2024-01

þÿ « Ÿ Á Ì » ¿ Â Ä · Â º Å ² µ Á ½ ¿ Ç Î Á ¿ Å

þÿ À ¿ » - ¼ ¿ Å : Ÿ À Ì » µ ¼ ¿ Â ¡ É Ã ¯ ± Â

þÿ ± Ä - » · Â £ . , š É ½ Ã Ä ± ½ Ä ¯ ½ ¿ Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± ” ¹ µ ¸ ½ Î ½ £ Ç - Ã µ É ½ , £ Ä Á ± Ä · ³ ¹ º ® Â º ± ¹ ‘ Ã Æ ¬ » µ ¹ ± Á

þÿ š ¿ ¹ ½ É ½ ¹ º Î ½ • À ¹ Ã Ä · ¼ Î ½ , ¤ µ Ç ½ Î ½ º ± ¹ ‘ ½ ¸ Á É À ¹ Ã Ä ¹ º Î ½ £ À ¿ Å ´ Î ½ , ± ½ µ À ¹ Ã Ä ®

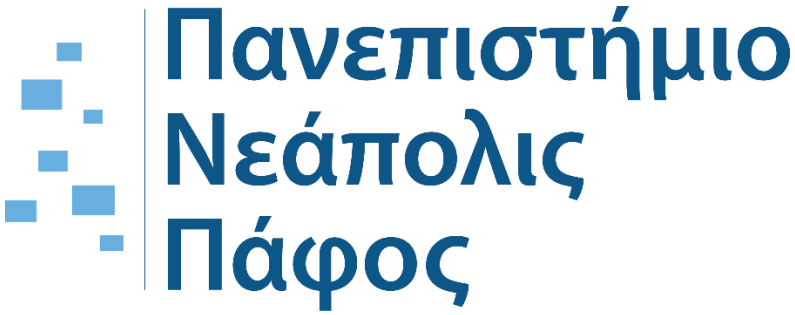
Πανεπιστήμιο Νεάπολις Πάφος

Σχολή: ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

«Ο ρόλος του κυβερνοχώρου ως πεδίο πολέμου: Ο πόλεμος Ρωσίας - Ουκρανίας»

Πατέλης Σ. Κωνσταντίνος

Ιανουάριος 2024



Σχολή: Κοινωνικών Επιστημών, Τεχνών και Ανθρωπιστικών Σπουδών

«Ο ρόλος της κυβερνοχώρου ως πεδίο πολέμου: Ο πόλεμος Ρωσίας - Ουκρανίας»

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση Μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις, Στρατηγική & Ασφάλεια στο Πανεπιστήμιο Νεάπολις Πάφος

Πατέλης Σ. Κωνσταντίνος

Ιανουάριος 2024

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος..... σ. iii

Περίληψη..... σ. iii

Λέξεις κλειδιά..... σ. iv

Abstract..... σ. iv

1. Εισαγωγή..... σ. 1

2. Ο Κυβερνοχώρος ως ένα πεδίο σύγκρουσης..... σ. 3

2.1 Τα χαρακτηριστικά του κυβερνοχώρου..... σ. 3

2.2 Η σημασία της κυβερνοπληροφόρησης..... σ. 7

2.3 Παραδείγματα διακρατικών συγκρούσεων στο κυβερνοχώρο..... σ. 12

3. Η Ρωσο-ουκρανική διένεξη στο κυβερνοχώρο..... σ. 16

3.1 Η χρησιμοποίηση του κυβερνοχώρου από την Ουκρανία και τη Ρωσία στο πλαίσιο της πολεμικής αντιπαράθεσής τους..... σ. 16

α) Οι επιβεβαιωμένες κυβερνοεπιθέσεις της Ουκρανίας εναντίον Ρωσικών κυβερνο-στόχων..... σ. 19

β) Οι επιβεβαιωμένες κυβερνοεπιθέσεις της Ρωσίας εναντίον Ουκρανικών κυβερνο-στόχων..... σ. 25

3.2 Η καθοριστικότητα του κυβερνοχώρου και των τεχνολογιών πληροφοριών και επικοινωνιών, για τη διεξαγωγή του πολέμου..... σ. 32

3.3 Ποια είναι τα μαθήματα που αντλούμε σε σχέση με αυτή τη μορφή πολέμου στον κυβερνοχώρο..... σ. 35

4. Συμπεράσματα..... σ. 40

5. Βιβλιογραφία - Πηγές Ξένες..... σ. 44

6. Βιβλιογραφία - Πηγές Ελληνικές..... σ. 44

7. Διαδικτυακές Πηγές..... σ. 44

Σελίδα Εγκυρότητας

Ονοματεπώνυμο Φοιτητή: Πατέλης Σ. Κωνσταντίνος

Τίτλος Διπλωματικής Εργασίας: «Ο ρόλος του κυβερνοχώρου ως πεδίο πολέμου: Ο πόλεμος Ρωσίας - Ουκρανίας».

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …… [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος) Ανδρέας Ν. Λιαρόπουλος [βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: Κωνσταντόπουλος Ιωάννης [βαθμίδα, υπογραφή] Μέλος Εξεταστικής Επιτροπής: Φλώρος Φλούρος [βαθμίδα, υπογραφή]

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Ο Πατέλης Κωνσταντίνος γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Ο ρόλος του κυβερνοχώρου ως πεδίο πολέμου: Ο πόλεμος Ρωσίας - Ουκρανίας», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο Δηλών

Πρόλογος

Η παρούσα διπλωματική εργασία είναι το αποτέλεσμα του ενδιαφέροντος μου για τις σύγχρονες πολιτικές εξελίξεις. Το μεταπτυχιακό αυτό πρόγραμμα μου έδωσε τις βάσεις για την περεταίρω εξέλιξή μου ως Υπεύθυνος Αξιωματικός Ασφαλείας του Ευρωπαϊκού προγράμματος ISPS των Βρυξελλών, ενώ ταυτόχρονα μου άλλαξε τον τρόπο με τον οποίο κατανοώ το σύνολο των διεργασιών που συνθέτουν την κοινωνία μας και τις νέες προκλήσεις που παρουσιάζονται σε γεωπολιτικό και στρατιωτικό επίπεδο. Παράλληλα, με την εισαγωγή στον κόσμο των Διεθνών Σχέσεων, της Στρατηγικής κι Ασφάλειας, μπόρεσα να διαμορφώσω μια καλύτερη εικόνα για τον τρόπο με τον οποίο μπορούν να αντιμετωπιστούν οι προκλήσεις που συνεχώς παρουσιάζονται. Όλα αυτά δε θα τα είχα καταφέρει χωρίς τη βοήθεια όλων των καθηγητών μου του προγράμματος του Πανεπιστημίου Νεάπολις/Πάφου-Κύπρου που τους ευχαριστώ όλους και ιδιαίτερα χωρίς τις πολύτιμες συμβουλές του επιβλέποντα καθηγητή μου Δρ. Λιαρόπουλου Αντρέα και των Καθηγητών συνεργατών του. Επίσης, θα ήθελα να ευχαριστήσω τη σύζυγό μου για τις πολύτιμες ώρες που της στέρησα και η οποία βρίσκεται πάντα δίπλα μου και με στηρίζει αλτρουιστικά σε ό,τι κι αν αποφασίσω, προσπαθώντας να επιτύχω έναν προσωπικό στόχο.

Περίληψη

Στις 24 Φεβρουαρίου 2022 η Ρωσία εισέβαλε στρατιωτικά στην Ουκρανία, παραβιάζοντας το χάρτη των Ηνωμένων Εθνών. Στον πόλεμο αυτό που διεξάγεται τα δύο τελευταία χρόνια και συνεχίζεται ακόμα, σημαντικό ρόλο έπαιξε ο κυβερνοχώρος ο οποίος αναδείχθηκε σε ένα νέο συμπληρωματικό πεδίο σύγκρουσης για τις αντιμαχόμενες πλευρές πέρα από την ξηρά, τη θάλασσα και τον αέρα. Μέσω του κυβερνοχώρου και της κυβερνοπληροφόρησης έγινε εφικτή η εφαρμογή στρατηγικής που αποσκοπούσε στην επικράτηση του ενός αντιπάλου εις βάρος του άλλου και βασίζονταν στον αιφνιδιασμό, την καταστροφή ή την προσωρινή βλάβη κρίσιμων υποδομών, στην υποκλοπή σημαντικών πληροφοριών και στη χειραγώγηση της κοινής γνώμης τόσο στο εσωτερικό των δύο συγκρουόμενων κρατών όσο και στο εξωτερικό.

Στόχος της παρούσας διπλωματικής εργασίας είναι, αφού αναφερθεί σύντομα το θεωρητικό μέρος του θέματος σύμφωνα με τη βιβλιογραφία, να αναδείξει πώς το νέο είδος απειλών που έκανε την εμφάνισή του στον παγκόσμιο χώρο τις τελευταίες δεκαετίες, αυτό της κυβερνοπληροφόρησης και των κυβερνοαπειλών, εφαρμόστηκε στον πόλεμο Ρωσίας-Ουκρανίας, ποιες ήταν οι επιπτώσεις και τα αποτελέσματά του μέχρι τώρα καθώς και ποια διδάγματα θα μπορούσαμε να αντλήσουμε από αυτό.

Η μεθοδολογία που ακολουθήσαμε στην εκπόνηση της παρούσας εργασίας αφορά στη μελέτη ακαδημαϊκών και διαδικτυακών πηγών και στηρίχτηκε ιδιαίτερα σε διαθέσιμα στο διαδίκτυο στοιχεία που καταγράφουν επιβεβαιωμένες κυβερνοεπιθέσεις μεταξύ των εμπόλεμων μερών αλλά και εναντίον άλλων χωρών που τις υποστηρίζουν.

Σύμφωνα με τις πηγές μας, φαίνεται ότι οι κυβερνοεπιθέσεις εφαρμόζονταν πολύ πριν την έναρξη του πολέμου και αποτελούν σημαντικό μέρος της προετοιμασίας μιας στρατιωτικής επέμβασης, ενώ στη διάρκεια του πολέμου αυτές επιδιώκουν να υποστηρίξουν φυσικές στρατιωτικές κινήσεις. Είναι σημαντικό να αναφέρουμε ότι στην περίπτωση του πολέμου που εξετάζουμε, οι κυβερνοεπιθέσεις αποτελούν καθημερινή πραγματικότητα και σ' αυτήν επιδίδονται συστηματικά τόσο η Μόσχα όσο και το Κίεβο μέχρι τις μέρες μας. Με βάση τα στοιχεία που συλλέξαμε καταλήξαμε στο συμπέρασμα ότι ενώ ο κυβερνοχώρος προσφέρει ένα ενδιαφέρον πεδίο σύγκρουσης και αποτελεί χρήσιμο εργαλείο εφαρμογής στρατηγικής, στην πραγματικότητα δεν μπορεί να αντικαταστήσει τις επιπτώσεις του πραγματικού πολέμου σε υλικό, πολιτικό, οικονομικό και ψυχολογικό επίπεδο. Οι κυβερνοεπιθέσεις και ιδιαίτερα η παραπληροφόρηση μέσω της κυβερνοπληροφόρησης επηρεάζουν ιδιαίτερα τον άμαχο πληθυσμό ο οποίος είναι πάντα ο μεγάλος χαμένος.

Πρέπει να αναφέρουμε ότι είναι πολύ νωρίς για να εξαχθούν οριστικά συμπεράσματα που σχετίζονται με τα αποτελέσματα της κυβερνοπληροφόρησης και του κυβερνοπολέμου κατά τη προετοιμασία και την εκτέλεση αυτού του είδους πολέμου στην Ουκρανία.

Λέξεις κλειδιά: Απειλή, Κυβερνοχώρος, Κυβερνοπόλεμος, Κυβερνοπληροφόρηση, ΤΠΕ (Τεχνολογίες Πληροφοριών Επικοινωνιών).

Abstract

On 24 February 2022, Russia invaded Ukraine militarily, in violation of the United Nations Charter. In this war, which has been waged for the last two years and is still going on, cyberspace has played an important role and has become a new complementary field of conflict for the warring sides beyond land, sea and air. Through cyberspace and cyber-information, it became possible to implement a strategy aimed at dominating one adversary at the expense of the other, based on surprise, the destruction or temporary damage of critical infrastructure, the interception of important information and the manipulation of public opinion both within the two conflicting states and abroad.

The aim of this thesis is, after briefly reviewing the theoretical part of the topic according to the literature, to highlight how the new type of threats that has emerged in the global arena in recent decades, that of cyber-information and cyber-threats, has been applied to the Russia-Ukraine war, what its impact and results have been so far, and what lessons could be learned from it. The methodology we followed in the preparation of this paper involves the study of academic and online sources and relied particularly on data available on the internet that document confirmed cyber-attacks between the warring parties and against other countries that support them.

According to our sources, it appears that cyber-attacks are implemented well before the start of war and are an important part of the preparation for a military intervention, while during war they seek to support physical military movements. It is important to note that in the case of the conflict under consideration, cyber-attacks are a daily reality and have been systematically engaged in by both Moscow and Kiev up to the present day. On the basis of the data we have collected, we will conclude that while cyberspace offers an interesting field of conflict and is a useful tool for implementing strategy, in reality it cannot replace the effects of real war on a material, political, economic and psychological level. Cyber-attacks and especially disinformation through cyber-information particularly affect the civilian population who are always the big losers.

It should be mentioned that it is too early to draw definitive conclusions related to the effects of cyber-information and cyber-warfare in the preparation and execution of this kind of war in Ukraine.

1. Εισαγωγή

Η παρούσα διπλωματική εργασία πραγματεύεται το ρόλο του κυβερνοχώρου ως πεδίο σύγκρουσης, της Ρωσικής εισβολής στην Ουκρανία. Ο πόλεμος μεταξύ των δύο κρατών, της Ρωσίας και της Ουκρανίας που ξέσπασε στις 24.02.2022 και συνεχίζεται μέχρι τις ημέρες μας, έχει πολύ μεγάλη σημασία επειδή διασαλεύει τη διεθνή έννομη τάξη υπονομεύοντας την ευρωπαϊκή και παγκόσμια άμυνα και ασφάλεια κι επισύροντας διεθνή ανησυχία. Η πόλεμος αυτός αποτελεί αντικείμενο έρευνας από τον επιστημονικό κλάδο των Διεθνών Σχέσεων καθώς αυτός παραβιάζει το χάρτη των Ηνωμένων Εθνών[1], συνιστώντας παραβίαση του Διεθνούς Δικαίου.

Στην παρούσα διπλωματική εργασία θα μελετήσουμε με ποιο τρόπο οι δύο δρώντες χρησιμοποίησαν την κυβερνοπληροφόρηση *(cyber information)* και τον κυβερνοπόλεμο *(cyber war)* στο πεδίο του κυβερνοχώρου *(cyberspace)* για να επιφέρουν πλήγματα ο ένας στον άλλον σε αυτή τους την πολεμική σύγκρουση ακόμη και πριν αυτή ξεκινήσει. Είναι η πρώτη φορά που η διεθνής κοινότητα παρακολουθεί σε πραγματικό χρόνο τη χρήση του κυβερνοχώρου ως πεδίου προετοιμασίας και συνοδείας πολεμικών ενεργειών επί του πεδίου.

Ο κυβερνοχώρος αποκτά ιδιαίτερη σημασία στην πολεμική σύγκρουση δύο κρατών λόγω των επιπτώσεων που μπορούν να επιφέρουν οι δράσεις σε αυτόν στις ζωές των απλών ανθρώπων πέρα από τη σημασία που προσλαμβάνει επιπλέον στο στρατιωτικό επίπεδο. Ο κυβερνοπόλεμος θεωρείται ότι είναι ένας «ασύμμετρος πόλεμος» λόγω της ανωνυμίας που αυτός μπορεί να προσφέρει στους φορείς των απειλών με συνέπεια να είναι δύσκολη η απόδοση ευθυνών. Όπως και ο πόλεμος με την παραδοσιακή του έννοια, αποσκοπούν και οι δύο στον αιφνιδιασμό του αντιπάλου κατά το δυνατόν, στην καταφορά πληγμάτων και σε όσο το δυνατόν μεγαλύτερο αρνητικό αντίκτυπο στον αντίπαλο. Παρόλα αυτά, ο ψηφιακός και ο πραγματικός πόλεμος διαφέρουν σημαντικά στην στρατηγική και την εκτέλεσή τους. Κάθε πόλεμος έχει πάντα μία αιτία και πολλές όμως αφορμές, είναι δηλαδή πολυπαραγοντικός.

Στην έρευνα που πραγματοποιήσαμε μελετήσαμε το ρόλο της πληροφόρησης στη διαδικτυακή της μορφή και την προσπάθεια της υπονόμευσης του αντιπάλου σε πολιτικό, οικονομικό, κοινωνικό, ψυχολογικό και στρατιωτικό επίπεδο μέσω του κυβερνοπολέμου.

[1]Duguin S. & Pavlova P., *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, p.4., στο: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf (δημοσιεύτηκε στις 04.09.2023).

Η μεθοδολογία που ακολουθήσαμε στην εκπόνηση της παρούσας εργασίας αφορά στη μελέτη ακαδημαϊκών και διαδικτυακών πηγών. Συγκεκριμένα η μελέτη μας στηρίχτηκε κυρίως σε ακαδημαϊκά συγγράμματα, στο πόρισμα της έκθεσης του Ευρωπαϊκού Κοινοβουλίου με ημερομηνία Σεπτέμβριος 2023 για το ρόλο του κυβερνοχώρου στο ρωσικό πόλεμο κατά της Ουκρανίας[2] και στα επίσημα ανακοινωμένα δεδομένα του Ινστιτούτου *Cyber Peace*[3] το οποίο έχει καταγράψει τις κυβερνοεπιθέσεις που πραγματοποιήθηκαν στη Ρωσία, την Ουκρανία και τις μη εμπλεκόμενες στη σύρραξη χώρες από την αρχή του πολέμου. Τα δεδομένα αυτά είναι διαθέσιμα στην πλατφόρμα *Cyber Attacks in Times of Conflict Platform #Ukraine*[4]. Στα στοιχεία που παρέχει σε τριμηνιαία βάση και είναι διαθέσιμα *on line* από το Ινστιτούτο *Cyber Peace,* αναφέρεται και το πόρισμα της έκθεσης του Ευρωπαϊκού Κοινοβουλίου στο οποίο προαναφερθήκαμε και επομένως αυτά αποτελούν αξιόπιστη και αναγνωρισμένη διαδικτυακή πηγή.

Η παρούσα διπλωματική εργασία διαρθρώνεται σε τέσσερα κεφάλαια. Αποτελείται από την εισαγωγή στο πρώτο κεφάλαιο, κατόπιν από το δεύτερο και τρίτο κεφάλαιο της κύριας ανάλυσης του θέματος που εξετάζουμε και από τα συμπεράσματα στο τέταρτο και τελευταίο κεφάλαιο.

Στο δεύτερο κεφάλαιο αφού δώσουμε τους απαραίτητους ορισμούς σύμφωνα με τη βιβλιογραφία, αναλύουμε τον κυβερνοχώρο *(cyberspace)* ως πεδίο σύγκρουσης, τον τρόπο που οι κυβερνοεπιθέσεις *(cyber attacks)* στοχεύουν να καταφέρουν πλήγματα στον αντίπαλο σε διαφορετικά επίπεδα, είτε πλήττοντας κρίσιμες υποδομές είτε με τη διάδοση ψεύτικων ειδήσεων *(fake news)* που έχουν στόχο την παραπληροφόρηση *(misinformation)* των στρατιωτικών επιτελείων του αντιπάλου, του άμαχου πληθυσμού και της διεθνούς κοινότητας. Στη συνέχεια αναφερόμαστε στα χαρακτηριστικά του κυβερνοχώρου και τα πλεονεκτήματα που αυτός παρουσιάζει για την πραγματοποίηση κυβερνοεπιθέσεων όπως είναι για παράδειγμα η ανωνυμία, η μη προβλεψιμότητα και η δυνατότητα πολλές φορές κακόβουλης δράσης χωρίς τιμωρία. Επίσης θα αναφερθούμε στη σημασία της κυβερνοπληροφόρησης και τον τρόπο που αυτή χρησιμοποιείται από τους δρώντες για την προώθηση των συμφερόντων τους, συμπεριλαμβάνοντας κι εκείνα τα στοιχεία που

[2] Duguin S. & Pavlova P., *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, όλη η έκθεση στο: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
[3] CyberPeace Institute, *«Cyber Attacks in Times of Conflict Platform # Ukraine»,* https://cyberconflicts.cyberpeaceinstitute.org/.
[4] Ό.π., *Cyber Dimensions of the Armed Conflict in Ukraine,* Quarterly Analysis Report - Q3 (July to September 2023) στο: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/ (δημοσιεύτηκε στις 21.12.2023).

προσδιορίζουν και καθορίζουν το κυβερνοέγκλημα. Τέλος, στο κεφάλαιο αυτό θα κάνουμε σύντομη αναφορά σε διακρατικές συγκρούσεις που παρατηρήθηκαν στον κυβερνοχώρο και σε άλλες χώρες πέρα από αυτές της Ρωσίας και της Ουκρανίας και αιφνιδίασαν τη διεθνή κοινότητα τα προηγούμενα χρόνια.

