ΚΕΔΙΣΑ KEDISA
ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

Κυβερνοπόλεμος, στο πλαίσιο του Ρωσο-Ουκρανικού πολέμου (2022-2023)

Παπαδάκης Κωνσταντίνος

Ερευνητική Εργασία νο. 103

ΚΕΔΙΣΑ KEDISA

ΚΕΝΤΡΟ ΔΙΕΘΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΑΝΑΛΥΣΕΩΝ
CENTER FOR INTERNATIONAL STRATEGIC ANALYSES

ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ ΚΕΔΙΣΑ

Δρ. Ανδρέας Γ. Μπανούτσος	Πρόεδρος
Δρ. Παναγιώτης Σφαέλος	Αντιπρόεδρος & Δ/ντης Ερευνών
Βασίλης Παπαγεωργίου	Γενικός Γραμματέας
Αργέττα Μαλιχουτσάκη	Οικονομική Διαχειρίστρια
Ευάγγελος Διπλάρας	Μέλος
Αναστασία Τσιμπίδη	Μέλος

Κυβερνοπόλεμος, στο πλαίσιο του Ρωσο-Ουκρανικού πολέμου (2022-2023)

Παπαδάκης Κωνσταντίνος

ΓΕΝΙΚΑ

Στον συνεχιζόμενο Ρώσο-Ουκρανικό πόλεμο, η Ρωσία παράλληλα με τις συμβατικές επιχειρήσεις, διεξάγει ένα σύνολο πληροφοριακών επιχειρήσεων (information Operations) οι οποίες περιλαμβάνουν ψυχολογικές επιχειρήσεις (Psychological Operations), επιχειρήσεις κυβερνοπολέμου (cyber warfare) και επιχειρήσεις παραπληροφόρησης (disinformation). Σε αυτού του είδους τις επιχειρήσεις, τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ), οι τηλεπικοινωνίες, τα ΜΜΕ και οι πάροχοι διαδικτύου διαδραματίζουν σημαντικό ρόλο τόσο στη μετάδοση πληροφοριών για τον πόλεμο όσο και στη διαμόρφωση της κοινής γνώμης.

Όσο αφορά στη ψηφιακή οπτική της σύγκρουσης είναι δόκιμο να την χαρακτηρίζουμε ως **υψηλής έντασης[1] υβριδική σύγκρουση[2]** στον κυβερνοχώρο ή καλύτερα στο ευρύτερο ενοποιημένο πληροφοριακό περιβάλλον μέρος του οποίου θεωρείται τόσο ο κυβερνοχώρος, όσο και το ηλεκτρομαγνητικό πεδίο.

ΑΝΑΛΥΣΗ

Η ρωσική στρατηγική στο ευρύτερο πληροφοριακό περιβάλλον έχει επηρεασθεί από το όραμα του στρατηγού Gerasimov[3], όπως αυτό διαμορφώθηκε από την εξελικτική πορεία του τρόπου σύγκρουσης στις αρχές του 2000[4] μεταξύ υβριδικών συγκρούσεων και μιας θολής λεπτής γραμμής μεταξύ πολέμου και ειρήνης.

Η νέα οπτική των συγκρούσεων αποδέχεται ότι:

- Η μορφή των πολέμων αλλάζει και η νέα τάση απαιτεί την ενίσχυση, της επιρροής επί της κοινής γνώμης και των μη στρατιωτικών μοχλών πίεσης.
- Η γνώση πληροφοριακού περιβάλλοντος και του κυβερνοχώρου, από τεχνικής και τακτικής πλευράς, και η χρησιμοποίηση του ως μοχλού επιρροής καθίσταται πλέον θεμελιώδης και επιβεβλημένη.

ΡΩΣΙΑ

Η Ρωσία δεν αναφέρεται σε κυβερνοασφάλεια αλλά σε πληροφοριακό πόλεμο.

Όπως υποδεικνύεται από την εξέλιξη του ρωσικού οράματος για τη σύγκρουση αλλά και την ασάφεια καθορισμού χωροχρονικών ορίων μεταξύ ειρήνης και πολέμου, καθώς και

---

[1] Οι λεγόμενες **συγκρούσεις υψηλής έντασης (high-intensity conflicts)** είναι συμμετρικές συγκρούσεις που περιλαμβάνουν ένοπλες δυνάμεις οι οποίες χρησιμοποιούν σύγχρονα, μεγάλης κλίμακας τεχνολογικά μέσα. Πρακτικά παραδείγματα που διαφοροποιούν αυτές τις συγκρούσεις από τις συγκρούσεις χαμηλής έντασης είναι η απουσία ή πολύ περιορισμένη χρήση οργανωμένου ανταρτοπόλεμου, η χρήση πυρηνικών ή μη πυρηνικών βαλλιστικών επιθέσεων, η ανάπτυξη ασυνήθιστων μεγάλων δυνάμεων (ποσοτικά και ποιοτικά) θάλασσας, αέρα και ξηράς (τανκς, αντιτορπιλλικά, βομβαρδιστικά κ.λπ.) και την κήρυξη πολέμου από τη μια χώρα σε μια άλλη.

[2] Η **υβριδική σύγκρουση (Hybrid conflict)** είναι ένα είδος σύγκρουσης που συνδυάζει πολλές μη συμβατικές μεθόδους πολέμου, όπως παραπληροφόρηση, χειραγώγηση της κοινής γνώμης, οικονομικός πόλεμος, δολιοφθορά, τρομοκρατία, κυβερνοεπίθεση και ανταρτοπόλεμο. Ως δρώντες οι οποίοι εμπλέκονται σε μια υβριδική σύγκρουση μπορεί να περιλαμβάνονται κράτη, τρομοκρατικές ομάδες, πολιτοφυλακές, ιδιωτικές εταιρείες και ιδιώτες. Η υβριδική σύγκρουση καθώς οι εμπλεκόμενοι φορείς, συχνά από αυξημένη πολυπλοκότητα, μπορεί να έχουν διαφορετικούς στόχους και διαφορετικές μεθόδους μάχης. Μπορεί να είναι δύσκολο για να προσδιοριστεί ποιος είναι υπεύθυνος για ενέργειες σε μια υβριδική σύγκρουση, καθώς οι εμπλεκόμενοι φορείς ενδέχεται να χρησιμοποιήσουν εύλογες τακτικές άρνησης για να αποκρύψουν τη συμμετοχή τους.

[3] Αυτό το όραμα επιβεβαιώθηκε από τον στρατηγό Gerasimov το 2019 στο συνέδριο της Ακαδημίας Στρατιωτικών Επιστημών, όπου και τόνισε τη σημασία των υβριδικών τακτικών και τη γνώση του ασύμμετρου πολέμου :
«Στις σύγχρονες συνθήκες, η αρχή της διεξαγωγής πολέμου έχει αναπτυχθεί με βάση τη συντονισμένη χρήση στρατιωτικών και μη στρατιωτικών μέτρων [...] οι Ένοπλες Δυνάμεις μας πρέπει να είναι έτοιμες να διεξάγουν πολέμους και ένοπλες συγκρούσεις νέου τύπου χρησιμοποιώντας κλασικές και ασύμμετρες μεθόδους δράσης. Επομένως, η αναζήτηση ορθολογικών στρατηγικών για τη διεξαγωγή πολέμου με διάφορους αντιπάλους είναι πρωταρχικής σημασίας σημασία για την ανάπτυξη της θεωρίας και της πρακτικής της στρατιωτικής στρατηγικής.»

[4] Η σκέψη της ρωσικής στρατιωτικής ελίτ, όπως αυτή του στρατηγού Gerasimov, έχει βαθιά επηρεασθεί από συγκρούσεις όπως ο Δεύτερος πόλεμος της Τσετσενίας (Αυγ.1999- Απρ.2009), την Αραβική Άνοιξη (2011), τον επακόλουθο εμφύλιο πόλεμο στη Συρία, και τελικά την Ουκρανική κρίση

την εξέλιξη των σύγχρονων συγκρούσεων προς έναν υβριδισμό μεταξύ συμβατικών και αντισυμ-βατικών μοχλών ισχύος, οι ρωσικές ελίτ βλέπουν τον κυβερνοχώρο ως μέρος του ευρύτερου πληροφοριακού περιβάλλοντος εντός του οποίου θα πρέπει να αποκτηθεί και να διατηρηθεί πληροφοριακή υπεροχή.

Ως εκ τούτου, έχουν δημιουργήσει τη δική τους αντίληψη για αυτό που οι δυτικοί ονομάζουν «κυβερνοασφάλεια» με την ονομασία «πληροφοριακή ασφάλεια». Προφανώς, η ίδια λογική μεταφέρεται από την αμυντική πλευρά στην επιθετική πλευρά, όπου αναφέρονται στον «πληροφοριακό πόλεμο» αντί της σύγκρουσης στον κυβερνοχώρο. Ο ρωσικός ορισμός περιλαμβάνει, εκτός από το όραμά της κλασικής κυβερνοασφάλειας, μια ψυχολογική και μια γνωστική διάσταση οι οποίες με τη βοήθεια τεχνικών μέσων είναι ικανές να καταστήσουν δυνατό τον έλεγχο του πληροφοριακού περιβάλλοντος.

