Μεταπτυχιακό Πρόγραμμα στις Διεθνείς και Ευρωπαϊκές Σπουδές

Τμήμα Διεθνών & Ευρωπαϊκών Σπουδών

Σχολή Οικονομικών, Επιχειρηματικών & Διεθνών Σπουδών

Πανεπιστήμιο Πειραιώς

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασύμμετρες Απειλές και Κυβερνοχώρος:

Ανάλυση Πολλών Διαστάσεων

Ονοματεπώνυμο Φοιτητή: Δημήτριος Μάλλιος

Αριθμός Μητρώου: ΜΘ22019

Μέλη Συμβουλευτικής Επιτροπής:

Επίκουρος Καθηγητής Ιωάννης Λ. Κωνσταντόπουλος (Επιβλέπων)

Καθηγητής Αθανάσιος Γ. Πλατιάς

Αναπληρωτής Καθηγητής Ανδρέας Ν. Λιαρόπουλος

Ιανουάριος 2026

Το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον, τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Δημήτριος Μάλλιος

Ευχαριστίες

Η παρούσα διατριβή εκπονήθηκε στο πλαίσιο των ακαδημαϊκών μου σπουδών και δεν θα μπορούσε να ολοκληρωθεί χωρίς την συμβολή και την στήριξη ορισμένων ανθρώπων.

Θα ήθελα πρωτίστως να εκφράσω τις θερμές μου ευχαριστίες προς τον επιβλέποντα καθηγητή μου, Κύριο Γιάννη Κωνσταντόπουλο, για την επιστημονική καθοδήγηση, τις πολύτιμες υποδείξεις και την συνεχή υποστήριξη καθ' όλη την διάρκεια της εκπόνησης της διατριβής.

Ευχαριστώ επίσης τα μέλη της τριμελούς επιτροπής για τον χρόνο τους και τις εύστοχες παρατηρήσεις τους, οι οποίες συνέβαλαν ουσιαστικά στην βελτίωση της εργασίας.

Ιδιαίτερες ευχαριστίες οφείλω στην οικογένειά μου και ιδιαίτερα στην σύζυγό μου Μαρούλα, για την ηθική υποστήριξη, την υπομονή και την ενθάρρυνση που μου παρείχαν καθ' όλη την διάρκεια των σπουδών μου.

Τέλος, θα ήθελα να ευχαριστήσω όλους όσοι, άμεσα ή έμμεσα, συνέβαλαν στην ολοκλήρωση της παρούσας διατριβής.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

Η παρούσα μεταπτυχιακή εργασία εξετάζει τις ασύμμετρες απειλές στον κυβερνοχώρο ως φαινόμενο στρατηγικής, πολιτικής και τεχνολογικής πολυπλοκότητας. Η μελέτη αναλύει το θεωρητικό πλαίσιο της κυβερνοασφάλειας, τις γεωπολιτικές διαστάσεις, τις νομικές και πολιτικές προσεγγίσεις, και παρουσιάζει εμβληματικές μελέτες περίπτωσης από τον πραγματικό κόσμο. Μέσα από ποιοτική και συγκριτική ανάλυση, προτείνονται θεσμικά, πολιτικά και εκπαιδευτικά μέτρα για την ενίσχυση της εθνικής ανθεκτικότητας και της διεθνούς συνεργασίας.

Λέξεις κλειδιά: ασύμμετρες απειλές, κυβερνοασφάλεια, στρατηγική, διεθνές δίκαιο, κυβερνοχώρος

Abstract

This thesis examines asymmetric threats in cyberspace as a multifaceted phenomenon encompassing strategic, political, and technological dimensions. It explores the theoretical framework of cybersecurity, analyzes geopolitical implications, legal and policy responses, and presents key case studies. Through qualitative and comparative analysis, the study proposes institutional, policy, and educational measures to enhance national resilience and international cooperation.

Keywords: asymmetric threats, cybersecurity, strategy, international law, cyberspace

Εισαγωγή

Η έννοια της ασφάλειας στο διεθνές σύστημα υπήρξε ιστορικά άρρηκτα συνδεδεμένη με την υλική ισχύ, την εδαφική κυριαρχία και την στρατιωτική ικανότητα των κρατών. Από τον κλασικό ρεαλισμό έως τις σύγχρονες θεωρίες διεθνών σχέσεων, η ισχύς νοήθηκε ως η δυνατότητα επιβολής βούλησης εντός ενός αναρχικού διεθνούς συστήματος. Ωστόσο, η είσοδος του κυβερνοχώρου ως αυτόνομου πεδίου στρατηγικής δράσης έχει επιφέρει μια δομική μετατόπιση στον τρόπο με τον οποίο παράγεται, ασκείται και αμφισβητείται η ισχύς.

Ο κυβερνοχώρος δεν αποτελεί απλώς τεχνική υποδομή επικοινωνίας ή οικονομικής δραστηριότητας, αλλά νέο πεδίο συγκρότησης πολιτικής ισχύος, στο οποίο τα παραδοσιακά όρια μεταξύ πολέμου και ειρήνης, εσωτερικού και εξωτερικού, κρατικής και μη κρατικής δράσης καθίστανται ολοένα και πιο δυσδιάκριτα. Η ψηφιακή τεχνολογία επιτρέπει την άσκηση επιρροής χωρίς φυσική παρουσία, την πρόκληση σοβαρών διαταραχών χωρίς χρήση συμβατικής βίας και την υπονόμευση της κυριαρχίας χωρίς τυπική παραβίαση εδαφικών συνόρων.

Στο πλαίσιο αυτό, οι ασύμμετρες απειλές αναδεικνύονται σε κεντρικό χαρακτηριστικό της σύγχρονης διεθνούς ασφάλειας. Η ασυμμετρία δεν αφορά μόνο την διαφορά ισχύος μεταξύ αντιπάλων, αλλά κυρίως την διαφορά στρατηγικής λογικής: μικρότεροι ή τεχνολογικά ευέλικτοι δρώντες μπορούν να εκμεταλλευθούν την πολυπλοκότητα, την διασύνδεση και την εξάρτηση των σύγχρονων κοινωνιών, επιφέροντας δυσανάλογες πολιτικές, οικονομικές ή κοινωνικές συνέπειες. Η ισχύς, υπό αυτήν την έννοια, δεν εκφράζεται πλέον αποκλειστικά μέσω στρατιωτικών μέσων, αλλά μέσω του ελέγχου της πληροφορίας, των δεδομένων και της αφήγησης.

Η εξέλιξη αυτή έχει σημαντικές επιπτώσεις στην ίδια την έννοια της κρατικής κυριαρχίας. Η παραδοσιακή κυριαρχία, θεμελιωμένη στον έλεγχο του εδάφους και του πληθυσμού, μετασχηματίζεται σε λειτουργική και ψηφιακή κυριαρχία, η οποία εξαρτάται από την ικανότητα του κράτους να προστατεύει τις ψηφιακές του υποδομές, να διασφαλίζει την ακεραιότητα της πληροφορίας και να ελέγχει κρίσιμες ροές δεδομένων. Η αδυναμία άσκησης ελέγχου στον κυβερνοχώρο συνεπάγεται, πλέον, απώλεια πολιτικής αυτονομίας και στρατηγικής επιρροής.

Παράλληλα, το διεθνές σύστημα εισέρχεται σε μια περίοδο κανονιστικής και θεσμικής αβεβαιότητας. Το διεθνές δίκαιο και οι υφιστάμενοι θεσμοί ασφάλειας επιχειρούν να προσαρμοσθούν σε ένα περιβάλλον όπου οι πράξεις ισχύος συχνά δεν πληρούν τα κλασικά κριτήρια ένοπλης επίθεσης, αλλά παράγουν αποτελέσματα συγκρίσιμα με εκείνα της στρατιωτικής σύγκρουσης. Η απουσία σαφών μηχανισμών απόδοσης ευθύνης, η πολυπλοκότητα της τεχνικής τεκμηρίωσης και η πολιτικοποίηση της ευθύνης δημιουργούν ένα γκρίζο πεδίο στρατηγικής δράσης, το οποίο ευνοεί την ανάπτυξη ασύμμετρων πρακτικών.

Η παρούσα μεταπτυχιακή διατριβή προσεγγίζει τις ασύμμετρες απειλές στον κυβερνοχώρο ως δομικό στοιχείο της μεταβαλλόμενης διεθνούς τάξης. Η ανάλυση δεν περιορίζεται στην περιγραφή κυβερνοεπιθέσεων ή τεχνολογικών κινδύνων, αλλά εστιάζει στην θεωρητική και πολιτική σημασία του κυβερνοχώρου ως πεδίου ισχύος, ανταγωνισμού και θεσμικής διαπραγμάτευσης. Μέσα από την σύνθεση θεωριών διεθνών σχέσεων, στρατηγικών σπουδών και πολιτικής ανάλυσης, η εργασία επιχειρεί να ερμηνεύσει πώς οι ασύμμετρες κυβερνοαπειλές επηρεάζουν την ισορροπία ισχύος, την λειτουργία των θεσμών και την σταθερότητα του διεθνούς συστήματος.

Ιδιαίτερη βαρύτητα αποδίδεται στον ρόλο της Ευρωπαϊκής Ένωσης και του ΝΑΤΟ, καθώς και στη θέση της Ελλάδας εντός αυτών των πλαισίων. Η Ελλάδα, ως κράτος με αυξημένη γεωπολιτική σημασία στην Ανατολική Μεσόγειο, καλείται να αντιμετωπίσει τις ασύμμετρες απειλές όχι μόνο ως τεχνικό ζήτημα ασφάλειας, αλλά ως στρατηγικό και πολιτικό πρόβλημα εθνικής κυριαρχίας και διεθνούς τοποθέτησης.

Ο παρούσα Εισαγωγή λειτουργεί ως θεωρητική εισαγωγή στο Κεφάλαιο 1, το οποίο αναπτύσσει αναλυτικά το εννοιολογικό πλαίσιο της έρευνας. Η κατανόηση των ασύμμετρων απειλών στον κυβερνοχώρο προϋποθέτει την αναγνώριση ότι η ισχύς, η κυριαρχία και η ασφάλεια δεν είναι στατικές έννοιες, αλλά μεταβαλλόμενες κατηγορίες που επαναπροσδιορίζονται μέσα από την τεχνολογική και πολιτική εξέλιξη. Υπό αυτήν την έννοια, η μελέτη του κυβερνοχώρου δεν αφορά μόνο το παρόν της διεθνούς πολιτικής, αλλά και το μέλλον της διεθνούς τάξης.

Κεφάλαιο 1: Εισαγωγή και Εννοιολογικό Πλαίσιο

Η κατανόηση των ασύμμετρων απειλών στον κυβερνοχώρο απαιτεί συνδυασμό στρατηγικής θεωρίας, τεχνολογικής ανάλυσης και γεωπολιτικής ερμηνείας. Ο κυβερνοχώρος δεν αποτελεί απλώς τεχνικό σύστημα, αλλά ένα νέο πεδίο ισχύος και επιρροής.

1.1 Εισαγωγή: Ο κυβερνοχώρος ως νέο πεδίο ισχύος

Η μετάβαση από την βιομηχανική στην ψηφιακή εποχή έχει μεταμορφώσει ριζικά τον τρόπο με τον οποίο ασκείται η ισχύς. Η πληροφορία, άλλοτε δευτερεύον στρατηγικό αγαθό, αποτελεί σήμερα τον θεμέλιο λίθο της πολιτικής, στρατιωτικής και οικονομικής επιρροής. Στον 21ο αιώνα, η κυβερνοασφάλεια δεν αποτελεί τεχνικό υποσύστημα των κρατών, αλλά βασικό άξονα της εθνικής ισχύος (Nye, 2010· DeNardis, 2020).

Ο κυβερνοχώρος (cyberspace) χαρακτηρίζεται από διασυνδεσιμότητα, αορατότητα και ταχύτητα. Οι ιδιότητες αυτές του προσδίδουν ταυτόχρονα στρατηγική αξία και εγγενή αστάθεια. Ο διττός χαρακτήρας του -ως εργαλείο ανάπτυξης και ως πεδίο αντιπαράθεσης- έχει οδηγήσει τους μελετητές να τον ορίσουν ως *«το πέμπτο πεδίο πολέμου»* (Rid, 2013· NATO CCDCOE, 2023).

Η ψηφιακή σύγκλιση τεχνολογιών όπως το Cloud, το Internet of Things (IoT), η Artificial Intelligence (AI) και τα Cyber-Physical Systems (CPS) έχει δημιουργήσει ένα πολύπλοκο οικοσύστημα εξάρτησης, όπου η ασφάλεια ενός κόμβου επηρεάζει το σύνολο του συστήματος. Η ENISA (2024) υπογραμμίζει ότι *«η κυβερνοανθεκτικότητα είναι συλλογική - η ασφάλεια του ενός εξαρτάται από την ασφάλεια όλων»*.

Στο πλαίσιο αυτό, η έννοια της ασύμμετρης απειλής στον κυβερνοχώρο αποκτά νέα σημασία: μικρότεροι δρώντες, κρατικοί ή μη, μπορούν να προκαλέσουν δυσανάλογες επιπτώσεις σε ισχυρότερους αντιπάλους, εκμεταλλευόμενοι την διασύνδεση, την εξάρτηση και την διαφάνεια των δικτύων.

1.2 Εννοιολογική προσέγγιση της ασυμμετρίας

Η έννοια της ασυμμετρίας στην διεθνή πολιτική ανάγεται στην στρατηγική θεωρία του 20ού αιώνα, με πρώιμες ρίζες στην έννοια του «ανορθόδοξου πολέμου» (Mack, 1975· Arreguín-Toft, 2001). Η ασυμμετρία εκφράζει την διαφορά μέσων και στρατηγικής μεταξύ δύο αντιπάλων, όταν ο ασθενέστερος επιδιώκει να εκμεταλλευθεί τα τρωτά σημεία του ισχυρότερου.

Στον κυβερνοχώρο, η ασυμμετρία μεταφράζεται σε τεχνολογική εκμετάλλευση, ταχύτητα και ευελιξία. Οι επιθέσεις είναι οικονομικά φθηνές, συχνά μη ανιχνεύσιμες, και με εν δυνάμει στρατηγικό αντίκτυπο.

Η «ψηφιακή ασυμμετρία» (digital asymmetry) συνίσταται στο γεγονός ότι, οι επιτιθέμενοι εκμεταλλεύονται την ίδια την υποδομή του αντιπάλου -τους servers, τα δίκτυα, τις πλατφόρμες- για να επιφέρουν ζημία (Kello, 2017).

Η παραδοσιακή έννοια της ισχύος (power) επαναπροσδιορίζεται. Ο Joseph Nye (2010) εισήγαγε τον όρο “cyber power”, περιγράφοντας την δυνατότητα χρήσης του κυβερνοχώρου για την επίτευξη εθνικών στόχων, είτε μέσω coercion (εξαναγκασμού) είτε μέσω attraction (επιρροής).

Η ασύμμετρη κυβερνοϊσχύς (asymmetric cyber power) συνεπώς δεν βασίζεται στην κατοχή υλικών πόρων, αλλά στην πληροφοριακή ικανότητα πρόκλησης αβεβαιότητας.

1.3 Ο κυβερνοχώρος ως στρατηγικό περιβάλλον

Ο κυβερνοχώρος παρουσιάζει χαρακτηριστικά που τον καθιστούν μοναδικό πεδίο στρατηγικής δράσης (NATO CCDCOE, 2023):

1. Άυλος και μη χωρικός – δεν έχει γεωγραφικά όρια.
2. Διασυνδεδεμένος – κάθε κόμβος αποτελεί πιθανό σημείο τρωτότητας.
3. Αόρατος – οι επιθέσεις συχνά δεν γίνονται αντιληπτές.
4. Ταχύς – οι συγκρούσεις διαδραματίζονται σε πραγματικό χρόνο.
5. Αποπολιτικοποιημένος – οι δράσεις συχνά αποδίδονται σε «ανώνυμους» δρώντες.

Η στρατηγική αξία του κυβερνοχώρου έγκειται στο ότι διαπερνά όλους τους άλλους τομείς ισχύος: στρατιωτικό, οικονομικό, κοινωνικό και πληροφοριακό.
Ο Kello (2017) σημειώνει ότι *«η σύγκρουση στον κυβερνοχώρο δεν είναι ούτε πόλεμος ούτε ειρήνη – είναι μια νέα ενδιάμεση κατάσταση αστάθειας»*.

Η «κυβερνοστρατηγική» (cyber strategy) των κρατών βασίζεται στην ανίχνευση, αποτροπή και ανάκαμψη (detect, deter, recover).

Η απουσία φυσικών συνόρων καθιστά την άμυνα περισσότερο αντιδραστική παρά προληπτική. Έτσι, το στοιχείο της προληπτικής δράσης (defend forward) -όπως το υιοθέτησε το U.S. Cyber Command- αποτελεί προσπάθεια προσαρμογής των κλασικών εννοιών αποτροπής στο άυλο περιβάλλον.

1.4 Ιστορική Εξέλιξη του Κυβερνοπολέμου (1989–2025)

Η εξέλιξη των κυβερνοεπιχειρήσεων από το 1989 έως σήμερα δείχνει την μετάβαση από μεμονωμένα περιστατικά σε κρατικά ενορχηστρωμένες στρατηγικές.

Περίοδος	Σημαντικά Γεγονότα	Στρατηγική Σημασία
1989–1999	“Morris Worm” (1989), επιθέσεις σε δίκτυα Pentagon (1998)	Πρώτες ενδείξεις κυβερνοκατασκοπείας
2000–2009	Estonia (2007), Georgia (2008)	Γέννηση της έννοιας “Cyberwarfare”
2010–2015	Stuxnet (2010), Snowden leaks (2013)	Συνειδητοποίηση κρατικής εμπλοκής
2016–2019	NotPetya (2017), WannaCry (2017)	Μαζικές επιθέσεις οικονομικού χαρακτήρα
2020–2025	SolarWinds (2020), Ukraine War (2022), AI-driven threats	Υβριδικός πόλεμος & γνωστικές επιχειρήσεις

Από το Stuxnet και μετά, οι κυβερνοεπιχειρήσεις εντάσσονται ρητά στα στρατιωτικά δόγματα. Η ΕΕ (ENISA, 2024) και το NATO (CCDCOE, 2023) αναγνωρίζουν πλέον την κυβερνοασφάλεια ως θεμελιώδη διάσταση συλλογικής άμυνας.

Η περίοδος 2020–2025 χαρακτηρίζεται από την εισβολή της Τεχνητής Νοημοσύνης στην επιθετική και αμυντική κυβερνοστρατηγική.

Η ENISA (2024) επισημαίνει ότι *«οι αυτοματοποιημένες επιθέσεις και η παραποίηση δεδομένων μέσω AI αποτελούν τον κύριο αναδυόμενο κίνδυνο για την ευρωπαϊκή ασφάλεια»*.

1.5 Θεωρητικά Πλαίσια Ερμηνείας

Η θεωρητική ανάλυση των ασύμμετρων απειλών στον κυβερνοχώρο απαιτεί την ενσωμάτωση διαφορετικών σχολών σκέψης:

Α. Ρεαλισμός και Νεορεαλισμός

Ο κυβερνοχώρος αντιμετωπίζεται ως άναρχο πεδίο ισχύος.
Τα κράτη ανταγωνίζονται για έλεγχο και αποτροπή.
Η αποτροπή εδώ είναι ασταθής, αφού το attribution είναι αβέβαιο (Slayton, 2016).