Στο τρίτο κεφάλαιο θα επικεντρωθούμε στο Ρωσο-ουκρανικό πόλεμο στον κυβερνοχώρο. Θα αναφερθούμε στο χρόνο έναρξης των επιβεβαιωμένων κυβερνοεπιθέσεων, τη μορφή που πήραν όλες τους και αναλυτικά στους στόχους που είχε η κάθε μία από αυτές όπως εκδηλώθηκαν από το κάθε κράτος ξεχωριστά. Θα μελετήσουμε το ρόλο που έπαιξαν οι τεχνολογίες πληροφοριών και τηλεπικοινωνιών στη διεξαγωγή του πολέμου και τη σημασία της κυβερνοπληροφόρησης. Τέλος θα προσπαθήσουμε να αντλήσουμε τα απαραίτητα μαθήματα από αυτή τη πολεμική αντιπαράθεση της Ρωσίας και της Ουκρανίας με βάση τα αποτελέσματα των κυβερνοεπιθέσεων μέχρι αυτή τη στιγμή και τα πιθανά διδάγματα που μπορούν να αντλήσουν τόσο οι δύο αντιμαχόμενες πλευρές όσο και οι εμπλεκόμενοι στους στρατιωτικούς σχεδιασμούς παγκοσμίως.

Ολοκληρώνοντας τη μελέτη μας στο τέταρτο κεφάλαιο θα αναφερθούμε στα συμπεράσματα που μπορούν να εξαχθούν από τα δεδομένα που εξετάσαμε σε σχέση με το πόλεμο μεταξύ της Μόσχας και του Κιέβου. Καθώς ο κυβερνοχώρος είναι πλέον αναγνωρισμένος τομέας στρατιωτικών επιχειρήσεων φαίνεται ότι θα παραμείνει τόπος αντιπαράθεσης μεταξύ αντιμαχόμενων πλευρών σε μελλοντικούς πολέμους ή και απλές συρράξεις αν και οι επιπτώσεις του φαίνεται ότι είναι περιορισμένες σε σχέση με τις επιχειρήσεις που πραγματοποιούνται σε πραγματικό πεδίο. Τονίζεται η σημασία του κυβερνοχώρου στην προετοιμασία του πολέμου και τη συλλογή πληροφοριών καθώς και η ανάγκη για συνεχή επαγρύπνηση και προετοιμασία των κρατών μέσω συμμαχιών και συνεργασίας με ιδιωτικές εταιρείες αιχμής της τεχνολογίας. Ο κυβερνοχώρος αποτελεί σήμερα το πλέον σύγχρονο μέσο άσκησης στρατηγικής επιρροής, πολιτικής και χειραγώγησης της κοινής γνώμης και ως τέτοιος αποτελεί απειλή για την εθνική ασφάλεια και ευημερία των κρατών.

2. Ο Κυβερνοχώρος ως ένα πεδίο σύγκρουσης

2.1. Τα χαρακτηριστικά του κυβερνοχώρου

Ως κυβερνοχώρος εννοείται το περιβάλλον που έχει προκύψει από τα δίκτυα των επικοινωνιών και τη χρήση των ηλεκτρονικών υπολογιστών και αποτελεί ένα παγκόσμιο δίκτυο όπου διασυνδέονται χρήστες, υπηρεσίες δημόσιες και ιδιωτικές μέσω του διαδικτύου.

Η σύνθετη λέξη κυβερνοχώρος αποτελείται πρώτον από την ελληνική λέξη «κυβερνώ[5]» η οποία υποδηλώνει εξουσία, διοίκηση, καθοδήγηση ατόμων ή υλικού και δεύτερον από τη λέξη «χώρος[6]» όπως αυτή εννοείται στη γλώσσα μας. Αυτή προσδιορίζει ένα πεδίο δράσης το οποίο αφορά στην περίπτωση που εξετάζουμε τη σύνδεση και τον έλεγχο των τηλεπικοινωνιακών δικτύων και το πλήθος των ψηφιακών δεδομένων που διακινούνται μέσα σε αυτά. Επομένως για την ύπαρξη του κυβερνοχώρου απαιτούνται δύο στοιχεία: η τεχνολογία και ο άνθρωπος και σ' αυτόν καταγράφεται το πλήθος των ανθρώπινων ενεργειών οι οποίες αντανακλούν στον ψηφιακό κόσμο το κοινωνικό και πολιτισμικό σύστημα της εποχής μας. Το βασικότερο σημείο αναφοράς του κυβερνοχώρου είναι ο ίδιος ο άνθρωπος που τον καθορίζει με τις πράξεις, τις λειτουργίες και τις ενέργειές του. Τα μηνύματα που ανταλλάσσουν οι χρήστες μέσω των Η/Υ, οι διαδικτυακές σελίδες *(web pages)* που επισκέπτονται ή ακόμη τα αρχεία που αποθηκεύουν στο διαδίκτυο/*Internet,* αποτελούν τμήμα του κυβερνοχώρου. Όλα τα παραπάνω είναι η ηλεκτρονική αποτύπωση ανθρώπινων σκέψεων ή πράξεων π.χ. μηνύματα, ημερολόγια, αρχεία, πληροφορίες, διευθύνσεις, απόρρητα έγγραφα κ.α. που περιλαμβάνουν αξιοποιήσιμα στοιχεία εκτός από τους δημιουργούς τους επίσης και από άλλους φορείς. Ο κυβερνοχώρος δεν έχει σύνορα ούτε όρια. Ο κυβερνοχώρος και το διαδίκτυο είναι ένας αλληλοσυνδεόμενος χώρος του παγκόσμιου δικτύου ηλεκτρονικών υπολογιστών που επιτυγχάνει προηγμένη δικτύωση πληροφορίας (*information networking)* και στηρίζεται σε τεχνολογίες όπως είναι α) οι οπτικές ίνες *(fiber optics), β*) η ασύρματη τεχνολογία *(wireless technology)* και γ) τα δορυφορικά συστήματα *(satellite systems).* Σε αυτόν, δεν υπάρχουν αποστάσεις και γεωγραφικές συντεταγμένες[7].

Η τεχνολογία, η δομή της κοινωνίας αλλά και το πολιτισμικό σύστημα, μεταλλάσσονται διαρκώς. Από τη μία μεριά εμφανίζονται καινοτομίες καθημερινά στο πεδίο της τεχνολογίας και από την άλλη η σχέση που διαμορφώνεται ανάμεσα στην ανθρώπινη κοινωνία και την τεχνολογία[8] εξελίσσονται κι αυτές διαρκώς. Ο κυβερνοχώρος και συγχρόνως ο όγκος της πληροφορίας που διακινείται εντός αυτού αυξάνεται συνεχώς, επηρεάζοντας πολλούς τομείς της καθημερινής ζωής των ανθρώπων. Ο κυβερνοχώρος διαμορφώνει ένα εικονικό πεδίο στο οποίο μπορεί να δρα ο άνθρωπος για να καλύπτει τις ψηφιακές ενέργειές του. Πέρα από την ανάγκη της ανθρώπινης επικοινωνίας που αυτός εξυπηρετεί, υπάρχει και η σκοτεινή πλευρά

[5] Λιαρόπουλος Α., *«Περί κυβερνοχώρου – Ερμηνεύοντας τον κυβερνοχώρο από τη σύνθεση στην εξήγηση»,* στο: Κυβερνοχώρος και Παγκόσμια Τάξη, Εκδόσεις: Παπαζήση, Αθήνα, 2023, σ.92.
[6] Ό.π., σ.99..
[7] Λιαρόπουλος Α., «*Παγκόσμια διακυβέρνηση του κυβερνοχώρου»,* : Α. Λιαρόπουλος & Α. Μποζίνης (επιμ.) , Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις, Εκδόσεις: Παπαζήση, Αθήνα (2022), σ.28.
[8] Λιαρόπουλος Α., Κυβερνοχώρος και Παγκόσμια Τάξη , σσ.73-74.

του. Στον κυβερνοχώρο βρίσκει πρόσβαση για να δράσει υπόγεια ένα διεθνές σύστημα με υπερεθνικό χαρακτήρα, κυρίως οργανωμένες ομάδες χάκερς[9], οι οποίοι με κακόβουλες επιθέσεις προσπαθούν να υπονομεύσουν την ισχύουσα τάξη και να προωθήσουν την ιδεολογία τους, δικά τους συμφέροντα ή άλλων κέντρων. Η διακυβέρνηση του κυβερνοχώρου συνδυάζει την τεχνολογία της προχωρημένης πληροφορικής επιστήμης των Η/Υ και των δικτύων τους και την κάθε μορφής επικοινωνία σε ένα ψηφιακό περιβάλλον πληροφορίας και πληροφόρησης. Μέσα σ' αυτόν είναι δυνατόν να πραγματοποιούνται από την μια μεριά κακόβουλες προσπάθειες υποκλοπής πολύτιμων πληροφοριών ή ακόμη να πραγματοποιείται προσπάθεια χειραγώγησης ή παραπλάνησης της κοινής γνώμης και από την άλλη να μεταφέρονται με ταχύτητα εμπιστευτικά κρυπτογραφημένα δεδομένα ή διαβαθμισμένες πληροφορίες που μπορούν να υποκλαπούν.

Ο κυβερνοχώρος αποτελεί έναν ιδιαίτερα ελκυστικό χώρο δράσης λόγω της ανωνυμίας[10] και τους διάφορους βαθμούς συγκάλυψης που αυτός προσφέρει σε σχέση με τον πραγματικό κόσμο, πράγμα που καθιστά την αντιμετώπιση των κακόβουλων ενεργειών δύσκολη υπόθεση για το διεθνές δίκαιο. Είναι γεγονός ότι στο διαδίκτυο οι χρήστες μπορούν επιτυχώς να εμφανίζονται με διαφορετική ταυτότητα ακόμα και όψη ή ακόμα και να δρουν ουσιαστικά αόρατοι για τους πολλούς. Αυτό συμβαίνει επειδή πολύ λίγα σημεία ή ακόμη πλευρές του κυβερνοχώρου, είναι αληθινά προσβάσιμα σε όσους δεν διαθέτουν τις απαραίτητες τεχνικές γνώσεις. Επομένως, το όνομα, το επάγγελμα, ή διάφορα επιπλέον κοινωνικά ή φυσικά γνωρίσματα του χρήστη μπορούν να φανερωθούν ή να καλυφθούν ανάλογα με την επιλογή του. Η δυνατότητα της κάλυψης της ταυτότητας και της δράσης χωρίς ίχνη που προσφέρει η τεχνολογία, δημιουργεί έναν ασφαλή χώρο μη απόδοσης ευθύνης[11], όπου ο εντοπισμός του δράστη, η σύλληψη και η τιμωρία του για τις κάθε είδους μή επιτρεπτές ενέργειες που επιχειρεί, καθίσταται εξαιρετικά δύσκολη υπόθεση. Οι κακόβουλες ψηφιακές ενέργειες και η έλλειψη αποδείξεων οφείλονται στο γεγονός ότι αυτές μπορούν να γίνονται από οποιοδήποτε μέρος του πλανήτη και να ακολουθούν πολύπλοκες ψηφιακές διαδρομές, ο εντοπισμός των οποίων απαιτεί εξειδικευμένο λογισμικό και επίσης προηγμένη τεχνολογία.

Ο κυβερνοχώρος είναι σκοτεινός επειδή οι δρώντες μπορούν να παραμείνουν καλά κρυμμένοι και οι χρήστες δεν γνωρίζουν τα κίνητρα πίσω από το περιεχόμενό του.

---

[9] Βιολάκης Π., *Κυβερνοεπιθέσεις, κυβερνοεξαναγκασμός και απόδοση ευθύνης στον κυβερνοχώρο»,* στο: Α. Λιαρόπουλος & Α. Μποζίνης (επιμ.) , Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις, Εκδόσεις: Παπαζήση, Αθήνα (2022), σ.180.

[10] Ζαμπατή Μ., & Κοντραφούρη Χ., *«Οι Κυβερνοεπιθέσεις στις διακρατικές συγκρούσεις»,* στο: Α. Λιαρόπουλος & Α. Μποζίνης (επιμ.), Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις, Εκδόσεις: Παπαζήση, Αθήνα (2022), σ.133.

[11] Βιολάκης Π., σ.181.

Για παράδειγμα οι χρήστες δεν γνωρίζουν σε βάθος τους σκοπούς του κάθε προμηθευτή υπηρεσιών του διαδικτύου/Internet *(ISP – Internet Service Provider) Vodafone-Cosmote κ.α,* ή τι ακριβώς μπορεί να αντιπροσωπεύει το κάθε ηλεκτρονικό κατάστημα που μαζεύουν τα προσωπικά δεδομένα των χρηστών. Ακόμη περισσότερο οι χρήστες του διαδικτύου δεν μπορούν να γνωρίζουν με ακρίβεια πού αποσκοπεί ο κάθε διαδικτυακός τόπος/ιστοσελίδα *(Website)* όπου καταγράφονται συνέχεια μέσα στα αρχεία (*log files)* που διαθέτουν οι ιστοσελίδες, όλες εκείνες οι πληροφορίες που αφορούν τις κινήσεις που πραγματοποιούνται στο δίκτυό τους, γνωρίζοντας αυτοί μόνο σε ποιες βάσεις δεδομένων τους καταχωρούνται και ταξινομούνται και ακόμη ποια θα είναι η χρήση τους.

Το νέο αυτό πεδίο που ονομάζεται κυβερνοχώρος διαθέτει μεγάλη δύναμη λόγω της διείσδυσης που έχει στον πληθυσμό (υπολογίζεται ότι το 2022 το 64% του παγκόσμιου πληθυσμού είχε πρόσβαση στο διαδίκτυο[12]) και της επιρροής που εξασκεί πάνω στους χρήστες . Η ύπαρξη σύνδεσης στο διαδίκτυο, η απώλεια της πρόσβασης και το αίσθημα της στέρησης που αυτή δημιουργεί, η ταχύτητα της διάδοσης της πληροφορίας και η δύναμη της εικόνας, όλα τα παραπάνω μπορούν να χρησιμοποιηθούν για την εξυπηρέτηση συμφερόντων σε περιόδους ειρήνης αλλά και για πολεμικούς σκοπούς, επομένως ο κυβερνοχώρος προσφέρεται επιπλέον ως πεδίο σύγκρουσης και εφαρμογής πολεμικής τακτικής κι ως στρατηγικής. Αξίζει να σημειωθεί ότι ο κυβερνοχώρος έχει αναγνωριστεί επίσημα από τον Οργανισμό του Βορειοατλαντικού Συμφώνου (NATO) ως τομέας στρατιωτικών επιχειρήσεων από το 2016[13]. Ο πόλεμος σε αυτή την περίπτωση μεταφέρεται από τον πραγματικό στον εικονικό κόσμο του διαδικτύου και εφαρμόζεται στρατηγικά με κυβερνοεπιθέσεις (*cyber attacks).* Σύμφωνα με τον ορισμό που παρέχει ο Κανόνας 92 του Ταλλίν 2.0. «*Κυβερνοεπίθεση είναι μια επιχείρηση, αμυντική ή επιθετική, η οποία εύλογα αναμένεται να προκαλέσει είτε τραυματισμό ή θάνατο ανθρώπων, είτε ζημιά ή καταστροφή υλικής υποδομής*»[14].

Οι κυβερνοεπιθέσεις επομένως αποτελούν στοχευμένες και καλά προετοιμασμένες κακόβουλες ενέργειες που έχουν σκοπό να πλήξουν καίρια τον αντίπαλο και να προκαλέσουν χάος, καταστροφή κρίσιμων υποδομών και να χειραγωγήσουν την κοινή γνώμη. Ο πόλεμος στον κυβερνοχώρο δεν μπορεί να σκοτώσει και να καταστρέψει υλικές υποδομές και

[12] Λιαρόπουλος, Α. & Μποζίνης Α., σ.22.
[13] Duguin S. & Pavlova P., p.18.
[14] Τσιριγώτης Α.Α., «*Κυβερνοεπιθέσεις: Ορίζοντας τα νέα όπλα»,* στο: Α. Λιαρόπουλος & Α. Μποζίνης (επιμ.) *Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις,* Εκδόσεις: Παπαζήση, Αθήνα (2022), σ.160.

προπαντός δεν μπορεί να καταλάβει εδάφη[15] είναι όμως ικανός να προκαλέσει βλάβη. Η ακτίνα επιρροής του και τα αποτελέσματά του είναι λιγότερο προβλέψιμα, ίσως και λιγότερο αποτελεσματικά, σε σχέση με εκείνα της αντιπαράθεσης στρατευμάτων στο πραγματικό πεδίο της μάχης. Οι κυβερνοεπιθέσεις όμως μπορούν να χρησιμοποιηθούν με μεγάλη επιτυχία για να προετοιμάσουν το έδαφος πριν τον πόλεμο ή επίσης να συνοδεύσουν στρατιωτικές επιχειρήσεις, αυξάνοντας τον αντίκτυπο της επίθεσης. Επομένως αποτελούν ένα νέο τύπο στρατιωτικής επιχείρησης που μπορεί να προηγείται ή να συντονίζει τις στρατιωτικές επιχειρήσεις, επί του πεδίου. Αυτός ο συνδυασμός έχει αποδιοργανωτικό και συγχρόνως αποσταθεροποιητικό χαρακτήρα[16] και στοχεύει εκτός από το να πλήξει κρίσιμες υποδομές και στο να επηρεάσει ψυχολογικά τον άμαχο πληθυσμό κυρίως με όχημα τη διασπορά ψευδών πληροφοριών[17].

2.2 Η σημασία της κυβερνοπληροφόρησης

Η πληροφορία αποτελεί αναπόσπαστο μέρος της ανθρώπινης επικοινωνίας και σύμφωνα με τον Mark Lowenthal[18] αφορά «οτιδήποτε μπορεί να καταστεί γνωστό». Η πληροφορία θεωρείται ότι αποτελεί μορφή και πηγή μεγάλης ισχύος, οπότε θα μπορούσε να είναι και να χρησιμοποιηθεί ως ένα είδος όπλου. Από τη συλλογή και ειδικά από την επεξεργασία της πληροφορίας προκύπτει η πληροφόρηση η οποία είναι υποσύνολό της καθώς περιλαμβάνει μόνο την υποκειμενικά χρήσιμη και αξιοποιήσιμη πληροφορία που έχει συλλεχθεί για να καλύψει συγκεκριμένες υπάρχουσες ανάγκες[19]. Οι πληροφορίες μπορούν να αποδιοργανώσουν τη διακυβέρνηση ενός αντίπαλου συστήματος παραπλανώντας τους αντιπάλους και μειώνοντας τη θέλησή τους για να αντισταθούν. Η πορεία των γεγονότων σε διεθνή κλίμακα χαρακτηρίζεται από μία προσπάθεια ελέγχου όχι μόνο του περιεχομένου αλλά και της συνεχούς ροής των πληροφοριών. Η πληροφοριακή υπεροχή στον κυβερνοχώρο αποτελεί ουσιαστικό στόχο για όλα τα κράτη. Εν ολίγοις η παραδοσιακή μορφή του πολέμου έχει αλλάξει στην εποχή του διαδικτύου.

---

[15] Levite A,E, *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict*, στο: https://carnegieendowment.org/files/Levite_Ukraine_Cyber_War.pdf p.10, (δημοσιεύτηκε στις 18.04.2023).
[16] Duguin S. & Pavlova P., p.6.
[17] Ό.π., pp 8-9.
[18] Κωνσταντόπουλος Ι., *«Πληροφόρηση και Ασφάλεια: Μια άρρηκτη σχέση»,* Τμήμα Οικονομικών Επιστημών, με κείμενα στην Οικονομική της Άμυνας & της Ασφάλειας, Πανεπιστημιακές Εκδόσεις: Θεσσαλίας, 2018, σ.7.
[19] Ό.π.

Από την πληροφόρηση προκύπτει η απαραίτητη γνώση *(knowledge)* η οποία προσφέρει στον κάτοχό της υπεροχή και ισχύ[20]. Επομένως η γνώση θεωρείται ο κατ' εξοχήν πολλαπλασιαστής ισχύος. Η πληροφόρηση *(intelligence)* υπήρχε και πριν τη χρήση του διαδικτύου και αποτελούσε αποτελεσματικό εργαλείο μυστικής δράσης για τις κυβερνητικές υπηρεσίες πληροφοριών αλλά και για πολεμικούς σκοπούς. Η πληροφόρηση είναι φορέας της ιδεολογικής, πολιτισμικής και πολιτικής προσέγγισης της εποχής της. Μετά την εμφάνιση του κυβερνοχώρου η κυβερνοπληροφόρηση *(cyber intelligence)* εξακολουθεί να παρέχει τις απαραίτητες πληροφορίες για αμυντικούς και επιθετικούς σκοπούς στους ενδιαφερόμενους και περιλαμβάνει όλα τα χαρακτηριστικά της πληροφόρησης που αυτοί χρειάζονται. Η κυβερνοπληροφόρηση έχει μεγάλη σημασία για την εθνική ασφάλεια κάθε κράτους.

Η έννοια της ασφάλειας είναι στενά συνδεδεμένη με την ελευθερία από απειλές που αποτελούν κίνδυνο για την επιβίωση κάθε κράτους[21]. Τα κράτη επιδιώκουν την ευημερία, την ανεξαρτησία και το πολιτικό κύρος και γόητρο[22]. Επομένως ένα κράτος είναι ασφαλές όταν δεν είναι ευάλωτο σε απειλές και όταν είναι σε θέση να εξασφαλίσει την υπεροχή σε μία σύρραξη όταν αυτό απειληθεί. Για κάποια κράτη είναι επίσης στόχος να επεκτείνουν την κυριαρχία τους εφόσον οι εθνικές και οι διεθνείς συνθήκες το επιτρέψουν. Το μέσο για να αποκτήσουν τα κράτη τη γνώση για πιθανές απειλές είναι η συγκέντρωση πληροφοριών. Αυτό σημαίνει ότι τα κράτη επιδιώκουν να συλλέξουν πληροφορίες που αφορούν τις προθέσεις ή τις δραστηριότητες ξένων κυβερνήσεων, ή των υπηρεσιών τους, επίσης ξένων οργανώσεων ή ιδιωτών[23] που μπορούν να υπονομεύσουν την ασφάλεια ή την ελευθερία τους. Επομένως τα κράτη προσπαθούν να γνωρίσουν όσο το δυνατόν περισσότερα σχετικά με τον πιθανό ή τους πιθανούς εχθρούς και αντιπάλους τους ώστε να λάβουν τις απαραίτητες αποφάσεις για να προχωρήσουν στις ανάλογες δράσεις ή τη χάραξη πολιτικής. Το ρόλο της συλλογής των πληροφοριών έχουν κυρίως οι μυστικές υπηρεσίες κάθε κράτους.

