ΕΛΛΗΝΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΣΤΡΑΤΗΓΙΚΩΝ ΜΕΛΕΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΠΡΑΚΤΙΚΗΣ ΑΣΚΗΣΗΣ ΦΟΙΤΗΤΩΝ ΑΕΙ
(16/05 – 15/07/2022)

ΣΥΝΤΟΝΙΣΤΡΙΑ : ΜΑΡΙΕΤΤΑ ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΥ

ΜΕΛΟΣ ΔΣ, ΕΜΠΕΙΡΟΓΝΩΜΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΚΠΑΙΔΕΥΣΗΣ

Τίτλος : «Cybersecurity: Επιχειρήσεις στον κυβερνοχώρο πριν από πολέμους και εντάσεις. Η περίπτωση της Ρωσίας με την Ουκρανία»

ΣΥΝΤΑΚΤΗΣ : ΑΡΙΣΤΕΑ ΠΛΙΑΓΚΟΥ

ΦΟΙΤΗΤΡΙΑ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ, ΤΜΗΜΑ ΔΙΕΘΝΩΝ & ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΕΠΙΒΛΕΠΩΝ : ΖΗΣΗΣ ΚΥΡΓΟΣ

ΜΕΛΟΣ ΕΛΙΣΜΕ , ΣΤΕΛΕΧΟΣ ΟΙΚΟΝΟΜΙΚΟΥ ΠΑ

Ημερομηνία Σύνταξης: 02/07/2022

Περιεχόμενα

Περίληψη-Abstract

Στην παρούσα εργασία μελετώνται οι επιχειρήσεις που πραγματοποιούνται στον Κυβερνοχώρο πριν από πολέμους και εντάσεις, με έμφαση στο παράδειγμα της Ρωσίας με την Ουκρανία. Για την πληρέστερη κατανόηση του θέματος, θα πραγματοποιηθεί αναφορά σε προηγούμενες ανάλογες περιπτώσεις και συγκεκριμένα σε αυτές της Ρωσίας εναντίον της Εσθονίας το 2007 και εναντίον της Γεωργίας το 2008. Πιο συγκεκριμένα, στην περίπτωση της Εσθονίας πραγματοποιήθηκαν επιθέσεις άρνησης υπηρεσιών σε ιστότοπους κυβερνητικών υπουργείων, μεγάλων τραπεζών, πολιτικών κομμάτων ακόμη και στη κρίσιμη οικονομική και πολιτική υποδομή της Εσθονίας. Ωστόσο, οι κυβερνοεπιθέσεις δεν συνοδεύτηκαν από πόλεμο και το φαινόμενο περιορίστηκε στην μορφή έντασης. Σχετικά με την Γεωργία, παρατηρήθηκαν επιθέσεις DDoS που κατέστρεψαν την υποδομή πληροφοριών, διακόπτοντας τις κυβερνητικές επικοινωνίες και παραβιάζοντας κυβερνητικούς ιστότοπους, ενώ άλλες κρίσιμες υποδομές δέχθηκαν επίσης επίθεση. Στην περίπτωση αυτή, οι κυβερνοεπιθέσεις συγχρονίστηκαν με την Ρωσογεωργιανή σύγκρουση του 2008. Περνώντας στην κύρια υπόθεση μελέτης, δηλαδή στις κυβερνοεπιθέσεις της Ρωσίας εναντίον της Ουκρανίας πριν και κατά τη διάρκεια του πολέμου του 2022, αυτή εξετάζεται σε επίπεδο Υψηλής Στρατηγικής και σε Στρατηγικό επίπεδο. Η Ουκρανία έχει υποστεί σημαντικές κυβερνοεπιθέσεις κυρίως στο δίκτυο παροχής ηλεκτρικού ρεύματος (2015) και την επίθεση NotPetya (2017) η οποία στόχευε στο δίκτυο των νοσοκομείων, των κεντρικών τραπεζών, τα αεροδρόμια, τις κρατικές εταιρείες ενέργειας, καθώς και σε ιδιωτικές επιχειρήσεις και συστήματα. Από την στιγμή της εισβολής της Ρωσίας, σύμφωνα με τις εκθέσεις της Microsoft, σημειώθηκαν στην Ουκρανία καταστροφικές επιθέσεις και επιχειρήσεις συλλογής πληροφοριών, ενώ οι ρωσικές στρατιωτικές δυνάμεις επιτίθονταν στη χώρα από ξηρά, αέρα και θάλασσα. Οι κυβερνοεπιθέσεις επιταχύνθηκαν αρκετά με το ξέσπασμα του πολέμου ενώ φάνηκε ότι οι επιθέσεις στον κυβερνοχώρο στόχευαν στη συλλογή πληροφοριών στρατιωτικής και εξωτερικής πολιτικής και στην απόκτηση πρόσβασης σε κρίσιμες υποδομές. Ωστόσο, παρατηρείται επίσης ότι, ενώ η Ουκρανία βρίσκεται σε εμπόλεμη κατάσταση, γενικά έχει σταθερή σύνδεση στο διαδίκτυο αλλά και σταθερή πρόσβαση στην παροχή ηλεκτρικού ρεύματος, εκτός από επιμέρους περιπτώσεις σχετικά με περιοχές που βρίσκονται υπό έντονη πολιορκία. Από το γεγονός αυτό, προκύπτει το συμπέρασμα ότι οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές εξαρτώνται και από άλλους παράγοντες. Πάντως και στις σε περιόδους πολέμων ή εντάσεων, σημειώνονται επιχειρήσεις στον κυβερνοχώρο με στόχο κρίσιμες υποδομές, συλλογή πληροφοριών και επιχειρήσεις επιρροής. Επίσης, στον πόλεμο Ρωσία - Ουκρανία σημαντική θέση καταλαμβάνουν οντότητες του ιδιωτικού τομέα χωρίς ξεκάθαρη αποστολή προστασίας στον κυβερνοχώρο, όπως η Microsoft με έκδοση εκθέσεων για τις κυβερνοεπιθέσεις, ενισχύοντας την πλευρά της Ουκρανίας. Τέλος, προκύπτει το συμπέρασμα ότι θα πρέπει πλέον να αποδίδεται ιδιαίτερη σημασία στις επιχειρήσεις στον κυβερνοχώρο, αφού φαίνεται να αποτελούν τον προάγγελο των στρατιωτικών συρράξεων ή να συνδυάζονται με αυτές.

1. Εισαγωγή

Είναι ευρέως γνωστό ότι τα τελευταία χρόνια οι τεχνολογικές εξελίξεις είναι ραγδαίες, με τις δυνατότητες που παρέχονται να εξελίσσουν όλες τις εκφάνσεις της ανθρώπινης ζωής. Η τεχνολογία έχει διευκολύνει την καθημερινή ζωή, ενώ παράλληλα το διαδίκτυο προσφέρει προοπτικές που παλαιότερα θα φάνταζαν αδύνατες. Οι εξελίξεις στο διεθνές και το παγκόσμιο περιβάλλον, μεταξύ άλλων, αποδεικνύουν ότι πλέον, το διαδίκτυο δεν αποτελεί μόνο τρόπο επικοινωνίας, αλλά και έναν χώρο, ικανό να επηρεάζει τις εξελίξεις τόσο στο εσωτερικό των κρατών, όσο και παγκοσμίως. Η ικανότητα αυτή, έχει φέρει στο προσκήνιο νέες έννοιες όπως ο κυβερνοχώρος, η κυβερνοασφάλεια αλλά και οι κυβερνοεπιθέσεις, οι οποίες παρουσιάζονται ως συχνό φαινόμενο. Υπό αυτό το πρίσμα, στην παρούσα εργασία θα εξεταστούν οι επιχειρήσεις που πραγματοποιούνται στον Κυβερνοχώρο πριν από πολέμους και εντάσεις. Για την πληρέστερη κατανόηση του θέματος, θα πραγματοποιηθεί αναφορά σε διάφορες περιπτώσεις[1] κρατών που προέβησαν σε επιχειρήσεις στο κυβερνοχώρο, εστιάζοντας περισσότερο στο επίκαιρο παράδειγμα της Ρωσίας με την Ουκρανία σε επίπεδο Υψηλής Στρατηγικής και σε Στρατηγικό επίπεδο, ως μια πολεμική σύγκρουση που τείνει να αλλάξει τις ισορροπίες των δυνάμεων στην περιοχή, επηρεάζοντας τα γειτονικά κράτη και επιφέροντας πληθώρα κρίσεων στην Ευρώπη.

