Επιθεώρηση Δημοσίου & Διεθνούς Δικαίου

Φοιτητικό Επιστημονικό Περιοδικό Δημοσίου & Διεθνούς Δικαίου της Νομικής Σχολής του Πανεπιστημίου Αθηνών

ΤΕΥΧΟΣ 1 | ΕΤΟΣ Α΄ | ΟΚΤΩΒΡΙΟΣ

ΑΡΘΡΟ

Στρατιωτικοί στόχοι στην εποχή των κυβερνοεπιθέσεων: Επανερμηνεύοντας την αρχή της διάκρισης

Λυδία Ρακοπούλου[1]

Abstract. Ο σύγχρονος κόσμος, χαρακτηριζόμενος από ραγδαία τεχνολογική εξέλιξη και εκτεταμένη ψηφιοποίηση, επιφέρει και νέους τρόπους διεξαγωγής εχθροπραξιών, μεταξύ των οποίων εξέχουσα θέση κατέχουν οι κυβερνοεπιχειρήσεις. Στο πλαίσιο αυτό, η αρχή της διάκρισης, ως θεμελιώδης κανόνας του Διεθνούς Ανθρωπιστικού Δικαίου, επιβάλλει την σαφή διάκριση μεταξύ πολιτικών και στρατιωτικών στόχων, διασφαλίζοντας την αποτελεσματική προστασία του άμαχου πληθυσμού. Ωστόσο, ο προσδιορισμός της έννοιας του «στρατιωτικού στόχου», του «αντικειμένου» και της «επίθεσης» στον κυβερνοπόλεμο αναδεικνύει ιδιαίτερες δυσχέρειες. Η παρούσα μελέτη εξετάζει κατά πόσο η παραδοσιακή έννοια του στρατιωτικού στόχου ανταποκρίνεται στις ιδιαιτερότητες του ψηφιακού πεδίου σύγκρουσης, εξετάζει την υλική και λειτουργική προσέγγισή του και διερευνά την ανάγκη ερμηνευτικής προσαρμογής της έννοιας και, κατ' επέκταση, της αρχής της διάκρισης υπό το πρίσμα των κυβερνοεπιχειρήσεων.

[1] Η Λυδία Ρακοπούλου είναι Προπτυχιακή Φοιτήτρια της Νομικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

Πίνακας περιεχομένων

Πίνακας περιεχομένων **62**

Εισαγωγή **63**

Η Αρχή Της Διάκρισης Και Η Έννοια Του Στρατιωτικού Στόχου Στο Διεθνές Ανθρωπιστικό Δίκαιο **66**

Ο Κυβερνοχώρος ως Νέο Πεδίο Στρατιωτικών Επιχειρήσεων **69**

Τα Ιδιαίτερα Χαρακτηριστικά του Κυβερνοχώρου **69**

Η Διασυνδεσιμότητα των Πληροφοριακών Συστημάτων & τα Αντικείμενα Διττής Χρήσης **72**

Ο Προσδιορισμός του Στρατιωτικού Στόχου Στις Κυβερνοεπιθέσεις **73**

Η Οριοθέτηση του «Αντικειμένου» **73**

Η Υλική Προσέγγιση **74**

Η Λειτουργική Προσέγγιση **75**

Το Ζήτημα των Δεδομένων **76**

Προς μια Επανερμηνεία του Στρατιωτικού Στόχου; **76**

Αξιολόγηση της Υλικής και της Λειτουργικής Προσέγγισης **76**

Συμπεράσματα & Προοπτικές Εξέλιξης του ΔΑΔ **79**

Βιβλιογραφία **83**

Εισαγωγή

Η ταχεία ψηφιοποίηση των κρατικών λειτουργιών και η αυξανόμενη εξάρτηση των σύγχρονων κοινωνιών από τα πληροφοριακά συστήματα έχουν μεταβάλει ουσιωδώς τον τρόπο διεξαγωγής των ενόπλων συγκρούσεων. Η νέα αυτή ψηφιοποιημένη πραγματικότητα οδήγησε στην εξέλιξη του κυβερνοχώρου σε αυτόνομο «πεδίο μάχης», εντός του οποίου κράτη και μη κρατικοί δρώντες δύνανται να προβαίνουν σε επιχειρήσεις ικανές να επηρεάσουν καθοριστικά τη διεξαγωγή των εχθροπραξιών. Οι κυβερνοεπιθέσεις δεν αποτελούν μεμονωμένα περιστατικά, και δεν περιορίζονται πλέον στην υποκλοπή πληροφοριών ή στην παραβίαση της εμπιστευτικότητας δεδομένων, αλλά μπορούν να επηρεάσουν άμεσα τη λειτουργία κρίσιμων υποδομών, να διαταράξουν τις στρατιωτικές επικοινωνίες ή να παραλύσουν συστήματα υγείας και μεταφορών. Πρόκειται για μια καινούρια τακτική πρακτική που ενσωματώνεται στις στρατιωτικές στρατηγικές των κρατών.[2] Η εξέλιξη αυτή καταδεικνύει ότι ο κυβερνοχώρος δεν αποτελεί πλέον απλώς ένα νέο τεχνολογικό περιβάλλον, αλλά έναν χώρο όπου είναι δυνατόν οι εχθροπραξίες να λάβουν διαστάσεις συγκρίσιμες με εκείνες των συμβατικών στρατιωτικών επιχειρήσεων.

Η ανωτέρω διαπίστωση έχει οδηγήσει στην διεθνή αναγνώριση του κυβερνοχώρου ως την πέμπτη ζώνη πολέμου, μαζί με την ξηρά, τη θάλασσα, τον αέρα και το διάστημα.[3] Ωστόσο, η αναγνώριση αυτή δεν συνοδεύτηκε από την υιοθέτηση ενός νέου, εξειδικευμένου διεθνούς νομικού καθεστώτος. Αντιθέτως, η κρατούσα άποψη στη θεωρία και στην κρατική πρακτική υποστηρίζει πως το νομικό πλαίσιο του Διεθνούς Ανθρωπιστικού Δικαίου (ΔΑΔ)[4] εξακολουθεί να

[2] Gisel, Rodenhäuser, and Dörmann , *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 3.
[3] Weisbord, *The Crime of Aggression*, 2019, 134.
[4] Το νομικό αυτό πλαίσιο αποτελείται κυρίως από τις 4 Συμβάσεις της Γενεύης (1949) και το Πρόσθετο Πρωτόκολλο Ι (1977) – που συνιστούν το εν στενή εννοία ΔΑΔ - αλλά και τη Σύμβαση της Χάγης (1907) για τους κανόνες που αφορούν στη διεξαγωγή του πολέμου, τις συμβάσεις που αφορούν στη ρύθμιση των επί μέρους όπλων (π.χ. Σύμβαση για Ορισμένα Συμβατικά Όπλα του 1980, Σύμβαση για τα Χημικά Όπλα του

εφαρμόζεται και στις κυβερνοεπιχειρήσεις, καθώς οι κανόνες του δικαίου των ενόπλων συγκρούσεων ισχύουν για όλες τις μορφές πολέμου και όλα τα είδη όπλων, συμπεριλαμβανομένων εκείνων «*του μέλλοντος*».[5] Επομένως, το κρίσιμο ζήτημα δεν είναι αν το ΔΑΔ εφαρμόζεται στον κυβερνοχώρο, αλλά με ποιον τρόπο οι παραδοσιακές έννοιες και οι κανόνες του μπορούν να προσαρμοστούν στις ιδιαιτερότητες του νέου αυτού πεδίου συγκρούσεων ώστε να διασφαλίζεται η αποτελεσματική προστασία των αμάχων.

Συγκεκριμένα, οι ιδιαιτερότητες του κυβερνοχώρου αναδεικνύουν την ανάγκη επανεξέτασης του τρόπου εφαρμογής ορισμένων θεμελιωδών αρχών του ΔΑΔ. Κεντρική θέση μεταξύ αυτών κατέχει η αρχή της διάκρισης *(principle of distinction),* η οποία αποτελεί τον ακρογωνιαίο λίθο της προστασίας των αμάχων αλλά και των αστικών αντικειμένων κατά τη διάρκεια των ενόπλων συγκρούσεων.[6] Η αρχή αυτή αποτυπώνει τη βασική επιδίωξη του ΔΑΔ να περιορίσει τις συνέπειες των εχθροπραξιών στους νόμιμους στρατιωτικούς στόχους και να διατηρήσει μία ισορροπία μεταξύ στρατιωτικής αναγκαιότητας και ανθρωπιστικής προστασίας.

