ΠΑΝΕΠΙΣΤΗΜΙΟ ΝΕΑΠΟΛΙΣ ΠΑΦΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

«ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ, ΣΤΡΑΤΗΓΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ»

ΜΕΤΑΠΤΥΧΙΑΚΉ ΔΙΑΤΡΙΒΉ ΜΕ ΤΙΤΛΟ

"Υβριδικές Απειλές και Πολιτικές Ασφάλειας: οι ρωσικές κυβερνοεπιθέσεις ως επιταχυντής Στρατηγικών Σχέσεων με το ΝΑΤΟ"

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:

Χρήστος Αλεξόπουλος

Α.Μ. 1237706075

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

Σπυρίδων Κατσούλας

Λευκωσία

Ιανουάριος 2025

# Πίνακας Περιεχομένων

# Περίληψη

Η παρούσα εργασία εξετάζει τον ρόλο των ρωσικών κυβερνοεπιθέσεων στη στρατηγική των κρατών και τις σχέσεις τους με το ΝΑΤΟ. Οι κυβερνοεπιθέσεις αναλύονται ως εργαλείο υβριδικού πολέμου, με στόχο την αποσταθεροποίηση, την άσκηση γεωπολιτικής πίεσης και τη διαμόρφωση ισορροπιών ισχύος. Η έρευνα επικεντρώνεται στις περιπτώσεις της Εσθονίας, της Ουκρανίας και της Πολωνίας, αναδεικνύοντας διαφορετικές στρατηγικές αντιδράσεις από τα κράτη-στόχους. Η μεθοδολογία βασίζεται στην ανάλυση δευτερογενών δεδομένων και περιπτωσιολογικών μελετών, οι οποίες επιλέχθηκαν λόγω της στρατηγικής σημασίας τους για την κατανόηση του ρωσικού υβριδικού πολέμου. Τα δεδομένα αξιολογούνται με βάση την επίδραση των κυβερνοεπιθέσεων στις στρατηγικές επιλογές και την ανθεκτικότητα των κρατών. Τα κύρια ευρήματα της έρευνας υπογραμμίζουν ότι οι ρωσικές κυβερνοεπιθέσεις δεν είναι τυχαίες ή απλές παραβιάσεις. Αντίθετα, αποτελούν ένα ισχυρό εργαλείο που χρησιμοποιεί η Ρωσία για να αποδυναμώσει κράτη-στόχους και να επηρεάσει τη γεωπολιτική ισορροπία. Υποστηρίζεται ότι οι κυβερνοεπιθέσεις λειτουργούν κυρίως ως επιταχυντές υπαρχουσών στρατηγικών κατευθύνσεων παρά ως καταλυτικοί παράγοντες ριζικών αλλαγών. Η έρευνα καταλήγει στο ότι η στρατηγική αντιμετώπιση των κυβερνοεπιθέσεων απαιτεί διεθνή συνεργασία και τη θεσμοθέτηση κανόνων στον κυβερνοχώρο. Η ενίσχυση της κυβερνοασφάλειας μέσω του ΝΑΤΟ και η υιοθέτηση τεχνολογικών και θεσμικών εργαλείων κρίνονται απαραίτητες για τη διασφάλιση της σταθερότητας και της διεθνούς ασφάλειας.

# Abstract

This thesis investigates the strategic role of Russian cyberattacks in shaping state strategies and their relationship with NATO. Cyberattacks, as a core tool of hybrid warfare, are analyzed for their ability to destabilize, exert geopolitical influence, and shift the balance of power in the international system. Through an in-depth examination of case studies from Estonia, Ukraine, and Poland, the research explores how these attacks impact the strategic decisions of target states and the resilience of their institutions. The methodology integrates secondary data analysis and case study evaluation, focusing on the 2010-2020 period, a decade marked by a significant increase in the scale and sophistication of cyber operations. By assessing specific incidents, including the 2007 Estonian DDoS attacks, the 2017 NotPetya operation in Ukraine, and espionage efforts against Polish governmental systems, the study highlights the multifaceted role of cyberattacks within broader hybrid warfare strategies. Furthermore, it examines the distinction between cyberattacks acting as accelerators of pre-existing strategies versus catalysts that drive fundamental strategic change, revealing how geopolitical contexts and institutional readiness shape the outcomes of such operations.

# Κεφάλαιο 1: Εισαγωγή

Ο κυβερνοχώρος έχει αναδειχθεί ως ένα από τα πιο κρίσιμα πεδία αντιπαράθεσης στη σύγχρονη γεωπολιτική, διαμορφώνοντας νέες προκλήσεις για τη διεθνή ασφάλεια. Στον 21ο αιώνα, οι κυβερνοεπιθέσεις δεν αποτελούν πλέον απλές παραβιάσεις πληροφοριακών συστημάτων. Αντίθετα, έχουν ενσωματωθεί σε ευρύτερες στρατηγικές υβριδικού πολέμου, όπου παραδοσιακά και μη παραδοσιακά μέσα συνδυάζονται για την αποσταθεροποίηση κρατών και την επίτευξη γεωπολιτικών στόχων. Η Ρωσία, ως πρωτοπόρος δύναμη στον κυβερνοχώρο, χρησιμοποιεί συστηματικά τις κυβερνοεπιθέσεις ως εργαλείο στρατηγικής αποσταθεροποίησης και πίεσης, ιδιαίτερα έναντι κρατών που ανήκουν στη σφαίρα επιρροής της ή έχουν στενές σχέσεις με το NATO. Η παρούσα εργασία εστιάζει στη διερεύνηση του στρατηγικού ρόλου των ρωσικών κυβερνοεπιθέσεων, εξετάζοντας τη φύση, τους στόχους και τις επιπτώσεις τους. Το κύριο ερευνητικό ερώτημα που επιχειρεί να απαντήσει είναι: Κατά πόσο οι ρωσικές κυβερνοεπιθέσεις αποτελούν καθοριστικό παράγοντα αλλαγής στη στρατηγική των κρατών-στόχων και πώς αυτές επηρεάζουν τη σχέση τους με το NATO; Μέσα από τη μελέτη περιπτώσεων της Εσθονίας, της Ουκρανίας και της Πολωνίας, η εργασία αξιολογεί τον ρόλο των κυβερνοεπιθέσεων ως επιταχυντών υπαρχουσών στρατηγικών ή ως καταλυτών θεμελιωδών αλλαγών. Η εργασία καταλήγει στο συμπέρασμα ότι οι ρωσικές κυβερνοεπιθέσεις σπάνια αποτελούν τον μοναδικό και καθοριστικό παράγοντα στρατηγικών αλλαγών. Αντίθετα, λειτουργούν κυρίως ως επιταχυντές υπαρχουσών στρατηγικών κατευθύνσεων ή ως ενισχυτικοί μηχανισμοί ήδη διαμορφωμένων πολιτικών. Οι περιπτώσεις της Εσθονίας, της Ουκρανίας και της Πολωνίας καταδεικνύουν ότι οι κυβερνοεπιθέσεις, ενώ προκαλούν σημαντικές συνέπειες και αναδεικνύουν αδυναμίες, συνήθως δεν αποτελούν την αφετηρία για ριζικές στρατηγικές μεταβολές. Παράλληλα, οι επιθέσεις αυτές αναδεικνύουν τη σημασία της συνεργασίας με διεθνείς οργανισμούς, όπως το NATO, και τη θεσμική προσαρμογή για την αντιμετώπιση των υβριδικών απειλών.

Η στρατηγική σημασία των κυβερνοεπιθέσεων έγκειται στην ικανότητά τους να προκαλούν δυσανάλογες επιπτώσεις με ελάχιστο κόστος και περιορισμένο ρίσκο. Σε αντίθεση με παραδοσιακές στρατιωτικές επιχειρήσεις, οι κυβερνοεπιθέσεις προσφέρουν ανωνυμία, ταχύτητα και ευελιξία, καθιστώντας τον κυβερνοχώρο ιδανικό πεδίο για ασύμμετρες τακτικές. Οι επιθέσεις στην Εσθονία τόσο το 2007 όσο και κατά τη δεκαετία 2010-2020, την Ουκρανία (2015-2017) και την Πολωνία (2010-2020) αποτελούν χαρακτηριστικά παραδείγματα του τρόπου με τον οποίο η Ρωσία αξιοποιεί τον κυβερνοχώρο για να αποδυναμώσει κράτη και να ανατρέψει τη στρατηγική τους συνοχή. Η ανάλυση αυτών των περιπτώσεων επικεντρώνεται όχι μόνο στις επιπτώσεις των κυβερνοεπιθέσεων στα κράτη-στόχους, αλλά και στη στρατηγική τους αντίδραση μέσω της ενίσχυσης των σχέσεων με το NATO. Εξετάζεται, επίσης, η αντίδραση του NATO, το οποίο έχει αναγνωρίσει τον κυβερνοχώρο ως αυτόνομο επιχειρησιακό πεδίο. Η Συμμαχία έχει αναγνωρίσει τον κυβερνοχώρο ως αυτόνομο επιχειρησιακό πεδίο, προσαρμόζοντας τη στρατηγική της μέσα από πρωτοβουλίες όπως το Cooperative Cyber Defence Centre of Excellence (CCDCOE) και κοινές ασκήσεις κυβερνοάμυνας, όπως το Locked Shields. Παρόλα αυτά, η διεθνής κοινότητα εξακολουθεί να αντιμετωπίζει προκλήσεις, όπως η έλλειψη δεσμευτικών κανονισμών στον κυβερνοχώρο και η αδυναμία πλήρους αποτροπής των υβριδικών απειλών.

Η δομή της εργασίας οργανώνεται ως εξής: Αρχικά, το θεωρητικό πλαίσιο εξετάζει τη σύνδεση των κυβερνοεπιθέσεων με τον υβριδικό πόλεμο και τη στρατηγική ασφάλεια. Στη συνέχεια, το επόμενο κεφάλαιο επικεντρώνεται στις σημαντικότερες ρωσικές κυβερνοεπιθέσεις της περιόδου 2010-2020, εστιάζοντας στις περιπτώσεις της Εσθονίας, της Ουκρανίας και της Πολωνίας. Η ανάλυση και η σύγκριση των περιπτώσεων αυτών πραγματοποιούνται στο πλαίσιο των στρατηγικών τους επιπτώσεων, ενώ το τελευταίο κεφάλαιο καταλήγει σε συμπεράσματα και προτάσεις πολιτικής. Η παρούσα εργασία στοχεύει στη δημιουργία ενός πλαισίου κατανόησης για την αντιμετώπιση των σύγχρονων προκλήσεων στον κυβερνοχώρο.

# Κεφάλαιο 2: Θεωρητικό Πλαίσιο

Το Κεφάλαιο 2 θέτει τα θεωρητικά θεμέλια της διατριβής, αναλύοντας βασικές έννοιες και θεωρητικές προσεγγίσεις που πλαισιώνουν το ερευνητικό ερώτημα. Σκοπός του κεφαλαίου είναι να προσφέρει έναν σαφή ορισμό και εννοιολογική κατανόηση των υβριδικών απειλών και των κυβερνοεπιθέσεων. Παράλληλα, εξετάζεται ο ρόλος αυτών των εργαλείων στον σύγχρονο γεωπολιτικό ανταγωνισμό και η σύνδεσή τους με τη στρατηγική ασφάλειας. Τέλος, αναδεικνύεται η σημασία της διεθνούς συνεργασίας, με ιδιαίτερη έμφαση στον ρόλο του ΝΑΤΟ.

Το κεφάλαιο οργανώνεται σε τρεις βασικές ενότητες. Η πρώτη ενότητα (2.1) επικεντρώνεται στον ορισμό και το θεωρητικό υπόβαθρο των υβριδικών απειλών και των κυβερνοεπιθέσεων, εστιάζοντας στη φύση, τους στόχους και τις επιπτώσεις αυτών των απειλών στη διεθνή ασφάλεια. Η δεύτερη ενότητα (2.2) αναλύει το θεωρητικό πλαίσιο του υβριδικού πολέμου, παρουσιάζοντας τις στρατηγικές που εφαρμόζει η Ρωσία και τη θέση του κυβερνοχώρου στον ευρύτερο μηχανισμό υβριδικών επιχειρήσεων. Η τρίτη ενότητα (2.3) εισάγει τη διάκριση μεταξύ επιταχυντικής και καταλυτικής δράσης των κυβερνοεπιθέσεων, που αποτελεί κεντρικό επιχείρημα της εργασίας. Ειδικότερα, εξηγείται πώς αυτές οι δύο διαστάσεις επηρεάζουν τη διαμόρφωση της στρατηγικής των κρατών-στόχων. Η διάκριση αυτή αναδεικνύει τον ρόλο των κυβερνοεπιθέσεων, είτε ως μηχανισμών που ενισχύουν προϋπάρχουσες στρατηγικές (επιταχυντική δράση) είτε ως παραγόντων που προκαλούν θεμελιώδεις αλλαγές (καταλυτική δράση).

## 2.1 Ορισμός και Θεωρητικό Υπόβαθρο των Υβριδικών Απειλών και των Κυβερνοεπιθέσεων

Οι υβριδικές απειλές συνιστούν έναν πολυδιάστατο τύπο σύγκρουσης που συνδυάζει στρατιωτικά και μη στρατιωτικά μέσα, με στόχο την επίτευξη στρατηγικών στόχων χωρίς την ανάγκη άμεσης στρατιωτικής σύγκρουσης. Αυτή η προσέγγιση περιλαμβάνει τη χρήση εργαλείων όπως η παραπληροφόρηση, η πολιτική αποσταθεροποίηση, η ενεργειακή πίεση και οι κυβερνοεπιθέσεις. Ο βασικός σκοπός είναι η εκμετάλλευση των αδυναμιών των κρατών-στόχων, ώστε να διαβρωθεί η κοινωνική συνοχή, να αποσταθεροποιηθούν οι πολιτικοί θεσμοί και να επιτευχθούν γεωπολιτικοί στόχοι με ελάχιστο κόστος (NATO, 2023). Η προσάρτηση της Κριμαίας από τη Ρωσία το 2014 αποτελεί ένα χαρακτηριστικό παράδειγμα εφαρμογής υβριδικών τακτικών σε στρατηγικό επίπεδο. Σε αυτή την περίπτωση, η Ρωσία συνδύασε τη χρήση στρατιωτικών δυνάμεων με παραπληροφόρηση και κυβερνοεπιθέσεις, προκειμένου να αποσταθεροποιήσει την Ουκρανία και να εδραιώσει τον έλεγχό της στην περιοχή. Επίσης, η Ρωσία έχει αξιοποιήσει ενεργειακούς πόρους, όπως το φυσικό αέριο, ως εργαλείο πίεσης στις χώρες της Ανατολικής Ευρώπης, χρησιμοποιώντας τη στρατηγική εξάρτηση αυτών των κρατών από τη ρωσική ενέργεια για την προώθηση γεωπολιτικών στόχων.

Αυτές οι τακτικές δεν περιορίζονται σε μεμονωμένα περιστατικά αλλά αποτελούν μέρος μιας ευρύτερης στρατηγικής, όπου διαφορετικά μέσα, συμβατικά και μη, αλληλοσυμπληρώνονται για την επίτευξη πολιτικών και στρατιωτικών στόχων.

Οι κυβερνοεπιθέσεις αποτελούν μια από τις πιο κρίσιμες διαστάσεις των υβριδικών απειλών. Ορίζονται ως οι εσκεμμένες ενέργειες παραβίασης, διατάραξης ή καταστροφής πληροφοριακών

συστημάτων και δεδομένων, με στόχο την επίτευξη πολιτικών, στρατηγικών ή οικονομικών στόχων (Rid, 2013). Σύμφωνα με τον Lewis (2021), αυτές οι επιθέσεις ξεχωρίζουν λόγω της ικανότητάς τους να παραλύουν κρίσιμες υποδομές και να προκαλούν ευρείας κλίμακας κοινωνική αναταραχή, συχνά χωρίς την ανάγκη φυσικής παρουσίας. Επιπλέον, η Giles (2016) υπογραμμίζει ότι ο κυβερνοχώρος παρέχει στους δράστες τη δυνατότητα ανωνυμίας, καθιστώντας τις κυβερνοεπιθέσεις ιδανικές για ασύμμετρες τακτικές σε γεωπολιτικά πλαίσια. Το NATO CCDCOE (2023) προσθέτει ότι οι κυβερνοεπιθέσεις δεν περιορίζονται μόνο σε τεχνικές παραβιάσεις, αλλά ενσωματώνονται σε ευρύτερα στρατηγικά σχέδια, όπως η παραπληροφόρηση και οι ψυχολογικές επιχειρήσεις. Οι κυβερνοεπιθέσεις χαρακτηρίζονται από την ικανότητά τους να προκαλούν δυσανάλογες συνέπειες σε σχέση με το κόστος υλοποίησής τους, αξιοποιώντας τη δυνατότητα ανωνυμίας και τη δυσκολία ταυτοποίησης του δράστη. Υπάρχουν διάφορα είδη κυβερνοεπιθέσεων, όπως οι επιθέσεις DDoS (Distributed Denial of Service), που στοχεύουν στην υπερφόρτωση δικτύων και τη διακοπή υπηρεσιών, οι επιθέσεις ransomware, που μπλοκάρουν την πρόσβαση σε δεδομένα με αντάλλαγμα λύτρα, και οι επιθέσεις κατασκοπείας, που αποσκοπούν στη συλλογή ευαίσθητων πληροφοριών. Οι επιθέσεις DDoS έχουν χρησιμοποιηθεί εκτενώς για να παραλύσουν κρίσιμες υποδομές, όπως στην περίπτωση της Εσθονίας το 2007 (Ottis, 2008). Το ransomware έχει εξελιχθεί σε μία από τις πιο αποδοτικές τακτικές στον κυβερνοχώρο, με χαρακτηριστικό παράδειγμα την επίθεση WannaCry, η οποία επηρέασε χιλιάδες υποδομές υγείας και επιχειρήσεις παγκοσμίως (Zetter, 2017). Η επίθεση NotPetya το 2017 προκάλεσε εκτεταμένες ζημιές στις υποδομές της Ουκρανίας, παραλύοντας τραπεζικά συστήματα και εταιρείες, όπως η Maersk, με οικονομικές απώλειες που ξεπέρασαν τα δισεκατομμύρια δολάρια (Greenberg, 2018).