Η ύπαρξη του διαδικτύου έκανε ευκολότερη την πρόσβαση στην πληροφορία και την πληροφόρηση, επομένως στην κυβερνοπληροφόρηση. Από το πλήθος των διαθέσιμων πληροφοριών στον κυβερνοχώρο οι μυστικές υπηρεσίες επιδιώκουν να συλλέξουν πληροφορίες οι οποίες έχουν σαν στόχο να αποφύγουν τον αιφνιδιασμό, να προλάβουν ή να

---

[20] Κωνσταντόπουλος Ι., *«Οικονομία και Κατασκοπεία, Θεωρία και Πράξη», «4.2 Ακαδημαϊκή ενασχόληση στην Ελλάδα και στο εξωτερικό με τις σπουδές σχετικά με την πληροφόρηση (Intelligence Studies)»*, Εκδόσεις: Ποιότητα, Αθήνα, 2010, σσ.199 & 202.

[21] Κωνσταντόπουλος Ι., *«Πληροφόρηση και Ασφάλεια: Μια άρρηκτη σχέση»,* Αθήνα, 2018, σ.3.

[22] Ό.π.

[23]Warner, M. , *Official Solutions,* στο: "Wanted: A Definition of Intelligence", *Studies in Intelligence,* Vol. 46, No. 3., pp 2-3, στο: https://www.cia.gov/static/72b2d4c0d01e4e05c60ff7d37fdd68b1/Wanted-Definition-of-Intel.pdf (δημοσιεύτηκε το 2002).

εξουδετερώσουν εχθρικές ενέργειες που μπορούν να απειλήσουν την εθνική ασφάλεια από εσωτερικές και εξωτερικές δυνάμεις (όπως π.χ. ύποπτες κινήσεις και τρομοκρατικές ενέργειες ή του οργανωμένου εγκλήματος). Οι μυστικές υπηρεσίες των κρατών προσπαθούν παράλληλα να παρέχουν την απαραίτητη γνώση στους υπεύθυνους για τη σωστή εκτίμηση του εθνικού και διεθνούς περιβάλλοντος για τη λήψη των κατάλληλων αποφάσεων και την προστασία των κρατικών ευαίσθητων πληροφοριών από την υποκλοπή τους από τις ξένες μυστικές υπηρεσίες[24]. Η συλλογή των πληροφοριών στον κυβερνοχώρο όπως και στον πραγματικό κόσμο είναι μια δύσκολη διαδικασία λόγω του πλήθους της διαθέσιμης πληροφορίας και της προστασίας που αυτή διαθέτει από τους κατόχους της.

Η υποκλοπή των πληροφοριών στον κυβερνοχώρο απαιτεί ειδική ανώτερη τεχνολογία, εξειδικευμένους χρήστες και προϋποθέτει μυστικότητα όπως και στον πραγματικό κόσμο. Μυστικότητα για να καλυφθούν τα ίχνη της υποκλοπής όταν αυτή συμβεί αλλά και γιατί οι πληροφορίες που συλλέχθηκαν δεν πρέπει να είναι διαθέσιμες στους πολλούς. Στην πραγματικότητα στον κυβερνοχώρο πραγματοποιείται ένας μυστικός πόλεμος μεταξύ των κρατών για την εξασφάλιση της κρίσιμης πληροφορίας όσο το δυνατόν πιο έγκαιρα. Αυτή χρησιμοποιείται για τη διαμόρφωση της εξωτερικής πολιτικής και τη διεξαγωγή μυστικών αποστολών ή κυβερνοεπιθέσεων για την εξασφάλιση της εθνικής ασφάλειας ή για τη σωστότερη εφαρμογή της εξωτερικής πολιτικής[25]. Στις μέρες μας κάθε κράτος μπορεί να επιλέξει το είδος των πληροφοριών που θα διαρρεύσει στον κυβερνοχώρο ανάλογα με τα συμφέροντά που το ίδιο έχει. Τα μέσα και οι πλατφόρμες της κοινωνικής δικτύωσης *(Social Media)* όπως είναι για παράδειγμα το *Facebook,* το *Twitter,* το *Tik Tok*, το *YouTube* και άλλα που συγκεντρώνουν το ενδιαφέρον των χρηστών, αποτελούν το καλύτερο όχημα για τη διασπορά ψευδών ειδήσεων, την παραπληροφόρηση και την προπαγάνδα. Η παραπληροφόρηση ή η προπαγάνδα έχουν σκοπό τη διάδοση και την κυκλοφορία ψευδών πληροφοριών για να περιορίσουν, να κρύψουν ή να εμποδίσουν την πρόσβαση του πληθυσμού σε έγκυρη, αξιόπιστη και επίσημη πληροφόρηση ώστε να δημιουργηθεί σκόπιμα σύγχυση και να μην αποκαλυφθεί η αλήθεια.

Οι φορείς της παραπληροφόρησης προσπαθούν είτε να επηρεάσουν τις πληροφορίες που κυκλοφορούν μέσω των επίσημων μέσων ενημέρωσης, αλλοιώνοντας ιστοτόπους ή αλλοιώνοντας κακόβουλα τις πληροφορίες μέσω κυβερνοεπιθέσεων για τη διάδοση πληροφοριών σύμφωνα με τα συμφέροντά τους και τον επηρεασμό της κοινής γνώμης.

[24] Κωνσταντόπουλος Ι., *«Πληροφόρηση και Ασφάλεια: Μια άρρηκτη σχέση»,* Αθήνα, 2018, σ.12.
[25] Warner, M., *The Missing Ingredient,* p.8.

Όλα αυτά είναι αντίθετα με την έννομη τάξη και το διεθνές δίκαιο[26]. Τα κράτη σήμερα με τον τρόπο που τα δεδομένα ψηφιοποιούνται και εντάσσονται σε ένα πολύ γρήγορο σύστημα από ψηφιακά στοιχεία (*data)* του μηδέν (0) και του ένα (1), έχουν να αντιμετωπίσουν τις εμφανιζόμενες κολεκτίβες χακτιβιστών, όπως αποδείχτηκε και στον πόλεμο μεταξύ της Ρωσίας και της Ουκρανίας. Οι ενέργειες των χακτιβιστών που πραγματοποιήθηκαν αγγίζουν τα όρια της εγκληματικής ενέργειας και οι κυβερνοεπιθέσεις επίσης τα όρια του κυβερνοεγκλήματος[27].

Ως εγκληματική πράξη ορίζεται η παραβίαση του ποινικού δικαίου το δε κυβερνοέγκλημα αφορά τις κακόβουλες ενέργειες στον κυβερνοχώρο που εμφανίζονται με παραβατικές συμπεριφορές που έχουν σχέση με τους Η/Υ. Θα μπορούσαμε επομένως να ορίσουμε ότι ως κυβερνοέγκλημα θεωρείται μία μεθοδική εγκληματική και επομένως παράνομη δραστηριότητα που χρησιμοποιεί τους Η/Υ ως εργαλεία[28] για τους σκοπούς που επιδιώκει να επιτύχει. Ως παράνομη δραστηριότητα επίσης, θα οριζόταν αυτή η οποία ενώ δεν έχει καμία εξουσιοδότηση για πρόσβαση σε ηλεκτρονικούς μεμονωμένους υπολογιστές ή ακόμη και σε πιο περίπλοκα συστήματα υπολογιστών, αυτή προσπερνά τα εμπόδια των ηλεκτρονικών τοίχων προστασίας (*firewalls)* που παρεμβάλλονται και επιτυγχάνει να εισχωρεί εντός των υπολογιστικών συστημάτων, υποκλέπτοντας πληροφορίες που θεωρεί απαραίτητες. Από τις πιο συνηθισμένες μορφές κακόβουλης επίθεσης είναι η εισαγωγή ιού-σκουληκιού *(warm)* σε κάποιο λογισμικό με στόχο να δώσει απομακρυσμένη πρόσβαση στον φορέα της απειλής ο οποίος αποκτά τον έλεγχο του υπολογιστικού συστήματος του θύματος[29]. Επίσης η κυβερνοεπίθεση μπορεί να εκδηλώνεται με *web jacking*[30] και *data jacking*[31], και να δημιουργεί επιθέσεις τύπου Δούρειου Ίππου (*Trojan Horse)*. Επιπλέον η κακόβουλη ενέργεια φθείρει τμήματα υπολογιστικών μονάδων, ή ακόμη καταστρέφει ολοκληρωτικά υπολογιστές κ.α. Επομένως στο πέρασμα του χρόνου θα λέγαμε ότι το κυβερνοέγκλημα επωάζεται στο σκοτεινό διαδίκτυο και αναπτύσσεται με ταχύτητα και σε εύρος που ξεπερνάει σύνορα και συμμαχίες.

Αναμφισβήτητα το κυβερνοέγκλημα λογαριάζεται ως ένα πρόβλημα παγκόσμιο και κατηγοριοποιείται σε διαδικτυακά εγκλήματα, σε παράνομο διαδικτυακό περιεχόμενο και σε

[26] Duguin S. & Pavlova P., p.14.
[27] Μουστάκης Φ., *«Κυβερνοέγκλημα και Ασφάλεια στο Διαδίκτυο»,* στο: Α. Λιαρόπουλος & Α. Μποζίνης σσ.236-239.
[28] Ό.π., σσ.235-243.
[29] Ζαμπατή Μ., & Κοντραφούρη Χ, σ.116.
[30] Λιαρόπουλος Α. & Μποζίνης Αθ., σ.239.
[31] Ό.π., Data diddling είναι οι μεταβολές δεδομένων τροφοδότησης και στοχοποίησης υπολογιστών για διάπραξη απάτης, σ.239.

απάτη στον κυβερνοχώρο. Για παράδειγμα έχουμε το ηλεκτρονικό ψάρεμα (*phishing),* όπως είναι η υποκλοπή κωδικών για πρόσβαση σε τραπεζικούς λογαριασμούς τρίτων. Σε αυτή την περίπτωση παρατηρείται παραβίαση της ιδιωτικότητας με άμεσο αποτέλεσμα την εμφάνιση θυμάτων στο διαδίκτυο[32]. Ακόμη στο κυβερνοέγκλημα ανήκει και η υποκλοπή ταυτοτήτων, το *(spamming)* δηλαδή η ανεπιθύμητη αλληλογραφία μαζικής κι αδιάκριτης αποστολής ηλεκτρονικών μηνυμάτων (*e-mails)* όπως επίσης και το κακόβουλο λογισμικό. Όλα τα κυβερνοεγκλήματα, οι διαδικτυακές απάτες ακόμη και οι παρενοχλήσεις ανηλίκων που πραγματοποιούνται διαμέσου των ηλεκτρονικών υπολογιστών, η διαχείριση επίσης δικτύων προγραμμάτων ρομπότ *(botnet management),* η πώληση προσωπικών και οικονομικών δεδομένων, παράγουν μία ρητορική μίσους. Είναι γεγονός ότι ο κυβερνοχώρος παραμένει χαώδης, χωρίς σαφήνεια, επομένως ανεξέλεγκτος άρα και επικίνδυνα σκιώδης.

Το κυβερνοέγκλημα σχετίζεται επίσης με κακόβουλες επιθέσεις οι οποίες στοχεύουν και δημιουργούν τρωτότητες σε υπάρχοντες τακτικούς σημαντικούς κυβερνητικούς τομείς ή μη. Αυτοί οι τομείς για παράδειγμα, μπορούν να είναι κρίσιμες υποδομές όπως οι μονάδες παραγωγής ενέργειας όλων των τύπων δηλαδή (ηλεκτρικής, κινητικής, δυναμικής, πυρηνικής, υδροδότησης, θερμικής, φυσικού αερίου, ανανεώσιμων πηγών ενέργειας, ακόμη τα δίκτυα μεταφορών και καθοδήγησης συρμών ή επιπλέον κυβερνητικές δομές όπως είναι τα Υπουργεία, οι διάφορες Υπηρεσίες, περεταίρω τα συστήματα Πληροφορίας ή καθοδήγησης συμβάντων) κ.α. τα οποία θα δούμε σε εφαρμογή πιο συγκεκριμένα στον πόλεμο Ρωσίας-Ουκρανίας που θα περιγράψουμε πιο κάτω. Η εξάπλωση της παραπληροφόρησης και της προπαγάνδας μέσω επιθέσεων στον τομέα των μέσων πληροφόρησης είναι αποσταθεροποιητική και υπονομεύει την εμπιστοσύνη του κοινού στους θεσμούς και στην εξυπηρέτηση της αλήθειας από αυτούς[33].

Ο τομέας του κυβερνοχώρου έχει κάνει δυνατή τη διασπορά της παραπληροφόρησης με μεγάλη ταχύτητα και σε πρωτοφανή κλίμακα. Τα πιο γνωστά μέσα που χρησιμοποιούνται για την εξαπόλυση κυβερνοεπιθέσεων σε διακρατικό επίπεδο είναι κυρίως αυτά που αναφέρονται παρακάτω:[34]

α) η αποστολή κακόβουλου λογισμικού *(malware)* που προκαλεί βλάβες σε Η/Υ και δίκτυα β) το λυτρισμικό (*ransomware)* που αφορά την κρυπτογράφηση δεδομένων και την παρεμπόδιση στην πρόσβαση των χρηστών στα δικτυακά ψηφιακά δεδομένα τους έως ότου να καταβληθούν λύτρα από αυτούς γ) η κατανεμημένη άρνηση υπηρεσίας *(Distributed denial*

[32] Λιαρόπουλος Α. & Μποζίνης Αθ., σσ.237-242.
[33] Ζαμπατή Μ., & Κοντραφούρη Χ, σσ.112-116.
[34] Ό.π.

of service) - DDoS), η οποία αναγκάζει τον ιστότοπο που έχει στοχοποιηθεί, να σταματήσει τη λειτουργία του μέσω υπερφόρτωσης με βλαβερά και άχρηστα δεδομένα που προκαλούν βλάβες και δ) διαδικτυακές επιθέσεις με εξαπάτηση θυμάτων και διακοπή υπηρεσιών ως μέσο απειλής[35] για τον πληθυσμό και ακόμη περισσότερο για τις κρατικές υπηρεσίες.

2.3 Παραδείγματα διακρατικών συγκρούσεων στον κυβερνοχώρο

Στη διεθνή βιβλιογραφία έχουν καταγραφεί πολλά περιστατικά διακρατικής σύγκρουσης στον κυβερνοχώρο, επιθέσεις σε κρίσιμες υποδομές και σε αμυντικά συστήματα με κακόβουλα λογισμικά όπως το *malware* όπου παρατηρούνται βλάβες σε συσκευές και δίκτυα. Έχουμε για παράδειγμα την επιχείρηση *Stuxnet* το 2010, η οποία αποτελεί την πρώτη κυβερνοεπίθεση που χρησιμοποιήθηκε για να προκαλέσει φυσική καταστροφή[36]. Το *Stuxnet* ήταν ένα κακόβουλο λογισμικό «σκουλήκι» το οποίο έπληξε το εργοστάσιο φυγοκέντρησης εμπλουτισμού «Ουρανίου» του Ιράν με στόχο την καθυστέρηση του πυρηνικού προγράμματος της χώρας, στόχος ο οποίος επιτεύχθηκε αφού το Ιρανικό εργοστάσιο μολύνθηκε για ένα μακρύ χρονικό διάστημα και συγκεκριμένα για μία περίοδο έξι μηνών. Πίσω από την επίθεση αυτή φαίνεται ότι κρύβονταν οι Ηνωμένες Πολιτείες της Αμερικής και το κράτος του Ισραήλ, ενώ οι αρχές του Ιράν καθυστέρησαν πολύ να αντιληφθούν το τι ακριβώς συνέβαινε στις δομές και τις εργοστασιακές εγκαταστάσεις του εξελισσόμενου πυρηνικού τους προγράμματος.

Η κυβερνοεπίθεση *BlackEnergy* το 2015 έπληξε την Ουκρανία και συγκεκριμένα κρατικές εταιρείες παροχής ενέργειας με αποτέλεσμα να διακοπεί η παροχή ηλεκτρικού ρεύματος από μία έως έξι ώρες η οποία έπληξε πολλές χιλιάδες καταναλωτών. Το *BlackEnergy* ήταν ένα κακόβουλο λογισμικό τύπου «Δούρειου Ίππου»[37] το οποίο έπληξε παράλληλα και το τηλεφωνικό δίκτυο της εταιρείας *Kyivoblenergo*. Η Ουκρανική κυβέρνηση απέδωσε την κυβερνοεπίθεση στη Ρωσία με τη δικαιολογία ότι αυτή είχε ως κίνητρο να αποτρέψει την ένταξη της Ουκρανίας στη Δύση. Επομένως αυτή η ενέργεια χρησιμοποιήθηκε από τη Ρωσία ως μέσο προειδοποίησης της Ουκρανίας για τυχόν μελλοντικές επιπτώσεις που θα είχε εάν τελικά αυτή προχωρούσε σε μια τέτοια παρόμοια κίνηση. Επίσης στη διεθνή βιβλιογραφία αναφέρεται η περίπτωση του λυτρισμικού *Wanna Cry*[38] όπου συγκεκριμένα στις 12 Μαίου 2017 επλήγησαν περισσότερα από 150 κράτη και συγκεκριμένα χώρες όπως ήταν η Αυστρία, η Βουλγαρία, η Κύπρος, η Δανία, η Φιλανδία, η Γερμανία, η Ουγγαρία η Λιθουανία, η

[35] Ζαμπατή Μ., & Κοντραφούρη Χ, σσ.112-116.
[36] Ό.π., σ.117.
[37] Ό.π., σσ.125-127.
[38] Ό.π. σσ.128-130.

Πορτογαλία, η Σλοβακία, η Σουηδία και επίσης το Βέλγιο, η Κροατία, η Τσεχία, η Εσθονία, η Γαλλία, η Ελλάδα, η Πολωνία, η Ιταλία, η Ισπανία και η Σλοβενία. Οι δράστες εκμεταλλεύτηκαν τα κενά που διαπίστωσαν ότι υπήρχαν στην ασφάλεια ενός πρωτοκόλλου του λειτουργικού συστήματος των *Windows* της εταιρείας *Microsoft* τα οποία επέτρεπαν την εξ αποστάσεως απόκτηση του ελέγχου οποιουδήποτε υπολογιστή.

Η επίθεση πραγματοποιήθηκε με τη χρήση ενός «σκουληκιού» που εξαπλώνεται μέσα στα δίκτυα του «λυτρισμικού» αυτού, επιφέροντας βλάβες στους Η/Υ. Σύμφωνα με τα στοιχεία που συλλέξαμε το «λυτρισμικό» *Wanna Cry* ως κακόβουλο λογισμικό βασίστηκε στο *Eternal Blue* της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ *(National Security Agency – NSA),* το οποίο υποκλάπηκε από τους *Shadow Brokers*, ομάδα χάκερ το καλοκαίρι του 2016. Η *NSA* αντιλήφθηκε το πρόβλημα και ενημέρωσε την *Microsoft* τον Φεβρουάριο 2017. Η εταιρεία *Microsoft* εξέδωσε ενημέρωση του λογισμικού της τον Μάρτιο του 2017 όμως τα συστήματα εκατοντάδων χιλιάδων υπολογιστών και συγκεκριμένα πάνω από 200.000 που δεν είχαν ακόμη ενημερωθεί, μολύνθηκαν[39]. Από τα θύματα της επίθεσης το λυτρισμικό ζητούσε την πληρωμή 300 δολαρίων ΗΠΑ σε κρυπτονομίσματα *(bitcoin*) μέσα σε τρεις ημέρες ή 600 δολάρια των ΗΠΑ σε επτά ημέρες. Πίσω από την επίθεση φαίνεται ότι κρύβονταν δράστες από τις χώρες της Κίνας ή της Βόρειας Κορέας. Από την επίθεση επλήγησαν κυρίως κρίσιμες υποδομές παγκοσμίως όπως για παράδειγμα, η Εθνική Υπηρεσία Υγείας του Ηνωμένου Βασιλείου *National Health Service - (NHS)*, το Υπουργείο Εσωτερικών της Ρωσίας *(Russia Interior Ministry)*, η σιδηροδρομική εταιρεία *Deutsche Bahn* της Γερμανίας και επίσης η εταιρεία τηλεπικοινωνιών *Telefonica* της Ισπανίας.

Το 2017 επίσης έχει καταγραφεί η επίθεση με το κακόβουλο λογισμικό NotPetya, την παραμονή της Ημέρας Συντάγματος της Ουκρανίας. Αυτή είχε ως στόχο φορείς του δημόσιου και ιδιωτικού τομέα στην Ουκρανία (οι οποίοι αποτελούσαν το 80% των προσβεβλημένων συστημάτων), συμπεριλαμβανομένων χρηματοπιστωτικών, ενεργειακών και κυβερνητικών ιδρυμάτων. Η επίθεση είχε ιδιαίτερα αποδιοργανωτικό χαρακτήρα, καθώς αχρήστευσε ηλεκτρονικούς υπολογιστές σβήνοντας τους σκληρούς δίσκους και εξαπλώθηκε χωρίς εξαίρεση σε εταιρείες που χρησιμοποιούσαν ένα δημοφιλές λογισμικό προετοιμασίας και υποβολής φορολογικών δηλώσεων, το (M.E.Doc). Το κακόβουλο λογισμικό ηλεκτρονικής παρείσφρησης (hacking) δεν είχε σχεδιαστεί για να από-κρυπτογραφηθεί. Αυτό σήμαινε ότι δεν υπήρχαν μέσα για τα θύματα να ανακτήσουν τα δεδομένα μετά την κρυπτογράφηση που είχε πραγματοποιηθεί κακόβουλα σε αυτά. Η επίθεση εξαπλώθηκε παγκοσμίως και μόλυνε, μεταξύ άλλων, το εγκατεστημένο σύστημα παρακολούθησης της ακτινοβολίας του

[39] Ζαμπατή Μ., & Κοντραφούρη Χ, σσ.128-130.

