Επιθεώρηση Δημοσίου & Διεθνούς Δικαίου

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

ΤΕΥΧΟΣ 1 | ΕΤΟΣ Α΄ | ΟΚΤΩΒΡΙΟΣ

ΑΡΘΡΟ

Η Μετεξέλιξη της Δέουσας Επιμέλειας στον Κυβερνοχώρο: Προς μια Τεχνοπροληπτική Υποχρέωση Κρατικής Ευθύνης στην Εποχή της Τεχνητής Νοημοσύνης

Ιωάννης Καρβέλας[1]

Abstract. Το παρόν άρθρο εξετάζει τη μετεξέλιξη της αρχής της δέουσας επιμέλειας στο Διεθνές Δίκαιο του κυβερνοχώρου, υπό το πρίσμα της ραγδαίας ανάπτυξης της Τεχνητής Νοημοσύνης. Δεδομένης της εγγενούς δυσχέρειας άμεσου νομικού καταλογισμού των ασύμμετρων κυβερνοεπιδέσεων, η δέουσα επιμέλεια αναδεικνύεται στο κρισιμότερο εργαλείο διασφάλισης της κρατικής λογοδοσίας. Μολονότι η επικείμενη έκδοση του Tallinn Manual 3.0 αναμένεται να παγιώσει περαιτέρω τον δεσμευτικό χαρακτήρα της εν λόγω αρχής, η μελέτη υποστηρίζει ότι η παραδοσιακή *ex post* κατασταλτική προσέγγιση καθίσταται πρακτικά ανεπαρκής έναντι των αυτόνομων ψηφιακών απειλών. Ως εκ τούτου, διατυπώνεται η κανονιστική πρόταση για τη μετάβαση της δέουσας επιμέλειας σε μια «τεχνοπροληπτική υποχρέωση». Η προσέγγιση αυτή επιτάσσει την ενεργή εποπτεία των ψηφιακών υποδομών και την αυστηρή ρύθμιση της ιδιωτικής αγοράς λογισμικού, εισάγοντας την πρωτότυπη έννοια της «τεχνο-κανονιστικής παράλειψης» του κράτους. Παράλληλα, προτείνεται ένα ολιστικό πλαίσιο «ψηφιακής επαγρύπνησης», το οποίο εδράζεται στη διακρατική συνεργασία. Το προτεινόμενο μοντέλο τελεί σε απόλυτη εναρμόνιση με το διεθνές δίκαιο ανθρωπίνων δικαιωμάτων, καθώς αποτρέπει τη μαζική παρακολούθηση φυσικών

[1] Ο Ιωάννης Καρβέλας είναι Προπτυχιακός Φοιτητής της Νομικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

προσώπων. Εν κατακλείδι, η τεχνοπροληπτική εφαρμογή της δέουσας επιμέλειας προβάλλεται ως η σύγχρονη «λυδία λίθος» για τη διαφύλαξη της κρατικής κυριαρχίας και της παγκόσμιας ασφάλειας στον 21ο αιώνα.

Πίνακας περιεχομένων

Εισαγωγή ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Προσεγγίζοντας τις Γενικές Αρχές του Δικαίου κατά το άρθρο 38(1)(γ) του Καταστατικού του Διεθνούς Δικαστηρίου της Χάγης: Πολυπλοκότητα, Αμφισημία και Όρια ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Γενικές Αρχές του Δικαίου που απορρέουν από τις εθνικές έννομες τάξεις ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Γενικές Αρχές του Δικαίου που δύνανται να διαμορφωθούν εντός του διεθνούς νομικού συστήματος ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Η Εσωτερική Διάσταση: Το *Ne Bis In Idem* ως Γενική Αρχή του Δικαίου σε Εθνικό Επίπεδο ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το *Ne Bis In Idem* ως Αρχή Κοινή στα Διάφορα Εθνικά Νομικά Συστήματα του Κόσμου Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Διαφορετικές Εφαρμογές του *Ne Bis In Idem* .. Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το Ζήτημα της Ταυτότητας των Αδικημάτων: Οι Προσεγγίσεις *Idem Crimen* και *Idem Factum* στις Διάφορες Δικαιοδοσίες ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το *Ne Bis In Idem* υπό την Προσέγγιση Idem Factum ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το *Ne Bis In Idem* υπό την Προσέγγιση Idem Crimen ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Η Έννοια του Αμετάκλητου στις Διάφορες Δικαιοδοσίες ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το Αμετάκλητο βάσει της Αυστηρότητας του *Res Judicata* Αποτελέσματος των Αποφάσεων .. Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Το Αμετάκλητο ως Απόφαση επί της Ουσίας της Υπόθεσης ή Απλώς ως Απόρριψη της Υπόθεσης; ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Συμπέρασμα ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Η Διακρατική Εφαρμογή της Αρχής *Ne Bis In Idem* υπό Εξέταση: Είναι Εφικτή η Μεταφορά της στο Διεθνές Δίκαιο; ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Συμπέρασμα ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Βιβλιογραφία ..... Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.

Εισαγωγή

Ο κυβερνοχώρος, ως ένα νεοφανές και δυναμικό πεδίο αλληλεπιδράσεων, έχει μετατοπιστεί από ζήτημα ψηφιακής διακυβέρνησης σε κεντρικό γεωστρατηγικό άξονα, εμπερικλείοντας πλέον τις διεθνείς αντιπαραθέσεις και απειλές.[2] Ως αναμενόμενο, αυτή η εξέλιξη θέτει πρωτοφανείς προκλήσεις στο υφιστάμενο πλαίσιο του Δημοσίου Διεθνούς Δικαίου, καθότι η εγγενής αναρχία του κυβερνοχώρου -σε συνδυασμό με την προσφερόμενη ταχύτητα και την ανωνυμία- καθιστά εξαιρετικά δύσκολη την άμεση απόδοση ευθύνης *(attribution)* για τις επιβλαβείς κυβερνοεπιθέσεις.[3] Αυτό το νομικό και πρακτικό αδιέξοδο υπονομεύει την αποτελεσματικότητα των παραδοσιακών μηχανισμών του διεθνούς δικαίου, καθιστώντας επιτακτική την αναζήτηση εναλλακτικών βάσεων λογοδοσίας.

Υπό αυτές τις συνθήκες, η αρχή της δέουσας επιμέλειας *(due diligence)* αναδεικνύεται ως ένα κρίσιμο,

---

[2] Ellie Winslow και Joanna Bouckaert, "How cybersecurity can best navigate geopolitics to secure a resilient and open digital future," World Economic Forum, 05.02.2026 (πρόσβαση: 30/4/2026), διαθέσιμο στο: https://www.weforum.org/stories/cybersecurity/cybersecurity-and-geopolitics-the-challenges-to-build-resilience-in-a-fragmented-world/.

[3] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10 (2001), άρθρα 4-11 [εφεξής: ARSIWA].
Η δυσκολία αυτή οφείλεται στο «πρόβλημα απόδοσης τριών επιπέδων» (three-level problem of attribution) στον κυβερνοχώρο. Πρώτον, στην τεχνική δυσκολία ταυτοποίησης του υπολογιστή από τον οποίο προήλθε η επίθεση, λόγω τεχνικών συγκάλυψης όπως το IP 'spoofing'. Δεύτερον, στο αποκαλούμενο «χάσμα ανθρώπου-μηχανής» (human-machine gap), καθώς η τοποθεσία ενός υπολογιστή σπάνια αποδεικνύει ποιο φυσικό πρόσωπο τον χειριζόταν. Τρίτον, στην πρόκληση νομικής απόδειξης του δεσμού (nexus) μεταξύ του δράστη και του κράτους, προκειμένου να ικανοποιηθούν τα αυστηρά κριτήρια των Άρθρων της Επιτροπής Διεθνούς Δικαίου για την Κρατική Ευθύνη (ARSIWA). Βλ. Luke Chircop, "A Due Diligence Standard of Attribution in Cyberspace," *International and Comparative Law Quarterly* 67, no. 3 (2018): 644-646.

παρότι δυνητικά παρεξηγήσιμο, εργαλείο κρατικής λογοδοσίας.[4] Όπως διαφαίνεται από την αναμενόμενη κωδικοποίηση του Tallinn Manual 3.0, η διεθνής κοινότητα τείνει να παγιώσει τη δέουσα επιμέλεια ως μια νομικά δεσμευτική υποχρέωση, αποβάλλοντας σταδιακά τον χαρακτήρα της απλής πολιτικής σύστασης. Εντούτοις, η παρούσα μελέτη υποστηρίζει ότι αυτή η εξέλιξη, εφόσον παραμείνει προσκολλημένη σε παραδοσιακά πρότυπα, δεν επαρκεί έναντι των σύγχρονων ψηφιακών απειλών. Προχωρώντας ένα βήμα πέρα από την κωδικοποίηση του ισχύοντος δικαίου, η έρευνα διατυπώνει την κανονιστική πρόταση ότι η εφαρμογή της δέουσας επιμέλειας επιβάλλεται να μετατοπιστεί από μια αμιγώς κατασταλτική υποχρέωση (*ex post*) -η οποία εστιάζει στην αντιμετώπιση των επιθέσεων αφού αυτές εκδηλωθούν- σε μια «τεχνοπροληπτική υποχρέωση».[5] Αυτή η μετάβαση δεν απαιτεί από τα κράτη να λαμβάνουν απλώς μέτρα για την παύση επιθέσεων προερχομένων από την επικράτειά τους· απαιτεί επιπλέον τη ρύθμιση και την ενεργή εποπτεία υποδομών και τεχνολογιών οι οποίες δύναται να χρησιμοποιηθούν ως πληρεξούσιοι (*proxies)* χωρίς άμεσο ανθρώπινο έλεγχο. Επομένως, η αποτελεσματική εφαρμογή της δέουσας επιμέλειας, υπό αυτό το νέο, προληπτικό πρίσμα, καθίσταται η «λυδία λίθος» της κυβερνο-κυριαρχίας στον 21ο αιώνα.

[4] Η αρχή της δέουσας επιμέλειας λειτουργεί ως υποχρέωση συμπεριφοράς (obligation of conduct) και όχι ως υποχρέωση αποτελέσματος (obligation of result). Βάσει αυτής, το κράτος δεν καθίσταται αντικειμενικά υπεύθυνο, αλλά τιμωρείται για τη δική του αμέλεια να λάβει τα κατάλληλα και εύλογα διαθέσιμα μέτρα για την ελαχιστοποίηση του κινδύνου. Εστιάζοντας στην κρατική παράλειψη και όχι στην ίδια την κακόβουλη πράξη, η δέουσα επιμέλεια επιτρέπει νομικά την πλήρη παράκαμψη του σκοπέλου της απόδοσης (circumventing attribution). Βλ. Karine Bannelier, "Due Diligence as a Cardinal Principle in the Fight against Malicious Cyber Activities," στο *Global Cybersecurity and International Law*, επιμ. Antonio Segura Serrano (London: Routledge, 2024), 61-62· Leonhard Kreuzer, *The Harm Prevention Rule in Cyberspace: An Obligation of Due Diligence* (Baden-Baden: Nomos, 2024), 24, 56.

