (information warfare) ο οποίο αποτελεί και τη θεωρητική βάση για τη μελέτη περίπτωσης Ρωσίας-Ουκρανίας. Στο τέλος, παρατίθενται κάποια συμπεράσματα αναφορικά με την αποτελεσματικότητα της αντίδρασης του ΝΑΤΟ και της Ουκρανίας αλλά και κάποιες προτάσεις για την αντιμετώπιση τέτοιων απειλών.

Κεφάλαιο 2 : Υβριδικές Απειλές στο Σύγχρονο Στρατηγικό Περιβάλλον

Όπως είδαμε και νωρίτερα οι υβριδικές απειλές βρίσκονται πλέον στον πυρήνα της συζήτησης για την ασφάλεια. Κράτη αλλά και διεθνείς οργανισμοί όπως το ΝΑΤΟ έχουν ήδη αναπτύξει στρατηγικές για την πρόληψη και την αντιμετώπιση υβριδικών απειλών ενώ κρίσιμη θεωρείται και η ανάγκη για την εμπέδωση της ανθεκτικότητας ειδικότερα στις κρίσιμες υποδομές στις δομές και στις διαδικασίες σε περίπτωση που δεν καταστεί εφικτή η αποτροπή τέτοιων απειλών[1].

2.1 Ορισμός και Χαρακτηριστικά Υβριδικών Απειλών.

Ο όρος υβριδικές απειλές έχει αποδειχθεί ιδιαίτερα δημοφιλής τα τελευταία χρόνια ιδιαίτερα μετά την ρωσο-ουκρανική σύγκρουση το 2014. Σύμφωνα με το ΝΑΤΟ, οι υβριδικές απειλές συνδυάζουν στρατιωτικά και μη στρατιωτικά μέσα με σκοπό να θολώσουν τα όρια μεταξύ πολέμου και ειρήνης με κύριο στόχο να καλλιεργήσουν

[1] Μποζίνης Αθανάσιος, Λιαρόπουλος Ανδρέας, Κωνσταντόπουλος Ιωάννης, «Υβριδικές και Αναδυόμενες Απειλές στις Διεθνείς Σχέσεις». Εκδόσεις Παπαζήση (2025) 10

αμφιβολίες στον πληθυσμό - στόχο.[2] Η ΕΕ χαρακτηρίζει τις υβριδικές απειλές *ως τον συνδυασμό καταναγκαστικής και ανατρεπτικής δραστηριότητας, συμβατικών και μη συμβατικών μεθόδων (π.χ. διπλωματικές, στρατιωτικές, οικονομικές, τεχνολογικές μέθοδοι) που χρησιμοποιούνται με συντονισμένο τρόπο από κρατικούς ή μη κρατικούς παράγοντες για την επίτευξη ειδικών στόχων, παραμένοντας ωστόσο κάτω από το όριο της επίσημης κήρυξης πολέμου*[3]. Για την αντιμετώπιση αυτών των σύνθετων απειλών, δεν αρκεί η μεμονωμένη αντιμετώπιση από ένα κράτος, αλλά αντιθέτως απαιτείται μία ολοκληρωμένη προσέγγιση μεταξύ των κρατών - μελών με σκοπό να διευκολύνεται η συλλογή και αξιολόγηση των πληροφοριών που σχετίζονται με αυτές τις δράσεις.

Ποιες όμως είναι μερικές από τις αιτίες πίσω από την αύξηση των υβριδικών προκλήσεων; Η ραγδαία ανάπτυξη της τεχνολογίας, ο διαρκώς αυξανόμενος αριθμός των χρηστών του διαδικτύου σε συνδυασμό με την ψηφιοποίηση πολλών δομών και διαδικασιών έχουν αυξήσει σε μεγάλο βαθμό και την τρωτότητα από κυβερνοεπιθέσεις. Συμπληρωματικά σε αυτό, η ανάπτυξη της τεχνητής νοημοσύνης αλλά και τεχνολογιών όπως τα μη επανδρωμένα οπλικά συστήματα έδωσαν σε μικρότερους δρώντες, νέες δυνατότητες που μέχρι τώρα ανήκαν αποκλειστικά σε μεγαλύτερες δυνάμεις.

