

ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ»

ΕΙΔΙΚΕΥΣΗ:

«ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ ΚΑΙ ΔΙΠΛΩΜΑΤΙΚΕΣ ΣΠΟΥΔΕΣ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

*«Η «Παραγωγική» Τεχνητή Νοημοσύνη ως Όπλο στην Υπηρεσία Τρομοκρατικών
Ομάδων: Ρύθμιση, Λογοδοσία και Προκλήσεις στον Κυβερνοχώρο»*

*«Generative Artificial Intelligence as a Weapon in the Service of Terrorist Groups:
Regulation, Accountability, and Challenges in Cyberspace»*



Αθήνα, 2026

Παναγιώτης Μπεκιάρης (2124M019)

Επιβλέπουσα Καθηγήτρια: Ντανιέλλα Μαρία Μαρούδα

ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ»

ΕΙΔΙΚΕΥΣΗ:

«ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ ΚΑΙ ΔΙΠΛΩΜΑΤΙΚΕΣ ΣΠΟΥΔΕΣ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

*«Η «Παραγωγική» Τεχνητή Νοημοσύνη ως Όπλο στην Υπηρεσία Τρομοκρατικών
Ομάδων: Ρύθμιση, Λογοδοσία και Προκλήσεις στον Κυβερνοχώρο»*

*«Generative Artificial Intelligence as a Weapon in the Service of Terrorist Groups:
Regulation, Accountability, and Challenges in Cyberspace»*



Αθήνα, 2026

Παναγιώτης Μπεκιάρης (2124M019)

Επιβλέπουσα Καθηγήτρια: Ντανιέλλα Μαρία Μαρούδα

Τριμελής Επιτροπή:

- **Μαρία Ντανιέλα Μαρούδα**, Αναπληρώτρια Καθηγήτρια Διεθνούς Δικαίου - Διεθνούς Ανθρωπιστικού Δικαίου του Πάντειου Πανεπιστημίου Αθηνών,
- **Νικόλας Τσαγκουριάς**, Καθηγητής Διεθνούς Δικαίου του Πανεπιστημίου Sheffield,
- **Γεώργιος Ανέσιου**, Δρ. Διεθνούς Δικαίου του Πάντειου Πανεπιστημίου Αθηνών, της Σχολής Ικάρων της Πολεμικής Αεροπορίας και του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών.



Copyright © Παναγιώτης Μπεκιάρης, 2026

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

Υπεύθυνη Δήλωση – Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης:

Δηλώνω ότι η παρούσα εργασία είναι αποτέλεσμα πρωτότυπης έρευνας και δεν χρησιμοποιεί πνευματική ιδιοκτησία τρίτων χωρίς αναφορές. Αναλαμβάνω δε, όλες τις προβλεπόμενες νομικές και διοικητικές συνέπειες, σε περίπτωση που η εργασία μου τυχόν αποδειχθεί ότι αποτελεί προϊόν λογοκλοπής ή προϊόν τρίτων.

Ο δηλών, Παναγιώτης Μπεκιάρης

*Στη γιαγιά μου, Μένιω. Πηγή ανεξάντλητης δύναμης και πρότυπο ζωής.
Της αφιερώνω την παρούσα εργασία για όλα όσα μου δίδαξε και μου προσέφερε απλόχερα.*

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές και ειλικρινείς μου ευχαριστίες προς την επιβλέπουσα καθηγήτρια, Καθηγήτρια Ντανιέλλα Μαρία Μαρούδα, για τη σταθερή υποστήριξη, την επιστημονική καθοδήγηση και την εμπιστοσύνη που επέδειξε καθ' όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας. Η συμβολή της υπήρξε καθοριστική τόσο στην οριοθέτηση του ερευνητικού αντικειμένου όσο και στη διαμόρφωση μιας στιβαρής και τεκμηριωμένης ανάλυσης. Οι παρατηρήσεις, οι υποδείξεις και το υψηλό ακαδημαϊκό της πρότυπο αποτέλεσαν για εμένα πολύτιμο οδηγό και κίνητρο για συνεχή βελτίωση.

Ευχαριστώ, επίσης, τα μέλη της τριμελούς εξεταστικής επιτροπής για τον χρόνο που αφιέρωσαν στην αξιολόγηση του έργου, καθώς και για τις ουσιαστικές επισημάνσεις τους, οι οποίες συνέβαλαν στη βελτίωση και στην πληρέστερη τεκμηρίωση της έρευνας. Η συμβολή τους τιμά τον θεσμό του μεταπτυχιακού προγράμματος και ενισχύει την ποιότητα της ακαδημαϊκής διαδικασίας.

Σε ένα πιο προσωπικό επίπεδο, αισθάνομαι την ανάγκη να αφιερώσω την πρώτη μου διπλωματική εργασία στον αδελφό μου, Γιάννη. Η παρουσία του στη ζωή μου αποτελεί διαρκή πηγή έμπνευσης, δύναμης και προσανατολισμού. Με έχει διδάξει, με τον δικό του τρόπο, τι σημαίνει επιμονή, αφοσίωση και συνεχής προσπάθεια, καθώς και πόσο σημαντικό είναι να συνεχίζει κανείς να εξελίσσεται, να μην επαναπαύεται και να επιδιώκει το καλύτερο.

Η δύναμη που αντλώ από τον Γιάννη υπήρξε καθοριστικός παράγοντας για τη δική μου πορεία. Κάθε επίτευγμα, μικρό ή μεγάλο, έχει και το δικό του αποτύπωμα, καθώς αντικατοπτρίζει τη δική μας κοινή διαδρομή. Η παρούσα εργασία του αφιερώνεται ως ένδειξη βαθιάς εκτίμησης και ευγνωμοσύνης για όσα μου έχει προσφέρει και συνεχίζει να μου προσφέρει.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ	8
ABSTRACT	9
ΕΙΣΑΓΩΓΗ	10
1. ΚΕΦΑΛΑΙΟ: ΕΝΝΟΙΟΛΟΓΙΚΟ ΚΑΙ ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ: ΠΑΡΑΓΩΓΙΚΗ ΤΝ, ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ ΚΑΙ ΤΡΟΜΟΚΡΑΤΙΑ	15
1.1. Παραγωγική Τεχνητή Νοημοσύνη (Generative AI)	16
1.1.1. Βασικές Αρχές Λειτουργίας και Διαφορές από την Παραδοσιακή ΤΝ	17
1.1.2. Κίνδυνοι Διπλής Χρήσης (Dual-Use)	18
1.2. Από τον Υβριδικό Πόλεμο στη Γνωσιακή Διακυβέρνηση	18
1.2.1. Κυβερνοπόλεμος και Υβριδικές Απειλές	19
1.2.2. Επιχειρήσεις Πληροφόρησης και Γνωσιακός Πόλεμος	19
1.2.3. Διακυβέρνηση Πλατφορμών και Θεωρία Ευθύνης	20
2. ΚΕΦΑΛΑΙΟ: ΤΡΟΜΟΚΡΑΤΙΚΕΣ ΟΡΓΑΝΩΣΕΙΣ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΚΡΑΤΙΚΗ ΣΥΝΔΕΣΗ	21
2.1. Η έννοια των non-state actors στη θεωρία και την πρακτική του διεθνούς δικαίου	22
2.2. Γιατί οι τρομοκρατικές οργανώσεις δεν βρίσκονται εκτός της διεθνούς έννομης τάξης	23
2.3. Κρατική υποστήριξη, ανοχή και έλεγχος τρομοκρατικών οργανώσεων	26
3. ΚΕΦΑΛΑΙΟ: ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΧΡΗΣΗ ΠΑΡΑΓΩΓΙΚΗΣ ΤΝ ΑΠΟ ΤΡΟΜΟΚΡΑΤΙΚΕΣ ΟΡΓΑΝΩΣΕΙΣ	28
3.1. Η GenAI ως Πολλαπλασιαστής Ισχύος: Από την Ψηφιακή Προπαγάνδα στον Γνωσιακό Πόλεμο	29
3.2. Κυβερνοτρομοκρατία: Από την Ψηφιακή Διατάραξη στην «AI-Υποβοηθούμενη Απειλή»	29
3.3. Η GenAI στην Υπηρεσία της Ριζοσπαστικοποίησης (Propaganda)	32
3.4. Γνωσιακός Πόλεμος (Cognitive Warfare) και Deepfakes	34
3.5. Κυβερνο-επιχειρήσεις και Αυτοματοποίηση	36
3.6. Μελέτες Περίπτωσης (Case Studies)	38
3.6.1. ISIS (Ισλαμικό Κράτος): Η Ανάδυση του «Ψηφιακού Χαλιφάτου»	39
3.6.2. Hezbollah (Χεζμπολάχ): Το Πρότυπο του «Υβριδικού Δρώντα» (Hybrid Actor)	40
4. ΚΕΦΑΛΑΙΟ: ΑΠΟΔΟΣΗ ΕΥΘΥΝΗΣ ΣΤΟ ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ: ΤΟ TALLINN MANUAL ΚΑΙ Η ΤΝ	41
4.1. Κρατική ευθύνη στο διεθνές δίκαιο - Θεμελιώδεις Αρχές και Τεχνολογική Ουδετερότητα	41
4.2. Tallinn Manual 1.0 & 2.0	43

4.2.2.	<i>Η Μετάβαση από το Tallinn 1.0 στο Tallinn 2.0: Η Διεύρυνση της Κρατικής Ευθύνης</i>	45
4.2.3.	<i>Η Υποχρέωση Δέουσας Επιμέλειας (Due Diligence): Το «Ανάχωμα» στην Ατιμωρησία</i>	46
4.3.	<i>AI-enabled πράξεις και attribution: Η πρόκληση της «Αλγοριθμικής Αυτονομίας»</i>	47
4.4.	<i>Αυτόνομα συστήματα & ευθύνη</i>	49
5.	ΚΕΦΑΛΑΙΟ: ΥΠΟΧΡΕΩΣΗ ΔΕΟΥΣΑΣ ΕΠΙΜΕΛΕΙΑΣ ΚΑΙ ΣΥΓΧΡΟΝΗ ΡΥΘΜΙΣΤΙΚΗ ΑΝΤΙΔΡΑΣΗ	51
5.1.	<i>Η Θεωρητική Θεμελίωση της Δέουσας Επιμέλειας</i>	52
5.2.	<i>Εφαρμογή στον Κυβερνοχώρο (Cyber Due Diligence)</i>	54
5.3.	<i>Ο Ρόλος του Ιδιωτικού Τομέα και η Κρατική Ρύθμιση</i>	56
5.4.	<i>Η Πράξη για την Τεχνητή Νοημοσύνη της ΕΕ (EU AI Act)</i>	58
	ΣΥΜΠΕΡΑΣΜΑΤΑ	60
	ΚΕΙΜΕΝΑ ΤΕΚΜΗΡΙΩΣΗΣ	64

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία διερευνά τις πολυδιάστατες επιπτώσεις της ενσωμάτωσης της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI) στο επιχειρησιακό δόγμα της σύγχρονης τρομοκρατίας. Κεντρικό ερευνητικό ερώτημα αποτελεί το κατά πόσον η χρήση προηγμένων αλγοριθμικών συστημάτων από μη κρατικούς δρώντες συνιστά μια απλή ποσοτική αναβάθμιση των δυνατοτήτων τους ή μια θεμελιώδη ποιοτική τομή που μεταβάλλει οντολογικά τη φύση της ασύμμετρης απειλής. Μέσα από την εξέταση μελετών περίπτωσης (ISIS, Χαμάς, Χεζμπολάχ), η ανάλυση τεκμηριώνει ότι η GenAI λειτουργεί ως στρατηγικός «πολλαπλασιαστής ισχύος» (force multiplier), επιτρέποντας τη διεξαγωγή επιχειρήσεων Γνωσιακού Πολέμου (Cognitive Warfare) μέσω της μαζικής παραγωγής deepfakes, αυτοματοποιημένης προπαγάνδας και ψυχολογικής χειραγώγησης. Παρά τον ψηφιακό χαρακτήρα της απειλής, η μελέτη αποδομεί τον μύθο της «αποεδαφικοποίησης», αποδεικνύοντας ότι η ψηφιακή τρομοκρατία παραμένει γεωπολιτικά εξαρτημένη από φυσικές υποδομές που φιλοξενούνται εντός «Αποτυχημένων Κρατών» (Failed States) ή «Γκρίζων Ζωνών». Στο νομικό σκέλος, η διατριβή εξετάζει την επάρκεια του Διεθνούς Δικαίου να διαχειριστεί την πρόκληση της αλγοριθμικής αυτονομίας («πρόβλημα του μαύρου κουτιού»). Διαπιστώνεται ότι τα παραδοσιακά κριτήρια ελέγχου δυσχεραίνουν την άμεση απόδοση ευθύνης (attribution). Ως απάντηση, προτείνεται η τελεολογική ερμηνεία του Άρθρου 8 του Παραρτήματος της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ, όπου η εντολή εισαγωγής δεδομένων (Prompt) εξισώνεται νομικά με την «Οδηγία» (Instruction), γεφυρώνοντας το χάσμα μεταξύ ανθρώπινης πρόθεσης και μηχανικού αποτελέσματος. Δεδομένων των δυσκολιών στον εντοπισμό του δράστη, η εργασία υποστηρίζει τη στροφή από την κατασταλτική στην προληπτική ευθύνη μέσω του δόγματος της Δέουσας Επιμέλειας (Due Diligence). Βασισόμενη στη νομολογία της υπόθεσης Corfu Channel και σε σύγχρονα ρυθμιστικά πρότυπα όπως το EU AI Act, συμπεραίνει ότι τα κράτη φέρουν θετική υποχρέωση θωράκισης των ψηφιακών τους υποδομών. Η παράλειψη άσκησης αποτελεσματικής εποπτείας δύναται να θεμελιώσει διεθνή ευθύνη, κλείνοντας έτσι το παράθυρο ατιμωρησίας που εκμεταλλεύονται οι τρομοκρατικές οργανώσεις.

ABSTRACT

This thesis investigates the multidimensional implications of integrating Generative Artificial Intelligence (Generative AI) into the operational doctrine of modern terrorism. The central research question posits whether the use of advanced algorithmic systems by non-state actors constitutes a mere quantitative upgrade of their capabilities or a fundamental qualitative shift that ontologically alters the nature of the asymmetric threat. Through the examination of case studies (ISIS, Hamas, Hezbollah), the analysis substantiates that GenAI functions as a strategic "force multiplier," enabling the conduct of Cognitive Warfare operations through the mass production of deepfakes, automated propaganda, and psychological manipulation. Despite the digital nature of the threat, the study deconstructs the myth of "de-territorialization," demonstrating that digital terrorism remains geopolitically dependent on physical infrastructures hosted within "Failed States" or "Gray Zones." In the legal domain, the thesis examines the adequacy of International Law in addressing the challenge of algorithmic autonomy (the "black box problem"). It is found that traditional control criteria hinder direct attribution. In response, a teleological interpretation of Article 8 of the Annex to UN General Assembly Resolution 56/83 is proposed, wherein the data input command (Prompt) is legally equated with an "Instruction," thereby bridging the gap between human intent and machine output. Given the difficulties in identifying the perpetrator, the thesis advocates a shift from repressive to preventive responsibility via the doctrine of Due Diligence. Drawing on the Corfu Channel case jurisprudence and contemporary regulatory standards such as the EU AI Act, it concludes that states bear a positive obligation to shield their digital infrastructures. Failure to exercise effective oversight can establish international responsibility, thus closing the window of impunity exploited by terrorist organizations.

ΕΙΣΑΓΩΓΗ

Η παρούσα διπλωματική εργασία εξετάζει τη χρήση της Παραγωγικής Τεχνητής Νοημοσύνης (Generative Artificial Intelligence – GenAI) από τρομοκρατικές οργανώσεις και τις προκλήσεις που η εξέλιξη αυτή εγείρει για την εφαρμογή του σύγχρονου διεθνούς δικαίου. Η τρομοκρατία συνιστά διαχρονικά αντικείμενο έντονης νομικής ανησυχίας, καθώς προσβάλλει θεμελιώδεις αξίες της διεθνούς έννομης τάξης, όπως η προστασία της ανθρώπινης ζωής, η διεθνής ειρήνη και ασφάλεια και το κράτος δικαίου.¹ Παράλληλα, η τεχνολογική πρόοδος μεταβάλλει ουσιαστικά τις μορφές και τα μέσα τέλεσης τρομοκρατικών πράξεων, χωρίς ωστόσο να αναιρεί αυτομάτως τη δυνατότητα εφαρμογής των υφιστάμενων νομικών κανόνων.

Η επιτάχυνση της τεχνολογικής εξέλιξης και η ενσωμάτωση ψηφιακών δυνατοτήτων σε κρίσιμες λειτουργίες της δημόσιας και ιδιωτικής σφαίρας μεταβάλλουν σταδιακά το περιβάλλον διεθνούς ασφάλειας και, συνακόλουθα, τις νομικές κατηγορίες με τις οποίες το διεθνές δίκαιο επιχειρεί να συλλάβει, να αποδώσει και να περιορίσει επιβλαβείς συμπεριφορές.² Η μεταβολή αυτή είναι ιδίως εμφανής στον τρόπο με τον οποίο μη κρατικοί δρώντες αποκτούν πρόσβαση σε τεχνολογίες υψηλής αποτελεσματικότητας, οι οποίες άλλοτε προϋπέθεταν κρατικούς πόρους, εξειδικευμένες υπηρεσίες και σημαντικές υποδομές.³ Η τρομοκρατία, ως κατεξοχήν μορφή ασύμμετρης απειλής, προσαρμόζεται διαρκώς σε αυτό το τεχνολογικό περιβάλλον, αξιοποιώντας τόσο το πληροφοριακό οικοσύστημα όσο και τις νέες δυνατότητες αυτοματοποίησης για στρατολόγηση, προπαγάνδα, επιχειρησιακή υποστήριξη και στοχευμένη διασπορά φόβου.⁴ Η ευρωπαϊκή αξιολόγηση της απειλής επιβεβαιώνει ότι οι τρομοκρατικές πρακτικές εξελίσσονται παράλληλα με τα διαθέσιμα τεχνολογικά μέσα, γεγονός που απαιτεί από τους θεσμούς και τα κράτη μέλη να προσαρμόζουν τα εργαλεία πρόληψης και απόκρισης, χωρίς να θίγεται ο πυρήνας του κράτους δικαίου.⁴ Στο διεθνές δίκαιο δεν υφίσταται ενιαίος, καθολικά δεσμευτικός ορισμός της τρομοκρατίας. Αντ' αυτού, η ρύθμιση επιτυγχάνεται κυρίως μέσω τομεακών συμβάσεων και—σε επίπεδο

¹ United Nations Security Council, Resolution 1373 (2001), §1-3. <https://documents.un.org/doc/undoc/gen/n01/557/43/pdf/n0155743.pdf>

² North Atlantic Treaty Organization. (2022). NATO 2022 Strategic Concept. Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022, p. 3. <https://www.nato.int/nato-static-fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf>

³ European Commission. (2020). Joint Communication to the European Parliament and the Council: EU Security Union Strategy, p. 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>

⁴ Europol. (2024). European Union Terrorism Situation and Trend Report (TE-SAT 2024). Publications Office of the European Union. (relevant sections on evolving threat landscape/technology). https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2024.pdf

δεσμευτικότητας και πολιτικής βαρύτητας—μέσω της πρακτικής του Συμβουλίου Ασφαλείας, το οποίο αντιμετωπίζει την τρομοκρατία ως απειλή για τη διεθνή ειρήνη και ασφάλεια και καλεί τα κράτη σε εκτεταμένη συνεργασία και πρόληψη.⁵ Μέσα σε αυτό το πλαίσιο, η ουσία της προβληματικής της παρούσας εργασίας δεν είναι η «αντιμετώπιση της τρομοκρατίας» ως πολιτική επιλογή, αλλά η νομική αποτίμηση της μετάβασης σε ένα τεχνολογικά ενισχυμένο επιχειρησιακό πρότυπο μη κρατικής βίας και, ιδίως, οι συνέπειες του για την απόδοση ευθύνης και τη λογοδοσία.⁶

Κομβικό παράγοντα στη νέα φάση της τεχνολογικής ενσωμάτωσης συνιστά η Παραγωγική Τεχνητή Νοημοσύνη (Generative AI), δηλαδή συστήματα που παράγουν αυτοτελώς νέο περιεχόμενο και λειτουργικές εξόδους (π.χ. κείμενο, εικόνα, ανάλυση, κώδικα) βάσει εκπαίδευσης σε μεγάλα σύνολα δεδομένων και στατιστικής πρόβλεψης.⁶ Η σχετική θεσμική και επιχειρησιακή βιβλιογραφία ήδη επισημαίνει ότι τα μεγάλα γλωσσικά μοντέλα και συναφείς εφαρμογές μπορούν να μεταβάλουν το πεδίο δράσης εγκληματικών και εξτρεμιστικών δρώντων, μειώνοντας το κόστος, τον χρόνο και το απαιτούμενο επίπεδο τεχνογνωσίας για σύνθετες κακόβουλες ενέργειες.⁷

Η παραγωγική ΤΝ έχει εγείρει ζητήματα θεσμικά ως την αντιμετώπιση της σαν ένα είδος τεχνολογίας «διπλής χρήσης», οι ίδιες δυνατότητες που υποστηρίζουν θεμιτούς σκοπούς (καινοτομία, αποτελεσματικότητα, πρόσβαση στη γνώση) μπορούν, υπό διαφορετική πρόθεση, να υποστηρίζουν κακόβουλες χρήσεις (παραπληροφόρηση, εξαπάτηση, αυτοματοποίηση κυβερνοεπιθέσεων, στοχευμένη προπαγάνδα).⁸ Η θεσμική αντίδραση της Ευρωπαϊκής Ένωσης κινείται προς μια ρυθμιστική προσέγγιση που επιδιώκει να διαχειριστεί κινδύνους και να δημιουργήσει υποχρεώσεις διαφάνειας, εποπτείας και λογοδοσίας για συστήματα τεχνητής νοημοσύνης, ιδίως όταν αυτά μπορούν να επηρεάσουν θεμελιώδη δικαιώματα ή κρίσιμα κοινωνικά αγαθά.⁹

⁵ United Nations Security Council. (2004). Resolution 1566 (2004) [S/RES/1566(2004)]. § 1-3. [https://docs.un.org/en/S/RES/1566\(2004\)](https://docs.un.org/en/S/RES/1566(2004))

⁶ European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

⁷ Europol. (2023). ChatGPT: The impact of Large Language Models on Law Enforcement, pp. 3-6 <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>

⁸ European Parliamentary Research Service. (2024). Artificial intelligence act: Overview and policy context (EPRS briefing, PE 698.792), p. 11. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf

⁹ Regulation (EU) 2024/1689 (Artificial Intelligence Act), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Σε αυτό ακριβώς το σημείο αναδεικνύεται η κεντρική νομική πρόκληση: το διεθνές δίκαιο παραμένει θεμελιωδώς κρατοκεντρικό, και η θεμελίωση διεθνούς ευθύνης προϋποθέτει, κατά κανόνα, απόδοση της επίμαχης πράξης σε κράτος ή σύνδεση με κρατική συμπεριφορά.¹⁰ Οι κανόνες περί διεθνούς ευθύνης, όπως κωδικοποιούνται στα Σχέδια Άρθρων της Επιτροπής Διεθνούς Δικαίου, δεν εξαρτώνται από το τεχνολογικό μέσο, αλλά από την ύπαρξη πράξης/παράλειψης που αποδίδεται στο κράτος και παραβιάζει διεθνή υποχρέωση.¹¹ Ειδικότερα, σε περιπτώσεις δράσης μη κρατικών δρώντων, το διεθνές δίκαιο εξετάζει κριτήρια όπως ο έλεγχος, η καθοδήγηση ή η υιοθέτηση της συμπεριφοράς, προκειμένου να κριθεί αν και πώς η πράξη μπορεί να αποδοθεί στο κράτος.¹²

Η χρήση Παραγωγικής ΤΝ από τρομοκρατικές οργανώσεις οξύνει τα ζητήματα απόδοσης πράξεων (attribution) με δύο τρόπους. Πρώτον, η αυτοματοποίηση και η αδιαφάνεια δυσχεραίνουν τον εντοπισμό της αλυσίδας ελέγχου (ποιος σχεδίασε, ποιος παρείχε δεδομένα/υποδομή, ποιος ενεργοποίησε/καθοδήγησε, ποιος ωφελήθηκε).¹³ Δεύτερον, Η τεχνική διαμεσολάβηση της παραγωγικής ΤΝ δυσχεραίνει ουσιωδώς την αποδεικτική ανασύνθεση των κρίσιμων στοιχείων που απαιτούνται για την τεκμηρίωση πρόθεσης/γνώσης και την αποτίμηση ουσιαστικής ανθρώπινης εμπλοκής, μεταθέτοντας έτσι το επίδικο από καθαρά νομικό σε σύγχετο τεχνικό και αποδεικτικό πρόβλημα.¹⁴ Παρά ταύτα, η ύπαρξη αποδεικτικών δυσχερειών δεν συνεπάγεται νομικό κενό: τα υφιστάμενα κριτήρια ευθύνης δεν ακυρώνονται από την τεχνολογία, αλλά απαιτούν προσαρμοσμένες μεθόδους τεκμηρίωσης και αξιολόγησης.¹⁵

Παράλληλα, η συζήτηση μετατοπίζεται αναπόφευκτα και προς την υποχρέωση δέουσας επιμέλειας (due diligence), δηλαδή την υποχρέωση των κρατών να λαμβάνουν εύλογα μέτρα πρόληψης ώστε να μην χρησιμοποιείται το έδαφος, οι υποδομές ή οι δυνατότητές τους κατά

¹⁰ UN General Assembly, Responsibility of States for internationally wrongful acts, 12 December 2001, A/RES/56/83, Annex, Art. 2, pp. 32–36. <https://docs.un.org/en/A/RES/56/83>

¹¹ Ibid, Art. 2 § 3–5, p. 34–36.

¹² Ibid, Art. 8 & 11 and commentaries, p. 47–50, 52–54.

¹³ United Nations Interregional Crime and Justice Research Institute & United Nations Counter-Terrorism Centre. (2021). Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes. UNICRI & UNCCT. https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf

¹⁴ Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. Harvard Journal of Law & Technology, p. 913–915. <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf>

¹⁵ Quezada Tavárez, K. (2021). Legal Challenges in Bringing AI Evidence to the Criminal Trial: Admissibility, Reliability, and Fair Trial Rights. <https://lirias.kuleuven.be/retrieve/638528>

τρόπο που προκαλεί βλάβη σε άλλα κράτη ή στη διεθνή κοινότητα.¹⁶ Η «due diligence» αποκτά ιδιαίτερη σημασία σε περιβάλλοντα όπου κρίσιμες τεχνολογικές ικανότητες αναπτύσσονται ή φιλοξενούνται από ιδιωτικούς φορείς εντός κρατικής δικαιοδοσίας και μπορούν να αξιοποιηθούν από μη κρατικούς δρώντες για διεθνώς επιβλαβείς σκοπούς.¹⁷ Επιπλέον, στο ευρωπαϊκό πλαίσιο, η εξέλιξη προς υποχρεώσεις διακυβέρνησης κινδύνου και λογοδοσίας για συστήματα ΤΝ λειτουργεί συμπληρωματικά ως «εσωτερική» κανονιστική υποστήριξη της λογικής της επιμέλειας και της πρόληψης.¹⁸

Υπό το πρίσμα των ανωτέρω, το ερευνητικό ερώτημα της παρούσας διπλωματικής διατυπώνεται ρητά ως εξής:

« Σε ποιον βαθμό η ενσωμάτωση της «Παραγωγικής» Τεχνητής Νοημοσύνης (Generative AI) στο επιχειρησιακό δόγμα τρομοκρατικών ομάδων σε παγκόσμια κλίμακα μετασχηματίζει ποιοτικά τη φύση της ασύμμετρης απειλής που αυτές στρέφουν κατά του κράτους ως θεσμικού φορέα εξουσίας και, συνακόλουθα, κατά της κοινωνίας, και με ποιον τρόπο ρυθμίζεται, στο πλαίσιο του ισχύοντος διεθνούς δικαίου, το ζήτημα της απόδοσης διεθνούς ευθύνης και της υποχρέωσης επιμέλειας;»²⁰

Για την πληρέστερη και συστηματική διερεύνηση του κεντρικού ερωτήματος, τίθενται τα εξής επιμέρους υπο-ερωτήματα που καθοδηγούν τη δομή της έρευνας:

- I.** Πώς η προσβασιμότητα και το χαμηλό κόστος της ΤΝ μετασχηματίζουν τα «αποτυχημένα κράτη» (failed states) και τις γκρίζες ζώνες της Μέσης Ανατολής σε παγκόσμιους κόμβους υβριδικού πολέμου;
- II.** Με ποιον τρόπο η αυτοματοποίηση της προπαγάνδας μέσω συνθετικών μέσων (deepfakes) και bots μεταβάλλει τη στρατηγική των οργανώσεων από τον ιδεολογικό προσηλυτισμό στη μαζική γνωσιακή χειραγώγηση και τον ψυχολογικό πόλεμο;
- III.** Μπορεί η νομική μετάβαση από το δόγμα της εκ των υστέρων «ασυλίας» στο δόγμα της προληπτικής «ευθύνης επιμέλειας» (duty of care), όπως επιχειρείται με τον νέο Κανονισμό για την ΤΝ (AI Act) της ΕΕ, να αποτελέσει τη λύση στο πρόβλημα της λογοδοσίας;

¹⁶ International Court of Justice. (1949). Corfu Channel (United Kingdom v. Albania), Judgment, p. 22. <https://icj-web.lemman.un-icc.cloud/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf>

¹⁷ A/RES/56/83, ubi Supra, n. 10, Art. 3, § 6–10.

