ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Θεοχαρούλας Αθανασίου (Α.Μ.:2201)
του Βασιλείου Κωνσταντίνου Χορταριά (Α.Μ.:2249)

ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ:ΝΟΜΙΚΑ ΚΑΙ ΤΕΧΝΙΚΑ ΖΗΤΗΜΑΤΑ
CYBERWAR: LEGAL AND TECHNICAL MATTERS

Επιβλέπουσα

Ευαγγελία Μήτρου

Πειραιάς, Φεβρουάριος 2024

Πίνακας Περιεχομένων

Κεφάλαιο Α 2
Περίληψη 2
Εισαγωγή 4
Ιστορική αναδρομή 5
Κεφάλαιο Β 5
Β.1 Χαρακτηριστικά του κυβερνοπολέμου 5
Β.2 Κυριότερες μορφές - μέθοδοι διεξαγωγής κυβερνοπολέμου 8
Β.3 Ανάλυση του όρου «επίθεση» 10
Β.4 Νομιμότητα κυβερνοπολέμου ως μέσου επίθεσης-αντεπίθεσης 16
Β.5 Κατάταξη επίθεσης στην κατηγορία του κυβερνοπολέμου 20
Κεφάλαιο Γ 28
Νομικά-ηθικά ζητήματα επιλογής στόχων-κανόνες εμπλοκής 28
Γ.1 Νομικά ζητήματα επιλογής στόχων – humanitarian law 28
Γ.2 Jus ad bellum – Jus in bello 30
Γ.3 Ευρωπαϊκή στρατηγική ασφάλειας 33
Κεφάλαιο Δ 36
Δ.1 Τρόποι επίθεσης 36
Δ.2 Αντίμετρα 49
Κεφάλαιο Ε 54
Ε.1.: Η Περίπτωση της Ουκρανίας 54
Συμπεράσματα 58
Βιβλιογραφία 59

Κεφάλαιο Α

Περίληψη

Η αλματώδης πρόοδος της τεχνολογίας τις τελευταίες δεκαετίες, έχουν οδηγήσει στη γέννηση ενός νέου είδους πολέμου, τον κυβερνοπόλεμο.

Παράλληλα, οι θεωρητικοί του δικαίου προσπαθούν να «χαρτογραφήσουν» τη νέα αυτή μορφή πολέμου. Τα κύρια χαρακτηριστικά του κυβερνοπολέμου είναι η έλλειψη ορίων όσον αφορά το μέγεθος των επιχειρήσεων, η ταχύτητα διεξαγωγής τους, η υπέρβαση της έννοιας των δικαιοδοσιών λόγω του παγκόσμιου χαρακτήρα του Διαδικτύου, ο υψηλός βαθμός μεταβλητότητάς του, η δυσκολία

καταλογισμού των επιθέσεων, η έλλειψη άμεσων απωλειών, σε αντίθεση με τον «παραδοσιακό» πόλεμο, το χαμηλό οικονομικό κόστος διεξαγωγής του και το δυσανάλογο κόστος προστασίας του αμυνόμενου και η αδυναμία πρόβλεψης των επιθέσεων.

Οι κυριότερες μορφές διεξαγωγής του κυβερνοπολέμου είναι η κυβερνο-κατασκοπεία, η διάδοση προπαγάνδας, οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (distributed denial of service attacks), οι επιθέσεις κατά οργανισμών κοινής ωφέλειας και υποδομών και η διανομή παραβιασμένου τεχνολογικού υλικού. Ο κυβερνοπόλεμος, ως μορφή διεξαγωγής πολέμου, υπάγεται στο Δίκαιο των Ενόπλων Συγκρούσεων, συνεπώς οι κυβερνοεπιχειρήσεις θα πρέπει να διεξάγονται με βάση τις βασικές αρχές του, οι οποίες διασφαλίζουν την (όσο είναι δυνατό) ομαλή και αναίμακτη διεξαγωγή τους.

Η κυριότερη συζήτηση γύρω από τον κυβερνοπόλεμο περιστρέφεται γύρω από τη νομιμότητά του ως μέσο επίθεσης και αντεπίθεσης. Οι στόχοι των κυβερνοεπιχειρήσεων θα πρέπει να επιλέγονται με γνώμονα το Δίκαιο των Ενόπλων Συγκρούσεων, φροντίζοντας να διασφαλίζεται η ακεραιότητα των πολιτικών υποδομών. Προς αντιμετώπιση των κυβερνοεπιχειρήσεων, έχει αναπτυχθεί πληθώρα αντιμέτρων, ενώ σε Ενωσιακό επίπεδο έχει θεσπιστεί η Ευρωπαϊκή Στρατηγική Ασφαλείας.

Summary

The leaps and bounds of technology in recent decades have led to the birth of a new type of warfare, cyber warfare. At the same time, legal theorists are trying to "map" this new form of war.

The main characteristics of cyber warfare are the lack of limits in terms of the size of operations, the speed of their conduct, the overcoming of the concept of jurisdictions due to the global nature of the Internet, its high degree of variability, the difficulty of attributing attacks, the lack of direct losses , in contrast to "traditional" war, the low economic cost of conducting it and the disproportionate cost of protecting the defender and the inability to predict attacks. The main forms of conducting cyber warfare are cyber-espionage, the spread of propaganda, distributed denial of service attacks, attacks on utilities and infrastructure, and the distribution of hacked technology.

Cyber warfare, as a form of warfare, is subject to the Law of Armed Conflict, therefore cyber operations should be conducted based on its basic principles, which ensure their (as far as possible) smooth and bloodless conduct. The main debate surrounding cyber warfare revolves around its legitimacy as a means of attack and counter-attack. The targets of cyber operations should be selected with the Law of Armed Conflict in mind, taking care to ensure the integrity of the political infrastructure. To deal with cyber operations, a multitude of countermeasures have been developed, while at the EU level the European Security Strategy has been established.

Εισαγωγή

Ο πόλεμος αποτελεί έννοια απόλυτα συνδεδεμένη με την ανθρώπινη ύπαρξη. Στη σημερινή εποχή, η ταχύτατη ανάπτυξη του διαδικτύου, οι συνεχόμενες τροποποιήσεις του διεθνούς πολιτικού σκηνικού, η ραγδαία ανάπτυξη της τεχνολογίας, έχουν δημιουργήσει το έδαφος έτσι ώστε μεμονωμένα άτομα, οργανισμοί, αλλά και ηγέτες κρατών να χρησιμοποιούν το διαδίκτυο για διάφορους λόγους, σε καθημερινή βάση. Ο Alexander Klimburg, εμπειρογνώμονας σε θέματα κυβερνοπολέμου στο Ινστιτούτο Διεθνούς Πολιτικής της Αυστρίας (oiip), δήλωσε στην ημερήσια εφημερίδα «Die Presse», κατόπιν του με αριθμού E-9680/2010 ερωτήματος προς την Επιτροπή βάσει του άρθρου 117 του Κανονισμού, ότι ο κυβερνοπόλεμος είναι ο κατ' εξοχήν ασύμμετρος πόλεμος: «Η χώρα εκείνη που εξαρτάται λιγότερο από συστήματα πληροφορικής, της οποίας ο στρατός εξαρτάται λιγότερο από τις ΤΠ, βρίσκεται σαφώς σε πλεονεκτική θέση. Η χώρα η οποία είναι εκτεθειμένη σε μια κυβερνο-επίθεση πιθανόν να μην γνωρίζει καν –τουλάχιστον στην αρχή– ότι μια άλλη δύναμη της έχει κηρύξει κυβερνοπόλεμο. Και όταν στη συνέχεια τα συστήματα πληροφορικής αποσυντονιστούν, συχνά δεν είναι εύκολο να διαπιστωθεί χωρίς αμφιβολία ποιος είναι ο επιτιθέμενος. Από την άλλη πλευρά, σε πλεονεκτική θέση βρίσκονται και εκείνες οι χώρες –όπως για παράδειγμα οι ΗΠΑ, οι χώρες της Ε.Ε. ή το Ισραήλ– οι οποίες μπορούν να εκμεταλλευτούν ισχυρούς πολλαπλούς εξυπηρετητές και να αναπτύξουν μεγαλύτερη αποτελεσματικότητα στον κυβερνοχώρο χάρη στα πλήθη των επιδέξιων προγραμματιστών τους. Μέχρι τώρα, ο κυβερνοπόλεμος ήταν γνωστός μόνο από ταινίες του James Bond όπως "Το Αύριο Ποτέ δεν Πεθαίνει", ή από τον "Εξολοθρευτή". Αυτό που μέχρι σήμερα βρισκόταν στη σφαίρα του Χόλιγουντ μοιάζει τώρα να είναι πραγματικότητα».

Στη σημερινή εποχή παρατηρείται όλο και περισσότερα κράτη να εφαρμόζουν αυτή την τακτική για να πλήξουν τον εχθρό τους, χωρίς να αφήνουν ίχνη. Ως μελέτη περίπτωσης αναφερόμαστε στον πόλεμο μεταξύ Ρωσίας - Ουκρανίας, εξετάζοντας παράλληλα και ποιες είναι οι επιλογές αλλά και πώς προδιαγράφεται το μέλλον των κοινωνιών και η ασφάλειά τους.

Ιστορική αναδρομή

Στο παρελθόν υπάρχουν πολλά παραδείγματα ως αναφορές για συγκρούσεις και πολεμικές ενέργειες που χρησιμοποιούσαν τακτικές ή άτακτες μεθόδους, όπως η ψυχολογική πίεση απέναντι στον εχθρό, που είναι ένα σκέλος του σημερινού κυβερνοπολέμου όπως τον γνωρίζουν. Ωστόσο, η πρώτη τέτοια μορφή στην ιστορία του κόσμου, που αφορά μία ανορθόδοξη τακτική, και αποτελεί προϊόν μυθοπλασίας περισσότερο παρά ιστορίας, ήταν ο Τρωϊκός Πόλεμος. (Jennings, 2017)

Όπως χαρακτηριστικά αναφέρει ο Σταμπουλής (2021), παλιότερα, η μέθοδος της ενδυνάμωσης στρατιωτών, που ακολουθήθηκε από γνωστούς στρατηλάτες της ιστορίας, όπως ο Μ. Αλέξανδρος αλλά και άλλους, γινόταν με διάφορους τρόπους (Σταμπουλής, 2021) Άλλο ένα τέτοιο χαρακτηριστικό παράδειγμα της ιστορίας είναι ο Πελοποννησιακός Πόλεμος, καθώς για την εξέλιξη του λοιμού, σύμφωνα με κάποιες θεωρίες, υπαίτιοι ήταν Σπαρτιάτες, που δηλητηρίασαν το νερό, ενώ οι Αθηναίοι αναγκάστηκαν να κλειστούν πίσω από τα τεύχη, ώστε να μην εξαπλωθεί η νόσος. (Χαραλαμπόπουλος, 2020) Υπάρχουν πολλά άλλα τέτοια παραδείγματα στην ιστορία που θυμίζουν τον σημερινό υβριδικό πόλεμο, ωστόσο με τα ανάλογα μέσα που υπήρχαν σε κάθε χρονική περίοδο, ασκήθηκε και η ανάλογη πίεση. Γι' αυτό άλλωστε και μέχρι σήμερα δεν υπάρχει ένας σαφής ορισμός για τον πόλεμο αυτόν, ενώ έχουν αποδοθεί διάφορες έννοιες από πολλούς μελετητές. (Παντελής, 2015) Υπάρχουν σαφώς πολλά άλλα τέτοια παραδείγματα στην ιστορία, όπως η Αμερικανική Επανάσταση, στην οποία χρησιμοποιήθηκαν πολλές άτακτες τακτικής, αλλά και κατά τη διάρκεια του Α' Παγκοσμίου Πολέμου. (Deep, 2015)

Στον 21ο αιώνα, τα παραδείγματα αυτά σχετίζονται με τον υβριδικό πόλεμο, όπως ο πόλεμος το 2006 εναντίον της Χεζομπολάχ, το 2014 ο πόλεμος στην Κριμαία (μεταξύ Ουκρανών και Ρώσων), με κυβερνοεπιθέσεις και άλλες πρακτικές, όπως εμπάργκο σε ενέργεια και προϊόντα. (Στραβοπόδης, 2019) Ο πιο πρόσφατος κυβερνοπόλεμος, που έχει πάρει και μεγάλες διαστάσεις, είναι αυτός μεταξύ Ρωσίας-Ουκρανίας, που θα αναλύσουμε σε επόμενο κεφάλαιο.

Κεφάλαιο Β

Β.1 Χαρακτηριστικά του κυβερνοπολέμου

Τα κύρια χαρακτηριστικά του κυβερνοπολέμου, που στην ουσία τον διαφοροποιούν και από το συμβατικό πόλεμο, αλλά και που δίνουν την ευρύτερη έννοια της διάστασής του είναι τα ακόλουθα:

Δεν υπάρχουν όρια. Το μέγεθος του διαδικτύου είναι τεράστιο και δεν έχει όρια, κάτι που διαφοροποιεί τον πόλεμο αυτόν και σε σχέση με τον παραδοσιακό τρόπο πολέμου, όπου εκεί έχουμε τα σύνορα των κρατών και μπορούν να γίνουν κάποιες συσχετίσεις. Ο κυβερνοπόλεμος λαμβάνει χώρα στον κυβερνοχώρο και από τη στιγμή που ο τελευταίος δεν έχει και κάποια σαφή όρια, το είδος του πολέμου

αυτού φαντάζει και ως μία τρομακτική εκδοχή του, που σε πολλές περιπτώσεις έχει ανησυχήσει ειδικούς, μελετητές, αλλά και απλούς πολίτες. (Geers, 2011). Σύμφωνα με τη Reich (2010), ο κυβερνοχώρος είναι τεράστιος και, υπό αυτή την έννοια, οι ενεργοί χρήστες σε αυτόν μπορεί να είναι δισεκατομμύρια άτομα, ενώ ο αριθμός τους συνεχώς αυξάνεται ραγδαία.

Διεξάγεται ταχύτατα. Ο πόλεμος αυτός διεξάγεται γρήγορα, άμεσα, καθώς επίσης και δεν χρειάζεται όλες τις προετοιμασίες, τους χάρτες, τις εκτιμήσεις, αλλά και γενικότερα όλες τις διαδικασίες που γίνονται σε έναν παραδοσιακό πόλεμο. Έτσι μπορεί κάποιος να «χτυπήσει» τον εχθρό του ταχύτατα, ξαφνικά χωρίς να ξέρει από πού προέρχεται ένα χτύπημα ή και να μπορεί να υποθέσει. Αυτή η τακτική βρίσκει και απροετοίμαστο τον απέναντι, ενώ διεξάγεται και με σύγχρονα όπλα, που χρησιμοποιούνται, όπως είναι τα κυβερνοόπλα. Μπορεί, δηλαδή, να πλήξει τον αντίπαλο μέσα σε κλάσματα δευτερολέπτου, προκαλώντας πολλές καταστροφές, όπως σε υποδομές και άλλα συστήματα. (Μαυραγάνη, 2019)

Ξεπερνά την έννοια των δικαιοδοσιών. Ένα επίσης πολύ βασικό χαρακτηριστικό είναι ότι δεν υπάρχουν σύνορα, οπότε όλα είναι εφικτά στο διαδίκτυο και ο καθένας μπορεί να το χρησιμοποιήσει, με σκοπό να επιτύχει το στόχο του. (Lin & Zegart, 2017) Σε αυτό το σημείο πρέπει να επισημανθεί ότι είναι πολύ σπάνιο να αποδοθεί ένας κυβερνοπόλεμος σε ένα κράτος ή ακόμη και σε επίσημες ομάδες του. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση του Stuxnet, όπου ακόμη και σήμερα κανείς δεν μπορεί να είναι σίγουρος ποιος ήταν ο υπεύθυνος, ακόμη κι αν λέγεται ότι πίσω από αυτό βρισκόταν το Ισραήλ.

Εμφανίζει συνεχείς αλλαγές. Ο κυβερνοπόλεμος διεξάγεται σε έναν αχανή χώρο, που τον διακρίνει η μεταβλητότητα, οι πιθανές αλλαγές, καθώς και αστάθμητοι παράγοντες. Είναι γεγονός ότι στο ίντερνετ τίποτε δεν είναι δεδομένο, με την έννοια ότι οποιαδήποτε στιγμή μπορεί να υπάρξει κάποια διακοπή, αδυναμία ή άλλη έλλειψη και υπό αυτή την έννοια δεν είναι μία προβλέψιμη προσέγγιση, κάτι που δεν συμβαίνει στο συμβατικό πόλεμο.

Απόκρυψη ταυτότητας και μη ανάληψη ευθύνης. Κάτι που είναι πολύ βασικό αλλά και εκμεταλλεύσιμο απο τους επιτιθέμενους, καθώς η πηγή των επιθέσεων δεν είναι καθόλου εύκολο να εντοπιστεί. Πρόκειται για μία πολύ συνηθισμένη πρακτική, που χρησιμοποιούν και οι απλοί hackers, για να βλάψουν ιστοσελίδες, μηνύματα ταχυδρομείου κ.λπ. (Schjølberg, 2017) .

Όπως χαρακτηριστικά αναφέρει ο Hoffman (2007), πρόκειται στην ουσία για μια αόρατη απειλή, με κύριο μέλημα να προκληθεί χάος ή καταστροφή στον αντίπαλο. (Haf fman, 2007) Θεωρείται από πολλούς, και όχι τυχαία βέβαια, ως η απόλυτη μορφή πολέμου, ενώ το κόστος του είναι πολύ μικρότερο συγκριτικά με την παραδοσιακή μορφή πολέμου. Κι αυτό διότι σήμερα η χρήση του Ίντερνετ δεν κοστίζει σχεδόν τίποτε σε σχέση με τα τεράστια ποσά που συνήθως δαπανούνται για μετακινήσεις και διάφορους εξοπλισμούς, τα οποία είναι αναγκαία στοιχεία για έναν συμβατικό πόλεμο. Ένα πολύ βασικό

χαρακτηριστικό της νέας αυτής μορφής πολέμου, είναι πώς δεν υπάρχει απώλεια ζωής. Όπως εύκολα γίνεται αντιληπτό, πρόκειται για ένα χώρο που στην κυριολεξία δεν έχει αρχή, τέλος ή κάποια όρια, οπότε για κάποιον χρήστη δεν υπάρχει κάποιος περιορισμός. (Σίμου, 2016) Σε αυτή την περίπτωση, για παράδειγμα, ο επιτιθέμενος μπορεί πολύ εύκολα να κρυφτεί πίσω από την ανωνυμία και να κρατήσει την ταυτότητα, τα στοιχεία του, αλλά και τους στόχους του κρυφά και, υπό αυτή την έννοια, ο εχθρός μπορεί μόνο να κάνει εικασίες και ανάλογα σενάρια. Παράλληλα, σε αυτή την περίπτωση, η απέναντι πλευρά μπορεί να μην έχει κανένα στοιχείο για ποιος επιτίθεται, γιατί, αλλά και ποιος είναι ο τελικός σκοπός του.

Αυτό είναι και ένα στοιχείο που διαφοροποιεί σημαντικά τον κυβερνοπόλεμο από τον παραδοσιακό τρόπο πολέμου, όπου εκεί ο επιτιθέμενος είναι γνωστός, καθώς και οι σκοποί του απέναντι στον εχθρό, ενώ στον κυβερνοπόλεμο κανείς δεν γνωρίζει τίποτε για τον επιτιθέμενο ή και για τις επιδιώξεις του. Ένα επίσης βασικό χαρακτηριστικό είναι ότι οι επιθέσεις αυτές, αν και μπορεί να μην είναι φονικές (δηλαδή μπορεί να μην πλήξουν τους πολίτες ενός κράτους), ωστόσο μπορούν να προκαλέσουν τεράστιες ζημιές σε υποδομές και άλλα συστήματα όπως αναφέραμε παραπάνω. Επιπλέον, είναι πολύ δύσκολο ένα κράτος να αμυνθεί σε μία τέτοια ενέργεια, γιατί στην ουσία δεν γνωρίζει τίποτε για τον εχθρό, ενώ δεν μπορούν να προβλεφθούν και πολλά άλλα ζητήματα, κυρίως δευτερεύοντα, όπως πιθανές οικονομικές συνέπειες ή θέματα ασθένειας του πληθυσμού κ.λπ. (Reich, 2010)

Δεν χάνονται ζωές. Αυτό άλλωστε είναι και ένα σημαντικό στοιχείο διαφοροποίησης του νέου αυτού πολέμου με τον συμβατικό, καθώς εδώ δεν υφίσταται η περίπτωση της απώλειας ζωής. (Schackelford, 2013) Τουλάχιστον όχι με την άμεση έννοια, διότι μπορεί πλήττοντας κάποιες υποδομές να υπάρξουν κάποιες έμμεσες απώλειες. Ένα στοιχείο που διαφοροποιεί επίσης σημαντικό τον πόλεμο αυτό από τον συμβατικό, καθώς στην ιστορία υπάρχουν πολλά παραδείγματα από πολέμους που είχαν τραγικές συνέπειες με εκατοντάδες νεκρούς. Έτσι, κατά κανόνα, θα μπορούσαμε να πούμε ότι οι επιθέσεις αυτές δεν οδηγούν σε τραυματισμό ή και σε θάνατο ατόμου, τουλάχιστον όχι άμεσα, ενώ ταυτόχρονα, το είδος του πολέμου αυτού έχει την δυναμική να αφανίσει πληθυσμούς κρατών. Ο πόλεμος αυτός συμβαίνει με ψηφιακά μέσα και στοχεύοει ψηφιακές υποδομές, με σκοπό να πλήξει, να καταστρέψει ή να προκαλέσει αναταραχή στον απέναντι.

Χαμηλό οικονομικό κόστος. Αυτό συμβαίνει διότι δεν χρειάζεται να δαπανηθούν οικονομικά κονδύλια για την αγορά εξοπλισμού και άλλου υλικού, όπως γίνεται στον κανονικό πόλεμο, όπως π.χ., για άρματα, όπλα κ.λπ. Στην περίπτωση του ψηφιακού κόσμου χρησιμοποιούνται τα λεγόμενα κυβερνοόπλα. Όπως αναφέρουν ο Hammes (2004) και ο Schmidt (2013), και καθώς και όπως αναφέρεται στο «Εγχειρίδιο του Ταλίν», ως κυβερνοόπλα ορίζονται εκείνα τα μέσα, τα εργαλεία, τα όργανα ή τα λογισμικά που μπορούν να προκαλέσουν ζημιά, θάνατο ή τραυματισμό μέσω διαδικτύου. (Hammes, 2004; Schmidt, 2013) Κυρίως, η επιλογή τους γίνεται για να πλήξουν ή να απενεργοποιήσουν

συστήματα και υποδομές του αντιπάλου, όπως για παράδειγμα αυτά που σχετίζονται με την άμυνα και για να προωθήσουν προπαγανδιστικές μεθόδους, μέσα από διάφορες πλατφόρμες και ιστοσελίδες στο διαδίκτυο. Ο στόχος σε αυτές τις περιπτώσεις είναι η απειλή, ο εκφοβισμός, όπως για παράδειγμα απειλή για να πλήξουν βασικές υποδομές ενός κράτους, όπως την υδροδότηση ή την παροχή φυσικού αερίου και άλλα παρόμοια. Χαρακτηριστικό παράδειγμα αποτελεί η επίθεση του Ισραήλ το 2007 στη Συρία, που ως κύριο στόχο είχε να πλήξη την αεράμυνα της χώρας, ώστε η επίθεσή του την από αέρος να μην μπορεί να γίνει αντιληπτή από κανέναν και να είναι πιο εύκολος ο στόχος. Κάτι ανάλογο συνέβη και περίπου έναν χρόνο μετά, όπου η Ρωσία επιτέθηκε στη Γεωργία, μία επίθεση που αξίζει να αναφερθεί ότι ξεκίνησε και με τον παραδοσιακό τρόπο σύγκρουσης, αλλά και με τη χρήση απειλών μέσω του διαδικτύου, δηλαδή με υβριδικό πόλεμος, από διάφορες ιστοσελίδες. (Clarke & Knake, 2010)

Κόστος προστασίας για τον αμυνόμενο. Κύριος στόχος αυτών που αμύνονται στην περίπτωση του κυβερνοπολέμου είναι η προστασία διάφορων συστημάτων, υποδομών, για την προστασία δεδομένων και στοιχείων από τον εχθρό σε μία τέτοια επίθεση, αλλά και η προστασία απέναντι στον πληθυσμό μιας χώρας που μπορεί να διατρέχει οποιονδήποτε παράπλευρο κίνδυνο από τέτοιες επιθέσεις. Ένας από τους κύριους σκοπούς στις αμυντικές επιχειρήσεις είναι η πρόληψη, ο εντοπισμός, καθώς και η αξιολόγηση, αλλά και τα ανάλογα μέτρα που θα ληφθούν ενάντια στον επιτιθέμενο. Σε γενικές γραμμές, η άμυνα μπορεί να γίνει σε διάφορα επίπεδο, ανάλογα με την προτεραιότητα και τη δυσκολία του προβλήματος, αλλά και του συντονισμού που χρειάζεται σε κάθε διαφορετική περίπτωση. (Libicki, 2009)

Αδυναμία προβλέψεων και συνεπειών μιας επίθεσης Αφού ολοκληρωθεί η διαδικασία του κυβερνοπολέμου, ο επιτιθέμενος συνήθως επιδιώκει να καλύψει τα ίχνη του και κάθε στοιχείο της ταυτότητάς του, έτσι ώστε να προστατεύσει σε κάθε περίπτωση την ανωνυμία του. Στη συνέχεια υπάρχουν διάφορες επιλογές, ανάλογα πάντα και με το στόχο, όπως είναι η περίπτωση της εκμετάλλευσης, της χρήσης στοιχείων, της προσβολής, της καταστροφής και άλλα. (Γεωργαντάς, 2016; Σίμου, 2016) Ένα επίσης βασικό στοιχείο που πρέπει να επισημανθεί όσον αφορά τα χαρακτηριστικά του, είναι ότι η επίτευξη της κυριαρχίας έναντι του άλλου είναι αδύνατη, ενώ κανείς δεν μπορεί να γνωρίζει ποια ακριβώς θα είναι η κατάληξη ενός κυβερνοπολέμου, διότι εμπερικλείονται πολλοί παράγοντες, όπως να υπάρξει κάποιο πρόβλημα στη σύνδεση, να πάει κάτι λάθος κ.λπ.

Β.2 Κυριότερες μορφές - μέθοδοι διεξαγωγής κυβερνοπολέμου

Ο κυβερνοπόλεμος μπορεί να διεξαχθεί με πληθώρα μεθόδων, ανάλογα με τις συνθήκες της επιχείρησης (battlefield conditions/operational conditions) και το βαθμό μυστικότητας που απαιτείται για την εκάστοτε επιχείρηση (degree of visibility/degree of secrecy). Οι διακρίσεις αυτές έχουν οδηγήσει στην αποκρυστάλλωση διάφορων «σχολών» κυβερνοπολέμου, οι οποίες παρουσιάζουν μεγάλες ομοιότητες με τα διάφορα στρατιωτικά δόγματα. Η κυριότερη διάκριση μεταξύ των «σχολών» αυτών

είναι η ευθύτητα ή όχι της διενεργούμενης επίθεσης και επικουρικά ο βαθμός μυστικότητάς της (direct attack-indirect attack/subterfuge).

Οι κυριότερες μορφές κυβερνοπολέμου είναι η κυβερνο-κατασκοπεία, η διάδοση προπαγάνδας, οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (distributed denial of service attacks), οι επιθέσεις κατά οργανισμών κοινής ωφέλειας και υποδομών και η διανομή παραβιασμένου τεχνολογικού υλικού (distribution/introduction of compromised technological material).

Η κυβερνο-κατασκοπεία (cyber-espionage) αποτελεί μια από τις πιο συχνές πράξεις κυβερνοπολέμου, και επιτρέπει στον επιτιθέμενο να συλλέξει πληροφορίες για τον στόχο, οι οποίες θα αξιοποιηθούν για την προώθηση των συμφερόντων του επιτιθέμενου, είτε μέσω της διευκόλυνσης των επιχειρήσεων του επιτιθέμενου είτε μέσω του εκβιασμού του αντικειμένου, αν αυτό αποτελεί μεμονωμένο άτομο ή ομάδα ατόμων ως πρόδρομος των επιθέσεων κοινωνικής μηχανικής προς εύρεση «αδύναμου κρίκου».

Η διάδοση προπαγάνδας αποτελεί κατά γενική ομολογία την πιο διαδεδομένη πράξη κυβερνοπολέμου. Κύρια μέσα αυτής είναι οι λεγόμενες «φάρμες τρολ» (troll farms). Οι «φάρμες τρολ» συνίστανται σε σύνολα ατόμων, σε πολλές περιπτώσεις ομάδων bots ελεγχόμενων από έναν χειριστή (controller), τα οποία ενεργούν ως ομάδες πίεσης (societal pressure groups/crisis actors) με σκοπό να στρεβλώσουν την κοινή γνώμη του κράτους-στόχου.

Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης είναι από τις πλέον αποτελεσματικότερες μεθόδους διεξαγωγής κυβερνοπολέμου, λόγω της ευελιξίας ως προς την εφαρμογή τους και της καταστρεπτικής τους δύναμης. Μια τέτοια επίθεση λαμβάνει χώρα όταν ένας ικανός αριθμός χρηστών προσπαθεί να αποκτήσει πρόσβαση σε έναν πόρο διαδικτύου ή τηλεφώνου, με σκοπό να υπερκεράσει τον εκάστοτε εξυπηρετητή (server), οδηγώντας στην απενεργοποίησή του. Επιθέσεις τέτοιου είδους είναι, λόγω της εκ σχεδιασμού άναρχης δομής του Διαδικτύου, πρακτικά αδύνατο να προβλεφθούν και κυρίως είναι ιδιαίτερα δύσκολη η απόκρουσή τους.

Η πλέον καταστρεπτική μέθοδος διεξαγωγής κυβερνοπολέμου, γύρω από την οποία περιστρέφεται η πλειονότητα των συζητήσεων περί της νομιμότητας του κυβερνοπολέμου και των ορίων διεξαγωγής του, είναι η διενέργεια επιθέσεων κατά οργανισμών κοινής ωφελείας και υποδομών. Οι επιθέσεις αυτές διενεργούνται με οποιοδήποτε από τους τρόπους που αναφέρουμε σε αυτή την ενότητα, ενώ παρουσιάζουν μια πρωτοτυπία, τη χρήση κυβερνο-όπλων (cyber-weapons), στα οποία θα αναφερθούμε εκτενέστερα σε επόμενη ενότητα. Το κύριο χαρακτηριστικό των επιθέσεων αυτών είναι ο υψηλός βαθμός πολυπλοκότητάς τους, πράγμα που τις καθιστά πραγματοποιήσιμες μόνο από συγκεκριμένα κράτη.

Η τελευταία από τις κυριότερες μορφές διεξαγωγής κυβερνοπολέμου, και η δυσκολότερη, είναι η διανομή παραβιασμένου τεχνολογικού υλικού. Ως παραβιασμένο τεχνολογικό υλικό ορίζεται αυτό που έχει τροποποιηθεί, ώστε να διευκολύνει τη διεξαγωγή κυβερνοπολέμου. Το παραβιασμένο τεχνολογικό υλικό χωρίζεται σε δύο κατηγορίες, το υλικό παρακολούθησης (surveillance hardware) και το υλικό επίθεσης (attack hardware). Το πρώτο διευκολύνει την κυβερνο-κατασκοπεία, παρέχοντας διακριτική πρόσβαση στο σύστημα του αντικειμένου της επίθεσης, ενώ το δεύτερο δύναται να εξαπολύσει επίθεση, πολλές φορές χωρίς εξωτερική παρέμβαση. Παραδείγματα του πρώτου μπορούν να βρεθούν στον αντίστοιχο κατάλογο της NSA (Electronic Frontier Foundation,2013).

Β.3 Ανάλυση του όρου «επίθεση»

Προκειμένου να εξεταστεί ο κυβερνοπόλεμος υπό το πρίσμα του δικαίου του πολέμου (laws of war), πρέπει να αποκρυσταλλωθεί η έννοια της «επίθεσης», η οποία αποτελεί τον πυρήνα του δικαίου του πολέμου και τον κύριο ρυθμιστή της έννοιας της νομιμότητας εντός του. Καθώς δεν έχει διαμορφωθεί ένας ορισμός της «επίθεσης», θα προσπαθήσουμε να τον εξάγουμε με υπαγωγή.

Η απλούστερη λύση είναι η υπαγωγή της διενέργειας κυβερνοπολέμου στη συλλογιστική περί «ένοπλης επίθεσης», όπως αυτή ορίζεται από τον Οργανισμό Ηνωμένων Εθνών, υπό το πρίσμα του διεθνούς δικαίου. Σύμφωνα με τον ΟΗΕ, η κατάταξη μιας ενέργειας ως «ένοπλης επίθεσης» απαιτεί την ύπαρξη τριών διαφορετικών στοιχείων: α) της Ratione Materie (η καθ' ύλην αρμοδιότητα στο διεθνές δίκαιο, εδώ το «υλικό στοιχείο» της επίθεσης), β) της Ratione Personae (η θέση εξουσίας του ατόμου στο διεθνές δίκαιο, εδώ η εκτίμηση της προέλευσης της επίθεσης) και γ) της Ratione Temporis (ο σχετικός χρόνος στο διεθνές δίκαιο, εδώ ο χρόνος εκτέλεσης της επίθεσης), από τα οποία συνδυαστικά μπορούμε να αντλήσουμε τον ορισμό της «ένοπλης επίθεσης» (Melin, 2021, σς. 7,8,9).