2.2 Μορφές Υβριδικών Απειλών

Οι υβριδικές απειλές όπως έχει ήδη αναφερθεί μπορούν να λάβουν αρκετές μορφές με στρατιωτικά ή μη μέσα. Στο παρόν κεφάλαιο θα εξετάσουμε κάποιες από τις βασικές μορφές αυτών των επιχειρήσεων. Αξίζει να σημειώθεί, ότι η υιοθέτηση μίας συγκεκριμένης μορφής δεν συνεπάγεται τον αποκλεισμό άλλων μορφών. Αντιθέτως, στην πράξη παρατηρείται συχνά η ταυτόχρονη αξιοποίηση υβριδικών δράσεων, οι οποίες λειτουργούν συμπληρωματικά.

Παρόλο που ο υβριδικός πόλεμος τις περισσότερες φορές δεν εκδηλώνεται ως μία συμβατική στρατιωτική σύγκρουση, οι στρατιωτικές ενέργειες αποτελούν σημαντικό σκέλος της έννοιας. Όπως έγινε και αντιληπτό στην περίπτωση της Ουκρανίας κατά τη ρωσο-ουκρανική σύγκρουση (2014) με την εμφάνιση στρατιωτών που δεν έφεραν

[2] NATO, «Countering hybrid threats», 7/5/2024, τελευταία πρόσβαση 20/11/2025 https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[3] Ευρωπαϊκή Επιτροπή, «Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών Απόκριση της Ευρωπαϊκής Ένωσης» τελευταία πρόσβαση 20/11/2025 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52016JC0018

διακριτικά. Έγινε αντιληπτή η προσπάθεια για τη δημιουργία τετελεσμένων χωρίς να είναι εφικτή η άμεση στρατιωτική απάντηση λόγω της εσκεμμένης αμφιβολίας για την προέλευση των εμπλεκομένων.

Μία από τις πιο αναγνωρίσιμες μορφές του υβριδικού πολέμου είναι αυτή των κυβερνοεπιθέσεων. Μέσα από αυτές ο δρών μπορεί να στοχεύσει κρίσιμες υποδομές και δίκτυα επικοινωνιών με σκοπό να αποσπάσει πληροφορίες ή να προκαλέσει αποσταθεροποίηση. Βασικό στοιχείο των κυβερνοεπιθέσεων είναι η ανωνυμία που προσφέρει ο κυβερνοχώρος, καθιστώντας δυσκολότερη την απόδοση ευθυνών.

Οι υβριδικές απειλές μπορούν να λάβουν επίσης και τη μορφή του οικονομικού εξαναγκασμού. Ο οικονομικός εξαναγκασμός μπορεί να προέλθει από κυρώσεις, έλεγχο πρώτων υλών ή ακόμα και από τον έλεγχο των ενεργειακών πόρων με αποτέλεσμα, την πρόκληση οικονομικής αστάθειας και κοινωνικής δυσαρέσκειας.

2.3 Ο ρόλος της πληροφορίας και ο πληροφοριακός πόλεμος (information warfare)

Στο κεφάλαιο αυτό θα εστιάσουμε σε μία ιδιαίτερη μορφή υβριδικής απειλής, αυτής του πληροφοριακού πολέμου (information warfare). Η πληροφορία και συγκεκριμένα η χειραγώγηση αυτής αποτελεί θεμελιώδες στοιχείο για τις υβριδικές προκλήσεις. Ο πληροφοριακός πόλεμος αναφέρεται στη σκόπιμη χρήση οποιασδήποτε πληροφορίας με βασικό στόχο να επηρεαστεί η διαδικασία λήψης αποφάσεων του αντιπάλου και να επιτευχθεί ένας στρατηγικός στόχος.[4] Μέσω της παραπληροφόρησης αλλά και της δημιουργίας στοχευμένων αφηγημάτων οι δρώντες επιδιώκουν να επηρεάσουν την κοινή γνώμη, να υπονομεύσουν τους θεσμούς καθώς και να προκαλέσουν κοινωνικές διαιρέσεις.

Ο πληροφοριακός πόλεμος μπορεί να περιλαμβάνει τη συλλογή κρίσιμων πληροφοριών, τον έλεγχο αξιοπιστίας της πληροφορίας, τη διάδοση προπαγάνδας/ παραπληροφόρησης, την υπονόμευση της πληροφορίας του αντιπάλου καθώς και την άρνηση να συλλέξει πληροφορίες.[5]

[4] Albert, C. D., Mullaney, S., Huitt, J., Hunter, L. Y., & Snider, L. (2023). Weaponizing Words: Using Technology to Proliferate Information Warfare. *The Cyber Defense Review*, *8*(3), 15–32.
[5] Damjanović, D. Z., (2017). TYPES OF INFORMATION WARFARE AND EXAMPLES OF MALICIOUS PROGRAMS OF INFORMATION WARFARE. Vojnotehnicki glasnik/Military Technical Courier, 65(4), 1044-1059.