Το πληροφοριακό περιβάλλον δεν αποτελεί χώρο διέλευσης αλλά έναν χώρο που πρέπει να ελέγχεται με μακροπρόθεσμη προοπτική καθώς αποτελεί ευέλικτο χώρο που επιτρέπει επιρροή σε περιόδους ειρήνης και κυριαρχία σε περιόδους πολέμου . Η θεμελιώδης αυτή αντίλη-ψη του πληροφοριακού πολέμου επεκτάθηκε πέρα από την παραδοσιακή δυτική προσέγγιση της κυβερνοασφάλειας και παρουσιάζεται ως εξής από το Ρωσικό Υπουργείο Άμυνας:

«...Ο Πληροφοριακός πόλεμος είναι μια αντιπαράθεση μεταξύ δύο ή περισσότερων κρατών στο πληροφοριακό περιβάλλον με στόχο να προκαλέσει ζημιά σε συστήματα πληρο-φοριών, διαδικασίες και πόρους, κρίσιμες και άλλες δομές, υπονόμευση πολιτικών, οικονομικών και κοινωνικών συστημάτων, μαζική ψυχολογική χειραγώγηση του πληθυσμού για την αποσταθεροποίηση της κοινωνίας και του κράτους, καθώς και τον εξαναγκασμό των κρατών να πάρουν αποφάσεις προς το συμφέρον της αντίπαλης πλευράς...».

Υπό το παραπάνω πρίσμα της νέας αντίληψης η Ρωσία προχώρησε στα παρακάτω βασικά βήματα:

- Αναδιοργάνωσε (ποσοτικά, ποιοτικά, θεσμικά) τις κυβερνομονάδες της σε δυνάμεις πληροφοριακών επιχειρήσεων ικανές να υποστηρίξουν ένα σύνολο πληροφοριακών δραστηριοτήτων μέσω του κυβερνοχώρου.
- Ενέταξε στον επιχειρησιακό σχεδιασμό της, ομάδες ιδιωτών (χακτιβιστικές ομάδες), ώστε να αναβαθμίσει τις τεχνικές ικανότητες στο πεδίο του κυβερνοχώρου και να αντιμετωπίσει προβλήματα όπως η απόδοση ευθυνών για επιθέσεις σε πολιτικούς στόχους ή άλλες χώρες εκτός Ουκρανίας.

Χαρακτηριστικό παράδειγμα αποτελεί το δίκτυο KillNet, το οποίο αποτελείται από έναν αριθμό χακτιβιστικών κυβερνοομάδων ίδιου προσανατολισμού και έχει στόχο:

- ✓ Τη δημοσιότητα, η οποία τους επιτρέπει να διεξάγουν έναν πόλεμο επιρροής με στόχο να προσβάλουν το ηθικό του ευρωπαϊκού πληθυσμού.
- ✓ Την ενίσχυση της εικόνας η οποία δηλώνει ότι η Ρωσία έχει ικανότητα επέμβασης ακόμα και εκεί που δεν έχει στρατεύματα.
- ✓ Την ενίσχυση της πεποίθησης ότι οι ευρωπαϊκές κυβερνήσεις δεν είναι ικανές να προστατέψουν τις υποδομές και τους πολίτες τους σε όλα τα μέτωπα και πεδία.
- ✓ Την απόκρυψη μέσω της δημοσιότητας, των ενεργειών ομάδων διείσδυσης οι οποίες αποτελούν μακροχρόνιες απειλές (Advanced Persistent Threats-APT).

- Εμπλούτισε το οπλοστάσιο της με νέου τύπου κυβερνοόπλα αιχμής (λογισμικό διαγραφής, λυτρισμικό, κλπ), τα οποία είναι μη ανιχνεύσιμα και ικανά να δημιουργήσουν σοβαρά προβλήματα στους αντιπάλους.

Τρόπος επιχειρήσεων (Modus Operandi)

Η Ρωσία σχεδιάζει, διεξάγει και συντονίζει τις παρακάτω επιχειρήσεις, στο πλαίσιο ενός αναβαθμισμένου σχεδιασμού πληροφοριακών επιχειρήσεων μέσω κυβερνοχώρου με στόχο την απόκτηση πληροφοριακού πλεονεκτήματος στο ευρύτερο πληροφοριακό περιβάλλον:

- <u>Επιχειρήσεις αρχικής απόκτησης επαφής</u> σε στόχους εντός και εκτός Ουκρα-νίας,[5] με στόχο τη κεκαλυμμένη διείσδυση σε πληροφοριακά συστήματα και σκοπό τη

[5] Σε τεχνικό επίπεδο, κοινές τακτικές και τεχνικές συμπεριλαμβάνουν την εκμετάλλευση διαδικτυακών εφαρμογών, κερκόπορτες (backdoors) παράνομων εκδόσεων λογισμικού (Microsoft Office) και στοχευμένη ηλ. εξαπάτηση (spear phishing)

μεταγενέστερη επίθεση και καταστροφή τους ή την παρατεταμένη κατασκοπεία και συλλογή πληροφοριών.

- Στοχευμένες επιθέσεις (κυρίως εντός Ουκρανίας) με χρήση κακόβουλου λογισμικού διαγραφής δεδομένων (wiper-type destruction malware), με σκοπό τη καταστροφή των υπό στόχευση πληροφοριακών συστημάτων και την δημιουργία συναισθημάτων σύγχυσης και αποπροσανατολισμού των ληπτών απόφασης.
- Κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS), με άμεσο αποτέλεσμα τη διακοπή (για συγκεκριμένο χρόνο) των προσφερόμενων υπηρεσιών ιστοτόπων και έμμεσο τη δημιουργία κατάλληλων ψυχολογικών αποτελεσμάτων (φόβος, δυσπιστία, κλπ) σε επιλεγμένα ακροατήρια. Οι επιθέσεις τέτοιου είδους έχουν ως σκοπό τον ηθικό αντίκτυπο, προσπαθώντας να δημιουργήσουν και να συντηρήσουν ένα αίσθημα ανασφάλειας για τα συστήματα και τις υποδομές μεταξύ των στοχευόμενων πληθυσμών επιτρέποντας τη διατήρηση σταθερής κοινωνικό-πολιτικής πίεσης με χαμηλό κόστος παράλληλα με μια πολιτική ή στρατιωτική σύγκρουση. Δίνει επίσης ένα πολιτικό πλεονέκτημα (**σύστημα "πλεονεκτήματος-μόχλευσης (leverage advantage)"**[6], διεξάγοντας επιθετικές επιχειρήσεις αντιποίνων χωρίς να εμπλέκεται διπλωματικά ή στρατιωτικά το κράτος που οργανώνει τους επιτιθέμενους.
- Επιχειρήσεις αλλοίωσης περιεχομένου ιστοτόπων (defacement), με άμεσο αποτέλεσμα την αλλοίωση του περιεχομένου τους και έμμεσο τον αποπροσανατολισμό και παραπληροφόρηση των ακροατηρίων τους.
- Εκστρατείες παραπληροφόρησης που στοχεύουν σε διαφορετικά είδη ακροατηρίων:
  - ✓ Τον ρωσικό πληθυσμό, με στόχο τη διατήρηση και την υποστήριξη για τον πόλεμο.
  - ✓ Τον ουκρανικό πληθυσμό ώστε να υπονομεύσει την εμπιστοσύνη του στην ικανότητα της Ουκρανίας να αντισταθεί στις ρωσικές επιθέσεις.
  - ✓ Το ευρωπαϊκό και το αμερικανικό κοινό ώστε να δημιουργήσει αμφιβολίες για τη Δυτική ενότητα ενάντια στη Ρωσία και σχετικά με τη σημασία της υποστήριξης της Ουκρανίας και την αντιμετώπιση εσωτερικών ζητημάτων.

- Συλλογή πληροφοριών μέσω της διείσδυσης σε δίκτυα και τη στοχοποίηση κυβερνήσεων εκτός Ουκρανίας οι οποίες αποτελούν μέρος του συνασπισμού των χωρών που την υποστηρίζουν. Κύριος στόχος είναι οι κυβερνητικές υπηρεσίες, ακολουθούμενες από ΜΚΟ (είτε ανθρωπιστικές ομάδες που συμμετέχουν στην παροχή βοήθειας στον άμαχο πληθυσμό είτε δεξαμενές σκέψης που παρέχουν συμβουλές για την εξωτερική πολιτική). Στη συνέχεια, αρκετές εταιρείες σε κρίσιμους τομείς, όπως η ενέργεια, η άμυνα ή η πληροφορική, έχουν επηρεαστεί από τη ρωσική κυβερνοκατασκοπεία η οποία στοχεύει στην υποστήριξη της πολεμικής της προσπάθειας.
- Επιχειρήσεις επιρροής, μεγάλο μέρος των οποίων διεξάγεται μέσω διαδικτύου και Μέσων Κοινωνικής Δικτύωσης (ΜΚΔ), οι οποίες έχουν τακτικά αναβαθμισθεί μέσω των δεσμών που αποκτήθηκαν μεταξύ κυβερνοομάδων και ομάδων χακτιβιστών στο ευρύτερο πληροφο-ριακό περιβάλλον. Οι νέες τακτικές υλοποιούνται με συγκεκριμένα βήματα:
  - ✓ Πρώτον, ρωσικές ομάδες επιρροής προσπαθούν να απλοποιήσουν τη διαδικασία εξακρίβωσης και επαλήθευσης γεγονότων, άρθρων και ειδήσεων (fact checking) ώστε να είναι σε θέση να διασπείρουν τα αφηγήματα του Κρεμλίνου.