Πρώτο στοιχείο του ορισμού είναι η Ratione Materie, η οποία αναφέρεται στην υλική διάσταση της ένοπλης επίθεσης. Το άρθρο 3 του υπ' αριθμ. 3314/14-12-1974 ψηφίσματος του ΟΗΕ περιέχει τις απαραίτητες κατευθυντήριες γραμμές περί του υλικού στοιχείου της επίθεσης: "Οποιαδήποτε από τις ακόλουθες πράξεις, ανεξαρτήτως κήρυξης πολέμου, η οποία υπόκειται και συμπίπτει με τις διατάξεις του άρθρου 2, χαρακτηρίζεται ως πράξη επίθεσης:

(α) Η εισβολή ή επίθεση από τις ένοπλες δυνάμεις ενός κράτους στο έδαφος ενός άλλου κράτους, ή κάθε στρατιωτική κατοχή, έστω και προσωρινή, που προκύπτει από την εισβολή ή την επίθεση αυτή, ή κάθε προσάρτηση με τη χρήση βίας του εδάφους άλλου κράτους ή μέρους αυτού,

(β) βομβαρδισμό από τις ένοπλες δυνάμεις ενός Κράτους κατά του εδάφους ενός άλλου Κράτους ή της χρήση οποιουδήποτε όπλου από ένα Κράτος κατά του εδάφους ενός άλλου Κράτους,

(γ) ο αποκλεισμός των λιμένων ή ακτών ενός Κράτους από τις ένοπλες δυνάμεις ενός άλλου Κράτους,

(δ) Επίθεση από τις ένοπλες δυνάμεις ενός Κράτους κατά των χερσαίων, θαλάσσιων ή εναέριων δυνάμεων ή των θαλάσσιων και εναέριων στόλων άλλου κράτους,

(ε) Η χρήση ενόπλων δυνάμεων ενός Κράτους που βρίσκονται στο έδαφος ενός άλλου Κράτους με τη συμφωνία του κράτους υποδοχής, κατά παράβαση των όρων που προβλέπονται στη συμφωνία ή οποιαδήποτε παράταση της παρουσίας τους στο έδαφος αυτό πέραν της λήξης της συμφωνίας,

(στ) Η ενέργεια ενός Κράτους που επιτρέπει στο έδαφός του, το οποίο έχει θέσει στη διάθεση άλλου κράτους, να χρησιμοποιηθεί από το άλλο αυτό κράτος για τη διάπραξη επιθετικής πράξης κατά ενός τρίτου κράτους,

(ζ) Η αποστολή από ή για λογαριασμό ενός Κράτους ένοπλων ομάδων, ατάκτων ή μισθοφόρων, οι οποίες εκτελούν πράξεις ένοπλης βίας κατά άλλου Κράτους τέτοιας σοβαρότητας ώστε να ισοδυναμούν με πράξεις που απαριθμούνται ανωτέρω, ή την ουσιαστική συμμετοχή του σε αυτές". (3314/14-12-1974).

Λαμβάνοντας υπόψιν τα ανωτέρω συνδυαστικά με το άρθρο 4 του ίδιου ψηφίσματος το οποίο αναφέρει ότι, μπορούμε να κάνουμε λόγο για μια «κλίμακα» βαρύτητας ενεργειών, η οποία έχει δύο βαθμίδες, αυτή της «επιθετικής ενέργειας» (act of aggression) και της «ένοπλης επίθεσης» (armed attack), με τη δεύτερη έχει το περισσότερο ειδικό βάρος. Την ίδια διαπίστωση έκανε και ο ΟΗΕ, οδηγώντας στη δημιουργία της Ειδικής Επιτροπής επί του Ερωτήματος περί Ορισμού της Επιθετικής Ενέργειας (Special Committee on the Question of Defining Aggression). Η Επιτροπή επιβεβαίωσε την ύπαρξη της ανωτέρω «κλίμακας» και έκανε λόγο περί «κλίμακας και επιπτώσεων» (scale and effects) της ενέργειας του ενός μέρους-κράτους στο άλλο, ώστε να χαρακτηριστεί η ενέργεια αυτή επί της ανωτέρω κλίμακας βαρύτητας. Η απόφαση αυτή της Επιτροπής αποτελεί απόφαση-σταθμό καθώς μέσω αυτής μπορούμε να εφαρμόσουμε τις αρχές του Χάρτη των Ηνωμένων Εθνών επί του κυβερνοπολέμου, καθώς η κύρια διαφορά του από τον «παραδοσιακό» πόλεμο είναι η έλλειψη ενός «σταθερού» μέτρου ενεργειών (measured actions) του επιτιθέμενου και είναι αδύνατος ο εκ των προτέρων προσδιορισμός την εντονότητας τους (intensity of actions), προκειμένου να γίνει ο «παραδοσιακός» χαρακτηρισμός επί της κλίμακας, καθώς δεν δύνανται να συνυπάρχουν πάντα το στοιχείο της ενέργειας και του αποτελέσματος κατά τη διεξαγωγή της επίθεσης (για παράδειγμα επιθέσεις με σκοπό την εγκατάσταση backdoors). Συνεπώς, μπορεί να γίνει λόγος για ένα «όριο» το οποίο πρέπει να ξεπεραστεί ώστε η κυβερνοεπίθεση ενός κράτους σε άλλο να θεωρηθεί «επίθεση». Καθώς είναι αδύνατο να υπάρξει ένας ενιαίος προσδιορισμός του ορίου αυτού, οι κυβερνήσεις και οι διεθνείς οργανισμοί καλούνται να το προσδιορίσουν εξ ιδίων. Έχοντας τα ανωτέρω υπόψιν, οδηγούμαστε στο συμπέρασμα ότι δεν είναι αρκετή η «εντονότητα» της ενέργειας του επιτιθέμενου ώστε αυτή να χαρακτηριστεί ως «επίθεση», αλλά αυτή πρέπει να είναι σε θέση να επιφέρει καταστροφικές συνέπειες, άρα πρέπει να εμφανίζει σωρευτικά τα στοιχεία της εντονότητας, της δυνατότητας φυσικής επενέργειας στο κράτος-στόχο, και της πρόκλησης ζημιών σε αυτό. Συνεπώς, μπορούμε να πούμε ότι μια κυβερνοεπίθεση θεωρείται «επίθεση»

μόνο αν είναι σε θέση να επιφέρει ζημιές στον στόχο. Μια τέτοια εκτίμηση θα οδηγούσε σε κενό λογικής, καθώς δεν είναι όλες οι μέθοδοι διεξαγωγής κυβερνοπολέμου καταστρεπτικές. Αυτό το κενό λογικής έρχεται να θεραπεύσει η έννοια της «ζημίας», η οποία σε συνδυασμό με την ανωτέρω διαπίστωση ότι η κυβερνοεπίθεση πρέπει απλά να μπορεί να επιφέρει ζημίες στο κράτος-στόχο, επιτρέπει στον αμυνόμενο να προβεί σε διαστολή της ad hoc, εξασφαλίζοντας την προστασία του από το διεθνές δίκαιο.

Καθώς όμως δεν είναι δυνατός πάντα ο χαρακτηρισμός μιας ενέργειας κυβερνοπολέμου ως επίθεσης, όπως αναφέραμε παραπάνω, και για να προστατευτεί ακόμα περισσότερο ο εκάστοτε στόχος από το ανωτέρω «κενό λογικής», μπορούμε να εφαρμόσουμε το λεγόμενο «δόγμα της καρφίτσας» (pinprick doctrine). Το «δόγμα της καρφίτσας» στηρίζεται στη σκέψη ότι υπάρχει ακολουθία μεταξύ των ενεργειών, συνεπώς πολλαπλές ενέργειες κυβερνοπολέμου ή ακόμα και προπαρασκευαστικές ενέργειες κυβερνοπολέμου, όπως είναι η εξαπόλυση επιθέσεων προς αναγνώριση της δομής των συστημάτων του στόχου (probing attacks), μπορούν να θεωρηθούν επίθεση, σε περίπτωση που αποδεδειγμένα αποτελούν μέρος ευρύτερου σχεδίου του επιτιθέμενου κράτους. Με τον τρόπο αυτό εντάσσονται και οι μη καταστρεπτικές ενέργειες κυβερνοπολέμου στον ορισμό της επίθεσης, καθώς και οι ενέργειες παθητικής κυβερνο-κατασκοπείας. Μπορούμε επίσης να χρησιμοποιήσουμε τη θεωρία του «βαρελιού πυρίτιδας» (powder keg theory), προκειμένου να κατηγοριοποιήσουμε τις ενέργειες κυβερνοπολέμου ως επιθέσεις. Σύμφωνα με τη θεωρία αυτή, μεταξύ δύο κρατών, ανεξάρτητα από την ύπαρξη προηγούμενων εντάσεων, υπάρχει ένα «όριο», η υπέρβαση του οποίου οδηγεί στην «έκρηξη» του «βαρελιού πυρίτιδας» (burst/fulfillment). Η «έκρηξη» μπορεί να είναι οποιαδήποτε επιθετική ενέργεια η οποία προκαλείται ως συνέπεια των ενεργειών των κρατών που οδήγησαν στην «πλήρωση» του βαρελιού, η λεγόμενη «ενέργεια κορύφωσης» (culminatory action). Κάθε ενέργεια στην προκειμένη περίπτωση κρίνεται τόσο κατά μόνας (individual assessment), όσο και υπό το πρίσμα του συνόλου, σε περίπτωση που δυνητικά αποτελεί μέρος γενικευμένου σχεδίου, προκειμένου να διαπιστωθεί αν είναι ικανή να «γεμίσει το βαρέλι». Η διπλή αυτή αξιολόγηση της κάθε ενέργειας καθιστά τη θεωρία αυτή πιο αξιόπιστη και ακριβής από το «δόγμα της καρφίτσας», καθώς δύνανται να ενταχθούν σε αυτή πραγματικά όλες οι μορφές διεξαγωγής κυβερνοπολέμου, ακόμα και η διάδοση προπαγάνδας, η οποία μπορεί να παράγει αποτελέσματα μόνο μακροσκοπικά και σε βάθος χρόνου, μπορούμε δηλαδή να κάνουμε λόγο για «κίνηση της βελόνας» (moving the needle) με κάθε ενέργεια καθενός από τα κράτη «μέσα στο βαρέλι».

Το δεύτερο στοιχείο της «ένοπλης επίθεσης», προκειμένου να κριθεί δόκιμη η αυτοάμυνα είναι η ratione personae. Η ratione personae αναφέρεται στον παράγοντα (actor) που εξαπέλυσε την επίθεση στο στόχο. Να σημειωθεί ότι αυτό το κριτήριο αφορά καθαρά «παράνομη» επίθεση (illegal use of force). Ως παράνομη χρήση βίας-επίθεση ορίζεται στο άρθρο 2 του Χάρτη των Ηνωμένων Εθνών η απειλή ή χρήση βίας με στόχο την εδαφική ακεραιότητα από ένα κράτος-μέλος κατά ετέρου κράτους-μέλους. Συνεπώς, οδηγούμαστε στο συμπέρασμα ότι η ratione personae εκτείνεται μόνο σε κρατικές οντότητες

και όχι σε μη κρατικούς παράγοντες (non-state actors). Η διαπίστωση αυτή οδηγεί σε κενό λογικής, καθώς είναι αδύνατο να εντοπιστούν μέσα σε εύλογο χρονικό διάστημα δεσμοί μεταξύ του επιτιθέμενου και κάποιας κρατικής οντότητας. Η θεωρητικοί του δικαίου έχουν δώσει μια λύση στο κενό αυτό με τη δημιουργία του «πλάσματος δικαίου» των κρατικώς χρηματοδοτουμένων οντοτήτων (state sponsored entities).

Ο όρος αυτός αποτελεί όρο-ομπρέλα για παράγοντες οι οποίοι ναι μεν δε διαθέτουν (άμεσα τουλάχιστον) αποδεικνυόμενους δεσμούς με κρατικές οντότητες, αλλά τα επιχειρησιακά τους χαρακτηριστικά προδίδουν κρατική παρέμβαση. Ως επιχειρησιακά χαρακτηριστικά ορίζονται ο βαθμός πολυπλοκότητας (degree of sophistication) της επίθεσης, η ποιότητα και ποσότητα των υποδομών αυτής (infrastructure index) και ο τρόπος δράσης τους. Η έννοια του «τρόπου δράσης» περιλαμβάνει τόσο τα οργανωτικά στοιχεία του παράγοντα (οργανογραμματική δομή, τυχόν συστήματα συντονισμού δράσης), όσο και την ανάλυση των κινήτρων της επίθεσης. Η προσπάθεια κατηγοριοποίησης των παραγόντων ως κρατικώς χρηματοδοτουμένων οντοτήτων ξεκινάει συνήθως από την προσπάθεια αποκωδικοποίησης του κινήτρου της επίθεσης (forensic motive analysis). Ο ΟΗΕ έχει κρίνει (UNGA A/RES/3314) ότι επίθεση συνιστά και η αποστολή ενόπλων ομάδων, συμμοριών, ατάκτων ή μισθοφόρων συνιστά επιθετική ενέργεια (act of aggression), συνεπώς μπορούμε να πούμε ότι καλύπτει και τις ανωτέρω οντότητες, οι οποίες δύνανται να εμπίπτουν σε έναν από τους τρεις αυτούς όρους, ανάλογα τη σύνθεση και τον τρόπο δράσης τους.

Το τρίτο και τελευταίο στοιχείο της «ένοπλης επίθεσης» είναι η ratione temporis και, θυμίζοντας το ποινικό δίκαιο, αναφέρεται στο σχετικό χρόνο τέλεσης της ενέργειας από τον επιτιθέμενο. Στην πρώτη παράγραφο του άρθρου 2 της Συνθήκης της Γενεύης αναφέρεται ότι «Εκτός από τις διατάξεις που εφαρμόζονται σε καιρό ειρήνης, η παρούσα Συνθήκη εφαρμόζεται σε όλες τις περιπτώσεις κηρυγμένου πολέμου ή οποιασδήποτε άλλης ένοπλης σύγκρουσης που μπορεί να προκύψει μεταξύ δύο ή περισσότερων Υψηλών Συμβαλλομένων Μερών, ακόμη και αν η κατάσταση πολέμου δεν αναγνωρίζεται από ένα από αυτά.». Με τη γραμματική ερμηνεία της διάταξης εντοπίζουμε ότι η προστασία που παρέχει η Συνθήκη συνδέεται με την ανωτέρω «κλίμακα» εντονότητας ενεργειών του επιτιθέμενου, καθώς περιέχει τις έννοιες «κηρυγμένου πολέμου» και «ένοπλης σύγκρουσης». Αξιοσημείωτη είναι η χρήση του προσδιορισμού «κηρυγμένου», καθώς έτσι αποκλείονται από προστασία συγκρούσεις χαμηλής έντασης (low intensity conflicts/bush wars), εφόσον δεν υπάρχει επίσημη κήρυξη πολέμου. Παραδείγματα τέτοιων συγκρούσεων είναι η σύγκρουση Κίνας-Ινδίας στη συνοριακή τους γραμμή και η σύγκρουση μεταξύ της Νότιας Αφρικής, της Ανγκόλα και της Νοτιοδυτικής Αφρικής (πλέον Ναμίμπια), γνωστή και ως «Συνοριακός Πόλεμος της Νότιας Αφρικής». Η φράση «ακόμη και αν η κατάσταση πολέμου δεν αναγνωρίζεται από ένα από αυτά» λειτουργεί ως «δικλείδα ασφαλείας» στην περίπτωση αυτή. Λαμβάνοντας υπόψιν τα ανωτέρω συνδυαστικά με το «δόγμα της καρφίτσας» που αναλύσαμε παραπάνω, μπορούμε να πούμε ότι η «κατάσταση άμυνας» (defence situation) ξεκινάει από το χρόνο

τέλεσης της ενέργειας του επιτιθέμενου, χωρίς να λαμβάνονται υπόψιν τυχόν προπαρασκευαστικά στάδια, συμπέρασμα που ενισχύεται από την πρώτη παράγραφο του άρθρου 6 της Συνθήκης (Η παρούσα Συνθήκη εφαρμόζεται από την έναρξη κάθε σύγκρουσης ή κατοχής που αναφέρεται στο άρθρο 2). Έχοντας εντοπίσει το σημείο έναρξης του σχετικού χρόνου, μπορούμε να προχωρήσουμε στον εντοπισμό του σημείου λήξης. Το άρθρο 6 της Συνθήκης της Γενεύης αναφέρει ότι «στο έδαφος των μερών της σύρραξης, η εφαρμογή της παρούσας Συνθήκης παύει με τη γενική λήξη των στρατιωτικών επιχειρήσεων», συνεπώς μπορούμε να πούμε ότι σε σχέση με τον κυβερνοχώρο, το σημείο λήξης είναι η στιγμή της ολοκλήρωσης της τελευταίας κυβερνοεπίθεσης μεταξύ των μερών της σύγκρουσης. Πρέπει να σημειωθεί ότι ο όρος «γενική λήξη» περιλαμβάνει και την «τελευταία ομοβροντία» (final salvo), δηλαδή την τελευταία επιθετική πράξη (act of aggression) μεταξύ των μερών, καλύπτοντας έτσι και τυχόν επιθέσεις με αντικείμενο την αξιολόγηση των προκληθεισών ζημιών στον στόχο (damage assessment missions/network reconnaissance).

Φυσική συνέχεια των ανωτέρω είναι η εξέταση της αντεπίθεσης από μέρους του κράτους-στόχου. Όπως εκθέσαμε παραπάνω, υπάρχει ένα «όριο» (threshold) το οποίο πρέπει να ξεπεράσει ο επιτιθέμενος ώστε οι ενέργειές του να θεωρηθούν «ένοπλη επίθεση». Ο χαρακτηρισμός τους αυτός είναι σημαντικός για τη θεμελίωση της αυτοάμυνας, καθώς το άρθρο 51 του Χάρτη των Ηνωμένων Εθνών, από το οποίο πηγάζει και η «νομιμοποίηση» της αυτοάμυνας, απαιτεί την ύπαρξη «ένοπλης επίθεσης» ώστε να δικαιολογηθεί η αυτοάμυνα. Σε περίπτωση που οι ενέργειες του επιτιθέμενου δεν «αρκούν» ώστε να στοιχειοθετηθεί «ένοπλη επίθεση», π.χ. σε περίπτωση που ο επιτιθέμενος εξαπολύσει μη καταστρεπτικές κυβερνοεπιχειρήσεις, όπως «κυβερνοεπιθέσεις ανίχνευσης» (probing cyberattacks), η νομολογία του Διεθνούς Δικαστηρίου έχει δεχτεί (Nicaragua Case (n 7) para 249) ότι το κράτος-στόχος μπορεί να «απαντήσει» αναλογικά (proportional response), όχι όμως σε βαθμό που να συνιστά «ένοπλη επίθεση». Παράλληλα, όπως αναφέραμε παραπάνω, εφαρμόζεται το «δόγμα της καρφίτσας» (pinprick doctrine), οπότε επιθέσεις που αποτελούν μέρος ευρύτερου σχεδίου του επιτιθέμενου δύνανται να ξεπεράσουν το «όριο» και να θεωρηθούν συλλογικά «ένοπλες επιθέσεις». Προκειμένου να εντοπιστεί το ανωτέρω όριο του άρθρου 51, το Διεθνές Δικαστήριο έχει θεσπίσει τη «δοκιμασία κλίμακας και επιπτώσεων» (scale and effect test), η οποία μπορεί να βοηθήσει στη διάκριση μεταξύ της «χρήσης βίας» (use of force) και της «ένοπλης επίθεσης» (NICARAGUA, 1986 para 191,195). Σύμφωνα με την απόφαση του Διεθνούς Δικαστηρίου επί της υπόθεσης Νικαράγουα, μια «ένοπλη επίθεση» θέτει υψηλότερο όριο σοβαρότητας (threshold of severity) από μια περίπτωση «χρήσης βίας», ενώ παράλληλα ένα λιγότερο «έντονο και σοβαρό περιστατικό» (severe and grave incident) το οποίο βρίσκεται μεταξύ της «χρήσης βίας» και της «ένοπλης επίθεσης», δεν ενεργοποιεί το δικαίωμα αυτοάμυνας του άρθρου 51 ((Islamic Republic of Iran v. U.S.), Judgment, 2003 I.C.J. 161, 51 (Nov. 6)). Από τα παραπάνω εξάγεται ότι σε περίπτωση που δεν πληρούνται οι προϋποθέσεις για θεμελίωση αυτοάμυνας, ενώ υπάρχει

αποδεδειγμένη εχθρική ενέργεια, το αμυνόμενο κράτος δύναται να λάβει αντίμετρα (countermeasures), σύμφωνα με το διεθνές δίκαιο, τα οποία δε θα ξεπερνούν το «όριο» ώστε να θεωρηθούν αυτοάμυνα.

Προκειμένου το αμυνόμενο κράτος να ενεργήσει επί του δικαιώματός του στην αυτοάμυνα, πρέπει να κινείται σύμφωνα με συγκεκριμένες κατευθυντήριες γραμμές του διεθνούς δικαίου (international law requirements). Πρώτη και κύρια κατευθυντήρια γραμμή είναι η διάγνωση της αναγκαιότητας της αυτοάμυνας. Το αμυνόμενο κράτος πρέπει, πριν ασκήσει το δικαίωμά του στην αυτοάμυνα, να αναζητήσει εναλλακτικές λύσεις μη επιθετικού χαρακτήρα (non-forcible measures), σε περίπτωση που είναι διαθέσιμες (cyber warfare and the jus ad bellum pg14). Από αυτή την κατευθυντήρια γραμμή συνάγεται ότι η αυτοάμυνα θα πρέπει να ασκείται ως τελευταία επιλογή του αμυνόμενου. Σε περίπτωση που κριθεί αναγκαία η διενέργεια αυτοάμυνας, το αμυνόμενο κράτος θα πρέπει να έχει προχωρήσει σε καταλογισμό (attribution) της «ένοπλης επίθεσης», ο οποίος ορίζεται στα άρθρα 8,9 και 11 του Σχεδίου Άρθρων σχετικά με την Ευθύνη των Κρατών για Διεθνείς Παραβατικές Πράξεις (Draft Articles on Responsibility of States for Internationally Wrongful Acts), τα οποία έχουν ως εξής: 8 The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct 9 The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority 11 Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

Δεύτερη κατευθυντήρια γραμμή είναι η τήρηση της αρχής της αναλογικότητας (principle of proportionality). Σύμφωνα με αυτή, η βίαιη απάντηση του αμυνόμενου σε περίπτωση άσκησης του δικαιώματος της αυτοάμυνας θα πρέπει να εξαντλείται στην απόκρουση της «ένοπλης επίθεσης», ενώ θα πρέπει να έχει ίδια κλίμακα με την επίθεση. (Nicaragua, 1986 I.C.J. at 94.)

Τρίτη κατευθυντήρια γραμμή είναι η τήρηση της αρχής της αμεσότητας (principle of immediacy), σύμφωνα με την οποία το αμυνόμενο κράτος θα πρέπει να προβεί σε αυτοάμυνα εντός εύλογου χρονικού διαστήματος από το χρόνο της «ένοπλης επίθεσης». Δεν υπάρχει σταθερός ορισμός του όρου «εύλογο χρονικό διάστημα», καθώς αυτό εξαρτάται από τις δυνατότητες αυτοάμυνας και τις επιχειρησιακές ανάγκες του κράτους-στόχου, οπότε μπορούμε να «δανειστούμε» τον όρο «παράθυρο αντεπίθεσης» (counterattack window) από τη στρατιωτική ακαδημαϊκή παραγωγή. Σύμφωνα με τον όρο αυτό, μετά το πέρας ή και κατά τη διάρκεια της επίθεσης του κράτους-επιτιθέμενου, ο αμυνόμενος αποκτά τη δυνατότητα διενέργειας αντεπίθεσης (άνοιγμα του παραθύρου) με την πρώτη ευκαιρία, δυνατότητα η οποία εκλείπει όταν οι συνθήκες δεν είναι πρόσφορες χρονικά ή υλικά (κλείσιμο του

παραθύρου). Στην προκειμένη περίπτωση, το «παράθυρο» κλείνει μετά την πάροδο χρονικού διαστήματος το οποίο είναι αναντίστοιχο με τις δυνατότητες αυτοάμυνας και τις επιχειρησιακές ανάγκες του αμυνόμενου, δηλαδή μετά τη μη διενέργεια αντεπίθεσης, ενώ έχει επιτευχθεί η επιχειρησιακή ετοιμότητα (operational readiness).

Β.4 Νομιμότητα κυβερνοπολέμου ως μέσου επίθεσης-αντεπίθεσης

Ο κυβερνοπόλεμος είναι ιδιαίτερα σχετικός με την κοινωνία της πληροφορίας, ένας όρος που αναφέρεται σε κοινωνίες όπου η δημιουργία, διανομή, χρήση, ενσωμάτωση και χειραγώγηση πληροφοριών είναι μια σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Σε μια κοινωνία της πληροφορίας, η λειτουργία των υποδομών ζωτικής σημασίας, η οικονομία, οι κρατικές υπηρεσίες και η καθημερινή ζωή των πολιτών εξαρτώνται σε μεγάλο βαθμό από ψηφιακά συστήματα και δίκτυα. Ως αποτέλεσμα, ο κυβερνοπόλεμος μπορεί να έχει εκτεταμένες επιπτώσεις, διακόπτοντας βασικές υπηρεσίες και διαδίδοντας παραπληροφόρηση. Στο πλαίσιο της κοινωνίας της πληροφορίας, ο κυβερνοπόλεμος αναλαμβάνει έναν ιδιαίτερα κρίσιμο ρόλο λόγω της διάχυτης ενσωμάτωσης των ψηφιακών τεχνολογιών σχεδόν σε κάθε πτυχή της κοινωνικής λειτουργίας. Μια κοινωνία της πληροφορίας χαρακτηρίζεται από την κυριαρχία των δραστηριοτήτων που σχετίζονται με την πληροφόρηση στην οικονομική, πολιτική και πολιτιστική σφαίρα της. Αυτή η κοινωνική δομή εξαρτάται σε μεγάλο βαθμό από τη δημιουργία, τη διανομή και τη χρήση πληροφοριών, η οποία διευκολύνεται κατά κύριο λόγο μέσω ψηφιακών μέσων.

Σε τέτοιες κοινωνίες, τομείς ζωτικής σημασίας υποδομών, όπως η υγειονομική περίθαλψη, οι μεταφορές, η ενέργεια και τα οικονομικά, εξαρτώνται όλο και περισσότερο από ψηφιακά συστήματα και δίκτυα. Αυτή η εξάρτηση εκτείνεται πέρα από τις υποδομές για να συμπεριλάβει τις κυβερνητικές λειτουργίες, όπου οι ψηφιακές πλατφόρμες χρησιμοποιούνται για τα πάντα, από τη διαχείριση δημόσιων υπηρεσιών έως τη διεξαγωγή εκλογών. Η οικονομία είναι επίσης βαθιά συνυφασμένη με την ψηφιακή τεχνολογία, με το ηλεκτρονικό εμπόριο, τις ηλεκτρονικές τραπεζικές συναλλαγές και τις ψηφιακές αγορές να διαδραματίζουν κεντρικούς ρόλους. Επιπλέον, η καθημερινή ζωή των πολιτών είναι σε μεγάλο βαθμό ψηφιοποιημένη, από τις κοινωνικές αλληλεπιδράσεις και την ψυχαγωγία έως την εκπαίδευση και τη διαχείριση προσωπικών δεδομένων.

Δεδομένης αυτής της εκτεταμένης εξάρτησης από τα ψηφιακά συστήματα, ο κυβερνοπόλεμος εγκυμονεί σημαντικούς κινδύνους. Οι επιθέσεις στον κυβερνοχώρο που στοχεύουν κρίσιμες υποδομές μπορεί να οδηγήσουν σε εκτεταμένη διακοπή, όπως διακοπές ρεύματος ή σε κίνδυνο συστήματα παροχής νερού. Οι επιθέσεις στα χρηματοπιστωτικά συστήματα μπορούν να αποσταθεροποιήσουν τις οικονομίες, ενώ οι παραβιάσεις στα κυβερνητικά δίκτυα μπορούν να υπονομεύσουν την εθνική ασφάλεια και την εμπιστοσύνη του κοινού. Επιπλέον, η διάδοση παραπληροφόρησης μέσω ψηφιακών

καναλιών μπορεί να χειραγωγήσει την κοινή γνώμη, να επηρεάσει τις εκλογές και να προκαλέσει κοινωνική αναταραχή.

Η διάχυτη χρήση της τεχνολογίας στις κοινωνίες της πληροφορίας αυξάνει επίσης την πιθανή κλίμακα και τον αντίκτυπο του κυβερνοπολέμου. Σε αντίθεση με τον παραδοσιακό πόλεμο, όπου οι επιπτώσεις είναι συχνά γεωγραφικά περιορισμένες, ο κυβερνοπόλεμος μπορεί να έχει άμεσες και εκτεταμένες συνέπειες πέρα από τα εθνικά σύνορα. Για παράδειγμα, μια κυβερνοεπίθεση σε μια χώρα μπορεί γρήγορα να κυματίσει τα παγκόσμια δίκτυα, επηρεάζοντας το διεθνές εμπόριο, τις παγκόσμιες χρηματοπιστωτικές αγορές και τις διεθνείς σχέσεις.

Επιπλέον, η ανωνυμία και τα χαμηλά εμπόδια εισόδου που συνδέονται με τον κυβερνοπόλεμο τον καθιστούν ένα ιδιαίτερα ελκυστικό εργαλείο για κρατικούς και μη κρατικούς φορείς. Οι κυβερνοεπιθέσεις μπορούν να εξαπολυθούν εξ αποστάσεως και διακριτικά, καθιστώντας δύσκολη την αναγνώριση των δραστών και την αποτελεσματική απόκριση.

Ο κυβερνοπόλεμος (γνωστός και ως πληροφοριακός) εκτυλίσσεται με διαδικτυακά μέσα, με διάφορους τρόπους και πρακτικές, ενώ μπορεί να έχει πολλές δυσμενείς συνέπειες για τη λειτουργία του θύματος/κράτους ή διαφόρων εγκαταστάσεών του. (Finkelstein et al., 2015) Πιο συγκεκριμένα, λαμβάνει χώρα μέσα σε έναν αχανή και χωρίς όρια κυβερνοχώρο, με πολλές προεκτάσεις και συνέπειες. Έτσι, στη σημερινή εποχή ανακύπτουν μία σειρά από συζητήσεις και αναφορές γύρω από το θέμα αυτό, όπου εμπλέκονται κράτη, οργανισμοί, απλοί πολίτες και επιχειρήσεις. (Lieberthal & Singer, 2011) Θεωρείται - και όχι τυχαία άλλωστε - ότι αποτελεί μία από τις πιο ύπουλες μορφές σύγκρουσης της σημερινής εποχής. Πιο αναλυτικά, συνήθως η διαδικασία εκδήλωσης ενός τέτοιου σύγχρονου πολέμου εκδηλώνεται με καλά οργανωμένες επιθέσεις και ανάλογες στρατηγικές στο διαδίκτυο, απέναντι στον εχθρό, με σκοπό να πλήξει και να καταστρέψει υποδομές, φορείς και οργανισμούς στρατηγικής σημασίας της απέναντι πλευράς. (Singer et al., 2014)

Η κυβερνοεπίθεση είναι μία μέθοδος που διεξάγεται ο νέος πληροφοριακός πόλεμος. Στον κυβερνοχώρο μπορούν να λάβουν μέρος διάφορες ενέργειες, εκτός από τις απλές συνδιαλλαγές, επικοινωνίες μεταξύ προσώπων, όπως συγκρούσεις ή, αλλιώς, κυβερνοσυγκρούσεις, και επιθέσεις. Όπως χαρακτηριστικά αναφέρει ο Libicki (2009), οι κυβερνοεπιθέσεις σχετίζονται με τη σύγκρουση ή την αντιπαράθεση που μπορεί να προκύψει μεταξύ δύο ή περισσότερο πλευρών, με παράλληλα άσκηση κυβερνοεπίθεσης της μιας απέναντι στην άλλη ή στις άλλες.

Πρόκειται, πλέον, για έναν ασύμμετρο πόλεμο, που χρησιμοποιεί ακανόνιστες μεθόδους και παράτυπα στοιχεία, με σκοπό την αποσταθεροποίηση κυβερνήσεων, οργανισμών και κρατών με στόχο διάφορα οφέλη κάθε φορά. (Berlund & Souleimanov, 2019) Για παράδειγμα, στο Κόσοβο, το 1999, στον πόλεμο, hackers από τη Σερβία, με τη βοήθεια συμμάχων τους από άλλα κράτη, όπως ανατολικοευραπαϊκών κρατών, οργάνωσαν κυβερνοεπίθεση στα υπολογιστικά συστήματα σε κράτη

μέλη του ΝΑΤΟ. Σε αυτή την περίπτωση, όπως αναφέρει ο Thornton (2007), αν και οι επιτιθέμενοι γνώριζαν ότι δεν θα μπορούσαν να υπερισχύσουν έναντι του αντιπάλου, ωστόσο προχώρησαν με αυτή την επιλογή για να προκαλέσουν μεγάλη αναστάτωση, χάος και αναδιοργάνωση, έτσι ώστε να αναδειχθούν οι αδυναμίες πιθανώς του ΝΑΤΟ σε τέτοιες ανταποκρίσεις. (Thornton, 2007)

Σήμερα, επίσης, γίνεται πολύς λόγος για τον λεγόμενο πληροφοριακό πόλεμο, που γίνεται όλο και περισσότερο ευρέως γνωστός, ενώ τα ψηφιακά όπλα αναπτύσσονται όλο και περισσότερο. (Schackelford, 2013) Υπάρχουν διάφορες τέτοιες συγκρούσεις, που λαμβάνουν χώρο στο διαδίκτυο, όπως οι κυβερνοσυγκρούσεις, όπως αυτές πλέον είναι γνωστές, οι οποίες μπορεί να διαρκέσουν από λίγες ώρες μέχρι και κάποια χρόνια, ανάλογα με το σκοπό τους, τον εχθρό τους, αλλά και τις επιδιώξεις των διοργανωτών. Οι συνέπειες που μπορεί να επιφέρουν μπορεί να σχετίζονται με μία μεγάλη γκάμα από ενέργειες, όπως είναι οι τρομοκρατικές, αλλά μπορούν να πλήξουν και διάφορα συστήματα μιας χώρας, όπως ασύρματα και δορυφορικά δίκτυα, επικοινωνίες, κυκλοφορία οχημάτων, αεροπλάνων, τραπεζικά δίκτυα, εργοστάσια πυρηνικής ενέργειας, αγωγούς κοιτασμάτων και πολλά άλλα. (Charney, 2009).