Η αποτελεσματική εφαρμογή της αρχής της διάκρισης προϋποθέτει, ωστόσο, τη δυνατότητα σαφούς προσδιορισμού της έννοιας του «στρατιωτικού στόχου». Στο πλαίσιο των παραδοσιακών ενόπλων συγκρούσεων αυτή στηρίζεται στην παραδοχή ότι ο χαρακτηρισμός ενός αντικειμένου ως στρατιωτικού στόχου μπορεί, κατά κανόνα, να πραγματοποιηθεί βάσει αντικειμενικών και ευχερώς διαπιστώσιμων κριτηρίων, τα οποία θα παρατεθούν αναλυτικά κατωτέρω. Η παραδοχή αυτή, ωστόσο, δοκιμάζεται στον κυβερνοχώρο όπου τα όρια μεταξύ στρατιωτικών και αστικών αντικειμένων καθίστανται ιδιαίτερα δυσδιάκριτα.[7] Η πλειονότητα των ψηφιακών υποδομών εξυπηρετεί ταυτόχρονα

1993) και, τέλος τους εθιμικούς κανόνες ανθρωπιστικού δικαίου και τους γενικά παραδεδεγμένους κανόνες δικαίου.

[5] Gisel, Rodenhäuser, and Dörmann , *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 12-13. Schmitt, *Tallinn Manual 2.0*, 2017, *Κανόνας 80*, παρ. 1.

[6] ICRC, *The Principle Of Distinction (Cyber Operations During Armed Conflict)*, 2023, 1.

[7] Geiß, Lahmann, *Cyber warfare: Applying the principle of distinction in an interconnected space*, 2012, 381.

στρατιωτικές και αστικές λειτουργίες, ενώ η ίδια τεχνολογική υποδομή μπορεί να χρησιμοποιείται από τις ένοπλες δυνάμεις, δημόσιες υπηρεσίες, ιδιωτικές επιχειρήσεις και ιδιώτες χρήστες.[8]

Παράλληλα, ο άυλος χαρακτήρας των περισσότερων στοιχείων του κυβερνοχώρου δημιουργεί πρόσθετες ερμηνευτικές δυσχέρειες. Σε αντίθεση με τα παραδοσιακά υλικά αντικείμενα, οι κυβερνοεπιθέσεις στρέφονται συχνά κατά δεδομένων, λογισμικού ή λειτουργιών πληροφοριακών συστημάτων, χωρίς να προκαλείται αναγκαστικά φυσική καταστροφή του υλικού εξοπλισμού. Το γεγονός αυτό εγείρει το κρίσιμο ερώτημα κατά πόσον τα δεδομένα μπορούν να θεωρηθούν «αντικείμενα» υπό την έννοια του άρθρου 52 του Πρώτου Πρόσθετου Πρωτοκόλλου των Συμβάσεων της Γενεύης,[9] και, κατ' επέκταση, εάν είναι δυνατόν να χαρακτηριστούν ως στρατιωτικοί στόχοι.[10] Η απουσία ομοφωνίας στη διεθνή θεωρία και πρακτική έχει οδηγήσει στην ανάπτυξη διαφορετικών ερμηνευτικών προσεγγίσεων, οι οποίες προτείνουν είτε μια στενά υλική είτε μια ευρύτερη λειτουργική αντίληψη της έννοιας του στρατιωτικού στόχου στις κυβερνοεπιθέσεις.

Υπό το πρίσμα των ανωτέρω, καθίσταται εμφανές ότι η εφαρμογή της αρχής της διάκρισης στον κυβερνοχώρο δεν μπορεί να συνίσταται σε απλή μεταφορά των παραδοσιακών κανόνων του ΔΑΔ σε ένα νέο τεχνολογικό περιβάλλον, αλλά απαιτεί την επανεξέταση βασικών εννοιών υπό το φως των ιδιαιτεροτήτων των κυβερνοεπιχειρήσεων. Η παρούσα μελέτη εξετάζει κατά πόσον η παραδοσιακή έννοια του στρατιωτικού στόχου, όπως αποτυπώνεται στο άρθρο 52 παρ. 2 του Πρώτου Πρόσθετου Πρωτοκόλλου,[11] επαρκεί για την αντιμετώπιση των ιδιαιτεροτήτων των κυβερνοεπιθέσεων.

---

[8] ICRC, *The Principle Of Distinction (Cyber Operations During Armed Conflict)*, 2023, 1.

[9] Άρθρο 52, *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*

[10] Gisel, Rodenhäuser, and Dörmann , *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 31.

[11] Ν. 1786/1988 *«Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*

Ειδικότερα, πρόκειται να αναλυθεί η έννοια του στρατιωτικού στόχου υπό το ισχύον ΔΑΔ, να εξετασθούν οι ιδιαιτερότητες του κυβερνοχώρου ως σύγχρονου πεδίου ενόπλων συρράξεων και να παρουσιασθούν οι κυριότερες ερμηνευτικές προσεγγίσεις που έχουν αναπτυχθεί στη θεωρία, με ιδιαίτερη έμφαση στις θέσεις του Tallinn Manual - ενός μη δεσμευτικού εγχειριδίου που συντάχθηκε από ομάδα ανεξάρτητων εμπειρογνωμόνων διεθνούς δικαίου με πρωτοβουλία του Συνεργατικού Κέντρου Αριστείας για την Κυβερνοάμυνα του NATO, με σκοπό να αποσαφηνίσει την εφαρμογή των υφιστάμενων κανόνων του διεθνούς δικαίου στις κυβερνοεπιχειρήσεις, καθώς και στις θέσεις της Διεθνούς Επιτροπής του Ερυθρού Σταυρού. Τελικός σκοπός είναι να αξιολογηθεί αν η υφιστάμενη ερμηνεία της έννοιας του στρατιωτικού στόχου εξακολουθεί να διασφαλίζει την αποτελεσματική προστασία των αμάχων ή εάν οι εξελίξεις στον κυβερνοχώρο επιβάλλουν μία περισσότερο λειτουργική και τεχνολογικά προσαρμοσμένη προσέγγιση.

Η εξέταση της έννοιας του στρατιωτικού στόχου στο πλαίσιο των κυβερνοεπιχειρήσεων προϋποθέτει, αρχικώς, την ανάλυση του κανονιστικού πλαισίου που διέπει τη νομιμότητα των επιθέσεων στο ΔΑΔ. Η αρχή της διάκρισης βρίσκεται στο κέντρο του πλαισίου αυτού. Ως εκ τούτου, η κατανόηση του περιεχομένου, του σκοπού και των ορίων αυτής αποτελεί αναγκαία προϋπόθεση για την αξιολόγηση των ερμηνευτικών ζητημάτων που ανακύπτουν στον κυβερνοχώρο.

Η Αρχή Της Διάκρισης Και Η Έννοια Του Στρατιωτικού Στόχου Στο Διεθνές Ανθρωπιστικό Δίκαιο

Η αρχή της διάκρισης *(principle of distinction)* αποτελεί τον ακρογωνιαίο λίθο και μια από τις παλαιότερες αρχές του ΔΑΔ.[12] Το Διεθνές Δικαστήριο της Χάγης τη χαρακτηρίζει ως «θεμελιώδη» και «απαραβίαστη» αρχή που αποτελεί μέρος της ίδιας της «υπόστασης» του δικαίου των ένοπλων συγκρούσεων.[13] Η εφαρμογή της είναι καθολική καθώς εφαρμόζεται τόσο σε διεθνείς όσο και μη διεθνείς

[12] ICRC, *The Principle Of Distinction (Cyber Operations During Armed Conflict)*, 2023, 1.
[13] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996, παρ. 78–79.

ένοπλες συρράξεις, ενώ η αναγνώρισή της ως κανόνα διεθνούς εθιμικού δικαίου εξασφαλίζει την δέσμευση όλων των κρατών, ανεξάρτητα από το αν έχουν επικυρώσει τα Πρόσθετα Πρωτόκολλα των Συμβάσεων της Γενεύης.[14] Η κύρια συμβατική κωδικοποίηση της αρχής για τις διεθνείς ένοπλες συγκρούσεις βρίσκεται στο Άρθρο 48 του Πρώτου Πρόσθετου Πρωτοκόλλου[15] και συνίσταται στην ανάγκη των μερών μιας ένοπλης σύγκρουσης να διακρίνουν πάντοτε μεταξύ πολιτών (αμάχων) και μαχητών και μεταξύ αστικών αντικειμένων και στρατιωτικών στόχων, κατευθύνοντας κατά συνέπεια τις επιχειρήσεις τους αποκλειστικά κατά των τελευταίων.