[5] Ο όρος «τεχνοπροληπτική υποχρέωση» (*proactive technical due diligence* / *techno-preventive due diligence*) ανανοηματοδοτείται στην παρούσα μελέτη για τις ανάγκες του Δημοσίου Διεθνούς Δικαίου. Ενώ στον εταιρικό τομέα (M&A) ο όρος περιγράφει τον προληπτικό έλεγχο των υποδομών μιας εταιρείας, στο παρόν πλαίσιο μεταφέρεται στο επίπεδο της Κρατικής Ευθύνης.

Η μεθοδολογία της παρούσας μελέτης υιοθετεί μια συγκριτική και αναλυτική προσέγγιση, εξετάζοντας την εξέλιξη της αρχής της δέουσας επιμέλειας από το Tallinn Manual 2.0[6] στο επερχόμενο Tallinn Manual 3.0.[7] Θα αναλυθεί πώς η νέα έκδοση αναμένεται να κωδικοποιήσει την εξελισσόμενη κρατική πρακτική και τις νομικές απόψεις εμπειρογνωμόνων, παρέχοντας μεγαλύτερη σαφήνεια στο περιεχόμενο και την εφαρμογή της αρχής, ιδίως σχετικά με τις νέες τεχνολογίες και την κρατική ευθύνη για ενέργειες ιδιωτών. Επιπλέον, θα διερευνηθεί η επίδραση των αναδυόμενων τεχνολογιών στο περιεχόμενο και την εφαρμογή αυτής της αρχής, αναδεικνύοντας την ανάγκη προσαρμογής των νομικών προτύπων στο διαρκώς μεταβαλλόμενο ψηφιακό περιβάλλον. Συνεπώς, η παρούσα ανάλυση φιλοδοξεί να συμβάλει στον διευρυνόμενο διάλογο περί της κρατικής ευθύνης στον κυβερνοχώρο, προσφέροντας μια νέα οπτική στην αντιμετώπιση των σύγχρονων προκλήσεων.

Η Νομική Φύση της Δέουσας Επιμέλειας στον Κυβερνοχώρο

Από την Υπόθεση της Κέρκυρας στον Κυβερνοχώρο

Η αρχή της δέουσας επιμέλειας αποτελεί έναν θεμελιώδη πυλώνα του διεθνούς δικαίου, εδραζόμενη στο κλασικό νομικό αξίωμα *"sic utere tuo ut alienum non laedas"* (χρησιμοποίησε την ιδιοκτησία σου με τρόπο που να μην βλάπτεις εκείνη του άλλου). Για την ορθή δογματική της θεμελίωση, η δέουσα επιμέλεια εν προκειμένω λειτουργεί πρωτίστως ως το «πρότυπο συμπεριφοράς» (standard of conduct) -δηλαδή ως το μέτρο της απαιτούμενης κρατικής επαγρύπνησης για την εκπλήρωση της πρωτογενούς υποχρέωσης πρόληψης διασυνοριακής βλάβης και προστασίας των δικαιωμάτων τρίτων κρατών- και όχι ως ένας αφηρημένος ή αυτοτελής πρωτογενής κανόνας καθ' αυτόν.

[6] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).
[7] Michael N. Schmitt (ed.), *Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, forthcoming).

Ιστορικά, η αρχή αποκρυσταλλώθηκε στη Διαιτησία των «Απαιτήσεων της Αλαμπάμα», η οποία έκρινε ότι ένα κράτος οφείλει να επιδεικνύει την ανάλογη επαγρύπνηση ώστε να μην επιτρέπει τη χρησιμοποίηση της επικράτειάς του από ιδιωτικούς φορείς προς βλάβη τρίτων κρατών.[8] Η νομική αυτή υποχρέωση ενισχύθηκε περαιτέρω με τη διαιτητική απόφαση στην υπόθεση *Trail Smelter* (1941), η οποία καθιέρωσε ότι ουδέν κράτος δύναται να χρησιμοποιεί ή να επιτρέπει τη χρήση του εδάφους του με τρόπο επιβλαβή για το έδαφος άλλου κράτους ή για περιουσίες εντός αυτού, προσδιορίζοντας τη δέουσα επιμέλεια ως το απαιτούμενο μέτρο προστασίας από διασυνοριακές περιβαλλοντικές βλάβες.[9]

Εν συνεχεία, η εμβληματική υπόθεση του Στενού της Κέρκυρας το 1949 καθιέρωσε την υποχρέωση κάθε κράτους «να μην επιτρέπει εν γνώσει του τη χρήση του εδάφους του για πράξεις αντίθετες προς τα δικαιώματα άλλων κρατών».[10]

---

[8] *Alabama claims of the United States of America against Great Britain*, 14.09.1872, Reports of International Arbitral Awards [RIAA], vol. XXIX, 125, https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf.

[9] *Trail smelter case (United States, Canada)*, 11.03.1941, RIAA, vol. III, 1905-1982.

[10] *Corfu Channel Case (United Kingdom v. Albania)*, Merits, Judgment, I.C.J. Reports 1949, 4, 22.

Αξίζει να σημειωθεί ότι στις υποθέσεις αυτές εντοπίζονται τα νομικά θεμέλια για την αντιμετώπιση των σύγχρονων προκλήσεων του κυβερνοχώρου. Στη διαιτησία της Αλαμπάμα (1872), το δικαστήριο καθιέρωσε την αρχή ότι η έλλειψη σχετικής εθνικής νομοθεσίας δεν απαλλάσσει το κράτος από τη διεθνή του ευθύνη, αρχή που σήμερα εφαρμόζεται κατ' αναλογία στην υποχρέωση ελέγχου ιδιωτικών εταιρειών που εξάγουν τεχνολογίες υψηλού κινδύνου (Βλ. Jan Martin Lemnitzer, "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace," *European Journal of International Law* 33, no. 3 (2022): 801-802). Αντίστοιχα, στην υπόθεση του Στενού της Κέρκυρας, αν και το Δικαστήριο απέρριψε την αυτόματη «τεκμαιρόμενη γνώση» (*constructive knowledge*), δέχθηκε τη χρήση έμμεσων αποδείξεων για να καταλήξει ότι η Αλβανία «δεν θα μπορούσε να μη γνωρίζει» (*must have known*) τον κίνδυνο. Το κρίσιμο στοιχείο αυτής της απόφασης είναι ότι επιδίκασε αποζημίωση υπέρ του Ηνωμένου Βασιλείου θεμελιώνοντας ευθύνη λόγω παράλειψης, χωρίς να χρειαστεί ποτέ να αποδειχθεί ποιος πραγματικά τοποθέτησε τις νάρκες. Η προσέγγιση αυτή παρέχει σήμερα ένα ισχυρό νομικό προηγούμενο για την παράκαμψη του ακανθώδους προβλήματος της απόδοσης (*circumventing attribution*) επιθέσεων στον κυβερνοχώρο (Lemnitzer, "Back to the Roots," 801-806).

Στη συγκεκριμένη υπόθεση, η δέουσα επιμέλεια λειτούργησε ως το *standard of conduct* που καθόρισε το επίπεδο της απαιτούμενης κρατικής συμπεριφοράς, θεμελιώνοντας την ευθύνη του παράκτιου κράτους στην παράλειψη προειδοποίησης για την ύπαρξη ναρκών στα χωρικά του ύδατα.

Αυτή η πρωτογενής υποχρέωση, αρχικά διατυπωμένη σε ένα πλαίσιο εδαφικής κυριαρχίας και φυσικών συνόρων, βρίσκει πλέον εφαρμογή στο «άυλο» και διασυνοριακό πεδίο του κυβερνοχώρου, όπου η έννοια του «εδάφους» αποκτά νέα διάσταση. Είναι, λοιπόν, η μετάβαση από τον φυσικό στον ψηφιακό χώρο, που επιτάσσει την εφαρμογή της αρχής *mutatis mutandis*, διατηρώντας αλώβητο τον πυρήνα της: την κρατική ευθύνη για την πρόληψη βλαβών προερχομένων από την επικράτεια του κράτους.

Στον κυβερνοχώρο, η «επικράτεια» δεν περιορίζεται σε γεωγραφικά όρια· επεκτείνεται στις ψηφιακές υποδομές, τους διακομιστές και τα δίκτυα εντός των φυσικών συνόρων ενός κράτους. Κατ' αναλογία με τις θαλάσσιες νάρκες, το καθήκον δέουσας επιμέλειας επιβάλλει στα κράτη να λαμβάνουν όλα τα εύλογα και αναγκαία μέτρα προς αποτροπή της χρήσης τέτοιων ψηφιακών υποδομών (π.χ. ως ορμητήρια *botnets)* για την εκδήλωση επιβλαβών κυβερνοεπιθέσεων εναντίον άλλων κρατών.[11] Ωστόσο, η πολυπλοκότητα της τεχνολογίας και η δυσκολία στον εντοπισμό της προέλευσης των επιθέσεων καθιστούν την εφαρμογή αυτής της αρχής ιδιαίτερα απαιτητική. Συνεπώς, η αναζήτηση και ο ακριβής προσδιορισμός του απαιτούμενου μέτρου επιμέλειας στον κυβερνοχώρο αποτελεί κεντρικό ζήτημα του σύγχρονου διεθνούς δικαίου.

«Πρότυπο Συμπεριφοράς» ή «Κανόνας»

Χρήζει αναφοράς ότι η νομική φύση της δέουσας επιμέλειας στον κυβερνοχώρο αποτελεί αντικείμενο διαρκούς

[11] Eric Talbot Jensen και Sean Watts, "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?," *Texas Law Review* 95, no. 7 (2017): 1566-1567.

συζήτησης στη διεθνή κοινότητα, με δύο βασικές προσεγγίσεις να αναδεικνύονται. Αφενός, οι Ομάδες Κυβερνητικών Εμπειρογνωμόνων του ΟΗΕ (UNGGE)[12] και η Ομάδα Εργασίας Ανοικτής Σύνθεσης (Open-ended Working Group - OEWG)[13] έχουν υιοθετήσει μια προσέγγιση που τείνει να αντιμετωπίζει τη δέουσα επιμέλεια μάλλον ως μη δεσμευτικό κανόνα ή πολιτική σύσταση, παρά ως δεσμευτικό κανόνα εθιμικού διεθνούς δικαίου. Αυτή η θέση βασίζεται στην άποψη ότι δεν υπάρχει επαρκής κρατική πρακτική (state practice) και πεποίθηση δικαίου (*opinio juris*) ώστε να θεμελιωθεί η δεσμευτικότητα της αρχής στον κυβερνοχώρο. Επομένως, η δέουσα επιμέλεια θεωρείται ως μια βέλτιστη πρακτική ή μια πολιτική δέσμευση, η παραβίαση της οποίας δεν συνεπάγεται απαραίτητα διεθνή ευθύνη.[14]

Αφετέρου, το Tallinn Manual, ένα έργο εμπειρογνωμόνων που αναπτύχθηκε από το NATO Cooperative Cyber Defence Centre of Excellence

---

[12] UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (2021) [GGE Report 2021].

[13] UN General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816 (2021).