Οι υβριδικές απειλές και οι κυβερνοεπιθέσεις αναδεικνύονται ως κρίσιμα εργαλεία στη γεωπολιτική σκακιέρα, επηρεάζοντας τη διεθνή ασφάλεια. Επηρεάζουν άμεσα τις κρίσιμες υποδομές των κρατών-στόχων, όπως ενεργειακά δίκτυα, συστήματα επικοινωνίας και κυβερνητικές βάσεις δεδομένων, δημιουργώντας αστάθεια και υπονομεύοντας την κοινωνική συνοχή. Παράλληλα, επηρεάζουν την εμπιστοσύνη των πολιτών προς τους κρατικούς θεσμούς, προκαλώντας πολιτική και κοινωνική αποσταθεροποίηση (Lewis, 2021). Ένα χαρακτηριστικό παράδειγμα είναι οι επιθέσεις που δέχθηκε η Εσθονία το 2007, οι οποίες στόχευαν την παράλυση κρίσιμων υποδομών μέσω επιθέσεων DDoS. Αυτή η περίπτωση αποτέλεσε σημείο καμπής για την κατανόηση της σημασίας των κυβερνοεπιθέσεων και της ανάγκης για διεθνή συνεργασία στον τομέα της κυβερνοασφάλειας.

Η κατανόηση των υβριδικών απειλών και των κυβερνοεπιθέσεων είναι ζωτικής σημασίας για τη διατριβή, καθώς αποτελούν τα βασικά εργαλεία που χρησιμοποιεί η Ρωσία στον γεωπολιτικό ανταγωνισμό. Μέσα από την ανάλυση αυτών των εννοιών, αναδεικνύεται ο τρόπος με τον οποίο οι κυβερνοεπιθέσεις επηρεάζουν τη στρατηγική ασφάλειας των κρατών-στόχων και τη σχέση τους με το NATO.

## 2.2 Ρωσική Στρατηγική στον Υβριδικό Πόλεμο

Ο υβριδικός πόλεμος αποτελεί μια σύγχρονη στρατηγική προσέγγιση που συνδυάζει στρατιωτικά και μη στρατιωτικά μέσα για την επίτευξη γεωπολιτικών στόχων.Η Ρωσία έχει αναδειχθεί σε κύριο εφαρμοστή αυτής της στρατηγικής, ιδιαίτερα μετά την προσάρτηση της Κριμαίας το 2014. Οι τακτικές της ενσωματώνουν ένα ευρύ φάσμα εργαλείων, συνδυάζοντας στρατιωτική δύναμη και κυβερνοεπιθέσεις με ψυχολογικές επιχειρήσεις, με στόχο τη διαμόρφωση των γεωπολιτικών ισορροπιών.

Η στρατηγική της Ρωσίας βασίζεται στην αντίληψη ότι ο κυβερνοχώρος και οι υβριδικές τακτικές μπορούν να χρησιμοποιηθούν για την αποσταθεροποίηση κρατών και τη διαμόρφωση της κοινής γνώμης. Η χρήση παραπληροφόρησης αποτελεί αναπόσπαστο μέρος αυτής της στρατηγικής. Μέσω συντονισμένων

εκστρατειών στα κοινωνικά δίκτυα και κρατικά ελεγχόμενα ΜΜΕ, η Ρωσία επιχειρεί να διαμορφώσει αφηγήσεις που ευνοούν τα στρατηγικά της συμφέροντα. Παραδείγματα αυτής της τακτικής περιλαμβάνουν τις εκστρατείες που στόχευσαν τις προεδρικές εκλογές στις Ηνωμένες Πολιτείες το 2016, όπου η Ρωσία φέρεται να χρησιμοποίησε ψευδείς ειδήσεις και διαδικτυακές πλατφόρμες για να επηρεάσει την κοινή γνώμη (Lewis, 2021). Αντίστοιχα, η παραπληροφόρηση κατά τη διάρκεια του πολέμου στην Ουκρανία ενίσχυσε τις ρωσικές στρατιωτικές επιχειρήσεις, αποδυναμώνοντας την εμπιστοσύνη προς την ουκρανική κυβέρνηση και τους δυτικούς συμμάχους της.

Η Ρωσία χρησιμοποιεί επίσης μη κρατικούς δρώντες, όπως ομάδες χάκερ που σχετίζονται με τις υπηρεσίες ασφαλείας της χώρας, για να επιτύχει τους στόχους της. Αυτές οι ομάδες, όπως οι APT28 (Fancy Bear) και APT29 (Cozy Bear), συχνά λειτουργούν υπό την αιγίδα του κράτους, αλλά παρέχουν τη δυνατότητα στη Ρωσία να διατηρεί την αμφισημία σχετικά με την εμπλοκή της (Schmitt, 2017).

Οι ρωσικές υβριδικές στρατηγικές έχουν άμεσο αντίκτυπο στη στρατηγική του NATO, το οποίο έχει αναγνωρίσει τον κυβερνοχώρο ως αυτόνομο επιχειρησιακό πεδίο. Το NATO έχει επενδύσει σημαντικά στην ενίσχυση της ανθεκτικότητας των κρατών-μελών του μέσω πρωτοβουλιών όπως το Cyber Defence Pledge και η ίδρυση του Κέντρου Αριστείας Συνεργατικής Κυβερνοάμυνας (CCDCOE) (NATO, 2023). Παράλληλα, οι κοινές ασκήσεις κυβερνοάμυνας, όπως οι Locked Shields, ενισχύουν την ετοιμότητα των κρατών-μελών να αντιμετωπίσουν συντονισμένες κυβερνοεπιθέσεις μεγάλης κλίμακας. Η Συμμαχία έχει υιοθετήσει επίσης το Άρθρο 5 για την αντιμετώπιση κυβερνοεπιθέσεων, στέλνοντας σαφές μήνυμα ότι τέτοιες ενέργειες θεωρούνται ισοδύναμες με παραδοσιακές στρατιωτικές επιθέσεις.

Η στρατηγική της Ρωσίας στον υβριδικό πόλεμο αναδεικνύει τη σημασία του κυβερνοχώρου ως πεδίου στρατηγικής αντιπαράθεσης. Η χρήση συνδυαστικών τακτικών, όπως παραπληροφόρησης και κυβερνοεπιθέσεων, επιτρέπει στη Ρωσία να επιτυγχάνει γεωπολιτικούς στόχους με χαμηλό κόστος και χωρίς να προκαλεί άμεσες στρατιωτικές απαντήσεις. Το NATO, αναγνωρίζοντας τη σοβαρότητα αυτών των απειλών, συνεχίζει να επενδύει στη συλλογική κυβερνοάμυνα και στη στρατηγική ανθεκτικότητα των κρατών-μελών του, προσπαθώντας να προσαρμοστεί στις προκλήσεις ενός διαρκώς μεταβαλλόμενου γεωπολιτικού περιβάλλοντος.

## 2.3 Η Ανάπτυξη των Ρωσικών Ικανοτήτων στον Κυβερνοχώρο (2010-2020)

Κατά τη δεκαετία 2010-2020, η Ρωσία κατέστη μία από τις πιο δραστήριες και ικανές δυνάμεις στον κυβερνοχώρο, αναδεικνύοντας τον στρατηγικό της προσανατολισμό στις κυβερνοεπιχειρήσεις. Οι κυβερνοεπιθέσεις ενσωματώθηκαν πλήρως στη στρατηγική της, λειτουργώντας ως βασικό εργαλείο για την επίτευξη γεωπολιτικών στόχων και την αποσταθεροποίηση των αντιπάλων της. Το Κρεμλίνο αντιλήφθηκε ότι ο κυβερνοχώρος παρέχει τη δυνατότητα πρόκλησης σοβαρών επιπτώσεων με χαμηλό κόστος και ελάχιστο κίνδυνο άμεσης στρατιωτικής σύγκρουσης (Rid, 2013). Η ανάπτυξη των ρωσικών δυνατοτήτων στον κυβερνοχώρο βασίστηκε στην τεχνολογική ενίσχυση και στη δημιουργία εξειδικευμένων ομάδων κυβερνοεπιθέσεων. Ομάδες όπως οι APT28 (Fancy Bear) και APT29 (Cozy Bear), που φέρονται να συνδέονται με τη GRU (Υπηρεσία Στρατιωτικών Πληροφοριών) και την FSB (Ομοσπονδιακή Υπηρεσία Ασφαλείας), χρησιμοποίησαν προηγμένες τεχνικές για να παραβιάσουν κυβερνητικά συστήματα, να συλλέξουν δεδομένα και να διαδώσουν παραπληροφόρηση. Ειδικότερα, αυτές οι ομάδες στόχευσαν κρίσιμες υποδομές, κυβερνητικά δίκτυα και οικονομικούς οργανισμούς, επιδεικνύοντας υψηλή τεχνογνωσία και συντονισμό (Lewis, 2021).

Οι στρατηγικές που εφαρμόζει η Ρωσία στον κυβερνοχώρο περιλαμβάνουν μια σειρά από τεχνικές, όπως επιθέσεις DDoS, κακόβουλο λογισμικό (ransomware), και εκστρατείες παραπληροφόρησης. Παραδείγματα αυτών των στρατηγικών είναι:

- **Επίθεση στο Bundestag (2015):** Μία από τις πιο γνωστές επιχειρήσεις κυβερνοκατασκοπείας, όπου ρωσικές ομάδες απέκτησαν πρόσβαση στα δίκτυα του γερμανικού κοινοβουλίου, προκαλώντας πολιτική κρίση (Giles, 2016).
- **Επιχείρηση NotPetya (2017):** Ένα κακόβουλο λογισμικό που ήταν παρόμοιο με ransomware αλλά είχε ως βασικό στόχο την καταστροφή δεδομένων. Η επίθεση αυτή προκάλεσε τεράστιες οικονομικές ζημιές, επηρεάζοντας όχι μόνο την Ουκρανία αλλά και πολυεθνικές εταιρείες.

Οι κυβερνοεπιθέσεις της Ρωσίας συνδυάζονται συχνά με εκστρατείες παραπληροφόρησης, στοχεύοντας να ενισχύσουν τη σύγχυση και να υπονομεύσουν την εμπιστοσύνη στους θεσμούς των κρατών-στόχων. Η χρήση κοινωνικών μέσων για τη διάδοση ψευδών πληροφοριών αποτελεί έναν από τους πιο αποτελεσματικούς μηχανισμούς της στρατηγικής αυτής.

Η Ρωσία εκμεταλλεύτηκε το κενό στο διεθνές νομικό πλαίσιο για τη χρήση του κυβερνοχώρου, δρώντας με σχετική ατιμωρησία. Παρά τις διεθνείς προσπάθειες για τη δημιουργία κανονισμών, όπως το Tallinn Manual 2.0, η Μόσχα συνέχισε να χρησιμοποιεί τον κυβερνοχώρο ως εργαλείο γεωπολιτικής πίεσης. Οι επιχειρήσεις της χαρακτηρίζονται από τη δυνατότητα άρνησης ευθύνης (plausible deniability), καθιστώντας δύσκολη την άμεση σύνδεση των επιθέσεων με την κρατική πολιτική (Schmitt, 2017). Η δεκαετία 2010-2020 αποτέλεσε περίοδο ραγδαίας εξέλιξης για τις ρωσικές ικανότητες στον κυβερνοχώρο. Η Ρωσία κατάφερε να δημιουργήσει έναν ολοκληρωμένο μηχανισμό κυβερνοεπιχειρήσεων, ο οποίος συνδυάζει τεχνολογική υπεροχή, εξειδικευμένο ανθρώπινο δυναμικό και στρατηγική ευελιξία (Conley et al., 2016; Schmitt, 2017). Οι κυβερνοεπιθέσεις της αναδεικνύονται ως ένα από τα πιο σημαντικά εργαλεία στη γεωπολιτική σκακιέρα, παρέχοντας στη Ρωσία τη δυνατότητα να επηρεάζει την παγκόσμια ισορροπία δυνάμεων χωρίς την ανάγκη άμεσης στρατιωτικής παρέμβασης (Giles, 2016; Rid, 2013).

## 2.4 Επιταχυντική και Καταλυτική Δράση των Κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις έχουν αναδειχθεί σε κρίσιμο εργαλείο υβριδικού πολέμου, προσφέροντας τη δυνατότητα στα κράτη να επιτυγχάνουν γεωπολιτικούς στόχους χωρίς να καταφεύγουν σε ανοιχτές στρατιωτικές συγκρούσεις. Η επίδρασή τους στις στρατηγικές των κρατών-στόχων διαφοροποιείται, ανάλογα με το πλαίσιο και τη φύση της κάθε επίθεσης. Στην ανάλυση αυτής της επίδρασης, οι έννοιες της επιταχυντικής και της καταλυτικής δράσης προσφέρουν ένα χρήσιμο θεωρητικό εργαλείο για την κατανόηση των διαφορών στον αντίκτυπο των κυβερνοεπιθέσεων.

Αν και στις τρεις περιπτώσεις οι κυβερνοεπιθέσεις αποδεικνύεται ότι λειτούργησαν επιταχυντικά, παρατηρούνται σημαντικές διαφοροποιήσεις στον τρόπο και το εύρος της επιτάχυνσης, καθώς και στον βαθμό στον οποίο οι επιθέσεις ενίσχυσαν ήδη υπάρχουσες στρατηγικές. Και στις τρεις περιπτώσεις υπήρχαν ήδη στρατηγικές ή κατευθύνσεις που σχετίζονταν με την κυβερνοασφάλεια. Και οι τρεις χώρες αξιοποίησαν τις κυβερνοεπιθέσεις για να εμβαθύνουν τη συνεργασία με το ΝΑΤΟ, ενισχύοντας τις δυνατότητες άμυνάς τους. Οι κυβερνοεπιθέσεις ανέδειξαν τη σημασία του κυβερνοχώρου ως πεδίου γεωπολιτικής αντιπαράθεσης.

Στην Εσθονία, η επιτάχυνση ήταν θεσμική και τεχνολογική, ενώ στην Ουκρανία επικεντρώθηκε κυρίως στην αντίδραση σε συνθήκες κρίσης. Στην Πολωνία, η επιτάχυνση είχε περισσότερο προληπτικό

χαρακτήρα, ενσωματώνοντας τις κυβερνοεπιθέσεις σε ένα ήδη ισχυρό στρατηγικό πλαίσιο. Η Ουκρανία, ως χώρα εκτός ΝΑΤΟ, εξαρτήθηκε περισσότερο από την εξωτερική υποστήριξη, ενώ η Εσθονία και η Πολωνία αξιοποίησαν τη θεσμική στήριξη της Συμμαχίας.

Οι ρωσικές κυβερνοεπιθέσεις λειτούργησαν επιταχυντικά και στις τρεις χώρες, αλλά με διαφορετικό εύρος, βάθος και προσανατολισμό. Ενώ οι επιθέσεις ανέδειξαν τις αδυναμίες και τις ανάγκες κάθε κράτους, ενίσχυσαν παράλληλα τις προϋπάρχουσες στρατηγικές, προσφέροντας χρήσιμα διδάγματα για τη διεθνή συνεργασία και την προσαρμογή στον κυβερνοχώρο.

## Επιταχυντική Δράση

Η επιταχυντική δράση αφορά περιπτώσεις όπου οι κυβερνοεπιθέσεις δεν προκαλούν ριζικές αλλαγές ή ανατροπές στις στρατηγικές των κρατών-στόχων, αλλά λειτουργούν ενισχυτικά, επιταχύνοντας την εφαρμογή ή την εξέλιξη ήδη υφιστάμενων στρατηγικών κατευθύνσεων. Οι επιθέσεις αναδεικνύουν τις αδυναμίες, τις ευκαιρίες ή τις προτεραιότητες ενός κράτους, ενθαρρύνοντας τις αρμόδιες αρχές να επιταχύνουν τη λήψη αποφάσεων ή την υλοποίηση πολιτικών που βρίσκονταν ήδη σε πορεία υλοποίησης. Η επιτάχυνση αυτή μπορεί να αφορά διάφορους τομείς: Επενδύσεις σε τεχνολογίες κυβερνοασφάλειας και αναβάθμιση κρίσιμων υποδομών για την πρόληψη μελλοντικών επιθέσεων. Δημιουργία νέων εθνικών στρατηγικών κυβερνοασφάλειας ή ιδρυμάτων, όπως το NASK στην Πολωνία ή το CCDCOE στην Εσθονία. Εμβάθυνση της συνεργασίας με συμμάχους, όπως το ΝΑΤΟ, και συμμετοχή σε κοινές ασκήσεις ή πρωτοβουλίες για την αντιμετώπιση υβριδικών απειλών. Προγράμματα εκπαίδευσης για πολίτες και κρατικούς λειτουργούς, τα οποία μπορεί να επιταχύνθηκαν λόγω της αναγνώρισης του κινδύνου από τις επιθέσεις.