Αναπόσπαστα συνδεδεμένη με αυτή είναι η απαγόρευση των αδιάκριτων επιθέσεων, όπως αυτή προβλέπεται στην παρ. 4 του Άρθρου 51 του Πρώτου Πρόσθετου Πρωτοκόλλου. Σύμφωνα με αυτό: *«Επιθέσεις, άνευ διακρίσεως, απαγορεύονται. Επιθέσεις, άνευ διακρίσεως, είναι: α) αυτές, που δεν κατευθύνονται σε ειδικό στρατιωτικό στόχο, β) αυτές, οι οποίες χρησιμοποιούν μία μέθοδο ή μέσον μάχης που δε δύναται να κατευθύνεται σε συγκεκριμένο στρατιωτικό στόχο ή, γ) αυτές οι οποίες χρησιμοποιούν μέθοδο ή μέσο μάχης, τα αποτελέσματα της οποίας δεν μπορεί να είναι περιορισμένα, όπως απαιτείται από το παρόν Πρωτόκολλο και κατά συνέπεια, σε καθεμία από αυτές τις περιπτώσεις, είναι τέτοιας φύσεως ώστε να πλήττουν στρατιωτικούς στόχους και ιδιώτες ή αστικούς στόχους χωρίς διάκριση.»*[16] Με τον τρόπο αυτό, η αρχή της διάκρισης λειτουργεί ως μηχανισμός εξισορρόπησης μεταξύ της στρατιωτικής αναγκαιότητας και της ανθρωπιστικής προστασίας, επιτρέποντας στα εμπλεκόμενα μέρη να επιδιώκουν νόμιμους στρατιωτικούς σκοπούς χωρίς να προκαλούν αδικαιολόγητες βλάβες στον άμαχο πληθυσμό.

Στο σημείο αυτό καθίσταται σαφές ότι η αποτελεσματικότητα της αρχής της διάκρισης εξαρτάται

---

[14] *Ibid.*, Henckaerts, Doswald-Beck, *Customary International Humanitarian Law, Vol. 1*, 2005, Commentary Rule 1 at 3ff.

[15] Άρθρο 48 *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*

[16] Άρθρο 51 παρ. 4, *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*

άμεσα από τον σαφή προσδιορισμό των αντικειμένων που μπορούν νομίμως να αποτελέσουν αντικείμενο επίθεσης. Εάν δεν είναι δυνατή η ασφαλής διάκριση μεταξύ αστικών αντικειμένων και στρατιωτικών στόχων, ο κίνδυνος υπονόμευσης της ίδιας της αρχής παρουσιάζεται μεγάλος, έως και αυτονόητος. Για τον λόγο αυτό, θεμελιώδη σημασία αποκτά η έννοια του στρατιωτικού στόχου, όπως αυτή διαμορφώνεται στην παρ. 2 του Άρθρου 52 του Πρώτου Πρόσθετου Πρωτοκόλλου.[17]

Σύμφωνα με την διάταξη αυτή, προκειμένου να χαρακτηριστεί ένα αντικείμενο ως στρατιωτικός στόχος πρέπει να συντρέχουν δύο θεμελιώδεις προϋποθέσεις. Αρχικώς, το αντικείμενο πρέπει να προσφέρει εκ της φύσεως, της τοποθεσίας, του σκοπού ή της χρήσης του μια αποτελεσματική συμβολή στην στρατιωτική δράση. Η «φύση» αναφέρεται σε αντικείμενα που είναι εγγενώς στρατιωτικά, ήτοι όπλα, στρατώνες και στρατιωτικά συστήματα επικοινωνιών.[18] Η «τοποθεσία» αφορά γεωγραφικά σημεία τα οποία αποκτούν μια ιδιαίτερη στρατιωτική σημασία, όπως ένα στρατιωτικό πέρασμα.[19] Τέλος, ο «σκοπός» αναφέρεται στην επιδιωκόμενη μελλοντική χρήση ενός αντικειμένου για στρατιωτικούς σκοπούς,[20] ενώ η «χρήση» συνίσταται ακριβώς στην τροπή πολιτικών αντικειμένων σε στρατιωτικών όταν αξιοποιούνται για στρατιωτικούς στόχους.[21] Ως δεύτερη προϋπόθεση, πρέπει η μερική ή ολική καταστροφή, κατάληψη ή εξουδετέρωση του αντικειμένου να προσφέρει, υπό τις επικρατούσες συνθήκες, ένα σαφές στρατιωτικό πλεονέκτημα στον επιτιθέμενο. Το πλεονέκτημα αυτό απαιτείται να είναι συγκεκριμένο και αντιληπτό, όχι υποθετικό και απροσδιόριστο. Επιπλέον, απαιτείται να έχει στρατιωτική φύση και να αποκτάται από την επίθεση στο σύνολό της, όχι μόνο από μέρη ή τμήματα αυτής.[22]

---

[17] Ν. 1786/1988 *«Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*
[18] Pascucci, *Distinction and Proportionality in Cyber War*, 2017, 435.
[19] *Ibid.*
[20] *Ibid.*
[21] Pascucci, *Distinction and Proportionality in Cyber War*, 2017, 435.
[22] *Ibid.*

Σε αντίθεση με τα στρατιωτικά, τα αστικά αντικείμενα ορίζονται *a contrario* στην παρ. 1 του Άρθρου 52 του Πρόσθετου Πρωτοκόλλου Ι ως *«όλα όσα δεν είναι στρατιωτικά αντικείμενα κατά την έννοια της παραγράφου 2»* και απαγορεύεται ρητά να αποτελέσουν αντικείμενο επίθεσης.[23] Ακριβώς τα ίδια κριτήρια για τον χαρακτηρισμό ενός αντικειμένου ως στρατιωτικό και αστικό στόχο αντίστοιχα υιοθετεί και το Εγχειρίδιο του Ταλλίν σχετικά με το εφαρμόσιμο διεθνές δίκαιο στις κυβερνοεπιχειρήσεις στον Κανόνα 100.[24]

Η Διεθνής Επιτροπή του Ερυθρού Σταυρού φαίνεται να υποστηρίζει μία μάλλον περιοριστική προσέγγιση της έννοιας του στρατιωτικού στόχου, δίνοντας έμφαση στην ανάγκη στενής ερμηνείας των εξαιρέσεων από αυτήν και στον αποκλεισμό πιθανών έμμεσων πλεονεκτημάτων.[25] Στο ίδιο πνεύμα κινείται και το τεκμήριο της παρ. 3 του Άρθρου 52 του Πρώτου Πρόσθετου Πρωτοκόλλου, σύμφωνα με το οποίο, σε περίπτωση αμφιβολίας ως προς το εάν ένα αντικείμενο χρησιμοποιείται για στρατιωτικούς σκοπούς, αυτό θεωρείται αστικό αντικείμενο.[26] Επιπροσθέτως, η Επιτροπή απορρίπτει σθεναρά την ερμηνεία ότι οικονομικά αντικείμενα που απλώς συντηρούν την ικανότητα διεξαγωγής πολέμου συνιστούν στρατιωτικούς στόχους, υποστηρίζοντας ότι ο σύνδεσμος με το απαιτούμενο *«στρατιωτικό πλεονέκτημα»* είναι πολύ απομακρυσμένος.[27]

Ο Κυβερνοχώρος ως Νέο Πεδίο Στρατιωτικών Επιχειρήσεων

Τα Ιδιαίτερα Χαρακτηριστικά του Κυβερνοχώρου

[23] Άρθρο 52 παρ. 1 *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*
[24] Schmitt, *Tallinn Manual 2.0*, 2017, 435-438.
[25] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (Report prepared...for the 28th International Conference of the Red Cross and Red Crescent 2003), 2025, 4.
[26] Άρθρο 52 παρ. 3 *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*
[27] Hathaway, Khan & Revkin, *The Dangerous Rise of "Dual-Use" Objects in War*, 2024, 2738.