πυρηνικού αντιδραστήρα του εργοστασίου Τσερνομπίλ και οργανισμούς υγειονομικής περίθαλψης των ΗΠΑ. Η επίθεση έχει χαρακτηριστεί ως η "πιο καταστροφική κυβερνοεπίθεση στην ιστορία[40]".

Από κάποιους αναλυτές επισημαίνεται ότι ενώ το NotPetya κόστισε στην παγκόσμια οικονομία εκατομμύρια δολάρια, μάλλον δεν απέφερε ιδιαίτερα οφέλη στη Ρωσία[41]. Από το 2022 ο μη κυβερνητικός Οργανισμός *CyberPeace Institute* που αναφέραμε παραπάνω, καταγράφει επιβεβαιωμένες κυβερνοεπιθέσεις που πραγματοποιούνται στον κυβερνοχώρο εναντίων κρίσιμων υποδομών και μη στρατιωτικών στόχων παγκόσμια, δραστηριότητες οι οποίες όπως φαίνεται συμβαίνουν σχεδόν σε καθημερινή βάση. Συγκεκριμένα πρόσφατα περιστατικά από διακρατικές συγκρούσεις στον κυβερνοχώρο σύμφωνα με τη τριμηνιαία έκθεση ανάλυσης Ιουλίου - Σεπτεμβρίου 2023 (Q3) του *CyberPeace Institute*[42] για τη χρονική περίοδο εξέτασης από τον Ιανουάριο 2022 μέχρι τον Σεπτέμβριο 2023, παρατηρήθηκαν (1896) επιβεβαιωμένα περιστατικά κατά οντοτήτων σε άλλες χώρες εκτός της Ουκρανίας και της Ρωσίας. Συγκεκριμένα καταγράφηκαν κυβερνοεπιθέσεις σε πέντε κύριες χώρες στόχους οι οποίες ήταν: η Πολωνία με (315) περιστατικά, η Λιθουανία με (157), η Γερμανία με (136), οι Ηνωμένες Πολιτείες της Αμερικής με (101) και η Εσθονία με (93) περιστατικά. Στις πέντε αυτές χώρες οι τομείς στόχευσης ήταν οι εξής: η δημόσια διοίκηση με (575) περιστατικά, οι μεταφορές με (372), ο τομέας των οικονομικών με (199), η μεταποίηση με (122) και τα ΜΜΕ *(media)* με (99) περιστατικά.

Συγκεκριμένα το *CyberPeace Institute* παρατηρεί ότι στο υπό εξέταση 3ο τρίμηνο του 2023[43] οι τάσεις που επικράτησαν σε ό,τι αφορά το πλήθος των κυβερνοεπιθέσεων σε χώρες εκτός των εμπόλεμων Ρωσίας και Ουκρανίας, το ποσοστό 99,4% των περιστατικών που πραγματοποιήθηκαν, αφορούσε σε επιθέσεις τύπου DDoS (*Distributed denial of service)* σε (37) χώρες παγκοσμίως. Το υπόλοιπο 0,6% αφορούσαν επιθέσεις τύπου κακόβουλου λογισμικού κατασκοπείας *(Cyberespionage malware)*, παραβίαση και διαρροή δεδομένων *hack and leak data* και επιπλέον συλλογή πληροφοριών μέσω του κυβερνοχώρου *Cyber-enabled information operation,* οι οποίες αποτελούν εξαιρετικά μικρό ποσοστό. Στο 99,4% των παραπάνω περιπτώσεων επιθέσεων τύπου DDoS οι πιο στοχευμένοι τομείς ήταν αυτοί:

[40] Papapetrou, N., *NotPetya Attack,* στο: https://cyberpeaceinstitute.org/cyberattacks/notpetya-attack/ (δημοσιεύτηκε 27.07.2017).
[41] Lewis J.A, *Cyber War and Ukraine",* p.8, στο: https://www.csis.org/analysis/cyber-war-and-ukraine, (δημοσιεύτηκε 16.06.2022).
[42] Cyber Peace Institute, Quarterly Analysis Report - Q3 (July to September 2023) p.3 στο: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf
[43] Ό.π. p.10.

πρώτος της δημόσιας διοίκησης με (135) περιπτώσεις, δεύτερος των μεταφορών με (113), τρίτος της οικονομίας με (67), τέταρτος των ΜΜΕ *(media)* με (34) και πέμπτος της διοικητικής υποστήριξης με (22) περιπτώσεις. Στο διάστημα των τριών μηνών που εξετάστηκε από τον Ιούλιο έως τον Σεπτέμβριο του 2023 τα επιβεβαιωμένα περιστατικά που προαναφέραμε αφορούσαν τις παρακάτω δέκα πρώτες χώρες στόχους, πάντα εκτός των δύο εμπόλεμων κρατών, συγκεκριμένα την μεν Πολωνία με (77) περιστατικά, τη Λιθουανία με (46), την Ισπανία με (30), την Ολλανδία με (25), τη Γαλλία πάλι με (25), την Ιταλία κι αυτή πάλι με (25), τη Γερμανία με (23), την Εσθονία με (22), τη Λετονία με (21) και τέλος τη Μολδαβία με (19) περιστατικά[44].

Το σημαντικό στοιχείο το οποίο παρατηρεί το *CyberPeace Institute* στην πρόσφατη τριμηνιαία έκθεσή του στην οποία προαναφερθήκαμε, είναι ότι στο υπό εξέταση χρονικό διάστημα από τον Ιούλιο έως το Σεπτεμβρίου του 2023 σε μη εμπλεκόμενες χώρες στη συνεχιζόμενη σύγκρουση στην Ουκρανία, υπήρξε συνολική μείωση 3,7% στις επιβεβαιωμένες κυβερνοεπιθέσεις σε σχέση με το προηγούμενο τρίμηνο του 2023, ωστόσο παραμένει σχετικά υψηλό ιδίως σε σύγκριση με το αντίστοιχο τρίμηνο του 2022 παρουσιάζοντας την εντυπωσιακή αύξηση του 234,1%. Οι φιλορωσικοί φορείς κυβερνοαπειλών αποτελούν τη μεγαλύτερη ομάδα των δραστηριοποιούμενων στο χώρο με πάνω από (400) περιπτώσεις κυβερνοεπιθέσεων ανά τρίμηνο από τις αρχές του 2023, πλήττοντας χώρες εκτός των εμπόλεμων Ρωσίας-Ουκρανίας[45]. Επίσης το *CyberPeace Institute* παρατηρεί αυξομειώσεις στη δραστηριότητα γνωστών και μη φορέων κυβερνοαπειλών με την εμφάνιση νέων παικτών σε αυτό το χώρο.

Συγκεκριμένα σημειώνεται μία συνεχής μείωση του Ρωσικού φορέα απειλητικής κυβερνοδραστηριότητας *Killnet,* στην οποία αποδίδονται μόνο τρία περιστατικά στο υπό εξέταση τρίμηνο. Το *CyberPeace Institute* καταγράφει την εμφάνιση δύο ακόμη νέων φορέων απειλών, τους *Net Worker Alliance* και *Zulic Group*. Πρόκειται για ομάδες χακτιβιστών που επικοινωνούν τις κυβερνοεπιθέσεις τους *DDoS* μέσω καναλιών *Telegram,* τα οποία επιτρέπουν τη μετάδοση μηνυμάτων σε απεριόριστο αριθμό ανύποπτων συνδρομητών. Η Εσθονία αποτέλεσε τον πιο μεγάλο στόχο αυτών των κυβερνοπιθέσεων με (9) περιστατικά του φορέα της *Net Worker Alliance* και η Πολωνία αντίστοιχα με (9) περιστατικά της *Zulic Group.* Έκτοτε, τα κανάλια *Telegram* και των δύο απειλητικών φορέων δεν παρουσιάζουν δραστηριότητα[46].

[44] Cyber Peace Institute, Quarterly Analysis Report - Q3 (July to September 2023), p.10.
[45] Ό.π, p.11.
[46] Ο.π.

Συμπεραίνουμε επομένως ότι στις μη εμπόλεμες χώρες η δραστηριότητα των κυβερνοεπιθέσεων με στόχο κρίσιμες υποδομές κρατών, αποτελεί μια διαρκή και πραγματική απειλή ιδιαίτερα σε αυτές που υποστηρίζουν τις δύο αντιμαχόμενες πλευρές της Ρωσίας και της Ουκρανίας. Είναι σημαντικό να αναφέρουμε ότι στην περίπτωση του πολέμου που εξετάζουμε, οι κυβερνοεπιθέσεις αποτελούν δυστυχώς καθημερινή πραγματικότητα και σ' αυτήν επιδίδονται συστηματικά τόσο η Μόσχα όσο και το Κίεβο μέχρι τις μέρες μας.

3. Η Ρωσο-ουκρανική διένεξη στο κυβερνοχώρο.

3.1 Η χρησιμοποίηση του κυβερνοχώρου από την Ουκρανία και τη Ρωσία στο πλαίσιο της πολεμικής αντιπαράθεσής τους.

Επιχειρώντας να διερευνήσουμε τη Ρωσο-ουκρανική διένεξη έχει σημασία να αναφέρουμε ότι η χρήση επιχειρήσεων συγκεκριμένα στο πεδίο του κυβερνοχώρου είναι αποτέλεσμα στρατηγικού σχεδιασμού και λαμβάνουν χώρα κρυφά και διαρκώς τόσο σε καιρό ειρήνης όσο και πολέμου. Η στόχευση και υπονόμευση ευαίσθητων δικτύων σε καιρό ειρήνης επιτρέπει στους επιτιθέμενους να προετοιμάσουν το έδαφος και να θέσουν τις βάσεις για τη χρήση κακόβουλου λογισμικού που προορίζεται για εφαρμογή σε καιρό πολέμου[47]. Σύμφωνα με τους ερευνητές[48], η στρατηγική της Μόσχας στην Ουκρανία περιελάμβανε σημαντικές μακροχρόνιες επενδύσεις στην κατασκοπεία και τις επιχειρήσεις πληροφοριών με σκοπό την προετοιμασία του πεδίου μάχης. Οι μέθοδοι που χρησιμοποιήθηκαν σε αυτή την περίπτωση από τη Ρωσία αφορούσαν στη διείσδυση και εκμετάλλευση δικτύων με σκοπό την κλοπή ευαίσθητων πληροφοριών. Αξίζει να σημειωθεί ότι και οι δύο χώρες διέθεταν ισχυρή βάση τεχνολογίας πληροφοριών και πολλούς χάκερς οι οποίοι είχαν πραγματοποιήσει και στο παρελθόν επιθέσεις τύπου *DDoS*[49] , πριν την εισβολή του 2022. Όπως έχει καταγραφεί, το 2012 ύποπτοι Ρώσοι παράγοντες φέρεται να χρησιμοποίησαν τα κακόβουλα λογισμικά *backdoors Wipbot* και *Snake* για μακροχρόνια κυβερνοκατασκοπεία.

Το 2013, η "Επιχείρηση Αρμαγεδδών" - μια ρωσική εκστρατεία κατασκοπείας στον κυβερνοχώρο που φέρεται πως είχε ως στόχο αξιωματούχους της ουκρανικής κυβέρνησης,

---

[47] Duguin S. & Pavlova P, p.6.

[48] Weedon J., *Beyond "Cyber War": Russia's Use of Strategic Cyber Espionage and information Operations in Ukraine*, Ch.8. στο: Cyber War in Perspective: Russian Aggression against Ukraine, p.67, στο: https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

[49] Libicki M., *The Cyber War that Wasn't*, Ch.5, στο: Cyber War in Perspective: Russian Aggression against Ukraine, p.50, https://ccdcoe.org/uploads/2018/10/Ch05_CyberWarinPerspective_Libicki.pdf (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

των υπηρεσιών επιβολής του νόμου και του στρατού - έχει πιθανότατα συμβάλει στην παροχή στρατιωτικού πλεονεκτήματος στη Ρωσία έναντι της Ουκρανίας από τα μυστικά που συλλέγονταν συστηματικά από την κατασκοπεία που επιτεύχθηκε στον κυβερνοχώρο. Μεταξύ του 2013 και του 2014, οι δράστες που χρησιμοποίησαν το κακόβουλο λογισμικό *Snake/Uroburos/Turla* έπληξαν τα ουκρανικά συστήματα υπολογιστών σε δεκάδες κυβερνοεπιχειρήσεις. Αυτό το κακόβουλο λογισμικό ήταν εξαιρετικά πολύπλοκο, ανθεκτικό στα αντίμετρα και πιστεύεται ότι δημιουργήθηκε το 2005. Στα τέλη του 2014, οι ερευνητές αποκάλυψαν μια μακροχρόνια ενεργή ρωσική ομάδα με την ονομασία *Sandworm,* στα θύματα της οποίας περιλαμβάνονταν η Βορειοατλαντική Συμμαχία – *(NATO),* η Ουκρανική κυβέρνηση, άλλες κυβερνήσεις της Ευρωπαϊκής Ένωσης, επίσης εταιρείες ενέργειας και τηλεπικοινωνιών και ακόμη ένας αμερικανικός ακαδημαϊκός οργανισμός. Η ομάδα χρησιμοποιούσε τα κενά ασφαλείας και αδυναμίες *exploits*[50] μηδενικής ημέρας *zero day*[51] ως κακόβουλα προγράμματα (μία από τις βασικές τεχνικές που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου) και μόλυνε τα θύματα με διάφορα μέσα, συμπεριλαμβανομένων κακόβουλων συνημμένων εικόνων γραφικών *(PowerPoint)* και της εργαλειοθήκης *BlackEnergy.*

Τον Αύγουστο του 2015, μια ομάδα ερευνητών ασφαλείας περιέγραψε την επιχειρηματική προσπάθεια πίσω από το κακόβουλο λογισμικό *Gameover ZeuS.* Αυτό του είδος κακόβουλου λογισμικού χρησιμοποιήθηκε για να διευκολύνει τόσο το έγκλημα στον κυβερνοχώρο όσο και την κατασκοπεία. Επιπλέον, οι ερευνητές ανακάλυψαν εντολές στο κακόβουλο λογισμικό που υποδεικνύουν ότι οι δράστες επεδίωκαν να συλλέξουν διαβαθμισμένες πληροφορίες από θύματα στις χώρες της Ουκρανίας, της Γεωργίας και της Τουρκίας, γεγονός που υποδηλώνει μια σύνδεση μεταξύ των συνδικάτων κυβερνοεγκλήματος της Ρωσίας και των κυβερνητικών φορέων κατασκοπείας. Η εδαφική εισβολή στην Ουκρανία τον Φεβρουάριο του 2022 από τις ένοπλες δυνάμεις της Ρωσίας συνοδεύτηκε από κυβερνοεπιθέσεις σε κρίσιμες υποδομές, που είχαν σχεδιαστεί για να υπονομεύσουν την τηλεπικοινωνιακή υποδομή της Ουκρανίας. Αυτές οι ενέργειες της Ρωσίας είχαν ως αποτέλεσμα να διακοπεί η ροή πληροφοριών στον Ουκρανικό χώρο εθνικής ασφάλειας για μεγάλα χρονικά διαστήματα και επιπλέον να

[50] Το exploit είναι ένα τμήμα κώδικα ή ένα πρόγραμμα που εκμεταλλεύεται κακόβουλα, τρωτά σημεία ή ελαττώματα ασφαλείας σε λογισμικό ή υλικό για να διεισδύσει και να ξεκινήσει μια επίθεση άρνησης υπηρεσίας (DoS) ή να εγκαταστήσει κακόβουλο λογισμικό, όπως λογισμικό υποκλοπής, ransomware, Trojan horses, worms ή ιούς.

[51] Το zero-day- μηδενική ημέρα (γνωστό και ως 0-day) είναι μια ευπάθεια ή ένα κενό ασφαλείας σε ένα λογισμικό άγνωστο στους δημιουργούς του, στους προγραμματιστές ή σε οποιονδήποτε μπορεί να το μετριάσει. Έως ότου αποκατασταθεί η ευπάθεια, οι φορείς της απειλής μπορούν να την εκμεταλλευτούν σε μια επίθεση zero-day.

επηρεαστεί όσο γινόταν περισσότερο η κοινή γνώμη. Είναι σημαντικό να αναφέρουμε ότι αυτές οι κυβερνοεπιθέσεις συντονίστηκαν επιπλέον με πραγματικές στρατιωτικές επιχειρήσεις στο πεδίο[52].

Από την έναρξη της ένοπλης εισβολής της Ρωσίας στην Ουκρανία τον Φεβρουάριο του 2022, το Ινστιτούτο *Cyber Peace* καταγράφει πλήθος κυβερνοεπιθέσεων εναντίον κρίσιμων υποδομών αλλά και μη στρατιωτικών στόχων στην Ουκρανία και τη Ρωσική Ομοσπονδία και δημοσιεύει εκθέσεις σε τριμηνιαία βάση παράλληλα και για τις δύο αντιμαχόμενες χώρες. Όπως αναφέρεται στην τελευταία έκθεση του Ινστιτούτου για το τρίτο τρίμηνο 2023[53], από τον Ιανουάριο του 2022 έως τον Σεπτέμβριο του 2023 καταγράφηκαν συνολικά (2776) περιστατικά στον κυβερνοχώρο, τα οποία πραγματοποιήθηκαν από (106) διαφορετικούς φορείς απειλών. Όλα αυτά τα δεδομένα διατίθενται μέσω της πλατφόρμας *Cyber Attacks in Times of Conflict, Platform 1 #Ukraine*[54]. Πιο συγκεκριμένα σημειώθηκαν οι παρακάτω ενέργειες:

Για την Ουκρανία[55] και για το παραπάνω διάστημα, καταγράφηκαν (574) περιστατικά κατά οντοτήτων εναντίον της από φορείς απειλών, όπως ο *People's CyberArmy* με (217) επιθέσεις όπου αυτός ήταν ο πιο ενεργός συλλογικός φορέας απειλών των χακτιβιστών, ενώ ο *Sanworm*-21 ήταν ο πιο ενεργός ρωσικός φορέας απειλών από την έναρξη της στρατιωτικής εισβολής στην Ουκρανία τον Φεβρουάριο του 2022. Επιπλέον οι πέντε κυριότεροι τομείς-στόχοι ήταν αυτός της Δημόσιας Διοίκησης με (132) επιθέσεις, του τομέα των Οικονομικών με (63), των Μέσων Μαζικής Ενημέρωσης με (61), των ΤΠΕ/Τεχνολογιών Πληροφοριών Επικοινωνιών με (59) και ακόμη της Ενέργειας με (31) επιθέσεις.

Σύμφωνα με τα στοιχεία που δίνει το Ινστιτούτο Cyber Peace για τη Ρωσική Ομοσπονδία[56] το ίδιο διάστημα σημειώθηκαν (306) περιστατικά κατά οντοτήτων εναντίον της, όπου οι *Anonymous Italia* με (62) επιθέσεις ήταν πολύ δραστήρια κολεκτίβα χάκερ, ενώ ο *IT Army* της Ουκρανίας με (75) επιθέσεις αποτελεί την πιο δραστήρια κολεκτίβα χάκερ η οποία είναι ενεργός ουκρανικός κρατικά υποστηριζόμενος φορέας απειλών από την έναρξη του πολέμου το 2022. Κι εδώ επίσης όπως και στη προηγούμενη περίπτωση της Ουκρανίας έχουμε για τη Ρωσία πάλι πέντε κύριους τομείς οι οποίοι έγιναν στόχος, με έναν από αυτούς μόνο να είναι διαφορετικός (αυτός δηλαδή των Μεταφορών κι όχι της ενέργειας) και είναι οι εξής: αρχικά ο τομέας της Δημόσιας Διοίκησης με (55) επιθέσεις, των Οικονομικών με (44), Τεχνολογιών

[52] Duguin S. & Pavlova P., p.6.
[53] Cyber Peace Institute, Quarterly Analysis Report - Q3 (July to September 2023) p.3
[54] Ό.π., Attack details, https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
[55] Ό.π, Quarterly Analysis Report - Q3 (July to September 2023) p.3
[56] Ό.π.

Πληροφοριών Επικοινωνιών - ΤΠΕ με (31), των ΜΜΕ (30), τέλος των Μεταφορών με (25) επιθέσεις.

Παρακάτω παρατίθενται κάποιες από τις επιβεβαιωμένες κυβερνοεπιθέσεις μεταξύ Ουκρανίας – Ρωσίας από τον Φεβρουάριο 2022 με τις πιο πρόσφατα καταγεγραμμένες μόλις το Νοέμβριο 2023, από το Cyber Peace Institute, και είναι οι εξής[57]:

α) Οι επιβεβαιωμένες Κυβερνοεπιθέσεις της Ουκρανίας εναντίον Ρωσικών κυβερνοστόχων:

30.11.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* κατά των πόρων του Διαδικτύου και της υποδομής διακομιστών ενός ρωσικού παρόχου υπηρεσιών Διαδικτύου που δραστηριοποιείται στο Ντόνετσκ.

Επίπτωση: Διακόπηκε η πρόσβαση στο Διαδίκτυο.

26.11.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε και πάλι επίθεση DDoS κατά των πόρων του Διαδικτύου και της υποδομής διακομιστών ενός ρωσικού παρόχου υπηρεσιών Διαδικτύου που δραστηριοποιείται κι αυτός στη πόλη Ντόνετσκ.