---

[6] Το σύστημα **"πλεονεκτήματος-μόχλευσης" (leverage)** αναφέρεται στη χρήση κάποιου πόρου ή μηχανισμού προκειμένου να επιτευχθούν καλύτερα αποτελέσματα και με μεγαλύτερη επίδραση από ό,τι θα ήταν δυνατό με μόνο τη χρήση βασικών πόρων.
Στον οικονομικό και επιχειρηματικό τομέα, η έννοια του "πλεονεκτήματος-μόχλευσης" αναφέρεται συχνά στη χρήση χρηματοοικονομικών μέσων, όπως των δανείων, προκειμένου να αυξηθεί ο χρηματοοικονομικός αντίκτυπος μιας επενδυτικής ή επιχειρηματικής απόφασης. Με άλλα λόγια, η χρήση μόχλευσης επιτρέπει σε ένα άτομο ή μια εταιρεία να χρησιμοποιήσει λίγα χρήματα για να κερδίσει πολύ περισσότερα χρήματα, εκμεταλλευόμενοι τη δυνατότητα δανεισμού. Το σύστημα "πλεονεκτήματος-μόχλευσης" ή αλλιώς "leveraged advantage" στις επιχειρήσεις κυβερνοχώρου αναφέρεται στον τρόπο που μια επιχείρηση μπορεί να χρησιμοποιήσει την τεχνολογία και τις ψηφιακές πλατφόρμες για να ενισχύσει την ανταγωνιστική της θέση και να δημιουργήσει οφέλη. Στον κυβερνοχώρο, η έννοια της μόχλευσης αναφέρεται στο πώς οι επιχειρήσεις μπορούν να χρησιμοποιήσουν την τεχνολογία, τα δεδομένα και τις ψηφιακές πλατφόρμες για να ενισχύσουν τις δραστηριότητές τους, να βελτιώσουν την απόδοσή τους και να δημιουργήσουν νέες ευκαιρίες. Αυτό μπορεί να συμπεριλαμβάνει την ανάπτυξη νέων τεχνολογικών λύσεων, την αποτελεσματική χρήση των δεδομένων για λήψη αποφάσεων, και την ενσωμάτωση των ψηφιακών πλατφορμών για την αναβάθμιση των υπηρεσιών και των διαδικασιών. Με την ορθή χρήση της μόχλευσης, οι επιχειρήσεις κυβερνοχώρου μπορούν να επιτύχουν ανταγωνιστικό πλεονέκτημα και να ενισχύσουν την ικανότητά τους να παρέχουν αποτελεσματικές υπηρεσίες και προϊόντα.

✓ Δεύτερον, φιλορωσικές ομάδες συνεχώς διασπείρουν διαδικτυακά πληροφορίες οι οποίες υποτίθεται έχουν προέρθει από διαρροές στοχοποιώντας πολιτικούς και κυβερνήσεις που υποστηρίζουν την Ουκρανία.

✓ Τρίτον, η Ρωσική κυβέρνηση και οι συνδεόμενες με αυτήν οντότητες συχνά διοργανώνουν επισκέψεις τύπου (press tours) σε όλη την κατεχόμενη Ουκρανία ώστε να υπάρχει διεθνής επικοινωνιακή κάλυψη από φίλια μέσα και να επιτευχθούν ευκολότερα οι επικοινωνιακοί στόχοι.

✓ Τέταρτον, επιπρόσθετα με τις επιχειρήσεις οι οποίες στοχεύουν τη Μολδαβία, η Ρωσία συνεχίζει τις επιχειρήσεις επιρροής στην περιφέρεια της Ουκρανίας και σε ολόκληρη την Ευρώπη ώστε να διευρύνει την διαίρεση των ακροατήριών, να απαξιώσει τις φιλοουκρανικές ηγεσίες και να προάγει τα φιλορωσικά δίκτυα σε αυτές τις χώρες.

Στόχοι των ρωσικών κυβερνοεπιθέσεων εντός και εκτός Ουκρανίας αποτελούν:

- Κυβερνητικοί Ιστότοποι.
- Ιστότοποι ΜΜΕ.
- Τραπεζικό σύστημα και Χρηματοπιστωτικά ιδρύματα.
- Στρατιωτικές υποδομές
- Κρίσιμες υποδομές: Ενέργεια, ύδρευση, μεταφορές.
- Δορυφορικές επικοινωνίες.

ΟΥΚΡΑΝΙΑ

Αν και η Ουκρανία έχει περιορισμένες δυνατότητες αντεπιθέσεων στο πεδίο του κυβερνοχώρου, έχει προσπαθήσει να ενισχύσει την κυβερνοάμυνα μέσω των παρακάτω δράσεων:

- Αναδιοργάνωση και αναβάθμιση κρατικών υπηρεσιών κυβερνοασφάλειας.
- Σχηματισμό ενός «στρατού» πληροφορικής με τη συμμετοχή διεθνών εθελοντών.
- Εμπλοκή του συνόλου της Ουκρανικής κυβερνοκοινότητας στην κυβερνοάμυνα της χώρας.
- Συνεργασίες Δημόσιου και Ιδιωτικού τομέα.
- Εξωτερική βοήθεια η οποία περιλαμβάνει:

✓ Την ανταλλαγή πληροφοριών απειλών κυβερνοχώρου.

✓ Την αποστολή από ΕΕ και φίλιες χώρες, ομάδων αντιμετώπισης κυβερνο-περιστατικών.

✓ Συμμετοχή εξωτερικών υβριδικών δρώντων (χακτιβιστές) στις κυβερνοεπιχειρήσεις εναντίον της Ρωσίας.

Σε αντίποινα για τις ρωσικές επιθέσεις, η Ουκρανία έχει εξαπολύσει έναν μεγάλο αριθμό επιθέσεων άρνησης παροχής υπηρεσιών (DDoS) καθώς και επιθέσεις διαγραφής δεδομένων. Στους στόχους περιλαμβάνονται ρωσικοί κυβερνητικοί στόχοι, πληροφοριακά συστήματα μεγάλων ρωσικών ΜΜΕ, χρηματοπιστωτικά ιδρύματα, αμυντικές εγκαταστάσεις, δίκτυα ηλεκτ-ρικής ενέργειας και οι σιδηρόδρομοι.

Ως μέρος των αντεπιθέσεων στον κυβερνοχώρο, ανεξάρτητοι χάκερ από όλο τον κόσμο έχουν υποκλέψει και εκθέσει ρωσικά κυβερνητικά και οικονομικά δεδομένα, όπως ηλ. μηνύματα (emails), πληροφορίες που αφορούν σε τραπεζικές δραστηριότητες, παραγωγή ενέργειας και δραστηριότητες προπαγάνδας καθώς επίσης και διαβαθμισμένες λεπτομέρειες που αφορούν τις ρωσικές ΕΔ και τη δράση πρακτόρων της Ομοσπονδιακής Υπηρεσίας Ασφάλειας (FSB). Οι ευαίσθητες αυτές πληροφορίες μοιράζονται στη συνέχεια με παγκόσμιους ακτιβιστές ως τρόπος τιμωρίας της Ρωσίας για τα εγκλήματά της στην Ουκρανία.

Ένα δευτερεύον αποτέλεσμα των πρόσφατων δραστηριοτήτων των χάκερ είναι η επιτυχία τους να προκαλέσουν χάος στα ρωσικά κυβερνο-συστήματα και να συντρίψουν την αντίληψη για την απόρθητη κυβερνοάμυνα της Ρωσίας.

ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

Στο ψήφισμά της 1ης Μαρτίου 2022, το Ευρωπαϊκό Κοινοβούλιο ζήτησε την άμεση και πλήρη εφαρμογή όλων των αποφάσεων που θα βελτίωναν τη συμβολή της ΕΕ στην ενίσχυση των αμυντικών ικανοτήτων της Ουκρανίας, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο. Επιπλέον, το Κοινοβούλιο προέτρεψε την ΕΕ, το ΝΑΤΟ και άλλους ομοϊδεάτες εταίρους να εντείνουν τη βοήθειά τους στην Ουκρανία στο πεδίο του κυβερνοχώρου, ζητώντας παράλληλα την πλήρη ενεργοποίηση του καθεστώτος κυρώσεων στον κυβερνοχώρο της ΕΕ κατά ατόμων, οντοτήτων και φορέων που ευθύνονται ή εμπλέκονται σε κυβερνοεπιθέσεις κατά της Ουκρανίας.

Οι ενέργειες της ΕΕ μπορεί να συνοψιστούν στα παρακάτω:

- Ενίσχυση της ανθεκτικότητας της υποδομής επικοινωνιών.

Η διατήρηση λειτουργικών των τηλεπικοινωνιακών υπηρεσιών της Ουκρανίας είναι ζωτικής σημασίας για τη διασφάλιση της κανονικής λειτουργίας της ουκρανικής κυβέρνησης, καθώς και για την ανακούφιση από την ανθρωπιστική κρίση.

- Απαγόρευση της ρωσικής προπαγάνδας στον πόλεμο της κατά της Ουκρανίας.

Η καταπολέμηση της πολεμικής προπαγάνδας και της παραπληροφόρησης είναι ένα ιδιαίτερα πιεστικό ζήτημα στον πόλεμο της Ρωσίας

- Ενίσχυση της εργαλειοθήκης της ΕΕ κατά της παραπληροφόρησης.

Υπάρχουν ήδη προτάσεις για την αύξηση της χρηματοδότησης της Task Force East StratCom και την επέκταση του συστήματος ταχείας προειδοποίησης της ΕΕ για την παραπληροφόρηση, ώστε να καλύπτει την Ουκρανία και άλλα ενδιαφερόμενα μέρη.

- Υποστήριξη του αγώνα της Ουκρανίας κατά των απειλών στον κυβερνοχώρο.

Για το σκοπό αυτό έχει αναπτυχθεί μια ομάδα ταχείας απόκρισης στον κυβερνοχώρο που αποτελείται από εμπειρογνώμονες της ΕΕ.

- Ενίσχυση των ικανοτήτων της ΕΕ στον τομέα της κυβερνοασφάλειας.

Έχουν ανακοινωθεί περαιτέρω πρωτοβουλίες για τη διασφάλιση της ανθεκτικότητας της υποδομής και των δικτύων ηλεκτρονικών επικοινωνιών στην Ευρώπη, συμπεριλαμ-βανομένης της περισσότερης συνεργασίας σε επιχειρησιακό επίπεδο, μιας μελλοντικής πράξης για την ανθεκτικότητα στον κυβερνοχώρο και της δημιουργίας ταμείου αντιμετώπισης κατασ-τάσεων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο.

- Περιορισμός της πρόσβασης της Ρωσίας σε τεχνολογίες διπλής χρήσης.