Η εφαρμογή των ανωτέρω κανόνων προϋποθέτει, κατ' αρχήν, ότι το αντικείμενο της επίθεσης μπορεί να προσδιορισθεί και να χαρακτηρισθεί με σχετική σαφήνεια, με βάσει τα προαναφερθέντα κριτήρια. Ωστόσο, η τήρηση των επιταγών της αρχής της διάκρισης και, κατ' επέκταση, της απαγόρευσης των αδιάκριτων επιθέσεων, καθίστανται ιδιαίτερα δυσχερείς στο πλαίσιο του κυβερνοχώρου, του οποίου τα γνωρίσματα δεν προσιδιάζουν σε αυτά του παραδοσιακού πεδίου μάχης, βάσει του οποίου διαμορφώθηκε αρχικώς το συμβατικό ΔΑΔ.

Η Διεθνής Επιτροπή του Ερυθρού Σταυρού ορίζει ειδικώς τις κυβερνοεπιχειρήσεις στο πλαίσιο μίας ένοπλης σύγκρουσης ως «*επιχειρήσεις εναντίον ενός υπολογιστικού συστήματος ή δικτύου, ή άλλης συνδεδεμένης συσκευής, μέσω μιας ροής δεδομένων, όταν χρησιμοποιούνται ως μέσο ή μέθοδος πολέμου*».[28] Ο τομέας αυτός πολέμου αποτελεί μια γραφική αναπαράσταση δεδομένων που αντλούνται από κάθε υπολογιστικό σύστημα, δημιουργώντας ένα περιβάλλον εξαιρετικής τεχνικής πολυπλοκότητας. Κατά συνέπεια, πρόκειται για έναν χώρο με πληθώρα χαρακτηριστικών που τον καθιστούν ένα μοναδικό και εξαιρετικά περίπλοκο πεδίο μάχης, όπου το ΔΑΔ χρήζει προσαρμογής προκειμένου να εφαρμοστεί αποτελεσματικά.

Αρχικώς, η ανώνυμη και εικονική φύση του κυβερνοχώρου μεταβάλλει την παραδοσιακή έννοια των απτών και σαφών γεωγραφικών συνόρων, με αποτέλεσμα να παρουσιάζεται πολύπλοκος και προβληματικός ο προσδιορισμός της κρατικής κυριαρχίας όσον αφορά τις επιθέσεις.[29] Ένα πληροφοριακό σύστημα μπορεί να προσβληθεί από οπουδήποτε στον κόσμο, ενώ τα δεδομένα που το απαρτίζουν ενδέχεται να φιλοξενούνται ταυτόχρονα σε διακομιστές διαφορετικών κρατών. Συναφώς, η ταυτοποίηση του δράστη μιας κυβερνοεπίθεσης είναι εξίσου δύσκολη και χρονοβόρα εξαιτίας της χρήσης τεχνικών απόκρυψης όπως τα

[28] Gisel, Rodenhäuser, and Dörmann , *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 11.
[29] Weisbord, *The Crime of Aggression*, 2019, 141.

VPNs,[30] αλλά και τους πολέμους μέσω πληρεξουσίων (*proxy wars*), αποποιούμενα της ευθύνης τους.[31]

Κατά δεύτερον, οι ταχύτητες με τις οποίες εκτελούνται οι επιχειρήσεις στον κυβερνοχώρο οδηγούν στην ακαριαία πληγή στόχων σε οποιοδήποτε σημείο του πλανήτη και στην ραγδαία εξάπλωση προπαγάνδας, η οποία συνιστά κομβικό στοιχείο της στρατηγικής των ψηφιακών πολέμων, καταργώντας τους περιορισμούς του χρόνου και της φυσικής απόστασης.[32] Επιπροσθέτως, ο κυβερνοχώρος επιτρέπει την διεξαγωγή επιχειρήσεων που βρίσκονται υπό του ορίου της ανοιχτής ένοπλης σύγκρουσης, ήτοι τη διενέργεια ψηφιακής κατασκοπείας, δολιοφθοράς κρίσιμων υποδομών και προπαγάνδας – όπως προαναφέρθηκε – γεγονός το οποίο θολώνει την καθαρή διάκριση μεταξύ περιόδου ειρήνης και πολέμου, δημιουργώντας μία νομικά «γκρίζα ζώνη», εύκολα εκμεταλλεύσιμη από τα κράτη.[33]

Ιδιαίτερη σημασία παρουσιάζει, τέλος, ο κατεξοχήν μη υλικός χαρακτήρας του κυβερνοχώρου. Οι περισσότερες κυβερνοεπιθέσεις δεν προκαλούν φυσική καταστροφή αντικειμένων, αλλά περιορίζονται στη διαγραφή, αλλοίωση ή αδυναμία πρόσβασης σε δεδομένα, καθώς και στη διακοπή της λειτουργίας πληροφοριακών συστημάτων. Η εξέλιξη αυτή θέτει στο επίκεντρο το ερμηνευτικό ζήτημα της έννοιας της «βίας» στο ΔΑΔ, η οποία πρέπει να διευρυνθεί σαφώς ώστε να περιλαμβάνει και την άυλη βλάβη και να εξασφαλισθεί η αποτελεσματικότερη προστασία των αμάχων και, αντιστοίχως, των αστικών αντικειμένων.[34]

---

[30] Τα VPNs (Virtual Private Networks / Εικονικά Ιδιωτικά Δίκτυα) είναι μια τεχνολογία που δημιουργεί μια ασφαλή, κρυπτογραφημένη σύνδεση ανάμεσα στην εκάστοτε συσκευή και το διαδίκτυο, αλλάζοντας την πραγματική διεύθυνση IP της συσκευής και κρύβοντας την τοποθεσία της.
[31] Chaumette, *International Criminal Responsibility of Individuals in Case of Cyberattacks*, 2018, 24-25.
[32] Łubiński, *International Humanitarian Law and Hybrid Warfare*, 2025, 229.
[33] Nihreieva, *State responsibility... Russian invasion of Ukraine*, 2025, 6.
[34] Gisel, Rodenhäuser, and Dörmann , *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 28.

Η Διασυνδεσιμότητα των Πληροφοριακών Συστημάτων & τα Αντικείμενα Διττής Χρήσης

Πέραν των ανωτέρω χαρακτηριστικών, η σημαντικότερη ίσως ιδιαιτερότητα του κυβερνοχώρου είναι η διασυνδεσιμότητα των πληροφοριακών συστημάτων. Τα περισσότερα συστήματα λειτουργούν ως τμήματα ευρύτερων δικτύων, εντός των οποίων η δυσλειτουργία ενός μόνο στοιχείου μπορεί να προκαλέσει αλυσιδωτές επιπτώσεις σε μεγάλο αριθμό άλλων συστημάτων.[35] Η στενή διασύνδεση των πληροφοριακών συστημάτων έχει ως αναπόφευκτη συνέπεια τη λειτουργική αλληλεξάρτηση στρατιωτικών και αστικών δικτύων. Η αλληλεξάρτηση αυτή συνεπάγεται ότι πολλές ψηφιακές υποδομές δεν εξυπηρετούν αποκλειστικά έναν μόνο σκοπό, αλλά χρησιμοποιούνται παράλληλα για στρατιωτικές και αστικές λειτουργίες. Κατά συνέπεια, η έννοια των υποδομών και αντικειμένων διττής χρήσης αποκτά ιδιαίτερη σημασία για την εφαρμογή της αρχής της διάκρισης στον κυβερνοχώρο.

Η Διεθνής Επιτροπή του Ερυθρού Σταυρού ορίζει ως αντικείμενο διττής χρήσης *(dual-use object)* κάθε αντικείμενο, εγκατάσταση ή οντότητα που χαρακτηρίζεται από το γεγονός ότι εξυπηρετεί ταυτόχρονα στρατιωτικές και αστικές, μη μάχιμες λειτουργίες,[36] ωστόσο δεν αναγνωρίζει το *«dual-use object»* ως νομικό όρο και τάσσεται υπέρ της αξιολόγησης οιουδήποτε αντικειμένου βάσει του ανωτέρω ορισμού του Άρθρου 52 του Πρώτου Πρόσθετου Πρωτοκόλλου.[37] Το ΝΑΤΟ υιοθετεί τον ίδιο ορισμό.[38] Υπό αυτή την έννοια, τα αστικά δίκτυα, τα καλώδια οπτικών ινών, οι δρομολογητές και οι δορυφόροι στα οποία σήμερα οι στρατιωτικές δυνάμεις βασίζονται σε μεγάλο βαθμό για τις επικοινωνίες τους συνιστούν τέτοια αντικείμενα.[39] Το 98% των κυβερνητικών επικοινωνιών των ΗΠΑ, για παράδειγμα, διακινείται μέσω δικτύων που ανήκουν σε ιδιώτες χωρίς ειδικό

---

[35] *Ibid*, 8.
[36] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2003: "*A particular problem arises with regard to so-called dual-use objects, i.e. objects that serve both civilian and military purposes, such as airports or bridges.*"
[37] *Ibid.*
[38] NATO, *Standard AJP 3.9: Allied Joint Doctrine for Joint Targeting*, 2021, 4-6.
[39] ICRC, *The Principle Of Distinction (Cyber Operations During Armed Conflict)*, 2023, 2.