¹⁸ European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Art. 9–11, 14, Recitals 47, 61, 80. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Η πολυπλοκότητα του υπό εξέταση φαινομένου επιβάλλει την υιοθέτηση μιας διεπιστημονικής μεθοδολογικής προσέγγισης, η οποία συνδυάζει τη νομική δογματική έρευνα (legal dogmatics).

Η μεθοδολογία της έρευνας θα βασιστεί στην εις βάθος ανάλυση του ισχύοντος θεσμικού πλαισίου (lex lata). Συγκεκριμένα θα εξεταστούν ο Χάρτης των Ηνωμένων Εθνών και τα Άρθρα της Επιτροπής Διεθνούς Δικαίου (ILC) περί Ευθύνης των Κρατών, για τη διερεύνηση των ορίων της απόδοσης ευθύνης στον κυβερνοχώρο, τα Ψηφίσματα του Συμβουλίου Ασφαλείας του ΟΗΕ, και ειδικότερα το Ψήφισμα 2396 (2017) που αφορά τη χρήση τεχνολογίας και βιομετρικών δεδομένων στον αντιτρομοκρατικό αγώνα, καθώς και το Ψήφισμα 2178 (2014) για τους Ξένους Τρομοκράτες Μαχητές, ως νομική βάση για τη διεθνή συνεργασία, η Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα του Συμβουλίου της Ευρώπης, ως το βασικό διεθνές κείμενο ποινικού δικαίου για τον κυβερνοχώρο, το Εγχειρίδιο του Ταλίν 1.0 (2013) για το Διεθνές Δίκαιο που είναι Εφαρμοστέο στον Κυβερνοπόλεμο (Tallinn Manual on the International Law Applicable to Cyber Warfare) & Ταλίν 2.0 (2017) για το Διεθνές Δίκαιο που είναι Εφαρμοστέο στις Κυβερνοεπιχειρήσεις (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations), τέλος ο νέος Κανονισμός (ΕΕ) 2024/1689 για την Τεχνητή Νοημοσύνη (AI Act), ο οποίος αποτελεί την πρώτη παγκοσμίως νομοθετική προσπάθεια ρύθμισης της τεχνολογίας βάσει κινδύνου (risk-based approach) και εισάγει υποχρεώσεις για τα μοντέλα γενικού σκοπού (GPAI) που δύνανται να χρησιμοποιηθούν για τρομοκρατικούς σκοπούς.

Η Ποιοτική Ανάλυση και Μελέτες Περίπτωσης (Case Studies). Η θεωρητική και νομική ανάλυση θα τεκμηριωθεί εμπειρικά μέσω της συγκριτικής εξέτασης τριών διακριτών μοντέλων τρομοκρατικής δράσης, προκειμένου να αναδειχθεί το εύρος και η ποικιλομορφία της απειλής:

1. ISIS: Εξετάζεται η χρήση αυτοματοποιημένων συστημάτων (bots) και η παραγωγή συνθετικού περιεχομένου για την αναβίωση του «Ψηφιακού Χαλιφάτου» και τη διατήρηση της ανθεκτικότητας του δικτύου απέναντι στις διαγραφές περιεχομένου.
2. Χαμάς: Αναλύεται η στρατηγική χρήση deepfakes και οπτικοακουστικής παραποίησης κατά τον πόλεμο της 7ης Οκτωβρίου, ως εργαλείο ψυχολογικού πολέμου και πρόκλησης σύγχυσης (fog of war).
3. Χεζμπολάχ: Μελετάται ως παράδειγμα κρατικά υποστηριζόμενης (state-sponsored) κυβερνο-τρομοκρατίας, με έμφαση στη χρήση προηγμένων ψηφιακών μέσων για επιθέσεις σε κρίσιμες υποδομές.

Η εργασία διαρθρώνεται σε πέντε κεφάλαια και τα συμπεράσματα, ακολουθώντας μια λογική πορεία από το θεωρητικό και εννοιολογικό πλαίσιο, στην εμπειρική ανάλυση και τέλος στη νομική αξιολόγηση και τις προτάσεις.

Κεφάλαιο 1: θέτει το απαραίτητο εννοιολογικό υπόβαθρο, ορίζοντας την Παραγωγική ΤΝ και τα χαρακτηριστικά διπλής χρήσης (dual-use) που την καθιστούν απειλή, ενώ εντάσσει το φαινόμενο στο ευρύτερο θεωρητικό πλαίσιο του Υβριδικού Πολέμου.

Κεφάλαιο 2: αναλύει το γεωπολιτικό περιβάλλον, εστιάζοντας στο πώς τα «αποτυχημένα κράτη» της Μέσης Ανατολής λειτουργούν ως εργαστήρια υβριδικών απειλών και πώς η θεωρία του «Ψηφιακού Τζιχάντ» κωδικοποιείται σε αλγορίθμους.

Κεφάλαιο 3: εξετάζει συνδυαστικά την επιχειρησιακή εφαρμογή της ΤΝ. Αναλύει τις μεθόδους αυτοματοποιημένης προπαγάνδας, γνωσιακού πολέμου και κυβερνοεπιθέσεων, συνδέοντας κάθε θεωρητική κατηγορία με την αντίστοιχη μελέτη περίπτωσης (ISIS, Hamas, Hezbollah) για την ανάδειξη της πρακτικής διάστασης.

Κεφάλαιο 4: αποτελεί τον πυρήνα της νομικής ανάλυσης. Διερευνά την εφαρμογή του υφιστάμενου Διεθνούς Δίκαιου, αναλύει το πρόβλημα της απόδοσης ευθυνών σε αυτόνομα συστήματα και τεκμηριώνει την ανάγκη μετάβασης στο δόγμα της «ευθύνης επιμέλειας» (duty of care).

Κεφάλαιο 5: αξιολογεί τις θεσμικές αντιδράσεις και τις στρατηγικές ανάχησης που έχουν υιοθετήσει το ΝΑΤΟ, η ΕΕ και οι ΗΠΑ, κρίνοντας την αποτελεσματικότητά τους απέναντι στη νέα απειλή.

Συμπεράσματα: συνοψίζει τα ευρήματα της έρευνας, επιβεβαιώνει την υπόθεση εργασίας και καταθέτει συγκεκριμένες προτάσεις (de lege ferenda) για τη δημιουργία ενός διεθνούς πλαισίου ρύθμισης που θα εξισορροπεί την ανάγκη για ασφάλεια με την προστασία των θεμελιωδών δικαιωμάτων στον ψηφιακό χώρο.

1. ΚΕΦΑΛΑΙΟ: ΕΝΝΟΙΟΛΟΓΙΚΟ ΚΑΙ ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ: ΠΑΡΑΓΩΓΙΚΗ ΤΝ, ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ ΚΑΙ ΤΡΟΜΟΚΡΑΤΙΑ

Το παρόν κεφάλαιο θέτει το αναγκαίο εννοιολογικό και θεωρητικό υπόβαθρο για την ανάλυση που ακολουθεί, προκειμένου να καταστεί δυνατή η νομική αξιολόγηση της χρήσης συστημάτων Παραγωγικής Τεχνητής Νοημοσύνης από τρομοκρατικές οργανώσεις.¹⁹ Η

¹⁹ Pauwels, E. (2022). Safeguarding against the misuse and abuse of artificial intelligence, Global Center on Cooperative Security, p. 1–2. https://www.globalcenter.org/wp-content/uploads/GCCS_PB_Safeguarding_Against_Misuse_Artificial_Intelligence_web.pdf

σταδιακή ενσωμάτωση προηγμένων ψηφιακών τεχνολογιών στο επιχειρησιακό οπλοστάσιο τρομοκρατικών και άλλων βίαιων μη κρατικών δρώντων έχει αναγνωριστεί ως εξέλιξη που αυξάνει την πολυπλοκότητα της ασύμμετρης απειλής και επιτείνει τις δυσχέρειες διακυβέρνησης κινδύνου και πρόληψης.²⁰ Υπό τις συνθήκες αυτές, η αποσαφήνιση βασικών εννοιών καθίσταται αναγκαία, καθώς οι όροι «τεχνητή νοημοσύνη», «Παραγωγική ΤΝ» και «διπλή χρήση» χρησιμοποιούνται συχνά χωρίς ενιαίο περιεχόμενο, γεγονός που επηρεάζει άμεσα τη νομική αποτίμηση κινδύνων και την κανονιστική συζήτηση.²¹

Παράλληλα, το κεφάλαιο εντάσσει το φαινόμενο αυτό στο ευρύτερο θεωρητικό πλαίσιο των υβριδικών απειλών/υβριδικού πολέμου, όπου η σύζευξη κρατικών και μη κρατικών δυνατοτήτων και η αξιοποίηση ψηφιακών μέσων επιτρέπουν την επίτευξη στρατηγικών αποτελεσμάτων κάτω από το κατώφλι της παραδοσιακής ένοπλης σύγκρουσης.²² Με τον τρόπο αυτό, διαμορφώνεται ένα συνεκτικό αναλυτικό πλαίσιο, το οποίο επιτρέπει στα επόμενα κεφάλαια να εξετάσουν συστηματικά τις προκλήσεις που ανακύπτουν για την εφαρμογή των κανόνων διεθνούς ευθύνης και της υποχρέωσης δέουσας επιμέλειας των κρατών.²³

1.1. Παραγωγική Τεχνητή Νοημοσύνη (Generative AI)

Η Παραγωγική Τεχνητή Νοημοσύνη (Generative AI ή GenAI) συνιστά μια εξελικτική κατηγορία συστημάτων τεχνητής νοημοσύνης, τα οποία δεν περιορίζονται στην ανάλυση υπαρχόντων δεδομένων, αλλά διαθέτουν την ικανότητα να συνθέτουν πρωτότυπο περιεχόμενο —όπως κείμενο, κώδικα, εικόνα και ήχο— που προσομοιάζει την ανθρώπινη δημιουργία.²⁴ Σε αντίθεση με τα συμβατικά μοντέλα μηχανικής μάθησης, η GenAI βασίζεται σε προηγμένες αρχιτεκτονικές νευρωνικών δικτύων, όπως τα Μεγάλα Γλωσσικά Μοντέλα (Large Language Models - LLMs), τα οποία εκπαιδεύονται σε τεράστια σύνολα δεδομένων ώστε να

²⁰ Pauwels, E. (2022). Ibid, p. 2.

²¹ Boucher, P. (2020). «Artificial intelligence: How does it work, why does it matter, and what can we do about it», European Parliamentary Research Service (EPRS), p. 4 & 10. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU%282020%29641547_EN.pdf

²² Uziębło, J. J. (2017). «United in ambiguity? EU and NATO approaches to hybrid threats», (pp. 3–4: introducing “hybrid”; College of Europe, EU Diplomacy Paper 5/2017, p. 6–8. https://www.coleurope.eu/sites/default/files/research-paper/edp-5-2017_uzieblo_0.pdf

²³ A/RES/56/83, ubi supra, n. 10, Art. 1 & 2.

²⁴ Rai, A., Constantinides, P., & Sarker, S. (2025). Inventing with machines: Generative AI and the evolving landscape of IS research. Information Systems Research, 36(4). <https://pubsonline.informs.org/doi/10.1287/isre.2025.editorial.v36.n4>

αναγνωρίζουν μοτίβα και να παράγουν νέες δομές πληροφορίας με συνοχή και λογική αλληλουχία.²⁵

1.1.1. Βασικές Αρχές Λειτουργίας και Διαφορές από την Παραδοσιακή ΤΝ

Η θεμελιώδης διάκριση μεταξύ της Παραγωγικής και της Παραδοσιακής (ή Διακριτικής) ΤΝ έγκειται στον τελικό τους στόχο. Σύμφωνα με τη βιβλιογραφία, η Παραδοσιακή ΤΝ (Traditional AI) εστιάζει κυρίως στην αναγνώριση προτύπων και την ταξινόμηση δεδομένων (pattern recognition & classification) με σκοπό την πρόβλεψη ή τη λήψη αποφάσεων βάσει προκαθορισμένων κανόνων.²⁶ Αντιθέτως, η Παραγωγική ΤΝ λειτουργεί μέσω της σύνθεσης νέων δεδομένων (data synthesis). Δεν απαντά απλώς σε ερωτήματα επιλέγοντας από μια βάση γνώσεων, αλλά «κατασκευάζει» την απάντηση λέξη προς λέξη ή pixel προς pixel, μαθαίνοντας την υποκείμενη κατανομή των δεδομένων εκπαίδευσης. Αυτή η μετάβαση από την «ερμηνεία» στη «δημιουργία» καθιστά τα συστήματα αυτά ικανά να επιλύουν προβλήματα για τα οποία δεν έχουν προγραμματιστεί ρητά, προσφέροντας ωστόσο νέες προκλήσεις ασφαλείας.²⁷ Χαρακτηριστικά: Αυτονόμηση, Κλιμάκωση και Αναπαραγωγικότητα. Η ακαδημαϊκή κοινότητα εντοπίζει τρία κρίσιμα χαρακτηριστικά που καθιστούν την GenAI ιδιαίτερα σημαντική στο πλαίσιο της διεθνούς ασφάλειας:

- Αυτονόμηση (Autonomy): Τα σύγχρονα συστήματα GenAI εξελίσσονται σε "πράκτορες" (agents) με ικανότητα εκτέλεσης πολύπλοκων αλληλουχιών ενεργειών χωρίς συνεχή ανθρώπινη επίβλεψη, γεγονός που αυξάνει τον κίνδυνο ανεξέλεγκτων ενεργειών στον κυβερνοχώρο.²⁸
- Κλιμάκωση (Scalability): Η τεχνολογία επιτρέπει την εκθετική αύξηση του όγκου των επιχειρήσεων. Όπως επισημαίνουν ερευνητές του Alan Turing Institute, η GenAI επιτρέπει σε

²⁵ Al-Ma'aitah, M. (2025). Generative AI in academia: A comprehensive review of applications and implications for the research process. ResearchGate. https://www.researchgate.net/publication/387962069_Generative_AI_in_Academia_A_Comprehensive_Review_of_Applications_and_Implications_for_the_Research_Process

²⁶ MIT Industrial Liaison Program. (2024, October 22). Exploring the shift from traditional to generative AI. The Curve. <https://curve.mit.edu/exploring-shift-traditional-generative-ai>

²⁷ Ennazar, Y., & En-Naimi, E. M. (2024). Traditional AI vs generative AI: The role in modern cyber security. International Journal of Engineering Technology and Management Sciences. https://www.researchgate.net/publication/386248918_TRADITIONAL_AI_VS_GENERATIVE_AI_THE_ROLE_IN_MODERN_CYBER_SECURITY

²⁸ Cybernetic Global Intelligence. (2025, October 20). AI and generative AI: Dual-use risks and autonomous threats. <https://www.cyberneticgi.com/dual-use-risks-and-autonomous-threats/>

κακόβουλους δρώντες να παράγουν απειλές (π.χ. phishing emails, κακόβουλο κώδικα) με ταχύτητα και όγκο που δεν θα μπορούσε να επιτευχθεί χειροκίνητα.²⁹

- Αναπαραγωγικότητα (Replicability): Η δυνατότητα των μοντέλων να αναπαράγουν με ακρίβεια πολύπλοκα ψηφιακά σήματα (φωνή, βίντεο) υπονομεύει την εμπιστοσύνη στην ψηφιακή πραγματικότητα, καθιστώντας δυσδιάκριτα τα όρια μεταξύ αυθεντικού και παραποιημένου υλικού.³⁰

1.1.2. Κίνδυνοι Διπλής Χρήσης (Dual-Use)

Στη διεθνή βιβλιογραφία, η Παραγωγική ΤΝ χαρακτηρίζεται ως τεχνολογία «διπλής χρήσης» (dual-use technology), καθώς οι ίδιες δυνατότητες που προάγουν την επιστήμη και την καινοτομία μπορούν να εργαλειοποιηθούν για κακόβουλους σκοπούς.³¹ Ειδικότερα για τις τρομοκρατικές ομάδες, μελέτες του International Centre for Counter-Terrorism (ICCT) καταδεικνύουν ότι η GenAI μειώνει δραστικά το τεχνικό όριο εισόδου (barrier to entry). Αυτό επιτρέπει σε άτομα χωρίς εξειδικευμένες τεχνικές γνώσεις να αποκτήσουν επιχειρησιακές δυνατότητες κυβερνοπολέμου, όπως η ανάπτυξη κακόβουλου λογισμικού και η διεξαγωγή εκστρατειών παραπληροφόρησης, «εκδημοκρατίζοντας» ουσιαστικά την ικανότητα πρόκλησης βλάβης.³²

1.2. Από τον Υβριδικό Πόλεμο στη Γνωσιακή Διακυβέρνηση

Η ανάλυση της χρήσης της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI) από τρομοκρατικές ομάδες δεν μπορεί να περιοριστεί σε μια τεχνοκρατική περιγραφή εργαλείων. Αντιθέτως, απαιτεί την ένταξή της σε ένα ευρύτερο θεωρητικό πλαίσιο που συνθέτει τρεις αλληλένδετες έννοιες της σύγχρονης στρατηγικής και νομικής θεωρίας: τον υβριδικό πόλεμο, τις επιχειρήσεις στον πληροφοριακό χώρο και τη θεωρία ευθύνης των ψηφιακών πλατφορμών.

²⁹ Stockwell, S., et al. (2025). Evaluating malicious generative AI capabilities. Centre for Emerging Technology and Security (CETaS). <https://cetas.turing.ac.uk/publications/evaluating-malicious-generative-ai-capabilities>

³⁰ Gozalo-Brizuela, R., & Garrido-Merchan, E. C. (2023). Generative artificial intelligence reproducibility and consensus. arXiv. <https://arxiv.org/html/2307.01898v2>

³¹ Mouter, N., et al. (2024). Dual use concerns of generative AI and large language models. Journal of Responsible Innovation, 11(1). <https://www.tandfonline.com/doi/full/10.1080/23299460.2024.2304381>

³² Mehra, T. (2024, June 10). Exploitation of generative AI by terrorist groups. International Centre for Counter-Terrorism (ICCT). <https://icct.nl/publication/exploitation-generative-ai-terrorist-groups>

1.2.1. Κυβερνοπόλεμος και Υβριδικές Απειλές

Η παραδοσιακή διάκριση μεταξύ πολέμου και ειρήνης έχει πλέον αμβλυνθεί, δίνοντας τη θέση της στην έννοια των «υβριδικών απειλών» (hybrid threats). Σύμφωνα με την Ευρωπαϊκή Επιτροπή και το NATO, οι υβριδικές απειλές ορίζονται ως ο συντονισμένος και συγχρονισμένος συνδυασμός συμβατικών και μη συμβατικών μέσων — διπλωματικών, στρατιωτικών, οικονομικών και τεχνολογικών — που χρησιμοποιούνται από κρατικούς και μη κρατικούς δρώντες για την εκμετάλλευση των τρωτών σημείων του αντιπάλου, παραμένοντας συχνά κάτω από το κατώφλι του επίσημου πολέμου.³³

Σε αυτό το πλαίσιο, ο κυβερνοπόλεμος (cyberwarfare) δεν λειτουργεί ως αυτοσκοπός, αλλά ως ένα ευέλικτο εργαλείο εντός της ευρύτερης «εργαλειοθήκης» του υβριδικού πολέμου. Όπως επισημαίνει το «Ινστιτούτο Egmont», οι κυβερνοεπιθέσεις λειτουργούν ως πολλαπλασιαστές ισχύος, επιτρέποντας σε ασύμμετρους δρώντες, όπως οι τρομοκρατικές οργανώσεις, να προκαλούν δυσανάλογα μεγάλη ζημιά σε σχέση με τους πόρους τους.³⁴

Η θεωρητική καινοτομία έγκειται στην παραδοχή ότι οι τρομοκρατικές ομάδες υιοθετούν πλέον στρατηγικές που προσιδιάζουν σε κρατικές οντότητες. Η βιβλιογραφία αναφέρεται σε αυτό το φαινόμενο ως «πολυαιτιακή σύγκρουση» (multi-causal conflict), όπου οι δρώντες κινούνται ταυτόχρονα στο φυσικό και το ψηφιακό πεδίο. Ο κυβερνοχώρος προσφέρει το ιδανικό περιβάλλον για αυτή τη σύγκλιση, καθώς επιτρέπει την ανωνυμία και την άρνηση ευθύνης (plausible deniability), στοιχεία κρίσιμα για τη διεξαγωγή υβριδικών επιχειρήσεων.³⁵ Συνεπώς, η χρήση της TN από τρομοκράτες πρέπει να εξετάζεται υπό το πρίσμα της υβριδικότητας: δεν είναι απλώς ένα εργαλείο επικοινωνίας, αλλά ένα όπλο στρατηγικής αποσταθεροποίησης που στοχεύει στην παράλυση των διαδικασιών λήψης αποφάσεων του αντιπάλου

1.2.2. Επιχειρήσεις Πληροφόρησης και Γνωσιακός Πόλεμος

³³ European Commission. (n.d.). Hybrid threats. Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

³⁴ Siman, M. (2022). *Hybrid warfare is not synonymous with cyber: The threat of influence operations*. Egmont Institute. https://www.egmontinstitute.be/app/uploads/2022/02/spb155-siman-final-version_0222.pdf?type=pdf

³⁵ Mumford, A., & Reis, B. C. (2015). *The role of counter terrorism in hybrid warfare*. NATO Defense College. <https://www.tmmm.tsk.tr/publication/researches/04-TheRoleofCounterTerrorisminHybridWarfare.pdf>

Η μετεξέλιξη των Επιχειρήσεων Πληροφόρησης (Information Operations - InfoOps) σε αυτό που το NATO και η σύγχρονη στρατηγική αποκαλεί «Γνωσιακό Πόλεμο» (Cognitive Warfare). Ενώ οι παραδοσιακές επιχειρήσεις πληροφοριών στόχευαν στον έλεγχο της ροής της πληροφορίας, ο γνωσιακός πόλεμος στοχεύει στον έλεγχο του τρόπου με τον οποίο ο εγκέφαλος επεξεργάζεται την πληροφορία και αντιδρά σε αυτήν.³⁶ Ο στόχος, σύμφωνα με αναλύσεις του Innovation Hub του NATO, είναι η «οπλοποίηση της κοινής γνώμης».³⁷ Η Παραγωγική ΤΝ αποτελεί τον καταλύτη αυτής της εξέλιξης. Μέσω της δημιουργίας πειστικών deepfakes και συνθετικών αφηγημάτων, οι τρομοκρατικές οργανώσεις δεν επιδιώκουν απλώς την προπαγάνδα, αλλά τη «γνωσιακή κυριαρχία» (cognitive superiority). Θεωρητικά, αυτό περιγράφεται ως μια διαδικασία «αντιληπτικής πειρατείας» (perceptual hacking), όπου ο επιτιθέμενος εκμεταλλεύεται τις γνωσιακές προκαταλήψεις (cognitive biases) του κοινού για να σπείρει διχόνοια και δυσπιστία προς τους θεσμούς.³⁸ Πρέπει να επισημανθεί ότι η επιτυχία αυτών των επιχειρήσεων δεν εξαρτάται από την αλήθεια του μηνύματος, αλλά από την ικανότητά του να προκαλεί συναισθηματική αντίδραση και να πολώνει. Σε αυτό το πλαίσιο, η ΤΝ επιτρέπει την εξατομίκευση του ψυχολογικού πολέμου σε μαζική κλίμακα, καθιστώντας κάθε χρήστη του διαδικτύου εν δυνάμει στόχο και φορέα της επίθεσης.

1.2.3. Διακυβέρνηση Πλατφορμών και Θεωρία Ευθύνης

Η κανονιστική «ασάφεια» στη διακυβέρνηση των ψηφιακών πλατφορμών είναι ένα φλέγον ζήτημα είναι το δίλημμα της ευθύνης των ενδιαμέσων (intermediary liability). Παραδοσιακά, οι πλατφόρμες αντιμετωπίζονταν ως «ουδέτεροι αγωγοί» πληροφορίας, απολαμβάνοντας ασυλία για το περιεχόμενο τρίτων (όπως κατοχυρώνεται στο Άρθρο 230 στις ΗΠΑ ή στην Οδηγία για το Ηλεκτρονικό Εμπόριο στην ΕΕ).³⁹ Ωστόσο, η ακαδημαϊκή έρευνα

³⁶ Claverie, B., & du Cluzel, F. (2022). The cognitive warfare concept. NATO Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf

³⁷ Du Cluzel, F. (2020). Cognitive warfare. NATO Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

³⁸ Bernal, A., Cheng, C., Poblete, E., Panicia, T., McIntyre, N., & Calvin, A. (2020). Cognitive warfare: An attack on truth and thought. NATO Innovation Hub. <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf>

³⁹ Communications Decency Act of 1996, 47 U.S.C. § 230 (1996). <https://www.govinfo.gov/app/details/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec230> & Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Official Journal of the European Communities, L 178, 1-16. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>

αναδεικνύει την ανεπάρκεια αυτού του μοντέλου στην εποχή της αλγοριθμικής επιμέλειας (algorithmic curation).⁴⁰

Η σύγχρονη θεωρία ευθύνης υποστηρίζει ότι οι πλατφόρμες δεν είναι πλέον παθητικοί διαμεσολαβητές, αλλά ενεργοί διαμορφωτές του δημόσιου λόγου, καθώς οι αλγόριθμοί τους ιεραρχούν, προωθούν και ενίοτε «νομιμοποιούν» το εξτρεμιστικό περιεχόμενο χάριν της δέσμευσης των χρηστών (engagement).⁴¹ Η εμφάνιση της Παραγωγικής ΤΝ περιπλέκει περαιτέρω το ζήτημα: όταν ένα chatbot που φιλοξενείται σε μια πλατφόρμα «συνομιλεί» με έναν χρήστη και τον καθοδηγεί προς τη ριζοσπαστικοποίηση, ποιος φέρει την ευθύνη; Η πλατφόρμα, ο δημιουργός του μοντέλου ή ο χρήστης; Μελέτες του Πανεπιστημίου George Washington και νομικών επιθεωρήσεων προτείνουν τη μετάβαση από ένα μοντέλο «ασυλίας» σε ένα μοντέλο «ευθύνης επιμέλειας» (duty of care), όπου οι πλατφόρμες θα λογοδοτούν όχι μόνο για την αποτυχία αφαίρεσης περιεχομένου, αλλά και για τον σχεδιασμό των αλγορίθμων που διευκολύνουν την τρομοκρατική δράση.⁴² Η θεωρητική αυτή μετατόπιση είναι αναγκαία για την αντιμετώπιση του παραδόξου όπου οι τεχνολογικοί κολοσσοί καρπώνονται τα οφέλη της προσοχής των χρηστών, ενώ το κόστος της ριζοσπαστικοποίησης μετακυλίεται στην κοινωνία.

2. ΚΕΦΑΛΑΙΟ: ΤΡΟΜΟΚΡΑΤΙΚΕΣ ΟΡΓΑΝΩΣΕΙΣ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΚΡΑΤΙΚΉ ΣΥΝΔΕΣΗ

Η ανάλυση της χρήσης προηγμένων τεχνολογιών από τρομοκρατικές οργανώσεις δεν μπορεί να αποσυνδεθεί από τη θέση τους στο διεθνές δίκαιο ως μη κρατικών δρώντων και από τις σχέσεις τους με κράτη, στον βαθμό που τίθενται ζητήματα διεθνούς ευθύνης μέσω συμπεριφοράς (ενέργειας ή παράλειψης) αποδιδόμενης στο κράτος και παραβίασης διεθνούς υποχρέωσης.⁴³ Όπως έχει ξανά επισημανθεί παρά τον παραδοσιακά κρατοκεντρικό χαρακτήρα

⁴⁰ Gillespie, T. (2017). Governance of/by platforms. Microsoft Research. <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/Gillespie-Regulation-ofby-Platforms-PREPRINT.pdf>

⁴¹ Hoyer, J. (2024). Down the alt-right rabbit hole: The role of social media platforms in the radicalization of domestic right-wing terrorists. Southern California Interdisciplinary Law Journal, 33(1). <https://gould.usc.edu/why/students/orgs/ilj/assets/docs/33-1-hoyer.pdf>

⁴² Program on Extremism. (2023). Moderating extremism: The state of online terrorist content removal policy in the United States. The George Washington University. <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf>

⁴³ A/RES/56/83, ubi supra, n. 10, Art. 1 & 2.