Οι κυρώσεις της ΕΕ που εγκρίθηκαν στις 25 Φεβρουαρίου 2022 σκοπεύουν, κυρίως, να περιορίσουν την πρόσβαση της Ρωσίας σε κρίσιμης σημασίας προηγμένη τεχνολογία. Τεχνολογίες διπλής χρήσης – συγκεκριμένα αυτές που μπορούν να χρησιμο-ποιηθούν τόσο για ειρηνικούς όσο και για στρατιωτικούς στόχους – όπως ημιαγωγοί ή τεχνολογίες αιχμής, τεχνολογία ραδιοεπικοινωνιών και κρυπτοστοιχεία, δεν πρέπει να πωλούνται ή να παρέχονται με άλλο τρόπο για χρήση στη Ρωσία ή σε Ρωσική οντότητα

ΚΙΝΑ

Είναι πλέον γνωστό ότι οι Κινέζοι χάκερ εκτελούν κυβερνοεπιθέσεις[7] κατά της Ουκρανίας, αν και μόνο υποθέσεις μπορούμε να κάνουμε για το αν αυτές (επιθέσεις) είχαν οποιουδήποτε είδους κρατική υποστήριξη. Επίσης γνωστό είναι ότι κινέζοι χάκερ

[7] Σύμφωνα με πληροφορίες που εξασφάλισε το περιοδικό Times, υπήρξε πιθανή οργάνωση μέσω Κίνας (χωρίς να γνωρίζουμε αν υπήρξε κυβερνητική εμπλοκή) μιας μαζικής εκστρατείας κυβερνοεπιθέσεων εναντίον ουκρανικών στρατιωτικών και πυρηνικών εγκαταστάσεων πριν από την εισβολή της Ρωσίας. Περισσότεροι των 600 ιστότοπων του Υπουργείου Άμυνας στο Κίεβο και άλλων ιδρυμάτων υπέστησαν χιλιάδες απόπειρες διείσδυσης (hacking), σύμφωνα με τις πληροφορίες οι οποίες είχαν ομαδοποιηθεί με τίτλο «Κινεζικές επιθέσεις στην Ουκρανική κυβερνητική υποδομή καθώς και σε Ιατρικά & Εκπαιδευτικά Δίκτυα.

εκμεταλλευόμενοι την παρούσα σύγκρουση εκτελούν επιχειρήσεις κυβερνοχώρου και εναντίον της Ρωσίας.

Η αμφίδρομη σχέση μεταξύ Κίνας και Ρωσίας στο ευρύτερο πληροφοριακό περιβάλλον και ιδιαίτερα στο πεδίο του κυβερνοχώρου υλοποιείται σε δυο επιχειρησιακούς άξονες:

- Διεξαγωγή κυβερνοεπιχειρήσεων (επιθέσεων) πριν και κατά τη διάρκεια της Ρωσο-ουκρανικής σύγκρουσης.
- Διπλασιασμό των προσπαθειών στοχοποίησης και διείσδυσης τόσο σε ουκρανικούς όσο και σε ρωσικούς στόχους.

ΒΑΣΙΚΑ ΣΗΜΕΙΑ-ΣΥΜΠΕΡΑΣΜΑΤΑ-ΔΙΔΑΓΜΑΤΑ

Κίνδυνοι πλαισίωσης και εξάπλωσης

Η διασυνδεσιμότητα των πληροφοριακών συστημάτων και η εμπλοκή στις κυβερνο-επιχειρήσεις ανεξάρτητων χακτιβιστικών κυβερνοομάδων, με μικρό ή και καθόλου κρατικό έλεγχο, αυξάνει τους κινδύνους της εξάπλωσης των κυβερνοεπιθέσεων ή των αποτελεσμάτων αυτών και εκτός Ουκρανίας.

Η απειλή των κυβερνοεπιθέσεων σε ευρωπαϊκό έδαφος έχει δυο όψεις:

Πρώτον, οι επιθέσεις κατά των Ουκρανικών δικτύων θα μπορούσαν να εξαπλωθούν και στα ευρωπαϊκά δίκτυα.

Δεύτερον, η Ρωσία θα μπορούσε να επιλέξει να εξαπολύσει άμεσες επιθέσεις σε ευρωπαϊκούς στόχους μέσω των υπηρεσιών πληροφοριών της ή των κυβερνο-εγκληματικών ομάδων της, με σκοπό τη διατάραξη των ενεργειών της Δύσης στην ουκρανική κρίση.

Μεγάλες Επιθέσεις Και Σύγκρουση Υψηλής Έντασης

Σε περίπτωση κλιμάκωσης των εφαρμοζόμενων μέσων και της ριζοσπαστικότητας της σύγκρουσης, η ένταση των επιχειρήσεων στο ευρύτερο πληροφοριακό περιβάλλον και ιδιαίτερα στον κυβερνοχώρο μπορεί επίσης να αυξηθεί και ως εκ τούτου είναι σημαντικό, καταρχάς, να επιστρέψουμε στα χαρακτηριστικά που κατέχει, και επιτρέπει κάτω υπό ορισμένες προϋποθέσεις, ώστε να προτείνουμε λύσεις όπου τα συμβατικά μέσα ενδέχεται να είναι περιορισμένα.

Το θέμα της προ-τοποθέτησης

Κατά τον καθορισμό αξιόπιστων σεναρίων, το ζήτημα της πρωτοποθέτησης είναι ουσιαστικό γιατί επιτρέπει στη Ρωσία να ορίζει μια ακριβή θέση για μια επίθεση σε έναν οργανισμό, μεγιστοποιώντας επομένως τακτικά και στρατηγικά αποτελέσματα.

Για να αποφευχθεί η αποτελεσματική εκ των προτέρων τοποθέτηση Ρώσων δρώντων στα ουκρανικά συστήματα, οι ΗΠΑ διεξάγουν αμυντικές ενέργειες εύρεσης για να απενεργοποιήσουν τις επιθετικές ικανότητες της ρωσικής απειλής που έχουν ήδη θέσει σε κίνδυνο την ουκρανική υποδομή.

Κακόβουλο λογισμικό ως υπηρεσία
Malware-As-A-A-Service (MAAS)

Θα πρέπει να επισημανθεί ότι σήμερα τα κυβερνοόπλα δεν χρειάζεται να διέλθουν από όλες τις φάσεις της παραγωγής καθώς τα τελευταία χρόνια σχεδόν τα πάντα είναι διαθέσιμα ως υπηρεσίες «as-a-service». Τα τελευταία χρόνια έχει εμφανιστεί η δυνατότητα της απόκτησης «κακόβουλου λογισμικού ως υπηρεσία» (MaaS-Malware-as-a-Service) ή το «κυβερνοέγκλημα ως υπηρεσία» (CaaS-Cybercrime-as-a-Service).

Έλεγχος & Διοίκηση κακόβουλων δικτύων ως υπηρεσία
Command & Control as a service (C2aaS)

Οι υπηρεσίες «ελέγχου κακόβουλων δικτύων» (C2aaS-C2 as a Service) γίνονται όλο και περισσότερο διαθέσιμες στην αγορά. Οι υπηρεσίες αυτές έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να προσφέρουν σε τεχνικά άπειρους δρώντες με λίγους πόρους, την ικανότητα να εξαπολύουν κυβερνοεπιθέσεις κυρίως κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS). Τέτοιου είδους υπηρεσία προσφέρει ένα στόλο κακόβουλων Η/Υ (bot) που θα χρησιμοποιηθούν σε επιθέσεις (DDoS). Αυτές οι δυνατότητες υποδηλώνουν ότι ο αριθμός των κυβερνο-δρώντων στη ρωσο-ουκρανική σύγκρουση θα μπορούσε να αυξηθεί μαζί με τις δυνατότητες αυτών των υπηρεσιών χαμηλού κόστους.

Χάκερ για μίσθωση
(Hacker for Hire or hacker-for-hire proxy or Hacker as a Service-Haas)

Η επιλογή της Ρωσίας να χρησιμοποιήσει «χάκερ με μίσθωση» ως ενδιάμεσους (hacker-for-hire proxy) για την επιδίωξη των τακτικών και στρατηγικών της στόχων, της επιτρέπει να διατηρήσει ένα υψηλό επίπεδο άρνησης ευθύνης των συγκεκριμένων ενεργειών.

Κίνδυνος κλιμάκωσης της σύγκρουσης στο διαστημικό πεδίο

Οι δορυφορικές υποδομές είναι βασικά συστήματα σε καιρό πολέμου καθώς επιτρέπουν τον συντονισμό των χερσαίων στρατευμάτων μέσω εικόνων και τηλεπικοινωνιών, υπό αυτό το πρίσμα, η διακοπή της λειτουργίας της δορυφορικής υποδομής του αντιπάλου κατά τη διάρκεια των επιχειρήσεων επιτρέπει την απόκτηση σημαντικών τακτικών πλεονεκτημάτων στο στρατιωτικό πεδίο. Η Ρωσία διαθέτει αντιδιαστημικές δυνατότητες ή δυνατότητες εναντίον δορυφόρων (anti-satellite-ASAT) τόσο κινητικές (π.χ. πύραυλοι, συστήματα lazer, κλπ), όσο και μη κινητικές (ΗΠ, κυβερνοόπλα), ικανές να προκαλέσουν φυσικές αλλά και εικονικές αναστρέψιμες και στοχευμένες ζημιές καθιστώντας την απόδοση ευθυνών σύνθετη.

Η στρατιωτική ηγεσία της Ρωσίας θεωρεί τα όπλα στον κυβερνοχώρο ως υποκατάστατο ή/και ως συμπλήρωμα των όπλων Ηλεκτρονικού Πολέμου, υπονοώντας την πιθανή χρήση τους από κοινού σε μια επιχείρηση (μια επιχείρηση ΗΠ θα μπορούσε να προηγείται μιας κυβερνο-επίθεσης σε ένα σύστημα που βασίζεται στο διάστημα και αντίστροφα.