έλεγχο ή προστασία αυτών.[40] Κατά συνέπεια, θα μπορούσε να υποστηριχθεί πως κάθε κομμάτι της ψηφιακής υποδομής αποτελεί αντικείμενο διττής φύσης. Αυτή η συστηματική διπλή φύση των αντικειμένων έχει τη δυνατότητα να μετατρέψει αστικά δίκτυα όπως τράπεζες, δίκτυα ηλεκτρισμού ή νοσοκομεία σε στρατιωτικούς στόχους υπό την έννοια του ΔΑΔ,[41] παραβιάζοντας την αρχή της διάκρισης και – κατά συνέπεια – την απαγόρευση των αδιάκριτων επιθέσεων.

Ο Προσδιορισμός του Στρατιωτικού Στόχου Στις Κυβερνοεπιθέσεις

Η Οριοθέτηση του «Αντικειμένου»

Η σημαντικότερη ίσως πρόκληση δεν αφορά μόνο τον χαρακτηρισμό μιας ψηφιακής υποδομής ως πολιτικού ή στρατιωτικού στόχου, αλλά προηγουμένως την οριοθέτηση της ίδιας της έννοιας του «αντικειμένου» επί του οποίου θα εφαρμοστούν οι κανόνες του ΔΑΔ. Στο σημείο αυτό ανακύπτει το ερώτημα εάν μία κυβερνοενέργεια που προκαλεί αποκλειστικά απώλεια λειτουργικότητας ενός πληροφοριακού συστήματος, χωρίς φυσική καταστροφή της υλικής του υποδομής, συνιστά «επίθεση» κατά την έννοια του άρθρου 49 παρ. 1 του Πρώτου Πρόσθετου Πρωτοκόλλου. Η σημασία αυτού του ερωτήματος επιτείνεται από το γεγονός ότι, στο πλαίσιο του ΔΑΔ, η «βία» ως αναγκαίο συστατικό της «επίθεσης»[42] ορίζεται παραδοσιακά ως κινητική *(kinetic force),*[43] σε αντίθεση με τη βία στον κυβερνοχώρο *(cyber/non-kinetic force),* η οποία δεν συνεπάγεται αναγκαστικά κινητικά, φυσικά αποτελέσματα.[44] Η απάντηση στο ζήτημα αυτό συνδέεται άμεσα με την ερμηνεία της έννοιας του «αντικειμένου» του άρθρου 52 παρ. 2, καθώς τίθεται το ερώτημα εάν μπορεί να θεωρηθεί επίθεση υπό την

[40] Jensen, *Cyber Warfare and Precautions against the Effects of Attacks*, 2009, 1534.
[41] Geiß, Lahmann, *Cyber warfare: Applying the principle of distinction in an interconnected space*, 2012, 389.
[42] Όπως αμφότερες αναφέρονται στο Άρθρο 49 παρ. 1 *Ν. 1786/1988 «Κύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.».*
[43] Biggio, *Regulating non-kinetic effects... under International Humanitarian Law*, 2025, 242.
[44] *Ibid.*

ανωτέρω έννοια η ζημία άυλων στοιχείων του κυβερνοχώρου (όπως τα δεδομένα), και όχι αποκλειστικά αυτή των στοιχείων με υλική υπόσταση. Η απάντηση στο ζήτημα αυτό έχει προκαλέσει έντονο θεωρητικό προβληματισμό και έχει οδηγήσει στη διαμόρφωση δύο βασικών ερμηνευτικών προσεγγίσεων: την υλική και την λειτουργική.

Η Υλική Προσέγγιση

Η υλική προσέγγιση βασίζεται στην παραδοσιακή ερμηνεία της Διεθνούς Επιτροπής του Ερυθρού Σταυρού, σύμφωνα με την οποία ως «αντικείμενα» νοούνται μόνο όσα έχουν απτή, φυσική υπόσταση.[45] Στον κυβερνοχώρο, η έννοια αυτή αναμφισβήτητα περιλαμβάνει την υλική υποδομή, όπως τους υπολογιστές, τους διακομιστές και τα καλώδια.[46] Η προσέγγιση αυτή ερείδεται στην γραμματική διατύπωση του Πρώτου Πρόσθετου Πρωτοκόλλου, το οποίο αναφέρεται σε καταστροφή, σύλληψη ή εξουδετέρωση των αντικειμένων που δύνανται να αποτελέσουν νόμιμους στρατιωτικούς στόχους[47], όροι οι οποίοι, κατά την κοινή τους σημασία, παραπέμπουν σε αντικείμενα με υλική υπόσταση. Υπό το πρίσμα αυτό, σύμφωνα με τον Κανόνα 92 του Tallinn Manual, μία κυβερνοεπιχείρηση συνιστά «επίθεση» υπό την έννοια του Άρθρου 49 παρ. 1 του Πρώτου Πρόσθετου Πρωτοκόλλου[48] όταν αυτή αναμένεται εύλογα να προκαλέσει θάνατο, τραυματισμό ή φυσική ζημία σε υλικά αντικείμενα.[49] Συγκεκριμένα, η έννοια της «ζημίας» συνδέεται κατ' αρχήν με τη φυσική αλλοίωση ή την απώλεια της λειτουργικότητας ενός υλικού αντικειμένου εφόσον για την αποκατάστασή της απαιτείται η αντικατάσταση φυσικών εξαρτημάτων.[50] Αντιθέτως, επιχειρήσεις όπως η κυβερνοκατασκοπεία, η διαδικτυακή προπαγάνδα ή οι απλές ηλεκτρονικές παρεμβολές δεν χαρακτηρίζονται ως «επιθέσεις» υπό την

[45] ICRC, *Additional Protocols Commentary*, 1987, παρ. 2007-2008.
[46] Pascucci, *Distinction and Proportionality in Cyber War*, 2017, 433.
[47] *Άρθρο 52 παρ. 2*, Πρώτο Πρόσθετο Πρωτόκολλο των Συμβάσεων της Γενεύης, 1977.
[48] «*"Attacks" means acts of violence against the adversary, whether in offence or in defence.*»
[49] Schmitt, *Tallinn Manual 2.0*, 2017, 415.
[50] *Ibid*, 417.

αυστηρή νομική έννοια, εκτός εάν προκαλούν το απαιτούμενο επίπεδο φυσικής ή λειτουργικής ζημίας.[51]

Η Λειτουργική Προσέγγιση

Διαφορετική ερμηνευτική αφετηρία υιοθετεί η λειτουργική προσέγγιση, η οποία αποδίδει καθοριστική σημασία όχι στη φυσική υπόσταση ενός αντικειμένου, αλλά στη λειτουργία αυτού, καθώς και τον ρόλο που αυτό επιτελεί στο πλαίσιο των στρατιωτικών επιχειρήσεων. Σύμφωνα με αυτή, η έννοια της «ζημίας» δεν περιλαμβάνει μόνο την φυσική αλλοίωση ή την καταστροφή των υλικών υποδομών, αλλά και την απώλεια λειτουργικότητας *(loss of functionality)* ενός συστήματος, ακόμη κι όταν αυτή δεν μπορεί να αποκατασταθεί με αντικατάσταση φυσικών εξαρτημάτων.[52] Ενόψει τούτου, μία μερίδα ειδικών της Διεθνούς Επιτροπής του Ερυθρού Σταυρού προκρίνει μια ευρύτερη ανθρωπιστική ερμηνεία, υποστηρίζοντας ότι οποιαδήποτε επιχείρηση έχει σχεδιαστεί για να εξουδετερώσει ή να καταστήσει ανενεργή την λειτουργία ενός συστήματος αποτελεί επίθεση, ανεξάρτητα από τον τρόπο που επιτυγχάνεται αυτό.[53] Η προσέγγιση αυτή στηρίζεται συγκεκριμένα στην αναφορά του Άρθρου 52 παρ. 2 του Πρώτου Πρόσθετου Πρωτοκόλλου όχι μόνο στην καταστροφή ή την κατάληψη, αλλά και στην «εξουδετέρωση» *(neutralization)* ενός στρατιωτικού στόχου. Υποστηρίζεται, επομένως, ότι η έννοια της εξουδετέρωσης θα στερούνταν νοήματος εάν περιοριζόταν αποκλειστικά σε περιπτώσεις φυσικής καταστροφής του αντικειμένου.[54] Σε κάθε περίπτωση, πληθώρα ειδικών υποστηρίζουν ότι η έννοια της «βίας» στο Άρθρο 49 του Πρώτου Πρόσθετου Πρωτοκόλλου πρέπει να επεκταθεί ώστε να λαμβάνει υπόψη τις τρέχουσες τεχνολογικές εξελίξεις και την «παράλυση» των υποδομών χωρίς φυσική καταστροφή αυτών.[55]