Στην περίπτωση της Ουκρανίας, οι κυβερνοεπιθέσεις δεν προκάλεσαν τη στροφή της χώρας προς το ΝΑΤΟ ούτε την απόφαση για ανάπτυξη στρατηγικής κυβερνοάμυνας. Αυτές οι κατευθύνσεις είχαν ήδη τεθεί σε εφαρμογή, ως αποτέλεσμα της στρατιωτικής απειλής που προέκυψε από την προσάρτηση της Κριμαίας και τις συγκρούσεις στο Ντονμπάς. Ωστόσο, οι κυβερνοεπιθέσεις λειτουργούσαν επιταχυντικά, αναδεικνύοντας τη σοβαρότητα των υβριδικών απειλών και ενισχύοντας την ανάγκη για ταχύτερη και πιο αποφασιστική υλοποίηση των σχετικών πολιτικών.

Η διαφορά μεταξύ μιας καταλυτικής και μιας επιταχυντικής δράσης μπορεί να συνοψιστεί ως εξής: Η καταλυτική δράση προκαλεί μια νέα στρατηγική κατεύθυνση ή ανατρέπει ριζικά την υπάρχουσα. Για παράδειγμα, μια επίθεση που θα ανάγκαζε την Ουκρανία να αλλάξει ολοκληρωτικά το στρατηγικό της προσανατολισμό από μια ουδέτερη στάση σε πλήρη ένταξη στο ΝΑΤΟ. Η επιταχυντική δράση ενισχύει την υλοποίηση μιας ήδη καθορισμένης στρατηγικής. Στην περίπτωση της Ουκρανίας, οι κυβερνοεπιθέσεις ενίσχυσαν την επείγουσα ανάγκη για θεσμικές μεταρρυθμίσεις, διεθνή συνεργασία και ενίσχυση των υποδομών κυβερνοασφάλειας.

Οι κυβερνοεπιθέσεις, όπως το BlackEnergy (2015) και το NotPetya (2017), δεν άλλαξαν τον στόχο της Ουκρανίας για συνεργασία με το ΝΑΤΟ. Αντίθετα, επιβεβαίωσαν την ορθότητα της κατεύθυνσης αυτής και επιτάχυναν την εφαρμογή μέτρων για την ενίσχυση της στρατηγικής κυβερνοάμυνας. Αυτός ο επιταχυντικός ρόλος είναι κρίσιμος για την κατανόηση του τρόπου με τον οποίο οι κυβερνοεπιθέσεις λειτουργούν ως μέρος ενός ευρύτερου πλαισίου υβριδικών απειλών.

Ένα άλλο παράδειγμα επιταχυντικής δράσης παρατηρείται στην Πολωνία, όπου οι ρωσικές κυβερνοεπιθέσεις της δεκαετίας 2010-2020 ενίσχυσαν την εστίαση της χώρας στην προστασία κρίσιμων υποδομών και τη διεθνή συνεργασία. Οι επιθέσεις δεν αποτέλεσαν την πρωταρχική αιτία για τις

στρατηγικές επιλογές της Πολωνίας, καθώς η χώρα είχε ήδη έναν ισχυρό στρατηγικό προσανατολισμό προς το ΝΑΤΟ και την Ευρωπαϊκή Ένωση. Ωστόσο, οι επιθέσεις επιτάχυναν τις προσπάθειες θεσμικής ενίσχυσης, οδηγώντας στην αναθεώρηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας το 2019.

Η Εσθονία μπορεί να φαίνεται ότι αποτελεί μια περίπτωση καταλυτικής δράσης λόγω της ριζικής αλλαγής στη στρατηγική της κυβερνοασφάλειας μετά τις επιθέσεις του 2007. Ωστόσο, πρέπει να λάβουμε υπόψη ότι η στρατηγική της Εσθονίας για την ενίσχυση της κυβερνοασφάλειας δεν ξεκίνησε αποκλειστικά εξαιτίας των επιθέσεων. Η χώρα είχε ήδη επενδύσει σημαντικά στην ψηφιοποίηση και τη χρήση τεχνολογίας στις δημόσιες υπηρεσίες, γεγονός που δημιούργησε τις βάσεις για τη θεσμική της αντίδραση.Οι κυβερνοεπιθέσεις λειτούργησαν ως επιταχυντής για την εφαρμογή αυτών των αλλαγών, ενισχύοντας την αντίληψη για την αναγκαιότητα της κυβερνοασφάλειας. Παρόλο που οι επιθέσεις του 2007 αποτέλεσαν σημείο καμπής, δεν δημιούργησαν από το μηδέν τη στρατηγική κυβερνοάμυνας της Εσθονίας. Αντίθετα, επιτάχυναν τις εξελίξεις και ενίσχυσαν τη διεθνή συνεργασία της χώρας, ιδίως με το ΝΑΤΟ.

## Καταλυτική Δράση

Η καταλυτική δράση αναφέρεται σε περιπτώσεις όπου οι κυβερνοεπιθέσεις οδηγούν σε θεμελιώδεις και άμεσες αλλαγές στη στρατηγική των κρατών-στόχων. Σε αυτές τις περιπτώσεις, οι επιθέσεις λειτουργούν ως «σημεία καμπής», που αναγκάζουν τα κράτη να προσαρμόσουν τη στρατηγική τους από τη βάση.

Η επίθεση Stuxnet το 2010 αποτελεί ένα από τα πλέον χαρακτηριστικά παραδείγματα καταλυτικής δράσης στον κυβερνοχώρο. Το κακόβουλο λογισμικό Stuxnet, το οποίο αποδίδεται σε συνεργασία των Ηνωμένων Πολιτειών και του Ισραήλ, σχεδιάστηκε ειδικά για να στοχεύσει τις φυγοκεντρητές του πυρηνικού προγράμματος του Ιράν, προκαλώντας σοβαρές ζημιές στις φυσικές υποδομές. Η επίθεση αυτή δεν είχε μόνο τεχνικές και υλικές συνέπειες, αλλά επέφερε σημαντικές αλλαγές στη στρατηγική και την αντίληψη για τον κυβερνοχώρο παγκοσμίως.

Η επίθεση οδήγησε σε αναπροσαρμογή του πυρηνικού προγράμματος του Ιράν, καθώς οι φυσικές ζημιές συνοδεύτηκαν από την ανάγκη για αυξημένη κυβερνοασφάλεια και ανθεκτικότητα. Το Ιράν αναγνώρισε τον κυβερνοχώρο ως μία από τις κύριες απειλές για τις εθνικές του υποδομές και επένδυσε σημαντικά στη θωράκιση των κρίσιμων συστημάτων του. Η επίθεση Stuxnet αποτέλεσε σημείο καμπής για την παγκόσμια αντίληψη της κυβερνοασφάλειας. Κατέδειξε την ικανότητα των κυβερνοεπιθέσεων να προκαλούν σημαντικές φυσικές ζημιές και να επηρεάζουν στρατηγικές εθνικής ασφάλειας. Ως αποτέλεσμα, πολλές χώρες αναγνώρισαν την ανάγκη για τη δημιουργία στρατηγικών κυβερνοασφάλειας, ενώ ο κυβερνοχώρος άρχισε να αντιμετωπίζεται ως αυτόνομο στρατηγικό πεδίο, ισότιμο με τα παραδοσιακά πεδία σύγκρουσης (χερσαίο, θαλάσσιο, εναέριο, διαστημικό). Η ανάγκη για κανονιστικά πλαίσια στον κυβερνοχώρο ενισχύθηκε μετά το Stuxnet. Οδήγησε σε διεθνείς συζητήσεις για τη θέσπιση κανόνων που θα διέπουν τη χρήση κυβερνοόπλων και θα καθορίζουν τα όρια των κυβερνοεπιχειρήσεων στο διεθνές δίκαιο. Το Tallinn Manual αποτελεί ένα χαρακτηριστικό παράδειγμα αυτής της προσπάθειας, παρέχοντας κατευθυντήριες γραμμές για την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο (Schmitt, 2017).

Η διάκριση μεταξύ επιταχυντικής και καταλυτικής δράσης βασίζεται στη φύση των στρατηγικών αλλαγών που προκαλούνται από τις κυβερνοεπιθέσεις. Η επιταχυντική δράση λειτουργεί ως ενισχυτής ή

επιταχυντής ήδη υπαρχουσών στρατηγικών κατευθύνσεων, επιταχύνοντας την εφαρμογή ή την υλοποίησή τους. Αντίθετα, η καταλυτική δράση επιφέρει ριζικές και θεμελιώδεις αλλαγές στη στρατηγική των κρατών-στόχων, αναδιαμορφώνοντας πλήρως το στρατηγικό τους πλαίσιο. Στην πράξη, υπάρχουν περιπτώσεις όπου η διάκριση μπορεί να φαίνεται δυσδιάκριτη, καθώς η επίδραση μιας κυβερνοεπίθεσης μπορεί να ενσωματώνει στοιχεία και των δύο δράσεων. Ωστόσο, οι δύο έννοιες παραμένουν διακριτές βάσει του βαθμού αλλαγής που προκαλούν.

Για παράδειγμα, η Εσθονία συνδυάζει καταλυτικά και επιταχυντικά στοιχεία. Οι κυβερνοεπιθέσεις του 2007 αποτέλεσαν το σημείο καμπής για τη θεσμική της μεταρρύθμιση, αλλά οι αλλαγές που πραγματοποιήθηκαν βασίστηκαν σε προϋπάρχουσες τάσεις ψηφιοποίησης και συνεργασίας με διεθνείς οργανισμούς. Η κατανόηση των δύο εννοιών είναι κρίσιμη για τη μελέτη της επίδρασης των κυβερνοεπιθέσεων. Η διάκριση μεταξύ επιταχυντικής και καταλυτικής δράσης βοηθά στη διαμόρφωση πιο στοχευμένων στρατηγικών κυβερνοάμυνας. Επιπλέον, αναδεικνύει τη σημασία της διεθνούς συνεργασίας και της θεσμικής ανθεκτικότητας ως κεντρικών στοιχείων για την αντιμετώπιση των υβριδικών απειλών.

# Κεφάλαιο 3: Ιστορική Ανασκόπηση (2010-2020)

Η περίοδος 2010-2020 χαρακτηρίστηκε από μια ραγδαία αύξηση κυβερνοεπιθέσεων, με τη Ρωσία να αναδεικνύεται σε έναν από τους κυρίαρχους δρώντες στον κυβερνοχώρο (Giles, 2016; Schmitt, 2017; Lewis, 2021). Κατά τη διάρκεια αυτής της δεκαετίας, οι κυβερνοεπιθέσεις εξελίχθηκαν από μεμονωμένα περιστατικά σε συντονισμένες εκστρατείες, που στόχευαν κρατικές υποδομές και ιδιωτικούς φορείς. Οι επιθέσεις αυτές δεν είχαν μόνο άμεσες υλικές συνέπειες, αλλά εντάχθηκαν σε ένα ευρύτερο πλαίσιο υβριδικού πολέμου, στοχεύοντας στην πολιτική αποσταθεροποίηση, την παραπληροφόρηση και τη διάβρωση της εμπιστοσύνης στους κρατικούς θεσμούς. Παράλληλα, η περίοδος αυτή ανέδειξε τον κυβερνοχώρο ως ένα νέο πεδίο αντιπαράθεσης, με κράτη και διεθνείς οργανισμούς, όπως το ΝΑΤΟ, να επενδύουν σημαντικά στην ανάπτυξη στρατηγικών και υποδομών κυβερνοασφάλειας.

Το ερώτημα που εξετάζεται στο παρόν κεφάλαιο είναι: Πώς χρησιμοποιεί η Ρωσία τις κυβερνοεπιθέσεις ως εργαλείο στη στρατηγική της για την επίτευξη γεωπολιτικών στόχων; Από την ανάλυση προκύπτει ότι αυτές οι επιθέσεις εντάσσονται σε μια ευρύτερη στρατηγική υβριδικού πολέμου, όπου ο κυβερνοχώρος αξιοποιείται όχι μόνο για την πρόκληση ζημιών, αλλά κυρίως για την άσκηση πίεσης, την αποσταθεροποίηση και την επίτευξη στρατηγικών πλεονεκτημάτων.

Οι χώρες-δείγματα που επιλέχθηκαν, δηλαδή η Εσθονία, η Ουκρανία και η Πολωνία, προσφέρουν μια αντιπροσωπευτική εικόνα της ρωσικής στρατηγικής. Η Εσθονία είναι η πρώτη χώρα που βίωσε μια συντονισμένη κυβερνοεπίθεση μεγάλης κλίμακας το 2007. Η επίθεση αυτή αποτέλεσε ορόσημο για την παγκόσμια κατανόηση των κυβερνοαπειλών και την ανάπτυξη στρατηγικών κυβερνοασφάλειας. Αναλύοντας την περίπτωση της Εσθονίας, βλέπουμε πώς μια μικρή, ψηφιοποιημένη χώρα μπορεί να μετατρέψει μια κρίση σε ευκαιρία, εξελισσόμενη σε ηγέτη της κυβερνοασφάλειας. Η Ουκρανία είναι μια χώρα που αποτέλεσε πεδίο συνδυασμένων επιχειρήσεων κυβερνοεπιθέσεων και στρατιωτικής επιθετικότητας, ιδιαίτερα κατά την περίοδο της προσάρτησης της Κριμαίας το 2014 και του πολέμου στο Ντονμπάς. Οι κυβερνοεπιθέσεις, όπως το NotPetya (2017), είχαν ως στόχο όχι μόνο τις υποδομές της χώρας, αλλά και την αποσταθεροποίηση της κοινωνίας και της οικονομίας της. Η Πολωνία, ως μέλος του ΝΑΤΟ και στρατηγικός εταίρος στην Ανατολική Ευρώπη, έχει δεχθεί κυβερνοεπιθέσεις που στόχευαν την υπονόμευση της εμπιστοσύνης στους θεσμούς και στη Συμμαχία. Η στρατηγική σημασία της Πολωνίας έγκειται στο γεγονός ότι αποτελεί κομβικό σημείο για την ανατολική πτέρυγα του ΝΑΤΟ, γεγονός που την καθιστά στόχο επιχειρήσεων υβριδικού πολέμου. Οι ρωσικές κυβερνοεπιθέσεις εδώ δείχνουν πώς η Μόσχα επιχειρεί να διαμορφώσει τις γεωπολιτικές ισορροπίες και να περιορίσει τη δυτική επιρροή.

*Συνολικά, Οι ρωσικές κυβερνοεπιθέσεις δεν είναι τυχαίες ή απλές παραβιάσεις. Είναι ένα ισχυρό εργαλείο που η Ρωσία χρησιμοποιεί για να αποδυναμώσει άλλα κράτη και να ελέγξει την ισορροπία δυνάμεων στον κόσμο.*

## 3.1 Μελέτες Περίπτωσης: Εσθονία

## Η Εσθονία ως Στόχος και η Ανάδειξη του Κυβερνοχώρου

Η Εσθονία αποτελεί χαρακτηριστική περίπτωση χώρας που βίωσε την καταστροφική ισχύ των κυβερνοεπιθέσεων και χρησιμοποίησε αυτήν την εμπειρία για να εδραιώσει τη θέση της ως ηγέτιδα δύναμη στην κυβερνοασφάλεια. Οι επιθέσεις που δέχθηκε δεν περιορίστηκαν μόνο στο 2007, αλλά συνεχίστηκαν σε όλη τη δεκαετία 2010-2020, αναδεικνύοντας τη Ρωσία ως κύριο αντίπαλο στον κυβερνοχώρο . Η επίθεση του 2007 αποτέλεσε την πρώτη μεγάλη συντονισμένη κυβερνοεπίθεση κατά κράτους στην Ευρώπη. Οι στόχοι περιλάμβαναν κυβερνητικούς οργανισμούς, τράπεζες, μέσα μαζικής ενημέρωσης και παρόχους υπηρεσιών διαδικτύου, προκαλώντας σημαντική διατάραξη των κρίσιμων υποδομών της χώρας (Giles, 2016). Οι επιθέσεις πραγματοποιήθηκαν μέσω της μεθόδου “distributed denial of service” (DDoS), όπου μεγάλος όγκος αιτημάτων υπερφόρτωσε τους διακομιστές, καθιστώντας τους μη λειτουργικούς. Περίπου 58 κυβερνητικές ιστοσελίδες, συμπεριλαμβανομένων εκείνων του κοινοβουλίου και τραπεζικών οργανισμών, επηρεάστηκαν σοβαρά, με ορισμένες να παραμένουν ανενεργές για μέρες. Το πραγματικό πλήγμα δεν περιορίστηκε μόνο στις επιχειρησιακές συνέπειες, αλλά είχε και ευρύτερο γεωπολιτικό αντίκτυπο. Η επίθεση αποκάλυψε την ευπάθεια ενός από τα πιο ψηφιοποιημένα κράτη στον κόσμο και ανέδειξε τον κυβερνοχώρο ως νέο πεδίο γεωπολιτικής σύγκρουσης (Schmitt, 2017; Zetter, 2017). Η άμεση σύνδεση της κυβερνοασφάλειας με τη συνολική εθνική ασφάλεια έγινε εμφανής, ενώ παράλληλα αναδείχθηκε η ανάγκη για διεθνή συνεργασία και ανταλλαγή πληροφοριών στον τομέα αυτό.