Στρατιωτικός τομέας
Βασικές παρατηρήσεις και συμπεράσματα

Οι επιθέσεις στον κυβερνοχώρο είναι ικανές να διαταράξουν τα συστήματα διοίκησης και ελέγχου (C2C), τα οποία είναι κρίσιμα για τον συντονισμό και τη διεξαγωγή των στρατιωτικών επιχειρήσεων. Οι επιτιθέμενοι έχουν την ικανότητα διείσδυσης σε τέτοια συστήματα και παρέμ-βασης στις επικοινωνίες με στόχο τον αποσυντονισμό της διαδικασίας λήψης απόφασης. Οι κυβερνοεπιθέσεις εναντίον του στρατιωτικού τομέα μπορεί να οδηγήσουν σε έκθεση συντεταγμένων δυνάμεων, διαρροή στρατιωτικής κίνησης ή/και προγραμματισμένα δεδομένα επιθετικής/αμυντικής δράσης, καθιστώντας την προστασία του στρατιωτικού τομέα ζωτικής σημασίας για τη προστασία του προσωπικού, του εξοπλισμού και την απόκτηση/διατήρηση της υπεροχής έναντι του εχθρού.

Ο στρατιωτικός κυβερνοχώρος της Ουκρανίας αποτελεί πεδίο μάχης υψηλής έντασης με συνεχιζόμενες απειλές και επιθέσεις, προερχόμενες από διαφορετικούς δρώντες και διαφορετικές χώρες, οι οποίες ως επί το πλείστον στοχεύουν στην κλοπή δεδομένων, τη διεξαγωγή κατασκοπείας και την καταστροφή περιουσιακών στοιχείων επιδιώκοντας να δημιουργήσουν έναν άμεσο και έμμεσο αντίκτυπο στην ικανότητα της Ουκρανίας να πολεμήσει.

Η Ουκρανία έπρεπε να επιταχύνει σημαντικά την ανάπτυξη και την ενίσχυση των κυβερνοδυνατοτήτων της στον στρατιωτικό τομέα με νέες ικανότητες οι οποίες αναβαθμίζουν τις «παραδοσιακές» λύσεις κυβερνοάμυνας:

- Ξεχωριστή μονάδα εντός της στρατιωτικής δομής υπεύθυνης για την κυβερνοάμυνα, ικανή να διεξάγει δραστηριότητες απόκτησης πληροφοριών, επιχειρήσεις στον κυβερνοχώρο, πληροφοριακές επιχειρήσεις κυβερνοχώρου.
- Εγκαθίδρυση μηχανισμού προσέλκυσης του απαραίτητου αριθμού ειδικών για να αποκρουσθεί η επιθετικότητα στον κυβερνοχώρο.

- Δυνατότητα ταχείας δημιουργίας νέων ασφαλών καναλιών επικοινωνίας, λύσεων λογισμικού.
- Ταχεία διερεύνηση νέων απειλών, παράδοση αποτελεσμάτων έρευνας σε οντότητες κυβερνοασφάλειας καθώς και παραγωγή, αναθεώρηση και επεξεργασία σχεδίων αντιμετώπισης περιστατικών.
- Καθιέρωση σταθερής επικοινωνίας με ξένους εταίρους από στρατιωτικούς και εμπορικούς τομείς.
- Προσαρμογή των ταχέως αναπτυσσόμενων συστημάτων κυβερνο-προστασίας στην υφιστάμενη νομοθεσία και κανονιστικών οδηγιών.
- Αν και δεν αφορά συγκεκριμένα την άμυνα στον κυβερνοχώρο, συνιστάται η γρήγορη ανάπτυξη πύργων επικοινωνίας GSM/4G για περίπτωση στρατιωτικής σύγκρουσης ή φυσικής καταστροφής. Αυτοί είναι αυτοκινούμενοι (γεννήτριες) πύργοι επικοινωνίας τοποθετημένοι σε όχημα που εκτείνονται σε τοποθεσίες που υποφέρουν από διακοπές ρεύματος και παρέχουν επικοινωνία φωνής και δεδομένων μέσω δορυφόρου ή σύνδεσης οπτικής επαφής, και μπορεί καλύπτουν εμβέλεια 3-6 km.

Ψηφιακές υπηρεσίες προς υποστήριξη της πολεμικής προσπάθειας

Τα παραδοσιακά κανάλια επικοινωνίας και ενημέρωσης (τηλεόραση, ραδιόφωνο, ειδήσεις, κλπ) εξακολουθούν να είναι σημαντικά αλλά δεν επιτρέπουν ταχείες προειδοποιήσεις για επικίνδυνα γεγονότα, όπως αεροπορικά πλήγματα ή χτυπήματα πυροβολικού, φυσικές καταστροφές και απειλές στον κυβερνοχώρο.

Υπάρχει επίσης σημαντική ανάγκη για διαφορετικά είδη ανατροφοδότησης από τον πληθυσμό, όπως πληροφορίες για εχθρικές στρατιωτικές μονάδες σε κατεχόμενα εδάφη, κατεστραμμένες κρίσιμες υποδομές κλπ. Το διαδίκτυο μέσω κινητής τηλεφωνίας, διάφορα συστήματα μηνυμάτων (messenger), ειδικές εφαρμογές για κινητά, είναι κάποιες σύγχρονες ψηφιακές υπηρεσίες, που μπορούν να εξυπηρετήσουν καλύτερα σε αυτόν τον ρόλο.

Από την άλλη πλευρά, η εισαγωγή ψηφιακών υπηρεσιών αυξάνει τον κίνδυνο απειλών στον κυβερνοχώρο, τόσο για τις υπηρεσίες όσο και για τους χρήστες τους.

Ακολουθούν διάφορα παραδείγματα ψηφιακών υπηρεσιών που έχουν δημιουργηθεί στην Ουκρανία, προς υποστήριξη της πολεμικής προσπάθειας:

ΥΠΗΡΕΣΙΕΣ	
ΥΠΗΡΕΣΙΑ	**ΠΕΡΙΓΡΑΦΗ**
Εθνική περιαγωγή[8] **National roaming**	Με την εθνική περιαγωγή κατέστη δυνατή η σύνδεση στο δίκτυο άλλων φορέων εκμετάλλευσης εάν η σύνδεση εξαφανιστεί.
Σύστημα Προειδοποίησης Πληθυσμού Έκτακτης Ανάγκης[9] **Emergency Population Warning System**	Το νέο σύστημα ειδοποιήσεων λειτουργεί με βάση την τεχνολογία Cell Broadcast, η οποία έχει σημαντικά πλεονεκτήματα έναντι της ειδοποίησης SMS: ταχύτερη λήψη ειδοποιήσεων, ευελιξία στην επιλογή τοποθεσιών που θα ειδοποιούνται και παρουσία ηχητικού σήματος ακόμα κι αν ο ήχος στο smartphone του συνδρομητή είναι απενεργοποιημένος. Δεν είναι απαραίτητο να εγκαταστήσετε κάτι συγκεκριμένο το τηλέφωνο - όλοι οι Ουκρανοί χρήστες μπορούν να λάβουν τα σήματα
Telegram bot[10]	Ανήκει στις Υπηρεσίες Ασφαλείας της Ουκρανίας @stop_russian_war_bot, που δημιουργήθηκε από την SSU στην αρχή της ευρείας κλίμακας εισβολής της Ρωσίας για να επιτρέπει στους ανθρώπους να στέλνουν ειδοποιήσεις για εχθρικά στρατεύματα και οχήματα, τις τοποθεσίες, τις κινήσεις τους, τα εγκλήματα πολέμου, τους συνεργάτες, κ.λπ. Στις 18 Οκτωβρίου 2022, αναφέρθηκε ότι το bot είχε λάβει πάνω από 100.000 μηνύματα από Ουκρανούς. Αυτό βοήθησε στην καταστροφή εκατοντάδων μονάδων εχθρικού στρατιωτικού εξοπλισμού και ακόμη και στην εξάλειψη αρκετών Ρώσων στρατηγών.
Διαδραστικός χάρτης[11] **Interactive map of the territory**	Η Κρατική Υπηρεσία Έκτακτης Ανάγκης της Ουκρανίας ανέπτυξε έναν διαδραστικό χάρτη περιοχών οι οποίες είναι δυνητικά μολυσμένες με εκρηκτικά αντικείμενα. Αυτός ο χάρτης εμφανίζει τις τοποθεσίες όπου έχουν ήδη βρεθεί εκρηκτικά αντικείμενα ή είναι πιθανό να βρεθούν και το επίπεδο απειλής που

[8] https://www.kmu.gov.ua/en/news/mincifri-ukrayinski-operatori-dozvolyat-peremikatisya-mizh-merezhami-shchob-lishatisya-na-zvyazku

[9] https://mediacenter.org.ua/emergency-population-warning-system-of-state-emergency-service-covers-67-of-subscribers/

[10] https://ssu.gov.ua/en/novyny/zavdiaky-chatbotu-sbu-znyshcheno-sotni-odynyts-vorozhoi-tekhniky-i-navit-dekilkokh-heneraliv-illia-vitiuk