Παρόλο που ο κυβερνοπόλεμος αποτελεί μια σχετικά νέα εξέλιξη της φιλοσοφίας διεξαγωγής πολεμικών επιχειρήσεων, η πλειονότητα των επιστημόνων του δικαίου συμφωνούν ότι δεν απαιτείται στροφή στο δίκαιο του πολέμου και ότι η υπάρχουσα νομοθεσία είναι ικανή να τον καλύψει. Η σκέψη αυτή πηγάζει από τη Ρήτρα Μάρτινς (Martens Clause), η οποία έλαβε το όνομά της από τον Φρίντριχ Μάρτινς (Friedrich Martens), διπλωματικό εκπρόσωπο της Ρωσίας κατά την Ειρηνευτική Διάσκεψη της Χάγης το 1899. Το κείμενό της, το οποίο αποτελεί ένα από τα πρώτα δείγματα διεθνούς δικαίου, ενσωματώθηκε στο προοίμιο της Συνθήκης της Χάγης του 1899 και έκτοτε στη Συνθήκη της Χάγης του 1907 και στα πρόσθετα Πρωτόκολλα της Συνθήκης της Γενεύης (1949), έχει ως εξής: Μέχρις ότου εκδοθεί ένας πληρέστερος κώδικας των νόμων του πολέμου, τα Υψηλά Συμβαλλόμενα Μέρη θεωρούν σκόπιμο να δηλώσουν ότι, στις περιπτώσεις που δεν περιλαμβάνονται στους κανονισμούς που υιοθετήθηκαν από αυτά, οι κάτοικοι και οι εμπόλεμοι παραμένουν υπό την προστασία και τον κανόνα των αρχών του δικαίου των εθνών, όπως αυτές απορρέουν από τις συνήθειες που έχουν καθιερωθεί μεταξύ των πολιτισμένων λαών, από τους νόμους της ανθρωπότητας και τις επιταγές της δημόσιας συνείδησης. Μια τέτοια ρήτρα διασφαλίζει ότι η Συνθήκη δε θα βρίσκεται ποτέ «εκτός εποχής», αφήνοντας περιθώριο ρύθμισης καταστάσεων από τα συμβαλλόμενα μέλη της και αποφεύγοντας νομικά κενά τα οποία θα μπορούσαν να επηρεάσουν αρνητικά τα διεθνή όργανα που περιστρέφονται γύρω από το δίκαιο του πολέμου, όπως το Διεθνές Ποινικό Δικαστήριο (International Criminal Court). Η ερμηνεία που έχει δοθεί από τη νομολογία του Διεθνούς Δικαστηρίου (ICJ,1996, παρ. 78) ενισχύει το περιεχόμενο της Ρήτρας, καθώς αυτή κρίθηκε ως «ένα αποτελεσματικός τρόπος συμβάδισης με την εξελισσόμενη στρατιωτική τεχνολογία (Meron, 2000,σ.87). Τα ανωτέρω, σε συνδυασμό με το γεγονός ότι ο κυβερνοχώρος είναι άρρηκτα συνδεδεμένος με τον «πραγματικό κόσμο», καθώς οι παράγοντες που τον διεξάγουν (actors)

προβαίνουν σε φυσικές ενέργειες με επενέργεια στον κυβερνοχώρο, ενώ ήδη έχει αποκρυσταλλωθεί η «σύνδεση» των ενεργειών των παραγόντων και τις μεταβολές που αυτές επιφέρουν στον κυβερνοχώρο μέσω των νομικών διεργασιών γύρω από το Διαδίκτυο, κυρίως της νομοθεσίας περί ανταγωνισμού μεταξύ των παρόχων, περί ηλεκτρονικών πληρωμών και περί ηλεκτρονικού εμπορίου, οι οποίες δεν κάνουν καμία απολύτως διάκριση μεταξύ «πραγματικού κόσμου» και κυβερνοχώρου.

Η Ε.Ε., μέσα από τις σχετικές επιθέσεις, συγκρούσεις και απειλές, έχει δημιουργήσει ένα πλαίσιο για να μειώσει ή και να εξαλείψει τέτοιου είδους ενέργειες, για να προστατέψει όσο είναι δυνατόν τα κράτη και τους πολίτες τους. (Council of Europe, 2001) Αρχικά, το θέμα που απασχολεί την ΕΕ είναι η ασφάλεια στο χώρο του Διαδικτύου, κάτι που προχώρησε με τη σχετική Οδηγία NIS 2, που προτάθηκε 3 χρόνια πριν (δηλαδή, το Δεκέμβριου του 2020), ώστε να αντιμετωπίσουν καλύτερα θέματα κυβερνοεπιθέσεων, με ανάλογες ρήτρες. Πρέπει να τονιστεί ότι η συγκεκριμένη Οδηγία αποτελεί την πρώτη πράξη, σε νομικό πλαίσιο, που διευθετήθηκε από την ΕΕ για την ασφάλεια στον κυβερνοχώρο. (IN.gr., 2023)

Οι Κυβερνοεπιθέσεις διεξάγονται για την επίτευξη κάποιου συγκεκριμένου σκοπού. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικώς όμως ανήκει σε μία από τις παρακάτω κατηγορίες: α) Εκμετάλλευση (exploitation) Στην περίπτωση της εκμετάλλευσης βασικός στόχος του δράστη είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών που είναι συνδεδεμένες με αυτόν. β) Παραπλάνηση (deception) Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις πληροφορίες τις οποίες αυτός συλλέγει, αναλύει ή παράγει, στοχεύοντας ουσιαστικά στο σύστημα λήψης αποφάσεων του αντιπάλου. γ) Καταστροφή (destruction) Στην περίπτωση της καταστροφής ο επιτιθέμενος, μέσω της χρήσης πληροφοριακών συστημάτων, καθιστά αδύνατη τη λειτουργία του στόχου, καταστρέφοντας τον ίδιο ή τα συστήματα υποστήριξης που είναι απαραίτητα για τη λειτουργία του. Στην περίπτωση αυτή πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου, αλλά η κρίσιμη υποδομή του

Ο κυβερνοπόλεμος είναι ιδιαίτερα σχετικός με την κοινωνία της πληροφορίας, ένας όρος που αναφέρεται σε κοινωνίες όπου η δημιουργία, διανομή, χρήση, ενσωμάτωση και χειραγώγηση πληροφοριών είναι μια σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Σε μια κοινωνία της πληροφορίας, η λειτουργία των υποδομών ζωτικής σημασίας, η οικονομία, οι κρατικές υπηρεσίες και η καθημερινή ζωή των πολιτών εξαρτώνται σε μεγάλο βαθμό από ψηφιακά συστήματα και δίκτυα.

Η διάχυτη χρήση της τεχνολογίας στις κοινωνίες της πληροφορίας αυξάνει επίσης την πιθανή κλίμακα και τον αντίκτυπο του κυβερνοπολέμου. Σε αντίθεση με τον παραδοσιακό πόλεμο, όπου οι επιπτώσεις είναι συχνά γεωγραφικά περιορισμένες, ο κυβερνοπόλεμος μπορεί να έχει άμεσες και εκτεταμένες συνέπειες πέρα από τα εθνικά σύνορα. Για παράδειγμα, μια κυβερνοεπίθεση σε μια χώρα μπορεί γρήγορα να κυματίσει τα παγκόσμια δίκτυα, επηρεάζοντας το διεθνές εμπόριο, τις παγκόσμιες χρηματοπιστωτικές αγορές και τις διεθνείς σχέσεις.

Υπάρχουν διάφορες τέτοιες συγκρούσεις, που λαμβάνουν χώρο στο διαδίκτυο, όπως οι κυβερνοσυγκρούσεις, όπως αυτές πλέον είναι γνωστές, οι οποίες μπορεί να διαρκέσουν από λίγες ώρες μέχρι και κάποια χρόνια, ανάλογα με το σκοπό τους, τον εχθρό τους, αλλά και τις επιδιώξεις των διοργανωτών. Οι συνέπειες που μπορεί να επιφέρουν μπορεί να σχετίζονται με μία μεγάλη γκάμα από ενέργειες, όπως είναι οι τρομοκρατικές, αλλά μπορούν να πλήξουν και διάφορα συστήματα μιας χώρας, όπως ασύρματα και δορυφορικά δίκτυα, επικοινωνίες, κυκλοφορία οχημάτων, αεροπλάνων, τραπεζικά δίκτυα, εργοστάσια πυρηνικής ενέργειας, αγωγούς κοιτασμάτων και πολλά άλλα. (Charney, 2009).

Β.5 Κατάταξη επίθεσης στην κατηγορία του κυβερνοπολέμου

Η ταξινόμηση των επιθέσεων στον κυβερνοπόλεμο παρέχει ένα πλαίσιο για την κατανόηση του ποικίλου και πολύπλοκου τοπίου των απειλών στον κυβερνοχώρο. Η αναγνώριση του είδους και της φύσης αυτών των επιθέσεων είναι το πρώτο βήμα για την ανάπτυξη ισχυρών μέτρων ασφαλείας και τη διασφάλιση της ανθεκτικότητας των ψηφιακών υποδομών έναντι των απειλών στον κυβερνοχώρο.

Στην ψηφιακή εποχή, η κατανόηση της φύσης και του είδους των απειλών στον κυβερνοχώρο είναι ζωτικής σημασίας για την εφαρμογή αποτελεσματικών μέτρων κυβερνοασφάλειας. Η ταξινόμηση αυτών των επιθέσεων βασίζεται σε διάφορους παράγοντες όπως η πρόθεση του εισβολέα, οι μέθοδοι που χρησιμοποιούνται, η κλίμακα του αντίκτυπου και η ευπάθεια του στόχου. Με την κατηγοριοποίηση των επιθέσεων στον κυβερνοχώρο, οι οργανισμοί και τα άτομα μπορούν να κατανοήσουν καλύτερα τις πιθανές απειλές τους και να προσαρμόσουν ανάλογα τις αμυντικές στρατηγικές τους.

Οι επιθέσεις στον κυβερνοχώρο έχουν εξελιχθεί σημαντικά, γίνονται πιο εξελιγμένες και ποικίλες. Η ταξινόμηση αυτών των επιθέσεων βοηθά στην κατανόηση της φύσης, του σκοπού και των μεθόδων που χρησιμοποιούνται, κάτι που είναι απαραίτητο για την ανάπτυξη αποτελεσματικών πρωτοκόλλων ασφαλείας και στρατηγικών απόκρισης.

Ήδη απο τα τέλη της δεκατίας 1990 προτείνονται επτά κριτήρια κατάταξης και αξιολόγησης μίας κατάστασης ως κυβερνοπόλεμος (Michael Schmitt). Τα κριτήρια αυτά είναι:

- Η δριμύτητα /σφοδρότητα (severity) της επίθεσης.
- Χρονική αμεσότητα (immediacy) μεταξύ της επίθεσης και των αποτελεσμάτων.
- Αιτιακή αμεσότητα (directness)μεταξύ επίθεσης και αποτελεσμάτων.
- Διεισδυτικότητα της επίθεσης (invasiveness), για τις ηλεκτρονικές άμυνες του κράτους–στόχου.
- Μετρησιμότητα’ (measurability)των ποσοτικών αποτελεσμάτων της επίθεσης.
- Έλλειψη κατ’ αρχήν νομιμότητας (ή έστω νομιμοφάνειας) (presumptive legitimacy) της επίθεσης.
- Κρατική ευθύνη (responsibility) για την επίθεση.

Οι Jarno και Rid θεωρούν οτι “ο κυβερνοπόλεμος είναι ένα μέρος της εξέλιξης του συμβατικού πολέμου, ο οποίος είναι άρρηκτα συνδεδεμένος με ευρύτερες κοινωνικές και πολιτικές αλλαγές.” Έτσι,

δεν είναι πλέον εύκολο να φανταστεί κανείς κάποια σύρραξη η οποία δεν θα περιλαμβάνει κάποιο στοιχείο κυβερνοδραστηριότητας όπως η παρακολούθηση ή το σαμποτάζ. “Το να αναρωτιόματε εαν ο κυβερνοπόλεμος είναι αληθινός είναι λιγότερο σημαντικό από το να συγκεντρωνόμαστε στο πώς θα ανασχεθούν οι απειλές που προκύπτουν από τη χρήση της τεχνολογίας υπολογιστών. Άλλωστε, η κυβερνοεπίθεση δεν είναι απαραίτητο να σκοτώσει κάποιον ή να προξενήσει μεγάλη υλική ζημιά για να θεωρηθεί επικίνδυνη.” Ο Αντισμήναρχος της Πολεμικής Αεροπορίας των Η.Π.Α. Gregory J. Rattray στο βιβλίο του “Strategic Warfare in Cyberspace” ορίζει τον κυβερνοπόλεμο ως “στρατιωτικές επιχειρήσεις στον κυβερνοχώρο με σκοπό την επίθεση εναντίον του εχθρού και την προστασία των φίλιων κέντρων βάρους.” Εναλλακτικοί ορισμοί αναφέρουν οτι ο κυβερνοπόλεμος είναι “κάθε ενέργεια που λαμβάνει χώρα στον κυβερνοχώρο και στοχεύει κατά της ισχύος μιάς χώρας ή κατά ενός μη κρατικού δρώντα (πρόσωπα, οργανισμούς, εταιρείες κλπ).” Ο πρώην σύμβουλος ασφαλείας του Λευκού Οίκου, Richard Clarke, αναφέρει οτι “Ο κυβερνοπόλεμος είναι η καταστροφή, η αναστάτωση ή η πρόκληση ζημιάς σε συστήματα του πραγματικού κόσμου μέσω των επιθέσεων με συστήματα υπολογιστών, κάτι που συμβαίνει μόνο κατά τη διάρκεια κάποιου πολέμου ή, υποθέτω, κάποιας μυστικής δράσης. Άρα, πρόκειται να συμβεί όταν κράτη θα πάνε σε πόλεμο μεταξύ τους.” Ο Jonathan Kirshner θεωρεί οτι ο κυβερνοπόλεμος είναι αναπόσπαστο τμήμα της παγκοσμιοποίησης και οτι αποτελεί μια νέα στρατηγική απειλή.

Πριν διαχωριστούν οι τρεις αυτές φαινομενικά παρόμοιες αλλά ουσιαστικά πολύ διαφορετικές έννοιες, πρέπει να ξεκαθαριστεί ο όρος κυβερνοαπειλή.

Σύμφωνα λοιπόν με την Susan Brenner, “Κυβερνοαπειλή (cyberthreat) γενικά είναι η χρήση της τεχνολογίας των υπολογιστών με σκοπό την εμπλοκή τους σε δραστηριότητες οι οποίες υποδαυλίζουν την ικανότητα της κοινωνίας να διατηρήσει την εσωτερική και την εξωτερική τάξη.

“Ο κυβερνοπόλεμος δεν είναι απλά ένα νέο σύνολο από επιχειρησιακές τεχνικές. Είναι ένας αναδυόμενος, νέος τρόπος πολέμου που θα απαιτήσει νέες προσεγγίσεις για τη σχεδίαση και τη δημιουργία πλάνων αντιμετώπισης καθώς και νέες μορφές δογμάτων και οργάνωσης.”Ο Jeffrey M. Bale, ερευνητής και αναπληρωτής καθηγητής στο Monterey Terrorism Research and Education Program αναφέρει τις δυσχέρειες που υπάρχουν λόγω των επικαλυπτόμενων όρων που χρησιμοποιούνται σε διάφοροες προσπάθειες να δοθεί ορισμός στην έννοια του κυβερνοπολέμου. Συχνά η κυβερνοτρομοκρατία, το κυβερνοσαμποτάζ και ο κυβερνοπόλεμος συγχέονται σε επίπεδο ορισμού ενώ δεν αποτελούν ταυτόσημες έννοιες.

Σε αυτό το πλαίσιο θα προσπαθήσουμε να προχωρήσουμε στην κατάταξη μίας επίθεσης στην έννοια του κυβερνοπολέμου.

Κριτήριο: Κλίμακα μορφών

Απλές μορφές κυβερνοπολέμου

Επιθέσεις για την προσωρινή διακοπή λειτουργίας ηλεκτρονικών υπηρεσιών όπως κρατικές ιστοσελίδες, για παράδειγμα υπουργεία, εκπαιδευτικά ιδρύματα και δίαφοροι άλλοι φορείς.

Επιθέσεις σε υπηρεσίες ηλέκτρονικών ταχυδρομείων, υπηρεσίες νέφους κλπ καθώς και αλλοίωση υπηρεσιών όπως ιστοσελίδες (συνήθως εμφανίζουν κάποιο μήνυμα που θέλουν να περάσουν).

Οι απλές μορφές κυβερνοπολέμου γίνονται συνήθως για εντυπωσιασμούς χωρίς αυτό να σημαίνει ότι δεν επηρεάζεται η ζωή των πολιτών. Για παράδειγμα μια επίθεση σε μια υπηρεσία ενός υπουργείου σταματάει τους πολίτες απο το να μπορούν να πραγματοποιούν κάποιες ενέργειες όπως: να τυπώσουν τα έγγραφα τους, να πληρώσουν τις υποχρεώσεις τους. Μια επίθεση σε ένα εκπαιδευτικό ίδρυμα σταματά την διεξαγώγη των μαθημάτων. Οι επιθέσεις αυτές είναι χαμηλής ισχύος, αλλά προκαλούν ζημία και ταλαιπωρία στους πολίτες διότι δεν λειτουργούν δίαφορες υπηρεσίες.

Διαρκούν συνήθως μικρό χρονικό διάστημα και η αποκατάσταση του συστήματος γίνεται σε γρήγορο χρονικό διάστημα.

Οι επιθέσεις σε υπηρεσίες ηλεκτρονικών ταχυδρομείων και όχι η είσοδος σε αυτά και η υποκλοπή, έχουν ώς αποτέλεσμα την πάυση της ανταλλαγής των συνομιλιών.

Οι επιθέσεις σε υπηρεσίες νέφους ως αποτέλεσμα την πάυση αποστολής και λήψης εγγράφων. Οι επιθέσεις αυτές μπορούν να προκαλέσουν χάος σε μια χώρα αλλά δεν είναι ζωτικής σημασίας.

Μορφές κυβερνοπολέμου ζωτικής σημασίας

Επίθεσεις σε εργοστάσια ηλεκτρισμού. Δεν χρειάζεται φυσική πρόσβαση και οι επιθέσεις μπορούν να γίνουν εξ αποστάσεως.

Επιθέσεις σε υποδομές ύδρευσης και τροφίμων. Μερικές απο αυτές τις επιθέσεις μπορούν να πραγμοτοποιηθούν εξ αποαστάσεως και μερικές άλλες απαιτούν φυσική παρουσία.

Επιθέσεις σε στρατιωτικές εγκαταστάσεις. Χημικά, πυρηνικά όπλα, οπλικά συστήματα. Απαιτείται αποκλειστικα φυσική παρουσία διότι οι υπηρεσίες αυτές είναι αποσυνδεδεμένες απο το διαδίκτυο και βρίσκονται σε άλλες μορφές δικτύων.

Επίθεσεις σε εργοστάσια όπως ηλεκτρισμού. Παρα πολλοί άνθρωποι με προβλήματα υγείας σε υποδομές όπως νοσοκομεία κλινικές κλπ η ακόμη και σε σπίτια ζούν με την υποστήρικη μηχανημάτων. Μια επίθεση μεγάλης χρονικής διάρκειας σε αυτό το κομμάτι επιφέρει θανάτους εκτός του οτι δεν λειτουργεί σχεδόν τίποτα. Προχωρώντας και πιο βαθιά στις επιθέσεις σε σταθμούς ηλεκτρισμού οι επιτιθέμενοι μπορούν μέσω των λογισμικών να αλλάξουν διάφορες τιμές του ρέυματος σε σχέση με την τάση και την ισχύ που μπορού να επιφέρουν θανάτους αλλά και καταστροφές μηχανημάτων.

Επιθέσεις σε υποδομές ύδρευσης και τροφίμων. Οι επιθέσεις σε υποδομές ύδρευσης επιφέρουν επίσης απώλεια ζωής απο τη έλειψη νερού αν αυτή είναι κάποιας σημαντικής χρονικής διάρκειας. Σε αυτή την περίπτωση οι επιτιθέμενοι θα μπορούσαν μέσα απο την αλλαγή διαφόρων τιμών η μέσα απο της ανάμοιξη διαφόρων ουσιών να δηλητηριάσουν το νερό η και τα τρόφιμα που θα κυκλοφορήσουν στην αγορά με θανατηφόρες συνέπειες.

Κριτήριο: Σκοπός επίθεσης

Μέσω μιας κυβερνοεπίθεσης, είθισται να επιδιώκεται εναλλακτικά α) η διακοπή της λειτουργίας του συστήματος (επίθεση σε υποδομές π.χ. δίκτυο διανομής ηλεκτροδότησης) β) ο αποκλεισμός χρηστών

από την πρόσβαση σ' ένα σύστημα (π.χ. απαγόρευση χρήσης υπηρεσιών) γ) η κυβερνοκατασκοπεία (συλλογή απόρρητων πληροφοριών) και δ) η αλλοίωση των δεδομένων που διακινούνται σ' ένα σύστημα (λ.χ. καταστροφή ή μεταβολή περιεχομένου ιστοσελίδων). Οι στόχοι αυτοί δύναται να περιλαμβάνουν τις εχθρικές τηλεπικοινωνίες, το δίκτυο ύδρευσης, τα χρηματοπιστωτικά ιδρύματα, τις μεταφορές, τις τραπεζοασφαλιστικές και ταχυδρομικές υπηρεσίες και, τέλος, τις στρατιωτικές εγκαταστάσεις. Το πλεονέκτημα του Κυβερνοπολέμου έγκειται στο γεγονός ότι η επίθεση σχεδόν ανέξοδα, χωρίς την εμπλοκή συμβατικών μέσων κρούσης (αεροσκάφη, πυραύλους κτλ), μπορεί δε να επιφέρει σχεδόν ίδιας σημασίας πλήγματα σε εγκαταστάσεις ζωτικής σημασίας, και να οδηγήσει στην κατάρρευση του αντίπαλου κράτους. Επίσης, μπορεί να προλειάνει το έδαφος για μια δεύτερη επίθεση με συμβατικά όπλα. Η «μη γραμμικότητα» της επίθεσης, μπορεί να προκαλέσει χάος, αποσυντονισμό των υπηρεσιών του κράτους και καταβαράθρωση του ηθικού του λαού.

Οι κυβερνοεπιχειρήσεις χρησιμοποιούνται για να επιτεθούν, εξαπατήσουν, υποβαθμίσουν, διασπάσουν, εμποδίσουν, εκμεταλλευτούν και να υπερασπιστούν ηλεκτρονικές πληροφορίες και υποδομές ή γενικότερα οποιοσδήποτε διαδικτυακή εισβολή ή άμυνα. Ωστόσο πιο συχνά ακούμε τον όρο κυβερνοεπίθεση ο οποίος δεν αντανακλά απαραίτητα όλες τις επιχειρήσεις του κυβερνοχώρου. Η διμερής συμφωνία για ζητήματα κυβερνοασφάλειας που υπεγράφη ανάμεσα σε ΗΠΑ και Ρωσία το 2014 είναι ένα παράδειγμα διακρατικής συμφωνίας που κατηγοριοποιεί και ορίζει τις επιχειρήσεις του κυβερνοχώρου. Ως κυβερνοεπίθεση ορίζεται η επιθετική χρήση ενός κυβερνοόπλου που προορίζεται να βλάψει έναν καθορισμένο στόχο. Όσες διεξάγονται από κρατική ή άλλη οργάνωση χρησιμοποιώντας τα πληροφοριακά δίκτυα για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες ή εμπιστευτικές πληροφορίες με κρυφά μέσα συνιστούν κυβερνοκατασκοπεία. Επιμέρους κατηγορίες των κυβερνοεπιχειρήσεων είναι η κυβερνοεπίθεση, το κυβερνοέγκλημα και η κυβερνο-κατασκοπεία. Είδη μηχανισμών των κυβερνοεπιχειρήσεων συνιστούν το κακόβουλο λογισμικό, η μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση και η άρνηση εξυπηρέτησης στο νόμιμο χρήστη (Denial of Service attack). Στο σημείο αυτό όμως αυτό χρειάζεται να αναρωτηθούμε αν είμαστε σε θέση να αποκρυπτογραφήσουμε την πρόθεση μιας κυβερνοεπιχείρησης δηλαδή ενός κώδικα προγραμματισμού.

Πιστεύεται ότι στόχος μιας επιχείρησης στον κυβερνοχώρο μπορεί να είναι αβλαβής ή επιβλαβής ενώ ο σκοπός του κυβερνοπολέμου είναι πάντα να προκαλέσει ζημιά στον στόχο του. Μπορούν να διακριθούν τρεις κυρίως τύποι κυβερνοεπιχειρήσεων: α) Εκμετάλλευσης Δικτύων Υπολογιστών (CNE = Computer Network Exploitations). Είναι λειτουργίες που διεισδύουν στο εσωτερικό δίκτυο για να κλέψουν πληροφορίες ιδανικά χωρίς να αφήσουν ίχνη. β) Επιθέσεις Δικτύου Υπολογιστών (CNA = Computer Network Attack). Είναι επιθέσεις σε συστήματα για διακοπή, ζημιά ή ακόμη και καταστροφή αυτών, συμπεριλαμβανομένων και των αποθηκευμένων πληροφοριών τους. Οι CNA ενέχουν τον μεγαλύτερο κίνδυνο , ιδίως όταν στρέφονται κατά υποδομών ζωτικής σημασίας, και γ) Επιχειρήσεις Πληροφορίας (IO = Information Operations). Αυτές εξαπολύονται από ένα κράτος προκειμένου να

επηρεάσουν τις απόψεις της κοινής γνώμης σε ένα άλλο κράτος υπέρ των δικών τους προθέσεων. (Dahinden M. 2021).

Εάν λάβουμε υπόψη και την συχνά συνεργατική σύμπραξη μεταξύ κάποιων από τις παραπάνω κατηγορίες με κίνητρο το πρόσκαιρα κοινό όφελος, εύκολα αντιλαμβανόμαστε την πολυπλοκότητα της εξεύρεσης της ενδεχόμενης απόφασης για λήψη μέτρων τόσο για την πρόληψη όσο και για την αντιμετώπιση του φαινομένου. Χαρακτηριστικό παράδειγμα συνεργατικής δράσης με κοινό παρονομαστή το οικονομικό συμφέρον ως κίνητρο παράλληλης δράσης δύο κατηγοριών με φαινομενικά διαφορετική αφετηρία είναι η ναρκοτρομοκρατία (narcoterrorism). Εδώ, ο αντικειμενικός σκοπός των κυκλωμάτων εμπορίας ναρκωτικών (η ασφαλής μεταφορά των ναρκωτικών από το χώρο παραγωγής/επεξεργασίας τους στους τόπους αρχικής διάθεσής τους) και ο αντικειμενικός σκοπός κάποιων τρομοκρατικών οργανώσεων (οικονομικό κέρδος για υποστήριξη της τρομοκρατικής τους δράσης, η οποία σχεδόν πάντα έχει κάποια υποστηρίζουσα ιδεολογική βάση) είναι σε πλήρη αρμονία, οδηγώντας στην αποδοχή μιας λύσης win--win για τα δύο μέρη: οι τρομοκράτες, παρέχοντας ένοπλη κάλυψη έναντι αμοιβής στις ομάδες εμπορίας ναρκωτικών, εξασφαλίζουν στο μέτρο του δυνατού την ασφάλεια της μεταφοράς του παράνομου εμπορεύματος, το οποίο ταξιδεύοντας με μεγαλύτερη ασφάλεια, φτάνει φθηνότερο στους τόπους διάθεσης και έτσι όλοι οι εμπλεκόμενοι είναι οικονομικά κερδισμένοι.

Σοβαρές μορφές κυβερνοπολέμου, υποκλοπή ευαίσθητων πληροφοριών και πλούτου

Κατασκοπεία – αντικατασκοπεία ανθρώπων, συστημάτων και τεχνολογιών. Εισχώρηση σε βάσεις δεδομένων. Δημιουργούνται καταστροφικές συνέπειες για τους πολίτες και τα κράτη

Υποκλοπή πληροφοριών όπως συνομιλίες απο τηλεφωνικά δίκτυα gsm, κοινωνικά δίκτυα, ηλεκτρονικό ταχυδρομείο, υπηρσίες τηλεφωνίας voip. Εδώ σε αυτό το κομμάτι και ειδικά στην περίπτωση υποκλοπήςτου τηλεφωνικού δικτύου χρειάζονται εξιδικευμένα μηχανήματα και η παίζουν ρόλο και οι αποστάσεις. Πάυει πλέον ο κυβερνοπόλεμος να έιναι εντελώς εξ αποστάσεως και χρειάζεται κάποια κοντινή επαφή, κάποια απόσταση.Οι επιθέσεις εδώ γίνονται συνήθως απο πράκτορες ξένων υπηρεσιών που παρακολουθούν τους στόχους και τις υποδομές απο κοντά.

Για παράδειγμα παγιδέυσεις οικοδομικών τεταγώνων και υποκλοπή πληροφοριών μέσω καλωδίων η παρεμβολή και υποκλοπή μέσω συχνοτήτων αποστάσεις κάποιοων μέτρων και χιλιομέτρων. Οι υποκλοπές συνομιλιών voip χωρίς να αφηθούν ίχνοι καθώς και οι υποκλοπές κοινωνικών δικύων και ηλεκτρονικού ταχυδρομείου για να έχουν μεγάλη επιτυχία πρέπει να υπάρχει μια απόσταση πάλι. Μπορεί να γίνει και υποκλοπή μέσω διαφόρων τεχνικών και απο μακρία απλά αφήνου ίχνη. Σε αυτό το κομμάτι εννοούμαι πάντα των κυβερνοπόλεμο μέσω δυο χωρών όπου σε καμία απο τις δυο δεν υπάρχουν σέρβερς φιλοξενίας κοινωνικών δικτύων, ηλεκτρονικού ταχυδρομείου και voip.

Χτυπημάτα σε τράπεζες, οικονομικά ιδρύματα και οργανισμούς.

Κριτήριο:επιτιθέμενος

Κρατική ή μη κρατική οντότητα

Οι κατηγορίες των πιθανών εμπλεκομένων σε περιστατικά κυβερνοπολέμου δεν είναι εύκολο να ταξινομηθούν με μαθηματική σαφήνεια, ωστόσο διακρίνονται σε δύο μεγάλες κατηγορίες. Η διάκριση αυτή φέρει το χαρακτηριστικό της μεταβεστφαλιανής εποχής αφού πρόκειται ουσιαστικά για τον διαχωρισμό των δρώντων (ή οντοτήτων) σε κρατικούς και σε μη κρατικούς. Στην περίπτωση των κρατικών δρώντων αναφερόμαστε ξεκάθαρα σε κυρίαρχα κράτη, τα οποία έχουν εντάξει τον κυβερνοπόλεμο ως μια επιλογή η οποία παραμένει διαθέσιμη για ενεργοποίηση ανάλογα των περιστάσεων. Βέβαια, όπως συνηθίζεται, πάντα γίνεται λόγος για κυβερνοάμυνα ή κυβερνοπροστασία και σχεδόν ποτέ για κυβερνοπόλεμο με την αρνητική διάσταση που αποκτά συχνά ο όρος αυτός. Το οτι όλοι αυτοί οι δρώντες είναι πλήρως έτοιμοι για να πραγματοποιήσουν το πρώτο χτύπημα κυβερνοπολέμου είναι μια ανομολόγητη πραγματικότητα.

Από την άλλη πλευρά υπάρχουν οντότητες που ενώ δεν είναι κράτη εντούτοις έχουν σοβαρές δυνατότητες κυβερνοπολέμου. Αυτό δεν είναι καινοφανές, αφού για παράδειγμα υπάρχουν εξτρεμιστικές ομάδες με σημαντική στρατιωτική εκπαίδευση, στελέχωση και εξοπλισμό. Η πρόσκτηση επιπλέον δυνατότητας πραγματοποίησης κυβερνοπολέμου δεν είναι κάτι ασύλληπτο. Αντίθετα μάλιστα, είναι ευκολότερο (και σημαντικά οικονομικότερο) για κάποια οργάνωση π.χ. όπως η Χεζμπολά, να αποκτήσει κυβερνοόπλα από το αποκτήσει σύγχρονα αντιαρματικά μέσα. Αυτές οι μη κρατικές οντότητες συνιστούν την έτερη μεγάλη ομάδα δρώντων στο πεδίο του κυβερνοπολέμου. Εαν ο εντοπισμός, η αξιολόγηση και η εκτίμηση των δυνατοτήτων για πραγματοποίηση κυβερνοπολέμου των οντοτήτων της δεύτερης κατηγορίας δρώντων φαίνεται να μην είναι απλή περίπτωση, δεν ισχύει το ίδιο για τους κρατικούς δρώντες αφού τα ίδια τα κράτη καταρτίζουν σχέδια κυβερνοπολέμου (κυβερνοάμυνας) στοιχεία των οποίων βλέπουν το φως της δημοσιότητας.

Τελευταία υποκατηγορία μη κρατικών δρώντων είναι οι λεγόμενες ανεξάρτητες οντότητες. Συνηθέστερα πρόκειται για συνομαδώσεις ατόμων και σπανιότερα συναντούμε τα άτομα που δρουν ανεξάρτητα και μεμονωμένα. Στην πλειονότητα των περιπτώσεων η δράση των ανεξαρτήτων οντοτήτων δεν οδηγείται από κάποια υψηλού επιπέδου κινητήρια ιδεολογία, όπως η περίπτωση των κυβερνοπολεμιστών της Χεζμπολά, οι οποίοι υπηρετούν την ιδεολογία της κεντρικής οργάνωσης από το μετερίζι του κυβερνοχώρου. Εδώ συχνά η κυβερνοεπίθεση γίνεται για την κυβερνοεπίθεση ή για λόγους που είναι άμεσα συνδεδεμένοι με την ίδια την δομή του διαδικτύου. Θα μπορούσε απλουστευτικά να θεωρηθεί οτι στην υποκατηγορία αυτή εντάσσονται αυτομάτως όλοι οι χάκερ εαν και ο όρος είναι τόσο ευρείας χρήσης που ίσως η απλούστευση αυτή να αποτελεί παρακινδυνευμένη προσέγγιση. Ωστόσο, με την έννοια του χάκερ που δίδει ο Jeremie Zimmermann, φίλος και συνεργάτης του Julian Assange των Wikileaks, εύκολα ξεκαθαρίζεται οτι, πράγματι, οι χάκερ μπορεί να θεωρηθεί οτι εμπίπτουν σε αυτήν την κατηγορία δρώντων, τουλάχιστον στα αρχικά τους βήματα.