Η διαμόρφωση αντιλήψεων αλλά και η χειραγώγηση των αφηγημάτων μέσα από την επίδραση που έχουν στην ψυχολογία του στόχου πολλές φορές παράγουν αποτελέσματα αντίστοιχα αν όχι ανώτερα από εκείνα των κλασικών στρατιωτικών μέσων.

Μέσω της ραγδαίας ανάπτυξης του διαδικτύου και ειδικότερα των μέσων κοινωνικής δικτύωσης διευκολύνεται η διασπορά ψευδών ειδήσεων ενώ παράλληλα η χρήση αυτοματοποιημένων λογαριασμών καθιστά την εξάπλωση της πληροφορίας ταχύτερη.

Αναφορικά με το NATO ο πληροφοριακός πόλεμος εγείρει κρίσιμα ζητήματα. Αρχικά μέσα από την προσπάθεια επηρεασμού της κοινής γνώμης, αυξάνεται σημαντικά ο κίνδυνος να μειωθεί η δυνατότητα συλλογικής λήψης αποφάσεων ανάμεσα στα κράτη - μέλη ενώ παράλληλα στοχεύει σε θεμελιώδεις αξίες όπως είναι η δημοκρατική λειτουργία. [6]

3. Μελέτη Περίπτωσης: Ρωσο- ουκρανικός πόλεμος (2022-)

Ο πόλεμος στην Ουκρανία αποτελεί μία από τις πιο χαρακτηριστικές περιπτώσεις όπου υβριδικές τακτικές λαμβάνουν χώρα παράλληλα με τον συμβατικό πόλεμο. Η Ρωσία ήδη από το 2014 κατέστησε ξεκάθαρη τη δυνατότητα της να συνδυάζει τόσο τη στρατιωτική της δράση όσο και τις υβριδικές επιχειρήσεις. Ωστόσο, η ικανότητα της Ρωσίας να διεξάγει τέτοιου είδους επιχειρήσεις δεν αποτελεί κάτι καινούργιο. Στη Σοβιετική Ένωση κατά την περίοδο του Ψυχρού Πολέμου εμφανίζεται η έννοια των ενεργών μέτρων (aktivnyye meropriyatiya) που διαφέρει από την κατασκοπεία, την αντικατασκοπεία και την παραδοσιακή διπλωματία αλλά στοχεύει στην άσκηση επιρροής σε άτομα, κυβερνήσεις ή στην κοινή γνώμη.[7] Αξίζει να σημειωθεί πως η στρατηγική της Ρωσίας στον πληροφοριακό πόλεμο δεν διαφοροποιείται ανάμεσα στην περίοδο ειρήνης και σύγκρουσης ούτε μεταξύ στρατιωτικών και πολιτικών στόχων.[8] Ενώ ακόμα και πιο πρόσφατα η Ρωσία έχει αποδείξει ότι διαθέτει ένα ευρύ δίκτυο σε πλατφόρμες κοινωνικής δικτύωσης για την προώθηση των αφηγημάτων που επιθυμεί.[9]

---

[6] Baptist, J., & Gluck, J. (2021). The Gray Legion: Information Warfare Within Our Gates. *Journal of Strategic Security*, *14*(4), 37–55.
[7] Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, *11*(4), 50–85.
[8] Mullaney, S. (2022). Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020. *The Cyber Defense Review*, *7*(4), 193–212.
[9] Hanlon, B. (2018). *It's Not Just Facebook: Countering Russia's Social Media Offensive*. German Marshall Fund of the United States.

Ένας από τους πιο καταλυτικούς παράγοντες στη χρήση των social media αποτέλεσε και η χρήση αυτοματοποιημένων λογαριασμών. [10]

Με την έναρξη του πολέμου το 2022, βασικός στόχος της Ρωσίας συμπληρωματικά με τις στρατιωτικές επιχειρήσεις ήταν να δημιουργήσει ένα ολοκληρωμένο πλαίσιο υβριδικών επιθέσεων που θα επηρεάσουν τόσο το επιχειρησιακό πεδίο όσο και το ευρύτερο διεθνές πλαίσιο. Πρόθεση της Ρωσίας αποτέλεσε η υπονόμευση της ουκρανικής ανθεκτικότητας και της δυτικής συνοχής.