[1]Η αναφορά σε προηγούμενες περιπτώσεις επιχειρήσεων στον κυβερνοχώρο έχει στο επίκεντρο της την Ρωσία και συγκεκριμένα τις δράσεις αυτής προς την Εσθονία (2007) και την Γεωργία (2008). Σε αντίθεση με την περίπτωση της Εσθονίας, όπου οι κυβερνοεπιχειρήσεις περιορίστηκαν σε φαινόμενο έντασης, στην περίπτωση της Γεωργίας οι αντίστοιχες επιχειρήσεις συνδυάστηκαν με ένοπλη σύρραξη.

2. Ερευνητικό Πλαίσιο – Μεθοδολογία

Όπως αποδεικνύει η ιστορία, η ανθρωπότητα έχει βιώσει διάφορες περιπτώσεις στρατιωτικών συγκρούσεων, όπως οι Α και Β Παγκόσμιοι Πόλεμοι. Οι ένοπλες διακρατικές συγκρούσεις διαδραματίζονταν παραδοσιακά στη ξηρά, στην θάλασσα ή στον εναέριο χώρο. Ωστόσο, τα τελευταία χρόνια στο προσκήνιο εισέρχονται το διάστημα και ο κυβερνοχώρος. Προκειμένου, λοιπόν, να κατανοηθούν καλύτερα οι πολεμικές επιχειρήσεις στον κυβερνοχώρο, κρίνεται αναγκαία η παράθεση κάποιων σχετικών ορισμών. Αρχικά, σύμφωνα με το Λεξικό Στρατιωτικών Όρων του Υπουργείου Άμυνας των ΗΠΑ (DoD 2010), *«ο κυβερνοχώρος αποτελεί έναν παγκόσμιο τομέα στο περιβάλλον πληροφοριών ο οποίος αποτελείται από το αλληλεξαρτώμενο δίκτυο υποδομών τεχνολογίας πληροφοριών, συμπεριλαμβανομένου του διαδικτύου, των δικτύων τηλεπικοινωνιών, των συστημάτων υπολογιστών και των ενσωματωμένων επεξεργαστών και ελεγκτών»*. Ένας άλλος ορισμός, ορίζει τον κυβερνοχώρο ως *«το εικονικό περιβάλλον στο οποίο πραγματοποιούνται ηλεκτρονικές επικοινωνίες, όπως το διαδίκτυο. Αποτελεί λοιπόν, ένα δίκτυο ψηφιακών πληροφοριών και επικοινωνιακών υποδομών, το οποίο είναι συνδεδεμένο παγκοσμίως»* (Robin, 2013). Ακόμη, ο κυβερνοχώρος ορίζεται ως *«ένας παγκόσμιος κλάδος (τομέας) εντός του χώρου πληροφόρησης που αντιπροσωπεύεται από ένα σύνολο αλληλεξαρτώμενων υποδομών και τεχνολογιών πληροφόρησης, συμπεριλαμβανομένου του Διαδικτύου, των τηλεπικοινωνιακών δικτύων, των συστημάτων υπολογιστών, των επεξεργαστών και των ελεγκτών»*. Ο τελευταίος ορισμός που παρουσιάζεται ορίζει τον κυβερνοχώρο ως κάτωθι: *«Αποτελεί το ηλεκτρονικό περιβάλλον, στο οποίο η δημιουργία, η αποθήκευση, η προσαρμογή, η μετάδοση και η διαγραφή των πληροφοριών γίνεται με ψηφιακά σήματα»* (Starodubtsev, Balenko, Vershennik, and Fedorov 2020).

Εν συνεχεία, σύμφωνα με το Υπουργείο Άμυνας των ΗΠΑ (DoD 2010), οι επιχειρήσεις στον κυβερνοχώρο ορίζονται ως *«η χρήση ικανοτήτων στον κυβερνοχώρο όπου ο πρωταρχικός σκοπός είναι η επίτευξη αντικειμενικών σκοπών μέσω του κυβερνοχώρου. Τέτοιες επιχειρήσεις περιλαμβάνουν την προστασία των κρίσιμων υποδομών από κυβερνοεπιθέσεις, την ασφάλεια πληροφοριών αλλά και επιθετικές επιχειρήσεις εναντίον αντιπάλων στόχων στον κυβερνοχώρο»*. Οι επιχειρήσεις στον κυβερνοχώρο, μεταξύ άλλων, μπορούν να πάρουν την μορφή εχθρικών ενεργειών (Lin, 2010). Οι ενέργειες αυτές παρουσιάζονται ως cyber attacks και cyber exploitation. Τα cyberattacks έχουν καταστροφική φύση και επιδιώκουν να παραβιάσουν τα συστήματα και τα δίκτυα του αντιπάλου, ώστε να μην είναι προσβάσιμα, διαθέσιμα ή αξιόπιστα και επομένως λιγότερο χρήσιμα. Οι επιχειρήσεις cyber exploitation είναι μη καταστροφικές. Ειδικότερα, αφορούν την χρήση ενεργειών και λειτουργιών ώστε να επιτευχθεί η πρόσβαση σε πληροφορίες ηλεκτρονικών συστημάτων και δικτύων του αντιπάλου, οι οποίες υπό άλλες συνθήκες, θα διατηρούνταν εμπιστευτικές.

Επιπρόσθετα, μεταβαίνοντας στην έννοια του κυβερνοπολέμου, ο Clarke (2010) την ορίζει ως *«τις δραστηριότητες ενός έθνους-κράτους, οι οποίες έχουν σκοπό να διεισδύσει στους Η/Υ και στα δίκτυα του*

αντιπάλου με στόχο την διάρρηξη ή καταστροφή τους, καθιστώντας απαραίτητο το κριτήριο της εθνικοκρατικής παρουσίας στις εν λόγω συρράξεις, ώστε να θεωρούνται κυβερνοπολεμικές».

Τέλος, η σημαντικότερη έννοια που χρήζει ορισμού είναι εκείνη της κυβερνοασφάλειας. Ειδικότερα, ο όρος κυβερνοασφάλεια έχει αποτελέσει αντικείμενο της ακαδημαϊκής συζήτησης και βιβλιογραφίας, ενώ χρησιμοποιείται ευρέως και οι ορισμοί του είναι εξαιρετικά ποικίλοι. Σύμφωνα με τον Kemmerer (2003), *«η κυβερνοασφάλεια αποτελείται σε μεγάλο βαθμό από αμυντικές μεθόδους που χρησιμοποιούνται για τον εντοπισμό και την αποτροπή επίδοξων εισβολέων».* Ένας άλλος ορισμός, αναφέρει ότι *«η κυβερνοασφάλεια αφορά τη μείωση του κινδύνου της κακόβουλης επίθεσης σε λογισμικό, υπολογιστές και δίκτυα. Αυτό περιλαμβάνει εργαλεία που χρησιμοποιούνται για την ανίχνευση παραβιάσεων και ιών, τον αποκλεισμό κακόβουλης πρόσβασης, την επιβολή ελέγχου, την ενεργοποίηση κρυπτογραφημένων επικοινωνιών και άλλα»* (Amoroso, 2006). Επιπλέον, η κυβερνοασφάλεια περιγράφεται ως *«συλλογή εργαλείων, πολιτικών, εννοιών ασφαλείας, δικλείδων ασφαλείας, κατευθυντήριων γραμμών, προσεγγίσεων διαχείρισης κινδύνων, ενεργειών, κατάρτισης, βέλτιστων πρακτικών, διασφάλισης και τεχνολογιών που μπορούν να χρησιμοποιηθούν για την προστασία του περιβάλλοντος και της οργάνωσης του κυβερνοχώρου και των περιουσιακών στοιχείων του χρήστη»* (ITU, 2009). Ένας τελευταίος ορισμός που καθίσταται αναγκαίο να παρατεθεί ορίζει την έννοια της κυβερνοασφάλειας ως *«το σύνολο των τεχνολογιών, των διαδικασιών, των πρακτικών και των μέτρων αντίδρασης και μετριασμού, που αποσκοπούν στην προστασία των δικτύων, των υπολογιστών, των προγραμμάτων και των δεδομένων από επίθεση, καταστροφή ή μη εξουσιοδοτημένη πρόσβαση, ώστε να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα»* (Public Safety Canada, 2014).