του διεθνούς δικαίου, η διεθνής πρακτική και θεωρία έχουν αναγνωρίσει ότι οι πράξεις μη κρατικών δρώντων, συμπεριλαμβανομένων τρομοκρατικών οργανώσεων, εντάσσονται σε κανονιστικά πλαίσια που επιτρέπουν νομική αξιολόγηση και, υπό προϋποθέσεις, απόδοση ευθύνης.⁴⁴ Η προσέγγιση αυτή είναι κρίσιμη ιδίως σε περιβάλλοντα όπου η πρόσβαση σε τεχνολογικά προηγμένα μέσα προϋποθέτει κρατικές υποδομές, τεχνογνωσία ή εδαφικό έλεγχο.⁴⁵

Στο πλαίσιο αυτό, το παρόν κεφάλαιο επιδιώκει να αποδομήσει το αφήγημα της «αυτόνομης τρομοκρατίας», εξετάζοντας τις τρομοκρατικές οργανώσεις ως δρώντες που λειτουργούν εντός σύνθετων δικτύων κρατικών και μη κρατικών σχέσεων.⁴⁶ Η κατανόηση της νομικής θέσης μη κρατικών οντοτήτων και της ενδεχόμενης κρατικής εμπλοκής στη δράση τους αποτελεί αναγκαίο προαπαιτούμενο για την ανάλυση ζητημάτων απόδοσης διεθνούς ευθύνης σύμφωνα με το ισχύον διεθνές δίκαιο, επί των οποίων θα εδράζεται η περαιτέρω εξέταση της επιχειρησιακής χρήσης της Παραγωγικής Τεχνητής Νοημοσύνης.⁴⁷

2.1. Η έννοια των non-state actors στη θεωρία και την πρακτική του διεθνούς δικαίου

Οι τρομοκρατικές οργανώσεις αντιμετωπίζονται στη διεθνή πρακτική ως μη κρατικοί δρώντες, στο μέτρο που συνιστούν οργανωμένες συλλογικότητες εκτός κρατικής δομής, των οποίων η δράση δύναται να απειλήσει τη διεθνή ειρήνη και ασφάλεια και, ως εκ τούτου, να ενεργοποιήσει το κανονιστικό πεδίο του διεθνούς δικαίου.⁴⁸ Το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών έχει αναγνωρίσει ρητά ότι τρομοκρατικές πράξεις που τελούνται από μη κρατικούς δρώντες συνιστούν απειλή για τη διεθνή ειρήνη και ασφάλεια, επιβάλλοντας στα

⁴⁴ Clapham, A. (2006). Human rights obligations of non-state actors in conflict situations. *International Review of the Red Cross*, 88(863), p. 496. https://international-review.icrc.org/sites/default/files/irrc_863_3.pdf

⁴⁵ Council of Europe, Committee on Counter-Terrorism (CDCT). (2025). Report on the emerging patterns of misuse of technology by terrorist actors. Council of Europe, p. 6. <https://rm.coe.int/report-on-the-emerging-patterns-of-misuse-of-technology-by-terrorist-a/4880281a94>

⁴⁶ Cassese, A. (2006). The multifaceted criminal notion of terrorism in international law. *Journal of International Criminal Justice*, 4(5), p. 946–949. <https://academic.oup.com/jicj/article/4/5/933/835024?login=true>

⁴⁷ Stefan Talmon, The Responsibility of Outside Powers for Acts of Secessionist Entities, *International and Comparative Law Quarterly*, Vol. 58, No. 3 (2009), p. 493–496. [https://users.ox.ac.uk/~sann2029/ICLQ%2058%20\(2009\),%20493-517.pdf](https://users.ox.ac.uk/~sann2029/ICLQ%2058%20(2009),%20493-517.pdf)

⁴⁸ United Nations Security Council. (2001). Resolution 1373 (2001), S/RES/1373 (2001), § 3–5. <https://documents.un.org/doc/undoc/gen/n01/557/43/pdf/n0155743.pdf>

κράτη δεσμευτικές υποχρεώσεις πρόληψης, καταστολής και ποινικοποίησης της δράσης τρομοκρατικών οργανώσεων.⁴⁹

Στο πλαίσιο αυτό, οι τρομοκρατικές οργανώσεις δεν νοούνται ως υποκείμενα διεθνούς δικαίου με πλήρη νομική προσωπικότητα, αλλά ως αντικείμενα διεθνούς ρύθμισης, των οποίων η δράση ρυθμίζεται έμμεσα μέσω υποχρεώσεων που επιβάλλονται στα κράτη.⁵⁰

Η Γενική Συνέλευση του ΟΗΕ έχει, ήδη από το 1994, περιγράψει τις τρομοκρατικές πράξεις ως εγκληματικές ενέργειες που αποσκοπούν στη δημιουργία κατάστασης τρόμου στο κοινό για πολιτικούς σκοπούς, αποδίδοντάς τες σε οργανωμένες ομάδες εκτός κρατικών δομών.⁵¹ Παράλληλα, η διεθνής νομική θεωρία έχει επισημάνει ότι η ένταξη των τρομοκρατικών οργανώσεων στο ρυθμιστικό πεδίο του διεθνούς δικαίου δεν αποσκοπεί στη νομιμοποίησή τους, αλλά στη δυνατότητα νομικής αξιολόγησης της δράσης τους και, υπό προϋποθέσεις, στη θεμελίωση διεθνούς ευθύνης μέσω κρατικής εμπλοκής ή ανοχής.⁵² Η προσέγγιση αυτή επιβεβαιώνει ότι οι τρομοκρατικές οργανώσεις δεν βρίσκονται εκτός της διεθνούς έννομης τάξης, αλλά εντάσσονται σε αυτήν ως μη κρατικοί δρώντες των οποίων η δράση ρυθμίζεται μέσω κανόνων διεθνούς ασφάλειας, διεθνούς ποινικού δικαίου και, σε ορισμένες περιπτώσεις, διεθνούς ανθρωπιστικού δικαίου.⁵³

2.2.Γιατί οι τρομοκρατικές οργανώσεις δεν βρίσκονται εκτός της διεθνούς έννομης τάξης

Οι τρομοκρατικές οργανώσεις, ως βίαιοι μη κρατικοί δρώντες (Non-State Actors), δε λειτουργούν σε νομικό κενό, αλλά δεσμεύονται από θεμελιώδεις κανόνες της διεθνούς έννομης τάξης.⁵⁴ Συγκεκριμένα, στο πλαίσιο του Διεθνούς Ανθρωπιστικού Δικαίου (ΔΑΔ), το οποίο εφαρμόζεται σε ένοπλες συρράξεις, οι μη κρατικές ένοπλες ομάδες αποτελούν άμεσους αποδέκτες υποχρεώσεων, όπως ρητά ορίζει το Κοινό Άρθρο 3 των Συμβάσεων της Γενεύης

⁴⁹ United Nations Security Council. (2001). Ibid, §1 a-d, 2e.

⁵⁰ United Nations Security Council. (2004). Resolution 1540 (2004), S/RES/1540 (2004), § 1-2. <https://documents.un.org/doc/undoc/gen/n04/328/43/pdf/n0432843.pdf>

⁵¹ United Nations General Assembly. (1994). Declaration on Measures to Eliminate International Terrorism, A/RES/49/60, § 3. <https://documents.un.org/doc/undoc/gen/n95/768/19/pdf/n9576819.pdf>

⁵² Talmon, S. (2009). The responsibility of outside powers for acts of secessionist entities. International & Comparative Law Quarterly, 58(3), p. 495. [https://users.ox.ac.uk/~sann2029/ICLO%2058%20\(2009\),%20493-517.pdf](https://users.ox.ac.uk/~sann2029/ICLO%2058%20(2009),%20493-517.pdf)

⁵³ United Nations Security Council. (2014). Resolution 2178 (2014), S/RES/2178 (2014), § 4-6. <https://documents.un.org/doc/undoc/gen/n14/547/98/pdf/n1454798.pdf>

⁵⁴ Greenwood, C. (2002). International law and the 'war against terrorism'. International Affairs, 78(2), p. 302. <https://library.fes.de/libalt/journals/swetsfulltext/12995288.pdf>

του 1949, το οποίο δεσμεύει «κάθε μέρος στη σύγκρουση» σε περιπτώσεις μη διεθνών ενόπλων συρράξεων.⁵⁵ Η δέσμευση αυτή έχει επιβεβαιωθεί από το Διεθνές Δικαστήριο της Χάγης (ICJ) στην υπόθεση Nicaragua, όπου κρίθηκε ότι οι κανόνες του Κοινού Άρθρου 3 αντικατοπτρίζουν «στοιχειώδεις εκτιμήσεις ανθρωπισμού» και αποτελούν εθνικό δίκαιο που δεσμεύει όλους τους δρώντες, ανεξαρτήτως της νομικής τους προσωπικότητας.⁵⁶ Επιπλέον, το Πρόσθετο Πρωτόκολλο II του 1977 εξειδικεύει περαιτέρω τις υποχρεώσεις οργανωμένων ενόπλων ομάδων που ασκούν έλεγχο επί εδάφους, καθιστώντας τες υπεύθυνες για την τήρηση κανόνων προστασίας του άμαχου πληθυσμού.⁵⁷ Αυτό σημαίνει πρακτικά ότι μια τρομοκρατική οργάνωση που ελέγχει περιοχές (όπως συνέβη με τον ISIS ή τη Χαμάς) δεν είναι απλώς ένας εγκληματίας του κοινού ποινικού δικαίου, αλλά ένας δρών που οφείλει να σέβεται τις αρχές της διάκρισης και της αναλογικότητας, η παραβίαση των οποίων γεννά διεθνή ευθύνη.⁵⁸

Πέρα από το ανθρωπιστικό δίκαιο, η ένταξη των τρομοκρατικών οργανώσεων στο ρυθμιστικό πεδίο επιτυγχάνεται μέσω του Διεθνούς Ποινικού Δικαίου, το οποίο μετατοπίζει την εστίαση από την ευθύνη της ομάδας στην ατομική ποινική ευθύνη των μελών και της ηγεσίας της.⁵⁹ Το Καταστατικό της Ρώμης του Διεθνούς Ποινικού Δικαστηρίου (ΔΠΔ) ορίζει ότι άτομα που διαπράττουν εγκλήματα πολέμου ή εγκλήματα κατά της ανθρωπότητας, ακόμη και αν ενεργούν ως μέλη μη κρατικών οργανώσεων, υπέχουν ποινικής ευθύνης διεθνώς.⁶⁰ Χαρακτηριστικό παράδειγμα αποτελεί η νομολογία του Ειδικού Δικαστηρίου για τον Λίβανο (STL), το οποίο στην απόφασή του το 2011 αναγνώρισε ότι υφίσταται ορισμός της τρομοκρατίας στο διεθνές εθνικό δίκαιο, εφαρμόσιμος και σε περιόδους ειρήνης, δημιουργώντας έτσι άμεση σύνδεση μεταξύ των πράξεων της οργάνωσης και της διεθνούς

⁵⁵ International Committee of the Red Cross (ICRC). (2016). Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 3 §505. <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3/commentary/2016?activeTab=3>

⁵⁶ International Court of Justice (ICJ). (1986). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 114, § 218 - 219. <https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>

⁵⁷ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Art. 1 § 1. <https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and-0>

⁵⁸ Sivakumaran, S. (2011). Lessons for the law of armed conflict from commitments of armed groups. International Review of the Red Cross, 93(882), p. 464-466. <https://international-review.icrc.org/sites/default/files/irrc-882-sivakumaran.pdf>

⁵⁹ Cassese, A. (2006). The Multifaceted Criminal Notion of Terrorism in International Law. Journal of International Criminal Justice, 4(5), p. 935. <https://academic.oup.com/jicj/article/4/5/933/835024>

⁶⁰ UN General Assembly. (1998). Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998, Art. 25 § 3. <https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf>

ποινικής καταστολής.⁶¹ Επομένως, οι τρομοκρατικές οργανώσεις δεν βρίσκονται στο απυρόβλητο λόγω έλλειψης κρατικής υπόστασης, καθώς οι πράξεις τους χαρακτηρίζονται ως διεθνή εγκλήματα που προσβάλλουν την παγκόσμια κοινότητα.⁶²

Σε επίπεδο διεθνούς ασφάλειας, το Συμβούλιο Ασφαλείας του ΟΗΕ έχει διαδραματίσει καθοριστικό "νομοθετικό" ρόλο, υπάγοντας τις τρομοκρατικές ομάδες σε ένα αυστηρό καθεστώς κυρώσεων και περιορισμών μέσω Ψηφισμάτων που εκδίδονται βάσει του Κεφαλαίου VII του Χάρτη.⁶³ Το Ψήφισμα 1373 (2001), που υιοθετήθηκε μετά την 11η Σεπτεμβρίου, επέβαλε στα κράτη την υποχρέωση να παγώσουν περιουσιακά στοιχεία και να ποινικοποιήσουν την παροχή υποστήριξης σε τρομοκρατικές οντότητες, αναγνωρίζοντας έμμεσα τις ομάδες αυτές ως διακριτές οντότητες με ικανότητα πρόκλησης απειλής στη διεθνή ειρήνη.⁶⁴ Πιο πρόσφατα, το Ψήφισμα 2178 (2014) για τους Ξένους Τρομοκράτες Μαχητές (FTFs) επέκτεινε τη ρυθμιστική εμβέλεια του διεθνούς δικαίου, στοχεύοντας στη διασυννοριακή κίνηση και στρατολόγηση ατόμων από μη κρατικές ομάδες.⁶⁵ Τέλος, σε ευρωπαϊκό επίπεδο, η Οδηγία (ΕΕ) 2017/541 για την καταπολέμηση της τρομοκρατίας εναρμονίζει τους ορισμούς των τρομοκρατικών εγκλημάτων, συμπεριλαμβανομένων των εγκλημάτων στον κυβερνοχώρο, επιβεβαιώνοντας ότι η τεχνολογική δράση των ομάδων αυτών εμπίπτει πλήρως στον νομικό έλεγχο.⁶⁶ Συνεπώς, οι τρομοκρατικές οργανώσεις αποτελούν "αντικείμενα" διεθνούς ρύθμισης και η συμπεριφορά τους αξιολογείται συνεχώς βάσει κανόνων που έχουν θεσπιστεί από τη διεθνή κοινότητα για την προστασία θεμελιωδών αγαθών.⁶⁷

⁶¹ Special Tribunal for Lebanon (STL). (2011). Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case No. STL-11-01/I, Appeals Chamber, p. 49 § 85. <https://www.refworld.org/jurisprudence/caselaw/stl/2011/en/77425>

⁶² Cassese, A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law. *European Journal of International Law*, 12(5), p. 994. <https://www.ejil.org/pdfs/12/5/1558.pdf>

⁶³ United Nations Security Council. (1945). Charter of the United Nations, Chapter VII. <https://www.un.org/en/about-us/un-charter/chapter-6>

⁶⁴ United Nations Security Council. (2001). Resolution 1373 (2001), S/RES/1373, § 1 (c) & 2 (a). [https://docs.un.org/en/S/RES/1373\(2001\)](https://docs.un.org/en/S/RES/1373(2001))

⁶⁵ United Nations Security Council. (2014). Resolution 2178 (2014), S/RES/2178, §6. [https://docs.un.org/en/S/RES/2178\(2014\)](https://docs.un.org/en/S/RES/2178(2014))

⁶⁶ European Parliament and Council of the European Union. (2017). Directive (EU) 2017/541 of 15 March 2017 on combating terrorism, Official Journal of the European Union, L 88, Art. 3 & 14. <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32017L0541>

⁶⁷ Henckaerts, J.-M., & Doswald-Beck, L. (Eds.). (2005). Customary International Humanitarian Law, Volume I: Rules. Cambridge University Press, Rule 139. <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule139>

2.3.Κρατική υποστήριξη, ανοχή και έλεγχος τρομοκρατικών οργανώσεων

Η ανάλυση της σχέσης μεταξύ κρατών και τρομοκρατικών οργανώσεων δεν περιορίζεται σε μια διπολική διάκριση μεταξύ πλήρους κρατικού ελέγχου και απόλυτης αυτονομίας των δευτέρων, αλλά εκτείνεται σε ένα φάσμα διαβαθμισμένης εμπλοκής που κυμαίνεται από την ενεργό υποστήριξη έως την παθητική ανοχή.⁶⁸ Στο σύγχρονο διεθνές δίκαιο, η κρατική εμπλοκή λαμβάνει ποικίλες μορφές, όπως η παροχή οικονομικών πόρων, η στρατιωτική εκπαίδευση, η προμήθεια οπλισμού, και πλέον, η διάθεση τεχνολογικών υποδομών και ψηφιακού ασύλου (safe havens) για τη διεξαγωγή κυβερνοεπιχειρήσεων.⁶⁹ Το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών, ειδικότερα μετά την 11η Σεπτεμβρίου, με το Ψήφισμα 1373 (2001), κατέστησε σαφές ότι τα κράτη οφείλουν να απέχουν από κάθε μορφή ενεργητικής ή παθητικής υποστήριξης προς οντότητες που εμπλέκονται σε τρομοκρατικές πράξεις, συμπεριλαμβανομένης της παροχής τεχνογνωσίας.⁷⁰

Για τη θεμελίωση της διεθνούς ευθύνης ενός κράτους για πράξεις ιδιωτών, το διεθνές δίκαιο αναζητά τον βαθμό ελέγχου που ασκείται επί των δραστών. Σύμφωνα με το Άρθρο 8 των «Άρθρων για την Ευθύνη των Κρατών» (ARSIWA) της Επιτροπής Διεθνούς Δικαίου (ILC), η συμπεριφορά ενός μη κρατικού δρώντα αποδίδεται στο κράτος εάν αυτός ενεργεί κατ' εντολή (instructions) ή υπό τη διεύθυνση (direction) ή τον έλεγχο (control) του κράτους.⁷¹ Οι έννοιες αυτές έχουν ερμηνευτεί με απόλυτη σαφήνεια και αυστηρότητα. Το Διεθνές Δικαστήριο της Χάγης (ICJ), στην υπόθεση Nicaragua v. United States (1986), όπως είχε προαναφερθεί η συγκεκριμένη υπόθεση καθιέρωσε το κριτήριο του «αποτελεσματικού ελέγχου» (effective control), κρίνοντας ότι για να αποδοθούν οι πράξεις των Κόντρας στις ΗΠΑ, δεν αρκούσε η γενική χρηματοδότηση και ο εξοπλισμός, αλλά απαιτούνταν απόδειξη ότι το κράτος είχε τον έλεγχο επί των συγκεκριμένων επιχειρήσεων κατά τις οποίες τελέστηκαν οι παραβιάσεις.⁷²

Αντίθετα, το Διεθνές Ποινικό Δικαστήριο για την Πρώην Γιουγκοσλαβία (ICTY), στην υπόθεση Tadić (1999), πρόκρινε το ελαστικότερο κριτήριο του «συνολικού ελέγχου» (overall control) για οργανωμένες ένοπλες και παραστρατιωτικές ομάδες, δεχόμενο ότι η ευθύνη

⁶⁸ A/RES/56/83, ubi supra, n. 10, art. 8.

⁶⁹ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. Rules 7 & 8 p. 34 – 36. <https://www.onlinelibrary.iuhl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>

⁷⁰ United Nations Security Council. (2001). ubi supra, §2 (c).

⁷¹ A/RES/56/83, ubi supra, n. 10, art. 8.

⁷² International Court of Justice (ICJ). (1986). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986. § 115.

θεμελιώνεται όταν το κράτος έχει ρόλο στην οργάνωση, τον συντονισμό ή τον σχεδιασμό των στρατιωτικών δράσεων, χωρίς να απαιτείται η έκδοση οδηγιών για κάθε συγκεκριμένη πράξη.⁷³ Παρ' όλα αυτά, το Διεθνές Δικαστήριο επέμεινε στο αυστηρό κριτήριο του αποτελεσματικού ελέγχου και στη μεταγενέστερη απόφασή του για τη Γενοκτονία στη Βοσνία (2007), διατηρώντας ψηλά τον πήχη για την άμεση απόδοση ευθύνης (attribution).⁷⁴

Πέραν του ελέγχου, η ευθύνη δύναται να προκύψει και εκ των υστέρων μέσω της «υιοθέτησης» (adoption). Σύμφωνα με το Άρθρο 11 της ILC, πράξεις που δεν είναι αρχικά καταλογιστές στο κράτος, καθίστανται τέτοιες εάν το κράτος τις αναγνωρίσει και τις υιοθετήσει ως δικές του, όπως κρίθηκε στην υπόθεση Tehran Hostages (1980), όπου η ιρανική κυβέρνηση ενέκρινε και διαιώνισε την κατάληψη της πρεσβείας από φοιτητές.⁷⁵ Ωστόσο, η πιο κρίσιμη διάσταση για τη σύγχρονη κυβερνοτρομοκρατία αφορά την ευθύνη λόγω παράλειψης (omission) και γνώσης. Η θεμελιώδης αρχή που διατυπώθηκε στην υπόθεση Corfu Channel (1949) ορίζει ότι κανένα κράτος δεν δικαιούται να επιτρέπει εν γνώσει του (knowingly) τη χρήση του εδάφους του για πράξεις που προσβάλλουν τα δικαιώματα άλλων κρατών.⁷⁶

Η έννοια της γνώσης δεν περιορίζεται στην αποδεδειγμένη βεβαιότητα, αλλά εκτείνεται και στην «εποικοδομητική γνώση» (constructive knowledge), δηλαδή στο τι το κράτος όφειλε να γνωρίζει βάσει των μέσων που διαθέτει.⁷⁷ Ειδικά στο πεδίο των νέων τεχνολογιών, η ανοχή ενός κράτους στη φιλοξενία διακομιστών ή την ανάπτυξη αλγορίθμων Τεχνητής Νοημοσύνης από τρομοκρατικές ομάδες εντός της δικαιοδοσίας του, εφόσον το κράτος γνωρίζει ή οφείλει να γνωρίζει τον κίνδυνο και παραλείπει να λάβει μέτρα, ενεργοποιεί την υποχρέωση δέουσας επιμέλειας (due diligence).⁷⁸ Η παράλειψη αυτή μετατρέπει την εδαφική κυριαρχία από δικαίωμα σε πηγή ευθύνης, καθώς η διεθνής κοινότητα απαιτεί πλέον από τα κράτη να μην

⁷³ International Criminal Tribunal for the former Yugoslavia (ICTY). (1999). *Prosecutor v. Duško Tadić*. Judgment, Appeals Chamber, Case No. IT-94-1-A, p. 49 § 120. <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>

⁷⁴ International Court of Justice (ICJ). (2007). 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, p. 169 § 400. <https://www.acerislaw.com/wp-content/uploads/2024/04/Application-of-the-Convention-on-the-Prevention-and-Punishment-of-the-Crime-of-Genocide.pdf>

⁷⁵ International Court of Justice (ICJ). (1980). United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran). Judgment, I.C.J. Reports 1980, p. 35 § 70. <https://www.icj-cij.org/sites/default/files/case-related/64/064-19800524-JUD-01-00-EN.pdf>

⁷⁶ International Court of Justice (ICJ). (1949). *ubi supra*, p. 22.

⁷⁷ Koivurova, T. (2012). Due Diligence. Max Planck Encyclopedia of Public International Law (MPEPIL), § C. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1034>

⁷⁸ United Nations General Assembly. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174, p. 8 § 13 (c). <https://docs.un.org/en/A/70/174>

λειτουργούν ως παθητικοί παρατηρητές ασύμμετρων απειλών που εκπορεύονται από το έδαφός τους.⁷⁹

3. ΚΕΦΑΛΑΙΟ: ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΧΡΗΣΗ ΠΑΡΑΓΩΓΙΚΗΣ ΤΝ ΑΠΟ ΤΡΟΜΟΚΡΑΤΙΚΕΣ ΟΡΓΑΝΩΣΕΙΣ

Το παρόν κεφάλαιο εξετάζει την επιχειρησιακή ενσωμάτωση της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI) στο οπλοστάσιο των μη κρατικών δρώντων, αναλύοντας τον τρόπο με τον οποίο η τεχνολογία αυτή μεταβάλλει το *modus operandi* των τρομοκρατικών οργανώσεων. Η μετάβαση από τη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) ως μέσων υποστήριξης στην άμεση εργαλειοποίηση αλγορίθμων μηχανικής μάθησης συνιστά ποιοτική μεταβολή της απειλής, η οποία αποκτά υβριδικά χαρακτηριστικά, συνδυάζοντας την ψηφιακή δράση με φυσικά αποτελέσματα.⁸⁰

Η τεχνολογία λειτουργεί ενισχυτικά, επαυξάνοντας τον αντίκτυπο (*amplifying impact*) και τις συνέπειες των τρομοκρατικών ενεργειών στα θύματα.⁸¹ Παράλληλα, η ευρεία διαθεσιμότητα αυτών των μοντέλων μειώνει δραστικά τα τεχνικά εμπόδια (*lowering the barrier to entry*), επιτρέποντας σε δρώντες με περιορισμένες δεξιότητες να εκτελούν σύνθετες επιχειρήσεις που προηγουμένως απαιτούσαν υψηλή εξειδίκευση.⁸² Το φαινόμενο αυτό επιτρέπει σε δρώντες περιορισμένων πόρων να διεξάγουν επιχειρήσεις «Γνωσιακού Πολέμου» (*Cognitive Warfare*), στοχεύοντας στην αλλοίωση της αντίληψης και τη συστημική αποσταθεροποίηση του αντιπάλου, χωρίς απαραίτητα την προσφυγή σε κινητική βία.⁸³ Η εν λόγω εξέλιξη θέτει ζητήματα συμβατότητας με το υφιστάμενο νομικό πλαίσιο, καθώς πολλές από τις ενέργειες αυτές κινούνται «κάτω από το κατώφλι της χρήσης βίας».⁸⁴

⁷⁹ Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. Yale Law Journal Forum, 125, 68-81, p. 70-71. https://yalelawjournal.org/pdf/Schmitt_PDF_g9py96jc.pdf

⁸⁰ UNICRI & UNCCT. (2021). *ubi supra*, p. 17.

⁸¹ UNICRI & UNCCT. (2021). *Ibid*, p. 17.

⁸² Mercer, S., & Watson, T. (2024). Generative AI in Cybersecurity: Assessing impact on current and future malicious software. Centre for Emerging Technology and Security (CETaS), p 6-10. https://cetas.turing.ac.uk/sites/default/files/2024-06/cetas_briefing_paper_-_generative_ai_in_cybersecurity.pdf

⁸³ Claverie, B., & du Cluzel, F. (2022). *ubi supra*, p. 2.

⁸⁴ Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention, p. 8 § 20. <https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf>

3.1. Η GenAI ως Πολλαπλασιαστής Ισχύος: Από την Ψηφιακή Προπαγάνδα στον Γνωσιακό Πόλεμο

Η κρίσιμη καμπή σε αυτή την εξέλιξη εντοπίζεται στην εμφάνιση και τη ραγδαία διάδοση της Παραγωγικής Τεχνητής Νοημοσύνης (Generative Artificial Intelligence - GenAI). Σε αντίθεση με τις προγενέστερες ψηφιακές τεχνολογίες, οι οποίες λειτουργούσαν βάσει προκαθορισμένων κανόνων και απαιτούσαν εξειδικευμένη ανθρώπινη παρέμβαση, τα συστήματα GenAI (όπως τα Μεγάλα Γλωσσικά Μοντέλα - LLMs και οι αλγόριθμοι σύνθεσης εικόνας/ήχου) χαρακτηρίζονται από δύο ιδιότητες που ανατρέπουν τα δεδομένα ασφαλείας: την αυτονομία και την επεκτασιμότητα (scalability).⁸⁵

Η τεχνολογία αυτή επιφέρει την «εκδημοκρατικοποίηση της βλάβης» (democratization of harm). Μειώνει δραστικά το τεχνικό και οικονομικό εμπόδιο εισόδου (barrier to entry), επιτρέποντας σε τρομοκρατικές ομάδες με περιορισμένους πόρους να αποκτήσουν δυνατότητες που παραδοσιακά απαιτούσαν κρατικές υπηρεσίες πληροφοριών. Η ικανότητα παραγωγής αληθοφανών βίντεο deepfakes για ψυχολογικές επιχειρήσεις, η αυτοματοποιημένη συγγραφή πολυμορφικού κακόβουλου λογισμικού (polymorphic malware) και η μαζική, εξατομικευμένη στρατολόγηση μέσω διαλογικών συστημάτων (chatbots), συνιστούν μια ποιοτική αναβάθμιση της απειλής. Η τρομοκρατία παύει να είναι μια σποραδική ενέργεια και μετατρέπεται σε μια διαρκή, αυτοματοποιημένη εκστρατεία φθοράς.⁸⁶

3.2. Κυβερνοτρομοκρατία: Από την Ψηφιακή Διατάραξη στην «AI-Υποβοηθούμενη Απειλή»

Η ραγδαία ψηφιοποίηση των σύγχρονων κοινωνιών δεν έχει μετασχηματίσει μόνο την παγκόσμια οικονομία και επικοινωνία, αλλά έχει επαναπροσδιορίσει θεμελιωδώς και τη φύση των ασύμμετρων απειλών, φέρνοντας στο προσκήνιο την έννοια της κυβερνοτρομοκρατίας (cyberterrorism). Αν και ο όρος χρησιμοποιείται ευρέως στον δημόσιο διάλογο, παραμένει αντικείμενο έντονης ακαδημαϊκής και νομικής διαμάχης ως προς το ακριβές περιεχόμενό του.

⁸⁵ Europol. (2024). European Union Terrorism Situation and Trend Report 2024 (TE-SAT). Publications Office of the European Union, <https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf>

⁸⁶ Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. <https://rm.coe.int/1680081561>

Η κατανόηση του φαινομένου απαιτεί την υπέρβαση της απλοϊκής θεώρησής του ως μια μορφή «ηλεκτρονικού εγκλήματος» και την ανάλυση των βαθύτερων πολιτικών και ιδεολογικών κινήτρων που το διακρίνουν. Στη βιβλιογραφία, συχνά αναφέρεται ο αφορισμός ότι η κυβερνοτρομοκρατία είναι «hacking με ανθρώπινα θύματα», υποδηλώνοντας την ανάγκη για φυσική καταστροφή ώστε να στοιχειοθετηθεί ο όρος. Ωστόσο, σύγχρονοι μελετητές και οργανισμοί όπως το Κέντρο Αριστείας Κυβερνοάμυνας του NATO (CCDCOE) υιοθετούν μια ευρύτερη προσέγγιση, ορίζοντας την κυβερνοτρομοκρατία ως προμελετημένες, πολιτικά υποκινούμενες επιθέσεις εναντίον πληροφοριακών συστημάτων, οι οποίες έχουν ως στόχο να προκαλέσουν βία ή φόβο εναντίον μη μάχιμων στόχων.