[11] https://mine.dsns.gov.ua/

ΥΠΗΡΕΣΙΕΣ	
ΥΠΗΡΕΣΙΑ	**ΠΕΡΙΓΡΑΦΗ**
	συνιστούν, σύμφωνα με τις πληροφορίες που διαθέτει η Κρατική Υπηρεσία Έκτακτης Ανάγκης (το σφάλμα εντοπισμού είναι έως 30 μέτρα). Υπάρχει και αντίστοιχη εφαρμογή για κινητά τηλέφωνα (τόσο Android όσο και iOS) με διαδραστικό χάρτη, καθώς και συστάσεις για τον τρόπο ανίχνευσης επικίνδυνων αντικειμένων, οδηγίες ασφαλείας κ.λπ. Περιέχει επίσης λειτουργία ειδοποίησης με άμεση σήμα εάν το άτομο εισέλθει στην κόκκινη ζώνη.
eVorog Bot[12]	Αυτοματοποιημένο σύστημα (bot) της Telegram που αναπτύχθηκε από το Υπουργείο Ψηφιακού Μετασχηματισμού της Ουκρανίας, πλήρως ενσωματωμένο με την Diia (Ukraine digital service) και προηγμένη λειτουργικότητα για ανίχνευση: • Εχθρικού εξοπλισμού και στρατευμάτων. • Δραστηριοτήτων φιλορώσων συνεργατών. • Εκρηκτικών ή ύποπτων αντικειμένων. • Φωτογραφιών/βίντεο Ρώσων στρατιωτικών σε αποστρατικοποιημένους οικισμούς.
єППО[13]	Ένα σύστημα ειδοποίησης πρόληψης αεροπορικών επιδρομών. Η Ουκρανία δημιούργησε μια εφαρμογή για κινητά τηλέφωνα που θα βοηθήσουν τις μονάδες αεράμυνας να συμπληρώνουν πληροφορίες ραντάρ σχετικά με εναέριους στόχους για την επακόλουθη καταστροφή τους. Πώς λειτουργεί η εφαρμογή: εάν κάποιο άτομο εντοπίσει οπτικά έναν εναέριο στόχο, για παράδειγμα, έναν πύραυλο ή ένα drone καμικάζι, πρέπει να ανοίξει την εφαρμογή єППО στο smartphone του, να επιλέξει τον τύπο του εναέριου στόχου, να στρέψει το smartphone του προς την κατεύθυνση του, να τον στοχεύσει και να πατήσει το μεγάλο κόκκινο κουμπί. Με αυτόν τον τρόπο τα στοιχεία του στόχου (θέση, είδος, κλπ) καταλήγουν άμεσα σε μονάδες τις Ουκρανικής Αεράμυνας.

Η Ουκρανία έχει επιδείξει τεχνογνωσία με την ευρεία χρήση ψηφιακών τεχνολογιών για τη διασφάλιση σταθερών επικοινωνιών μεταξύ του πληθυσμού και των φορέων διαχείρισης του κράτους και αντίστροφα, κατά τη διάρκεια της περιόδου της κρίσεως.

Οι μέθοδοι επικοινωνίας καταδεικνύουν τη σημασία της βιώσιμης πρόσβασης του πληθυσμού στις υπηρεσίες επικοινωνίας και το διαδίκτυο, καθώς και την ενημέρωση όλων των πολιτών για τυχόν πιθανές απειλές, επιτρέποντάς τους έτσι να βοηθήσουν τις ένοπλες δυνάμεις στον εντοπισμό του εχθρού.

Κάθε χώρα ή συμμαχία θα πρέπει να εξετάσει το ενδεχόμενο να έχει μια καλά ανεπτυγμένη, δοκιμασμένη και αξιόπιστη δημόσια επικοινωνία και σύστημα έγκαιρης προειδοποίησης.

Επίσης, αξίζει να σημειωθεί ότι ένα αυτόνομο σύστημα δεν επαρκεί στο σημερινό πολύπλοκο επικοινωνιακό τοπίο, και γι'αυτό το λόγο οι φορείς κρατικής ασφάλειας και οι κρατικοί κυβερνητικοί φορείς θα πρέπει να διατηρούν διαδικτυακή παρουσία εντός τέτοιων δικτύων όπως το Signal, το Telegram, το Twitter και άλλα. Το βασικό σημείο είναι ότι οι λογαριασμοί σε τέτοιες πλατφόρμες πρέπει να επαληθεύονται και να είναι αξιόπιστοι. Η εμπιστοσύνη και η εμπιστευτικότητα σε τέτοιους λογαριασμούς πρέπει να είναι σε υψηλό επίπεδο για να αποφευχθούν πλαστοπροσωπία ή παραπληροφόρηση.

ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

Η χρήση του κυβερνοχώρου ως πεδίου για τη διεξαγωγή επιχειρήσεων ουσιαστικά ξεκίνησε για πρώτη φορά το 2007 με τις κυβερνοεπιθέσεις στην Εσθονία, συνεχίστηκε με τις επιθέσεις στην Γεωργία το 2008 όπου χρησιμοποιήθηκαν κυβερνοεπιθέσεις και επιχειρήσεις επιρροής στον κυβερνοχώρο παράλληλα με τις συμβατικές επιχειρήσεις.

Η πλήρης ενσωμάτωση τέτοιου είδους επιχειρήσεων στην όλη στρατιωτική προσπάθεια συνέβη κατά τη διάρκεια του πολέμου στην Ουκρανία, όπου οι κυβερνοεπιχειρήσεις έπαιξαν και συνεχίζουν, σημαντικό ο ρόλο ακόμη και πριν την έναρξη των συμβατικών επιχειρήσεων, ακρωτηριάζοντας τις επιθετικές και αμυντικές ικανότητες του αντιπάλου, επηρεάζοντας έτσι το ηθικό του. Οι ενέργειες στον κυβερνοχώρο από την πλευρά της Ρωσίας είχαν ως βασικό στόχο την υποστήριξη των συμβατικών, κυρίως χερσαίων

[12] https://en.interfax.com.ua/news/telecom/810765.html
[13] Українці через застосунок єППО можуть допомогти зенітникам збивати ворожі дрони та ракети

επιχειρήσεων αλλά και την δημιουργία κατάλληλων ψυχολογικών επιπτώσεων σε συγκεκριμένα ακροατήρια στόχος.

Σύμφωνα με τη στατιστική έκθεση του Κρατικού Κέντρου Κυβερνοπροστασίας της Ουκρανίας, το 2022 υπήρχαν 2,8 φορές περισσότερα περιστατικά στον κυβερνοχώρο από ό,τι το 2021. Ο αριθμός των περιστατικών στον κυβερνοχώρο όσο αφορά τη διασπορά κακόβουλου λογισμικού και ανάκτησης πληροφοριών αυξήθηκαν κατά 18,3 και 2,2 φορές αντίστοιχα.

Ο αριθμός των συμβάντων που εντοπίστηκαν και σχετίζονται με τη Ρωσία αυξήθηκε κατά 26%. Το 2022, εντοπίστηκαν και διερευνήθηκαν επίσημα 2194 επιθέσεις στον κυβερνοχώρο (1655 από τον Φεβρουάριο του 2022).

Οι επιθετικές κυβερνοεπιχειρήσεις της Ρωσίας, μαζί με τον ηλεκτρονικό πόλεμο, απέτυχαν να διαλύσουν το σύστημα διοίκησης και ελέγχου (C2) της Ουκρανίας και την κρίσιμη, ιδιωτική και δημόσια υποδομή του για παρατεταμένη χρονική περίοδο. Η Ουκρανία, με τη βοήθεια ιδιωτικών εταιρειών και δυτικών κυβερνήσεων, κατάφερε όχι μόνο να μετριάσει την πλειονότητα των επιθέσεων στον κυβερνοχώρο κατά της υποδομής της αλλά επίσης και να αναπτύξει δικές τις επιθετικές κυβερνο-δυνατότητες.

Η μεγαλύτερη απειλή στον κυβερνοχώρο για την Ουκρανία είναι οι ομάδες χάκερ που σχετίζονται με τη FSB, τη GRU και τη SVR. Σε ένα μικρότερο βαθμό, οι ομάδες χάκερ με οικονομικά κίνητρα και οι φιλορωσικές ομάδες χακτιβιστών αποτελούν επίσης απειλή. Οι πιο ενεργές ομάδες hacking είναι οι Sandworm, APT28, EmberBear, Turla, Gamaredon, Calisto και APT29, ενώ οι KillNet, NoName057, People's Cyber Army, Xaknet Team και RaHDit είναι οι πιο δραστήριες φιλορωσικές χακτιβιστικές ομάδες.

Συμπεράσματα στο πεδίο (κυβερνοχώρος)

Τα δυο χρόνια του πολέμου στην Ουκρανία έδωσε αρκετά συμπεράσματα ως προς την χρήση κυβερνοδυνατοτήτων κατά την διάρκεια μια συμβατικής σύγκρουσης:

- Η Ρωσία ανέπτυξε και εξάντλησε τις αρχικές κυβερνοδυνατότητες της λίγο πριν και κατά την έναρξη της εισβολής στις 24 Φεβρουαρίου 2022. Οι ρωσικές κυβερνοεπιχειρήσεις είχαν ως στόχο να υπονομεύσουν τις στρατιωτικές επιχειρήσεις της Ουκρανίας, οικονομικούς και κυβερνητικούς τομείς, να αποκτήσουν πρόσβαση σε κρίσιμες υποδομές καθώς και στο να απαγορεύσουν από το κοινό την πρόσβαση στην πληροφορία. Πολλές επιθέσεις στόχευσαν την κρίσιμη υποδομή της Ουκρανίας με στόχο να διαταράξουν τη λειτουργία της.

- Οι Ρωσικές κυβερνοεπιθέσεις απέτυχαν στο να δημιουργήσουν σοβαρό μακροχρόνιο πρόβλημα στις Ουκρανικές κρίσιμες υποδομές.

- Οι Ρώσοι επικεντρώνονται κυρίως σε επιθέσεις Κατανεμημένης Άρνησης Παροχής Υπηρεσιών (DDoS), σε επιχειρήσεις προπαγάνδας και δυσφήμισης καθώς και επιχειρήσεις ηλεκτρονικής εξαπάτησης (phishing). Ως αποτέλεσμα, η Ουκρανία δίνει μεγαλύτερη προσοχή στις ιδιαιτερότητες τέτοιων επιθέσεων.