2.1 Επίπεδα στρατηγικής: Συνοπτική ανάλυση

Πριν παρατεθεί η κύρια ανάλυση του θέματος, κρίνεται απαραίτητη η αναφορά στην έννοια και τα επίπεδα της Στρατηγικής. Στρατηγική λοιπόν, είναι, κατά τη στρατιωτική - στρατιωτικοκεντρική ερμηνεία του όρου, η σύζευξη μέσων και σκοπών ενόψει μιας πραγματικής ή ενδεχόμενης σύγκρουσης. Η έννοια της στρατηγικής συνίσταται στο τρίπτυχο μέσα, σκοποί και αντίπαλος (Κολιόπουλος, 2010). Σύμφωνα με τη θεωρία πολέμου, οι στρατιωτικές επιχειρήσεις διεξάγονται σε τέσσερα διαφορετικά επίπεδα ως εξής (Κονδύλης, 2004): Το επίπεδο της Υψηλής Στρατηγικής – Πολιτικό Επίπεδο, το επίπεδο της Στρατιωτικής Στρατηγικής, το Επιχειρησιακό επίπεδο και το Τακτικό επίπεδο.

2.1.1 Επίπεδο Υψηλής Στρατηγικής

Σε αυτό το επίπεδο, η Κυβέρνηση διαμορφώνει και καθορίζει την πολιτική η οποία στοχεύει είτε στην διεξαγωγή πολέμου, είτε στην αποφυγή του. Ακόμη, διαμορφώνονται οι συνθήκες ειρήνης μετά τον πόλεμο. Επομένως, στον τομέα αυτό περιλαμβάνεται η Εθνική Πολιτική για θέματα άρρηκτα συνδεδεμένα με την διατήρηση της ανεξαρτησίας, της εδαφικής ακεραιότητας καθώς και με την

υπεράσπιση εθνικών συμφερόντων και τον καθορισμό των εθνικών Αντικειμενικών Σκοπών (ΑΝ.ΣΚ.). Ακόμη, συμπεριλαμβάνεται η Εθνική Στρατηγική, η οποία αποτελεί την επιστήμη της ανάπτυξης και της χρήσης των παραγόντων της Εθνικής Ισχύος σε περίοδο ειρήνης, κρίσεως και πολέμου, αφενός, προς διασφάλισης των εθνικών ΑΝ.ΣΚ. και των συμφερόντων, και αφετέρου, προς υποστήριξη της εθνικής πολιτικής. Όπως διαπιστώνεται, ο στρατηγικός σχεδιασμός και η συστράτευση πολλών παραγόντων (πολιτικών, διπλωματικών, οικονομικών κ.α.) προϊσταται, προκειμένου να επιτευχθεί ο εθνικός ΑΝ.ΣΚ.

2.1.2 Στρατιωτικό Στρατηγικό Επίπεδο

Εν συνεχεία, στο επίπεδο αυτό, διαμορφώνεται το συστατικό της Υψηλής Στρατηγικής, η στρατιωτική στρατηγική. Πιο συγκεκριμένα, πρόκειται για τον τρόπο ανάπτυξης και εμπλοκής των Ενόπλων Δυνάμεων ώστε να επιτευχθούν οι στόχοι του προαναφερθέντος επιπέδου ενώ, ως μέρος της εθνικής στρατηγικής, επιδιώκει την ισχυροποίηση του ρόλου μιας χώρας στο διεθνές περιβάλλον.

2.1.3 Επιχειρησιακό Επίπεδο

Σε ό,τι αφορά το επιχειρησιακό επίπεδο, πρόκειται για το επίπεδο πολέμου στο οποίο σχεδιάζονται οι επιχειρήσεις. Μέσω της επιχειρησιακής τέχνης, λειτουργεί ως συνδετικός κρίκος μεταξύ των δυνάμεων και των αντικειμενικών στρατηγικών σκοπών. Η επιχειρησιακή τέχνη ορίζεται ως η επιδεξιότητα χρήσης των στρατιωτικών μέσων για επίτευξη των στρατιωτικών ΑΝ.ΣΚ., μέσω σχεδιασμού, οργάνωσης και διεξαγωγής επιχειρήσεων.

2.1.4 Τακτικό Επίπεδο

Στο τελευταίο επίπεδο, σχεδιάζονται και εκτελούνται τακτικές στρατιωτικές ενέργειες από τακτικούς σχηματισμούς και μονάδες. Η τακτική είναι η τέχνη της διάταξης χερσαίων, ναυτικών, αεροπορικών και ειδικών δυνάμεων με σκοπό την νίκη και κατ' επέκταση, την επίτευξη των στρατιωτικών αντικειμενικών σκοπών.

Για τον σκοπό της παρούσας εργασίας, θα εξεταστεί το επίπεδο Υψηλής Στρατηγικής καθώς και το Στρατιωτικό Στρατηγικό Επίπεδο.

3. Ανασκόπηση Βιβλιογραφίας

Σχετικά με τις κυβερνοεπιχειρήσεις και τις κυβερνοεπιθέσεις της Ρωσίας κατά της Ουκρανίας έχουν αναπτυχθεί διάφορες αναλύσεις, κάποιες από τις οποίες παρατίθενται στην παρούσα εργασία. Πιο συγκεκριμένα, ο Limnéll (2015) αναφέρει ότι η περίπτωση της Ουκρανίας προσφέρει μια οπτική στον υβριδικό πόλεμο για τον οποίο η Δύση πρέπει να προετοιμάζεται. Πρόκειται για μάχες στις οποίες οι παραδοσιακές χερσαίες δυνάμεις συνδυάζονται με τις κυβερνοεπιθέσεις για την αντιμετώπιση ενός εχθρού. Επίσης, απεικονίζει τις δυσκολίες που αντιμετωπίζουν τα έθνη στον εντοπισμό και την άμυνα έναντι των επιτιθέμενων στον κυβερνοχώρο. Τα όρια μεταξύ του πραγματικού πολέμου και άλλων ασκήσεων εξουσίας γίνονται ασαφή και τα μέσα του κυβερνοπολέμου γίνονται όλο και πιο σημαντικά στον κόσμο. Η ρωσική επιθετικότητα στην Ουκρανία θεωρείται ως η καλύτερη δυνατή μελέτη περίπτωσης μέχρι σήμερα σχετικά με τις πτυχές του σύγχρονου πολέμου στον κυβερνοχώρο. Κατά τη διάρκεια του συνεχιζόμενου ρωσο-ουκρανικού πολέμου, σημειώθηκε ένα ευρύ φάσμα διαδικτυακών δραστηριοτήτων, κυβερνοεπιθέσεων χαμηλού επιπέδου, κυβερνοκατασκοπείας και του τρόπου με τον οποίο ο τομέας του κυβερνοχώρου χρησιμοποιείται στον πόλεμο των πληροφοριών. Οι επιθέσεις Distributed Denial-of-Service (DDoS), οι παραβιάσεις ιστοτόπων, οι εκστρατείες κατασκοπείας στον κυβερνοχώρο και άλλες κυβερνοεπιθέσεις με πολιτικά κίνητρα έχουν εξυπηρετήσει τους ευρύτερους σκοπούς των στρατηγικών στόχων της Ρωσίας. Βέβαια, ακόμα κι αν η Ρωσία έχει πιθανότατα τις δυνατότητες να εξαπολύσει στρατηγικές επιθέσεις στον κυβερνοχώρο, ο ρωσο-ουκρανικός πόλεμος δείχνει ότι η Ρωσία έχει επιδείξει αυτοσυγκράτηση, προτιμώντας να αποτρέψει περαιτέρω κλιμάκωση ή απλώς να διατηρήσει την ικανότητα για στρατηγικό αιφνιδιασμό, αφού δεν επιθυμεί να καταστρέψει τις υποδομές της Ουκρανίας. Ωστόσο, ούτε η Ουκρανία έχει εξαπολύσει στρατηγικές κυβερνοεπιθέσεις εναντίον ρωσικών στόχων. Αντίθετα, ομάδες χάκερ, οι οποίοι δεν αποτελούν απαραίτητα εκτελεστικά όργανα των κυβερνήσεων, και στις δύο πλευρές έχουν πραγματοποιήσει πολλές διαφορετικές επιχειρήσεις χαμηλού επιπέδου στον κυβερνοχώρο.