Η δυσκολία στον ορισμό επιτείνεται από τη σύγχυση με έννοιες όπως ο «κυβερνοπόλεμος» (cyber warfare) και το «κυβερνοέγκλημα» (cybercrime). Όπως επισημαίνουν οι Dogrul et al. (2011), η ειδοποιός διαφορά έγκειται στην πρόθεση και τον στόχο: ενώ ο κυβερνοπόλεμος αφορά συγκρούσεις μεταξύ κρατικών δρώντων με στόχο την καταστροφή εχθρικών υποδομών, η κυβερνοτρομοκρατία διεξάγεται κυρίως από μη κρατικούς δρώντες με σκοπό τον εξαναγκασμό κυβερνήσεων και την πρόκληση τρόμου. Το Γραφείο των Ηνωμένων Εθνών για τον Έλεγχο των Ναρκωτικών και το Έγκλημα (UNODC) τονίζει ότι η νομική ασάφεια δημιουργεί κενά λογοδοσίας, καθώς πολλές ενέργειες που φέρουν τα χαρακτηριστικά τρομοκρατίας διώκονται τελικά ως απλές παραβιάσεις ασφάλειας δικτύων, αποτυγχάνοντας να αναγνωρίσουν το πολιτικό υπόβαθρο της πράξης. Η έλλειψη μιας καθολικά αποδεκτής διεθνούς σύμβασης για την κυβερνοτρομοκρατία επιτρέπει στους δράστες να εκμεταλλεύονται τα νομικά κενά μεταξύ διαφορετικών δικαιοδοσιών (jurisdictional arbitrage), καθιστώντας την καταπολέμησή της εξαιρετικά δυσχερή.

Μια από τις πιο ανησυχητικές εξελίξεις στον χώρο αυτό είναι η λεγόμενη «σύγκλιση» (convergence) ή ο δεσμός μεταξύ οργανωμένου εγκλήματος και τρομοκρατίας (crime-terror nexus) στον κυβερνοχώρο. Σύμφωνα με πρόσφατες έρευνες του UNICRI (2024), οι τρομοκρατικές οργανώσεις δεν λειτουργούν πλέον σε στεγανά, αλλά συνεργάζονται ολοένα και περισσότερο με διεθνικά εγκληματικά δίκτυα για την απόκτηση τεχνογνωσίας και πόρων. Ο κυβερνοχώρος λειτουργεί ως επιταχυντής αυτής της σύγκλισης, επιτρέποντας σε τρομοκράτες να αγοράζουν κακόβουλο λογισμικό και υπηρεσίες επιθέσεων (Cybercrime-as-a-Service) από το "Dark Web", αποκτώντας έτσι επιχειρησιακές δυνατότητες που παλαιότερα διέθεταν μόνο κρατικές οντότητες. Όπως αναλύουν οι Pratama και Yuliatin (2020), το διαδίκτυο έχει μετατραπεί σε ένα παγκόσμιο φόρουμ για την προπαγάνδα, τη στρατολόγηση και τη χρηματοδότηση, καθιστώντας τα σύνορα μεταξύ της φυσικής και της ψηφιακής τρομοκρατίας δυσδιάκριτα. Στη σύγχρονη εποχή, ο κυβερνοχώρος έχει διττή χρήση για τους

τρομοκράτες. Αφενός η χρήση του είναι άμεση μέσω την άμεση αξιοποίησης των κυβερνοεπιθέσεων, αφετέρου με έμμεσο τρόπο μέσω διευκόλυνσης που προσφέρει για την επιχειρησιακή οργάνωση τρομοκρατικών επιθέσεων μέσω παραδοσιακών μεθόδων. Ο κυβερνοχώρος αποτελεί ένα αξιοσημείωτο εργαλείο για αυτή της νέας υβριδικής τρομοκρατίας με σκοπό την διάδοση των πολιτικών τους στόχων.

Η διαφορά της παραδοσιακής τρομοκρατίας με την κυβερνοτρομοκρατία, είναι ότι η δεύτερη έχει τη δυνατότητα να επηρεάσει άμεσα μεγαλύτερο αριθμό ανθρώπων σε σχέση με την πρώτη. Ο κυβερνοχώρος δεν περιορίζεται από γεωγραφικά όρια, δεν ελέγχεται αποτελεσματικά και η προσβασιμότητα του είναι ανεξέλεγκτη. Συμπερασματικά, ο κυβερνοχώρος προσφέρει στους τρομοκράτες ένα τέλειο στρατηγικό μέσο, μέσω του οποίου δεν μπορεί να τεθεί η ζωή τους σε κίνδυνο, καθώς οι πράξεις τους πραγματοποιούνται στο ψηφιακό κόσμο.

Η εξέλιξη αυτή σηματοδοτεί τη μετάβαση σε μια νέα, πιο επικίνδυνη φάση: την «ΑΙ-υποβοηθούμενη τρομοκρατία» (AI-enabled terrorism). Η ενσωμάτωση της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI) λειτουργεί ως πολλαπλασιαστής ισχύος, μειώνοντας δραστικά το τεχνικό όριο εισόδου για επίδοξους τρομοκράτες. Ο Farber (2025) υποστηρίζει ότι η «στρατιωτικοποίηση» της ΤΝ από τρομοκρατικές ομάδες θολώνει τις γραμμές μεταξύ ειρήνης και σύγκρουσης, καθώς επιτρέπει την αυτοματοποίηση πολύπλοκων επιθέσεων με ταχύτητα και κλίμακα που είναι αδύνατον να αντιμετωπιστούν με συμβατικά μέσα. Μελέτες του Combating Terrorism Center στο West Point επιβεβαιώνουν ότι τα Μεγάλα Γλωσσικά Μοντέλα (LLMs) μπορούν να χρησιμοποιηθούν για την αποτελεσματικότερη σχεδίαση επιθέσεων και τη μαζική ριζοσπαστικοποίηση ατόμων μέσω εξατομικευμένης προπαγάνδας, δημιουργώντας ένα περιβάλλον όπου η απειλή είναι πανταχού παρούσα και συνεχώς μεταβαλλόμενη.

Πέρα από την τεχνική διάσταση, η πιο ύπουλη πτυχή της σύγχρονης κυβερνοτρομοκρατίας εστιάζει στον ανθρώπινο ψυχισμό. Οι τρομοκρατικές οργανώσεις έχουν αντιληφθεί ότι ο «τρόμος» στον 21ο αιώνα δεν προκαλείται απαραίτητα από φυσική καταστροφή, αλλά από την κατάρρευση της εμπιστοσύνης και την πρόκληση ψυχολογικής δυσφορίας. Οι Gross, Canetti και Vashdi (2017) σε έρευνά τους καταρρίπτουν τον μύθο ότι οι κυβερνοεπιθέσεις αποτελούν απλώς μια «ενόχληση», αποδεικνύοντας ότι μπορούν να προκαλέσουν επίπεδα ψυχολογικού τραύματος και άγχους συγκρίσιμα με αυτά της συμβατικής τρομοκρατίας. Η αίσθηση ευαλωτότητας που προκαλείται όταν παραβιάζονται προσωπικά δεδομένα ή κρίσιμες υποδομές υπονομεύει την εμπιστοσύνη των πολιτών στην ικανότητα του κράτους να τους προστατεύσει. Επιπλέον, οι Benson και McAlaney (2019) εισάγουν την έννοια της «φοβοφοβίας» (phobophobia) στον κυβερνοχώρο, περιγράφοντας μια κουλτούρα διαρκούς φόβου και

καχυποψίας που διαβρώνει την κοινωνική συνοχή και οδηγεί τους πολίτες σε συμπεριφορές αποφυγής, ενισχύοντας τελικά τους στόχους των τρομοκρατών.

Συμπερασματικά, η κυβερνοτρομοκρατία δεν αποτελεί πλέον μια στατική έννοια, αλλά ένα δυναμικό και εξελισσόμενο φαινόμενο που συνδυάζει την τεχνολογική καινοτομία με ψυχολογικές επιχειρήσεις. Η μετάβαση από τις απλές κυβερνοεπιθέσεις στις σύνθετες, υποβοηθούμενες από ΤΝ υβριδικές απειλές, και η στενή συνεργασία με το οργανωμένο έγκλημα, απαιτούν την αναθεώρηση των παραδοσιακών αμυντικών δογμάτων. Η διεθνής κοινότητα καλείται να αντιμετωπίσει όχι μόνο τις τεχνικές προκλήσεις της απόδοσης ευθυνών (attribution dilemma), αλλά και τις βαθύτερες κοινωνικοπολιτικές επιπτώσεις ενός «αόρατου πολέμου» που στοχεύει εξίσου στις υποδομές και στο μυαλό των πολιτών.

3.3.Η GenAI στην Υπηρεσία της Ριζοσπαστικοποίησης (Propaganda)

Η έλευση των Μεγάλων Γλωσσικών Μοντέλων (LLMs) μετασχηματίζει ριζικά τη νομική υπόσταση της τρομοκρατικής στρατολόγησης, καθώς επιτρέπει την αυτοματοποιημένη παραγωγή προπαγανδιστικού υλικού που είναι πρακτικά μη διακρίσιμο από το ανθρώπινο κείμενο, καθιστώντας εξαιρετικά δυσχερή την απόδειξη του δόλου και την εφαρμογή των παραδοσιακών διατάξεων περί υποκίνησης σε βία⁸⁷. Η δυνατότητα αυτών των συστημάτων να προσαρμόζουν το ύφος και τη γλώσσα του μηνύματος σε πραγματικό χρόνο καταργεί τα εδαφικά και γλωσσικά εμπόδια που παλαιότερα περιόριζαν τη δράση των στρατολόγων, δημιουργώντας ζητήματα διασυννοριακής δικαιοδοσίας για τις διωκτικές αρχές.⁸⁸ Πλέον, η διαδικασία της ριζοσπαστικοποίησης αποσυνδέεται από την ανάγκη φυσικής ή άμεσης ανθρώπινης αλληλεπίδρασης, καθώς η τεχνητή νοημοσύνη μειώνει δραστικά το κόστος της προπαγάνδας, επιτρέποντας σε κακόβουλους δρώντες να διεξάγουν εκστρατείες επιρροής μαζικής κλίμακας με ελάχιστους πόρους.⁸⁹

Η στρατηγική της «μικρο-στόχευσης» (micro-targeting) εισέρχεται σε μια νέα φάση λειτουργικής ωριμότητας, καθώς αλγόριθμοι συστάσεων (recommendation algorithms) αναλύουν τη συμπεριφορά των χρηστών για να εντοπίσουν άτομα με ψυχολογική

⁸⁷ Europol. (2023). ChatGPT. ubi supra, p. 8.

⁸⁸ Organization for Security and Co-operation in Europe (OSCE). (2024). New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons. Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, p. 13. <https://www.osce.org/sites/default/files/f/documents/7/d/579715.pdf>

⁸⁹ Goldstein, J. A., et al. (2023). Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations, p. 2-6. <https://arxiv.org/pdf/2301.04246>

ευαλωτότητα, οδηγώντας τα σταδιακά σε μια διαδικασία «αυτο-ριζοσπαστικοποίησης» (self-radicalization) μέσω της αποκλειστικής έκθεσης σε εξτρεμιστικό περιεχόμενο.⁹⁰ Αυτοί οι μηχανισμοί δημιουργούν στεγανοποιημένους ψηφιακούς χώρους ή «θαλάμους αντήχησης» (echo chambers), όπου η επαναληπτική προβολή πολωτικών μηνυμάτων ενισχύει τις πεποιθήσεις του ατόμου και αποκλείει αντίθετες απόψεις, λειτουργώντας ως καταλύτης για την ταχεία ιδεολογική μεταστροφή.⁹¹ Παράλληλα, η χρήση της παραγωγικής τεχνητής νοημοσύνης επιτρέπει πλέον την «οπλοποίηση» της ψηφιακής εγγραμματοσύνης, καθώς τα τρομοκρατικά δίκτυα κατασκευάζουν εξατομικευμένα αφηγήματα που παρουσιάζουν τη βία ως θρησκευτική υποχρέωση, προσαρμοσμένη ακριβώς στις πνευματικές αναζητήσεις του εκάστοτε στόχου.⁹² Σε νομικό επίπεδο, η χρήση τέτοιων αλγορίθμων θέτει πρωτοφανή ζητήματα, καθώς η κακόβουλη χρήση της τεχνητής νοημοσύνης για την αλλοίωση της ανθρώπινης κρίσης υπερβαίνει τα παραδοσιακά όρια της προπαγάνδας, αγγίζοντας τα όρια της ψυχολογικής χειραγώγησης και του καταναγκασμού.⁹³

Η επιχειρησιακή δομή της στρατολόγησης ενισχύεται περαιτέρω μέσω της χρήσης αυτοματοποιημένων λογισμικών (bots) σε κρυπτογραφημένες πλατφόρμες όπως το Telegram, τα οποία επιτρέπουν τη μαζική διανομή προπαγάνδας και την αρχική διαλογή υποψηφίων χωρίς ανθρώπινη παρέμβαση, καθιστώντας τον εντοπισμό των κεντρικών διαχειριστών νομικά και τεχνικά δυσχερή.⁹⁴ Η στρατηγική αυτή επεκτείνεται πλέον πέραν των παραδοσιακών μέσων κοινωνικής δικτύωσης, διεισδύοντας σε πλατφόρμες διαδικτυακών παιχνιδιών (όπως το Roblox), όπου εξτρεμιστικές ομάδες εκμεταλλεύονται το νεανικό κοινό διασπείροντας ρητορική μίσους μέσω διαδραστικού περιεχομένου, παρακάμπτοντας έτσι τους γονικούς ελέγχους και τα φίλτρα ασφαλείας.⁹⁵ Επιπλέον, παρατηρείται η συστηματική παραγωγή

⁹⁰ Donghee Shin & Kulsawasd Jitkajornwanich. (2024). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review*, 42(4), pp. 1020-1040, p. 1035. https://www.researchgate.net/publication/382731522_How_Algorithms_Promote_Self-Radicalization_Audit_of_TikTok%27s_Algorithm_Using_a_Reverse_Engineering_Method

⁹¹ Soumya Awasthi (2025). From clicks to chaos: How social media algorithms amplify extremism. Observer Research Foundation. § 3. <https://www.orfonline.org/expert-speak/from-clicks-to-chaos-how-social-media-algorithms-amplify-extremism>

⁹² The Durant Dispatch (2025). Digital jihad: weaponization of AI literacy as religious obligation. <https://www.duranddispatch.com/p/digital-jihad-weaponization-of-ai-literacy-as-religious-obligation>

⁹³ UN Office of Counter Terrorism. (2021). ubi supra, p.18.

⁹⁴ <https://www.tandfonline.com/doi/full/10.1080/09546553.2023.2169141>

⁹⁵ Linda Schlegel, Constantin Winkler, & Lars Wiegold. (2025, October 28). Youth Radicalisation in the Gaming Sphere: An Exploration of Identity-Based Hate and Extremist Content on Roblox. Global Network on Extremism & Technology (GNET). <https://gnet-research.org/2025/10/28/youth-radicalisation-in-the-gaming-sphere-an-exploration-of-identity-based-hate-and-extremist-content-on-roblox/>

ψηφιακού υλικού που έχει σχεδιαστεί ειδικά για την «εκπαίδευση» ανηλίκων, με τη μορφή φαινομενικά αθώων εκπαιδευτικών εφαρμογών, οι οποίες όμως λειτουργούν ως εργαλεία μακροχρόνιας ιδεολογικής κατήχησης και προετοιμασίας της επόμενης γενιάς τρομοκρατών.⁹⁶

Συνεπώς, το κρίσιμο ζήτημα που ανακύπτει δεν είναι η απουσία νομικού πλαισίου, αλλά η αδυναμία αποτελεσματικής εφαρμογής του σε ένα ψηφιακό περιβάλλον που μεταβάλλεται ραγδαία. Παρόλο που υφίστανται νομικά εργαλεία, η έλλειψη ενός καθολικά αποδεκτού ορισμού για την κυβερνοτρομοκρατία και οι αποκλίσεις στις εθνικές νομοθεσίες εξακολουθούν να εμποδίζουν την αποτελεσματική δικαστική συνεργασία μεταξύ των κρατών-μελών, επιτρέποντας στους δράστες να εκμεταλλεύονται δικαιοδοτικά κενά.⁹⁷ Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι, παρά την εφαρμογή του Κανονισμού για την αντιμετώπιση της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο (TCO Regulation), οι τρομοκρατικές ομάδες συνεχίζουν να διαχέουν επιτυχώς την προπαγάνδα τους σε ποικίλες πλατφόρμες, αποδεικνύοντας στην πράξη το χάσμα που χωρίζει τη νομοθέτηση από την επιβολή του νόμου.⁹⁸ Επιπροσθέτως, η νομική εποπτεία καθίσταται δυσχερής λόγω της αδιαφάνειας των πλατφορμών, καθώς οι τρέχουσες πρακτικές αναφοράς διαφάνειας είναι συχνά ανεπαρκείς για να επιτρέψουν μια ανεξάρτητη αξιολόγηση του κατά πόσον τα μέτρα που λαμβάνονται είναι αποτελεσματικά και συμβατά με τα ανθρώπινα δικαιώματα.⁹⁹

3.4.Γνωσιακός Πόλεμος (Cognitive Warfare) και Deepfakes

Η πιο επικίνδυνη πτυχή της παραγωγικής τεχνητής νοημοσύνης (GenAI) δεν περιορίζεται στην απλή παραγωγή ψευδών ειδήσεων, αλλά επεκτείνεται στη διεξαγωγή ενός ολοκληρωτικού «γνωσιακού πολέμου» (cognitive warfare), όπου τα deepfakes χρησιμοποιούνται ως ψυχολογικά όπλα για να προκαλέσουν έντονη συναισθηματική φόρτιση

⁹⁶ Europol's EU Internet Referral Unit. (2023, December 21). Crackdown on material designed to 'educate' future terrorists. Europol Media Press. https://www.europol.europa.eu/media-press/newsroom/news/crackdown-material-designed-to-%E2%80%98educate%E2%80%99-future-terrorists?mtm_campaign=newsletter

⁹⁷ Kapsokoli, E. (2022). The challenge of defining cyberterrorism within the EU. In Challenges of the common security and defence policy (pp. 183-196). Publications Office of the European Union, p. 186. <https://op.europa.eu/en/publication-detail/-/publication/e3706908-db0f-11ec-a95f-01aa75ed71a1/language-en>

⁹⁸ Europol. (2023). European Union Terrorism Situation and Trend Report 2023 (TE-SAT). Publications Office of the European Union, p. 6,19. <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat>

⁹⁹ OECD. (2024). Transparency Reporting on Terrorist and Violent Extremist Content Online (4th ed.). OECD Publishing, p. 4. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency-reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf

και να θολώσουν τα όρια μεταξύ αλήθειας και κατασκευασμένου αφηγήματος, όπως παρατηρήθηκε πρόσφατα στη σύγκρουση Ισραήλ-Χαμάς.¹⁰⁰ Σε αυτό το πλαίσιο, αναδύεται το φαινόμενο του «μερίσματος του ψεύτη» (Liar's Dividend), κατά το οποίο η απλή ύπαρξη και η ευκολία πρόσβασης σε τέτοια εργαλεία κλονίζει την εμπιστοσύνη του κοινού σε κάθε ψηφιακό τεκμήριο, επιτρέποντας σε κακόβουλους δρώντες να αμφισβητούν ακόμη και γνήσια αποδεικτικά στοιχεία, χαρακτηρίζοντάς τα ψευδώς ως προϊόντα τεχνητής νοημοσύνης.¹⁰¹ Στρατηγικός στόχος αυτών των επιχειρήσεων δεν είναι πλέον μόνο ο έλεγχος της ροής πληροφοριών, αλλά η «παραβίαση» (hacking) του ίδιου του ανθρώπινου μυαλού, ώστε να αλλάξει ο τρόπος σκέψης και αντίδρασης των στόχων, οδηγώντας σε βαθιά κοινωνική αποσταθεροποίηση.¹⁰²

Η δημιουργία αυτού του περιβάλλοντος «επιστημικής αναρχίας» δεν λειτουργεί απλώς ως παράγοντας σύγχυσης, αλλά εξελίσσεται σε μηχανισμό στρατηγικού εξαναγκασμού (coercion), καθώς επιτρέπει στις τρομοκρατικές οργανώσεις να χειραγωγούν τις πολιτικές αποφάσεις του κράτους-στόχου μέσω της πίεσης που ασκεί το παραπληροφορημένο κοινωνικό σύνολο. Όπως επισημαίνει η Καψοκόλη (2025), η μετεξέλιξη του «Ψηφιακού Τζιχάντ» αξιοποιεί την τεχνητή νοημοσύνη για να κατασκευάσει τεχνητές κρίσεις —όπως η σκηνοθετημένη βεβήλωση θρησκευτικών συμβόλων ή η κατασκευή ψευδών εγκλημάτων πολέμου— οι οποίες υποχρεώνουν τις κυβερνήσεις να αντιδράσουν σπασμωδικά υπό το βάρος της κοινής γνώμης, χάνοντας έτσι την κυρίαρχη βούλησή τους.¹⁰³ Αυτή η μορφή «γνωσιακής περικύκλωσης» παραβιάζει ουσιαδώς την αρχή της μη επέμβασης στις εσωτερικές υποθέσεις, καθώς η χρήση deepfakes για την υποκίνηση βίαιων ταραχών ή την αλλοίωση εκλογικών συμπεριφορών συνιστά μια μορφή ψηφιακής δολιοφθοράς που, αν και στερείται κινητικής βίας, επιφέρει αποτελέσματα συγκρίσιμα με αυτά μιας συμβατικής εχθρικής ενέργειας.¹⁰⁴

Η επιχειρησιακή εκμετάλλευση αυτού του κλίματος αμφισβήτησης προσφέρει στις τρομοκρατικές ομάδες το στρατηγικό πλεονέκτημα της «εύλογης άρνησης» (plausible deniability), καθιστώντας εξαιρετικά δυσχερή την τεκμηρίωση εγκλημάτων και την απόδοση

¹⁰⁰ Wired. (2023). Generative AI Is Playing a Surprising Role in Israel-Hamas Disinformation. <https://www.wired.com/story/israel-hamas-war-generative-artificial-intelligence-disinformation/>

¹⁰¹ Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), p. 1785. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship

¹⁰² NATO Review. (2021). Countering cognitive warfare: awareness and resilience. <https://www.scribd.com/document/838634646/NATO-Review-Countering-cognitive-warfare-awareness-and-resilience-2021>

¹⁰³ Καψοκόλη, Ε. (2025). Ψηφιακό Τζιχάντ: Η στρατηγική χρήση του κυβερνοχώρου από την Al Qaeda και το ISIS. Εκδόσεις Παπαζήση, σελ. 217, 221.

¹⁰⁴ Claverie, B., & du Cluzel, F. (2022). *ubi supra*, p. 1, 5.

ευθύνης σύμφωνα με τα πρότυπα του διεθνούς δικαίου.¹⁰⁵ Όπως επισημαίνεται, οι δράστες εργαλαιοποιούν τον γενικευμένο σκεπτικισμό για να απαξιώσουν προκαταβολικά γνήσια ενοχοποιητικά στοιχεία ως προϊόντα *deepfake*, δημιουργώντας ένα νομικό κενό λογοδοσίας που τους επιτρέπει να αποφεύγουν τις κυρώσεις.¹⁰⁶ Αυτή η συνθήκη ρευστότητας υπονομεύει άμεσα την «υπεροχή στη λήψη αποφάσεων» (*decision superiority*) των κρατικών μηχανισμών, καθώς, η αδυναμία άμεσης επαλήθευσης της πληροφορίας παραλύει τα αντανakλαστικά ασφαλείας και εμποδίζει τη νομιμοποίηση αμυντικών αντιμέτρων, επιτρέποντας στον αντίπαλο να επιτυγχάνει τους στόχους του χωρίς φυσική συμπλοκή.¹⁰⁷

Κατ' επέκταση, η στρατηγική στόχευση αυτών των υβριδικών επιχειρήσεων μετατοπίζεται από την απλή παραπλάνηση του ατόμου στη διάβρωση του ίδιου του «κοινωνικού συμβολαίου» που συνέχει την πολιτεία. Το κέντρο βάρους (*center of gravity*) στον Γνωσιακό Πόλεμο δεν είναι πλέον οι στρατιωτικές υποδομές, αλλά η κοινωνική συνοχή, η οποία βάλλεται μέσω της συστηματικής καλλιέργειας δυσπιστίας προς τους θεσμούς.¹⁰⁸ Όταν οι πολίτες αδυνατούν να συμφωνήσουν σε μια κοινή πραγματικότητα λόγω της επίδρασης των *deepfakes*, δημιουργούνται ρήγματα που οι τρομοκρατικές οργανώσεις, όπως το ISIS, εκμεταλλεύονται για να υποκινήσουν εσωτερικές συγκρούσεις και να απονομιμοποιήσουν την κρατική εξουσία.¹⁰⁹ Αυτή η μορφή αποσταθεροποίησης, συνιστά μια «υπαρξιακή απειλή» για τις δημοκρατίες, καθώς επιτυγχάνει πολιτικά αποτελέσματα —όπως την αλλαγή καθεστώτος ή την απόσυρση δυνάμεων, τα οποία παραδοσιακά απαιτούσαν μακροχρόνιες ένοπλες συρράξεις.¹¹⁰

3.5.Κυβερνο-επιχειρήσεις και Αυτοματοποίηση

Η ενσωμάτωση της Παραγωγικής Τεχνητής Νοημοσύνης (GenAI) στο επιχειρησιακό περιβάλλον της τρομοκρατίας σηματοδοτεί μια θεμελιώδη μετατόπιση στη μεθοδολογία των κυβερνοεπιθέσεων, μεταβάλλοντας ριζικά τη σχέση μεταξύ της τεχνικής εξειδίκευσης του δράστη και της καταστροφικής του ικανότητας.¹¹¹ Η κατάχρηση της GenAI αποτελεί πλέον

¹⁰⁵ Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), p. 1786. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship

¹⁰⁶ Chesney, R., & Citron, D. (2019). *Ibid*, p. 1786.

¹⁰⁷ Claverie, B., & du Cluzel, F. (2022). *ubi supra*, p. 5.

¹⁰⁸ NATO Review. (2021, May 20). *ubi supra*, p. 1.

¹⁰⁹ Kapsokoli, E. (2023). 'ISIS's Digital Jihad'. *National Security and the Future*, Vol. 24, No. 3, p. 45. <https://nsf-journal.hr/Portals/0/Dokumenti/Volume24,%20No3%202023/004-NSF-2023-VOL-24-No%203%20-%20Kapsokoli%20-%2039-66%20-%20IZ%C4%8C.pdf>

¹¹⁰ Καψοκόλη, Ε. (2025). *ubi supra*, p. 92.

¹¹¹ Europol. (2023). *ubi supra*, p. 9.

κεντρική ανησυχία για τις αρχές ασφαλείας, καθώς τα Μεγάλα Γλωσσικά Μοντέλα (LLMs) παρέχουν στους χρήστες πρωτοφανείς δυνατότητες για την άμεση παραγωγή κώδικα υπολογιστών, διευκολύνοντας τη δημιουργία κακόβουλου λογισμικού (malware). Η συγκεκριμένη δυνατότητα αυτόματης συγγραφής κώδικα επιτρέπει σε άτομα με ελάχιστες ή ακόμη και μηδενικές γνώσεις προγραμματισμού να αναπτύξουν λειτουργικά εργαλεία ψηφιακής επίθεσης.¹¹² Το γεγονός αυτό χαμηλώνει δραστικά το «εμπόδιο εισόδου» (barrier to entry) για αρχάριους εγκληματίες και ιδεολογικά κινούμενους "hacktivists", οι οποίοι αποκτούν πρόσβαση σε δυνατότητες που παλαιότερα απαιτούσαν έμπειρους hackers.¹¹³ Επιπλέον, τα μοντέλα αυτά λειτουργούν και ως εργαλεία τεχνικής υποστήριξης, εξηγώντας λάθη στον κώδικα ή προτείνοντας βελτιώσεις για τη λειτουργικότητα των scripts, επιταχύνοντας έτσι τη διαδικασία μάθησης για τους επίδοξους κυβερνο-τρομοκράτες.¹¹⁴

Πέραν της αρχικής δημιουργίας, η τεχνητή νοημοσύνη προσφέρει τη δυνατότητα ανάπτυξης «πολυμορφικού κώδικα» (polymorphic code). Από έρευνες, αποδείχθηκε πρακτικά η ικανότητα των LLMs να «συνθέτουν λειτουργικότητα σε πραγματικό χρόνο» (synthesize functionality at runtime), δημιουργώντας κακόβουλο λογισμικό που μεταβάλλεται συνεχώς και καθίσταται «μη ανιχνεύσιμο» (undetectable) από τα σύγχρονα συστήματα ασφαλείας.¹¹⁵ Οι επιτιθέμενοι αξιοποιούν την τεχνολογία για να δημιουργήσουν επιθέσεις που προσαρμόζονται δυναμικά και καθιστούν τις παραδοσιακές μεθόδους ανίχνευσης, που βασίζονται σε στατικές υπογραφές (signatures), λιγότερο αποτελεσματικές.¹¹⁶ Αυτή η ικανότητα δυναμικής συγκάλυψης (obfuscation) επιτρέπει σε τρομοκρατικές ομάδες να διαπερνούν κρίσιμες υποδομές που προστατεύονται από συμβατικά συστήματα ασφαλείας, καθώς το κακόβουλο λογισμικό μπορεί να αποφύγει την ψηφιακή ταυτοποίηση. Συνεπώς, η πιθανότητα επιτυχίας αυξάνεται ακόμη και έναντι καλά θωρακισμένων στόχων, δημιουργώντας συνθήκες ασύμμετρης απειλής στον κυβερνοχώρο.¹¹⁷

¹¹² Europol. (2023). Ibid. p. 8.

¹¹³ National Cyber Security Centre (NCSC). (2024). The near-term impact of AI on the cyber threat. NCSC Assessment, London. <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>

¹¹⁴ Europol. (2023). ubi supra, p. 9.