Επίπτωση: Διακόπηκε η πρόσβαση στο Διαδίκτυο.

17.11.2023 Για τρίτη φορά ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση DDoS κατά των πόρων του Διαδικτύου και της υποδομής διακομιστών ενός ρωσικού παρόχου υπηρεσιών Διαδικτύου που δραστηριοποιείται και πάλι στη πόλη Ντόνετσκ.

Επίπτωση: Η διακοπή της σύνδεσης με υπηρεσίες, συμπεριλαμβανομένου του συστήματος πληρωμών.

13.11.2023 Ο CERT-UA *(Computer Emergency Response Team of Ukraine)* ανέφερε μια εκστρατεία phishing για λογαριασμό της Υπηρεσίας Ασφαλείας της Ουκρανίας με φερόμενο στόχο την UAC-0050 η οποία πιθανότατα έχει

[57] Cyber Peace Institute Attack details, https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details.
Σημείωση: τα δεδομένα συλλέχθηκαν από την παραπάνω λίστα κυβερνοεπιθέσεων που δίνει το Ινστιτούτο Cyber Peace, επιλέγοντας τις επιθέσεις που αναφέρονται για την Ουκρανία και τη Ρωσία. Τα στοιχεία που παραθέτουμε αφορούν μόνο τις επιβεβαιωμένες επιθέσεις που σημειώνονται με πράσινη κουκίδα. Η λεπτομερής αναφορά για κάθε κυβερνοεπίθεση (περιγραφή του γεγονότος και επίπτωση) δίνεται στο γράμμα (i), δίπλα στην πράσινη κουκίδα. Με πορτοκαλί χρώμα κουκίδες δηλώνονται οι δυνατές να έχουν συμβεί επιθέσεις ενώ με μπεζ οι πιθανές. Στη συνέχεια έχουμε επιλέξει να παραθέσουμε μόνο τις επιβεβαιωμένες κυβερνοεπιθέσεις.

Ρωσική προέλευση. Το email περιέχει ένα κακόβουλο αρχείο, το οποίο μόλις εκτελεστεί εγκαθιστά το τηλεχειριστήριο *Remcos RAT – Sophisticated Remote AccessTrojan.*

Επίπτωση: Άγνωστη.

22.09.2023 Κυβερνοεπιθέσεις εναντίον ρωσικών παρόχων υπηρεσιών Διαδικτύου που δραστηριοποιούνται στην Κριμαία, σύμφωνα με σύμβουλο του Ρώσου κυβερνήτη της παράνομα προσαρτημένης χερσονήσου της Κριμαίας.

Επίπτωση: Άγνωστη.

24.08.2023 Ο Στρατός Πληροφορικής της Ουκρανίας διεξήγαγε επιχείρηση παραμόρφωσης κατά της ιστοσελίδας μιας ρωσικής ομοσπονδιακής οργάνωσης.

Επίπτωση: Άγνωστη.

24.08.2022 Ο Στρατός Πληροφορικής της Ουκρανίας ισχυρίζεται ότι διεξήγαγε κυβερνοεπίθεση και επιχείρηση παραβίασης κατά του μεγαλύτερου ρωσικού παρόχου Διαδικτύου στην Κριμαία.

Επίπτωση: Η διακοπή της λειτουργίας του.

09.08.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* εναντίον της ιστοσελίδας ενός ρωσικού παρόχου υπηρεσιών Διαδικτύου που δραστηριοποιείται στην παράνομα προσαρτημένη περιοχή του Λουχάνσκ.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

23.07.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση DDoS εναντίον διακομιστή Ρωσικού παρόχου Διαδικτύου που δραστηριοποιείται στο Λουχάνσκ.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

13.07.2023 Ο *CERT-UA* έχει αναφέρει για μια κυβερνοεπίθεση που διανέμει κακόβουλο λογισμικό τύπου *SmokeLoader* μέσω *email* ηλεκτρονικού ψαρέματος που παρουσιάζονται ως τιμολόγιο από παραβιασμένους λογαριασμούς *email.* Η εκστρατεία έχει αποδοθεί στον παράγοντα απειλών *UAC-0006.*

Επίπτωση: Χρησιμοποιώντας παραβιασμένους λογαριασμούς *email,* ο φορέας των απειλών έστελνε μηνύματα ηλεκτρονικού ψαρέματος που παριστάνονταν ως

τιμολόγιο. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου περιείχαν στην πραγματικότητα το κακόβουλο λογισμικό *SmokeLoader*. Εάν εκτελεστεί, αυτό το κακόβουλο λογισμικό δίνει πρόσβαση στη συσκευή του στόχου στο φορέα απειλής.

05.07.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση DDoS εναντίον της ιστοσελίδας μιας ρωσικής κρατικής εταιρείας σιδηροδρόμων.

Επίπτωση: Η διακοπή σύνδεσης με τους ιστότοπους και την εφαρμογή για τα κινητά τηλέφωνα.

08.06.2023 Ένας άγνωστος παράγοντας απειλών διεξήγαγε μια επιχείρηση παραποίησης της εικόνας κατά της ιστοσελίδας μιας ρωσικής υπηρεσίας δανείων.

Επίπτωση: Ο ιστότοπος αντικαταστάθηκε με ένα φιλοουκρανικό μήνυμα που ενθαρρύνει τους Ρώσους να διαμαρτυρηθούν και να υποστηρίξουν τις Ουκρανικές Ένοπλες Δυνάμεις. Ο παραμορφωμένος ιστότοπος περιλάμβανε επίσης μια συχνή ερώτηση σχετικά με τη σύγκρουση.

08.06.2023 Το *Cyber Anarchy Squad,* ένας φιλο-ουκρανικός παράγοντας απειλών, διεξήγαγε μια άγνωστη μορφή κυβερνοεπίθεσης εναντίον ρωσικού παρόχου υπηρεσιών Διαδικτύου.

Επίπτωση: Ο φορέας απειλής μπόρεσε να παραβιάσει τα συστήματα πληροφορικής του στόχου, καταστρέφοντας ένα μέρος του εξοπλισμού του δικτύου και καταργώντας τις υπηρεσίες *Internet Service Provider – (ISP)* για 33 ώρες. Διάφοροι πελάτες του *(ISP)* φέρεται να αποκόπηκαν από το Διαδίκτυο ως αποτέλεσμα.

07.06.2023 Ραδιοφωνικοί σταθμοί σε μια περιοχή της Ρωσίας έγιναν στόχος ενός άγνωστου φιλο-ουκρανικού παράγοντα απειλών σε μια επιχείρηση πληροφόρησης μέσω κυβερνοχώρου. Οι ραδιοφωνικοί σταθμοί φέρεται να έπαιξαν μηνύματα υπέρ της Ουκρανίας.

Επίπτωση: Σύμφωνα με πληροφορίες, οι ραδιοφωνικοί σταθμοί έπαιξαν φιλοουκρανικά μηνύματα που είχαν σκοπό να εκφοβίσουν τους Ρώσους πολίτες.

05.06.2023 Ένας ραδιοφωνικός σταθμός που εκπέμπει σε διάφορες περιοχές της Ρωσίας στοχοποιήθηκε από έναν άγνωστο φιλο-ουκρανικό παράγοντα απειλών σε μια επιχείρηση πληροφόρησης μέσω του κυβερνοχώρου. Ο ραδιοφωνικός

σταθμός φέρεται να έπαιξε ένα ψεύτικο μήνυμα του προέδρου Πούτιν που ανήγγειλε εισβολή στη Ρωσική Ομοσπονδία.

Επίπτωση: Από τις 12:41 έως τις 13:18, οι ραδιοφωνικοί σταθμοί φέρεται να έπαιξαν ένα ψεύτικο μήνυμα του προέδρου Βλαντιμίρ Πούτιν που ανήγγειλε την εισβολή στη Ρωσική Ομοσπονδία με σκοπό να εκφοβίσει Ρώσους πολίτες.

28.05.2023 Ένα ρωσικό πρόγραμμα υψηλής τεχνολογίας επιβεβαίωσε ότι υπήρξε επιχείρηση εισβολής και διαρροής πληροφοριών που διεξήχθη εναντίον της εταιρείας από έναν φιλο-ουκρανικό παράγοντα απειλών. Ο παράγοντας της απειλής απέκτησε μερική πρόσβαση σε έναν αριθμό συστημάτων πληροφοριών και πόρων του δικτύου, συγκεκριμένα στην ανταλλαγή αρχείων, που βρίσκονται στα φυσικά στοιχεία του στόχου.

Επίπτωση: Ο παράγοντας της απειλής απέκτησε μερική πρόσβαση σε έναν αριθμό συστημάτων πληροφοριών και πόρων δικτύου. Συγκεκριμένα, η ανταλλαγή αρχείων, που βρίσκεται στα φυσικά περιουσιακά στοιχεία του στόχου, παραβιάστηκε. Οι δημόσιοι πόροι πληροφόρησης του στόχου, όπως ο ιστότοπος και οι διαδικτυακές υπηρεσίες, ήταν προσωρινά απρόσιτοι.

17.05.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε πάλι επίθεση DDoS εναντίον του υποτομέα της κυβέρνησης μιας ρωσικής περιοχής.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

12.05.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση DDoS εναντίον του ιστότοπου μιας ρωσικής πλατφόρμας μάρκετινγκ.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

06.05.2023: Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε και πάλι επίθεση *DDoS* εναντίον της ιστοσελίδας μιας ρωσικής υπηρεσίας κρατήσεων ξενοδοχείων.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

27.04.2023 Ο Στρατός Πληροφορικής της Ουκρανίας διεξήγαγε επανειλημμένα επιθέσεις *DDoS* εναντίον του ιστότοπου ενός ρωσικού μέσου λογιστικών ειδήσεων επί δύο συνεχόμενες ημέρες.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

23.04.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* εναντίον της ιστοσελίδας ενός ρωσικού αθλητικού ιστοτόπου.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

10.04.2023 Ένας άγνωστος φιλο-ουκρανός παράγοντας απειλών πραγματοποίησε κυβερνοεπίθεση εναντίον ρωσικής ομοσπονδιακής υπηρεσίας.

Επίπτωση: Οι πόροι πληροφορικής της Ομοσπονδιακής Τελωνειακής Υπηρεσίας έγιναν στόχος κυβερνοεπίθεσης. Ενώ ορισμένες υπηρεσίες μπόρεσαν να αποκατασταθούν, άλλες υπηρεσίες έμειναν για πολύ εκτός λειτουργίας, αναγκάζοντας ορισμένα σημεία ελέγχου να επανέλθουν στην παραδοσιακή γραφειοκρατία.

04.04.2023 Η *Cyber Resistance,* ένας φιλο-ουκρανικός παράγοντας απειλών, παραβίασε τον λογαριασμό και διέπραξε οικονομική απάτη εναντίον ενός Ρώσου *blogger,* ξοδεύοντας (25.000 $), που συγκεντρώθηκαν αρχικά για τον ρωσικό στρατό, σε παιχνίδια για ενήλικες.

Επίπτωση: Ο φορέας της απειλής εισέβαλε στον λογαριασμό του μπλόγκερ στο *AliExpress* και ξόδεψε χρήματα που συγκεντρώθηκαν αρχικά για τον ρωσικό στρατό σε παιχνίδια για ενήλικες.

25.03.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* κατά της ιστοσελίδας ενός ρωσικού μέσου επικοινωνίας.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

22.03.2023 Ο Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* εναντίον της ιστοσελίδας μιας ρωσικής τράπεζας.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

28.02.2023 Ένας άγνωστος παράγοντας απειλών πραγματοποίησε κυβερνοεπίθεση εναντίον περιφερειακών ραδιοφωνικών και τηλεοπτικών σταθμών στη Ρωσία. Αυτό είχε ως αποτέλεσμα τη μετάδοση πληροφοριών για υποτιθέμενο αεροπορικό συναγερμό.

Επίπτωση: Διάφοροι περιφερειακοί ραδιοφωνικοί και τηλεοπτικοί σταθμοί σε διάφορες περιοχές της Ρωσίας φέρεται να δέχθηκαν επίθεση με αποτέλεσμα να εκπέμψουν μια υποτιθέμενη ειδοποίηση αεροπορικής επιδρομής.

22.02.2023 Ένας άγνωστος φορέας απειλής φέρεται να επιτέθηκε στους διακομιστές εμπορικών ραδιοφωνικών σταθμών σε διάφορες περιοχές της Ρωσίας. Αυτό είχε ως αποτέλεσμα τη μετάδοση πληροφοριών για υποτιθέμενο αεροπορικό συναγερμό και την απειλή επίθεσης πυραύλων.

Επίπτωση: Οι διακομιστές εμπορικών ραδιοφώνων σε διάφορες περιοχές της Ρωσίας φέρεται να δέχθηκαν επίθεση με αποτέλεσμα να εκπέμψουν μια υποτιθέμενη ειδοποίηση αεροπορικής επιδρομής και τον κίνδυνο επίθεσης με πυραύλους.

30.01.2023 Ο απειλητικός φορέας *Anonymous Italia*, για την υποστήριξη της Ουκρανίας, διεξήγαγε μια επιχείρηση παραβίασης τεσσάρων ιστοσελίδων μιας ρωσικής εταιρείας διανομής Τύπου.

Επίπτωση: Ο ιστότοπος παραμορφώθηκε και αντικαταστάθηκε με μήνυμα από τους *Anonymous Italia* που καταδικάζει τον πόλεμο στην Ουκρανία.

22.12.2022 Ο φορέας Στρατός Πληροφορικής της Ουκρανίας πραγματοποίησε επίθεση *DDoS* εναντίον των διακομιστών μιας ρωσικής πλατφόρμας ανεξάρτητων επαγγελματιών.

Επίπτωση: Σύμφωνα με ένα δελτίο τύπου του οργανισμού-στόχου, η επίθεση *DDoS* ήταν η μεγαλύτερη επίθεση εναντίον των διακομιστών του στόχου από την έναρξη της σύγκρουσης.

10.10.2022 Ο φορέας Στρατός της Ουκρανίας πραγματοποίησε επίθεση *DDoS* εναντίον ρωσικής τράπεζας.

Επίπτωση: Σύμφωνα με τον οργανισμό-στόχο, η επίθεση *DDoS* έκανε τις υπηρεσίες απομακρυσμένης συντήρησης να λειτουργούν πιο αργά.

16.06.2022 Το Εθνικό Κέντρο Αντιμετώπισης Συμβάντων Υπολογιστών και Συντονισμού της Ρωσικής Ομοσπονδίας ανακάλυψε μια εκστρατεία ηλεκτρονικού ψαρέματος που διανέμει κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου εκ μέρους του *NCIRCC* και της ομάδας αντιμετώπισης συμβάντων πληροφορικής.

Επίπτωση: Άγνωστη.

Επομένως σύμφωνα με τα παραπάνω όπως καταγράφεται στην έκθεση του *Cyber Peace Institute*[58], οι τύποι των κυβερνοεπιθέσεων που χρησιμοποιήθηκαν από την Ουκρανία εναντίον της Ρωσίας μπορούν να συνοψιστούν σε:

1. Επιθέσεις εναντίον παρόχων υπηρεσιών του διαδικτύου σε διαφορετικές Ρωσικές πόλεις,
2. Εκστρατείες ψαρέματος *phishing* με κακόβουλα αρχεία
3. Παραμόρφωση ιστοσελίδων/ιστοτόπων
4. Παραβίαση λογαριασμών ηλεκτρονικού ταχυδρομείου *emails* με διασπορά κακόβουλων λογισμικών
5. Επιθέσεις εναντίον ραδιοφωνικών και τηλεοπτικών σταθμών
6. Επιθέσεις εναντίον εταιρειών με διαρροή πληροφοριών
7. Επιθέσεις εναντίον τομέων και ομοσπονδιακών υπηρεσιών της ρωσικής κυβέρνησης
8. Επιθέσεις εναντίον διαφόρων τύπων λογαριασμών ιδιωτών και εναντίον τραπεζών και του χρηματοπιστωτικού συστήματος
9. Επιθέσεις εναντίον πλατφορμών ιδιωτών επαγγελματιών.

β) Οι επιβεβαιωμένες Κυβερνοεπιθέσεις της Ρωσίας εναντίων Ουκρανικών κυβερνοστόχων:

30.11.2023 Ο CERT-UA *(Computer Emergency Response Team of Ukraine)* ανακάλυψε μια εκστρατεία ηλεκτρονικού "ψαρέματος" (phishing) με θέμα "Δικαστικές κλήσεις στο δικαστήριο", από νόμιμους παραβιασμένους λογαριασμούς μιας από τις δικαστικές αρχές της Ουκρανίας. Τα μηνύματα ηλεκτρονικού ταχυδρομείου περιείχαν ένα συνημμένο αρχείο, το οποίο όταν εκτελούνταν εκτελούσε το πρόγραμμα απομακρυσμένου ελέγχου RemcosRAT.

Επίπτωση: Ηλεκτρονικό μήνυμα στο ηλεκτρονικό ταχυδρομείο τύπου ηλεκτρονικού "ψαρέματος" phishing που στάλθηκε σε περισσότερους από 15000 παραλήπτες χρησιμοποιώντας νόμιμους λογαριασμούς μίας από τις δικαστικές αρχές της Ουκρανίας.

[58] Cyber Peace Institute Attack details, βλπ παραπάνω σ. 19.

28.11.2023 Ο *UserSec*, ένας φιλορώσος φορέας απειλών, διεξήγαγε μια επιχείρηση παραμόρφωσης κατά του ιστότοπου ενός ουκρανικού καταστήματος προϊόντων ομορφιάς.

Επίπτωση: Ο ιστότοπος παραμορφώθηκε και αντικαταστάθηκε με φιλορωσικό μήνυμα από τον φορέα απειλών.

19.11.2023 Η κακόβουλη κυβερνοδραστηριότητα *KillNet* διεξήγαγε επιχείρηση παραμόρφωσης κατά της ιστοσελίδας ενός ουκρανικού τουριστικού γραφείου.

Επίπτωση: Ο ιστότοπος παραμορφώθηκε και αντικαταστάθηκε με φιλορωσικό μήνυμα από τον παράγοντα απειλών.

14.11.2023 Η *KillNet* διεξήγαγε μια επιχείρηση παραμόρφωσης κατά της ιστοσελίδας ενός ουκρανικού πανεπιστημιακού εργαστηρίου γενετικής έρευνας.

Επίπτωση: Ο ιστότοπος παραμορφώθηκε και αντικαταστάθηκε με φιλορωσικό μήνυμα από τον παράγοντα απειλών.

27.09.2023 Το *CERT-UA (Computer Emergency Response Team of Ukraine)* ανέφερε κυβερνοεπιθέσεις εναντίον τουλάχιστον 11 ουκρανικών παρόχων τηλεπικοινωνιών. Οι επιθέσεις κυμαίνονται από τις 11 Μαΐου 2023 έως τις 27 Σεπτεμβρίου 2023. Η καμπάνια έχει αποδοθεί στον φορέα απειλών *UAC-0165.*

Επίπτωση: Χρησιμοποιώντας προηγουμένως παραβιασμένα συστήματα, ο παράγοντας απειλής ήταν σε θέση να σαρώσει δίκτυα για ανοιχτές θύρες και να αποκτήσει πρόσβαση με τηλεχειρισμό. Μόλις μπήκε μέσα στο δίκτυο, ο παράγοντας της απειλής μπόρεσε να αποκτήσει προπαντός απομακρυσμένη πρόσβαση και να παρέμβει στα συστήματα πληροφοριών και επικοινωνιών (11) παρόχων τηλεπικοινωνιών της Ουκρανίας απενεργοποιώντας τον ενεργό εξοπλισμό δικτύου και διακομιστή καθώς και τα συστήματα αποθήκευσης δεδομένων. Αυτό οδηγεί σε διακοπές στην παροχή υπηρεσιών στους καταναλωτές.

04.09.2023 Το *CERT-UA* ανέφερε για μια κυβερνοεπίθεση που στόχευε την εγκατάσταση κρίσιμης ενεργειακής υποδομής στην Ουκρανία, που αποδίδεται στο *APT28* (Ομάδα χάκερ-κατασκόπων).

Επίπτωση: Άγνωστη

31.08.2023 Το *CERT-UA* ανέφερε για μια κυβερνοεπίθεση που στόχευε ουκρανικές οντότητες, εκμεταλλευόμενη διάφορα τρωτά σημεία, που αποδίδονται στη *UNC1151* (Ομάδα χάκερ που πιστεύεται ότι συνδέεται με τις μυστικές υπηρεσίες της Λευκορωσίας).

Επίπτωση: Άγνωστη

31.08.2023 Ο *Solntsepek*, ένας φιλορώσος παράγοντας απειλών, διεξήγαγε μια επιχείρηση δυσφήμησης κατά του ιστότοπου μιας ουκρανικής κρατικής ιστοσελίδας.

Επίπτωση: Η πρώτη σελίδα του ιστότοπου παραμορφώθηκε και αντικαταστάθηκε από ένα φιλορωσικό μήνυμα.

19.07.2023 Ο *People's CyberArmy*, ένας φιλορώσος παράγοντας απειλών, διεξήγαγε μια επιχείρηση παραβίασης του ιστότοπου ενός ουκρανικού διαδικτυακού καταστήματος υλικού.

Επίπτωση: Η πρώτη σελίδα του ιστότοπου παραμορφώθηκε και αντικαταστάθηκε από ένα φιλορωσικό μήνυμα.