Ο συγγραφέας συμπεραίνει ότι υπό το πρίσμα της ουκρανικής εμπειρίας, φαίνεται πιο πιθανό οι κυβερνοεπιχειρήσεις να αναπτυχθούν σε μελλοντικούς πολέμους και συγκρούσεις για να διαμορφώσουν τον χώρο μάχης, παρά ως μεμονωμένες δραστηριότητες. Σχετικά με τους μελλοντικούς πολέμους και συγκρούσεις, είναι αναμενόμενη η χρήση των δυνατοτήτων του κυβερνοχώρου σε συνδυασμό με πιο συμβατικά όπλα. Οι κρατικοί και μη κρατικοί φορείς χρησιμοποιούν όλο και περισσότερο τον κυβερνοχώρο σε συγκρούσεις και πολέμους για να συγκεντρώσουν πληροφορίες, να προωθήσουν τις αφηγήσεις τους υποτιμώντας αυτές των αντιπάλων και να ενσωματώσουν τις κυβερνοεπιχειρήσεις με τις φυσικές επιχειρήσεις. Ο ρωσο-ουκρανικός πόλεμος έδωσε ένα παράδειγμα στον υπόλοιπο κόσμο πώς μπορεί να χρησιμοποιηθεί ο τομέας του κυβερνοχώρου κατά τη διάρκεια του υβριδικού πολέμου, ακόμη και με «φειδώ».

Οι Valuch και Hamulak (2018) κάνουν λόγο για τον κυβερνοχώρο του οποίου η κανονιστική ρύθμιση αποτελεί μεγάλη πρόκληση για το σύγχρονο διεθνές δίκαιο. Θεωρούν ότι πράγματι, έχει αρχίσει να παίζει σημαντικό ρόλο σε συγκρούσεις και εχθροπραξίες, αφού τα περιστατικά στον κυβερνοχώρο χρησιμοποιούνται όλο και περισσότερο για να βλάψουν ή να αποδυναμώσουν αντιστοίχως. Υπό αυτό το πρίσμα, εξετάζουν τις διάφορες μορφές των παραβιάσεων που επιδιώκονται στον κυβερνοχώρο κατά τη διάρκεια της σύγκρουσης στην Ουκρανία. Μάλιστα, χαρακτηρίζουν την σύγκρουση αυτή ως παράδειγμα της πολυπλοκότητας της νομικής προσέγγισης και της έλλειψης της νομικής κατανόησης των επιχειρήσεων και των επιθέσεων στον κυβερνοχώρο. Επιδιώκουν λοιπόν, να τονίσουν αυτή την πολυπλοκότητα και να καθορίσουν τις επιχειρήσεις που πραγματοποιούνται στον κυβερνοχώρο της Ουκρανίας με γνώμονα το Διεθνές Δίκαιο.

Ο Lewis (2015) αναλύει τις γεωπολιτικές επιπτώσεις των επιθέσεων στον κυβερνοχώρο. Πιο συγκεκριμένα, παρουσιάζει δύο παραμέτρους: τις στρατηγικές επιπτώσεις που μειώνουν την θέληση ή την ικανότητα ενός αντιπάλου να πολεμήσει, και τις τακτικές επιδράσεις που υποβαθμίζουν την στρατιωτική δύναμη. Στη συνέχεια, αναφέρεται στην περίπτωση των κυβερνητικών επιθέσεων της Ρωσίας προς την Ουκρανία. Ακόμη, συγκρίνει τις ρωσικές επιχειρήσεις στην Ουκρανία με τις αντίστοιχες στην Εσθονία και την Γεωργία και καταλήγει στο γεγονός ότι δεν επιτεύχθηκε στρατηγική επίδραση, αλλά μόνο περιορισμένα και βραχυπρόθεσμα πολιτικά αποτελέσματα.

3.1 Το παράδειγμα Ρωσία – Εσθονία (2007)

Τον Απρίλιο του 2007, η εσθονική κυβέρνηση μετέφερε τον Χάλκινο Στρατιώτη - ένα μνημείο για τη σοβιετική απελευθέρωση της Εσθονίας από τους Ναζί - στο Στρατιωτικό Κοιμητήριο του Ταλίν. Αυτή η απόφαση πυροδότησε αντιδράσεις μεταξύ των ρωσόφωνων μειονοτήτων σε τέτοιο βαθμό, ώστε η Εσθονία να υποστεί πληθώρα κυβερνοεπιθέσεων με εμφανή πολιτικά κίνητρα οι οποίες διήρκεσαν είκοσι δύο ημέρες. Πιο συγκεκριμένα, εκτός από τις ταραχές και τη βία που σημειώθηκαν αρχικά, επιθέσεις DDoS στον κυβερνοχώρο με στόχο την υποδομή της χώρας κατέστησαν μη διαθέσιμους τους ιστότοπους όλων των κυβερνητικών υπουργείων, μεγάλων τραπεζών και πολλών πολιτικών κομμάτων. Ακόμη, οι χάκερ απενεργοποίησαν τον κοινοβουλευτικό διακομιστή email. Άλλες επιθέσεις επικεντρώθηκαν σε ακόμη πιο ζωτικούς στόχους, όπως την ηλεκτρονική τραπεζική καθώς και τη κρίσιμη οικονομική και πολιτική υποδομή της Εσθονίας.

Γενικότερα, η εξάρτηση της Εσθονίας από την τεχνολογία πληροφοριών παρείχε στους χάκερ αρκετούς στόχους για επιθέσεις. Άλλωστε, όπως τα περισσότερα άλλα δυτικά κράτη, η Εσθονία βασίζεται στο Διαδίκτυο για την κρίσιμη υποδομή της. Τα ηλεκτρονικά δίκτυα αποτελούν αναπόσπαστο κομμάτι της λειτουργίας των κρατικών λειτουργιών της, των δικτύων ηλεκτρικής ενέργειας, των τραπεζικών υπηρεσιών, ακόμη και της παροχής νερού του Ταλίν. Οι δυτικές χώρες, σε μια προσπάθεια αντιμετώπισης της απειλής, καταπολέμησαν αποτελεσματικά τις ρωσικές επιθέσεις στον κυβερνοχώρο

της Εσθονίας, ελαχιστοποιώντας τις επιπτώσεις. Γενικότερα, το φαινόμενο περιορίστηκε σε ένταση και δεν έλαβε την μορφή πολέμου. Όπως διαπιστώνεται με το παράδειγμα αυτό, το Διαδίκτυο επιτρέπει σε διάφορες ομάδες να διεξάγουν επιθετικές επιχειρήσεις, απειλώντας την κυριαρχία των εθνών-κρατών στον κυβερνοχώρο. Παράλληλα, οι απαντήσεις στις ρωσικές κυβερνοεπιθέσεις καταδεικνύουν το αυξανόμενο ενδιαφέρον των κρατών για την υπεράσπιση της εθνικής κυριαρχίας στη σφαίρα του κυβερνοχώρου (Herzog, 2011).

3.2 Το παράδειγμα Ρωσία – Γεωργία (2008)

Η δεύτερη περίπτωση κυβερνοεπιθέσεων που εξετάζεται είναι αυτή εναντίον της Γεωργίας η οποία συγχρονίστηκε με τη ρωσογεωργιανή σύγκρουση το 2008. Οι εντάσεις μεταξύ της Ρωσίας και της Γεωργίας είχαν αυξηθεί τα προηγούμενα χρόνια, πριν το 2008, λόγω της εξωτερικής πολιτικής της Γεωργίας, η οποία είχε γίνει όλο και πιο δυτική υπό τον Πρόεδρο Μιχαήλ Σαακασβίλι, καθώς και λόγω της σχέσης της Γεωργίας με αυτονομιστικές δημοκρατίες της Νότιας Οσετίας και της Αμπχαζίας. Η στρατιωτική επέμβαση της Γεωργίας στη Νότια Οσετία στις 7 Αυγούστου, φαινομενικά για να αποτρέψει τον βομβαρδισμό της γεωργιανής επικράτειας από την Οσετία, ώθησε τη Ρωσία να πραγματοποιήσει μια μεγάλης κλίμακας χερσαία, αεροπορική και θαλάσσια εισβολή στη Γεωργία την επόμενη μέρα.