Κριτήριο:Μέθοδος επίθεσης

Οι μέθοδοι που χρησμοποιούνται απο κράτη αλλά και τρομοκρατικές οργανώσεις πολλές φορές είναι οι ίδιοι, πολλές φορές διαφέρουν. Ανάλογα με την περίσταση, τον στόχο και την δυσκολία.

Συχνή μέθοδος επιθέσεων της πρώτης κατηγορίας είναι η άρνηση εξυπηρέτησης του συστήματος. Το σύστημα υπερφορτώνεται με παραπάνω χρήστες απο ότι μπορεί να αντέξει και καταρέει. Η άρνηση υπηρεσίας (DoS) προκαλεί συντριβή ενός συστήματος για να το κάνει απρόσιτο.

Στη δέυτερη κατηγορία οι μέθοδοι που χρησιμοποιούνται είναι η δηλητηρίαση, η ανακτατεύθυνση της κίνησης και των δεδομένων, η οσμή των πακέτων, η ωμή βία, η πλαστογράφηση τον τομέων τον ονομάτων, η πλαστογράφηση και η ψευδής υπογραφή κλειδίων κρυπτογράφησης και αποκρυπτογράφησης και έγκυρων διαπιστευτηρίων, η κλονωποίηση και άλλες. Κακόβουλα δηλαδή λογισμικά που περιλαμβάνουν ιούς, ιούς τύπου worm και trojans. Phishing, παραπλανητικές επικοινωνίες για την κλοπή ευαίσθητων πληροφοριών καθώς και Man-in-the-Middle (MitM), υποκλοπή επικοινωνίας μεταξύ δύο μερών

Στην τρίτη κατηγορία οι μέθοδοι διεξαγωγής επιθέσεων είναι οι ίδιοι με την διαφορά ότι απαιτείται η φυσική πρόσβαση στα δίκτυα αλλά και η παρουσία άλλων ειδικοτήτων εκτός ανθρώπων της πληροφορικής σε περιπτώσεις χημικών, πυρηνικών, ιατρικών κλπ επιθέσεων.

Κριτήριο:Βλάβη έννομου αγαθού

Παραβίαση δεδομένων: Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.

Διακοπή εξυπηρέτησης: Διακοπή υπηρεσιών.

Οικονομική Ζημιά: Άμεση ή έμμεση οικονομική ζημία.

Ζημιά φήμης: Επίπτωση στη φήμη της στοχευόμενης οντότητας.

Το Stuxnet στοχεύει σε συστήματα εποπτικού ελέγχου και συλλογής δεδομένων (SCADA) και πιστεύεται ότι είναι υπεύθυνο για την πρόκληση σημαντικής ζημιάς στο πυρηνικό πρόγραμμα του Ιράν. Αν και καμία χώρα δεν έχει παραδεχτεί ανοιχτά την ευθύνη, πολλοί ανεξάρτητοι ειδησεογραφικοί οργανισμοί αναγνωρίζουν ότι το Stuxnet είναι ένα όπλο στον κυβερνοχώρο που κατασκευάστηκε από κοινού από τις Ηνωμένες Πολιτείες και το Ισραήλ σε μια συλλογική προσπάθεια γνωστή ως Operation Olympic Games. Το πρόγραμμα, που ξεκίνησε κατά τη διάρκεια της κυβέρνησης Μπους, επεκτάθηκε γρήγορα μέσα στους πρώτους μήνες της προεδρίας του Μπαράκ Ομπάμα. Το Stuxnet στοχεύει ειδικά προγραμματιζόμενους λογικούς ελεγκτές (PLC), οι οποίοι επιτρέπουν την αυτοματοποίηση ηλεκτρομηχανικών διεργασιών, όπως αυτές που χρησιμοποιούνται για τον έλεγχο μηχανημάτων και βιομηχανικών διεργασιών, συμπεριλαμβανομένων των φυγοκεντρητών αερίου για τον διαχωρισμό πυρηνικών υλικών. Το Stuxnet έχει τρεις ενότητες: ένα worm που εκτελεί όλες τις ρουτίνες που σχετίζονται με το κύριο ωφέλιμο φορτίο της επίθεσης. ένα αρχείο συνδέσμου που εκτελεί αυτόματα τα πολλαπλασιαζόμενα αντίγραφα του ιού τύπου worm και ένα στοιχείο rootkit υπεύθυνο για την απόκρυψη όλων των κακόβουλων αρχείων και διεργασιών, για την αποφυγή εντοπισμού του Stuxnet. Τυπικά εισάγεται στο περιβάλλον στόχο μέσω μιας μολυσμένης μονάδας flash USB , διασχίζοντας έτσι οποιοδήποτε κενό αέρα . Το σκουλήκι στη συνέχεια διαδίδεται σε όλο το δίκτυο, σαρώνοντας το λογισμικό Siemens Step σε υπολογιστές που ελέγχουν ένα PLC. Ελλείψει οποιουδήποτε κριτηρίου, το Stuxnet γίνεται αδρανές μέσα στον υπολογιστή. Εάν πληρούνται και οι δύο προϋποθέσεις,

το Stuxnet εισάγει το μολυσμένο rootkit στο λογισμικό PLC και Step, τροποποιώντας τον κώδικα και δίνοντας απροσδόκητες εντολές στο PLC ενώ επιστρέφει στους χρήστες έναν βρόχο τιμών του συστήματος κανονικής λειτουργίας.

Επίσης, το σκουλήκι υπολογιστών (worm) WannaCry, γνωστό και ως WannaCry Cryptoworm, ήταν μια κυβερνοεπίθεση λυτρισμικού (ransomware) σε υπολογιστές σε όλο τον κόσμο που τρέχουν το λειτουργικό σύστημα Windows, με την οποία κρυπτογραφούνταν αρχεία και ζητούνταν λύτρα 300-600 δολαρίων μέσω Bitcoin για να αποκτήσει ο χρήστης και πάλι πρόσβαση στα αρχεία του. Η επίθεση κράτησε τρεις μέρες, από τις 12 Μαΐου μέχρι τις 15 Μαΐου 2017.

Το WannaCry είναι βασισμένο στο EternalBlue της NSA, ένα exploit του πρωτοκόλλου SMB των Windows. Διέρρευσε από τους Shadow Brokers στις 9 Απριλίου, ένα μήνα πριν την επίθεση. Η Microsoft, στις 14 Μαρτίου, έβγαλε μια ενημέρωση που προστατεύει τα λειτουργικά της συστήματα απ' αυτό το exploit. Η ενημέρωση αυτή είναι γνωστή και ως MS17-010. Κάποιες από τις πρώτες επιθέσεις, στις 12 Μαΐου, συνέβησαν στο Εθνικό Σύστημα Υγείας στο Ηνωμένο Βασίλειο, σε υπηρεσία κινητής τηλεφωνίας στην Ισπανία, στην εταιρεία μεταφορών FedEx και σε εταιρία τρένων. Μια μέρα μετά την εκκίνηση της επίθεσης, γνωστοποιήθηκε πως το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης είναι ανάμεσα στους παγκόσμιους οργανισμούς που χτυπήθηκαν από τον ιό.

Τέλος, η παραβίαση SolarWinds είναι ο συνήθως χρησιμοποιούμενος όρος για την παραβίαση της εφοδιαστικής αλυσίδας που αφορούσε το σύστημα SolarWinds Orion. Σε αυτή την περίπτωση κυβερνοπολέμου, ύποπτοι χάκερ εθνικών κρατών που έχουν αναγνωριστεί ως ομάδα γνωστή ως Nobelium από τη Microsoft και συχνά αναφέρονται απλώς ως SolarWinds Hackers από άλλους ερευνητές απέκτησαν πρόσβαση στα δίκτυα, τα συστήματα και τα δεδομένα χιλιάδων πελατών. Το εύρος της ενέργειας είναι πρωτοφανές και ένα από τα μεγαλύτερα, αν όχι το μεγαλύτερο, του είδους που έχουν καταγραφεί ποτέ. Περισσότεροι από 30.000 δημόσιοι και ιδιωτικοί οργανισμοί, συμπεριλαμβανομένων τοπικών, κρατικών και ομοσπονδιακών υπηρεσιών χρησιμοποιούν το σύστημα διαχείρισης δικτύου Orion για τη διαχείριση των πόρων πληροφορικής τους. Ως αποτέλεσμα, το hack έθεσε σε κίνδυνο τα δεδομένα, τα δίκτυα και τα συστήματα χιλιάδων όταν η SolarWinds παρέδωσε κατά λάθος το κακόβουλο λογισμικό backdoor ως ενημέρωση του λογισμικού Orion.

Οι πελάτες της SolarWinds δεν ήταν οι μόνοι που επηρεάστηκαν. Επειδή το hack αποκάλυψε τις εσωτερικές λειτουργίες των χρηστών του Orion, οι χάκερ θα μπορούσαν ενδεχομένως να αποκτήσουν πρόσβαση στα δεδομένα και τα δίκτυα των πελατών και των συνεργατών τους , επιτρέποντας στα θύματα να αυξηθούν εκθετικά.

Κεφάλαιο Γ

Νομικά-ηθικά ζητήματα επιλογής στόχων-κανόνες εμπλοκής

Γ.1 Νομικά ζητήματα επιλογής στόχων – humanitarian law

Το αμέσως επόμενο στάδιο μετά την αποκρυστάλλωση της έννοιας της «επίθεσης» υπό το πρίσμα του κυβερνοπολέμου, είναι να εξετάσουμε αν το Διεθνές Ανθρωπιστικό Δίκαιο (International Humanitarian Law) ή αλλιώς Δίκαιο των Ενόπλων Συγκρούσεων δύναται να εφαρμοστεί επ' αυτού. Το Δίκαιο των Ενόπλων Συγκρούσεων συνίσταται σε ένα σύνολο κανόνων το οποίο έχει σκοπό την οριοθέτηση και τον περιορισμό των επιπτώσεων των ενόπλων συγκρούσεων, την προστασία των ατόμων που δε λαμβάνουν μέρος στις εχθροπραξίες και τον περιορισμό των μεθόδων διεξαγωγής πολέμου βάσει ανθρωπιστικών κριτηρίων.

Ο κυβερνοπόλεμος συνιστά ανθρωπιστικό ζήτημα καθώς παίζει όλο και μεγαλύτερο ρόλο στη διεξαγωγή ενόπλων συγκρούσεων μεταξύ κρατών και μια από τις κύριες μεθόδους διεξαγωγής του είναι η εξαπόλυση κυβερνοεπιθέσεων κατά κρίσιμων υποδομών και οργανισμών κοινής ωφελείας, με αποτέλεσμα να πλήττεται ο άμαχος πληθυσμός. Το Δίκαιο των Ενόπλων Συγκρούσεων (jus in bello) καλύπτει τις ενέργειες κυβερνοπολέμου οι οποίες λαμβάνουν χώρα κατά τη διάρκεια ένοπλης σύγκρουσης μεταξύ κρατών. Παρόλο που δεν υπάρχει ειδική πρόβλεψη για τις ενέργειες κυβερνοπολέμου (κυβερνοεπιχειρήσεις/cyber operations), οι θεμελιώδεις αρχές του Δικαίου των Ενόπλων Συγκρούσεων μας επιτρέπουν να το εφαρμόσουμε και σε αυτές, ειδικότερα η αρχή της διάκρισης (principle of distinction), σύμφωνα με την οποία τα εμπόλεμα μέρη πρέπει να διακρίνουν ανάμεσα στον άμαχο πληθυσμό και τις ένοπλες δυνάμεις και ανάμεσα σε στρατιωτικούς στόχους και μη, ενώ θα πρέπει να εκτελούν επιχειρήσεις μόνο κατά στρατιωτικών στόχων (Art. 48 AP I; Rules 1 and 7 ICRC Customary IHL Study. International Court of Justice, Legality of the threat or the use of nuclear weapons, Advisory Opinion, 8 July 1996, παρ. 78). Στην πράξη, σπάνια γίνεται διάκριση μεταξύ στρατιωτικών στόχων και μη, ενώ αρκετά διαδεδομένη είναι η χρήση κυβερνο-όπλων, τα οποία είναι σχεδιασμένα ώστε να προκαλούν τη μέγιστη ζημιά. Ο απόλυτος βαθμός διασυνδεσιμότητας που χαρακτηρίζει τον κυβερνοχώρο μπορεί να οδηγήσει στο να επηρεαστούν περαιτέρω συστήματα από τα συστήματα-στόχους, γεγονός που αποτελεί κατάφορη παράβαση της αρχής της διάκρισης και μπορεί να οδηγήσει σε παράπλευρα πλήγματα κατά αμάχων (collateral damage). Το «κενό» αυτό έρχονται να καλύψουν οι αρχή της αναλογικότητας (principle of proportionality) και η αρχή της προφύλαξης (principle of precaution), οι οποίες εφαρμόζονται ταυτόχρονα με την αρχή της διάκρισης, ώστε να διασφαλιστεί η συμμόρφωση της διεξαγωγής των πολεμικών επιχειρήσεων με τους κανόνες του Δικαίου των Ενόπλων Συγκρούσεων. Σύμφωνα με την αρχή της αναλογικότητας, απαγορεύεται η εξαπόλυση επίθεσης σε περίπτωση που αυτή δύναται να οδηγήσει με βεβαιότητα σε απώλειες αμάχων ή ζημιές σε μη

στρατιωτικούς στόχους και το στρατιωτικό αποτέλεσμα αυτής (π.χ. κατάληψη εδάφους, εκπλήρωση αντικειμενικών σκοπών) είναι αντιστρόφως ανάλογο με τη ζημιά που θα προκληθεί στο άμαχο πληθυσμό, ενώ σύμφωνα με την αρχή της προφύλαξης οι στρατιωτικές επιχειρήσεις θα πρέπει να διενεργούνται με γνώμονα τη διαφύλαξη του αμάχου πληθυσμού και των μη στρατιωτικών στόχων. Λαμβάνοντας υπόψιν τα ανωτέρω και γνωρίζοντας την άναρχη δομή του Διαδικτύου και του κυβερνοχώρου, καθώς και το στοιχείο του αγνώστου που χαρακτηρίζει τα συστήματα-στόχους στην πλειοψηφία των περιπτώσεων, οδηγούμαστε στο συμπέρασμα ότι είναι εξαιρετικά δύσκολο να εκτελεσθούν κυβερνοεπιχειρήσεις πλήρως εναρμονισμένες με το Δίκαιο των Ενόπλων Συγκρούσεων, ζήτημα το οποίο δεν επιδέχεται τεχνική λύση, όπως θα αναλύσουμε παρακάτω.

Ο κυβερνοχώρος δεν περιορίζεται μόνο στα διαβαθμισμένα δίκτυα που χρησιμοποιούνται για στρατιωτικούς σκοπούς, αλλά φιλοξενεί ως επί το πλείστον «πολιτικού χαρακτήρα» εφαρμογές (civilian applications). Λόγω της άναρχης δομής του Διαδικτύου, της φιλοσοφίας της διασύνδεσης πόρων (inter-nodal connectivity) που το διακατέχει, καθώς και της πρακτικής των «υποδομών δύο ταχυτήτων» (multi-track infrastructure/rental infrastructure) είναι πρακτικά αδύνατο να επιτευχθεί πλήρης διαχωρισμός μεταξύ του στρατιωτικού και πολιτικού τομέα του κυβερνοχώρου. Η πλειοψηφία των συστημάτων Ελέγχου και Διοίκησης (Command and Control systems) χρησιμοποιεί ως βασικό κορμό το Διαδίκτυο και κατ' επέκταση πολιτικές υποδομές τηλεπικοινωνιών, ενώ τα ίδια συστήματα πλοήγησης που χρησιμοποιούνται από τους απλούς πολίτες χρησιμοποιούνται και για στρατιωτικούς σκοπούς. Συνεπώς, γεννάται η ανάγκη να «ζυγιστεί» ο πολιτικός χαρακτήρας των υποδομών αυτών και η ανάγκη επίτευξης στρατιωτικών αντικειμενικών σκοπών (objectives), προκειμένου να προκειμένου να κριθεί αν δύνανται να προστατευτούν από το Δίκαιο των Ενόπλων Συγκρούσεων. Παράλληλα, το Δίκαιο των Ενόπλων Συγκρούσεων προστατεύει ρητά ειδικότερες κατηγορίες υποδομών από επίθεση, όπως αυτές που αφορούν τη δημόσια υγεία και γενικότερα τις υποδομές που κρίνονται απαραίτητες για την επιβίωση του άμαχου πληθυσμού (π.χ. συστήματα διαχείρισης υδροδότησης).

Υπό το πρίσμα του Δικαίου των Ενόπλων Συγκρούσεων, ο ορισμός της επίθεσης πηγάζει από το 49ο άρθρο του Πρόσθετου Πρωτοκόλλου της Συνθήκης της Γενεύης, στο οποίο αναφέρεται: "*1. "Attacks" means acts of violence against the adversary, whether in offence or in defence.*

2. The provisions of this Protocol with respect to attacks apply to all attacks in whatever territory conducted, including the national territory belonging to a Party to the conflict but under the control of an adverse Party.

3. The provisions of this Section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They further apply to all attacks from the sea or

from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air.

4. The provisions of this Section are additional to the rules concerning humanitarian protection contained in the Fourth Convention, particularly in Part II thereof, and in other international agreements binding upon the High Contracting Parties, as well as to other rules of international law relating to the protection of civilians and civilian objects on land, at sea or in the air against the effects of hostilities."

Συνεπώς, προκειμένου να χαρακτηριστεί μια κυβερνοεπίθεση ως «επίθεση» σύμφωνα με το Δίκαιο των Ενόπλων Συγκρούσεων, θα πρέπει να λαμβάνει χώρα στο πλαίσιο στρατιωτικής επιχείρησης (κυβερνοεπιχείρηση). Κυβερνοεπιχειρήσεις οι οποίες έχουν ως αντικειμενικό σκοπό ή δύνανται να προκαλέσουν ζημιές σε εγκαταστάσεις ή ανθρώπινες απώλειες χαρακτηρίζονται ως «επιθέσεις» σύμφωνα με το Δίκαιο των Ενόπλων Συγκρούσεων. Πρέπει να σημειωθεί ότι κυβερνοεπιχειρήσεις οι οποίες δεν προκαλούν «φυσικές» ζημιές σε συστήματα, αλλά τα θέτουν εκτός λειτουργίας, επίσης χαρακτηρίζονται ως «επιθέσεις», καθώς κρίνονται με βάση την επενέργειά τους. Παραδείγματος χάρη, μια επίθεση η οποία καθιστά το δίκτυο διανομής ηλεκτρικού ρεύματος μη διαθέσιμο χωρίς όμως να προκαλεί φυσικές ζημιές στα συστήματά του, θεωρείται επίθεση, καθώς έχει επενέργεια η οποία δύναται να προκαλέσει υλικές ζημιές ή ανθρώπινες απώλειες.

Φυσική συνέχεια των ανωτέρω είναι η εξέταση της αντεπίθεσης από μέρους του κράτους-στόχου. Όπως εκθέσαμε παραπάνω, υπάρχει ένα «όριο» (threshold) το οποίο πρέπει να ξεπεράσει ο επιτιθέμενος ώστε οι ενέργειές του να θεωρηθούν «ένοπλη επίθεση». Ο χαρακτηρισμός τους αυτός είναι σημαντικός για τη θεμελίωση της αυτοάμυνας, καθώς το άρθρο 51 του Χάρτη των Ηνωμένων Εθνών, από το οποίο πηγάζει και η «νομιμοποίηση» της αυτοάμυνας, απαιτεί την ύπαρξη «ένοπλης επίθεσης» ώστε να δικαιολογηθεί η αυτοάμυνα. Σε περίπτωση που οι ενέργειες του επιτιθέμενου δεν «αρκούν» ώστε να στοιχειοθετηθεί «ένοπλη επίθεση», π.χ. σε περίπτωση που ο επιτιθέμενος εξαπολύσει μη καταστρεπτικές κυβερνοεπιχειρήσεις, όπως «κυβερνοεπιθέσεις ανίχνευσης» (probing cyberattacks), η νομολογία του Διεθνούς Δικαστηρίου έχει δεχτεί (Nicaragua Case (n 7) para 249) ότι το κράτος-στόχος μπορεί να «απαντήσει» αναλογικά (proportional response), όχι όμως σε βαθμό που να συνιστά «ένοπλη επίθεση». Παράλληλα, όπως αναφέραμε παραπάνω, εφαρμόζεται το «δόγμα της καρφίτσας» (pinprick doctrine), οπότε επιθέσεις που αποτελούν μέρος ευρύτερου σχεδίου του επιτιθέμενου δύνανται να ξεπεράσουν το «όριο» και να θεωρηθούν συλλογικά «ένοπλες επιθέσεις».

Γ.2 Jus ad bellum – Jus in bello

Η επίθεση κατατάσσεται παραδοσιακά στην έννοια του κυβερνοπολέμου στην περίπτωση παραβίασης διατάξεων του Χάρτη ΗΕ, δίκαιο της χρήσης βίας (jus ad bellum). Στο κείμενο του Χάρτη των Ηνωμένων Εθνών, που υπογράφηκε μετά τη λήξη του Β΄ Παγκοσμίου Πολέμου, περιλαμβάνονται μεταξύ

άλλων και διατάξεις από το συνδυασμό των οποίων προκύπτει το βασικό ρυθμιστικό πλαίσιο του δικαίου της χρήσης βίας, δηλαδή ο κύριος μηχανισμός, που αποβλέπει στην επίτευξη του βασικού στόχου του Οργανισμού των ΗΕ, τη διατήρηση της διεθνούς ειρήνης και ασφάλειας, μέσω της γενικής απαγόρευσης της χρήσης βίας, ως μέσου για την επίλυση των διαφορών που δημιουργούνται μεταξύ των μελών του Οργανισμού. Όταν εγκρίθηκε ο Χάρτης των Ηνωμένων Εθνών (1945), τα κράτη απειλούνταν μόνο με κινητικά μέσα και μεθόδους πολέμου και στο πλαίσιό του η επιθετικότητα κατανοήθηκε ως η χρήση ένοπλης δύναμης κατά της κυριαρχίας, της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας άλλου κράτους (ΟΗΕ Ψήφισμα 3314). Οι εναέριοι βομβαρδισμοί, οι χερσαίες επιθέσεις, οι πυραυλικές επιδρομές και άλλες εδαφικές επιδρομές ήταν οι παραδοσιακές κινητικές μέθοδοι πολέμου στο στρατιωτικό πεδίο μάχης. Οι στρατιωτικές επιχειρήσεις επικεντρώνονταν πάντα στην καταστροφή των εχθρικών δυνάμεων μέσω της εφαρμογής των φυσικών επιπτώσεων με τη χρήση κινητικών μέσων πολέμου. Ο θάνατος, ο τραυματισμός και η καταστροφή που προκλήθηκαν από κινητικές επιθέσεις ήταν το προαπαιτούμενο κριτήριο για να οριστεί μια επίθεση ως «μη εξουσιοδοτημένη χρήση βίας». Στην πραγματικότητα ούτε ο ορισμός της «επίθεσης» ούτε ο ορισμός της κυβερνοεπίθεσης είναι επίσημα καθορισμένοι. (Pipyros, A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual)

Συγκεκριμένα ορίζεται ότι:

- *Όλα τα Μέλη στις διεθνείς τους σχέσεις θα απέχουν από την απειλή ή τη χρήση βίας, που εκδηλώνεται εναντίον της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους*

  είτε με οποιαδήποτε άλλη ενέργεια ασυμβίβαστη προς τους Σκοπούς των Ηνωμένων Εθνών. **(Άρθρο 2 παράγραφος 4)**

- *Το Συμβούλιο Ασφαλείας θα αποφαίνεται αν υπάρχει απειλή για την ειρήνη, διατάραξη της ειρήνης ή επιθετική ενέργεια και θα κάνει συστάσεις ή θα αποφασίζει ποια μέτρα θα λαμβάνονται σύμφωνα με τα Άρθρα 41 και 42, για να διατηρηθεί ή να αποκατασταθεί η διεθνής ειρήνη και ασφάλεια.* **(Άρθρο 39)**
- *Το Συμβούλιο Ασφαλείας μπορεί να αποφασίζει ποια μέτρα, που δε συνεπάγονται τη χρησιμοποίηση ένοπλης δύναμης θα λαμβάνονται για να εξασφαλίζουν την εκτέλεση των αποφάσεών του, και μπορεί να καλεί τα Μέλη των Ηνωμένων Εθνών να εφαρμόζουν αυτά τα μέτρα. Αυτά μπορεί να περιλαμβάνουν πλήρη ή μερική διακοπή των οικονομικών σχέσεων, των σιδηροδρομικών, θαλάσσιων, εναέριων, συγκοινωνιών, των ταχυδρομικών, τηλεγραφικών, ραδιοφωνικών και άλλων μέσων επικοινωνίας, καθώς και τη διακοπή διπλωματικών σχέσεων.* **(Άρθρο 41)**

- *Αν το Συμβούλιο Ασφαλείας κρίνει ότι τα μέτρα που προβλέπονται από το Άρθρο 41 θα ήταν ανεπαρκή ή ότι έχουν αποδειχτεί ανεπαρκή, μπορεί να προχωρήσει με αεροπορικές, θαλάσσιες ή χερσαίες δυνάμεις στην ανάληψη της δράσης που θα ήταν αναγκαία για τη διατήρηση ή την αποκατάσταση της διεθνούς ασφάλειας και ειρήνης. Αυτή η δράση θα μπορούσε να περιλαμβάνει στρατιωτικές επιδείξεις, αποκλεισμό και άλλες επιχειρήσεις αεροπορικών, θαλάσσιων ή χερσαίων δυνάμεων των Μελών των Ηνωμένων Εθνών.* **(Άρθρο 42)**
- *Καμιά διάταξη αυτού του Χάρτη δε θα εμποδίζει το φυσικό δικαίωμα της ατομικής ή συλλογικής νόμιμης άμυνας, σε περίπτωση που ένα Μέλος των Ηνωμένων Εθνών δέχεται ένοπλη επίθεση, ως τη στιγμή που το Συμβούλιο Ασφαλείας θα πάρει τα αναγκαία μέτρα για να διατηρήσει τη διεθνή ειρήνη και ασφάλεια. Τα μέτρα που θα παίρνουν τα Μέλη των Ηνωμένων Εθνών κατά την άσκηση αυτού του δικαιώματος της νόμιμης άμυνας θα ανακοινώνονται αμέσως στο Συμβούλιο Ασφαλείας, και σε καμία περίπτωση δε θα θίγουν την εξουσία και την υποχρέωση που έχει το Συμβούλιο Ασφαλείας, σύμφωνα με αυτόν το Χάρτη, να αναλαμβάνει οποτεδήποτε τη δράση που κρίνει αναγκαία για τη διατήρηση ή για την αποκατάσταση της διεθνούς ειρήνης και ασφάλειας.* **(Άρθρο 51)**

Η επίθεση επίσης κατατάσσεται στην έννοια του κυβερνοπολέμου στην περίπτωση που έχουν παραβιασθεί συμβατικοί και εθιμικοί κανόνες. Το παραδοσιακό δίκαιο δηλαδή του πολέμου (jus in bello). Με τον όρο Δίκαιο του πολέμου, νοείται το σύνολο των συμβατικών και εθιμικών κανόνων του Διεθνούς Δικαίου, που ρυθμίζουν τη συμπεριφορά των αντίπαλων μερών κατά τη διάρκεια μιας πολεμικής αντιπαράθεσης. Στην περίπτωση της τέλεσης μιας κυβερνοεπίθεσης, ενόσω οι γενικευμένες εχθροπραξίες είναι σε εξέλιξη, η εφαρμογή κάποιων εκ των αρχών του δικαίου του πολέμου, που απορρέουν από τα τρία βασικά ρυθμιστικά κείμενα τις Συνθήκες της Γενεύης (1949) και τα Πρωτόκολλα που προστέθηκαν σ' αυτές (1977), δημιουργεί ποικίλους προβληματισμούς.

Ειδικότερα πρόκειται για τις εξής αρχές: την αρχή της στρατιωτικής αναγκαιότητας, την αρχή της διάκρισης και την αρχή της αναλογικότητας. Στο άναρχο σύστημα του κυβερνοχώρου, οι δράστες οι οποίοι επιδίδονται σε παράνομες δραστηριότητες, ομαδοποιούνται γενικώς σε κατηγορίες, κυρίως με βάση το σκοπό για τον οποίο δραστηριοποιούνται.

Το μεγαλύτερο μέρος της δραστηριότητας που παρατηρείται σήμερα στον Κυβερνοχώρο ποικίλει από την απλή εισβολή σε ένα σύστημα και τον έλεγχό του για λόγους πρόκλησης και περιέργειας, μέχρι την εισβολή σε ένα σύστημα για λόγους εκδίκησης, κλοπής πληροφοριών, πρόκλησης, παρενόχλησης, υπεξαίρεσης χρημάτων ή πρόκλησης εσκεμμένης τοπικής βλάβης σε υπολογιστές ή καταστροφής μεγαλύτερης έκτασης σε υποδομές.

Οι επιπτώσεις όμως της κατηγορίας αυτής των Κυβερνοεπιθέσεων που εκδηλώνονται από χάκερ, ακτιβιστές χάκερ, το οργανωμένο έγκλημα, τη βιομηχανική κατασκοπία και τους εσωτερικούς δράστες, οι οποίες μπορεί να είναι ιδιαίτερα σοβαρές και δεν πρέπει να υποτιμώνται, χαρακτηρίζονται ως χάκινγκ, κυβερνοβλάβες, κλοπή, εκδίκηση, κατασκοπία, οργανωμένο έγκλημα και εμπίπτουν στη δικαιοδοσία της επιβολής του νόμου και της απονομής δικαιοσύνης.

Η χρήση των Κυβερνοόπλων και οι τεχνικές για την προσβολή διαφόρων στόχων μπορεί να αποτελούν κριτήριο κατάταξης μίας επίθεσης στην έννοια του κυβερνοπόλεμου.

Γ.3 Ευρωπαϊκή στρατηγική ασφάλειας

Ένα από τα σημαντικότερα ισχυρά σημεία της προσέγγισης της ΕΕ είναι το μείγμα ήπιας και σκληρής ισχύος που τη χαρακτηρίζει. Χρησιμοποιεί μέσα ασφαλείας και άμυνας παράλληλα με διπλωματικά μέσα, κυρώσεις, αναπτυξιακή συνεργασία και το εμπόριο με σκοπό την πρόληψη των συγκρούσεων. Προωθεί την ειρήνη, την χωρίς αποκλεισμούς ανάπτυξη, τα ανθρώπινα δικαιώματα, το κράτος δικαίου και την προστασία του περιβάλλοντος, τόσο στο εσωτερικό όσο και στο εξωτερικό. Αν και η ήπια ισχύς δεν αρκεί από μόνη της σε έναν κόσμο που χαρακτηρίζεται από αστάθεια, η ολοκληρωμένη αυτή προσέγγιση αποτελεί κεντρική προϋπόθεση για βιώσιμη ασφάλεια.

Η ΕΕ, μέσα από τις νέες εξελίξεις που γίνονται με τους κυβερνοπολέμους, τις σχετικές επιθέσεις, συγκρούσεις και απειλές, έχει δημιουργήσει ένα πλαίσιο για να μειώσει ή και να εξαλείψει τέτοιου είδους ενέργειες, για να προστατέψει όσο είναι δυνατόν τα κράτη και τους πολίτες τους. (Council of Europe, 2001) Αρχικά, το θέμα που απασχολεί την ΕΕ είναι η ασφάλεια στο χώρο του Διαδικτύου, κάτι που προχώρηση με τη σχετική Οδηγία NIS 2, που προτάθηκε 3 χρόνια πριν (δηλαδή, το Δεκέμβριου του 2020), ώστε να αντιμετωπίσουν καλύτερα θέματα κυβερνοεπιθέσεων, με ανάλογες ρήτρες. Πρέπει να τονιστεί ότι η συγκεκριμένη Οδηγία αποτελεί την πρώτη πράξη, σε νομικό πλαίσιο, που διευθετήθηκε από την ΕΕ για την ασφάλεια στον κυβερνοχώρο. (IN.gr., 2023)

Η ΕΕ στη σύγχρονη εποχή έχει προβεί σε μία σειρά από νέους κανόνες και οδηγίες σε σχέση με τις απειλές, όπως αυτές διαμορφώνονται σήμερα με τις νέες γεωπολιτικές εξελίξεις, αλλά και τις επιθέσεις που λαμβάνουν χώρο στο διαδίκτυο. Βασικός σκοπός είναι να προστατευθούν σε κάθε περίπτωση οι πολίτες από απάτες, απειλές και κυβερνοεπιθέσεις. (Monar, 2015) Κι αυτό διότι οι υβριδικές απειλές τείνουν να πάρουν μεγάλες διαστάσεις, ενώ μπορούν να απειλήσουν σημαντικές υποδομές, άμαχους και κοινωνίες ολόκληρες. Εκτιμάται ότι περίπου 450 περιστατικά ασφάλειας που σχετίζονται με βασικές υποδομές σε ευρωπαϊκό χώρο έλαβαν χώρα μόνο για το έτος 2019, μεταξύ των οποίων και τομείς της ενέργειας και ο χρηματοπιστωτικός.