---

[51] *Ibid.,* 418.
[52] Gisel, Rodenhäuser, and Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 27.
[53] Gisel, Rodenhäuser, and Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 27.
[54] Dörmann, "Applicability of the Additional Protocols to Computer Network', 2004, 4.
[55] Roscini, Cyber Operations and the Use of Force in International Law, 2014, 181.

Το Ζήτημα των Δεδομένων

Άμεση απόρροια της αντιπαράθεσης μεταξύ της υλικής και της λειτουργικής προσέγγισης είναι ο προβληματισμός σχετικά με το νομικό χαρακτηρισμό των δεδομένων. Η συζήτηση επικεντρώνεται στο αν τα δεδομένα μπορούν να θεωρηθούν «αντικείμενα», καθώς αυτό καθορίζει το επίπεδο της προστασίας τους από επιθέσεις κατά το Άρθρο 52 του Πρώτου Πρόσθετου Πρωτοκόλλου. Οι περισσότεροι ειδικοί - υποστηρικτές της υλικής προσέγγισης - ισχυρίζονται ότι τα ψηφιακά δεδομένα δεν αποτελούν «αντικείμενα» υπό την έννοια του ΔΑΔ, καθώς είναι άυλα.[56] Ως εκ τούτου, μια κυβερνοεπιχείρηση που στοχεύει αποκλειστικά δεδομένα, χωρίς να προκαλεί φυσική ζημιά στο υπολογιστικό σύστημα, δεν θεωρείται «επίθεση». Αντίθετη θέση υποστηρίζεται από την Διεθνή Επιτροπή του Ερυθρού Σταυρού και μια μειοψηφία ειδικών, οι οποίοι τάσσονται υπέρ της αντιμετώπισης των ψηφιακών δεδομένων ως «αντικειμένων».[57] Ειδικότερα, επισημαίνουν ότι στον σύγχρονο ψηφιακό κόσμο, η διαγραφή κρίσιμων πολιτικών δεδομένων - όπως τραπεζικοί λογαριασμοί, φορολογικά μητρώα ή προσωπικά ιατρικά δεδομένα - μπορεί να παραλύσει την κοινωνία και να προκαλέσει μεγαλύτερη ανθρωπιστική βλάβη από την καταστροφή φυσικών αντικειμένων,[58] με αποτέλεσμά η εξαίρεσή τους από την προστασία να δημιουργεί ένα επικίνδυνο «κενό προστασίας».

Προς μια Επανερμηνεία του Στρατιωτικού Στόχου;

Αξιολόγηση της Υλικής και της Λειτουργικής Προσέγγισης

Η ανωτέρω ανάλυση κατέδειξε ότι οι αποκλίνουσες ερμηνευτικές προσεγγίσεις ως προς την έννοια της επίθεσης, του αντικειμένου και του στρατιωτικού στόχου δεν συνιστούν μία αμιγώς θεωρητική αντιπαράθεση. Αντιθέτως, επηρεάζουν άμεσα το εύρος εφαρμογής της αρχής της διάκρισης και, κατ'

[56] Schmitt, *Tallinn Manual*, 2013, 127.
[57] *Ibid.*
[58] Gisel, Rodenhäuser, and Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, 2020, 31.

επέκταση, το επίπεδο προστασίας που παρέχει το ΔΑΔ στους αμάχους και στα αστικά αντικείμενα κατά τη διεξαγωγή κυβερνοεπιχειρήσεων. Το κρίσιμο ζήτημα, συνεπώς, δεν είναι μόνο ποια ερμηνεία ανταποκρίνεται πληρέστερα στη γραμματική διατύπωση του Πρώτου Πρόσθετου Πρωτοκόλλου, αλλά κυρίως ποια διασφαλίζει αποτελεσματικότερα την επίτευξη του ανθρωπιστικού σκοπού του.

Η υλική προσέγγιση παρουσιάζει αναμφίβολα το πλεονέκτημα της μεγαλύτερης ασφάλειας δικαίου, καθώς ο περιορισμός της έννοιας του «αντικειμένου» σε στοιχεία με φυσική υπόσταση εξασφαλίζει σαφέστερα όρια ως προς τον προσδιορισμό των νόμιμων στρατιωτικών στόχων και αποτρέπει μία υπέρμετρη διεύρυνση της έννοιας της επίθεσης. Παράλληλα, η ερμηνεία αυτή εμφανίζεται περισσότερο συμβατή με τη γραμματική διατύπωση των Άρθρων 49 και 52 του Πρώτου Πρόσθετου Πρωτοκόλλου, τα οποία, εξάλλου, υιοθετήθηκαν σε μία εποχή κατά την οποία οι κυβερνοεπιχειρήσεις αποτελούσαν μακρινό μέλλον και η έννοια της στρατιωτικής βλάβης ήταν άρρηκτα συνδεδεμένη με την πρόκληση φυσικής καταστροφής. Ωστόσο, η προσέγγιση αυτή συνεπάγεται και σημαντικούς περιορισμούς, δεδομένου ότι στον κυβερνοχώρο η στρατιωτική βλάβη δεν εξαρτάται πάντοτε από την πρόκληση φυσικής καταστροφής.

Πράγματι, οι σύγχρονες κυβερνοεπιθέσεις επιδιώκουν σε μεγάλο βαθμό όχι την καταστροφή της υλικής υποδομής των υπολογιστικών συστημάτων, αλλά την αδρανοποίηση των λειτουργιών που αυτή επιτελεί. Η προσωρινή ή μόνιμη απώλεια λειτουργικότητας ενός συστήματος ηλεκτροδότησης ή ενός δικτύου επικοινωνιών μπορεί να προκαλέσει σοβαρότατες συνέπειες στο πλαίσιο του ΔΑΔ, ακόμη και αν κανένα φυσικό στοιχείο του συστήματος δεν έχει υποστεί βλάβη. Η αυστηρή και αποκλειστική σύνδεση της έννοιας της επίθεσης με την ύπαρξη φυσικής ζημίας ενδέχεται, επομένως, να οδηγήσει στον αποκλεισμό τέτοιων κυβερνοενεργειών από το πεδίο εφαρμογής των κανόνων του ΔΑΔ. Το αποτέλεσμα θα ήταν η δημιουργία ενός κανονιστικού κενού, εντός του οποίου κυβερνοεπιχειρήσεις με ιδιαίτερα σοβαρές συνέπειες για τον άμαχο πληθυσμό, τα αστικά αντικείμενα, αλλά και τα αντικείμενα διπλής χρήσης, δεν θα υπόκειντο στις θεμελιώδεις εγγυήσεις που παρέχει η αρχή της διάκρισης.

Στον αντίποδα, η λειτουργική προσέγγιση, αποδίδοντας μεγαλύτερη έμφαση στη λειτουργία ενός συστήματος, αντί στη φυσική του υπόσταση, καθιστά περισσότερο σύνθετο τον προσδιορισμό της «βλάβης», της «βίας» και της «επίθεσης» εν γένει, καθώς απουσιάζουν καθιερωμένα κριτήρια βάσει των οποίων δύναται να αξιολογηθεί το πότε μία κυβερνοενέργεια συνιστά κυβερνοεπίθεση, ρυθμιζόμενη από το ΔΑΔ. Η δυσχέρεια αυτή είναι αναπόσπαστα συνδεδεμένη με την έλλειψη κοινώς αποδεκτών κριτηρίων και για τον προσδιορισμό της «απώλειας λειτουργικότητας»[59] ενός υπολογιστικού συστήματος. Κατά συνέπεια, η διαφωνία αυτή ενδέχεται να οδηγήσει σε αποκλίνουσες κρατικές ερμηνείες και, κατ' επέκταση, σε μειωμένη προβλεψιμότητα ως προς την εφαρμογή του ΔΑΔ.