Η σημασία της επίθεσης έγκειται επίσης στον τρόπο με τον οποίο λειτούργησε ως σημείο εκκίνησης για τη συζήτηση σχετικά με την ευθύνη και τη λογοδοσία στον κυβερνοχώρο. Η απουσία σαφών νομικών πλαισίων δημιούργησε ένα κενό, το οποίο εκμεταλλεύτηκαν οι δράστες (Tikk et al., 2010). Αυτό το κενό οδήγησε σε διεθνείς πρωτοβουλίες για την καθιέρωση κατευθυντήριων γραμμών, όπως το Tallinn Manual, ενισχύοντας την αντίληψη ότι ο κυβερνοχώρος δεν είναι απλώς ένας τεχνικός τομέας, αλλά ένα κρίσιμο πεδίο στρατηγικής σημασίας (Schmitt, 2017; Giles, 2016). Επιπλέον, η επίθεση υπογράμμισε τη σημασία της ανθεκτικότητας σε εθνικό επίπεδο. Η Εσθονία, ως χώρα που βασίζεται έντονα στην ψηφιακή της υποδομή, κλήθηκε να ενισχύσει τις άμυνες της όχι μόνο τεχνικά, αλλά και μέσω της ευαισθητοποίησης του πληθυσμού και της ενίσχυσης της κοινωνικής συνοχής. Ταυτόχρονα, η συνεργασία με διεθνείς εταίρους αποτέλεσε κρίσιμο βήμα για την ανάπτυξη ολοκληρωμένων στρατηγικών αντιμετώπισης κυβερνοαπειλών. Η έλλειψη θεσπισμένων κανόνων για τον κυβερνοχώρο εκείνη την εποχή αποτέλεσε κίνητρο για την ανάπτυξη διεθνών κανόνων. Η Εσθονία λειτούργησε ως καταλύτης για την εισαγωγή νομικών πλαισίων που καθορίζουν την ευθύνη και την απόκριση στις κυβερνοεπιθέσεις. Οι προτάσεις για κατευθυντήριες γραμμές που απορρέουν από αυτές τις επιθέσεις επηρέασαν καθοριστικά την ανάπτυξη του διεθνούς δικαίου στον κυβερνοχώρο (Tikk, Kaska και Vihul, 2010).

Η συζήτηση που ξεκίνησε τότε έχει εξελιχθεί σε έναν ευρύτερο διάλογο για την ανάγκη δημιουργίας διεθνών συνθηκών που θα ρυθμίζουν τη χρήση κυβερνοεπιθέσεων ως εργαλείου στρατηγικής (Schmitt, 2017; Tikk et al., 2010). Οι επιπτώσεις της επίθεσης στην Εσθονία υπήρξαν μακροχρόνιες, καθιστώντας τη χώρα σημείο αναφοράς για την ανθεκτικότητα και τη στρατηγική στον κυβερνοχώρο (Ottis, 2008). Το παράδειγμα της Εσθονίας απέδειξε ότι ακόμη και τα μικρότερα κράτη μπορούν να επηρεάσουν σημαντικά τη διεθνή σκηνή μέσω καινοτομίας, στρατηγικής σκέψης και διεθνούς συνεργασίας (Giles, 2016; Herzog, 2011).

## Η Αντίδραση της Εσθονίας και η Εξέλιξη της Κυβερνοστρατηγικής της

Η αντίδραση της Εσθονίας ήταν άμεση και πολυδιάστατη. Η ίδρυση του Κέντρου Αριστείας Συνεργατικής Κυβερνοάμυνας του NATO (CCDCOE) το 2008 αποτέλεσε μια από τις πιο σημαντικές πρωτοβουλίες που ανέδειξαν την Εσθονία ως κεντρικό παίκτη στην παγκόσμια κυβερνοασφάλεια (Conley et al., 2016). Το κέντρο έγινε σημείο αναφοράς για την ανάλυση κυβερνοεπιθέσεων, την εκπαίδευση και την ανάπτυξη διεθνών στρατηγικών αντιμετώπισης. Μέσα από τις δράσεις του CCDCOE, η Εσθονία μπόρεσε να συμβάλει στη δημιουργία διεθνών πρωτοκόλλων που ενίσχυσαν τη συνεργασία μεταξύ των κρατών-μελών του NATO και παρείχαν έναν οδικό χάρτη για την αντιμετώπιση παρόμοιων επιθέσεων στο μέλλον. Οι πρωτοβουλίες αυτές ενίσχυσαν την εικόνα της Εσθονίας ως ηγέτιδας στον τομέα της κυβερνοασφάλειας και ανέδειξαν την ανάγκη για συλλογική δράση στον κυβερνοχώρο.

Η Εσθονία επίσης εισήγαγε πρωτοποριακά μέτρα όπως οι data embassies, τα οποία αποτελούν εφεδρικές υποδομές για την αποθήκευση κυβερνητικών δεδομένων εκτός συνόρων. Αυτή η προσέγγιση εξασφάλισε τη συνέχεια της λειτουργίας της κυβέρνησης ακόμα και σε περιπτώσεις ευρείας κλίμακας κρίσεων ή επιθέσεων. Τα μέτρα αυτά ενίσχυσαν την εμπιστοσύνη προς την κυβέρνηση και δημιούργησαν ένα πρότυπο που ακολουθήθηκε και από άλλες χώρες. Για παράδειγμα, τα δεδομένα της Εσθονίας φιλοξενούνται σε διακομιστές που βρίσκονται στην Ελβετία, διασφαλίζοντας την πρόσβαση σε κρίσιμες πληροφορίες ακόμα και αν οι φυσικές υποδομές της χώρας υποστούν επίθεση. Αυτή η καινοτομία υπογράμμισε τη σημασία της τεχνολογικής ανθεκτικότητας ως αναπόσπαστου μέρους της εθνικής ασφάλειας (Herzog, 2011).

Η επένδυση στην εκπαίδευση και ευαισθητοποίηση του κοινού υπήρξε επίσης κρίσιμη. Το εκπαιδευτικό σύστημα της Εσθονίας ενσωμάτωσε μαθήματα κυβερνοασφάλειας, ενώ πραγματοποιήθηκαν εκστρατείες ενημέρωσης για τους πολίτες. Αυτές οι δράσεις συνέβαλαν στη μείωση της ευπάθειας της κοινωνίας απέναντι στις κυβερνοαπειλές (Tikk et al., 2010). Επιπλέον, η κυβέρνηση της Εσθονίας διοργάνωσε προγράμματα προσομοίωσης κυβερνοεπιθέσεων, στα οποία συμμετείχαν δημόσιοι υπάλληλοι, εταιρείες και μαθητές, δημιουργώντας μια κουλτούρα εγρήγορσης και άμεσης απόκρισης. Αυτή η ολιστική προσέγγιση, που συνδύαζε τεχνολογική αναβάθμιση και κοινωνική συνοχή, κατέστησε την Εσθονία παράδειγμα για την οικοδόμηση ανθεκτικών κρατικών και κοινωνικών δομών. (CCDCOE, 2021).

Η συνεργασία με ιδιωτικούς φορείς αποτέλεσε ένα ακόμα στοιχείο της στρατηγικής της Εσθονίας. Η συμμετοχή τεχνολογικών εταιρειών σε κοινές πρωτοβουλίες και η ανταλλαγή πληροφοριών σχετικά με απειλές στον κυβερνοχώρο ενίσχυσαν τη συνολική ετοιμότητα της χώρας. Οι ιδιωτικοί φορείς παρείχαν τεχνογνωσία και εργαλεία που συνέβαλαν στην ταχεία ανάκαμψη από κυβερνοεπιθέσεις, ενώ ταυτόχρονα ενίσχυσαν την καινοτομία στον τομέα της κυβερνοασφάλειας.

## Η Συνεργασία με το NATO και η Διεθνής Συνεισφορά

Η συνεργασία της Εσθονίας με το NATO ενίσχυσε σημαντικά τη θέση της χώρας στον διεθνή χώρο. Μέσα από ασκήσεις όπως οι Locked Shields και οι Cyber Coalition, η Εσθονία ανέπτυξε εξειδικευμένες ικανότητες αντιμετώπισης κυβερνοεπιθέσεων μεγάλης κλίμακας. Οι ασκήσεις αυτές προσομοίωσαν σύνθετα σενάρια κυβερνοπολέμου, βοηθώντας τα μέλη του NATO να αναπτύξουν αποτελεσματικές στρατηγικές άμυνας. Επιπλέον, η συνεισφορά της Εσθονίας στη διαμόρφωση του Tallinn Manual αποτέλεσε μια από τις σημαντικότερες εξελίξεις στη ρύθμιση του κυβερνοχώρου. Το εγχειρίδιο αυτό θέτει τις αρχές του διεθνούς δικαίου για τη χρήση του κυβερνοχώρου σε στρατιωτικά και μη στρατιωτικά πλαίσια (Schmitt, 2017). Η καθοριστική συμμετοχή της Εσθονίας ανέδειξε τη χώρα ως

παράδειγμα για τη διεθνή κοινότητα. Η διεθνής συνεργασία αποτέλεσε τον πυρήνα της στρατηγικής της Εσθονίας. Η εστίαση στη συλλογική ασφάλεια και η ανταλλαγή τεχνογνωσίας ενίσχυσαν τη θέση της Εσθονίας ως ηγέτιδας δύναμης στην κυβερνοασφάλεια (Janczewski και Colarik, 2008).

Η περίπτωση της Εσθονίας αποδεικνύει ότι οι κυβερνοεπιθέσεις λειτούργησαν κυρίως ως επιταχυντής της στρατηγικής κυβερνοασφάλειας της χώρας. Αν και οι επιθέσεις του 2007 ανέδειξαν τις ευπάθειες ενός έντονα ψηφιοποιημένου κράτους, η Εσθονία ήδη διέθετε τη στρατηγική κατεύθυνση προς την ενίσχυση της τεχνολογικής και κοινωνικής ανθεκτικότητας. Οι επιθέσεις δεν επέφεραν ριζική αλλαγή στις στρατηγικές επιλογές της χώρας, αλλά επιτάχυναν την εφαρμογή μέτρων, όπως η ίδρυση του CCDCOE, η ανάπτυξη των *data embassies* και η ενίσχυση της διεθνούς συνεργασίας με το NATO.

Αυτό σημαίνει ότι η Εσθονία δεν χρειάστηκε να αλλάξει εντελώς πορεία, όπως θα συνέβαινε στην περίπτωση καταλυτικής δράσης. Αντίθετα, η εμπειρία από τις κυβερνοεπιθέσεις επιβεβαίωσε τη στρατηγική που είχε ήδη χαράξει και ενίσχυσε την αποφασιστικότητα της χώρας να επενδύσει στην ανθεκτικότητα και την καινοτομία. Οι θεσμικές και τεχνολογικές αλλαγές ήταν συνέπεια μιας ενισχυμένης αντίληψης της σημασίας του κυβερνοχώρου, παρά μιας απόλυτης αναδιάρθρωσης της στρατηγικής της.

## 3.2 Μελέτη Περίπτωσης: Ουκρανία

### Οι Κυβερνοεπιθέσεις ως Εργαλείο Αποσταθεροποίησης (2010-2020)

Η Ουκρανία αποτελεί κομβική περίπτωση για την κατανόηση του ρόλου των ρωσικών κυβερνοεπιθέσεων, οι οποίες εντάσσονται σε ένα ευρύτερο πλαίσιο υβριδικού πολέμου που συνδυάζει στρατιωτικές επιχειρήσεις, παραπληροφόρηση και πολιτική αποσταθεροποίηση (Schmitt, 2017). Οι κυβερνοεπιθέσεις που δέχθηκε η Ουκρανία κατά τη δεκαετία 2010-2020 ήταν συστηματικές και πολυδιάστατες, στοχεύοντας τόσο στη διατάραξη κρίσιμων υποδομών όσο και στη δημιουργία κοινωνικής και πολιτικής αστάθειας. Σε αυτό το πλαίσιο, η ανάλυση συγκεκριμένων παραδειγμάτων, όπως οι επιθέσεις *BlackEnergy* και *NotPetya*, φωτίζει τη στρατηγική φύση και τον ευρύτερο αντίκτυπο αυτών των κυβερνοεπιχειρήσεων στη διαμόρφωση της στρατηγικής ασφάλειας της Ουκρανίας..

Η επίθεση BlackEnergy (2015) ήταν μία από τις πρώτες που προκάλεσε άμεσες και μετρήσιμες επιπτώσεις. Οι χάκερς χρησιμοποίησαν εξελιγμένο κακόβουλο λογισμικό για να διεισδύσουν στα δίκτυα ενεργειακών εταιρειών, διακόπτοντας την ηλεκτροδότηση σε μεγάλα τμήματα της χώρας και αφήνοντας χιλιάδες νοικοκυριά χωρίς ρεύμα για ώρες. Το περιστατικό αυτό δεν ήταν μόνο τεχνικά εντυπωσιακό, αλλά ανέδειξε και την ευπάθεια των κρίσιμων υποδομών σε ψηφιακές απειλές, προκαλώντας ανησυχία σε εθνικό και διεθνές επίπεδο. Οι αναλύσεις δείχνουν ότι η επίθεση είχε διπλό στόχο: αφενός την αποδιοργάνωση της λειτουργίας του κράτους και αφετέρου την υπονόμευση της εμπιστοσύνης των πολιτών προς την κυβέρνηση (Zetter, 2017).

Η επίθεση NotPetya (2017) αποτέλεσε ένα ακόμη πιο καταστροφικό περιστατικό, καθώς οι χάκερς κατάφεραν να παραλύσουν κυβερνητικά δίκτυα, τραπεζικά συστήματα και ιδιωτικές εταιρείες,

προκαλώντας συνολικές οικονομικές ζημιές που ξεπέρασαν το ένα δισεκατομμύριο δολάρια (Greenberg, 2018). Το κακόβουλο λογισμικό εξαπλώθηκε ταχύτατα, επηρεάζοντας όχι μόνο την Ουκρανία αλλά και διεθνείς εταιρείες που δραστηριοποιούνταν στη χώρα. Οι ειδικοί θεωρούν ότι η επίθεση NotPetya είχε στόχο να προκαλέσει χάος και να υπονομεύσει τη λειτουργία του κράτους, ενώ ταυτόχρονα λειτούργησε ως μήνυμα προς άλλες χώρες σχετικά με τη δύναμη του ρωσικού κυβερνοοπλοστασίου.

Η στρατηγική αυτών των επιθέσεων εστίαζε στην αποσταθεροποίηση της πολιτικής και κοινωνικής συνοχής της Ουκρανίας. Οι επιθέσεις δεν περιορίζονταν μόνο στην πρόκληση υλικών ζημιών, αλλά στόχευαν και στη δημιουργία μιας εικόνας αδυναμίας των κρατικών θεσμών. Μέσω της διάδοσης παραπληροφόρησης και ψεύτικων ειδήσεων στα κοινωνικά δίκτυα, οι χάκερς προσπάθησαν να δημιουργήσουν κλίμα φόβου και αβεβαιότητας, ενισχύοντας την πολιτική και κοινωνική αστάθεια. Για παράδειγμα, τα ψευδή αφηγήματα που διαδόθηκαν κατά τη διάρκεια της κρίσης στο Ντονμπάς υπονόμευσαν την ενότητα της Ουκρανίας, προωθώντας τις ρωσικές γεωπολιτικές επιδιώξεις (NATO CCDCOE, 2023). Παράλληλα, οι επιθέσεις αυτές συνδυάστηκαν με εκστρατείες παραπληροφόρησης που είχαν ως στόχο να χειραγωγήσουν την κοινή γνώμη, τόσο στην Ουκρανία όσο και στο εξωτερικό. Χρησιμοποιώντας μέσα κοινωνικής δικτύωσης, οι χάκερς και οι παραστρατιωτικοί δρώντες προωθούσαν αφηγήματα που ενίσχυαν τη δυσπιστία προς τη δυτική υποστήριξη και υπογράμμιζαν την ανικανότητα της κυβέρνησης να διαχειριστεί τις κρίσεις (Tikk et al., 2010; Greenberg, 2018). Αυτός ο συνδυασμός κυβερνοεπιθέσεων και προπαγάνδας αποτέλεσε τον πυρήνα της ρωσικής στρατηγικής υβριδικού πολέμου, καταδεικνύοντας την αποτελεσματικότητα της χρήσης του κυβερνοχώρου ως εργαλείου γεωπολιτικής πίεσης

## Εξέλιξη της Στρατηγικής Προσέγγισης πριν από την Εισβολή του 2022

Η περίοδος πριν από την εισβολή του 2022 σηματοδότησε μια σημαντική αλλαγή στη φύση και τον στόχο των ρωσικών κυβερνοεπιθέσεων. Σε αντίθεση με την προηγούμενη δεκαετία, οι επιθέσεις δεν περιορίστηκαν στην αποσταθεροποίηση, αλλά στόχευσαν άμεσα στην υποστήριξη στρατιωτικών επιχειρήσεων μεγάλης κλίμακας. Οι αλλαγές στη στρατηγική αυτή αντανακλούσαν την ανάγκη της Ρωσίας να ενισχύσει την επιρροή της και να προετοιμάσει το έδαφος για την επερχόμενη στρατιωτική σύγκρουση. Χαρακτηριστικά παραδείγματα αποτελούν τα κακόβουλα λογισμικά Industroyer2 και WhisperGate, τα οποία σχεδιάστηκαν για να παραλύσουν κρίσιμες υποδομές, όπως ενεργειακά δίκτυα και τηλεπικοινωνιακά συστήματα. Η επίθεση Industroyer2 στοχεύει ειδικά στα συστήματα SCADA (Supervisory Control and Data Acquisition), τα οποία ελέγχουν τις βιομηχανικές διαδικασίες και τις ενεργειακές υποδομές. Αυτές οι επιθέσεις δεν περιορίστηκαν στη δημιουργία διαταραχών, αλλά επιδίωκαν να προκαλέσουν συστημική κατάρρευση που θα δυσχέραινε τις αντιδράσεις της Ουκρανίας σε στρατιωτικό επίπεδο (NATO CCDCOE, 2023). Παράλληλα, το WhisperGate, ένα εξελιγμένο κακόβουλο λογισμικό που συνδυάζει ransomware και καταστροφικές λειτουργίες, προκάλεσε εκτεταμένες ζημιές σε κυβερνητικά και ιδιωτικά δίκτυα, δυσχεραίνοντας περαιτέρω τη λειτουργία των κρατικών υπηρεσιών. Οι επιθέσεις αυτές συνδυάστηκαν με συντονισμένες προσπάθειες διακοπής στρατιωτικών επικοινωνιών. Οι ρωσικές επιχειρήσεις στον κυβερνοχώρο επικεντρώθηκαν στην εξουδετέρωση των συστημάτων επικοινωνίας της Ουκρανίας, γεγονός που καθυστέρησε τη διεθνή ανθρωπιστική βοήθεια και δημιούργησε χάος στον πληθυσμό. Η έλλειψη άμεσης πρόσβασης σε κρίσιμες πληροφορίες δυσχέρανε τη λήψη αποφάσεων, ενώ οι ρωσικές δυνάμεις εκμεταλλεύτηκαν τη σύγχυση για να ενισχύσουν την αποτελεσματικότητα των στρατιωτικών τους επιχειρήσεων.