14.07.2023 Ο Λαϊκός Κυβερνοστρατός, ένας φιλορώσος παράγοντας απειλών, πραγματοποίησε επίθεση τύπου *DDoS* εναντίον του ιστότοπου ενός ουκρανικού ειδησεογραφικού μέσου.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

08.07.2023 Το *CERT-UA* έχει αναφέρει για επίθεση ψαρέματος *phishing* για τη λήψη δεδομένων ελέγχου ταυτότητας για υπηρεσίες δημόσιας αλληλογραφίας της Ουκρανίας. Η επίθεση έχει αποδοθεί και πάλι στο *APT28.*

Επίπτωση: Το *CERT-UA* ανακάλυψε αρχεία κανόνων διαμόρφωσης - εμφάνισης περιεχομένων *Hyper Text Markup Language – (HTML)* που μιμούνται τη διεπαφή των υπηρεσιών αλληλογραφίας που χρησιμοποιούνται για την εξαγωγή δεδομένων ελέγχου ταυτότητας που εισάγονται από τον στόχο χρησιμοποιώντας αιτήματα *HTTP POST*, μεταφέροντας τα κλεμμένα δεδομένα χρησιμοποιώντας προηγουμένως παραβιασμένες συσκευές καταγραφής - *Ubiquiti.*

07.07.2023 Ο *CERT-UA* έχει αναφέρει για μια κυβερνοεπίθεση που διανέμει κακόβουλο λογισμικό *PicassoLoader* κατά κυβερνητικών υπηρεσιών της Ουκρανίας.

Η κυβερνοεπίθεση έχει αποδοθεί στο *UAC-0057* γνωστό και ως *GhostWriter* και παρακολουθείται ως *UNC1151* από το *CyberPeace Institute.*

Επίπτωση: Με το *phishing* ως φορέα, ο παράγοντας απειλών διανέμει το κακόβουλο λογισμικό *PicassoLoader*. Μόλις αναπτυχθεί αυτό το κακόβουλο λογισμικό στη συνέχεια κατεβάζει και εκτελεί το βοηθητικό πρόγραμμα απομακρυσμένης πρόσβασης *njRAT* δίνοντας στον παράγοντα απειλής πρόσβαση στη συσκευή του στόχου και τη δυνατότητα να εξαπλωθεί σε όλο το δίκτυο της συσκευής.

05.07.2023 Κρατική Υπηρεσία Ειδικής Επικοινωνίας και Προστασίας Πληροφοριών της Ουκρανίας ανέφερε για κυβερνοεπίθεση εναντίον ουκρανικής κυβερνητικής υπηρεσίας. Ο φιλορώσος φορέας απειλών είχε στείλει ένα κακόβουλο λογισμικό - «υαλοκαθαριστήρων» που επηρέαζε ορισμένες συσκευές και έτσι μπόρεσε να αποκτήσει πρόσβαση στην επίσημη ιστοσελίδα της κυβερνητικής υπηρεσίας στο *Facebook*, όπου ανακοινώθηκε ότι η υπηρεσία είχε δεχτεί επίθεση και ότι είχαν κλαπεί δεδομένα. Ο Σόλτσενπεκ αναλαμβάνει την ευθύνη για την επίθεση.

Επίπτωση: Ο φορέας της απειλής χρησιμοποίησε «λογισμικό υαλοκαθαριστήρα» για να διακόψει αρκετούς σταθμούς εργασίας κρατικών υπαλλήλων προκειμένου να αποκτήσει πρόσβαση στην επίσημη σελίδα του στόχου στο *Facebook.* Στη συνέχεια, ο φορέας των απειλών δημοσίευσε μια ανάρτηση στην οποία ανέφερε ότι η υπηρεσία είχε δεχτεί επίθεση και ότι τα δεδομένα είχαν κλαπεί. Το *SSSCIP* η Κρατική Υπηρεσία Ειδικών Επικοινωνιών και Προστασίας Πληροφοριών της Ουκρανίας δήλωσε ότι το εταιρικό δίκτυο έχει αποσυνδεθεί και ότι ο ιστότοπος έχει ανασταλεί προσωρινά, αλλά ότι δεν προκλήθηκε ζημιά στους πόρους της Υπηρεσίας.

14.06.2023 Ένα ουκρανικό ειδησεογραφικό μέσο ανέφερε για μια κυβερνοεπίθεση που επηρεάζει τη διαθεσιμότητα ορισμένων ιστοσελίδων. Ο *Solntsepek,* ένας φιλορώσος παράγοντας απειλών, ανέλαβε την ευθύνη για την επίθεση.

Επίπτωση: Ορισμένοι ιστότοποι δεν ήταν προσωρινά διαθέσιμοι.

11.06.2023 Ο *People's CyberArmy,* ένας φιλορωσικός παράγοντας απειλών, διεξήγαγε επίθεση *DDoS* εναντίον του υποτομέα μιας ουκρανικής τράπεζας.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

23.05.2023 Η *Zarya* (Ρωσική νέα ομάδα hacking που γεννήθηκε από τη διαβόητη για τις κυβερνοεπιθέσεις της οργάνωση Killnet), διεξήγαγε επιχειρήσεις παραμόρφωσης κατά της ιστοσελίδας ενός ουκρανικού επιστημονικού ινστιτούτου.

Επίπτωση: Ο ιστότοπος παραμορφώθηκε και αντικαταστάθηκε από μια φιλορωσική δήλωση.

12.05.2023 Ο *CERT-UA* και η *Insikt Group* εντόπισαν μια εκστρατεία κυβερνοκατασκοπείας κατά οντοτήτων δημόσιας διοίκησης της Ουκρανίας. Στους στόχους στάλθηκαν μηνύματα ηλεκτρονικού ψαρέματος με νέα για τη σύγκρουση, ως δέλεαρ. Τα μηνύματα ηλεκτρονικού ψαρέματος εκμεταλλεύονταν τις ευπάθειες του *Roundcube*, θέτοντας άμεσα σε κίνδυνο τη συσκευή του στόχου. Στο στόχαστρο έγιναν περισσότερες από 40 ουκρανικές οργανώσεις. Η εκστρατεία έχει αποδοθεί στο φορέα απειλών *APT28.*

Επίπτωση: Στους στόχους στάλθηκαν μηνύματα ηλεκτρονικού ψαρέματος με νέα για τη σύγκρουση ως δέλεαρ. Τα μηνύματα ηλεκτρονικού ψαρέματος εκμεταλλεύονταν γνωστά τρωτά σημεία του *Roundcube*, θέτοντας αμέσως σε κίνδυνο τη συσκευή του στόχου μόλις ανοίξει το *email* του. Αυτό επέτρεψε στον παράγοντα απειλής να ανακατευθύνει τα μελλοντικά εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου ενός στόχου σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου ελεγχόμενη από τους φορείς απειλών και να δώσει πλήρη πρόσβαση στα εισερχόμενα του στόχου, επιτρέποντας στον παράγοντα απειλής να εξάγει δεδομένα από τα εισερχόμενα, συμπεριλαμβανομένου και του βιβλίου διευθύνσεων του στόχου. Περισσότερες από σαράντα οργανώσεις της Ουκρανίας στοχοποιήθηκαν με τέτοιου είδους *(email*).

01.03.2023 Το *KillNet* πραγματοποίησε επίθεση *DDoS* εναντίον της ιστοσελίδας ενός αντιπολιτευόμενου ρωσικού μέσου.

Επίπτωση: Η διακοπή σύνδεσης με τον ιστότοπο.

10.06.2022 Περισσότεροι από 500 παραλήπτες μεταξύ οργανισμών μέσων ενημέρωσης της Ουκρανίας (ραδιοφωνικοί σταθμοί, εφημερίδες, πρακτορεία ειδήσεων

κ.λπ.) έλαβαν ένα κακόβουλο *email* που περιείχε ένα αρχείο *docx* το οποίο αν ανοίξει θα παραδώσει το κακόβουλο λογισμικό *CrescentImp*.

Επίπτωση: Άγνωστη.

18.03.2022 Το *CERT-UA* ανέφερε εκστρατείες *phishing* εναντίον ουκρανικών οργανισμών που διέδωσαν την κερκόπορτα *LoadEdge*. Το περιστατικό αποδόθηκε στην *UAC-0035,* μια ομάδα χάκερ με φερόμενους δεσμούς με τη ρωσική ομάδα προηγμένης επίμονης απειλής *APT-(UAC-0010).*

Επίπτωση: Δεν είναι ακόμη γνωστή.

24.02.2022 Μια κυβερνοεπίθεση διέκοψε την ευρυζωνική δορυφορική πρόσβαση στο Διαδίκτυο που συνέπεσε με την εισβολή της Ρωσίας στην Ουκρανία. Η κυβερνοεπίθεση απενεργοποίησε τα μόντεμ που επικοινωνούν με τον δορυφόρο της εταιρείας επικοινωνίας Viasat, η οποία παρέχει πρόσβαση στο Διαδίκτυο σε ορισμένους πελάτες στην Ευρώπη, συμπεριλαμβανομένης της Ουκρανίας. Περισσότερο από δύο εβδομάδες αργότερα, ορισμένα παραμένουν εκτός σύνδεσης. Οι ερευνητές της *SentinelLabs* ανακάλυψαν ένα νέο κακόβουλο λογισμικό υαλοκαθαριστήρων που ονόμασαν *«AcidRain»*, το οποίο επιβεβαιώθηκε από την εταιρεία επικοινωνίας ότι χρησιμοποιήθηκε στην επίθεση στις 24 Φεβρουαρίου 2022 κατά των μόντεμ.

Επίπτωση: Πρόσβαση στο Διαδίκτυο εκτός σύνδεσης για περισσότερες από 2 εβδομάδες. Σχεδόν (9.000) συνδρομητές ενός παρόχου υπηρεσιών δορυφορικού Διαδικτύου στερήθηκαν το διαδίκτυο στη Γαλλία. Περίπου το ένα τρίτο των (40.000) συνδρομητών άλλου παρόχου υπηρεσιών δορυφορικού Διαδικτύου στην Ευρώπη (Γερμανία, Γαλλία, Ουγγαρία, Ελλάδα, Ιταλία, Πολωνία) επλήγησαν. Μια μεγάλη γερμανική ενεργειακή εταιρεία έχασε την πρόσβαση απομακρυσμένης παρακολούθησης σε περισσότερες από (5.800) ανεμογεννήτριες. Επηρέασε αρκετές χιλιάδες πελάτες που βρίσκονται στην Ουκρανία και δεκάδες χιλιάδες άλλους πελάτες σταθερής ευρυζωνικής σύνδεσης

23.02.2022 Οι ιστότοποι πολλών ουκρανικών τραπεζών και κυβερνητικών υπηρεσιών, συμπεριλαμβανομένων του Υπουργείου Εξωτερικών, του Υπουργείου Άμυνας, του Υπουργείου Εσωτερικών, της Υπηρεσίας Ασφαλείας *(SBU)* και του Υπουργικού Συμβουλίου έγιναν απρόσιτες μετά από μια μεγάλη επίθεση

τύπου *DDoS*. Οι περισσότεροι άλλοι ιστότοποι επανήλθαν στο διαδίκτυο μέσα σε δύο ώρες από την επίθεση, αλλά η καθυστέρηση και οι διακοπές συνεχίστηκαν και την επόμενη μέρα για άλλους.

Επίπτωση: Άγνωστη.

Όπως καταγράφεται στην έκθεση του Ευρωπαϊκού Κοινοβουλίου[59] στην οποία προαναφερθήκαμε, οι τύποι των κυβερνοεπιθέσεων που χρησιμοποιήθηκαν από τη Μόσχα εναντίον του Κιέβου μπορούν να διακριθούν σε:

1. Καταστροφικές επιθέσεις: Κυβερνοεπιθέσεις που αποσκοπούν στη μόνιμη διαγραφή δεδομένων ή στη βλάβη των συστημάτων καθιστώντας τα μη ανακτήσιμα.
2. Αποδιοργανωτικές επιθέσεις: Κυβερνοεπιθέσεις που έχουν στόχο τη διακοπή των υπηρεσιών σε ουκρανικούς οργανισμούς. Οι επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών DDoS ήταν οι πιο διαδομένοι τύποι επιθέσεων που παρατηρήθηκαν κατά τη διάρκεια αυτού του πολέμου, επηρεάζοντας ιδιαίτερα τον δημόσιο και τον χρηματοπιστωτικό τομέα.
3. Οπλοποίησης δεδομένων: Επιθέσεις στον κυβερνοχώρο που οδηγούν στην κλοπή δεδομένων για σκοπούς κατασκοπείας, παρακολούθησης ή πληροφόρησης και η διαρροή τους στον κυβερνοχώρο εξυπηρετώντας συγκεκριμένη στρατηγική.
4. Επιθέσεις παραπληροφόρησης: Ο τομέας του κυβερνοχώρου προσφέρεται ιδιαίτερα για τη διάδοση ψευδών πληροφοριών και τον αποπροσανατολισμό της κοινής γνώμης.

Να σημειώσουμε ότι η παραπάνω καταγραφή αφορά μόνο στις επιβεβαιωμένες επιθέσεις.

Είναι σημαντικό να αναφέρουμε ότι σύμφωνα με το Ινστιτούτο Cyber Peace κατά το τρίτο τρίμηνο του 2023 που αφορά η τελευταία δημοσιευμένη έκθεσή του, παρατηρήθηκε μείωση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο που διαπράττονται από φιλορωσικούς απειλητικούς φορείς με στόχο οντότητες στην Ουκρανία σε σχέση με το δεύτερο τρίμηνο του 2023[60]. Ο Sandworm-(21) φέρεται πως είναι ο πιο ενεργός κρατικά υποστηριζόμενος απειλητικός φορέας (hacker group) που διεξάγει κακόβουλες ενέργειες κατά Ουκρανικών οντοτήτων.

[59] Duguin S. & Pavlova P., p.8.
[60] Cyber Peace Institute, Quarterly Analysis Report - Q3 (July to September 2023) p.6.

3.2 Η καθοριστικότητα του πεδίου του κυβερνοχώρου και οι τεχνολογίες πληροφοριών και επικοινωνιών

Όπως είδαμε παραπάνω ο πόλεμος πληροφόρησης και προπαγάνδας με κυβερνοεπιθέσεις σε κρίσιμες υποδομές κι επίσης στον τομέα των μέσων κοινωνικής δικτύωσης (ιδίως από τη ρωσική πλευρά) ήταν από τα βασικά όπλα αυτού του κυβερνοπολέμου. Όλα παραπέμπουν σε ένα σταθερό ρωσικό μοτίβο χρήσης διαφόρων επιθετικών μέσων στον κυβερνοχώρο σε καιρό ειρήνης και πολέμου ως πολιτικά μέσα παρενόχλησης, ανατροπής ή και εξαναγκασμού. Η Ρωσία χρησιμοποιεί συστηματικά τέτοιες μεθόδους για να προβάλει την επιρροή της και να διαμορφώσει ευνοϊκά προς αυτή το πολιτικό περιβάλλον, διεξάγοντας μία μαζική εκστρατεία παραπληροφόρησης που απευθύνεται σε ένα ευρύ φάσμα ακροατηρίων τα οποία είναι: στο εσωτερικό της, στην Ουκρανία, στην Ευρώπη, τις ΗΠΑ ακόμα και στην Ασία και την Αφρική. Τα μέσα κοινωνικής δικτύωσης είναι ένα δίκτυο που παρέχει γόνιμο έδαφος για τη συλλογή πληροφοριών, τη διάδοση προπαγάνδας και τις ψυχολογικές επιχειρήσεις *(PSYOPS)*[61] ως μία ξεχωριστή – άλλου τύπου στρατιωτική δραστηριότητα με σκοπό να επηρεαστεί η κοινή γνώμη, να διασπείρουν αμφιβολίες και να οδηγήσουν τους αντιπάλους σε λάθος εκτιμήσεις και αποφάσεις. Αυτές οι ενέργειες αποσκοπούν στον επηρεασμό των αντιλήψεων, των στάσεων και των συμπεριφορών των πληθυσμών ως στόχους[62]. Χρησιμοποιούνται για να προετοιμάσουν φυσικές επιθέσεις και να υποστηρίξουν ή να συνοδεύσουν εχθρικές στρατιωτικές δράσεις στο έδαφος. Στις μέρες μας οι επιθέσεις στον κυβερνοχώρο έχουν αντικαταστήσει σημαντικά τις φυσικές δολιοφθορές σε κρίσιμες υποδομές.

Στην Ουκρανία, οι ρωσικές κυβερνοεπιθέσεις δημιούργησαν φόβο, αβεβαιότητα και αμφιβολίες σχετικά με την οικονομική, πολιτιστική και εθνική ασφάλεια της Ουκρανίας, ενώ παράλληλα προώθησαν υποστηρικτικά μηνύματα για το ρόλο της Ρωσίας στην Κριμαία και την ανατολική Ουκρανία[63]. Επομένως τα κράτη πρέπει να είναι κατάλληλα προετοιμασμένα να αντιμετωπίσουν αυτές τις απειλές προτάσσοντας την απαραίτητη άμυνα απέναντι σε τέτοιες επιθέσεις, με πρώτο βήμα τον έγκαιρο εντοπισμό τους, την αποτελεσματική αμφισβήτησή τους και την ανάπτυξη μίας ανθεκτικής πολιτικής αφήγησης που να αντέχει στην ψευδή προπαγάνδα. Οι στρατηγικές επικοινωνίες *StratCom* είναι ένας τρόπος σκέψης

---

[61] Lange-Ionatamishvili E. & Svetoka S.,*Strategic Communications and Social Media In the Russia Ukraine Conflict*, Ch. 12, στο: Cyber War in Perspective: Russian Aggression against Ukraine, p.105, https://ccdcoe.org/uploads/2018/10/Ch12_CyberWarinPerspective_Lange_Svetoka.pdf , (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

[62] Lange-Ionatamishvili E. & Svetoka S, σ.107.

[63] Geers K., *Introduction: Cyber War in Perspective*, Ch.1, στο: Cyber War in Perspective: Russian Aggression against Ukraine, p.18., https://ccdcoe.org/uploads/2018/10/Ch01_CyberWarinPerspective_Geers.pdf, , (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

που βάζει στο επίκεντρο της στρατηγικής την επικοινωνία. Αυτό σημαίνει ότι οι δραστηριότητες των κρατών βασίζονται στην αφήγηση και αυτή την ενέργεια την επικοινωνούν σε διαφορετικά ακροατήρια μέσω συντονισμένων λέξεων, εικόνων και πράξεων στα μέσα κοινωνικής δικτύωσης που χρησιμοποιούν. Στην αρχή της σύγκρουσης, είδαμε τη στρατηγική επικοινωνία σε δράση. Μέσω των πλατφορμών του *Twitter* και του *YouTube,* άγνωστοι επιτιθέμενοι δημοσιοποίησαν μια υποκλαπείσα τηλεφωνική συνομιλία μεταξύ της βοηθού υπουργού Εξωτερικών των ΗΠΑ *Victoria Nuland* και του *Geoffrey Pyatt,* πρέσβη των ΗΠΑ στην Ουκρανία[64]. Με αυτή την κίνηση, οι δράστες προσπάθησαν να δυσφημίσουν τη δυτική πολιτική και να ανακοινώσουν την πρόσβασή τους στις δυτικές γραμμές κυβερνητικής επικοινωνίας. Έτσι, πραγματοποιήθηκε η τεχνική εκμετάλλευση ενός ξένου πληροφοριακού συστήματος όσο και μια ψυχολογική επίθεση κατά της Δύσης με τη χρησιμοποίηση των μέσων κοινωνικής δικτύωσης. Πολυάριθμες αναρτήσεις στα μέσα κοινωνικής δικτύωσης φαίνεται πως διαδόθηκαν με σκοπό τη χειραγώγηση των ανθρώπων στην ανατολική Ουκρανία.

Ο κυβερνοχώρος διαδραματίζει ολοένα και σημαντικότερο ρόλο στη στρατηγική επικοινωνίας, καθώς η εξάρτησή μας από τις σύγχρονες τεχνολογίες, τα δίκτυα υπολογιστών και το διαδίκτυο αυξάνεται διαρκώς. Ωστόσο, η σύγκρουση στην Ουκρανία έδειξε ότι ο κυβερνοχώρος μπορεί επίσης να διαδραματίσει ρόλο στη διεξαγωγή μιας επιχείρησης με βάση την αφήγηση, όπου οι κύριοι στόχοι δεν είναι οι μηχανές ή τα δίκτυα αλλά τα μυαλά των ανθρώπων. Η οπλοποίηση των μέσων κοινωνικής δικτύωσης μπορεί να παρομοιαστεί με μία κοινωνική κυβερνοεπίθεση[65] η οποία περιλαμβάνει δράση με ψευδή ή και ανώνυμα προσχήματα είτε με την απελευθέρωση ενός παραποιημένου σήματος στα μέσα κοινωνικής δικτύωσης είτε ακόμη με την εσκεμμένη αλλαγή ενός υπάρχοντος σήματος, προκειμένου να επιτευχθούν επιθυμητά αποτελέσματα δηλαδή χάος, πανικός, μαζικές διαταραχές, όπως ορίζεται από τη Δρ. Rebecca Goolsby[66]. Αυτός ο τύπος των κυβερνοεπιθέσεων προσφέρει μία διαφορετική άποψη σε σχέση με τις παραδοσιακές απόψεις για τις επιθέσεις στο κυβερνοπεριβάλλον, καθώς τα αποτελέσματα αυτών των επιθέσεων είναι καθαρά ψυχολογικά. Άλλωστε η διάδοση φημών είναι μία από τις πιο αποτελεσματικές τακτικές κοινωνικής κυβερνοεπίθεσης. Το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης, λόγω της ικανότητάς τους να πολλαπλασιάζουν τις πληροφορίες με μεγάλη ταχύτητα και μικρό κόστος, χρησιμοποιούνται όλο και περισσότερο για προπαγάνδα, πόλεμο πληροφοριών και

[64] Lange-Ionatamishvili E. & Svetoka S., p. 107.
[65] Ό.π., p. 105.
[66] Ό.π., p.106.