Χρονιά ορόσημο για την καταπολέμηση του κυβερνοεγκλήματος αποτέλεσε το 2001, οπότε και υπεγράφη η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο (Convention on Cyber Crime), ή αλλιώς η Σύμβαση της Βουδαπέστης, όπως αποκαλείται

εν συντομία λόγω του τόπου υπογραφής της. Αντικείμενο - στόχο της Σύμβασης αποτέλεσε η εναρμόνιση των εθνικών νομοθεσιών των κρατών μελών στον τομέα της αντιμετώπισης της εγκληματικότητας στον κυβερνοχώρο. Παράλληλα θεσπίστηκαν διατάξεις, απαραίτητες για την έρευνα, δίωξη και εκδίκαση τέτοιων εγκλημάτων, καθώς και τις διαδικασίες συλλογής αποδεικτικών στοιχείων (Πίπυρος,2018)

Για το 2020-2025, η έχει καταρτίσει μία συγκεκριμένη πολιτική στρατηγικής με γνώμονα την προστασία και την ασφάλεια, για να βοηθήσει τα κράτη της, σε ένα μεγάλο εύρος πεδίων, όπως από την απλή απειλή και την πάταξη της τρομοκρατίας μέχρι και απειλές για υβριδικές επιθέσεις.

Στις μέρες μας δημιουργούνται πολλά προβλήματα, συγκρούσεις και απάτες σε σχέση με το διαδίκτυο, καθώς επίσης ένα πολύ σημαντικό και επικίνδυνο στοιχείο που αναδεικνύεται είναι ο πόλεμος και η επίθεση μέσω Διαδικτύου. Γι' αυτό και η ΕΕ έχει θεσπίσει μία σειρά από κανόνες, για να αποφεύγονται όσο είναι δυνατόν τέτοιες κακόβουλες πράξεις, αλλά και να διασφαλιστεί η ασφάλεια των πολιτών και των κρατών. Οι αναβαθμίσεις που έχουν γίνει ως προς αυτό είναι πολύ ουσιαστικά, ειδικά στο τομέα των κυβερνοεπιθέσεων, ωστόσο βέβαια υπάρχουν και κάποια κενά. (Ζάννη, 2005) Σε αντίθεση με άλλα είδη πολέμου, ο κυβερνοπόλεμος έχει κάποια ιδιαίτερα στοιχεία τα οποία, όπως χαρακτηριστικά αναφέρει η Μαρούδα (2015), θέτουν σε αμφισβήτηση κάποια στοιχεία που σχετίζονται με το Δίκαιο που εφαρμοζόταν παραδοσιακά σε τέτοιες περιπτώσεις, αλλά και το νομικό πλαίσιο που διέπει τον κυβερνοχώρο.

Είναι γεγονός, όπως τονίζει η ίδια, ότι δεν υπάρχουν ειδικές διατάξεις που να καλύπτουν τις «διαστάσεις του» και, κατά συνέπεια, μπορεί να προκύψουν πολλές ασάφειες ή να μην μπορεί να υπάρξει μία λύση ή να αποδοθεί δικαιοσύνη ή ποινή κ.λπ. Λόγω όμως της κρισιμότητας της κατάστασης, όπως αυτή δημιουργείται με τέτοιες επιχειρήσεις, ιδιαίτερα τις τελευταίες δεκαετίες, ο έλεγχός του απαιτεί τη χρήση του Δ. Δικαίου, καθώς η εφαρμογή κάποιων διατάξεων του, που ωστόσο υφίστανται και έχουν ανακύψει με στοιχεία που αφορούν έναν κανονικό, παραδοσιακό πόλεμο. (Μαρούδα, 2015) Έτσι εύκολα αντιλαμβάνεται κανείς ότι δεν υπάρχουν σαφείς ρήτρες ή κώδικες για τον κυβερνοπόλεμο, οπότε σίγουρα οι αντιστοιχίες σε αυτόν θα έχουν κάποια κενά ή ασαφή σημεία, με αποτέλεσμα να μην μπορεί να λειτουργήσει με τον καλύτερο τρόπο το Δίκαιο στην περίπτωση αυτή.

Αξίζει να σημειωθεί ότι κατά καιρούς έχουν προταθεί διάφορες εκδοχές για να διευθετηθεί το θέμα αυτό και να υπάρξουν νέες και συγκεκριμένες διατάξεις, ωστόσο προς το παρόν τουλάχιστον κάτι τέτοιο δεν υφίσταται. (Κωνσταντοπούλου, 1986) Το νομικό πλαίσιο είναι βασικό να υπάρχει, ώστε να καλύπτονται τέτοια θέματα και οι επεκτάσεις αυτών με κάποιους κανόνες και νόμους, όπως άλλωστε γίνεται και στον παραδοσιακό τρόπο πολέμου, όπου ακολουθείται το Διεθνές Δίκαιο (π.χ., για αμάχους, για ανθρωπιστική βοήθεια κ.ά.). Ωστόσο, μέχρι σήμερα δεν υπάρχουν σαφείς κανόνες, σε παγκόσμιο επίπεδο, που να αφορούν τη διαδίκτυο και, πιο συγκεκριμένα, σε επιθέσεις, συγκρούσεις ή καταστροφές που μπορεί να συμβούν μέσα από αυτά, όπως θα ήταν για παράδειγμα μια κυβερνοσύμβαση. Αντί αυτού, όπως χαρακτηριστικά επισημαίνει η Eilstrup-Sangiovanni (2018), υπάρχουν κάποιες συνεργασίες

(που δεν μπορούν να χαρακτηριστούν ως επίσημες), αλλά και στρατηγικές περιορισμού και μείωσης τέτοιων φαινομένων, με βασικό σκοπό να αποτραπούν τέτοια γεγονότα, όμως και δεν είναι αρκετά μέτρα. (Eilstrup-Sangiovanni, 2018) Δηλαδή, διάφορες επιθετικές πράξεις και ένοπλη βία κατά κρατών με ψηφιακά μέσα του κυβερνοχώρου δεν καλύπτονται από το Διεθνές Δίκαιο. (Γεωργαντάς, 2016)

Υπάρχουν πολλά και συγκεκριμένα στοιχεία που δεν έχουν αποσαφηνιστεί. Σύμφωνα με τον ΟΗΕ, δεν μπορεί ένα κράτος που έχει δεχθεί μια κυβερνοεπίθεση, να ανταποδώσει, όπως γίνεται για παράδειγμα στις κανονικές συγκρούσεις στους τόπους μάχης. Για να μπορέσει να αμυνθεί ένα κράτος, σε περίπτωση που υπάρξει ανάγκη, θα πρέπει να αποδειχθεί με κάποιον τρόπο ότι οι επιθέσεις που δέχθηκε θεωρούνται ως ένοπλη επίθεση. Κάτι που, όπως εύκολα αντιλαμβάνεται κανείς είναι πολύ δύσκολο να συμβεί, λόγω της ασάφειας και των κενών που υπάρχουν στο Δίκαιο. Όπως χαρακτηριστικά επισημαίνει η Σίμου (2016), αυτό δεν μπορεί στην ουσία να γίνει διότι μια επίθεση μέσω διαδικτύου δεν μπορεί να χαρακτηριστεί ως «φονική» και, κατά συνέπεια, δεν άπτεται στη χρήση βίας. Ακόμη, όμως, κι αν αποδειχθεί κάτι τέτοιο (που είναι εξαιρετικά σπάνιο), δεν υπάρχουν κυρώσεις, καθώς αποφεύγονται οι αποδόσεις ευθυνών κατηγορώντας πολίτες τους. Κατά συνέπεια, υπάρχουν πολλά κενά όσον αφορά τον τομέα αυτόν σε νομικό πλαίσιο. (Σίμου, 2016; Γεωργαντάς, 2016)

Το ΔΑΔ έχει δημιουργηθεί για να προσφέρει προστασία των ατόμων που λαμβάνουν μέρος σε διάφορες εχθροπραξίες και συγκρούσεις, αλλά και για τον περιορισμό διαφόρων μέσω που χρησιμοποιούνται στους πολέμους. Με βάση κάποιες αρχές, που θα αναλύσουμε παρακάτω, το ΔΑΔ δρα ως βασικό «εργαλείο» θέτει κάποιες υποχρεώσεις που είναι υποχρεωμένα να ακολουθούν τα κράτη που βρίσκονται σε συγκρούσεις ή πόλεμο. (Ohlin et al., 2015) Παρ’ όλα αυτά, είναι βασικό να τονιστεί ότι φαίνεται να υπάρχουν κάποια κενά ή ελλείψεις καθώς μέχρι τώρα σε ανάλογες περιπτώσεις, εμπειρογνώμονες δεν κατάφεραν να εξασφαλίσουν ή να διευθετήσουν κάποιου είδους συναίνεσης μεταξύ εχθροπραξιών, κι αυτό σχετίζονται με τις διατάξεις και πώς αυτές ερμηνεύονται σε πολλές περιπτώσεις. Χαρακτηριστικό παράδειγμα είναι οι αναφορές σε «πλειοψηφίες» και «μειοψηφίες», που στην πράξη είναι δύσκολο να καθοριστούν και έτσι η κάθε πλευρά μπορεί να έχει τη δική της εκδοχή πάνω σε αυτό. (Schmidt, 2013) Οι πιο βασικές από αυτές τις Αρχές είναι οι παρακάτω, οι οποίες -σημειωτέων- πρέπει να τονιστεί ότι συμπεριλαμβάνονται στο Πρόσθετο Πρωτόκολλο Ι του 1977, και στην ουσία κωδικοποιούν το βασικό σκοπό του ΔΑΔ ότι οι εμπόλεμοι στις ένοπλες συρράξεις δεν είναι δυνατόν να δρουν χωρίς κανέναν περιορισμό στις μέρες μας.

Κεφάλαιο Δ

Δ.1 Τρόποι επίθεσης

Όπως προαναφέραμε, οι ενέργειες κυβερνοπολέμου μπορούν να κατηγοριοποιηθούν σε πέντε διακριτές μεθόδους. Στην ενότητα αυτή θα συμπληρώσουμε και θα εμβαθύνουμε τα όσα αναφέραμε στην εισαγωγή.

Η κυβερνο-κατασκοπεία, όπως αναφέραμε ανωτέρω, είναι μια από τις πλέον διαδεδομένες και συχνές μεθόδους κυβερνοπολέμου, με αποτέλεσμα την ανάπτυξη διαφόρων «σχολών» κυβερνο-κατασκοπείας, οι οποίες προσομοιάζουν τα στρατιωτικά δόγματα.

Οι «σχολές» αυτές διακρίνονται κυρίως ανάλογα με την διεισδυτικότητα της κατασκοπευτικής ενέργειας (degree of penetration) και την «ορατότητά» της (degree of visibility). Συνεπώς, μπορούμε να κάνουμε λόγο για «παθητική» κυβερνο-κατασκοπεία, κατά την οποία ο επιτιθέμενος συλλέγει δεδομένα χωρίς καταστρεπτική παρέμβαση στο σύστημα του στόχου και για «ενεργητική» κυβερνο-κατασκοπεία, κατά την οποία ο επιτιθέμενος αποκτά βίαια πρόσβαση στα συστήματα του στόχου και προβαίνει σε κλοπή δεδομένων (data theft).

Η «παθητική» κυβερνο-κατασκοπεία χαρακτηρίζεται από τις «χαμηλού επιπέδου» εφαρμογές της (low-level applications). Ως χαμηλού επιπέδου εφαρμογές ορίζονται οι πράξεις κυβερνο-κατασκοπείας οι οποίες δεν επιδεικνύουν υψηλό βαθμό επεμβατικότητας (degree of invasiveness). Τέτοιες επιθέσεις βασίζονται στη στοχοποίηση των περιφερειακών συστημάτων του στόχου και την εφαρμογή παθητικών τεχνικών παρακολούθησης (passive monitoring appplications). Ως περιφερειακό σύστημα ορίζεται το υλικολογισμικό το οποίο χρησιμοποιείται προς υποστήριξη της λειτουργίας του στόχου, όπως είναι ο εξοπλισμός γραφείου (πληκτρολόγια, εκτυπωτές), ο εξοπλισμός δικτύου (δρομολογητές,εξυπηρετητές) και τα διάφορα λογισμικά εγκατεστημένα στον υπολογιστή-στόχο (για παράδειγμα λογισμικά εταιρικής διασύνδεσης όπως το AnyDesk). Τα ανωτέρω μπορούν να εκμεταλλευτούν από τον επιτιθέμενο ώστε αυτός να εγκαταστήσει λύσεις παρακολούθησης (surveillance solutions), κυρίως καταγραφείς πληκτρολόγησης (keyloggers) και εφαρμογές παρακολούθησης δικτύου (network monitoring solutions-network taps). Οι λύσεις αυτές προτιμώνται καθώς μπορούν να λάβουν τη μορφή τόσο υλικού όσο και λογισμικού, καθιστώντας τες πλήρως ευέλικτες και παραμετροποιήσιμες, γεγονός που αυξάνει την ελευθερία του επιτιθέμενου όσον αφορά τον τρόπο διεξαγωγής της επίθεσης. Ο επιτιθέμενος μπορεί να επιδιώξει να επέμβει «στον πραγματικό κόσμο», είτε αποκτώντας πρόσβαση στο χώρο του στόχου, είτε μέσω επίθεσης στην εφοδιαστική αλυσίδα του (supply chain attack). Παρά το σχετικά χαμηλό ρίσκο τους, οι πρακτικές αυτές αργούν να αποφέρουν αποτελέσματα, καθώς τα δεδομένα που παράγουν μπορούν να αξιολογηθούν μόνο μετά από ανάλυση μοτίβων (pattern analysis) καθιστώντας τες εξαιρετικά χρονοβόρες και κατά συνέπεια ασύμφορες σε συνθήκες πολέμου.

Η «ενεργητική» κυβερνο-κατασκοπεία βασίζεται στη «βίαιη» επίτευξη πρόσβασης στα συστήματα του στόχου και την απόκτηση των αποθηκευμένων σε αυτά δεδομένων και η δράση της

αναπτύσσεται σε δύο άξονες, την κοινωνική μηχανική (social engineering) και την επεμβατική επίθεση (invasive attack). Ως κοινωνική μηχανική ορίζεται η χρήση ψυχολογικών τακτικών χειραγώγησης (psychological manipulation tactics) από τον επιτιθέμενο, ώστε αυτός να κερδίσει την εμπιστοσύνη του ατόμου-στόχου, αποκτώντας πρόσβαση στα συστήματά του. Οι κύριες κατηγορίες κοινωνικής μηχανικής είναι οι τακτικές δολώματος (baiting), οι προσχηματικές τακτικές (pretexting) και το «ηλεκτρονικό ψάρεμα» (phishing). Οι τακτικές δολώματος χρησιμοποιούν μια απατηλή υπόσχεση (false promise), ώστε να εκμεταλλευτούν το ενδιαφέρον του στόχου και να τον οδηγήσουν στο να διαπράξει «λάθη ασφαλείας» (security mistakes). Η «απατηλή υπόσχεση» μπορεί να είναι είτε φυσικό αντικείμενο (physical object), είτε ένας πόρος Διαδικτύου (network resource, για παράδειγμα μια απατηλή διαφήμιση ή ιστοσελίδα. Με τις προσχηματικές τακτικές ο επιτιθέμενος κερδίζει και εκμεταλλεύεται την εμπιστοσύνη του θύματος. Συνήθως ο επιτιθέμενος υιοθετεί την ταυτότητα ατόμου εντός του οργανισμού του στόχου, ώστε να παρακάμψει τις άμυνές του και να τον ωθήσει στο να εκτελέσει μια ενέργεια ή να προβεί σε «λάθος ασφαλείας». Τρίτη και τελευταία μέθοδος είναι το «ηλεκτρονικό ψάρεμα» (phishing). Ως «ηλεκτρονικό ψάρεμα» ορίζεται η χρήση ιστοσελίδων, μηνυμάτων ηλεκτρονικού ταχυδρομείου και ενίοτε μηνυμάτων μέσω κινητού τηλεφώνου (SMS), τα οποία είναι σχεδιασμένα ώστε να δημιουργήσουν λάθος εντυπώσεις στον στόχο, ωθώντας τον στο να προβεί σε «λάθος ασφάλειας». Το spear phishing αποτελεί μια ειδικότερη παραλλαγή, κατά το οποίο ο επιτιθέμενος στοχεύει αποκλειστικά συγκεκριμένα άτομα ή οργανισμούς, προσαρμόζοντας την τακτική του στα ιδιαίτερα χαρακτηριστικά τους.

Ο δεύτερος άξονας της «ενεργητικής» κυβερνο-κατασκοπείας είναι η επεμβατική επίθεση, η οποία μπορεί να έχει ως αφετηρία μια επιχείρηση κοινωνικής μηχανικής ή μπορεί να εξαπολυθεί μόνη της, σε περίπτωση που είναι αδύνατο να επιτευχθεί πρόσβαση στο σύστημα του στόχου με μέσα κοινωνικής μηχανικής. Η κύρια μορφή επεμβατικής επίθεσης είναι η παραβίαση δεδομένων (data breach), κατά την οποία ο επιτιθέμενος καταφέρνει να παραβιάσει τα μέτρα ασφαλείας του συστήματος του στόχου και να προχωρήσει σε κλοπή δεδομένων (data theft). Η ανάλυση των τεχνικών απόκτησης πρόσβασης, οι οποίες είναι πρακτικά όσες και τα δυνητικά συστήματα-στόχοι, καθώς κάθε σύστημα παρουσιάζει μοναδικές προκλήσεις ασφαλείας (security challenges), ξεφεύγουν από τα όρια της εργασίας, οπότε θα αναφερθούμε επιγραμματικά σε αυτές. Η κύρια τεχνική επίτευξης πρόσβασης είναι η επίθεση μέσω κωδικών πρόσβασης (password attack). Οι επιθέσεις μέσω κωδικών πρόσβασης προσπαθούν να «μαντέψουν» τον κωδικό πρόσβασης του στόχου ώστε να αποκτήσουν πρόσβαση στο σύστημά του. Υπάρχουν πολλοί διεξαγωγής τέτοιων επιθέσεων, οι οποίοι συγκεντρώνονται σε τρια ξεχωριστά αρχέτυπα. Πρώτο αρχέτυπο είναι οι επιθέσεις «ωμής δύναμης» (brute force attacks), με τις οποίες ο επιτιθέμενος χρησιμοποιεί την υπολογιστική του ισχύ ώστε να δοκιμάσει όσο περισσότερους κωδικούς πρόσβασης γίνεται, μέχρι να βρει το σωστό. Η ταχύτητα διεξαγωγής τέτοιων επιθέσεων καθώς και ο βαθμός επιτυχίας τους συνδέεται άρρηκτα με τη διαθέσιμη υπολογιστική ισχύ του επιτιθέμενου. Δεύτερο αρχέτυπο επιθέσεων είναι οι επιθέσεις με βάση μια προ-δομημένη λίστα πιθανών κωδικών

πρόσβασης, οι λεγόμενες «επιθέσεις λεξιλογίου» (dictionary attacks). Ο επιτιθέμενος εκμεταλλεύεται τη συνήθεια των στόχων να θέτουν αδύναμους κωδικούς πρόσβασης, ειδικά σε περίπτωση που ο στόχος είναι οργανισμός ο οποίος εκδίδει ο ίδιος τα διαπιστευτήρια των χρηστών του, οπότε υπάρχει διαθέσιμη «μήτρα» αυτών, την οποία μπορεί να εκμεταλλευτεί ο επιτιθέμενος. Λόγω του χαρακτήρα τους, οι επιθέσεις αυτές είναι αμφιβόλου επιτυχίας καθώς η αποτελεσματική πρόβλεψη των «τάσεων» γύρω από τη θέση κωδικών πρόσβασης είναι αδύνατη και η ύπαρξη «μήτρας» κωδικών πρόσβασης ενός οργανισμού ή έστω δειγμάτων κωδικών πρόσβασης του στόχου δε μπορεί να εγγυηθεί. Τρίτο και τελευταίο αρχέτυπο, το οποίο συνδυάζει τα ανωτέρω δύο, είναι οι λεγόμενες «επιθέσεις πίνακα ουρανίου τόξου» (rainbow table password attacks). Οι επιθέσεις αυτές εκμεταλλεύονται το γεγονός ότι τα περισσότερα συστήματα χρησιμοποιούν μια ξεχωριστή βάση δεδομένων η οποία περιέχει τους κωδικούς πρόσβασης (password database), η οποία είναι κωδικοποιημένη μέσω ενός αλγορίθμου κατακερματισμού (hashing algorithm). Η κωδικοποίηση διαφέρει από την κρυπτογράφηση, καθώς αντί το απλό κείμενο (plaintext), στην προκειμένη περίπτωση οι κωδικοί πρόσβασης, να κρυπτογραφείται, κωδικοποιείται, με κάθε χαρακτήρα κειμένου (character) να λαμβάνει ειδικό κώδικα (unique hash). Η διαδικασία αυτή είναι μόνιμη και το αρχικό κείμενο δε μπορεί να επανέλθει στην αρχική του μορφή, παρά μόνο με την εφαρμογή του αλγορίθμου με τον οποίο έγινε η αρχική κωδικοποίηση. Ο επιτιθέμενος μπορεί, εφόσον έχει αποκτήσει πρόσβαση είτε σε βάση δεδομένων με κωδικούς πρόσβασης είτε σε «καθαρές» αξίες κατακερματισμού (raw hash values), να εντοπίσει τον αλγόριθμο που χρησιμοποιείται και, χρησιμοποιώντας το μοντέλο «ουράνιου τόξου» (rainbow hash model) να «από-κατακερματίσει» τις αξίες, ώστε να προκύψει το αρχικό κείμενο των κωδικών πρόσβασης. Να σημειωθεί ότι σχεδόν το σύνολο τέτοιου είδους αλγορίθμων είναι δημόσια προσβάσιμο καθώς η κύρια χρήση τους είναι στον τομέα της διασφάλισης ακεραιότητας δεδομένων, ενώ οι δύο δημοφιλέστεροι (MD5, SHA11) έχουν παραβιαστεί τουλάχιστον προ δεκαετίας αλλά συνεχίζουν να χρησιμοποιούνται ευρύτατα.

Το δεύτερο στάδιο της «ενεργητικής» κυβερνο-κατασκοπείας είναι η διενέργεια της κλοπής των δεδομένων. Για το σκοπό αυτό έχουν αναπτυχθεί ειδικά εργαλεία, τα οποία χωρίζονται σε δύο κατηγορίες, το κακόβουλο λογισμικό αντιγραφής (data exfiltration virus/worm) και το κακόβουλο λογισμικό διαγραφής (wiper malware). Ο επιτιθέμενος εισάγει στο σύστημα-στόχο ένα κακόβουλο λογισμικό αντιγραφής, το οποίο θα κωδικοποιήσει (hashing) και θα αντιγράψει τα δεδομένα του στόχου, στέλνοντάς τα στο αποθετήριο (repository) του επιτιθέμενου. Μόλις η διαδικασία αυτή ολοκληρωθεί, ο επιτιθέμενος, αν θέλει να προκαλέσει περαιτέρω ζημιές, μπορεί να εισάγει στο σύστημα-στόχο ένα κακόβουλο λογισμικό διαγραφής δεδομένων.

Η διάδοση προπαγάνδας είναι η πιο διαδεδομένη μορφή διεξαγωγής κυβερνοπολέμου, λόγω της ιδιαίτερα αυξημένης αναλογίας αποτελέσματος προς κόστους (cost-to-benefit rate). Θα πρέπει να σημειωθεί ότι η διάδοση προπαγάνδας δεν εντάσσεται στη σφαίρα του «πολέμου της πληροφορίας» (information warfare), καθώς εντάσσεται στις επιχειρήσεις ψυχολογικού πολέμου (psy-ops), άρα αποτελεί πολεμική ενέργεια και όχι πράξη έχουσα επενέργεια επί της πληροφορίας, ενώ παράλληλα ο

όρος «πληροφορία» με στενή έννοια υπό το πρίσμα του «πολέμου της πληροφορίας» εξειδικεύεται στην πληροφορία που συλλέγεται και μεταδίδεται από τα συστήματα διοίκησης, ελέγχου και επικοινωνίας των ενόπλων δυνάμεων του κράτους-στόχου (Command and Control systems) (Borden. 1999 σ.3).

Ειδικότερες μορφές προπαγάνδας, οι οποίες υφίστανται και στην κυβερνο-προπαγάνδα, είναι η μαύρη προπαγάνδα (black propaganda) και η λευκή προπαγάνδα (white propaganda). Ως μαύρη προπαγάνδα ορίζεται αυτή η οποία προορίζεται να εκληφθεί από τα υποκείμενα ως προερχόμενη από αυτούς που υποτίθεται ότι δυσφημίζει, ενώ ως λευκή προπαγάνδα ορίζεται αυτή η οποία δεν αποκρύπτει την προέλευση ή τη φύση της. Όπως είναι φυσικό, η λευκή προπαγάνδα δε μπορεί να αποτελέσει αποτελεσματικό όπλο αποσταθεροποίησης του αντιπάλου, ιδίως λόγω των αυξημένων ευαισθησιών των πολιτών και κυρίως της αυξημένης δυνατότητας για ενημέρωση και διεύρυνση των οριζόντων των πολιτών λόγω της ραγδαίας εξέλιξης της τεχνολογίας, ιδίως των κινητών εφαρμογών (smartphones, κινητό internet) και της ραγδαίας μείωσης του οικονομικού «ορίου πρόσβασης» (barrier of access) στην τεχνολογία αυτή. Για το σκοπό αυτό οι εκάστοτε επιτιθέμενοι στρέφονται στην λεγόμενη «γκρίζα» προπαγάνδα, η οποία συνδυάζει στοιχεία των ανωτέρω μορφών. Κύριο χαρακτηριστικό της, και αυτό το οποίο την καθιστά τόσο αποτελεσματική υπό το πρίσμα του κυβερνοπολέμου, είναι ο μειωμένος βαθμός «υπερβολής» της (degree of overtness), γεγονός που καθιστά δύσκολο το συσχετισμό της με τον «εχθρό». Κύριοι μηχανισμοί διάδοσης της «γκρίζας» προπαγάνδας είναι οι «φάρμες τρολ» (troll farms) και τα «συνθετικά πολυμέσα» (synthetic media). Σκοπός μιας «φάρμας τρολ» είναι να δημιουργήσει ρεύματα κοινής γνώμης. Προς επίτευξη του σκοπού αυτού έχουν αναπτυχθεί τρεις «σχολές» διεξαγωγής τέτοιων επιχειρήσεων. Η πρώτη είναι τα λεγόμενα «έμμισθα τρολ» (paid trolls). Οι χρήστες αυτοί είναι υπαρκτά πρόσωπα και στην πλειονότητα των περιπτώσεων χρησιμοποιούν τα προσωπικά τους προφίλ στα κοινωνικά δίκτυα, γεγονός που προσδίδει κύρος στα λεγόμενά τους και καθιστά δυσκολότερο τον εντοπισμό τους, καθώς η χρήση αληθινών προσωπικών λογαριασμών προσδίδει «οργανικότητα» στην όλη επιχείρηση. Τα δυο πιο γνωστά παραδείγματα αυτής της φιλοσοφίας είναι το «Κόμμα των Πενήντα Λεπτών» (50 Cent Party-Wumao) της Λαικής Δημοκρατίας της Κίνας, το οποίο έχει λάβει την ονομασία του από το ποσό των 50 Γιουάν που λαμβάνουν οι υπάλληλοί του ανά δημοσίευση ή σχόλιο στα κοινωνικά δίκτυα (King,Pan,Roberts,2017 σσ. 1,3,4) και οι «Ιντερνετικές Ταξιαρχίες» (Internet Brigades) της Ρωσικής Ομοσπονδίας (Sindelar,2014). Πρέπει όμως να σημειωθεί ότι ακόμα και σε τέτοιες επιχειρήσεις ανάπτυξης «φάρμας τρολ» ενδέχεται να χρησιμοποιηθούν ψεύτικα προφίλ στα κοινωνικά δίκτυα (sockpuppeting). Το sockpuppeting αποτελεί τη δεύτερη «σχολή» διεξαγωγής επιχειρήσεων και βασίζεται στην κατάρχην ανώνυμη φύση του Διαδικτύου, η οποία επιτρέπει στον οποιονδήποτε με τις απαραίτητες τεχνικές γνώσεις να υιοθετήσει όποια ταυτότητα θέλει (Wikipedia,2023). Οι επιχειρήσεις sockpuppeting συνίστανται στη δημιουργία ψεύτικων προφίλ στα κοινωνικά δίκτυα με σκοπό τον επηρεασμό της κοινής γνώμης. Προκειμένου να επιτύχει μια τέτοια επιχείρηση, η δράση της αναπτύσσεται σε δύο άξονες. Πρώτον, τα ψεύτικα προφίλ στα κοινωνικά δίκτυα θα πρέπει να διαθέτουν ένα πλήρες «ιστορικό» (background), το οποίο θα πρέπει

να περιέχει όλες τις απαραίτητες λεπτομέρειες ώστε το προφίλ να θεωρηθεί αληθινό από τους υπόλοιπους χρήστες, να διαθέτει τις απαραίτητες υποστηρικτικές λεπτομέρειες (supporting details) προς διασταύρωση του ιστορικού του, και κυρίως να καθίσταται η παρουσία του στον κυβερνοχώρο (cyber-presence) πολιτισμικά και γεωγραφικά συναφής με τους χρήστες-στόχους. Η διαδικασία αυτή απαιτεί εξειδικευμένες γνώσεις, πολιτισμικές παραστάσεις συναφείς με αυτές των χρηστών-στόχων και κυρίως γλωσσική, εθιμολογική και πολιτική ανάλυση των χρηστών-στόχων, συνεπώς οι μόνοι παράγοντες (actors) που μπορούν να οργανώσουν τέτοιες επιχειρήσεις είναι κυβερνήσεις. Το πλέον «διάσημο» παράδειγμα τέτοιας επιχείρησης είναι η «Επιχείρηση Σοβαρή Φωνή» (Operation Earnest Voice) των ΗΠΑ, κατά την οποία η κυβέρνηση των ΗΠΑ ανέθεσε στην εταιρεία λύσεων διαδικτυακής ασφάλειας Ntrepid να αναπτύξει ειδικό λογισμικό, με το οποίο Αμερικανοί προπαγανδιστές θα μπορούσαν να αναρτήσουν δημοσιεύσεις σε κοινωνικά δίκτυα ανά τη Μέση Ανατολή, παράλληλα με την κατασκευή «ταυτοτήτων» για τα ψεύτικα προφίλ στα κοινωνικά δίκτυα από τα οποία θα γίνονταν οι δημοσιεύσεις (Fielding, Cobain,2011). Ο δεύτερος άξονας των επιχειρήσεων sockpuppeting είναι η ανάπτυξη υποδομών εξυπηρέτησης, οι οποίες λαμβάνουν κυρίως τη μορφή Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks-VPN) με τα οποία επιτυγχάνεται η απόκρυψη της πραγματικής τοποθεσίας από όπου γίνονται οι δημοσιεύσεις και η ανάπτυξη ειδικού λογισμικού μέσω του οποίου θα δύνανται να ελέγχονται πολλαπλά προφίλ από ένα άτομο ή ομάδα ατόμων (Fielding, Cobain,2011). Η τρίτη «σχολή» διεξαγωγής επιχειρήσεων συνίσταται στην πλήρη αυτοματοποίηση των ανωτέρω διαδικασιών, με την χρήση bots, συνεπώς εδώ γίνεται λόγος για social bots και όχι trolls, καθώς εκλείπει το ανθρώπινο στοιχείο. Η λειτουργία τέτοιου είδους «φαρμών τρολ» δεν απαιτεί υψηλού επιπέδου υποδομές, καθώς το μόνο που χρειάζεται είναι ένας υπολογιστής με το απαραίτητο λογισμικό.

Ο όρος «συνθετικά μέσα» (synthetic media) αναφέρεται στην αλλοίωση, τροποποίηση και δημιουργία πολυμέσων χρησιμοποιώντας εφαρμογές Παραγωγικής Τεχνητής Νοημοσύνης (Generative AI). Εδώ πρέπει να σημειωθεί ότι ο όρος «μέσα» αποτελεί την ελληνική απόδοση του όρου «media» και, παρόλο που δεν καθίσταται σαφές, περιλαμβάνει και σύνολα δεδομένων (data sets), πέρα από τα «παραδοσιακά» πολυμέσα (Synthesia.io,2023). Πρέπει επίσης να σημειωθεί ότι η δημιουργία συνθετικών μέσων δεν είναι αρκετά αποτελεσματική από μόνη της, καθώς δεν περιλαμβάνει «οχήματα» διάδοσής τους, για το σκοπό αυτό αυτά χρησιμοποιούνται σε συνδυασμό με τις «φάρμες τρολ», ώστε να μεγιστοποιηθούν οι αποδέκτες τους. Ένα πρόσφατο παράδειγμα χρήσης συνθετικών μέσων είναι η δημιουργία deepfake βίντεο που απεικονίζει τον Πρόεδρο της Ουκρανίας Ζελένσκι να απευθύνεται στις Ένοπλες Δυνάμεις της χώρας καλώντας τις σε παράδοση και η μεταφόρτωσή του σε Ουκρανική ιστοσελίδα ειδήσεων από Ρώσους χάκερ το Μάρτιο του 2022 (npr.org,2022), περιστατικό που συνδυάζει τόσο συνθετικά μέσα, όσο και «ιντερνετικό βανδαλισμό» (web vandalism). Ως ιντερνετικός βανδαλισμός ορίζεται η αλλοίωση ή τροποποίηση του περιεχομένου ιστοσελίδας από τον επιτιθέμενο. Όπως εκθέσαμε ανωτέρω, η τακτική αυτή αποτελεί ένα από τα «οχήματα» διάδοσης προπαγάνδας. (Gazula, 2017,σ.87). Πρέπει να σημειωθεί ότι ο ιντερνετικός βανδαλισμός διαφέρει ουσιαστικά από την

κυβερνοεπίθεση σε ιστοσελίδα καθώς μόνο το αντικείμενο είναι η επενέργεια του επιτιθέμενου στο περιεχόμενο της ιστοσελίδας και όχι στον κώδικά της ή το λοιπό δομικό της πλαίσιο.