Β. Φιλελευθερισμός

Η ασφάλεια μπορεί να επιτευχθεί μέσω θεσμών και συνεργασίας.
Ο ΟΗΕ, η ΕΕ και η ENISA λειτουργούν ως καθεστώτα διαχείρισης κινδύνου (Keohane & Nye, 2012).

Γ. Κονστρουκτιβισμός

Οι κυβερνονορμές (cyber norms) συγκροτούνται κοινωνικά, μέσω αποδοχής και νομιμοποίησης (Finnemore & Hollis, 2016).

Η ΕΕ επιδιώκει να καταστεί νομοθετική δύναμη στον κυβερνοχώρο.

Δ. Θεωρία Πληροφορίας

Η ισχύς απορρέει από τον έλεγχο των ροών δεδομένων και την ικανότητα διαχείρισης αφηγήματος (Lindsay, 2013).

Η πληροφορία είναι ταυτόχρονα όπλο, στόχος και πεδίο μάχης.

1.6 Ο κυβερνοχώρος ως πεδίο ασύμμετρης στρατηγικής

Η φύση του κυβερνοχώρου προσφέρει ένα μοναδικό στρατηγικό πλεονέκτημα σε δρώντες με περιορισμένους πόρους. Ενώ στο παρελθόν η στρατιωτική ισχύς απαιτούσε υποδομές και ανθρώπινο δυναμικό, σήμερα η τεχνολογική ευφυΐα και η πρόσβαση σε δίκτυα μπορούν να προκαλέσουν συγκρίσιμα αποτελέσματα.

Η ασύμμετρη κυβερνοϊσχύς (asymmetric cyber power) εκδηλώνεται όταν ένας δρών χρησιμοποιεί καινοτομία, απροσδόκητες μεθόδους ή ψυχολογικές επιθέσεις για να υπερκεράσει την ανωτερότητα του αντιπάλου (Libicki, 2009· Nye, 2010).

Η ασυμμετρία δεν αφορά μόνο τα μέσα, αλλά κυρίως την αντίληψη και τον χρονισμό. Οι επιτιθέμενοι εκμεταλλεύονται την αργή λήψη αποφάσεων των κρατών, την πολιτική πολυπλοκότητα και το κενό μεταξύ τεχνολογίας και νομοθεσίας.

Παράδειγμα αυτής της λογικής αποτελούν οι επιθέσεις NotPetya (2017) και SolarWinds (2020), όπου η στόχευση ήταν η εμπιστοσύνη στα συστήματα και όχι η φυσική υποδομή. Η ENISA (2024) τονίζει ότι *«η ασφάλεια των δεδομένων έχει μετατραπεί σε θεμέλιο της εθνικής κυριαρχίας»*.

Ο κυβερνοχώρος λειτουργεί έτσι ως επιταχυντής στρατηγικής αβεβαιότητας, όπου η ισορροπία ισχύος δεν καθορίζεται από τον αριθμό όπλων, αλλά από τον έλεγχο των πληροφοριακών ροών.

1.7 Τεχνολογική εξέλιξη και ασυμμετρία

Η τεχνολογία ενισχύει την ασυμμετρία μέσω δύο παραγόντων: της αυτοματοποίησης και της προσβασιμότητας.

1.7.1 Τεχνητή Νοημοσύνη (AI) και Αυτοματισμός Επιθέσεων

Η Τεχνητή Νοημοσύνη (AI) επιτρέπει την αυτόματη δημιουργία επιθέσεων, την προσαρμογή malware και την διεξαγωγή επιθέσεων με deepfakes.
Η ENISA (2024) προβλέπει ότι η AI-driven κυβερνοεγκληματικότητα θα αποτελέσει το μεγαλύτερο πεδίο ασύμμετρης απειλής έως το 2030.
Επιπλέον, η χρήση εργαλείων machine learning καθιστά δυνατή την «εξατομίκευση» των επιθέσεων (π.χ. spear-phishing μέσω προφίλ στα social media).

1.7.2 Κβαντική Υπολογιστική (Quantum Computing)

Η ανάπτυξη των κβαντικών υπολογιστών θέτει σε κίνδυνο τα σημερινά συστήματα κρυπτογράφησης.
Η μετάβαση σε post-quantum standards θεωρείται αναγκαία για την διασφάλιση κρίσιμων υποδομών (OECD, 2023).

1.7.3 Cloud και 5G Υποδομές

Η εξάρτηση από cloud υπηρεσίες και 5G δίκτυα αυξάνει την επιφάνεια επίθεσης, αλλά και την ευκαιρία για συνεργατική άμυνα.

Η ΕΕ επενδύει μέσω του προγράμματος GAIA-X στην δημιουργία ευρωπαϊκού οικοσυστήματος «ψηφιακής κυριαρχίας».

Συνολικά, η τεχνολογική καινοτομία αυξάνει την δυνατότητα επιθέσεων, ενώ ταυτόχρονα δημιουργεί ευκαιρίες για ανίχνευση, πρόβλεψη και πρόληψη.

1.8 Ο ανθρώπινος παράγοντας και οι γνωστικές επιχειρήσεις

Η ανθρώπινη διάσταση της ασφάλειας αποτελεί κρίσιμο παράγοντα.
Περίπου το 82% των περιστατικών παραβίασης το 2023 προήλθαν από ανθρώπινα λάθη, αμέλεια ή εξαπάτηση (Verizon Data Breach Report, 2024).

Οι γνωστικές επιχειρήσεις (cognitive operations) εστιάζουν στην χειραγώγηση της αντίληψης και της συμπεριφοράς των ατόμων ή των κοινωνιών.

Η Ρωσία, η Κίνα και άλλοι δρώντες αξιοποιούν ψυχολογικές επιχειρήσεις, παραπληροφόρηση και “narrative laundering” για να διαμορφώσουν πολιτικά περιβάλλοντα (NATO StratCom COE, 2023).

Η παραπληροφόρηση (disinformation) έχει αναχθεί σε βασικό όπλο της ασύμμετρης ισχύος. Οι εκλογικές παρεμβάσεις στις ΗΠΑ (2016–2020), στη Γαλλία (2017) και αλλού απέδειξαν ότι, η πληροφοριακή επιρροή μπορεί να αποσταθεροποιήσει δημοκρατίες χωρίς φυσική βία.

Η αντιμετώπιση αυτής της απειλής απαιτεί:

- Κριτική παιδεία (media literacy).
- Στρατηγική επικοινωνία από κράτη και θεσμούς.
- “Resilience by design”, δηλαδή ενσωμάτωση της ασφάλειας σε κοινωνικά και τεχνολογικά συστήματα (ENISA, 2024).

1.9 Ο κυβερνοχώρος ως παράγοντας γεωπολιτικής αστάθειας

Ο κυβερνοχώρος έχει αναδειχθεί σε καθοριστικό παράγοντα γεωπολιτικής αστάθειας, καθώς επιτρέπει την άσκηση ισχύος με τρόπους που υπερβαίνουν τα παραδοσιακά όρια της διεθνούς πολιτικής και της στρατιωτικής σύγκρουσης (Kello, 2017).
Σε αντίθεση με τα κλασικά πεδία αντιπαράθεσης, οι κυβερνοεπιχειρήσεις μπορούν να διεξάγονται χωρίς φυσική παρουσία, χωρίς άμεση ανάληψη ευθύνης και με χαμηλό πολιτικό κόστος για τον επιτιθέμενο (Nye, 2010).

Η αυξανόμενη εξάρτηση κρατών και κοινωνιών από ψηφιακές υποδομές καθιστά τον κυβερνοχώρο πεδίο στρατηγικής ευαλωτότητας, στο οποίο ακόμη και περιορισμένης κλίμακας επιθέσεις μπορούν να προκαλέσουν δυσανάλογες πολιτικές, οικονομικές και κοινωνικές συνέπειες (DeNardis, 2020).

Η διατάραξη πληροφοριακών συστημάτων, η παραβίαση κρίσιμων δικτύων και η χειραγώγηση δεδομένων επηρεάζουν άμεσα τη λειτουργία του κράτους και την εμπιστοσύνη των πολιτών προς τους θεσμούς (ENISA, 2024).

Στο πλαίσιο αυτό, η γεωπολιτική αστάθεια δεν εκδηλώνεται πλέον αποκλειστικά μέσω ένοπλων συγκρούσεων, αλλά μέσω μιας διαρκούς κατάστασης στρατηγικής αβεβαιότητας, η οποία

κινείται στη λεγόμενη «γκρίζα ζώνη» μεταξύ πολέμου και ειρήνης (Kello, 2017). Οι κυβερνοεπιχειρήσεις επιτρέπουν στα κράτη να επιδιώκουν πολιτικά και στρατηγικά οφέλη χωρίς να παραβιάζουν ρητά το διεθνές δίκαιο ή να ενεργοποιούν μηχανισμούς συλλογικής άμυνας (Schmitt, 2017).

Η δυσκολία απόδοσης ευθύνης (attribution) εντείνει περαιτέρω τη γεωπολιτική αστάθεια, καθώς περιορίζει την αποτελεσματικότητα της αποτροπής και αυξάνει τον κίνδυνο λανθασμένων πολιτικών ή στρατιωτικών αντιδράσεων (Slayton, 2016).
Η τεχνική αβεβαιότητα και η πολιτικοποίηση της ευθύνης επιτρέπουν στους δρώντες να αρνούνται εμπλοκή, δημιουργώντας συνθήκες ατιμωρησίας και ενισχύοντας τις ασύμμετρες πρακτικές ισχύος (Schmitt, 2017).

Οι μεγάλες δυνάμεις αξιοποιούν τον κυβερνοχώρο ως εργαλείο γεωπολιτικού ανταγωνισμού, εντάσσοντας τις κυβερνοεπιχειρήσεις σε ευρύτερες στρατηγικές επιρροής και αποσταθεροποίησης (Giles, 2021).

Οι Ηνωμένες Πολιτείες, η Ρωσία και η Κίνα χρησιμοποιούν τον κυβερνοχώρο τόσο για κατασκοπεία όσο και για πολιτική πίεση, επιδιώκοντας τη διαμόρφωση ευνοϊκών συσχετισμών ισχύος σε παγκόσμιο και περιφερειακό επίπεδο (NATO CCDCOE, 2023).

Παράλληλα, η Ευρωπαϊκή Ένωση αντιλαμβάνεται τον κυβερνοχώρο ως πεδίο κανονιστικής και θεσμικής παρέμβασης, επιδιώκοντας τη σταθεροποίηση του διεθνούς περιβάλλοντος μέσω συλλογικής ανθεκτικότητας και κανόνων συμπεριφοράς (European Commission, 2023).

Η προσέγγιση αυτή αντανακλά τη μετάβαση από τη στρατιωτική αποτροπή στην θεσμική διαχείριση της αστάθειας, με έμφαση στη συνεργασία και την πρόληψη (ENISA, 2024).

Ιδιαίτερη σημασία για τη γεωπολιτική αστάθεια έχει και η διάσταση των γνωστικών επιχειρήσεων.
Η παραπληροφόρηση, η χειραγώγηση αφηγήσεων και η στοχευμένη επιρροή μέσω ψηφιακών πλατφορμών υπονομεύουν τη δημοκρατική νομιμοποίηση και τη συνοχή των κοινωνιών, χωρίς να απαιτείται φυσική σύγκρουση (NATO StratCom COE, 2023).
Η γνωστική αυτή διάσταση της ασύμμετρης ισχύος μετατρέπει την πληροφορία σε στρατηγικό όπλο, ικανό να παράγει μακροχρόνια αποσταθεροποίηση (OECD, 2023).

Συνεπώς, ο κυβερνοχώρος λειτουργεί ως πολλαπλασιαστής γεωπολιτικής αστάθειας, καθώς συνδυάζει τεχνολογική καινοτομία, πολιτική αβεβαιότητα και θεσμικά κενά. Η κατανόηση αυτής της δυναμικής είναι κρίσιμη για την ερμηνεία της σύγχρονης διεθνούς τάξης και για τη διαμόρφωση στρατηγικών ασφάλειας που να ανταποκρίνονται στις ασύμμετρες προκλήσεις του ψηφιακού περιβάλλοντος (Kello, 2017; Nye, 2020).

Η Ανατολική Μεσόγειος καθίσταται πεδίο αυξημένου κινδύνου λόγω ενεργειακών υποδομών και γεωπολιτικών εντάσεων (CCDCOE, 2023).

Η Ελλάδα και η Κύπρος αντιμετωπίζουν ολοένα αυξανόμενες ασύμμετρες κυβερνοεπιθέσεις, κυρίως σε περιόδους πολιτικής έντασης με την Τουρκία.

1.10 Μεθοδολογική προσέγγιση της έρευνας

Η παρούσα έρευνα υιοθετεί ποιοτική–συγκριτική μεθοδολογία, με έμφαση σε περιπτωσιολογικές αναλύσεις (case studies) και θεσμικά κείμενα.

Βασικά στάδια:

1. Θεωρητική Ανάλυση – Επισκόπηση σχολών διεθνών σχέσεων και στρατηγικής σκέψης.
2. Εμπειρική Ανάλυση – Εξέταση κυβερνοεπιθέσεων και αντίδρασης θεσμών.
3. Συγκριτική Ερμηνεία – Αντιπαραβολή στρατηγικών (ΗΠΑ, ΕΕ, Ρωσία, Κίνα, Ελλάδα).
4. Σύνθεση Προτάσεων Πολιτικής – Διατύπωση θεσμικών και εκπαιδευτικών προτάσεων για την Ελλάδα.

Η μεθοδολογία στηρίζεται σε δευτερογενείς πηγές (επιστημονικά άρθρα, θεσμικές εκθέσεις ENISA, NATO, OECD, ΟΗΕ) και σε συγκριτική αξιολόγηση βάσει δεικτών κυβερνοανθεκτικότητας.

1.11 Συνοπτικά συμπεράσματα

Το Κεφάλαιο 1 ανέδειξε τον κυβερνοχώρο ως πυρήνα ασύμμετρης ισχύος και ως πεδίο γεωπολιτικής αντιπαράθεσης.

Οι βασικές διαπιστώσεις είναι:

1. Ο κυβερνοχώρος αποτελεί πολυεπίπεδο σύστημα που συνδέει τεχνολογία, πολιτική και κοινωνία.
2. Οι ασύμμετρες απειλές αναδεικνύουν την μετατόπιση ισχύος από το φυσικό στο πληροφοριακό επίπεδο.
3. Η ιστορική εξέλιξη δείχνει κλιμάκωση από μεμονωμένες επιθέσεις σε κρατικά ενορχηστρωμένες στρατηγικές.
4. Η τεχνητή νοημοσύνη και η ψηφιακή σύγκλιση ενισχύουν την ταχύτητα, πολυπλοκότητα και αβεβαιότητα των επιθέσεων.
5. Η ανθεκτικότητα και η διεθνής συνεργασία αποτελούν βασικούς πυλώνες αποτροπής.

Η επόμενη φάση της διατριβής -στο Θεωρητικό Πλαίσιο- θα αναλύσει πιο βαθιά τις σχολές σκέψης, τα μοντέλα κυβερνοαποτροπής και την σχέση ισχύος–τεχνολογίας στην διαμόρφωση του νέου παγκόσμιου συστήματος ασφάλειας.

Ενδεικτική Βιβλιογραφία (APA 7th)

Arreguín-Toft, I. (2001). *How the Weak Win Wars: A Theory of Asymmetric Conflict*. International Security, 26(1), 93–128.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

ENISA. (2024). *Threat Landscape 2024*. https://www.enisa.europa.eu

Finnemore, M., & Hollis, D. (2016). *Constructing Norms for Global Cybersecurity*. American Journal of International Law, 110(3), 425–479.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lindsay, J. R. (2013). *Stuxnet and the Limits of Cyberwarfare*. Security Studies, 22(3), 365–404.

NATO CCDCOE. (2023). *Cyber Defence Review 2023*. https://ccdcoe.org

Nye, J. S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs.

OECD. (2023). *Digital Security Risk Management Guidelines*. https://www.oecd.org

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.

Slayton, R. (2016). *What is the Cyber Offense-Defense Balance?* International Security, 41(3),

72–109.

Verizon. (2024). *Data Breach Investigations Report 2024*. https://www.verizon.com

Κεφάλαιο 2: Θεωρητικό Πλαίσιο και Ανάλυση Εννοιών

Η θεωρητική προσέγγιση του κυβερνοχώρου συνιστά τον πυρήνα της κατανόησης της νέας διεθνούς πραγματικότητας. Οι ασύμμετρες απειλές αποτελούν όχι μόνο τεχνικά φαινόμενα, αλλά δομικές μεταβλητές της σύγχρονης στρατηγικής ισορροπίας.

2.1 Εισαγωγή – Η αναγκαιότητα θεωρητικής προσέγγισης

Η μελέτη της κυβερνοασφάλειας, παρότι εντάσσεται στα πεδία της τεχνολογίας και των πληροφοριακών συστημάτων, απαιτεί βαθιά θεωρητική θεμελίωση.
Η ανάλυση των ασύμμετρων απειλών δεν μπορεί να περιοριστεί σε τεχνικούς όρους· συνιστά αντικείμενο διεθνών σχέσεων, στρατηγικής θεωρίας και πολιτικής φιλοσοφίας (Kello, 2017· DeNardis, 2020).

Στη διεθνή βιβλιογραφία, ο κυβερνοχώρος αντιμετωπίζεται είτε ως νέο πεδίο ισχύος (fifth domain) είτε ως διευρυμένη σφαίρα πληροφορίας, όπου η εξουσία διαμορφώνεται μέσω ελέγχου της γνώσης και των δικτύων (Nye, 2010).

Η θεωρητική κατανόηση των ασύμμετρων απειλών επομένως, απαιτεί ανάλυση της φύσης της ισχύος, των σχέσεων εξάρτησης και της νορμοποίησης που καθορίζει την συμπεριφορά των κρατών στον ψηφιακό χώρο.

2.2 Η θεωρία της ισχύος και η έννοια της κυβερνοϊσχύος

Η έννοια της ισχύος (power) έχει αποτελέσει αντικείμενο μελέτης από τον Θουκιδίδη έως τον Morgenthau και τον Waltz. Στο πεδίο των διεθνών σχέσεων, η ισχύς ορίζεται ως η ικανότητα ενός δρώντα να επιβάλλει τη βούλησή του (Morgenthau, 1948).

Στην ψηφιακή εποχή, ο Nye (2010) αναπροσάρμοσε την έννοια αυτή μέσω της θεωρίας της "cyber power", η οποία περιλαμβάνει τρεις μορφές:

1. Hard Cyber Power: Η χρήση επιθετικών δυνατοτήτων (cyber offense) για εξαναγκασμό.
2. Soft Cyber Power: Η διαμόρφωση αφηγήματος και επιρροής μέσω πληροφοριών, δεδομένων και κανόνων.

3. Smart Cyber Power: Συνδυασμός επιθετικών, θεσμικών και επικοινωνιακών στρατηγικών.

Η κυβερνοϊσχύς επομένως, δεν περιορίζεται στην στρατιωτική διάσταση· επεκτείνεται στην οικονομία, την τεχνολογία και την κοινωνία.

Ο Kello (2017) σημειώνει ότι *«ο κυβερνοπόλεμος δεν είναι απλώς νέα μορφή πολέμου, αλλά νέος τρόπος πολιτικής αλληλεπίδρασης»*.