Η Ρωσία μέσω του πληροφοριακού πολέμου, προσπάθησε να αποπροσανατολίσει τον ουκρανικό πληθυσμό προσπαθώντας με αυτόν τον τρόπο να πλήξει την εμπιστοσύνη στους θεσμούς αλλά και την ηγεσία της χώρας. Η διάδοση αφηγημάτων περί κατάρρευσης της ουκρανικής κυβέρνησης και της φυγής του προέδρου της Ουκρανίας Ζελένσκι στόχευε στην αποδυνάμωση της επιχειρησιακής λειτουργίας των ουκρανικών ενόπλων δυνάμεων, στην υπονόμευση της ηθικής αντοχής και στην επιρροή της διεθνούς κοινής γνώμης.

Πιο συγκεκριμένα, βασικοί στόχοι της Ρωσίας αποτέλεσαν η πτώση του ηθικού του στρατού και του πληθυσμού, η διαστρέβλωση γεγονότων αναφορικά με την ανάγκη της ρωσικής στρατιωτικής επιχείρησης, και τέλος, η υποστήριξη μερίδας τόσο του ουκρανικού λαού όσο και του δυτικού κόσμου στις επιλογές της Ρωσίας.[11] Κάποια από τα βασικά αφηγήματα που χρησιμοποίησε η Ρωσία για να καταφέρει να επηρεάσει τη κοινή γνώμη ήταν:

1. Εξαναγκαστική επιστράτευση: παρουσιαζόταν άτομα που η Ρωσία υποστήριζε ότι εξαναγκάζονταν να καταταχθούν στον ουκρανικό στρατό,
2. Διαφθορά πολιτικών προσώπων: Μέσα από την παρουσίαση αυτών των εικόνων η Ρωσία προσπάθησε να καλλιεργήσει την άποψη ότι δεν αξίζει κανείς να θυσιαστεί για ένα διεφθαρμένο καθεστώς.
3. Δωροδοκία ανώτατων αξιωματικών: Όπως και στην προηγούμενη περίπτωση, παρουσιάστηκαν αξιωματικοί των ενόπλων δυνάμεων ως διεφθαρμένοι. [12]

---

[10] Marigliano, R., Ng, L.H.X. & Carley, K.M. Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Soc. Netw. Anal. Min.* **14**, 170 (2024).

[11] Liaropoulos, Andrew Information as an Instrument of Power - Lessons learned from the War in Ukraine, NATO OPEN Publications, vol.7, no.6 (2022)

[12] Mysyshyn, A. (2024). AI in Information Warfare. In *Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights* (pp. 14–17). German Marshall Fund of the United States.

Ως απάντηση η Ουκρανία έδωσε ιδιαίτερη έμφαση στην πληροφοριακή διάσταση του πολέμου. Υιοθέτησε μία στρατηγική επικοινωνιακή προσέγγιση που μέσα από τα κοινωνικά δίκτυα επιχείρησε να προβάλει τα δικά της μηνύματα ως απάντηση στα ρωσικά αφηγήματα, προσπαθώντας παράλληλα να διασφαλίσει και την υποστήριξη της Δύσης. Την ίδια στιγμή, αξιοποίησε και τις νέες τεχνολογίες και ειδικότερα το κομμάτι των UAV τα οποία χρησιμοποίησε σε μεγάλο βαθμό για τη συλλογή πληροφοριών.

Ειδικότερα σε αντίθεση με την περίπτωση της Κριμαίας, η ηγεσία της Ουκρανίας απάντησε πολύ γρήγορα στις πληροφοριακές επιχειρήσεις της Ρωσίας προσπαθώντας να διαδώσει το δικό της αφήγημα. Εξέφρασε την υποστήριξή της στις ένοπλες δυνάμεις και τον λαό της Ουκρανίας, προσπάθησε να ενισχύσει το ηθικό του στρατιωτικού προσωπικού αναφορικά με την έκβαση του πολέμου, υπογράμμισε την απομόνωση και τις συνέπειες που θα αντιμετωπίσει η Ρωσία, ενώ τόνισε και την ανάγκη για διεθνή βοήθεια.[13] Η Ουκρανία κατάφερε μέσα από την επικοινωνιακή της στρατηγική να κερδίσει τη δημόσια υποστήριξη, ενώ παράλληλα δεν παρέλειψε αρκετές φορές να δημοσιοποιήσει οπτικό υλικό από τις νίκες της στα πεδία των μαχών. [14]

Το ΝΑΤΟ, έχοντας πλέον αναλάβει αρκετές πρωτοβουλίες μετά το 2014, ενίσχυσε άμεσα μετά την έναρξη του πολέμου τόσο τους μηχανισμούς ανάλυσης και ανταλλαγής πληροφοριών ενώ παράλληλα έλαβε μέτρα για την αντιμετώπιση της παραπληροφόρησης. Σημαντικό στοιχείο στην αντίδραση του ΝΑΤΟ αποτέλεσε και η έμφαση που δόθηκε στον τομέα της κυβερνοασφάλειας.