¹¹⁵ HYAS Labs. (2023). BlackMamba: AI-Synthesized Polymorphic Keylogger. <https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware>

¹¹⁶ Sourì, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. Human-centric Computing and Information Sciences, p. 3. <https://link.springer.com/article/10.1186/s13673-018-0125-x>

¹¹⁷ Pfaff, C. A. (Ed.). (2025). The weaponization of AI: The next stage of terrorism and warfare. Centre of Excellence Defence Against Terrorism, p. 7. <https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf>

Σε επίπεδο επιχειρησιακής κλίμακας, η αυτοματοποίηση λειτουργεί καταλυτικά, επιτρέποντας την ταχύτατη σάρωση δικτύων για τον εντοπισμό τρωτών σημείων. Αλγόριθμοι μηχανικής μάθησης χρησιμοποιούνται πλέον για την «αυτοματοποιημένη ανακάλυψη ευπαθειών» (automated vulnerability discovery) σε λογισμικό και συστήματα, μειώνοντας δραστικά τον χρόνο που απαιτείται για την προετοιμασία μιας επίθεσης.¹¹⁸ Ενώ οι άνθρωποι χειριστές απαιτούν σημαντικό χρόνο για να ελέγξουν δίκτυα, τα συστήματα ΑΙ μπορούν να επεξεργαστούν τεράστιους όγκους δεδομένων σχεδόν ακαριαία, εντοπίζοντας στόχους ευκαιρίας με ταχύτητα μηχανής.¹¹⁹ Η ικανότητα των μοντέλων αυτών να κατανοούν και να βελτιώνουν τον κώδικα επιτρέπει στους δράστες να αναβαθμίζουν συνεχώς το οπλοστάσιό τους χωρίς ανθρώπινη παρέμβαση, δημιουργώντας έναν αυτοτροφοδοτούμενο κύκλο απειλών.¹²⁰ Τελικά, η απειλή μετασχηματίζεται από μεμονωμένα περιστατικά υψηλής τεχνικής δυσκολίας σε μια μαζική διαδικασία φθοράς, όπου η αμυντική πλευρά καλείται να αντιμετωπίσει επιθέσεις που αυξάνουν εκθετικά την «ισχύ και την αποτελεσματικότητά» τους.¹²¹

3.6.Μελέτες Περίπτωσης (Case Studies)

Η σύγχρονη διεθνής τρομοκρατία διέρχεται μια φάση ριζικού μετασχηματισμού, όπου η χρήση των αναδυόμενων τεχνολογιών αναδιαμορφώνει τη στρατηγική των μη κρατικών δρώντων. Στο πλαίσιο του Διεθνούς Δικαίου, η ψηφιοποίηση της απειλής δημιουργεί νέες προκλήσεις για την κρατική ευθύνη και την αποτελεσματικότητα των διεθνών συμβάσεων.¹²² Οι περιπτώσεις του ISIS και της Χεζμπολάχ αποτελούν αντιπροσωπευτικά παραδείγματα αυτής της εξέλιξης, καθώς καταδεικνύουν την ικανότητα προσαρμογής σε υβριδικές μορφές πολέμου μέσω της τεχνητής νοημοσύνης.¹²³ Η ανάλυση αυτών των δρώντων επιτρέπει την

¹¹⁸ Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation, p. 25 <https://arxiv.org/pdf/1802.07228>

¹¹⁹ Brundage, M., et al. (2018). Ibid , p. 28.

¹²⁰ Group-IB. (2025). High-tech crime trends 2024/2025, Exposes how global events fuel regional and local threats. Group-IB. <https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2024-2025>

¹²¹

¹²² United Nations Office of Counter-Terrorism. (2021). Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. UNICRI, p. 12 § 2. <https://www.google.com/search?q=https://unicri.org/sites/default/files/2021-08/Algorithms-and-Terrorism.pdf>

¹²³ Kapsokoli, E. (2023). Cyberterrorism: A New Wave of Terrorism or Not. In M. A. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (Eds.), Hybrid Threats, Cyberterrorism, and Cyberwarfare, p. 59 § 3. <https://www.google.com/search?q=https://www.taylorfrancis.com/books/edit/10.1201/9781003314721/hybrid-threats-cyberterrorism-cyberwarfare>

κατανόηση του πώς ο κυβερνοχώρος λειτουργεί ως καταλύτης για τη διατήρηση της επιρροής τους, παρά τις εδαφικές απώλειες ή τους γεωπολιτικούς περιορισμούς.¹²⁴

3.6.1. ISIS (Ισλαμικό Κράτος): Η Ανάδυση του «Ψηφιακού Χαλιφάτου»

Η μετάβαση του ISIS από μια εδαφική οντότητα σε ένα «Ψηφιακό Χαλιφάτο» αποτελεί την πιο εξελιγμένη μορφή τρομοκρατικής προσαρμογής στον κυβερνοχώρο.¹²⁵ Παρά την κατάρρευση των φυσικών του προπυργίων, η οργάνωση κατάφερε να διατηρήσει την παγκόσμια απήχησή της μέσω της στρατηγικής χρήσης αυτοματοποιημένων δικτύων και bots.¹²⁶ Τα ψηφιακά αυτά εργαλεία επιτρέπουν τη μαζική διάχυση προπαγανδιστικού υλικού, διασφαλίζοντας ότι το μήνυμά της οργάνωσης παραμένει προσβάσιμο παρά τις προσπάθειες καταστολής από τις πλατφόρμες κοινωνικής δικτύωσης.¹²⁷ Σύμφωνα με το Συμβούλιο Ασφαλείας του ΟΗΕ, η χρήση τεχνολογιών αιχμής από το ISIS διευκολύνει τη στρατολόγηση και τη χρηματοδότηση μέσω ανώνυμων καναλιών.¹²⁸

Η ενσωμάτωση της Παραγωγικής Τεχνητής Νοημοσύνης (GenAI) αναμένεται να αναζωογονήσει την προπαγανδιστική μηχανή της οργάνωσης, επιτρέποντας τη δημιουργία εξαιρετικά ρεαλιστικού περιεχομένου με ελάχιστους πόρους.¹²⁹ Η δυνατότητα παραγωγής "deepfakes" και αυτόματων μεταφράσεων σε δεκάδες γλώσσες ενισχύει την ικανότητα του ISIS να διεισδύει σε τοπικές κοινωνίες και να ριζοσπαστικοποιεί άτομα σε παγκόσμια κλίμακα.¹³⁰ Αυτή η ψηφιακή ανθεκτικότητα υπογραμμίζει την ανάγκη για ένα νέο πλαίσιο στο

¹²⁴ European Union Terrorism Situation and Trend Report (2023). *ubi supra*, p. 15 §4

¹²⁵ Kapsokoli, E. (2023). ISIS's Digital Jihad. *National Security and the Future*, 24(3), 39-66, p. 40 § 1. <https://nsf-journal.hr/NSF-Volumes/Focus/id/1486>

¹²⁶ Kapsokoli, E. (2019). The transformation of Islamic terrorism through cyberspace: the case of ISIS. *Proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS 2019*, 677-684, p. 678 §3. https://www.academia.edu/40088253/The_Transformation_of_Islamic_Terrorism_Through_Cyberspace_The_Case_of_ISIS

¹²⁷ Alrhoun, A., Winter, C., & Kertesz, J. (2023). Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem. *Terrorism and Political Violence*, 36(4), 409-424, p. 410 § 2. <https://www.tandfonline.com/doi/pdf/10.1080/09546553.2023.2169142>

¹²⁸ UN Security Council. (2024). Letter dated 19 July 2024 from the Chair of the Security Council Committee (S/2024/556). United Nations, p. 8 § 24. <https://www.google.com/search?q=https://undocs.org/pdf%3Fsymbol%3Den/S/2024/556>

¹²⁹ Criezis, M. (2024). AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI. *Global Network on Extremism & Technology*, p. 2 §4 <https://www.google.com/search?q=https://gnet-research.org/wp-content/uploads/2024/02/AI-Caliphate-Pro-Islamic-State-Propaganda-and-Generative-AI.pdf>

¹³⁰ Nelu, C. (2024). Exploitation of Generative AI by Terrorist Groups. *International Centre for Counter-Terrorism*, p. 4 § 2. <https://www.google.com/search?q=https://www.icct.nl/sites/default/files/2024-06/Exploitation-of-Generative-AI-by-Terrorist-Groups.pdf>

Διεθνές Δίκαιο, καθώς οι πράξεις που τελούνται στον κυβερνοχώρο έχουν άμεσα αποτελέσματα στον φυσικό κόσμο.¹³¹ Η διεθνής κοινότητα αντιμετωπίζει πλέον μια «διάχυτη» απειλή, όπου η έλλειψη κεντρικής διοίκησης αντικαθίσταται από αλγοριθμική καθοδήγηση (Europol, 2024, σελ. 22, παρ. 1).¹³²

3.6.2. Hezbollah (Χεζμπολάχ): Το Πρότυπο του «Υβριδικού Δρώντα» (Hybrid Actor)

Η περίπτωση της Χεζμπολάχ αποτελεί την επιτομή του «Υβριδικού Δρώντα», καθώς συνδυάζει χαρακτηριστικά πολιτικού κόμματος, κοινωνικού φορέα και παραστρατιωτικής οργάνωσης με κυβερνο - δυνατότητες κρατικού επιπέδου.¹³³ Ως βασικός "proxy" (δια αντιπροσώπου) δρών του Ιράν, η οργάνωση επωφελείται από μια συνεχή μεταφορά τεχνογνωσίας, η οποία πλέον επεκτείνεται στον τομέα της Τεχνητής Νοημοσύνης και των αυτόνομων συστημάτων.¹³⁴ Αυτή η τεχνολογική αναβάθμιση επιτρέπει στη Χεζμπολάχ να διεξάγει σύνθετες επιχειρήσεις στον κυβερνοχώρο, οι οποίες αμφισβητούν τα παραδοσιακά σύνορα μεταξύ κρατικής και μη κρατικής βίας.¹³⁵ Από νομική άποψη, η στενή επιχειρησιακή διασύνδεση με το Ιράν εγείρει κρίσιμα ζητήματα έμμεσης κρατικής ευθύνης, ειδικά όταν οι κυβερνοεπιθέσεις της οργάνωσης προκαλούν ζημιές σε υποδομές τρίτων κρατών.¹³⁶

Η χρήση της Τεχνητής Νοημοσύνης από τη Χεζμπολάχ δεν περιορίζεται μόνο στην προπαγάνδα, αλλά επεκτείνεται στη συλλογή πληροφοριών και τη βελτιστοποίηση της στόχευσης στο πεδίο των μαχών.¹³⁷ Η ικανότητα της οργάνωσης να ενσωματώνει AI

¹³¹ Καποκόλη, Ε. (2025). Η χρήση του κυβερνοχώρου από τους τρομοκράτες: η περίπτωση του ISIS. Στο Α. Λιαρόπουλος & Α. Μποζίνης (Επιμ.), Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις (σελ. 211-234). Εκδόσεις Παπαζήση, p. 215.

¹³² uropol. (2024). EU Terrorism Situation and Trend Report (EU TESAT) 2024. Publications Office of the European Union, p. 22 § 1. <https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf>

¹³³ Kapsokoli, E. (2023). Cyberterrorism: A New Wave of Terrorism or Not. In M. A. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (Eds.), Hybrid Threats, Cyberterrorism, and Cyberwarfare (1st ed., pp. 57-80). Routledge, p. 62 §2. <https://www.google.com/search?q=https://www.taylorfrancis.com/books/edit/10.1201/9781003314721/hybrid-threats-cyberterrorism-cyberwarfare>

¹³⁴ Kapsokoli, E. (2025). Cybersecurity in the Western Balkans: is the 'Brussels Effect' in play? In F. Asderaki et al. (Eds.), ESDC Autumn University Book 2021. The Common Security and Defence Policy (pp. 132-143). Publications Office of the European Union, p. 135 §4. <https://www.google.com/search?q=https://op.europa.eu/en/publication-detail/-/publication/27a93540-8774-11ef-a704-01aa75ed71a1>

¹³⁵ Europol. (2023). European Union Terrorism Situation and Trend Report 2023 (TE-SAT), p. 28 § 3.

¹³⁶ UN Security Council. (2024). Letter dated 19 July 2024 (S/2024/556), p. 14 § 42. <https://undocs.org/pdf?symbol=en/S/2024/556>

¹³⁷ Muhanad, S. (2025). Veiled Intentions: Hamas's Strategic Deception and Intelligence Success on 7 October 2023. Intelligence and National Security, 1-28, p. 15 § 2.

αλγορίθμους σε drones και συστήματα επιτήρησης δημιουργεί μια νέα μορφή «ψηφιακής αποτροπής» έναντι κρατικών αντιπάλων.¹³⁸ Σύμφωνα με το Διεθνές Δίκαιο, η παροχή τέτοιων προηγμένων εργαλείων από ένα κράτος σε μια ένοπλη ομάδα μπορεί να στοιχειοθετήσει παραβίαση της αρχής της μη επέμβασης και της απαγόρευσης χρήσης βίας.¹³⁹ Καθώς η Χεζμπολάχ εξελίσσεται σε έναν «τεχνολογικά αυτόνομο» δρώντα, η διεθνής κοινότητα καλείται να επαναπροσδιορίσει τα κριτήρια της «συνενοχής» (complicity) των κρατών-υποστηρικτών στην ψηφιακή εποχή.¹⁴⁰

4. ΚΕΦΑΛΑΙΟ: ΑΠΟΔΟΣΗ ΕΥΘΥΝΗΣ ΣΤΟ ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ: ΤΟ TALLINN MANUAL ΚΑΙ Η ΤΝ

4.1. Κρατική ευθύνη στο διεθνές δίκαιο - Θεμελιώδεις Αρχές και Τεχνολογική Ουδετερότητα

Η θεμελίωση της διεθνούς ευθύνης για πράξεις που τελούνται με τη χρήση προηγμένων ψηφιακών μέσων, όπως η Παραγωγική Τεχνητή Νοημοσύνη (Generative AI), δεν απαιτεί την επινόηση νέων νομικών κανόνων, αλλά την ορθή εφαρμογή των υφιστάμενων αρχών του εθιμικού διεθνούς δικαίου. Ο ακρογωνιαίος λίθος της νομικής αυτής κατασκευής εντοπίζεται στα «Άρθρα για την Ευθύνη των Κρατών για Διεθνώς Άδικες Πράξεις» (ARSIWA) της Επιτροπής Διεθνούς Δικαίου (ILC) του 2001, και αυτά όπως ενσωματώθηκαν στην απόφαση της Γενικής Συνέλευσης με την απόφαση A/56/83, τα οποία κωδικοποιούν το εθιμικό δίκαιο.¹⁴¹ Σύμφωνα με το Άρθρο 1, κάθε διεθνώς άδικη πράξη ενός κράτους συνεπάγεται τη διεθνή

<https://www.google.com/search?q=https://www.tandfonline.com/doi/pdf/10.1080/02684527.2024.2443478>

¹³⁸ Warrick, J. (2017, February 21). Use of Weaponized Drones by ISIS Spurs Terrorism Fears. Washington Post, p. 3 § 5. https://www.google.com/search?q=https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/93ad0432-f851-11e6-aa1e-5f735ee31334_story.html

¹³⁹ United Nations Office of Counter-Terrorism. (2021). *ubi supra*, p. 34 § 1.

¹⁴⁰ Kapsokoli, E. (2022). The challenge of defining cyberterrorism within the EU. In F. Asderaki et al. (Eds.), *Challenges of the common security and defence policy* (pp. 183-196). Publications Office of the European Union, p. 188 § 2. <https://www.google.com/search?q=https://op.europa.eu/en/publication-detail/-/publication/e3706908-db0f-11ec-a95f-01aa75ed71a1>

¹⁴¹ A/RES/56/83, *ubi supra*, n. 10, *ubi supra*, art. 1 § 1.

ευθύνη του, μια αρχή που εφαρμόζεται καθολικά ανεξαρτήτως των μέσων που χρησιμοποιήθηκαν για την τέλεση της πράξης.¹⁴²

Για να στοιχειοθετηθεί, ωστόσο, μια τέτοια ευθύνη στο περιβάλλον των νέων τεχνολογιών, πρέπει να πληρούνται σωρευτικά οι δύο προϋποθέσεις που ορίζει το Άρθρο 2 των ARSIWA: α) η συμπεριφορά (πράξη ή παράλειψη) να μπορεί να αποδοθεί στο κράτος (attribution) και β) η συμπεριφορά αυτή να συνιστά παραβίαση διεθνούς υποχρέωσης του κράτους.¹⁴³ Η πρόκληση που εισάγει η Τεχνητή Νοημοσύνη δεν αφορά το δεύτερο σκέλος (την παραβίαση), αλλά κυρίως το πρώτο, δηλαδή τον νομικό σύνδεσμο μεταξύ του φυσικού αυτουργού (ή του αλγορίθμου) και του κράτους.¹⁴⁴ Το Διεθνές Δικαστήριο της Χάγης (ICJ) έχει επιβεβαιώσει διαχρονικά την αρχή της «τεχνολογικής ουδετερότητας», κρίνοντας στη Γνωμοδότηση για τα Πυρηνικά Όπλα (1996) ότι οι κανόνες του διεθνούς δικαίου εφαρμόζονται σε όλες τις μορφές πολέμου και σε όλα τα όπλα, ακόμη και σε αυτά που δεν είχαν εφευρεθεί όταν θεσπίστηκαν οι κανόνες.¹⁴⁵

Συνεπώς, η χρήση της GenAI από τρομοκρατικές ομάδες ή κρατικούς δρώντες δεν συνιστά νομικό κενό, αλλά ενεργοποιεί τους κανόνες απόδοσης ευθύνης για τη δράση κρατικών οργάνων ή ιδιωτών που ενεργούν υπό κρατικό έλεγχο. Σύμφωνα με το Άρθρο 4 των ARSIWA, οι πράξεις οποιουδήποτε κρατικού οργάνου, μεταξύ των οποίων είναι οι κυβερνο-μονάδες στρατού ή υπηρεσίες πληροφοριών που χειρίζονται εργαλεία AI, θεωρούνται αυτοδικαίως πράξεις του κράτους.¹⁴⁶ Το ζήτημα καθίσταται πιο σύνθετο όταν η χρήση της τεχνολογίας γίνεται από μη κρατικούς δρώντες, όπως τρομοκρατικές οργανώσεις. Σε αυτή την περίπτωση, όπως ορίζει το Άρθρο 8, η συμπεριφορά αποδίδεται στο κράτος μόνο εάν το άτομο ή η ομάδα ενεργεί υπό τη διεύθυνση ή τον έλεγχο του κράτους.¹⁴⁷

Η νομολογία έχει θέσει υψηλά τον πήχη για την απόδειξη αυτού του «ελέγχου», προστατεύοντας τα κράτη από την εύκολη απόδοση ευθύνης για πράξεις τρίτων. Το κριτήριο του «αποτελεσματικού ελέγχου» (effective control), όπως καθιερώθηκε στην υπόθεση Nicaragua (1986), απαιτεί απόδειξη ότι το κράτος είχε τον έλεγχο επί της συγκεκριμένης επιχειρησιακής πράξης και όχι απλώς ότι παρείχε γενική υποστήριξη ή εξοπλισμό.¹⁴⁸

¹⁴² Ibid, Art. 1.

¹⁴³ Ibid, Art. 2.

¹⁴⁴ Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0*. ubi supra, p. 84, § 15.

¹⁴⁵ International Court of Justice (ICJ). (1996). *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion, I.C.J. Reports 1996, p. 259 § 86. <https://api.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>

¹⁴⁶ A/RES/56/83, ubi supra, n. 10, ubi supra, Art. 4.

¹⁴⁷ Ibid, Art. 8.

¹⁴⁸ *Nicaragua case*. ubi supra, p. 65 § 115.

Στην εποχή της Τεχνητής Νοημοσύνης, αυτό μετατρέπεται στο ερώτημα: ελέγχει το κράτος τον συγκεκριμένο αλγόριθμο ή την κυβερνοεπίθεση τη στιγμή της εκδήλωσής της; Η Ομάδα Εμπειρογνομόνων του ΟΗΕ (UN GGE) έχει ρητά τονίσει ότι οι κατηγορίες για οργάνωση και εκτέλεση άδικων πράξεων μέσω ΤΠΕ πρέπει να τεκμηριώνονται και να μην αποδίδονται σε ένα κράτος απλώς και μόνο επειδή η δραστηριότητα προέρχεται από την επικράτειά του ή τις υποδομές του.¹⁴⁹

4.2. Tallinn Manual 1.0 & 2.0

4.2.1. Το Tallinn Manual ως Ερμηνευτικό Πρότυπο: Κωδικοποίηση του Εθιμικού Δικαίου και η Πρόκληση της Κυβερνο-Απόδοσης

Η κανονιστική πρόκληση που θέτει η κυβερνοτρομοκρατία δεν έγκειται στην απουσία κανόνων, αλλά στην ερμηνευτική προσαρμογή των υφιστάμενων αρχών του διεθνούς δικαίου στο άυλο και τεχνικά περίπλοκο περιβάλλον του κυβερνοχώρου.¹⁵⁰ Το Tallinn Manual, στην αρχική του έκδοση (2013) και κυρίως στην αναθεωρημένη έκδοση 2.0 (2017), δεν συνιστά δεσμευτική διεθνή συνθήκη, αλλά αποτελεί τη σημαντικότερη μέχρι σήμερα προσπάθεια κωδικοποίησης του εθιμικού διεθνούς δικαίου (*lex lata*) από ακαδημαϊκή ομάδα εμπειρογνομόνων υπό την αιγίδα του NATO.¹⁵¹ Η αξία του έγκειται στο γεγονός ότι μεταφράζει τις αναλογικές έννοιες της «φυσικής βίας» και της «εδαφικής κυριαρχίας» σε ψηφιακά ισοδύναμα, παρέχοντας τον αναγκαίο οδικό χάρτη για την εφαρμογή των κανόνων της κρατικής ευθύνης.¹⁵²

Στον πυρήνα της ανάλυσης του Tallinn Manual βρίσκεται το ζήτημα της απόδοσης ευθύνης (*attribution*). Οι συντάκτες του εγχειριδίου, ακολουθώντας πιστά τη νομολογία του Διεθνούς Δικαστηρίου της Χάγης (ICJ), διακρίνουν αυστηρά μεταξύ πράξεων κρατικών

¹⁴⁹ United Nations General Assembly. (2015). *ubi supra*, p. 13 §8 (f).

¹⁵⁰ Schmitt, M. N., & Vihul, L. (2014). The Nature of International Law Cyber Norms. Tallinn Paper No. 5, NATO CCDCOE, p. 12. <https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf>

¹⁵¹ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0. *ubi supra*, p. 3.

¹⁵² Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law*, 112(4), p. 586. <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/54FBA2B30081B53353B5D2F06F778C14/S0002930018000866a.pdf/a-rule-book-on-the-shelf-tallinn-manual-20-on-cyberoperations-and-subsequent-state-practice.pdf>

οργάνων και πράξεων μη κρατικών δρώντων.¹⁵³ Σύμφωνα με τον Κανόνα 15 (Rule 15), κυβερνοεπιχειρήσεις που διεξάγονται από όργανα του κράτους – όπως οι υπηρεσίες πληροφοριών, οι στρατιωτικές διοικήσεις κυβερνοπολέμου (Cyber Commands) ή άλλες κυβερνητικές υπηρεσίες – αποδίδονται αυτοδικαίως στο κράτος.¹⁵⁴ Η νομική αυτή παραδοχή είναι απόλυτη και δεν κάμπτεται ακόμη και στην περίπτωση που το όργανο ενήργησε καθ' υπέρβαση εξουσίας (*ultra vires*), εφόσον δρούσε υπό την επίσημη ιδιότητά του, όπως ρητά ορίζει το άρθρο 7 των ARSIWA.¹⁵⁵

Ωστόσο, η πολυπλοκότητα αυξάνεται εκθετικά όταν εξετάζεται η δράση «ιδιωτών» χάκερ ή τρομοκρατικών ομάδων που λειτουργούν ως πληρεξούσιοι (*proxies*). Ο Κανόνας 17 (Rule 17) του Tallinn Manual 2.0 υιοθετεί το κριτήριο του «αποτελεσματικού ελέγχου» (*effective control*), όπως αυτό καθιερώθηκε στην υπόθεση *Nicaragua v. United States* (1986).¹⁵⁶ Σύμφωνα με την ερμηνεία αυτή, για να αποδοθεί η κυβερνοεπίθεση μιας τρομοκρατικής ομάδας σε ένα κράτος-χορηγό, δεν αρκεί η απόδειξη γενικής χρηματοδότησης, παροχής εξοπλισμού (*hardware/software*) ή εκπαίδευσης.¹⁵⁷ Απαιτείται η απόδειξη ότι το κράτος εξέδωσε συγκεκριμένες εντολές (*issued specific instructions*) ή ασκούσε επιχειρησιακό έλεγχο επί της συγκεκριμένης ψηφιακής ενέργειας τη στιγμή που αυτή εκδηλωνόταν.¹⁵⁸ Η ακαδημαϊκή κριτική επί της θέσης αυτής είναι έντονη. Υποστηρίζεται ότι η άκαμπτη εφαρμογή του κριτηρίου «Case Nicaragua» στον κυβερνοχώρο δημιουργεί ένα «κενό λογοδοσίας» (*accountability gap*), καθώς η τεχνική φύση των κυβερνοεπιθέσεων επιτρέπει στα κράτη να κατευθύνουν τους δρώντες μέσω αλγορίθμων και ανώνυμων δικτύων, καθιστώντας την απόδειξη των «συγκεκριμένων οδηγιών» πρακτικά αδύνατη.¹⁵⁹ Παρ' όλα αυτά, το Διεθνές Δικαστήριο, στην απόφασή του για τη Γενοκτονία στη Βοσνία (2007)¹⁶⁰, απέρριψε ρητά το ελαστικότερο κριτήριο του «συνολικού ελέγχου» (*overall*

¹⁵³ A/RES/56/83, *ubi supra*, n. 10, *ubi supra*, Art. 4 & 8.

¹⁵⁴ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0, *ubi supra*, Rule 15, σελ. 87.

¹⁵⁵ A/RES/56/83, *ubi supra*, n. 10, *ubi supra*, Art. 8.

¹⁵⁶ *Nicaragua case*. *ubi supra*, p. 65 § 115.

¹⁵⁷ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0, *ubi supra*, Rule 17 § 8, σελ. 96.

¹⁵⁸ Healey, J. (2011). Beyond Attribution: Seeking National Responsibility for Cyber Attacks. Atlantic Council Issue Brief, p. 2. https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF

¹⁵⁹ Shackelford, S. J., & Andres, R. B. (2011). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Georgetown Journal of International Law, 42, 971-1016. https://heinonline.org/HOL/Page?handle=hein.journals/geojintl42&div=35&g_sent=1&casa_token=&collection=journals

¹⁶⁰ International Court of Justice (ICJ). (2007). Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzegovina v. Serbia and Montenegro*). Judgment of 26 February 2007, I.C.J. Reports 2007, p. 171 § 406. <https://www.acerislaw.com/wp-content/uploads/2024/04/Application-of-the-Convention-on-the-Prevention-and-Punishment-of-the-Crime-of-Genocide.pdf>

control) που είχε προτείνει το ICTY στην υπόθεση Tadić¹⁶¹, επιβεβαιώνοντας ότι το διεθνές δίκαιο απαιτεί υψηλό βαθμό απόδειξης για την απόδοση ευθύνης σε κράτη για πράξεις ιδιωτών.