Καθώς οι ρωσικές στρατιωτικές δυνάμεις μετακινήθηκαν στη Νότια Οσετία, μια σειρά από επιθέσεις DDoS κατέστρεψαν την υποδομή πληροφοριών της Γεωργίας, διακόπτοντας τις κυβερνητικές επικοινωνίες και παραβιάζοντας κυβερνητικούς ιστότοπους. Τράπεζες της Γεωργίας, εταιρείες μεταφορών και ιδιωτικοί πάροχοι τηλεπικοινωνιών δέχθηκαν επίσης επίθεση, διαταράσσοντας τις υπηρεσίες. Την ημέρα που ξεκίνησε ο πόλεμος, ιστότοποι ρωσικών χάκερ-ακτιβιστών, όπως το stopgeorgia.ru, παρείχαν λίστες γεωργιανών τοποθεσιών για επίθεση, οδηγίες, κακόβουλα λογισμικά και αξιολογήσεις μετά την ενέργεια. Υπό αυτό το πρίσμα, η Γεωργία υποβλήθηκε σε εικονικό αποκλεισμό στον κυβερνοχώρο, με τους περισσότερους από τους δράστες να εντοπίζονται τελικά σε διακομιστές στη Ρωσία και την Τουρκία που ήταν συνδεδεμένοι με το Russian Business Network (RBN). Δεν αποτελεί έκπληξη το γεγονός ότι η ρωσική κυβέρνηση αρνήθηκε ανάμειξη, με έναν εκπρόσωπο της ρωσικής πρεσβείας να δηλώνει ότι ήταν πιθανό άτομα στη Ρωσία ή αλλού να είχαν αναλάβει να ξεκινήσουν τις επιθέσεις, εν αγνοία της κυβέρνησης. Για άλλη μια φορά, η εμπλοκή της ρωσικής κυβέρνησης δεν μπορούσε να αποδειχθεί οριστικά , αν και ο χρόνος των επιθέσεων παρείχε ισχυρές ενδείξεις ότι το Κρεμλίνο συντόνιζε τις επιθέσεις.

Ενώ ο συνολικός αντίκτυπος των κυβερνοεπιθέσεων ήταν ελάχιστος—η υποδομή πληροφορικής της Γεωργίας ήταν περιορισμένη το 2008 και η γεωργιανή κυβέρνηση κατάφερε τελικά να αναδρομολογήσει το μεγαλύτερο μέρος της επισκεψιμότητας και της πρόσβασης στους ιστότοπους της μέσω διακομιστών σε άλλες χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών, της Εσθονίας

και της Πολωνίας— ήταν η πρώτη γνωστή περίπτωση ευρείας κλίμακας επιθετικών επιχειρήσεων στον κυβερνοχώρο που τοποθετούνται για την υποστήριξη συμβατικών στρατιωτικών επιχειρήσεων. Οι επιθέσεις που χρησιμοποιήθηκαν από τις ομάδες χάκερ ήταν σχετικά απλές — κυρίως επιθέσεις DDoS (Markoff, 2008). Ωστόσο, ο βαθμός συντονισμού που τις χαρακτηρίζει, υποδηλώνει ότι αποτελούσαν μέρος ενός συντονισμένου σχεδίου εκστρατείας, ο σχεδιασμός και η προετοιμασία του οποίου προηγήθηκαν των ρωσικών συμβατικών επιχειρήσεων κατά αρκετές εβδομάδες. Μεταγενέστερες έρευνες αποκάλυψαν ότι χάκερ διερευνούσαν και κατά καιρούς επιτέθηκαν σε κυβερνητικούς διακομιστές της Γεωργίας τουλάχιστον από τις 20 Ιουλίου. Σε ορισμένες περιπτώσεις, οι επιθέσεις ευθυγραμμίστηκαν επίσης γεωγραφικά με τις ρωσικές συμβατικές επιχειρήσεις. Για παράδειγμα, Ρώσοι χάκερ επιτέθηκαν σε κυβερνητικούς ιστότοπους στην πόλη Γκόρι στην ανατολική Γεωργία, μαζί με ειδησεογραφικούς ιστότοπους, λίγο πριν από τις ρωσικές αεροπορικές επιθέσεις στην πόλη αυτή (Conell and Vogler, 2016).

4. Κυρίως Ανάλυση

Περνώντας στην ανάλυση των κυβερνοεπιθέσεων της Ρωσίας προς την Ουκρανία, διαπιστώνεται ότι ακόμη και πριν την έναρξη της εισβολής της Ρωσίας στις 24 Φεβρουαρίου 2022, έχουν σημειωθεί καταστροφικές κυβερνοεπιθέσεις κατά της ουκρανικής ψηφιακής υποδομής. Η επίθεση στο ουκρανικό δίκτυο ηλεκτρικής ενέργειας το 2015 ήταν η πρώτη τεκμηριωμένη κυβερνοεπίθεση κατά κρίσιμων υποδομών που οδήγησε σε διακοπή ρεύματος (FireEye, 2016) και η πρώτη γνωστή επίθεση σε ένα ενεργειακό δίκτυο που πραγματοποιήθηκε εξ ολοκλήρου από απόσταση (McLellan, 2016). Ξεκίνησε τον Δεκέμβριο του 2015, με την παράνομη είσοδο στα συστήματα και τους υπολογιστές SCADA της εταιρείας διανομής ηλεκτρικής ενέργειας Kyivoblenergo. Μετά την επίθεση, 30 υποσταθμοί διανομής αποσυνδέθηκαν για τρεις ώρες και οι χειριστές αναγκάστηκαν να περάσουν σε χειροκίνητη λειτουργία (E-ISAC, 2016). Η διακοπή επηρέασε αρκετές εταιρείες διανομής, με αποτέλεσμα διακοπές ρεύματος για 225.000 χρήστες (Rõigas, 2018). Σύμφωνα με ορισμένες πηγές μέσων ενημέρωσης, η ουκρανική κυβέρνηση σχεδόν αμέσως έδειξε τη Ρωσία ως πιθανή πηγή της επίθεσης (Kovacs 2015, Nakashima 2016, Hern 2016), ωστόσο η επίσημη απόδοση αναβλήθηκε εν αναμονή των αποτελεσμάτων της έρευνας (Polityuk, 2015). Τον Ιανουάριο του 2016, το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ παρενέβη για να βοηθήσει στη διερεύνηση της υπόθεσης (Volz και Finkle 2016), αλλά δεν εκδόθηκε ποτέ επίσημη απόδοση ευθύνης. Η μόνη αναφορά δόθηκε από την αμερικανική ιδιωτική εταιρεία πληροφοριών στον κυβερνοχώρο iSIGHT Partners, η οποία συνέδεσε την επιχείρηση με τη Ρωσία, υποστηρίζοντας ότι εκτελέστηκε από μια ομάδα γνωστή ως «Sandworm» (Newsweek, 2016 και Hultquist, 2016) με τη χρήση ενός κακόβουλου λογισμικού, BlackEnergy. Ωστόσο, δεν υπήρξε ενιαία θέση μεταξύ των ειδικών στον κυβερνοχώρο σχετικά με τη σχέση μεταξύ BlackEnergy και Ρωσίας.