- Η Ρωσία προσπαθεί να βρει νέους συμμάχους οι οποίοι θα την βοηθήσουν στις κυβερνο/στρατιωτικές επιχειρήσεις της, κάτι που ενδεχομένως θα δημιουργήσει μεγαλύτερη ζημιά καθώς στην προσπάθεια της να πετύχει τους στόχους της, πιθανώς να στραφεί προς την Κίνα η οποία ελπίζει να λάβει ενεργό μέρος στην διαμορφωθείσα γεωπολιτική κατάσταση στην Ευρώπη.

- Είναι σχεδόν βέβαιο ότι Ρωσικοί φορείς κυβερνοαπειλών, χρηματοδοτούμενοι από το κράτος θα συνεχίσουν τις δραστηριότητές τους για την προώθηση των στρατηγικών και τακτικών στόχων του ρωσικού στρατού στην Ουκρανία.

- Παρόλο που οι ρωσικές κυβερνο-δραστηριότητες επικεντρώνονται κυρίως σε στόχους στην Ουκρανία, υπάρχει μεγάλη πιθανότητα οι επιθέσεις να μεταφερθούν-επεκταθούν (διάχυση) στην Ευρώπη και στις χώρες που υποστηρίζουν την Ουκρανία.

- Δεδομένου ότι η Ρωσία εστιάζει στην καταστροφή ή τη δημιουργία σημαντικού προβλήματος στη κρίσιμη υποδομή της Ουκρανίας, είναι ασφαλές να δεχτούμε ότι οι επιχειρήσεις στον κυβερνοχώρο είναι και θα χρησιμοποιηθούν στο μέλλον εντός του διακλαδικού σχεδιασμού επιχειρήσεων για την υποστήριξη των συμβατικών κινητικών πολεμικών επιχειρήσεων.

- Η Ουκρανία κατάφερε να περιορίσει τη ζημιά στις υποδομές της, μεταφέροντας πολλές από τις υπηρεσίες της σε υποδομή «νέφους-cloud» εκτός χώρας. Μετά από κάθε κυβερνοεπίθεση, τα συστήματα υποδομής της Ουκρανίας γίνονταν λιγότερο ευάλωτα. Αρχικά, αν και η άμυνα ήταν η κύρια προτεραιότητα στην προστασία των υποδομών, με τον καιρό έχει μεταβληθεί σε μια επιθετική στρατηγική

- Η συνεργασία μεταξύ ιδρυμάτων, οργανισμών και κρατών αποτελεί κρίσιμο παράγοντα για τη διατήρηση της προστασίας των υποδομών σε υψηλό επίπεδο.

- Η ασφάλεια στον κυβερνοχώρο δεν είναι πλέον θέμα που αφορά ειδικούς. Σε κάθε χώρα, οι άνθρωποι είναι η πρώτη γραμμή άμυνα έναντι επιθέσεων στον κυβερνοχώρο.

- Η άμυνα εναντίον μια στρατιωτικής εισβολής προϋποθέτει για τις περισσότερες χώρες την ικανότητα να εξάγουν και να διανέμουν ψηφιακές λειτουργίες τους πέρα από τα σύνορά τους και σε άλλες χώρες.

Η Ρωσία από την αρχή της σύγκρουσης στόχευσε παράλληλα με συμβατικά (πυραύλους) και ψηφιακά μέσα (λογισμικό διαγραφής), την πληροφοριακή υποδομή της Ουκρανίας. Ωστόσο, η Ουκρανία κατάφερε να μεταφέρει και με αυτόν τον τρόπο να προστατεύσει μεγάλο μέρος των πολιτικών και στρατιωτικών της ψηφιακών υποδομών σε υπηρεσίες νέφους (cloud hosting) κυρίως εκτός της χώρας.

- Η πρόσφατη πρόοδος η οποία έχει επιτευχθεί στον τομέα της συλλογής πληροφοριών απειλών (cyber threat intelligence) και της προστασίας τελικού σημείου (end-point protection) βοήθησε την Ουκρανία να αντιμετωπίσει ένα μεγάλο ποσοστό των Ρωσικών καταστροφικών κυβερνοεπιθέσεων.

Στην σημερινή σύγκρουση οι ρωσικές κυβερνοεπιθέσεις είναι διαφορετικές από αυτές που παρατηρήθηκαν το 2017 με την περίπτωση του κακόβουλου λογισμικού NotPetya. Στη συγκεκριμένη επίθεση (2017) χρησιμοποιήθηκε καταστροφικό κακόβουλο λογισμικό το οποίο είχε την ικανότητα ανεξέλεγκτης διασποράς σε αλληλοσυνδεόμενα συστήματα εντός και εκτός χώρας. Στις σημερινές ρωσικές επιθέσεις έχει παρατηρηθεί περιορισμός της διασποράς του κακόβουλου λογισμικού εκτός Ουκρανίας με παράλληλη αύξηση της προσπάθειας συγχρονισμού των κυβερ-νοεπιθέσεων με τις αντίστοιχες συμβατικές επιχειρήσεις. Η χρήση από πλευράς αμυνόμενων, διαδικασιών συλλογής πληροφοριών απειλών με τη βοήθεια τεχνητής νοημοσύνης (Artificial Intelligence-AI) καθώς και λύσεων προστασίας τελικού σημείου κατέστησαν δυνατό τον ταχύτατο διαμοιρασμό λογισμικού/κώδικα προστασίας ώστε να εντοπισθούν και αντιμετωπισθούν οι επιθέσεις.

- Καθώς ένας συνασπισμός χωρών έχει συγκεντρωθεί για να υπερασπιστεί την Ουκρανία, οι ρωσικές υπηρεσίες πληροφοριών ενίσχυσαν τις προσπάθειες κατασκοπείας και διείσδυσης σε πληροφοριακά δίκτυα με στόχο συμμαχικές κυβερνήσεις εκτός Ουκρανίας.

Έχουν εντοπισθεί ενέργειες διείσδυσης σε 128 οργανισμούς σε 42 χώρες εκτός Ουκρανίας. Κύριο στόχο αποτελούν χώρες οι οποίες συνδράμουν την Ουκρανία όπως: οι ΗΠΑ, η Πολωνία, οι βαλτικές χώρες, η Δανία, η Νορβηγία, η Φιλανδία, η Τουρκία καθώς και

άλλες Ναtοϊκές χώρες. Η λίστα των στόχων σε αυτές τις χώρες περιλαμβάνει κυβερνητικές υποδομές, δεξαμενές σκέψης (think tanks), ανθρωπιστικές οργανώσεις, εταιρείες πληροφορικής, υποδομές παροχής ενέργειας και κρίσιμων υποδομών καθώς και τις εταιρείες υποστήριξης τους.

- Σε συνδυασμό με τις ήδη υπάρχουσες κυβερνοδραστηριότητες, οι ρωσικές υπηρεσίες διεξάγουν αντίστοιχες κυβερνοεπιχειρήσεις επιρροής σε παγκόσμιο επίπεδο προς υποστήριξη των πολεμικών της προσπαθειών.

Οι συγκεκριμένες επιχειρήσεις συνδυάζουν τακτικές που έχουν αναπτυχθεί πριν από δεκαετίες από την KGB με τις νέες ψηφιακές τεχνολογίες και το διαδίκτυο ώστε να δώσουν στις επιχειρήσεις επιρροής μεγαλύτερη γεωγραφική κάλυψη, ταχύτητα, προσαρμοστικότητα, πιο ακριβή στόχευση και μεγαλύτερη ισχύ. Τέτοιου είδους επιχειρήσεις με επαρκή σχεδιασμό και τεχνογνωσία μπορούν να εκμεταλλευθούν την αμεσότητα και ευρύτητα των δημοκρατικών κοινωνιών.

Υπό αυτήν την οπτική οι Ρώσοι επικέντρωσαν τις επιχειρήσεις επιρροής τους σε τέσσερα ακροατήρια με συγκεκριμένους στόχους:

- Ρωσικός πληθυσμός: Τη συνεχιζόμενη υποστήριξη της πολεμικής προσπάθειας.
- Ουκρανικός πληθυσμός: Την υπονόμευση της εμπιστοσύνης στην θέληση και ικανότητα της χώρας να αντισταθεί στις ρωσικές επιθέσεις.
- Αμερικανικά και Ευρωπαϊκά ακροατήρια: Την υπονόμευση της δυτικής ενότητας και την εκτροπή των επικρίσεων για τα Ρωσικά εγκλήματα πολέμου>
- Ακροατήρια μη συμμαχικών χωρών: Για τη διατήρηση της υποστήριξης προς τη Ρωσία στα ΗΕ και άλλους οργανισμούς.

Οι ρωσικές κυβερνοεπιχειρήσεις επιρροής είναι άμεσα συνδεδεμένες με τακτικές οι οποίες δημιουργήθηκαν για άλλου είδους κυβερνοεπιχειρήσεις όπως οι τακτικές των ομάδων διαρκούς απειλής (Advanced Persistent Threat-APT) των ρωσικών υπηρεσιών πληροφοριών, τις ομάδες διαρκούς χειραγώγησης (Advanced Persistent Manipulation-APM) οι οποίες σχετίζονται με κυβερνητικές υπηρεσίες και δρουν μέσω Μέσων Κοινωνικής Δικτύωσης και ψηφιακών πλατφορμών.