Επιπλέον, η κυβερνοϊσχύς διαμορφώνεται μέσα από το οικοσύστημα εξάρτησης (dependence ecosystem), όπου η τεχνολογία αποτελεί ταυτόχρονα πηγή ισχύος και τρωτότητας (OECD, 2023). Η κατοχή τεχνολογικών υποδομών (π.χ. cloud, 5G, AI) συνεπάγεται επιρροή, αλλά και ευθύνη διαχείρισης των κινδύνων.

2.3 Η κυβερνοστρατηγική και η θεωρία της πληροφορίας

Η θεωρία της πληροφορίας (information theory) αναγνωρίζει την πληροφορία ως στρατηγικό αγαθό και όπλο.

Η πληροφορία δεν είναι ουδέτερη: παράγει εξουσία, καθοδηγεί αποφάσεις και διαμορφώνει πραγματικότητες (Lindsay, 2013).

Σύμφωνα με το NATO CCDCOE (2023), η κυβερνοστρατηγική (cyber strategy) βασίζεται σε τρεις αρχές:

1. Ανίχνευση (Detection): Προληπτικός εντοπισμός απειλών και ανάλυση δεδομένων.
2. Αποτροπή (Deterrence): Μείωση κινήτρων για επίθεση μέσω ικανότητας άμυνας.
3. Ανάκαμψη (Resilience): Επανόρθωση και διατήρηση λειτουργίας μετά από επίθεση.

Η πληροφορία ως μέσο ισχύος έχει διττό χαρακτήρα: λειτουργεί τόσο ως εργαλείο επιβολής όσο και ως πλαίσιο νομιμοποίησης.

Η ENISA (2024) υπογραμμίζει ότι «η ισχύς στον κυβερνοχώρο ασκείται μέσω της εμπιστοσύνης». Εάν οι πολίτες, οι θεσμοί και τα κράτη πάψουν να εμπιστεύονται τις πληροφορίες, καταρρέει η ίδια η δομή της εξουσίας.

Η κυβερνοστρατηγική συνεπώς δεν είναι μόνο τεχνική λειτουργία αλλά πολιτική πρακτική, που εδράζεται στη διαχείριση της αβεβαιότητας.

2.4 Ο κυβερνοχώρος υπό το πρίσμα των σχολών διεθνών σχέσεων

Η ερμηνεία του κυβερνοχώρου μέσω των θεωριών διεθνών σχέσεων αποκαλύπτει διαφορετικές διαστάσεις της ασφάλειας:

Θεωρία	Κεντρική Αντίληψη	Εφαρμογή στον Κυβερνοχώρο
Ρεαλισμός	Η ισχύς είναι το κύριο μέσο ασφάλειας	Κυβερνοχώρος ως πεδίο ανταγωνισμού ισχύος και αποτροπής
Νεορεαλισμός	Η αναρχία επιβάλλει στρατηγική επιβίωση	Cyber deterrence, επιθετικο-αμυντική ισορροπία
Φιλελευθερισμός	Η συνεργασία μειώνει την αβεβαιότητα	ENISA, ΕΕ, NATO – θεσμική διακυβέρνηση ασφάλειας
Κονστρουκτιβισμός	Οι ιδέες διαμορφώνουν την συμπεριφορά	Cyber norms, κοινωνική κατασκευή νομιμοποίησης

Οι ρεαλιστές αντιλαμβάνονται τον κυβερνοχώρο ως άναρχο σύστημα ισχύος όπου κυριαρχεί η λογική της αποτροπής. Οι φιλελεύθεροι τον θεωρούν ως πεδίο θεσμικής συνεργασίας και οικοδόμησης εμπιστοσύνης (Keohane & Nye, 2012).
Ο κονστρουκτιβισμός, τέλος, τονίζει τον ρόλο της κοινωνικής νομιμοποίησης: οι κυβερνονορμές δεν επιβάλλονται, αλλά διαμορφώνονται μέσω αλληλεπίδρασης (Finnemore & Hollis, 2016).

Η ενσωμάτωση αυτών των σχολών δημιουργεί το πλαίσιο μιας πολυπαραγοντικής θεωρίας κυβερνοασφάλειας, όπου η ισχύς, η συνεργασία και η νομιμοποίηση συνυπάρχουν.

2.5 Η θεωρία της σύνθετης αλληλεξάρτησης και η κυβερνοεξάρτηση

Η θεωρία της σύνθετης αλληλεξάρτησης (complex interdependence) των Keohane και Nye (2012) βρίσκει την φυσική της εξέλιξη στον κυβερνοχώρο.
Τα κράτη είναι ταυτόχρονα συνεργάτες και αντίπαλοι, συνδεδεμένα μέσω κοινών υποδομών και ροών πληροφορίας.

Η κυβερνοεξάρτηση (cyber interdependence) έχει δύο όψεις:

- Θετική: Ενισχύει την οικονομική ανάπτυξη και την διακρατική επικοινωνία.
- Αρνητική: Αυξάνει την ευπάθεια σε διασυνοριακές επιθέσεις και κρίσεις.

Παραδείγματα όπως το NotPetya (2017) και το SolarWinds (2020) αποδεικνύουν ότι η επίθεση σε έναν κόμβο μπορεί να έχει παγκόσμιες αλυσιδωτές συνέπειες.
Η ΕΕ αναγνωρίζει ότι «η κυβερνοασφάλεια είναι συλλογική ευθύνη» (European Commission, 2023).

Η θεωρία της αλληλεξάρτησης, συνεπώς, προσφέρει εννοιολογικό υπόβαθρο για την κατανόηση του κυβερνοχώρου ως δικτύου αμοιβαίων εξαρτήσεων, όπου η ασφάλεια του ενός εξαρτάται από την ευπάθεια του άλλου.

2.6 Η θεωρία της αποτροπής στον κυβερνοχώρο

Η αποτροπή (deterrence) αποτελεί θεμελιώδη έννοια των στρατηγικών σπουδών.
Στην κλασική της μορφή, βασίζεται στην απειλή αντιποίνων ως μέσο αποφυγής επίθεσης (Schelling, 1966).

Ωστόσο, η εφαρμογή της στον κυβερνοχώρο παρουσιάζει σημαντικές ιδιαιτερότητες.

Σύμφωνα με τον Libicki (2009), η κυβερνοαποτροπή (cyber deterrence) αποδυναμώνεται από τρεις παράγοντες:

1. Δυσκολία απόδοσης ευθύνης (attribution problem): συχνά είναι αδύνατη η άμεση ταυτοποίηση του δράστη.
2. Ασυμμετρία κόστους: το κόστος επίθεσης είναι ελάχιστο σε σχέση με το κόστος άμυνας.
3. Απουσία φυσικής ζημίας: δυσχεραίνει την δικαιολόγηση αντιποίνων βάσει διεθνούς δικαίου.

Η Taddeo (2019) προτείνει την έννοια της “αποτροπής μέσω ανθεκτικότητας” (deterrence by resilience), όπου ο στόχος δεν είναι η τιμωρία, αλλά η μείωση της αποτελεσματικότητας των επιθέσεων.

Η ανθεκτικότητα (resilience) ορίζεται ως η ικανότητα ενός συστήματος να προβλέπει, αντέχει και ανακάμπτει από επιθέσεις (ENISA, 2024).

Ο Slayton (2016) επισημαίνει ότι η ισορροπία επίθεσης–άμυνας στον κυβερνοχώρο είναι ρευστή, εξαρτώμενη από τεχνολογικές και θεσμικές εξελίξεις.
Έτσι, η αποτροπή δεν μπορεί να θεωρηθεί στατική στρατηγική, αλλά διαδικασία δυναμικής προσαρμογής.

2.7 Πόλεμος πληροφορίας και γνωστικές επιχειρήσεις

Η μετάβαση από τις φυσικές συγκρούσεις στις πληροφοριακές αποτελεί ίσως το πιο χαρακτηριστικό γνώρισμα της σύγχρονης ασυμμετρίας.

Ο πόλεμος πληροφορίας (information warfare) περιλαμβάνει τεχνικές παραπληροφόρησης, χειραγώγησης και ψυχολογικής πίεσης (NATO StratCom COE, 2023).

Η έννοια του "γνωστικού πολέμου" (cognitive warfare) εισήχθη από το NATO το 2021, για να περιγράψει τις επιχειρήσεις που στοχεύουν την ανθρώπινη αντίληψη και κρίση.
Σε αυτό το πλαίσιο, η ισχύς δεν ασκείται μέσω φυσικής βίας αλλά μέσω ελέγχου αφήγησης (narrative control).

Παραδείγματα γνωστικών επιχειρήσεων

- Εκλογές ΗΠΑ (2016–2020): χρήση fake news και botnets για επηρεασμό της κοινής γνώμης.
- Πανδημία COVID-19: εκστρατείες παραπληροφόρησης για εμβόλια και κρατικές πολιτικές (OECD, 2023).
- Πόλεμος στην Ουκρανία (2022–2023): συνδυασμός κυβερνοεπιθέσεων και ψυχολογικών επιχειρήσεων για απονομιμοποίηση θεσμών (NATO CCDCOE, 2023).

Η αντιμετώπιση των γνωστικών επιχειρήσεων απαιτεί πολυεπίπεδη στρατηγική:

- Ενίσχυση media literacy.
- Δημιουργία μηχανισμών ελέγχου αξιοπιστίας πληροφοριών.
- Συνεργασία κρατών και τεχνολογικών εταιρειών για περιορισμό των ψευδών ειδήσεων.

Η ENISA (2024) χαρακτηρίζει την παραπληροφόρηση ως «μη τεχνική απειλή με τεχνικές επιπτώσεις», καθώς μπορεί να οδηγήσει σε πραγματική κοινωνική αστάθεια.

2.8 Θεωρητικές προσεγγίσεις στην νορμοποίηση του κυβερνοχώρου

Η έννοια της νορμοποίησης (norm-building) αποτελεί βασικό στοιχείο της θεωρίας του κονστρουκτιβισμού.
Στον κυβερνοχώρο, η νορμοποίηση αφορά την δημιουργία κανόνων υπεύθυνης κρατικής συμπεριφοράς, όπως επιχειρείται από τον ΟΗΕ μέσω των ομάδων GGE και OEWG (United Nations, 2023).

Η Finnemore και ο Hollis (2016) υποστηρίζουν ότι οι κυβερνονορμές διαμορφώνονται διαδικαστικά και όχι επιτακτικά: μέσα από αλληλεπίδραση, συναίνεση και διαφάνεια. Η ΕΕ, με το Cyber Diplomacy Toolbox, επιδιώκει να θεσπίσει ένα πλαίσιο συλλογικής αποτροπής και κυρώσεων κατά κρατικών και μη κρατικών δραστών.

Το Tallinn Manual 2.0 (Schmitt, 2017) αποτελεί την σημαντικότερη νομική προσπάθεια ερμηνείας της εφαρμογής του διεθνούς δικαίου στον κυβερνοπόλεμο.
Αν και μη δεσμευτικό, λειτουργεί ως de facto πρότυπο για την ερμηνεία της κρατικής ευθύνης.

Η νορμοποίηση του κυβερνοχώρου εξαρτάται από την ισορροπία ανάμεσα σε κυριαρχία, διαφάνεια και συνεργασία.

Η πρόκληση είναι διττή: να διασφαλισθεί η κρατική ανεξαρτησία χωρίς να υπονομευθεί η παγκόσμια διαλειτουργικότητα.

2.9 Η κυβερνοασφάλεια ως παγκόσμιο δημόσιο αγαθό

Η έννοια του παγκόσμιου δημόσιου αγαθού (global public good) εφαρμόζεται πλέον στην κυβερνοασφάλεια (OECD, 2021).

Η αδυναμία ενός κράτους ή μιας επιχείρησης να προστατευθεί μπορεί να προκαλέσει διασυνοριακές συνέπειες.

Η Ευρωπαϊκή Ένωση έχει αναπτύξει το δόγμα της συλλογικής ανθεκτικότητας (collective resilience).

Η Οδηγία NIS2 (2023) και η Cybersecurity Act (2019) καθιστούν την ασφάλεια υποχρέωση όλων των κρίσιμων φορέων.

Η ENISA (2024) σημειώνει ότι «η κυβερνοασφάλεια είναι αδιαίρετο αγαθό – η απειλή σε έναν κρίκο της αλυσίδας θέτει σε κίνδυνο το σύνολο».
Η θεώρηση της ασφάλειας ως δημόσιου αγαθού μεταβάλλει το νομικό παράδειγμα από το "εθνικό δίκαιο προστασίας" στο "διεθνές καθεστώς συνεργασίας".

2.10 Θεωρητική σύνθεση και ερευνητικό μοντέλο

Η σύνθεση των ανωτέρω προσεγγίσεων οδηγεί σε ένα ολιστικό μοντέλο κατανόησης της ασφάλειας στον κυβερνοχώρο.

Βασικές Μεταβλητές:

- Ισχύς (Power): Ρεαλιστική θεώρηση της επιβολής μέσω τεχνολογίας.
- Πληροφορία (Information): Θεωρία πληροφορίας και πληροφοριακός πόλεμος.
- Αλληλεξάρτηση (Interdependence): Θεσμική και τεχνολογική εξάρτηση.
- Ανθεκτικότητα (Resilience): Νέα μορφή αποτροπής και συνεργασίας.
- Νομιμοποίηση (Legitimacy): Θεωρία νορμών και κονστρουκτιβισμός.

Σχηματικό Μοντέλο Θεωρητικής Ανάλυσης:
Ασύμμετρη Ισχύς → Έλεγχος Πληροφορίας → Επιρροή / Παραπληροφόρηση →
Θεσμική Αντίδραση → Ανθεκτικότητα → Νορμοποίηση / Σταθερότητα
Η κυβερνοασφάλεια μπορεί επομένως να αναλυθεί ως σύστημα δυναμικής ισορροπίας μεταξύ ισχύος και θεσμών, όπου η αποτροπή αντικαθίσταται από ανθεκτικότητα και προσαρμογή.

2.11 Συνοπτικά συμπεράσματα

Το Κεφάλαιο 2 θεμελίωσε το θεωρητικό πλαίσιο της διατριβής. Αναδείχθηκε ότι ο κυβερνοχώρος δεν είναι απλώς τεχνική υποδομή, αλλά σύστημα διεθνούς εξουσίας.

Η ισχύς εκδηλώνεται μέσω πληροφοριών, η ασφάλεια διασφαλίζεται μέσω συνεργασίας, και η σταθερότητα επιτυγχάνεται μέσω νορμοποίησης.

Οι θεωρίες των διεθνών σχέσεων, προσαρμοσμένες στο ψηφιακό περιβάλλον, επιτρέπουν την κατανόηση του κυβερνοχώρου ως θεσμικού πεδίου ισχύος και επιρροής.
Η επόμενη ενότητα της διατριβής θα μεταφέρει την ανάλυση στο γεωπολιτικό επίπεδο, εξετάζοντας την στρατηγική χρήση των ασύμμετρων απειλών από κράτη και συνασπισμούς.

Ενδεικτική Βιβλιογραφία (APA 7th)

Carr, M. (2010). *Inside Cyber Warfare*. O'Reilly.

DeNardis, L. (2020). *The Internet in Everything*. Yale University Press.

ENISA. (2024). *Threat Landscape 2024*. https://www.enisa.europa.eu

European Commission. (2023). *NIS2 Directive*. https://digital-strategy.ec.europa.eu

Finnemore, M., & Hollis, D. (2016). *Constructing Norms for Global Cybersecurity*. *AJIL, 110*(3), 425–479.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Keohane, R. O., & Nye, J. S. (2012). *Power and Interdependence in the Information Age*. Harvard University Press.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lindsay, J. R. (2013). *Stuxnet and the Limits of Cyberwarfare*. *Security Studies, 22*(3), 365–404.

NATO CCDCOE. (2023). *Cyber Defence Review 2023*. https://ccdcoe.org

NATO StratCom COE. (2023). *Cognitive Warfare and Strategic Communication*. https://stratcomcoe.org

Nye, J. S. (2010). *Cyber Power*. Belfer Center.

OECD. (2023). *Digital Security Risk Management Guidelines*. https://www.oecd.org

Schelling, T. (1966). *Arms and Influence*. Yale University Press.

Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Slayton, R. (2016). *What is the Cyber Offense-Defense Balance? International Security, 41*(3), 72–109.

Taddeo, M. (2019). *The Limits of Deterrence Theory in Cyberspace*. *Philosophy & Technology,*

32(3), 331–344.

United Nations. (2023). *OEWG Report on Developments in ICT*. A/78/112.

Κεφάλαιο 3: Γεωπολιτική και Στρατηγική Διάσταση των Ασύμμετρων Απειλών

Ο κυβερνοχώρος έχει μετατραπεί σε ένα πολυσύνθετο γεωπολιτικό περιβάλλον, όπου η ισχύς εκφράζεται μέσω δεδομένων, αλγορίθμων και δικτύων, επαναπροσδιορίζοντας τα όρια μεταξύ ασφάλειας, κυριαρχίας και στρατηγικής.

3.1 Εισαγωγή

Η άνοδος του κυβερνοχώρου ως νέου στρατηγικού πεδίου ισχύος έχει αναδιαμορφώσει τον τρόπο με τον οποίο τα κράτη, οι συνασπισμοί και οι μη κρατικοί δρώντες αντιλαμβάνονται τη γεωπολιτική ασφάλεια.

Η «ψηφιακή επανάσταση» έχει μετατρέψει την πληροφορία σε βασικό πυλώνα εθνικής ισχύος, οικονομικής ανάπτυξης και κοινωνικής σταθερότητας (DeNardis, 2020· Nye, 2020).

Η παραδοσιακή γεωπολιτική, που βασιζόταν στη γεωγραφία και τον έλεγχο φυσικών πόρων, έχει δώσει τη θέση της στη γεωπολιτική του κυβερνοχώρου - ενός πεδίου όπου η ισχύς δεν περιορίζεται σε εδάφη, αλλά εκδηλώνεται μέσα από δίκτυα και υποδομές πληροφορίας.

Όπως τονίζει το NATO CCDCOE (2023), ο κυβερνοχώρος *«δεν είναι απλώς τεχνικό πεδίο, αλλά το νέο υπόστρωμα της διεθνούς ισορροπίας ισχύος»*.
Η κατανόηση των ασύμμετρων απειλών στο πλαίσιο αυτό αποτελεί προϋπόθεση για την χάραξη εθνικών και διακρατικών στρατηγικών ασφάλειας.

3.2 Η έννοια της Κυβερνογεωπολιτικής

Η κυβερνογεωπολιτική (cybergeopolitics) αποτελεί την μελέτη της σχέσης μεταξύ ισχύος, τεχνολογίας και πληροφορίας στο διεθνές σύστημα (Deibert, 2013).
Σε αντίθεση με την κλασική γεωπολιτική, που εξετάζει τον έλεγχο φυσικών περιοχών, η κυβερνογεωπολιτική εστιάζει στον έλεγχο των ψηφιακών ροών - δεδομένων, επικοινωνιών και υποδομών.

Τα δίκτυα τηλεπικοινωνιών, οι πάροχοι υπηρεσιών cloud, τα data centers και οι δορυφορικές συνδέσεις αποτελούν τα νέα "γεωγραφικά σύνορα" της ισχύος (Kello, 2017). Η έννοια της ψηφιακής κυριαρχίας (digital sovereignty), που προωθείται από την ΕΕ (European Commission, 2023), αντικατοπτρίζει ακριβώς αυτήν την μετάβαση.