Ακόμη, τον Ιούνιο του 2017, η χώρα βίωσε την κυβερνοεπίθεση NotPetya[2], κατά την οποία ένα κακόβουλο εργαλείο κρυπτογράφησης δεδομένων εισήχθη σε ένα κομμάτι λογισμικού που χρησιμοποιείται από τα περισσότερα χρηματοπιστωτικά και κυβερνητικά ιδρύματα της Ουκρανίας. Στις 14 Φεβρουαρίου 2018, το Εθνικό Κέντρο Κυβερνοασφάλειας του Ηνωμένου Βασιλείου ανακοίνωσε την αξιολόγησή του για την επίθεση, η οποία διαπίστωσε ότι ο ρωσικός στρατός ήταν *«σχεδόν σίγουρα υπεύθυνος»* για αυτήν. Στη συνέχεια, αρκετές ώρες πριν τα ρωσικά τανκς ξεκινήσουν τη στρατιωτική επίθεση στην Ουκρανία, το Κέντρο Πληροφοριάκων Απειλών της Microsoft εντόπισε νέες κυβερνοεπιθέσεις εναντίον ουκρανικών ψηφιακών στόχων. Στις 28 Φεβρουαρίου, η Microsoft δήλωσε ότι ανησυχεί ιδιαίτερα για τις πρόσφατες κυβερνοεπιθέσεις σε μη στρατιωτικούς ψηφιακούς στόχους, συμπεριλαμβανομένων των υπηρεσιών απόκρισης έκτακτης ανάγκης και των προσπαθειών

[2]Το NotPetya ήταν μια καταστροφική επίθεση κακόβουλου λογισμικού που στόχευε κυρίως την Ουκρανία τον Ιούνιο του 2017, προκαλώντας αδιάκριτες ζημιές στο δίκτυο στα νοσοκομεία, την κεντρική τράπεζα, τα αεροδρόμια και τις κρατικές εταιρείες ενέργειας, καθώς και σε ιδιωτικές επιχειρήσεις και συστήματα. Με τις συνολικές ζημιές που υπολογίζονται από τον Λευκό Οίκο να ξεπερνούν τα 10 δισεκατομμύρια δολάρια, το NotPetya έχει θεωρηθεί «η πιο καταστροφική κυβερνοεπίθεση στην ιστορία» (Greenberg 2018).

ανθρωπιστικής βοήθειας. Σύμφωνα με τον Μπραντ Σμιθ, τότε Πρόεδρο της Microsoft, *«αυτές οι επιθέσεις σε μη στρατιωτικούς ψηφιακούς στόχους εγείρουν σοβαρές ανησυχίες βάσει της Σύμβασης της Γενεύης και έχουμε μοιραστεί πληροφορίες με την ουκρανική κυβέρνηση για καθέναν από αυτούς»*. Επίσης, δήλωσε ότι η Microsoft είχε ενημερώσει την κυβέρνηση της Ουκρανίας σχετικά με πρόσφατες προσπάθειες στον κυβερνοχώρο για κλοπή ενός ευρέους φάσματος δεδομένων, συμπεριλαμβανομένων υγειονομικών και άλλων κρατικών δεδομένων που περιέχουν στοιχεία προσωπικών δεδομένων. Επίσης, κυβερνοεπιθέσεις παρατηρήθηκαν και στον τομέα της υγείας της Ουκρανίας, αν και πριν από την εισβολή, η χώρα είχε προβεί σε ψηφιακό μετασχηματισμό στον τομέα αυτό, με τη βοήθεια του έργου EU4 Digital.

Μετά την εισβολή και κατά την διάρκεια του πολέμου, οι εκτεταμένες κυβερνοεπιθέσεις της Ρωσίας στην Ουκρανία παρέχουν πληροφορίες για τον τρόπο με τον οποίο αναπτύσσει κυβερνοεπιθέσεις τόσο σε ένοπλες συγκρούσεις όσο και στον υβριδικό πόλεμο εναντίον της Δύσης. Στις 27 Απριλίου 2022, η Μονάδα Ψηφιακής Ασφάλειας της Microsoft εξέδωσε μια έκθεση που απαριθμούσε και ανέλυε όλες τις γνωστές ρωσικές κυβερνοεπιθέσεις στην Ουκρανία τους πρώτους μήνες του πολέμου. Η έκθεση κατέληξε στο συμπέρασμα ότι η ρωσική στρατιωτική υπηρεσία πληροφοριών (κοινώς γνωστή ως GRU), η ξένη υπηρεσία πληροφοριών (ή SVR) και η ομοσπονδιακή υπηρεσία ασφαλείας (ή FSB) *«διεξήγαγαν καταστροφικές επιθέσεις, επιχειρήσεις συλλογής πληροφοριών ή και τα δύο, ενώ οι ρωσικές στρατιωτικές δυνάμεις επιτίθονταν στη χώρα από ξηρά, αέρα και θάλασσα».* Ο στόχος ήταν «*να διαταραχθεί ή να υποβαθμιστεί η ουκρανική κυβέρνηση και οι στρατιωτικές λειτουργίες και να υπονομευθεί η εμπιστοσύνη των πολιτών στους ίδιους αυτούς θεσμούς».* Οι κυβερνοεπιθέσεις επιταχύνθηκαν αρκετά με το ξέσπασμα του πολέμου, με την Microsoft να καταγράφει τον Δεκέμβριο του 2021, 15 ρωσικές κυβερνοεπιθέσεις κατά της Ουκρανίας, αριθμός που αυξήθηκε σε 125 τον Μάρτιο του 2022. Η εταιρεία εκτιμά ότι η Ρωσία άρχισε να προετοιμάζεται για κυβερνοεπιθέσεις στην Ουκρανία τον Μάρτιο του 2021, την ίδια στιγμή που άρχισε να αναπτύσσει τα στρατεύματα της κατά μήκος των συνόρων της με την Ουκρανία. Οι επιθέσεις στον κυβερνοχώρο φαίνεται ότι στόχευαν στη συλλογή πληροφοριών στρατιωτικής και εξωτερικής πολιτικής και στην απόκτηση πρόσβασης σε κρίσιμες υποδομές, όπως οι πάροχοι υπηρεσιών ενέργειας και πληροφορικής.

Ακόμη, η Microsoft καταλήγει στο συμπέρασμα ότι *«οι καταστροφικές επιθέσεις σηματοδοτούν επικείμενη εισβολή»*. Σημείωσε επίσης, ότι η Ρωσία εξαπέλυσε το WhisperGate (που διαγράφει τους σκληρούς δίσκους και καθιστά τους υπολογιστές μη εκκινήσιμους) σε περιορισμένο αριθμό ουκρανικών κυβερνητικών συστημάτων και συστημάτων πληροφορικής όταν οι διπλωματικές συνομιλίες μεταξύ Ρωσίας, Ουκρανίας, ΝΑΤΟ και κρατών της ΕΕ απέτυχαν στις 13 Ιανουαρίου 2022, με την Ρωσία να προχωρά σε επιθέσεις άρνησης παροχής υπηρεσιών σε ιστότοπους της ουκρανικής κυβέρνησης. Την παραμονή του πολέμου στις 23 Φεβρουαρίου 2022, η GRU της Ρωσίας εξαπέλυσε το FoxBlade, σε εκατοντάδες ουκρανικά στρατιωτικά και κυβερνητικά δίκτυα ταυτόχρονα. Η

Microsoft παρατήρησε επίσης συνδέσεις μεταξύ συγκεκριμένων στρατιωτικών ενεργειών και κυβερνοεπιθέσεων. Για παράδειγμα, οι κυβερνοεπιθέσεις επικεντρώθηκαν γεωγραφικά γύρω από το Κίεβο και το Ντονμπάς και στόχευαν την εταιρεία πυρηνικής ενέργειας της Ουκρανίας την ίδια στιγμή που η Ρωσία κατέλαβε τον μεγαλύτερο πυρηνικό σταθμό της Ουκρανίας στη Ζαπορίζια. Κατά τη διάρκεια του πολέμου, οι επιθέσεις στον κυβερνοχώρο είναι πιο συχνές, πιο καταστροφικές και συντονίζονται με στρατιωτική δράση (Orenstein, 2022).