Συμπεράσματα

Δεν χωράει αμφιβολία πως οι υβριδικές απειλές αποτελούν και θα συνεχίσουν να αποτελούν κεντρικό παράγοντα του στρατηγικού σχεδιασμού ασφάλειας κάθε κράτους και διεθνούς οργανισμού. Η σύγκρουση Ρωσίας - Ουκρανίας, κατέδειξε με σαφή τρόπο πως οι πληροφοριακές επιχειρήσεις, η παραπληροφόρηση και η ψηφιακή τεχνολογία αποτελούν οργανικό κομμάτι του στρατηγικού σχεδιασμού ασφάλειας.

Παράλληλα, κατέστη σαφές πως η ικανότητα μία χώρας να διαμορφώνει, να μεταδίδει και να προστατεύει την πληροφορία, επηρεάζει σε μεγάλο βαθμό τη δυνατότητά της

[13] Liaropoulos, Andrew Information as an Instrument of Power - Lessons learned from the War in Ukraine, NATO OPEN Publications, vol.7, no.6 (2022)
[14] Bronk, C., Collins, G., & Wallach, D. S. (2023). The Ukrainian Information and Cyber War. *The Cyber Defense Review*, *8*(3), 33–50.

να διαφυλάξει τη διεθνή υποστήριξη και την εμπιστοσύνη της κοινής γνώμης. Όπως και στην περίπτωση της Ουκρανίας αποδείχθηκε ότι η διατήρηση της δημοκρατίας εξαρτάται σε μεγάλο βαθμό από την ικανότητα των πολιτών να αναγνωρίζουν κακόβουλες πληροφορίες. Σε αυτή την προσπάθεια αξίζει να υπογραμμιστεί η επίδραση της τεχνολογίας που καθορίζει σημαντικά, τον τρόπο με τον οποίο η πληροφορία μεταδίδεται και καταναλώνεται. Η ραγδαία ταχύτητα με την οποία η πληροφορία κινείται πολλές φορές δεν επιτρέπει την έγκαιρη επαλήθευσή της.

Το ΝΑΤΟ για να μπορέσει να αντιμετωπίσει τέτοιες απειλές θα πρέπει να υιοθετήσει ένα κοινό πλαίσιο ανάλυσης πληροφοριακού πολέμου, ενώ παράλληλα θα πρέπει να επενδύσει στην ανθεκτικότητα. Συμπληρωματικά σε αυτό, μέσα από την τεχνολογία οφείλει να δημιουργήσει εργαλεία και πρωτόκολλα με τα οποία θα μπορεί να ανιχνεύει όσο το δυνατόν ταχύτερα τα fake news, τα deepfakes και γενικότερα τα εργαλεία που χρησιμοποιούνται για τη δημιουργία αφηγημάτων. Αξίζει να σημειωθεί πως η κρισιμότητα των υβριδικών απειλών αποδεικνύεται και από το γεγονός ότι το ΝΑΤΟ πλέον μπορεί να ενεργοποιήσει το Άρθρο 5 σε περίπτωση που κράτος-μέλος δεχθεί κάποια υβριδική επίθεση.

Η σύγκρουση αποτελεί μια σύνθετη, πολυεπίπεδη υβριδική αντιπαράθεση, όπου η πληροφορία, η τεχνολογία και η κοινωνική συνοχή λειτουργούν ως κρίσιμοι πολλαπλασιαστές ισχύος. Συμπερασματικά, η αντιμετώπιση του πληροφοριακού πολέμου δεν αποτελεί ένα ακόμα τεχνικό ζήτημα. Συνιστά θεμελιώδη προϋπόθεση για τη διατήρηση της δημοκρατίας, την εμπιστοσύνη στους θεσμούς, την αποτελεσματικότητα της συλλογικής και εθνικής άμυνας αλλά και της κοινωνικής ανθεκτικότητας. Παράγοντες που επηρεάζουν άμεσα την έκβαση μίας σύγκρουσης.