Η τρίτη από τις κύριες μεθόδους διεξαγωγής κυβερνοπολέμου είναι οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS attacks). Όπως αναφέραμε στην εισαγωγή σκοπός των επιθέσεων αυτών είναι η υπερκέραση των εξυπηρετητών (servers) του στόχου, ώστε να αποκλειστεί η πρόσβαση σε αυτούς, με ότι αυτό συνεπάγεται για τις εξαρτώμενες υπηρεσίες ή πόρους λογισμικού. Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης χωρίζονται σε τρεις κατηγορίες, ανάλογα με την «τροχιά» επίθεσης (vector of attack). Η πρώτη κατηγορία επιθέσεων είναι οι επιθέσεις με βάση τον όγκο (volume based attacks), οι οποίες έχουν στόχο τον κορεσμό του διαθέσιμου εύρους σύνδεσης (bandwidth) του στόχου, στερώντας τον από τον πόρο Διαδικτύου (network node) του. Οι κυριότερες μορφές επιθέσεων με βάσει τον όγκο είναι οι επιθέσεις «πλημμύρας» πακέτων δεδομένων και οι επιθέσεις «πλημμύρας» αλλοιωμένων πακέτων δεδομένων (spoofed packet attacks). Οι επιθέσεις «πλημμύρας» πακέτων δεδομένων χωρίζονται σε επιθέσεις μέσω πακέτων δεδομένων UDP και μέσω πακέτων δεδομένων ICMP. Οι επιθέσεις μέσω πακέτων δεδομένων UDP (User Datagram Protocol) χρησιμοποιούν την ιδιότητά τους ως «μη απαιτούμενων σύνδεσης» (connectionless) πακέτων δεδομένων, τα οποία «ρωτούν» τον εξυπηρετητή στόχο περί της διαθεσιμότητας κάποιου προγράμματος, δυναμικού σημείου εισαγωγής ή υπολογιστικού πόρου (resource allocation request), ώστε να αναγκάσουν τον εξυπηρετητή-στόχο να απαντήσει στο εισερχόμενο πακέτο δεδομένων UDP με ένα πακέτο δεδομένων ICMP (ping packet), το οποίο ενημερώνει τον αποστολέα του πακέτου δεδομένων UDP για την αδυναμία ή μη εκπλήρωσης του αιτήματος του εν λόγω πακέτου δεδομένων, οδηγώντας σε κορεσμό, αν επαναληφθεί αρκετές φορές. Οι επιθέσεις «πλημμύρας» πακέτων δεδομένων ICMP ακολουθούν την ίδια φιλοσοφία. Ένα πακέτο δεδομένων ICMP (Internet Control Message Protocol) περιέχει αίτημα προς τη συσκευή-στόχο, σχετικά με την υγεία και τη διαθεσιμότητά (health and connectivity) της. Η συσκευή-στόχος «απαντά» αυτόματα, με συνέπεια να κορεστεί αν η διαδικασία επαναληφθεί πολλές φορές. Τέλος, οι επιθέσεις μέσω αλλοιωμένων πακέτων δεδομένων (spoofed packet attacks) χρησιμοποιούν πακέτα δεδομένων τα οποία αποστέλλονται από «πλαστές» διευθύνσεις IP, οι οποίες μιμούνται αυτές των διαβαθμισμένων «πελατών» του δικτύου (trusted network clients). Η αποστολή αυτών των πακέτων δεδομένων αναγκάζει τον εξυπηρετητή-στόχο να τα επεξεργαστεί, οδηγώντας στον κορεσμό, αν η διαδικασία επαναληφθεί αρκετές φορές.

Δεύτερος τρόπος διεξαγωγής επίθεσης είναι οι επιθέσεις πρωτοκόλλου (protocol attacks). Οι επιθέσεις αυτές εκμεταλλεύονται τη δομή και τις αδυναμίες των πρωτοκόλλων επικοινωνίας του Διαδικτύου (internet protocols), προκειμένου να κορέσουν τόσο τον εξυπηρετητή-στόχο, όσο και τα περιφερειακά του συστήματα, όπως τείχη προστασίας (firewalls), δρομολογητές (routing engines) και συστήματα διαχείρισης φορτίου δεδομένων (load balancers). Οι μορφές αυτού του είδους επιθέσεων ποικίλουν ανάλογα το πρωτόκολλο διαδικτυακής επικοινωνίας που χρησιμοποιεί ο στόχος, όμως μπορούμε να εντοπίσουμε τρείς επιμέρους κατηγορίες, οι οποίες βασίζονται σε ευρέως

χρησιμοποιούμενα πρωτόκολλα διαδικτυακής επικοινωνίας με γνωστές αδυναμίες. Πρώτη κατηγορία τέτοιου είδους επιθέσεων είναι οι επιθέσεις παρεμπόδισης του Πρωτοκόλλου Πύλης Συνόρων (Border Gateway Protocol highjacking). Το συγκεκριμένο πρωτόκολλο χρησιμοποιείται στη δρομολόγηση δικτύων (network routing) και επιτρέπει στον διαχειριστή του εκάστοτε δικτύου να «ανακοινώσει» το σύνολο των διαθέσιμων διευθύνσεων για σύνδεση στο δίκτυο (network address range announcement). Η ενέργεια αυτή είναι απαραίτητη για την ύπαρξη του δικτύου, καθώς στην πράξη αυτό «οριοθετείται» από τις διαθέσιμες αυτές διευθύνσεις. Συνεπώς, ο επιτιθέμενος θα μπορούσε, παραβιάζοντας το Πρωτόκολλο Πύλης Συνόρων, να δρομολογήσει την κυκλοφορία (network traffic routing) ενός δικτύου σε άλλο, οδηγώντας στον κορεσμό. Οι επιθέσεις τέτοιου είδους απαιτούν ειδικές γνώσεις για τη δομή του ανωτέρω πρωτοκόλλου που χρησιμοποιείται από το στόχο και γι' αυτό το λόγο δύνανται να συνδυαστούν με χρήση τακτικών κοινωνικής μηχανικής (social engineering) και κυβερνο-κατασκοπείας (cyber-espionage) προς λήψη πληροφοριών για το δίκτυο του στόχου. Τρίτη και τελευταία κατηγορία κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης είναι οι επιθέσεις «πλημμύρας» πακέτων δεδομένων SYN (synchronise packet). Τα συγκεκριμένα πακέτα δεδομένων αποτελούν το ένα από τα τρία βασικά στοιχεία μιας «χειραψίας» αυθεντικοποίησης (handshake) του πρωτοκόλλου TCP. Η «χειραψία» αυτή είναι απαραίτητη για τη δημιουργία σύνδεσης μεταξύ του εξυπηρετητή και του πελάτη. Το πρώτο βήμα αυτής είναι η αποστολή από τον πελάτη ενός πακέτου δεδομένων SYN, το οποίο περιέχει το αίτημα για τη δημιουργία της ανωτέρω σύνδεσης. Ο εξυπηρετητής αυτόματα θα απαντήσει αποστέλλοντας ένα πακέτο δεδομένων SYN-ACK (synchronise-acknowledge), το οποίο περιέχει την ένδειξη διαθεσιμότητας της ανωτέρω σύνδεσης (connection availability). Τέλος, ο πελάτης αποκρίνεται με ένα πακέτο δεδομένων ACK (acknowledge), το οποίο περιέχει το μήνυμα αποδοχής της σύνδεσης, ολοκληρώνοντας τη «χειραψία». Ο επιτιθέμενος μπορεί να εκμεταλλευτεί το αυτόματο της διαδικασίας ώστε να προκαλέσει κορεσμό, αποστέλλοντας αλλεπάλληλα πακέτα δεδομένων SYN στον εξυπηρετητή-στόχο, ο οποίος θα αναγκαστεί να ξοδέψει υπολογιστικούς πόρους και εύρος σύνδεσης περιμένοντας ο πελάτης-επιτιθέμενος να ολοκληρώσει τη «χειραψία». Ο κορεσμός στην περίπτωση αυτή οδηγεί στην καταβολή αρκετών πόρων του εξυπηρετητή-στόχου, ώστε η επεξεργασία πραγματικών αιτημάτων σύνδεσης να καθίσταται ανέφικτη.

Τρίτη κατηγορία επιθέσεων είναι οι επιθέσεις σε επίπεδο εφαρμογής (application layer DDoS attacks). Οι επιθέσεις αυτού του είδους μπορούν να στραφούν μόνο κατά διακομιστών αιχμής (edge servers), οι οποίοι παραδοσιακά χρησιμοποιούνται για την εκτέλεση εφαρμογών. Οι επιθέσεις αυτές βασίζονται στο σύστημα αιτημάτων HTTP (HTTP requests) στους διακομιστές αιχμής. Ο επιτιθέμενος, εκμεταλλευόμενος την δυσανάλογη κατανάλωση πόρων μεταξύ του ιδίου και του στόχου, «βομβαρδίζει» τον διακομιστή-στόχο με αιτήματα HTTP, προκαλεί κορεσμό, τόσο στους τους υπολογιστικούς πόρους, όσο και στο εύρος σύνδεσης και τους πόρους δικτύου του στόχου. Θα πρέπει να σημειωθεί ότι τα κακόβουλα αιτήματα HTTP είναι εξαιρετικά δύσκολο να εντοπιστούν, καθώς

αποτελούν μέρος της κανονικής λειτουργίας του Διαδικτύου, καθώς μέσω αυτών ο πελάτης ζητά από τον εξυπηρετητή να εμφανίσει συγκεκριμένη ιστοσελίδα (webpage request).

Όπως αναφέραμε παραπάνω, η επιτυχία των κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης εξαρτάται από τον αριθμό των πελατών δικτύου που μπορεί να στρέψει ο επιτιθέμενος εναντίον του εξυπηρετητή-στόχου. Για την επίτευξη του στόχου αυτού ακολουθούνται δύο διαφορετικές τακτικές. Πρώτη εξ' αυτών είναι η δημιουργία από τον επιτιθέμενο ενός αρκετά μεγάλου δικτύου πελατών δικτύου με τον «παραδοσιακό» τρόπο. Η διαδικασία αυτή απαιτεί διόλου ευκαταφρόνητους πόρους, καθώς ο επιτιθέμενος θα πρέπει να αποκτήσει αρκετά υπολογιστικά συστήματα, ώστε να δημιουργήσει τον προσδοκώμενο κορεσμό στον εξυπηρετητή-στόχο. Όπως είναι φυσικό, ένα τέτοιο εγχείρημα είναι απολύτως ασύμφορο, καθώς το κόστος που απαιτείται για τη δημιουργία τέτοιας υποδομής είναι αντιστρόφως ανάλογο των αποτελεσμάτων, καθώς η σύγχρονη αρχιτεκτονική του Διαδικτύου το καθιστά ανθεκτικό σε τέτοιου είδους επιθέσεις, ενώ η ραγδαία εξέλιξη των μέτρων προστασίας, κατά κύριο λόγω των παρόχων «δικτύων απορρόφησης» (buffer networks), όπως η εταιρεία με την επωνυμία Cloudflare, η οποία διατηρεί το μεγαλύτερο τέτοιο δίκτυο στον κόσμο και παρέχει τις υπηρεσίες της τόσο σε ιδιώτες όσο και σε κυβερνήσεις (λόγου χάρη στην κυβέρνηση της Ουκρανίας) (Starzak,2022), καθιστά αβέβαιη την επιτυχία της επίθεσης. Γνωρίζοντας τα ανωτέρω, οι κακόβουλοι παράγοντες που επιδίδονται σε τέτοιου είδους επιθέσεις προχώρησαν στην ανάπτυξη μιας πλέον αποτελεσματικής λύσης, των botnets, η οποία αποτελεί και την πλέον «χρηστική» οδό επίθεσης. Ως botnet ορίζεται μια ομάδα υπολογιστών η οποία έχει προσβληθεί από κακόβουλο λογισμικό (malware) και βρίσκεται υπό έλεγχο κακόβουλου παράγοντα (malicious actor). Ο όρος botnet αποτελεί «μίξη» των όρων bot (στην προκειμένη περίπτωση υπολογιστής υπό τον έλεγχο κακόβουλου παράγοντα) και network (ομάδα τέτοιων υπολογιστών συνδεδεμένων μεταξύ τους υπό κεντρικό έλεγχο από τον κακόβουλο παράγοντα). Στις περισσότερες περιπτώσεις το κακόβουλο αυτό λογισμικό παραμένει αδρανές στον προσβληθέντα υπολογιστή, αναμένοντας εντολές από τον ελεγκτή του botnet (bot herder). Ο έλεγχος των μελών ενός botnet επιτυγχάνεται μέσω μιας «ροής τερματικού εργασίας» (workstation flow), κατά την οποία, ακριβώς όπως ένα τερματικό εργασίας μέσα σε εταιρικό δίκτυο, ο προσβεβλημένος υπολογιστής συνδέεται σε κεντρικό εξυπηρετητή ώστε να λάβει οδηγίες. Σε αντίθεση με το παραπάνω μοντέλο πελάτη-εξυπηρετητή (client-server model), ο δεύτερος τρόπος ελέγχου ενός botnet βασίζεται στην αρχή της αποκέντρωσης (decentralisation). Ένα τέτοιο μοντέλο, το οποίο ονομάζεται «μοντέλο ομότιμου δικτύου» (peer-to-peer model) Σύμφωνα με το μοντέλο αυτό, εκλείπει το κεντρικό σημείο ελέγχου, εξαλείφοντας αυτό το «σημείο αποτυχίας» (point of failure) στο botnet και καθιστώντας την αντιμετώπισή του δυσκολότερη. Μεταξύ των ομότιμων μελών του botnet υπάρχουν συγκεκριμένα μέλη με διαβαθμισμένη πρόσβαση (trusted members) τα οποία μπορούν να στείλουν οδηγίες στα υπόλοιπα μέλη.

Η πλέον καταστρεπτική μέθοδος διεξαγωγής κυβερνοπολέμου είναι η διενέργεια επιθέσεων κατά οργανισμών κοινής ωφέλειας και κρίσιμων υποδομών του αμυνόμενου.Ο πλέον αποδεκτός ορισμός του όρου «κρίσιμες υποδομές» είναι αυτός του Ευρω-Ατλαντικού Συμβουλίου Συνεργασίας

(Euro-Atlantic Partnership Council) του NATO, σύμφωνα με τον οποίο κρίσιμες υποδομές (critical infrastructure) είναι οι εγκαταστάσεις, οι υπηρεσίες και τα συστήματα που είναι τόσο ζωτικής σημασίας για ένα κράτος, ώστε η ανικανότητα ή η καταστροφή τους να οδηγήσει στην αποδυνάμωση της εθνικής ασφάλειας, της εθνικής οικονομίας, της δημόσιας υγείας και ασφάλειας καθώς και την εύρυθμη λειτουργία της κυβέρνησης (Steiner, 2011, σ.12). Κύριο χαρακτηριστικό των κρίσιμων υποδομών είναι η αλληδενδετότητά τους, η οποία αγγίζει την αλληλεξάρτηση (inter-dependent critical infrastructure). Όπως είναι φυσικό, όσο αυξάνεται ο βαθμός αλληλεξάρτησης των υποδομών, τόσο αυξάνεται και ο κίνδυνος δημιουργίας κενών ασφαλείας. Οι επιθέσεις κατά κρίσιμων υποδομών μπορούν να λάβουν πρακτικά άπειρες μορφές, συνεπώς, ώστε να παραμείνουμε εντός των ορίων της εργασίας θα αναλύσουμε τις πλέον συνηθισμένες περιπτώσεις τέτοιων επιθέσεων. Να σημειωθεί ότι σε αυτή την υποενότητα δε θα γίνει λόγος περί τεχνικών ζητημάτων των επιθέσεων αυτών, πέρα από το «όχημα» και τον τρόπο διεξαγωγής τους, καθώς αυτά αναπτύσσονται στην παρούσα ενότητα.

Πρώτο από αυτά τα είδη και το πλέον δημοφιλές είναι η διενέργεια κυβερνοεπιθέσεων στις υποδομές του δικτύου παραγωγής και διανομής ηλεκτρικού ρεύματος. Οι επιθέσεις αυτές είναι πολυεπίπεδες (multi-level attacks), καθώς προσβάλλουν το στόχο με πολλαπλούς τρόπους ταυτόχρονα. Η πιο συνηθισμένη τακτική είναι η εξαπόλυση επιχείρησης «ηλεκτρονικού ψαρέματος» (phishing) κατά των υπαλλήλων του παρόχου ηλεκτρικής ενέργειας, σε συνδυασμό με επιθέσεις με σκοπό την ανάπτυξη κακόβουλου λογισμικού (malware deployment) στα συστήματά του. Παράλληλα, δεν αποκλείεται και η εξαπόλυση επίθεσης κατανεμημένης άρνησης υπηρεσίας (DDoS) κατά των συστημάτων του παρόχου, ώστε να παρεμποδιστεί ο συντονισμός της άμυνάς του. Μάλιστα, έχει παρατηρηθεί και η διενέργεια επιθέσεων άρνησης εξυπηρέτησης τηλεφωνίας (Telephony Denial of Service attacks) στον προσβληθέντα πάροχο ηλεκτρικής ενέργειας, ώστε οι χρήστες του να αδυνατούν να αναφέρουν τη βλάβη που επέφερε η επίθεση. Το περιστατικό αυτό σημειώθηκε στις 23 Δεκεμβρίου 2015, όταν η ομάδα χάκερ με την ονομασία «Sandworm», στην υπηρεσία της Ρωσικής Ομοσπονδίας, εξαπέλυσε επίθεση κατά των συστημάτων του παρόχου ηλεκτρικής ενέργειας με την επωνυμία «Prykarpattyaoblenergo» (wired.com,2016).

Η δεύτερη κατηγορία επιθέσεων κατά κρίσιμων υποδομών είναι οι επιθέσεις στον τραπεζικό τομέα. Λόγω της στροφής στη χρήση πιστωτικών και χρεωστικών καρτών για την εκτέλεση καθημερινών συναλλαγών, όπως και της γενικότερης «στροφής» μακριά από το φυσικό χρήμα, ο επιτιθέμενος δύναται να προκαλέσει μεγάλη ζημιά στην οικονομία του στόχου, καθώς και πανικό στους πολίτες, προκαλώντας πτώση του ηθικού. Η κύρια μέθοδος διεξαγωγής τέτοιου είδους επιθέσεων είναι η εξαπόλυση επιθέσεων κατανεμημένης άρνησης εξυπηρέτησης κατά των εξυπηρετητών των τραπεζών-στόχων. Παράλληλα, ο επιτιθέμενος μπορεί να στοχοποιήσει το σύστημα ανταλλαγής τραπεζικών μηνυμάτων (banking instruction messaging) SWIFT (Society for Worldwide Interbank Financial Telecommunication), ώστε να διακόψει τη διενέργεια διατραπεζικών συναλλαγών ή να χρησιμοποιήσει το περιεχόμενο των μηνυμάτων, τα οποία περιέχουν οδηγίες πληρωμής, αριθμούς λογαριασμών και κυρίως token

εξουσιοδότησης, ώστε να αποσπάσει χρηματικά ποσά. Οι επιθέσεις κατά του συστήματος SWIFT συνδέονται άρρηκτα με τις επιθέσεις κατά τραπεζών, καθώς ο επιτιθέμενος πρέπει να έχει αποκτήσει πρόσβαση στα διαπιστευτήρια μιας τράπεζας-μέλους του δικτύου SWIFT ώστε να προβεί σε επίθεση. Ένα τέτοιο παράδειγμα είναι οι κυβερνο-επιθέσεις από Βορειοκορεατική ομάδα χάκερ με την ονομασία APT 38, οι οποίοι κατάφεραν να παραβιάσουν τα συστήματα τραπεζών-μελών του συστήματος SWIFT, ειδικότερα την Κεντρική Τράπεζα του Μπαγκλαντές, την Κεντρική Τράπεζα του Βιετνάμ, και την τράπεζα με την επωνυμία «Banco del Austro» στο Εκουαδόρ, εκδίδοντας πλαστές εντολές συναλλαγών, τις οποίες απέστειλαν μέσω του συστήματος SWIFT, αποσπώντας τεράστια χρηματικά ποσά (BBC, 2021).

Η τρίτη μορφή επιθέσεων κατά κρίσιμων υποδομών είναι οι επιθέσεις στον τομέα των υποδομών οργανισμών κοινής ωφέλειας, όπως παρόχων υδροδότησης. Τέτοιου είδους επιθέσεις διαφέρουν ουσιωδώς από τις επιθέσεις κατά παρόχων ηλεκτρικής ενέργειας, καθώς είναι πολύ πιο στοχευμένες και εκλείπει το πολυεπίπεδο στοιχείο, λόγω της μειωμένης πολυπλοκότητας του στόχου. Ειδικότερα, στην πράξη έχει αποδειχθεί ότι αρκεί η επίθεση στα συστήματα βιομηχανικού ελέγχου (industrial control systems) των παρόχων υδροδότησης, ώστε ο επιτιθέμενος να λάβει τον πλήρη έλεγχό της, λόγω της δομής των συστημάτων υδροδότησης, η οποία παρουσιάζει μοναδικό σημείο αποτυχίας (single point of failure) στο σύνδεσμο μεταξύ των συστημάτων βιομηχανικού ελέγχου και των συστημάτων ελέγχου και διοίκησης που τους αντιστοιχούν. Ένα πρόσφατο παράδειγμα τέτοιου σημείου αποτυχίας είναι η επίθεση κατά του εθνικού παρόχου υδροδότησης του Ισραήλ το 2020, κατά την οποία άγνωστοι χάκερ εκμεταλλευόμενοι την αδυναμία αυτή κατάφεραν να αποκτήσουν τον έλεγχο πέντε σταθμών υδροδότησης και σχεδόν κατάφεραν να αυξήσουν το επίπεδο χλωρίου στις δεξαμενές σε βλαπτικά για τον άνθρωπο επίπεδα, πριν η επίθεση αποκρουστεί, μόνο όμως μετά από φυσική επέμβαση στα συστήματα ελέγχου (Wall, 2022).

Η τέταρτη κατηγορία επιθέσεων κατά κρίσιμων υποδομών είναι οι διεξαγωγή επιχειρήσεων κατά του τομέα των μεταφορών. Ο τομέας των μεταφορών, όπως και ο τομέας της ενέργειας, παρουσιάζει μεγάλο βαθμό αλληλεξάρτησης μεταξύ των στοιχείων που τον αποτελούν (π.χ. συστήματα κράτησης θέσεων, συστήματα διοίκησης), καθώς και υψηλό βαθμό τεχνολογικής ενσωμάτωσης. Ο επιτιθέμενος εκμεταλλεύεται την αποκεντρωμένη φύση των συστημάτων διοίκησης και ελέγχου μεταφορών, η οποία συνεπάγεται και την ύπαρξη πολλαπλών σημείων αποτυχίας, ώστε να τα θέσει εκτός λειτουργίας, παρεμποδίζοντας τη διενέργεια μεταφορών. Κύριοι τρόποι επίθεσης είναι οι επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης κατά των ιστοσελίδων κράτησης θέσεων και έκδοσης εισιτηρίων και οι επιθέσεις ransomware κατά συστημάτων ελέγχου και διοίκησης (command and control systems), όπως συστήματα διαχείρισης ωρολογίων προγραμμάτων (timetable management systems), συστήματα καταγραφής και διαχείρισης εμπορευμάτων (inventory management systems) και συστήματα ανταλλαγής πληροφοριών φορτίου (manifest management systems). Η έμφαση στην ασφάλεια που χαρακτηρίζει τον τομέα των μεταφορών λειτουργεί υπέρ του επιτιθέμενου, καθώς οι ιθύνοντες προχωρούν σε αναστολή μεταφορών, είτε επιβατών είτε φορτίου, μέχρι να αποκατασταθεί η βλάβη. Παράδειγμα τέτοιας επίθεσης είναι οι

αλλεπάλληλες επιθέσεις κατά αεροδρομίων, αεροπορικών εταιρειών, λιμανιών και σιδηροδρόμων από τη Ρωσική Ομοσπονδία κατά διαφόρων χωρών ανά την Ευρώπη από την έναρξη της Ρωσικής εισβολής στην Ουκρανία (CyberPeace Institute,2023).

Πέμπτη και τελευταία κατηγορία επιθέσεων κατά κρίσιμων υποδομών είναι οι επιθέσεις που στρέφονται κατά των τηλεπικοινωνιών του κράτους-στόχου. Ο τομέας των τηλεπικοινωνιών αποτελεί έναν πολύ «ελκυστικό» στόχο, λόγω της χαώδους, φύσης του. Αρχικά, ο τομέας των τηλεπικοινωνιών παρουσιάζει σχεδόν απόλυτο βαθμό διασυνδεσιμότητας (inter-connectivity) μεταξύ των στοιχείων που τον αποτελούν, ιδίως των δικτύων των διάφορων παρόχων, πράγμα που σημαίνει ότι ο επιτιθέμενος δε χρειάζεται να καταβάλει ιδιαίτερα μεγάλη προσπάθεια ώστε να προκαλέσει σοβαρές βλάβες, καθώς η υψηλή διασυνδεσιμότητα είναι αλληλένδετη με την αλληλεξάρτηση μεταξύ των υποδομών, αφού οι τηλεπικοινωνίες αποτελούν τον κύριο δίαυλο πρόσβασης στα λοιπά συστήματα-στόχους του κράτους-στόχου. Δεύτερον, ο εξοπλισμός τηλεπικοινωνιών χαρακτηρίζεται από μακροζωία, γεγονός που τον καθιστά ευάλωτο σε επιθέσεις όσο περνούν τα χρόνια, καθώς εντοπίζονται τα ευάλωτά του σημεία. Η κατάσταση αυτή ενισχύεται από την αρχή της συμβατότητας που διέπει τις τηλεπικοινωνίες, σύμφωνα με την οποία ο εξοπλισμός των παρόχων θα πρέπει να μπορεί να εξυπηρετήσει και αρκετά παλαιότερες συσκευές, με το πλέον τρανταχτό παράδειγμα τη δυνατότητα χρήσης κινητών τηλεφώνων τεχνολογίας 2G σήμερα, η οποία έχει ξεπεράσει εικοσαετία ζωής, με ότι αυτό συνεπάγεται αναφορικά με τα κενά ασφαλείας που δημιουργεί η χρήση πεπαλαιωμένου εξοπλισμού με ήδη γνωστές αδυναμίες. Τρίτον, η ραγδαία τεχνολογική εξέλιξη σε συνδυασμό με την ώθηση που δίνεται από τις κυβερνήσεις για μετάβαση σε νέες τεχνολογίες τηλεπικοινωνιών, όπως είναι το 5G, δημιουργεί μοναδικές προκλήσεις ασφαλείας, καθώς είναι αδύνατο να ελεγχθεί ο νέος αυτός εξοπλισμός για κενά ασφαλείας τηρώντας ταυτόχρονα τα ασφυκτικά κυβερνητικά (στην περίπτωση της Ελλάδας και Ενωσιακά) χρονοδιαγράμματα, με αποτέλεσμα να αυξάνεται ο κίνδυνος ασφαλείας, ενώ δημιουργείται πρόσφορο έδαφος για επιθέσεις στην εφοδιαστική αλυσίδα. Τέλος, οι πάροχοι τηλεπικοινωνιών αποθηκεύουν ευαίσθητες πληροφορίες των συνδρομητών τους, όπως είναι τα προσωπικά και οικονομικά τους στοιχεία, συνεπώς μια επίθεση θα μπορούσε να εκθέσει άτομα ενδιαφέροντος (persons of interest) για τον επιτιθέμενο, βοηθώντας τον να επιτεθεί απευθείας σε αυτά.

Η πιο δύσκολη μέθοδος διεξαγωγής κυβερνοπολέμου είναι η διανομή παραβιασμένου τεχνολογικού υλικού, η οποία εντάσσεται στις ευρύτερη κατηγορία επιθέσεων κατά υλικού (attacks on hardware). Οι επιθέσεις κατά υλικού λαμβάνουν δυο διακριτές μορφές: α) επίθεση στην εφοδιαστική αλυσίδα του υλικού (supply chain attack) και β) επιχειρήσεις με σκοπό την καταστροφή υλικού προς στέρηση ικανότητας στον αντίπαλο. Οι επιθέσεις κατά της εφοδιαστικής αλυσίδας του υλικού έχουν άκρως μυστικό χαρακτήρα και έχουν ως κύριο στόχο την αναχαίτησή του πριν φτάσει στα χέρια του αντιπάλου (interception) και επικουρικά τη διευκόλυνση της διανομής του παραβιασμένου τεχνολογικού υλικού. Πρέπει να σημειωθεί ότι μορφή επίθεσης αναχαίτισης δύναται να αποτελέσει και η επιβολή

περιορισμών εισαγωγής ή εξαγωγής συγκεκριμένου τεχνολογικού υλικού προς μη φιλικά προσκείμενα στον επιβάλλοντα κράτη, οι λεγόμενες «κυβερνο-κυρώσεις» (cyber sanctions).

Όσον αφορά το ίδιο το παραβιασμένο τεχνολογικό υλικό, αυτό, πέρα από το διαχωρισμό σε υλικό παρακολούθησης και υλικό επίθεσης που εκθέσαμε στην εισαγωγή, διαχωρίζεται και σε «υλικό μίμησης» (dummy hardware/software) και «λειτουργικό υλικό» (functional hardware). Το «υλικό μίμησης» διαφέρει κατά ουσιαστικό τρόπο από το αντίστοιχο πραγματικό, καθώς δεν δύναται να χρησιμοποιηθεί με τον ίδιο τρόπο, καθώς έχει εντελώς διαφορετική λειτουργία. Το κλασσικότερο παράδειγμα «υλικού μίμησης» είναι τα «κατασκοπευτικά chip» (spy chips) που αναπτύσσονται κατά καιρούς σε υλικό υπολογιστών, κυρίως μητρικές πλακέτες, από τις υπερδυνάμεις. Τα chips αυτά, τα οποία «πλεονάζουν» του σχεδίου του μολυσμένου συστήματος, φαινομενικά εκτελούν «αθώες» λειτουργίες, για παράδειγμα έλεγχο της τάσης του ρεύματος ή έλεγχο ζωτικών σημείων του συστήματος, στην πραγματικότητα υποκρύπτουν εντελώς διαφορετικές λειτουργίες, οι οποίες κυμαίνονται από απλή αναπαραγωγή της δραστηριότητας του προσβεβλημένου συστήματος μέχρι και τη λήψη απομακρυσμένου ελέγχου (Donohoe, 2023).

Το «λειτουργικό υλικό» δεν διαφέρει καθόλου από το αντίστοιχο πραγματικό και μπορεί να εκτελέσει όλες τις λειτουργίες του πραγματικού υλικού παράλληλα με τη διεξαγωγή επίθεσης. Τέτοιου είδους υλικό είναι πρακτικά αδύνατο να εντοπιστεί πριν τη χρήση του από αυτόν που δέχεται την επίθεση, ενώ σε πολλές περιπτώσεις είναι αδύνατο να εντοπιστεί και κατά τη χρήση του. Η πιο διαδεδομένη μέθοδος διεξαγωγής της επίθεσης αυτής είναι το backdoor, το οποίο κατηγοριοποιείται σε hardware backdoor και software backdoor. Οι επιθέσεις hardware backdoor εκτελούνται με την τροποποίηση του ενσωματωμένου κυκλώματος (chip), ώστε αυτό να μπορεί να χρησιμοποιηθεί για τη διενέργεια κυβερνοπολέμου. Κύριο χαρακτηριστικό τους είναι η πληθώρα εφαρμογών τους, καθώς οποιοδήποτε παράδειγμα υπολογιστικού υλικού (hardware) είναι δυνατό να «χτυπηθεί», γεγονός που επιτρέπει στον επιτιθέμενο να παρακάμψει τα όποια μέτρα ασφαλείας του στόχου, καθώς εξ ορισμού αυτά επικεντρώνονται στις διεργασίες των εσωτερικών εξαρτημάτων (internal components) του υπολογιστικού συστήματος, οπότε μια τέτοια επίθεση εκτελούμενη μέσω των περιφερειακών του εν λόγω υπολογιστικού συστήματος απαιτεί πλήρη αναδιαμόρφωση της στρατηγικής ασφαλείας (security strategy) του αμυνόμενου καθώς και την επένδυση σημαντικών πόρων από μέρους του. Παράδειγμα τέτοιου είδους επίθεσης είναι η εισαγωγή στο χώρο του στόχου ενός πληκτρολογίου υπολογιστή με τροποποιημένα chips, το οποίο καταγράφει κάθε πληκτρολόγηση.

Οι επιθέσεις software backdoor εκτελούνται χρησιμοποιώντας έναν πόρο λογισμικού (software resource) αναπτυγμένο εντός λογισμικού, το οποίο είτε προϋπάρχει της εγκατάστασης του εν λόγω λογισμικού στο σύστημα του στόχου είτε εγκαθίσταται εκ των υστέρων από τον επιτιθέμενο. Στόχος των επιθέσεων αυτών είναι κυρίως η εξαγωγή δεδομένων και η επίτευξη ελέγχου επί του συστήματος του στόχου.