4.2.2. Η Μετάβαση από το Tallinn 1.0 στο Tallinn 2.0: Η Διεύρυνση της Κρατικής Ευθύνης

Η μετάβαση από την πρώτη έκδοση του Tallinn Manual (2013) στη δεύτερη (2017) σηματοδοτεί μια θεμελιώδη δογματική στροφή στην κατανόηση της κυβερνο-απειλής, η οποία είναι κρίσιμη για τη νομική αξιολόγηση της σύγχρονης τρομοκρατίας. Ενώ το Tallinn 1.0 περιορίστηκε αποκλειστικά στο Δίκαιο των Ενόπλων Συρράξεων (*jus in bello*) και στο Δίκαιο Προσφυγής στη Βία (*jus ad bellum*), εξετάζοντας κυρίως πότε μια κυβερνοεπίθεση ισοδυναμεί με «ένοπλη επίθεση», η πρακτική κατέδειξε ότι η πλειονότητα των εχθρικών ενεργειών παραμένει κάτω από αυτό το υψηλό κατώφλι.¹⁶² Τρομοκρατικές οργανώσεις και κρατικοί δρώντες σπανίως εξαπολύουν «ψηφιακό Pearl Harbor», προτιμώντας υβριδικές τακτικές χαμηλής έντασης που προκαλούν δυσλειτουργία χωρίς φυσική καταστροφή.¹⁶³

Η έκδοση 2.0 ήρθε να καλύψει αυτό το ρυθμιστικό κενό, εισάγοντας ένα ολοκληρωμένο πλαίσιο για το Διεθνές Δίκαιο που εφαρμόζεται σε καιρό ειρήνης (International Law Applicable to Cyber Operations). Η σημαντικότερη νομική καινοτομία αυτής της μετάβασης αφορά τη νομική φύση της Κρατικής Κυριαρχίας. Στο Tallinn 1.0, η κυριαρχία αντιμετωπιζόταν κυρίως ως αρχή που διέπει τη δικαιοδοσία. Αντίθετα, στο Tallinn 2.0, η Διεθνής Ομάδα Εμπειρογνομόνων (IGE) – αν και με διαφωνίες – κατέληξε κατά πλειοψηφία στη θέση ότι η Κυριαρχία αποτελεί πρωτογενή κανόνα του διεθνούς δικαίου (*primary rule*) και όχι απλώς «αρχή».¹⁶⁴

Σύμφωνα με τον Κανόνα 4 (Rule 4), ένα κράτος (ή μη κρατικός δρών που ενεργεί υπό τον έλεγχό του) παραβιάζει το διεθνές δίκαιο όταν διεξάγει κυβερνοεπιχειρήσεις που, αν και δεν προκαλούν φυσική βλάβη, παρεμβαίνουν στις εγγενείς κυβερνητικές λειτουργίες (*inherent*

¹⁶¹ International Criminal Tribunal for the former Yugoslavia (ICTY). (1999). *Prosecutor v. Duško Tadić*. Judgment of 15 July 1999, Case No. IT-94-1-A (Appeals Chamber). <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>

¹⁶² Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and insights. *Georgetown Journal of International Law*, 48(3), p. 732. <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>

¹⁶³ Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies (CSIS), p. 8. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

¹⁶⁴ Schmitt, M. N., & Vihul, L. (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, 95, p. 1641-1649. https://texaslawreview.org/wp-content/uploads/2017/11/Schmitt.Vihul_.pdf

governmental functions) άλλου κράτους ή σφετερίζονται τον έλεγχο των κυβερνο-υποδομών του.¹⁶⁵ Η διάκριση αυτή είναι κεφαλαιώδους σημασίας για την αντιμετώπιση της «ΑΙ-υποβοηθούμενης τρομοκρατίας». Όταν, για παράδειγμα, μια τρομοκρατική οργάνωση χρησιμοποιεί αλγορίθμους για να αλλοιώσει εκλογικούς καταλόγους ή να παραλύσει ψηφιακά ένα κρατικό σύστημα φορολογίας, χωρίς να προκαλέσει θανάτους, η πράξη αυτή βάσει του Tallinn 1.0 θα βρισκόταν σε νομικό κενό. Βάσει του Tallinn 2.0, όμως, συνιστά παραβίαση εθνικής κυριαρχίας, επιτρέποντας στο θιγόμενο κράτος να λάβει νομικά αντίμετρα (countermeasures), ακόμη και εν καιρώ ειρήνης.¹⁶⁶

Ωστόσο, πρέπει να επισημανθεί ότι η άποψη περί «κυριαρχίας ως κανόνα» έχει αμφισβητηθεί έντονα από κράτη όπως το Ηνωμένο Βασίλειο, τα οποία υποστηρίζουν ότι η παραβίαση κυριαρχίας από μόνη της δεν γεννά διεθνή ευθύνη, εκτός αν συνοδεύεται από απαγορευμένη επέμβαση (prohibited intervention).¹⁶⁷ Το Tallinn 2.0 επιχειρεί να γεφυρώσει αυτή τη διαφορά, θέτοντας ως κριτήριο παραβίασης της αρχής της μη επέμβασης (Κανόνας 66) το στοιχείο του εξαναγκασμού (coercion). Συνεπώς, η χρήση Τεχνητής Νοημοσύνης από τρομοκράτες εμπίπτει στο απαγορευτικό πεδίο του διεθνούς δικαίου όταν στοχεύει να εξαναγκάσει ένα κράτος σε πράξη ή παράλειψη, αφαιρώντας του τη δυνατότητα κυρίαρχης επιλογής.¹⁶⁸ Αυτή η λεπτή νομική διάκριση καθιστά το Tallinn 2.0 απαραίτητο εργαλείο για την αξιολόγηση ψυχολογικών επιχειρήσεων και εκστρατειών παραπληροφόρησης (cognitive warfare) που δεν περιλαμβάνουν κινητική βία.

4.2.3. Η Υποχρέωση Δέουσας Επιμέλειας (Due Diligence): Το «Ανάχωμα» στην Ατιμωρησία

Αναγνωρίζοντας το αδιέξοδο που συχνά δημιουργεί η δυσκολία του attribution, το Tallinn Manual 2.0 μετατοπίζει το νομικό βάρος από την «πράξη» στην «πρόληψη», μέσω της θεωρίας της δέουσας επιμέλειας (due diligence). Οι Κανόνες 6 και 7 (Rules 6 & 7) θεμελιώνουν την υποχρέωση κάθε κράτους να μην επιτρέπει εν γνώσει του (knowingly) τη χρήση της επικράτειάς του – συμπεριλαμβανομένων των ψηφιακών υποδομών, όπως servers και δίκτυα

¹⁶⁵ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0, ubi supra, p. 17, Rule 4.

¹⁶⁶ Schmitt, M. N. (2017). Grey Zones in the International Law of Cyberspace. The Yale Journal of International Law Online, 42(2), p. 6-7. <https://yjil.yale.edu/posts/2017-05-08-grey-zones-in-the-international-law-of-cyberspace>

¹⁶⁷ Attorney General's Office (UK). (2018). Cyber and International Law in the 21st Century. Speech by the Attorney General Jeremy Wright QC MP. <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>

¹⁶⁸ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0, ubi supra, p. 312, Rule 66.

οπτικών ινών – για τη διενέργεια πράξεων που βλάπτουν τα δικαιώματα άλλων κρατών.¹⁶⁹ Αφετηρία αυτής της αρχής η απόφαση Corfu Channel (1949), όπου το Δικαστήριο έκρινε ότι η Αλβανία είχε ευθύνη όχι επειδή η ίδια τοποθέτησε τις νάρκες, αλλά επειδή γνώριζε την ύπαρξή τους και δεν προειδοποίησε τα διερχόμενα πλοία.¹⁷⁰

Στο πλαίσιο της Τεχνητής Νοημοσύνης και της τρομοκρατίας, η εφαρμογή του κανόνα αυτού αποκτά νέα δυναμική. Όπως αναλύει ο Schmitt (2015), η υποχρέωση δέουσας επιμέλειας στον κυβερνοχώρο είναι υποχρέωση συμπεριφοράς (obligation of conduct) και όχι υποχρέωση αποτελέσματος (obligation of result).¹⁷¹ Αυτό σημαίνει ότι το κράτος δεν είναι υποχρεωμένο να αποτρέψει κάθε επίθεση, αλλά οφείλει να χρησιμοποιήσει «όλα τα εφικτά μέσα» (all feasible measures) για να τερματίσει μια κακόβουλη δραστηριότητα μόλις λάβει γνώση αυτής.¹⁷² Το κρίσιμο νομικό ζήτημα εδώ είναι το «πρότυπο γνώσης» (standard of knowledge). Η θεωρία διακρίνει μεταξύ της «πραγματικής γνώσης» (actual knowledge) και της «εποικοδομητικής γνώσης» (constructive knowledge). Ενώ το Tallinn Manual είναι επιφυλακτικό ως προς την επιβολή μιας γενικής υποχρέωσης παρακολούθησης του διαδικτύου, η οποία θα μπορούσε να προσκρούσει στα ανθρώπινα δικαιώματα, όμως μερίδα της ακαδημαϊκής κοινότητας συγκλίνει στην άποψη ότι όταν ένα κράτος ενημερωθεί αξιόπιστα για τη χρήση των υποδομών του από τρομοκράτες, η αδράνεια συνιστά παραβίαση του διεθνούς δικαίου.¹⁷³ Συνεπώς, η δέουσα επιμέλεια λειτουργεί ως η «εφεδρική δικλείδα ασφαλείας» του διεθνούς συστήματος: ακόμη και αν δεν μπορεί να αποδειχθεί ότι το κράτος διέταξε την επίθεση (attribution), μπορεί να θεμελιωθεί ευθύνη επειδή επέτρεψε την εκδήλωσή της μέσω της εδαφικής του κυριαρχίας.¹⁷⁴

4.3. AI-enabled πράξεις και attribution: Η πρόκληση της «Αλγοριθμικής Αυτονομίας»

Η μετάβαση από τις συμβατικές κυβερνοεπιχειρήσεις στην εποχή της «AI-υποβοηθούμενης τρομοκρατίας» (AI-enabled terrorism) θέτει σε δοκιμασία τα παραδοσιακά κριτήρια απόδοσης ευθύνης (attribution), καθώς εισάγει τον παράγοντα της «λειτουργικής

¹⁶⁹ Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0*, ubi supra, p. 30 Rule 6 & 7.

¹⁷⁰ Corfu Channel case (1949). ubi supra, p. 22.

¹⁷¹ Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum*, 125, p. 72. https://yalelawjournal.org/pdf/Schmitt_PDF_g9pv96jc.pdf

¹⁷² Koivurova, T. & Singh K. (2012). Due Diligence. *Oxford Public International Law*, § 23. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1034?print=pdf>

¹⁷³ Buchan, R. (2016). Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm. *Journal of Conflict and Security Law*, 21(3), p. 4-5. <https://eprints.whiterose.ac.uk/id/eprint/103386/1/Buchan%20FINAL%20Cyberspace.pdf>

¹⁷⁴ United Nations General Assembly. (2015). A/70/174, ubi supra, p. 8 § 13 (c).

αυτονομίας» (functional autonomy) στη νομική εξίσωση. Ενώ στα παραδοσιακά κυβερνο-όπλα υπάρχει μια γραμμική σχέση αιτίου-αποτελέσματος μεταξύ της εντολής του χειριστή και του ψηφιακού αποτελέσματος, τα συστήματα Παραγωγικής Τεχνητής Νοημοσύνης, λόγω της ιδιότητάς τους να μαθαίνουν και να προσαρμόζονται (machine learning), δύνανται να παράγουν επιβλαβείς εξόδους (outputs) που ούτε είχαν προγραμματιστεί ρητά ούτε είχαν προβλεφθεί από το κράτος-σχεδιαστή.¹⁷⁵ Αυτό το χαρακτηριστικό, γνωστό στη βιβλιογραφία ως το πρόβλημα του «μαύρου κουτιού» (black box problem), δημιουργεί τον κίνδυνο ενός «κενού λογοδοσίας» (accountability gap),¹⁷⁶ καθώς ένα κράτος θα μπορούσε θεωρητικά να αρνηθεί την ευθύνη για μια τρομοκρατική ενέργεια που διευκολύνθηκε από δικό του αλγόριθμο, ισχυριζόμενο ότι η συγκεκριμένη ενέργεια ήταν αποτέλεσμα «απρόβλεπτης παρέκκλισης» του συστήματος και όχι κρατικής εντολής.¹⁷⁷ Ωστόσο, η διεθνής νομική θεωρία απαντά πως το δίκαιο δεν καταρρέει μπροστά στην τεχνολογία, καθώς η ευθύνη δεν εδράζεται αποκλειστικά στον έλεγχο της τελικής πράξης, αλλά μετατοπίζεται στην αρχική απόφαση της ενεργοποίησης και ανάπτυξης (deployment) ενός αυτόνομου συστήματος σε μη ελεγχόμενο περιβάλλον.¹⁷⁸

Εξειδικεύοντας το κριτήριο των «οδηγιών» (instructions) στο περιβάλλον της Παραγωγικής ΤΝ, η νομική ανάλυση βασίζεται στο Άρθρο 8 των Άρθρων περί Κρατικής Ευθύνης, όπως αυτά υιοθετήθηκαν από τη Γενική Συνέλευση του ΟΗΕ με την Απόφαση 56/83.¹⁷⁹ Σύμφωνα με τη διάταξη αυτή, η συμπεριφορά ενός προσώπου ή οντότητας αποδίδεται στο κράτος εάν ενεργεί κατόπιν οδηγιών του. Στην περίπτωση των συστημάτων GenAI, η εισαγωγή των παραμέτρων και των εντολών (prompts) από τον κρατικό χειριστή συνιστά τη νομική ισοδυναμία της «οδηγίας», καθώς καθορίζει τον επιδιωκόμενο στόχο, λειτουργώντας ως ο «μαγνήτης λογοδοσίας» (accountability attractor) που συνδέει την ανθρώπινη βούληση με

¹⁷⁵ Liivoja, R., & Väljataga, A. (Eds.). (2021). Autonomous Cyber Capabilities under International Law. NATO CCDCOE Publications, p. 5. <https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf>

¹⁷⁶ Sparrow, R. (2007). Killer Robots. *Journal of Applied Philosophy*, 24(1), p. 69-71. <https://eclass.uoa.gr/modules/document/file.php/PHILOSOPHY875/%CE%9C%CE%A0%CE%9F%CE%A5%CE%A4%CE%9B%CE%91%CE%A3%20%CE%9F%CE%A0%CE%9B%CE%91%20%CE%9C%CE%91%CE%96%CE%99%CE%9A%CE%97%CE%A3%20%CE%9A%CE%91%CE%A4%CE%91%CE%A3%CE%A4%CE%A1%CE%9F%CE%A6%CE%97%CE%A3%20%20Killer%20Robots%20Journal%20of%20Applied%20Philosophy%20Volume%2024%20issue%201%202007.pdf> & Chengeta, T. (2016). Accountability Gap, Autonomous Weapon Systems and Modes of Responsibility in International Law. *Denver Journal of International Law and Policy*, 45(1), p. 2. <https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1011&context=djilp>

¹⁷⁷ Liivoja, R., & Väljataga, A. (Eds.). (2021). *ubi supra*, p. 138

¹⁷⁸ Sassòli, M. (2014). Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to Be Clarified. *International Law Studies*, 90, p. 324. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1017&context=ils>

¹⁷⁹ United Nations General Assembly. (2002). A/RES/56/83, *ubi supra*, Art. 8.

το αποτέλεσμα της μηχανής.¹⁸⁰ Αυτή η ερμηνεία γεφυρώνει το αιτιάδες χάσμα, διότι η αυτονομία του συστήματος στα «μέσα» (means) δεν αναιρεί την ανθρώπινη κυριότητα επί του «σκοπού» (ends), διατηρώντας ακέραιο τον σύνδεσμο απόδοσης ευθύνης στο κράτος που έδωσε το αρχικό έναυσμα.¹⁸¹ Συνεπώς, η νομική αξιολόγηση μετατοπίζεται από τον τεχνικό έλεγχο του κώδικα στον έλεγχο της επιχειρησιακής πρόθεσης (mens rea), καθιστώντας το Prompt τεκμήριο κρατικής εντολής.¹⁸²

Μολονότι το νομικό πλαίσιο για την απόδοση ευθύνης υφίσταται, η πρακτική εφαρμογή του προσκρούει στη δυσχέρεια της «τεκμηριωμένης απόδειξης» (evidentiary proof) στο ψηφιακό περιβάλλον. Σε αντίθεση με τις συμβατικές επιθέσεις, η χρήση συστημάτων Τεχνητής Νοημοσύνης παρέχει στα κράτη το στρατηγικό πλεονέκτημα της «εύλογης άρνησης» (plausible deniability), καθώς μπορούν να ισχυριστούν ότι η ζημιογόνος ενέργεια δεν προήλθε από κρατική εντολή, αλλά από αλγοριθμικό σφάλμα του συστήματος.¹⁸³ Αυτό το χαρακτηριστικό καθιστά τον τεχνικό εντοπισμό της αρχικής πηγής εξαιρετικά δύσκολο, αφού η αλυσίδα της εντολής μπορεί να κρυπτογραφηθεί ή να χαθεί μέσα στην πολυπλοκότητα των νευρωνικών δικτύων, καθιστώντας την απόδοση ευθύνης περισσότερο τέχνη πιθανολόγησης παρά θετική επιστήμη.¹⁸⁴ Συνεπώς, ενώ το δίκαιο δεν έχει κενά ως προς την κατανομή της ευθύνης, δημιουργείται ένα de facto «κενό επιβολής» (enforcement gap), το οποίο μπορεί να καλυφθεί μόνο μέσω της ανάπτυξης νέων τεχνικών ψηφιακής εγκληματολογίας (AI forensics) που θα μπορούν να ανιχνεύσουν τα «ψηφιακά ίχνη» του ανθρώπινου χειριστή πίσω από την απόφαση της μηχανής.

4.4. Αυτόνομα συστήματα & ευθύνη

Η πολυπλοκότητα των συστημάτων Παραγωγικής Τεχνητής Νοημοσύνης (GenAI) επιβάλλει την απομάκρυνση από τη μονολιθική αντίληψη της κρατικής ευθύνης και την

¹⁸⁰ Amoroso, D., & Tamburrini, G. (2020). Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. *Current Robotics Reports*, 1, p. 5. <https://www.iris.unina.it/retrieve/e268a732-272c-4c8f-e053-1705fe0a812c/Amoroso%20D%20Tamburrini%20G%20Autonomous%20Weapons%20Systems%20and%20Meaningful%20Human%20Control%20Current%20Robotics%20Reports.pdf>

¹⁸¹ McFarland, T., & McCormack, T. (2014). Mind the Gap: Can Developers of Autonomous Weapons Systems be Liable for War Crimes? *International Law Studies*, p. 363. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1016&context=ils>

¹⁸² Sassòli, M. (2014). *ubi supra*, p. 324.

¹⁸³ Brundage, M. et al. (2018). *ubi supra*, p. 17. <https://arxiv.org/pdf/1802.07228>

¹⁸⁴ Lin, H. (2016). *Attribution of Malicious Cyber Incidents: From Soup to Nuts*. Hoover Institution Working Group on National Security, Technology, and Law, p. 81. https://www.jstor.org/stable/pdf/90012598.pdf?refreqid=fastly-default%3A9022a89aab47f056d4f10e05d4638cba&ab_segments=&initiator=&acceptTC=1

υιοθέτηση μιας λειτουργικής προσέγγισης, όπου η λογοδοσία επιμερίζεται ανάλογα με τον βαθμό ελέγχου και την αιτιώδη συμβολή του κάθε δρώντος. Η πρωταρχική ευθύνη στο διεθνές δίκαιο βαρύνει το «Κράτος Χρήσης» (State of Deployment), δηλαδή το κράτος που λαμβάνει την απόφαση να ενεργοποιήσει και να αναπτύξει ένα σύστημα Τεχνητής Νοημοσύνης σε επιχειρησιακό περιβάλλον. Βάσει του γενικού κανόνα της αντικειμενικής ευθύνης, το κράτος που εντάσσει στο οπλοστάσιό του ένα μέσο, αναλαμβάνει και τον κίνδυνο που απορρέει από τη λειτουργία του.¹⁸⁵ Στην περίπτωση της GenAI, το επιχείρημα ότι το σύστημα ενήργησε «αυτόνομα» ή «απρόβλεπτα» (unpredictably) δεν απαλλάσσει το Κράτος Χρήσης από την ευθύνη του, καθώς η επιλογή χρήσης ενός συστήματος με εγγενή στοχαστική συμπεριφορά σε ευαίσθητες συνθήκες συνιστά από μόνη της ανάληψη κινδύνου. Ειδικότερα, εάν το Κράτος Χρήσης είναι αυτό που τροφοδότησε το σύστημα με τα δεδομένα στόχευσης (prompts) ή καθόρισε τις παραμέτρους της αποστολής, τότε η πράξη του συστήματος του καταλογίζεται πλήρως βάσει του Άρθρου 4 ή του Άρθρου 8 του Παραρτήματος της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ. Όπως επισημαίνει ο Sassòli, η ευθύνη δεν εξαφανίζεται επειδή το όπλο είναι «έξυπνο»: το κράτος που αποφασίζει να χρησιμοποιήσει ένα εργαλείο του οποίου τις αντιδράσεις δεν μπορεί να προβλέψει πλήρως, ευθύνεται για τις συνέπειες της αμέλειάς του να ελέγξει το μέσο που επέλεξε.¹⁸⁶

Πέραν του κράτους που χρησιμοποιεί την τεχνολογία, ένα πιο σύνθετο νομικό ζήτημα ανακύπτει αναφορικά με την ευθύνη του «Κράτους Ανάπτυξης» (State of Development), στην επικράτεια του οποίου σχεδιάστηκε ο αλγόριθμος. Κατά κανόνα, το διεθνές δίκαιο δεν αναγνωρίζει «ευθύνη προϊόντος» (product liability), επομένως το γεγονός ότι ένας αλγόριθμος κατασκευάστηκε σε ένα κράτος δεν το καθιστά αυτομάτως υπεύθυνο για την παράνομη χρήση του από τρίτους.¹⁸⁷ Ωστόσο, η αρχή αυτή κάμπτεται υπό το πρίσμα της υποχρέωσης δέουσας επιμέλειας (due diligence) και της πρόληψης διάδοσης όπλων διττής χρήσης. Το Κράτος Ανάπτυξης έχει τη θετική υποχρέωση να διασφαλίσει ότι τα συστήματα GenAI που παράγονται στην επικράτειά του διαθέτουν ενσωματωμένες δικλείδες ασφαλείας («safety by design»), ώστε να μην μπορούν να μετατραπούν εύκολα σε κυβερνο-όπλα.¹⁸⁸ Εάν το Κράτος Ανάπτυξης γνωρίζει ότι μια τεχνολογία έχει σοβαρά κενά ασφαλείας και παρ' όλα αυτά επιτρέπει την

¹⁸⁵ Sassòli, M. (2014). *ubi supra*, p. 324.

¹⁸⁶ Sassòli, M. (2014). *Ibid*, p. 326.

¹⁸⁷ McFarland, T., & McCormack, T. (2014). Mind the Gap: Can Developers of Autonomous Weapons Systems be Liable for War Crimes? *International Law Studies*, p. 363. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1016&context=ils>

¹⁸⁸ Pauwels, E. (2022). Safeguarding against the misuse and abuse of artificial intelligence, *Global Center on Cooperative Security*, p. 1–2. https://www.globalcenter.org/wp-content/uploads/GCCS_PB_Safeguarding_Against_Misuse_Artificial_Intelligence_web.pdf

ανεξέλεγκτη εξαγωγή της, ενδέχεται να στοιχειοθετηθεί ευθύνη για «συνέργεια» (complicity) βάσει του Άρθρου 16 του Παραρτήματος της Απόφασης 56/83, εφόσον γνώριζε ότι η τεχνολογία θα χρησιμοποιηθεί για τη διάπραξη διεθνώς άδικης πράξης.¹⁸⁹

Τέλος, στο χαμηλότερο αλλά κρισιμότερο επίπεδο βρίσκεται ο «Ανθρώπινος Χειριστής» (Human Operator), η παρουσία του οποίου (human-in-the-loop) αποτελεί τη νομική γέφυρα που συνδέει την αλγοριθμική πράξη με την ατομική ποινική ευθύνη. Η έννοια του «Ουσιαστικού Ανθρώπινου Ελέγχου» (Meaningful Human Control) είναι θεμελιώδης, καθώς το διεθνές ποινικό δίκαιο δεν δικάζει μηχανές. Εάν ο χειριστής βασιστεί τυφλά στην απόφαση ενός συστήματος AI (automation bias) χωρίς να ασκήσει κριτική εποπτεία, και το σύστημα διαπράξει έγκλημα, ο χειριστής δεν απαλλάσσεται.¹⁹⁰ Η νομική θεωρία διακρίνει εδώ μεταξύ δόλου (intent), εάν το σύστημα λειτούργησε όπως είχε προγραμματιστεί, και εγκληματικής αμέλειας (recklessness), εάν το σύστημα έδρασε απρόβλεπτα και ο χειριστής απέτυχε να παρέμβει.¹⁹¹ Η ανάθεση φονικής ισχύος σε έναν αλγόριθμο χωρίς τη δυνατότητα ανθρώπινης παρέμβασης («human-out-of-the-loop») συνιστά από μόνη της παραβίαση της υποχρέωσης προφύλαξης, καθιστώντας τον ανθρώπινο παράγοντα τον τελικό εγγυητή της νομιμότητας απέναντι στην αλγοριθμική αυθαιρεσία.¹⁹²

5. ΚΕΦΑΛΑΙΟ: ΥΠΟΧΡΕΩΣΗ ΔΕΟΥΣΑΣ ΕΠΙΜΕΛΕΙΑΣ ΚΑΙ ΣΥΓΧΡΟΝΗ ΡΥΘΜΙΣΤΙΚΉ ΑΝΤΙΔΡΑΣΗ

Η διακρίβωση των τεχνικών και νομικών δυσχερειών που διέπουν την άμεση απόδοση ευθύνης (attribution) σε περιπτώσεις χρήσης Παραγωγικής Τεχνητής Νοημοσύνης από τρομοκρατικές ομάδες, καθιστά επιτακτική την αναζήτηση ενός εναλλακτικού κανονιστικού αναχώματος. Στο παρόν κεφάλαιο υποστηρίζεται ότι, όταν η αλγοριθμική αδιαφάνεια και η

¹⁸⁹ United Nations General Assembly. (2002). A/RES/56/83, ubi supra, Art. 16.

¹⁹⁰ Amoroso, D., & Tamburrini, G. (2020). Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. Current Robotics Reports, 1, p. 5. <https://www.iris.unina.it/retrieve/e268a732-272c-4c8f-e053-1705fe0a812c/Amoroso%20D%20Tamburrini%20G%20Autonomous%20Weapons%20Systems%20and%20Meaningful%20Human%20Control%20Current%20Robotics%20Reports.pdf>

¹⁹¹ Chengeta, T. (2016). Accountability Gap, Autonomous Weapon Systems and Modes of Responsibility in International Law. Denver Journal of International Law and Policy, 45(1), p. 2. <https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1011&context=djilp>

¹⁹² Liivoja, R., & Väljataga, A. (Eds.). (2021). Autonomous Cyber Capabilities under International Law. NATO CCDCOE Publications, p. 138. <https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf>

πολυπλοκότητα του κυβερνοχώρου εμποδίζουν τον εντοπισμό του φυσικού αυτουργού που «πάτησε το κουμπί», το διεθνές δίκαιο οφείλει να εστιάσει στη συμπεριφορά του κράτους που δεν απέτρεψε την πράξη ενώ όφειλε και μπορούσε.¹⁹³ Η κεντρική θέση της ανάλυσης μετατοπίζεται από την κατασταλτική λογική της τιμωρίας του δράστη στην προληπτική υποχρέωση της Δέουσας Επιμέλειας (Due Diligence), η οποία λειτουργεί ως το «δίχτυ ασφαλείας» της διεθνούς έννομης τάξης.¹⁹⁴ Μέσα από την εξέταση της θεωρητικής θεμελίωσης αυτής της αρχής, της εφαρμογής της στο ψηφιακό περιβάλλον και της σύγχρονης ρυθμιστικής αντίδρασης, όπως αυτή εκφράζεται μέσω του EU AI Act, επιδιώκεται η πλήρης κάλυψη του ρυθμιστικού κενού που εκμεταλλεύεται η σύγχρονη τρομοκρατία¹⁹⁵

5.1. Η Θεωρητική Θεμελίωση της Δέουσας Επιμέλειας

Η υποχρέωση δέουσας επιμέλειας στο διεθνές δίκαιο εδράζεται στην ιστορική απόφαση του Διεθνούς Δικαστηρίου της Χάγης (ICJ) στην υπόθεση Corfu Channel (1949), η οποία καθιέρωσε την αρχή ότι κανένα κράτος δεν επιτρέπεται να χρησιμοποιεί την επικράτειά του — ή να επιτρέπει εν γνώσει του σε τρίτους να τη χρησιμοποιούν — για πράξεις που παραβιάζουν τα δικαιώματα άλλων κρατών.¹⁹⁶ Η θεμελιώδης αυτή παραδοχή μετατοπίζει το κέντρο βάρους της διεθνούς ευθύνης από την «ευθύνη αποτελέσματος» (obligation of result), όπου το κράτος θα έπρεπε να εγγυηθεί την αποτροπή κάθε επίθεσης, στην «ευθύνη συμπεριφοράς» (obligation of conduct).¹⁹⁷ Η τελευταία απαιτεί από το κράτος να επιδεικνύει την απαραίτητη επιμέλεια και να λαμβάνει όλα τα εύλογα μέτρα πρόληψης, χωρίς να καθίσταται το ίδιο αντικειμενικά υπεύθυνο για την τρομοκρατική ενέργεια καθαυτή, αλλά για την αμέλειά του να λάβει τα απαραίτητα μέτρα αποτροπής της.¹⁹⁸

Στο πλαίσιο των σύγχρονων κυβερνο-απειλών, το κρίσιμο νομικό ζήτημα για τη θεμελίωση της κρατικής ευθύνης εντοπίζεται στο πρότυπο της γνώσης που οφείλει να διαθέτει το κράτος για τις δραστηριότητες εντός της επικράτειάς του.¹⁹⁹ Ενώ υπάρχει διεθνής σύγκλιση στην ανάγκη ύπαρξης γνώσης της επιβλαβούς δραστηριότητας, η ακαδημαϊκή και νομική διαμάχη παραμένει έντονη ως προς το αν η «εποικοδομητική γνώση» (constructive knowledge)

¹⁹³ UNICRI & UNCCT. (2021). *ubi supra*, p. 20.

¹⁹⁴ United Nations General Assembly. (2002). A/RES/56/83, *ubi supra*, Art. 2 & 12.

¹⁹⁵ European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 12. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

¹⁹⁶ International Court of Justice. (1949). *ubi supra*, p. 22.

¹⁹⁷ Schmitt, M. N. (2015). *ubi supra*, p. 71§ 2.

¹⁹⁸ Kapsokoli, E. (2022). *ubi supra*, p. 185.

¹⁹⁹ Schmitt, M. N. (2015). *ubi supra*, p. 71.