Διαπιστώνεται λοιπόν, ότι η Ρωσία αναπτύσσει κυβερνοεπιθέσεις ως προειδοποίηση ή απειλή, συχνά για να ενισχύσει διπλωματικές ενέργειες. Προς επίρρωση αυτού, στις 8 Απριλίου 2022, ενώ ο Πρόεδρος της Ουκρανίας Ζελένσκι έδωσε ομιλία στο φινλανδικό κοινοβούλιο, τα φινλανδικά υπουργεία Εξωτερικών και Άμυνας επλήγησαν από μια επίθεση άρνησης υπηρεσίας. Τα φινλανδικά κυβερνητικά συστήματα επανήλθαν σε μια ώρα, αλλά δεδομένων των συνθηκών, αυτή η κυβερνοεπίθεση φαίνεται να έχει σχεδιαστεί για να σηματοδοτήσει τη δυσαρέσκεια της Ρωσίας με τα σχέδια της Φινλανδίας να ενταχθεί στο ΝΑΤΟ και την υποστήριξή της στην Ουκρανία. Αυτή η επίθεση ενισχύθηκε από ρωσικές διπλωματικές δηλώσεις που προειδοποιούσαν τη Φινλανδία για *«δράσεις αντιποίνων»* λόγω της επικείμενης ένταξης στο ΝΑΤΟ. Η πράξη αυτή, αποτελεί μια από τις σημαντικότερες κυβερνοεπιθέσεις εναντίον της Φινλανδίας ή της Σουηδίας, τη στιγμή που σχεδίαζαν τις αιτήσεις τους για ένταξη στη συμμαχία.

Λαμβάνοντας υπόψη την κατάσταση στον κυβερνοχώρο της Ουκρανίας κατά τους πρώτους μήνες της ρωσικής εισβολής στην χώρα, ανάγονται κάποια συμπεράσματα (Smith, 2022). Πρώτον, υποστηρίζεται ότι η άμυνα έναντι μιας στρατιωτικής εισβολής απαιτεί για τις περισσότερες χώρες τη δυνατότητα να διανέμουν ψηφιακές λειτουργίες και στοιχεία δεδομένων πέρα από τα σύνορα τους και σε άλλες χώρες. Δεύτερον, οι πρόσφατες πρόοδοι στις πληροφορίες για τις απειλές στον κυβερνοχώρο και την προστασία τελικών σημείων βοήθησαν την Ουκρανία να αντέξει ένα υψηλό ποσοστό καταστροφικών ρωσικών κυβερνοεπιθέσεων. Τρίτον, καθώς ένας συνασπισμός χωρών έχει συγκεντρωθεί για να υπερασπιστεί την Ουκρανία, οι ρωσικές υπηρεσίες πληροφοριών έχουν εντείνει τη διείσδυση στο δίκτυο και τις δραστηριότητες συλλογής πληροφοριών με στόχο συμμαχικές κυβερνήσεις εκτός Ουκρανίας. Ακόμη, σε συντονισμό με άλλες δραστηριότητες στον κυβερνοχώρο, οι ρωσικές υπηρεσίες διεξάγουν παγκόσμιες επιχειρήσεις κυβερνοεπιρροής για να υποστηρίξουν τις πολεμικές τους προσπάθειες. Τέλος, διαπιστώνεται ότι τα διδάγματα από την περίπτωση της Ουκρανίας απαιτούν μια συντονισμένη και συνολική στρατηγική για την ενίσχυση της άμυνας ενάντια σε όλο το φάσμα των καταστροφικών επιχειρήσεων, συλλογής πληροφοριών και επιρροής στον κυβερνοχώρο.

Η Ουκρανία από την πλευρά της, προετοιμάζεται για απειλές στον κυβερνοχώρο που συνδέονται με τη σύγκρουση, με τη βοήθεια των συμμάχων της. Στις 26 Φεβρουαρίου 2022, ο αντιπρόεδρος της κυβέρνησης και υπουργός ψηφιακού μετασχηματισμού της Ουκρανίας, Mykhailo Fedorov ανακοίνωσε τη δημιουργία ενός στρατού πληροφορικής για την άμυνα έναντι των χάκερ. Επιπλέον, οι ΗΠΑ

παρείχαν χρηματοδότηση και την τεχνογνωσία της ΕΕ για την ενίσχυση της κυβερνοασφάλειας στην Ουκρανία. Εν τω μεταξύ, η Microsoft έχει δώσει πληροφορίες και αμυντικές συμβουλές σε Ουκρανούς αξιωματούχους σχετικά με πρόσφατες επιθέσεις στον κυβερνοχώρο σε μια σειρά στόχων, συμπεριλαμβανομένων των κυβερνητικών υπηρεσιών (Microsoft, 2022).

5. Συμπεράσματα

Έπειτα από εξέταση των δεδομένων, καθίσταται σαφές ότι ο κυβερνοχώρος καθώς και οι επιχειρήσεις που πραγματοποιούνται σε αυτόν, διαδραματίζουν ολοένα και αυξανόμενο ρόλο με την πάροδο των ετών τόσο σε περιόδους εντάσεων, όσο και σε περιόδους πολέμου. Η σύγχρονη ιστορία αποδεικνύει ότι η Ρωσία αξιοποιεί τις δυνατότητες που παρέχονται ηλεκτρονικά, ώστε να επιτύχει τους σκοπούς της. Παρόλα αυτά, διαπιστώνεται ότι στην περίπτωση της Ουκρανίας, οι παραβιάσεις δεν σημειώνονται σε κρίσιμες υποδομές όπως η διαθεσιμότητα του διαδικτύου, δεδομένου ότι η χώρα μέχρι στιγμής έχει σταθερή σύνδεση, εκτός από κάποιες πόλεις υπό έντονη πολιορκία. Ακόμη, καθίσταται εμφανές ότι ο πόλεμος αυτός, αν και στρατιωτικός, καλύπτει ένα ευρύ φάσμα τομέων, γεγονός που αιτιολογείται από την παρουσία δρώντων εκτός από τους πολιτικούς και τους μη πολιτικούς. Πιο συγκεκριμένα, σε αντίθεση με τα προηγούμενα χρόνια, στην πολεμική σύρραξη μεταξύ της Ρωσίας και της Ουκρανίας, σημαντική θέση καταλαμβάνουν οντότητες του ιδιωτικού τομέα, χωρίς ξεκάθαρη αποστολή προστασίας στον κυβερνοχώρο, όπως η Microsoft, η οποία εκδίδει εκθέσεις και παρέχει πληροφορίες σχετικά με τις κυβερνοεπιθέσεις που πραγματοποιούνται. Το γεγονός αυτό, καταδεικνύει ότι πλέον οι πόλεμοι είναι ποικιλόμορφοι και σύνθετοι λαμβάνοντας νέες διαστάσεις. Από την παραπάνω μελέτη, λοιπόν, προκύπτει ότι τόσο στην περίπτωση της Εσθονίας όσο και στην περίπτωση της Γεωργίας, πραγματοποιήθηκαν κυβερνοεπιθέσεις σε κρίσιμες υποδομές. Ειδικότερα, στην Εσθονία καταγράφηκαν σε ιστότοπους κυβερνητικών υπουργείων, μεγάλων τραπεζών, πολιτικών κομμάτων ακόμη και στη κρίσιμη οικονομική και πολιτική υποδομή της Εσθονίας. Σχετικά με την Γεωργία, παρατηρήθηκαν επιθέσεις DDoS που κατέστρεψαν την υποδομή πληροφοριών της Γεωργίας, διακόπτοντας τις κυβερνητικές επικοινωνίες και παραβιάζοντας κυβερνητικούς ιστότοπους ενώ, τράπεζες της Γεωργίας, εταιρείες μεταφορών και ιδιωτικοί πάροχοι τηλεπικοινωνιών δέχθηκαν επίσης επίθεση. Σε αντίθεση με αυτές τις δύο περιπτώσεις και όπως προκύπτει από τα συγκεκριμένα δεδομένα υπό εξέταση, η Ουκρανία έχει υποστεί σημαντικές κυβερνοεπιθέσεις κυρίως στο δίκτυο παροχής ηλεκτρικού ρεύματος (2015) και την επίθεση NotPetya (2017). Από την στιγμή της εισβολής της Ρωσίας (2022), σύμφωνα με τις εκθέσεις της Microsoft, σημειώθηκαν στην Ουκρανία καταστροφικές επιθέσεις, επιχειρήσεις συλλογής πληροφοριών ενώ οι ρωσικές στρατιωτικές δυνάμεις επιτίθονταν στη χώρα από ξηρά, αέρα και θάλασσα. Οι κυβερνοεπιθέσεις επιταχύνθηκαν αρκετά με το ξέσπασμα του πολέμου ενώ φάνηκε ότι οι επιθέσεις στον κυβερνοχώρο στόχευαν στη συλλογή πληροφοριών στρατιωτικής και εξωτερικής πολιτικής και στην απόκτηση πρόσβασης σε κρίσιμες υποδομές. Ωστόσο, παρατηρείται επίσης ότι, ενώ η Ουκρανία βρίσκεται σε εμπόλεμη κατάσταση, γενικά έχει σταθερή σύνδεση στο διαδίκτυο αλλά και σταθερή πρόσβαση στην παροχή ηλεκτρικού ρεύματος, εκτός από επιμέρους περιπτώσεις σχετικά με περιοχές που βρίσκονται υπό έντονη πολιορκία. Από το γεγονός αυτό, προκύπτει το συμπέρασμα ότι οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές εξαρτώνται και από άλλους παράγοντες. Πάντως και στις τρις περιπτώσεις σημειώθηκαν επιχειρήσεις στον κυβερνοχώρο με στόχο κρίσιμες υποδομές, συλλογή πληροφοριών και επιχειρήσεις επιρροής. Ακόμη, προκύπτει το