[14] Η προσέγγιση αυτή, ωστόσο, αντανακλά έναν διπλωματικό συμβιβασμό (*strategic ambiguity*) παρά νομική ομοφωνία. Ισχυρές κυβερνοδυνάμεις, όπως οι ΗΠΑ, το Ηνωμένο Βασίλειο και το Ισραήλ, αρνούνται ρητά ότι η αρχή της δέουσας επιμέλειας έχει αποκρυσταλλωθεί σε δεσμευτικό κανόνα του εθιμικού διεθνούς δικαίου για τον κυβερνοχώρο, φοβούμενες τον υπερβολικό φόρτο ευθυνών που αυτό θα συνεπαγόταν (Lemnitzer, "Back to the Roots," 791-792· Bannelier, "Due Diligence as a Cardinal Principle," 48). Αντιθέτως, η πλειονότητα των κρατών -συμπεριλαμβανομένης της Γαλλίας, της Γερμανίας και πολλών κρατών της Λατινικής Αμερικής- τη θεωρούν νομικά δεσμευτική (Bannelier, "Due Diligence as a Cardinal Principle," 48· Lemnitzer, "Back to the Roots," 791-792). Αυτή η διάσταση απόψεων αποτυπώνεται χαρακτηριστικά στις Εκθέσεις των Ομάδων Κυβερνητικών Εμπειρογνωμόνων του ΟΗΕ του 2015 και του 2021, όπου χρησιμοποιήθηκε σκόπιμα το προαιρετικό «θα έπρεπε» (*should*) αντί για το επιτακτικό «πρέπει» (*must*), υποβιβάζοντας την αρχή σε εθελοντικό κανόνα συμπεριφοράς (UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (2015) para. 13(c)· UNGA, GGE Report 2021, para. 30). Η ίδια διαφωνία οδήγησε και στην αφαίρεση της σχετικής ενότητας από το συναινετικό κύριο κείμενο της τελικής έκθεσης της Ομάδας Ανοικτής Σύνθεσης (UN OEWG) το 2021, μεταφέροντάς την στη μη δεσμευτική Επιστολή του Προέδρου (Lemnitzer, "Back to the Roots," 792-793).

(CCDCOE), υιοθετεί μια πιο αποφασιστική στάση, θεωρώντας ότι η υποχρέωση δέουσας επιμέλειας δεν αποτελεί απλή πολιτική σύσταση, αλλά συνιστά υφιστάμενο κανόνα του εθιμικού διεθνούς δικαίου (*lex lata*).[15] Το Tallinn Manual 2.0, ειδικότερα, περιλαμβάνει κανόνες που επιβάλλουν στα κράτη την υποχρέωση να λαμβάνουν κάθε εφικτό μέτρο για να τερματίσουν κυβερνοεπιθέσεις προερχόμενες από την επικράτειά τους και στρεφόμενες εναντίον άλλων κρατών, εφόσον έχουν γνώση της επίθεσης (Rule 6). Η προσέγγιση αυτή αντιμετωπίζει τη δέουσα επιμέλεια ως δυναμική εξειδίκευση και εφαρμογή της γενικής αρχής του διεθνούς δικαίου -που διατυπώθηκε στην απόφαση *Corfu Channel*- στο περιβάλλον του κυβερνοχώρου, αποδεικνύοντας ότι ο διαρθρωτικός της πυρήνας προσαρμόζεται στις απαιτήσεις της ψηφιακής εποχής.

Η ένταση μεταξύ των δύο προσεγγίσεων δεν εξαντλείται σε ζήτημα διπλωματικής ασάφειας· εγείρει το κρίσιμο δογματικό ερώτημα του δεσμού του «επίμονου αντιρρησία» *(persistent objector)* στο εθιμικό διεθνές δίκαιο. Σύμφωνα με την παγιωμένη αρχή, ένα κράτος το οποίο εναντιώνεται σταθερά και απροκάλυπτα σε έναν αναδυόμενο εθιμικό κανόνα καθ' όλη τη διάρκεια της διαμόρφωσής του δεν δεσμεύεται από αυτόν, ακόμη κι αν ο κανόνας τελικώς κρυσταλλωθεί για το σύνολο της διεθνούς κοινότητας. Η ρητή και επανειλημμένη άρνηση κρατών όπως οι ΗΠΑ, το Ηνωμένο Βασίλειο και το Ισραήλ να αναγνωρίσουν τη δέουσα επιμέλεια ως δεσμευτικό κανόνα εθιμικού δικαίου στον κυβερνοχώρο δεν είναι επομένως απλώς πολιτική επιφύλαξη, αλλά ενδέχεται να συνιστά τυπική άσκηση του δικαιώματος επίμονης αντίρρησης. Αυτό σημαίνει ότι, ακόμη και υπό το ενδεχόμενο πλήρους παγίωσης της αρχής ως δεσμευτικού κανόνα για την πλειονότητα των κρατών, η δεσμευτικότητά της έναντι αυτών των συγκεκριμένων -και ιδιαιτέρως ισχυρών σε κυβερνοϊκανότητες- κρατών θα παρέμενε αμφισβητήσιμη, με προφανείς συνέπειες για την πρακτική αποτελεσματικότητα οποιασδήποτε υποχρέωσης, η οποία -όπως θα αναλυθεί παρακάτω- θα βασιζόταν εν πολλοίς σε αυτά ακριβώς τα κράτη για την υλοποίησή της. Η παρούσα

[15] Schmitt, *Tallinn Manual 2.0*, 29 (Rule 6, para 1).

μελέτη αναγνωρίζει το ζήτημα αυτό ως όριο της προτεινόμενης θεωρητικής μετάβασης, χωρίς ωστόσο αυτό να αναιρεί τη σκοπιμότητα της πρότασης ως εργαλείου *de lege ferenda*.

Το Tallinn Manual 3.0

Η επικείμενη έκδοση του Tallinn Manual 3.0 αναμένεται να ενισχύσει τη θέση ότι η δέουσα επιμέλεια αποτελεί πλέον αυτόνομο κανόνα του διεθνούς δικαίου στον κυβερνοχώρο.[16] Παρότι το ίδιο το εγχειρίδιο δεν συνιστά μήτε διεθνή συνθήκη μήτε δεσμευτικό εθιμικό κανόνα, η νομική του βαρύτητα θεμελιώνεται στο Άρθρο 38(1)(δ) του Καταστατικού του Διεθνούς Δικαστηρίου της Δικαιοσύνης (ICJ Statute), ως «*διδασκαλία των πλέον αναγνωρισμένων δημοσιολόγων*» (*teachings of the most highly qualified publicists*), λειτουργώντας έτσι ως επικουρικό μέσο για τον προσδιορισμό των δικαιικών κανόνων. Υπό αυτό το πρίσμα, η νέα έκδοση, η οποία βρίσκεται υπό ανάπτυξη από το CCDCOE, στοχεύει στην επικαιροποίηση και επέκταση των κανόνων του Tallinn Manual 2.0, λαμβάνοντας υπόψιν τις ραγδαίες τεχνολογικές εξελίξεις και την εξελισσόμενη κρατική πρακτική των τελευταίων ετών.

Το εγχειρίδιο στοχεύει να κωδικοποιήσει περαιτέρω τις νομικές απόψεις των εμπειρογνωμόνων, παρέχοντας ένα λεπτομερέστερο πλαίσιο για το «δέον μέτρο» *(standard of care)* που απαιτείται από τα κράτη βάσει των τεχνικών δυνατοτήτων τους. Ειδικότερα, θα εξεταστεί πώς το εγχειρίδιο

[16] Αυτή η εξέλιξη κρίνεται επιβεβλημένη προκειμένου να καλυφθούν τα κενά της προηγούμενης έκδοσης. Το Tallinn Manual 2.0 έχει δεχθεί έντονη ακαδημαϊκή κριτική διότι υιοθέτησε μια εξαιρετικά στενή ερμηνεία του εθιμικού δικαίου, απορρίπτοντας την ύπαρξη νομικής υποχρέωσης «πρόληψης» *(duty to prevent)* και «προετοιμασίας» *(duty to prepare)* των κρατών έναντι των κυβερνοαπειλών. Ουσιαστικά, περιόρισε την αρχή της δέουσας επιμέλειας αποκλειστικά στην εκ των υστέρων *(reactive)* υποχρέωση ενός κράτους να προσπαθήσει να τερματίσει μια επίθεση που βρίσκεται ήδη σε εξέλιξη, και αυτό μόνο εφόσον έχει λάβει γνώση (Lemnitzer, "Back to the Roots," 807-808· Bannelier, "Due Diligence as a Cardinal Principle," 58-59). Η νέα έκδοση (Tallinn Manual 3.0) αναμένεται να αναθεωρήσει αυτή τη συσταλτική προσέγγιση, ανταποκρινόμενη στις σύγχρονες απαιτήσεις της διεθνούς κυβερνοασφάλειας.

θα αντιμετωπίσει ζητήματα αιχμής, όπως η υποχρέωση των κρατών να ρυθμίζουν την ανάπτυξη και χρήση επιθετικών εργαλείων AI από ιδιωτικούς φορείς εντός της επικράτειάς τους, καθώς και η ανάγκη για διεθνή συνεργασία και ανταλλαγή πληροφοριών απειλών *(threat intelligence).* Συνεπώς, το Tallinn Manual 3.0 αναμένεται να αποτυπώσει τη δυναμική εξέλιξη της κρατικής πρακτικής, καταγράφοντας την αυξανόμενη τάση της διεθνούς κοινότητας να αντιμετωπίζει τη δέουσα επιμέλεια όχι ως απλή πολιτική δέσμευση, αλλά ως μια αναδυόμενη ή παγιωμένη νομική υποχρέωση με σαφέστερο κανονιστικό -και ενδεχομένως προληπτικό- περιεχόμενο.

Το Περιεχόμενο της Υποχρέωσης και το Ζήτημα των Ιδιωτών/Proxies
Η Γνώση ως Προϋπόθεση (Actual vs. Constructive Knowledge)

Η στοιχειοθέτηση της κρατικής ευθύνης, υπό το πρίσμα της αρχής της δέουσας επιμέλειας, προαπαιτεί την ύπαρξη «γνώσης» εκ μέρους του κράτους αναφορικά με τις επιβλαβείς κυβερνοδραστηριότητες που εκπορεύονται από την επικράτειά του. Στο πλαίσιο αυτό, η διεθνής πρακτική και η σχετική νομική θεωρία προβαίνουν σε σαφή διαχωρισμό μεταξύ της πραγματικής *(actual knowledge)* και της τεκμαιρόμενης *(constructive knowledge)* γνώσης.[17]
Η πραγματική γνώση εδραιώνεται στις περιπτώσεις κατά τις οποίες το κράτος έχει στη διάθεσή του σαφή και αδιαμφισβήτητα δεδομένα περί μιας επικείμενης ή ήδη εξελισσόμενης κυβερνοεπίθεσης. Σύμφωνα με τη σύγχρονη κρατική πρακτική, όπως αυτή αποτυπώνεται στη «Βασική Θέση» της Ιαπωνίας[18] η λήψη «αξιόπιστης ειδοποίησης» *(credible notification)* από τρίτο κράτος συνιστά επαρκές θεμέλιο πραγματικής γνώσης, το οποίο ενεργοποιεί τη νομική υποχρέωση του αποδέκτη να αξιοποιήσει την ικανότητα

[17] Tomohiro Mikanagi, "Application of the Due Diligence Principle to Cyber Operations," *International Law Studies* 97 (2021): 1034-1035.
[18] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (2021), πρόσβαση: 15/05/2026, https://www.mofa.go.jp/files/100200935.pdf.