Η DeNardis (2020) υποστηρίζει ότι, ο έλεγχος της πληροφορίας δεν είναι μόνο τεχνικός, αλλά πολιτικός: *«η αρχιτεκτονική του διαδικτύου καθορίζει την κατανομή της εξουσίας»*. Έτσι, η κυβερνογεωπολιτική μελετά πώς η τεχνολογική εξάρτηση και η διασύνδεση υποδομών καθιστούν τα κράτη ταυτόχρονα ισχυρά και ευάλωτα.

3.3 Η ασυμμετρία στην παγκόσμια στρατηγική ισχύ

Η κυβερνοασφάλεια είναι από την φύση της ασύμμετρη. Οι δρώντες με περιορισμένους πόρους -κρατικοί ή μη- μπορούν να επιφέρουν δυσανάλογες ζημιές σε ισχυρότερους αντιπάλους μέσω χαμηλού κόστους επιθέσεων (ENISA, 2024).
Η «ψηφιακή ασυμμετρία» (digital asymmetry) αποτελεί το χαρακτηριστικό γνώρισμα της νέας εποχής ισχύος.

Κύρια χαρακτηριστικά της ασυμμετρίας:

1. Χαμηλό κόστος – υψηλός αντίκτυπος: Η ανάπτυξη malware, ransomware και DDoS επιθέσεων απαιτεί ελάχιστους πόρους, ενώ τα αποτελέσματα είναι στρατηγικής σημασίας.
2. Αορατότητα και άρνηση ευθύνης: Η τεχνολογική φύση των επιθέσεων επιτρέπει στους δρώντες να διατηρούν plausible deniability (Nye, 2017).
3. Συνδυασμός επιπέδων: Οι κυβερνοεπιχειρήσεις συνδυάζονται με πολιτικές, οικονομικές και ψυχολογικές στρατηγικές (Giles, 2021).

Η ασυμμετρία αυτή έχει επιφέρει μετατόπιση ισχύος από το στρατιωτικό στο πληροφοριακό πεδίο.

Σύμφωνα με το NATO CCDCOE (2023), *«οι ασύμμετρες επιθέσεις στον κυβερνοχώρο αποτελούν τον καταλύτη της στρατηγικής ανασφάλειας του 21ου αιώνα»*.

3.4 Στρατηγικές Μεγάλων Δυνάμεων

3.4.1 Ηνωμένες Πολιτείες Αμερικής

Οι ΗΠΑ διατηρούν τον πιο ανεπτυγμένο μηχανισμό κυβερνοστρατηγικής. Το U.S. Cyber Command (USCYBERCOM), σε συνεργασία με την NSA, εφαρμόζει το δόγμα "Defend Forward" (2020), δηλαδή προληπτική δράση εντός των δικτύων αντιπάλων για αποτροπή και διακοπή απειλών.

Η National Cybersecurity Strategy (2023) τονίζει ότι, η κυβερνοασφάλεια είναι υπόθεση "shared defense", όπου δημόσιος και ιδιωτικός τομέας συνεργάζονται. Οι ΗΠΑ προωθούν επίσης την διεθνή κυβερνοδιπλωματία, μέσα από το Cyber Diplomacy Act (2022).

Η στρατηγική των ΗΠΑ συνδυάζει τεχνολογική υπεροχή με θεσμική ηγεσία, στοχεύοντας στην παγκόσμια κανονιστική επιρροή.

3.4.2 Ρωσική Ομοσπονδία

Η Ρωσία αντιμετωπίζει τον κυβερνοχώρο ως πολιτικό όπλο επιρροής και μέσο αποσταθεροποίησης αντιπάλων.

Στο πλαίσιο του δόγματος Gerasimov, οι κυβερνοεπιχειρήσεις εντάσσονται στην έννοια του υβριδικού πολέμου.

Οι ομάδες APT28 (Fancy Bear) και APT29 (Cozy Bear) συνδέονται με επιχειρήσεις κυβερνοκατασκοπείας, εκλογικές παρεμβάσεις και επιθέσεις σε κρίσιμες υποδομές (Giles, 2021).
Η ρωσική στρατηγική δίνει έμφαση στην γνωστική επιρροή και στην διαμόρφωση αφηγήματος μέσω fake news και κοινωνικών δικτύων (NATO StratCom COE, 2023).

3.4.3 Λαϊκή Δημοκρατία της Κίνας

Η Κίνα αναπτύσσει μια μακροπρόθεσμη στρατηγική τεχνολογικής κυριαρχίας. Το Δόγμα Κυβερνοκυριαρχίας (Cyber Sovereignty) προωθεί τον εθνικό έλεγχο των ψηφιακών υποδομών και των δεδομένων.

Η PLA Unit 61398 και άλλες ομάδες APT έχουν εμπλακεί σε κυβερνοκατασκοπεία και βιομηχανική κατασκοπεία (Mandiant, 2022).

Παράλληλα, η Digital Silk Road Initiative (μέρος του Belt & Road) δημιουργεί δίκτυα τεχνολογικής εξάρτησης, μεταφέροντας την κινεζική επιρροή σε αναπτυσσόμενες χώρες (OECD, 2023).

Η Κίνα χρησιμοποιεί την "τεχνολογική εξάρτηση ως στρατηγικό εργαλείο ισχύος", οικοδομώντας παράλληλα το δικό της μοντέλο κυβερνοδιακυβέρνησης.

3.4.4 Ευρωπαϊκή Ένωση

Η ΕΕ λειτουργεί ως κανονιστική δύναμη στον κυβερνοχώρο. Η στρατηγική της εστιάζει στην ανθεκτικότητα, την κανονιστική ισχύ και την συλλογική ασφάλεια.
Κύρια εργαλεία:

- ENISA (2024) – παρακολούθηση απειλών και προώθηση κοινών προτύπων.
- NIS2 Directive (2023) – υποχρεωτική ασφάλεια κρίσιμων υποδομών.
- EU Cybersecurity Act (2019) – μηχανισμός πιστοποίησης.
- Joint Cyber Unit (2021) – επιχειρησιακή συνεργασία κρατών-μελών.

Η ΕΕ επιδιώκει τη συλλογική κυβερνοανθεκτικότητα (collective resilience) ως μέσο αποτροπής. Σύμφωνα με την Ευρωπαϊκή Επιτροπή (2023), η στρατηγική της Ένωσης βασίζεται στην «δημιουργία οικοσυστήματος εμπιστοσύνης και συνεργασίας».

3.4.5 Ιράν, Ισραήλ και Βόρεια Κορέα

- Ιράν: Επενδύει σε ασύμμετρες επιθέσεις μέσω ομάδων APT33/35, στοχεύοντας ενεργειακές και οικονομικές υποδομές.

- Ισραήλ: Αναγνωρισμένο κέντρο κυβερνοκαινοτομίας, με στρατηγική έμφαση στην πρόληψη και στην επιθετική αποτροπή.
- Βόρεια Κορέα: Συνδυάζει κυβερνοεπιθέσεις και οικονομικό κυβερνοέγκλημα για άντληση πόρων (Lazarus Group).

Αυτά τα κράτη επιβεβαιώνουν ότι, οι ασύμμετρες απειλές αποτελούν εργαλείο ισχύος για μη ηγεμονικές δυνάμεις.

3.5 Συγκριτική Ανάλυση Εθνικών Δογμάτων Κυβερνοστρατηγικής

Κράτος / Οργανισμός	Δόγμα	Κύριοι Άξονες	Παράδειγμα Εφαρμογής
ΗΠΑ	Defend Forward	Προληπτική δράση, αποτροπή, συνεργασία	Stuxnet, SolarWinds απάντηση
Ρωσία	Information Warfare	Υβριδικές επιχειρήσεις, παραπληροφόρηση	Εκλογές ΗΠΑ 2016
Κίνα	Cyber Sovereignty	Τεχνολογική αυτοδυναμία, εξάρτηση	Digital Silk Road
ΕΕ	Collective Resilience	Κανονιστική ισχύς, θεσμική διακυβέρνηση	NIS2 Directive
Ιράν	Asymmetric Retaliation	Αντεπίθεση μέσω κυβερνοπολέμου	Aramco (2019)
Ισραήλ	Proactive Deterrence	Επιθετική κυβερνοάμυνα	Επιχειρήσεις εναντίον APTs

Η συγκριτική ανάλυση δείχνει ότι οι κυβερνοστρατηγικές δεν είναι ομοιογενείς· αντανακλούν τις πολιτικές, τεχνολογικές και πολιτισμικές παραμέτρους κάθε κράτους. Παρά τις διαφορές, όλες κατατείνουν στην ανάγκη θεσμικής ανθεκτικότητας και διακρατικής συνεργασίας.

3.6 NATO και Κυβερνοαποτροπή

Το NATO αποτέλεσε τον πρώτο διακρατικό Οργανισμό που αναγνώρισε επίσημα τον κυβερνοχώρο ως "Operational Domain" το 2016, ισότιμο με ξηρά, θάλασσα, αέρα και διάστημα (NATO, 2016).

Από τότε, η Συμμαχία έχει υιοθετήσει μια ολοκληρωμένη προσέγγιση κυβερνοαποτροπής (cyber deterrence), η οποία βασίζεται στην αρχή της συλλογικής άμυνας (Άρθρο 5).

Η έννοια της αποτροπής στο NATO δεν περιορίζεται στην απειλή αντιποίνων· επεκτείνεται στην ανθεκτικότητα και την συνεργατική ασφάλεια.
Σύμφωνα με το NATO CCDCOE (2023), η στρατηγική της Συμμαχίας περιλαμβάνει:

1. Αποτροπή μέσω άρνησης (Deterrence by Denial): ενίσχυση της άμυνας και της ανθεκτικότητας.
2. Αποτροπή μέσω κόστους (Deterrence by Punishment): πολιτικές, οικονομικές ή στρατιωτικές κυρώσεις.
3. Αποτροπή μέσω κανόνων (Normative Deterrence): διαμόρφωση διεθνών νορμών συμπεριφοράς.

Το Cooperative Cyber Defence Centre of Excellence (CCDCOE), με έδρα το Ταλίν, αποτελεί τον πυρήνα ερευνητικής και επιχειρησιακής δράσης του NATO.
Η Συμμαχία έχει διεξάγει ασκήσεις όπως Locked Shields και Crossed Swords, που προσομοιώνουν συνθήκες μαζικών επιθέσεων σε κρίσιμες υποδομές.

Η Στρατηγική Αντίληψη του NATO (NATO Strategic Concept, 2022) επιβεβαιώνει ότι «μια σημαντική κυβερνοεπίθεση μπορεί να προκαλέσει συλλογική απάντηση».
Η πρόκληση, ωστόσο, παραμένει η πολιτική συναίνεση και η τεχνική απόδειξη ευθύνης.

3.7 Η Ευρωπαϊκή Ένωση και η Πολυεπίπεδη Διακυβέρνηση του Κυβερνοχώρου

Η Ευρωπαϊκή Ένωση (ΕΕ) προσεγγίζει την κυβερνοασφάλεια ως συλλογικό, κανονιστικό και θεσμικό αγαθό.

Η ΕΕ λειτουργεί όχι ως στρατιωτικός συνασπισμός, αλλά ως ρυθμιστής κανόνων και προτύπων.

Η στρατηγική της ΕΕ για την κυβερνοασφάλεια διαρθρώνεται σε τρεις άξονες:

1. Θεσμικός και Επιχειρησιακός Άξονας

- ENISA: παρέχει τεχνική υποστήριξη, συντονισμό και ανάλυση κινδύνου.
- CSIRTs Network: διακρατική ανταλλαγή πληροφοριών για περιστατικά ασφαλείας.
- Joint Cyber Unit (2021): πλατφόρμα άμεσης αντίδρασης σε κρίσεις.

2. Νομοθετικός Άξονας

- NIS2 Directive (2023): ενίσχυση των απαιτήσεων ασφάλειας για κρίσιμες υποδομές.
- EU Cybersecurity Act (2019): πλαίσιο πιστοποίησης προϊόντων και υπηρεσιών ασφάλειας.
- Cyber Resilience Act (2024): νέοι κανόνες για την αλυσίδα εφοδιασμού λογισμικού.

3. Διπλωματικός Άξονας

- EU Cyber Diplomacy Toolbox (2021): καθορίζει μέτρα κυρώσεων κατά κρατικών δραστών.
- Cybersecurity Skills Academy (2024): πρωτοβουλία για εκπαίδευση και κατάρτιση ειδικών.

Η ΕΕ στοχεύει στην δημιουργία "Digital Strategic Autonomy", δηλαδή της ικανότητας να προστατεύει τις ψηφιακές υποδομές της χωρίς εξάρτηση από τρίτους (European Commission, 2023).

Η κανονιστική ισχύς (Normative Power Europe) εκφράζεται μέσα από την ικανότητα της Ένωσης να επιβάλλει κανόνες συμπεριφοράς και να λειτουργεί ως παγκόσμιος ρυθμιστής στον τομέα της κυβερνοασφάλειας.

3.8 Η Ανατολική Μεσόγειος και η Ελληνική Κυβερνοστρατηγική

Η Ανατολική Μεσόγειος αναδεικνύεται σε έναν από τους πιο ευαίσθητους χώρους κυβερνογεωπολιτικής αντιπαράθεσης, λόγω:

- των ενεργειακών υποδομών (ΑΟΖ Ελλάδας–Κύπρου),
- της στρατιωτικής παρουσίας μεγάλων δυνάμεων,
- και των περιφερειακών εντάσεων (Ελλάδα–Τουρκία, Ισραήλ–Ιράν).

Ελλάδα

Η Ελλάδα έχει εκπονήσει την Εθνική Στρατηγική Κυβερνοασφάλειας (2020–2025), που βασίζεται σε πέντε πυλώνες:

1. Θεσμική διακυβέρνηση και ρόλος της ΕΑΚ (Εθνική Αρχή Κυβερνοασφάλειας).
2. Προστασία κρίσιμων υποδομών (ενέργεια, μεταφορές, τηλεπικοινωνίες).
3. Εκπαίδευση και ευαισθητοποίηση πολιτών.
4. Συνεργασία με διεθνείς οργανισμούς (ΕΕ, NATO, ENISA).
5. Έρευνα και καινοτομία (Cybersecurity Innovation Hub).

Η Ελλάδα συμμετέχει ενεργά στο CCDCOE και σε ευρωπαϊκές ασκήσεις όπως το Cyber Europe.
Επιπλέον, έχει ενισχύσει την συνεργασία με το Ισραήλ και την Κύπρο, δημιουργώντας έναν τριμερή άξονα κυβερνοασφάλειας.

Τουρκία

Η Τουρκία, μέσω του δόγματος "Milli Siber Güvenlik Stratejisi" (Εθνική Στρατηγική Κυβερνοασφάλειας), έχει αναπτύξει ισχυρή κρατική υποδομή κυβερνοάμυνας.
Η ρητορική της για «ψηφιακή ανεξαρτησία» εντάσσεται στη στρατηγική της τεχνολογικής αυτοδυναμίας.

Ισραήλ

Το Ισραήλ αποτελεί παγκόσμιο πρότυπο κυβερνοκαινοτομίας.
Η Israel National Cyber Directorate (INCD) ενοποιεί την άμυνα, την βιομηχανία και την εκπαίδευση, ενώ το κράτος λειτουργεί ως "Cyber Power Broker" στην περιοχή.

Η Ανατολική Μεσόγειος μετατρέπεται έτσι σε περιφερειακό εργαστήριο κυβερνοστρατηγικών ανταγωνισμών, όπου οι ασύμμετρες απειλές συχνά λειτουργούν ως εργαλεία πολιτικής πίεσης.

3.9 Ο Υβριδικός Πόλεμος και η Γνωστική Διάσταση της Στρατηγικής

Ο υβριδικός πόλεμος (hybrid warfare) είναι η σύζευξη στρατιωτικών, οικονομικών, κυβερνο- και πληροφοριακών εργαλείων για την επίτευξη πολιτικών στόχων.
Σύμφωνα με το NATO (2023), οι υβριδικές απειλές περιλαμβάνουν:

- Κυβερνοεπιθέσεις σε κρίσιμες υποδομές.
- Εκστρατείες παραπληροφόρησης.
- Ενεργειακό εκβιασμό.
- Παρεμβάσεις σε εκλογικές διαδικασίες.

Παραδείγματα:

- Ουκρανία (2014–2023): συνδυασμός κυβερνοεπιθέσεων και στρατιωτικών επιχειρήσεων.
- ΕΕ (2019–2024): εκστρατείες παραπληροφόρησης σε κοινωνικά δίκτυα.
- Ελλάδα (2020–2023): επιθέσεις DDoS και παραπληροφόρηση κατά περιόδους έντασης με την Τουρκία.

Η γνωστική διάσταση (cognitive dimension) των ασύμμετρων απειλών στοχεύει στην αντίληψη του αντιπάλου.

Ο πόλεμος της πληροφορίας δεν διεξάγεται μόνο στα δίκτυα, αλλά και στις συνειδήσεις των πολιτών.

Ο έλεγχος του αφηγήματος (“narrative control”) είναι πλέον εξίσου σημαντικός με τον έλεγχο των δεδομένων (NATO StratCom COE, 2023).

3.10 Συμπεράσματα – Το νέο γεωπολιτικό παράδειγμα

Η γεωπολιτική του κυβερνοχώρου επιβεβαιώνει ότι η ισχύς στον 21ο αιώνα είναι δικτυωμένη, διαμοιρασμένη και ασύμμετρη.

Η στρατηγική σημασία των δεδομένων, η εξάρτηση των υποδομών και η διασύνδεση των κοινωνιών καθιστούν την κυβερνοασφάλεια αναπόσπαστο πυλώνα διεθνούς πολιτικής.

Βασικές διαπιστώσεις:

1. Η ασύμμετρη ισχύς αναδεικνύεται σε κανονικότητα του διεθνούς συστήματος.
2. Η ΕΕ, μέσω της κανονιστικής της ισχύος, μπορεί να λειτουργήσει ως παγκόσμιος σταθεροποιητής.

3. Το ΝΑΤΟ και η ΕΕ πρέπει να ενισχύσουν την συνέργεια μεταξύ στρατιωτικής και θεσμικής ασφάλειας.
4. Η Ελλάδα διαθέτει τα εχέγγυα να εξελιχθεί σε περιφερειακό κόμβο κυβερνοανθεκτικότητας.

Το νέο γεωπολιτικό παράδειγμα θεμελιώνεται σε μια ολοκληρωμένη στρατηγική προσέγγιση, όπου η ασφάλεια, η τεχνολογία και η γνώση συνυπάρχουν.
Ο κυβερνοχώρος δεν είναι πια το «πέμπτο πεδίο πολέμου» - είναι ο συνδετικός ιστός όλων των πεδίων.

Ενδεικτική Βιβλιογραφία (APA 7th)

CCDCOE. (2023). *Cyber Defence Review 2023*. NATO Cooperative Cyber Defence Centre of Excellence.

Deibert, R. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. McClelland & Stewart.

DeNardis, L. (2020). *The Internet in Everything*. Yale University Press.

ENISA. (2024). *Threat Landscape Report 2024*. https://www.enisa.europa.eu

European Commission. (2023). *NIS2 Directive & Cyber Resilience Act*. https://digital-strategy.ec.europa.eu

Giles, K. (2021). *Russia's Hybrid War in Ukraine: Lessons for the West*. NATO Defence College.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Mandiant. (2022). *APT Activity Report: China and Cyber Espionage Trends*. https://www.mandiant.com

NATO. (2016). *Warsaw Summit Communiqué*. NATO Headquarters.