επιχειρήσεις επιρροής, οι οποίες μπορούν να αλλάξουν αισθητά τόσο την αντίληψη όσο και τη συμπεριφορά του κοινού-στόχου[67]. Πρόκειται για ένα εξαιρετικά δυναμικό, καθοδηγούμενο από τους χρήστες συνεχώς μεταβαλλόμενο περιβάλλον, όπου είναι εύκολο να γίνει ένα μήνυμα - *viral.* Αξίζει να αναφέρουμε ότι στις 21 Ιουλίου 2022 σημειώθηκε μία επιβεβαιωμένη κυβερνοεπίθεση σε Ουκρανικό ραδιοφωνικό σταθμό κατά την οποία οι δράστες μετέδωσαν μια φωνή που έλεγε ότι ο Ουκρανός πρόεδρος βρισκόταν στην εντατική και ισχυρίζονταν ψευδώς ότι ο πρόεδρος του Ανώτατου Συμβουλίου της Ουκρανίας που αποτελεί τη νομοθετική εξουσία της χώρας, θα αναλάμβανε τα καθήκοντα του Προέδρου[68]. Σύμφωνα με τον Martin Libicki[69], το γεγονός ότι οι δύο χώρες μοιράζονται μια κοινή γλώσσα, τη ρωσική, έκανε τα πράγματα ευκολότερα για τη Μόσχα στις κυβερνο-επιθέσεις της με στόχο την παραπληροφόρηση στα Ουκρανικά μέσα μαζικής δικτύωσης.

Το πόσο καθοριστικό είναι το πεδίο του κυβερνοχώρου και οι τεχνολογίες πληροφοριών και επικοινωνιών για τη διεξαγωγή του πολέμου αυτού μπορεί να γίνει αντιληπτό από το γεγονός ότι η ρωσική εισβολή στην Ουκρανία συνοδεύτηκε από εντατικές επιθέσεις στον κυβερνοχώρο, που περιελάμβαναν τακτικές κατανεμημένης άρνησης παροχής υπηρεσιών DDoS, εναντίον υπολογιστικών συστημάτων στο Κίεβο. Για τους επιτιθέμενους είναι σημαντικό να περιορίσουν τη δυνατότητα των τοπικών πολιτικών και στρατιωτικών ηγετών του αντιπάλου να κάνουν σωστή εκτίμηση των γεγονότων που εξελίσσονται γρήγορα και να δημιουργήσουν αμφιβολίες και σύγχυση στο αντίπαλο στρατόπεδο. Με αυτό τον τρόπο μπορεί να κερδηθεί πολύτιμος χρόνος τις κρίσιμες ώρες και ημέρες που εξελίσσεται η φυσική επίθεση. Όπως αποδείχτηκε, η ουκρανική ψηφιακή υποδομή (ιδίως οι πύργοι κινητής τηλεφωνίας και οι διακομιστές δεδομένων) μπόρεσε να απορροφήσει ικανοποιητικά μαζικές ρωσικές πυραυλικές καθώς και κυβερνοεπιθέσεις και να συνεχίσει να λειτουργεί, παρά κάποιες προσωρινές διακοπές.

Οι ψηφιακές πληροφορίες, οι τηλεπικοινωνίες, η πλοήγηση και τα μέσα μαζικής επικοινωνίας είναι ζωτικής σημασίας για τις σύγχρονες πολεμικές επιχειρήσεις όπου πολλές από αυτές λαμβάνουν χώρα πλέον και στο διάστημα ή μέσω αυτού π.χ. η επίθεση στη *Viasat*[70] ή ακόμη και άλλες προσπάθειες παρεμπόδισης δορυφορικών επικοινωνιών που επιχειρήθηκαν.

[67] Lange-Ionatamishvili E. & Svetoka S., p. 106.
[68] Cyber Peace Institute, *Cyber Dimensions of the armed conflict in Ukraine*, Quarterly Analysis Report - Q3 (July to September 2022), p.5, στο: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2022/ (δημοσιεύτηκε 16.12.2022).
[69] Libicki M., p.51.
[70] Levite A,E, p.8,

Σύμφωνα με τον James A. Lewis[71], η αποτελεσματικότητα των κυβερνοεπιθέσεων κρίνεται από το κατά πόσον η κυβερνοεπιχείρηση ανάγκασε τον αντίπαλο να κάνει παραχωρήσεις ή να αλλάξει τη στρατηγική του, κάτι που δεν φάνηκε να συμβαίνει μέχρι τώρα στην περίπτωση του Ρωσο-ουκρανικού πολέμου. Επίσης διαπιστώνεται ότι οι ζημιές που μπορούν να επιφέρουν οι κυβερνοεπιθέσεις σε πολλές περιπτώσεις δεν είναι μόνιμη, όπως είναι για παράδειγμα η κατεδάφιση κτιρίων από βομβαρδισμούς[72].

3.3 Ποια είναι τα μαθήματα που αντλούμε σε σχέση με αυτή τη διένεξη στον κυβερνοχώρο:

Από τη μέχρι τώρα εμπειρία και καθώς ο πόλεμος μεταξύ Ρωσίας- Ουκρανίας συνεχίζεται ακόμα, η διεθνής κοινότητα και κυρίως τα επιτελεία των κρατών φαίνεται ότι μπορούν να αντλήσουν ήδη διδάγματα από τη πολεμική διένεξη των δύο κρατών στον κυβερνοχώρο. Όπως πάντα, τα μαθήματα εξαρτώνται από την πλευρά που βρίσκονται οι ενδιαφερόμενοι, δηλαδή την πολιτική, στρατιωτική, οικονομική, τηλεπικοινωνιακή, επικοινωνιακή ή κοινωνική πλευρά, του επιτιθέμενου ή του αμυνόμενου, επομένως είναι διαφορετικά για τους διάφορους αποδέκτες. Συνοψίζοντας θα αναφέρουμε τα παρακάτω:

Οι κυβερνοεπιθέσεις και οι επιχειρήσεις στον κυβερνοχώρο αποτελούν πλέον έναν καθιερωμένο τύπο στρατιωτικής επιχείρησης και συντονίζονται ή συγχρονίζονται με κινητικές στρατιωτικές επιχειρήσεις. Αυτός ο συνδυασμός είναι αποδιοργανωτικός και αποσταθεροποιητικός. Σε τακτικό επίπεδο, διαπιστώνουμε ότι οι κυβερνοεπιθέσεις παρέχουν πλεονεκτήματα όταν συνδυάζονται με συμβατικά όπλα. Για παράδειγμα, μια κυβερνοεπίθεση μπορεί να αχρηστεύσει ή να προκαλέσει σύγχυση στα δίκτυα διοίκησης του αντιπάλου, ώστε οι κινητικές επιθέσεις του εισβολέα να στοχεύουν με μεγαλύτερη αποτελεσματικότητα. Ο επιτυχής συντονισμός κυβερνο- και κινητικών ενεργειών απαιτεί υψηλό βαθμό σχεδιασμού[73].

Οι εξελιγμένες κυβερνοεπιθέσεις όπως αυτή στη Viasat απαιτούν τεράστια προετοιμασία και παίρνουν χρόνο. Σύμφωνα με τον Economist[74], η επίθεση της GRU, της Ρωσικής

---

[71] Lewis J.A, p.2.
[72] Ό.π.
[73] Ό.π., pp. 3-4.
[74] Economist Article : *Lessons from Russia's cyber-war in Ukraine* στο: https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=Cj0KCQiAkeSsBhDUARIsAK3tiefyBGjitsk6VMkTtgF9-KCDIFZgfsyl-4zr_wcWfMcijlrDoOwtwIMaAqwDEALw_wcB&gclsrc=aw.ds, δημοσιεύτηκε στις 03.12.2022 (άγνωστου συγγραφέα).

στρατιωτικής υπηρεσίας πληροφοριών με το παραπάνω ακρωνύμιο (Κεντρικό Διευθυντήριο Πληροφοριών), χρησιμοποίησε μία κυβερνο-ομάδα hacker (που έδρασε τοπικά αλλά και εξ' αποστάσεως) και χτύπησε το κεντρικό δίκτυο ηλεκτρικής ενέργειας της Ουκρανίας το 2015. Για αυτή της την ενέργεια είχαν απαιτηθεί δέκα εννέα μήνες σχεδιασμού, ενώ για την επίθεση που πραγματοποίησε το 2016 απαιτήθηκαν δυόμιση χρόνια.

Όπως σημειώνεται, η πραγματοποίηση τέτοιων επιθέσεων έχει το μειονέκτημα ότι αποκαλύπτει στον αντίπαλο τα εργαλεία (δηλαδή τον κώδικα) και την υποδομή (διακομιστές) που χρησιμοποιούνται με αποτέλεσμα να αποκαλύπτονται κρίσιμες πληροφορίες της στρατηγικής και του εξοπλισμού που διαθέτει ο επιτιθέμενος και επομένως να τον κάνουν ευάλωτο σε αντίποινα. Μέχρι σήμερα, οι επιχειρήσεις στον κυβερνοχώρο από μόνες τους δεν εγγυώνται την επίτευξη των στρατηγικών στόχων στις ένοπλες συγκρούσεις. Όπως φαίνεται, αυτές μπορούν να καταστρέψουν χρήσιμες υποδομές, να διασπείρουν ψευδές ειδήσεις και να επηρεάσουν ψυχολογικά τον αντίπαλο, οι μάχες όμως στο πεδίο είναι αυτές που κερδίζουν τον πόλεμο. Οι κυβερνοεπιθέσεις επομένως δεν φαίνεται πως είναι μία εφαρμογή-δολοφόνος όπως κάποιοι περίμεναν[75].

Ο κυβερνοπόλεμος φαίνεται να έχει περιορισμένες επιπτώσεις καθώς ο αμυνόμενος εντοπίζει τις αδυναμίες του και τις διορθώνει. Στην περίπτωση του Ρωσο-ουκρανικού πολέμου, η Ουκρανία αναγνωρίζοντας ότι έχει γίνει αντικείμενο κυβερνοεπιθέσεων τα προηγούμενα χρόνια όπως προαναφέραμε, κατάφερε να προετοιμαστεί και να αναπτύξει αποτελεσματικά την άμυνά της στον κυβερνοχώρο μετριάζοντας έτσι τις επιπτώσεις των κυβερνοεπιθέσεων[76]. Η Ουκρανία κατάφερε να ενισχύσει την ανθεκτικότητα της εθνικής υποδομής της σε ό,τι αφορά τον τομέα των τηλεπικοινωνιών και της πληροφορικής για την αντιμετώπιση περιστατικών στον κυβερνοχώρο πριν και κατά τη διάρκεια του πολέμου, σε συνεργασία με συμμαχικές κυβερνήσεις και ιδιωτικές εταιρείες[77].

Ο ιδιωτικός τομέας της Ουκρανίας συμμετείχε σ' αυτό το σκοπό επίσης σε σημαντικό βαθμό. Με την έναρξη του πολέμου ιδιωτικοί φορείς όπως η Microsoft, η Google και η Amazon αναγνώρισαν δημόσια τη συνεισφορά τους σε ό,τι αφορά στον εντοπισμό και την πρόβλεψη απειλών στον κυβερνοχώρο και τη συμμετοχή τους σε άλλες μορφές συνεργασίας με την Ουκρανία ώστε να θωρακιστεί η χώρα κατά των Ρωσικών κυβερνοαπειλών[78].

[75] Economist Article : *Lessons from Russia's cyber-war in Ukraine* (βλπ παραπομπή 74).
[76] Duguin S. & Pavlova P., p.7.
[77] Ό.π.
[78] Ό.π.

Σύμφωνα με τον Economist[79], όταν άρχισε η εισβολή, η κυβερνοδιοίκηση της Ουκρανίας είχε έτοιμο ένα σχέδιο έκτακτης ανάγκης. Ορισμένοι αξιωματούχοι διασκορπίστηκαν από το Κίεβο σε ασφαλέστερα μέρη της χώρας. Άλλοι μετακινήθηκαν σε θέσεις διοίκησης κοντά στις γραμμές του μετώπου. Κρίσιμες υπηρεσίες μεταφέρθηκαν σε κέντρα δεδομένων αλλού στην Ευρώπη, εκτός της εμβέλειας των ρωσικών πυραύλων. Οι ένοπλες δυνάμεις της Ουκρανίας, γνωρίζοντας ότι οι δορυφόροι μπορούσαν να διαταραχθούν, είχαν προετοιμάσει εναλλακτικά μέσα επικοινωνίας.

Η ανθεκτικότητα επομένως του αντιπάλου στις κυβερνοεπιθέσεις κτίζεται με το χρόνο και αφαιρεί από τον επιτιθέμενο την ικανότητα να χτυπήσει καίρια υποδομές όταν έχει χάσει και το πλεονέκτημα του αιφνιδιασμού. Η ικανότητα άμεσης και αποτελεσματικής αντίδρασης στις κυβερνοεπιθέσεις φαίνεται πως είναι το κλειδί της επιτυχημένης άμυνας.

Η χρήση του κυβερνοχώρου στον πόλεμο Ρωσίας-Ουκρανίας δεν περιορίστηκε στους κρατικούς φορείς Μόσχας και Κιέβου αλλά παρατηρήθηκε μεγάλης κλίμακας συμμετοχής μη κρατικών φορέων[80]. Οι κυβερνοαπειλές μπορούν πλέον να προέρχονται από εθνικά κράτη αλλά και φορείς που συνδέονται με εθνικά κράτη, συλλογικότητες, χακτιβιστές, καθώς και ομάδες κυβερνοεγκληματιών. Σύμφωνα με το Ινστιτούτο Cyber Peace[81], από την έναρξη του πολέμου μέχρι τις 31 Μαίου 2023 καταγράφηκαν κυβερνοεπιθέσεις από εννενήντα οκτώ διαφορετικούς φορείς, ενώ το 80% αυτών των επιθέσεων χαρακτηρίζονται ως «αυτοαποδιδόμενες», δηλαδή μη προερχόμενες από κρατικούς φορείς Μόσχας-Κιέβου επιθέσεις, όπου οι φορείς των απειλών αποκαλύπτουν δημόσια την κυβερνοεπίθεση και αποδίδουν στην ομάδα τους την ιδιότητα του δράστη πίσω από την επίθεση. Όπως έχουν παραδεχθεί και οι δύο πλευρές, με την έναρξη του πολέμου αυτές ζήτησαν την υποστήριξη ατόμων που ήθελαν και μπορούσαν να ενταχθούν σε έναν «κυβερνοστρατό» για να υποστηρίξουν με τις γνώσεις και τις ικανότητές τους τις κυβερνοεπιθέσεις που σχεδίαζαν τα επιτελεία των δύο χωρών.

Το Killnet είναι μια ομάδα χακτιβιστών που συνδέεται με τη Ρωσία και είναι ιδιαίτερα ενεργό σε επιθέσεις DDoS. Ο Στρατός Πληροφορικής της Ουκρανίας είναι ένας λιγότερο συμβατικός παίκτης που κατευθύνει τις κυβερνοενέργειές του με επιθέσεις DDoS καταφέροντας πλήγματα σε ρωσικές διαδικτυακές υποδομές.

Με την έναρξη του πολέμου το Υπουργείο Ψηφιακού Μετασχηματισμού της

[79] Economist Article: *Lessons from Russia's cyber-war in Ukraine* (βλπ παραπομπή 74).
[80] Duguin S. & Pavlova P., pp. 9-10.
[81] Ό.π., p. 10.

Ουκρανίας ανακοίνωσε πρόσκληση για ένα στρατό ειδικών πληροφορικής που θα μπορούσε να πολεμήσει για την Ουκρανία στον κυβερνοχώρο. Σ' αυτή την πρόσκληση ανταποκρίθηκαν, εκτός από Ουκρανούς, ειδικοί από όλο τον κόσμο σαν αποτέλεσμα της διεθνούς κατακραυγής για τη ρωσική επίθεση, πράγμα που ήγειρε ερωτήσεις για τους πιθανούς κινδύνους που μπορεί να προκύπτουν για την ασφάλεια των άμαχων ειδικών που συμμετέχουν στον κυβερνοπόλεμο και άνοιξε ένα καινούργιο κεφάλαιο στο Διεθνές Ανθρωπιστικό Δίκαιο[82] σχετικά με τον ορισμό του άμαχου και του συμμετέχοντα σε ένοπλη σύρραξη.

Τέλος, η συμμετοχή ομάδων εθελοντών στις κυβερνοεπιθέσεις που δεν έχουν την κατάλληλη εκπαίδευση σχετικά με τους κανόνες εμπλοκής δημιουργεί προκλήσεις για την απόδοση ευθυνών και ασάφεια όσον αφορά τον πραγματικό δράστη. Ο κυβερνοχώρος έτσι μετατρέπεται σε ένα άναρχο πεδίο δράσης όπου οι εμπόλεμες χώρες αδυνατούν να ελέγξουν τις εξελίξεις, πράγμα επικίνδυνο ακόμα κι αν τα αποτελέσματα είναι υπέρ τους. Σημειώνεται ότι σύμφωνα με το Ινστιτούτο Cyber Peace, τόσο οι φιλορωσικοί όσο και οι φιλοουκρανικοί φορείς απειλών διεξάγουν ακόμα και σήμερα κυβερνοεπιθέσεις με στόχο χώρες εκτός της Ρωσίας και της Ουκρανίας[83], πράγμα που μπορεί να επηρεάσει τις διεθνείς σχέσεις και την οικονομία παγκοσμίως.

Η χρήση κυβερνοεπιθέσεων και επιχειρήσεων στο πλαίσιο του πολέμου στην Ουκρανία έχει μια σημαντική ανθρώπινη συνιστώσα. Αυτές οι επιθέσεις για παράδειγμα σε εταιρείες ενέργειας ή τηλεπικοινωνιών, τράπεζες, τη δημόσια διοίκηση ή σε φορείς υγείας, μπορεί να εκθέσουν τον άμαχο πληθυσμό σε σοβαρούς κινδύνους, καθώς βασικές υπηρεσίες για την κοινωνία και τις οικονομίες εξαρτώνται από αυτές τις υποδομές. Κυβερνοεπιθέσεις με την ανάπτυξη κακόβουλου λογισμικού wiper όπως αυτές που έγιναν εναντίον Ουκρανικών οργανισμών, μπορούν να οδηγήσουν στη διαγραφή δεδομένων καθιστώντας τα μη ανακτήσιμα. Επίσης η διακοπή της λειτουργίας υπηρεσιών επηρεάζουν την καθημερινότητα των πολιτών και δημιουργούν ανασφάλεια. Η παραπληροφόρηση μπορεί να δημιουργήσει χάος και πλήττει την ψυχολογία των απλών πολιτών. Επιπλέον, οι επιχειρήσεις στον κυβερνοχώρο προσθέτουν άλλο ένα επίπεδο αβεβαιότητας όσον αφορά τη ζημιά στον πληθυσμό, καθώς ο αντίκτυπος στα

[82] Duguin S. & Pavlova P., p.11.
[83] Cyber Peace Institute, Quarterly Analysis Report - Q3 (July to September 2023) p.3.

θύματα μπορεί σε ορισμένες περιπτώσεις να διαπιστωθεί μόνο με χρονική καθυστέρηση ή να είναι έμμεσος, αλλά να προκαλεί ζημία[84].

Κάτι άλλο που είναι σημαντικό να αναφερθεί είναι η χρήση των κινητών τηλεφώνων από τους ιδιώτες και η δυνατότητα του πληθυσμού να παρέχει πληροφορίες άμεσα στον ψηφιακό κόσμο τη στιγμή που συμβαίνουν τα γεγονότα. Αυτό σημαίνει ότι ο έλεγχος της πληροφορίας από τις κρατικές υπηρεσίες στις μέρες μας είναι εξαιρετικά δύσκολη υπόθεση καθώς η πληροφορία είναι πλέον δημόσια διαθέσιμο αγαθό[85]. Αυτές οι δημόσιες, μη κυβερνητικές πηγές πληροφοριών υπονομεύουν κάθε προσπάθεια ελέγχου της αφήγησης και ενημερώνουν τόσο το εσωτερικό όσο και τη διεθνή κοινότητα για το τι πραγματικά συμβαίνει.

Ο πόλεμος στην Ουκρανία επίσης διδάσκει ότι για τα κράτη είναι ζωτικής σημασίας οι επενδύσεις στις υποδομές τηλεπικοινωνιών και εξοπλισμού αιχμής καθώς και η διατήρηση εναλλακτικών καναλιών. Επίσης υπάρχει αυξημένη ανάγκη τεχνικής και τακτικής ικανότητας καθώς και επάρκεια δυνάμεων στο επίπεδο του κυβερνοχώρου παράλληλα με την ύπαρξη στρατηγικής. Θα πρέπει να αναφερθεί ότι παρόλες τις ενέργειες που έχουν πραγματοποιήσει τα κράτη για την αντιμετώπιση του κινδύνου του κυβερνοπολέμου, πρέπει να αναδιαμορφώσουν το στρατιωτικό τους σχεδιασμό περαιτέρω. Επιπλέον πρέπει τα κράτη να χαράξουν νέες πολιτικές τακτικές, έτσι ώστε να υπάρχει πάντα η κατάλληλη προετοιμασία ενόψει του ενδεχομένου διεξαγωγής αυτού του σύγχρονου είδους πολέμου. Αναδεικνύεται η σημασία της δράσης στον κυβερνοχώρο τόσο σε καιρό ειρήνης όσο και πολέμου μα και σε καταστάσεις όπου οι προθέσεις του αντιπάλου είναι αδιευκρίνιστες. Επισημαίνεται ότι τα ψηφιακά δεδομένα και οι πληροφορίες στον κυβερνοχώρο μπορεί να εμφανίζονται αλλοιωμένα ως προς την εμπιστευτικότητα, την ακεραιότητα, την προέλευση και τη διαθεσιμότητά τους, επειδή όλοι ανεξαιρέτως οι δρώντες μπορούν να διεξάγουν εκτεταμένες επιχειρήσεις πληροφοριών και παραπληροφόρησης στο πεδίο αυτό[86].