—δηλαδή η γνώση που το κράτος όφειλε να έχει βάσει των διαθέσιμων μέσων του— επαρκεί για τη στοιχειοθέτηση διεθνούς παράλειψης.²⁰⁰ Η υποχρέωση αυτή συνδέεται άμεσα με την έννοια της «κυβερνο-υγιεινής» (cyber hygiene), καθώς η αποτυχία ενός κράτους να εποπτεύσει τις ψηφιακές του υποδομές ή να αντιδράσει σε κακόβουλες ενέργειες που διευκολύνονται από συστήματα Τεχνητής Νοημοσύνης, μετατρέπει την κυριαρχία του από δικαίωμα σε πηγή διεθνούς ευθύνης λόγω παράλειψης (omission), σύμφωνα με το Άρθρο 2 του Παραρτήματος της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ.²⁰¹

Η μετεξέλιξη της διεθνούς ευθύνης στο ψηφιακό περιβάλλον απαιτεί τη σαφή διάκριση μεταξύ της «υποχρέωσης αποτελέσματος» και της «υποχρέωσης συμπεριφοράς» (obligation of conduct).²⁰² Στο πεδίο της Τεχνητής Νοημοσύνης, αυτό σημαίνει ότι η ευθύνη του κράτους δεν ενεργοποιείται αυτόματα από την εκδήλωση μιας τρομοκρατικής επίθεσης, αλλά από την αποτυχία του να επιδείξει τη δέουσα επιμέλεια μέσω της λήψης προληπτικών μέτρων που θα περιόριζαν την κατάχρηση των αλγορίθμων.²⁰³ Η σύγχρονη προσέγγιση της διεθνούς ασφάλειας υπογραμμίζει ότι τα κράτη οφείλουν να αναπτύσσουν ισχυρά εγχώρια κανονιστικά πλαίσια για τη διακυβέρνηση της ΤΝ, προκειμένου να αποτρέπουν τη χρήση των υποδομών τους για κακόβουλες ενέργειες από μη κρατικούς δρώντες.²⁰⁴ Συνεπώς, η Δέουσα Επιμέλεια αναδεικνύεται σε έναν δυναμικό κανόνα «προτύπου συμπεριφοράς» (standard of conduct), όπου η διεθνής παράνομη πράξη συνίσταται στην αμέλεια του κράτους να προσαρμόσει τους εποπτικούς του μηχανισμούς στις απαιτήσεις της ψηφιακής εποχής.²⁰⁵

Η πρακτική εφαρμογή της δέουσας επιμέλειας στο ψηφιακό πεδίο απαιτεί τη μετάβαση από την παραδοσιακή «αντιδραστική» κρατική στάση σε μια «προληπτική» στρατηγική διαχείρισης κινδύνων.²⁰⁶ Τα κράτη οφείλουν να ενσωματώνουν μηχανισμούς τεχνικής επαλήθευσης και ελέγχου της αλγοριθμικής διαφάνειας, καθώς η παράλειψη εποπτείας των

²⁰⁰ Buchan, R. (2016). Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm. *Journal of Conflict and Security Law*, p. 441. <https://academic.oup.com/jcsl/article/21/3/429/2566738>

²⁰¹ United Nations General Assembly. (2002). *ubi supra*, Art. 2.

²⁰² OECD. (2024). Transparency Reporting on Terrorist and Violent Extremist Content Online. Fourth Edition, p. 10. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency-reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf

²⁰³ United Nations General Assembly. (2015). *ubi supra*, p. 7 §13c.

²⁰⁴ Council of Europe (2020). Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, p. 7 § 1.4. [https://search.coe.int/cm/#{%22CoEIdentifier%22:%2209000016809e1154%22,%22sort%22:\[%22CoEValidationDate%20Descending%22\]}](https://search.coe.int/cm/#{%22CoEIdentifier%22:%2209000016809e1154%22,%22sort%22:[%22CoEValidationDate%20Descending%22]})

²⁰⁵ UN General Assembly. (2001). Responsibility of States for internationally wrongful acts. Resolution adopted by the General Assembly, A/RES/56/83, p. 65 § 3.

²⁰⁶ Global Commission on the Stability of Cyberspace (GCSC). (2019). Advancing Cyberstability, p. 24. <https://hcss.nl/global-commission-on-the-stability-of-cyberspace-final-report/>

αυτοματοποιημένων συστημάτων μπορεί να θεωρηθεί παραβίαση της υποχρέωσης συμπεριφοράς.²⁰⁷ Η διεθνής κοινότητα αναγνωρίζει πλέον ότι η δέουσα επιμέλεια περιλαμβάνει την υποχρέωση των κρατών να διασφαλίζουν ότι οι τεχνολογικές υποδομές δεν καθίστανται «καταφύγια» για την ανάπτυξη κακόβουλων λογισμικών ή τρομοκρατικών εργαλείων ΤΝ.²⁰⁸ Κατά συνέπεια, η νομική φύση της δέουσας επιμέλειας εξελίσσεται σε ένα δυναμικό πρότυπο «ψηφιακής επαγρύπνησης», όπου η ευθύνη του κράτους κρίνεται από την επάρκεια των τεχνικών και κανονιστικών εγγυήσεων που παρέχει για την προστασία του διεθνούς συνόλου.²⁰⁹

5.2. Εφαρμογή στον Κυβερνοχώρο (Cyber Due Diligence)

Η πρακτική εφαρμογή της δέουσας επιμέλειας απαιτεί από τα κράτη να μην λειτουργούν ως παθητικοί παρατηρητές, αλλά να επιδεικνύουν «ψηφιακή επαγρύπνηση» ανάλογη με τα μέσα που διαθέτουν.²¹⁰ Η νομική φύση αυτής της υποχρέωσης ορίζει ότι η διεθνής ευθύνη του κράτους δεν ενεργοποιείται αυτόματα με την εκδήλωση μιας κυβερνοεπίθεσης, αλλά όταν το κράτος αποτυγχάνει να λάβει τα απαραίτητα μέτρα πρόληψης ενώ γνώριζε ή όφειλε να γνωρίζει τον κίνδυνο.²¹¹ Ειδικά στην περίπτωση των botnets που χρησιμοποιούνται για τρομοκρατικούς σκοπούς, η υποχρέωση του κράτους συνίσταται στον εντοπισμό και την εξουδετέρωση των κακόβουλων κόμβων εντός της δικαιοδοσίας του, προκειμένου να προστατευθούν τα δικαιώματα τρίτων κρατών.²¹² Το κριτήριο της «δυνατότητας» (capacity) είναι εδώ καθοριστικό, καθώς το διεθνές δίκαιο αναγνωρίζει ότι δεν διαθέτουν όλα τα κράτη το ίδιο επίπεδο τεχνολογικής ανάπτυξης για την εποπτεία πολύπλοκων αλγοριθμικών συστημάτων.²¹³

²⁰⁷ European Commission. (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust, p. 11. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf&ved=2ahUKEwjn5Krrp-CSAxVKQUEAHdAfDgAQFnoECBcQAO&usq=AOvVaw1a0R-XZIGQTiTjcbt3F8E

²⁰⁸ African Union. (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention), Art. 25 § 2. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

²⁰⁹ Organization of American States (OAS). (2020). Improving Transparency: International Law and State Cyber Operations, p. 15. https://www.oas.org/en/sla/iajc/docs/CJI-doc_615-20_rev1_ENG.pdf

²¹⁰ International Court of Justice (ICJ). (1949). ubi supra, p. 22 § 4.

²¹¹ United Nations General Assembly. (2002). ubi supra, Art. 2 § 1.

²¹² Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0. ubi supra, Rule 6, p. 32.

²¹³ Liivoja, R., & Väljataga, A. (Eds.). (2021). Autonomous Cyber Capabilities under International Law, p. 142. <https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf>

Παρόλα αυτά, η εσκεμμένη παράλειψη θέσπισης ενός στοιχειώδους πλαισίου κυβερνοασφάλειας μπορεί να θεωρηθεί παραβίαση της υποχρέωσης συμπεριφοράς, μετατρέποντας την εδαφική κυριαρχία σε πηγή ευθύνης για το κράτος.²¹⁴

Η μετάβαση από την απλή κατοχή πληροφοριών στη νομική τεκμηρίωση της «γνώσης» (knowledge) αποτελεί το πλέον δυσχερές σημείο της κυβερνο-επιμέλειας.²¹⁵ Το διεθνές δίκαιο, όπως αποκρυσταλλώνεται στο Tallinn Manual 2.0, ορίζει ότι η υποχρέωση του κράτους ενεργοποιείται όχι μόνο με την «πραγματική γνώση» μιας επιβλαβούς πράξης, αλλά και με την «εποικοδομητική γνώση» (constructive knowledge), δηλαδή όταν οι περιστάσεις καθιστούν την κακόβουλη χρήση των υποδομών προφανή βάσει των μέσων που διαθέτει το κράτος.²¹⁶ Στην περίπτωση της Παραγωγικής ΤΝ, η χρήση προηγμένων αλγορίθμων από τρομοκρατικά δίκτυα για τη δημιουργία «ψηφιακών οπλοστασίων» απαιτεί από τα κράτη να αναπτύξουν μηχανισμούς τεχνικής επαλήθευσης που να αντιστοιχούν στην επιχειρησιακή τους ικανότητα.²¹⁷ Η παράλειψη άσκησης αποτελεσματικής εποπτείας επί των ψηφιακών συστημάτων εντός της δικαιοδοσίας τους δύναται να θεμελιώσει διεθνή ευθύνη, καθώς η εδαφική κυριαρχία μετατρέπεται από απόλυτο δικαίωμα σε πηγή ευθύνης λόγω παράλειψης. Συνεπώς, η δέουσα επιμέλεια λειτουργεί ως ρυθμιστικό «δίκτυ ασφαλείας», επιτρέποντας τη λογοδοσία του κράτους που αμέλησε να ελέγξει την τεχνολογία, κλείνοντας έτσι το παράθυρο ατιμωρησίας που εκμεταλλεύεται η σύγχρονη τρομοκρατία.²¹⁸

Πέραν της γνώσης, η ενεργοποίηση της κρατικής ευθύνης στον κυβερνοχώρο προϋποθέτει την ύπαρξη ενός «ουσιώδους κινδύνου» ή την πρόκληση «σοβαρών δυσμενών συνεπειών» στα δικαιώματα άλλων κρατών.²¹⁹ Το Tallinn Manual 2.0 διευκρινίζει ότι η υποχρέωση δέουσας επιμέλειας δεν αφορά κάθε είδους ψηφιακή όχληση, αλλά εστιάζει σε επιχειρήσεις που πλήττουν κρίσιμες υποδομές ή παραβιάζουν την κυριαρχία με τρόπο που προκαλεί φυσική ζημία ή σοβαρή λειτουργική δυσλειτουργία.²²⁰ Στο πλαίσιο της τρομοκρατίας, η χρήση της Παραγωγικής ΤΝ για τον σχεδιασμό κυβερνοεπιθέσεων μεγάλης κλίμακας εμπίπτει ακριβώς σε αυτό το κατώφλι σοβαρότητας, καθιστώντας την αδράνεια του κράτους διεθνώς άδικη πράξη.²²¹ Η νομική αυτή οριοθέτηση διασφαλίζει ότι τα κράτη δεν θα επιβαρύνονται με μια ανέφικτη υποχρέωση καθολικής αστυνόμευσης του διαδικτύου, αλλά θα επικεντρώνουν τους

²¹⁴ United Nations General Assembly. (2002). *ubi supra*, Art. 2.

²¹⁵ International Court of Justice (ICJ). (1949). *ubi supra*, p. 22.

²¹⁶ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0. *ubi supra*, Rule 6 § 11.

²¹⁷ UNICRI & UNCCT. (2021). *ubi supra*, p. 24.

²¹⁸ United Nations General Assembly. (2002). *ubi supra*, Art. 2.

²¹⁹ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0. *ubi supra*, Rule 6.

²²⁰ Liivoja, R., & Väljataga, A. (Eds.). (2021). *ubi supra*, p. 139

²²¹ UNICRI & UNCCT. (2021). *ubi supra*, p. 36.

πόρους τους στην αποτροπή ενεργειών που απειλούν τη διεθνή ειρήνη και ασφάλεια.²²²

5.3. Ο Ρόλος του Ιδιωτικού Τομέα και η Κρατική Ρύθμιση

Η ραγδαία ανάπτυξη συστημάτων Παραγωγικής ΤΝ από ιδιωτικούς τεχνολογικούς κολοσσούς δημιουργεί μια νέα πρόκληση για το διεθνές δίκαιο, καθώς η υποδομή στην οποία βασίζεται η σύγχρονη τρομοκρατία παραμένει υπό τον έλεγχο ιδιωτικών οντοτήτων. Παρόλο που οι ιδιωτικοί φορείς δεν αποτελούν άμεσα υποκείμενα του διεθνούς δικαίου, τα κράτη υπέχουν τη διεθνή υποχρέωση να ρυθμίζουν αποτελεσματικά τις δραστηριότητες που τελούν υπό τη δικαιοδοσία τους.²²³ Η υποχρέωση αυτή συνδέεται άμεσα με τη δέουσα επιμέλεια, καθώς η παράλειψη θέσπισης ενός αυστηρού ρυθμιστικού πλαισίου που να επιβάλλει κανόνες ασφαλείας («Security by Design») στα συστήματα ΑΙ, μπορεί να θεωρηθεί διεθνώς άδικη παράλειψη του κράτους.²²⁴ Η σύγχρονη θεωρία της κρατικής ευθύνης υποστηρίζει ότι το κράτος φέρει την «ευθύνη εποπτείας» (supervisory responsibility), οφείλοντας να διασφαλίζει ότι οι ιδιωτικοί αλγόριθμοι δεν μετατρέπονται σε εργαλεία στα χέρια τρομοκρατικών οργανώσεων για τη διάδοση προπαγάνδας ή τον σχεδιασμό επιθέσεων.²²⁵ Συνεπώς, η κρατική ρύθμιση των Big Tech δεν αποτελεί απλώς μια εσωτερική πολιτική επιλογή, αλλά μια διεθνή νομική επιταγή για την πρόληψη διασυννοριακών κινδύνων που απορρέουν από την κακόβουλη χρήση της τεχνολογίας.²²⁶

Η αποτελεσματική άσκηση της δέουσας επιμέλειας απαιτεί πλέον από τα κράτη να επιβάλλουν στις εταιρείες τεχνολογίας την αρχή της «ασφάλειας εκ σχεδιασμού» (Security by Design). Στο πλαίσιο της Παραγωγικής ΤΝ, αυτό μεταφράζεται στην υποχρέωση των κρατών να διασφαλίζουν ότι οι ιδιωτικοί φορείς εφαρμόζουν «κόκκινες γραμμές» (red-teaming) και αυστηρά πρωτόκολλα δοκιμών πριν τη διάθεση των μοντέλων στο κοινό, ώστε να ελαχιστοποιείται η δυνατότητα παραγωγής επιβλαβούς περιεχομένου από τρομοκρατικές

²²² United Nations General Assembly. (2002). *ubi supra*, Art. 2 § 3,4,5.

²²³ Council of Europe. (2001). *ubi supra*, p. 23 § 145 – 146.

²²⁴ Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0. *ubi supra*, Rule 6 § 1, p. 30.

²²⁵ Pauwels, E. (2022). Safeguarding against the misuse and abuse of artificial intelligence. Global Center on Cooperative Security, p. 1-2. https://www.globalcenter.org/wp-content/uploads/GCCS_PB_Safeguarding_Against_Misuse_Artificial_Intelligence_web.pdf

²²⁶ Program on Extremism. (2023). Moderating extremism: The state of online terrorist content removal policy in the United States. The George Washington University, p. 12-14. <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf>

ομάδες.²²⁷ Ωστόσο, η ανάδυση μοντέλων ανοιχτού κώδικα (Open-Source AI) περιπλέκει τη διεθνή ευθύνη, καθώς τα κράτη δυσκολεύονται να ελέγξουν τη διασπορά τεχνολογιών που δεν υπόκεινται σε κεντρική εποπτεία, δημιουργώντας κινδύνους «αλγοριθμικής τρομοκρατίας» που ξεπερνούν τα παραδοσιακά σύνορα.²²⁸ Παράλληλα, η κρατική πίεση προς τις εταιρείες για αυτοματοποιημένη αφαίρεση περιεχομένου εγείρει σοβαρά ζητήματα συμβατότητας με το διεθνές δίκαιο ανθρωπίνων δικαιωμάτων, καθώς οι αλγόριθμοι συχνά αδυνατούν να διακρίνουν το πλαίσιο (context), οδηγώντας σε αδικαιολόγητους περιορισμούς της ελευθερίας του λόγου.²²⁹ Τέλος, η διεθνής κοινότητα προκρίνει τη μετάβαση από την απλή εσωτερική νομοθεσία σε ένα «συμμετοχικό μοντέλο διακυβέρνησης», όπου τα κράτη υπέχουν την ευθύνη να συντονίζουν τη δράση των ιδιωτικών κολοσσών μέσω διεθνών προτύπων ασφαλείας, διασφαλίζοντας ότι η τεχνολογική ισχύς δεν θα λειτουργεί εις βάρος της παγκόσμιας ασφάλειας.²³⁰

Η πρακτική εφαρμογή της δέουσας επιμέλειας μετατοπίζεται πλέον από τον απλό έλεγχο περιεχομένου στην επιβολή τεχνικών προτύπων ασφαλείας κατά το στάδιο της ανάπτυξης. Σύμφωνα με το Άρθρο 15 του EU AI Act, η κρατική εποπτεία επιβάλλει τη διασφάλιση της ανθεκτικότητας των συστημάτων έναντι προσπαθειών χειραγώγησης (poisoning) και κακόβουλης χρήσης, απαιτώντας αυστηρές δοκιμές προσομοίωσης επιθέσεων (red-teaming).²³¹ Η ανάγκη αυτή καθίσταται επιτακτική λόγω της ανάδυσης μοντέλων ανοιχτού κώδικα (Open-Source AI), όπου η δυνατότητα τροποποίησης του κώδικα (fine-tuning) από τρομοκρατικές ομάδες καθιστά την κατάχρηση της τεχνολογίας «μη αναστρέψιμη» και τη διεθνή ευθύνη του κράτους δυσχερέστερη.²³² Ωστόσο, η διεθνής νομική επιταγή για ασφάλεια οριοθετείται από τις αρχές του ΟΗΕ, οι οποίες προειδοποιούν ότι η υπερεξάρτηση από την αυτοματοποίηση (overdependence on automation) και οι ασαφείς ορισμοί της τρομοκρατίας

²²⁷ European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act). Recitals 40-44 & Art.15. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

²²⁸ Seger, E., et al. (2023). Open-Sourcing Highly Capable Foundation Models: An Assessment of Risks and Benefits. Centre for the Governance of AI, p. 18-20. <https://www.governance.ai/research-paper/open-sourcing-highly-capable-foundation-models>

²²⁹ United Nations Special Rapporteur on Freedom of Opinion and Expression. (2018). Report on content moderation and the role of the private sector in the digital age, A/HRC/38/35, p. 10-11, § 26-29. <https://docs.un.org/en/A/HRC/38/35>

²³⁰ OECD. (2024). Explaining the OECD AI Principles: Accountability and Governance. OECD Digital Economy Papers, § 1.4-1.5. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

²³¹ European Union. (2024). ubi supra, Art. 15.

²³² Seger, E., et al. (2023). ubi supra, §1.4 – 1.5.

κινδυνεύουν να υπονομεύσουν την ελευθερία της έκφρασης.²³³ Συνεπώς, προκρίνεται ένα μοντέλο διακυβέρνησης βασισμένο στην ιχνηλασιμότητα (traceability) και τη συστηματική διαχείριση κινδύνου, διασφαλίζοντας ότι οι εταιρείες παραμένουν υπόλογες (accountable) για τη λειτουργία των συστημάτων τους σε όλο τον κύκλο ζωής τους.²³⁴

5.4. Η Πράξη για την Τεχνητή Νοημοσύνη της ΕΕ (EU AI Act)

Η Πράξη για την Τεχνητή Νοημοσύνη (EU AI Act) δεν αποτελεί απλώς μια περιφερειακή ρύθμιση, αλλά το πρώτο ολοκληρωμένο «lex specialis» παγκοσμίως, το οποίο εξειδικεύει την υποχρέωση δέουσας επιμέλειας των κρατών στον ψηφιακό χώρο. Η δομή της βασίζεται στην προσέγγιση βάσει κινδύνου (Risk-Based Approach), η οποία κατηγοριοποιεί τα συστήματα ΤΝ ανάλογα με την απειλή που συνιστούν για τα θεμελιώδη δικαιώματα και την ασφάλεια. Στο πλαίσιο της αντιμετώπισης της τρομοκρατίας, η Πράξη εισάγει μια κρίσιμη εξαίρεση στις απαγορευμένες πρακτικές (Unacceptable Risk). Ενώ η βιομετρική ταυτοποίηση σε πραγματικό χρόνο απαγορεύεται γενικά, το Άρθρο 5 επιτρέπει τη χρήση της από τις αρχές επιβολής του νόμου για την πρόληψη «συγκεκριμένων και επικείμενων τρομοκρατικών επιθέσεων».²³⁵ Αυτή η διάταξη μεταφέρει τη διεθνή υποχρέωση πρόληψης του κράτους στο επίπεδο της τεχνολογικής επιτήρησης, απαιτώντας όμως ταυτόχρονα δικαστική έγκριση για την αποφυγή αυθαιρεσιών.²³⁶

Ιδιαίτερη έμφαση δίνεται στα συστήματα Υψηλού Κινδύνου (High-Risk), τα οποία μπορούν να χρησιμοποιηθούν για τη διαχείριση κρίσιμων υποδομών ή την αξιολόγηση της επικινδυνότητας ατόμων. Εδώ, η Πράξη επιβάλλει στους παρόχους (Providers) την εγκαθίδρυση ενός Συστήματος Διαχείρισης Κινδύνου, το οποίο απαιτεί συνεχή έλεγχο των δεδομένων εκπαίδευσης για την αποφυγή προκαταλήψεων που θα μπορούσαν να οδηγήσουν σε λανθασμένες τρομοκρατικές στοχοποιήσεις.²³⁷ Η υποχρέωση αυτή συνδέεται με τη θεωρία

²³³ UN Human Rights Council. (2018). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/38/35), § 26 & 29. <https://digitallibrary.un.org/record/1631686?v=pdf>

²³⁴ OECD. (2024). ubi supra, § 1.4 & 1.5.

²³⁵ European Union. (2024). ubi supra, Art. 5.

²³⁶ Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. Computer Law & Security Review, p. 101. https://pure.uva.nl/ws/files/154819168/VealeBorgesius2021_typeset.pdf

²³⁷ Madiega, T. (2024). Artificial Intelligence Act: European Parliament briefing. European Parliamentary Research Service, p. 2. <https://www.dirittobancario.it/wp->

της «προληπτικής διοίκησης», όπου το κράτος υπέχει διεθνή ευθύνη να εγγυηθεί ότι οι ιδιωτικές τεχνολογίες που λειτουργούν στο έδαφός του δεν παραβιάζουν το διεθνές δίκαιο ανθρωπίνων δικαιωμάτων κατά την άσκηση αντιτρομοκρατικών πολιτικών.²³⁸

Κεντρικό πυλώνα της Πράξης αποτελεί η Ανθρώπινη Εποπτεία (Human Oversight - Article 14). Η απαίτηση να υπάρχει πάντα ένας «άνθρωπος στον βρόχο» (human-in-the-loop) έχει βαθιές προεκτάσεις στο Διεθνές Δίκαιο της Κρατικής Ευθύνης. Συγκεκριμένα, η δυνατότητα ενός φυσικού προσώπου να παρεμβαίνει, να αγνοεί ή να τερματίζει τη λειτουργία ενός συστήματος ΤΝ διασφαλίζει ότι η συμπεριφορά του συστήματος μπορεί να αποδοθεί στο κράτος σύμφωνα με το Άρθρο 8 της απόφασης 56/83 της Γενικής Συνέλευσης, εφόσον το άτομο αυτό ενεργεί υπό τις οδηγίες ή τον έλεγχο της κρατικής εξουσίας.²³⁹ Χωρίς την ανθρώπινη εποπτεία, θα δημιουργούνταν ένα «κενό ευθύνης» (accountability gap), όπου το κράτος θα μπορούσε να επικαλεστεί την «αυτόνομη» δράση του αλγορίθμου για να αποποιηθεί τις διεθνείς του υποχρεώσεις.²⁴⁰

Τέλος, η Πράξη αντιμετωπίζει την απειλή των Deepfakes και της ψηφιακής παραπληροφόρησης μέσω αυστηρών κανόνων Διαφάνειας και Ψηφιακής Σήμανσης (Watermarking). Το Άρθρο 50 υποχρεώνει τους παρόχους να επισημαίνουν το περιεχόμενο που παράγεται από ΤΝ σε μορφή αναγνώσιμη από μηχανές. Η ρύθμιση αυτή είναι ζωτικής σημασίας για την αποτροπή της «πληροφοριακής τρομοκρατίας», καθώς επιτρέπει στα κράτη να ιχνηλατούν την προέλευση προπαγανδιστικού υλικού και να περιορίζουν τη διάδοση ψευδών ειδήσεων που αποσκοπούν στην πρόκληση πανικού.

Η διεξοδική ανάλυση του νομικού πλαισίου καταδεικνύει ότι η Δέουσα Επιμέλεια (Due Diligence) λειτουργεί ως το θεμελιώδες «δίχτυ ασφαλείας» του Διεθνούς Δικαίου στην ψηφιακή εποχή. Ενώ η παραδοσιακή «Απόδοση Ευθύνης» (Attribution) προσκρούει συχνά στην τεχνική πολυπλοκότητα, την ανωνυμία και τον κατακερματισμό που προσφέρει η Παραγωγική ΤΝ, η υποχρέωση δέουσας επιμέλειας επιτρέπει τη λογοδοσία του κράτους για την παράλειψή του να ρυθμίσει αποτελεσματικά τις τεχνολογικές δραστηριότητες εντός της δικαιοδοσίας του. Όπως προκύπτει από τη συνδυαστική εφαρμογή των σύγχρονων κανονισμών της απόφασης 56/83 της Γενικής Συνέλευσης, η διεθνής ευθύνη μετατοπίζεται από την εκ των υστέρων τιμωρία μιας τρομοκρατικής πράξης στην εκ των προτέρων εποπτεία της διαδικασίας

<content/uploads/2024/09/Documento-riassuntivo-dellAI-Act-Parlamento-europeo-settembre-2024.pdf>

²³⁸ Floridi, L. (2021). The European Legislation on Artificial Intelligence: Ethics, Law, and Technology. *Minds and Machines*, 31(2), 255-263, p. 216.
<file:///Users/panagiotisbekiariis/Downloads/s13347-021-00460-9.pdf>

²³⁹ United Nations General Assembly. (2002). A/RES/56/83, ubi supra, Art. 8.

²⁴⁰ European Union. (2024). ubi supra, Art. 50.

ανάπτυξης και διάθεσης της τεχνολογίας. Το κράτος που αμελεί να επιβάλει σταθερές δικλίδες ασφαλείας, παραβιάζει την υποχρέωσή του να μην επιτρέπει τη χρησιμοποίηση του εδάφους του για ενέργειες που βλάπτουν τα δικαιώματα άλλων κρατών, μετατρέποντας τις εγχώριες ψηφιακές υποδομές σε ένα εν δυνάμει «ασφαλές καταφύγιο» (digital safe haven) για μη κρατικούς δρώντες.

Παράλληλα, η ανάδυση ρυθμιστικών προτύπων όπως ο EU AI Act σηματοδοτεί τη μετάβαση σε ένα συμμετοχικό μοντέλο διακυβέρνησης, όπου η τεχνική ικανότητα του ιδιωτικού τομέα υποτάσσεται στη νομική εποπτεία του κράτους. Η ενσωμάτωση απαιτήσεων για ανθρώπινη εποπτεία (Human Oversight) και διαφάνεια (Watermarking) κλείνει το ρυθμιστικό κενό, διασφαλίζοντας ότι η τεχνολογική εξέλιξη δεν θα λειτουργεί σε νομικό κενό. Συμπερασματικά, η δέουσα επιμέλεια δεν αποτελεί μια απλή ηθική προτροπή, αλλά μια δεσμευτική νομική επιταγή που υποχρεώνει τα κράτη να ισορροπήσουν ανάμεσα στην τεχνολογική καινοτομία και την παγκόσμια ασφάλεια. Με αυτόν τον τρόπο, η διεθνής κοινότητα αποκτά τα εργαλεία να εγκαλέσει το κράτος όχι απαραίτητα ως «συνεργό» στην τρομοκρατία, αλλά ως εγγυητή της διεθνούς έννομης τάξης που απέτυχε να ασκήσει τον οφειλόμενο έλεγχο σε ένα εργαλείο με διττή υπόσταση, όπως η Παραγωγική Τεχνητή Νοημοσύνη.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ολοκλήρωση της παρούσας μελέτης, η οποία επιχείρησε να χαρτογραφήσει την αχαρτογράφητη περιοχή όπου η εκθετική τεχνολογική πρόοδος της Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI) συναντά την βιαιότητα της τρομοκρατίας, οδηγεί σε μια σειρά κρίσιμων διαπιστώσεων που υπερβαίνουν την απλή καταγραφή νέων επιχειρησιακών δυνατοτήτων. Το κεντρικό ερευνητικό ερώτημα που τέθηκε εξ αρχής —κατά πόσον δηλαδή η GenAI συνιστά μια απλή γραμμική εξέλιξη ή μια θεμελιώδη τομή στο παράδειγμα της διεθνούς ασφάλειας και δικαίου— απαντάται πλέον καταφατικά υπέρ της δεύτερης εκδοχής: βρισκόμαστε ενώπιον μιας οντολογικής μεταλλαγής της απειλής, η οποία επαναπροσδιορίζει όχι μόνο τον τρόπο διεξαγωγής των συγκρούσεων, αλλά και τα θεμέλια της κρατικής ευθύνης. Η ανάλυση που προηγήθηκε, συνθέτοντας τα γεωπολιτικά δεδομένα των "αποτυχημένων κρατών", την τεχνολογική πραγματικότητα του "Γνωσιακού Πολέμου" και τα κανονιστικά εργαλεία του Παραρτήματος της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ και της

Δέουσας Επιμέλειας, αποκαλύπτει ότι η διεθνής κοινότητα καλείται να διαχειριστεί το φαινόμενο της «Υβριδικής Αλγοριθμικής Τρομοκρατίας».