NATO. (2022). *Strategic Concept 2022*. NATO Headquarters.

NATO StratCom COE. (2023). *Cognitive Warfare and Strategic Communication*. https://stratcomcoe.org

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

OECD. (2023). *Digital Security Risk Management Guidelines*. https://www.oecd.org

Κεφάλαιο 4: Πολιτικές και Νομικές Προσεγγίσεις των Ασύμμετρων Απειλών

Η πολιτική και νομική διάσταση της κυβερνοασφάλειας καθορίζει το πλαίσιο μέσα στο οποίο τα κράτη και οι διεθνείς Οργανισμοί επιχειρούν να διαχειρισθούν ένα ασταθές, άυλο και διασυνοριακό περιβάλλον ασύμμετρης ισχύος.

4.1 Εισαγωγή

Η διαχείριση των ασύμμετρων απειλών στον κυβερνοχώρο συνιστά μία από τις μεγαλύτερες προκλήσεις διακυβέρνησης του 21ου αιώνα.
Ο κυβερνοχώρος υπερβαίνει τα εδαφικά σύνορα, περιλαμβάνει ιδιωτικούς και κρατικούς φορείς, και χαρακτηρίζεται από αορατότητα, διαλειτουργικότητα και νομική αβεβαιότητα.
Η πολιτική και νομική αντιμετώπιση του φαινομένου απαιτεί πολυεπίπεδη διακυβέρνηση (multi-level governance):

- σε διεθνές επίπεδο, καθορισμό νορμών συμπεριφοράς·
- σε ευρωπαϊκό επίπεδο, θεσμική εναρμόνιση·
- και σε εθνικό επίπεδο, ανάπτυξη ανθεκτικών θεσμών και πολιτικών.

Η ENISA (2024) επισημαίνει ότι «η πολιτική ασφάλειας δεν είναι στατική αλλά εξελικτική – εξαρτάται από την νομιμοποίηση και την συνεργασία».
Η διαμόρφωση θεσμικών και νομικών μηχανισμών είναι συνεπώς ζωτικής σημασίας για την επιβίωση των κρατών στον νέο κυβερνο-κόσμο.

4.2 Το Διεθνές Δίκαιο και ο Κυβερνοχώρος

Παρότι δεν υπάρχει ακόμη ενιαία δεσμευτική συνθήκη για τις κυβερνοεπιθέσεις, το διεθνές δίκαιο παρέχει κατευθυντήριες αρχές.

Σύμφωνα με τον Χάρτη των Ηνωμένων Εθνών (1945), οι βασικές αρχές της κυριαρχίας, της μη επέμβασης και της αυτοάμυνας ισχύουν και στον κυβερνοχώρο (Schmitt, 2017).

Η εφαρμογή του διεθνούς δικαίου στον κυβερνοπόλεμο επικεντρώνεται σε τρία ερωτήματα:

1. Πότε μια κυβερνοενέργεια συνιστά χρήση βίας ή ένοπλη επίθεση;
2. Πώς αποδίδεται ευθύνη σε κρατικούς και μη κρατικούς δρώντες;
3. Ποια είναι τα όρια της αυτοάμυνας στο ψηφιακό πεδίο;

Η νομική επιστήμη εξελίσσεται με οδηγό το Tallinn Manual 2.0 (Schmitt, 2017), το οποίο ορίζει 154 κανόνες εφαρμογής του διεθνούς δικαίου στον κυβερνοχώρο.
Αν και μη δεσμευτικό, το Manual λειτουργεί ως de facto σημείο αναφοράς για κράτη και θεσμούς όπως το NATO και η ΕΕ.

Η αρχή της κυριαρχίας (principle of sovereignty) στο ψηφιακό περιβάλλον είναι αντικείμενο έντονου διαλόγου:
ενώ τα κράτη επιθυμούν έλεγχο των δικτύων τους, η φύση του Διαδικτύου επιβάλλει παγκόσμια διαλειτουργικότητα.

Η ένταση μεταξύ αυτών των δύο αξιών -ασφάλεια και ελευθερία- διαμορφώνει τον πυρήνα του διεθνούς κυβερνοδικαίου (Tikk & Kerttunen, 2023).

4.3 ΟΗΕ, GGE και OEWG: Νορμοποίηση και Διεθνής Διάλογος

Ο Οργανισμός Ηνωμένων Εθνών αποτελεί το βασικό φόρουμ θεσμικής νορμοποίησης του κυβερνοχώρου.

Οι δύο κύριες πρωτοβουλίες του -το Group of Governmental Experts (GGE) και το Open-Ended Working Group (OEWG)- έχουν καθοριστικό ρόλο στην διαμόρφωση κανόνων υπεύθυνης συμπεριφοράς.

Το GGE (2004–2021) εισήγαγε την ιδέα ότι οι αρχές του διεθνούς δικαίου εφαρμόζονται πλήρως στον κυβερνοχώρο.

Το OEWG (2021–2025), με ευρύτερη συμμετοχή κρατών, επικεντρώνεται σε μέτρα οικοδόμησης εμπιστοσύνης (CBMs) και σε μηχανισμούς συνεργασίας για διαχείριση περιστατικών.

Η Έκθεση του ΟΗΕ (A/78/112, 2023) υπογράμμισε τη σημασία:

- της διαφάνειας και της ανταλλαγής πληροφοριών,
- της ενίσχυσης των ικανοτήτων των αναπτυσσόμενων κρατών,
- και της διαδικασίας επίλυσης διαφορών μέσω διαλόγου.

Η UN νορμοποίηση συνιστά βήμα προς μια “Cyber Charter of Conduct”, αν και η απουσία μηχανισμού επιβολής περιορίζει την αποτελεσματικότητά της.

4.4 Κυριαρχία, Ευθύνη και Απόδοση Ευθύνης

Η απόδοση ευθύνης (attribution) είναι το σημαντικότερο νομικό ζήτημα της κυβερνοασφάλειας.
Σύμφωνα με το Tallinn Manual 2.0, η κρατική ευθύνη προϋποθέτει απόδειξη άμεσης συμμετοχής ή κρατικής καθοδήγησης (Article 8, ILC 2001).
Η τεχνική πολυπλοκότητα των επιθέσεων καθιστά αυτό το έργο εξαιρετικά δύσκολο.

Η ENISA (2024) προτείνει την υιοθέτηση πολυεπίπεδης μεθοδολογίας attribution, που συνδυάζει τεχνικά δεδομένα (forensics), αναλυτικά ευρήματα και διπλωματική εκτίμηση.
Η κρατική κυριαρχία μετασχηματίζεται σε λειτουργική κυριαρχία, που εξαρτάται από την δυνατότητα ενός κράτους να προστατεύει τις ψηφιακές του υποδομές.

Η ΕΕ έχει θεσπίσει το Cyber Sanctions Regime (2019), το οποίο επιτρέπει κυρώσεις κατά δραστών κυβερνοεπιθέσεων, ακόμη και χωρίς πλήρη απόδειξη ευθύνης.
Αυτό σηματοδοτεί την μετάβαση από την «απόδειξη» στην πολιτική ερμηνεία της ευθύνης - στοιχείο ασυνήθιστο για το κλασικό διεθνές δίκαιο.

4.5 Το Tallinn Manual 2.0 και το Διεθνές Εθιμικό Δίκαιο

Το Tallinn Manual 2.0 (2017), έργο του NATO CCDCOE, θεωρείται το σημαντικότερο κείμενο για την εφαρμογή του διεθνούς δικαίου στον κυβερνοπόλεμο.
Αναγνωρίζει ότι οι αρχές της κυριαρχίας, αναλογικότητας και αυτοάμυνας ισχύουν και για τον κυβερνοχώρο, με προσαρμογές.
Σύμφωνα με τον Schmitt (2017):

- Μια κυβερνοεπίθεση συνιστά «ένοπλη επίθεση» αν προκαλεί υλικές συνέπειες αντίστοιχες φυσικής βίας.
- Οι κυβερνοενέργειες χαμηλότερης έντασης υπόκεινται στο διεθνές δίκαιο μη επέμβασης.

Η ερμηνεία του Manual προσφέρει εργαλείο "soft law" που επιτρέπει στα κράτη να ευθυγραμμίζουν την εθνική νομοθεσία τους.

Ωστόσο, η εφαρμογή του είναι ανεπίσημη και εθελοντική, γεγονός που υπογραμμίζει την ανάγκη για παγκόσμια συνθήκη κυβερνοασφάλειας.

4.6 Η Ευρωπαϊκή Θεσμική Αρχιτεκτονική Κυβερνοασφάλειας

Η ΕΕ έχει αναπτύξει ένα πολυεπίπεδο σύστημα διακυβέρνησης κυβερνοασφάλειας, το οποίο συνδυάζει νομικές, πολιτικές και τεχνικές πτυχές:

Πυλώνας	Θεσμοί / Πολιτικές	Περιγραφή
Νομοθετικός	NIS2 Directive (2023), Cybersecurity Act (2019), GDPR	Εναρμόνιση κανόνων, προστασία δεδομένων
Θεσμικός	ENISA, CSIRTs Network, Joint Cyber Unit	Επιχειρησιακός συντονισμός
Πολιτικός	Cyber Diplomacy Toolbox (2021), Cyber Sanctions	Κυρώσεις, διεθνής συνεργασία

Η ΕΕ επιδιώκει τη δημιουργία ενός ενιαίου "Cybersecurity Framework", που θα επιτρέπει διαλειτουργικότητα και κοινή απόκριση σε απειλές.

Η ENISA (2024) λειτουργεί ως *think tank* για στρατηγική πρόβλεψη κινδύνων και ανάλυση τάσεων.

Το NIS2 αποτελεί ορόσημο, καθώς επεκτείνει το ρυθμιστικό πλαίσιο σε νέους τομείς, όπως οι μεταφορές, η υγεία και οι δημόσιες υπηρεσίες.

4.7 Το Νομικό Πλαίσιο της Ελλάδας

Η Ελλάδα έχει υιοθετήσει πλήρως το ευρωπαϊκό μοντέλο κυβερνοασφάλειας. Κύριες θεσμικές παρεμβάσεις:

- Νόμος 4577/2018: ενσωμάτωση της Οδηγίας NIS, σύσταση Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ).
- Νόμος 4727/2020: Κώδικας Ψηφιακής Διακυβέρνησης και προστασία ψηφιακών υπηρεσιών.
- Εθνική Στρατηγική Κυβερνοασφάλειας (2020–2025): ενίσχυση θεσμικής συνεργασίας και συμμετοχής σε ευρωπαϊκά σχήματα.
- CERT-ΕΛ: λειτουργεί ως εθνικό σημείο επαφής για συμβάντα κυβερνοασφάλειας.

Η Ελλάδα συμμετέχει ενεργά στην ENISA, στο CCDCOE και στο GFCE (Global Forum on Cyber Expertise).

Παρά την πρόοδο, προκλήσεις παραμένουν στην στελέχωση, στην διαλειτουργικότητα φορέων και στην εκπαίδευση δημοσίων υπαλλήλων.

4.8 Δημόσιος και Ιδιωτικός Τομέας: Διακυβέρνηση και Συνεργασία

Η κυβερνοασφάλεια δεν αποτελεί αποκλειστικά κρατική αρμοδιότητα.
Η συντριπτική πλειονότητα των κρίσιμων υποδομών -ενέργεια, τηλεπικοινωνίες, χρηματοπιστωτικά συστήματα- ανήκει ή λειτουργεί από τον ιδιωτικό τομέα. Επομένως, η διασφάλιση της κυβερνοανθεκτικότητας απαιτεί δημόσιο-ιδιωτική συνεργασία (Public–Private Partnership, PPP).

Μορφές Συνεργασίας

1. Information Sharing and Analysis Centers (ISACs): θεσμικές πλατφόρμες ανταλλαγής πληροφοριών.
2. Cyber Exercises: κοινές ασκήσεις προσομοίωσης κυβερνοεπιθέσεων (π.χ. *Cyber Europe 2024* της ENISA).
3. Certification Frameworks: υποχρεωτική συμμόρφωση σε πρότυπα ασφάλειας (ISO 27001, NIS2).

4. Cyber Insurance & Risk Management: ανάπτυξη μηχανισμών κάλυψης κινδύνου.

Η ENISA (2024) υπογραμμίζει ότι η συνεργασία δημόσιου–ιδιωτικού τομέα είναι «ο ακρογωνιαίος λίθος της συλλογικής ανθεκτικότητας».
Στην Ελλάδα, το Εθνικό Δίκτυο Κυβερνοασφάλειας επιδιώκει την διασύνδεση κρατικών φορέων, τραπεζών και τηλεπικοινωνιακών εταιρειών για κοινή στρατηγική απόκρισης.

4.9 Νομικά και Ηθικά Διλήμματα

Η εφαρμογή του δικαίου στον κυβερνοχώρο εγείρει σειρά ηθικών και νομικών ζητημάτων:

1. Απόδοση Ευθύνης (Attribution):
   Η τεχνική ταυτοποίηση δεν επαρκεί για νομική ευθύνη· απαιτείται πολιτική βούληση και διαφάνεια (Tikk & Kerttunen, 2023).
2. Αναλογικότητα Αντίδρασης:
   Πότε μια κυβερνοεπίθεση δικαιολογεί στρατιωτική ή οικονομική απάντηση;
   Το Tallinn Manual προβλέπει ότι η αντίδραση πρέπει να είναι *"necessary and proportionate"*.
3. Ιδιωτικότητα έναντι Ασφάλειας:
   Η ισορροπία μεταξύ προστασίας δεδομένων (GDPR) και εθνικής ασφάλειας αποτελεί διαρκές δίλημμα (DeNardis, 2020).
4. Κρατική Ευθύνη Ιδιωτικών Πράξεων:
   Όταν ιδιωτικές ομάδες ενεργούν με σιωπηρή υποστήριξη κρατών, πώς τεκμηριώνεται η εμπλοκή τους; (United Nations, 2023).
5. Ανθρώπινα Δικαιώματα στον Κυβερνοχώρο:
   Η μαζική παρακολούθηση και οι κυβερνοεπιχειρήσεις εγείρουν ζητήματα ελευθερίας λόγου και ψηφιακής ιδιωτικότητας (OECD, 2023).

Η νομοθετική πρόοδος δεν μπορεί να αποτρέψει πλήρως τις συγκρούσεις αυτών των αξιών. Απαιτείται ηθική διακυβέρνηση (ethical governance) που θα βασίζεται σε διαφάνεια, λογοδοσία και πολυμερή εποπτεία.

4.10 Παραδείγματα Εφαρμογής και Νομολογίας

Η πρακτική εμπειρία από σημαντικές κυβερνοεπιθέσεις αποδεικνύει την ανάγκη ενίσχυσης του νομικού πλαισίου:

Περιστατικό	Ζήτημα	Νομική / Πολιτική Αντίδραση
Stuxnet (2010)	Κυριαρχία – Αυτοάμυνα	Απουσία επίσημης νομικής αντίδρασης· διεθνής σιωπή
Sony Hack (2014)	Κρατική εμπλοκή	Κυρώσεις ΗΠΑ στη Βόρεια Κορέα
NotPetya (2017)	Απόδοση ευθύνης	ΕΕ & ΝΑΤΟ απέδωσαν την ευθύνη στη Ρωσία
SolarWinds (2020)	Κατασκοπεία	Κυρώσεις ΗΠΑ & NIS2 ενίσχυση ευρωπαϊκής άμυνας
Colonial Pipeline (2021)	Ενεργειακή ασφάλεια	Νομοθετική πρωτοβουλία ΗΠΑ για cyber resilience

Τα παραδείγματα αυτά αποδεικνύουν ότι το διεθνές δίκαιο στον κυβερνοχώρο λειτουργεί πρωτίστως πολιτικά: η νομική αναγνώριση συχνά εξαρτάται από την στρατηγική σκοπιμότητα.

4.11 Πολιτικές Αποτροπής και Θεσμικές Στρατηγικές

Η αποτροπή (deterrence) στον κυβερνοχώρο δεν είναι μονοδιάστατη· απαιτεί πολυεπίπεδη προσέγγιση:

Μορφή Αποτροπής	Μηχανισμός	Παράδειγμα
Μέσω Κόστους	Κυρώσεις, αποκλεισμοί, διπλωματική πίεση	ΕΕ 2019 – Sanctions Regime
Μέσω Άρνησης	Ενίσχυση αμυντικών ικανοτήτων	ENISA – Resilience Framework
Μέσω Νομιμοποίησης	Διαμόρφωση νορμών συμπεριφοράς	UN OEWG – Responsible State Behavior

Η ΕΕ έχει υιοθετήσει πολιτική “deterrence by resilience”, δηλαδή ενίσχυση ανθεκτικότητας μέσω θεσμών, εκπαίδευσης και διακρατικής συνεργασίας (ENISA, 2024).
Η Ελλάδα, στο πλαίσιο της ΕΕ και του ΝΑΤΟ, εναρμονίζεται με αυτήν την προσέγγιση, επενδύοντας στην προληπτική εκπαίδευση και τη συντονισμένη απόκριση.

4.12 Προτάσεις Πολιτικής και Θεσμικής Ενοποίησης

Με βάση τα πορίσματα της έρευνας, προτείνονται οι ακόλουθες κατευθύνσεις πολιτικής:

1. Διεθνής Διάσταση

- Δημιουργία Διεθνούς Συνθήκης Κυβερνοασφάλειας υπό την αιγίδα του ΟΗΕ.
- Θεσμοθέτηση μηχανισμού διαιτησίας για απόδοση ευθύνης (Cyber Arbitration Panel).
- Καθιέρωση παγκόσμιου μητρώου κυβερνοεπιθέσεων για διαφάνεια και πρόληψη.

2. Ευρωπαϊκή Διάσταση

- Εναρμόνιση νομοθεσίας κυβερνοδικαίου στα κράτη-μέλη.
- Δημιουργία Ευρωπαϊκού Οργανισμού Ψηφιακής Κυβερνοδικαιοσύνης (EADC).
- Ανάπτυξη κοινού μηχανισμού “Cyber Rapid Reaction Teams” για κρίσεις.

3. Εθνική Διάσταση (Ελλάδα)

- Αναβάθμιση της ΕΑΚ με αρμοδιότητα εποπτείας ιδιωτικών παρόχων.
- Καθιέρωση Εθνικού Μηχανισμού Κυβερνοαποτροπής σε συνεργασία με το ΥΠΕΞ και το ΥΠΕΘΑ.
- Ενίσχυση της κυβερνοεκπαίδευσης στα σώματα ασφαλείας και στην δημόσια διοίκηση.
- Ανάπτυξη Cyber Education & Research Network στα πανεπιστήμια.

Η υλοποίηση αυτών των προτάσεων θα ενίσχυε την θεσμική συνοχή, θα μείωνε την κατακερματισμένη ευθύνη και θα προήγαγε μια κουλτούρα συνεργατικής ασφάλειας.

4.13 Συμπεράσματα Κεφαλαίου

Η πολιτική και νομική θεώρηση του κυβερνοχώρου αναδεικνύει την ανάγκη συστημικής προσέγγισης.
Οι ασύμμετρες απειλές δεν μπορούν να αντιμετωπιστούν από μεμονωμένα κράτη ή νόμους· απαιτούν διεθνή συνεργασία, θεσμική συνέργεια και κοινωνική ανθεκτικότητα.