Παρά τις ανωτέρω επιφυλάξεις, η λειτουργική προσέγγιση φαίνεται να ανταποκρίνεται πληρέστερα στον προστατευτικό σκοπό της αρχής της διάκρισης. Η προσέγγιση αυτή μετατοπίζει το επίκεντρο της αξιολόγησης από την υλική μορφή του αντικειμένου στον πραγματικό αντίκτυπο μιας κυβερνοεπιχείρησης επί της λειτουργίας κρίσιμων συστημάτων και, τελικώς, επί του άμαχου πληθυσμού. Η προστασία που επιδιώκει να διασφαλίσει η αρχή της διάκρισης δεν περιορίζεται από την υλική υπόσταση των αντικειμένων καθαυτής, αλλά αποσκοπεί πάντοτε στην αποτροπή των συνεπειών που προκαλούν οι εχθροπραξίες στους αμάχους και τα αστικά αντικείμενα. Επομένως, όταν μία κυβερνοεπιχείρηση οδηγεί στην αδυναμία λειτουργίας ενός αστικού δικτύου, με τρόπο που επηρεάζει ουσιωδώς την παροχή βασικών υπηρεσιών, η απουσία φυσικής καταστροφής δεν θα πρέπει να αποκλείει την εφαρμογή των προστατευτικών κανόνων του ΔΑΔ.

Η ίδια προβληματική αναδεικνύεται εξίσου έντονα ως προς τον νομικό χαρακτηρισμό των δεδομένων. Η άποψη σύμφωνα με την οποία τα δεδομένα εξαιρούνται εξ ορισμού από την έννοια του αντικειμένου φαίνεται να αποδυναμώνει ουσιωδώς την αποτελεσματικότητα της αρχής της διάκρισης.

[59] ICRC, *The Principle Of Distinction (Cyber Operations During Armed Conflict)*, 2023, 2-3.

Συγκεκριμένα, στην περίπτωση που μία κυβερνοεπιχείρηση που πλήττει κρίσιμα δεδομένα των πολιτών παραμείνει εκτός του ορισμού της επίθεσης αποκλειστικά λόγω μη επηρεασμού του φυσικού εξοπλισμού, ή μη υλικής φύσης των δεδομένων per se, τότε ένα σημαντικό τμήμα των επιβλαβών συνεπειών των κυβερνοεπιθέσεων παραμένει εκτός του προστατευτικού πεδίου του ΔΑΔ. Κατ' αυτόν τον τρόπο, δημιουργείται ένα κρίσιμο ρυθμιστικό κενό, το οποίο δυσχεραίνει την προστασία των αμάχων έναντι μορφών βλάβης που δεν ήταν δυνατό να προβλεφθούν κατά τον χρόνο σύνταξης του Πρώτου Πρόσθετου Πρωτοκόλλου. Αντιθέτως, η αναγνώριση, υπό συγκεκριμένες προϋποθέσεις, ορισμένων κατηγοριών δεδομένων ως «αντικειμένων» δεν συνεπάγεται κατ' ανάγκην ανεπίτρεπτη διεύρυνση της έννοιας του στρατιωτικού στόχου, αλλά επιτρέπει την προσαρμογή των υφιστάμενων κανόνων στις ιδιαιτερότητες του κυβερνοχώρου, χωρίς να αλλοιώνει τη βασική τους λογική.

Συμπεράσματα & Προοπτικές Εξέλιξης του ΔΑΔ

Οι παραπάνω προτάσεις δεν επιδιώκουν τη διεύρυνση της έννοιας του στρατιωτικού στόχου εις βάρος της προστασίας των αμάχων, αλλά αποσκοπούν στη διατήρηση της πρακτικής αποτελεσματικότητας της αρχής της διάκρισης στο σύγχρονο πεδίο ενόπλων συγκρούσεων. Η εξέλιξη των τεχνολογικών μέσων και της διεξαγωγής των εχθροπραξιών δεν μεταβάλλει τον ανθρωπιστικό σκοπό του ΔΑΔ, μεταβάλλει, όμως, τον τρόπο με τον οποίο οι κανόνες του καλούνται να επιτύχουν τον σκοπό αυτό. Συμπερασματικά, καθώς η ραγδαία τεχνολογική πρόοδος έχει μεταβάλει ουσιωδώς τον τρόπο με τον οποίο ασκείται η στρατιωτική ισχύς, η ερμηνεία των παραδοσιακών θεμελιωδών εννοιών του ΔΑΔ υπό το πρίσμα της νέας πραγματικότητας καθίσταται πιο επιτακτική από ποτέ, ώστε η αρχή της διάκρισης να εξακολουθήσει να επιτελεί τον κατεξοχήν σκοπό της: την αποτελεσματική προστασία των αμάχων και των αστικών αντικειμένων από τις συνέπειες των ενόπλων συγκρούσεων. Η πρόκληση, επομένως, δεν έγκειται κατ' ανάγκη στη δημιουργία ενός νέου, αυτοτελούς και ειδικού δικαίου για τον κυβερνοπόλεμο, αλλά στην καθιέρωση μια ενιαίας ερμηνείας των ήδη ισχυουσών αρχών και εννοιών που θα εξασφαλίζει την μέγιστη και πληρέστερη προστασία που επιδιώκει να επιτύχει το ΔΑΔ.

Κεντρική θέση στην προσπάθεια αυτή κατέχει η ανάγκη σαφέστερου προσδιορισμού της έννοιας του «στρατιωτικού στόχου». Το Άρθρο 52 παρ. 2 του Πρώτου Πρόσθετου Πρωτοκόλλου εξακολουθεί να αποτελεί το βασικό σημείο αναφοράς, ωστόσο η εφαρμογή των κριτηρίων του σε ψηφιακά περιβάλλοντα δημιουργεί νομικές αβεβαιότητες. Ο προβληματισμός δεν αφορά μόνο τον χαρακτηρισμό ενός συγκεκριμένου συστήματος ως στρατιωτικού ή αστικού αντικειμένου, αλλά και τον προσδιορισμό του ίδιου του «αντικειμένου» που μπορεί να αποτελέσει στόχο μιας κυβερνοεπίθεσης, ιδίως όταν η επίθεση δεν προκαλεί φυσική καταστροφή αλλά απώλεια ή σοβαρή διατάραξη της λειτουργικότητας.

Η ανάγκη αυτή παρουσιάζεται ακόμη σπουδαιότερη ως προς τα αντικείμενα διττής χρήσης, δεδομένου ότι η εκτεταμένη εξάρτηση των στρατιωτικών δραστηριοτήτων από υποδομές που εξυπηρετούν ταυτόχρονα στρατιωτικές και μη ανάγκες καθιστά ολοένα δυσχερέστερη την διάκριση μεταξύ στρατιωτικών και μη αντικειμένων. Η διττή αυτή λειτουργία δεν θα πρέπει να οδηγεί αυτομάτως στον χαρακτηρισμό των εν λόγω υποδομών ως στρατιωτικών στόχων. Αντιθέτως, αποτελεσματικότερη παρουσιάζεται η θέσπιση προστατευτικών μέτρων όπως ο τεχνικός και φυσικός διαχωρισμός στρατιωτικών και αστικών δικτύων[60] ή η εξαίρεση επιθέσεων κατά βασικών κυβερνοεγκαταστάσεων και στοιχείων υποδομών που μπορεί να χαρακτηριστούν ως νόμιμοι στρατιωτικοί στόχοι, αλλά εξυπηρετούν αστικές λειτουργίες ζωτικής σημασίας.[61] Παράλληλα, απαιτείται μια δυναμική ερμηνεία της έννοιας της «βλάβης» των αστικών αντικειμένων, ώστε αυτή να περιλαμβάνει – πέραν της φυσικής καταστροφής - και την απώλεια λειτουργικότητας των υποδομών.