Η εντατικοποίηση της παραπληροφόρησης ήταν ένα ακόμη χαρακτηριστικό στοιχείο της στρατηγικής. Κατά τη διάρκεια αυτής της περιόδου, οι ρωσικές επιχειρήσεις χρησιμοποίησαν κοινωνικά δίκτυα και άλλες διαδικτυακές πλατφόρμες για τη διάδοση ψευδών αφηγημάτων που δικαιολογούσαν τις στρατιωτικές ενέργειες της Μόσχας. Με αφηγήματα που περιλάμβαναν ισχυρισμούς για «εθνοκάθαρση»

στο Ντονμπάς ή «ναζιστική απειλή», η Ρωσία προσπάθησε να χειραγωγήσει τη διεθνή κοινή γνώμη και να κερδίσει υποστήριξη από συγκεκριμένες ομάδες πληθυσμού. Αυτή η στρατηγική αποδείχθηκε αποτελεσματική στη δημιουργία σύγχυσης και την αποδυνάμωση της διεθνούς αντίδρασης στις ενέργειές της. Η στρατηγική της Ρωσίας στον κυβερνοχώρο προσαρμόστηκε στις γεωπολιτικές της επιδιώξεις, αποδεικνύοντας την ευελιξία και την προσαρμοστικότητα των τακτικών της. Κατά την περίοδο 2010-2020, οι ρωσικές κυβερνοεπιθέσεις επικεντρώθηκαν στη διάβρωση της εμπιστοσύνης στους κρατικούς θεσμούς και στη δημιουργία κοινωνικού και πολιτικού διχασμού. Για παράδειγμα, οι επιθέσεις DDoS έχουν χρησιμοποιηθεί εκτενώς για να παραλύσουν κρίσιμες υποδομές, όπως στην περίπτωση της Εσθονίας το 2007 (Ottis, 2008).Στις παραμονές της εισβολής του 2022, οι επιθέσεις απέκτησαν πιο επιχειρησιακό χαρακτήρα, λειτουργώντας ως πολλαπλασιαστές ισχύος για στρατιωτικές επιχειρήσεις. Χαρακτηριστικά παραδείγματα αποτελούν τα κακόβουλα λογισμικά Industroyer2 και WhisperGate, τα οποία στόχευσαν κρίσιμες υποδομές, όπως τα ενεργειακά δίκτυα και οι τηλεπικοινωνίες. Οι επιθέσεις αυτές συνδυάστηκαν με προσπάθειες διακοπής στρατιωτικών επικοινωνιών, καθυστερώντας τη διεθνή ανθρωπιστική βοήθεια και δημιουργώντας χάος στον πληθυσμό (CISA, 2022).Η στρατηγική της Ρωσίας στον κυβερνοχώρο προσαρμόζεται στις γεωπολιτικές της επιδιώξεις, αποδεικνύοντας την ευελιξία και την προσαρμοστικότητα των τακτικών της. Η μετάβαση από επιθέσεις που εστίαζαν στην αποσταθεροποίηση σε επιχειρήσεις που υποστήριζαν άμεσα στρατιωτικές κινήσεις υπογραμμίζει τη στρατηγική σημασία του κυβερνοχώρου στις σύγχρονες συγκρούσεις και την ικανότητα της Ρωσίας να προσαρμόζει τα εργαλεία της στις εκάστοτε συνθήκες.

## Η Απάντηση της Ουκρανίας και οι Σχέσεις με το ΝΑΤΟ

Η Ουκρανία αντέδρασε υιοθετώντας μια πολυεπίπεδη στρατηγική κυβερνοάμυνας, η οποία περιλάμβανε θεσμικές μεταρρυθμίσεις, τεχνολογικές αναβαθμίσεις και διεθνή συνεργασία. Κατά την περίοδο 2010-2020, η χώρα ανέπτυξε κέντρα κυβερνοάμυνας και ενίσχυσε τη νομοθεσία της για την προστασία κρίσιμων υποδομών. Το Εθνικό Κέντρο Κυβερνοασφάλειας, που ιδρύθηκε το 2016, αποτέλεσε βασικό φορέα για τη διαχείριση απειλών και την εκπαίδευση προσωπικού. Παράλληλα, η Ουκρανία επένδυσε στη δημιουργία εφεδρικών υποδομών και στον εκσυγχρονισμό των ενεργειακών της δικτύων, μειώνοντας την ευπάθειά της σε επιθέσεις που στόχευαν στην υποδομή της χώρας. Η συνεργασία της Ουκρανίας με το ΝΑΤΟ ενισχύθηκε σημαντικά μετά το 2014, καθώς οι δύο πλευρές αναγνώρισαν την ανάγκη για στενότερη συνεργασία στον τομέα της κυβερνοασφάλειας. Μέσα από κοινές ασκήσεις, όπως η Cyber Coalition, η Ουκρανία απέκτησε πρόσβαση σε τεχνογνωσία και προηγμένα εργαλεία, ενώ οι εταίροι του ΝΑΤΟ επωφελήθηκαν από την εμπειρία της Ουκρανίας στην αντιμετώπιση κυβερνοεπιθέσεων μεγάλης κλίμακας (NATO, 2023).

Η περίπτωση της Ουκρανίας καταδεικνύει τη στρατηγική προσαρμοστικότητα της Ρωσίας στον κυβερνοχώρο, όπου οι κυβερνοεπιθέσεις εξελίχθηκαν από εργαλεία αποσταθεροποίησης (2010-2020) σε μέσα υποστήριξης στρατιωτικών επιχειρήσεων (2022). Η σύγκριση των δύο περιόδων αναδεικνύει πώς η Ρωσία χρησιμοποιεί τον κυβερνοχώρο για να εξυπηρετήσει διαφορετικούς γεωπολιτικούς στόχους. Παράλληλα, η στρατηγική απάντηση της Ουκρανίας έδειξε τη σημασία της διεθνούς συνεργασίας και της επένδυσης σε ανθεκτικές υποδομές για την προστασία από υβριδικές απειλές. Η ενίσχυση της κυβερνοστρατηγικής της Ουκρανίας μέσα από διεθνή συνεργασία και η εμπειρία που απέκτησε από τις επιθέσεις την κατέστησαν κρίσιμο σύμμαχο για το ΝΑΤΟ στον τομέα της κυβερνοασφάλειας. Η δυναμική αυτή ενίσχυσε τη θέση της Ουκρανίας στη διεθνή σκηνή, ενώ ταυτόχρονα ανέδειξε τον κυβερνοχώρο ως

κρίσιμο εργαλείο τόσο για την άμυνα όσο και για την επιθετική στρατηγική σε ένα διαρκώς εξελισσόμενο γεωπολιτικό περιβάλλον.

## 3.3 Μελέτη Περίπτωσης: Πολωνία (2010-2020)

### Η Στρατηγική Σημασία της Πολωνίας και οι Κυβερνοεπιθέσεις

Η Πολωνία, ως κράτος-μέλος του NATO και της Ευρωπαϊκής Ένωσης, κατέχει κομβική γεωπολιτική θέση στην ανατολική Ευρώπη, λειτουργώντας ως προπύργιο της Συμμαχίας έναντι της ρωσικής επιρροής. Η γεωγραφική της θέση, ως πύλη μεταξύ της δυτικής Ευρώπης και της Ρωσίας, την καθιστά στρατηγικό παράγοντα για την ασφάλεια της περιοχής. Αυτή η γεωστρατηγική σημασία, σε συνδυασμό με την ιστορική ένταση στις σχέσεις Πολωνίας-Ρωσίας, κατέστησε τη χώρα έναν από τους πρωταρχικούς στόχους της ρωσικής στρατηγικής υβριδικού πολέμου κατά τη δεκαετία 2010-2020 (Giles, 2016; NATO, 2023). Η Ρωσία, αντιλαμβανόμενη τη στρατηγική σημασία της Πολωνίας, εφάρμοσε μια σειρά από συντονισμένες κυβερνοεπιθέσεις, οι οποίες δεν περιορίστηκαν σε μεμονωμένα περιστατικά αλλά εντάχθηκαν σε έναν ευρύτερο σχεδιασμό υβριδικού πολέμου. Ο σχεδιασμός αυτός περιλάμβανε τη χρήση τεχνικών κυβερνοκατασκοπείας για την απόκτηση κρίσιμων πληροφοριών, τη διάδοση παραπληροφόρησης και τη διεξαγωγή ψυχολογικών επιχειρήσεων. Αυτές οι στρατηγικές δεν είχαν μόνο άμεσες επιπτώσεις, αλλά στόχευαν και στη μακροπρόθεσμη αποσταθεροποίηση της πολιτικής και κοινωνικής συνοχής της Πολωνίας (Schmitt, 2017).

Ένα από τα πιο σοβαρά περιστατικά σημειώθηκε το 2016, όταν ρωσικές ομάδες κυβερνοκατασκοπείας απέκτησαν πρόσβαση σε απόρρητες επικοινωνίες του πολωνικού Υπουργείου Εξωτερικών. Αυτή η κυβερνοεπίθεση οδήγησε στη διαρροή ευαίσθητων πληροφοριών, οι οποίες χρησιμοποιήθηκαν για να προκαλέσουν πολιτική κρίση και να ενισχύσουν την αίσθηση ανασφάλειας. Η στρατηγική της Ρωσίας συνδύαζε αυτές τις επιθέσεις με την παραπληροφόρηση, χρησιμοποιώντας πλατφόρμες κοινωνικών μέσων όπως το Facebook και το Twitter για τη διάδοση ψευδών ειδήσεων που στόχευαν στη διχόνοια και τον κοινωνικό διχασμό (Lewis, 2021). Η παραπληροφόρηση, ως μέρος του ευρύτερου σχεδιασμού, εστίασε σε ζητήματα όπως η μεταναστευτική κρίση, η οικονομική πολιτική της Ευρωπαϊκής Ένωσης και η παρουσία στρατιωτικών δυνάμεων του NATO στην περιοχή. Αυτές οι εκστρατείες επηρέασαν την κοινή γνώμη, καλλιεργώντας αντιευρωπαϊκά και εθνικιστικά αισθήματα που αποδυνάμωσαν τη φιλοδυτική στάση της Πολωνίας. Επιπλέον, οι ψυχολογικές επιχειρήσεις υπονόμευσαν την εμπιστοσύνη του πολωνικού λαού προς την κυβέρνηση και τους θεσμούς, ενισχύοντας την αποσταθεροποιητική επιρροή της Ρωσίας (Wągrowska, 2020). Αυτό που καθιστά την περίπτωση της Πολωνίας ιδιαίτερη είναι η πολυπλοκότητα και η ένταση των κυβερνοεπιθέσεων. Οι επιθέσεις δεν περιορίστηκαν μόνο στις κρατικές δομές αλλά επεκτάθηκαν και στον ιδιωτικό τομέα, συμπεριλαμβανομένων τραπεζικών οργανισμών και κρίσιμων υποδομών, όπως τα ενεργειακά δίκτυα. Αυτές οι ενέργειες είχαν ως αποτέλεσμα την πρόκληση οικονομικών ζημιών και τη μείωση της εμπιστοσύνης προς τη διακυβέρνηση, αποδεικνύοντας τον μακροπρόθεσμο σχεδιασμό της Ρωσίας να αποδυναμώσει τη θέση της Πολωνίας στην Ευρωπαϊκή Ένωση και το NATO.

## Η Αντίδραση της Πολωνίας και οι Θεσμικές Πρωτοβουλίες

Η Πολωνία αντέδρασε στις κυβερνοεπιθέσεις με μια στρατηγική που συνδύαζε εθνικές πρωτοβουλίες και διεθνή συνεργασία. Το 2019, υιοθέτησε την Εθνική Στρατηγική Κυβερνοασφάλειας, η οποία έθεσε ως κύριες προτεραιότητες την προστασία κρίσιμων υποδομών, τη βελτίωση της τεχνολογικής υποδομής και την ενίσχυση της συνεργασίας με διεθνείς οργανισμούς. Αυτή η στρατηγική διαμορφώθηκε μέσα από τη στενή συνεργασία με το Εθνικό Κέντρο Ασφάλειας Πληροφοριών (NASK), το οποίο ανέλαβε την παρακολούθηση και πρόληψη κυβερνοεπιθέσεων, την εκπαίδευση εξειδικευμένου προσωπικού και τη διαχείριση κρίσεων (Schmitt, 2017). Μία από τις σημαντικές δράσεις της Πολωνίας ήταν η δημιουργία ενός πολυεπίπεδου συστήματος κυβερνοάμυνας. Αυτό περιλάμβανε την ανάπτυξη εφεδρικών συστημάτων, την ενίσχυση των δικτύων επικοινωνίας και την προστασία των ενεργειακών και τραπεζικών υποδομών, οι οποίες είχαν γίνει στόχοι προηγούμενων κυβερνοεπιθέσεων. Οι επενδύσεις αυτές διασφάλισαν τη διαλειτουργικότητα των κρίσιμων υποδομών, ακόμα και σε περιόδους κρίσης (Wągrowska, 2020).

Η Πολωνία επένδυσε σημαντικά και στην εκπαίδευση του ανθρώπινου δυναμικού, προωθώντας εκπαιδευτικά προγράμματα σε πανεπιστήμια και οργανισμούς κατάρτισης. Τα προγράμματα αυτά στόχευαν στην ενίσχυση των δεξιοτήτων κυβερνοασφάλειας, ενώ παράλληλα οργανώθηκαν εθνικές εκστρατείες ευαισθητοποίησης για τους πολίτες, ώστε να μειωθεί η ευπάθεια της κοινωνίας σε επιθέσεις παραπληροφόρησης. Αυτή η προσέγγιση δημιούργησε ένα κλίμα εμπιστοσύνης και ενίσχυσε τη γενική ανθεκτικότητα της κοινωνίας απέναντι στις κυβερνοαπειλές (Grzegorzewski, 2019). Επιπλέον, η Πολωνία υιοθέτησε νέες νομοθετικές πρωτοβουλίες για την ενίσχυση της κυβερνοασφάλειας. Ένας από τους στόχους ήταν η καθιέρωση αυστηρών κανονισμών για την προστασία δεδομένων και η ενίσχυση των μηχανισμών διαχείρισης κρίσεων. Παράλληλα, θεσπίστηκαν μηχανισμοί άμεσης ανταπόκρισης σε κυβερνοαπειλές, ενισχύοντας τη συνεργασία μεταξύ κρατικών υπηρεσιών και ιδιωτικών φορέων. Η διεθνής συνεργασία αποτέλεσε επίσης βασικό πυλώνα της στρατηγικής αντίδρασης της Πολωνίας. Μέσα από τη συμμετοχή της σε κοινές ασκήσεις κυβερνοάμυνας με το NATO, όπως οι Locked Shields, και μέσω διμερών συμφωνιών με κράτη-μέλη της Ευρωπαϊκής Ένωσης, η Πολωνία ενίσχυσε την τεχνογνωσία της και βελτίωσε την ικανότητά της να ανταποκρίνεται σε διακρατικές απειλές. Αυτή η συνεργασία προσέφερε επίσης πρόσβαση σε καινοτόμες τεχνολογίες και εργαλεία κυβερνοασφάλειας, συμβάλλοντας στη συνολική ασφάλεια της χώρας (NATO CCDCOE, 2021). Η περίπτωση της Πολωνίας αποδεικνύει ότι η ολοκληρωμένη αντίδραση στις κυβερνοεπιθέσεις δεν περιορίζεται μόνο στις τεχνολογικές λύσεις. Η ενίσχυση των θεσμών, η εκπαίδευση του ανθρώπινου δυναμικού και η διεθνής συνεργασία αποτελούν κρίσιμες παραμέτρους για την επιτυχία μιας εθνικής στρατηγικής κυβερνοασφάλειας.