Βασικά συμπεράσματα:

1. Το διεθνές δίκαιο εφαρμόζεται στον κυβερνοχώρο, αλλά χρειάζεται επικαιροποίηση.
2. Η ΕΕ διαμορφώνει πρότυπο πολυεπίπεδης διακυβέρνησης.
3. Η Ελλάδα έχει σημειώσει πρόοδο, αλλά απαιτείται ολοκληρωμένη θεσμική στρατηγική.
4. Η απόδοση ευθύνης και η νορμοποίηση παραμένουν τα μεγαλύτερα νομικά ζητήματα.
5. Η ανθεκτικότητα και η εκπαίδευση είναι τα ισχυρότερα μέσα αποτροπής.

Η σύγχρονη ασφάλεια στον κυβερνοχώρο δεν περιορίζεται στην τεχνολογία - είναι πολιτική πράξη, που αντικατοπτρίζει τις αξίες, τα θεσμικά συστήματα και την ωριμότητα των δημοκρατιών.

Ενδεικτική Βιβλιογραφία (APA 7th)

DeNardis, L. (2020). *The Internet in Everything*. Yale University Press.

ENISA. (2024). *Threat Landscape 2024*. https://www.enisa.europa.eu

European Commission. (2023). *NIS2 Directive & Cyber Resilience Act*. https://digital-strategy.ec.europa.eu

OECD. (2023). *Digital Security Policy Framework*. https://www.oecd.org

Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Taddeo, M. (2019). *The Limits of Deterrence Theory in Cyberspace*. *Philosophy & Technology*, *32*(3), 331–344.

Tikk, E., & Kerttunen, M. (2023). *Attribution and International Law in Cyberspace*. CCDCOE Publications.

United Nations. (2023). *Report of the Open-Ended Working Group on Developments in ICT*. A/78/112.

Υπουργείο Ψηφιακής Διακυβέρνησης. (2020). *Εθνική Στρατηγική για την Κυβερνοασφάλεια 2020–2025*. https://mindigital.gr

Council of the EU. (2019). *Cyber Sanctions Regime*. Brussels.

Κεφάλαιο 5: Μελέτες Περίπτωσης και Εφαρμοσμένα Παραδείγματα Ασύμμετρων Απειλών

5.1 Εισαγωγή

Οι κυβερνοεπιθέσεις του 21ου αιώνα αποδεικνύουν ότι ο κυβερνοχώρος έχει μετατραπεί σε πεδίο άσκησης ισχύος και πολιτικού εκβιασμού. Η ανάλυση των ασύμμετρων απειλών στον κυβερνοχώρο δεν μπορεί να περιοριστεί αποκλειστικά στην θεωρητική ή θεσμική διάσταση, αλλά απαιτεί την εμπειρική διερεύνηση πραγματικών περιπτώσεων, μέσω των οποίων καθίσταται ορατός ο τρόπος με τον οποίο η ψηφιακή ισχύς μεταφράζεται σε πολιτικά και γεωπολιτικά αποτελέσματα. Οι μελέτες περίπτωσης επιβεβαιώνουν ότι η ασύμμετρη δράση μικρών ή μη κρατικών δρώντων μπορεί να έχει στρατηγικά αποτελέσματα συγκρίσιμα με ένοπλες επιχειρήσεις. Περαιτέρω, οι μελέτες περίπτωσης επιτρέπουν την σύνδεση της θεωρίας με την πράξη, αποκαλύπτοντας τόσο τις επιχειρησιακές πρακτικές, όσο και τις στρατηγικές λογικές που διέπουν την χρήση του κυβερνοχώρου ως πεδίου ασύμμετρης δράσης.

Για τον λόγο αυτό, το παρόν κεφάλαιο υιοθετεί διττή μεθοδολογική προσέγγιση. Στο πρώτο μέρος αναλύονται συγκεκριμένα περιστατικά κυβερνοεπιθέσεων (incident-based case studies), τα οποία λειτούργησαν ως ορόσημα στην διεθνή ασφάλεια και ανέδειξαν νέες μορφές ψηφιακής απειλής. Στο δεύτερο μέρος, η ανάλυση μετατοπίζεται σε κρατοκεντρικές περιπτωσιολογικές μελέτες (state-based case studies), εξετάζοντας πώς διαφορετικοί δρώντες (ΗΠΑ, Ρωσία, Κίνα, Ευρωπαϊκή Ένωση) ενσωματώνουν τον κυβερνοχώρο στην συνολική τους στρατηγική. Η διάκριση αυτή επιτρέπει την κατανόηση τόσο των μεμονωμένων επιχειρήσεων, όσο και των βαθύτερων στρατηγικών και γεωπολιτικών προτύπων που διαμορφώνουν την ασύμμετρη ισχύ στον κυβερνοχώρο.

ΜΕΡΟΣ Α΄: Σ*υγκεκριμένα περιστατικά κυβερνοεπιθέσεων*

Η ανάλυση πραγματικών περιστατικών κυβερνοεπιθέσεων προσφέρει πολύτιμη κατανόηση των προτύπων ασύμμετρης συμπεριφοράς και των μηχανισμών στρατηγικής επιρροής.

Οι μελέτες περίπτωσης αποκαλύπτουν τον τρόπο με τον οποίο οι τεχνολογικές πράξεις μεταφράζονται σε πολιτικά και γεωπολιτικά αποτελέσματα.

5.2 Stuxnet (2010): Η Γένεση του Ψηφιακού Πολέμου

Η επίθεση Stuxnet αποτελεί το πρώτο τεκμηριωμένο παράδειγμα κυβερνοεπιχείρησης που προκάλεσε φυσική καταστροφή κρίσιμης υποδομής. Η στοχευμένη αλλοίωση των βιομηχανικών συστημάτων ελέγχου στο πυρηνικό πρόγραμμα του Ιράν ανέδειξε τον κυβερνοχώρο ως μέσο στρατηγικής προληπτικής δράσης. Το περιστατικό αυτό κατέδειξε ότι η κυβερνοϊσχύς μπορεί να λειτουργήσει ως υποκατάστατο στρατιωτικής επέμβασης, δημιουργώντας προηγούμενο για τη χρήση ψηφιακών μέσων σε ζητήματα υψηλής πολιτικής. Αναπτύχθηκε από ΗΠΑ και Ισραήλ στο πλαίσιο της επιχείρησης "Olympic Games", με στόχο τις πυρηνικές εγκαταστάσεις του Ιράν στο Νατάνζ.

Τεχνικά χαρακτηριστικά:

- Πολυσύνθετο worm που εκμεταλλεύτηκε τέσσερα zero-day exploits.
- Παραβίασε το σύστημα ελέγχου Siemens SCADA και άλλαξε τις ταχύτητες φυγοκεντρητών.
- Είχε τη δυνατότητα να αυτοαναπαράγεται χωρίς ανθρώπινη παρέμβαση.

Αποτελέσματα:

- Καταστροφή περίπου 1.000 φυγοκεντρητών.
- Καθυστέρηση του ιρανικού πυρηνικού προγράμματος για τουλάχιστον δύο έτη (Zetter, 2014).
- Παγκόσμια συζήτηση για τη νομιμότητα των "κυβερνοόπλων".

Στρατηγική Σημασία:

Το Stuxnet άνοιξε την εποχή του κυβερνοπολέμου υψηλής πολυπλοκότητας, εισάγοντας το μοντέλο "digital preemption" - προληπτική ψηφιακή επίθεση για στρατηγική αποτροπή.

5.3 WannaCry (2017): Η Παγκοσμιοποίηση του Ransomware

Το WannaCry ήταν η πρώτη παγκόσμια επίθεση ransomware που έδειξε την παγκοσμιοποιημένη φύση της ψηφιακής εξάρτησης.
Η ταχύτατη εξάπλωση του κακόβουλου λογισμικού (μέσα σε 48 ώρες, προσέβαλε 230.000 συστήματα σε 150 χώρες, παραλύοντας νοσοκομεία, επιχειρήσεις και δημόσιες Υπηρεσίες), αποκάλυψε την ευαλωτότητα κρίσιμων δημόσιων υποδομών και την διασύνδεση της

κυβερνοασφάλειας με την κοινωνική ευημερία. Η περίπτωση αυτή επιβεβαιώνει ότι, ακόμη και μη στρατηγικά σχεδιασμένες επιθέσεις μπορούν να παράγουν συστημική αστάθεια.

Κύρια Στοιχεία:

- Εκμεταλλεύτηκε την ευπάθεια EternalBlue των Windows, η οποία είχε διαρρεύσει από την NSA.
- Ζητούσε πληρωμή λύτρων σε Bitcoin.
- Χτύπησε ιδιαίτερα το βρετανικό σύστημα υγείας (NHS).

Απόδοση Ευθύνης:

Η επίθεση αποδόθηκε στη Βόρεια Κορέα (ομάδα Lazarus) από ΗΠΑ, Ηνωμένο Βασίλειο και ΕΕ (ENISA, 2024).

Στρατηγική Ανάγνωση:

Το WannaCry αποκάλυψε ότι η ασφάλεια των κρίσιμων υποδομών εξαρτάται από παλαιά συστήματα, δείχνοντας την ανάγκη για διαρκή τεχνολογική αναβάθμιση και διεθνή συντονισμό.

5.4 NotPetya (2017): Ο Πόλεμος της Καταστροφής Δεδομένων

Το NotPetya, αρχικά παρουσιάστηκε ως ransomware, αλλά στην πραγματικότητα ήταν όπλο κυβερνοσαμποτάζ. Σε αντίθεση με το WannaCry, το NotPetya σχεδιάστηκε με σκοπό την καταστροφή και όχι το οικονομικό όφελος. Η μαζική απώλεια δεδομένων και οι παγκόσμιες οικονομικές επιπτώσεις κατέδειξαν ότι ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί ως εργαλείο στρατηγικού σαμποτάζ. Το περιστατικό αυτό υπογραμμίζει τη μετάβαση από την κυβερνοεγκληματικότητα στον κυβερνοπόλεμο χαμηλής έντασης.

Ξεκίνησε από την Ουκρανία και εξαπλώθηκε σε όλο τον κόσμο, επηρεάζοντας επιχειρήσεις όπως η Maersk και η Merck.

Τεχνική Ανάλυση:

- Διαδόθηκε μέσω της εφαρμογής λογιστικής M.E.Doc.
- Προκάλεσε οριστική καταστροφή δεδομένων, χωρίς δυνατότητα ανάκτησης.

- Χρησιμοποίησε τεχνικές lateral movement και credential theft.

Αποτίμηση:

- Οικονομική ζημία > 10 δισ. δολάρια (Greenberg, 2019).
- Αναστάτωση σε κρίσιμους τομείς μεταφορών και φαρμακοβιομηχανίας.

Απόδοση Ευθύνης:

Η επίθεση αποδόθηκε σε μονάδες της Ρωσικής GRU (APT28).
Το Ηνωμένο Βασίλειο και οι ΗΠΑ κατήγγειλαν επισήμως τη Ρωσία για κρατικά υποκινούμενη κυβερνοεπίθεση (Council on Foreign Relations, 2023).

Στρατηγική Σημασία:

Το NotPetya αποτέλεσε ορόσημο στον κυβερνοσαμποτάζ και έδειξε πως μια επίθεση σε έναν μικρό τομέα μπορεί να προκαλέσει παγκόσμια οικονομική κρίση.

5.5 SolarWinds (2020): Η Αθέατη Διείσδυση

Η επίθεση SolarWinds αποκαλύπτει τη νέα μορφή συστημικής ευπάθειας των αλυσίδων εφοδιασμού (supply chain vulnerability).
Μέσω μιας "αθώας" ενημέρωσης λογισμικού Orion, οι επιτιθέμενοι απέκτησαν πρόσβαση σε περισσότερους από 18.000 οργανισμούς, συμπεριλαμβανομένων αμερικανικών κυβερνητικών Υπηρεσιών.
Ανάλυση:

- Εισαγωγή κακόβουλου κώδικα στο στάδιο ανάπτυξης του λογισμικού.
- Παρακολούθηση χωρίς άμεση καταστροφή· στόχος η κατασκοπεία.
- Παραβίαση των Υπουργείων Οικονομικών, Ενέργειας και Άμυνας των ΗΠΑ.

Απόδοση Ευθύνης:

Αποδόθηκε στη ρωσική ομάδα APT29 (Cozy Bear) (Mandiant, 2022).

Στρατηγική Ερμηνεία:

Η επίθεση ανέδειξε τη σημασία της ασφάλειας εφοδιαστικής αλυσίδας λογισμικού (Software Supply Chain Security) και της ανάγκης ελέγχου των τρίτων παρόχων. Οδήγησε στην αμερικανική Executive Order 14028 (2021) για την ενίσχυση της κυβερνοασφάλειας σε εθνικό επίπεδο.

5.6 Colonial Pipeline (2021): Κυβερνοεπίθεση στην Ενεργειακή Αλυσίδα

Η επίθεση στη Colonial Pipeline στις ΗΠΑ (Μάιος 2021) αποτέλεσε σημείο καμπής για τη σύνδεση ψηφιακής και φυσικής ασφάλειας.
Η ομάδα DarkSide πραγματοποίησε επίθεση ransomware, διακόπτοντας τη λειτουργία του μεγαλύτερου αγωγού καυσίμων της χώρας, μήκους 8.800 χλμ.
Επιπτώσεις:

- Διακοπή εφοδιασμού σε 12 πολιτείες για πέντε ημέρες.
- Οικονομικές απώλειες και πανικός στην αγορά ενέργειας.
- Πληρωμή λύτρων ύψους 4,4 εκατ. δολαρίων σε Bitcoin.

Αντίδραση:
Η αμερικανική κυβέρνηση ενεργοποίησε τον μηχανισμό CISA–FBI–DOE, ενώ η Executive Order 14028 (2021) θεσμοθέτησε νέα πρότυπα cyber resilience για κρίσιμες υποδομές (CISA, 2022).

Στρατηγική Ανάγνωση:

Η Colonial Pipeline αποκάλυψε την αλληλεξάρτηση κυβερνοχώρου και ενεργειακής ασφάλειας, επιβεβαιώνοντας ότι η προστασία των “critical infrastructures” είναι πλέον ζήτημα εθνικής επιβίωσης (OECD, 2023).

Τα παραπάνω περιστατικά αποδεικνύουν ότι οι κυβερνοεπιθέσεις δεν αποτελούν μεμονωμένα τεχνικά γεγονότα, αλλά εντάσσονται σε ευρύτερες στρατηγικές λογικές. Ωστόσο, η ανάλυση μεμονωμένων επιθέσεων δεν επαρκεί για την κατανόηση της ασύμμετρης ισχύος στον κυβερνοχώρο. Απαιτείται η διερεύνηση των κρατικών στρατηγικών που παράγουν, αξιοποιούν ή ρυθμίζουν αυτές τις πρακτικές.

ΜΕΡΟΣ Β΄: Κ*ρατοκεντρικές περιπτωσιολογικές μελέτες*

5.7 Ηνωμένες Πολιτείες Αμερικής: Κυβερνοϊσχύς και προληπτική αποτροπή

Οι Ηνωμένες Πολιτείες αποτελούν την πλέον χαρακτηριστική περίπτωση κράτους που αντιλαμβάνεται τον κυβερνοχώρο ως πυλώνα εθνικής ισχύος και όχι απλώς ως τεχνικό πεδίο ασφάλειας. Η αμερικανική κυβερνοστρατηγική ενσωματώνεται πλήρως στο ευρύτερο στρατιωτικό και γεωπολιτικό δόγμα της χώρας, συνδέοντας την κυβερνοασφάλεια με την αποτροπή, την προβολή ισχύος και τη διατήρηση της διεθνούς ηγεμονίας (Nye, 2010; Kello, 2017).

Η ίδρυση του U.S. Cyber Command (USCYBERCOM) και η αναβάθμισή του σε ανεξάρτητη διοίκηση (2018) σηματοδότησαν τη θεσμική αναγνώριση του κυβερνοχώρου ως πεδίου επιχειρήσεων. Το δόγμα “Defend Forward”, όπως αποτυπώνεται στη U.S. National Cyber Strategy (2018, 2023), προβλέπει προληπτική δράση εντός των δικτύων του αντιπάλου, με στόχο την αποτροπή επιθέσεων πριν αυτές εκδηλωθούν.

Η υπόθεση Stuxnet αποτελεί εμβληματικό παράδειγμα αυτής της στρατηγικής. Η χρήση κυβερνοεπιθέσεων για την επίτευξη στρατηγικών στόχων χωρίς άμεση στρατιωτική εμπλοκή κατέδειξε τη δυνατότητα των ΗΠΑ να αξιοποιούν τον κυβερνοχώρο ως εργαλείο ασύμμετρης υπεροχής, ακόμη και απέναντι σε κρατικούς αντιπάλους (Zetter, 2014). Παράλληλα, επιθέσεις όπως το SolarWinds (2020) ανέδειξαν τα όρια της αμερικανικής άμυνας και την τρωτότητα των αλυσίδων εφοδιασμού.

Συνολικά, η αμερικανική περίπτωση δείχνει ότι η κυβερνοϊσχύς λειτουργεί ταυτόχρονα ως μέσο αποτροπής και πηγή αστάθειας, καθώς η προληπτική δράση μπορεί να οδηγήσει σε κλιμάκωση και αλυσιδωτές αντιδράσεις στο διεθνές σύστημα.

5.8 Ρωσική Ομοσπονδία: Ασύμμετρη Κυβερνοστρατηγική και Υβριδικός Πόλεμος

Η Ρωσία αποτελεί την κατεξοχήν περίπτωση κράτους που χρησιμοποιεί τον κυβερνοχώρο ως εργαλείο ασύμμετρης στρατηγικής αντιστάθμισης έναντι της συμβατικής στρατιωτικής και οικονομικής υπεροχής της Δύσης. Η ρωσική προσέγγιση δεν βασίζεται στην τεχνολογική

υπεροχή per se, αλλά στη συνδυαστική χρήση κυβερνοεπιθέσεων, παραπληροφόρησης και ψυχολογικών επιχειρήσεων (Giles, 2021).

Στο πλαίσιο της λεγόμενης υβριδικής στρατηγικής, οι κυβερνοεπιχειρήσεις εντάσσονται σε ένα ευρύτερο φάσμα δράσεων που περιλαμβάνει εκλογικές παρεμβάσεις, οικονομική πίεση και γνωστικό πόλεμο. Οι επιθέσεις στην Εσθονία (2007), στην Ουκρανία (2015–2023) και οι παρεμβάσεις στις εκλογές των ΗΠΑ (2016) συνιστούν χαρακτηριστικά παραδείγματα χρήσης του κυβερνοχώρου για πολιτική αποσταθεροποίηση.

Η περίπτωση NotPetya (2017) ανέδειξε την πρόθεση της Ρωσίας να χρησιμοποιήσει τον κυβερνοχώρο όχι μόνο για κατασκοπεία, αλλά και για μαζική καταστροφή δεδομένων, με παγκόσμιες οικονομικές επιπτώσεις. Το γεγονός ότι η επίθεση ξεκίνησε από την Ουκρανία αλλά επηρέασε πολυεθνικές εταιρείες υποδηλώνει την αποδοχή του διεθνούς κόστους ως μέρους της στρατηγικής πίεσης (Greenberg, 2019).

Η ρωσική περίπτωση καταδεικνύει ότι ο κυβερνοχώρος λειτουργεί ως εργαλείο αποσταθεροποίησης της διεθνούς τάξης, ιδιαίτερα όταν συνδυάζεται με την αμφισβήτηση θεσμών και τη διάβρωση της εμπιστοσύνης στις δημοκρατικές διαδικασίες.