επιρροής του με σκοπό την αναχαίτιση της εν λόγω επιχείρησης. Εντούτοις, στο περιβάλλον του κυβερνοχώρου, όπου η συλλογή πληροφοριών καθίσταται εγγενώς δυσχερής και οι δράστες μετέρχονται συστηματικών μεθόδων απόκρυψης των ιχνών τους, η έννοια της τεκμαιρόμενης γνώσης αποκτά βαρύνουσα σημασία.

Συνεπώς, ένα κράτος δύναται να θεωρηθεί ότι «όφειλε να γνωρίζει» *(ought to have known)* εάν, σταθμίζοντας τις εκάστοτε περιστάσεις, διαπιστωθεί ότι δεν επέδειξε τον επιβαλλόμενο βαθμό επαγρύπνησης. Η συγκεκριμένη *in concreto* αξιολόγηση, όπως επισημάνθηκε από το Διεθνές Δικαστήριο Δικαιοσύνης (ICJ) στην Υπόθεση της Γενοκτονίας της Βοσνίας,[19] τελεί σε άμεση συνάρτηση με την «ικανότητα επιρροής» *(capacity to influence)* που ασκεί το κράτος επί των δραστών. Στο πεδίο των κυβερνοεπιχειρήσεων, η ικανότητα αυτή άπτεται του τεχνικού ελέγχου επί των ψηφιακών υποδομών, καθώς και της ισχύος των δεσμών μεταξύ των κρατικών αρχών και των εκάστοτε εμπλεκόμενων δρώντων.[20]

Ο επιβαλλόμενος δε στα κράτη βαθμός επαγρύπνησης δεν προσεγγίζεται ως απόλυτο μέγεθος, αλλά συναρτάται με ένα σύνολο μεταβλητών παραμέτρων. Ήδη από τη Διαιτησία των «Απαιτήσεων της Αλαμπάμα», έχει παγιωθεί η αρχή ότι η δέουσα επιμέλεια οφείλει να ασκείται «*κατ' αναλογία προς τον κίνδυνο*» (*in proportion to the risk*). Κατά συνέπεια, όσο

[19] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, 43, para. 430.

[20] Στη νομολογία του Διεθνούς Δικαστηρίου (ICJ), η έννοια της πραγματικής γνώσης και της αντίστοιχης ικανότητας αποτροπής (*capacity)* επιβεβαιώθηκε ρητά στην υπόθεση των *Διπλωματικών και Προξενικών Υπαλλήλων στην Τεχεράνη* (Bannelier, "Due Diligence as a Cardinal Principle," 49-50). Αντιθέτως, όσον αφορά την τεκμαιρόμενη γνώση (constructive knowledge), το γεγονός και μόνο ότι μια κυβερνοεπίθεση εκπορεύτηκε από το έδαφος ενός κράτους δεν δημιουργεί μαχητό τεκμήριο *(rebuttable presumption)* ότι το κράτος γνώριζε (Kreuzer, *Harm Prevention Rule in Cyberspace*, 252· Bannelier, "Due Diligence as a Cardinal Principle," 50). Το διεθνές δίκαιο άλλωστε δεν επιβάλλει στα κράτη την υποχρέωση να παρακολουθούν το σύνολο των ψηφιακών δραστηριοτήτων στην επικράτειά τους, καθώς κάτι τέτοιο θα προσέκρουε στις υποχρεώσεις σεβασμού των ανθρωπίνων δικαιωμάτων και της ιδιωτικότητας (Kreuzer, *Harm Prevention Rule in Cyberspace*, 255· Bannelier, "Due Diligence as a Cardinal Principle," 51).

μεγαλύτερη είναι η διαφαινόμενη απειλή κατά κρίσιμων υποδομών -όπως χαρακτηριστικά υπογραμμίζεται και στη Δεύτερη Δήλωση της Οξφόρδης[21] αναφορικά με την προστασία του τομέα της υγείας- τόσο υψηλότερο καθίσταται το νομικώς απαιτούμενο επίπεδο επαγρύπνησης. Ειδικότερα, ένα κράτος το οποίο διαθέτει προηγμένες δυνατότητες κυβερνοάμυνας αναμένεται να επιδεικνύει αντιστοίχως αυξημένο επίπεδο επαγρύπνησης· εξάλλου, η αντικειμενική αδυναμία εντοπισμού μιας κυβερνοεπίθεσης δεν απαλλάσσει αυτοδικαίως το κράτος από την ευθύνη του, εφόσον η εν λόγω παράλειψη απορρέει από την απουσία δέουσας επιμέλειας ως προς την ανάπτυξη των θεμελιωδών εθνικών του δυνατοτήτων (*capacity building*) στον κυβερνοχώρο.

Ιδιώτες Κυβερνοεισβολείς (Hackers) και Κρατικοί Πληρεξούσιοι (Proxies)

Ένα από τα πλέον περίπλοκα νομικά ζητήματα αναφορικά με την εφαρμογή της αρχής της δέουσας επιμέλειας στον κυβερνοχώρο, συνίσταται στη διακριτότητα μεταξύ ανεξάρτητων ιδιωτών κυβερνοεισβολέων *(hackers)* και κρατικών πληρεξουσίων *(proxies).* Συχνά, οι επιβλαβείς κυβερνοεπιχειρήσεις σχεδιάζονται και εκτελούνται από μη κρατικούς δρώντες *(non-state actors),* οι οποίοι είτε ενεργούν πλήρως αυτόνομα είτε τελούν υπό την υποστήριξη, την καθοδήγηση ή τον έλεγχο κρατικών οντοτήτων. Η εγγενής δυσχέρεια στην τεκμηρίωση της σχέσης ελέγχου μεταξύ ενός κράτους και ενός μη κρατικού φορέα καθιστά τον νομικό καταλογισμό στο κράτος εξαιρετικά δυσχερή.

Όπως έχει αναδειχθεί από τη νομολογία του Διεθνούς Δικαστηρίου Δικαιοσύνης στην εμβληματική Υπόθεση της Νικαράγουας,[22] ο άμεσος καταλογισμός προαπαιτεί την απόδειξη «αποτελεσματικού ελέγχου» *(effective control)* επί

[21] Oxford Institute for Ethics, Law and Armed Conflict, "The Second Oxford Statement on International Law Protections of the Healthcare Sector during Covid-19: Safeguarding Vaccine Research," The Oxford Process, 2020, *πρόσβαση*: 18.05.2026,
[22] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, 14, para. 115.

των ενεργειών των μη κρατικών δρώντων.[23] Το εν λόγω αυστηρό νομικό κριτήριο καθίσταται πρακτικά σχεδόν αδύνατο να ικανοποιηθεί στο σύγχρονο περιβάλλον της ψηφιακής ανωνυμίας. Υπό αυτό το πρίσμα, η αρχή της δέουσας επιμέλειας επιτελεί τον ρόλο μιας κρίσιμης «γέφυρας» για την εδραίωση της λογοδοσίας του φιλοξενούντος κράτους *(host state),* ακόμη και στις περιπτώσεις όπου δεν καθίσταται εφικτή η στοιχειοθέτηση άμεσου ελέγχου ή έμπρακτης καθοδήγησης.

Στις περιπτώσεις όπου ένα κράτος δεν ασκεί μεν άμεσο έλεγχο επί ιδιωτών δρώντων στον κυβερνοχώρο, αλλά συγχρόνως παραλείπει να λάβει τα προσήκοντα μέτρα για την αποτροπή κυβερνοεπιθέσεων που εκπορεύονται από την επικράτειά του, δύναται να στοιχειοθετηθεί διεθνής ευθύνη του βάσει της παραβίασης της δέουσας επιμέλειας. Η εν λόγω ευθύνη εμπεριέχει πρωτίστως την υποχρέωση των κρατικών αρχών να προβαίνουν στη λήψη κατασταλτικών μέτρων για την παύση των επιβλαβών επιχειρήσεων και την ελαχιστοποίηση της προκληθείσας ζημίας, καθώς και -στο μέτρο του εφικτού- να διερευνούν, να διώκουν και να τιμωρούν τους υπαίτιους. Το Tallinn Manual 2.0, επί παραδείγματι, κατοχυρώνει ρητώς αυτή την υποχρέωση, υπογραμμίζοντας ότι τα κράτη οφείλουν να επιδεικνύουν τη δέουσα επιμέλεια προκειμένου να τερματίσουν (ή να αναχαιτίσουν, εφόσον επίκεινται άμεσα) κυβερνοεπιχειρήσεις που χρησιμοποιούν την επικράτειά τους ως ορμητήριο εις

[23] Το αυστηρό κριτήριο του «αποτελεσματικού ελέγχου» *(effective control),* όπως διατυπώθηκε νομολογιακά, αποτελεί τον κυρίαρχο κανόνα ερμηνείας για την εφαρμογή του Άρθρου 8 των Άρθρων της Επιτροπής Διεθνούς Δικαίου για την Κρατική Ευθύνη (ARSIWA) (Βλ. Fiona Middleton και Nicholas Tsagourias, "Cyber Attribution and Its Challenges," στο *Global Cybersecurity and International Law*, επιμ. Antonio Segura Serrano (London: Routledge, 2024), 74). Αντιμετωπίζοντας τη δυσχέρεια απόδειξης αυτού του επιπέδου ελέγχου σε περιπτώσεις ομάδων όπως οι «πατριώτες χάκερς» (patriotic hackers) ή ο «Στρατός Πληροφορικής της Ουκρανίας» (IT Army of Ukraine), ορισμένοι μελετητές προτείνουν την αλλοίωση του παραδοσιακού κανόνα, προκρίνοντας τη μετάβαση στο χαλαρότερο κριτήριο του «συνολικού ελέγχου» (overall control) της υπόθεσης Tadić ή την αναγνώριση «σιωπηρών οδηγιών» (implicit instructions) (Middleton και Tsagourias, "Cyber Attribution and Its Challenges," 80-83). Η εφαρμογή της δέουσας επιμέλειας ως πρωτεύοντος κανόνα (primary rule), ωστόσο, παρακάμπτει κομψά αυτή την ανάγκη επισφαλούς αλλοίωσης των κανόνων καταλογισμού.

βάρος τρίτων, εφόσον έχουν λάβει γνώση αυτών. Συνεπώς, η εφαρμογή της δέουσας επιμέλειας διευρύνει το πεδίο της κρατικής ευθύνης πέραν των θετικών κρατικών ενεργειών *(acts)*, ενσωματώνοντας και τις παραλείψεις *(omissions)* που ανέχονται ή διευκολύνουν την ανενόχλητη δράση ιδιωτών.