Στο πλαίσιο αυτό, ιδιαίτερη σημασία δύναται να έχει η διαμόρφωση κοινά αποδεκτών ερμηνευτικών κατευθύνσεων από τα κράτη και την Διεθνή Επιτροπή του Ερυθρού

[60] IRRC, *ICRC Position Paper: International humanitarian law and cyber operations during armed conflicts*, 2020, 487.
[61] Id., Geiß, Lahmann, *Cyber warfare: Applying the principle of distinction in an interconnected space*, 2012, 398.

Σταυρού. Η ανάπτυξη κρατικής πρακτικής και *opinio juris* ως προς το περιεχόμενο των εννοιών «επίδεση», «αντικείμενο», «βία» και «στρατιωτικός στόχος» - στο πλαίσιο πάντοτε του κυβερνοπολέμου – περιορίζει την υφιστάμενη αβεβαιότητα και ενισχύει την προβλεψιμότητα και τον προστατευτικό σκοπό του δικαίου. Η συμβολή της Διεθνούς Επιτροπής, καθώς και η περαιτέρω επεξεργασία της σχετικής θεωρίας, έχουν την δυνατότητα να οδηγήσουν στη διαμόρφωση κοινών ερμηνευτικών προτύπων, ιδίως σε ζητήματα όπου δεν έχει ακόμη διαμορφωθεί κρατική συναίνεση. Η εξέλιξη δεν χρήζει κατ' ανάγκην άμεσης τροποποίησης του Πρώτου Πρόσθετου Πρωτοκόλλου. Η ερμηνεία των υφιστάμενων κανόνων υπό το φως του νέου πεδίου ενόπλων συγκρούσεων, σε συνδυασμό με τη σταδιακή διαμόρφωση διεθνούς πρακτικής, δύναται να επιτρέψει την προσαρμογή του ΔΑΔ στις τεχνολογικές εξελίξεις, διατηρώντας παράλληλα τη συνοχή του υφιστάμενου νομικού πλαισίου. Μία τέτοια προσέγγιση παρουσιάζεται ιδιαίτερα σημαντική στον κυβερνοχώρο, όπου η ταχύτητα της τεχνολογικής εξέλιξης καθιστά δυσχερή την πρόβλεψη των μορφών που θα λάβουν οι μελλοντικές κυβερνοεπιχειρήσεις.

Εν πάσει περιπτώσει, το ζητούμενο είναι να διατηρήσει το ΔΑΔ την κανονιστική του αποτελεσματικότητα απέναντι στο «πέμπτο πεδίο μάχης». Η πρόκληση που θέτουν οι κυβερνοεπιδέσεις δεν συνίσταται στην ανάγκη εγκατάλειψης των θεμελιωδών αρχών του ΔΑΔ, αλλά στην προσαρμογή της ερμηνείας τους στις ιδιαιτερότητες του ψηφιακού περιβάλλοντος. Η έννοια του στρατιωτικού στόχου, ως βασικό εργαλείο εφαρμογής της αρχής της διάκρισης, δεν μπορεί να παραμείνει απολύτως αμετάβλητη όταν τα μέσα άσκησης της στρατιωτικής ισχύος μετασχηματίζονται ριζικά. Η επανερμηνεία της, με γνώμονα πάντοτε τον ανθρωπιστικό σκοπό του ΔΑΔ και την κατά το δυνατόν πληρέστερη προστασία των αμάχων, αποτελεί αναγκαία προϋπόθεση ώστε η αρχή της διάκρισης να εξακολουθήσει να επιτελεί τον προστατευτικό της ρόλο και στην εποχή των κυβερνοεπιδέσεων. Η σαφέστερη οριοθέτηση του στρατιωτικού στόχου και η θέσπιση νομικών υποχρεώσεων για την προστασία των αντικειμένων διττής χρήσης αποτελούν βασικές προϋποθέσεις. Εν τέλει, η ικανότητα του ΔΑΔ να ανταποκριθεί σε αυτή την πρόκληση θα κριθεί, όχι από την ικανότητά του να προβλέψει κάθε νέα τεχνολογική εξέλιξη,

αλλά από την ικανότητά του να διατηρήσει αναλλοίωτο τον πυρήνα της ανθρωπιστικής του αποστολής μέσα σε ένα περιβάλλον που μεταβάλλεται διαρκώς.

Βιβλιογραφία

- Biggio, Giacomo. Regulating non-kinetic effects of cyber operations: the 'Loss of Functionality' approach and the military necessity-humanity balance under International Humanitarian Law. (Journal of Conflict & Security Law, 2025, 30, 241–263). https://doi.org/10.1093/jcsl/kraf008.

- Chaumette, Anne-Laure. International Criminal Responsibility of Individuals in Case of Cyberattacks. (International Criminal Law Review 18 (1): 1–35, 2018). https://doi.org/10.1163/15718123-01801004.

- Dörmann, Knut. Applicability of the Additional Protocols to Computer Network Attacks. (Armed Forces at Sea, 1949). https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/applicabilityofihltocna.pdf.

- Geiß, Robin, and Henning Lahmann. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. (Israel Law Review, 2012). 45 (3): 381–99. https://doi.org/10.1017/s0021223712000179.

- Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts. (International Review of the Red Cross, 2020) 102 (913): 287–334. https://doi.org/10.1017/s1816383120000387.

- Hathaway, Oona A, Azmat Khan, and Mara Redlich Revkin. The Dangerous Rise of Dual-Use Objects in War. (The Yale Law Journal, 2024). https://doi.org/10.2139/ssrn.4938707.

- Henckaerts, Jean-Marie, Louise Doswald-Beck, Carolin Alvermann, Knut Dörmann, and Baptiste Rolle. Customary International Humanitarian Law, Volume 1. (Cambridge University Press, 2005). https://doi.org/10.1017/cbo9780511804700.

- ICRC. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 1987.

- ICRC. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report Prepared by the International Committee of the Red Cross. (Geneva, 2003). https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/reaf_and_dev-main_report-oct_2003.pdf.

- ICRC. The Principle of Distinction (Cyber Operations during Armed Conflict). (2023). https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.

- International Court of Justice. Legality of the Threat or Use of Nuclear Weapons. (1996). https://www.icj-cij.org/case/95.

- IRRC. International humanitarian law and cyber operations during armed conflicts, ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. [(2020), 102 (913), 481–492]. https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf.

- IRRC. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report Prepared by the International Committee of the Red Cross for the 28th International Conference of the Red Cross and Red Crescent 2–6 December 2003. (2025). https://international-review.icrc.org/articles/reports-and-documents-ihl-and-the-challenges-of-contemporary-armed-conflicts-927.

- Jensen, Eric Talbot. Cyber Warfare and Precautions against the Effects of Attacks, 88. (Texas Law Review, 1533, 2009). https://digitalcommons.law.byu.edu/faculty_scholarship/224/.

- Łubiński, Piotr. International Humanitarian Law and Hybrid Warfare. (Routledge Research in the Law of Armed Conflict, 2025). https://doi.org/10.4324/9781003198857.

- NATO. Allied Joint Doctrine for Joint Targeting (AJP-3.9). (2008). https://nllp.jallc.nato.int/cmnt/cied-coi/CIED%20PUBLICATIONS/Handbooks%20and%20Doctrines/AJP%203.9.%20DOCTRINE%20OF%20JOINT%20TARGETING.pdf.

- Nihreieva, Olena. State Responsibility for Cyberattacks as a Use of Force in the Context of the 2022 Russian Invasion of Ukraine. (IDP. Revista de Internet, Derecho Y Política, no. 42 (March): 1–13, 2025). https://doi.org/10.7238/idp.v0i42.430724.

- Pascucci, CDR Peter. Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. (Minnesota Journal of International Law 26 (2): 419, 2017). https://doi.org/10.24926/19441992.606.

- Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (June 8, 1977).

- Roscini, Marco. Cyber Operations and the Use of Force in International Law. (Oxford University Press, 2014). https://doi.org/10.1093/acprof:oso/9780199655014.001.0001.

- Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. (Cambridge University Press, 2013). https://doi.org/10.1017/CBO9781139169288.

- Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (Cambridge University Press, 2017). https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N.*Schmitt-Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017*.pdf.

- Weisbord, Noah. The Crime of Aggression: The Quest for Justice in an Age of Drones, Cyberattacks, Insurgents, and Autocrats. (Princeton University Press, 2019). https://doi.org/10.2307/j.ctvc77d8t.