## Συνεργασία με το NATO και Ενίσχυση της Συλλογικής Ασφάλειας

Η συνεργασία της Πολωνίας με το NATO υπήρξε καθοριστική για την ενίσχυση των δυνατοτήτων κυβερνοασφάλειας της χώρας. Μέσα από κοινές ασκήσεις, όπως οι Locked Shields, η Πολωνία βελτίωσε την επιχειρησιακή της ετοιμότητα και απέκτησε πρόσβαση σε προηγμένα εργαλεία και τεχνογνωσία. Το NATO αναγνώρισε τη στρατηγική σημασία της Πολωνίας ως κομβικού σημείου για την ασφάλεια της ανατολικής Ευρώπης, παρέχοντας συνεχή υποστήριξη μέσω ομάδων κυβερνοασφάλειας και στρατιωτικής συνεργασίας (NATO CCDCOE, 2021). Η γεωπολιτική θέση της Πολωνίας ενίσχυσε τη σημασία της ως βασικού εταίρου στην αντιμετώπιση υβριδικών απειλών. Η χώρα διαδραμάτισε κεντρικό ρόλο στη διαμόρφωση πολιτικών κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση, συμβάλλοντας στη δημιουργία κοινού πλαισίου για την αντιμετώπιση κυβερνοαπειλών σε ευρωπαϊκό επίπεδο (Kowalski, 2018).

Η Πολωνία χρησιμοποίησε τις εμπειρίες της από τις κυβερνοεπιθέσεις για να ενισχύσει την ανθεκτικότητά της και να βελτιώσει τη στρατηγική της κυβερνοασφάλειας. Οι επιθέσεις, όπως αυτές που σημειώθηκαν το 2016 και στόχευσαν κρίσιμες υποδομές και κυβερνητικές επικοινωνίες, ανέδειξαν την ανάγκη για αναβαθμισμένα μέτρα κυβερνοάμυνας (Grzegorzewski, 2019). Παρότι οι κυβερνοεπιθέσεις δεν υπήρξαν ο αποκλειστικός λόγος για την υιοθέτηση μιας ισχυρής στρατηγικής ασφάλειας, λειτούργησαν ως επιταχυντές για την ενίσχυση των εθνικών δυνατοτήτων και της διεθνούς συνεργασίας (Wągrowska, 2020).

Η Πολωνία εστίασε ιδιαίτερα στη συνεργασία με διεθνείς οργανισμούς, όπως το NATO και η Ευρωπαϊκή Ένωση, προκειμένου να αποκτήσει πρόσβαση σε προηγμένες τεχνογνωσίες και εργαλεία κυβερνοάμυνας (NATO CCDCOE, 2021). Παράλληλα, οι συμμετοχές της σε κοινές ασκήσεις, όπως το *Locked Shields*, της επέτρεψαν να αναπτύξει εξειδικευμένες ικανότητες διαχείρισης κυβερνοαπειλών μεγάλης κλίμακας (Schmitt, 2017).

Η περίπτωση της Πολωνίας καταδεικνύει τη σημασία της συλλογικής άμυνας και της πολυμερούς συνεργασίας για την αντιμετώπιση των σύγχρονων υβριδικών απειλών. Η εμπειρία της χώρας υπογραμμίζει ότι η αποτελεσματική κυβερνοάμυνα δεν είναι μόνο τεχνολογικό ζήτημα αλλά και πολιτικό, με την οικοδόμηση ανθεκτικών δομών να εξαρτάται από τη στενή συνεργασία μεταξύ εθνικών φορέων και διεθνών συμμάχων (Giles, 2016).

# Κεφάλαιο 4: Ανάλυση και Σύγκριση των Μελετών

Η ανάλυση και σύγκριση των μελετών περίπτωσης είναι κρίσιμη για την εξαγωγή συμπερασμάτων σχετικά με τη στρατηγική των ρωσικών κυβερνοεπιθέσεων και τη συνολική τους επίδραση. Στο παρόν κεφάλαιο, εξετάζονται τα κοινά στοιχεία και οι διαφορές στις κυβερνοεπιθέσεις που δέχθηκαν η Εσθονία, η Ουκρανία και η Πολωνία, προσφέροντας μια ολοκληρωμένη εικόνα της ρωσικής στρατηγικής και των αποτελεσμάτων της. Η σύγκριση επικεντρώνεται σε τρεις κύριες πτυχές: Τα κοινά χαρακτηριστικά των επιθέσεων, όπως οι στόχοι και οι τακτικές. Οι διαφοροποιήσεις στην εφαρμογή της ρωσικής στρατηγικής, ανάλογα με τη γεωπολιτική θέση και τις δυνατότητες των κρατών-στόχων.Οι αντιδράσεις των κρατών-δειγμάτων και ο ρόλος της διεθνούς συνεργασίας, με ιδιαίτερη έμφαση στη συνεισφορά του NATO. Σκοπός αυτού του κεφαλαίου είναι να αναδείξει πώς οι ρωσικές κυβερνοεπιθέσεις χρησιμοποιούνται ως εργαλείο υβριδικού πολέμου για την αποδυνάμωση των κρατών και τη γεωπολιτική ανακατανομή ισχύος. Παράλληλα, εξετάζεται η αποτελεσματικότητα των απαντήσεων των κρατών-δειγμάτων και η ενίσχυση της ανθεκτικότητάς τους μέσω θεσμικών και διεθνών πρωτοβουλιών. Η σύγκριση αυτή συμβάλλει στην κατανόηση του τρόπου με τον οποίο οι κυβερνοεπιθέσεις διαμορφώνουν τη σύγχρονη γεωπολιτική και παρέχει τη βάση για τη διατύπωση συμπερασμάτων και προτάσεων για μελλοντική στρατηγική και πολιτική.

## 4.1 Κοινά Στοιχεία στις Μελέτες Περίπτωσης

Οι μελέτες περίπτωσης της Εσθονίας, της Ουκρανίας και της Πολωνίας αναδεικνύουν τις ομοιότητες στη στρατηγική των ρωσικών κυβερνοεπιθέσεων, παρέχοντας μια συνολική εικόνα των κοινών μοτίβων που χαρακτηρίζουν την εφαρμογή της. Οι επιθέσεις αυτές λειτουργούν ως κεντρικός άξονας ενός ευρύτερου υβριδικού πολέμου, σχεδιασμένου να αποσταθεροποιήσει κράτη-στόχους και να προωθήσει γεωπολιτικούς στόχους της Ρωσίας. Ένας από τους κύριους στόχους των ρωσικών κυβερνοεπιθέσεων είναι η διατάραξη κρίσιμων υποδομών και κυβερνητικών λειτουργιών. Στην Εσθονία (2007), οι επιθέσεις DDoS παρέλυσαν κυβερνητικούς ιστότοπους και τραπεζικές υπηρεσίες, αποκαλύπτοντας την ευπάθεια ακόμα και των πιο ψηφιοποιημένων κρατών (Ottis, 2008). Στην Ουκρανία, οι επιθέσεις BlackEnergy (2015) και NotPetya (2017) στόχευσαν συστήματα ενέργειας και επικοινωνιών, προκαλώντας εκτεταμένες διακοπές λειτουργίας που επηρέασαν την καθημερινή ζωή και την οικονομία (Schmitt, 2017). Αντίστοιχα, στην Πολωνία, οι παραβιάσεις κυβερνητικών συστημάτων και η υποκλοπή επικοινωνιών το 2016 υπονόμευσαν την πολιτική σταθερότητα και την εμπιστοσύνη στους θεσμούς . Η εστίαση στις κρίσιμες υποδομές δεν είναι τυχαία. Η πρόκληση ζημιών σε τομείς όπως η ενέργεια, οι επικοινωνίες και οι τραπεζικές υπηρεσίες υπονομεύει τη συνολική λειτουργία του κράτους, ενισχύοντας την πολιτική και κοινωνική αποσταθεροποίηση (Conley et al., 2016).

Οι κυβερνοεπιθέσεις δεν λειτουργούν απομονωμένα αλλά συνδυάζονται με εκστρατείες παραπληροφόρησης. Στην Ουκρανία, η παραπληροφόρηση ενίσχυσε την αίσθηση χάους, διασπείροντας ψευδείς ειδήσεις για τις ικανότητες της κυβέρνησης να προστατεύσει τους πολίτες της . Στην Πολωνία, οι εκστρατείες μέσω κοινωνικών δικτύων, όπως το Facebook και το Twitter, έθεσαν στο στόχαστρο την εμπιστοσύνη των πολιτών στην Ευρωπαϊκή Ένωση, υποδαυλίζοντας αντιευρωπαϊκές και εθνικιστικές αφηγήσεις. Η συνδυαστική χρήση κυβερνοεπιθέσεων και παραπληροφόρησης αυξάνει τον αντίκτυπο, δημιουργώντας ένα πολύπλευρο πλαίσιο αποσταθεροποίησης που είναι δύσκολο να αντιμετωπιστεί αποτελεσματικά (Schmitt, 2017). Για την Εσθονία, οι κυβερνοεπιθέσεις συνοδεύτηκαν επίσης από εκστρατείες παραπληροφόρησης που στόχευαν στη δημιουργία διχασμών και σύγχυσης στον πληθυσμό. Μετά τις επιθέσεις DDoS το 2007, διαδόθηκαν ψευδείς αφηγήσεις που αποσκοπούσαν στην ενίσχυση της

δυσπιστίας των πολιτών προς τους κυβερνητικούς θεσμούς, υπονομεύοντας την πολιτική συνοχή της χώρας. Μέσω των μέσων κοινωνικής δικτύωσης και κρατικά ελεγχόμενων μέσων, η Ρωσία επιδίωξε να παρουσιάσει την Εσθονία ως ένα εύθραυστο κράτος που δεν μπορούσε να προστατεύσει τις κρίσιμες υποδομές της (Tikk, Kaska και Vihul, 2010). Η συνδυαστική χρήση κυβερνοεπιθέσεων και παραπληροφόρησης στην Εσθονία αποτέλεσε πρωτοποριακό παράδειγμα υβριδικού πολέμου, επηρεάζοντας την αντίληψη της χώρας για την ανάγκη ενίσχυσης της κυβερνοασφάλειας και διεθνούς συνεργασίας.

Η Ρωσία εκμεταλλεύεται την ασυμμετρία και την ανωνυμία του κυβερνοχώρου για να πλήξει τους στόχους της χωρίς να προκαλεί άμεση στρατιωτική αντίδραση. Οι επιθέσεις DDoS στην Εσθονία και οι παραβιάσεις στην Πολωνία δείχνουν πώς η Ρωσία μπορεί να ενεργεί με σχετική ατιμωρησία, χρησιμοποιώντας μη κρατικούς δρώντες και παραστρατιωτικές ομάδες όπως οι APT28 (Fancy Bear). Αυτή η στρατηγική μειώνει την πιθανότητα διπλωματικών κυρώσεων ή στρατιωτικής αντίδρασης, ενώ παράλληλα μεγιστοποιεί την αποσταθεροποιητική ισχύ των επιθέσεων (Conley et al., 2016; Schmitt, 2017).

Η χρήση μη κρατικών δρώντων, σε συνδυασμό με την ανωνυμία του κυβερνοχώρου, επιτρέπει στη Ρωσία να αρνείται οποιαδήποτε ευθύνη, ενισχύοντας τη στρατηγική αμφισημία. Στην Εσθονία, η έλλειψη ξεκάθαρων αποδείξεων για κρατική ευθύνη της Ρωσίας περιόρισε την άμεση διεθνή αντίδραση, παρά τη μεγάλη κλίμακα των επιθέσεων (Ottis, 2008). Η στρατηγική της Ρωσίας αποδεικνύει ότι οι κυβερνοεπιθέσεις αποτελούν όχι μόνο τεχνικό μέσο αποσταθεροποίησης αλλά και εργαλείο γεωπολιτικής επιρροής. Οι κοινές τακτικές που εφαρμόστηκαν στις χώρες-δείγματα αναδεικνύουν τη συνέπεια της ρωσικής στρατηγικής, η οποία προσαρμόζεται στις ανάγκες και τις αδυναμίες κάθε κράτους-στόχου (Schmitt, 2017; NATO, 2023).

## 4.2 Διαφορές και Ιδιαίτερες Περιστάσεις

Παρά τα κοινά χαρακτηριστικά που παρατηρούνται στις μελέτες περίπτωσης, υπάρχουν σαφείς διαφορές στον τρόπο με τον οποίο οι κυβερνοεπιθέσεις επηρέασαν την Εσθονία, την Ουκρανία και την Πολωνία. Αυτές οι διαφορές αντανακλούν τη γεωπολιτική θέση, την πολιτική και κοινωνική δομή κάθε κράτους, καθώς και τη στρατηγική προσαρμοστικότητα της Ρωσίας.

Η Εσθονία αντιμετώπισε την πρώτη μεγάλης κλίμακας κυβερνοεπίθεση το 2007, η οποία αποτέλεσε σημείο καμπής για την κατανόηση των κυβερνοαπειλών. Ωστόσο, σε αντίθεση με άλλες χώρες, η Εσθονία χρησιμοποίησε την εμπειρία αυτή για να εδραιωθεί ως πρότυπο κυβερνοασφάλειας. Οι επιθέσεις ενίσχυσαν τη συνεργασία της με το NATO, οδηγώντας στην ίδρυση του CCDCOE, ενώ η καινοτομία των data embassies κατέδειξε τη μακροπρόθεσμη δέσμευση της χώρας στην προστασία των κρίσιμων δεδομένων της (Ottis, 2008; Schmitt, 2017). Κατά την περίοδο 2010-2020, η Εσθονία συνέχισε να αποτελεί στόχο κυβερνοεπιθέσεων, αν και καμία από αυτές δεν είχε την ίδια έκταση και αντίκτυπο με τις επιθέσεις του 2007. Οι μετέπειτα επιθέσεις στόχευσαν κυρίως κυβερνητικές υπηρεσίες και υποδομές, με χαρακτηριστικά περιστατικά να περιλαμβάνουν παραβιάσεις δεδομένων και εκστρατείες παραπληροφόρησης. Αυτές οι επιθέσεις ενίσχυσαν περαιτέρω την αποφασιστικότητα της χώρας να επενδύσει στην κυβερνοασφάλεια και να ενισχύσει τη διεθνή συνεργασία μέσω του NATO και της Ευρωπαϊκής Ένωσης (Giles, 2016; Tikk et al., 2010).

Η εστίαση της Εσθονίας στην εκπαίδευση, τη διακυβέρνηση και την καινοτομία, σε συνδυασμό με τη συνεργασία με διεθνείς εταίρους, λειτούργησε ως ασπίδα απέναντι στις συνεχιζόμενες απειλές. Επιπλέον, τα μαθήματα που αποκόμισε από τις αρχικές επιθέσεις της επέτρεψαν να προσαρμόσει τη στρατηγική της, καθιστώντας την έναν από τους πιο ανθεκτικούς και πρωτοπόρους παίκτες στην παγκόσμια κυβερνοασφάλεια.

Η Ουκρανία αποτέλεσε πεδίο εντατικών και συνδυασμένων κυβερνοεπιθέσεων που στόχευαν όχι μόνο κρίσιμες υποδομές αλλά και την κοινωνική συνοχή της χώρας. Οι επιθέσεις BlackEnergy (2015) και NotPetya (2017) εντάχθηκαν σε ένα ευρύτερο πλαίσιο ένοπλων συγκρούσεων και πολιτικής αποσταθεροποίησης. Σε αντίθεση με την Εσθονία, η Ουκρανία αντιμετώπισε τις κυβερνοεπιθέσεις ως μέρος μιας γενικότερης στρατιωτικής και πολιτικής απειλής, γεγονός που επηρέασε δραστικά τη δυνατότητα αποτελεσματικής αντίδρασης (Giles, 2016; NATO, 2023).

Η Πολωνία, ως μέλος του NATO, είχε μια διαφορετική εμπειρία. Οι κυβερνοεπιθέσεις στόχευσαν κυρίως στην υπονόμευση της συνεργασίας με την Ευρωπαϊκή Ένωση και στη διατάραξη της κοινωνικής συνοχής μέσω εκστρατειών παραπληροφόρησης. Ωστόσο, η θεσμική ωριμότητα και η στρατηγική συνεργασία με το NATO επέτρεψαν στην Πολωνία να αναπτύξει αποτελεσματικούς μηχανισμούς κυβερνοάμυνας. Η υιοθέτηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας το 2019 ενίσχυσε τη θωράκιση των κρίσιμων υποδομών της χώρας και την ετοιμότητά της για μελλοντικές απειλές (Lewis, 2021; CCDCOE, 2021).