Ωστόσο, η συγκεκριμένη «γέφυρα» λογοδοσίας εγκυμονεί τον κίνδυνο να μετεξελιχθεί σε παράγοντα αποσταθεροποίησης των διεθνών σχέσεων, εφόσον τύχει εσφαλμένης εργαλειοποίησης. Επισημαίνεται, άλλωστε, ότι η παραβίαση της δέουσας επιμέλειας συνιστά ένα αυτοτελές διεθνές αδίκημα που θεμελιώνεται σε παράλειψη και όχι σε θετική πράξη επιθετικότητας. Κατά συνέπεια, δεν παρέχει στο κράτος-θύμα το απαιτούμενο νομικό έρεισμα προκειμένου να εξαπολύσει δυσανάλογα αντίμετρα *(countermeasures)* εναντίον του κράτους προέλευσης, εξισώνοντάς το κατ' ουσίαν με τον αρχικό επιτιθέμενο δρώντα.

Η διάκριση αυτή καθίσταται κεφαλαιώδους σημασίας για τη διασφάλιση της προστασίας των λεγόμενων «κρατών-διαμετακομιστών» *(transit states)*. Η απλή τεχνική διέλευση κακόβουλων πακέτων δεδομένων *(routing)* μέσω των ψηφιακών κόμβων ενός κράτους δεν αρκεί για να γεννήσει αυτοδίκαια υποχρέωση δέουσας επιμέλειας. Τα όποια λαμβανόμενα αντίμετρα, που αποσκοπούν στην αναχαίτιση της κυβερνοεπίθεσης, οφείλουν να διέπονται αυστηρά από την αρχή της αναλογικότητας *(proportionality)*. Με αυτόν τον τρόπο, αποτρέπεται η αδικαιολόγητη κλιμάκωση στο διεθνές στερέωμα και προστατεύονται τα ανύποπτα κράτη, τα οποία καθίστανται και τα ίδια έμμεσα θύματα της ψηφιακής εκμετάλλευσης των υποδομών τους από τους πραγματικούς δράστες.

Το «Δέον Μέτρο» (Standard of Care) και η Τεχνική Ικανότητα

Ο εννοιολογικός προσδιορισμός του «δέοντος μέτρου» *(standard of care)*, το οποίο αξιώνεται από τα υποκείμενα του διεθνούς δικαίου στο πλαίσιο της αρχής της

δέουσας επιμέλειας στον κυβερνοχώρο, συνιστά ένα δυναμικό και διαρκώς εξελισσόμενο ζήτημα. Η νομική δέσμευση που απορρέει από τη δέουσα επιμέλεια συνιστά, εκ φύσεως, υποχρέωση συμπεριφοράς *(obligation of conduct)* και επ' ουδενί υποχρέωση αποτελέσματος *(obligation of result).*[24]

Τούτο συνεπάγεται ότι τα κράτη δεν υπέχουν αντικειμενική ευθύνη για οιαδήποτε επιβλαβή κυβερνοεπίθεση εκπορεύεται από την επικράτειά τους. Αντιθέτως, η στοιχειοθέτηση της κρατικής ευθύνης προϋποθέτει την απόδειξη ότι το κράτος παρέλειψε να λάβει τα εύλογα και αναγκαία μέτρα (*reasonable and necessary measures)* προς τον σκοπό της πρόληψης ή της αναχαίτισης της εν λόγω δραστηριότητας.

Η υφιστάμενη τεχνική ικανότητα και οι διαθέσιμοι εθνικοί πόροι διαδραματίζουν καταλυτικό ρόλο στην *in concreto* εξειδίκευση αυτού του «δέοντος μέτρου». Ειδικότερα, ένα κράτος το οποίο διαθέτει προηγμένες τεχνολογικές υποδομές και υψηλής εξειδίκευσης ανθρώπινο δυναμικό, υπέχει την υποχρέωση εφαρμογής σαφώς πιο σύνθετων και εξελιγμένων μέτρων κυβερνοασφάλειας, συγκριτικά με ένα αναπτυσσόμενο κράτος.

Εντούτοις, η συγκεκριμένη διαφοροποίηση δεν συνεπάγεται την πλήρη απαλλαγή των κρατών με περιορισμένους πόρους από τις δεσμεύσεις της δέουσας επιμέλειας. Τουναντίον, τα εν λόγω κράτη βαρύνονται με την υποχρέωση να καταβάλλουν τη μέγιστη δυνατή προσπάθεια για την ενίσχυση και την οικοδόμηση των εθνικών ψηφιακών τους ικανοτήτων, καθώς και να επιδιώκουν ενεργά τη διεθνή συνεργασία για τη θωράκιση της κυβερνοασφάλειάς τους.

Συμπερασματικά, καίτοι η αρχή της δέουσας επιμέλειας επιδέχεται μια διαφοροποιημένη (ή ασύμμετρη) εφαρμογή η οποία σταθμίζει τις εθνικές ιδιαιτερότητες και δυνατότητες, ταυτοχρόνως λειτουργεί ως βασικός νομικός μοχλός για την προώθηση και εδραίωση ενός ελάχιστου

[24] Jensen και Watts, "Cyber Duty of Due Diligence," 1566.

κατώτατου ορίου ασφαλείας *(minimum baseline of security)* στο παγκόσμιο ψηφιακό οικοσύστημα.[25]

Νεοφανείς Προκλήσεις: Τεχνητή Νοημοσύνη Κυβερνοεπιχειρήσεις Καθοδηγούμενες από Τεχνητή Νοημοσύνη (AI-Driven Cyber Operations)

Η ολοένα και αυξανόμενη ενσωμάτωση συστημάτων Τεχνητής Νοημοσύνης (Artificial Intelligence - AI) στο επιχειρησιακό πεδίο του κυβερνοχώρου αναδιαμορφώνει άρδην το κανονιστικό πλαίσιο της δέουσας επιμέλειας, εισάγοντας πρωτόγνωρες παραμέτρους πολυπλοκότητας και ταχύτητας. Η αυτοματοποίηση των επιθετικών ενεργειών μέσω αλγορίθμων, οι οποίοι διαθέτουν την ικανότητα να εντοπίζουν τρωτότητες *(vulnerabilities)* και να εκτελούν πλήγματα με ελάχιστη ή μηδενική ανθρώπινη παρέμβαση, εκμηδενίζει ουσιαστικά τον διαθέσιμο χρόνο αντίδρασης των κρατών.[26] Ως εκ τούτου, οι παραδοσιακές προσεγγίσεις εφαρμογής της δέουσας επιμέλειας, οι οποίες εδράζονται στην ανθρώπινη εποπτεία *(human-in-the-loop),* καθίστανται πρακτικά ανεπαρκείς έναντι ασύμμετρων απειλών που διαθέτουν την ικανότητα αυτόνομης μάθησης και δυναμικής προσαρμογής.

---

[25] Για την έμπρακτη ικανοποίηση αυτού του ελάχιστου κατώτατου ορίου (minimum baseline), το διεθνές δίκαιο αξιώνει από τα κράτη να υιοθετήσουν συγκεκριμένα δεσμικά και διαδικαστικά μέτρα (*institutional and procedural measures*). Πρωτίστως, η αρχή της δέουσας επιμέλειας επιτάσσει τη θέσπιση εθνικής ποινικής νομοθεσίας για την καταπολέμηση του κυβερνοεγκλήματος, με κατευθυντήριο γνώμονα νομικά κείμενα όπως η Σύμβαση της Βουδαπέστης (Budapest Convention on Cybercrime), καθώς τα κράτη που στερούνται σχετικού πλαισίου μετατρέπονται ακούσια σε «ασφαλή ψηφιακά καταφύγια» *(cyber safe havens)* (Kreuzer, *Harm Prevention Rule in Cyberspace*, 235-236· Bannelier, "Due Diligence as a Cardinal Principle," 60). Δευτερευόντως, απαιτείται η εγκαθίδρυση Εθνικών Ομάδων Αντιμετώπισης Έκτακτων Αναγκών (CERTs/CSIRTs), οι οποίες λειτουργούν ως τα αναγκαία εθνικά σημεία επαφής *(points of contact)* για τη λήψη ειδοποιήσεων και τη διεθνή συνεργασία (Kreuzer, *Harm Prevention Rule in Cyberspace*, 267-270). Ενώ η αδυναμία αναχαίτισης μιας τεχνολογικά προηγμένης επίθεσης μπορεί να δικαιολογηθεί λόγω έλλειψης τεχνικών πόρων, η απουσία αυτών των στοιχειωδών νομοθετικών και διοικητικών δομών συνιστά αμέλεια που δεν μπορεί να δικαιολογηθεί επαρκώς μέσω της γενικής επίκλησης περιορισμένων εθνικών ικανοτήτων.

[26] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Oxford: Future of Humanity Institute, University of Oxford 2018), 25, 33-34.

Η ραγδαία ταχύτητα εκτέλεσης των AI-καθοδηγούμενων κυβερνοεπιθέσεων επιβεβαιώνει την κεντρική ερευνητική υπόθεση της παρούσας μελέτης: η αρχή της δέουσας επιμέλειας επιβάλλεται να μετεξελιχθεί σε μία τεχνοπροληπτική υποχρέωση *(techno-preventive obligation).* Τα κράτη δεν διαθέτουν πλέον την ευχέρεια να εστιάζουν αποκλειστικά στην εκ των υστέρων (*ex post*) κατασταλτική αντίδραση.[27] Αντιθέτως, υπέχουν την επιτακτική