Οι κύριες μορφές των επιθέσεων αυτών είναι τα system backdoors, τα application backdoors και τα cryptographic backdoors (Wysopal, Eng, 2006). Οι επιθέσεις τύπου system backdoors δίνουν στον επιτιθέμενο πρόσβαση στο σύστημα του στόχου σε διάφορα επίπεδα (πρόσβαση σε επίπεδο διεργασιών, πρόσβαση στον αποθηκευτικό χώρο), ανάλογα με την πολυπλοκότητά τους. Να σημειωθεί ότι ως system backdoor θεωρούνται και οι ενέργειες οι οποίες ναι μεν εμπίπτουν στην «κανονική» λειτουργία του συστήματος του στόχου, αλλά εκτελούνται από τον επιτιθέμενο προς προώθηση των σκοπών του (deliberate system mis-configuration), χωρίς να απαιτείται τροποποιημένο λογισμικό-κομιστής επίθεσης (vector of attack). Το πιο σύνηθες παράδειγμα τέτοιας επίθεσης είναι η αλλαγή των ρυθμίσεων ασφαλείας του συστήματος-στόχου από τον επιτιθέμενο ώστε να γίνει δεκτικό απομακρυσμένης πρόσβασης (remote desktop hijacking). Τα application backdoors διαφέρουν εντελώς διαμετρικά από τα system backdoors, καθώς το «όχημα επίθεσης» (vector of attack) είναι μια κατά τα άλλα πλήρως λειτουργική εγκατάσταση ενός λογισμικού. Ο επιτιθέμενος «διοχετεύει» τον κώδικά του στην εν λόγω εγκατάσταση-διανομή του λογισμικού-κομιστή επίθεσης, είτε νόμιμα, σε περίπτωση που το backdoor δημιουργείται από τον προγραμματιστή ανάπτυξης του λογισμικού, είτε παράνομα, σε περίπτωση που ο επιτιθέμενος έχει καταφέρει να αποκτήσει πρόσβαση στον πηγαίο κώδικα (source code) ή τα δυαδικά αρχεία (binaries) του εν λόγω λογισμικού μέσω άλλης ενέργειας κυβερνοπολέμου. Τα cryptographic backdoors συνίστανται σε ηθελημένες «αδυναμίες» ενός συστήματος κρυπτογράφησης, οι οποίες επιτρέπουν στον επιτιθέμενο να το παρακάμψει και να αποκτήσει πρόσβαση στα δεδομένα στα οποία αυτό εφαρμόζεται. Η ειδοποιός διαφορά των cryptographic backdoors από τις άλλες μορφές backdoor είναι το γεγονός ότι αυτά δεν έχουν «παραδοσιακό» όχημα επίθεσης, καθώς δε μπορεί να διασφαλιστεί ότι ο στόχος χρησιμοποιεί το προσβεβλημένο σύστημα κρυπτογράφησης. Προκειμένου να πετύχει το στόχο του ο επιτιθέμενος θα αναγκαστεί να πραγματοποιήσει υποστηρικτικές ενέργειες (supporting actions), ώστε ο στόχος να «πειστεί» να υιοθετήσει το εν λόγω κρυπτογραφικό σύστημα, όπως η διενέργεια επιθέσεων κοινωνικής μηχανικής (social engineering) σε «αδύναμους κρίκους» της οργανογραμματικής αλυσίδας του στόχου. Όπως είναι φυσικό, η προσέγγιση αυτή δεν είναι πάντα επιτυχής, ειδικά αν ο στόχος είναι κρατική δομή (state actor), όπου είναι σίγουρο ότι τηρείται πρωτόκολλο εναρμόνισης των συστημάτων κρυπτογράφησης. Οι δημιουργοί των cryptographic backdoors, γνωρίζοντας τα ανωτέρω, στοχεύουν πλέον στην ανάπτυξη «ανοιχτών» κρυπτογραφικών συστημάτων, τα οποία παρουσιάζουν χαρακτηριστικά τυποποίησης (standardisation) με σκοπό την υιοθέτησή τους από όσους περισσότερους χρήστες ή προγραμματιστές ανάπτυξης εφαρμογών ή κατασκευαστές υπολογιστικού υλικού γίνεται. Από τα ανωτέρω εμφαίνεται ότι τα cryptographic backdoors είναι δύσκολο να τύχουν πρακτικής εφαρμογής όσον αφορά τη διενέργεια κυβερνοπολέμου, καθώς δύνανται να χρησιμοποιηθούν μόνο σε μη σκληρυμένους στόχους (non-hardened targets), οι οποίοι δεν υπακούν σε πρωτόκολλα εναρμόνισης, όπως χαμηλού επιπέδου συστήματα (non-privileged systems), ή ιστοσελίδες (προκειμένου να ακολουθήσει επίθεση κυβερνο-βανδαλισμού).

Δ.2 Αντίμετρα

Αν και πρόκειται για μία πολύ δύσκολη κατάσταση να αντιμετωπιστεί, λόγω του γεγονότος ότι το Διαδίκτυο είναι αχανές, αλλά και λόγω άλλων παραγόντων που αναλύσαμε παραπάνω, ωστόσο υπάρχουν αντίμετρα κυβερνοπολέμου. Κατά συνέπεια, χρειάζεται σωστός χειρισμός για τη σωστή αντιμετώπιση τέτοιων θεμάτων, σύμφωνα με ανάλογες στρατηγικές και στόχους, έτσι ώστε να δημιουργηθεί ένα σαφές λειτουργικό πλαίσιο ασφάλειας.

Προληπτικά, χρειάζεται να ληφθούν υπόψη ισχυρά πρωτόκολλα κυβερνοασφάλειας (Εγχειρίδιο Κυβερνοασφάλειας, Υπουργείο Ψηφιακής Διακυβέρνησης). Η δημιουργία ολοκληρωμένων πρωτοκόλλων κυβερνοασφάλειας είναι ζωτικής σημασίας. Αυτό περιλαμβάνει τη ρύθμιση ισχυρών ελέγχων πρόσβασης, την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων και τη διασφάλιση τακτικών ελέγχων και αξιολογήσεων ασφαλείας. Επιπλέον, είναι πολύ σημαντικό να τηρούνται οι τακτικές ενημερώσεις λογισμικού. Η διατήρηση του λογισμικού και των συστημάτων ενημερωμένα είναι ζωτικής σημασίας για την προστασία από γνωστά τρωτά σημεία. Αυτό περιλαμβάνει την έγκαιρη επιδιόρθωση των ελαττωμάτων ασφαλείας και την ενημέρωση λογισμικού προστασίας από ιούς και κακόβουλου λογισμικού.

Κρίσιμης σημασίας είναι η χρήση προηγμένων εργαλείων κυβερνοασφάλειας. Η χρήση εργαλείων κυβερνοασφάλειας τελευταίας τεχνολογίας είναι απαραίτητη. Τα τείχη προστασίας παρέχουν μια πρώτη γραμμή άμυνας έναντι μη εξουσιοδοτημένης πρόσβασης, ενώ τα συστήματα ανίχνευσης εισβολής βοηθούν στην παρακολούθηση και ανάλυση της κυκλοφορίας του δικτύου για ύποπτες δραστηριότητες.

Η κρυπτογράφηση είναι κρίσιμης σημασίας διαδικασία για την προστασία της ακεραιότητας και του απορρήτου των δεδομένων, τόσο κατά τη μεταφορά όσο και σε κατάσταση ηρεμίας. Ανάμεσα στις στρατηγικές απόκρισης εμπεριέχονται τα σχέδια Αντιμετώπισης Συμβάντων. Η ανάπτυξη και η διατήρηση ολοκληρωμένων σχεδίων αντιμετώπισης συμβάντων επιτρέπει στους οργανισμούς να αντιμετωπίζουν γρήγορα και αποτελεσματικά τις απειλές στον κυβερνοχώρο. Αυτά τα σχέδια θα πρέπει να περιγράφουν τους ρόλους, τις ευθύνες και τις διαδικασίες για την απόκριση σε περιστατικά στον κυβερνοχώρο.

Η ταχεία αναγνώριση και εξουδετέρωση απειλών αποτελεί ίσως το μεγαλύτερο πλεονέκτημα που μπορεί να αποκτήσει ο επιτιθέμενος. Η ικανότητα γρήγορης αναγνώρισης και εξουδετέρωσης απειλών είναι κρίσιμη. Αυτό περιλαμβάνει την ύπαρξη αποκλειστικών ομάδων κυβερνοασφάλειας και εξελιγμένων συστημάτων ανίχνευσης για τον εντοπισμό ανωμαλιών και πιθανών παραβιάσεων.

Η ανίχνευση είναι σημαντικό να γίνεται έγκαιρα, ώστε να υπάρχει ο χρόνος να αναχαιριστεί οποιαδήποτε κακόβουλη ενέργεια. Σε αυτό το σημείο πρέπει να σημειωθεί ότι ο επιτιθέμενος μπορεί να χρησιμοποιεί πολλά μολυσμένα λογισμικά ή τα λεγόμενα bots. Αν και αυτές οι πράξεις είναι δύσκολο να εντοπιστούν διότι τα δεδομένα μπορεί να προέρχονται από πολλές και διαφορετικές τοποθεσίες, ωστόσο είναι απαραίτητο να υπάρχουν τα ανάλογα όργανα ώστε κάτι τέτοιο να γίνεται αντιληπτό από

την αρχή. Κι αυτό διότι πολλές τέτοιες επιθέσεις μπορεί να ξεκινούν σχετικά με σιγανό ρυθμό και σταδιακά να προχωρούν προς το στόχο τους. Έτσι, η ΕΕ δίνει ιδιαίτερη βαρύτητα σε θέματα καινοτομίας και έρευνα, αλλά και σε όλα τα σχετικά ψηφιακά εργαλεία που μπορούν να προβλέψουν και να αντιμετωπίσουν καλύτερα τέτοιους κινδύνους, όπως είναι οι υβριδικές απειλές. (Lehne, 2016) Η γνώση και η πληροφόρηση σχετικά με τους κινδύνους που ανακύπτουν από το κυβερνοέγκλημα μπορούν να λειτουργήσουν υπέρ των ατόμων και των κοινοτήτων, και είναι ένα θέμα που προάγεται από την ΕΕ. (Missiroli, 2015)

Η επαναφορά σε ασφαλές περιβάλλον όλων των δικτύων που έχουν πληγεί είναι ένας εξίσου σημαντικός παράγοντας για τον οποίον μεριμνά η ΕΕ. (McClure et al., 2009) Ο αμυνόμενος είναι βασικό να πάρει τις αναγκαίες προφυλάξεις, όπως για παράδειγμα να προστατέψει τον άμαχο πληθυσμό, ειδικά όταν πρόκειται να «χτυπηθούν» κάποιες υποδομές.

Οι μεγάλες δυνατότητες του συνδυασμού IoT με το Cloud δημιουργούν λύσεις για την απόδοση, την ευελιξία, την σταθερότητα, αλλά και την ανοχή σφαλμάτων. Σε αυτό το πλαίσιο αναπτύσσονται τα Κυβερνοφυσικά Συστήματα CPS (Cyper Physical System). Φυσικά αλλά και ψηφιακά συστήματα επικοινωνούν μεταξύ τους, καταγράφοντας πληροφορίες, που εξασφαλίζουν την ορθή αλλά και ευφυή λειτουργία τους. Για να γίνει αυτό εφικτό, τα CPS αξιοποιούν αισθητήρες επικοινωνίας για να ικανοποιήσουν τις εκάστοτε ανάγκες και απαιτήσεις. Αυτά τα συστήματα είναι τα λεγόμενα SCADA, που έχουν ως άμεση ευθύνη την παρακολούθηση διαδικασιών με την εφαρμογή κατάλληλων ελέγχων. Με τον όρο SCADA περιγράφεται μια κατηγορία συστημάτων αυτομάτου βιομηχανικού ελέγχου και τηλεμετρίας. Το χαρακτηριστικό των συστημάτων SCADA είναι ότι αποτελούνται από τοπικούς ελεγκτές, που ελέγχουν επιμέρους στοιχεία και μονάδες μιας εγκατάστασης, συνδεδεμένους σε ένα κεντρικό τερματικό.

Η δημιουργία ανθεκτικών συστημάτων που μπορούν να αντέξουν τις επιθέσεις είναι το κλειδί. Αυτό περιλαμβάνει το σχεδιασμό συστημάτων με πλεονασμό και ασφάλειες αστοχίας για να διασφαλιστεί η συνεχής λειτουργία κατά τη διάρκεια μιας επίθεσης. Τα αντίγραφα ασφαλείας που ενημερώνονται τακτικά είναι απαραίτητα για την ανάκτηση μετά από μια επίθεση. Αυτά τα αντίγραφα ασφαλείας θα πρέπει να αποθηκεύονται με ασφάλεια και να ελέγχονται συχνά για να διασφαλίζεται ότι μπορούν να αποκατασταθούν αποτελεσματικά. Αναντίρρητα, χρειάζονται πάντα σχέδια αποκατάστασης από καταστροφές. Η ύπαρξη ενός καλά προετοιμασμένου σχεδίου αποκατάστασης από καταστροφές επιτρέπει τη γρήγορη αποκατάσταση των υπηρεσιών και ελαχιστοποιεί το χρόνο διακοπής λειτουργίας. Αυτό το σχέδιο θα πρέπει να ενημερώνεται τακτικά και να δοκιμάζεται για να διασφαλίζεται η αποτελεσματικότητά του σε διάφορα σενάρια.

Ο αποτελεσματικός τρόπος αντιμετώπισης των ζητημάτων ασφαλείας ενός δικτύου, για το πόσο ευάλωτο είναι στις επιθέσεις, εξαρτάται από την ανθεκτικότητα του. Τα μοντέλα αντιπάλων περιγράφουν τους στόχους επίθεσης και τις οικονομικές τους επιπτώσεις. Για τον βέλτιστο χειρισμό τους,

κύριος παράγοντας είναι η τεχνική συστημάτων ασφαλείας που ορίζει τους κινδύνους σε κόμβους αναφοράς σε ένα δίκτυο. Προκειμένου να οριστεί η τεχνική συστημάτων ασφαλείας, είναι σημαντικό να αναγνωριστούν οι ιδιότητες του συστήματος, καθώς επίσης και να αναλυθούν οι επιπτώσεις οι οποίες θα βοηθήσουν στο να ληφθούν κατάλληλα μέτρα μετριασμού των κινδύνων στους κόμβους αναφοράς.

Η συνεχής παρακολούθηση των δραστηριοτήτων στον κυβερνοχώρο είναι απαραίτητη για την έγκαιρη ανίχνευση και απάντηση σε απειλές. Αυτό περιλαμβάνει την ανάλυση της κυκλοφορίας του δικτύου, των αρχείων καταγραφής συστήματος και άλλων πηγών δεδομένων για δείκτες συμβιβασμού.

Οι τακτικές αξιολογήσεις ευπάθειας και οι δοκιμές διείσδυσης βοηθούν στον εντοπισμό αδυναμιών στο σύστημα που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς.

Εξίσου σημαντικό είναι να πραγματοποιούνται τακτικές ασκήσεις και εκπαίδευση, οι οποίες αποτελούν διαχρονικό αντίμετρο του κυβερνοπολέμου. Η διεξαγωγή τακτικών ασκήσεων και εκπαιδευτικών συνεδριών διασφαλίζει ότι οι ομάδες απόκρισης είναι προετοιμασμένες και ενήμερες για τις διαδικασίες που πρέπει να ακολουθήσουν κατά τη διάρκεια ενός πραγματικού περιστατικού στον κυβερνοχώρο.

Η συμμετοχή σε πλατφόρμες κοινής χρήσης πληροφοριών απειλών επιτρέπει την ανταλλαγή πληροφοριών σχετικά με αναδυόμενες απειλές και τρωτά σημεία. Η κοινή χρήση πληροφοριών σχετικά με απειλές, τρωτά σημεία και βέλτιστες πρακτικές με άλλα έθνη και οργανισμούς ενισχύει τη στάση της συλλογικής ασφάλειας στον κυβερνοχώρο.

Η συνεργασία σε αμυντικές στρατηγικές και κοινές ασκήσεις με διεθνείς εταίρους μπορεί να βελτιώσει την ετοιμότητα και τις ικανότητες αντίδρασης. Η προσπάθεια για την εναρμόνιση των νομικών και κανονιστικών πλαισίων διασφαλίζει μια συνεκτική προσέγγιση για την αντιμετώπιση των απειλών στον κυβερνοχώρο διασυνοριακά.

Πιο αναλυτικά, υπάρχουν οδηγίες και σχετικοί κανόνες σχετικά με την κυβερνοασφάλεια, που εντάσσονται μέσα στη Γενική Στρατηγική της ΕΕ, για την περίοδο 2020-2025, η οποία δημοσιεύθηκε τον Ιούλιο του 2020. Πρέπει να αναφερθεί ότι ήδη από το 2013, η ΕΕ έχει προχωρήσει σε ανάλογες ενέργειες ώστε ο κυβερνοχώρος να διέπεται από ασφάλεια και ως προς αυτό το στοιχείο εισηγήθηκαν διάφορες προτάσεις, ώστε να ληφθούν σαφή βήματα για μείωση του εγκλήματος, για ενίσχυση της ανθεκτικότητας, για ανάπτυξη ανάλογων πολιτικών, αλλά και για καθιέρωση μιας συγκεκριμένης πολιτικής που θα ακολουθείτο από όλα τα κράτη-μέλη.

Ένα από τα βασικά σημεία της ΕΕ ως προς αυτά τα στοιχεία είναι η Οδηγία 2016/1148 για ανεπτυγμένο επίπεδο ασφάλειας όσον αφορά θέματα πληροφορίας στον κυβερνοχώρο (NIS Directive), που ισχύει από εκείνη τη χρονιά (2016). Σύμφωνα με την Οδηγία αυτή τα κράτη πρέπει να συνεργάζονται μεταξύ τους, να προάγουν την εμπιστοσύνη και την ανταλλαγή στοιχείων για την καλύτερη αντιμετώπιση αυτών των θεμάτων. (European Commission, 2013) Πάνω σε αυτή την Οδηγία έχουν προταθεί να γίνει κάποιες αλλαγές, έτσι ώστε να γίνει πιο ισχυρή η ανθεκτικότητα των δικτύων σε έναν κυβερνοπόλεμο.

Υπό αυτή την έννοια, η αναθεώρηση της συγκεκριμένης Οδηγίας μπορεί να δώσει νέες δυνατότητες, αλλά και μεγαλύτερη ασφάλεια σε διάφορους τομείς, όπως άλλωστε ανακοινώθηκε και στο πλαίσιο της στρατηγικής για την Ένωση Ασφάλειας 2020-2025, συγχρόνως όμως κρίνεται απαραίτητα να επαναξεταστούν και όλα τα στοιχεία γύρω από τη νομοθεσία.

Ο καλύτερος τρόπος για να μειωθούν τέτοιοι κίνδυνοι είναι να ενισχυθεί ο τομέας της πρόληψης. Κάτι που θα μπορέσει τουλάχιστον να μετριάσει τους κινδύνους, όπως για παράδειγμα να υπάρχει ο κατάλληλος έλεγχος, καθώς και το ανάλογο φιλτράρισμα διάφορων στοιχείων και πληροφοριών, καθώς φυσικά και η αυθεντικοποίηση των δρώντων στο χώρο του Διαδικτύου. Πάνω σε αυτό, ωστόσο, όπως αναφέρει ο Shostack (2014) πρέπει να δίνεται ιδιαίτερη προσοχή μεταξύ έγκρισης πρόσβασης και αυθεντικοποίησης. (Shostack, 2014).

Παράλληλα, η ΕΕ επεξεργάζεται και άλλα στοιχεία και διευθετήσεις σχετικά με την ανθεκτικότητα, όπως σε διάφορα προϊόντα και προγράμματα περιήγησης. Η μείωση του εγκλήματος και διαχείριση κινδύνων είναι ένα από τα βασικά ζητήματα που προέτασε η ΕΕ από το 2013 ήταν η ευαισθητοποίηση των ατόμων των κρατών-μελών, κι αυτό διότι ο μέσος χρήστης έχει σημαντικό ρόλο στην ασφάλεια των δικτύων. Κατά συνέπεια, ο χρήστης πρέπει να είναι ενήμερος για τους κινδύνους που διατρέχει, ώστε να προσπαθεί όσον αυτό είναι εφικτό να προφυλάσσεται ο ίδιος, καθώς και να προφυλάσσει τα προσωπικά του δεδομένα, όπως ταυτότητα, κωδικούς κ.λπ. Ένα βασικό στοιχείο, όπως αναφέρει ο Χαίδης είναι να γίνουν όλα εκείνα που είναι απαραίτητα, ώστε να αποτρέπεται ένα τέτοιο περιστατικό, όπως ο κυβερνοπόλεμος. (Χαίδης, 2012) Ωστόσο, πολλές φορές από πολλούς μελετητές, εγείρονται κάποια ερωτήματα, όπως για παράδειγμα, αν η αποτροπή μπορεί να βοηθήσει στον κυβερνοχώρο, όπως βοήθησε για παράδειγμα κατά τον ψυχρό πόλεμο. Γίνεται εύκολα αντιληπτό ότι ενώ υπάρχουν μέθοδοι αποτροπής αυτοί δεν είναι εύκολο να επιτευχθούν, κυρίως διότι είναι ήδη ενδεικτικές οι ελλείψεις και τα κενά που παρουσιάζει ο χώρος που εκτυλίσσεται ο κυβερνοπόλεμος (Χαίδης). Σε άλλα παραδείγματα στο πέρασμα της ιστορίας, η πυρηνική αποτροπή θεωρήθηκε ένα επιτυχές αποτελέσμα, που ήταν ορατό, διότι θα μπορούσαν να είχαν προκληθεί πολύ δυσάρεστες εκπλήξεις. Ωστόσο, οι επιπτώσεις ή οι οποιεσδήποτε συνέπειες από τις κυβερνοεπιθέσεις δεν μπορεί να είναι ορατές (Burton, 2018)

Η ΕΕ έχει προχωρήσει παράλληλα και θέματα αναθεωρήσεων για συστήματα πληροφορίας (που αφορούν την κυβερνοασφάλεια), ενώ πάνω στο θέμα αυτό έχει καθορίσει και βασικές προτεραιότητες για τις συνεχείς απειλές στον κόσμο. Ως προς αυτό, έχει επισημάνει και κάτι που σκοπεύει να κάνει στο μέλλον είναι η άμεση ανάγκη για δημιουργία μιας Κοινής Μονάδας Κυβερνοχώρου, που θα λειτουργεί κάτω από συγκεκριμένους διαρθρωμένους κανόνες και με συνεργασία. Παράλληλα, συνεχίζει να αναπτύσσει ένα δίκτυο πάνω σε καλές σχέσεις εταιρειών, σε διεθνές επίπεδο, για την καλύτερη

αντιμετώπιση τέτοιων δύσκολων θεμάτων. Έτσι προωθεί διάφορα ενωσιακά πρότυπα, μεταξύ των χωρών-μελών.

Επιπλέον, θέτει πιο αυστηρές απαιτήσεις από τις χώρες, σε θέματα κυρίως εποπτείας και εφαρμογής και, ως προς αυτό, έχει κάνει και άλλα βήματα για να ενισχύσει την αλληλοεπίδραση και συνεργασία των κρατών-μελών ώστε να ανταλλάσσουν σημαντικές πληροφορίες και στοιχεία για την κυβερνοασφάλεια. (ENISA) Πιο αναλυτικά διάφοροι τομείς όπως παραγωγή προϊόντων, ηλεκτρονικά είδη, διάφορες ταχυδρομικές και άλλες ψηφιακές υπηρεσίες υπόκεινται, πλέον, κάτω από πιο αυστηρούς και μεθοδικούς ελέγχους, έτσι ώστε να περιοριστούν σημαντικά κίνδυνοι στο διαδίκτυο. Επίσης, έχει κάνει και βήματα ώστε να ενισχύσει ψηφιακά και τον χρηματοοικονομικό τομέα, ώστε να είναι πιο ανθεκτικός και να προστατεύεται από τυχόν κυβερνοεπιθέσεις (DORA), ένας κανονισμός που έχει ήδη εγκριθεί εδώ και ένα χρόνο. Καθώς είναι ένας χώρος ο οποίος έχει πολλές συναλλαγές και αλληλοεπιδράσεις από το διαδίκτυο. Όπως τονίζει ο Ιγγλεζάκης (2023), ο σχετικός νόμος σχετίζεται με θέματα ψηφιακής ανθεκτικότητας του συγκεκριμένου κλάδου, υποχρεώνοντας επιχειρήσεις να μπορούν να ανταπεξέρχονται σε τυχόν προβλήματα και διαταραχές που αφορούν τις νέες ΤΠΕ. Πρέπει να σημειωθεί ότι οι κανόνες αυτοί ισχύουν για όλες τις υπηρεσίες αυτού του κλάδου, όπως εταιρείες επενδύσεων, τράπεζες κ.λπ. (Ιγγλεχάκης, 2023)

Επίσης πρέπει να υπάρχει και η ανάλογη διασφάλιση. Κάτι που μπορεί να προωθηθεί με τα ανάλογα «εργαλεία», τους τακτικούς και ενδελεχείς ελέγχους, με διάφορες στρατηγικές. Για παράδειγμα, η ΕΕ μεριμνά με σαφείς κανόνες για όλες αυτές και παράπλευρες απειλές, όπως για κακόβουλα λογισμικά, για κλοπή προσωπικών στοιχείων, ταυτοτήτων, ενώ προωθεί και θέματα για έρευνες όπως ψηφιακές σε σχέση με το Νόμο, όπως ζητήματα που αφορούν την τεχνητή νοημοσύνη, τρομοκρατία και άλλα παρόμοια. Ένα επίσης βασικό στοιχείο που προωθεί ως προς αυτό είναι η καλή συνεργασία για ανταλλαγή πληροφοριών και στοιχείων μεταξύ των κρατών, κάτι που μπορεί να βοηθήσει σημαντικά στην καλύτερη διασφάλιση εμπιστευτικών και άλλων στοιχείων.

Πρέπει να σημειωθεί ότι μελέτες που έχουν γίνει πάνω στο θέμα αυτό έχουν δείξει ότι η ισορροπία μεταξύ της ευκολίας πρόσβασης και άλλων στοιχείων για τον χρήση και παράλληλα η προστασία των πληροφοριών μπορούν να είναι τα βασικά στοιχεία για να ενισχυθούν σημαντικές στρατηγικές ασφάλειας για το διαδίκτυο. Η ασφάλεια όλων αυτών έχει άμεση σχέση επίσης με τα μέτρα που λαμβάνονται καθώς και με σχετικές αντιλήψεις των κοινωνιών. Πιο αναλυτικά, η στρατηγική της ασφάλειας θα πρέπει επίσης να καλύπτεται από μία σειρά από στοιχεία, όπως ελέγχους, νομικά και λειτουργικά θέματα κ.λπ. Τα είδη των στρατηγικών αυτών είναι τα λειτουργικά και τα τεχνικά συστήματα, τα δίκτυα υπολογιστών κ.λπ. Σύμφωνα με τους McClure et al. (2009) είναι βασικό να υπάρχει εμπιστευτικότητα, έτσι ώστε να μη μπορούν να συμβούν διάφορες ανεπιθύμητες ενέργειες (όπως αφαίρεση κάποιων στοιχείων) από άτομα που δεν έχουν κάποια σχετική εξουσιοδότηση. Παράλληλα,

όπως υποστηρίζει, είναι βασικό να ενδυναμωθούν και στοιχεία πρόσβασης, με τις σχετικές επαληθεύσεις στοιχείων, έτσι ώστε να αποτρέπεται κάποιο ατυχές γεγονός. (McClure et al., 2009) Πάνω σε αυτό το θέμα, ο Τσουραμάνης (2006) επισημαίνει ότι επίσης πρέπει να ισχύει και το θέμα της εμπιστευτικότητας, κάτι για το οποίο πρέπει να ενημερώνονται καλύτερα οι πολίτες, ώστε να μην αποκαλύπτουν τα στοιχεία τους σε τρίτους. Έτσι, η προσπέλαση σε ευαίσθητα στοιχεία, όπως για παράδειγμα σε λογαριασμούς τραπεζών, θα πρέπει να γίνεται μόνο από τα πρόσωπα που είναι εξουσιοδοτημένα. (Τσουραμάνης, 2006)

Συνοπτικά, η αποτελεσματική αντιμετώπιση του κυβερνοπολέμου απαιτεί μια ολοκληρωμένη στρατηγική που περιλαμβάνει προληπτικά μέτρα, δυνατότητες ταχείας αντίδρασης, ανθεκτικότητα και σχεδιασμό ανάκτησης, συνεχή ανάλυση πληροφοριών και απειλών καθώς και διεθνή συνεργασία. Καθένα από αυτά τα στοιχεία διαδραματίζει κρίσιμο ρόλο στη δημιουργία μιας ισχυρής άμυνας ενάντια στο εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο.

Κεφάλαιο Ε

Ε.1.: Η Περίπτωση της Ουκρανίας

Ένα από τα πιο πρόσφατα χαρακτηριστικά παραδείγματα κυβερνοεπίθεσης είναι η ψηφιακή επίθεση της Ρωσίας στην Ουκρανία, πριν εκδηλωθεί η στρατιωτική επίθεση. Σύμφωνα με στοιχεία, σε μία διάρκεια μεταξύ 2 μηνών, μεταξύ Φεβρουαρίου και Απριλίου του 2022, η Microsoft κατέγραψε 37 κυβερνοεπιθέσεις της πρώτης στη δεύτερη. (Newsroom, 2022) Πρέπει να επισημανθεί σε αυτό το σημείο ότι οι διαφορές μεταξύ των δύο αυτών πλευρών δεν είναι μία καινούργια υπόθεση, αλλά αφορά μία σύγκρουση που έχει ξεκινήσει εδώ και αρκετά χρόνια και πιο συγκεκριμένα τον Φεβρουάριο του 2014. Ενώ σήμερα ο πόλεμος αυτός έχει πάρει τεράστιες διαστάσεις, κυρίως λόγω του κυβερνοπολέμου και τις επιπτώσεις που έχει για το παρόν αλλά και για το μέλλον όχι μόνο της συγκεκριμένης χώρας, αλλά και για άλλες χώρες. Κι αυτό διότι ο κυβερνοπόλεμος μπορεί εύκολα να επεκταθεί και σε άλλες κοινωνίες ως απειλή για παράδειγμα προς τρίτες δυνάμεις, ώστε να μην αναμειχθούν.

Όσον αφορά στη συγκεκριμένη περίπτωση, ο κυβερνοπόλεμος απέναντι στην Ουκρανία αποτελεί μία από τις πιο σύγχρονες συγκρούσεις στην ιστορία με αυτόν τον τρόπο μέχρι σήμερα. Αξίζει να τονιστεί ότι έχουν καταγραφεί σημαντικές αυξήσεις σε κυβερνοεπιθέσεις ενάντια στην Ουκρανία. Εκτιμάται ότι οι κυβερνοεπιθέσεις σε αυτή την χώρα αυξήθηκαν κατά ένα ποσοστό της τάξεως του 196% ήδη από τις πρώτες μέρες της μάχης σε σύγκριση με το Φεβρουάριο του 2022. (Creative, 2023) Πριν ξεσπάσει ο πόλεμος, όπως τον γνωρίζουμε αυτή την εποχή, μεταξύ των δύο πλευρών είχε προηγηθεί κυβερνοπόλεμος, με μία σειρά από πλήγματα προς τον αντίπαλο που σχετίζονταν με επιθέσεις μέσω διαδικτύου, όπου χάκερς προωθούσαν κακόβουλα λογισμικά με πολλές και άσχημες συνέπειες. Πολλές από αυτές σχετίζονταν με παράλυση διαφόρων δημόσιων φορέων (κεντρικές τράπεζες, υπουργείο

Άμυνας, Κοινοβούλιο της χώρας κ.ά.), διακοπές ρεύματος, συνδέσεων και πληροφορίας όπου πολλές ιστοσελίδες σημαντικών υπουργείων και έρευνας δέχθηκαν μαζικές επιθέσεις, με πολλές συνέπειες, με αποτέλεσμα να διακοπή η λειτουργία του, ενώ η κατάσταση εκείνο το διάστημα για τη χώρα αυτή χαρακτηριζόταν από ένα χάος. Παράλληλα, ωστόσο, αυτή η κυβερνοεπίθεση προκάλεσε και μεγάλη ανησυχία και φόβο και σε αρκετά κράτη της Δύσης. Αναμφισβήτητα, ήδη από τότε γινόταν λόγος για έναν υβριδικό πόλεμο εναντίον της Ρωσίας, όπου σύμφωνα με το υπουργείο Ψηφιακής της Ανάπτυξης, μία μέρα μετά τις εκτιμήσεις της Microsoft, η ουκρανική πλευρά έκανε λόγο ότι πολλές υπηρεσίες της κυρίως δημόσιο φορέα επλήγησαν από τη χρήση κακόβουλου λογισμικό. Μια πρώτη τέτοια επίθεση έγινε το 2015, όπου χάκερς απείλησαν το ενεργειακό δίκτυο της χώρας, ενώ μόλις δύο χρόνια αργότερα εκτυλίχθηκε ένα ανάλογο περιστατικό, στο σιδηροδρομικό δίκτυο της Ουκρανίας. Παράλληλα την περίοδο εκείνη η Ρωσία είχε εξαπολύσει και έναν ιό με την ονομασία NotPetya, όπου ξέφυγε από την επικράτεια και τα σύνορα της Ουκρανίας, με αποτέλεσμα πολλές επιχειρήσεις στον κόσμο να χρειαστεί να ξοδέψουν πολλά λεφτά για να προστατευθούν. (Kathimerini.gr., 2023)

Ωστόσο πρέπει να σημειωθεί ότι αυτή δεν είναι η πρώτη φορά που κάτι τέτοιο λαμβάνει χώρα στην Ουκρανία. Σύμφωνα με άρθρο της efsyn (2023), το 2017 είχε συμβεί στη χώρα αυτή κάτι ανάλογο, όταν προκλήθηκαν ζημιές περίπου 10 δις δολαρίων από τον ιό με την ονομασία «NotPetya», στα δίκτυα της χώρας καταστρέφοντας παράλληλα πολλά δεδομένα. Στο πρόσφατο παρελθόν συνέβη κάτι ανάλογο. (efsyn., 2023)

Πρέπει να σημειωθεί ότι η Ρωσία πολλές φορές έχει χρησιμοποιήσει τέτοιους τρόπους όπως αναφέραμε και παραπάνω, για να αναστατώσει τους αντιπάλους της όπως συνέβη με τη Γεωργία το 2008 και σε άλλες περιπτώσεις. Η σχετικά πρόσφατη εισβολή στην Ουκρανία δημιούργησε μία μεγάλη αναστάτωση και στις υπηρεσίες της ΕΕ για θέματα ασφάλειας. Αν και όπως γράφεται το προσωπικό της ΕΕ είχε ειδοποιηθεί για μία ενδεχόμενη τέτοια κατάσταση, ο ανάλογος οργανισμός της, ο ENISA εξέδωσαν μία σειρά από προειδοποιήσεις για διάφορες υπηρεσίες, δημόσιες και ιδιωτικές ώστε να προφυλαχθούν από μία ενδεχόμενη απειλή. (Ψύλος, 2022)

Ο κυβερνοπόλεμος αυτό που ξεκίνησε πριν από περίπου δύο χρόνια, πολλοί θεωρούν ότι είναι ένα βασικό στοιχείο για το πώς μπορεί να εξελιχθούν τα πράγματα στο μέλλον, ενώ δεν είναι τυχαίο ότι το Πεντάγωνο έκανε λόγο για τον «πόλεμο 360», όπου τα όπλα όπως ο περισσότερος πληθυσμός της γης μπορεί να τα γνωρίζει όπως αεροπλάνα, βόμβες και άλλα είναι ένα μόνο μέρος μιας στρατηγικής, που εκτυλίσσεται σε πολλά πεδία και «εργαλεία», με στόχο εκτός του άλλον και τον αποπροσανατολισμό του εχθρού, καθώς και την παραπληροφόρηση.