Οι συγκεκριμένες επιχειρήσεις επιρροής μέσω κυβερνοχώρου, προτοποθετούσαν αφηγήματα σχεδόν με τον ίδιο τρόπο που έτερες κυβερνοεπιχειρήσεις προτοποθετούσαν κακόβουλο λογισμικό σε πληροφοριακά συστήματα. Στη συνέχεια εκκινούσαν μια ευρεία και ταυτόχρονη «αναφορά» των συγκεκριμένων αφηγημάτων από ιστότοπους οι οποίοι βρίσκονταν κάτω από τον έλεγχο της ρωσικής κυβέρνησης μεγεθύνοντας παράλληλα μέσω τεχνολογιών εργαλείων εκμετάλλευσης των Μέσων Κοινωνικής δικτύωσης. Πρόσφατα παραδείγματα περιλαμβάνουν αφηγήσεις γύρω από τα βιοεργαστήρια και πολλαπλές προσπάθειες για τη συγκάλυψη των στρατιωτικών επιθέσεων εναντίον ουκρανών αμάχων. Εκτιμάται ότι οι ρωσικές επιχειρήσεις επιρροής στον κυβερνοχώρο αύξησαν με επιτυχία τη διάδοση της ρωσικής προπαγάνδας μετά την έναρξη του πολέμου κατά 216% στην Ουκρανία και 82% στις Ηνωμένες Πολιτείες.

- Τα διδάγματα από την Ουκρανία απαιτούν μια ολοκληρωμένη και συντονισμένη στρατηγική για την ενίσχυση της άμυνας εναντίον όλου του φάσματος των κυβερνοεπιχειρήσεων είτε αυτές εκδηλώνονται με τη μορφή καταστροφικών κυβερνοεπιθέσεων, κυβερνοκατασκοπείας ή επιχειρήσεων επιρροής.

Ενώ υπάρχουν βασικές διαφορές μεταξύ των παραπάνω επιχειρήσεων, η Ρωσική κυβέρνηση τις αντιμετωπίζει ως μέρος μια ευρύτερης πληροφοριακής επιχείρησης η οποία αν και έχει τους δικούς αντικειμενικούς σκοπούς και στόχους βρίσκεται σε πλήρη συγχρονισμό με τις συμβατικές επιχειρήσεις. Αυτή η νέα πραγματικότητα απαιτεί τελείως διαφορετική προσέγγιση όσο αφορά στην αντιμετώ-πιση και αποτροπή τέτοιων απειλών.

Η αποτροπή τέτοιου είδους απειλών θα πρέπει να στηριχθεί καταρχήν στις παρακάτω παραδοχές:

- Οι ρωσικές απειλές στον κυβερνοχώρο προωθούνται από ένα κοινό σύνολο δρώντων (ομάδων, υπηρεσιών, κλπ) εντός και εκτός της ρωσικής κυβέρνησης οι

οποίοι χρησιμοποιούν παρόμοιες ψηφιακές τακτικές. Ως αποτέλεσμα, θα χρειαστεί πρόοδος τόσο στην ψηφιακή τεχνολογία, την τεχνητή νοημοσύνη όσο και στην διαχείριση των δεδομένων για την αντιμετώπισή τους.

- Σε αντίθεση με τις παραδοσιακές απειλές του παρελθόντος, οι αντιδράσεις σε τέτοιου είδους επιθέσεις στον κυβερνοχώρο πρέπει να βασίζονται σε μεγαλύτερη δημόσια και ιδιωτική συνεργασία.
- Υπάρχει ανάγκη για στενή και κοινή πολυμερή συνεργασία μεταξύ των κυβερνήσεων για την προστασία των ανοιχτών και δημοκρατικών κοινωνιών.
- Το αμυντικό δόγμα θα πρέπει να υποστηρίζει την ελεύθερη έκφραση και να αποφεύγει τη λογοκρισία στις δημοκρατικές κοινωνίες, ακόμη και όταν χρειάζονται νέα βήματα για την αντιμετώπιση του πλήρους φάσματος των απειλών στον κυβερνοχώρο που περιλαμβάνουν και τις επιχειρήσεις επιρροής στον κυβερνο-χώρο.

ΜΕΛΛΟΝ

Δεδομένου της αυξανόμενης στενής συνεργασίας μεταξύ Ρωσίας και Κίνας και την προσπάθεια της τελευταίας για αναβάθμιση της γεωπολιτικής της θέσης, αναμένεται αύξηση των κατασκοπευτικών δραστηριοτήτων κινεζικών κυβερνοομάδων, όπως π.χ. οι APT27, APT30, APT31, Ke3chang, Gallium και Mustang Panda, έναντι των κρατών μελών της ΕΕ και του NATO, παράλληλα με τις συνεχείς απειλές από τις πολιτικά υποκινούμενες ρωσικές κυβερνοομάδες.

Λαμβάνοντας υπόψη τη σημαντική εμπειρία και τις δυνατότητες των ρωσικών ειδικών υπηρεσιών, είναι επίσης σημαντική η προστασία υποδομών αποθήκευσης και διακίνησης δεδομένων και του εξοπλισμού δικτύου από μη εξουσιοδοτημένη πρόσβαση και λογισμικό που θα μπορούσε να επιτρέψει στους επιτιθέμενους να έχουν απομακρυσμένη πρόσβαση σε συστήματα στόχων.

Στο μέλλον θα υπάρξει μια συνεχώς αυξανόμενη επένδυση τόσο στις αμυντικές όσο και στις επιθετικές δυνατότητες στον κυβερνοχώρο, κάτι το οποίο είναι απαραίτητο για τον μετριασμό των κινδύνων για την ασφάλεια. Οι οργανισμοί μπορούν να μειώσουν σημαντικά την ευπάθειά τους σε επιθέσεις στον κυβερνοχώρο με την εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και προγράμματα εκπαίδευσης εργαζόμενων. Επιπλέον, η ύπαρξη μιας ολοκληρωμένης στρατηγικής άμυνας στον κυβερνοχώρο μπορεί να βοηθήσει στην ελαχιστοποίηση του αντίκτυπου μιας επιτυχημένης επίθεσης. Η επένδυση στην άμυνα στον κυβερνοχώρο είναι ουσιαστική αυτοάμυνα για τις επιχειρήσεις και κυβερνήσεις ενάντια στην αυξανόμενη απειλή επιθέσεων στον κυβερνοχώρο. Το κόστος μιας επιτυχημένης επίθεσης μπορεί να είναι καταστροφικό, και οι κίνδυνοι αυξάνονται καθώς ο κόσμος μας γίνεται πιο ψηφιακός.

Η επανάσταση της τεχνολογίας έχει φτάσει ακόμα και στους πιο καθημερινούς ανθρώπους σε όλο τον κόσμο, και οι κυβερνοαπειλές ακολούθησαν. Πλέον, η ασφάλεια στον κυβερνοχώρο δεν αφορά μόνο τους επαγγελματίες. Οι άνθρωποι είναι η πρώτη γραμμή άμυνας κατά των επιθέσεων στον κυβερνοχώρο σε κάθε χώρα. Είναι συχνά το πρώτο σημείο επαφής με πιθανές απειλές, και οι ενέργειές τους μπορούν είτε να αυξήσουν είτε να μειώσουν την πιθανότητα μιας επιτυχημένης επίθεσης. Εκπαιδεύοντας τους ανθρώπους για τους κινδύνους και η χρήση βέλτιστων πρακτικών μπορούν να βοηθήσουν στην αποτροπή επιθέσεων και στην ελαχιστοποίηση της ζημιάς σε περίπτωση επιτυχίας της επίθεσης. Από την παροχή πληροφοριών μέσω κρατικών και ιδιωτικών ΜΜΕ, όπως η τηλεόραση και το ραδιόφωνο, μέχρι την εκπαίδευση και την κατάρτιση σε σχολεία και πανεπιστήμια, η ευαισθητοποίηση στον κυβερνοχώρο και η άμυνα πρέπει να διδαχθούν και να γίνουν αντικείμενο εκπαίδευσης.

Η πρόσφατη έκρηξη της τεχνολογίας τεχνητής νοημοσύνης (Artificial Intelligence-AI) έχει τη δυνατότητα να αλλάξει το παιχνίδι στον κυβερνοπόλεμο. Η τεχνητή νοημοσύνη χρησιμοποιείται ήδη στην άμυνα στον κυβερνοχώρο για τον εντοπισμό και την αντιμετώπιση απειλών πιο γρήγορα και αποτελεσματικά, αλλά μπορεί κάλλιστα να χρησιμοποιηθεί από επιτιθέμενους για τη διεξαγωγή εξελιγμένων επιθέσεων στον κυβερνοχώρο.

Ένας τρόπος με τον οποίο μπορεί να αναπτυχθεί η τεχνητή νοημοσύνη στον κυβερνοπόλεμο είναι μέσω της χρήσης αλγορίθμων μηχανικής μάθησης (Machine Learning-ML Algorithms) για τον εντοπισμό προτύπων και ανωμαλιών στην κυκλοφορία του δικτύου. Θα μπορούσε να εξασφαλίσει την ανίχνευση και την απόκριση σε πραγματικό χρόνο σε απειλές και βελτιωμένη ταχύτητα και ακρίβεια της άμυνας στον κυβερνοχώρο.

Μια άλλη πιθανή χρήση της τεχνητής νοημοσύνης στον κυβερνοπόλεμο είναι η ανάπτυξη αυτόνομου κακόβουλου λογισμικού που μπορεί να προσαρμοστεί και να εξελιχθεί ως απάντηση στις μεταβαλλόμενες συνθήκες. Θα μπορούσε να διεξάγει επιθέσεις στον κυβερνοχώρο, θα ήταν δυσκολότερο να εντοπιστεί και να αντιμετωπισθεί από τους αμυνόμενους. Συνολικά, ενώ η τεχνητή νοημοσύνη έχει τη δυνατότητα να είναι ισχυρό εργαλείο για την άμυνα στον κυβερνοχώρο, θέτει επίσης σημαντικές προκλήσεις για όσους εργάζονται στον τομέα. Ως τέτοιο, θα είναι, σημαντικό οι επαγγελματίες της κυβερνοασφάλειας να αναπτύξουν νέες στρατηγικές και εργαλεία για την αντιμετώπιση των απειλών που δημιουργούνται από την τεχνητή νοημοσύνη στον κυβερνοπόλεμο.