[27] Στην παραδοσιακή θεωρία αλλά και στη σύγχρονη κρατική πρακτική, η αμιγώς «εκ των υστέρων» *(reactive)* φύση της δέουσας επιμέλειας έχει υποστηριχθεί σθεναρά ως το απόλυτο νομικό «δίχτυ ασφαλείας» *(failsafe)* για τα κράτη-θύματα. Στην ισχυρότερη εκδοχή αυτού του επιχειρήματος, ο Michael N. Schmitt υποστηρίζει ότι τα κράτη δεν έχουν καμία υποχρέωση προληπτικής παρακολούθησης των δικτύων τους και η ευθύνη τους γεννάται μόνο αφού λάβουν γνώση μιας εν εξελίξει επίθεσης (Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum* 125 (2015): 75-76). Σε νεότερη ανάλυσή του (βλ. Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review* 3, no. 3 (2020): 32-47), ο Schmitt επιβεβαιώνει ότι τα κράτη αποδέχονται πλέον τη δέουσα επιμέλεια ως δεσμευτικό κανόνα ακριβώς επειδή απουσιάζει οποιαδήποτε απαίτηση για λήψη προληπτικών μέτρων *(absence of any requirement to take preventive measures).* Η προσέγγιση αυτή επιτρέπει στα κράτη να ερμηνεύουν τους κανόνες του διεθνούς δικαίου με τρόπο που μεγιστοποιεί τις επιλογές αντίδρασής τους απέναντι σε επιθέσεις: εάν το εδαφικό κράτος αδρανήσει, το κράτος-θύμα νομιμοποιείται να πλήξει ψηφιακές υποδομές εντός του αμελούς κράτους (ακόμα και αν ανήκουν σε ιδιώτες), καθώς αίρεται ο άδικος χαρακτήρας της προσβολής της κυριαρχίας του, παρακάμπτοντας έτσι πλήρως το αδιέξοδο της απόδοσης ευθυνών *(circumventing attribution)* (Schmitt, "In Defense of Due Diligence," 79-80). Προς διευκόλυνση αυτής της κατασταλτικής αντίδρασης, ισχυρά κράτη -όπως η Γαλλία, η Ολλανδία και το Ηνωμένο Βασίλειο- επιχειρηματολογούν πλέον υπέρ της πλήρους παράκαμψης της υποχρέωσης «προειδοποίησης» *(notice)* πριν τη λήψη αντιμέτρων, επικαλούμενα την ταχύτητα των κυβερνοεπιθέσεων και την ανάγκη προστασίας των απόρρητων ικανοτήτων τους.
Ωστόσο, η παρούσα μελέτη αντιτείνει ότι αυτή η αμιγώς κατασταλτική προσέγγιση -όπου τα κράτη απλώς περιμένουν να δεχθούν επίθεση για να εξαπολύσουν αιφνιδιαστικά αντίμετρα- καθίσταται επιχειρησιακά παρωχημένη και νομικά μάλλον επισφαλής σε μια εποχή αυτόνομης Τεχνητής Νοημοσύνης. Η αστραπιαία ταχύτητα των αλγορίθμων εκμηδενίζει τον διαθέσιμο χρόνο αντίδρασης, ενώ η νομιμοποιημένη ευχέρεια για άμεσα, αυτοματοποιημένα αντίμετρα εναντίον υποδομών τρίτων κρατών (όπως τα «κράτη-διαμετακομιστές»/*transit states)* αυξάνει δραματικά τον κίνδυνο «ακούσιων εμπλοκών» *(unintended engagements)* και ανεξέλεγκτης κλιμάκωσης από τα αμυντικά AI συστήματα. Για τον λόγο αυτό, εν όψει των ασύμμετρων ψηφιακών απειλών, η δέουσα επιμέλεια οφείλει να μετεξελιχθεί από ένα απλό νομικό άλλοθι για τη χρήση εκ των υστέρων αντιμέτρων σε μια αυστηρή, προληπτική «τεχνο-κανονιστική υποχρέωση».

υποχρέωση να αναπτύξουν και να εγκαθιδρύσουν προηγμένα συστήματα αυτόματης ανίχνευσης απειλών και ενεργού άμυνας. Εντούτοις, η επιχειρησιακή αξιοποίηση τέτοιων αυτόνομων αμυντικών συστημάτων εγείρει, με τη σειρά της, αναδυόμενα νομικά ζητήματα. Πρωτίστως, ανακύπτει ο σοβαρός κίνδυνος «ακούσιων εμπλοκών» *(unintended engagements)* ή εσφαλμένης κλιμάκωσης, η οποία ενδέχεται να πυροδοτηθεί ανεξέλεγκτα από τα αυτόνομα συστήματα του αμυνόμενου κράτους.[28]

Συμπερασματικά, η Τεχνητή Νοημοσύνη δεν μπορεί πλέον να προσεγγίζεται υπό ένα αμιγώς εργαλειακό πρίσμα. Αντίθετα, αναδεικνύεται στον κρίσιμο παράγοντα που επιβάλλει τη νομική μετάβαση της δέουσας επιμέλειας: από μια παραδοσιακή υποχρέωση που επαφίεται στην εκ των υστέρων ανθρώπινη αντίδραση, σε ένα δυναμικό, τεχνοπροληπτικό κανονιστικό πρότυπο, το οποίο απαιτεί την αυτοματοποιημένη θωράκιση των εθνικών υποδομών.

Η Ευθύνη για «Αλγοριθμική Παράλειψη»

[28] Tom van Benthem, "Symposium on Military AI and the Law of Armed Conflict: Responsible Deployments of Militarised AI - The Power of Information to Prevent Unintended Engagements", *Opinio Juris*, 02.04.2024, πρόσβαση: 20/05/2026, https://opiniojuris.org/2024/04/02/symposium-on-military-ai-and-the-law-of-armed-conflict-responsible-deployments-of-militarised-ai-the-power-of-information-to-prevent-unintended-engagements/.
Επιπλέον, σημειωτέον ότι η υιοθέτηση επιθετικών τεχνικών «ενεργού άμυνας» (*active cyber defence*) ή αυτοματοποιημένων αντεπιθέσεων *(hack-backs)* από συστήματα Τεχνητής Νοημοσύνης εγείρει σοβαρότατα ζητήματα νομιμότητας στο διεθνές δίκαιο. Όπως υπογραμμίζεται στη νομική θεωρία, τα αντίμετρα στον κυβερνοχώρο υπόκεινται σε αυστηρούς περιορισμούς: πρέπει να είναι αναλογικά και να έχουν ως αποκλειστικό σκοπό τον εξαναγκασμό του παραβάτη σε συμμόρφωση (Kreuzer, *Harm Prevention Rule in Cyberspace*, 288-291). Η εσφαλμένη, αυτοματοποιημένη στοχοποίηση «κρατών-διαμετακομιστών» *(transit states)* ή ανύποπτων ιδιωτικών υποδομών από έναν αμυντικό αλγόριθμο δεν βρίσκει νομικό έρεισμα. Τουναντίον, τέτοιες ενέργειες δύνανται να συνιστούν παραβίαση της εδαφικής κυριαρχίας *(territorial sovereignty)* και της αποκλειστικής δικαιοδοσίας του εδαφικού κράτους, παραβίαση της αρχής της μη επέμβασης ή -ανάλογα με την κλίμακα και τα αποτελέσματά τους- ακόμη και παραβίαση της απαγόρευσης χρήσης βίας (Kreuzer, *Harm Prevention Rule in Cyberspace*, 127-128).

Εν συνεχεία, η ραγδαία εξέλιξη της Τεχνητής Νοημοσύνης εισάγει ένα καινοφανές νομικό ζήτημα στο πεδίο της κρατικής ευθύνης: την έννοια της «τεχνο-κανονιστικής παράλειψης» *(techno-regulatory omission).* Η συγκεκριμένη θεωρητική σύλληψη αναφέρεται στο ενδεχόμενο να στοιχειοθετηθεί διεθνής ευθύνη ενός κράτους, βάσει της αρχής της δέουσας επιμέλειας, σε περίπτωση που το τελευταίο παραλείψει να θεσπίσει το προσήκον ρυθμιστικό πλαίσιο για τον έλεγχο της ανάπτυξης και της χρήσης επιθετικών εργαλείων τεχνητής νοημοσύνης από ιδιωτικούς δρώντες εντός της επικράτειάς του.

Οι παραδοσιακές νομικές έννοιες της «γνώσης» *(knowledge)* και του «ελέγχου» *(control)* του κράτους επί των δραστηριοτήτων που λαμβάνουν χώρα στο έδαφός του -όπως αυτές αναλύθηκαν εκτενώς στο Κεφάλαιο 2- υφίστανται σημαντική διεύρυνση σε ένα ψηφιακό περιβάλλον όπου οι αλγόριθμοι διαθέτουν την ικανότητα να επιχειρούν αυτόνομα και να προκαλούν διασυνοριακές βλάβες *(cross-border harm)* ελλείψει άμεσης ανθρώπινης παρέμβασης.[29] Ως εκ τούτου, ο καταλογισμός της κρατικής ευθύνης δεν περιορίζεται πλέον αποκλειστικά στην ενεργή κρατική υποστήριξη ή την παθητική ανοχή των φυσικών αυτουργών, αλλά επεκτείνεται στην εγγενή αδυναμία ή την παράλειψη επαρκούς ρυθμιστικής εποπτείας *(regulatory oversight).*

Αυτή η μετατόπιση της ευθύνης στο ίδιο το Κράτος έρχεται σε αντιδιαστολή με την παραδοσιακή προσέγγιση του Δικαίου των Ένοπλων Συγκρούσεων (LOAC/International Humanitarian Law) σχετικά με τα αυτόνομα οπλικά συστήματα. Στο παραδοσιακό πεδίο της μάχης, υποστηρίζεται από κορυφαίους μελετητές -όπως οι Schmitt και Thurnher- ότι οι άνθρωποι δεν βρίσκονται ποτέ πραγματικά «εκτός βρόχου» *(out of the loop)* και ότι η ατομική ποινική ευθύνη για πιθανά εγκλήματα πολέμου μέσω της χρήσης αυτόνομων συστημάτων θα βαρύνει πάντα τα φυσικά πρόσωπα, δηλαδή τους στρατιωτικούς διοικητές, τους χειριστές ή τους προγραμματιστές.

[29] Ahmet Küçükuncular, "Addressing Ethical Challenges in Cyber-space Governance: Recommendations for the Digital Sovereignty Era," *Digital Society* 5, άρθρο 3 (2026): 25-26.

Ωστόσο, στον ασύμμετρο και ρευστό κυβερνοχώρο - όπου οι αυτόνομες επιθέσεις συχνά αναπτύσσονται από ιδιωτικές εταιρείες και εκτελούνται υπό καθεστώς απόλυτης ανωνυμίας κάτω από το κατώφλι της ένοπλης σύγκρουσης *(below the threshold of armed conflict)*- αυτή η ατομικο-ποινική προσέγγιση καταρρέει επιχειρησιακά. Ελλείψει της δυνατότητας άμεσου εντοπισμού του φυσικού αυτουργού πίσω από τον αλγόριθμο, η μόνη δικαιικά συνεπής λύση προκειμένου να μην υπάρξει κενό λογοδοσίας είναι η επιβολή διεθνούς κρατικής ευθύνης στο ίδιο το εδαφικό κράτος για την «τεχνο-κανονιστική του παράλειψη» να ρυθμίσει και ελέγξει τα συστήματα που αναπτύσσονται και επιχειρούν από την επικράτειά του.