5.9 Λαϊκή Δημοκρατία της Κίνας: Κυβερνοχώρος, Τεχνολογία και Ψηφιακή Κυριαρχία

Η Κίνα ακολουθεί μια διαφορετική, μακροπρόθεσμη στρατηγική στον κυβερνοχώρο, εστιάζοντας όχι τόσο στη βραχυπρόθεσμη αποσταθεροποίηση, όσο στη δομική αναδιαμόρφωση της διεθνούς ισορροπίας ισχύος. Η κινεζική προσέγγιση βασίζεται στην έννοια της “cyber sovereignty”, δηλαδή στο δικαίωμα του κράτους να ελέγχει πλήρως το ψηφιακό του οικοσύστημα (DeNardis, 2020).

Η εκτεταμένη κυβερνοκατασκοπεία, κυρίως σε τομείς τεχνολογίας, άμυνας και βιομηχανικής καινοτομίας, αποτελεί βασικό πυλώνα της κινεζικής στρατηγικής. Ομάδες όπως η PLA Unit 61398 έχουν συνδεθεί με μαζικές υποκλοπές πνευματικής ιδιοκτησίας, συμβάλλοντας στην ταχεία τεχνολογική άνοδο της χώρας (Mandiant, 2022).

Παράλληλα, μέσω της Digital Silk Road, η Κίνα επεκτείνει την επιρροή της σε τρίτες χώρες, δημιουργώντας σχέσεις τεχνολογικής εξάρτησης σε υποδομές 5G, cloud και έξυπνων πόλεων. Αυτή η μορφή ασύμμετρης ισχύος δεν εκδηλώνεται ως άμεση επίθεση, αλλά ως μακροπρόθεσμη γεωοικονομική και γεωπολιτική επιρροή.

Η κινεζική περίπτωση δείχνει ότι οι ασύμμετρες κυβερνοαπειλές μπορούν να είναι σιωπηρές, σταδιακές και θεσμικά ενσωματωμένες, μεταβάλλοντας τη διεθνή τάξη χωρίς ανοικτή σύγκρουση.

5.10 Ευρωπαϊκή Ένωση: Κανονιστική Ισχύς και Συλλογική Ανθεκτικότητα

Η Ευρωπαϊκή Ένωση αποτελεί ιδιότυπη περιπτωσιολογική μελέτη, καθώς δεν λειτουργεί ως ενιαίο κράτος, αλλά ως κανονιστικός και θεσμικός δρών. Η ΕΕ προσεγγίζει τον κυβερνοχώρο όχι πρωτίστως ως πεδίο στρατιωτικής ισχύος, αλλά ως χώρο θεσμικής ρύθμισης και συλλογικής ανθεκτικότητας (European Commission, 2023).

Μέσω της ENISA, της Οδηγίας NIS2, του Cybersecurity Act και του Cyber Diplomacy Toolbox, η ΕΕ επιχειρεί να περιορίσει τις ασύμμετρες απειλές μέσω κανόνων, προτύπων και συνεργασίας. Η στρατηγική αυτή αντανακλά την ευρωπαϊκή αντίληψη της ισχύος ως normative power, δηλαδή ως ικανότητας διαμόρφωσης κανόνων συμπεριφοράς στο διεθνές σύστημα.

Ωστόσο, η περίπτωση της ΕΕ αποκαλύπτει και τις εγγενείς αδυναμίες της: η έλλειψη ενιαίας στρατιωτικής διοίκησης, οι διαφοροποιήσεις μεταξύ κρατών-μελών και η εξάρτηση από ιδιωτικούς παρόχους περιορίζουν την άμεση αποτρεπτική ικανότητα της Ένωσης (ENISA, 2024).

Παρά ταύτα, η ευρωπαϊκή προσέγγιση συνιστά εναλλακτικό μοντέλο διαχείρισης της ασυμμετρίας, βασισμένο στη θεσμική ανθεκτικότητα, τη συνεργασία και τη νομιμοποίηση, αντί της στρατιωτικής κλιμάκωσης.

Συνολική Αποτίμηση των Κρατοκεντρικών Περιπτώσεων

Οι τέσσερις περιπτώσεις καταδεικνύουν ότι οι ασύμμετρες κυβερνοαπειλές δεν ακολουθούν ενιαίο πρότυπο.
Αντίθετα, αντανακλούν διαφορετικές στρατηγικές κουλτούρες:
Οι ΗΠΑ δίνουν έμφαση στην προληπτική αποτροπή και την επιχειρησιακή δράση.

Η Ρωσία χρησιμοποιεί τον κυβερνοχώρο ως εργαλείο αποσταθεροποίησης και υβριδικού πολέμου.

Η Κίνα επενδύει στη μακροπρόθεσμη ψηφιακή κυριαρχία και την τεχνολογική εξάρτηση.

Η ΕΕ προωθεί τη θεσμική ρύθμιση και τη συλλογική ανθεκτικότητα.

Η ανάλυση αυτή ενισχύει την βασική θέση της διατριβής ότι, ο κυβερνοχώρος αποτελεί κεντρικό πεδίο αναδιαμόρφωσης της διεθνούς τάξης, όπου η ασύμμετρη ισχύς λειτουργεί ως καταλύτης γεωπολιτικής αστάθειας.

5.11 Cognitive Warfare και Ψυχολογικές Επιχειρήσεις

Η έννοια του “cognitive warfare” αποτελεί την πιο εξελιγμένη μορφή ασύμμετρης απειλής. Στόχος δεν είναι τα συστήματα, αλλά η ανθρώπινη σκέψη.

Το NATO StratCom COE (2023) ορίζει τον γνωστικό πόλεμο ως “συντονισμένη προσπάθεια διαμόρφωσης της αντίληψης και της κρίσης των κοινωνιών μέσω πληροφοριακών και ψυχολογικών μέσων”.

Μέσα Γνωστικού Πολέμου:

- Deepfakes και τεχνητά οπτικοακουστικά δεδομένα.
- Αλγοριθμική χειραγώγηση κοινωνικών τάσεων.
- Narrative control μέσω influencers και bots.
- “Truth decay” – σταδιακή απώλεια εμπιστοσύνης στην πληροφορία.

Η Τεχνητή Νοημοσύνη (AI) έχει επιταχύνει αυτόν τον πόλεμο, καθιστώντας δύσκολη τη διάκριση αλήθειας–ψεύδους.

Η ΕΕ και το OECD (2023) εργάζονται στην ανάπτυξη μηχανισμών AI-driven content verification.

Συμπέρασμα:
Ο γνωστικός πόλεμος μετατρέπει την πληροφόρηση σε όπλο μαζικής αποσταθεροποίησης. Η "ανθεκτικότητα της γνώσης" (cognitive resilience) καθίσταται στρατηγική προτεραιότητα των δημοκρατιών.

5.12 Η Ελλάδα ως Πεδίο Ψηφιακής Αντιπαράθεσης

Η Ελλάδα, λόγω της γεωπολιτικής της θέσης στην Ανατολική Μεσόγειο και της συμμετοχής της σε ΕΕ και ΝΑΤΟ, έχει καταστεί στόχος κυβερνοεπιθέσεων με πολιτικά και συμβολικά χαρακτηριστικά.

Ενδεικτικά Περιστατικά:

- 2020–2021: Επιθέσεις DDoS σε κυβερνητικούς ιστότοπους (ΥΠΕΞ, Βουλή, ΓΓΠΣ).
- 2022: Απόπειρες phishing σε ελληνικές τράπεζες και πανεπιστήμια.
- 2023–2024: Καμπάνιες παραπληροφόρησης μέσω social media κατά την προεκλογική περίοδο.

Η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ), σε συνεργασία με την ENISA και την CERT-EU, ενίσχυσε τους μηχανισμούς άμυνας.
Η Ελλάδα συμμετείχε σε ευρωπαϊκές ασκήσεις όπως Cyber Europe 2022 και σε διακρατικές πρωτοβουλίες με το Ισραήλ και την Κύπρο.
Προκλήσεις:

- Περιορισμένη εκπαίδευση προσωπικού ασφαλείας.
- Έλλειψη εθνικού πλαισίου κυβερνοεκπαίδευσης για πολίτες.
- Ανάγκη για σύστημα early warning και threat intelligence sharing (ΕΑΚ, 2024).

Η Ελλάδα μπορεί να εξελιχθεί σε περιφερειακό κέντρο κυβερνοανθεκτικότητας, εφόσον συνδυάσει θεσμική ωριμότητα, τεχνολογική καινοτομία και πολιτική συνεργασία.

5.13 Μαθήματα Πολιτικής και Στρατηγικής

Από τις μελέτες περίπτωσης προκύπτουν σημαντικά διδάγματα:

1. Η Κυβερνοανθεκτικότητα ως Πολιτική Αποτροπής:
   Η επένδυση σε ανθεκτικές υποδομές μειώνει την αποτελεσματικότητα των επιθέσεων.
2. Η Εκπαίδευση ως Εργαλείο Εθνικής Άμυνας:
   Η ανθρώπινη άγνοια είναι η μεγαλύτερη τρωτότητα.
   Προτείνεται ενσωμάτωση κυβερνοεκπαίδευσης στο εκπαιδευτικό σύστημα.
3. Η Συνεργασία Δημόσιου–Ιδιωτικού Τομέα:
   Οι κρίσιμες υποδομές πρέπει να υπόκεινται σε κοινά πρότυπα ασφάλειας.
4. Η Διεθνής Συνέργεια:
   Ο κυβερνοχώρος είναι παγκόσμιο δίκτυο - η ασφάλεια δεν μπορεί να είναι εθνική υπόθεση.
5. Η Πληροφοριακή Ανθεκτικότητα:
   Ο έλεγχος της πληροφορίας είναι κρίσιμος παράγοντας για την κοινωνική σταθερότητα.

5.14 Συμπεράσματα Κεφαλαίου

Οι κυβερνοεπιθέσεις των τελευταίων δεκαετιών απέδειξαν ότι οι ασύμμετρες απειλές αποτελούν μόνιμο συστατικό της διεθνούς ασφάλειας.

Η ισχύς στον κυβερνοχώρο είναι πολυδιάστατη, συνδυάζοντας τεχνικά, οικονομικά και ψυχολογικά στοιχεία.

Τα κράτη καλούνται να αναπτύξουν συνδυαστικές στρατηγικές αποτροπής, που περιλαμβάνουν:

- τεχνολογική υπεροχή,
- θεσμική ανθεκτικότητα,
- εκπαίδευση,
- και διεθνή συνεργασία.

Η Ελλάδα, ενταγμένη στο ευρωπαϊκό και νατοϊκό πλαίσιο, διαθέτει το δυναμικό να εξελιχθεί σε περιφερειακό πρότυπο κυβερνοανθεκτικότητας, εφόσον συνεχίσει να επενδύει σε γνώση, θεσμούς και καινοτομία.

Ενδεικτική Βιβλιογραφία (APA 7th)

Cadwalladr, C. (2019). *The Cambridge Analytica Files*. *The Guardian*.

CISA. (2022). *Pipeline Cybersecurity and Resilience Report*. U.S. Department of Homeland Security.

Council on Foreign Relations. (2023). *Cyber Operations Tracker*. https://www.cfr.org

ENISA. (2024). *Threat Landscape 2024*. https://www.enisa.europa.eu

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar*. Doubleday.

Mandiant. (2022). *APT29: Supply Chain Compromise Report*. https://www.mandiant.com

NATO CCDCOE. (2023). *Cyber Conflict in Ukraine: Lessons for NATO*. https://ccdcoe.org

NATO StratCom COE. (2023). *Cognitive Warfare and Strategic Communication*. https://stratcomcoe.org

OECD. (2023). *Digital Security Risk Management Guidelines*. https://www.oecd.org

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.

Υπουργείο Ψηφιακής Διακυβέρνησης. (2024). *Ετήσια Έκθεση για την Κυβερνοασφάλεια στην Ελλάδα 2024*.

Κεφάλαιο 6: Συμπεράσματα – Προτάσεις – Ερευνητικές Προεκτάσεις

Η κυβερνοασφάλεια έχει μετατραπεί σε καθοριστικό παράγοντα εθνικής κυριαρχίας και διεθνούς σταθερότητας. Η ανάλυση των ασύμμετρων απειλών αποκαλύπτει τη μετάβαση από την κλασική στρατιωτική ισχύ στην πληροφοριακή ισχύ – από τον πόλεμο των όπλων στον πόλεμο των δεδομένων.

6.1 Επισκόπηση Βασικών Συμπερασμάτων

Η ολοκληρωμένη μελέτη των ασύμμετρων απειλών στον κυβερνοχώρο ανέδειξε την πολυδιάστατη φύση της ισχύος και της ασφάλειας στη σύγχρονη εποχή. Το διεθνές σύστημα βρίσκεται σε φάση μετασχηματισμού, όπου η πληροφορία, η τεχνολογία και οι αφηγήσεις καθορίζουν την ισορροπία δυνάμεων.

Κύριες Διαπιστώσεις:

1. Οι ασύμμετρες κυβερνοαπειλές είναι διαρκής πραγματικότητα, όχι παροδικό φαινόμενο.
2. Η ισχύς στον κυβερνοχώρο είναι πολλαπλασιαστική, συνδυάζοντας πολιτικά, τεχνολογικά και ψυχολογικά στοιχεία.
3. Η κυβερνοανθεκτικότητα (resilience) είναι η νέα μορφή αποτροπής.
4. Η νορμοποίηση (norm-building) και η θεσμική συνεργασία είναι κρίσιμες για τη σταθερότητα.
5. Η Ελλάδα έχει τις προϋποθέσεις να αναδειχθεί σε περιφερειακό κόμβο κυβερνοασφάλειας.

Όπως σημειώνει το NATO CCDCOE (2023), «η αποτροπή στον κυβερνοχώρο δεν στηρίζεται πλέον στον φόβο της τιμωρίας, αλλά στην ικανότητα ανθεκτικής επιβίωσης».

6.2 Πολιτικές και Θεσμικές Προτάσεις για την Ελλάδα

Η Ελλάδα, λόγω της γεωγραφικής της θέσης και της συμμετοχής της στην ΕΕ και το ΝΑΤΟ, βρίσκεται στο σταυροδρόμι ψηφιακών και γεωπολιτικών ροών. Η ανάπτυξη εθνικής στρατηγικής κυβερνοανθεκτικότητας πρέπει να βασιστεί σε πέντε πυλώνες:

1. Θεσμική Ενοποίηση και Διακυβέρνηση

- Αναβάθμιση της ΕΑΚ σε επιτελικό όργανο χάραξης πολιτικής.
- Ενίσχυση συνεργασίας ΕΑΚ – ΕΥΠ – ΥΠΕΘΑ – CERT-ΕΛ για ολοκληρωμένο μηχανισμό αντιμετώπισης κρίσεων.
- Δημιουργία Εθνικού Κέντρου Ανάλυσης Απειλών και Πληροφοριών Κυβερνοχώρου (National Cyber Threat Intelligence Center).

2. Εκπαίδευση και Κατάρτιση

- Εισαγωγή μαθημάτων κυβερνοεκπαίδευσης στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση.
- Δημιουργία Προγραμμάτων Μεταπτυχιακών Σπουδών στην κυβερνοπολιτική και κυβερνοδιπλωματία (σε συνεργασία Πανεπιστημίων–Υπουργείων).
- Καθιέρωση Cybersecurity Academy για εκπαίδευση δημοσίων λειτουργών, στρατιωτικών και στελεχών επιχειρήσεων.

3. Δημόσιο–Ιδιωτική Συνεργασία

- Υποχρεωτική συμμόρφωση ιδιωτικών παρόχων κρίσιμων υποδομών στα πρότυπα NIS2.
- Δημιουργία Εθνικού Δικτύου Ανταλλαγής Πληροφοριών (Cyber ISAC).
- Κίνητρα για επιχειρήσεις που επενδύουν σε κυβερνοανθεκτικότητα και προστασία δεδομένων.

4. Νομοθετική Αναθεώρηση και Ρύθμιση

- Εναρμόνιση της ελληνικής νομοθεσίας με το EU Cyber Resilience Act (2024).
- Θέσπιση Εθνικού Πλαισίου Κυβερνοδικαιοσύνης, με εξειδικευμένα δικαστικά σώματα για κυβερνοεγκλήματα.
- Προώθηση ρυθμίσεων για ανθρώπινα δικαιώματα στον κυβερνοχώρο (privacy–security balance).

5. Κουλτούρα Ασφάλειας και Ανθεκτικότητα Κοινωνίας

- Καμπάνιες ευαισθητοποίησης για κυβερνοκινδύνους.
- Εθνική Εβδομάδα Κυβερνοασφάλειας υπό την αιγίδα του Υπουργείου Ψηφιακής Διακυβέρνησης.
- Προώθηση αξιών “digital trust” και “security awareness” στην κοινωνία των πολιτών.

6.3 Διεθνείς Συνεργασίες και Πολυμερής Διακυβέρνηση

Η Ελλάδα πρέπει να ενισχύσει τον ρόλο της στα διεθνή fora, συμμετέχοντας ενεργά στην ανάπτυξη κανόνων συμπεριφοράς και διαχείρισης κρίσεων.

Κύριοι Θεσμοί Συμμετοχής:

- ENISA: συντονισμός ευρωπαϊκής πολιτικής κυβερνοασφάλειας.
- NATO CCDCOE: ανάπτυξη κοινών δογμάτων αποτροπής και κυβερνοεκπαίδευσης.
- OEWG (OHE): υποστήριξη θεσμοθέτησης *Cyber Charter of Conduct*.
- GFCE (Global Forum on Cyber Expertise): ανταλλαγή τεχνογνωσίας και ικανοτήτων.
- OSCE: μέτρα οικοδόμησης εμπιστοσύνης (CBMs) για τη διαχείριση κυβερνοκρίσεων.

Η συμμετοχή της Ελλάδας σε διεθνή προγράμματα, όπως το EU–NATO Cyber Defence Pledge (2023), ενισχύει τον ρόλο της ως "Cyber Resilience Partner State".

6.4 Νομική και Ρυθμιστική Ενοποίηση σε Παγκόσμιο Επίπεδο

Η έλλειψη ενιαίου νομικού πλαισίου καθιστά αναγκαία τη δημιουργία μιας Παγκόσμιας Συνθήκης Κυβερνοασφάλειας, κατά τα πρότυπα της Συνθήκης της Βουδαπέστης (2001).

Προτείνεται:

1. Cybersecurity Convention (UN): Καθολική συνθήκη για το κυβερνοέγκλημα, τις επιθέσεις σε κρίσιμες υποδομές και τα ανθρώπινα δικαιώματα.
2. Cyber Arbitration Panel: Μηχανισμός διεθνούς διαιτησίας για απόδοση ευθύνης και αποζημίωση θυμάτων.
3. International Attribution Mechanism: Τυποποίηση τεχνικών και πολιτικών διαδικασιών για αναγνώριση δραστών.
4. Common Cyber Law Standards: Εναρμόνιση κανόνων ευθύνης και αποτροπής.

Το OECD (2023) υπογραμμίζει ότι η «ομοιογενοποίηση των κυβερνορυθμίσεων αποτελεί προϋπόθεση για την παγκόσμια σταθερότητα».

6.5 Εκπαίδευση, Έρευνα και Πολιτική Ανθεκτικότητα

Η ανθρώπινη διάσταση παραμένει ο πιο κρίσιμος παράγοντας κυβερνοασφάλειας. Το 2024, το Verizon Data Breach Report κατέγραψε ότι το 82% των περιστατικών παραβίασης οφείλεται σε ανθρώπινα λάθη.