Σε ένα πρώτο επίπεδο ανάλυσης, η έρευνα κατέδειξε ότι η ενσωμάτωση της GenAI στο οπλοστάσιο των μη κρατικών δρώντων λειτουργεί ως ο απόλυτος «πολλαπλασιαστής ισχύος» (force multiplier), επιφέροντας τον εκδημοκρατισμό της καταστροφικής δυνατότητας. Ενώ ιστορικά η "ασυμμετρία" αναφερόταν στη διαφορά στρατιωτικής ισχύος, η νέα τεχνολογική πραγματικότητα εξισώνει τους όρους του παιχνιδιού στο πεδίο της πληροφορίας και της ψυχολογίας. Όπως τεκμηριώθηκε μέσω των περιπτωσιολογικών μελετών του ISIS και της Χεζμπολάχ, η ειδοποιός διαφορά δεν έγκειται πλέον στην κατοχή βαρέως οπλισμού, αλλά στην ικανότητα διεξαγωγής επιχειρήσεων Γνωσιακού Πολέμου (Cognitive Warfare). Η δυνατότητα παραγωγής αληθοφανών deepfakes, η αυτοματοποιημένη δημιουργία προπαγάνδας προσαρμοσμένης στα ψυχολογικά προφίλ των στόχων (micro-targeting) και η μαζική διασπορά παραπληροφόρησης, επιτρέπουν σε τρομοκρατικές ομάδες να προκαλούν συστημική διατάραξη, κοινωνική πόλωση και διάβρωση της εμπιστοσύνης στους θεσμούς, με ελάχιστο οικονομικό κόστος. Αυτή η ποιοτική αναβάθμιση μετατρέπει την τρομοκρατία από μια πράξη φυσικής βίας σε μια διαρκή ψυχολογική επιχείρηση, όπου το "πεδίο της μάχης" είναι η ανθρώπινη αντίληψη. Η διαπίστωση αυτή είναι κρίσιμη, διότι καταδεικνύει ότι τα παραδοσιακά μέτρα αντιτρομοκρατίας, τα οποία εστιάζουν στον έλεγχο των φυσικών συνόρων και των χρηματοροών, καθίστανται ανεπαρκή αν δεν συνοδευτούν από μηχανισμούς ελέγχου της ψηφιακής σφαίρας.

Περαιτέρω, η παρούσα διατριβή προχώρησε στην αποδόμηση ενός εκ των πλέον διαδεδομένων μύθων της ψηφιακής εποχής: της υποτιθέμενης «εδαφικοποίησης» της απειλής. Παρά την άυλη φύση των αλγορίθμων και την παγκόσμια εμβέλεια του διαδικτύου, η ανάλυση των γεωπολιτικών παραμέτρων στο δεύτερο κεφάλαιο απέδειξε ότι η ψηφιακή τρομοκρατία παραμένει άρρηκτα συνδεδεμένη με το φυσικό έδαφος. Η λειτουργία πολύπλοκων μοντέλων Τεχνητής Νοημοσύνης δεν συντελείται σε κενό· απαιτεί φυσικές υποδομές, εκτεταμένα κέντρα δεδομένων (server farms), σταθερή παροχή ενέργειας και, κυρίως, ασφαλή καταφύγια για τους εξειδικευμένους χειριστές. Υπό αυτό το πρίσμα, η έννοια των «Αποτυχημένων Κρατών» (Failed States) και των «Γκρίζων Ζωνών» αποκτά νέα βαρύτητα. Αυτές οι περιοχές δεν αποτελούν απλώς κρησφύγετα ένοπλων ανταρτών, αλλά εξελίσσονται σε "ψηφιακά άσυλα", όπου η απουσία κρατικού ελέγχου επιτρέπει την ανάπτυξη και δοκιμή κυβερνο-όπλων χωρίς τον φόβο νομικών κυρώσεων. Η περίπτωση της Χεζμπολάχ, η οποία εξετάστηκε ως το αρχέτυπο του "κρατικά υποστηριζόμενου δρώντα", επιβεβαιώνει ότι η τεχνολογική αναβάθμιση των τρομοκρατών είναι συχνά αποτέλεσμα κρατικής αρωγής. Εδώ αναδεικνύεται

μια νέα μορφή πολέμου δι' αντιπροσώπων (proxy warfare), όπου τα κράτη-χορηγοί δεν παρέχουν πλέον πυραύλους, αλλά πρόσβαση σε υπολογιστική ισχύ και αλγοριθμική τεχνογνωσία, επιτυγχάνοντας τους στρατηγικούς τους στόχους με ακόμη μεγαλύτερη δυνατότητα άρνησης της εμπλοκής τους.

Ακρογωνιαίος λίθος της νομικής προβληματικής που ανέδειξε η εργασία είναι η ανεπάρκεια των κλασικών κανόνων απόδοσης ευθύνης (attribution) μπροστά στην πολυπλοκότητα της αλγοριθμικής αυτονομίας. Το Παράρτημα της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ και το κριτήριο του «αποτελεσματικού ελέγχου», όπως αυτό παγιώθηκε στη νομολογία της Χάγης, δομήθηκαν σε μια εποχή όπου η σχέση εντολέα-εντολοδόχου ήταν γραμμική και διαφανής. Στην εποχή της GenAI, ωστόσο, παρεμβάλλεται το «πρόβλημα του μαύρου κουτιού» (black box problem). Η ικανότητα των συστημάτων μηχανικής μάθησης να λαμβάνουν αποφάσεις –όπως η επιλογή στόχων ή η παραγωγή περιεχομένου– που δεν έχουν ρητά προγραμματιστεί, δημιουργεί ένα σοβαρό κίνδυνο «κενού λογοδοσίας» (accountability gap). Ένα κράτος μπορεί εύλογα να ισχυριστεί ότι μια κυβερνοεπίθεση ή μια εκστρατεία παραπληροφόρησης ήταν αποτέλεσμα "αλγοριθμικού σφάλματος" του συστήματος, και όχι πολιτικής βούλησης, αξιοποιώντας έτσι το στρατηγικό πλεονέκτημα της «εύλογης άρνησης» (plausible deniability). Αυτή η τεχνική πραγματικότητα απειλεί να δημιουργήσει μια ζώνη νομικής ατιμωρησίας, όπου η ανθρώπινη ευθύνη εξατμίζεται μέσα στην πολυπλοκότητα του κώδικα.

Ωστόσο, η μελέτη κατέληξε στο συμπέρασμα ότι το Διεθνές Δίκαιο διαθέτει τις απαραίτητες ερμηνευτικές εφεδρείες για να αποτρέψει αυτή την κατάρρευση. Μέσω μιας τελεολογικής και δυναμικής ερμηνείας του Άρθρου 8 του Παραρτήματος της Απόφασης 56/83 της Γενικής Συνέλευσης του ΟΗΕ, υποστηρίχθηκε σθεναρά ότι η έννοια της «Οδηγίας» (Instruction) πρέπει να προσαρμοστεί στα ψηφιακά δεδομένα. Συγκεκριμένα, το «Prompt», δηλαδή η εισαγωγή παραμέτρων και εντολών στόχευσης στο σύστημα, συνιστά τη νομική ισοδυναμία της κρατικής εντολής. Το κρίσιμο στοιχείο για την απόδοση ευθύνης δεν είναι ο έλεγχος των τεχνικών μέσων, δηλαδή πώς ακριβώς δρα ο αλγόριθμος, αλλά ο έλεγχος του επιχειρησιακού σκοπού. Από τη στιγμή που ο ανθρώπινος χειριστής θέτει τον στόχο και ενεργοποιεί το σύστημα, η αλυσίδα της ευθύνης παραμένει ακέραια, ανεξαρτήτως του βαθμού αυτονομίας της μηχανής. Αυτή η προσέγγιση είναι ζωτικής σημασίας για τη διατήρηση της κανονιστικής ισχύος του δικαίου, καθώς επαναφέρει τον άνθρωπο στο κέντρο της εξίσωσης, λειτουργώντας ως "μαγνήτης λογοδοσίας" (accountability attractor) που δεν επιτρέπει την απόκρυψη πίσω από την τεχνολογία.

Παρά τη θεωρητική πληρότητα αυτής της ερμηνείας, η εργασία αναγνώρισε με ρεαλισμό ότι το πρακτικό πρόβλημα της απόδειξης παραμένει οξύ. Η δυσκολία της ψηφιακής εγκληματολογίας (AI forensics) να εντοπίσει με βεβαιότητα την πηγή μιας επίθεσης, ειδικά όταν παρεμβάλλονται τεχνικές ανωνυμοποίησης, δημιουργεί συχνά ένα αδιέξοδο επιβολής. Σε αυτό το σημείο, η μελέτη πρόκρινε ως αναγκαία λύση τη στροφή από την κατασταλτική στην προληπτική ευθύνη, μέσω του δόγματος της Δέουσας Επιμέλειας (Due Diligence). Το συμπέρασμα είναι σαφές: η κρατική κυριαρχία στον κυβερνοχώρο δεν συνεπάγεται μόνο δικαιώματα, αλλά και αυξημένες υποχρεώσεις. Βασισόμενη στη θεμελιώδη αρχή της υπόθεσης «Corfu Channel», η ανάλυση κατέδειξε ότι τα κράτη φέρουν τη θετική υποχρέωση (positive obligation) να θωρακίζουν τις ψηφιακές τους υποδομές και να αποτρέπουν τη χρήση τους για βλαπτικές ενέργειες τρίτων.

Αυτή η μετατόπιση του βάρους από την «πράξη» στην «παράλειψη» αποτελεί ίσως τη σημαντικότερη νομική εξέλιξη στην εποχή της Τεχνητής Νοημοσύνης. Ακόμη και αν είναι αδύνατο να αποδειχθεί ποιος "πάτησε το κουμπί", το κράτος μπορεί να καταστεί υπεύθυνο επειδή αμέλησε να λάβει τα απαραίτητα μέτρα εποπτείας, επιτρέποντας στο έδαφός του να μετατραπεί σε ορμητήριο ψηφιακής τρομοκρατίας. Η σημασία σύγχρονων ρυθμιστικών κειμένων, όπως η Πράξη για την Τεχνητή Νοημοσύνη της ΕΕ (EU AI Act), αναδεικνύεται εδώ καταλυτική. Η θέσπιση υποχρεωτικών κανόνων για ανθρώπινη εποπτεία (human oversight), διαφάνεια των αλγορίθμων και διαχείριση κινδύνου, δεν αποτελεί απλώς μια εσωτερική κανονιστική ρύθμιση, αλλά συμβάλλει στη διαμόρφωση ενός νέου διεθνούς εθιμικού κανόνα επιμέλειας ("standard of care"). Η μη συμμόρφωση με αυτά τα ελάχιστα πρότυπα ασφαλείας δεν θα θεωρείται πλέον απλή διοικητική παράβαση, αλλά θα μπορεί να θεμελιώσει διεθνή ευθύνη του κράτους για αμέλεια, κλείνοντας έτσι το παράθυρο ατιμωρησίας που εκμεταλλεύονται οι τρομοκρατικές οργανώσεις.

Συγκεφαλαιώνοντας, η παρούσα εργασία καταλήγει στη διαπίστωση ότι η έλευση της Παραγωγικής Τεχνητής Νοημοσύνης, αν και προκαλεί ισχυρούς κλυδωνισμούς, δεν καθιστά το Διεθνές Δίκαιο παρωχημένο. Αντιθέτως, αναδεικνύει την προσαρμοστικότητά του. Το πρόβλημα που εξετάστηκε είναι διττό και σύνθετο: αφορά την επιχειρησιακή μετάλλαξη της τρομοκρατίας σε μια υβριδική, γνωσιακή απειλή και την ταυτόχρονη νομική ασάφεια που προκαλεί η αλγοριθμική αυτονομία. Οι λύσεις που προτάθηκαν κινούνται σε δύο παράλληλους άξονες που αλληλοσυμπληρώνονται. Στον ερμηνευτικό άξονα, η εξίσωση του "Prompt" με την "Οδηγία" διασφαλίζει ότι η ανθρώπινη πρόθεση παραμένει η βάση του καταλογισμού. Στον κανονιστικό άξονα, η ενίσχυση της Δέουσας Επιμέλειας διασφαλίζει ότι τα κράτη δεν μπορούν να νίπτουν τα χείρας τους για όσα συμβαίνουν στις ψηφιακές τους επικράτειες.

Εν τέλει, η μάχη κατά της σύγχρονης τρομοκρατίας δεν θα κριθεί αποκλειστικά στα πεδία των στρατιωτικών επιχειρήσεων, αλλά στην ικανότητα της διεθνούς κοινότητας να επιβάλει το κράτος δικαίου στον ψηφιακό χώρο. Η τεχνολογία, όσο προηγμένη και αν είναι, παραμένει εργαλείο στα χέρια ανθρώπων και κρατών. Η νομική επιστήμη οφείλει να αρνηθεί τον τεχνολογικό ντετερμινισμό και να επιμείνει στη θέση ότι πίσω από κάθε αλγόριθμο, πίσω από κάθε deepfake και πίσω από κάθε κυβερνοεπίθεση, υπάρχει πάντα μια ανθρώπινη απόφαση και μια κρατική ευθύνη. Η αναγνώριση και η νομική θωράκιση αυτής της αλήθειας αποτελεί τη μοναδική εγγύηση για τη διατήρηση της διεθνούς ειρήνης και ασφάλειας στην εποχή της Τεχνητής Νοημοσύνης.

ΚΕΙΜΕΝΑ ΤΕΚΜΗΡΙΩΣΗΣ

Νομικά Κείμενα, Διεθνείς Συνθήκες & Δικαστικές Αποφάσεις:

1. African Union. (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
2. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). <https://rm.coe.int/1680081561>
3. European Parliament and Council of the European Union. (2017). Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. Official Journal of the European Union, L 88. <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32017L0541>
4. European Union. (2000). Directive 2000/31/EC on certain legal aspects of information society services (Directive on electronic commerce). Official Journal of the European Communities, L 178. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031>
5. European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
6. International Court of Justice. (1949). Corfu Channel (United Kingdom v. Albania), Judgment. I.C.J. Reports 1949, p. 4. <https://icj-web.ileman.un-icc.cloud/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf>
7. International Court of Justice. (1980). United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment. I.C.J. Reports 1980, p. 3. <https://www.icj-cij.org/sites/default/files/case-related/64/064-19800524-JUD-01-00-EN.pdf>

8. International Court of Justice. (1986). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 14. <https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>
9. International Court of Justice. (1996). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. I.C.J. Reports 1996, p. 226. <https://api.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>
10. International Court of Justice. (2007). 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, p. 43. <https://www.acerislaw.com/wp-content/uploads/2024/04/Application-of-the-Convention-on-the-Prevention-and-Punishment-of-the-Crime-of-Genocide.pdf>
11. International Criminal Tribunal for the former Yugoslavia (ICTY). (1999). Prosecutor v. Duško Tadić, Judgment, Case No. IT-94-1-A. <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>
12. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II). (1977). <https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and-0>
13. Special Tribunal for Lebanon (STL). (2011). Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case No. STL-11-01/I. <https://www.refworld.org/jurisprudence/caselaw/stl/2011/en/77425>
14. United Nations General Assembly. (1994). Declaration on Measures to Eliminate International Terrorism, A/RES/49/60. <https://documents.un.org/doc/undoc/gen/n95/768/19/pdf/n9576819.pdf>
15. United Nations General Assembly. (2002). Responsibility of States for internationally wrongful acts, A/RES/56/83. <https://documents.un.org/doc/undoc/gen/n02/461/88/pdf/n0246188.pdf>
16. United Nations Security Council. (1945). Charter of the United Nations. <https://www.un.org/en/about-us/un-charter/chapter-6>
17. United Nations Security Council. (2001). Resolution 1373 (2001), S/RES/1373. <https://documents.un.org/doc/undoc/gen/n01/557/43/pdf/n0155743.pdf>
18. United Nations Security Council. (2004). Resolution 1540 (2004), S/RES/1540. <https://documents.un.org/doc/undoc/gen/n04/328/43/pdf/n0432843.pdf>
19. United Nations Security Council. (2004). Resolution 1566 (2004), S/RES/1566. [https://docs.un.org/en/S/RES/1566\(2004](https://docs.un.org/en/S/RES/1566(2004)
20. United Nations Security Council. (2014). Resolution 2178 (2014), S/RES/2178. <https://documents.un.org/doc/undoc/gen/n14/547/98/pdf/n1454798.pdf>
21. United States Code. (1996). 47 U.S.C. § 230 - Protection for private blocking and screening of offensive material (Communications Decency Act). <https://www.govinfo.gov/app/details/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec230>

Βιβλιογραφία:

22. Henckaerts, J.-M., & Doswald-Beck, L. (Eds.). (2005). Customary International Humanitarian Law, Volume I: Rules. Cambridge University Press. <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule139>
23. Καποκόλη, Ε. (2025). Ψηφιακό Τζιχάντ: Η στρατηγική χρήση του κυβερνοχώρου από την Al Qaeda και το ISIS. Εκδόσεις Παπαζήση.
24. Καποκόλη, Ε. (2025). Η χρήση του κυβερνοχώρου από τους τρομοκράτες: η περίπτωση του ISIS. Στο Α. Λιαρόπουλος & Α. Μποζίνης (Επιμ.), Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις (σελ. 211-234). Εκδόσεις Παπαζήση.
25. Kapsokoli, E. (2022). The challenge of defining cyberterrorism within the EU. In F. Asderaki et al. (Eds.), Challenges of the common security and defence policy (pp. 183-196). Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/e3706908-db0f-11ec-a95f-01aa75ed71a1>
26. Kapsokoli, E. (2023). Cyberterrorism: A New Wave of Terrorism or Not. In M. A. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (Eds.), Hybrid Threats, Cyberterrorism, and Cyberwarfare (1st ed., pp. 57-80). Routledge. <https://www.taylorfrancis.com/books/edit/10.1201/9781003314721/hybrid-threats-cyberterrorism-cyberwarfare>
27. Kapsokoli, E. (2025). Cybersecurity in the Western Balkans: is the ‘Brussels Effect’ in play? In F. Asderaki et al. (Eds.), ESDC Autumn University Book 2021: The Common Security and Defence Policy (pp. 132-143). Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/27a93540-8774-11ef-a704-01aa75ed71a1>
28. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>

Αρθρογραφία & Επιστημονικές Μελέτες:

29. Al-Ma'aitah, M. (2025). Generative AI in academia: A comprehensive review of applications and implications for the research process. ResearchGate. <https://www.researchgate.net/publication/387962069>
30. Alrhoun, A., Winter, C., & Kertesz, J. (2023). Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem. Terrorism and Political Violence, 36(4), 409-424. <https://www.tandfonline.com/doi/pdf/10.1080/09546553.2023.2169142>
31. Amoroso, D., & Tamburrini, G. (2020). Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. Current Robotics Reports, 1, 1-7. <https://www.iris.unina.it/retrieve/e268a732-272c-4c8f-e053-1705fe0a812c/Amoroso%20D%20Tamburrini%20G%20Autonomous%20Weapons%20Systems%20and%20Meaningful%20Human%20Control%20Current%20Robotics%20Reports.pdf>
32. Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. Harvard Journal of Law & Technology, 31(2), 889-938. <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf>

33. Buchan, R. (2016). Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm. *Journal of Conflict and Security Law*, 21(3), 429-453. <https://academic.oup.com/jcs/article/21/3/429/2566738>
34. Cassese, A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law. *European Journal of International Law*, 12(5), 993-1001. <https://www.ejil.org/pdfs/12/5/1558.pdf>
35. Cassese, A. (2006). The multifaceted criminal notion of terrorism in international law. *Journal of International Criminal Justice*, 4(5), 933-958. <https://academic.oup.com/jicj/article/4/5/933/835024>
36. Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753-1820. https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship
37. Clapham, A. (2006). Human rights obligations of non-state actors in conflict situations. *International Review of the Red Cross*, 88(863), 491-523. https://international-review.icrc.org/sites/default/files/irrc_863_3.pdf
38. Donghee Shin & Kulsawasd Jitkajornwanich. (2024). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review*, 42(4), 1020-1040. https://www.researchgate.net/publication/382731522_How_Algorithms_Promote_Self-Radicalization
39. Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law*, 112(4), 583-657. <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/rule-book-on-the-shelf-tallinn-manual-20-on-cyberoperations-and-subsequent-state-practice/54FBA2B30081B53353B5D2F06F778C14>
40. Ennazar, Y., & En-Naimi, E. M. (2024). Traditional AI vs generative AI: The role in modern cyber security. *International Journal of Engineering Technology and Management Sciences*. <https://www.researchgate.net/publication/386248918>
41. Floridi, L. (2021). The European Legislation on Artificial Intelligence: Ethics, Law, and Technology. *Minds and Machines*, 31(2), 255-263. <https://link.springer.com/article/10.1007/s11023-021-09562-2>
42. Gozalo-Brizuela, R., & Garrido-Merchan, E. C. (2023). Generative artificial intelligence reproducibility and consensus. *arXiv*. <https://arxiv.org/html/2307.01898v2>
43. Greenwood, C. (2002). International law and the 'war against terrorism'. *International Affairs*, 78(2), 301-317. <https://library.fes.de/libalt/journals/swetsfulltext/12995288.pdf>
44. Hoyer, J. (2024). Down the alt-right rabbit hole: The role of social media platforms in the radicalization of domestic right-wing terrorists. *Southern California Interdisciplinary Law Journal*, 33(1). <https://gould.usc.edu/why/students/orgs/ilj/assets/docs/33-1-hoyer.pdf>
45. Kapsokoli, E. (2019). The transformation of Islamic terrorism through cyberspace: the case of ISIS. *Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS 2019)*, 677-684. <https://www.academia.edu/40088253>
46. Kapsokoli, E. (2023). ISIS's Digital Jihad. *National Security and the Future*, 24(3), 39-66. <https://nsf-journal.hr/Portals/0/Dokumenti/Volume24,%20No3%202023/004-NSF-2023-VOL-24-No%203%20-%20Kapsokoli%20-%2039-66%20-%20IZ%C4%8C.pdf>

47. Mouter, N., et al. (2024). Dual use concerns of generative AI and large language models. *Journal of Responsible Innovation*, 11(1). <https://www.tandfonline.com/doi/full/10.1080/23299460.2024.2304381>
48. Muhanad, S. (2025). Veiled Intentions: Hamas's Strategic Deception and Intelligence Success on 7 October 2023. *Intelligence and National Security*, 1-28. <https://www.tandfonline.com/doi/pdf/10.1080/02684527.2024.2443478>
49. Rai, A., Constantinides, P., & Sarker, S. (2025). Inventing with machines: Generative AI and the evolving landscape of IS research. *Information Systems Research*, 36(4). <https://pubsonline.informs.org/doi/10.1287/isre.2025.editorial.v36.n4>
50. Sassòli, M. (2014). Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to Be Clarified. *International Law Studies*, 90, 308-340. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1017&context=ils>
51. Schmitt, M. N. (2015). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum*, 125, 68-81. https://yalelawjournal.org/pdf/Schmitt_PDF_g9pv96jc.pdf
52. Schmitt, M. N. (2017). Grey Zones in the International Law of Cyberspace. *The Yale Journal of International Law Online*, 42(2). <https://yjil.yale.edu/posts/2017-05-08-grey-zones-in-the-international-law-of-cyberspace>
53. Schmitt, M. N., & Vihul, L. (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, 95, 1639-1670. https://texaslawreview.org/wp-content/uploads/2017/11/Schmitt.Vihul_.pdf
54. Shackelford, S. J., & Andres, R. B. (2011). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law*, 42, 971-1016. <https://heinonline.org/HOL/Page?handle=hein.journals/geojint142&div=35>
55. Sivakumaran, S. (2011). Lessons for the law of armed conflict from commitments of armed groups. *International Review of the Red Cross*, 93(882), 463-482. <https://international-review.icrc.org/sites/default/files/irrc-882-sivakumaran.pdf>
56. Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-centric Computing and Information Sciences*. <https://link.springer.com/article/10.1186/s13673-018-0125-x>
57. Sparrow, R. (2007). Killer Robots. *Journal of Applied Philosophy*, 24(1), 62-77. <https://eclass.uoa.gr/modules/document/file.php/PHILOSOPHY875/ROBERT%20SPARROW%20--%20Killer%20Robots.pdf>
58. Talmon, S. (2009). The responsibility of outside powers for acts of secessionist entities. *International & Comparative Law Quarterly*, 58(3), 493-517. [https://users.ox.ac.uk/~sann2029/ICLQ%2058%20\(2009\),%20493-517.pdf](https://users.ox.ac.uk/~sann2029/ICLQ%2058%20(2009),%20493-517.pdf)
59. Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law & Security Review*, 42. https://pure.uva.nl/ws/files/154819168/VealeBorgesius2021_typeset.pdf
60. Εκθέσεις Οργανισμών & Λοιπά (Briefings, Speeches, Reports)
61. Attorney General's Office (UK). (2018). Cyber and International Law in the 21st Century. Speech by Jeremy Wright QC MP. <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>
62. Bernal, A., et al. (2020). Cognitive warfare: An attack on truth and thought. *NATO Innovation Hub*. <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf>

63. Boucher, P. (2020). Artificial intelligence: How does it work, why does it matter, and what can we do about it. European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU%282020%29641547_EN.pdf
64. Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. <https://arxiv.org/pdf/1802.07228>
65. Claverie, B., & du Cluzel, F. (2022). The cognitive warfare concept. NATO Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf
66. Council of Europe, Committee on Counter-Terrorism (CDCT). (2025). Report on the emerging patterns of misuse of technology by terrorist actors. <https://rm.coe.int/report-on-the-emerging-patterns-of-misuse-of-technology-by-terrorist-a/4880281a94>
67. Criezis, M. (2024). AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI. Global Network on Extremism & Technology. <https://gnet-research.org/wp-content/uploads/2024/02/AI-Caliphate-Pro-Islamic-State-Propaganda-and-Generative-AI.pdf>
68. Cybernetic Global Intelligence. (2025). AI and generative AI: Dual-use risks and autonomous threats. <https://www.cyberneticgi.com/dual-use-risks-and-autonomous-threats/>
69. European Commission. (2020). Joint Communication: EU Security Union Strategy. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>
70. European Commission. (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf
71. European Parliamentary Research Service. (2024). Artificial intelligence act: Overview and policy context. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf
72. Europol. (2023). ChatGPT: The impact of Large Language Models on Law Enforcement. <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>
73. Europol. (2024). European Union Terrorism Situation and Trend Report (TE-SAT 2024). https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2024.pdf
74. Goldstein, J. A., et al. (2023). Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations. <https://arxiv.org/pdf/2301.04246>
75. Group-IB. (2025). High-tech crime trends 2024/2025. <https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2024-2025>
76. HYAS Labs. (2023). BlackMamba: AI-Synthesized Polymorphic Keylogger. <https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware>
77. International Committee of the Red Cross (ICRC). (2016). Commentary on the First Geneva Convention: Article 3. <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3/commentary/2016>

78. Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
79. Liivoja, R., & Väljataga, A. (Eds.). (2021). Autonomous Cyber Capabilities under International Law. NATO CCDCOE. <https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf>
80. Mehra, T. (2024). Exploitation of generative AI by terrorist groups. International Centre for Counter-Terrorism (ICCT). <https://icct.nl/publication/exploitation-generative-ai-terrorist-groups>
81. MIT Industrial Liaison Program. (2024). Exploring the shift from traditional to generative AI. <https://curve.mit.edu/exploring-shift-traditional-generative-ai>
82. Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention. Chatham House. <https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf>
83. Mumford, A., & Reis, B. C. (2015). The role of counter terrorism in hybrid warfare. NATO Defense College. <https://www.tmmm.tsk.tr/publication/researches/04-TheRoleofCounterTerrorisminHybridWarfare.pdf>
84. National Cyber Security Centre (NCSC). (2024). The near-term impact of AI on the cyber threat. <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>
85. North Atlantic Treaty Organization (NATO). (2022). NATO 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
86. OECD. (2024). Transparency Reporting on Terrorist and Violent Extremist Content Online (4th ed.). https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency-reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf
87. Pauwels, E. (2022). Safeguarding against the misuse and abuse of artificial intelligence. Global Center on Cooperative Security. https://www.globalcenter.org/wp-content/uploads/GCCS_PB_Safeguarding_Against_Misuse_Artificial_Intelligence_web.pdf
88. Pfaff, C. A. (Ed.). (2025). The weaponization of AI: The next stage of terrorism and warfare. COE-DAT. <https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf>
89. Program on Extremism. (2023). Moderating extremism: The state of online terrorist content removal policy in the United States. George Washington University. <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf>
90. Quezada Tavárez, K. (2021). Legal Challenges in Bringing AI Evidence to the Criminal Trial. <https://lirias.kuleuven.be/retrieve/638528>
91. Seger, E., et al. (2023). Open-Sourcing Highly Capable Foundation Models: An Assessment of Risks and Benefits. <https://www.governance.ai/research-paper/open-sourcing-highly-capable-foundation-models>
92. Stockwell, S., et al. (2025). Evaluating malicious generative AI capabilities. Centre for Emerging Technology and Security (CETaS).

<https://cetas.turing.ac.uk/publications/evaluating-malicious-generative-ai-capabilities>

93. UNICRI & UNCCT. (2021). Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes. https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf
94. United Nations General Assembly. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications. A/70/174. <https://docs.un.org/en/A/70/174>
95. United Nations Security Council. (2024). Letter dated 19 July 2024 from the Chair of the Security Council Committee (S/2024/556). <https://undocs.org/pdf?symbol=en/S/2024/556>