Η εν λόγω διεύρυνση του πεδίου εφαρμογής της κρατικής ευθύνης επιτάσσει στα κράτη την εκπόνηση αυστηρών κανονιστικών πλαισίων, τα οποία θα διασφαλίζουν την υπεύθυνη ανάπτυξη των συστημάτων AI, με ιδιαίτερη έμφαση στους τομείς που άπτονται της εθνικής και διεθνούς ασφάλειας. Η συμβατική αυτή υποχρέωση εμπεριέχει την επιβολή προηγμένων προτύπων κυβερνοασφάλειας, την αυστηρή απαίτηση για «αλγοριθμική διαφάνεια» *(algorithmic transparency)*, καθώς και τη θέσπιση δεσμευτικών μηχανισμών εταιρικής λογοδοσίας *(corporate accountability)* για τους φορείς ανάπτυξης τέτοιου είδους λογισμικού.[30]

[30] Η αναγκαιότητα αυτής της ρυθμιστικής παρέμβασης επιβεβαιώνεται από τη σύγχρονη κρατική πρακτική σχετικά με τον έλεγχο εξαγωγών κυβερνο-όπλων *(export controls of cyber weapons)*. Αντλώντας έρεισμα από το ιστορικό προηγούμενο της Διαιτησίας της Αλαμπάμα -η οποία καθιέρωσε ότι η έλλειψη εσωτερικής νομοθεσίας δεν δικαιολογεί την κρατική αδράνεια- τα κράτη καλούνται πλέον να ασκούν αυστηρή εποπτεία και να επιβάλλουν συστήματα αδειοδότησης σε ιδιωτικές εταιρείες που αναπτύσσουν επιθετικά λογισμικά (Lemnitzer, "Back to the Roots," 814-815). Χαρακτηριστικό παράδειγμα αποτελεί η ένταξη των λογισμικών παραβίασης *(intrusion software)* στον Διακανονισμό του Wassenaar (Wassenaar Arrangement) για τις τεχνολογίες διπλής χρήσης, καθώς και οι πρόσφατες διεθνείς νομικές αντιδράσεις απέναντι σε εταιρείες όπως η ισραηλινή NSO Group. Τα παραδείγματα αυτά καταδεικνύουν ότι η ανοχή ή η απουσία κρατικού ελέγχου στην ανάπτυξη και πώληση ψηφιακών όπλων όχι μόνο υποθάλπει την ποινικά κολάσιμη «κατάχρηση συσκευών» *(misuse of devices)*, αλλά πλέον τείνει να παγιωθεί ως σαφής παραβίαση της διεθνούς υποχρέωσης δέουσας

Η παράλειψη δέσπισης των προαναφερθέντων ρυθμιστικών μηχανισμών δύναται νομικώς να ερμηνευθεί ως ευθεία παραβίαση της υποχρέωσης δέουσας επιμέλειας, καθιστώντας το κράτος διεθνώς υπόλογο για τις έννομες συνέπειες των τεχνο-κανονιστικών του παραλείψεων. Συμπερασματικά, η προαναφερθείσα έννοια αναδεικνύει την επιτακτική αναγκαιότητα μετάβασης σε μία προληπτική και κανονιστική *(preventive and regulatory)* προσέγγιση της αρχής της δέουσας επιμέλειας, απολύτως προσαρμοσμένης στις ραγδαίες τεχνολογικές προκλήσεις της εποχής της Τεχνητής Νοημοσύνης.

Προς ένα Διεθνές Πλαίσιο «Ψηφιακής Επαγρύπνησης»

Η εγγενής πολυπλοκότητα και ο υπερεθνικός (διασυνοριακός) χαρακτήρας των σύγχρονων κυβερνοαπειλών, σε άμεση συνάρτηση με την εκθετική εξέλιξη της Τεχνητής Νοημοσύνης, καθιστούν αδήριτη την ανάγκη συγκρότησης ενός συνεκτικού διεθνούς κανονιστικού πλαισίου «ψηφιακής επαγρύπνησης» *(digital vigilance).* Το εν λόγω κανονιστικό πλαίσιο οφείλει να ενσωματώνει οργανικά την ενισχυμένη διακρατική συνεργασία, καθώς και την ενεργή, συστηματική ανταλλαγή πληροφοριών σχετικά με τις κυβερνοαπειλές *(cyber threat intelligence),* ανάγοντάς τες σε αναπόσπαστο συστατικό στοιχείο της νομικής υποχρέωσης της δέουσας επιμέλειας[31].

Η αποτελεσματική πρόληψη και η έγκαιρη αναχαίτιση των κυβερνοεπιθέσεων προαπαιτούν πλέον τη σύμπραξη και τη συλλογική δράση της διεθνούς κοινότητας. Τούτο διότι κανένα υποκείμενο του διεθνούς δικαίου, ανεξαρτήτως του επιπέδου των εθνικών τεχνολογικών του δυνατοτήτων, δεν δύναται να θωρακιστεί απόλυτα έναντι των ασύμμετρων

επιμέλειας του κράτους (Lemnitzer, "Back to the Roots," 815-816· Kreuzer, *Harm Prevention Rule in Cyberspace*, 244-245).

[31] Maulana Anwar και Afkarul Azmi, "Cyber Sovereignty and International Law: Legal Challenges in the Digital Age," *Iustitia: Journal of Legal Theory, Politics, and International Relations* 1, no. 1 (2026): 54-55.

ψηφιακών απειλών δρώντας μεμονωμένα. Συνεπώς, η θεσμοθετημένη διεθνής συνεργασία αναδεικνύεται σε κεφαλαιώδη προϋπόθεση εθνικής και παγκόσμιας ασφάλειας. Η θεμελίωση της «ψηφιακής επαγρύπνησης» προϋποθέτει, επιπροσθέτως, την υιοθέτηση μιας κοινά αποδεκτής νομικής αντίληψης *(common legal understanding)* ως προς τα αποδεκτά πρότυπα συμπεριφοράς *(norms of behavior)* στον κυβερνοχώρο, καθώς και την ανάπτυξη αποτελεσματικών εποπτικών μηχανισμών για τον έλεγχο της κρατικής συμμόρφωσης. Η συγκεκριμένη στόχευση εξειδικεύεται μέσω της σύστασης θεσμικών διεθνών φόρουμ για τον επιχειρησιακό συντονισμό της ασφάλειας, της διαμόρφωσης ενοποιημένων πρωτοκόλλων αντιμετώπισης περιστατικών *(incident response)* και, όλως ιδιαιτέρως, της διαρκούς ενίσχυσης των ψηφιακών ικανοτήτων και υποδομών των αναπτυσσόμενων κρατών *(capacity building).*[32]

Παρότι η επικείμενη έκδοση του Tallinn Manual 3.0 αναμένεται να προσφέρει έναν χρήσιμο ερμηνευτικό άξονα για την προσαρμογή του ισχύοντος διεθνούς δικαίου στις νεοπαγείς ψηφιακές συνθήκες, η ραγδαία εξέλιξη των απειλών καθιστά αναγκαία τη δογματική του υπέρβαση. Κατά συνέπεια, η μετάβαση προς το προτεινόμενο ολιστικό πλαίσιο της «ψηφιακής επαγρύπνησης» υπερβαίνει την αναμενόμενη κωδικοποίηση. Δεν εξαντλείται στη σφαίρα της απλής πολιτικής σκοπιμότητας, αλλά αναδεικνύεται ως αυστηρή νομική αναγκαιότητα για τη διαφύλαξη της σταθερότητας

[32] Η απουσία ψηφιακών ικανοτήτων δεν απαλλάσσει τα κράτη από το ελάχιστο όριο της δέουσας επιμέλειας, αλλά καθιστά τη θεσμική διεθνή υποστήριξη επιβεβλημένη, προκειμένου να μην μετατραπούν τα τεχνολογικά ασθενέστερα κράτη σε «ακούσια ασφαλή καταφύγια» *(unwitting safe havens)* για κακόβουλους δρώντες (Bannelier, "Due Diligence as a Cardinal Principle," 52). Είναι γεγονός ότι, επί του παρόντος, στις διαδικασίες του ΟΗΕ (όπως η OEWG), πολλά κράτη αντιμετωπίζουν την ανταλλαγή πληροφοριών και τη συνεργασία ως προαιρετικά «Μέτρα Οικοδόμησης Εμπιστοσύνης» (Confidence-Building Measures - CBMs) και όχι ως νομικές υποχρεώσεις (Kreuzer, *Harm Prevention Rule in Cyberspace*, 186, 199). Ωστόσο, το πλαίσιο της «ψηφιακής επαγρύπνησης» επιτάσσει ότι η διεθνής συνεργασία, και ειδικότερα η εγκαθίδρυση και στενή δικτύωση Εθνικών Ομάδων Αντιμετώπισης Έκτακτων Αναγκών (CERTs/CSIRTs) ως μόνιμων σημείων επαφής, πρέπει να αποκρυσταλλωθεί άμεσα ως μια νομικά δεσμευτική διαδικαστική υποχρέωση *(procedural due diligence obligation)* (Kreuzer, *Harm Prevention Rule in Cyberspace*, 268-271).

εντός ενός ρευστού και διαρκώς μεταβαλλόμενου ψηφιακού οικοσυστήματος.

Η Τεχνοπροληπτική Πρόταση και οι Εγγυήσεις του Διεθνούς Δικαίου Ανθρωπίνων Δικαιωμάτων

Υπό το πρίσμα της ανωτέρω δικαιικής και τεχνολογικής εξέλιξης, και προκειμένου να αποφευχθεί οποιαδήποτε εννοιολογική σύγχυση με τις αναμενόμενες - πλην όμως εγγενώς συντηρητικότερες- κωδικοποιήσεις τύπου Tallinn Manual 3.0, η παρούσα μελέτη πρότεινε την αναβάθμιση της δέουσας επιμέλειας σε μια τεχνοπροληπτική υποχρέωση. Η ιδιάζουσα αυτή υποχρέωση εδράζεται σε δύο αλληλένδετους πυλώνες: αφενός, στην αυστηρή ρύθμιση για την αποτροπή της «τεχνο-κανονιστικής παράλειψης» και, αφετέρου, στην ενεργή εποπτεία των ψηφιακών υποδομών. Δεδομένου ότι η μετάβαση σε ένα προληπτικό μοντέλο εγείρει εύλογες ενστάσεις ως προς τον πιθανό κίνδυνο προσβολής των ανθρωπίνων δικαιωμάτων, η προτεινόμενη θεωρητική κατασκευή θωρακίζεται μέσω συγκεκριμένων δικαιικών δικλείδων ασφαλείας, οι οποίες αποκλείουν κατηγορηματικά την κρατική αυθαιρεσία.

Πρώτον, η ψηφιακή επαγρύπνηση επικεντρώνεται αποκλειστικά στις υποδομές και στους αλγορίθμους, όχι στα φυσικά πρόσωπα. Η υποχρέωση δέουσας επιμέλειας δεν απαιτεί από το κράτος να κατασκοπεύει τις ιδιωτικές επικοινωνίες των πολιτών του, αλλά επιτάσσει την ενεργή εποπτεία εκείνων των τεχνολογιών (όπως *servers ή botnets)* που δύνανται να εργαλειοποιηθούν ως «κρατικοί πληρεξούσιοι» *(proxies)* χωρίς άμεσο ανθρώπινο έλεγχο. Σε απόλυτη συνάρτηση με αυτό, η προτεινόμενη ανταλλαγή πληροφοριών απειλών αφορά αμιγώς τη διακίνηση τεχνικών δεδομένων (όπως IP διευθύνσεις κακόβουλων διακομιστών και ψηφιακές υπογραφές λογισμικού) και ουδέποτε αγγίζει το προστατευόμενο περιεχόμενο των ιδιωτικών επικοινωνιών.

Δεύτερον, το προτεινόμενο μοντέλο μετατοπίζει το βάρος στη ρύθμιση της ιδιωτικής αγοράς, αποτρέποντας τη δημιουργία ενός κρατικού 'Panopticon'. Μέσω της τεχνο-

κανονιστικής υποχρέωσης, το κράτος δεν μετατρέπεται σε παρακολουθούντα, αλλά καλείται να υποχρεώσει διά νόμου τις εταιρείες ανάπτυξης επιθετικών εργαλείων Τεχνητής Νοημοσύνης να εφαρμόζουν εντός της επικράτειάς του αυστηρή «αλγοριθμική διαφάνεια» *(algorithmic transparency)* και μηχανισμούς εταιρικής λογοδοσίας *(corporate accountability).* Κατ' αυτόν τον τρόπο, η πρόληψη επιτυγχάνεται εκ του σχεδιασμού *(by design)* στην πηγή παραγωγής της τεχνολογίας, καθιστώντας περιττή την εκ των υστέρων κρατική επέμβαση στα προσωπικά δεδομένα των χρηστών.