συμπέρασμα ότι θα πρέπει πλέον να αποδίδεται ιδιαίτερη σημασία στις επιχειρήσεις στον κυβερνοχώρο, αφού φαίνεται να αποτελούν τον προάγγελο των στρατιωτικών επιχειρήσεων ή να συνδυάζονται με αυτές.

5.1 Περαιτέρω Μελέτη

Από την ανωτέρω μελέτη προκύπτουν και άλλα πεδία έρευνας. Πιο συγκεκριμένα, θα μπορούσε να πραγματοποιηθεί λεπτομερής ανάλυση στο τεχνικό επίπεδο των επιχειρήσεων στον κυβερνοχώρο εξετάζοντας τι συμβαίνει συγκεκριμένα και ποιες μέθοδοι χρησιμοποιούνται. Επιπλέον, άξιο διερεύνησης θεωρείται το γεγονός ότι η Ρωσία μέχρι στιγμής, δεν έχει προβεί σε καταστροφικές επιθέσεις στις κρίσιμες υποδομές της Ουκρανίας.

5.2 Περιορισμοί

Τέλος, είναι απαραίτητο να επισημανθεί ότι λόγω γλωσσικού περιορισμού, δεν υπήρξε αξιοποίηση αμιγώς ρωσικών ή ουκρανικών πηγών, αλλά κυρίως αγγλικής βιβλιογραφίας. Επομένως, το ζήτημα διερευνήθηκε περισσότερο από την πλευρά της Δύσης. Ακόμη, δεδομένου ότι ο πόλεμος στην Ουκρανία είναι εν εξελίξει, απαιτεί συνεχή παρακολούθηση και συνεπάγεται εξελίξεις που ανά πάσα στιγμή μπορεί να μεταβάλλουν τα δεδομένα.

Βιβλιογραφία

Ξενόγλωσση

Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

Clarke, R., Knake, R. 2010. Cyberwar - The Next Threat to National Security and What to do about it, New York: HarperCollins Publishers.

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. https://timreview.ca/article/835 [Accessed 4 June 2022]

Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina .2022. Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? Journal of Cyber Policy, 7:1, 97-135, DOI: 10.1080/23738871.2022.2041061

Department of Defense (2001), "Dictionary of Military and Associated Terms", Amend. 2010, DoD, https://irp.fas.org/doddir/dod/jp1_02-april2010.pdf?fbclid=IwAR2OpJJb86P0g42uGOBrXiW_bVQn0ztK2xffcAdhyBu0JJ0Kq1fZxRFFZrU [Accessed 4 June 2022]

E-ISAC. 2016. TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. March 18. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [Accessed 7 June 2022]

FireEye. 2016. Cyber Attacks on the Ukrainian Grid: What You Should Now. FireEye Industry Intelligence Report. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf [Accessed 7 June 2022]

Greenberg, Andy. 2018. "The Untold Story of Not Petya, the Most Devastating Cyberattack in History." WIRED, August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 8 June 2022]

Hern, Alex. 2016. "Ukrainian blackout caused by hackers that attacked media company, researchers say." *The Guardian*, January 7. https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company [Accessed 10 June 2022]

Herzog, S. 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), 49–60. https://www.jstor.org/stable/26463926?seq=1 [Accessed 6 June 2022]

Hultquist, John. 2016. "Threat Research: Sandworm Team and the Ukrainian Power Authority Attacks." *FireEye Blog*, January 8. https://www.mandiant.com/resources/ukraine-and-sandworm-team [Accessed 9 June 2022]

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en [Accessed 7 June 2022]

Kemmerer, R. A. 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715.

Kovacs, Eduard. 2015. "Ukraine Accuses Russia of Hacking Power Companies." *Security Week*, December 30. https://www.securityweek.com/ukraine-accuses-russia-hacking-power-companies [Accessed 12 June 2022]

Lewis, J. A., 2015. 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine., Tallin: NATO CCD COE Publications.

Lin, H., 2010. Offensive Cyber Operations and the Use of Force. Journal of National Security Law and Policy, VOLUME 4(ISSUE 1). Available at: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf [Accessed 4 June 2022]

Markoff, J. 2008. "Before the Gunfire, Cyberattacks," NYT Online (12 August 2008), Available at: https://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 [Accessed 2 June 2022]

McLellan, Charles. 2016. "How hackers attacked Ukraine's power grid: Implications for Industrial IoT security." ZDNet, March 4. https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/ [Accessed 7 June 2022]

Nakashima, Ellen. 2016. "Russian hackers suspected in attack that blacked out parts of Ukraine." *The Washington Post*, January 5. https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html [Accessed 7 June 2022]

Newsweek. 2016. "U.S. Says Cyber Attack Caused Ukraine Power Outage." Newsweek, February 25 https://www.newsweek.com/ukraine-power-outage-cyber-attack-russia-putin-sandworm-430556 [Accessed 7 June 2022]

Orenstein, M., 2022. Russia's Use of Cyberattacks: Lessons from the Second Ukraine War, FPRI: Foreign Policy Research Institute https://policycommons.net/artifacts/2470242/russias-use-of-cyberattacks/3492222/ [Accessed 10 June 2022]

Ottis, R. 2008. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168.

Polityuk, Pavel. 2015. "Ukraine to probe suspected Russian cyber attack on grid." *Reuters*, December 31. https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231 [Accessed 8 June 2022]

Public Safety Canada. 2014. Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada.

R. A. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 705-715, DOI: 10.1109/ICSE.2003.1201257

Robin G. 2013. "Cyber Warfare: Implications for Non-international Armed Conflicts" vol. 89, no.627

Rõigas, Henry. 2018. “Cyber War in Perspective: Lessons from the Conflict in Ukraine.” In A Civil-Military Response to Hybrid Threats, edited by E. Cusumano, and M. Corbe, pp.233–257. London: Palgrave Macmillan.

Samarasekera, U., 2022. Cyber risks to Ukrainian and other health systems. THE LANCET Digital Health, 30 March, VOLUME 4(ISSUE 5), pp. 297-298.

Smith, B., 2022. Defending Ukraine: Early Lessons from the Cyber War, s.l.: Microsoft.

Starodubtsev, Y. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020). Cyberspace: Terminology, Properties, Problems of Operation. 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). DOI:10.1109/fareastcon50210.2020

Valuch, J., Hamulak, O. 2018. Cyber Operations During the Conflict in Ukraine and the Role of International Law. In: Sayapin, S., Tsybulenko, E. (eds) The Use of Force against Ukraine and International Law. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-222-4_10

Vogler, S. and Connell M., 2016. *Russia’s Approach to Cyber,* s.l.: Center for Naval Analyses.

Ελληνόγλωσση

Κολιόπουλος, Κ. 2010. *Η Στρατηγική Σκέψη από την Αρχαιότητα έως Σήμερα*. Εκδόσεις Ποιότητα.

Κονδύλης, Π. 2004. *Η Θωρία του Πολέμου*. Εκδόσεις Θεμέλιο.

Χανιώτης, Α. Κ. 2016. *Clausewitz-ιανή και Ελληνορθόδοξη προσέγγιση του πολέμου: συγκριτική ανάλυση και ενδεχόμενη σύνθεση*. Εκδόσεις Πάνδημος, Παντειακές Δημοσιεύσεις.