Οι διαφορές στις αντιδράσεις και τις επιπτώσεις των κυβερνοεπιθέσεων στις τρεις χώρες αντικατοπτρίζουν τη σημασία της προσαρμογής της στρατηγικής κάθε κράτους στις ιδιαίτερες συνθήκες του. Η Εσθονία επένδυσε σε καινοτομία και διεθνή συνεργασία, η Ουκρανία βρέθηκε να αντιμετωπίζει έναν πολυδιάστατο πόλεμο, ενώ η Πολωνία ενίσχυσε τη θεσμική της ανθεκτικότητα, καθιστώντας την έναν από τους πιο προετοιμασμένους συμμάχους του NATO στον κυβερνοχώρο. Οι κυβερνοεπιθέσεις δεν λειτουργούν με τον ίδιο τρόπο σε όλα τα κράτη. Οι διαφορετικές επιπτώσεις και αντιδράσεις αντανακλούν τις προϋπάρχουσες στρατηγικές και την ετοιμότητα κάθε χώρας. Αυτό το εύρημα ενισχύει την κεντρική υπόθεση της εργασίας: οι κυβερνοεπιθέσεις λειτουργούν συχνά ως επιταχυντές προϋπαρχουσών στρατηγικών, αντί ως καταλύτες ριζικών αλλαγών.

## 4.3 Συνολική Αξιολόγηση

Η ανάλυση των μελετών περίπτωσης της Εσθονίας, της Ουκρανίας και της Πολωνίας αποκαλύπτει τις διαφορετικές διαστάσεις των ρωσικών κυβερνοεπιθέσεων, καθώς και τη στρατηγική τους σημασία στο πλαίσιο του υβριδικού πολέμου. Παρόλο που οι χώρες-δείγματα παρουσίασαν ποικίλες αντιδράσεις και επιπτώσεις, η χρήση του κυβερνοχώρου από τη Ρωσία αποδεικνύεται συνεπής και πολυδιάστατη.

Οι κυβερνοεπιθέσεις που στοχεύουν κρίσιμες υποδομές προκαλούν χάος και διαταράσσουν την κανονικότητα. Στην Εσθονία, οι επιθέσεις DDoS παρέλυσαν τις κυβερνητικές υπηρεσίες, αποκαλύπτοντας την ευπάθεια των ψηφιοποιημένων συστημάτων. Στην Ουκρανία, οι επιθέσεις BlackEnergy και NotPetya έδειξαν πώς ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί για τη διάλυση των βασικών λειτουργιών ενός κράτους. Η σύνδεση κυβερνοεπιθέσεων με εκστρατείες παραπληροφόρησης αποδείχθηκε αποτελεσματική τακτική. Στην Πολωνία, οι εκστρατείες μέσω κοινωνικών δικτύων ενίσχυσαν τον κοινωνικό διχασμό και αποδυνάμωσαν τη δημόσια υποστήριξη προς την Ευρωπαϊκή Ένωση και το NATO (Giles, 2016). Οι

κυβερνοεπιθέσεις παρέχουν στη Ρωσία τη δυνατότητα να επιτίθεται χωρίς να προκαλεί άμεση στρατιωτική αντίδραση, εκμεταλλευόμενη την αδυναμία ταυτοποίησης του δράστη. Οι μη κρατικοί δρώντες, όπως οι APT28, λειτουργούν ως προεκτάσεις του κράτους, ενισχύοντας τη στρατηγική αμφισημία (Conley et al., 2016).

Η διεθνής συνεργασία διαδραμάτισε κρίσιμο ρόλο στην ενίσχυση της ανθεκτικότητας των χωρών-δειγμάτων: Στην Εσθονία, η ίδρυση του CCDCOE αποτέλεσε τη βάση για την ενίσχυση της συλλογικής κυβερνοάμυνας, ενώ οι καινοτομίες όπως οι data embassies ανέδειξαν τη δέσμευση της χώρας για προστασία δεδομένων. Η Ουκρανία, παρά την ευπάθειά της, επωφελήθηκε από την ενίσχυση της συνεργασίας με το NATO, η οποία περιλάμβανε εκπαίδευση, τεχνογνωσία και πρόσβαση σε διεθνή δίκτυα κυβερνοάμυνας. Στην Πολωνία, η υιοθέτηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας το 2019 και η ενεργός συμμετοχή της σε ασκήσεις όπως οι Locked Shields ενίσχυσαν τη στρατηγική της ετοιμότητα και τη συνεργασία με τους συμμάχους της (CCDCOE, 2021). Οι κυβερνοεπιθέσεις όπως το BlackEnergy (2015) και το NotPetya (2017) επιτάχυναν τη διαδικασία στρατηγικής εναρμόνισης της Ουκρανίας με το NATO. Πριν από αυτές τις επιθέσεις, η Ουκρανία είχε ήδη ξεκινήσει τη συνεργασία με τη Συμμαχία λόγω της προσάρτησης της Κριμαίας (2014) και της σύγκρουσης στο Ντονμπάς. Οι κυβερνοεπιθέσεις κατέδειξαν τις αδυναμίες της Ουκρανίας στην κυβερνοάμυνα, ενισχύοντας την ανάγκη για θεσμικές μεταρρυθμίσεις και αυξημένη διεθνή συνεργασία (Zetter, 2017; Greenberg, 2018; NATO CCDCOE, 2023).

Παρότι οι κυβερνοεπιθέσεις είχαν σημαντικές επιπτώσεις, δεν αποτέλεσαν τον μοναδικό ή κύριο λόγο για τη στρατηγική στροφή των χωρών-δειγμάτων. Στην Εσθονία, η εμπειρία του 2007 λειτουργεί ως καταλύτης για τη μετατροπή της σε παγκόσμιο ηγέτη στην κυβερνοασφάλεια, αλλά η στρατηγική της βασίστηκε επίσης στην πρωτοβουλία και την καινοτομία. Η Ουκρανία βίωσε τις κυβερνοεπιθέσεις ως μέρος ενός γενικότερου πολέμου, όπου ο στρατιωτικός παράγοντας υπερείχε. Οι κυβερνοεπιθέσεις επιτάχυναν τη στρατηγική συνεργασία της με το NATO, αλλά η γενικευμένη εισβολή το 2022 άλλαξε δραματικά τις προτεραιότητες της χώρας. Στην Πολωνία, οι κυβερνοεπιθέσεις λειτούργησαν ως ενισχυτικός μηχανισμός για μια ήδη καθιερωμένη στρατηγική συνεργασία με το NATO και την Ευρωπαϊκή Ένωση.

Η ανάλυση των τριών χωρών δείχνει ότι οι ρωσικές κυβερνοεπιθέσεις δεν είναι τυχαίες ή αποσπασματικές ενέργειες, αλλά εντάσσονται σε ένα ευρύτερο στρατηγικό σχέδιο. Παρουσιάζουν σημαντική προσαρμοστικότητα ανά περίπτωση. Στόχοι όπως η Εσθονία, με έντονη ψηφιοποίηση, αντιμετώπισαν επιθέσεις που στόχευαν τις τεχνολογικές υποδομές τους. Αντίθετα, η Ουκρανία βίωσε πιο σύνθετες επιθέσεις, ενταγμένες σε ένα πολυδιάστατο υβριδικό πόλεμο. Στην Πολωνία, η Ρωσία εστίασε στις πληροφοριακές επιχειρήσεις και την υπονόμευση της πολιτικής συνοχής. Αυτή η διαφοροποίηση υπογραμμίζει τη στρατηγική χρήση του κυβερνοχώρου, καθιστώντας τις επιθέσεις μέρος ενός ευρύτερου γεωπολιτικού σχεδιασμού. Ο κυβερνοχώρος χρησιμοποιείται ως εργαλείο γεωπολιτικής πίεσης, αποδεικνύοντας την αναγκαιότητα για ισχυρές διεθνείς συνεργασίες. Η χρήση του κυβερνοχώρου από τη Ρωσία έχει εξελιχθεί σε έναν κρίσιμο παράγοντα στις σύγχρονες συγκρούσεις, υπογραμμίζοντας τη στρατηγική σημασία της κυβερνοασφάλειας στο διεθνές σύστημα.

# Κεφάλαιο 5: Συνολική Αξιολόγηση και Συμπεράσματα

Το παρόν κεφάλαιο αποσκοπεί στη συνολική αξιολόγηση των ευρημάτων της έρευνας και στη διατύπωση των τελικών συμπερασμάτων. Στο πλαίσιο αυτό, εξετάζεται η υπόθεση εργασίας: **Κατά πόσο οι ρωσικές κυβερνοεπιθέσεις αποτελούν καθοριστικό παράγοντα αλλαγής στη στρατηγική των κρατών-στόχων και πώς αυτές επηρεάζουν τη σχέση τους με το ΝΑΤΟ;**

Η ανάλυση των μελετών περίπτωσης (Εσθονία, Ουκρανία, Πολωνία) ανέδειξε ότι οι ρωσικές κυβερνοεπιθέσεις δεν αποτελούν από μόνες τους τον αποκλειστικό και καθοριστικό παράγοντα στρατηγικών αλλαγών. Αντίθετα, λειτουργούν κυρίως ως **επιταχυντές προϋπαρχουσών στρατηγικών κατευθύνσεων**, ενισχύοντας την αντίδραση των κρατών-στόχων και την αναζήτηση μεγαλύτερης ασφάλειας μέσω της διεθνούς συνεργασίας. Συγκεκριμένα, οι κυβερνοεπιθέσεις που δέχθηκαν η Εσθονία και η Πολωνία ενίσχυσαν τη συνεργασία τους με το ΝΑΤΟ, αλλά δεν προκάλεσαν ριζικές αλλαγές στη στρατηγική τους, καθώς ήδη είχαν προσανατολιστεί προς τη Συμμαχία. Στην περίπτωση της Ουκρανίας, οι κυβερνοεπιθέσεις επιτάχυναν τη διαδικασία προσέγγισης με τη Δύση, αλλά δεν αποτέλεσαν τον βασικό λόγο αλλαγής στρατηγικής – αυτή είχε ήδη τεθεί σε εφαρμογή λόγω της ρωσικής στρατιωτικής απειλής.

Ως εκ τούτου, η έρευνα καταλήγει στο συμπέρασμα ότι οι ρωσικές κυβερνοεπιθέσεις ενισχύουν τη στρατηγική των κρατών-στόχων να βελτιώσουν την κυβερνοασφάλειά τους και να ενισχύσουν τη συνεργασία τους με το ΝΑΤΟ, αλλά δεν ανατρέπουν ριζικά τις υφιστάμενες στρατηγικές επιλογές τους.

## 5.1 Κύρια Ευρήματα της Έρευνας

Η ανάλυση των μελετών περίπτωσης και των στρατηγικών πλαισίων που εξετάστηκαν στην παρούσα εργασία ανέδειξε σημαντικά ευρήματα σχετικά με τη στρατηγική χρήση των κυβερνοεπιθέσεων από τη Ρωσία και τη συμβολή τους στις διεθνείς γεωπολιτικές εξελίξεις. Η Ρωσία έχει ενσωματώσει τις κυβερνοεπιθέσεις ως βασικό πυλώνα της στρατηγικής του υβριδικού πολέμου. Οι επιθέσεις κατά της Εσθονίας το 2007, αν και πρωτόγονες σε σχέση με τις μεταγενέστερες, κατέδειξαν τη δυνατότητα του κυβερνοχώρου να παραλύσει κρίσιμες λειτουργίες ενός κράτους. Στην Ουκρανία, οι επιθέσεις NotPetya (2017) και BlackEnergy (2015) στόχευσαν κρίσιμες υποδομές, δημιουργώντας χάος και αποδυναμώνοντας την ικανότητα του κράτους να διαχειριστεί εσωτερικές και εξωτερικές κρίσεις. Η στρατηγική της Ρωσίας δεν περιορίζεται στη φυσική καταστροφή των υποδομών αλλά επεκτείνεται στην πολιτική και κοινωνική αποσταθεροποίηση, γεγονός που επιβεβαιώθηκε και στην Πολωνία με εκστρατείες παραπληροφόρησης (Giles, 2016; NATO, 2023).

Κάθε χώρα-δείγμα επηρεάστηκε με διαφορετικούς τρόπους, ανάλογα με τις εγχώριες συνθήκες και τη γεωπολιτική της θέση.Στην Εσθονία, οι κυβερνοεπιθέσεις στόχευσαν την ψηφιακή υποδομή ενός από τα πιο τεχνολογικά ανεπτυγμένα κράτη. Ωστόσο, η χώρα αντέδρασε αποτελεσματικά, μετατρέποντας την απειλή σε ευκαιρία, μέσω της ίδρυσης του CCDCOE και της ανάπτυξης καινοτομιών όπως τα data embassies. Στην Ουκρανία, οι κυβερνοεπιθέσεις εντάχθηκαν σε ένα γενικότερο πλαίσιο ένοπλης σύγκρουσης. Η στρατηγική της Ρωσίας εστίασε στην αποσταθεροποίηση μέσω ταυτόχρονων επιθέσεων στον κυβερνοχώρο και στο στρατιωτικό πεδίο, γεγονός που δημιούργησε μια πολυεπίπεδη κρίση για τη χώρα. Στην Πολωνία, η Ρωσία χρησιμοποίησε εκστρατείες παραπληροφόρησης και κυβερνοκατασκοπείας για να πλήξει τη συνεργασία της χώρας με το ΝΑΤΟ και την Ευρωπαϊκή Ένωση. Οι προσπάθειες αυτές

στόχευαν περισσότερο τη δημιουργία κοινωνικού διχασμού παρά την άμεση αποσταθεροποίηση των υποδομών (Lewis, 2021).

Ο κυβερνοχώρος παρέχει στη Ρωσία έναν χώρο δράσης που είναι εξαιρετικά δύσκολο να ελεγχθεί, λόγω της ανωνυμίας και της ασυμμετρίας που τον χαρακτηρίζουν. Οι ομάδες APT28 (Fancy Bear) και APT29 (Cozy Bear) έχουν αποδείξει την ικανότητα της Ρωσίας να χρησιμοποιεί μη κρατικούς δρώντες, διευκολύνοντας την άρνηση εμπλοκής σε κυβερνοεπιθέσεις μεγάλης κλίμακας. Η έλλειψη σαφών διεθνών κανονισμών για την αντιμετώπιση των κυβερνοεπιθέσεων καθιστά δύσκολη τη λογοδοσία και επιτρέπει στη Ρωσία να διατηρεί ένα στρατηγικό πλεονέκτημα στον κυβερνοχώρο (Schmitt, 2017).

Η διεθνής συνεργασία αποτέλεσε βασικό εργαλείο για την ενίσχυση της κυβερνοασφάλειας στις χώρες-δείγματα: Η Εσθονία αξιοποίησε την εμπειρία της από τις κυβερνοεπιθέσεις για να δημιουργήσει ένα ισχυρό θεσμικό πλαίσιο, το οποίο αναγνωρίστηκε διεθνώς. Η συνεργασία της με το ΝΑΤΟ κατέστησε τη χώρα σημείο αναφοράς για την κυβερνοάμυνα. Η Ουκρανία επωφελήθηκε από τη διεθνή βοήθεια, ιδιαίτερα μετά την προσάρτηση της Κριμαίας. Η στρατηγική υποστήριξη του ΝΑΤΟ συνέβαλε στην ενίσχυση των κυβερνοδυνατοτήτων της. Η Πολωνία επένδυσε στη θεσμική και στρατιωτική συνεργασία, θωρακίζοντας τις κρίσιμες υποδομές της και αναπτύσσοντας αποτελεσματικούς μηχανισμούς κυβερνοάμυνας (CCDCOE, 2021).

Επειδή οι κυβερνοεπιθέσεις δεν υπήρξαν ο μοναδικός καθοριστικός παράγοντας για τη στρατηγική στροφή των χωρών, λειτούργησαν ως επιταχυντές. Στην Εσθονία και την Πολωνία, οι επιθέσεις ενίσχυσαν τη συνεργασία με το ΝΑΤΟ και την Ευρωπαϊκή Ένωση. Στην Ουκρανία, αποτέλεσαν σημαντικό παράγοντα πίεσης για την εξασφάλιση διεθνούς υποστήριξης.Τα ευρήματα καταδεικνύουν τη σημασία της στρατηγικής προσαρμογής και της διεθνούς συνεργασίας στην αντιμετώπιση των κυβερνοεπιθέσεων. Η Ρωσία χρησιμοποιεί τον κυβερνοχώρο ως μέσο πολλαπλασιαστικής πίεσης, γεγονός που υπογραμμίζει την αναγκαιότητα ισχυρών διεθνών μηχανισμών και συλλογικής ασφάλειας.

## 5.2 Αξιολόγηση της Υπόθεσης Εργασίας

Η υπόθεση εργασίας που τέθηκε προς διερεύνηση είναι η εξής: Κατά πόσο οι ρωσικές κυβερνοεπιθέσεις αποτελούν καθοριστικό παράγοντα αλλαγής στη στρατηγική των κρατών-στόχων και πώς αυτές επηρεάζουν τη σχέση τους με το ΝΑΤΟ; Ωστόσο, μέσα από την ανάλυση προσεγγίστηκε και το ζήτημα του κατά πόσο αυτές οι επιθέσεις λειτουργούν ως καθοριστικός παράγοντας στρατηγικών αλλαγών ή αν απλώς επιταχύνουν ήδη υφιστάμενες στρατηγικές τάσεις.