Τρίτον και κυριότερον, η τεχνοπροληπτική θεώρηση τελεί σε συστηματική εναρμόνιση με το Διεθνές Δίκαιο Ανθρωπίνων Δικαιωμάτων. Ως υποχρέωση συμπεριφοράς, η δέουσα επιμέλεια ρητώς απαγορεύει τη μαζική παρακολούθηση, καθώς κάτι τέτοιο θα κατέλυε τον πυρήνα του δικαιώματος στην ιδιωτικότητα. Το διεθνές δίκαιο δεν αξιώνει ένα κράτος-παντεπόπτη, αλλά την εφαρμογή εύλογων και αναλογικών μέτρων. Συνεπώς, η παρούσα πρόταση προσφέρει ένα βιώσιμο δογματικό εργαλείο, το οποίο αναβαθμίζει την ασφάλεια απέναντι στις ραγδαίες τεχνολογικές εξελίξεις, σεβόμενη παράλληλα τον βαθύ πυρήνα των ατομικών ελευθεριών στον κυβερνοχώρο.

Συμπεράσματα

Η παρούσα μελέτη κατέδειξε τη βαθιά μετασχηματιστική επίδραση που ασκεί το περιβάλλον του κυβερνοχώρου και η ραγδαία εξέλιξη των αναδυόμενων τεχνολογιών -με προεξάρχουσα την Τεχνητή Νοημοσύνη- επί της αρχής της δέουσας επιμέλειας *(due diligence)* στο πεδίο του Διεθνούς Δικαίου. Όπως τεκμηριώθηκε εκτενώς, η εγγενής δυσχέρεια στον άμεσο νομικό καταλογισμό των επιβλαβών κυβερνοεπιχειρήσεων, αναδεικνύει τη δέουσα επιμέλεια ως το πλέον δόκιμο και αξιόπιστο κανονιστικό εργαλείο για την εδραίωση της διεθνούς λογοδοσίας. Η ενδελεχής δογματική αναδρομή στην ιστορική εξέλιξη της εν λόγω αρχής -από την εμβληματική νομολογία της Υπόθεσης του Στενού της Κέρκυρας έως τις σύγχρονες θεωρητικές

προσεγγίσεις περί της νομικής της φύσης- επιβεβαίωσε την προοδευτική παγίωσή της ως δεσμευτικού κανόνα του διεθνούς εθιμικού δικαίου. Η τάση αυτή εκτιμάται ότι θα αποτυπωθεί πληρέστερα στην επικείμενη έκδοση του Tallinn Manual 3.0, το οποίο αναμένεται να επιβεβαιώσει ότι η δέουσα επιμέλεια αποβάλλει τον χαρακτήρα μιας αμιγώς προαιρετικής κατευθυντήριας γραμμής, μετεξελισσόμενη σε μια θεμελιώδη νομική υποχρέωση - έστω και υπό την επιφύλαξη της στάσης των επίμονων αντιρρησιών.

Ωστόσο, προχωρώντας πέραν της κωδικοποίησης του υφιστάμενου δικαίου (*de lege lata*), κεντρικό θεωρητικό άξονα και κανονιστική πρόταση (*de lege ferenda*) της παρούσας έρευνας αποτέλεσε η επιχειρηματολογία ότι η δέουσα επιμέλεια επιβάλλεται να μετατοπιστεί από τη σφαίρα μιας παθητικής, εκ των υστέρων (*ex post*) κατασταλτικής αντίδρασης, σε αυτήν μιας «τεχνοπροληπτικής υποχρέωσης». Η εν λόγω κανονιστική μετάβαση, την οποία εισάγει η μελέτη, επιτάσσει στα υποκείμενα του διεθνούς δικαίου όχι απλώς τη λήψη κατασταλτικών μέτρων, αλλά την ενεργή και συστηματική εποπτεία των ψηφιακών υποδομών που ευρίσκονται υπό τη δικαιοδοσία τους. Υπό το πρίσμα αυτό, η θεωρητική κατασκευή της «τεχνο-κανονιστικής παράλειψης» αναδείχθηκε ως μείζον νομικό εργαλείο, καταδεικνύοντας την αδήριτη αναγκαιότητα άμεσης θέσπισης στιβαρών ρυθμιστικών πλαισίων. Τα πλαίσια αυτά οφείλουν να διασφαλίζουν την υπεύθυνη ανάπτυξη, διαχείριση και επιχειρησιακή χρήση αυτόνομων συστημάτων εκ μέρους των ιδιωτικών δρώντων. Κατά συνέπεια, η αποτελεσματική πραγμάτωση της αρχής στην εποχή της Τεχνητής Νοημοσύνης απαιτεί πλέον την υιοθέτηση μιας ολιστικής στρατηγικής «ψηφιακής επαγρύπνησης», εντός της οποίας συγκεράζονται και αλληλεπιδρούν οργανικά οι νομικές, τεχνικές και διπλωματικές διαστάσεις της κρατικής δράσης.
Εν κατακλείδι, το νομικό καθήκον της δέουσας επιμέλειας αναδεικνύεται ως η σύγχρονη «λυδία λίθος» της κρατικής κυριαρχίας και της διεθνούς ευθύνης στον 21ο αιώνα. Η ουσιαστική και καθολική εφαρμογή της συνιστά την ικανή και αναγκαία συνθήκη για τη διαφύλαξη της παγκόσμιας σταθερότητας και ασφάλειας, παρέχοντας θεσμική θωράκιση έναντι των δυνητικώς ολέθριων συνεπειών των

κυβερνοεπιθέσεων. Προεκτείνοντας τον θεωρητικό ορίζοντα, η συστηματική νομική αξιολόγηση των επιπτώσεων που συνεπάγονται οι ρηξικέλευθες αναδυόμενες τεχνολογίες - όπως, επί παραδείγματι, η κβαντική υπολογιστική (*quantum computing*)- οριοθετεί το επόμενο κρίσιμο ερευνητικό διακύβευμα. Η έγκαιρη και εις βάθος θεωρητική ενασχόληση με τις εν λόγω τεχνολογίες θα διασφαλίσει ότι το Δημόσιο Διεθνές Δίκαιο θα διατηρήσει την κανονιστική του επικαιρότητα και ανθεκτικότητα, λειτουργώντας ως ένα αδιαπέραστο θεσμικό ανάχωμα απέναντι στις διαρκώς μεταβαλλόμενες, ασύμμετρες προκλήσεις του ψηφιακού μέλλοντος.

Πίνακας Αναφορών
Νομολογία

- *Alabama claims of the United States of America against Great Britain*. 14.09.1872. Reports of International Arbitral Awards, vol. XXIX, 125–134. https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf.
- *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. Judgment. I.C.J. Reports 2007, 43.
- *Corfu Channel (United Kingdom v. Albania)*. Merits, Judgment. I.C.J. Reports 1949, 4.
- *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. Merits, Judgment. I.C.J. Reports 1986, 14.
- *Trail smelter case (United States, Canada)*. 11.03.1941. Reports of International Arbitral Awards, vol. III, 1905–1982.

Διεθνή Έγγραφα & Εκδέσεις του ΟΗΕ

- International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. A/56/10, 2001.
- UN General Assembly. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/76/135, 2021.
- UN General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174, 2015.
- UN General Assembly. *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/75/816, 2021.

Βιβλιογραφία

- Anwar, Maulana, and Afkarul Azmi. "Cyber Sovereignty and International Law: Legal Challenges in the Digital Age." *Iustitia: Journal of Legal Theory, Politics, and International Relations* 1, no. 1 (2026): 47–56.
- Bannelier, Karine. "Due Diligence as a Cardinal Principle in the Fight against Malicious Cyber Activities." Στο *Global Cybersecurity and International Law*, ed. Antonio Segura Serrano. London: Routledge, 2024.
- Brundage, Miles, Shahar Avin, Jack Clark, et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford: Future of Humanity Institute, University of Oxford, 2018.
- Chircop, Luke. "A Due Diligence Standard of Attribution in Cyberspace." *International and Comparative Law Quarterly* 67, no. 3 (2018): 643–668.
- Jensen, Eric Talbot, και Sean Watts. "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?" *Texas Law Review* 95, no. 7 (2017): 1555–1577.
- Kreuzer, Leonhard. *The Harm Prevention Rule in Cyberspace: An Obligation of Due Diligence*. Baden-Baden: Nomos, 2024.
- Küçükuncular, Ahmet. "Addressing Ethical Challenges in Cyberspace Governance: Recommendations for the Digital Sovereignty Era." *Digital Society* 5, άρθρο 3 (2026): 1–34.
- Lemnitzer, Jan Martin. "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace." *European Journal of International Law* 33, no. 3 (2022): 789–819.
- Middleton, Fiona, και Nicholas Tsagourias. "Cyber Attribution and Its Challenges." Στο *Global Cybersecurity and International Law*, επιμ. Antonio Segura Serrano, [...]. London: Routledge, 2024.

- Mikanagi, Tomohiro. "Application of the Due Diligence Principle to Cyber Operations." *International Law Studies* 97 (2021): 1019–1038.
- Ministry of Foreign Affairs of Japan. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*. 2021. Πρόσβαση 15.05.2026. https://www.mofa.go.jp/files/100200935.pdf.
- Oxford Institute for Ethics, Law and Armed Conflict. "The Second Oxford Statement on International Law Protections of the Healthcare Sector during Covid-19: Safeguarding Vaccine Research." The Oxford Process, 2020. Πρόσβαση 18.05.2026. https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-second-oxford-statement/.
- Schmitt, Michael N. "In Defense of Due Diligence in Cyberspace." *Yale Law Journal Forum* 125 (2015): 68–81.
- Schmitt, Michael N. "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace." *Texas National Security Review* 3, no. 3 (2020): 32–47.
- Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
- Schmitt, Michael N., ed. *Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, υπό έκδοση.
- van Benthem, Tom. "Symposium on Military AI and the Law of Armed Conflict: Responsible Deployments of Militarised AI – The Power of Information to Prevent Unintended Engagements." *Opinio Juris*, 02.04.2024. https://opiniojuris.org/2024/04/02/symposium-on-military-ai-and-the-law-of-armed-conflict-responsible-deployments-of-militarised-ai-the-power-of-information-to-prevent-unintended-engagements/.
- Winslow, Ellie, και Joanna Bouckaert. "How Cybersecurity Can Best Navigate Geopolitics to Secure a

Resilient and Open Digital Future." World Economic Forum, 05.02.2026. https://www.weforum.org/stories/cybersecurity/cybersecurity-and-geopolitics-the-challenges-to-build-resilience-in-a-fragmented-world/.