Όταν ξέσπασε η πρώτη υποψία για μια μάχη στο διαδίκτυο, στις 14 Ιανουαρίου, με έναν ιό που εντόπισε η εταιρεία Microsoft και άλλες αρχές και εταιρείες στον κόσμο διαπίστωσαν ότι υπάρχουν κάποια προβλήματα, ενώ είναι σημαντικό να αναφερθεί ότι μία επιχείρηση στο Τέξας των ΗΠΑ

αναφέρθηκε σε κάποιες διαπιστώσεις και υποθέσεις που έκανε, λέγοντας ο τρόπος της επίθεσης αυτή μοιάζει με έναν συγκεκριμένο τρόπο που χρησιμοποιεί μια ομάδα χάκερς στη Ρωσία, με την επωνυμία Voodoo Bear. Σε αυτό το σημείο είναι σημαντικό να αναφερθεί ότι τέτοιου είδους ομάδες είναι πολύ έμπειρες, γνώστες των πραγμάτων και της πληροφορίας, αλλά και πολύ καλά οργανωμένες. (Ψύλος, 2022)

Αργότερα βέβαια τα πράγματα έγιναν πιο ξεκάθαρα, αφού υπήρξαν διάφορες κυβερνοεπιθέσεις προς δημόσιους οργανισμούς, τράπεζες και υπουργεία της χώρας, ενώ παράλληλα πολλές ιστοσελίδες της χώρας σταμάτησαν να λειτουργούν. Όπως ήταν φυσικό αυτό προκάλεσε τη μεγάλη ανησυχία, πιθανώς και το φόβο των πολιτών, ενώ μερικοί φοβήθηκαν και για την ίδια τους της ζωή. Μια εταιρεία κυβερνοασφάλειας αναφέρθηκε ότι έγινε χρήση κακόβουλου λογισμικού, που μπορεί να προκαλέσει μεγάλες καταστροφές και μολύνσεις, αλλά και ενδέχεται να στοχεύουν και διάφορες σημαντικές υποδομές της χώρας. (Naftemporiki.gr., 2022β) Κατά συνέπεια, συνέστησε προσοχή, ενώ διάφορες χώρες του κόσμου απλώς μπορούν να εικάζουν για το τι ακριβώς συμβαίνει, αλλά και για να διαπιστώσουν την ταυτότητα του επιτιθέμενου. Ωστόσο μόνο υπηρεσίες των ΗΠΑ για παράδειγμα έχουν αναπτύξει πολύ εξελιγμένες υπηρεσίες, καθώς και η βρετανική και η ρωσική, για να μπορούν να διαλευκάνουν ή να βρουν περισσότερες πληροφορίες σχετικά με τους hackers. Κι αυτό διότι είναι λίγο δύσκολο καθώς πολλοί hackers για παράδειγμα προχωρούν σε επιθέσεις με ψευδή στοιχεία, όπου τέτοιες γνωστές ομάδες ανά τον κόσμο είναι για παράδειγμα οι Anonymous.

Σύμφωνα με άρθρο της Naftemporiki.gr (2022β), όσον αφορά το θέμα αυτό, ένας αναλυτής αναφέρει ότι είναι πολύ δύσκολο να γίνουν οι ανάλογες συσχετίσεις και να βρεθεί μια λύση σε τέτοιες περιπτώσεις, καθώς σχετίζονται πολλοί παράγοντες. Παράλληλα πρέπει να γίνει σύγκριση στοιχείων, δειγμάτων, αλλά και να ληφθούν υπόψη και άλλες παράμετροι, όπως πώς δρα μια συγκεκριμένη ομάδα, ποιος είναι ο σκοπός της και, υπό αυτή την έννοια, να προσπαθήσουν να τη συσχετίσουν με κάποια δύναμη ή με μια ομάδα γνωστών hackers. Παράλληλα, με όλες αυτές τις εξελίξεις και οι ΗΠΑ έδειχναν να ανησυχούν για να μην επεκταθεί περαιτέρω η κατάσταση αυτή και με τον έναν ή τον άλλον τρόπο έχει αντίκτυπο και στη χώρα αυτή. Άλλωστε, και στο παρελθόν έχουν καταγραφεί κυβερνοεγκλήματα από Ρώσους hackers απέναντι σε διάφορους οργανισμούς και επιχειρήσεις των ΗΠΑ. Πάνω σε τέτοιες εικασίες, αλλά και πιθανά ενδεχόμενα, ο πρόεδρος των ΗΠΑ, Μπάιντεν δήλωσε ότι η χώρα του σε ένα τέτοιο ενδεχόμενο που επιχειρήσει η Ρωσία είναι έτοιμη να ανταποδώσει αλλά και να αμυνθεί με τον καλύτερο τρόπο. (Τσιριγωτάκη, 2022)

Οι κυβερνοεπιθέσεις που πραγματοποιήθηκαν ενάντια της Ουκρανίας, ήδη πριν την εισβολή του στρατού στόχευαν το υπουργείο Άμυνας της χώρας, αλλά και τράπεζες, ενώ σύμφωνα με δηλώσεις που προέρχονται από την Ουκρανία, ήταν από τις χειρότερες ψηφιακές επιθέσεις που έχει ζήσει ποτέ η χώρα. Παράλληλα επλήγησαν και αρκετοί ιστότοποι της κυβέρνησης, όπως κάποιων υπουργείων, ώστε να προκληθεί αναταραχή και χάος.

Παράλληλα, ο κυβερνοπόλεμος αυτός, όπως ήταν φυσικό προκάλεσε και πολλές ανησυχίες σε χώρες της Δύσης, ενώ πολλά κράτη έσπευσαν να προσφέρουν κάθε είδους παροχής και βοήθειας στο Κίεβο και να συνεργαστούν μαζί του ώστε να αποτρέψουν μια πιθανή μεγαλύτερη καταστροφή. Όπως έγινε γνωστό ότι οι hackers που επιτέθηκαν ενάντια στην Ουκρανία χρησιμοποίησαν μεταξύ άλλων ένα λογισμικό με την ονομασία «υαλοκαθαριστήρες», που πρόκειται για ένα ιδιαίτερα καταστροφικό και κακόβουλο λογισμικό, το οποίο μπορεί να πλήξει από μακριά τους σκληρούς δίσκους υπολογιστών, προκαλώντας σημαντικά προβλήματα, μεταξύ των οποίων και διαγραφή πολλών στοιχείων και δεδομένων. Πρέπει να σημειωθεί ότι τέτοιες επιθέσεις που γίνονται μέσω του ψηφιακού κόσμου έχουν ως κύριο στόχο να προκαλέσουν τον πανικό του πληθυσμού, ώστε να χάσει την εμπιστοσύνη του απέναντι στην κυβέρνηση. (Ψύλος, 2022) Άλλωστε στη σημερινή εποχή τέτοιες μάχες, όπως αλλιώς αποκαλούνται και «σιωπηλές μάχες» γίνονται στον ψηφιακό κόσμο, χωρίς να επηρεάζονται (τις περισσότερες φορές πληθυσμοί), εκτός αν υπάρξουν παράπλευρες απώλειες, όμως μπορούν να προκαλέσουν και μεγάλη αστάθεια στις κοινωνίες, όπως να πλήξουν συστήματα για την παροχή νερού, φυσικού αερίου και άλλα ευαίσθητα συστήματα. Κάτι άλλωστε που στη συγκεκριμένη περίπτωση έχει γίνει και στο παρελθόν, όπως το 2015 σε μία ανάλογη περίσταση πάνω από 80.000 κάτοικοι δεν είχαν ρεύμα ή θέρμανση. Ψύλος, Μ. (2022).

Σύμφωνα με άρθρο του Ot.gr Newsroom (2022), πολλές κυβερνήσεις κρατών ανά τον κόσμο έδειξαν τη δυσαρέσκειά τους απέναντι στη Ρωσία, ενώ προσπάθησαν με κάθε τρόπο να βοηθήσουν την Ουκρανία. Ωστόσο, η Ρωσία έχει κατηγορηθεί πολλές φορές και στο παρελθόν ότι προβαίνει σε τέτοιου είδους επιθέσεις μέσω του διαδικτύου, για να παραπληροφορήσει, αλλά και γενικότερα να προβάλλει σημαντικά προβλήματα σε οικονομίες του κόσμου, υπονομεύοντας το διεθνές δίκαιο, αλλά και τους δημοκρατικούς θεσμούς που διέπουν τις κοινωνίες. (Ot.gr Newsroom, 2022) Πολλοί επίσης ισχυρίζονται ότι όντως η Ρωσία χρησιμοποιεί τέτοιες μεθόδους, για να αποσυντονίσει ή να προκαλέσει χάος. Δεν είναι τυχαίο άλλωστε ότι όπως ισχυρίζονται πηγές που προέρχονται από το Κίεβο, ότι η πλευρά της Ρωσίας σχεδόν σε κάθε πόλεμο με τον παραδοσιακό τρόπο, επιχειρεί και ανάλογες επιθέσεις μέσω του Διαδικτύου, με τις συνηθισμένες τακτικές που χρησιμοποιούν ομάδες από hackers. Όμως, πολλοί επισημαίνουν ότι η αποτελεσματικότητα ενός πολέμου ή μιας επίθεσης εξαρτάται από τις επιτυχίες και τις νίκες που εκτυλίσσονται στο πολεμικό πεδίο, και όχι μέσα από τους υπολογιστές. Ακόμη, τουλάχιστον, όπως χαρακτηριστικά αναφέρουν ειδικοί πάνω σε θέματα στρατιωτικά και άμυνας, ο κυβερνοπόλεμος δεν μπορεί να θεωρηθεί ως ένα μέσο που μπορεί να φέρει την έκβαση ενός πολέμου ή, ακόμη, και να καταφέρει να αναστρέψει μία κατάσταση. (Illiadi, 2023)

Συμπεράσματα

Ο κυβερνοπόλεμος, στη σημερινή εποχή, έχει πάρει πολύ μεγάλες διαστάσεις και, πλέον, έχει προκαλέσει την ανησυχία πολλών αναλυτών για τις διαστάσεις που μπορεί να πάρει στο μέλλον και τι αντίκτυπο μπορεί να έχουν στις κοινωνίες και στον άνθρωπο. Πρόκειται για μία από τις πιο σύγχρονες απειλές για τον άνθρωπο, τα κράτη, με συνέπειες που μπορεί να επιφέρουν πολύ σημαντικές καταστροφές: από πλήγματα σε υποδομές, μέχρι σε πλήγματα σε ΜΜΕ και πολλά άλλα. Κατά συνέπεια γίνεται αντιληπτό ότι πρόκειται για ένα θέμα που πρέπει να αντιμετωπιστεί άμεσα με τις ανάλογες ενέργειες, τακτικές και διευκρινίσεις σχετικά με το Δίκαιο που πρέπει να ακολουθείται σε τέτοιες περιπτώσεις.

Στην παρούσα εργασία αναλύσαμε όλες τις διαστάσεις του κυβερνοπολέμου, καθώς και πιο αναλυτικά αναφέραμε τον σύγχρονο αυτόν πόλεμο που διεξάγεται στην εποχή μας μεταξύ Ρωσίας και Ουκρανίας, με πολλές συνέπειες, και χωρίς κανείς να γνωρίζει -προς το παρόν τουλάχιστον- ποια θα είναι η κατάληξη τουλάχιστον όσον αφορά τις απειλές και την τροπή που μπορεί να πάρει ο κυβερνοπόλεμος. Πολλά κράτη σήμερα έχουν αναγάγει νέες μεθόδους και τακτικές για να πλήξουν τον εχθρό και πλέον ο κυβερνοχώρος αποτελεί ένα νέο «πεδίο μάχης», που θεωρείται ύπουλος, υποχθόνιος και σίγουρα αφορά μία νέα πραγματικότητα η οποία πρέπει να αντιμετωπιστεί από εδώ και πέρα με τους κατάλληλους τρόπους. Κάτι που είναι ιδιαίτερα σημαντικό, όπως για παράδειγμα πρέπει να υπάρξουν νέες ρήτρες και διατάξεις, για να καθορίσουν το Δίκαιο που πρέπει να διέπει έναν τέτοιον πόλεμο, μιας και το Διεθνές Δίκαιο δεν μπορεί να καλύψει όλες τις διαστάσεις και τα προβλήματα που προκύπτουν σε έναν κυβερνοπόλεμο, καθώς και όλες τις εκδοχές του, αν και χρησιμοποιείται στη σημερινή εποχή. Ωστόσο, όμως, όπως περιγράψαμε και σε προηγούμενα κεφάλαια έχει αρκετά προβλήματα, κυρίως ως προς τους τρόπους ερμηνείας του, που αναμφίβολα ανακύπτουν ασάφειες και πολλά προβλήματα. Υπό την έννοια αυτή, πρέπει να προκύψει πιο αυστηροί νόμοι για το θέμα που αναλύουμε.

Αποτελεί, θα λέγαμε, ένα πολύ βασικό στοιχείο, γιατί ο πόλεμος αυτός παίρνει όλο και μεγαλύτερες διαστάσεις και κανείς πλέον δεν γνωρίζει τι επιπτώσεις θα επιφέρει στο μέλλον ή ως ποιο σημείο μπορεί να φτάσει μια κυβερνοεπίθεση, για παράδειγμα, για τον άνθρωπο και τις κοινωνίες. Ο κυβερνοπόλεμος μεταξύ Ρωσίας και Ουκρανίας ήδη έχει προκαλέσει την ανησυχία πολλών μελετητών και δεν είναι τυχαίο ότι και πολλοί ηγέτες άλλων κρατών ανησυχούν για τις διαστάσεις που μπορεί να πάρει κυρίως ο πόλεμος που διεξάγεται από το Διαδίκτυο. Καθώς ακόμη όλα κρίνονται και τίποτε δεν έχει τελειώσει. Τέλος, είναι βασικό να προωθηθούν διάφορα μέσα για καλύτερη ενημέρωση του κόσμου πάνω σε τέτοια θέματα, αλλά και είναι ουσιαστικό να υπάρξουν ανάλογες συζητήσεις για μεγαλύτερη ευαισθητοποίηση.

Η τεχνολογία έχει προοδεύσει σημαντικά και ο πόλεμος πλέον διεξάγεται και μέσα από το Διαδίκτυο, όμως κανείς δεν γνωρίζει τις διαστάσεις που μπορεί να πάρει ένα τέτοιο θέμα και ως ποιο βαθμό ένας κυβερνοπόλεμος μπορεί να απειλήσει ακόμη και την εξέλιξη του ανθρώπου.

Βιβλιογραφία

Γεωργαντάς, Χ. (2016) *Ψυχολογικές επιχειρήσεις και χειρισμός κρίσεων: κρίση Κούβας κρίση Ιμίων* (ΜΑ). Πειραιάς: Πανεπιστήμιο Πειραιώς

Creative.gr. (2023). *Κυβερνοπόλεμο προκάλεσε η εισβολή της Ρωσίας στην Ουκρανία.* Διαθέσιμο στο: https://www.cretalive.gr/kosmos/kybernopolemo-prokalese-i-eisboli-tis-rosias-stin-oykrania (Ανακτήθηκε στις 3 Μαρτίου 2022)

Εγχειρίδιο Κυβερνοασφάλειας, Υπουργείο Ψηφιακής Δικαυβέρνησης, https://mindigital.gr/wp-

Efsyn.gr. (2023) *Για «υβριδικό πόλεμο» κατηγορεί η Ουκρανία τη Ρωσία.* Διαθέσιμο στο: https://www.efsyn.gr/kosmos/eyropi/327870_gia-ybridiko-polemo-katigorei-i-oykrania-ti-rosia (Ανακτήθηκε στις 16 Ιανουαρίου 2022)

Ιγγλεζάκης, Ι. (2023) *Κυβερνοασφάλεια: Οι νέοι κανόνες της ΕΕ για την καταπολέμηση του ηλεκτρονικού εγκλήματος*. Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-oi-neoi-kanones-tis-ee-gia-tin-katapolemisi-toy-ilektronikoy-egklimatos (Ανακτήθηκε στις 22 Σεπτεμβρίου 2023)

Illiadi, Th. (2023) *Ο κυβερνοπόλεμος Ρωσίας – Ουκρανίας*. Διαθέσιμο στο: https://gr.euronews.com/2023/02/21/o-kyvernopolemos-rosias-oukranias (Ανακτήθηκε στις 21 Φεβρουαρίου 2023).

Καλαβρός, Γ.-Ε. Φ. & Γεωργόπουλος, Θ. (2017) *Το Δίκαιο της Ευρωπαϊκής Ένωσης - Ουσιαστικό Δίκαιο* (τόμος ΙΙ). Αθήνα: Νομική Βιβλιοθήκη

Κωνσταντοπούλου, Δ. (1986) *Δημόσιον Διεθνές Δίκαιο ΙΙΙ.* Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Μαρούδα, Μ. Ν. (2015) *Διεθνές Ανθρωπιστικό Δίκαιο*. Αθήνα: Εκδόσεις Σιδέρης

Μαυραγάνης, Κ. (2019). *Αθανάσιος Κοσμόπουλος: Ανάγκη οικοδόμησης μηχανισμού για την εντόπιση των fake news*. Διαθέσιμο στο: https://www.huffingtonpost.gr/entry/athanasios-kosmopoelos-anayke-oikodomeses-mechanismoe-yia-ton-entopismo-ton-fake-news_gr_5cbed797e4b00b3e70ceb50c?ovf (Ανακτήθηκε στις 25 Απριλίου 2019)

Νικκολό Μακιαβέλλι, Ο Ηγεμόνας, (Αθήνα: Κάκτος, 2006), σελ.133.

Newsroom. (2022) *Έκθεση της Microsoft επιβεβαιώνει τον υβριδικό πόλεμο της Ρωσίας στην Ουκρανία*. Διαθέσιμο στο: https://www.cnn.gr/tech/story/310247/ekthesi-tis-microsoft-epivevaionei-ton-yvridiko-polemo-tis-rosias-stin-oykrania (Ανακτήθηκε στις 27 Απριλίου 2022)

Ορφανουδάκης, Σ. (2003) *Η αρχή της αναλογικότητας στην ελληνική έννομη τάξη: Από τη νομολογιακή εφαρμογή της στη συνταγματική της καθιέρωση*. Αθήνα: Εκδόσεις Σάκκουλα

Ot.gr Newsroom. (2022) *Ρωσία: Ετοιμάζει παγκόσμιο κυβερνο-πόλεμο; Τι φοβούνται οι αναλυτές.* Διαθέσιμο στο: https://www.ot.gr/2022/02/25/texnologia/rosia-etoimazei-pagkosmio-kyverno-polemo-ti-fovountai-oi-analytes/ (Ανακτήθηκε στις 25 Φεβρουαρίου 2022)

Παντελής, Κ. (2015) *Ποιος είναι ο σύγχρονος υβριδικός πόλεμος;.* Αθήνα: Κέντρο Διεθνών Στρατηγικών Αναλύσεων

Πιπυρος Κ. και Μήτρου Λ., Κυβερνοεπίθεση ή Κυβερνοπόλεμος, Νομική Βιβλιοθήκη, 2018, σελ. 193

Σίμου, Φ. (2016). *Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο (ΜΑ).* Πανεπιστήμιο Αιγαίου

Σταμπουλής, Π. (2021) Υβριδικές Συγκρούσεις στο παρελθόν έως το 2006. Στο: Ε. Ι. Μελετών, *Υβριδικοί Πόλεμοι* (σ. 93-107). Ινφογνώμων

Στραβοπόδης, Μ. (2019) *Υβριδικός Πόλεμος - Από τον Θουκυδίδη στο σήμερα*. Διαθέσιμο στο: https://www.huffingtonpost.gr/entry/evridikospolemos-apo-ton-thoekedide-sto-semera_gr_5cdd6160e4b09648227bf3f8 (Ανακτήθηκε στις 10 Αυγούστου 2020)

Deep, A. (2015). *Small Wars Journal*. Διαθέσιμο στο: https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques (Ανακτήθηκε στις 10 Μαρτίου 2020)

Σύνταξη IN. (2023). *Κυβερνοπόλεμος: Νέο πλαίσιο άμυνας στην ΕΕ εν μέσω ουκρανικής κρίσης*. Διαθέσιμο στο: https://www.in.gr/2022/05/13/in-science/technology/kyvernopolemos-neo-plaisio-amynas-stin-ee-en-meso-oukranikis-krisis/ (Ανακτήθηκε στις 13 Μαίου 2023)

Τσιριγωτάκη, Ε. (2022) *Ποια θα είναι η επόμενη φάση του κυβερνοπολέμου ανάμεσα στη Ρωσία και στην Ουκρανία*. Διαθέσιμο στο: https://www.ertnews.gr/eidiseis/poia-tha-einai-i-epomeni-fasi-toy-kyvernopolemoy-anamesa-sti-rosia-kai-tin-oykrania/ (Ανακτήθηκε στις 27 Φεβρουαρίου 2022)

Τσουραμάνης, Χ. (2006) *Κυβερνοέγκλημα.* Αθήνα: Εκδόσεις Παπαζήση.

Ζάννη, Α. (2005) *Το διαδικτυακό έγκλημα*. Αθήνα: Εκδόσεις Σάκκουλα

Χαίδης, Λ. (2012) *Οι Συγκρούσεις στον Κυβερνοχώρο: Ο κυβερνοπόλεμος και η Αποτροπή.* (Διπλωματική Εργασία). Πειραιάς: Πανεπιστήμιο Πειραιά

Χαραλαμπόπουλος, Ν. (2020) *Το φαινόμενο του Υβριδικού Πολέμου από την Αρχαιότητα έως σήμερα Μελέτες Περίπτωσης*. Διαθέσιμο στο: https://dspace.lib.uom.gr/bitstream/2159/24982/3/CharalampopoulosNikolaosMsc2020.pdf (Ανακτήθηκε στις 15 Δεκεμβρίου 2020)

Ψύλος, Μ. (2022) *Ο ατελείωτος κυβερνοπόλεμος της Ρωσίας κατά της Ουκρανίας*. Διαθέσιμο στο: https://www.naftemporiki.gr/kosmos/1302457/o-ateleiotos-kyvernopolemos-tis-rosias-kata-tis-oukranias/ (Ανακτήθηκε στις 26 Φεβρουαρίου 2022)

Berglund, C. & Souleimanov, E. (2019) *What is (not) asymmetric conflict? From conceptual stretching to conceptual structuring, Dynamics of Asymmetric Conflict*. Available at: https://doi.org/10.1080/17467586.2019.1680855

Check T. (2015) 'Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach'

Clarke, R. & Knake, R. (2010) *Cyber War. The Next Threat to National Security and What to Do About It*. USA: Harper Collins Publications

Dinniss, H. (2008) The Status and Use of Computer Network Attacks in International Humanitarian Law. London School of Economics and Political Science. Available at: http://etheses.lse.ac.uk/2

Hoffman, F. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies

Hoffman, F. (2009) *Hybrid vs. Compound War*. Armed Forces Journal. Available at: http://armedforcesjournal.com/hybrid-vs-compound-war/

Brenner, Susan W. 2007. "At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare. The Journal of Criminal Law and Criminology (Northwestern University School of Law) 97 (2): 379---475.

Burton, J. (2018) «*NATO Coopoaretive Cyber Defence Center of Excellence.»* ccdcoe.org. 2018. https://ccdcoe.org/publication-library.htm l (Ανακτήθηκε στις 25 Οκτωβρίου 2018)

Charney, S. (2009) *Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft White Paper*. Redmond, Microsoft Corp.9

Cohen, J. (2013) *The New Digital Age: Reshaping the Future of People, Nations and Business*. Murray Publishing

Council of Europe. (2001) European Treaty Series No 185. Convention on Cybercrime. Budapest. Available at:

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_b udapest_en.pdf (Retrieved 23rd October 2001)

Dahinden M. 2021. Swiss Neutrality in the Age of Cyber Warfare.ICT4peace Foundation. Geneva https://ict4peace.org/wp-content/uploads/2021/02/ICT4Peace-2021-Neutralitet-und-Cyberspace-eng.pdf σελ.7-8

Dipert, R. (2016) *The Ethics Of Cyberwarfare*. Journal Of Military Ethics: Vol 9, No 4

E-9680/10EN Answer given by Mr Šefčovič on behalf of the Commission (17.1.2011)https://www.europarl.europa.eu/doceo/document/E-7-2010-9680-ASW_EN.pdf

EEngle, E. (2012) The History of the General Principle of Proportionality. *Dartmouth Law Journal,* pp. 10 – 11

Eilstrup-Sangiovanni, M. (2018). Why the world needs an international cyberwar convention. Philosophy & Technology, 31(3), 379-407

European Commission. (2013) «eeas.europa.eu.» eeas.europa.eu. 7 Φεβρουάριος 2013. https://eeas.europa.eu/archives/docs/policies/eu-cybersecurity/cybsec_comm_en.pdf (Ανακτήθηκε στις 4 Νοεμβρίου 2018)

Finkelstein, C. & Goven, K. & Ohlin, J. (2015) Cyberwar Law and Ethics for Virtual Conflicts. UK: Oxford University Press pp. 140-149.

Gardam, J. (2004) *Necessity, Proportionality and the Use of Force by States*. Cambridge, CUP, pp. 202 84

Gibson, W. (1984) Neuromancer. London: Harper Collins Publications

Halder, D., and Jaishankar, K., Cyber crime and the Victimization of Women: Laws, Rights, and Regulations (Hershey:IGI Global, 2011).

Hammes, T. (2004) "The Sling and the Stone On War in the 21st Century". St. Paul, MN, MBI Publishing Company 71

Henckaerts, J. (2005) *Customary International Humanitarian Law*, Vol. 1. London: Cambridge University Press, pp. 55-66.

Higson, D. (2016) "Applying the Law of Neutrality While Transitioning the Seas of Cyberspace," *American University National Security Law Brief,* Vol.6, No.2

Jennings, M. N. (2017, 8 7). AUSA. Ανάκτηση 10 2020, από https://www.ausa.org/articles/washington-first-operational-artist-george

Kathimerini.gr. (2023) *Ουκρανία-Ρωσία: Ο άγνωστος πόλεμος στον κυβερνοχώρο.* Διαθέσιμο στο: https://www.kathimerini.gr/world/562602442/oykrania-rosia-o-agnostos-polemos-ston-kyvernochoro/ (Ανακτήθηκε στις 8 Σεπτεμβρίου 2023)

Lehne, S. (2016) *The EU Global Strategy, a Triumph of Hope Over Experience*, Carnegie Europe, 4 July 2016

Libicki M. (2007*) Conquest in Cyberspace, National Security and Information Warfare*. New York: Cambridge University Press

Libicki, M. (2009) *Cyberdeterrence and Cyberwar*. RAND. Library of Congress

Lieberthal, K. & Peter W. Singer, P. (2011) *Cyberspace Security and U.S- China Relations.* Brookings, Author's Note p. iv

Lin, H. (2010) 'Offensive Cyber Operations and the Use of Force' (2010)

Lin, H. & Zegart, A. (2017) *Introduction to the Special Issue on Strategic Dimensions of Offensive Cyber Operations*. London: Oxford University

Mcclure, S. & Scambray, J. & Kurtz, G. (2009). *Ασφάλεια Δικτύων*. Αθήνα: Εκδόσεις Γκιούρδας

Miller, M. (2014) "Momentary Memorials: Political Posters of the Lebanese Civil War and Hezbollah". (Undergraduate Honors Theses. Available at: https://core.ac.uk/download/pdf/54847305.pdf

Missiroli, A. (2015) (ed) Towards an EU Global Strategy – Background, Process, References. European Union Institute for Security Studies

Monar, J. (2015) The EU as an International Counter-terrorism Actor: Progress and Constraints. *Intelligence and National Security*, 30 (2-3), p. 333 - 356

Naftemporiki.gr. (2022). *ΕΕ: Ραγδαία αυξάνονται οι κυβερνοεπιθέσεις – Τι χρειάζεται να γίνει*. Διαθέσιμο στο: https://www.naftemporiki.gr/kosmos/1314450/ee-ragdaia-afxanontai-oi-kyvernoepitheseis-ti-chreiazetai-na-ginei/ (Ανακτήθηκε στις 29 Μαρτίου 2022)

Naftemporiki.gr. (2022β) *Ο ατελείωτος κυβερνοπόλεμος της Ρωσίας κατά της Ουκρανίας*. Διαθέσιμο στο: https://www.naftemporiki.gr/kosmos/1302457/o-ateleiotos-kyvernopolemos-tis-rosias-kata-tis-oukranias/ (Ανακτήθηκε στις 26 Φεβρουαρίου 2022)

Ohlin, J. D. & Govern, K. & Finkelstein, C. (Eds.) (2015) *Cyberwar, Law and Ethics for Virtual Conflicts.* Oxford, Oxford University Press

Pawlak, P. (2020) *Eu Cybersecurity Strategy 2020: First Impressions, Directions Cyber Digital Europe*, December. Available at: https://directionsblog.eu/eu-cybersecurity-strategy-2020-first-impressions/

Pipyros Kosmas, Thraskias Christos, Mitrou Lilian, Gritzalis Dimitris, Apostolopoulos Theodoros: A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, p.5

Reich, P. (2010) "Cyber Warfare: A Review Of Theories, Law, Policies, Actual Incidents – And The Dilemma Of Anonymity", *European Journal of Law and Technology 1.2*

Sheldon, J. (2011) Deciphering cyberpower strategic purpose in peace and war. Strategic Studies Quarterly και Jon R. Lindsay, Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, Volume 1, Issue 1

Shackelford, S. (2013) "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance." *American University Law Review 62,* no. 5

Schmitt, M. (2013) "Cyber Activities and the Law of Countermeasures" in Peacetime Regime for State Activities in Cyberspace, ed. Katharina Ziolkowski, p.659-674 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.645.1982&rep=rep1&type=pdf#page=69

Shostack, A. (2014) *Threat Modeling: Designing for Security.* John Wiley & Sons, Inc

Schjølberg, S. (2017) *The History of Cybercrime (1976-2016).* Germany: Cybercrime Research Institute, Vol. 11

Singer, P.W. & Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press

Thornton, R. (2007) Asymmetric Warfare: Threat and Response in the 21st Century. *Polity Press 69*

Quéguiner, J.(2006) Precautions under the Law Governing the Conduct of Hostilities. *International Review of the Red Cross,* Vol. 88, pp. 120-129

Wallace, D. (2018) Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Available at: https://ccdcoe.org/uploads/2018/10/TP11_2018.pdf

http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-stratigiki

http://www.ysun-greece.org/files/2007_pics/UN_charter_greek.pdf

https://en-m-wikipedia-org.translate.goog/wiki/Stuxnet?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

Electronic Frontier Foundation (2013) “NSA ANT Catalog”

Col. Andrew Borden, USAF (Ret.) (1999) “What is information warfare?”

Gary King, Jennifer Pan, Margaret E. Roberts (2017) “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument”, Harvard University Press

Daisy Sindelar (2014) “The Kremlin’s Troll Army”, The Atlantic

Wikipedia (2023) https://en.wikipedia.org/wiki/Sock_puppet_account (πρόσβαση στις 7/1/2024)

Nick Fielding, Ian Cobain (2011) “Revealed: US spy operation that manipulates social media”, The Guardian

Synthesia.io (2023), https://www.synthesia.io/glossary/synthetic-media (πρόσβαση στις 4/1/2024)

NPR.org (2022), https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia (πρόσβαση στις 4/1/2024)

Mohan B. Gazula (2017) “Cyber Warfare Conflict Analysis and Case Studies”, Cybersecurity Interdisciplinary Laboratory MIT

Elizabeth Flock (2011) “Operation Cupcake: MI6 replaces al-Qaeda bomb-making instructions with cupcake recipes”, The Washington Post

Alissa Starzak (2022) “The latest on attacks, traffic patterns and cyber protection in Ukraine”, https://blog.cloudflare.com/ukraine-update (πρόσβαση στις 9/1/2024)

Dr. Nicolae Steiner (2011) “Critical Infrastructure Protection in Healthcare Systems” Romanian National Centre for Training in Medical Management of Disasters

Wired.com (2016) “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid https://web.archive.org/web/20210208174448/https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (πρόσβαση μέσω web-archive 6/1/2024)

BBC.com (2021) “The Lazarus Heist: How North Korea almost pulled off a billion-dollar hack” https://www.bbc.com/news/stories-57520169 (πρόσβαση στις 8/1/2024)

Tyler Wall (2022) “Throwback Attack: Hackers attempt to flood Israeli water supply with chlorine” https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-hackers-attempt-to-flood-israeli-water-supply-with-chlorine/ (πρόσβαση στις 7/1/2024)

CyberPeace Institute writing team (2023) https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/transportation (πρόσβαση στις 4/1/2024)

Chay Donohoe (2023) https://www.bulletproof.co.uk/blog/tech-talk-supply-chain-hardware-hacking (πρόσβαση στις 6/1/2024)

Chris Wysopal, Chris Eng (2006) “Static Detection of Application Backdoors” Veracode Inc.

Tony Wu, Justin Chung, James Yamat, Jessica Richman (άνευ ημερομηνίας) “The ethics (or not) of massive government surveillance” Stanford University Department of Computer Science public repository https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html (πρόσβαση στις 7/1/2024)

Meron, T. (2000). The Martens Clause, Principles of Humanity, and Dictates of Public Conscience. American Journal of International Law, 94 (1), pp. 78-89. DOI: https://doi. org/10.2307/2555232

Inernational Court of Justice "Legality of the Threat and Use of Nuclear Weapons" (1996), ICJ Press Service

Victor Melin (2021) “Does the threshold for an ‘armed attack’ within the meaning of Article 51 of the UN Charter leave a state unable to act vis-à-vis an opponent using hybrid warfare strategies?” Swedish Defence University Publications