Η ανάλυση των μελετών περίπτωσης (Εσθονία, Ουκρανία, Πολωνία) ανέδειξε μια πιο σύνθετη εικόνα. Σε όλες τις περιπτώσεις, οι κυβερνοεπιθέσεις δεν αποτέλεσαν την αποκλειστική αιτία για τη διαμόρφωση νέων στρατηγικών κατευθύνσεων. Αντίθετα, λειτούργησαν ως επιταχυντές ήδη υπαρχουσών στρατηγικών τάσεων, αποκαλύπτοντας θεσμικές αδυναμίες και ενισχύοντας τη διεθνή συνεργασία για την ενίσχυση της κυβερνοάμυνας.

Η Εσθονία, για παράδειγμα, αξιοποίησε την εμπειρία της από τις επιθέσεις του 2007 για να ενισχύσει τη θέση της ως ηγέτιδας δύναμης στην κυβερνοασφάλεια, μέσα από θεσμικές και τεχνολογικές καινοτομίες. Η Ουκρανία, υπό την απειλή στρατιωτικής επιθετικότητας, είδε τις κυβερνοεπιθέσεις ως έναν καταλύτη για τη θεσμική της ενίσχυση και τη συνεργασία της με το ΝΑΤΟ. Η Πολωνία, τέλος, ενίσχυσε τη θεσμική της ετοιμότητα και τη συμμετοχή της στη συλλογική άμυνα του ΝΑΤΟ, αξιοποιώντας τις κυβερνοεπιθέσεις ως ευκαιρία για βελτίωση της ανθεκτικότητάς της.

Το τελικό επιχείρημα που προκύπτει είναι ότι οι ρωσικές κυβερνοεπιθέσεις, αν και εντάσσονται σε ευρύτερες στρατηγικές υβριδικού πολέμου, λειτουργούν περισσότερο ως επιταχυντές υπαρχουσών στρατηγικών κατευθύνσεων παρά ως καταλύτες ριζικών αλλαγών. Η επίδρασή τους διαφοροποιείται σημαντικά ανάλογα με τη θεσμική ετοιμότητα, τη γεωπολιτική συγκυρία και τη δυνατότητα διεθνούς συνεργασίας των κρατών-στόχων.

Στην περίπτωση της Εσθονίας, οι κυβερνοεπιθέσεις λειτούργησαν ως επιταχυντικά για την αναμόρφωση της στρατηγικής κυβερνοασφάλειας της χώρας. Οι επιθέσεις DDoS του 2007, που στόχευσαν κρίσιμες υποδομές, αποκάλυψαν την ευπάθεια ενός άκρως ψηφιοποιημένου κράτους. Παρά τη σοβαρότητα της απειλής, η Εσθονία αντέδρασε δυναμικά, εισάγοντας θεσμικές και τεχνολογικές καινοτομίες. Η ίδρυση του CCDCOE και η δημιουργία των data embassies αποτέλεσαν πρωτοποριακές λύσεις που θωράκισαν τη χώρα και ενίσχυσαν τη θέση της στο ΝΑΤΟ. Παρότι οι κυβερνοεπιθέσεις ήταν σημαντικός παράγοντας για τις αλλαγές αυτές, η θεσμική ωριμότητα και η στρατηγική συνεργασία της Εσθονίας έπαιξαν εξίσου καθοριστικό ρόλο. Η Εσθονία χρησιμοποίησε τις απειλές για να αναδειχθεί σε παγκόσμιο ηγέτη στον τομέα της κυβερνοασφάλειας.

Η περίπτωση της Ουκρανίας ήταν διαφορετική, καθώς οι κυβερνοεπιθέσεις εντάχθηκαν σε ένα πλαίσιο πολυδιάστατης σύγκρουσης. Οι επιθέσεις BlackEnergy (2015) και NotPetya (2017) προκάλεσαν εκτεταμένες ζημιές στις υποδομές και την οικονομία της χώρας, ενώ υπονόμευσαν την εμπιστοσύνη των πολιτών στους θεσμούς. Παρόλα αυτά, οι κυβερνοεπιθέσεις δεν αποτέλεσαν τον κύριο παράγοντα αποσταθεροποίησης. Η στρατιωτική απειλή, η απώλεια της Κριμαίας και οι συγκρούσεις στο Ντονμπάς ήταν πιο άμεσες και υπαρξιακές απειλές, που καθόρισαν τη στρατηγική στροφή της χώρας. Ωστόσο, οι κυβερνοεπιθέσεις λειτούργησαν ως πολλαπλασιαστές ισχύος για τις ρωσικές υβριδικές τακτικές, ενισχύοντας το συνολικό αποσταθεροποιητικό αποτέλεσμα.

Η Πολωνία προσφέρει μια τρίτη διάσταση. Ως μέλος του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης, η Πολωνία διέθετε ήδη ισχυρούς μηχανισμούς συνεργασίας και άμυνας. Οι ρωσικές κυβερνοεπιθέσεις στην Πολωνία επικεντρώθηκαν κυρίως σε εκστρατείες παραπληροφόρησης και κυβερνοκατασκοπείας, με στόχο την υπονόμευση της εμπιστοσύνης στους θεσμούς και τη διάσπαση της κοινωνικής συνοχής. Η απάντηση της Πολωνίας στις απειλές αυτές ήταν άμεση και συντονισμένη. Η υιοθέτηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας το 2019 και η ενεργός συμμετοχή της στις ασκήσεις του ΝΑΤΟ ενίσχυσαν την ανθεκτικότητα της χώρας. Ενώ οι κυβερνοεπιθέσεις δεν προκάλεσαν ριζικές αλλαγές στη στρατηγική της Πολωνίας, λειτούργησαν ως επιταχυντής για τη θεσμική ενίσχυση και την εμβάθυνση της διεθνούς συνεργασίας.

Συνολικά, η αξιολόγηση της υπόθεσης δείχνει ότι οι κυβερνοεπιθέσεις δεν είναι από μόνες τους ο αποκλειστικός παράγοντας που αλλάζει τη στρατηγική των κρατών-στόχων. Αντίθετα, λειτουργούν ως επιταχυντές ή ενισχυτικοί μηχανισμοί, που ωθούν τα κράτη να αναλάβουν δράσεις ενίσχυσης της ανθεκτικότητάς τους. Η πραγματική τους επίδραση εξαρτάται από τη γεωπολιτική θέση, τις δυνατότητες αντίδρασης και τη διεθνή συνεργασία κάθε κράτους. Επιπλέον, η χρήση των κυβερνοεπιθέσεων από τη Ρωσία αποδεικνύεται στρατηγικά συνεπής και προσαρμοστική, εστιάζοντας στη μεγιστοποίηση των επιπτώσεων μέσω του συνδυασμού τους με άλλες μορφές υβριδικών απειλών.

## 5.3 Ερμηνεία και Σύνδεση με τη Σύγχρονη Πραγματικότητα

Η στρατηγική χρήση των κυβερνοεπιθέσεων, όπως αναδείχθηκε μέσα από τις μελέτες περίπτωσης, παρέχει σημαντικά διδάγματα για τη σύγχρονη γεωπολιτική και τη διεθνή ασφάλεια. Ο κυβερνοχώρος έχει μετατραπεί σε ένα κεντρικό πεδίο αντιπαράθεσης, όπου οι κυβερνοεπιθέσεις δεν είναι απλώς τεχνικές παραβιάσεις, αλλά μέρος ευρύτερων στρατηγικών υβριδικού πολέμου. Η εμπειρία της Ουκρανίας, ειδικά μετά την εισβολή της Ρωσίας το 2022, επαναβεβαίωσε τη σύνδεση μεταξύ στρατιωτικών και κυβερνοεπιχειρήσεων. Οι συνδυασμένες επιθέσεις στον κυβερνοχώρο και στο φυσικό πεδίο απέδειξαν την ικανότητα της Ρωσίας να χρησιμοποιεί τον κυβερνοχώρο ως πολλαπλασιαστή ισχύος. Παράλληλα, οι κυβερνοεπιθέσεις κατά της Εσθονίας και της Πολωνίας έδειξαν πώς η Ρωσία στοχεύει συστηματικά στη διάβρωση της κοινωνικής συνοχής και στην υπονόμευση της εμπιστοσύνης στους θεσμούς, ακόμη και σε περιόδους μη ένοπλης σύγκρουσης.

Οι παραπάνω παρατηρήσεις αναδεικνύουν τη σημασία της προσαρμοστικότητας των κρατών και της διεθνούς συνεργασίας. Το ΝΑΤΟ έχει αναδειχθεί σε βασικό παράγοντα ενίσχυσης της συλλογικής κυβερνοάμυνας, όπως φαίνεται από τη συμβολή του στις στρατηγικές της Εσθονίας και της Πολωνίας. Ωστόσο, η απουσία δεσμευτικών διεθνών κανόνων για τον κυβερνοχώρο αποτελεί σημαντική αδυναμία, η οποία επιτρέπει τη συνέχιση των κυβερνοεπιθέσεων με σχετική ατιμωρησία. Η εμπειρία των χωρών-δειγμάτων υπογραμμίζει την ανάγκη για συνεχή επένδυση στην κυβερνοασφάλεια, τόσο σε τεχνολογικό όσο και σε θεσμικό επίπεδο. Η Εσθονία έδειξε πώς η καινοτομία και η διεθνής συνεργασία μπορούν να δημιουργήσουν ένα ανθεκτικό σύστημα κυβερνοασφάλειας. Από την άλλη, η Ουκρανία ανέδειξε τη σημασία της άμεσης στρατηγικής υποστήριξης από διεθνείς οργανισμούς σε περιόδους κρίσης. Η Πολωνία έδειξε ότι η θεσμική ωριμότητα και η συνεχής συνεργασία με το ΝΑΤΟ ενισχύουν την ετοιμότητα απέναντι στις κυβερνοαπειλές.

Συνολικά, η ανάλυση επιβεβαιώνει ότι οι κυβερνοεπιθέσεις δεν αποτελούν απλώς ένα τεχνικό ζήτημα, αλλά ένα εργαλείο γεωπολιτικής πίεσης με ευρύτερες επιπτώσεις. Η δημιουργία δεσμευτικών διεθνών συμφωνιών για τον κυβερνοχώρο, η ενίσχυση της συλλογικής άμυνας και η επένδυση σε ανθεκτικές υποδομές αποτελούν κρίσιμες προτεραιότητες για τη διεθνή κοινότητα. Το μέλλον της κυβερνοασφάλειας δεν εξαρτάται μόνο από την τεχνολογία, αλλά και από τη διαρκή δέσμευση των κρατών στη συλλογική δράση και την αποτελεσματική διακυβέρνηση του κυβερνοχώρου.

## 5.4 Συμπεράσματα και Προτάσεις

Η ανάλυση των μελετών περίπτωσης ανέδειξε τη στρατηγική σημασία των κυβερνοεπιθέσεων στη γεωπολιτική στρατηγική της Ρωσίας. Οι κυβερνοεπιθέσεις δεν είναι τυχαίες ή αποσπασματικές ενέργειες, αλλά μέρος ενός συνεκτικού πλαισίου υβριδικού πολέμου. Στην Εσθονία, οι κυβερνοεπιθέσεις του 2007 έδειξαν τη δυνατότητα πρόκλησης εκτεταμένων διαταραχών με ελάχιστο ρίσκο για τον δράστη. Στην Ουκρανία, οι κυβερνοεπιθέσεις ενισχύθηκαν από στρατιωτικές επιχειρήσεις, δημιουργώντας έναν πολυδιάστατο πόλεμο. Στην Πολωνία, οι εκστρατείες παραπληροφόρησης και κυβερνοκατασκοπείας στόχευσαν την κοινωνική συνοχή και τη σχέση της χώρας με την Ευρωπαϊκή Ένωση και το ΝΑΤΟ. Παρόλο που οι κυβερνοεπιθέσεις επηρεάζουν σημαντικά τη στρατηγική και τη λειτουργία των κρατών-στόχων, η αποτελεσματικότητά τους εξαρτάται από το γεωπολιτικό πλαίσιο, τη θεσμική ετοιμότητα και τη διεθνή συνεργασία. Στην Εσθονία, οι επιθέσεις οδήγησαν στη θεσμική ενίσχυση και τη διεθνή αναγνώριση.

Στην Ουκρανία, λειτούργησαν ως πολλαπλασιαστής της στρατιωτικής πίεσης, ενώ στην Πολωνία ενίσχυσαν την ανάγκη για διαρκή επένδυση στην κυβερνοασφάλεια.

## Απάντηση στο Ερευνητικό Ερώτημα

Οι ρωσικές κυβερνοεπιθέσεις, ενώ έχουν τη δυνατότητα να προκαλέσουν σοβαρές διαταραχές, δεν λειτουργούν ως καταλύτες θεμελιωδών αλλαγών στη στρατηγική των κρατών-στόχων. Αντίθετα, λειτουργούν ως επιταχυντές υπαρχουσών στρατηγικών κατευθύνσεων, ενισχύοντας την ανάγκη για διεθνή συνεργασία, τη βελτίωση της θεσμικής ανθεκτικότητας και την ανάπτυξη συστημάτων κυβερνοασφάλειας. Η επίδρασή τους διαφοροποιείται ανάλογα με τις γεωπολιτικές συνθήκες, τη θεσμική ετοιμότητα και τις στρατηγικές προτεραιότητες κάθε κράτους, ενώ ενισχύουν τη θέση του ΝΑΤΟ ως βασικού πυλώνα συλλογικής άμυνας στον κυβερνοχώρο.

## Κατευθύνσεις για Μελλοντική Έρευνα

Η παρούσα έρευνα ανοίγει τον δρόμο για περαιτέρω μελέτες στον τομέα της κυβερνοασφάλειας και του υβριδικού πολέμου. Μια σημαντική κατεύθυνση για μελλοντική έρευνα είναι η ανάλυση της στρατηγικής αποτροπής στον κυβερνοχώρο. Ποια μέτρα μπορούν να αποτρέψουν αποτελεσματικά τις κυβερνοεπιθέσεις και να ενισχύσουν τη συλλογική ασφάλεια; Επίσης, απαιτείται μεγαλύτερη διερεύνηση των επιπτώσεων των κυβερνοεπιθέσεων σε κράτη εκτός Ευρώπης, ώστε να κατανοηθούν οι διαφορετικές γεωπολιτικές συνθήκες. Τέλος, η μελέτη της διαμόρφωσης ενός διεθνούς πλαισίου συνεργασίας για την κυβερνοασφάλεια είναι εξαιρετικά σημαντική. Η έλλειψη δεσμευτικών κανονισμών για τον κυβερνοχώρο ενισχύει την αναγκαιότητα για μια πολυμερή προσέγγιση που θα περιλαμβάνει κρατικούς και μη κρατικούς δρώντες.

# Βιβλιογραφία


CISA (2022). Update: Destructive Malware Targeting Organizations in Ukraine. Ανακτήθηκε από: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

CCDCOE (2021). Locked Shields: Cyber Defence Exercise. Διαθέσιμο στο: https://ccdcoe.org (Πρόσβαση: 28 Δεκεμβρίου 2024).

CCDCOE (2021). Locked Shields: Insights from Poland's Participation in Cyber Defense Exercises. Cooperative Cyber Defence Centre of Excellence.

Conley, H., Mina, J., Stefanov, R., & Vladimirov, M. (2016). The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe. Center for Strategic and International Studies.

Czosseck, C., Ottis, R., & Talihärm, A. (2011). The Role of Cyber Forces in National Security: The Case of Poland. *Journal of Strategic Security, 4*(2), 59-72.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival, 53*(1), 23-40.

Giles, K. (2016). Russia's 'New' Tools for Confronting the West. Chatham House.

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Διαθέσιμο στο: https://www.wired.com/story/notpetya-cyberattack (Πρόσβαση: 20 Ιανουαρίου 2025).

Grzegorzewski, M. (2019). Cybersecurity in Poland: Between NATO and the EU. *Cyber Defense Review, 5*(3), 45-60.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60.

Hladik, M. (2020). Cyber Conflicts: Case Study of Georgia. *Security and Defence Quarterly*.

Janczewski, L., & Colarik, A. M. (2008). Cyber Warfare and Cyber Terrorism. IGI Global.

Kowalski, P. (2018). Hybrid Warfare and Cybersecurity in Central Europe: The Polish Perspective. *Central European Security Journal, 4*(2), 14-27.

Lewis, J. (2021). Cybersecurity and Cyber Warfare: A Theoretical Approach. Taylor & Francis.

NATO (2016). Cyber Defence Pledge. Διαθέσιμο στο: https://www.nato.int (Πρόσβαση: 28 Δεκεμβρίου 2024).

NATO (2023). Countering Hybrid Threats. Διαθέσιμο στο: https://www.nato.int (Πρόσβαση: 28 Δεκεμβρίου 2024).

NATO CCDCOE (2023). Industroyer2 and WhisperGate: New Threats to Critical Infrastructure. Διαθέσιμο στο: https://ccdcoe.org (Πρόσβαση: 20 Ιανουαρίου 2025).

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia. Cooperative Cyber Defence Centre of Excellence.

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

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

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence.

Traynor, I. (2007). Russia Accused of Unleashing Cyberwar to Disable Estonia. *The Guardian*.

Wągrowska, M. (2020). Polish National Cybersecurity Strategy: Challenges and Implementation. *European Cybersecurity Journal, 6*(1), 25-34.

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

Zetter, K. (2017). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Διαθέσιμο στο: https://www.wired.com/story/inside-cunning-unprecedented-hack-of-ukraines-power-grid (Πρόσβαση: 20 Ιανουαρίου 2025).