Οι αναλυτές σημειώνουν την ανάγκη της συνεργασίας μεταξύ των κρατών και των ιδιωτικών εταιρειών ώστε το ανθρώπινο δυναμικό των επιτελείων να λαμβάνει την κατάλληλη εκπαίδευση και να είναι συνεχώς ενημερωμένο για τις δυνατότητες που προσφέρει η τεχνολογία σχετικά με τις κυβερνοεπιθέσεις.

[84] Duguin S. & Pavlova P., p. 13.

[85] Lewis J.A, p.10.

[86] Duguin S. & Pavlova P., p. 13.

Τέλος, είναι σημαντικό να αυξηθεί η συνεργασία μεταξύ των κρατών ώστε να είναι εφικτή η ενημέρωση όλων των μερών σχετικά με την κατάσταση που επικρατεί στον κυβερνοχώρο, τη δραστηριότητα παλαιών και νέων φορέων απειλών, δηλαδή να μοιράζεται η πληροφόρηση μεταξύ των μυστικών υπηρεσιών για να αυξηθεί η κυβερνοασφάλεια και να είναι πιο αποτελεσματική η κυβερνοάμυνα[87]. Σύμφωνα με τους Grace Mueller, Benjamin Jensen, Brandon Valeriano, Ryan Maness and Jose Macias είναι ευκολότερο να αμυνθεί κανείς εναντίον του κακόβουλου λογισμικού παρά στην παραπληροφόρηση[88].

Οι προκλήσεις στην αντιμετώπιση της διασποράς ψευδών ειδήσεων και της προπαγάνδας είναι τόσο μεγάλες που καμία μεμονωμένη υπηρεσία ή πολιτική δεν μπορεί να τις αντιμετωπίσει. Επομένως η αλληλεγγύη και η σύμπραξη των κρατών είναι απαραίτητη προς αυτή την κατεύθυνση όποια και εάν είναι η ιδεολογική και πολιτική τους τοποθέτηση.

4. Συμπεράσματα

Από το Φεβρουάριο 2022 η διεθνής κοινότητα παρακολουθεί τις εξελίξεις στη σύγκρουση Μόσχας - Κιέβου και μετρά τις επιπτώσεις τόσο για τις δύο εμπλεκόμενες χώρες όσο και για τον υπόλοιπο κόσμο. Η εισβολή της Ρωσίας στην Ουκρανία δεν στηρίχτηκε μόνο στη χρήση στρατευμάτων αλλά συνοδεύτηκε από επιθέσεις στον κυβερνοχώρο υποστηρικτικές για τις παραδοσιακές στρατιωτικές δυνάμεις. Ο πόλεμος αυτός επιβεβαιώνει ότι ο κυβερνοχώρος αποτελεί ένα νέο τομέα πολέμου, συμπληρωματικό της ξηράς, του αέρα και της θάλασσας, πράγμα που σημαίνει ότι τα επιτελεία των κρατών θα πρέπει να είναι προετοιμασμένα ανάλογα καθώς όπως φαίνεται ο κυβερνοπόλεμος δεν είναι κάτι πρόσκαιρο αλλά ήρθε για να μείνει.

Στις σελίδες που προηγήθηκαν διαπιστώσαμε ότι ο κυβερνοπόλεμος μεταξύ Ρωσίας-Ουκρανίας δεν ήταν ο πρώτος που σημειώθηκε διεθνώς μέχρι τη στιγμή που ξέσπασε, όμως αποτελεί την πρώτη εμπόλεμη σύγκρουση στην οποία οι κυβερνοεπιθέσεις διεξήχθησαν σε μεγάλη κλίμακα και όπως είδαμε, αυτές συνεχίζονται μέχρι και σήμερα κι από τις δύο πλευρές και καθώς ο φυσικός πόλεμος συνεχίζεται μέχρι κι αυτή τη στιγμή.

[87] Lewis J.A, p.11.

[88] Mueller, G, Jensen B.,Valeriano B., Maness R, Macias J., *Cyber Operations during the Russo-Ukranian War: From Strange Patterns to Alternative Futures*, Recommendation 3: Reassess How to Counter Cyber-Enabled Information Operations, στο: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-russian-cyber-operations (δημοσιεύτηκε στις 01.07.2023).

Από το 2010 μέχρι το 2017 έχουν καταγραφεί ισχυρές διακρατικές κυβερνοεπιθέσεις κακόβουλου λογισμικού όπως ήταν το Stuxnet , το Black Energy, το Wanna Cry και το NotPetya, τα οποία επηρέασαν κρίσιμες υποδομές σε πολλές χώρες παγκοσμίως και συντάραξαν την κοινή γνώμη. Στην περίπτωση που εξετάσαμε και με βάση τις δημόσια διαθέσιμες πληροφορίες, φαίνεται ότι το 2022 η Ρωσία ξεκίνησε τις κακόβουλες ενέργειες λίγο πριν την εισβολή στην Ουκρανία ενώ οι μεγαλύτερες σε έκταση κυβερνοεπιθέσεις έλαβαν χώρα από την πρώτη ημέρα της εισβολής και είχαν σαν στόχο να πλήξουν κρίσιμες υποδομές όπως ήταν η Ουκρανική εταιρεία ενέργειας, η δημόσια διοίκηση, ο τραπεζικός τομέας, τα μέσα ενημέρωσης και κοινωνικής δικτύωσης αλλά κυριότερα η εταιρεία δορυφορικής επικοινωνίας Viasat, επηρεάζοντας όχι μόνο τις ουκρανικές τηλεπικοινωνίες αλλά και αυτές άλλων χωρών. Αυτή η κυβερνοεπίθεση φαίνεται πως είναι η σημαντικότερη που γνώρισε η διεθνής κοινότητα μετά το 2017, δεδομένου του αντίκτυπου που αυτή προκάλεσε σε χώρες εκτός των δύο αντιμαχομένων πλευρών.

Όπως παρατηρήσαμε, οι κυβερνοεπιθέσεις πέρα από τον καταστροφικό, τον αποδιοργανωτικό και τον εκφοβιστικό τους ρόλο, είχαν σκοπό την υποκλοπή πληροφοριών και την παραπληροφόρηση. Η πληροφορία αποτελεί διαχρονικά ισχυρό όπλο και η πληροφόρηση την καρδιά της προετοιμασίας των επιτελείων για τον πόλεμο και τον χειρισμό της κοινής γνώμης μέσω του διαδικτύου. Το διαδίκτυο λογίζεται ως κάτι που το έφτιαξε η ίδια η ανθρωπότητα και που δυστυχώς δεν μπορεί να το κατανοήσει επαρκώς.

Η κυβερνοπληροφόρηση στη σύγκρουση Μόσχας-Κιέβου πήρε τη μορφή της οπλοποίησης δεδομένων και της προπαγάνδας. Οι επιθέσεις στον κυβερνοχώρο που προηγήθηκαν της εισβολής είχαν σαν αποτέλεσμα τη συλλογή πληροφοριών και δεδομένων απαραίτητων από τη Ρωσική πλευρά στα πλαίσια της προετοιμασίας για τον πόλεμο. Η παραπληροφόρηση και η διάδοση ψευδών ειδήσεων είχαν στόχο τον επηρεασμό της κοινής γνώμης τόσο στο εσωτερικό των δύο εμπλεκόμενων χωρών όσο και στο εξωτερικό. Πέρα από τη μάχη για την κατάκτηση εδαφών στο πεδίο, η διεθνής κοινότητα παρακολούθησε τη μάχη για τον έλεγχο της αφήγησης που διεξαγόταν στον κυβερνοχώρο. Η Ρωσία προσπάθησε να επηρεάσει το Ουκρανικό κοινό, να υποστηρίξει τις επιθετικές ενέργειές της στο εσωτερικό της και να πείσει τη διεθνή κοινή γνώμη για το δίκαιο του αγώνα της όμως η προπαγάνδα δεν είναι αρκετή για να κρύψει τις παραβιάσεις του Διεθνούς Δικαίου. Φαίνεται ότι οι κυβερνοεπιθέσεις με στόχο την πληροφορία είναι περισσότερο χρήσιμες για την κατασκοπεία και λιγότερο για την παραπλάνηση.

Όπως παρατηρήσαμε, οι κυβερνοεπιθέσεις απαιτούν μακροχρόνια προετοιμασία και σχεδιασμό και δεν έχουν το αναμενόμενο αποτέλεσμα όταν χάνουν το πλεονέκτημα του

αιφνιδιασμού. Η Ουκρανία, έχοντας αντιμετωπίσει ρωσικές κυβερνοεπιθέσεις ήδη από το 2014, ήταν καλύτερα προετοιμασμένη το 2022 για να αντιμετωπίσει τις κακόβουλες ενέργειες που είχαν στόχο τα ψηφιακά της δίκτυα και τις κρίσιμες υποδομές της. Αυτή η προετοιμασία της επέτρεψε να αποκρούσει πολλές επιθετικές επιχειρήσεις στον κυβερνοχώρο, πράγμα που υποδηλώνει ότι μια καλά προετοιμασμένη κυβερνοάμυνα μπορεί να αποτρέψει αποτελεσματικά μια καλά προετοιμασμένη κυβερνοεπίθεση. Όπως είδαμε, η Ουκρανία κατάφερε να συγκεντρώσει την υποστήριξη και την έμπρακτη βοήθεια σε τεχνικό επίπεδο κρατών και ιδιωτικών εταιρειών - ηγετών στον τομέα της ψηφιακής τεχνολογίας, γεγονός που της έδωσε σημαντικό πλεονέκτημα και ανθεκτικότητα στις κυβερνοεπιθέσεις. Στον κυβερνοπόλεμο μεταξύ Ρωσίας - Ουκρανίας είδαμε ότι συμμετείχαν και συμμετέχουν ακόμα ενεργά μη κρατικοί φορείς, κυρίως ομάδες hacker με νέους παίκτες να εμφανίζονται καθημερινά. Αυτοί οι εθελοντές, ιδιώτες που συμμετέχουν σε δράσεις στον κυβερνοχώρο είναι δύσκολο να ελεγχθούν όμως μπορούν να προσφέρουν πολύτιμη βοήθεια στην κυβερνοάμυνα αν οι ενέργειές τους συντονιστούν σωστά με κυβερνητικές υπηρεσίες.

Παρόλα αυτά η συμμετοχή ιδιωτών στον κυβερνοπόλεμο εγείρει ανησυχίες για τον ορισμό του άοπλου και του συμμετέχοντα σε επιθετικές ενέργειες για το Διεθνές Δίκαιο. Από τον κυβερνοπόλεμο μεταξύ Μόσχας – Κιέβου, όπου η Ρωσία είναι ο επιτιθέμενος και η Ουκρανία ο αμυνόμενος, η διεθνής κοινότητα μπορεί να αντλήσει μαθήματα για τις μελλοντικές συγκρούσεις που αναπόφευκτα θα σημειωθούν. Το σημαντικότερο όλων θα λέγαμε είναι η διαπίστωση ότι ο κυβερνοπόλεμος μπορεί να είναι σημαντικός για την προετοιμασία του πολέμου και τον επηρεασμό της κοινής γνώμης όμως αυτός δεν κερδίζει εδάφη και οι επιπτώσεις του είναι περιορισμένες. Οι κυβερνοεπιθέσεις και από τις δύο μεριές δεν απέτρεψαν ούτε σταμάτησαν τις μάχες επί του πεδίου οι οποίες συνεχίζονται μέχρι και σήμερα. Η αποτελεσματικότητα του κυβερνοπολέμου μετριέται με τα αποτελέσματα, δηλαδή με την έκταση της ζημιάς και κατά πόσο η κυβερνοεπίθεση ανάγκασε τον αντίπαλο να κάνει παραχωρήσεις ή να αλλάξει τη στρατηγική του. Αυτό δεν είδαμε να συμβαίνει στον Ρωσο-ουκρανικό πόλεμο στον κυβερνοχώρο μέχρι τώρα για τους λόγους που προαναφέραμε. Με βάση τα στοιχεία που συλλέξαμε θα καταλήξουμε στο συμπέρασμα ότι ενώ ο κυβερνοχώρος προσφέρει ένα ενδιαφέρον πεδίο σύγκρουσης και αποτελεί χρήσιμο εργαλείο εφαρμογής στρατηγικής, στην πραγματικότητα δεν μπορεί να αντικαταστήσει τις επιπτώσεις του πραγματικού πολέμου σε υλικό, πολιτικό, οικονομικό και ψυχολογικό επίπεδο. Επίσης στην περίπτωση του κυβερνοπολέμου οι ζημιές δεν είναι μόνιμες σε αντίθεση με αυτές που προκαλούν οι πραγματικές μάχες. Ως εκ τούτου οι κυβερνοεπιθέσεις είναι συμπληρωματικές των στρατιωτικών επιθέσεων και μπορούν να λειτουργήσουν ως μέσο εκφοβισμού,

αποτροπής ή προειδοποίησης και να πετύχουν περιορισμένες επιπτώσεις, δηλαδή δεν φαίνεται ότι αποτελούν υπερ-όπλο.

Σύμφωνα με όλα όσα εξετάζονται οι αναλυτές επισημαίνουν ότι οι επιπτώσεις των κυβερνοεπιθέσεων μπορούν να γίνουν αντιληπτές σε βάθος χρόνου, επομένως μάλλον είναι νωρίς για να αποδοθεί η πραγματική βλάβη που αυτές έχουν προκαλέσει, να αναδειχθεί ο τελικός νικητής και να αποδοθεί η νίκη. Αυτό που είναι κοινά αποδεκτό αυτή τη στιγμή, είναι η ανάγκη προετοιμασίας όλων των χωρών για τη διεξαγωγή του κυβερνοπολέμου και την αντιμετώπιση των κυβερνοεπιθέσεων τόσο σε καιρό ειρήνης όσο και σε καιρό πολέμου και κυρίως ο σχεδιασμός για το πώς θα συνδυαστούν οι επιχειρήσεις στον κυβερνοχώρο με άλλους τρόπους επίθεσης ώστε να επιτευχθεί το μέγιστο δυνατό αποτέλεσμα. Η προετοιμασία αυτή θα πρέπει να περιλαμβάνει τη συνεργασία μεταξύ κρατικών φορέων και ιδιωτικών επιχειρήσεων αιχμής της τεχνολογίας, τομέας στον οποίον όλες οι χώρες μπορούν να γίνουν καλύτερες.

Επίσης ξεπερνώντας προκαταλήψεις πολλών ετών, φαίνεται ότι τα κράτη θα πρέπει να συνεργαστούν μεταξύ τους, ανταλλάσσοντας πληροφόρηση σε σχέση με τις ομάδες hacker που δραστηριοποιούνται στον κυβερνοχώρο και τη χάραξη όσο το δυνατόν κοινής πολιτικής για την αντιμετώπισή τους. Από τα θέματα που προέχουν είναι επομένως αυτό της ανάγκης για αποτελεσματική κυβερνοάμυνα και κυβερνοανθεκτικότητα. Η ικανότητα της άμεσης και αποτελεσματικής αντίδρασης στην κυβερνοεπίθεση φαίνεται ότι είναι το κλειδί για την κυβερνοάμυνα για αυτό και η προετοιμασία και η παρακολούθηση των διεθνών εξελίξεων στον τομέα της τεχνολογίας και των δυνατοτήτων που αυτή μπορεί να παρέχει, είναι εξαιρετικής σημασίας. Η διεθνής κοινότητα φαίνεται ότι είναι επίσης ευαισθητοποιημένη στις επιπτώσεις που έχουν οι κυβερνοεπιθέσεις στον άμαχο πληθυσμό από την υπονόμευση κρίσιμων υποδομών και κυρίως στο ψυχολογικό αντίκτυπο που αυτές συνεπάγονται από τη διασπορά ψευδών ειδήσεων τη στιγμή που μια χώρα βιώνει παράλληλα το κόστος της φυσικής επίθεσης.

Τέλος θα θέλαμε να αναφέρουμε ότι πρώτον ότι είναι πολύ νωρίς για να εξαχθούν οριστικά συμπεράσματα που σχετίζονται με τα αποτελέσματα της κυβερνοπληροφόρησης και το κυβερνοπολέμου κατά τη προετοιμασία και την εκτέλεση αυτού του είδους πολέμου στην Ουκρανία. Οι πληροφορίες που συγκεντρώνονται και οι απαντήσεις που δίνονται μπορεί να μην ισχύουν σε άλλες περιπτώσεις, επειδή οι μετρήσεις που πραγματοποιούνται για την αξιολόγηση των αποτελεσμάτων μπορεί να διαφέρουν όχι μόνο με την πάροδο του χρόνου και μεταξύ των πρωταγωνιστών, αλλά και από τη μία σύρραξη στην άλλη. Δεύτερον αν και όπως φαίνεται από τα δημόσια διαθέσιμα στοιχεία για την πορεία των

κυβερνοεπιθέσεων μεταξύ Ρωσίας – Ουκρανίας οι κακόβουλες ενέργειες σημείωσαν μείωση το τρίτο τρίμηνο του 2023, σημειώνεται ότι η αποκλιμάκωση της κυβερνοσύγκρουσης είναι αμφίβολο ότι θα συμβεί ακόμα και μετά την κατάπαυση των πολεμικών εχθροπραξιών στο πεδίο. Η διεθνής κοινότητα θα συνεχίσει να παρακολουθεί την έκβαση αυτού του πολέμου στον ψηφιακό και τον πραγματικό κόσμο με ανησυχία.

5. Βιβλιογραφία – Πηγές Ξένες.

1. Geers K., *Cyber War in Perspective, Russian aggression against Ukraine,* NATO CCDCOE, Ed. Tallinn, 2015.

2. Kuzio T. & Anieri D., *«The Sources of Russia's Great Power Politics. Ukraine and the Challenge to the European Order*, E-International Relations Publishing, UK, 2018.

3. Levite, A.E., *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict,* Carnegie Endowment for International Peace, US, 2023.

4. Libicki M., *«Cyberdeterrence and Cyberwar»,* Rand Corporation ed., U.S, 2009.

6. Βιβλιογραφία – Πηγές Ελληνικές.

1. Κωνσταντόπουλος Ι., *«Πληροφόρηση και Ασφάλεια: Μια άρρηκτη σχέση»,* Τμήμα Οικονομικών Επιστημών, Πανεπιστήμιο Θεσσαλίας, 2018.
2. Κωνσταντόπουλος Ι., *«Οικονομία και Κατασκοπεία, Θεωρία και Πράξη»,* Εκδόσεις Ποιότητα, Αθήνα, 2010.
3. Λιαρόπουλος, Α., *«Κυβερνοχώρος και Παγκόσμια Τάξη»,* Εκδόσεις Παπαζήση, Αθήνα, 2023.
4. Λιαρόπουλος Α. & Μποζίνης Αθ., *«Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις»,* Εκδόσεις Παπαζήση, Αθήνα, 2022.

7. Διαδικτυακές Πηγές:

1. CyberPeace Institute, *«Cyber Attacks in Times of Conflict Platform # Ukraine».* https://cyberconflicts.cyberpeaceinstitute.org/.

2. CyberPeace Institute, *Cyber Dimensions of the armed conflict in Ukraine* Quarterly Analysis Report - Q3 (July to September 2023) στο: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/ (δημοσιεύτηκε στις 21.12.2023).

3. Cyber Peace Institute, *Cyber Dimensions of the armed conflict in Ukraine*, Quarterly Analysis Report - Q3 (July to September 2022), στο: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2022/ (δημοσιεύτηκε 16.12.2022).

4.Duguin S. & Pavlova P., *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, στο: https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594 (δημοσιεύτηκε στις 04.09.2023).

5. Lange-Ionatamishvili E. & Svetoka S., *Strategic Communications and Social Media In the Russia Ukraine Conflict*, στο: https://ccdcoe.org/uploads/2018/10/Ch12_CyberWarinPerspective_Lange_Svetoka.pdf (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

6. *Lessons from Russia's cyber-war in Ukraine* στο: https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=Cj0KCQiAkeSsBhDUARIsAK3tiefyBGjitsk6VMkTtgF9-KCDIFZgfsyl-4zr_wcWfMcijlrDoOwtwIMaAqwDEALw_wcB&gclsrc=aw.ds, δημοσιεύτηκε στις 03.12.2022.

7. Levite, A.E., *Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict*, στο: https://carnegieendowment.org/files/Levite_Ukraine_Cyber_War.pdf (δημοσιεύτηκε στις 18.04.2023).

8. Lewis J.A, *Cyber War and Ukraine"*, διαθέσιμο στο: https://www.csis.org/analysis/cyber-war-and-ukraine, (δημοσιεύτηκε 16.06.2022).

9. https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/

10. Libicki M., *The Cyber War that Wasn't,* στο: https://ccdcoe.org/uploads/2018/10/Ch05_CyberWarinPerspective_Libicki.pdf, (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).

11. Mueller, G, Jensen B.,Valeriano B., Maness R, Macias J. . *Cyber Operations during the Russo-Ukranian War: From Strange Patterns to Alternative Futures*, στο: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-russian-cyber-operations (δημοσιεύτηκε στις 01.07.2023).

12. Papapetrou, N., *NotPetya Attack*, στο: https://cyberpeaceinstitute.org/cyberattacks/notpetya-attack/ (δημοσιεύτηκε 27.07.2017).

13. Warner, M. "Wanted: A Definition of Intelligence", *Studies in Intelligence*, Vol. 46, No. 3. στο: https://www.cia.gov/static/72b2d4c0d01e4e05c60ff7d37fdd68b1/Wanted-Definition-of-Intel.pdf (δημοσιεύτηκε το 2002).

14. Weedon J., Cyber War in Perspective: Russian Aggression against Ukraine στο: https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf (δημοσιεύτηκε από NATO CCD Publications, Tallinn, 2015).