Προτεινόμενα Μέτρα:

- Δημιουργία Εθνικού Δικτύου Κυβερνοεκπαίδευσης και Έρευνας, με την συνεργασία πανεπιστημίων, ΕΑΚ και στρατιωτικών σχολών.
- Χρηματοδότηση ερευνητικών προγραμμάτων για AI και κυβερνοασφάλεια.
- Ανάπτυξη “Cyber Drills” σε δημόσιο και ιδιωτικό τομέα.
- Εκπαίδευση των πολιτών στην ανθεκτικότητα στην παραπληροφόρηση και στην προστασία προσωπικών δεδομένων.

Η εκπαίδευση λειτουργεί ως στρατηγική επένδυση που μειώνει τον κίνδυνο και αυξάνει την αποτελεσματικότητα της άμυνας.

6.6 Νέες Απειλές και Μελλοντικές Προκλήσεις (2025–2035)

Οι τεχνολογικές εξελίξεις δημιουργούν νέα πεδία ασύμμετρων απειλών:

Τεχνολογία	Νέες Απειλές	Ανάγκες Πολιτικής
Τεχνητή Νοημοσύνη (AI)	Αυτοματισμός επιθέσεων, deepfakes, social engineering	Ηθικά πρότυπα AI και μηχανισμοί ελέγχου
Κβαντικοί Υπολογιστές	Παραβίαση κρυπτογραφίας	Ανάπτυξη post-quantum προτύπων
5G και IoT	Επέκταση επιφάνειας επίθεσης	Ρύθμιση προμηθευτών και ασφάλεια συσκευών
Διάστημα (Space Systems)	Επιθέσεις σε δορυφορικά δίκτυα	Διεθνής ρύθμιση “space-cyber domain”
Βιοψηφιακά Δεδομένα	Παραβίαση γενετικών πληροφοριών	Προστασία bioinformatics systems

Η περίοδος 2025–2035 θα σηματοδοτήσει την μετάβαση από την “cyber defence” στη “cyber sovereignty” – τη δυνατότητα κάθε κράτους να ελέγχει και να προστατεύει τα δίκτυα του με βάση διεθνείς κανόνες.

6.7 Ερευνητικές Προεκτάσεις

Η μελέτη ανοίγει νέους δρόμους για περαιτέρω έρευνα:

1. AI και Κυβερνοαποτροπή: Πώς η τεχνητή νοημοσύνη θα μεταβάλει την ισορροπία επίθεσης–άμυνας.
2. Κυβερνοδιπλωματία Μικρών Κρατών: Ο ρόλος της Ελλάδας και άλλων μεσαίων δυνάμεων.
3. Ψηφιακή Κυριαρχία και Ενεργειακή Ασφάλεια: Σχέση μεταξύ ενεργειακών υποδομών και κυβερνοπολιτικής.
4. Κλιματική Αλλαγή και Κυβερνοκινδύνους: Εξάρτηση “έξυπνων” δικτύων από ψηφιακά συστήματα.
5. Ηθική και Κυβερνοτεχνολογία: Ρύθμιση της τεχνητής νοημοσύνης και των αυτόνομων συστημάτων.

Η έρευνα για τις ασύμμετρες απειλές πρέπει να είναι διεπιστημονική, συνδέοντας τις διεθνείς σχέσεις, το δίκαιο, την τεχνολογία και τις κοινωνικές επιστήμες.

6.8 Επίλογος

Ο κυβερνοχώρος είναι πλέον το κεντρικό πεδίο άσκησης ισχύος στην διεθνή πολιτική. Οι ασύμμετρες απειλές συνιστούν την κανονικότητα της νέας εποχής, όπου οι συγκρούσεις διεξάγονται χωρίς στρατούς, αλλά με κώδικα και δεδομένα.

Η ασφάλεια του μέλλοντος θα καθοριστεί από:

- την συνεργασία αντί του ανταγωνισμού,
- την νομιμότητα αντί της αυθαιρεσίας,
- και την γνώση αντί της ισχύος.

Η Ελλάδα, αξιοποιώντας την γεωστρατηγική της θέση και την συμμετοχή της σε διεθνείς θεσμούς, μπορεί να διαμορφώσει το δικό της πρότυπο “Έξυπνης Εθνικής Ανθεκτικότητας

(Smart National Resilience)” - ένα υπόδειγμα που θα συνδυάζει τεχνολογική και πολιτισμική ασφάλεια.

Ο κυβερνοχώρος είναι, όπως σημειώνει ο Nye (2020), «ο καθρέφτης της παγκόσμιας τάξης πραγμάτων».
Η διασφάλισή του δεν είναι τεχνικό καθήκον· είναι ηθικό και πολιτικό καθήκον της ανθρωπότητας.

Ενδεικτική Βιβλιογραφία (APA 7th)

CISA. (2022). *Pipeline Cybersecurity and Resilience Report*. U.S. Department of Homeland Security.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

ENISA. (2024). *Threat Landscape 2024*. https://www.enisa.europa.eu

European Commission. (2024). *Cyber Resilience Act & Digital Services Act*. https://digital-strategy.ec.europa.eu

NATO CCDCOE. (2023). *Cyber Defence Review 2023*. https://ccdcoe.org

NATO StratCom COE. (2023). *Cognitive Warfare and Strategic Communication*. https://stratcomcoe.org

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

OECD. (2023). *Digital Security Policy Framework*. https://www.oecd.org

Taddeo, M. (2019). *The Limits of Deterrence Theory in Cyberspace*. *Philosophy & Technology, 32*(3), 331–344.

Υπουργείο Ψηφιακής Διακυβέρνησης. (2024). *Εθνική Στρατηγική για την Κυβερνοασφάλεια (Αναθεώρηση 2024–2030)*. https://mindigital.gr

Verizon. (2024). *Data Breach Investigations Report 2024*. https://www.verizon.com

Παράρτημα Α: Συνοπτικά Δεδομένα, Ακρωνύμια και Θεσμικοί Πίνακες

Α.1 Πίνακας Ακρωνύμιων και Συντομογραφιών

Ακρωνύμιο	Επεξήγηση	Οργανισμός / Έννοια
AI	Artificial Intelligence	Τεχνητή Νοημοσύνη
APT	Advanced Persistent Threat	Ομάδες προηγμένων επίμονων απειλών
CCDCOE	Cooperative Cyber Defence Centre of Excellence	Κέντρο Αριστείας Κυβερνοάμυνας του NATO (Εσθονία)
CERT	Computer Emergency Response Team	Ομάδα Απόκρισης Περιστατικών Κυβερνοασφάλειας
CISA	Cybersecurity and Infrastructure Security Agency	Υπηρεσία Κυβερνοασφάλειας ΗΠΑ
CSIRT	Computer Security Incident Response Team	Ομάδα Διαχείρισης Συμβάντων Ασφάλειας
ENISA	European Union Agency for Cybersecurity	Ευρωπαϊκή Υπηρεσία Κυβερνοασφάλειας
EU	European Union	Ευρωπαϊκή Ένωση
GFCE	Global Forum on Cyber Expertise	Παγκόσμιο Φόρουμ Ανάπτυξης Ικανοτήτων Κυβερνοασφάλειας
GDPR	General Data Protection Regulation	Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ)
GGE	Group of Governmental Experts	Ομάδα Κυβερνητικών Εμπειρογνωμόνων (ΟΗΕ)
IoT	Internet of Things	Διαδίκτυο των Πραγμάτων
NATO	North Atlantic Treaty Organization	Οργανισμός Βορειοατλαντικού Συμφώνου

Ακρωνύμιο	Επεξήγηση	Οργανισμός / Έννοια
NIS2	Network and Information Security Directive 2	Οδηγία ΕΕ για την Ασφάλεια Δικτύων και Πληροφοριών
OECD	Organisation for Economic Co-operation and Development	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
OEWG	Open-Ended Working Group	Ανοικτή Ομάδα Εργασίας ΟΗΕ για τον Κυβερνοχώρο
OSCE	Organization for Security and Co-operation in Europe	Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη
PPP	Public–Private Partnership	Συνεργασία Δημόσιου και Ιδιωτικού Τομέα
RaaS	Ransomware-as-a-Service	Υπηρεσία Ransomware προς ενοικίαση
UN	United Nations	Οργανισμός Ηνωμένων Εθνών
USCYBERCOM	United States Cyber Command	Διοίκηση Κυβερνοχώρου ΗΠΑ
ΥΠΨΔ	Υπουργείο Ψηφιακής Διακυβέρνησης	Εθνικός φορέας χάραξης πολιτικής κυβερνοασφάλειας Ελλάδας

Α.2 Κύριοι Θεσμικοί Φορείς και Οργανισμοί Κυβερνοασφάλειας

Φορέας / Οργανισμός	Πεδίο Δράσης	Βασικός Ρόλος
ΟΗΕ (UN)	Παγκόσμια διακυβέρνηση κυβερνοχώρου	Καθορισμός νορμών, GGE και OEWG
ΕΕ (EU)	Θεσμική πολιτική ασφάλειας	NIS2, Cybersecurity Act, GDPR
NATO	Συλλογική κυβερνοάμυνα	Αναγνώριση κυβερνοχώρου ως “operational domain”
ENISA	ΕΕ – Ανάλυση απειλών	Παρακολούθηση, εκπαίδευση, ανθεκτικότητα

Φορέας / Οργανισμός	Πεδίο Δράσης	Βασικός Ρόλος
CCDCOE (NATO)	Έρευνα & εκπαίδευση	Νομικές και στρατηγικές μελέτες, Tallinn Manual
OECD	Διεθνής οικονομική πολιτική	Κατευθυντήριες οδηγίες ψηφιακής ασφάλειας
GFCE	Παγκόσμια συνεργασία	Ανάπτυξη κυβερνοικανοτήτων
CISA (ΗΠΑ)	Εθνική ασφάλεια ΗΠΑ	Προστασία κρίσιμων υποδομών
OSCE	Ασφάλεια Ευρώπης	Μέτρα οικοδόμησης εμπιστοσύνης (CBMs)
ΥΠΨΔ (Ελλάδα)	Εθνική πολιτική κυβερνοασφάλειας	Εποπτεία ΕΑΚ, συντονισμός στρατηγικής Ελλάδας
ΕΑΚ	Εθνική Αρχή Κυβερνοασφάλειας Ελλάδας	Εποπτεία, εκπαίδευση, εθνική στρατηγική

Α.3 Εμβληματικές Κυβερνοεπιθέσεις (1989–2025)

Έτος	Περιστατικό	Χώρα/Δρών	Τύπος Επίθεσης	Επιπτώσεις
1989	Morris Worm	ΗΠΑ	Πρώτο malware μεγάλης κλίμακας	Προκάλεσε ζημίες $10 εκ.
2007	Estonia DDoS	Ρωσία	Επιθέσεις σε κρατικούς ιστότοπους	Πρώτη εθνικής κλίμακας κυβερνοκρίση
2010	Stuxnet	ΗΠΑ/Ισραήλ	Cyber-sabotage	Φυσική καταστροφή υποδομών Ιράν
2014	Sony Hack	Βόρεια Κορέα	Cyberespionage	Διαρροή δεδομένων, πολιτικές εντάσεις
2015	Ukraine BlackEnergy	Ρωσία	Cyberattack σε ενέργεια	Διακοπή ρεύματος 230.000 πολιτών

Έτος	Περιστατικό	Χώρα/Δρών	Τύπος Επίθεσης	Επιπτώσεις
2017	WannaCry	Βόρεια Κορέα	Ransomware	Παγκόσμια ζημία $4 δισ.
2017	NotPetya	Ρωσία	Destructive malware	Ζημίες $10 δισ., παγκόσμια κρίση
2020	SolarWinds	Ρωσία	Supply chain attack	Παραβίαση 18.000 οργανισμών
2021	Colonial Pipeline	DarkSide	Ransomware	Διακοπή ενεργειακής τροφοδοσίας ΗΠΑ
2022	Ukraine HermeticWiper	Ρωσία	Cyberwarfare	Καταστροφή δεδομένων εν μέσω πολέμου
2023	European Institutions Phishing	Μη κρατικοί	Espionage	Παραβίαση email ΕΕ
2024	AI-based Disinformation	Πολλαπλοί	Cognitive Warfare	Επηρεασμός κοινής γνώμης, εκλογικές επιδράσεις

Α.4 Πίνακας Πολιτικών και Νομικών Πρωτοβουλιών (ΕΕ – ΟΗΕ – ΝΑΤΟ – Ελλάδα)

Φορέας	Πρωτοβουλία / Πλαίσιο	Έτος	Περιγραφή
ΟΗΕ (UN)	OEWG Report on ICT Developments	2023	Κανόνες υπεύθυνης κρατικής συμπεριφοράς
NATO	Strategic Concept	2022	Κυβερνοχώρος ως “operational domain”
ΕΕ	NIS2 Directive	2023	Ρύθμιση κρίσιμων υποδομών και ανθεκτικότητας
ΕΕ	Cyber Resilience Act	2024	Ρυθμίσεις για ασφάλεια προϊόντων λογισμικού

Φορέας	Πρωτοβουλία / Πλαίσιο	Έτος	Περιγραφή
ΕΕ	Cyber Diplomacy Toolbox	2021	Κυρώσεις για κρατικές κυβερνοεπιθέσεις
Ελλάδα	Εθνική Στρατηγική Κυβερνοασφάλειας	2020–2025	Ενίσχυση θεσμών και εκπαίδευσης
Ελλάδα	Cyber Innovation Hub	2024	Ανάπτυξη έρευνας & startup κυβερνοασφάλειας
OECD	Digital Security Policy Framework	2023	Κατευθυντήριες για διεθνή συνεργασία
GFCE	Cyber Capacity Building Priorities	2023	Ανάπτυξη δυνατοτήτων κυβερνοασφάλειας

Α.5 Συνοπτικός Πίνακας Εννοιών-Κλειδιών

Έννοια	Ορισμός	Θεωρητική Προέλευση
Ασύμμετρη Ισχύς (Asymmetric Power)	Δυνατότητα επιβολής μέσω μη συμβατικών μέσων	Nye (2010), Libicki (2009)
Κυβερνοανθεκτικότητα (Cyber Resilience)	Ικανότητα πρόβλεψης και ανάκαμψης από επιθέσεις	ENISA (2024)
Κυβερνοαποτροπή (Cyber Deterrence)	Στρατηγική πρόληψης μέσω κόστους ή άρνησης	Taddeo (2019), Slayton (2016)
Ψηφιακή Κυριαρχία (Digital Sovereignty)	Έλεγχος δεδομένων και υποδομών	European Commission (2023)
Γνωστικός Πόλεμος (Cognitive Warfare)	Επιρροή μέσω πληροφορίας και αφηγήματος	NATO StratCom COE (2023)

Α.6 Βασική Βιβλιογραφία Παραρτήματος (APA 7th)

Council of the European Union. (2019). *Cyber Sanctions Regime*. Brussels.

ENISA. (2024). *Threat Landscape Report 2024*. https://www.enisa.europa.eu

European Commission. (2023). *NIS2 Directive & Cyber Resilience Act*. https://digital-strategy.ec.europa.eu

NATO CCDCOE. (2023). *Cyber Defence Review 2023*. https://ccdcoe.org

NATO. (2022). *Strategic Concept 2022*. NATO Headquarters.

OECD. (2023). *Digital Security Policy Framework*. https://www.oecd.org

United Nations. (2023). *Report of the Open-Ended Working Group on Developments in ICT*. A/78/112.

Υπουργείο Ψηφιακής Διακυβέρνησης. (2024). *Εθνική Στρατηγική Κυβερνοασφάλειας (Αναθεώρηση 2024–2030)*.

Verizon. (2024). *Data Breach Investigations Report 2024*. https://www.verizon.com

Βιβλιογραφία (APA 7th Edition)

Ακαδημαϊκές και Θεωρητικές Πηγές

Arreguín-Toft, I. (2001). *How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security, 26*(1), 93–128.

Carr, M. (2010). *Inside Cyber Warfare: Mapping the Cyber Underworld.* O'Reilly Media.

Clarke, R. A., & Knake, R. K. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* HarperCollins.

Deibert, R. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* McClelland & Stewart.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch.* Yale University Press.

Finnemore, M., & Hollis, D. (2016). *Constructing Norms for Global Cybersecurity. American Journal of International Law, 110*(3), 425–479.

Giles, K. (2021). *Russia's Hybrid War in Ukraine: Lessons for the West.* NATO Defence College.

Kello, L. (2017). *The Virtual Weapon and International Order.* Yale University Press.

Keohane, R. O., & Nye, J. S. (2012). *Power and Interdependence in the Information Age.* Harvard University Press.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* RAND Corporation.

Lindsay, J. R. (2013). *Stuxnet and the Limits of Cyberwarfare. Security Studies, 22*(3), 365–404.

Nye, J. S. (2010). *Cyber Power.* Belfer Center for Science and International Affairs.

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

Rid, T. (2013). *Cyber War Will Not Take Place.* Oxford University Press.

Slayton, R. (2016). *What is the Cyber Offense-Defense Balance? International Security, 41*(3), 72–109.

Taddeo, M. (2019). *The Limits of Deterrence Theory in Cyberspace. Philosophy & Technology, 32*(3), 331–344.

Θεσμικές Πηγές και Εκθέσεις (2021–2025)

CCDCOE. (2023). *Cyber Defence Review 2023.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

Council of the European Union. (2019). *Cyber Sanctions Regime.* Brussels.

Council on Foreign Relations. (2023). *Cyber Operations Tracker*. https://www.cfr.org

CISA. (2022). *Pipeline Cybersecurity and Resilience Report.* U.S. Department of Homeland Security.

ENISA. (2024). *Threat Landscape Report 2024.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Commission. (2023). *NIS2 Directive & Cyber Resilience Act.* Directorate-General for Communications Networks, Content and Technology. https://digital-strategy.ec.europa.eu

European Commission. (2024). *Digital Services Act (DSA).* https://digital-strategy.ec.europa.eu

GFCE. (2023). *Global Cyber Capacity Building Priorities.* Global Forum on Cyber Expertise. https://thegfce.org

Mandiant. (2022). *APT29: Supply Chain Compromise Report.* https://www.mandiant.com

NATO. (2016). *Warsaw Summit Communiqué.* NATO Headquarters.

NATO. (2022). *Strategic Concept 2022.* NATO Headquarters.

NATO CCDCOE. (2023). *Cyber Conflict in Ukraine: Lessons for NATO.* https://ccdcoe.org

NATO StratCom COE. (2023). *Cognitive Warfare and Strategic Communication.* Riga: NATO Strategic Communications Centre of Excellence.

OECD. (2023). *Digital Security Policy Framework.* Organisation for Economic Co-operation and Development. https://www.oecd.org

OECD. (2024). *AI Governance and Digital Risk Management Report.* https://www.oecd.org

Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Tikk, E., & Kerttunen, M. (2023). *Attribution and International Law in Cyberspace.* NATO CCDCOE Publications.

United Nations. (2023). *Report of the Open-Ended Working Group on Developments in ICT.* A/78/112.

Υπουργείο Ψηφιακής Διακυβέρνησης. (2024). *Εθνική Στρατηγική για την Κυβερνοασφάλεια (Αναθεώρηση 2024–2030).* https://mindigital.gr

Verizon. (2024). *Data Breach Investigations Report 2024.* Verizon Communications. https://www.verizon.com

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishing.