ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΕΡΓΑΣΙΑ

Της Βασιλικής Παπαθεοδώρου (Α.Μ.: ΜΔΙ2138)

ΤΟ ΔΙΕΘΝΕΣ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ & ΤΟ ΔΙΚΑΙΩΜΑ ΤΩΝ ΚΡΑΤΩΝ ΣΕ ΕΝΑΝ ΑΣΦΑΛΗ ΚΥΒΕΡΝΟΧΩΡΟ

Επιβλέπουσα:

Καθηγήτρια Λίλιαν Μήτρου

Πειραιάς, Ιούλιος 2023

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ ... 3
ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ ... 4
ΠΕΡΙΛΗΨΗ ... 5
ΚΕΦΑΛΑΙΟ 1: ... 6
ΕΙΣΑΓΩΓΗ ... 6
Α′ ΜΕΡΟΣ ... 9
ΑΛΛΑΓΗ ΤΩΝ ΔΙΕΘΝΩΝ ΣΥΝΘΗΚΩΝ: ΒΑΣΙΚΑ ΔΙΚΑΙΩΜΑΤΑ & ΥΠΟΧΡΕΩΣΕΙΣ, ΝΕΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΚΡΑΤΟΣ ... 9
ΚΕΦΑΛΑΙΟ 2: ... 10
ΚΡΑΤΟΣ & ΑΣΦΑΛΕΙΑ ... 10
2.1. Ισχύς ... 10
2.2. Συντελεστές Ισχύος ... 12
2.3. Νέες Προκλήσεις για τα κράτη ... 16
2.4. Χρήσιμοι ορισμοί ... 19
ΚΕΦΑΛΑΙΟ 3: ... 23
ΝΕΕΣ ΔΥΝΑΤΟΤΗΤΕΣ ΣΤΟΝ ΠΟΛΕΜΟ ... 23
3.1. Κυβερνοπόλεμος και στρατηγικές προσεγγίσεις ... 24
3.1.1. Κλαούζεβιτς ... 24
3.1.2. Σουν Τσου ... 26
3.1.3. Ναυτική Στρατηγική ... 28
3.1.4. Αεροπορική Στρατηγική ... 29
3.2. Ο κυβερνοπόλεμος ως υβριδικός πόλεμος ... 30
3.3. Κυβερνοεπιχειρήσεις τον 21ο αιώνα ... 35
3.3.1. Εσθονία ... 36
3.3.2. Γεωργία ... 37
3.3.3. Ουκρανία ... 38
3.3.4. Microsoft Exchange Server ... 40
Β′ ΜΕΡΟΣ ... 44
ΔΙΕΘΝΕΣ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ... 44
ΚΕΦΑΛΑΙΟ 4: ... 45
ΕΜΜΕΣΗΣ ΕΦΑΡΜΟΓΗΣ ΡΥΘΜΙΣΕΙΣ ... 45

4.1. Οργανισμός Ηνωμένων Εθνών - ΟΗΕ 45
4.1.1. Διεθνές Δίκαιο και Κυβερνοχώρος 47
4.1.2. Κρατική Κυριαρία & Δικαιοδοσία 48
4.1.3. Διεθνείς Νόρμες 49
4.1.4. Απόδοση Ευθύνης 50
4.1.5. Μέτρα Οικοδόμησης Εμπιστοσύνης 52
4.2. Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη - ΟΑΣΕ 53
4.3. Οργανισμός Βορειο-Ατλαντικού Συμφώνου – NATO (North Atlantic Treaty Organazation) 55
4.3.1. Χρήση βίας - Απειλή χρήσης βίας – Νόμιμη Αυτοάμυνα 58
ΚΕΦΑΛΑΙΟ 5: 63
'ΑΜΕΣΗΣ' ΕΦΑΡΜΟΓΗΣ ΡΥΘΜΙΣΕΙΣ 63
5.1. Ευρωπαϊκή Ένωση & Κυβερνοασφάλεια 63
5.1.1. Πράξη για την κυβερνοασφάλεια – Κανονισμός 2019/881 64
5.1.2. NIS I & NIS II – Οδηγία 2016/1148 & Οδηγία 2022/2555 66
5.1.3. Διπλωματική Εργαλειοθήκη 70
5.1.4. Μελλοντικές πρωτοβουλίες της ΕΕ 74
ΚΕΦΑΛΑΙΟ 6: 77
ΕΠΙΛΟΓΟΣ 77
ΒΙΒΛΙΟΓΡΑΦΙΑ 81

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Εικόνα 1 Επιθέσεις σε πληροφοριακά συστήματα ανά τον κόσμο 17
Εικόνα 2 Επιθετικές κυβερνο-ικανότητες παγκοσμίως. 17

ΠΕΡΙΛΗΨΗ

Το διεθνές περιβάλλον ρυθμίζεται από τις σχέσεις των κρατών και την ιεράρχηση αυτών με βάση τις ιδιαίτερες ικανότητες τους. Οι ικανότητες αυτές που αποτελούν και τους συντελεστές διαμορφώσεις της ισχύος τους, είναι το ουσιαστικότερο κριτήριο για την ανάδειξη των μεγάλων δυνάμεων. Ωστόσο, κομβικής σημασίας για την τελική τοποθέτηση των κρατών στη διεθνή σκακιέρα, είναι οι τεχνολογικές εξελίξεις κάθε ιστορικής περιόδου.

Επί των ημερών μας, ο κυβερνοχώρος αποτελεί την επιζητούμενη τεχνολογική καινοτομία. Ως εκ τούτου, τα κράτη έχουν διαμορφώσει τον τρόπο δράσης και προώθησης των πολιτικών αντικειμενικών τους σκοπών συμπεριλαμβάνοντάς τον. Υιοθετώντας έναν υβριδικό τρόπο επίλυσης των, διακρατικών και μη, διαφορών, έχουν εντάξει πλήρως τις κυβερνοεπιχειρήσεις και τον κυβερνοπόλεμο στην πολιτική τους ατζέντα. Οι νέες αυτές έννοιες έχουν ενσωματωθεί στις εθνικές στρατηγικές των περισσοτέρων κρατών και έχουν λάβει σάρκα και οστά στις σύγχρονες διακρατικές διενέξεις. Οι πρόσφατες συγκρούσεις του 21ου αιώνα απέδειξαν πως ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί ποικιλοτρόπως για την επίτευξη διαφορετικών πολιτικών στοχεύσεων (παραπληροφόρηση, προπαγάνδα, επικουρική βοήθεια στα πεδία των μαχών, αποκλειστικό πεδίο πολέμου).

Όλες αυτές οι ενέργειες, όμως, επισύρουν αλλαγές στο διεθνές κανονιστικό πλαίσιο ρύθμισης των διακρατικών σχέσεων. Ο ΟΗΕ και ο ΟΑΣΕ σε παγκόσμιο επίπεδο και το ΝΑΤΟ και η ΕΕ σε περιφερειακό και δυτικοκεντρικό -όπως η χώρα μας- έχουν αναλάβει την οριοθέτηση του νέου πεδίου πολιτικής δράσης, τη θέσπιση κανόνων και σχέσεων αμοιβαίας εμπιστοσύνης εντός αυτού και σε περίπτωση μη συμμόρφωσης την επιβολή κυρώσεων, ώστε να εξασφαλιστεί η, ει δυνατόν, καλύτερη διακρατική συμβίωση αποφεύγοντας τις παρερμηνείες και τις έκνομες ενέργειες που δημιουργούν έτι περισσότερη αστάθεια στο άναρχο διεθνές σύστημα.

ΚΕΦΑΛΑΙΟ 1:
ΕΙΣΑΓΩΓΗ

Το διεθνές σύστημα αποτελείται από τα κράτη, τα οποία συμβιώνουν σε αυτό και, δια των μεταξύ τους σχέσεων, διαμορφώνουν την ισορροπία του. Κάθε κρατική οντότητα διαθέτει κοινά στοιχεία με τις υπόλοιπες αλλά και μοναδικά χαρακτηριστικά που την ξεχωρίζουν. Χάρις σε αυτά τα στοιχεία και την αλληλεπίδραση με τα υπόλοιπα κράτη, αναδεικνύονται οι 'μεγάλες δυνάμεις' κάθε περιοχής και κάθε περιόδου. Για να αναδειχθούν τα ιδιαίτερα αυτά χαρακτηριστικά, είναι απαραίτητη και η μελέτη των εξωτερικών παραγόντων, όπως οι τεχνολογικές εξελίξεις. Στις μέρες μας, η συνεχώς αυξανόμενη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) έχει προκαλέσει ριζικές αλλαγές, όχι μόνο στην επικοινωνία, αλλά σε όλο το εύρος των καθημερινών μας δραστηριοτήτων, μετατρέποντας εν γένει την παγκόσμια οικονομική και κοινωνική τάξη πραγμάτων.

Η νέα αυτή καθημερινότητα έχει επηρεάσει και τις διεθνείς σχέσεις και έχει μεταβάλλει τον τρόπο δράσης των διεθνών παικτών. Νέες δυνατότητες και μέθοδοι προώθησης των κρατικών συμφερόντων έχουν αναδειχθεί, ενώ και οι πάλαι άλλοτε αδύναμοι δρώντες έχουν αποκτήσει θέση στο δημόσιο λόγο και ισχύ δυσανάλογη των δυνατοτήτων τους. Ο κυβερνοχώρος αποτελεί πλέον σημαντικό εργαλείο στα χέρια των διαμορφωτών της παγκόσμιας τάξης πραγμάτων, αλλά και εκείνων που θέλουν να δουν την αλλαγή του. Οι διακρατικές διαμάχες του 21ου αιώνα είναι πλήρως συνυφασμένες με τις τεχνολογικές εξελίξεις και κάθε προσπάθεια διατήρησης ή και ανατροπής του status quo συμπεριλαμβάνει και τη χρήση των νέων κυβερνοϊκανοτήτων.

Στην προσπάθεια θωράκισης των κρατών, κυρίως υπό την αιγίδα ποικίλων διεθνών οργανισμών, γίνεται προσπάθεια αναδιαμόρφωσης του θεσμικού πλαισίου, ώστε να ανταποκρίνεται στις νέες προκλήσεις και να περιορίζει τα όποια νομικά κενά επιτρέπουν στους παίκτες του διεθνούς συστήματος να τα εκμεταλλευτούν και να προωθήσουν τους σκοπούς τους. Τα κράτη

αναδιοργανώνουν το τρόπο δράσης τους στη διεθνή σκακιέρα και θεσπίζουν νέα δικαιώματα και υποχρεώσεις προσπαθώντας να περιχαρακώσουν τις ήδη υπάρχουσες αρχές και αξίες που διαμορφώνουν τις μεταξύ τους σχέσεις. Υπό αυτή τη λογική, προχώρησαν στην αναγνώριση του κυβερνοχώρου ως πεδίου προώθησης των πολιτικών τους επιδιώξεων, προσπάθησαν να ερμηνεύσουν τα κλασικά δεσμευτικά συμβατικά κείμενα και να θεσπίσουν κανόνες χρηστής συμπεριφοράς και χρήσης του κυβερνοχώρου, δημιουργώντας ενός είδους δικαίωμα, την ανάγκη των κρατών για κυβερνοασφάλεια. Το νέο αυτό δικαίωμα, δεν είναι μόνο θετικά επιφορτισμένο, αλλά επισύρει ευθύνες και υποχρεώσεις απέναντι στους πολίτες, το κράτος και τη διεθνή κοινότητα. Οι ευθύνες αυτές αποτυπώνονται κατά κύριο λόγο στις αποφάσεις των ομάδων εργασίας εντός των Ηνωμένων Εθνών, του θεσμικού ρυθμιστή της παγκόσμιας τάξης και ασφάλειας, αλλά και εκτός, σε περιφερειακό επίπεδο, που ως εκ τούτου υιοθετούνται μεγαλύτερου βάθους και εύρους δεσμεύσεις.

Η παρούσα εργασία, επομένως, θα εστιάσει στο κράτος, ως παίκτη του διεθνούς συστήματος, και στο πως αυτό διαμορφώνει τις διακρατικές του σχέσεις με το πέρασμα των χρόνων και την αλλαγή των συνθηκών ως απόρροια της προόδου της τεχνολογίας, προστάζοντας την μεταβολή των, έως τώρα γνωστών, τρόπων δράσης του στον αγώνα διατήρησης της πολυπόθητης ισχύος, αλλά και την επιβολή νέων παγκόσμιων και περιφερειακών κανόνων υπεύθυνης κρατικής συμπεριφοράς.

Πιο συγκεκριμένα, η εργασία έχει δομηθεί σε δύο μέρη, έκαστο αποτελούμενο από δύο κεφάλαια. Στο πρώτο κεφάλαιο του πρώτου μέρους (Κεφάλαιο 2) γίνεται παρουσίαση της έννοιας της ισχύος, ρυθμιστή των διακρατικών σχέσεων, και των συντελεστών που την διαμορφώνουν. Ακολουθεί η παρουσίαση των νέων απειλών/ προκλήσεων που αναδύονται για την ασφάλεια των κρατών ως αποτέλεσμα της ραγδαίας τεχνολογικής προόδου, καθώς και η παράθεση των ορισμών αυτών. Το δεύτερο κεφάλαιο του πρώτου μέρους (Κεφάλαιο 3) επικεντρώνεται στον δυνάμει στρατιωτικό χαρακτήρα του κυβερνοχώρου. Μέσα από την σύγκριση του με τα άλλα πεδία που πολέμου -γη, θάλασσα, αέρας- καθώς

και με την μελέτη του ως μέρους του υβριδικού πολέμου αναδεικνύονται τα πλεονεκτήματα και τα μειονεκτήματα της δράσης στον κυβερνοχώρο για την προώθηση των πολιτικών σκοπιμοτήτων των κρατών. Παρατίθενται, ακόμη, ορισμένα παραδείγματα της σύγχρονης ιστορίας χρήσης του κυβερνοχώρου για την επίλυση διακρατικών διαφορών.

Το δεύτερο μέρος της εργασίας παρουσιάζει το διεθνές ρυθμιστικό πλαίσιο της κυβερνοασφάλειας σε διεθνές (ΟΗΕ, ΟΑΣΕ) και σε περιφερειακό επίπεδο (ΝΑΤΟ, ΕΕ) προσανατολισμένο όμως στον ευρωπαϊκό χώρο. Στο πρώτο κεφάλαιο του δεύτερου μέρους (Κεφάλαιο 4) γίνεται αναφορά στις έμμεσης εφαρμογής ρυθμίσεις που προκύπτουν από τις consensus εκθέσεις, αποφάσεις και ψηφίσματα των ομάδων εργασίας των ΗΕ και των Γενικών Συνελεύσεων του ΟΑΣΕ και του ΝΑΤΟ. Στο δεύτερο κεφάλαιο (Κεφάλαιο 5), παρουσιάζεται το υπάρχον ευρωπαϊκό νομοθετικό οικοδόμημα στον τομέα της κυβερνοασφάλειας, καθώς και οι μελλοντικές προτάσεις για την περεταίρω οριοθέτηση του κυβερνοχώρου.

Τέλος, η εργασία ολοκληρώνεται με την αποτίμηση των ανωτέρω ευρημάτων (Κεφάλαιο 6) και με την διαπίστωση πως ο κυβερνοχώρος και τα εργαλεία του θα απασχολήσουν εις μακρόν τη διεθνή κοινότητα αναδιαμορφώνοντας συλλήβδην τον τρόπο πολιτικής διεκδίκηση και αντιπαράθεσης, καθώς και το νομικό και θεσμικό πλαίσιο παγκοσμίως δημιουργώντας νέα δικαιώματα, υποχρεώσεις και απειλές για τα κράτη.

Α΄ ΜΕΡΟΣ
ΑΛΛΑΓΗ ΤΩΝ ΔΙΕΘΝΩΝ ΣΥΝΘΗΚΩΝ: ΒΑΣΙΚΑ ΔΙΚΑΙΩΜΑΤΑ & ΥΠΟΧΡΕΩΣΕΙΣ, ΝΕΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΟ ΚΡΑΤΟΣ

ΚΕΦΑΛΑΙΟ 2:
ΚΡΑΤΟΣ & ΑΣΦΑΛΕΙΑ

2.1. Ισχύς

Η βασική μονάδα του διεθνούς συστήματος είναι το κράτος. Όλα τα κράτη αποτελούνται από τα ίδια συστατικά στοιχεία -λαό, έδαφος, κυβέρνηση & ανεξαρτησία- και χαίρουν της αναγνωρίσεως των υπολοίπων (Συρίγος, 2014, σ.108). Ως υποκείμενα του διεθνούς δικαίου φέρουν δικαιώματα και υποχρεώσεις, μοιάζοντας σε μεγάλο βαθμό ως προς τις βασικές τους λειτουργίες. Διαφέρουν, ωστόσο, ως προς τις δυνατότητές τους. Η δυνατότητα επιβίωσης και μακροημέρευσης, επιβολής της πολιτικής τους σε τοπικό, περιφερειακό ή και διεθνές επίπεδο αποτελούν ενδεικτικά στοιχεία της ισχύος τους. Η αλληλεπίδραση των κρατών με γνώμονα την ισχύ τους στο διεθνές πεδίο διαμορφώνει τις μεταξύ τους σχέσεις και οδηγεί στην ρύθμιση του άναρχου διεθνούς συστήματος.

Η ισχύς, επομένως, αποτελεί μια από τις βασικότερες έννοιες των διεθνών σχέσεων, η μελέτη της οποίας απασχόλησε κυρίως τους θιασώτες της ρεαλιστικής θεωρίας και χρησιμοποιείται ήδη από την αρχαιότητα και τον Θουκυδίδη. Πιο συγκεκριμένα, κατά τον Θουκυδίδη, η άνιση κατανομή της ισχύος μεταξύ των πόλεων-κρατών της αρχαίας Ελλάδας ήταν ο παράγοντας που φυσικά και αναπόφευκτα πυροδοτούσε τον μεταξύ τους ανταγωνισμό και το ξέσπασμα των πολέμων (Jackson & Sørensen, 2006, σ.114-116). Ως εκ τούτου, η επιβίωση, αν όχι η ευημερία των πόλεων, εξαρτιόταν αποκλειστικά και μόνο από τη δυνατότητα κατανόησής της θέσης τους σε σχέση με τις υπόλοιπες πόλεις, καθώς και τη δυνατότητα συμβιβασμού και προσαρμογής τους με την ισχύουσα ισορροπία. Επομένως, μόνο ο συνετός ηγέτης που υιοθετεί την ως άνω λογική και διαμορφώνει την εξωτερική του πολιτική συνδυάζοντας τα μακιαβελικά πρότυπα της ισχύος και της πανουργίας, μπορεί να προσφέρει την επιζητούμενη ασφάλεια που είναι απαραίτητη, ώστε η χώρα του να μην αποτελεί εύκολη λεία, παραβλέποντας ακόμα και κάθε είδους «(χριστιανική) ηθική» (Machiavelli, 2013, σ.105-108).

Για την ορθή λειτουργία του άναρχου διεθνούς συστήματος, η ιστορία έχει αποδείξει, πως χρειάζεται η ισορρόπηση της ισχύος τόσο σε περιφερειακό, όσο και σε διεθνές επίπεδο. Κάθε διαταραχή του δύναται να οδηγήσει στο ξέσπασμα ενός μεγάλου καταστροφικού πολέμου που σηματοδοτεί την αλλαγή της ισχύος μεταξύ των παικτών-κρατών και την αναδιαμόρφωση του συστήματος. Σε παγκόσμιο επίπεδο η ισορροπία έχει επιτευχθεί μέσω δύο συστημάτων, το διπολικό και το πολυπολικό. Το διπολικό σύστημα αναδύθηκε μετά τον Β' Παγκόσμιο Πόλεμο και επικράτησε μέχρι τη λήξη του Ψυχρού Πολέμου. Οι δύο υπερδυνάμεις -Ηνωμένες Πολιτείες της Αμερικής και Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών- ανέλαβαν την ευθύνη της παγκόσμιας τάξης μέσα από αμοιβαίους συμβιβασμούς και πέτυχαν τη σχετική σταθερότητα του συστήματος, αποτρέποντας έναν καταστροφικό πόλεμο μεταξύ τους και καταφεύγοντας σε περιφερειακές συγκρούσεις χαμηλής εντάσεως (Watson, 2010, σ.506, 523).

Στο πολυπολικό σύστημα, οι μεγάλες δυνάμεις κάθε περιόδου προσπαθούν να εξισορροπήσουν η μία την άλλη, με σκοπό την αποφυγή της συγκέντρωσης υπερβολικής ισχύος μίας εξ' αυτών, γεγονός που επιτυγχάνεται με τη δημιουργία συμμαχιών και συμφωνιών αμοιβαίας βοήθειας (Παπασωτηρίου, 2011, σ.25-27). Χαρακτηριστικό παράδειγμα λειτουργίας αλλά και επιτυχίας του πολυπολικού συστήματος ήταν η εκατονταετής ειρήνη (1815-1914) στην Ευρώπη που διήρκησε από την λήξη των Ναπολεόντειων πολέμων έως το ξέσπασμα του Α' Παγκοσμίου Πολέμου. Κατά τη διάρκεια της belle époque, οι πέντε μεγάλες δυνάμεις της εποχής -Μεγάλη Βρετανία, Πρωσία, Γαλλία, Αυστρο-Ουγγαρία και Ρωσία- επιδόθηκαν σε έναν αγώνα εξισορροπήσεων, στρατηγικών συμμαχιών, πολιτικών ανάσχεσης-επέκτασης και κατευνασμού (Παπασωτηρίου, 2011, σ.22-23) με σκοπό να αποφύγουν έναν μεγάλο καταστροφικό πόλεμο εντός της Ευρώπης που θα απειλούσε να ανατρέψει το ισχύον status quo και να αλλάξει τις ισορροπίες δυνάμεων (Kennedy, 1990, σ.206).

Σήμερα, ζούμε σε μια ιδιόμορφη πολυπολική περίοδο που ξεκίνησε μετά την κατάρρευση της ΕΣΣΔ και είχε ως αποτέλεσμα την ηγεμονία των ΗΠΑ. Τις

αμερικανικές ηγεμονικές τάσεις, όμως, που στόχο είχαν την αύξηση των σφαιρών επιρροής τους με την άσκηση επεμβατικών πολιτικών προσπαθούν να αμβλύνουν οι λοιπές 'μεγάλες' δυνάμεις, προτάσσοντας τη συμμετοχή και επίλυση των διαφορών στα διεθνή fora και προωθώντας την σύσταση νέων περιφερειακών οργανισμών για τη δημιουργία σχέσεων εμπιστοσύνης και αλληλοκατανόησης σε κάθε περιφέρεια του πλανήτη (Αρβανιτόπουλος & Ήφαιστος, 2003, σ.251).

Πέρα από την παγκόσμια ισορροπία ισχύος, προσπάθειες εξισορρόπησης λαμβάνουν χώρα και σε τοπικό/ περιφερειακό επίπεδο. Οι μεγάλες, μεσαίες και μικρές δυνάμεις κάθε περιφέρειας προσπαθούν να δημιουργήσουν σχέσεις ισορροπίας μεταξύ τους με σκοπό την πρόληψη επεκτατικών πολιτικών, την αποφυγή των μεταξύ τους εντάσεων και την επίτευξη της ευημερίας των λαών τους.

2.2. Συντελεστές Ισχύος

Οι συντελεστές της ισχύος αποτελούν ένα κομμάτι αντικειμενικότητας στον προσδιορισμό της ισχύος ενός κράτους. Είναι αυτοί που διαμορφώνουν τις ιδιαίτερες δυνατότητες κάθε κρατικής οντότητας, δυνατότητες που καθορίζουν την ταυτότητά της και την ξεχωρίζουν από τις άλλες κατά τα λοιπά όμοιες οντότητες. Η γεωγραφία, ο πληθυσμός, η οικονομία, οι ένοπλες δυνάμεις και η ποιότητα της κυβέρνησης είναι, λοιπόν, αυτά τα πέντε στοιχεία που μπορούν να επηρεάσουν τη θέση του κράτους μέσα στο άναρχο διεθνές σύστημα (Morgenthau, 2018, σ.185-233).

Αναλυτικότερα, ο όρος γεωγραφία περιλαμβάνει στοιχεία όπως η έκταση μιας χώρας και η γεωμορφολογία της και ως εκ τούτου αποτελεί τον πιο σταθερό παράγοντα διαμόρφωσης της ισχύος (Morgenthau, 2018, σ.188). Η ύπαρξη βουνών, ποταμών, λιμνών και θαλασσών σε συνδυασμό με το κλίμα της χώρας διαμορφώνουν την οικονομική, εμπορική, πολιτική, πολιτισμική και στρατιωτική της πορεία. Η θέση της, λοιπόν, στον χάρτη είναι ικανή να διαμορφώσει την

κουλτούρα της, τους πολιτικούς αντικειμενικούς σκοπούς[1](ΑΣΚ) και ως εκ τούτου τη σχέση της με τις γειτνιάζουσες χώρες. Η θέση της αμερικανικής ηπείρου μεταξύ δύο ωκεανών ήταν αυτή που επέτρεψε στην υιοθέτηση του δόγματος Μονρόε και του αμερικανικού απομονωτισμού, όπως και η θέση της Ρωσίας, μιας χώρας με τεράστια έκταση αλλά έλλειψη γεωγραφικών εμποδίων από δυσμάς, ήταν αυτή που επέτρεψε την εισβολή με μεγάλη ευκολία των Γερμανών (Β'ΠΠ) και των Γάλλων (Ναπολεόντειοι Πόλεμοι) στην επικράτεια της, αλλά συγχρόνως και αυτή που εμπόδισε την υποδούλωσή της.

Ο πληθυσμός αποτελεί ένα εξίσου σημαντικό στοιχείο διαμόρφωσης της ισχύος. Αν και από μόνος του, ως ποσοτική έννοια, δεν μπορεί να καταστήσει μια χώρα ισχυρή, η απουσία ενός μεγάλου πληθυσμού μπορεί να λειτουργήσει αρνητικά στη διαμόρφωση των ισορροπιών ισχύος (Morgenthau, 2018, σ.203). Μια πολυπληθής χώρα αξιοποιώντας τους πολίτες της μπορεί να μετατραπεί σε μεγάλη οικονομική και στρατιωτική δύναμη, όπως η Γερμανία και οι ΗΠΑ του 1940. Ωστόσο, ένας μεγάλος πληθυσμός έχει τη δυνατότητα να δράσει αρνητικά στην πορεία μιας χώρας, όταν οι απαιτούμενοι για τη διαβίωση του πόροι υστερούν και προκαλούν επιπλέον προβλήματα για τα κράτη (π.χ. λιμός, ασθένειες). Πέρα από το μέγεθος του πληθυσμού, καθοριστικό ρόλο παίζουν και άλλοι παράγοντες όπως το ηλικιακό φάσμα του, αλλά και η εθνική, θρησκευτική και πολιτισμική του ομοιογένεια του (Morgenthau, 2018, σ.206).

Τρίτος συντελεστής μέτρησης της ισχύος είναι η οικονομία. Μια χώρα της οποίας οι περισσότεροι οικονομικοί δείκτες έχουν θετική φορά καθίσταται οικονομικά ισχυρή. Κάθε οικονομικά ισχυρή χώρα μπορεί να εκμεταλλευτεί το γεγονός αυτό προς όφελος της, κάνοντας επενδύσεις στις υποδομές της με έργα βελτίωσης του οδικού και σιδηροδρομικού της δικτύου, των τηλεπικοινωνιών, κ.ά., που είναι χρήσιμα για την εξυπηρέτηση των αναγκών των πολιτών της, αλλά και σε περίπτωση πολέμου για την ταχύτερη ανάπτυξη των στρατιωτικών της δυνάμεων. Επενδύοντας σε άλλες χώρες (Άμεσες Ξένες Επενδύσεις-ΑΞΕ)

[1] Ως πολιτικό αντικειμενικό σκοπό ορίζουμε κάθε «*καθαρά προσδιορισμένο, αποφασιστικό και πραγματοποιήσιμο σκοπό*» που θέτει προς επίτευξη η κυβέρνηση έκαστης χώρας (Κολιόπουλος, 2008, σ.28).

δημιουργεί δεσμούς με αυτές και σχέσεις εξάρτησης που ίσως οδηγήσουν και σε συμμαχικούς δεσμούς. Η εξάρτηση αυτή είναι που υπαγορεύει τη σύμπλευση τους στο άναρχο περιβάλλον και προσφέρει ένα επίπεδο ισορροπίας (Jackson & Sørensen, 2006, σ.196-197). Ένα ακόμα σημαντικό πλεονέκτημα των οικονομικά ισχυρών χωρών είναι η δυνατότητα δέσμευσης πόρων για την προμήθεια εξοπλιστικών προγραμμάτων ή την επένδυση στη δική τους αμυντική βιομηχανία, τη βελτίωση της ποιότητας της εκπαίδευσης των στρατευμάτων τους, μετατρέποντας τελικά τη οικονομική τους ισχύ σε στρατιωτική (λ.χ. ΗΠΑ). Η στρατιωτική αποτελεσματικότητα, βέβαια, δεν είναι πάντοτε άμεσο αποτέλεσμα της οικονομικής ευμάρειας, ωστόσο, οι μεταβολές στις έως τώρα ισορροπίες της στρατιωτικής ισχύος ακολούθησαν τις αντίστοιχες παραγωγικές και η νίκη στους πολέμους έγειρε στην πλευρά με τους περισσότερους υλικούς πόρους (Kennedy, 1990, σ.562). Τέλος, στον τομέα της οικονομίας περιλαμβάνεται η ύπαρξη φυσικών πόρων, και η, εν απουσία αυτών, δυνατότητα πρόσβασης και εκμετάλλευσή τους. Η αυτάρκεια αποτελεί πηγή ισχύος. Χώρες που είχαν την τύχη να διαθέτουν πλούσια γη και υπέδαφος επιζητούν την μέγιστη δυνατή αυτονομία, ενώ παράλληλα προσπαθούν να ελέγξουν τις όποιες πλουτοπαραγωγικές πηγές είναι εκτός της σφαίρας επιρροής τους (Morgenthau, 2018, σ.190).

Επόμενος συντελεστής ισχύος δεν είναι άλλος από τις ένοπλες δυνάμεις. Μια ισχυρή χώρα στη διεθνή σκακιέρα οφείλει να διαθέτει στρατιωτική ισχύ. Αυτή δεν εξαρτάται από την ύπαρξη και μόνο στρατευμάτων αλλά και από την ποιότητα αυτών, η οποία οφείλει να συνοδεύεται από σύγχρονο στρατιωτικό εξοπλισμό και υποδομές. Ο συνδυασμός, βέβαια, των τεχνολογικών καινοτομιών, των ευφυιών στρατιωτικών ηγετών καθώς και του σωστού ποσοτικού καταμερισμού του στρατευμάτων, αποτελεί μια δυσεπίλυτη εξίσωση, η ορθότητα της οποία κρίνεται εκ των υστέρων (Morgenthau, 2018, σ.202). Παρόλα αυτά, όλες οι μεγάλες δυνάμεις ήταν και είναι στρατιωτικές δυνάμεις. Ο Ψυχρός Πόλεμος αποτελεί το πιο γλαφυρό παράδειγμα ισορροπίας ισχύος των δύο Μεγάλων, λόγω της ύπαρξης στρατιωτικής (πυρηνικής) απειλής. Η στρατιωτική υπεροχή ήταν δηλαδή η αιτία καθορισμού τους ως των δύο παγκόσμιων υπερδυνάμεων, αλλά ταυτόχρονα και ο λόγος ισορροπίας ολόκληρου του συστήματος.

Ο τελευταίος αλλά εξίσου σημαντικός συντελεστής ισχύος είναι η ποιότητα της κυβέρνησης. Με τον όρο «ποιότητα κυβέρνησης» αναφερόμαστε στη δεξιότητα της διπλωματίας, την ικανότητα της πολιτικής εξουσίας να θέτει εφικτούς στόχους και να διαλέγει τους κατάλληλους τρόπους και τα μέσα για την πραγμάτωσή τους, καθώς και τη δυνατότητα εξισορρόπησης των όποιων ανεπαρκειών (Morgenthau, 2018, σ.220-233). Όλα αυτά εξαρτώνται από τη μορφή του πολιτεύματος, τις πολιτικές φυσιογνωμίες που κυριαρχούν στην πολιτική σκηνή της χώρας, τον τρόπο επιλογής των πολιτικών αντικειμενικών σκοπών που θέτει προς υλοποίηση η κεντρική διοίκηση καθώς και τη συμμετοχή των πολιτών στην επιλογή αυτή. Η έννοια της κυβέρνησης, της πολιτικής δηλαδή εξουσίας που δρα εξ' ονόματος ενός λαού, η οποία ασκεί αποτελεσματικό έλεγχο επί ενός εδάφους και χαίρει της αναγνωρίσεως των υπολοίπων κρατών (Συρίγος, 2014, σ.112), είναι ουδέτερη. Η ποιοτική της υπεροχή έγκειται στην δυνατότητα συμμετοχής του λαού στην επιλογή των μεγάλων αποφάσεων και όχι στην παθητική τους αποδοχή (Συρίγος, 2018, σ.803). Προτάσσονται, επομένως, τα δημοκρατικά ιδεώδη, που παρόλα αυτά δεν επιβεβαιώνουν την καντιανή λογική του τερματισμού του πολέμου μεταξύ των δημοκρατιών (Kant, 1893), αποδεικνύοντας επανειλημμένως την δυνατότητά τους να μάχονται σαν να ήταν τυραννίες (Κονδύλης, 1999, σ.405). Απλώς, όπως θα συμπλήρωνε ο Κλαούζεβιτς, τα 'πολιτισμένα' κράτη επιδίδονται στην διεξαγωγή λιγότερο αιματηρών και καταστροφικών πολέμων, λόγω της πρότερης κοινωνικής τους κουλτούρας (Von Klausewitz, 1999, σ.33).

Ο σπουδαιότερος, όμως, παράγοντας εκθετικής μεταβολής της ισχύος είναι η διπλωματία και η ικανότητά της να προωθεί του κρατικούς στόχους αξιοποιώντας όλα τα διαθέσιμα μέσα και πόρους του έθνους. Αυτό είναι, βέβαια, εφικτό, όταν η κυβέρνηση είναι κατάλληλα στελεχωμένη και καταρτισμένη, ώστε να μπορεί σε συνδυασμό με την διπλωματία, να ισορροπήσει τους πολιτικούς της στόχους με τους υπάρχοντες πόρους (οικονομικούς, στρατιωτικούς), καθώς και να εξασφαλίσει την υποστήριξη του λαού που αντιπροσωπεύει και της διεθνούς κοινότητας στην οποία ζει και δρα (Morgenthau, 2018, σ.232).

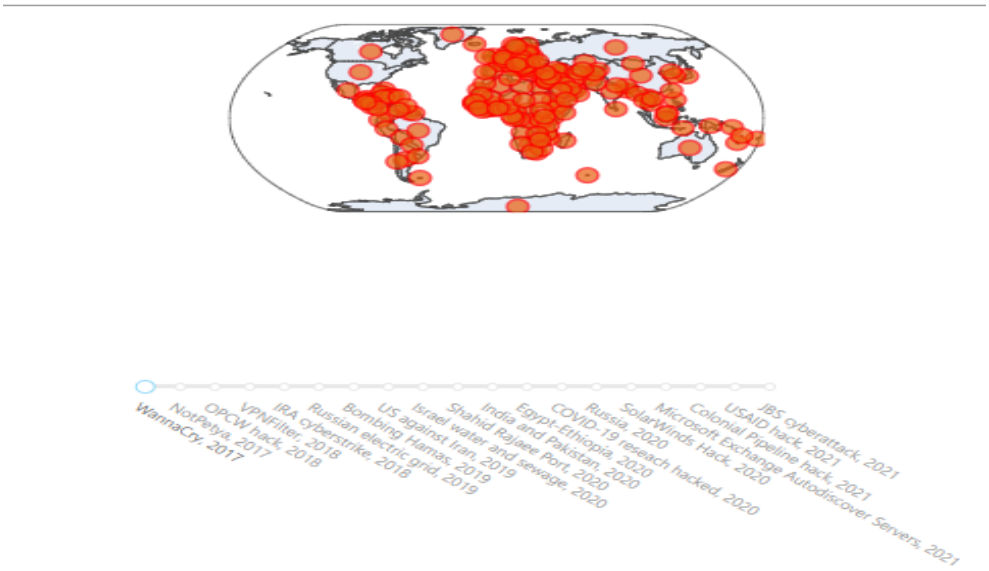
2.3. Νέες Προκλήσεις για τα κράτη

Η ισχύς, όμως, δεν αποτελεί μια ανεξάρτητη μεταβλητή. Πρέπει να μελετάται πάντα σε σχέση με την ισχύ των υπολοίπων κρατών, αλλά και σε σχέση με τις νέες τεχνολογικές εξελίξεις και τις επικείμενες απειλές που αυτές παράγουν για τα κράτη.

Η χρήση των ΤΠΕ έχει γίνει αναπόσπαστο κομμάτι της ζωής των σύγχρονων κοινωνιών επιφέροντας ριζικές αλλαγές στην παγκόσμια οικονομική και κοινωνική ζωή. Ολοένα και περισσότερες καθημερινές ενέργειες διεκπεραιώνονται με τη χρήση του διαδικτύου, του βασικού δηλαδή πυλώνα ψηφιακού μετασχηματισμού. Από τις ΤΠΕ εξαρτώνται, πλέον, βασικές και κρίσιμες λειτουργίες μιας κοινωνίας. Η επιχειρησιακή συνέχεια, επομένως, όλων των υποδομών και των υπηρεσιών ζωτικής σημασίας που αφορούν τους τομείς της υγείας, των μεταφορών, της ενέργειας, των χρηματοπιστωτικών αγορών, της παροχής νερού, των ψηφιακών εγκαταστάσεων, καθώς και της δημόσιας διοίκησης και κρατικής άμυνας και ασφάλειας (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019b), είναι απολύτως συνυφασμένη με την ασφαλή και συνεχή λειτουργία των ΤΠΕ. Ως εκ τούτου η ασφάλεια του κυβερνοχώρου, ενός *«παγκόσμιου πεδίου εντός του περιβάλλοντος πληροφοριών που αποτελείται από αλληλένδετα δίκτυα υποδομών τεχνολογίας της πληροφορίας και αποθηκευμένα δεδομένα, συμπεριλαμβανομένου του Διαδικτύου, τηλεπικοινωνιακών δικτύων, συστημάτων υπολογιστών και ενσωματωμένων επεξεργαστών και ελεγκτών για την παραγωγή και χρήση των πληροφοριών από ιδιώτες και οργανισμούς»* (DoD, 2016), (European Commission, 2018) να αποτελεί μείζονος σημασίας προτεραιότητα των κρατών για τη διασφάλιση της οικονομικής ευμάρειας, των θεμελιωδών δικαιωμάτων και προπάντων της εθνικής ασφάλειας και κυριαρχίας.

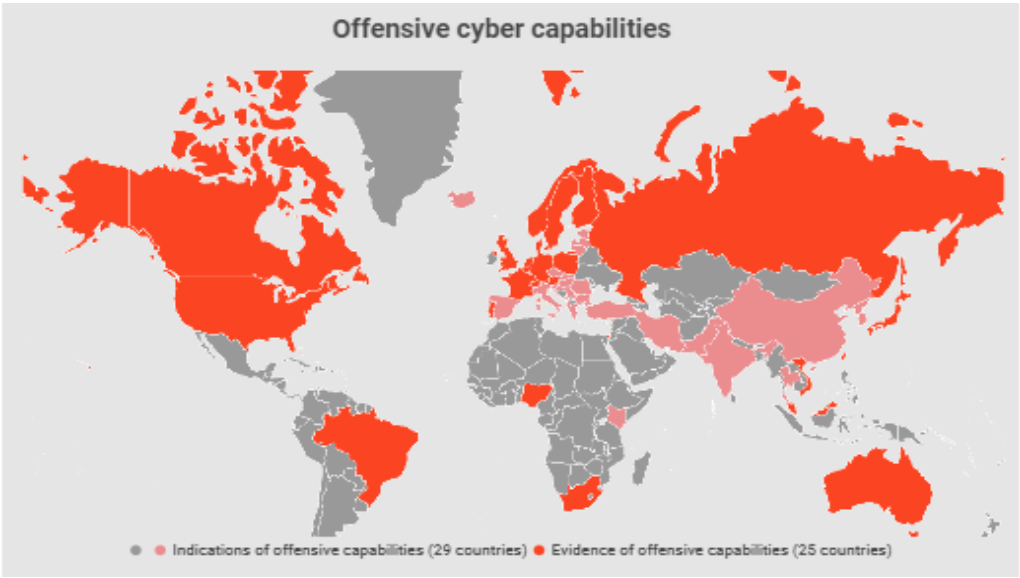
Η ολοένα και μεγαλύτερη εξάρτηση από τον κυβερνοχώρο έχει φέρει στο προσκήνιο μια νέα απειλή για την ασφάλεια των κρατών, καθώς ο «εχθρός» βρίσκεται, πλέον, εντός των τειχών. Την τελευταία δεκαετία έχουν καταγράφει παγκοσμίως δεκάδες επιθέσεις από και προς τα πληροφοριακά συστήματα (Εικόνα Ι), ενώ η αυξητική τους τάση έχει εκτιναχθεί από το ξέσπασμα της

πανδημίας του Covid 19 (Maigre, 2022). Το γεγονός αυτό σε συνδυασμό με την έλλειψη αποτελεσματικών αποτρεπτικών μέσων έχει οδηγήσει το ένα τρίτο των



Εικόνα 1 Επιθέσεις σε πληροφοριακά συστήματα ανά τον κόσμο, στο DigWatch, «UN GGE & OEWG», πηγή: https://dig.watch/processes/un-gge (έγινε πρόσβαση στις 8 Μαρίου 2022).

χωρών στην ανάπτυξη στρατιωτικών ικανοτήτων διεξαγωγής επιθετικών ενεργειών στον κυβερνοχώρο για την προστασία του (Εικόνα ΙΙ) (Digital Watch,



Εικόνα 2 Επιθετικές κυβερνο-ικανότητες παγκοσμίως, στο DigWatch, «UN GGE & OEWG», πηγή: https://dig.watch/processes/un-gge (έγινε πρόσβαση στις 8 Μαρίου 2022).

χ.χ.), ενώ η διαχωριστική γραμμή μεταξύ αμυντικών και επιθετικών εργαλείων, μέσων και ενεργειών είναι δυσδιάκριτη. Τα μέσα που χρησιμοποιούνται για την άμυνα χρησιμοποιούνται και για την επίθεση, ενώ η αποτελεσματικότητά τους

εξαρτάται από τον ταχύτατο κύκλο ζωής των κυβερνο-όπλων, η οποία μπορεί να χαθεί ακόμα και πριν τη χρήση τους (Robinson κ.ά., 2015).

Η σπουδαιότητα του κυβερνοχώρου και η ανάγκη προστασία του ώστε να διασφαλιστεί η κρατική ασφάλεια, έχει ήδη γίνει αντιληπτή από τα κράτη υιοθετώντας την στα στρατιωτικά τους δόγματα. Μάλιστα, τα κράτη-μέλη του Συμφώνου της Βόρειο-Ατλαντικής Συμμαχίας ανακήρυξαν τον κυβερνοχώρο σε πέμπτο πεδίο στρατιωτικής δράσης μετά τη γη, τη θάλασσα, τον αέρα και το διάστημα.[2]

Η προστασία και αυτοάμυνα των κρατών από τις εξωτερικές απειλές δεν αποτελεί καινοτομία των ημερών μας. Η ασφάλεια είναι πρωταρχικός στόχος των κρατών και ήδη συμβατικά κατοχυρωμένο δικαίωμα τους από τη Χάρτα των ΗΕ. Κάθε κράτος οφείλει, επομένως, να θωρακίζεται από τις όποιες απειλές μπορούν να θέσουν σε κίνδυνο την ευημερία των πολιτών του. Οι απειλές αυτές διαφέρουν από εποχή σε εποχή και ανανεώνονται με το πέρασμα των χρόνων και την εξέλιξη της τεχνολογίας. Κάποτε απειλή για τα κράτη αποτελούσε το κανόνι, αργότερα το πλοίο και το αεροπλάνο, σήμερα αποτελεί ο κυβερνοχώρος και τα εργαλεία του. Οι νέοι μέθοδοι δράσης, αντιμετώπισης και πρόληψης των κυβερνοαπειλών επιζητούν την ανανέωση του θεσμικού πλαισίου με σκοπό την συμπερίληψη των καινοτόμων και συνεχώς εξελισσόμενων πηγών κρατικής ανασφάλειας. Το θεσμικό κενό που τίθεται λόγω της μη ρητής αναφοράς του κυβερνοχώρου στα διεθνή κείμενα είναι συνέπεια της παλαιότητας αυτών που μειώνεται ωστόσο συνεχώς, λόγω της συνεχούς ανάπτυξης νέων, δεσμευτικών ή μη, περιφερειακών ή διεθνών συμβάσεων. Τα κράτη συντάσσουν καινούργιες και επικαιροποιημένες συμβάσεις ή ερμηνεύουν υφιστάμενα κείμενα με βάση τα σημερινά δεδομένα, ώστε να μειώσουν το χάσμα.

Η συμβατική αυτή αναθεώρηση έχει, όμως, ως αποτέλεσμα τη δημιουργία ενός «νέου» δικαιώματος για τα κράτη, το δικαίωμα στην κυβερνοασφάλεια. Αυτό το

[2] Στη Σύνοδο Κορυφής των κρατών-μελών του ΝΑΤΟ το 2016 ανακηρύχθηκε ο κυβερνοχώρος σε πέμπτο πεδίο στρατιωτικής δράσης για τα μέλη του Βορειοατλαντικού Συμφώνου (NATO, 2016b).

δικαίωμα, αν και αποτελεί επέκταση προγενέστερων δικαιωμάτων, όπως, το δικαίωμα στην ασφάλεια-αυτοάμυνα, τη μη επέμβαση στις εσωτερικές υποθέσεις και την ειρηνική επίλυση των διαφορών, επισύρει μια σειρά υποχρεώσεων των κρατών προς τη διεθνή κοινότητα. Τα κράτη επεκτείνουν την κυριαρχία τους, αλλά δεσμεύονται να ακολουθούν κοινώς αποδεκτούς κανόνες απόρροια διεθνών διακρατικών διαβουλεύσεων και να δρουν τουλάχιστον με βάση τις διεθνείς νόρμες της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο. Τίθενται δηλαδή τα ελάχιστα δυνατά όρια συμβίωσης, τα οποία μπορούν να διευρυνθούν και να αποκτήσουν περισσότερο βάθος στα πλαίσια περιφερειακών, διμερών ή και πολυμερών διακρατικών συναντήσεων.

2.4. Χρήσιμοι ορισμοί

Για την καλύτερη κατανόηση της ανάλυσης που θα ακολουθήσει σχετικά με τη δυνατότητα χρήσης του κυβερνοχώρου ως πεδίου διεξαγωγής διακρατικών αντιπαραθέσεων θα παρατεθούν κάποιοι χρήσιμοι ορισμοί.

Αν και ένας ευρέως αποδεκτός ορισμός της έννοιας της κυβερνοασφάλειας δεν υπάρχει, «*αυτή καλύπτει τις ασφαλιστικές δικλείδες και τις δράσεις που μπορούν να χρησιμοποιηθούν για την προστασία του κυβερνοχώρου, τόσο σε στρατιωτικό, όσο και σε μη στρατιωτικό πεδίο, από εκείνες τις απειλές που σχετίζονται με ή που μπορούν να βλάψουν τα ανεξάρτητα δίκτυα και τις υποδομές πληροφόρησης. Επιχειρεί να διατηρήσει τη διαθεσιμότητα και την ακεραιότητα των δικτύων και των υποδομών καθώς και την εμπιστευτικότητα των πληροφοριών που αυτά παρέχουν*» (European Commission, 2013).[3] Επομένως, η κυβερνοασφάλεια έχει ως στόχους την

[3] Βασικό στόχο της κυβερνοασφάλειας αποτελεί η διασφάλιση της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας των δικτύων, υποδομών και πληροφοριών. Πιο συγκεκριμένα, ο όρος «διαθεσιμότητα» δηλώνει τη διασφάλιση της ταχείας και αξιόπιστης πρόσβασης σε πληροφορίες καθώς και της χρήσης αυτών (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019, σ.8). Ο όρος «ακεραιότητα» αναφέρεται στην προστασία των πληροφοριών, είτε από την τροποποίησή τους με καταχρηστικό σκοπό, είτε από την καταστροφή τους, ή τη διασφάλιση της γνησιότητάς τους, και ο όρος «εμπιστευτικότητα» αφορά την προστασία των πληροφοριών, των δεδομένων ή των περιουσιακών στοιχείων των χρηστών από μη

πρόβλεψη, την ανίχνευση, την αντίδραση και την ανάκαμψη από κυβερνοπεριστατικά, τα οποία, εσκεμμένα ή μη, μπορούν να επηρεάσουν την ομαλή λειτουργία των δικτύων και υποδομών πληροφορικής, επιφέροντας ποικίλου μεγέθους ζημιές, τόσο ατομικά, όσο και συλλογικά (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019). Τέτοια περιστατικά θα μπορούσαν να είναι η κλοπή δεδομένων προσωπικού χαρακτήρα, χρηματικές απάτες, στοχευμένα χτυπήματα σε επιχειρήσεις ή σε υποδομές ζωτικής σημασίας μέχρι και παρεμβάσεις σε εκλογικές διαδικασίες με διοργάνωση και εκτέλεση εκστρατειών παραπληροφόρησης. Γίνεται έτσι κατανοητό, ότι η έννοια της κυβερνοασφάλειας δεν αφορά αποκλειστικά την ασφάλεια των δικτύων και των πληροφοριών, αλλά κάθε ενέργεια που κάνει χρήση των ψηφιακών τεχνολογιών. Ωστόσο, ο άυλος και χωρίς σύνορα χαρακτήρας του διαδικτύου αποτελεί εργαλείο για τους κάθε είδους «δράστες» (π.χ. εγκληματικές οργανώσεις, ακτιβιστικές ομάδες, κράτη), καθώς μπορούν να προκαλούν προβλήματα με εθνικό, περιφερειακό και διεθνή αντίκτυπο, χωρίς να επωμίζονται την ευθύνη της κακόβουλης ενέργειάς τους.

Η κυβερνοασφάλεια ως ένας πολυδιάστατος όρος περιλαμβάνει ένα ευρύ φάσμα προκλήσεων. Ως εκ τούτου, στην κυβερνοασφάλεια υπάγονται μια σειρά από θεματικές, των οποίων η ανάδειξη και ανάλυση θα ενισχύσει την κατανόηση, τόσο της κυβερνοασφάλειας, όσο και της σπουδαιότητάς της. Οι έννοιες αυτές καταδεικνύουν με τον καλύτερο τρόπο τα τρωτά σημεία του παγκόσμιου πληροφοριακού περιβάλλοντος, και την ανάγκη δημιουργίας ενός πλέγματος ασφαλείας, ώστε να μπορέσει να προστατευτεί η διεθνής κοινότητα από τις διαφορετικού κινήτρου και προελεύσεως απειλές. Η δημιουργία μιας επιτυχημένης «αμυντικής ζώνης» στον κυβερνοχώρο, η οποία δεν θα παρουσιάζει κενά ασφαλείας ή και θα μπορεί να ανταπεξέλθει σε οποιαδήποτε χτύπημα και ίσως και να ανταποδώσει, προϋποθέτει τη συλλογική δράση, αλλά πάνω απ' όλα την κατανόηση των κενών και των δυνατοτήτων που ήδη υπάρχουν σε αυτόν.

εξουσιοδοτημένη πρόσβαση σε αυτά ή κοινολόγησή τους (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019, σ.8).

Το κυβερνοέγκλημα (cyber crime) αφορά «*μια μεγάλης ποικιλίας εγκληματικές ενέργειες όπου οι ηλεκτρονικοί υπολογιστές και τα συστήματα πληροφοριών εμπλέκονται, είτε ως πρωταρχικά εργαλεία, είτε ως πρωταρχικοί στόχοι. Περιλαμβάνει παραδοσιακά αδικήματα, όπως η απάτη και η πλαστογραφία, αδικήματα περιεχομένου, π.χ. παιδική πορνογραφία, και αδικήματα που αφορούν μόνο τη λειτουργία των υπολογιστών, όπως κακόβουλα λογισμικά*». (European Commission, 2018, σ.15).

Οι επιχειρήσεις που διενεργούνται στον κυβερνοχώρο (κυβερνοεπιχειρήσεις) «*χρησιμοποιούν τις δυνατότητές του με πρωταρχικό σκοπό την επίτευξη στόχων σε αυτόν ή μέσω αυτού. Χρησιμοποιούν δηλαδή τους ηλεκτρονικούς υπολογιστές για να διακόψουν, να αρνηθούν, να υποβαθμίσουν, ή να καταστρέψουν αποθηκευμένες πληροφορίες σε υπολογιστές και δίκτυα υπολογιστών ή τους ίδιους τους υπολογιστές και τα δίκτυα*» (DoD, 2016). Επιπλέον, μπορούν να αξιοποιηθούν είτε ως προπαρασκευαστικές ενέργειες μιας άλλης, κύριας επίθεσης, είτε ως τρόπος απόκτησης κρίσιμων πληροφοριών/ κυβερνοκατασκοπεία (στρατιωτικές δυνατότητες, προθέσεις του αντιπάλου κλπ.), ή και επικουρικά σε μια ευρύτερη στρατιωτική επιχείρηση (Πιπύρος & Μήτρου, 2018).

Η έννοια της κυβερνοεπίθεσης (cyber attack) χρησιμοποιείται για να περιγράψει διάφορους τύπους εχθρικών ή κακόβουλων ενεργειών στον κυβερνοχώρο. Οι επιθέσεις αυτές δεν οδηγούν συνεκδοχικά στην ενεργοποίηση ενεργειών αυτοάμυνας, όπως οι ένοπλες επιθέσεις. Υπάρχουν ωστόσο και περιπτώσεις όπου ο 'πόλεμος' στηρίζεται αποκλειστικά στην κυβερνοεπίθεση (Εσθονία 2007).[4] Σκοπός σε αυτές τις περιπτώσεις είναι η χρήση των δυνατοτήτων που μας παρέχουν τα δίκτυα και οι υποδομές πληροφορικής, ώστε να επιτευχθούν στρατηγικά ή στρατιωτικά πλεονεκτήματα έναντι του αντιπάλου (English Oxford Company, χ.χ.). Για να θεωρηθεί, επομένως, μια κυβερνοεπίθεση ως κυβερνοπόλεμος θα πρέπει, πέρα από τη χρήση του κυβερνοχώρου με τρόπο που να επιφέρει επιζήμια για μια κρατική οντότητα αποτελέσματα, να υπάρχει και

[4] Βλ. σ.35.

πρόθεση (Robinson κ.ά., 2015) που αποσκοπεί στην προώθηση των πολιτικών αντικειμενικών σκοπών ενός κράτους.

ΚΕΦΑΛΑΙΟ 3:
ΝΕΕΣ ΔΥΝΑΤΟΤΗΤΕΣ ΣΤΟΝ ΠΟΛΕΜΟ

Ο κυβερνοχώρος έχει χρησιμοποιηθεί πολλές φορές για την προώθηση των πολιτικών σκοπών κρατικών και μη κρατικών δρώντων κάνοντας χρήση των δυνατοτήτων ή των ανεπαρκειών των δικτύων και των συστημάτων πληροφορικής. Ο άνευ συνόρων χαρακτήρας του κυβερνοχώρου, η αδυναμία απόδοσης ευθυνών, η ταχύτητα, οι επιθετικές του δυνατότητες καθώς και το χαμηλό κόστος των στρατιωτικών επιχειρήσεων που διενεργούνται μέσω αυτού ή και με τη χρήση αυτού, αποτελούν ένα πλεονέκτημα για όποιον είναι τεχνολογικά εξελιγμένος και ικανός να προχωρήσει στη χρήση των ανωτέρω. Η διεξαγωγή πολέμων, είτε αποκλειστικά μέσω κυβερνοεπιχειρήσεων, είτε με τη χρήση αυτών ως συμπληρωματικών μέσων μιας συμβατικής επιθέσεως, δημιουργεί συγκριτικό πλεονέκτημα έναντι του αντιπάλου με την επιφύλαξη όμως, ότι η όλο και μεγαλύτερη τεχνολογική μας εξάρτηση, μας καθιστά πιο ευάλωτους σε τέτοιου είδους απειλές.

Η σύγκριση των κυβερνοεπιχειρήσεων με τις κλασσικές προσεγγίσεις του πολέμου, παρουσιάζει τη σύγκλισή τους και ταυτόχρονα αναδεικνύει τις μεταξύ τους διαφορές καταδεικνύοντας τον καινοτόμο χαρακτήρα του κυβερνοχώρου. Ο κυβερνοχώρος προφανώς και αποτελεί νέο πεδίο δράσης, ωστόσο, δεν είναι κάτι το επαναστατικό (Rantapelkonen & Salminen, 2013, σ.169). Απλά αντανακλά την ταχεία εξέλιξη της τεχνολογίας. Προς αυτό συντείνει και η επακόλουθη ανάλυση του υβριδικού πολέμου, η οποία επιβεβαιώνει το γεγονός ότι το μοτίβο της συμπληρωματικότητας των συμβατικών και μη μέσων στη διεξαγωγή στρατιωτικών επιχειρήσεων, δεν αποτελεί κάποια καινοτομία στην διαμόρφωση της στρατιωτικής στρατηγικής. Συνηγορεί, ωστόσο, στην αλλαγή του τρόπου οργάνωσης και εκτέλεσης των πολεμικών επιχειρήσεων, συνδυάζοντας με έναν απρόβλεπτο τρόπο το σύνολο όλων των πεδίων πολέμου και όλων των στρατηγικών επιπέδων με τις νέες τεχνολογίες χωρίς παρόλα αυτά να αντικαθιστά την ουσία της έννοιας του πολέμου.

3.1. Κυβερνοπόλεμος και στρατηγικές προσεγγίσεις

Η μελέτη των έργων των κλασικών θεωρητικών της στρατηγικής σκέψης καθώς και των μελετών των στρατηγικών αναλυτών οδηγεί στην παρουσίαση των ομοιοτήτων και των διαφορών του κυβερνοπολέμου με τον 'παραδοσιακό' πόλεμο. Αν και τα κυβερνοεργαλεία και ο κυβερνοχώρος δεν μπορούν να αντικαταστήσουν πλήρως τα συμβατικά μέσα διεξαγωγής του πολέμου, η πρακτική του αξία δεν μπορεί να αναιρεθεί.

3.1.1. Κλαούζεβιτς

Η πρώτη και άκρως διαχρονική θεωρία πολέμου που θα παρουσιαστεί είναι αυτή του Καρλ φον Κλαούζεβιτς. Η κλαουζεβιτσιανή εκδοχή του πολέμου, εκ πρώτης όψεως, φαίνεται να μη συνάδει με την επιλογή του κυβερνοπολέμου ως ικανού τρόπου επίτευξης νίκης στο στρατιωτικό πεδίο. Για τον Κλαούζεβιτς, ο πόλεμος είναι μια πράξη βίας, μια μονομαχία σε μεγάλη κλίμακα όπου η νίκη είναι αποτέλεσμα αποφασιστικών μαχών (Von Klausewitz, 1999, σ.31). Στις μάχες αυτές συμμετέχει το κύριο μέρος των στρατιωτικών δυνάμεων των αντιπάλων και στόχος είναι η καταστροφή των ενόπλων δυνάμεων του εχθρού (Von Klausewitz, 1999, σ.58). Υπό αυτή τη λογική, εφόσον οι κυβερνοεπίθεσεις δεν επιφέρουν θανατηφόρα αποτελέσματα, αυτομάτως δεν πληρούν το κριτήριο υπαγωγής τους στις μορφές του πολέμου. Το γεγονός αυτό, όμως, δεν σημαίνει ότι δεν χρησιμοποιούν μέσα άσκησης εξαναγκασμού. Τα τεχνολογικά μέσα χρησιμοποιούν μικρή δόση δύναμης που παράγει μεγάλη ποσότητα βίας, (Θεοφίλης, 2018) κατατάσσοντας, έτσι, τις κυβερνοεπιχειρήσεις στην κατηγορία των ασύμμετρων απειλών. Βέβαια, δεν μπορεί να παραληφθεί το γεγονός ότι μια κυβερνοεπίθεση σε μια κρίσιμη υποδομή, όπως για παράδειγμα ένα νοσοκομείο, μπορεί να έχει θανάσιμα αποτελέσματα. Τα θύματα είναι εκτός πεδίου μάχης που ωστόσο εμμέσως συνεπικουρούν στην επίτευξη των πολιτικών αντικειμενικών σκοπών του επιτιθέμενου και στην υποταγή του αντίπαλου δέους στη θέλησή του. Η ως άνω έμμεση στρατηγική προσέγγιση χρήσης του άμαχου πληθυσμού για την

επίτευξη στρατιωτικών στόχων, μπορεί να μην ανταποκρίνεται στις διδαχές του Κλαούζεβιτς, ωστόσο, πετυχαίνει τον στόχο, την προώθηση δηλαδή των φίλιων πολιτικών αντικειμενικών σκοπών (Von Klausewitz, 1999, σ.57). Μάλιστα και ο ίδιος ο Κλαούζεβιτς κάνει αναφορά στη νίκη χωρίς μάχη, θεωρώντας πως αυτή η νίκη είναι αποτέλεσμα της επίγνωσης της επικείμενης ήττας στο στρατιωτικό πεδίο από τον αντίπαλο (Von Klausewitz, 1999).

Ο Κλαούζεβιτς αφιερώνει, επίσης, μεγάλο μέρος του έργου του στην αλληλεπίδραση της στρατηγικής με την τακτική[5] και τη σημασία αυτής της αλληλεπίδρασης στο πεδίο της μάχης (Κολιόπουλος, 2008, σ.167; Von Klausewitz, 1999). Πιο συγκεκριμένα, υποστηρίζει πως κάθε αλλαγή στη φύση της τακτικής, μπορεί να επιφέρει αλλαγές στο επίπεδο της στρατηγικής, και κατ' αναλογία κάθε τεχνολογική εξέλιξη μπορεί να τροποποιήσει τα μέσα και τους τρόπους που θα επιλεγούν για την επίτευξη των πολιτικών αντικειμενικών σκοπών. Ως εκ τούτου, η σχετικά σύγχρονη δυνατότητα χρήσης του κυβερνοχώρου για τη διενέργεια επιχειρήσεων προώθησης των πολιτικών στόχων, αποτελεί μια τακτική αλλαγή που θα δώσει νέες διαστάσεις στο επίπεδο της στρατιωτικής στρατηγικής και συνακόλουθα στον τρόπο διεξαγωγής του πολέμου.

Τρίτο και τελευταίο κομμάτι της κλαουζεβιτσιανής θεωρίας, στο οποίο θα γίνει αναφορά, είναι η πληροφορία (Von Klausewitz, 1999, σ.106-108). Η σπουδαιότητα της πριν την έναρξη των εχθροπραξιών, καθώς και κατά τη διάρκεια της διεξαγωγής του πολέμου είναι εξέχουσας σημασίας. Η απουσία αξιόπιστων και ακριβών πληροφοριών κατά την εκπόνηση των επιχειρησιακών σχεδίων ('ομίχλη του πολέμου') καθιστά έτι δυσκολότερη τη δουλεία της στρατιωτικής και της πολιτικής ηγεσίας (Von Klausewitz, 1999, σ.117-118, 230-235). Ο πόλεμος είναι

[5] Η έννοια της 'υψηλής στρατηγικής' περιλαμβάνει τη χρήση όλων μέσων που έχει στη διάθεση του ένα κράτος, τα οικονομικά και τα στρατιωτικά, με σκοπό την πραγμάτωση των πολιτικών αντικειμενικών σκοπών του. Με τον όρο 'στρατιωτική στρατηγική' γίνεται μνεία σε όλα τα διαθέσιμα στρατιωτικά μέσα που διαθέτει το κράτος ώστε να προωθήσει τους σκοπούς στου σε μια στρατιωτική σύγκρουση. Με τον όρο 'επιχειρησιακή τέχνη' αναφερόμαστε στην χρήση στρατιωτικών μονάδων για την επίτευξη στρατιωτικών στόχων στο πλαίσιο ενός θέατρου επιχειρήσεων, ενώ με τον όρο 'τακτική' ορίζεται η χρήση των στρατιωτικών μονάδων για την επίτευξη των πολιτικών σκοπών ενός κράτους σε μια συγκεκριμένη μάχη (Κολιόπουλος, 2008, σ.44-45, 2011, σ.29; Possen, 1984).

αποτέλεσμα πολιτικής απόφασης και συνεπώς η αδυναμία λήψης των απαραίτητων πληροφοριών για την κατάσταση των φίλιων και των εχθρικών δυνάμεων στο πεδίο της μάχης, αλλά και εκτός αυτού, την άποψη των κοινωνιών για την ανάγκη διεξαγωγής του πολέμου, αποτελεί υψίστης σπουδαιότητας στοιχείο για τη λήψη των αποφάσεων. Στις μέρες μας, η δυνατότητα χρήσης των τεχνολογιών πληροφορικής και επικοινωνιών για την απόκτηση ζωτικών για τον αντίπαλο πληροφοριών ή για την παρακώλυση του εχθρού από την εύρεση πληροφοριών ή επικοινωνίας, μπορεί να επιδράσει, τόσο θετικά, ξεκαθαρίζοντας αυτό το ομιχλώδες πεδίο, όσο και αρνητικά, θολώνοντας το έτι περισσότερο. Όλες αυτές οι απρόβλεπτες, για την έκβαση του πολέμου, ενέργειες είναι που μετατρέπουν τελικά τον πόλεμο από μια απλή πράξη σε κάτι πιο σύνθετο, αποδεικνύοντας πως η απλότητα δεν συνεπάγεται ευκολία (Von Klausewitz, 1999). Η 'τριβή' που προκαλεί η στρατιωτική χρήση του κυβερνοχώρου δρα εκθετικά στην έκβαση των επιχειρησιακών διεργασιών με τρόπο που στο 'κορυφαίο σημείο της επίθεσης' οι αντιμαχόμενες δυνάμεις να μην είναι ικανές να εξαργυρώσουν τον καρπό των κόπων τους (Von Klausewitz, 1999). Με επιθέσεις, παραδείγματος χάριν, κατά των ψηφιακών (πλέον) υποδομών command and control μιας κρατικής οντότητας, οι οποίες είναι ζωτικής σημασίας για την διεξαγωγή συντονισμών στρατιωτικών επιχειρήσεων, δύναται να τερματιστεί ο πόλεμος, καθώς στο 'κορυφαίο σημείο της επίθεση' δεν θα είναι ικανή να αναπτύξει στο μέγιστο τις δυνάμεις της και να πετύχει την υπεροχή που απαιτείται για την συνθηκολόγηση και την επακόλουθη κατοχύρωση των πολιτικών της επιδιώξεων. Συνεπώς, ακόμη και αν οι κυβερνοεπιθέσεις δεν αποτελούν μια νέα μορφή πολέμου και απλώς είναι ένα νέο εργαλείο στο πλαίσιο διεξαγωγής του, ο κυβερνοχώρος αποτελεί πλέον ένα πεδίο προώθησης στρατηγικών στόχων (Θεοφίλης, 2018).

3.1.2. Σουν Τσου

Η δεύτερη θεωρία πολέμου στην οποία θα γίνει μνεία είναι εκείνη του Σουν Τσου. Η έμμεση προσέγγιση που προτείνει στη διεξαγωγή του πολέμου και ο τρόπος επίτευξης της νίκης φαίνεται να είναι περισσότερο ταιριαστή με τον κυβερνοπόλεμο συγκριτικά με τον Κλαούζεβιτς. Αναλυτικότερα, ο κινέζος

θεωρητικός δίνει ιδιαίτερη έμφαση στον σύντομο πόλεμο στοχεύοντας στην οικονομία δυνάμεων και σε μια οριστική έκβαση του πολέμου χωρίς παρατεταμένες εχθροπραξίες που μόνο επιζήμιες μπορούν να προβούν τόσο για το στράτευμα όσο και για την οικονομία των δύο αντιμαχόμενων πλευρών. Προς επίτευξη αυτού, θα πρέπει η δράση των στρατευμάτων να είναι σαν το 'νερό' (ΣΟΥΝ ΤΣΟΥ, 2008, σ.104). Να προσαρμόζονται δηλαδή ανάλογα με τις ανάγκες σε κάθε συνθήκη, σε κάθε πεδίο μάχης, σε κάθε εχθρό. Αυτό, βέβαια, είναι εφικτό μόνο εφόσον έχεις πρώτα απόλυτη γνώση των δικών σου δυνατοτήτων και έπειτα εκείνων του αντιπάλου, καθώς όπως χαρακτηριστικά αναφέρει *«όταν γνωρίζεις καλά τον εχθρό και τον εαυτό σου, και εκατό μάχες να δώσεις, θα τις κερδίσεις»* (ΣΟΥΝ ΤΣΟΥ, 2008, σ.66). Προς επίτευξη αυτού, απαραίτητη κρίνεται και η παραπλάνηση του αντιπάλου, καθώς κάθε επιτυχημένη *«στρατιωτική επιχείρηση συνεπάγεται παραπλάνηση»* (ΣΟΥΝ ΤΣΟΥ, 2008,). Η χρήση του κυβερνοχώρου είναι ικανή να συνεισφέρει στους ως άνω τομείς, καθώς οι φίλιες δυνάμεις μπορούν να διεξάγουν έρευνες χωρίς να γίνουν αντιληπτές από τον εχθρό, υποκλέπτοντας πληροφορίες που αφορούν τον αντίπαλο, όπως οι προθέσεις του, οι ικανότητές του και τα τρωτά του σημεία. Σκοπός είναι ο αντίπαλος να διαμορφώσει λανθασμένη άποψη για τις δικές μας δυνατότητες και προθέσεις και έτσι σε συνδυασμό με την από πλευράς μας καλύτερη πληροφόρηση, να είμαστε σε θέση να τον αιφνιδιάσουμε και να κερδίσουμε τη μάχη.

Η χρήση, ακόμη, του κυβερνοχώρου δύναται να οδηγήσει στην ιδανική νίκη, αυτή δηλαδή που επιτυγχάνεται χωρίς καν να δοθεί μάχη (ΣΟΥΝ ΤΣΟΥ, 2008, σ.53). Δεν είναι παράλογο να ειπωθεί, ότι με τη χρήση των ΤΠΕ προωθούνται πολιτικοί και στρατιωτικοί σκοποί χωρίς να απαιτείται παράλληλη στρατιωτική υποστήριξη, η οποία συνεπάγεται την κινητοποίηση των ανθρώπινων και οικονομικών πόρων μιας κοινωνίας. Αλλά ακόμα και αν δεν αποφευχθεί ο πόλεμος, ο συνδυασμός συλλογής πληροφοριών, παραπληροφόρησης του αντιπάλου, δημιουργίας κωλυμάτων στην επικοινωνία του, καθώς και η δυσκολία απόδοσης ευθυνών έχει ως αποτέλεσμα την κατάπτωση του ηθικού του πληττόμενου λαού, κομβικού

στοιχείου για την νομιμοποίηση των στρατιωτικών διεργασιών και ως εκ τούτου για τη συνέχιση των εχθροπραξιών (ΣΟΥΝ ΤΣΟΥ, 2008).[6]

3.1.3. Ναυτική Στρατηγική

Η σύγκριση της ναυτικής στρατηγικής με τον κυβερνοπόλεμο δεν παρουσιάζει πολλές ομοιότητες. Σημείο σύγκλισης θα μπορούσε να θεωρηθεί η προσπάθεια επιβολής ελέγχου. Ωστόσο, ο θαλάσσιος έλεγχος, όπως και ο έλεγχος του κυβερνοχώρου, ποτέ δεν μπορεί να είναι απόλυτος (Κολιόπουλος, 2008, σ.191; Corbett, 2020, σ.91-106.). Σε περίπτωση, επομένως, πολέμου ο αποτελεσματικός έλεγχος των πληροφοριών που διακινούνται μέσω του κυβερνοχώρου ενδυναμώνει τις ενέργειες προώθησης των στρατιωτικών στόχων και παράλληλα προκαλεί σύγχυση στο αντίπαλο δέος. Εφικτή, επίσης, και στα δύο πεδία πολέμου- θάλασσα & κυβερνοχώρος- είναι η στρατηγική της εξουθένωσης. Ένας θαλάσσιος αποκλεισμός κατά Κόρμπετ, μπορεί να έχει στόχο τις εχθρικές ναυτικές δυνάμεις προκαλώντας τες να αποπλεύσουν, ώστε να δοθεί ναυμαχία, μπορεί, όμως, ο στόχος να είναι απλά η εξασθένιση της οικονομίας του αντιπάλου εξαναγκάζοντας τον να συνθηκολογήσει (Κολιόπουλος, 2008, σ.192-196; Corbett, 2020). Ομοίως και ο κυβερνοπόλεμος μπορεί να χρησιμοποιηθεί με στόχο την πρόκληση οικονομικών ανεπαρκειών με στοχευμένα 'χτυπήματα' εναντίον των χρηματοπιστωτικών ιδρυμάτων, του χρηματιστηρίου, μεγάλων παραγωγικών μονάδων, κ.ο.κ. Αυτό έχει ως αποτέλεσμα την οικονομική και ηθική εξουθένωση της αντίπαλης κοινωνίας αλλά και της πολιτικής ηγεσίας, η οποία καθίσταται ανίκανη να ικανοποιήσει τις ανάγκες των πολιτών της καθώς και να υποστηρίξει τη συνέχιση των πολεμικών διεργασιών. Η κυβερνοεπιχείρηση, βέβαια, μπορεί να στηρίζεται αποκλειστικά στη διατάραξη της οικονομίας (οικονομικός, νομισματικός πόλεμος), είτε ως αντίποινα σε μια εχθρική ενέργεια που δεν 'δικαιολογεί' ενός παραδοσιακού τύπου πόλεμο, είτε διότι η επίτευξη των

[6] Την ιδέα της 'κάμψης της θέλησης του αντιπάλου', βέβαια, δεν συμμερίζεται μόνο ο Σουν Τσου αλλά και ο Τζον Φρέντερικ Φούλερ. Ο βρετανός αξιωματικός διεύρυνε την έννοια του πολέμου 'ελιγμού' δίνοντας έμφαση στη θέληση του διοικητή για την πραγματοποίηση ενός σχεδίου δράσης καθώς και στη θέληση των στρατευμάτων του να την επιτελέσουν.

πολιτικών αντικειμενικών σκοπών, δεν απαιτεί την περαιτέρω κλιμάκωση της διαμάχης.

3.1.4. Αεροπορική Στρατηγική

Από την άλλη, η αεροπορική στρατηγική προσομοιάζει αρκετά με τις κυβερνοεπιχειρήσεις. Συγκεκριμένα, όπως διατυπώνει και ο Ντούετ, δεν υπάρχει διάκριση μεταξύ στρατιωτικών και μη στόχων. Τα χτυπήματα της αεροπορίας μπορεί να στοχεύουν και κατά αστικών, εμπορικών και βιομηχανικών κέντρων, όπως οι κυβερνοεπιθέσεις να κατευθύνονται εναντίον μη στρατιωτικών και μη κυβερνητικών στόχων. Συνέπεια αυτού του γεγονότος είναι η πτώση του ηθικού του αντιπάλου και η άρνηση του λαού να αντισταθεί (Κολιόπουλος, 2008, σ.228; Douhet, χ.χ.). Η πτώση του ηθικού μπορεί να αποσκοπεί και στη διεξαγωγή ενός πολέμου ελιγμού -κομβικό κομμάτι της αεροπορικής στρατηγικής. Σε αυτό ο αντίπαλος αντιμετωπίζεται ως σύστημα το οποίο και πρέπει να αποδιοργανωθεί (Rantapelkonen & Salminen, 2013, σ.178). Ο Γουόρντεν υποστήριξε ένα σύστημα πέντε ομόκεντρων κύκλων (Warden, 1995). Στο κέντρο του βρίσκεται η ηγεσία, ακολουθούν τα ουσιώδη ή οργανικά στοιχεία, οι υποδομές, ο πληθυσμός και τέλος οι ένοπλες δυνάμεις (Warden, 1995) (Κολιόπουλος, 2008, σ.248). Στόχος είναι η παράλυση του συστήματος πλήττοντας κάποιο από τα νευραλγικά του σημεία με σπουδαιότερο αυτό της εχθρικής ηγεσίας (Warden, 1995). Κατά αντιστοιχία οι κυβερνοεπιχειρήσεις μπορούν να στοχεύουν σε ένα από τα νευραλγικά σημεία του εχθρού, όπως η καταστροφή υποδομών ζωτικής σημασίας (κυβερνοεπίθεση στην Εσθονία), ο αποκλεισμός της ηγεσίας από την επικοινωνία με τον λαό του (κυβερνοεπίθεση στη Γεωργία), ή η καταστροφή των στρατιωτικών δυνάμεων (κυβερνοεπίθεση στον πυρηνικό πρόγραμμα του Ιράν) (Lasconjarias & Larsen, 2015, σ.166). Επίσης, ο αεροπορικός πόλεμος, όπως και ο κυβερνοπόλεμος, δίνουν μεγάλη έμφαση στην έννοια της ταχύτητας (Rantapelkonen & Salminen, 2013, σ.172). Η ταχύτητα δράσης, τόσο στον αέρα, όσο και στον κυβερνοχώρο, καθώς και η ακρίβεια στόχευσης είναι τα χαρακτηριστικά που κατατάσσουν τις ενέργειες και των δύο πεδίων πολέμου ως εκ φύσεως επιθετικές. Σε αυτή την περίπτωση όμως,

η επίθεση χρησιμοποιείται ως άμυνα, ενώ πολλές φορές γίνεται χρήση τους προληπτικά (Rantapelkonen & Salminen, 2013, σ179-180) με στόχο να αποφευχθεί μια επικείμενη επίθεση από τον εχθρό αποκομίζοντας τα οφέλη του 'πρώτου πλήγματος'[7].

Η χρήση, επομένως, του κυβερνοχώρου για στρατιωτικούς σκοπούς, αν και δεν μπορεί να εξεταστεί πλήρως υπό το πρίσμα των κλασσικών στρατηγικών αναλύσεων, είναι αυταπόδεικτο, ότι αποτελεί ένα νέο και συνεχώς εξελισσόμενο 'εργαλείο' προώθησης των κρατικών επιδιώξεων (Bachmann & Gunneriusson, 2015b).

3.2. Ο κυβερνοπόλεμος ως υβριδικός πόλεμος

Ο κυβερνοπόλεμος, αν και δεν ταυτίζεται απόλυτα με καμία από τις 'παραδοσιακές' θεωρίες ανάλυσης του πολέμου, όπως συμβαίνει με κάθε νέο πεδίο διεξαγωγής επιχειρήσεων στρατιωτικού χαρακτήρα, έχει αποτελέσει αντικείμενο μελέτης και ανάλυσης, είτε αυτοτελώς, είτε ως μέρος της ευρύτερης έννοιας του υβριδικού πολέμου. Τι είναι, όμως ο υβριδικός πόλεμος, και ποια η θεωρητική του αξία σε σχέση με τον κυβερνοπόλεμο.

Ο όρος 'υβριδικός πόλεμος' ξεκίνησε να χρησιμοποιείται στις αρχές του 21ου αιώνα προσπαθώντας να περιγράψει των συνδυασμό των συμβατικών δράσεων και τακτικών ανταρτοπόλεμου που χρησιμοποίησαν οι Τσετσένοι μαχητές εναντίον των ρωσικών δυνάμεων (Μπαζίνης, 2021; Phillips, 2010). Ωστόσο, έγινε ευρέως γνωστός μετά την ταύτιση του με τις ενέργειες της λιβανέζικης παραστρατιωτικής οργάνωσης, Χεζμπολλάχ, εναντίον του Ισραήλ κατά τη διάρκεια του δεύτερου πολέμου του Λιβάνου.

[7] Το 'πρώτο πλήγμα' αποτελεί μια τακτική απόκτησης στρατηγικού πλεονεκτήματος έναντι του αντιπάλου χρησιμοποιώντας την επίθεση ως άμυνα και αιφνιδιάζοντας τον αντίπαλο. Πιο συγκεκριμένα, ο αμυνόμενος αναλαμβάνει την ευθύνη της έναρξης του πολέμου διενεργώντας μια αιφνίδια, συντονισμένη και ακαριαία διακλαδική ενέργεια που στόχο έχει την εκμηδένιση των ζωτικών σημείων του εχθρού πριν αναπτύξει τις δυνάμεις του αποφεύγοντας μια μελλοντική ήττα. Η λογική που ακολουθεί η έννοια είναι αυτή της διατήρησης αμυντικής υψηλής στρατηγικής με ενεργητικά στοιχεία σε επιχειρησιακό και τακτικό επίπεδο (Γκίνης, 2017; Κονδύλης, 1999; Μαυρόπουλος, 2017).

Αυτό που παρατηρήθηκε στην περίπτωση του Λιβάνου, ήταν η σύζευξη συμβατικών και μη μέσων διεξαγωγής του πολέμου, με παράλληλη χρήση τρομοκρατικών και εγκληματικών ενεργειών, έτσι ώστε να επιτευχθούν οι πολιτικοί αντικειμενική σκοποί της παραστρατιωτικής οργάνωσης (ενός μη κρατικού δηλαδή δρώντα), με τη μεγαλύτερη δυνατή οικονομία δυνάμεων. Για την περιγραφή αυτού του τρόπου πολεμικής δράσης, ο Hoffman χρησιμοποίησε τον όρο 'υβριδικός πόλεμος' (2007).

Σύμφωνα, λοιπόν, με τον Hoffman, οι κρατικοί και μη κρατικοί δρώντες μπορούν να επιλέξουν ανάμεσα από ένα πλήθος, συμβατικών και μη συμβατικών μέσων, τακτικών και τεχνολογιών που ανταποκρίνονται με τον καλύτερο δυνατό τρόπο στη δική τους στρατηγική κουλτούρα[8] και τους δικούς τους πολιτικούς στόχους (Hoffman, 2007). Στον υβριδικό πόλεμο υπάρχει η δυνατότητα συνδυασμού διαφορετικών μέσων και τρόπων επίτευξης των στόχων, οι οποίοι μπορούν να διαφέρουν ανάλογα με το πεδίο δράσης. Οι επιλεγόμενες ενέργειες αφορούν όλα τα επίπεδα της στρατηγικής από εκείνο της υψηλής στρατηγικής έως και το τακτικό πεδίο (Hoffman, 2007) (Καρανικολός, 2021). Όλες αυτές οι δυνατότητες επιλογής και συνδυασμού δημιουργούν μια σύγχυση στην κατάταξη του υβριδικού πολέμου σε μια από τις ήδη υπάρχουσες μορφές, καθώς απορρίπτει την απλοϊκή λογική του άσπρου ή μαύρου (Hoffman, 2007). Ο υβριδικός πόλεμος ναι μεν δεν αποτελεί μια νέα αυτοτελή μορφή πολέμου, αλλά είναι κάτι το διαφορετικό που δεν μπορεί να περιγραφεί από κάποιον άλλο ήδη υπάρχοντα ορισμό (Hoffman, 2009).

Αν και η έννοια του 'υβριδικού πολέμου' είναι ευρέως διαδεδομένη και πολυσυζητημένη, δεν υπάρχει ένας κοινά αποδεκτός ορισμός. Συνήθως χρησιμοποιείται εναλλακτικά με τον όρο 'υβριδική απειλή' προσπαθώντας να

[8] Η 'στρατηγική κουλτούρα' αποτελεί μια πολυσύνθετη έννοια, η ανάλυση της οποίας συνδράμει στην κατανόηση του τρόπου δράσης των διεθνών δρώντων. Με άλλα λόγια, αντικατοπτρίζει τον τρόπο σκέψεις και δράσης μιας κρατικής ή και μη οντότητας μελετώντας και αναλύοντας τις αξίες και τις αρχές που συμμερίζεται ως μια κοινωνία, που φέρει γεωγραφικά καθορισμένα σύνορα και αίσθημα κοινής ιστορικής εμπειρίας. Τα στοιχεία αυτά είναι που διαμορφώνουν τους εθνικούς στόχους, αλλά και εκείνα που καθορίζουν τον τρόπο και τα επιλεγόμενα μέσα για να τους πραγματοποιήσουν (Ήφαιστος, 2008, σ.40-41; Κατσούλας, 2017).

συμπεριλάβει όλο το φάσμα των προκλήσεων, των πολλαπλών δρώντων καθώς και της ποικιλομορφίας των διαθέσιμων μέσων (Pawlak, 2015). Επομένως, έκαστος οργανισμός επιλέγει τη δική του εκδοχή ανάλογα με τις αρχές και αξίες που πρεσβεύει καθώς και τις ανάγκες των κρατών-μελών του.

Το ΝΑΤΟ είναι ο πρώτος οργανισμός που αντέδρασε στη νέα αυτή πρόκληση και προσπάθησε να την οριοθετήσει. Για τους Συμμάχους *«ως υβριδικές απειλές ορίζοντες αυτές που θέτουν οι αντίπαλοι, με την ικανότητα να χρησιμοποιούν ταυτόχρονα συμβατικά και μη συμβατικά μέσα προσαρμοσμένα στις ανάγκες επιδίωξης των στόχων τους»* (*Hybrid Warfare*, 2009; Ringsmose & Rynning, 2011). Η ΕΕ από την άλλη πλευρά, κάνει διάκριση μεταξύ των εννοιών και ορίζει ως *«υβριδική απειλή ένα φαινόμενο που προκύπτει από τη σύγκλιση και τη διασύνδεση διαφορετικών στοιχείων, τα οποία μαζί σχηματίζουν μια πιο σύνθετη και πολυδιάστατη απειλή»* και ως *«υβριδικό πόλεμο μια κατάσταση κατά την οποία μια χώρα καταφεύγει σε ανοιχτή χρήση ενόπλων δυνάμεων εναντίον μιας άλλης χώρας ή ενός μη κρατικού φορέα, επιπλέον ενός συνδυασμού άλλων μέσων (π.χ. οικονομικών, πολιτικών και διπλωματικών)»* (Pawlak, 2015).

Πέρα από τους διεθνείς και περιφερειακούς οργανισμούς, κράτη, όπως η ΗΠΑ, η Κίνα και η Ρωσία, τα οποία έχουν ενσωματώσει τις υβριδικές απειλές στα στρατιωτικά τους δόγματα έχουν διαμορφώσει αντίστοιχους ορισμούς. Για τις στρατιωτικές δυνάμεις των ΗΠΑ *«υβριδική είναι μια απειλή που χρησιμοποιεί ταυτόχρονα συμμετρικές και ασύμμετρες δυνάμεις, συμπεριλαμβανομένων τρομοκρατικών και εγκληματικών στοιχείων, για την επίτευξη του στόχου της, χρησιμοποιώντας μια συνεχώς μεταβαλλόμενη ποικιλία συμβατικών και μη συμβατικών τακτικών για την αντιμετώπιση πολλαπλών διλημμάτων.»* (*Hybrid Warfare*, 2009).

Η ποικιλομορφία των ορισμών δεν αποτελεί το πρόβλημα της έννοιας πολλώ δε μάλλον αναδεικνύει τον πολυδιάστατο χαρακτήρα της. Το πραγματικό πρόβλημα είναι ότι κινείται στα σύνορα ειρήνης και πολέμου, στη γκρίζα ζώνη. Εκεί ο εχθρός είναι δυσδιάκριτος, το πεδίο της μάχης ασαφές (Κοσμόπουλος, 2021), ενώ οι παραδοσιακοί συντελεστές ισχύος δεν φέρουν τη συμβατική τους βαρύτητα

(Μπαζίνης, 2021). Με αυτό τον τρόπο, τα κράτη εξουδετερώνουν την συμβατική υπεροχή των αντιπάλων τους στο πεδίο της μάχης (Bachmann & Gunneriusson, 2015b, 2015a), κάνοντας απροσδόκητους τεχνολογικούς και τακτικούς συνδυασμούς (Mattis & Hoffman, 2005). Μια μικρή ή μια μεγάλη χώρα, ένα ισχυρό ή ένα ανίσχυρο κράτος διαθέτουν τα ίδια όπλα και τις ίδιες, σε μεγάλο βαθμό, άμυνες. Σκοπός είναι η εξουθένωση και εξασθένιση του αντιπάλου κάνοντας χρήση των «short of war» επιλογών του Kennan, μετατοπίζοντας το βάρος της κλιμάκωσης στην αμυνόμενη πλευρά. Αυτός που δέχεται την επίθεση, δεν έχει παρά να αποδεχτεί το τετελεσμένο γεγονός, διαφορετικά αναλαμβάνει την ευθύνη του πολέμου. Βέβαια, σημαίνουσας σημασίας είναι η έγκαιρη αντίληψη της κακόβουλης ενέργειας (Κοσμόπουλος, 2021), καθώς πολλές φορές τα αποτελέσματα γίνονται, είτε μακροπρόθεσμα αντιληπτά, είτε αφομοιώνονται απαίδευτα από τον θιγόμενο λόγω της βαθμιαίας και μεθοδικής αλλαγής, επιβεβαιώνοντας το σύνδρομο του βραστού βατράχου[9].

Οι συγκρούσεις στη γκρίζα ζώνη, στο μεταίχμιο ειρήνης και πολέμου, αποτελούν στη πραγματικότητα έναν ακήρυχτο πόλεμο μεταξύ κρατών ή μεταξύ κρατών και άλλον μη κρατικών δρώντων, οι οποίοι προσπαθούν με έμμεσο τρόπο και μη διαταράσσοντας την παγκόσμια τάξη πραγμάτων, να αλλάξουν το status quo. Αυτός ο αθόρυβος τρόπος αλλαγής των συνθηκών, λειτουργεί προς όφελος των αναθεωρητικών δυνάμεων, καθώς ελαχιστοποιούν τις αρνητικές συνέπειες του συμβατικού πολέμου (Mumford, 2013). Η δράση κάτω από το κατώφλι του πολέμου, δημιουργεί θεσμικό κενό προς εκμετάλλευση. Από τη στιγμή που δεν υπάρχει επίσημη έναρξη πολέμου, οι παράνομες ενέργειες δεν μπορούν να ρυθμίζονται από το ανθρωπιστικό δίκαιο και τα σχετικά, με την επίθεση και

[9] Το σύνδρομο του 'βραστού βατράχου' αποτελεί δάνειο από την κοινωνική ψυχολογία, ενώ χρησιμοποιείται ευρέως από τις οικονομικές επιστήμες και το μάρκετινγκ. Στις διεθνείς σχέσεις αντικατοπτρίζει τη σταδιακή αλλαγή των συνθηκών και την τελική αφομοίωση τους από τον θιγόμενο, όπως συμβαίνει και με τον βάτραχο στην επακόλουθη αλληγορία. Πιο συγκεκριμένα, όταν αφήσεις έναν βάτραχο μέσα σε μια κατσαρόλα με χαμηλή φωτιά, αυτός δεν πηδάει έξω από την κατσαρόλα αλλά παραμένει μέσα σε αυτή έως ότου βράσει, σε αντίθεση με το να τον τοποθετήσεις κατευθείαν μέσα σε μια κατσαρόλα με καυτό νερό, όπου θα αντιδράσει άμεσα και θα απομακρυνθεί από αυτή (Μήτσιος, 2021; Dill, χ.χ.).

επέμβαση σε τρίτο κράτος, άρθρα του Χάρτη των ΗΕ, νομοθετικά δηλαδή κείμενα που εγείρουν ακόμα και τη συλλογική δράση των κρατών προς υπεράσπιση του δικαιώματος της ειρηνικής επίλυσης των διαφορών. Επομένως, το ξεκαθάρισμα του ομιχλώδους πεδίου προώθησης των πολιτικών σκοπιμοτήτων, αφήνεται στην ευχέρεια του αμυνόμενου, επιλέγοντας, είτε έναν 'μακροχρόνιο πόλεμο' τριβής, ή μια γενικευμένη σύρραξη αμφιβόλου εκβάσεως. Ως εκ τούτου, ο υβριδικός πόλεμος μειώνει την πιθανότητα κλιμάκωσης (Mumford, 2013), αλλά αυξάνει την εμφάνιση μικρών 'πολέμων' (Boot, 2008) (Hoffman, 2007).

Ο υβριδικός πόλεμος, πέρα από την εκμετάλλευση των τρωτών σημείων του αντιπάλου, δίνει μεγάλη έμφαση στις ψυχολογικές και πληροφοριακές επιχειρήσεις (Mattis & Hoffman, 2005) (Boot, 2008). Το παν είναι η πληροφορία και η αξία της πολλαπλασιάζεται εκθετικά σε μια εποχή όπου τα μέσα κοινωνικής δικτύωσης αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας. Τα κοινωνικά μέσα αποτελούν αναπόσπαστο μέρος του πεδίου μάχης (Bachmann & Gunneriusson, 2015a), κατέχοντας κεντρικό ρόλο στην έκβαση της στρατιωτικών επιχειρήσεων και των διπλωματικών διεργασιών. Χαρακτηριστικό παράδειγμα αποτελεί η υποδειγματική χρήση των μέσων κοινωνικής δικτύωσης από τους μαχητές του επονομαζόμενου Ισλαμικού Κράτους (ISIS), τόσο για τη στρατολόγηση νέων μαχητών, όσο και για την τρομοκράτηση των δυτικών κοινωνιών. Ο υβριδικός πόλεμος δεν απαιτεί πάντοτε εδαφικά κέρδη, πολλές φορές στοχεύει απλά στον επηρεασμό της πολιτικής σκηνής και της κοινής γνώμης (Μήτσιος, 2021). Ο 'εχθρός', επομένως, εκμεταλλευόμενος τον κυβερνοχώρο επιδίδεται σε εκστρατείες παραπληροφόρησης και προπαγάνδας για την προώθηση των σκοπιμοτήτων του, επεμβαίνοντας στις πολιτικές διαδικασίες και διεργασίες τρίτων χωρών (*Cyber Security in Estonia 2021* , 2021; Maigre, 2022), όπως συνέβη με τις αμερικανικές προεδρικές εκλογές το 2016 και τις γαλλικές το 2017 (Treverton κ.ά., 2018, σ.31-43).

Συνοψίζοντας, ο ομιχλώδης τρόπος διεξαγωγής των πολεμικών επιχειρήσεων τη νέα χιλιετηρίδα παρέχει τεράστιες δυνατότητες στους παίχτες του διεθνούς συστήματος, ώστε να επιτύχουν τους πολιτικούς αντικειμενικούς σκοπούς τους.

Καθώς η κήρυξη διακρατικών πολέμων μοιάζει να έχει εκλείψει, νέα πεδία προώθησης των κρατικών σκοπιμοτήτων έχουν αναδειχθεί. Η τεχνολογική πρόοδος και η όλο αυξανόμενη εξάρτηση μας από τις τεχνολογίες των επικοινωνιών και της πληροφορικής, έχουν μεταφέρει τα πεδία των μαχών στον κυβερνοχώρο. Εκεί δεν υπάρχουν σύνορα και γεωμορφολογικά εμπόδια, έκαστος δρών από οποιαδήποτε πλευρά του πλανήτη σε ελάχιστο χρόνο και με τεράστια ακρίβεια στόχευσης, μπορεί να 'επέμβει' στα εσωτερικά ενός κράτους και να προκαλέσει πολλαπλάσια του κόστους δράσης του ζημιά, χωρίς να καταφέρει ποτέ να ταυτοποιηθεί. Όλα αυτά τα χαρακτηριστικά είναι που κατατάσσουν τον κυβερνοχώρο στο νέο πολλά υποσχόμενο στρατιωτικό πεδίο. Η αυξανόμενη, μάλιστα, ενασχόληση των διεθνών και περιφερειακών οργανισμών ανά τον κόσμο με το αντικείμενο της κυβερνοαφάλειας, καταδεικνύοντας τον αντίκτυπο των κυβερνοπεριστατικών για τη διεθνή κοινότητα, αναδεικνύει τη σπουδαιότητα αυτού του πεδίου και την ιδιαίτερη στρατηγική του σημασία.

3.3. Κυβερνοεπιχειρήσεις τον 21ο αιώνα

Με την αλλαγή της χιλιετίας, έγινε εμφανές ότι η διεθνής κοινότητα άλλαξε τον τρόπο σκέψης και δράσης κατά την άσκηση της εξωτερικής της πολιτικής, επηρεαζόμενη από τις διεθνείς εξελίξεις και την τεχνολογική πρόοδο. Η απεριόριστη ισχύς της Αμερικής της δεκαετίας του 1990 έπρεπε πλέον να ελεγχθεί με διαφορετικούς τρόπους από εκείνον του κλασικού διακρατικού πολέμου, τα ισχυρά κράτη, οι αναδυόμενες δυνάμεις και οι μη κρατικοί δρώντες όφειλαν να προωθήσουν τα συμφέροντα τους με έμμεσους, αλλά συνάμα αποτελεσματικούς τρόπους, χωρίς να εγείρουν διεθνείς αντιδράσεις. Εκμεταλλευόμενοι, λοιπόν, τα νέα μέσα και τις καινοτόμες μεθόδους επέκτασης της πολιτικής τους επιρροής συνδυαστικά με τις συμβατικές μεθόδους, κατάφεραν να υπερκεράσουν τα εμπόδια των διεθνών απαγορεύσεων και να πετύχουν δρώντας στη γκρίζα ζώνη. Στο πλαίσιο αυτό, χρησιμοποιήθηκε η ήπια ισχύς (soft power)[10] του κυβερνοχώρου

[10] Με τον όρο 'ήπια ισχύς' περιγράφονται οι πολιτικές που επιδιώκουν την επίτευξη ενός σκοπού χωρίς τη χρήση της εξαναγκαστικής στρατιωτικής ισχύος. Η οικονομία, η

για να διατηρήσει το γόητρο και τους πολιτικούς αντικειμενικούς σκοπούς παραδοσιακών δυνάμεων που υστερούν σε στρατιωτική ισχύ έναντι των αντιπάλων τους, ή και δυνάμεων που θεωρούν, ότι η έμμεση χρήση της ισχύος τους έχει καλύτερα αποτελέσματα. Σε αυτό το μέρος, επομένως, του κεφαλαίου θα παρουσιαστούν χαρακτηριστικά παραδείγματα χρήσης του κυβερνοχώρου ως βέλτιστου πεδίου δράσης για την προώθηση πολιτικών σκοπιμοτήτων.

3.3.1. Εσθονία

Την άνοιξη του 2007, η Εσθονία δέχτηκε επίθεση κατανεμημένης άρνησης υπηρεσιών (DDoS)[11] με αποτέλεσμα ένα πλήθος υποδομών ζωτικής σημασίας της χώρας που στηρίζονταν στα συστήματα πληροφορικής, να τεθεί 'εκτός' λειτουργίας για 22 ημέρες. Το γεγονός αυτό, συνέπεσε με την ανακοίνωση της μεταφοράς ενός σοβιετικού μνημείου του Β' Παγκοσμίου Πολέμου από το κέντρο του Ταλλίν στα περίχωρά του και την επακόλουθη δυσαρέσκεια του ρωσόφωνου πληθυσμού της χώρας, ο οποίος ένιωσε, ότι περιθωριοποιείται, παρά το ότι αποτελεί το ένα τέταρτο του πληθυσμού της χώρας (Herzog, 2011).

Η επίθεση, αν και δεν μπόρεσε να αποδειχτεί, ότι προέρχεται από τη Ρωσική κυβέρνηση (Rid, 2012), είναι προφανές, ότι έλαβε την υποστήριξή της (Herzog, 2011). Καθ' όλη τη διάρκεια των επιθέσεων, ιστότοποι που διαχειρίζονταν η ρωσική διασπορά παρείχαν πληροφορίες για το πως μπορεί κάποιος να διαπράξει κυβερνο-επίθεση εναντίον των εσθονικών υποδομών (Goodman, 2010). Επιπλέον, σύμφωνα πάντα με τις Εσθονικές αρχές, στην επίθεση χρησιμοποιήθηκαν IP διευθύνσεις στελεχών του γραφείου του Πούτιν (Goodman, 2010). Προς επίρρωση

πολιτισμική και η ιδεολογική έλξη, η πρόοδος της τεχνολογίας και των επικοινωνιών είναι ορισμένες από τις πηγές ήπιας ισχύος που μπορούν να επηρεάσουν την άποψη της πολιτικής εξουσίας μιας κρατικής οντότητας προς όφελος μιας άλλης μακριά από τα πεδία των μαχών (Nye, 1990).

[11] Η επίθεση κατανεμημένης άρνησης υπηρεσιών/ distributed denial-of-service (DDoS) αποτελεί μια κακόβουλη προσπάθεια να διακοπεί η λειτουργία ενός διακομιστή, μιας υπηρεσίας ή ενός δικτύου, υποβάλλοντας στην υποδομή στόχο πληθώρα αιτημάτων χρήσης (*What is a DDoS attack?*, χ.χ.). Αυτό λαμβάνει χώρα με τη μόλυνση ευάλωτων υπολογιστών από το κακόβουλο λογισμικό 'bot' και κάνοντας χρήση των μολυσμένων από αυτό υπολογιστών 'ζόμπι', και του δικτύου 'botnet' που δημιουργούν οδηγώντας στην άμεση διακοπή λειτουργίας της συγκεκριμένης υπηρεσίας (Θεοφίλης, 2018).

της θέσης τους, οι Εσθονοί ισχυρίστηκαν, ότι στοιχείο απόδειξης της ρωσικής ενοχής αποτελεί η άρνηση παροχής δικαστικής βοήθειας για τη διενέργεια έρευνας κατά των Ρώσων πολιτών που ενδεχομένως να έλαβαν μέρος στην επίθεση, όπως προβλεπόταν από τη διμερή συμφωνία δικαστικής συνδρομής μεταξύ των δύο κρατών (Goodman, 2010).

Επομένως, αν δεχτούμε, ότι η κακόβουλη επίθεση που δέχτηκε η χώρα προήλθε από τη Ρωσία, η κυβερνοεπίθεση κατά της Εσθονίας αποτελεί ένα 'καθαρό' κυβερνοπόλεμο χωρίς χρήση συμβατικών μέσων πολέμου και μακριά από το κλασικό πεδίο μάχης. Στην συγκεκριμένη, μάλιστα, περίπτωση, καταδεικνύεται η αδυναμία απόδοσης ευθυνών λόγω του σύνθετου τρόπου δράσης στον κυβερνοχώρο. Η επιβολή αντίμετρων κατά της Ρωσίας, τουλάχιστον από τους συμμάχους της Εσθονίας, εφόσον δεν υπήρχαν αδιάσειστα στοιχεία ενοχής, ήταν ανέφικτη, με συνέπεια την αδυναμία κλιμάκωσης της σύγκρουσης από πλευράς άμυνας και την επακόλουθη αποδοχή του τετελεσμένου γεγονότος και την επιστροφή του μνημείου στην αρχική του θέση.

3.3.2. Γεωργία

Το Μάιο του 2008 στη Σύνοδο Κορυφής του Βουκουρεστίου, το ΝΑΤΟ ανακοίνωσε την έναρξη των διαδικασιών ένταξης της Ουκρανίας και της Γεωργία στους κόλπους της Συμμαχίας (NATO, 2008). Το γεγονός αυτό, προκάλεσε την αντίδραση της Ρωσίας, η οποία αντιμετωπίζει τις πρώην χώρες της ΕΣΣΔ στην ανατολική Ευρώπη ως χώρες της σφαίρας επιρροής της. Η μη ένταξη τους στις δυτικές συμμαχίες της γειτονιάς τους είναι ζωτικής σημασίας για τη Ρωσία, καθώς διαφορετικά θα αποκτήσει κοινά γεωγραφικά σύνορα με τον πάλαι άλλοτε 'εχθρό' (δόγμα του 'Εγγύς Εξωτερικού').

Τον Αύγουστο της ίδια χρονιάς, η Ρωσία με πρόσχημα την επέμβαση των γεωργιανών στρατιωτικών δυνάμεων στην αυτόνομη περιφέρεια της Νότιας Οσετίας, εισέβαλε, ώστε να προστατεύσει τους ρωσόφωνους κατοίκους της περιοχής (Rid, 2012). Λίγες μέρες πριν την είσοδο των στρατιωτικών δυνάμεων, γεωργιανές κυβερνητικές ιστοσελίδες, ιστοσελίδες κοινωνικής δικτύωσης καθώς

και σημαντικές υποδομές της χώρας άρχισαν να δέχονται επιθέσεις μέσω του κυβερνοχώρου. Οι επιθέσεις αυτές έλαβαν τη μορφή κατανεμημένης άρνησης παροχής υπηρεσιών, εκστρατειών παραπληροφόρησης και προπαγάνδας, βανδαλισμού των κυβερνητικών ιστοσελίδων και διασποράς κακόβουλων λογισμικών (Θεοφίλης, 2018) (Rid, 2012). Οι κακόβουλες αυτές ενέργειες κλιμακώθηκαν την 8η Αυγούστου, μέρα εισβολής των ρωσικών δυνάμεων στην γεωργιανή επικράτεια, επιτείνοντας ακόμα περισσότερο την 'ομίχλη του πολέμου'.

Όπως και στην περίπτωση της Εσθονίας, η απόδοση των κυβερνοεπιθέσεων που έλαβαν χώρο καθ' όλη τη διάρκεια του ολιγοήμερου διακρατικού πολέμου δεν οδήγησε σε κάποιο ασφαλές αποτέλεσμα διασύνδεσης του με τις ρωσικές αρχές (Rid, 2012) (Kikk κ.ά., 2010). Αν και η ταυτόχρονη δράση των ενόπλων δυνάμεων στο συμβατικό πεδίο και των χάκερς στον κυβερνοχώρο, ουδόλως τυχαία δεν μοιάζει. Τα χτυπήματα κατά των πληροφοριακών συστημάτων της Γεωργίας είχαν ως αποτέλεσμα την ψυχολογική κατάπτωση των κατοίκων, αλλά και της κυβέρνησης (Θεοφίλης, 2018), η οποία την κρίσιμη αυτή ώρα δεν μπορούσε να επικοινωνήσει με το εξωτερικό της περιβάλλον και να πείσει τους συμμάχους της, τόσο για την ανάγκη της στρατιωτικής της επιχείρησης στην Οσετία που προκάλεσε την 'ανθρωπιστική' δράση της Ρωσίας, όσο για τη παροχή υποστήριξης και στρατιωτικής βοήθειας από αυτούς (Goodman, 2010; Rid, 2012). Αποτέλεσμα ήταν η ανακήρυξη της Νότιας Οσετίας ως ανεξάρτητου κράτους και η παραίτηση του τότε Προέδρου της Γεωργίας, Μιχαήλ Σαακασβίλη, εγκαινιάζοντας μια παρατεταμένη περίοδο πολιτικής αστάθειας στη χώρα, και πετυχαίνοντας τους ρωσικούς πολιτικούς αντικειμενικούς σκοπούς στην περιοχή του Καυκάσου.

3.3.3. Ουκρανία

Η κρίση που ξεκίνησε στην Ουκρανία το φθινόπωρο του 2013 με τις κινητοποιήσεις των πολιτών στην πλατεία Maidan, γνωστή ως Euromaidan, αποσταθεροποιώντας την κυβέρνηση Γιανουκόβιτς και επιφέροντας την αναίμακτη προσάρτηση της Κριμαίας από τη Ρωσία (2014) και τη διαρκώς

υποσκάπτουσα κρατική κυριαρχία στις ανατολικές επαρχίες της χώρας (αυτοαποκαλούμενες ως Δημοκρατίες του Ντονέσκ και Λουχάνσκ), οδήγησε τελικά στην οριστική ρήξη και τη σύρραξη με τη Ρωσία. Ο τρόπος διεξαγωγής της συγκεκριμένης διακρατικής διαμάχης αποτυπώνει τον 'κλασικό' ορισμό του υβριδικού πολέμου.

Η Ρωσία χρησιμοποίησε τα μέσα κοινωνικής δικτύωσης για να προβάλει το αφήγημα της ανάγκης εισβολής για ανθρωπιστικούς λόγους (παροχή βοήθειας στους ομοεθνείς των οποίων τα δικαιώματα καταστρατηγούνται από την φασιστική κυβέρνηση της γείτονας χώρας) τόσο στο εσωτερικό όσο και στο εξωτερικό (Lella κ.ά., 2022). Από την άλλη πλευρά, η Ουκρανία χρησιμοποίησε το διαδίκτυο για να προβάλει την επίθεση που δέχεται, η οποία θέτει υπό αμφισβήτηση την κρατικής της κυριαρχία και επεμβαίνει στις εσωτερικές της υποθέσεις, χωρίς την προηγούμενη άδεια της.

Πέρα από την προσπάθεια προώθησης των αφηγημάτων έκαστης πλευράς, ο κυβερνοχώρος χρησιμοποιήθηκε και συνεχίζει να χρησιμοποιείται ως πεδίο πολέμου. Ρωσικές κρατικά υποστηριζόμενες ομάδες χάκερ χρησιμοποιήθηκαν πριν την εισβολή για να προετοιμάσουν το έδαφος των συμβατικών μαχών (Microsoft, 2022a). Σύμφωνα με στοιχεία της Microsoft, ήδη ένα χρόνο νωρίτερα είχαν ξεκινήσει εκστρατεία απόκτησης πρόσβασης στα κέντρα διοίκησης της κεντρικής και στρατιωτικής εξουσίας, τα σώματα ασφαλείας, τις κρίσιμες υποδομές, ακόμα και σε ανθρωπιστικές οργανώσεις (2022). Οι έρευνες έχουν ταυτοποιήσει πάνω από εννιά κακόβουλα κατασκοπευτικά προγράμματα (WhisperGate69 or WhisperKill, Hermetic Wiper70, CaddyWiper71 , DesertBlade72, AcidRain73, Industroyer254, IsaacWiper74, and DoubleZero75) που έχουν χρησιμοποιηθεί στον ουκρανικό κυβερνοχώρο (Microsoft, 2022a). Η πρόσβαση σε όλα τα επίπεδα οργάνωσης της Ουκρανίας αποτέλεσε επικουρικό στοιχείο των μαχών. Μάλιστα, αποκαλύφθηκε ότι είχαν στοχοποιηθεί ακόμα και οι δορυφορικές υποδομές πλήττοντας τις επικοινωνίες σε ολόκληρη την κεντρική Ευρώπη. Λίγες μέρες πριν την εισβολή και ενώ η διπλωματική λύση φαινόταν μακρινή άρχισαν να εξαπολύονται 'επιθέσεις' κατά των ουκρανικών φορέων

δημόσιας διοίκησης, των τραπεζικών ιδρυμάτων και ευρύτερα των κρίσιμων υποδομών. Αυτές κλιμακώθηκαν την παραμονή και ανήμερα της εισβολής (23-24/2/2022) (Microsoft, 2022c, 2022a; Smith, 2022). Αν και η σύνδεση μεταξύ των κυβερνοεπιθέσεων και των συμβατικών πληγμάτων δεν έχει αποδειχθεί, αυτά φαίνεται, ότι ήταν οργανωμένα, ώστε να πλήττουν με μικρή χρονική διαφορά τους στρατιωτικούς στόχους, ή την ευρύτερη περιοχή αυτών, προκαλώντας σύγχυση στη διοίκηση και υποσκάπτοντας την εμπιστοσύνη των πολιτών στην κυβέρνηση και τις δυνατότητες της να ανταπεξέλθει στην απειλή. Στόχος των φιλορωσικών ομάδων χάκερς αποτέλεσαν, επίσης, χώρες που κατέκριναν την ρωσική προκλητικότητα και για αυτό επέβαλαν κυρώσεις, όπως κράτη-μέλη του NATO, καθώς και δεκάδες οργανισμοί σε όλα τα μήκη και πλάτη του κόσμου (Smith, 2022).

Εκτός από τη Ρωσία και η Ουκρανία διεξήγαγε κυβερνοεπιχειρήσεις με τη βοήθεια ιδιωτών χάκερς. Στις 26 Φεβρουαρίου του 2022, ο ουκρανός υπουργός ψηφιακής μεταρρύθμισης ανακοίνωσε τη δημιουργία του 'IT Army of Ukraine'. Το ετερόκλητο αυτό σώμα αποτελείται από εθελοντές ακτιβιστές χάκερ, εθνικιστικές ομάδες και ομάδες που δρουν παράνομα στον κυβερνοχώρο και δρα υπό την καθοδήγηση του Telegram Channel, ακολουθώντας τα εσθονικά πρότυπα του Cyber Defence League. Αυτός ο κυβερνο-στρατός του πλήθος ('crowdsourced') αν και δεν φέρει συγκεκριμένη νομική προσωπικότητα ενεργεί στο πλευρό της κυβέρνησης διεξάγοντας επιθέσεις DDOS.

Παρόλο που το στρατιωτικό αποτέλεσμα είναι ακόμα αβέβαιο, ο πόλεμος στην Ουκρανία έχει αναδείξει τις νέες δυνατότητες που προσφέρουν οι τεχνολογικές εξελίξεις στον τρόπο διεξαγωγής του πολέμου. Ακόμα και αν ο 'καθαρός' κυβερνοπόλεμος δεν είναι εφικτός, ο συνδυασμός όλων τον στρατιωτικών πεδίων και μεθόδων αναδεικνύει το μέγεθος των επιθετικών ικανοτήτων και αμυντικών προκλήσεων για τη διεθνή κοινότητα τις επόμενες δεκαετίες.

3.3.4. Microsoft Exchange Server

Στις 2 Μαρτίου του 2021 η Microsoft and Volexity ανακοίνωσαν τον εντοπισμό πολλαπλών zero-day κενών ασφαλείας στον Microsoft Exchange Server. Την ίδια

μέρα η Microsoft προχώρησε στην κυκλοφορία ενημερώσεων για την αποκατάσταση αρκετών ευπαθειών (FBI & CISA, 2021)

Στις 19 Ιουλίου του 2021, με ανακοίνωση του Λευκού Οίκου, οι ΗΠΑ απέδωσαν την κακόβουλη ενέργεια εργαλειοποίησης των κενών ασφαλείας του Microsoft Exchange Server στην Λαϊκή Δημοκρατία της Κίνας και καταδίκασαν την παράνομη, κατά τις διεθνείς νόρμες, απόκτηση πρόσβασης σε εμπιστευτικά αρχεία κυβερνητικών υπηρεσιών, διεθνών οργανισμών, μη κυβερνητικών οργανισμών και επιχειρήσεων (The White House, 2021).

Σύμφωνα με την αμερικανική πλευρά, η κινεζική κυβέρνηση, εκμεταλλευόμενη ορισμένες τεχνικές ευπάθειες του Microsoft Exchange Server που ανακάλυψαν κρατικά υποστηριζόμενες ομάδες χάκερς, επιδίωξε την προώθηση των πολιτικών της σκοπών (CISA, 2022). Πιο συγκεκριμένα, μέσω της ομάδας TA413 APT, διεξήχθη εκστρατεία spear-phishing χρησιμοποιώντας 'μολυσμένα' αρχεία ZIP (Paganini, 2022). Με αυτό τον τρόπο, μολύνθηκε πλήθος επιχειρήσεων, κρατικών και μη οργανισμών ανά τον κόσμο -κυρίως δυτικά κράτη- με αποτέλεσμα να αποκτηθεί πρόσβαση σε αρχεία, βάσεις δεδομένων και υπηρεσίες περιήγησης (FBI & CISA, 2021; 'Microsoft Exchange & F5 Critical Vulnerabilities', 2021; *Overview of F5 vulnerabilities* , 2021). Μάλιστα, ο ιός είχε τη δυνατότητα να πραγματοποιεί αναγνώριση και να εισέρχεται κατά αυτόν τον τρόπο στις εφαρμογές σαν πιστοποιημένος χρήστης (Paganini, 2022).

Οι Ηνωμένες Πολιτείες και οι σύμμαχοι τους επέκριναν την κινεζική επιθετική ενέργεια, αλλά και ευρύτερα την κινεζική τακτική χρήση μισθωμένων από την κυβέρνηση ομάδων διεξαγωγής, κυρίως οικονομικού χαρακτήρα, κυβερνοεπιθέσεων, παραβλέποντας τις δεσμεύσεις της στα ΗΕ και ειδικότερα εκείνη της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο (The White House, 2021). Αντίστοιχη ανακοίνωση εξέδωσε και η Ύπατη Εκπρόσωπος της ΕΕ, η οποία εφιστά την προσοχή της Κίνας για τις κακόβουλες ενέργειες που λαμβάνουν χώρα από το έδαφος της και τις οποίες οφείλει να καταπολεμήσει, καθώς ανθίστανται στην αρχή του παγκόσμιου, ανοιχτού, ελεύθερου και ασφαλούς κυβερνοχώρου διαταράσσοντας την παγκόσμια οικονομία και

θέτοντας υπό αμφισβήτηση ήδη κατοχυρωμένες αρχές και αξίες (Council of the European Union, 2021).

Τα ως άνω περιστατικά αποτελούν το φυσικό επακόλουθο της μετεξέλιξης του μεταψυχροπολεμικού τρόπου άσκησης της εξωτερικής πολιτικής, λόγω της παγκοσμιοποίησης και της αυξανόμενης οικονομικής, πολιτικής και ψηφιακής διασυνδεσιμότητας των κρατών (Bachmann & Gunneriusson, 2015a; Pronk, 2021). Οι αντιπαραθέσεις μεταξύ των 'μεγάλων' δυνάμεων οφείλουν να κινούνται στα σύνορα του παραδοσιακού πολέμου, ώστε να επιτυγχάνουν τους στόχους τους μέσω του εξαναγκασμού και της πίεσης, αποφεύγοντας όμως μια γενικευμένη σύρραξη. Επομένως, κάθε χώρα ανάλογα με τις δυνατότητές της και τη κατάταξή της ανάμεσα στις άλλες, διαλέγει τα κατάλληλα μέσα και τις βέλτιστες πρακτικές ώστε να επηρεάσει προς όφελος της τις κυβερνήσεις τρίτων κρατών.

Η Ρωσία, από τη μία, προσπαθώντας να διατηρήσει το κύρος μιας πάλαι άλλοτε υπερδύναμης κάνει χρήση στρατιωτικών μέσων σε συνδυασμό με άλλα είδη εξαναγκασμού ήπιας ισχύος (Pronk, 2021). Δεν διστάζει να επέμβει στρατιωτικά σε περιοχές ζωτικής για την ύπαρξη της σημασίας, χρησιμοποιώντας κυρίως το αφήγημα της προστασίας των 'συμπατριωτών' της. Σε άλλες περιπτώσεις, δρα με μη συμβατικά μέσα, όπως ο κυβερνοχώρος, επιβάλλοντας εμμέσως την θέση της στο αντίπαλο δέος.

Η Κίνα, από την άλλη, ως μια δύναμη συνεχώς αυξανόμενης ισχύος, χρησιμοποιεί ήπιας μορφής τακτικές που επιφέρουν μακροπρόθεσμα αποτελέσματα (Pronk, 2021). Εστιάζει κυρίως στην οικονομική και πολιτική εξάρτηση των κρατών-στόχων. Έτσι και οι κυβερνοεπιθέσεις είναι οικονομικού και κατασκοπευτικού χαρακτήρα που αποσκοπούν στην απόκτηση πληροφοριών οικονομικής φύσεως και εταιρικών/ κυβερνητικών μυστικών από επιχειρήσεις και κυβερνήσεις συμμαχικών προς τις ΗΠΑ κρατών, καθώς και την παράκαμψη των νομοθεσιών περί πνευματικών δικαιωμάτων (Microsoft, 2022b).

Αν και τα προαναφερθέντα παραδείγματα και τακτικές κλονίζουν τις παγκόσμιες ισορροπίες, δεν θέτουν μόνο υπό αμφισβήτηση την κρατική ασφάλεια, αλλά και

το νομικό πλαίσιο που στοιχειοθετεί τις εξωτερικές σχέσεις των κρατών και τους κανόνες που τις διέπουν.

Β΄ ΜΕΡΟΣ
ΔΙΕΘΝΕΣ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

ΚΕΦΑΛΑΙΟ 4:
ΕΜΜΕΣΗΣ ΕΦΑΡΜΟΓΗΣ ΡΥΘΜΙΣΕΙΣ

Οι σχέσεις των κρατών ρυθμίζονται από τους κανόνες που τα ίδια τα κράτη θεσπίζουν και αποφασίζουν να τους δεσμεύουν. Σκοπός είναι η δημιουργία ενός πλαισίου δράσης όπου οι ενέργειες που έρχονται σε αντίθεση με τους ισχύοντες κανόνες να θεωρούνται έκνομες και να επισύρουν την καταδίκη τους από τη διεθνή κοινότητα, καθώς και την ενεργοποίηση των αντίστοιχων 'ποινών'.

Τα κράτη, επομένως, θέλοντας να προφυλάξουν τις ολοένα και περισσότερο ψηφιακά εξαρτώμενες κρίσιμες υποδομές τους από την αυξανόμενη τρωτότητα που επιφέρει ο ψηφιακός τους μετασχηματισμός (OEWG, 2021), προσφεύγουν σε διμερείς ή πολυμερείς συμφωνίες. Στο πλαίσιο αυτό, επιχειρούν να ορίσουν τα στοιχεία της υπεύθυνης κρατικής συμπεριφοράς και τις βέλτιστες πρακτικές που οφείλουν να ακολουθούν αποβλέποντας στην παγκόσμια σταθερότητα και ειρήνη.

Έχοντας αυτό ως βάση, το παρόν κεφάλαιο θα επικεντρωθεί στην ανάδειξη των ενεργειών που δρομολογούνται υπό την αιγίδα διεθνών και περιφερειακών οργανισμών -των οποίων η Ελλάδα είναι μέλος- αλλά που η ενσωμάτωσή τους στα εθνικά δίκαια επαφίεται στη διακρατική ευχέρεια των κρατών-μελών.

4.1. Οργανισμός Ηνωμένων Εθνών - ΟΗΕ

Στον ΟΗΕ, το προπύργιο της διεθνούς συνεργασίας και τον υπερασπιστή της ειρηνικής επίλυσης των διαφορών, η έννοια της ασφάλειας του κυβερνοχώρου εισήχθη ήδη από τη δεκαετία του 1990, με αφορμή το ρωσικό σχέδιο ψηφίσματος με τίτλο: *"Developments in the field of Information and Telecommunication in the context of International Security"*. Σημείο καμπής, όμως, αποτέλεσε η σύσταση της Διακυβερνητικής Ομάδας Εμπειρογνωμόνων σχετικά με την προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (UNGGE), έπειτα από την υιοθέτηση της αμερικανικής πρότασης, με το ψήφισμα 58/32 της Γενικής

Συνέλευσης των Ηνωμένων Εθνών (ΓΣ/ΗΕ) του 2003. Από την έναρξη της δράσης της και έως το 2021, η Ομάδα των Εμπειρογνωμόνων αποτέλεσε έναν εκ των βασικότερων πυλώνων που πραγματεύτηκε το διεθνές πλαίσιο για την υπεύθυνη κρατική συμπεριφορά στον κυβερνοχώρο. Έως τώρα έχουν συσταθεί έξι Διακυβερνητικές Ομάδες Εμπειρογνωμόνων, σύμφωνα με την αρχή της δίκαιης γεωγραφικής κατανομής, από τις οποίες μόνο οι τέσσερις προσέφεραν παραγωγικό αποτέλεσμα (2010, 2013, 2015, 2021). Πέρα από τις Ομάδες των Εμπειρογνωμόνων, στη μελέτη της υπεύθυνης κρατικής συμπεριφοράς έχει συνεισφέρει και η Ομάδα Εργασίας Ανοιχτής Διάρκειας για την ασφάλεια των ΤΠΕ και τη χρήσή τους (OEWG). Η Ομάδα αυτή δημιουργήθηκε μετά από πρόταση της Ρωσικής Ομοσπονδίας και την υπερψήφισή της από τη Γενική Συνέλευση (Ψήφισμα 73/27) (Digital Watch, χ.χ.). Μετά την επιτυχή λήξη της θητείας του πρώτου OEWG, η ΓΣ/ΗΕ με το Ψήφισμα 75/240 σύστησε τη δεύτερη διακρατική ομάδα, OEWG 2021-2025 (United Nations -GA, 2021). Η έκθεση του OEWG 2019-2021, η πρώτη ετήσια έκθεση του OEWG 2021-2025,[12] καθώς και οι άλλες τέσσερις της Ομάδας Εμπειρογνωμόνων, όλες υιοθετημένες με ομοφωνία, αποτελούν τον πυρήνα διαμόρφωσης του λεγόμενου διεθνούς πλαισίου της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο. Το πλαίσιο αυτό θα ενδυναμωθεί έτι περισσότερο από μια ακόμα πρωτοβουλία 59 κρατών-μελών του ΟΗΕ, το Programme of Action (PoA),[13] η οποία υπερψηφίστηκε τον Οκτώβριο του 2022 από τη ΓΣ/ΗΕ.

[12] Η πρώτη ετήσια έκθεση του OEWG (A/75/275) παρουσιάζει την πρόοδο του πρώτου έτους εργασιών αλλά και έναν 'χάρτη' της πορείας που θα ακολουθήσει η Ομάδα πάνω στους βασικούς πυλώνες που έθεσε η προηγούμενη ομάδα εργασίας OEWG 2019-2021 (OEWG, 2022).

[13] Το PoA αποτελεί έναν μόνιμο και χωρίς αποκλεισμούς μηχανισμό προσανατολισμένης δράσης υπό την αιγίδα του ΟΗΕ που στόχο έχει την περεταίρω ανάπτυξη του πλαισίου της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο λαμβάνοντας υπόψη τα κελεύσματα των reports του OEWG αλλά και προωθώντας τη συνεργασία με όλα τα ενδιαφερόμενα μέρη πέρα των κρατών. Θα αποτελεί μια διαδικασία λήψης αποφάσεων με γνώμονα τη συναίνεση των μελών (consensus-driven) και την παραγωγή αποτελεσμάτων (result-based), η οποία θα αναθεωρείται περιοδικά, ώστε να ανταποκρίνεται στις τρέχουσες γεωπολιτικές και τεχνολογικές εξελίξεις (France κ.ά., 2020; United Nations-GA, 2022; WILPF, 2022).

Το έργο της διαμόρφωσης της έννοιας της υπεύθυνης κρατικής συμπεριφοράς αρθρώθηκε και μελετήθηκε σε τρεις θεματικούς άξονες από τους Εμπειρογνώμονες. Ο πρώτος αφορά τη σχέση του διεθνούς δικαίου με το πεδίο του κυβερνοχώρου αποσκοπώντας στη ρύθμιση των ενεργειών της διεθνούς κοινότητας στη βάση ήδη υπαρχόντων αλλά και νέων κανόνων και αρχών. Ο δεύτερος θεματικός άξονας θέτει ζητήματα δικαιοδοσίας επί των πληροφοριακών και επικοινωνιακών συστημάτων των κρατών. Ο τρίτος ενθαρρύνει την προώθηση της κρατικής συνεργασίας, τη θέσπιση εθελοντικών και μη δεσμευτικών μέτρων οικοδόμησης εμπιστοσύνης, κυρίως στους κόλπους των περιφερειακών οργανισμών, καθώς και την οικοδόμηση των κυβερνοϊκανοτήτων των κρατών (Office of Disarmament Affairs, χ.χ.).

4.1.1. Διεθνές Δίκαιο και Κυβερνοχώρος

Έχοντας κατανοήσει τη σπουδαιότητα ύπαρξης κοινώς αποδεκτών κανόνων για τη διασφάλιση της αρμονικής συνύπαρξης των κρατών, οι εκπρόσωποι των δύο διακρατικών Ομάδων ήδη από το 2013 επισήμαναν την ισχύ των κανόνων του διεθνούς δικαίου, του Καταστατικού Χάρτη των Ηνωμένων Εθνών και της Οικουμενικής Διακήρυξης για τα Ανθρώπινα δικαιώματα, των θεμελιωδών δηλαδή δικαιωμάτων και ελευθεριών, και στον κυβερνοχώρο (GGE, 2015; Nations, 2013). Μάλιστα με την πάροδο του χρόνου γίνεται όλο και πιο λεπτομερής αλλά όχι εξαντλητική καταγραφή των εφαρμοστέων διάταξεων (United Nations-GA, 2022).

Πιο συγκεκριμένα, στην Έκθεση του 2021 γίνεται ρητή αναφορά στην αρχή της κυρίαρχης ισότητας (άρθρο 2 παρ. 1 Χάρτης ΗΕ), της ειρηνική επίλυση των διαφορών (αρ. 1 παρ. 1 & αρ. 2 παρ. 3 Χάρτης ΗΕ), της απαγόρευση απειλής χρήσης ή η χρήση βίας κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας ενός κράτους (αρ. 2 παρ. 4 Χάρτης ΗΕ), της απαγόρευσης επέμβασης στις εσωτερικές υποθέσεις τρίτων κρατών (αρθ.1 παρ.7 Χάρτης ΗΕ), καθώς και στην εφαρμοστική ισχύ του ανθρωπιστικού δικαίου σε περιόδους ένοπλων συγκρούσεων (OEWG, 2021). Η ιδιαίτερη μνεία στις ανωτέρω αρχές και ιδίως στο

'δίκαιο του πολέμου' επιβεβαιώνει το γεγονος ότι ο κυβερνοχώρος αποτελεί πέδιο δόξης λαμπρό για τη διεξαγωγή ενεργείων στρατιωτικού χαρακτήρα.

4.1.2. Κρατική Κυριαρία & Δικαιοδοσία

Ωστόσο, για να τεθούν σε ισχύ οι ανωτέρω κανόνες, η κακόβουλη ενέργεια θα πρέπει να αποδοθεί σε μια κρατική οντότητα. Έτσι από το 2013 οι Εμπερογνώμονες έχουν τονίσει, ότι οι ΤΠΕ που βρίσκονται στην επικράτεια ενός κράτους τελούν υπό την κυριαρχία και τη δικαιοδοσία του. Τα κράτη, επομένως, οφείλουν να φροντίζουν για την χρηστή χρήση τους και να μην επιτρέπουν εν γνώση τους τη διεξαγωγή κακόβουλων ενεργειών από το έδαφος τους (GGE, 2021). Αυτό βέβαια δε συνεπάγεται τη συνεχή κρατική παρακολούθηση των ΤΠΕ (GGE, 2021). Στην Έκθεση του 2015 καταγράφεται ρητά, ότι η έναρξη από, ή η χρήση των υποδομών μιας χώρας, για τη διεξαγωγή κακόβουλων επιθέσεων στον κυβερνοχώρο, δεν οδηγεί νομοτελειακά στην απόδοση ευθυνών σε αυτή. Για την επίρριψη ευθυνών και την επιβολή κυρώσεων σε τρίτο κράτος απαιτειται τεκμηριωμένη άποψη και επιβάλλεται η εύρεση αδιάσειστων στοιχείων σύνδεσης της ενέργειας με αυτό, καθώς κάθε πολιτική απόδοση ευθυνών δύναται να διαταράξει τις εξωτερικές του σχέσεις.

Τα κράτη, επομένως, οφείλουν να λαμβάνουν υπόψη τις υποχρεώσεις τους για κακόβουλες ενέργειες που προέρχονται από τις ΤΠΕ της επικράτειας τους. Σύμφωνα με την πιο πρόσφατη Έκθεση του GGE, το κράτος προέλευσης της απειλής οφείλει να ανιχνεύσει, να ερευνήσει και να εντοπίσει την κακόβουλη ενέργεια και στη συνέχεια να τη σταματήσει κάνοντας χρήση σωστών, αναλογικών και αποτελεσματικών μέσων που θεμελιώνονται στο διεθνές και το εσωτερικό του δίκαιο (GGE, 2021). Επιπλέον, όταν το κράτος πρόλευσης δεν διαθέτει την απαιτούμενη τεχνική γνώση και ικανότητα για να προβεί στις ανωτέρω δράσεις, μπορεί να το συνδράμει τρίτη χώρα ή ο ιδιωτικός τομέας (GGE, 2021). Η 'έπεμβαση' στο εσωτερικό μιας χώρας θα πρέπει πάντοτε να έπεται

αιτήματός της, όπως προστάζει το διεθνές δίκαιο,[14] ενώ η παροχή βοήθειας να γίνεται με σεβασμό στο επείγον της κατάστασης και της ευαισθησιας του ζημάτος (GGE, 2021), εφόσον θα χρειαστεί τρίτες χώρες να κάνουν χρήση αλλότριων κρίσιμων εθνικών υποδομών και να έρθουν σε επαφή με διαβαθμισμένες πληροφορίες που καθιστούν τρωτή την εθνική της ασφάλεια.

4.1.3. Διεθνείς Νόρμες

Έχοντας σκιαγραφήσει τις ισχύουσες παραδοχές σχετικά με την εφαρμογή του διεθνούς δικαίου επί των πληροφοριακών και επικοινωνιακών υποδομών, σημαντικό είναι να παρουσιαστούν οι έντεκα, εθελοντικές και μη δεσμευτικές (GGE, 2015), αλλά εξέχουσας σημασίας για τις Ομάδες των Εμπειρογνωμόνων, διεθνείς νόρμες/κανόνες, οι οποίες αποτελούν τα θεμέλια της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο. Πιο συγκεκριμένα, οι Εμπειρογνώμονες τονίζουν την ανάγκη συνεργασίας μεταξύ των κρατών με στόχο την επαύξηση της διεθνούς σταθερότητας και ασφάλειας και την πρόληψη ενεργειών που μπορούν να τις κλονίσουν, ενώ ακόμη θεωρούν πως για την ασφαλή χρήση του κυβερνοχώρου τα κράτη οφείλουν να σεβαστούν τα ψηφίσματα που πραγματεύονται την απόλαυση των ανθρωπίνων δικαιωμάτων στον διαδίκτυο (Ψηφίσματα 20/8 & 26/13 του Συμβουλίου για τα Ανθρώπινα Δικαιώματα των ΗΕ), καθώς και τα δικαιώματα στην ιδιωτική ζωή και την ελευθερία της έκφρασης (Ψηφίσματα 68/167 & 69/166 της ΓΣ/ΗΕ)(GGE, 2015). Μάλιστα στο πλαίσιο της δημιουργίας συνεργατικών μέτρων αντιμετώπισης των απειλών, επισημαίνουν ότι, σε περιπτώσεις κυβερνοπεριστατικών, τα κράτη πρέπει να αλληλοενημερώνονται. Το πληγέν κράτος οφείλει να κοινοποιεί προς τα υπόλοιπα πληροφορίες, όπως οι προκλήσεις που αντιμετωπίζει για την απόδοσης ευθύνης, τη φύση και την έκταση των συνεπειών του συμβάντος (GGE,

[14] Σύμφωνα με τους υφιστάμενους κανόνες και νόρμες του διεθνούς δικαίου & του διεθνούς εθιμικού δικαίου η συναίνεση κράτους για παροχή βοήθειας από τρίτη χώρα πρέπει να γίνεται: α. ελεύθερα, β. από τη νόμιμη κυβέρνηση, γ. να μην αποτελεί εν λευκώ εξουσιοδότηση, δ. οι παρεχόμενες δράσεις να μην βλάπτουν την εδαφική ακεραιότητα ή την πολιτική της ανεξαρτησία, και ε. να μην συγκρούεται με όλους κανόνες jus cogens (Cassese, 2012, σ.4).

2015). Από τα πιο κομβικά σημεία των Εκθέσεων και ειδικότερα των νορμών είναι η έννοια της 'γνώσης'. Τα κράτη πρέπει δηλαδή να εμποδίζουν την εν γνώσει τους διεξαγωγή παράνομων πράξεων με προέλευση από την επικράτειά τους, καθώς και να απαγορεύουν και να σταματούν τις εν γνώσει τους δραστηριότητες που αντίκειται στις διεθνείς τους υποχρεώσεις και δεσμεύσεις, βλάπτοντας ζωτικής σημασίας υποδομές για το κοινό (GGE, 2015). Συνεχίζουν απαγορεύοντας τις επιθετικές ενέργειες κατά των ομάδων απόκρισης για περιπτώσεις έκτακτης ανάγκης, καθώς και την κακόπιστη δράση εξ αυτών (GGE, 2015). Σύμφωνα με τους Εμπειρογνώμονες, τα κράτη οφείλουν να λαμβάνουν τα κατάλληλα μέτρα προστασίας των κρίσιμων υποδομών τους και να ενθαρρύνουν την αναφορά τρωτών σημείων των ΤΠΕ της επικράτειας τους, ενώ επισημαίνουν τη σπουδαιότητα ανταπόκρισης σε αιτήματα βοήθειας για την αντιμετώπιση κακόβουλων ενεργειών (GGE, 2015). Τέλος, επιμένουν για την ανάγκη λήψης εύλογων μέτρων για τη διατήρηση της ακεραιότητας της εφοδιαστικής αλυσίδας σκοπεύοντας στην αποτροπή της διάδοσης κακόβουλών εργαλείων και τεχνικών, καθώς και τον περιορισμό της χρήσης τους στον κυβερνοχώρο (GGE, 2015). Όλες αυτές οι ενέργειες, ακόμα και αν αποτελούν τα πρώτα και βασικά βήματα προς τη θεσμοποίηση της υπεύθυνης κρατικής συμπεριφοράς για την επιστημονική κοινότητα, παραμένουν, όπως έχει ήδη ειπωθεί, μη δεσμευτικές για τα κράτη με αποτέλεσμα ο περιορισμός των κακόβουλων συμβάντων στον κυβερνοχώρο να υπόκεινται στη διακριτική ευχέρεια των εθνικών κυβερνήσεων.

4.1.4. Απόδοση Ευθύνης

Ένα ακόμα θέμα που πραγματεύονται οι Εκθέσεις είναι η χρήση 'αντιπροσώπων' (proxies) από τα κράτη για τη διάπραξη κακόβουλων κυβερνοεπιστατικών. Αυτοί μπορεί να είναι ιδιώτες ή ομάδες χάκερς, οργανώσεις ακόμα και εγκληματικές οργανώσεις με οικονομικά, ιδεολογικά, πολιτικά ή και άλλα κίνητρα (GGE, 2010). Η μετάθεση της δράσης από το κράτος σε ιδιώτες προσφέρει πλεονεκτήματα τόσο στο κράτος, καθώς δυσχεραίνεται ο εντοπισμός του ως υπαιτίου για την επίθεση, όσο και για τον αντιπρόσωπο του, ο οποίος, ως ιδιώτης, ακόμα και αν

αποκαλυφθεί η δράση του, δύσκολα θα του επιβληθούν κυρώσεις. Το σύνηθες είναι να επιβάλλονται κυρώσεις ή να λαμβάνονται ενέργειες αυτοάμυνας από κράτος σε κράτος, καθώς όταν μια ενέργεια διεξάγεται από μη κρατικό δρώντα αποτελεί απλά μια παράνομη πράξη και όχι παραβίαση του διεθνούς δικαίου, των διεθνών συνθηκών, των συμβάσεων και των νορμών που θέτουν τους κανόνες ρύθμισης των διακρατικών σχέσεων (Schmitt, 2013, σ.46).

Για την επιβολή, όμως, κυρώσεων εναντίον μιας κρατικής οντότητας που διενήργησε κακόβουλα, επιζητείται η προηγούμενη απόδοση της ευθύνης σε αυτή. Σύμφωνα λοιπόν με τις ισχύουσες αρχές, η απόδοση κακόβουλων κυβερνοεπιστατικών αποτελείται από τρία συστατικά, την τεχνική, την νομική και την πολιτική απόδοση. Η διαδικασία ξεκινάει από το τεχνικό κομμάτι όπου γίνεται προσπάθεια εύρεσης της προέλευσης της κακόβουλης δράσης και του ατόμου ή της οντότητας που βρίσκεται πίσω από αυτή μελετώντας το λογισμικό που χρησιμοποιήθηκε, τους διακομιστές εντολών και ελέγχου, τα δεδομένα κίνησης και θέσης κλπ., ενώ βοήθημα αποτελούν τα εγχειρίδια τεχνικών εκθέσεων με νέα επιχειρησιακά δεδομένα που εκδίδουν ανά τακτά χρονικά διαστήματα ο ακαδημαϊκος χώρος και ο ιδιωτικός τομέας (Kastelic, 2022). Οι τεχνικές μέθοδοι συμπληρώνονται με κοινωνικοπολιτικά στοιχεία με σκοπό να παράγουν πιο αξιόπιστα αποτελέσματα (Kastelic, 2022).

Στη συνέχεια επιχειρείται η νομική απόδοση. Σημαντικό στοιχείο σε αυτό το σημείο αποτελεί η εύρεση συνδετικού κρίκου μεταξύ του φυσικού προσώπου ή της οντότητας με το κράτος που έδωσε τις οδηγίες, έλεγχε ή κατεύθυνε τις πράξης του/της. Όπως έχει επιβεβαιώσει και το διεθνές δικαστήριο, για την απόδοση ευθύνης σε κράτος δεν απαιτείται αποτελεσματικός έλεγχος επί των δράσεων (effective control), αλλά αρκεί ο συνολικός έλεγχος (overall control) (International Court of Justice, 1986). Μάλιστα, αν η έρευνα δείξει, ότι η λανθασμένη κατά τις διεθνείς νόρμες και κανόνες πράξη, προέρχεται από κρατική υπηρεσία ακόμα και αν οι αρμοδιότητες της είναι εκδιαμέτρου αντίθετες με επιχειρήσεις στο πεδίο του κυβερνοχώρου, τότε πάλι η ευθύνη αποδίδεται στο κράτος (Kastelic, 2022).

Τέλος, απαιτείται η πολιτική απόδοση ευθυνών, η οποία έρχεται να συγκεράσει τα δεδομένα που τις προσφέρουν οι άλλες δύο. Η απόφαση καταλογισμού μιας κακόβουλης ενέργειας σε μια τρίτη χώρα και οι συνέπειες που αυτή θα επιφέρει στις μεταξύ τους σχέσεις είναι και πρέπει να είναι αμιγώς πολιτική απόφαση, ιδιαίτερα όταν η πιθανότητα λάθους παραμένει εφικτή. Από την έρευνα ενδέχεται να μην υπάρχουν επαρκή, τόσο ποιοτικά όσο και ποσοτικά, στοιχεία, να χρησιμοποιηθούν έμμεσα αποδεικτικά στοιχεία, ενώ η απόφαση να παρθεί βεβιασμένα και βασισμένη σε πολιτικοϊστορικές προκαταλήψεις. Για τους ανωτέρω λόγους, η τελική απόφαση, δημοσιοποίησης ή μη, της παραβατικής ενέργειας με στόχο την κάμψη της φήμης του 'εχθρού' και την απακατάστασης της διεθνούς τάξης και ασφάλειας, ακόμα και αν πραγματοποιηθεί έπειτα από διαβουλεύσεις, διαμεσολάβηση και κάθε είδους μέσο ειρηνικής επίλυσης των διαφορών, οφείλει να ληφθεί αποκλειστικά και μόνο από την εκτελεστική εξουσία.

4.1.5. Μέτρα Οικοδόμησης Εμπιστοσύνης

Σημαντικό κομμάτι ενασχόλησης και των δύο διακρατικών Ομάδων είναι η συνεργασία μεταξύ των κρατών, του ιδιωτικού τομέα και της κοινωνίας των πολιτών με την προώθηση μέτρων οικοδόμησης εμπιστοσύνης. Η έμφυτη καχυποψία που υπάρχει μεταξύ των κρατών, λόγω της έλλεψης μια υπερεθνικής κυβέρνησης (Jackson & Sørensen, 2006), μπορεί να μετριαστεί με τη δημιουργία εθελοντικών και μη δεσμετικών μέτρων τα οποία θα διαμορφώνουν μια παγκόσμια κοινή αντίληψη για τα θέματα που αφορούν τον κυβερνοχώρο. Τα μέτρα αυτά αυξάνουν τη διαφάνεια και την προβλεψιμότητα των κρατικών αντιδράσεων, ενώ μειώνουν την πιθανότητα παρανοήσεων και ανασφάλειας με αποτέλεσμα τη δημιουργία ενός ειρηνικού διεθνούς περιβάλλοντος. Η Ομάδα Εργασίας 2021-2025, υπόσχεται τη διεξαγωγή ενδιάμεσων συνεδριάσεων όπου θα συμμετέχουν όλοι οι ενδιαφερόμενοι οργανισμοί, μη-κυβερνητικοί οργανισμοί, επιχειρήσεις και ο ακαδημαϊκος χώρος. Αν και ο ΟΗΕ αποτελεί τη θεμέλιο λίθο προώθησης του διαλόγου και της δημιουργίας κοινών κατευθυντήριων αρχών

παγκοσμίως, ενθαρρύνει και τις δράσεις σε περιφερειακό και διμερές επίπεδο. Σε αυτές τα κράτη λόγω κοινών πολιτισμικών, θρησκευτικών, πολιτικών ή και άλλων δεσμών προχωρούν πολύ πιο εύκολα σε δεσμεύσεις διευκολύνοντας τις επιδιώξείς του.

Στις Εκθέσεις δίνεται, επίσης, ιδιαίτερη έμφαση και στην οικοδόμηση ικανοτήτων κυβερνοασφάλειας, με ιδιαίτερη μνεία στις αναπτυσσόμενες χώρες. Ο Οργανισμός προτρέπει την παροχή υλικοτεχνικής, γνωστικής ακόμα και οικονομικής βοήθειας σ' αυτές (OEWG, 2021), ώστε να μπορέσουν να προσεγγίσουν τις δυνατότητες των υπολοίπων χωρών και να λυθούν τα προβλήματα που ανακύπτουν από την έλλειψη των απαραίτητων, για την προστασία τους, υποδομών. Κάθε χώρα βιώνει διαφορετικά τις απειλές ανάλογα το βαθμό ψηφιοποίησής της (OEWG, 2022), επομένως, σκοπός, σύμφωνα με την Έκθεση της Ομάδας OEWG 2019-2021, είναι η γνώση μέσα από την αμοιβαία ανταλλαγή πληροφοριών και βέλτιστων πρακτικών όπου όλοι επωφελούνται από την ασφάλεια των ΤΠΕ (two-way street) (OEWG, 2022). Παρατηρείται, λοιπόν, μια σφαιρική αντιμετώπιση της διαχείρισης του κυβερνοχώρου από τον ΟΗΕ, θέτοντας τα όρια, επανεπιβεβαιώνοντας τους κανόνες και προωθώντας τη στενότερη συνεργασία μεταξύ των κρατών.

4.2. Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη - ΟΑΣΕ

Ο ΟΑΣΕ από την ίδρυσή του (1975) φροντίζει για την διατήρηση της παγκόσμιας ασφάλειας. Στο πλαίσιο της θωράκισης του κυβερνοχώρου, τα κράτη-μέλη του έχουν υιοθετήσει δύο δέσμες εθελοντικών και μη δεσμευτικών μέτρων οικοδόμησης εμπιστοσύνης (ΜΟΕ). Στόχος τους είναι η προώθηση της μεταξύ τους συνεργασίας με τη δημιουργία διάφανων διαδικασιών και προβλέψιμων ενεργειών κατά τη χρήση των ΤΠΕ, που μειώνουν τον κίνδυνο παρερμηνειών, πιθανών εντάσεων και ως εκ τούτου αποσταθεροποίησης στην Ευρώπη (OSCE, χ.χ.).

Το 2013 εισήχθησαν τα πρώτα έντεκα μέτρα οικοδόμησης εμπιστοσύνης μεταξύ των κρατών-μελών. Σύμφωνα με αυτά, τα κράτη δύνανται να παρουσιάζουν τις

απόψεις τους σχετικά με εθνικές και διακρατικές απειλές στον τομέα των ΤΠΕ, καθώς και να διευκολύνουν την συνεργασία στην ανταλλαγή πληροφοριών μεταξύ των αρμόδιων αρχών για θέματα ασφάλειας (OSCE, 2013). Επιπλέον, οφείλουν να διατηρούν δίαυλους επικοινωνίας σε κάθε επίπεδο έτσι ώστε να αποφευχθεί η κλιμάκωση των διακρατικών εντάσεων από παρερμηνείες (OSCE, 2013). Η ανταλλαγή, βέβαια, των πληροφοριών που στόχο έχει τη διασφάλιση του παγκόσμιου, ανοιχτού, ελεύθερου και ασφαλούς διαδικτύου, μπορεί να πραγματοποιείται και μέσω του φερέγγυου περιβάλλοντος του ΟΑΣΕ (OSCE, 2013). Ο Οργανισμός, επιπλέον, παροτρύνει τα κράτη-μέλη να εκσυγχρονίσουν το νομικό τους πλαίσιο προς διευκόλυνση της διακρατικής συνεργασίας, καθώς και τις θεσμικές και οργανωτικές τους διαδικασίες, στοχεύοντας στην επέκταση αυτής και στον ιδιωτικό τομέα (OSCE, 2013). Για την καλύτερη επικοινωνία προτείνει την δημιουργία ενός κοινού εθνικού σημείου επαφής, ενώ ακόμη προς αποφυγή οιασδήποτε παρεξήγησης και παρερμηνείας, προτρέπει τα κράτη να προσκομίζουν στον Οργανισμό μια λίστα με την εν χρήση, από πλευράς τους, ορολογία, ώστε να δημιουργηθεί ένα κοινό 'λεξικό' (OSCE, 2013). Προτάσσεται, επίσης, η χρήση των πλατφορμών και μηχανισμών του ΟΑΣΕ για να διευκολυνθεί η επικοινωνία αναφορικά με τα ζητήματα που προκύπτουν από τα ως άνω μέτρα και, τέλος, προβλέπονται συναντήσεις -τουλάχιστον τρεις φορές τον χρόνο- των εθνικών Εμπειρογνωμόνων για θέματα ΤΠΕ, σε ανεπίσημη μορφή και υπό την Επιτροπή Ασφαλείας του Οργανισμού, για να συζητείται η πρόοδος επί των υιοθετηθέντων μέτρων και η μελλοντική τους εξέλιξη (OSCE, 2013).

Στο πλαίσιο των ως άνω συναντήσεων, αρθρώθηκαν πέντε νέα ΜΟΕ, τα οποία υιοθετήθηκαν από το Μόνιμο Συμβούλιο του ΟΑΣΕ τον Μάρτιο του 2016. Πιο συγκεκριμένα, τα καινούργια μέτρα παροτρύνουν τα κράτη-μέλη να διευκολύνουν την ανταλλαγή πληροφοριών μέσω διάφορων επίσημων ή και ανεπίσημων μηχανισμών προκειμένου να ενισχυθεί, τόσο η διακρατική συνεργασία, όσο και οι συμπληρωματικές, για τη διατήρηση του ειρηνικού διαδικτύου, δράσεις που διενεργούνται υπό την αιγίδα των ΗΕ, λαμβάνοντας, βέβαια, υπόψη τις ανάγκες των συμμετεχόντων κρατών καθώς και του ιδιωτικού και ακαδημαϊκού τομέα (OSCE, 2016). Επίσης, προβλέπεται η διοργάνωση

ενεργειών/δράσεων για τη δημιουργία και διατήρηση διαύλων επικοινωνίας μεταξύ των αρμόδιων κρατικών αρχών, και επιζητείται η αναδιάρθρωση της εσωτερικής νομοθεσίας προκειμένου να προαχθεί η συνεργασία κράτους-ιδιωτικού τομέα και η ανάπτυξη μεταξύ τους μηχανισμών αντιμετώπισης των κινδύνων ασφάλειας (OSCE, 2016). Ενθαρρύνεται, ακόμα, η συμμετοχή σε fora, περιφερειακού επιπέδου, αρμόδια για την προστασία των κρίσιμων υποδομών, ώστε να διευρυνθεί έτι περισσότερο η συνεργασία μεταξύ των κρατών ανταλλάσσοντας απόψεις, ανησυχίες, βέλτιστες πρακτικές, διαδικασίες θωράκισης των υποδομών και αντιμετώπισης των κινδύνων καθώς και χρηστών νομοθεσιών (OSCE, 2016). Τέλος, κρίσιμης σημασίας θεωρείται η αναφορά, σε κατάλληλο πάντα θεσμικό επίπεδο, τρωτών σημείων και πιθανών μέσων αντιμετώπισής τους, απαραίτητων δηλαδή στοιχείων για την θωράκιση των κρατών-μελών, αυτοσκοπού του Οργανισμού (OSCE, 2016).

Συνοψίζοντας, ο ΟΑΣΕ στοχεύει στη δημιουργία ασφαλών διαύλων επικοινωνίας για την ανταλλαγή ιδεών, βέλτιστων πρακτικών, τρωτών σημείων και διαθέσιμων διορθωτικών μέσων, καθώς και πληροφοριών οργανωτικού και διαδικαστικού χαρακτήρα σε διάφορα επίπεδα (εξουσιοδοτημένοι εκπρόσωποι κρατών, ακαδημαϊκοί, ιδιωτικός τομέας) και υπό διαφορετικές περιστάσεις (συναντήσεις υπό τον ΟΑΣΕ, συνέδρια, ομιλίες) με αποτέλεσμα τη δημιουργία μιας κοινής γλώσσας επικοινωνίας, κατάλληλης είτε για την αποφυγή παρερμηνειών, είτε για την ταχεία και έγκαιρη αντιμετώπιση τυχόν κυβερνοπεριστατικών από τις αρμόδιες κρατικές αρχές.

4.3. Οργανισμός Βορειο-Ατλαντικού Συμφώνου – NATO (North Atlantic Treaty Organazation)

Το NATO αναφέρθηκε πρώτη φορά στην ανάγκη προστασίας των Συμμάχων από τις κυβερνοεπιθέσεις στην Σύνοδο Κορυφής της Πράγας το 2002 (Brent, 2019; NATO, 2002), ενώ το 2008 υιοθέτησε την πρώτη συμμαχική πολιτική για την κυβερνοάμυνα (Brent, 2019; NATO, 2008). Λίγα χρόνια αργότερα (2016) και αφότου είχε αναγνωρίσει τον κυβερνοχώρο σε πέμπτο πεδίο στρατιωτικής

δραστηριότητας, προχώρησε σε Κοινή Δήλωση του Γενικού Γραμματέα του Οργανισμού με τον Πρόεδρο του Ευρωπαϊκού Συμβουλίου και τον Πρόεδρο της Ευρωπαϊκής Επιτροπής με την οποία συμφωνήθηκε η συνεργασία ΕΕ-ΝΑΤΟ και στον τομέα της κυβερνοασφάλειας. Η συμφωνία αυτή επανεπιβεβαιώνεται ανά τακτά χρονικά διαστήματα με νέα δεσμευτικά κείμενα επαύξησης της διατλαντικής συνεργασίας (Ευρωπαϊκό Κοινοβούλιο, 2021; Brent, 2019; NATO, 2016b). Την ίδια χρονιά, οι αρχηγοί των κρατών-μελών δεσμεύτηκαν από ένα πλέγμα δράσεων και ενεργειών, το Cyber Defence Pledge (NATO, 2016b). Σύμφωνα με αυτό, τα συμμαχικά κράτη οφείλουν να διαθέτουν επαρκείς πόρους για την ευαισθητοποίηση και την κατανόηση των απειλών που προέρχονται από τη χρήση των ΤΠΕ, καθώς και για την προώθηση της ανάπτυξης των κυβερνοϊκανοτήτων και δεξιοτήτων τους (Digital Watch, 2016; NATO, 2016a). Προβλέπεται, μάλιστα, ετήσια αξιολόγηση για την πρόοδο επ' αυτών κατά τη διάρκεια των συνόδων κορυφής (Digital Watch, 2016; NATO, 2016a).

Το Cooperative Cyber Defence Centre of Excellence,[15] υπό την αιγίδα του ΝΑΤΟ, ανέπτυξε το Tallinn Manual, ένα εγχειρίδιο εξέχουσας σημασίας που προσπαθεί να μεταφέρει του κανόνες του διεθνούς δικαίου στα μέτρα του κυβερνοχώρου δίνοντας έμφαση στις κυβερνοεπιχειρήσεις που παραβιάζουν την απαγόρευση χρήσης βίας και επισύρουν το δκαίωμα της νόμιμης αυτοάμυνας. Αν και το αποτέλεσμα της έρευνας δεν είναι δεσμευτικό για τη Συμμαχία ούτε εκφράζει τις απόψεις της, αποτελεί ένα σηματικό εγχειρίδιο που προσπαθεί να οριοθετήσει τις νέες δυνάμει στρατιωτικού χαρακτήρα δυνατότητες του κυβερνοχώρου, στα χέρια των διαμορφωτών της πάγκοσμιας τάξης πραγμάτων.

Στο πλαίσιο της Σύνοδου Κορυφής της Ουαλίας του 2014, το ΝΑΤΟ είχε εκρίνει τη συμμαχική Στρατηγική για την Κυβερνοάμυνα με την οποία αναγνωρίστηκε η

[15] Το Συνεργατικό Κέντρο Αριστείας για την Κυβερνοάμυνα αποτελεί ένα διεπιστημονικό και πολυεθνικό κόμβο έρευνας, εκπαίδευσης και ανάπτυξης αμυντικών δυνατοτήτων στο πεδίο του κυβερνοχώρου. Είναι πιστοποιημένο από το ΝΑΤΟ, αλλά δεν εκφράζει τις απόψεις του Οργανισμού. Η έδρα του βρίσκεται στο Ταλλίν της Εσθονίας (ΓΕΕΘΑ, 2015; CCDCEO, χ.χ.).

ενεργοποίηση του άρθρου 5 της Συνθήκης της Ουάσιγκτον[16] σε περίπτωση εκδήλωσης κυβερνοεπίθεσης σε κράτος-μέλος. Συνεπώς, το δικαίωμα της συλλογικής αυτοάμυνας επεκτείνεται και σε περιστατικά τα οποία προέρχονται από τον κυβερνοχώρο, χωρίς ωστόσο να τίθενται τα κριτήρια που θα οδηγούσαν στην ενεργοποίησή του. Αναλυτικότερα, αποφασίστηκε ότι η ενεργοποίηση του άρθρου 5 δε θα γίνεται αυτόματα μετά από επίθεση στα πληροφοριακά συστήματα οποιουδήποτε κράτους-μέλους, αλλά ύστερα από εξέταση της εκάστοτε περίπτωσης από το Συμμαχικό Συμβούλιο (case-by-case-basis) (NATO, 2014)

Στη βάση, επομένως, της Στρατηγικής για την Κυβερνοασφάλεια, αλλά και της διεθνούς πρακτικής, με τη γνωστοποίηση του συμβάντος το πληγέν κράτος δικαιούται να ζητήσει την πάυση της κακόβουλης ενέργειας, τη μη επανάληψη της, καθώς και επανόρθωση της ζημιάς που προκλήθηκε. Σε περίπτωση επίθεσης μεγάλης κλίμακας που επισύρει τη πιθανότητα ανταπάντησης με χρήση στρατιωτικών μέσων, με τη μη αντίδραση ή μέχρι την αντίδραση των διεθνών οργάνων επιβολής της τάξης, σύμφωνα με το διεθνές δίκαιο, το κράτος μπορεί να κάνει άσκηση του δικαιώματος της αυτοάμυνα τηρώντας τις προϋποθέσεις της αναγκαιότητας, της αμεσότητας και της αναλογικότητας, όπως τις έθεσε το διεθνές δικαστήριο στην υπόθεση Caroline, ενώ σύμφωνα με την απόφαση του «Νικαράγουα εναντίον ΗΠΑ», ερμηνεύοντας το άρθρο 51 του Καταστατικού Χαρτη του ΟΗΕ μιλάει για την 'πιο σοβαρή' (most grave) χρήση βίας (International Court of Justice, 1986), οδηγώντας στο συπμπέρασμα ότι μόνο μια κυβερνοεπιχείρηση που θα προκαλέσει μεγάλες καταστροφές, τραυματισμούς και ανθρώπινες απώλειες θα μπορούσε να ενεργοποιήσει το δικαίωμα της αυτοάμυνας.

[16] Άρθρο 5 της Συνθήκης της Ουάσιγκτον: «*Τα Συμβαλλόμενα Μέρη συμφωνούν ότι, ένοπλος επίθεσις εναντίον ενός ή πλειόνων εξ αυτών εν Ευρώπη ή Βορείω Αμερική θέλει θεωρηθεί επίθεσις εναντίον απάντων και, συνεπώς, [...] εν τη ασκήσει του υπό του άρθρου 51 του Χάρτου των Ηνωμένων Εθνών […] θα συνδράμη τα υφιστάμενα την επίθεσιν εν ή πλείονα Μέρη δια της αμέσου λήψεως, τόσον ατομικώς όσον και από συμφώνου μετά των ετέρων Μερών, των μέτρων άτινα θεωρεί αναγκαία περιλαμβανομένης της χρήσεως ενόπλου βίας [...]*» (NATO, 1949).

4.3.1. Χρήση βίας - Απειλή χρήσης βίας – Νόμιμη Αυτοάμυνα

Το ΝΑΤΟ, όπως προαναφέρθηκε, ήδη από το 2014 έχει ανακοινώσει την υπαγωγή των κυβερνοεπιθέσεων στο άρθρο 5 της Συμμαχίας και ως εκ τούτου τη χρήση συλλογικής βοήθειας για νόμιμη αυτοάμυνα και για τα κυβερνοπεριστατικά, ενώ παρόμοιο καθεστώς έχει θεσπίσει και η ΕΕ.[17] Ωστόσο, ουδείς Οργανισμός δεν έχει προβεί σε ανάλυση της έννοιας του μεγέθους της 'ζημίας' που θα πρέπει να έχει προκληθεί, ώστε να δικαιολογηθεί η χρήση στρατιωτικών μέσων για την αποκατάστασή της από το πληγέν κράτος και τους συμμάχους του. Τα αποτελέσματα μιας κυβερνοεπίθεσης άλλοτε μπορεί να είναι άμεσα και απτά, όπως η καταστροφή στρατιωτικού εξοπλισμού ή η απώλεια σε ανθρώπινες ζωές, άλλοτε μπορεί να είναι εμφανή μακροπρόθεσμα, μπορεί ωστόσο να είναι άμεσα αντιληπτά αλλά η κατηγοριοποίηση τους σε 'ζημία μεγάλης κλίμακας' ('most grave') να είναι αμφιλεγόμενη, όπως η διακοπή λειτουργίας των σέρβερς κρίσιμων για την λειτουργία ενός κράτους υποδομών, διχάζοντας την εγχώρια και διεθνή πολιτική ηγεσία για το μέγεθος των κυρώσεων που δύνανται να επιβληθούν.

Οι κυβερνοεπιθέσεις με βάση την ένταση τους και σύμφωνα με το ισχύον διεθνές νομικό πλαίσιο μπορούν να κατηγοροποιηθούν σε τέσσερα είδη· αυτές που δημιουργούν εμπόδια αποκλειστικά και μόνο στη λειτουργικότητα της κρατικής οντότητας, αυτές που ενεργοποιούν το αρθρο 2 (4) των ΗΕ και την 'χρήση βίας' ('use of force'), αυτές που ενεργοποιούν την επέμβαση του Συμβουλίου Ασφαλείας για την αποκατάσταση της διεθνούς τάξης και ασφάλειας,[18] και τέλος εκείνες που επισύρουν την χρήση στρατιωτικών μέσων ατομικής ή συλλογικής αυτοάμυνας (άρθρο 51 Χάρτη ΗΕ) (Pipyros κ.ά., 2017; Pipyros, Thraskias, κ.ά., 2016). Ωστόσο, οι ενέργειες που λαμβάνουν χώρα εντός του κυβερνοπεριβάλλοντος διαφέρουν από

[17] Βλ. σ. 69.

[18] Το Κεφάλαιο XII του Χάρτη των ΗΕ κάνει αναφορά τις ενέργειες που δύναται λάβει το ΣΑ/ΗΕ σε περίπτωση διατάραξης της ειρηνικής συνύπαρξης των κρατών. Πιο συγκεκριμένα, μπορεί να λάβει προσωρινά και μη στρατιωτικού χαρακτήρα μέτρα, όπως η διακοπή των διπλωματικών σχέσεων και η επιβολή εμπάργκο. Ωστόσο, ο μη τερματισμός της εχθρικής, για την διεθνή ειρήνη και ασφάλεια, ενέργειας μπορεί να επισύρει πιο επεμβατικές ενέργειες από τα ΗΕ έως και τη χρήση στρατιωτικών μέσων επιβολής της τάξης υπό την αιγίδα και καθοδήγηση του ΣΑ/ΗΕ (Οργανισμός Ηνωμένων Εθνών, 1945).

το συμβατικό πεδίο μάχης με αποτέλεσμα οι συνέπειες μιας κυβερνοεπίθεσης μην είναι εμφανείς όπως στα κλασικά πεδία πολέμου και η κατάταξη στην αντίστοιχη κατηγορία να είναι αρκετά δυσχερής έως και αδύνατη (Pipyros, Mitrou, κ.ά., 2016).

Το εγχειρίδιο του Ταλίν ήταν αυτό που έθεσε κάποια ενδεικτικά κριτήρια για τον καθορισμό των ενεργειών που αποτελούν χρήση βίας μεγάλης κλιμακας και επομένως μπορούν να ενεργοποιήσουν το άρθρο 51 περί νόμιμης ατομική ή συλλογικής αυτοάμυνας. Πρώτον θέτει το κριτήριο της σοβαρότητας της ζημιάς που προκλήθηκε σε άτομα και περιουσίες, σε σχέση με το σκοπό, τη διάρκεια και την ένταση της επίθεσης (Schmitt, 2013). Συνεχίζει με την αμεσότητα των αποτελεσμάτων και την αιτιώδη συνάφεια των επιθετικών ενεργειών με αυτά, θεωρώντας πως στις στρατιωτικές ενέργειες η αιτία και το αποτέλεσμα είναι άρρηκτα συνδεδεμένα (Schmitt, 2013). Έπειτα αναφέρεται στο βαθμό διείσδυσης της κακόβουλης δράσης στις υποδομές του πληττόμενου κράτους, και αν τα αποτελέσματα είναι μετρήσιμα, αν δηλαδή οι συνέπειες είναι ποσοτικοποιημές και αναγνωρίσιμες, ικανές να επιφέρουν την απαιτούμενη απόδοση ευθυνών (Schmitt, 2013). Η ύπαρξη προφανούς και στενής σχέση της κυβερνοεπίθεσης με μία κρατική οντότητα, καθώς και η σύνδεση της με άλλες επιχειρήσεις στρατιωτικού χαρακτήρα που ήδη λαμβάνουν χώρα (Schmitt, 2013). Τελευταίο κριτήριο αποτελεί η τεκμαιρόμενη νομιμότητα της επιθέσεως, εφόσον στο διεθνές δίκαιο όποια απαγόρευση δεν καταγράφεται ρητά, θεωρείται ότι επιτρέπεται (Schmitt, 2013).

Εναλλακτικά σε περιπτώσεις μικρότερης έντασης της βίας, το διεθνές δίκαιο παρέχει τη δυνατότητα χρήσης αντίμετρων. Τα μέτρα αυτά πρέπει να είναι μη αναγκαστικής φύσης, αναστρέψιμα, ποσοτικά και ποιοτικά ανάλογα της ζημιάς που προκλήθηκε, καθώς επίσης πρέπει να ασκούνται ατομικά και όχι συλλογικά (International Court of Justice, 1986). Όσον αφορά τα κυβερνοπεριστατικά, προτάσσεται η επιλογή των αντισταθμιστικών μέτρων (Pawlak & Biersteker, 2019). Αυτά, σε αντίθεση με τα δύο προηγούμενα, είναι νόμιμα και μη βίαια μέτρα τερματισμού μιας εχθρικής δράσης, όπως η διακοπή των διπλωματικών σχέσεων ή η επιβολή εμπάργκο.

Επομένως, στο εγχειρίδιο του Ταλίν έγινε μια προσπάθεια καθορισμού ορισμένων κριτηρίων για την υποβοήθηση των κρατών στην επιλογή των μέσων προστασίας της εθνικής τους κυριαρχίας. Τα ως άνω οκτώ κριτήρια ('Σοβαρότητα', 'Αμεσότητα', 'Ευθύτητας', 'Επεμβατικότητα', 'Μετρησιμότητα των αποτελεσμάτων', 'Πιθανή νομιμότητα', 'Κρατική συμμετοχή', 'Στρατιωτικός Χαρακτήρας'/ 'Severity', 'Immediacy', 'Directness', 'Invasiveness', 'Measurability of effects', 'Presumptive Legality', 'State Involvement', 'Military Character') που υιοθέτησε το Κέντρο Αριστείας ακολουθούν την προσέγγιση βάσει των συνεπειών της επίθεσης του Schmitt (1999). Είναι ποιοτικά στοιχεία αξιολόγησης των κυβερνοπεριστατικών που ωστόσο ο συνδυασμός τους μπορεί να παραγάγει χρήσιμα συμπεράσματα για την κατάταξη των κυβερνοεπιθέσεων στην κατηγορία της 'χρήσης βίας' (Schmitt, 1999). Μάλιστα ο Schmitt πρότεινε μια ακόμη κατηγοριοποίηση της 'χρήσης βία', τοποθετώντας την έννοια σε ένα φάσμα όπου στο ένα του άκρο βρίσκονται οι επιχειρήσεις που πληρούν τα κριτήρια υπαγωγής στις στρατιωτικού χαρακτήρα επιχειρήσεις, στο άλλο άκρο αυτές που δεν τις πληρούν και στο ενδιάμεσο εκείνες που ανήκουν στην 'γκρίζα ζώνη', στο μεταίχμιο ειρήνης και πολέμου (Pipyros κ.ά., 2018; Schmitt, 1999).

Πέρα από την προτάσεις του Schmitt, έχουν χρησιμοποιηθεί διάφοροι ποσοτικοί μέθοδοι τυποποίησης της λήψης αποφάσεων που χρησιμοποιούν τον συνδυασμό των ως άνω κριτηρίων. Πιο διαδεδομένη είναι η μέθοδος της απλής προσθετικής στάθμισης ('Simple Additive Weighting Method') (Pipyros, Thraskias, κ.ά., 2016). Σε αυτή το αποτέλεσμα της 'σοβαρότητας' της 'χρήσης βίας' αποτελεί το άθροισμα του βάρους των συντελεστών μέτρησης της απειλής επί του μέτρου απόδοσης των εναλλακτικών λύσεων (Pipyros κ.ά., 2018; Pipyros, Thraskias, κ.ά., 2016). Εναλλακτική μέθοδος είναι αυτή του σταθμισμένου προϊόντος ('The Weighting Product Method (WPM)') όπου το αποτέλεσμα της 'σοβαρότητας' της 'χρήσης βίας' είναι το γινόμενο των μέτρων απόδοσης των εναλλακτικών λύσεων στη δύναμη του βάρους των συντελεστών μέτρησης (Pipyros κ.ά., 2017, 2018), ενώ έχουν προταθεί και συνδυασμοί αυτών των μεθόδων. Μια τέτοια πρόταση παρουσιάζεται από τον Πιπύρο κ.α. (Pipyros κ.ά., 2017) όπου πρώτα υπολογίζεται η 'συνολική ένταση' ('total intensity') της απειλής ως το γινόμενο της 'έντασης' επί

της ‘μετρησιμότητας των αποτελεσμάτων’. Η ‘ένταση’ αποτελεί μια πολυπαραγοντική έννοια που αποτελείται από το άθροισμα της ‘σοβαρότητα’, της ‘αμεσότητα’, της ‘ευθύτητας’, και της ‘επεμβατικότητα’ της επίθεσης (Pipyros, 2019; Pipyros κ.ά., 2017). Στη συνέχεια η ‘συνολική ένταση’ πολλαπλασιάζεται με την πιθανή νομιμότητα της επίθεσης, την ύπαρξη κρατικής εμπλοκής σε αυτή καθώς και την παρουσία παράλληλων συμβατικών στρατιωτικών ενεργειών. Το αποτέλεσμα της παράγει το γινόμενο της ‘χρήσης βίας’ (Pipyros, 2019; Pipyros κ.ά., 2017). Μάλιστα, η ύπαρξη κρατικής εμπλοκής ή και παράλληλων συμβατικών στρατιωτικών δραστηριοτήτων αποτελούν τα πλέον χαρακτηριστικά στοιχεία υπαγωγής των κυβερνοεπιθέσεων στις ενέργειες στρατιωτικού χαρακτήρα που εμπίπτουν στο άρθρο 2(4) των ΗΕ (Pipyros κ.ά., 2017).

Όλα τα παραπάνω μοντέλα τυποποίησης της μέτρησης του επιπέδου της βίας μιας κυβερνοεπίθεσης μπορεί να είναι άκρως βοηθητικά για την κατηγοριοποίηση των ενεργειών σε εκείνες που νομιμοποιούν την χρήση στρατιωτικών μέσων για αυτοάμυνα ή όχι, ωστόσο, η τελική απόφασης απόδοσης της κακόβουλης ενέργειας και ανταπάντησης σε αυτή παραμένει πολιτική απόφαση. Η πολιτική ηγεσία της θιγόμενης κρατικής οντότητας είναι η πλέον αρμόδια να σταθμίσει τις επιπτώσεις της επιθετικής ενέργειας, αλλά και εκείνες που θα επιφέρει η από μέρους της ανάληψη στρατιωτικής δράσης, ώστε να λάβει τη βέλτιστη δυνατή, για τα συμφέροντα της, απόφαση.

Καταληκτικά, οι ως άνω διεθνείς οργανισμοί, οι οποίοι με εξαίρεση τον ΟΗΕ, συναντόνται αποκλειστικά στον δυτικό κόσμο -όπως και η χώρα μας-, έχουν καταβάλει ιδιαίτερη προσπάθεια στην περιχαράκωση των δικαιωμάτων των μελών τους από τις νέες συνθήκες (θετικές ή αρητικές) που δημιουργούνται από την έλευση του κυβερνοχώρου στην καθημερινότητα τους. Ορίζουν νέους κανόνες συνεργασίας και θέτουν κόκκινες γραμμές που πρέπει να είναι σεβαστές από τα κράτη-μέλη τους, αλλά και από τρίτους δρώντες του διεθνούς συστήματος, για να προστατευούν τα ίδια τα κράτη και κατ’ επέκταση οι Οργανισμοί, καθώς και να αποφευχθούν παρερμηνείες που είναι ικανές να καταστρατηγήσουν τα κρατικά

συμφέροντα και να κλονίσουν τις παγόσμιες ισορροπίες. Ωστόσο, τα δικαιώματα και οι υποχρεώσεις που επικαλούνται επηρεάζουν μόνο τα μέλη τους και στις περισσότερες περιπτώσεις δεν είναι κάν δευσμευτικά, αφήνοντας θεσμικά κενά και γκρίζες ζώνες δικαιοδοσίας εκμεταλλεύσιμα από τους επίδοξους δράστες.

ΚΕΦΑΛΑΙΟ 5:
'ΑΜΕΣΗΣ' ΕΦΑΡΜΟΓΗΣ ΡΥΘΜΙΣΕΙΣ

Η διαμόρφωση κανόνων μεγαλύτερης ομοφωνία και πρόθεσης για δέσμευση συναντάται συνήθως στους κόλπους περιφερειακών και υποπεριφερειακών οργανισμών με μικρό αριθμό μελών και μεγαλύτερη οικονομική, πολιτική και πολιτισμική συνάφεια, όπως η Ευρωπαϊκή Ένωση. Εκεί τα κράτη έχουν τη δυνατότητα ενεργότερης συμμετοχής στις διαπραγματεύσεις επί των τελικών κειμένων, ενώ τα συμφέροντα που διακυβεύονται, συνήθως λόγω της οικονομικής τους εξάρτησης, είναι η αιτία ανάληψης περισσότερων δεσμεύσεων και ευθυνών. Αποτέλεσμα είναι το φιλικό πλαίσιο ενός μικρότερου οργανισμού να δρα επιβοηθητικά στην ανάγκη οριοθέτησης κρίσιμων, για τα συμφέροντα των κρατών, τομέων. Αυτό γίνεται αντιληπτό και στο παρόν κεφάλαιο καθώς οι κανονισμοί και οι οδηγίες που δεσμεύουν τα ευρωπαϊκά κράτη είναι λεπτομερέστερες και εφαρμόζονται άμεσα και σχεδόν αυτόματα από τα μέλη της Ένωσης.

5.1. Ευρωπαϊκή Ένωση & Κυβερνοασφάλεια

Η εντατική ενασχόληση της ΕΕ με την ασφάλεια του κυβερνοχώρου ξεκίνησε το 2013 με την υιοθέτηση της Στρατηγικής της Ένωσης για την κυβερνοασφάλεια. Σύμφωνα με αυτή για να διατηρηθεί ο κυβερνοχώρος ανοιχτός, ασφαλής και ανθεκτικός, πρέπει να στηριχθεί πάνω στις αρχές, τις αξίες και τους κανόνες που εφαρμόζει η ίδια η ΕΕ. Η Στρατηγική θέτει πέντε, προς επίτευξη, άξονες δράσης: την ανθεκτικότητα του κυβερνοχώρου, την καταπολέμηση του κυβερνοεγκλήματος, την ανάπτυξη μιας πολιτικής κυβερνοάμυνας και δυνατότητες που έχουν άμεση σχέση με την Κοινή Πολιτική Άμυνας και Ασφάλειας (ΚΠΑΑ), την ανάπτυξη βιομηχανικών και τεχνολογικών πόρων για την κυβερνοασφάλεια και την εδραίωση συνεκτικής διεθνούς πολιτικής για τον κυβερνοχώρο από την ΕΕ προωθώντας τις θεμελιώδεις αξίες της (European Commission, 2013). Με αφετηρία αυτό το γεγονός, ακολούθησε πλήθος,

δεσμευτικών και μη, κειμένων σχετικά με την προστασία του κυβερνοχώρου και τη δράση ενάντια στις κακόβουλες ενέργειες προερχόμενες από αυτό ή σε αυτόν (Codagnone κ.ά., 2022). Για την αντιμετώπιση, λοιπόν, των όλο και αυξανόμενων κυβερνοεπιθέσεων, η στρατηγική της Ένωσης στηρίζεται, κυρίως, σε τρεις βασικούς πυλώνες. Αυτοί είναι ο κανονισμός 2019/881 «*σχετικά με τον ENISA και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών ή Πράξη για την κυβερνοασφάλεια*», οι οδηγίες 2016/1148 ή NIS και 2022/2555 ή NIS II «*σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*» (όπου η δεύτερη θα αντικαταστήσει την πρώτη εντός του 2024) και η «*Διπλωματική Εργαλειοθήκη για την απόκριση της ΕΕ σε κακόβουλες ενέργειες στον κυβερνοχώρο*».

5.1.1. Πράξη για την κυβερνοασφάλεια – Κανονισμός 2019/881

Με τον κανονισμό 2019/881, του Κοινοβουλίου και του Συμβουλίου της ΕΕ, ενισχύεται η θέση του ENISA λαμβάνοντας μόνιμη εντολή δράσης, μεγαλύτερο εύρος αρμοδιοτήτων και περισσότερους πόρους. Ο ENISA, λόγω της πολυετούς εμπειρίας του, του εξειδικευμένου προσωπικού του και της ανεξαρτησίας του, αποτελεί κέντρο εμπειρογνωσίας στον τομέα της κυβερνοασφάλειας που επικουρεί τόσο την ίδια την Ένωση και τους θεσμούς της όσο και τα κράτη-μέλη της. Ρόλος του ENISA είναι να χαράσσει και να εφαρμόζει πολιτικές ασφάλειας, να συμβάλλει στην ανάπτυξη των κυβερνοϊκανοτήτων της ΕΕ και να προωθεί την επιχειρησιακή συνεργασία (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Πέρα από την προώθηση της συνεργασίας μεταξύ των κρατών-μελών, στόχος είναι και η διασφάλιση του διαλόγου μεταξύ όλων των ενδιαφερόμενων μερών στον ιδιωτικό και δημόσιο τομέα, καθώς και όλων των ενδιαφερόμενων μερών ανά τον κόσμο (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Στον τομέα των αρμοδιοτήτων του δηλαδή εντάσσεται η ενίσχυση των σχέσεων της ΕΕ με τρίτες χώρες ή και με άλλους διεθνείς και περιφερειακούς οργανισμούς. Θεμελιώδης είναι ακόμη η συνεισφορά

του στην ευαισθητοποίησης του κοινού σε σχέση με τους κινδύνους που ελλοχεύουν στον κυβερνοχώρο και τη σημασία της προστασίας του, είτε μέσω της εκμάθησης και εφαρμογής ενεργειών κυβερνο-ϋγιεινής, είτε μέσω της προώθησης καινοτόμων ενεργειών ως αποτέλεσμα της έρευνας στον κλάδο της κυβερνοασφάλειας (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Τέλος, ο ENISA έχει ενεργητικό ρόλο στη διαμόρφωση και εφαρμογή του συστήματος πιστοποίησης που εγκαθιδρύει ο κανονισμός (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019).

Το δεύτερο μέρος του κανονισμού στοιχειοθετεί το πλαίσιο για την πιστοποίηση των προϊόντων, των υπηρεσιών και των διαδικασιών των τεχνολογιών πληροφορικής και επικοινωνιών. Η πιστοποίηση έχει διττό ρόλο. Πρώτον να ενισχύσει την εμπιστοσύνη σε προϊόντα ΤΠΕ και δεύτερον να αποφύγει τις συγκρούσεις και στις επικαλύψεις ως αποτέλεσμα συγκερασμού πολλών διαφορετικών εθνικών συστημάτων πιστοποίησης, στοχεύοντας στη βελτιστοποίηση της λειτουργίας της εσωτερικής αγοράς (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Προς αυτό το σκοπό, ο κανονισμός θέτει κοινές απαιτήσεις και κοινά κριτήρια αξιολόγησης δημιουργώντας ένα κοινό πλαίσιο για όλα τα κράτη. Επιπλέον, λόγω των κοινών προδιαγραφών, αναγνωρίζει αυτόματα την πιστοποίηση των προϊόντων από ένα κράτος-μέλος σε ολόκληρη την Ένωση (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Το πλαίσιο πιστοποίησης δίνει ακόμη τη δυνατότητα αυτοαξιολόγησης της συμμόρφωσης, η οποία, όπως και η πιστοποίηση, αποτελεί εθελοντικό μέτρο (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019). Βέβαια, καμία από τις δύο δεν μπορεί να εγγυηθεί ότι τα προϊόντα, οι υπηρεσίες ή και οι διαδικασίες ΤΠΕ είναι ασφαλή. Αποτελούν απλά έναν τρόπο μετριασμού του κινδύνου από κακόβουλες ενέργειες που προέρχονται από τον κυβερνοχώρο.

5.1.2. NIS I & NIS II – Οδηγία 2016/1148 & Οδηγία 2022/2555

Η NIS II αποτελεί αποκύημα της επανεξέτασης της Οδηγίας 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων σε ολόκληρη την Ένωση, την οποία και θα αντικαταστήσει. Η NIS αποσκοπούσε στη διασφάλιση ενός κοινού επιπέδου πανευρωπαϊκής ασφάλειας στον κυβερνοχώρο με υιοθέτηση εθνικών στρατηγικών κυβερνοασφάλειας αποτελούμενων από κοινές, έως ένα βαθμό, προδιαγραφές προστασία των κρίσιμων υποδομών των κρατών-μελών. Για τον σκοπό αυτό, δημιουργήθηκαν σε ενωσιακό και εθνικό επίπεδο οι θεσμοί των αρμόδιων αρχών, του ενιαίου σημείου επαφής καθώς και οι ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT) (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Παρά τις αλλαγές που επέφερε σε κανονιστικό και θεσμικό επίπεδο, πολύ σύντομα έφτασε στα όρια της (European Commission, 2020). Ο ψηφιακός μετασχηματισμός γνώρισε πρωτόγνωρους ρυθμούς κυρίως εξαιτίας των νέων αναγκών της καθημερινότητας που προέκυψαν μετά το ξέσπασμα της πανδημίας Covid-19 με αποτέλεσμα την ανάγκη θεσμικής αναδιοργάνωσης για την επίτευξη της εύρυθμη λειτουργίας της εσωτερικής αγοράς (del Mar Negreiro Achiaga, 2023). Η λύση φαίνεται να δόθηκε από την Επιτροπή με την εκπόνηση πρότασης νέας οδηγίας. Σκοπός του νέου νομοθετήματος είναι η λήψη πιο εκτεταμένων και μακροπρόθεσμων πολιτικών για την ενίσχυση της ασφάλειας στον κυβερνοχώρο (European Commission, 2020). Διατηρεί τις βασικές δομές που εισήγαγε η NIS προχωρώντας, όμως, σε αρκετές προσθήκες στο πεδίο εφαρμογής της και τις ρυθμιστικές, ελεγκτικές και εποπτικές δυνατότητες που καθιερώνει για τα κράτη-μέλη της.

Η νέα οδηγία εφαρμόζεται σε κάθε ιδιωτική και δημόσια οντότητα, η οποία εμπίπτει στις κατηγορίες των βασικών ή σημαντικών οντοτήτων που καταγράφονται στα παραρτήματα της I και II αντίστοιχα (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Τροποποιεί τις κατηγορίες στις οποίες ήταν διαρθρωμένες μέχρι πρότινος όλες οι οντότητες που

ενέπιπταν στο πεδίο εφαρμογής της NIS και ως εκ τούτου αντί για βασικές υπηρεσίες και παρόχους ψηφιακών υπηρεσιών έχουμε βασικές και σημαντικές οντότητες, ενώ προσθέτει και νέα είδη υπηρεσιών που ενσωματώνονται στις καινούργιες κατηγοριοποιήσεις της.[19] Θέτει, ακόμη, κοινό κριτήριο μεγέθους για τον προσδιορισμό των οντοτήτων που ρυθμίζει, συμπαρασύροντας όλες τις μεσαίου μεγέθους υπηρεσίες που ανήκουν σε κάποια από τις δύο κατηγορίες οντοτήτων (BDI, 2022; Kononenko, 2021), καθώς επίσης, με την προσθήκη, επί της δικαιοδοσίας της, "*των διαχειριστών συστημάτων ονομάτων τομέα, των υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων διαχειριζόμενων υπηρεσιών, των παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας καθώς και των παρόχων επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών κοινωνικής δικτύωσης*"(Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022), διευρύνει έτι περισσότερο το πεδίο εφαρμογής προσπερνώντας τα γεωγραφικά όρια της ΕΕ.

Καθιερώνει, ακόμη, την υποχρεωτική κοινοποίηση περιστατικών με σημαντικό ή δυνητικά σημαντικό αντίκτυπο (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Οι βασικές και σημαντικές οντότητες υποχρεούνται να προειδοποιούν για την ύπαρξη σημαντικού περιστατικού, χωρίς αδικαιολόγητη καθυστέρηση, εντός είκοσι τεσσάρων (24) ωρών και να προβαίνουν στην κοινοποίηση του εντός εβδομήντα δύο (72) ωρών (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Εξαίρεση αποτελούν οι πάροχοι υπηρεσιών εμπιστοσύνης, οι οποίοι οφείλουν να προβαίνουν σε κοινοποίηση των σημαντικών περιστατικών εντός είκοσι τεσσάρων (24) ωρών από τη στιγμή της αντίληψης τους (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Με τη λήψη της αρχικής προειδοποίησης οι αρμόδιες αρχές, εντός είκοσι

[19] Όσον αφορά τις βασικές υποδομές προστίθεται η δημόσια διοίκηση, οι διαστημικές υπηρεσίες και οι επιχειρήσεις διαχείρισης λυμάτων, ενώ στη νέα κατηγορία όπου εντάσσονται και οι ψηφιακοί πάροχοι συμπεριλήφθηκαν οι ταχυδρομικές υπηρεσίες, η διαχείριση αποβλήτων, οι επιχειρήσεις διαχείρισης χημικών προϊόντων, τροφίμων αλλά και κλάδοι του κατασκευαστικού τομέα (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

τεσσάρων (24) ωρών, απαντούν στην πληγούσα οντότητα (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Σε περίπτωση που το συμβάν επηρεάζει και άλλα κ-μ, τότε η αρμόδιες εθνικές αρχές προχωρούν στην ενημέρωσή τους (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Διευκρινίζεται, ωστόσο, πως οποιαδήποτε κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη, όπως είχε θεσπιστεί με την προγενέστερη της οδηγία (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016, 2022).

Στις νέες προσθήκες της NIS 2, οι διοικήσεις των σημαντικών και βασικών οντοτήτων οφείλουν να επιμορφώνονται, να εγκρίνουν, να εποπτεύουν και να λογοδοτούν για τις πολιτικές διαχείρισης κινδύνου (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Για την ασφάλεια, μάλιστα, των συστημάτων, των διαδικασιών καθώς και των παρεχόμενων υπηρεσιών προτάσσεται η λήψη, κατά προτεραιότητα, πιστοποιήσεων κυβερνοασφάλειας ευρωπαϊκών προτύπων.

Όσον αφορά την εποπτεία της συμμόρφωσης της αποτελεσματικότητας των πολιτικών και τεχνικών μέτρων ασφαλείας, οι αρμόδιες αρχές έχουν τη δικαιοδοσία να διενεργούν στις βασικές οντότητες ex-ante εποπτικούς ελέγχους. Μπορούν, μάλιστα, με αιτιολογημένα αιτήματα να ζητήσουν πληροφορίες, πρόσβαση σε δεδομένα και αποδεικτικά στοιχεία. Ακόμη έχουν τη δυνατότητα επιβολής μέτρων συμμόρφωσης και κυρώσεων, όπως, μεταξύ άλλων, αναστολή πιστοποίησης ή παύση φυσικών προσώπων εκ των διευθυντικών τους καθηκόντων ως αποτέλεσμα της ευθύνης τους για την έλλειψη συμμόρφωση έως ότου επέλθει η αποκατάστασή της (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Επισημαίνεται, όμως, ότι κάθε απόφαση θα εξετάζεται ανά περίπτωση. Παρά το γεγονός, ότι σε επίπεδο λήψης μέτρων συμμόρφωσης και κυρώσεων ισχύουν τα ίδια για τις δύο κατηγορίες οντοτήτων, οι σημαντικές υποβάλλονται μόνο σε εκ των υστέρων λήψη εποπτικών μέτρων (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

Σύμφωνα με τη νέα οδηγίας, τα κ-μ μπορούν να επιβάλλουν διοικητικά πρόστιμα του ύψους των € 10.000.000 ή έως το 2% του συνολικού παγκοσμίου ετήσιου κύκλου

εργασιών της μη συμμορφούμενης επιχείρησης που ανήκει στις βασικές οντότητες και πρόστιμα του ύψους των €7.000.000 ή έως 1,4% του συνολικού παγκοσμίου ετήσιου κύκλου εργασιών στις μη συμμορφούμενες σημαντικές οντότητες, ανάλογα με το ποιο ποσό είναι μεγαλύτερο (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022), θυμίζοντας τα πολύ υψηλά πρόστιμα του Γενικού Κανονισμού για την Προστασία Δεδομένων.

Τελευταίο σημείο παρατήρησης επί της οδηγίας αποτελεί η ενίσχυση της θέσης του ENISA μέσω της προσθήκης νέων τομέων δράσης. Στον μέχρι πρότινος προδραστικό του ρόλο, συμπεριλήφθηκαν η δημιουργία και διατήρηση του ευρωπαϊκού μητρώου τρωτών σημείων, η παροχή γραμματειακής βοήθειας στο νεοσυσταθέν EU CyCLoNe,[20] η έκδοση της διετούς έκθεσης που εξετάζει την κατάσταση της κυβερνοασφάλειας συλλογικά στην Ευρώπη καθώς επίσης, όποτε χρειάζεται καταρτίζει τις κατευθυντήριες γραμμές των προτεινόμενων συστημάτων τυποποίησης/ πιστοποίησης. Προστίθεται ακόμη η διοργάνωση και παροχή βοήθειας στις αξιολογήσεις των ομοτίμων,[21] η διατήρηση και μελέτη των δεδομένων που παρέχουν τα ενιαία κέντρα επαφής και εν συνεχεία έκδοση εκθέσεων με τεχνική καθοδήγηση, καθώς και η τήρηση καταλόγου των οντοτήτων που παρέχουν διασυνοριακές υπηρεσίες στην Ένωση (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Τέλος, συμμετέχει στη διενέργεια εκτιμήσεων αντικτύπου των εφοδιαστικών αλυσίδων ΤΠΕ,

[20] Η NIS 2 δημιουργεί μια νέα ευρωπαϊκή δομή, το δίκτυο οργανώσεων διασύνδεσης για τις κρίσης μεγάλης κλίμακας στον κυβερνοχώρο (EU CyCLONe). Αποτελείται από εκπροσώπους των εθνικών CERT και τον ENISA με αρμοδιότητα τη διαχείριση, σε επιχειρησιακό επίπεδο, μεγάλης κλίμακας περιστατικών και κρίσεων καθώς και τη διασφάλιση της ανταλλαγής των απαραίτητων γι' αυτές πληροφοριών μεταξύ των κρατών-μελών. Καθήκοντα της είναι ενίσχυση της επιχειρησιακής ετοιμότητας, δημιουργία κοινής οπτικής επί των καταστάσεων (situational awareness), συντονισμός και λήψη πολιτικών αποφάσεων κατά τη διαχείριση κρίσεων και συζήτηση επί των εθνικών σχεδίων διαχείρισης κρίσεων. Τέλος, ανά τακτά χρονικά διαστήματα υποβάλλει εκθέσεις μελέτης αντικτύπου των κυβερνοπεριστατικών για τις βασικές και σημαντικές οντότητες (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

[21] Οι αξιολογήσεις ομοτίμων, εμπειρογνωμόνων δηλαδή κυβερνοασφάλειας προερχόμενων από τα κ-μ, πραγματοποιούν, στη βάση της αρχής της καλής συνεργασίας, πραγματικές ή εικονικές αυτοψίες στις εγκαταστάσεις των κ-μ διαφορετικών από εκείνου της προέλευσης τους, για να αξιολογήσουν την αποτελεσματικότητα των πολιτικών κυβερνοασφάλειάς τους (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

λαμβάνοντας υπόψη τεχνικούς και μη παράγοντες κινδύνου (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022). Παρατηρείται, λοιπόν, μια προσπάθεια ανάδειξης του Οργανισμού ως τοποτηρητή του αγώνα θωράκισης του κυβερνοχώρου.

Η οδηγίας παρουσιάζει ένα πολύ φιλόδοξο σχέδιο μετριασμού των κενών της NIS. Με τη θέση της σε ισχύ τον Οκτώβριος του 2024, θα ενισχυθούν με κάθε τρόπο οι ελεγκτικές ικανότητες των κρατών επί των σημαντικών και βασικών οντοτήτων τους, θα επιβληθεί εξωεδαφική εποπτεία και γενικότερα θα ενδυναμωθούν οι ευρωπαϊκές θεσμικές δομές της κυβερνοασφάλειας.

5.1.3. Διπλωματική Εργαλειοθήκη

Το τρίτο κομμάτι του κεντρικού άξονα διαμόρφωσης της στρατηγικής της Ένωσης για την κυβερνοασφάλεια είναι η Διπλωματική Εργαλειοθήκη για την απόκριση σε κακόβουλες ενέργειες στο κυβερνοχώρο. Το θεσμικό πλαίσιο της οποίας είναι ένα συνονθύλευμα νομοθετικών κειμένων. Θεσπίστηκε με την Απόφαση του Ιούνιου 2017 του Συμβουλίου της ΕΕ και έκτοτε εμπλουτίστηκε με την έκδοση των κατευθυντήριων γραμμών του Οκτωβρίου 2017, της Απόφασης του Συμβουλίου για την Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (ΚΕΠΠΑ) 2019/797 και του Κανονισμού 2019/797 του Συμβουλίου.

Σύμφωνα με τα συμπεράσματα της Απόφασης της 7ης Ιουνίου, η δημιουργία ενός κοινού και αποδεκτού από όλα τα μέλη πλαισίου για τον μετριασμό και την αντιμετώπιση των κυβερνοπεριστατικών με διπλωματικά μέσα, προάγει τη σταθερότητα του διεθνούς συστήματος (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017a). Η ΕΕ αποδεχόμενη τις δεσμεύσεις των κρατών σε άλλους διεθνείς και περιφερειακούς οργανισμούς, προασπίζει την ειρηνική επίλυση των διαφορών στον κυβερνοχώρο κάνοντας χρήση κάθε είδους διπλωματικών μέσων που της παρέχουν η Συνθήκη για την Ευρωπαϊκή Ένωση καθώς και η Συνθήκη Λειτουργίας της (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017a).

Στο πλαίσιο αυτό, το Συμβούλιο δημοσίευσε τις κατευθυντήριες γραμμές πάνω στις οποίες θα στηριχθεί η Εργαλειοθήκη. Αυτή περιλαμβάνει διπλωματικά, πολιτικά και οικονομικά μέτρα πρόληψης και αντίδρασης σε κάθε μη φιλική ενέργεια που κάνει χρήση του κυβερνοχώρου, είτε προέρχεται από κρατικούς είτε μη κρατικούς δρώντες (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b). Τα μέτρα αυτά κατατάσσονται σε πέντε κατηγορίες και μπορούν να χρησιμοποιηθούν ανεξάρτητα ή και παράλληλα με άλλες στρατηγικές ενέργειες της ΕΕ (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b).

Η Διπλωματική Εργαλειοθήκη αρχικά υιοθετεί προληπτικά μέτρα αντιμετώπιση της εργαλειοποίησης του κυβερνοχώρου. Τέτοια μέτρα είναι η υιοθέτησης μέτρων οικοδόμησης εμπιστοσύνης, ώστε να καταπολεμηθεί η 'φυσική' ανασφάλεια που διαπνέει τις διακρατικές σχέσεις και να δημιουργηθούν σχέσεις εμπιστοσύνης μεταξύ των κρατών-μελών, η γνωστοποίηση των υιοθετηθέντων πολιτικών της Ένωσης για τον κυβερνοχώρο και στο εξωτερικό της περιβάλλον καθώς και των συνεπειών που η παράβαση τους επιφέρει, και τρίτον η προώθηση και υποστήριξη μέτρων ανάπτυξης των κυβερνοϊκανοτήτων τρίτων χωρών, εκτός των ευρωπαϊκών συνόρων (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b). Επόμενο στάδιο θωράκισης είναι τα μέτρα συνεργασίας με τα οποία επιδιώκεται η δημιουργία μόνιμων δίαυλων επικοινωνίας εντός του ουδέτερου θεσμικού περιβάλλοντος του Οργανισμού (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b). Τρίτη κατηγορία μέτρων είναι αυτά που επιδιώκουν τη διατήρηση της σταθερότητας μέσα από τη συνεχή ενημέρωση των κρατών για την κατάσταση στο κυβερνοχώρο, είτε αυτή εκφράζεται μέσω υψηλά ιστάμενων εκπροσώπων της ΕΕ, με δηλώσεις, παραδείγματος χάριν, της Ύπατης Εκπροσώπου που εκφράζουν ανησυχίες για τον τομέα και νέες μεθόδους κυβερνοεπιθέσεων, είτε μέσω διάφορων επιτροπών και θεσμικών οργάνων, ή και μέσω θεματικών διαλόγων σε άλλα πολυμερή όργανα και διεθνείς οργανισμούς (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b).

Η Εργαλειοθήκη, όμως, θεσπίζει και δύο ακόμη κατηγορίες μέτρων, οι οποίες, λόγω του δεσμευτικού τους χαρακτήρα και των επιπτώσεων που παράγουν,

απαιτούν την προηγούμενη απόδοση ευθυνών για την ενεργοποίησή τους. Τα περιοριστικά μέτρα/ κυρώσεις απευθύνονται σε τρίτες χώρες, σε φυσικά και νομικά πρόσωπα.[22] Στοχεύουν στον τερματισμό της παράνομης πράξης και δεν έχουν τιμωρητικό χαρακτήρα˙ τέτοια μέτρα είναι η απαγόρευση εισόδου στην ΕΕ, το εμπάργκο όπλων και το πάγωμα καταθέσεων (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b, 2019a, 2019b). Η πέμπτη και τελευταία κατηγόρια αφορά μέτρα που μπορούν να ενεργοποιήσουν τη συλλογική βοήθεια και επομένως, αθροιστικά τη δύναμη των κρατών-μελών (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2017b).

Κάθε κράτος-μέλος που έχει δεχτεί κυβερνοεπίθεση, μπορεί, είτε να προβεί σε άσκηση μη-βίαιων και αναλογικών αντίμετρων προς το κράτος 'δράστη' ή το κράτος που εν γνώσει του επιτρέπει το έδαφος του να χρησιμοποιείται για τη διάπραξη παράνομων ενέργειων, είτε να κάνει χρήση μέτρων αυτοάμυνας, όπως θεσπίζεται και από τα ΗΕ, ώστε να υπερασπιστεί την εθνική του κυριαρχία. Στο πλαίσιο, όμως, της Διπλωματικής Εργαλειοθήκης, παρέχεται ένα επιπλέον πλεονέκτημα στα κράτη-μέλη, η συλλογική αυτοάμυνα. Με αυτόν τον τρόπο, η ΕΕ εν μέρει 'ανεξαρτητοποιείται' από τον παραδοσιακό στρατηγικό της εταίρο σε θέματα στρατιωτικής συνδρομής, το ΝΑΤΟ. Αποκτά ελευθερία 'λόγου' και δράσης και σε περιπτώσεις όπου η συλλογική βοήθεια θα μπλοκαριζόταν από κράτη-μέλη που δεν συμμερίζονται τις ίδιες απόψεις και ιδεώδη στην άσκηση της εξωτερικής τους πολιτικής.

[22] Με την Απόφαση 2019/797 του Συμβουλίου και τον Κανονισμός 2019/796 του Συμβουλίου, η ΕΕ παρέθεσε μια λίστα από έξι είδη κυβερνοεπιθέσεων που μπορούν να οδηγήσουν στην επιβολή κυρώσεων, όπως επιθέσεις εναντίον κρίσιμων υποδομών, υπηρεσιών απαραίτητων για τη διατήρηση βασικών κοινωνικών και οικονομικών δραστηριοτήτων, σημαντικών κρατικών λειτουργιών, όπως η άμυνα και οι εκλογικές διαδικασίες, (εναντίον) της αποθήκευσης και επεξεργασίας διαβαθμισμένου υλικού, των εθνικών ομάδων CERT, της ίδιας της ΕΕ, των αντιπροσωπειών της σε τρίτες χώρες ή διεθνείς οργανισμούς, ακόμα και εναντίον των αποστολών και επιχειρήσεων που ενεργούν υπό την αιγίδα της ΚΕΠΠΑ (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2019a, 2019b; Pawlak & Biersteker, 2019).

Επομένως, είτε με την επίκληση του άρθρου 51 του Χάρτη των ΗΕ, είτε του άρθρου 42 (7) της ΣΕΕ[23], οποιοδήποτε κράτος-μέλος του οποίου τα δικαιώματα καταστρατηγούνται δύναται να ζητήσει την συνδρομή των υπολοίπων. Σύμφωνα, λοιπόν, με τη 'ρήτρα αμοιβαίας συνδρομής', εάν κράτος-μέλος δεχτεί (ένοπλη) επίθεση στο έδαφος του, μπορεί να ζητήσει την αρωγή των υπολοίπων μελών προς υπεράσπιση της κρατικής του κυριαρχίας. Η ζητούμενη βοήθεια απευθύνεται κατευθείαν στις κυβερνήσεις των κρατών-μελών, ως ανεξάρτητες δηλαδή κρατικές οντότητες που μοιράζονται τις ίδιες αρχές, αξίες και συμφέροντα, παρακάμπτοντας την γραφειοκρατία των Βρυξελλών (άρθρο 222 της ΣΛΕΕ[24]) (Κοππά, 2017, σ.82-84). Η παρεχόμενη, μάλιστα, βοήθεια δεν είναι απαραίτητα στρατιωτικού χαρακτήρα και μπορεί να χρησιμοποιηθεί από το πληγέν κράτος σε όλα τα θέατρα επιχειρήσεων στα οποία θεωρεί ότι χρίζει βοήθειας (Κοππά, 2017, σ.82-84). Σε αντίθεση, επομένως, με την ρήτρα αλληλεγγύης, ενός ακόμη εργαλείου στα χέρια της συλλογικής άμυνας της Ευρώπης, η συνδρομή των κρατών δεν γίνεται αυτόματα και με τη χρήση του κεντρικού ευρωπαϊκού διοικητικού μηχανισμού, αλλά απαιτείται, πρώτον, το προηγούμενο κάλεσμα για βοήθεια, και δεύτερον, η επιθυμία των υπολοίπων κυβερνήσεων για ανάληψη δράσης. Το σημαντικό, όμως, είναι, ότι παρέχεται ένα επιπλέον εργαλείο διασφάλισης της ακεραιότητας των κρατών-μελών και διατήρησης ενός υψηλού επιπέδου (κυβερνό)ασφάλειας, ώστε να διατηρηθεί η αξιοπιστία της ΕΕ, τόσο εσωτερικά όσο και ως δρώντας του διεθνούς συστήματος.

[23] Άρθρο 42 (7) της Συνθήκης για την Ευρωπαϊκής Ένωσης ή Ρήτρα Αμοιβαίας Συνδρομής: *"If a member is a victim of armed aggression on it's territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States."* (Ευρωπαϊκή Ένωση, 2008).

[24] Άρθρο 222 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης ή Ρήτρα Αλληλεγγύης: *"Η Ένωση και τα κράτη μέλη της ενεργούν από κοινού, με πνεύμα αλληλεγγύης, εάν ένα κράτος μέλος δεχτεί τρομοκρατική επίθεση ή πληγεί από φυσική καταστροφή ή ανθρωπογενή καταστροφή. Η Ένωση κινητοποιεί όλα τα μέσα που έχει στη διάθεσή της, συμπεριλαμβανομένων των στρατιωτικών μέσων που θέτουν στη διάθεσή της τα κράτη μέλη […]"* (Ευρωπαϊκή Ένωση, 2008).

5.1.4. Μελλοντικές πρωτοβουλίες της ΕΕ

Η ΕΕ προσεχώς θα εμπλουτίσει το υπάρχον κανονιστικό της πλαίσιο με δύο νέους κανονισμούς που προτάθηκαν από την Ευρωπαϊκή Επιτροπή, την πρόταση κανονισμού «Πράξη για την ανθεκτικότητα στον κυβερνοχώρο» (Cyber Resilience Act) και την πρόταση κανονισμού «Πράξη αλληλεγγύης στον κυβερνοχώρο» (Cyber Solidarity Act). Οι δύο νέες κανονιστικές προτάσεις θα συμπληρώσουν την Οδηγία NIS II, την Πράξη για την Κυβερνοασφάλεια καθώς και την Διπλωματική Εργαλειοθήκη αποσκοπώντας στην ενίσχυση της ασφάλειας των κρατών-μελών.

Η Πράξη για την ανθεκτικότητα στον κυβερνοχώρο (ή ο «*Κανονισμός σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020*») προτάθηκε το 2020 στο πλαίσιο της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, ώστε να συμπληρώσει την NIS II (European Commission, 2022b). Ο προτεινόμενος κανονισμός, που πλέον βρίσκεται σε διαδικασία τριλόγου, θέτει υποχρεωτικές απαιτήσεις ασφάλειας για τα προϊόντα με ψηφιακά στοιχεία.[25] Οι κατασκευαστές, οι εξουσιοδοτημένοι αντιπρόσωποι, οι εισαγωγείς και οι διανομείς (οικονομικοί φορείς) αναλαμβάνουν την ευθύνη κατασκευής και διατήρησης της ασφάλειας όλων των προϊόντων υλισμικού και λογισμικού που φέρουν ψηφιακά στοιχεία καθ' όλο τον κύκλο ζωής τους (European Commission, 2022a). Επιπλέον, είναι υπεύθυνοι για την αντιμετώπιση και γνωστοποίηση τρωτών σημείων, ενώ η μη συμμόρφωση με τις τεχνικές και τις διαδικαστικές απαιτήσεις και υποχρεώσεις που θέτει ο κανονισμός επισύρει διοικητικά πρόστιμα έως και το ύψος των 15.000.000 ευρώ (European Commission, 2022a).[26] Στόχος, επομένως, του

[25] Η πρόταση κανονισμού εφαρμόζεται σε όλα τα προϊόντα με ψηφιακά στοιχεία, δηλαδή σε κάθε προϊόν που συνδέεται άμεσα ή έμμεσα με άλλες συσκευές ή δίκτυα. Από το πεδίο εφαρμογής της εξαιρούνται τα λογισμικά ανοικτού κώδικα ή οι υπηρεσίες που καλύπτονται ήδη από τους υφιστάμενους κανόνες. Πιο συγκεκριμένα, οι υπηρεσίες που αφορούν τις ιατρικές συσκευές (κανονισμοί (ΕΕ) 2017/745 & 2017/746), την πολιτική αεροπορία (κανονισμός (ΕΕ) 2018/1139), τα μηχανοκίνητα και ρυμουλκούμενα οχήματα (κανονισμός (ΕΕ) 2019/2144), καθώς και τα προϊόντα που είναι σχεδιασμένα να εξυπηρετούν στρατιωτικές ανάγκες και τον τομέας της εθνικής ασφάλειας (European Commission, 2022a).

[26] Σύμφωνα με την πρόταση Κανονισμού, η μη συμμόρφωση με τις ουσιώδεις προδιαγραφές του κανονισμού συνεπάγεται διοικητικά πρόστιμα έως 15.000.000 ευρώ ή,

επικείμενου κανονισμού είναι δημιουργία συνθηκών ανάπτυξης ασφαλών προϊόντων με ψηφιακά στοιχεία, καθώς και η δημιουργία ενός περιβάλλοντος όπου οι χρήστες των προϊόντων αυτών θα επιζητούν την εκ του σχεδιασμού ασφάλειά τους, ενισχύοντας με αυτόν τον τρόπο το αίσθημα ασφάλειας δικαίου εντός της Ένωσης και περιορίζοντας τον κατακερματισμό των κατασκευαστικών απαιτήσεων στην εσωτερική αγορά.

Η δεύτερη πρόταση κανονισμού, Πράξη αλληλεγγύης στον κυβερνοχώρο (ή ο *«Κανονισμός σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας»)* προτάθηκε από την Επιτροπή τον Απρίλιο του 2023 στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», ώστε να βελτιστοποιηθούν οι διαδικασίες ανίχνευσης, προστασίας και αντιμετώπισης των κυβερνοπεριστατικών πανευρωπαϊκά (European Commission, 2023b). Ο κανονισμός θα αξιοποιήσει τις δομές της NIS II, θα προσθέσει νέες αρμοδιότητες στο ENISA και θα δρα συμπληρωματικά με τις πολιτικές της ΚΕΠΠΑ.

Πιο αναλυτικά, εγκαθιδρύει την ευρωπαϊκή υποδομή κέντρων επιχειρήσεων ασφάλειας, γνωστή ως «ευρωπαϊκή κυβερνοασπίδα», η οποία θα αποτελείται από εθνικά και διασυνοριακά κέντρα επιχειρήσεων ασφαλείας (European Commission, 2023a). Τα κέντρα αυτά θα είναι διασυνδεμένα ανταλλάσσοντας και αποθηκεύοντας πληροφορίες με στόχο την έγκαιρη αντίληψη, προετοιμασία και αντιμετώπιση κυβερνοπεριστατικών στον ευρωπαϊκό κυβερνοχώρο (European Commission, 2023a). Θεσπίζει, ακόμη, τον μηχανισμό έκτακτης ανάγκης για τη βελτίωση της ανθεκτικότητας στης ΕΕ από απειλές με δράσεις ετοιμότητας, αντιμετώπισης και αμοιβαίας συνδρομής (European Commission, 2023a). Τέλος,

---

αν πρόκειται για επιχείρηση, έως το 2,5% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της. Αν η μη συμμόρφωση αφορά δευτερεύουσες υποχρεώσεις του οικονομικού φορέα, τότε το πρόστιμο ενδέχεται να φτάσει το ποσό των 10.000.000 ευρώ ή το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης, ή τέλος, αν η κύρωση αφορά παροχή ελλιπών ή παραπλανητικών στοιχείων προς τις αρμόδιες εποπτικές αρχές, το πρόστιμο μπορεί να προσεγγίσει το ποσό των 5.000.000 ευρώ ή το 1% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης (European Commission, 2022a).

συστήνει τον μηχανισμό εξέτασης περιστατικών προσθέτοντας μια νέα αρμοδιότητα στον ENISA, ο οποίος, κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, εκπονεί εκθέσεις για τις επιπτώσεις σημαντικών κυβερνοπεριστατικών μετά από την μελέτη και την αξιολόγηση τυχόν τρωτών σημείων και ενδεχόμενων απειλών (European Commission, 2023a). Οι μηχανισμοί που εγκαθιδρύει επομένως ο προτεινόμενος κανονισμός συνεπικουρούν στην δημιουργία μια αμυντικής ζώνης στον κυβερνοχώρο της Ευρώπης.

Η ΕΕ, συνοψίζοντας, παρουσιάζει ένα ολοκληρωμένο σύστημα διαχείρισης του κυβερνοχώρου για τα κράτη-μέλη της. Με την ίδρυση του ENISA έθεσε υπό την αιγίδα ενός θεσμικού οργάνου το μεγαλύτερο μέρος των δράσεων που αφορούν τον κυβερνοχώρο προσπαθώντας να βελτιστοποιήσει τις οργανωτικές διαδικασίες μεταξύ των κρατών και της ίδιας. Επιπλέον, με την καθιέρωση της πιστοποίησης έθεσε τις ελάχιστες απαιτήσεις για τη λειτουργία της ελεύθερης αγοράς, καθώς και με την οδηγίες NIS και NIS II για την εσωτερική οργανωτική και διαδικαστική συμμόρφωση των βασικών και των σημαντικών οντοτήτων των μελών της, προσπαθώντας να περιχαρακώσει τα όποια κενά στην ασφάλεια τους μέσα από την ευαισθητοποίηση των επιχειρήσεων και τον συνεχή έλεγχο. Πέρα όμως από τη θέσπιση ενός 'ασφαλούς' εσωτερικού περιβάλλοντος, που διαθέτει όλα τα μέτρα υγιεινής που αντισταθμίζουν τις εξωτερικές απειλές, η ΕΕ με την Εργαλειοθήκη, δημιουργεί ένα πλαίσιο κυρωτικών ενεργειών απέναντι σε οποιαδήποτε κακόβουλο περιστατικό απειλεί την ασφάλεια των κρατών-μελών της, αλλά και της ίδιας. Διαβαθμίζοντας τα μέτρα δράσης της ανάλογα με το είδος της απειλής, προσπαθεί να διευθετήσει τις κρατικές διαφορές μην υπερβαίνοντας τους κανόνες του διεθνούς δικαίου αλλά και προστατεύοντας παράλληλα τα δικαιώματα της.

ΚΕΦΑΛΑΙΟ 6:
ΕΠΙΛΟΓΟΣ

Το διεθνές σύστημα, όπως έχει ήδη γίνει εμφανές από την ως άνω ανάλυση, αποτελεί ένα συνεχώς μεταβαλλόμενο περιβάλλον. Αν και αποτελείται από τα κράτη, τα οποία, λόγω της ομοειδούς σύστασή τους, του προσδίδουν μια φαινομενική δομική σταθερότητα, στην πραγματικότητα αποτελούν το κλειδί της αλλαγής. Τα κράτη στην προσπάθεια τους να προωθήσουν τα συμφέροντα τους με τον πιο αποδοτικό γι' αυτά τρόπο, επιδίδονται σε έναν ατέρμονο αγώνα απόκτησης ισχύος. Η ανάγκη για ισχύ είναι εξέχουσας σημασίας, καθώς με αυτή κατ' αρχήν μπορούν να εξασφαλίσουν την ύπαρξη τους, ως αυθύπαρκτου παίκτη τους διεθνούς συστήματος, και στη συνέχεια να διεκδικήσουν μια καλύτερη θέση στη σκακιέρα των διεθνών διαπραγματεύσεων. Η ισχύς είναι, λοιπόν, προαπαιτούμενο της κρατικής επιβίωσης και εν συνεχεία της κρατική ασφάλειας και ευημερίας. Όλο το σύστημα στηρίζεται στην προσπάθεια απόκτησης της επιζητούμενης εκ των κρατών ισχύος και την μετέπειτα ισορρόπηση της.

Οι ισορροπίες, όμως, μεταξύ των κρατών μεταβάλλονται συνεχώς, καθώς αναδεικνύονται νέοι 'επαναστατικοί' τρόποι άσκησης πολιτικής πίεσης. Η ραγδαία πρόοδος της τεχνολογίας και των επιστημών είναι αυτή που μεταβάλλει κάθε φορά του κανόνες του παιχνιδιού και γέρνει στην πλάστιγγα προς τη μια ή την άλλη χώρα. Ο χρόνος υιοθέτησης των τεχνολογικών καινοτομιών από κάθε κράτος είναι κρίσιμης σημασίας για τη μετέπειτα θέση του στο διεθνές περιβάλλον. Όσο πιο γρήγορα αφομοιώνει τις αλλαγές, τόσο αναβαθμίζει τη θέση του μεταξύ των υπολοίπων κρατών.

Ο κυβερνοχώρος, αποκύημα της τεχνολογικής προόδου στον τομέα των επικοινωνιών και της πληροφορικής, αποτελεί το νέο και πολλά υποσχόμενο πεδίο προώθησης πολιτικών επιδιώξεων. Η δράση, τόσο των κρατικών, όσο και των μην κρατικών δρώντων, στο κυβερνοπεριβάλλον έχει γνωρίσει πρωτόγνωρους ρυθμούς. Έκαστος δρών κάνει χρήση του αξιοποιώντας τα μοναδικού χαρακτήρα στοιχεία του. Ο χωρίς σύνορα χαρακτήρας του, η αδυναμία

απόδοσης ευθυνών, η ταχύτητα, οι επιθετικές του δυνατότητες καθώς και το χαμηλό κόστος διεξαγωγή επιχειρήσεων, στρατιωτικού ή μη χαρακτήρα, μέσω αυτού ή και με τη χρήση αυτού, αποτελούν ένα πλεονέκτημα για όποιον είναι τεχνολογικά εξελιγμένος και ικανός να προχωρήσει στη χρήση τους. Όλες οι σύγχρονες διακρατικές διαμάχες έχουν αξιοποιήσει το νέο αυτό πεδίο για την εκπλήρωση των κρατικών σκοπιμοτήτων τους. Άλλοτε οι διαφορές λύνονται αποκλειστικά σε αυτόν, άλλοτε με τη βοήθεια αυτού, πάντοτε, όμως, η χρήση του είναι κομβικής σημασίας για την αντιπαράθεση. Στην περίπτωση της Εσθονίας η δράση στον κυβερνοχώρο απέδειξε πως ήταν επαρκής και δεν επιζητούσε την χρήση συμβατικών στρατιωτικών μέσων για την επίτευξη του ρωσικού πολιτικού αντικειμενικού σκοπού, σε αντίθεση με την Ουκρανία, όπου ο ρόλος του ήταν και παραμένει επικουρικός των μαχών. Οι κινεζικές δράσεις και η σκοπιμότητά τους, από την άλλη πλευρά, δεν έχουν πλήρως αποκρυπτογραφηθεί, καθώς τα αποτελέσματα τους δεν είναι άμεσα αντιληπτά και η επίδραση τους στις σινοαμερικανικές σχέσεις δεν είναι ακόμη εμφανής. Η διατάραξη τους, όπως συνέβη με την εργαλειοποίηση των ευπαθειών του Microsoft Exchange Server, είναι η κορυφή του παγόβουνου σε μια προσπάθεια μεταβολής των διεθνών συνθηκών προς όφελος της Κίνας, η οποία, ως μια από τις πλέον ισχυρές χώρες παγκοσμίως, επιζητεί την συμπερίληψη και της δικής της κουλτούρας και αξιών στην παγκόσμια πολιτική σκηνή. Όλα αυτά τα στοιχεία επιβεβαιώνουν, ότι ο κυβερνοχώρος και τα εργαλεία του θα απασχολήσουν στο έπακρο τις σχέσεις των κρατών τις επόμενες δεκαετίες.

Ο υβριδικός αυτός τρόπος αλλαγής των συνθηκών και προώθησης των πολιτικών ιδεών και σκοπιμοτήτων αντίπαλων πολιτικών δεόντων επιβάλλει την αναθεώρηση των έως τώρα κανόνων και αρχών. Η αλλαγή, βέβαια, δεν χρειάζεται να είναι ριζική με αναδιαμόρφωση όλου το νομικού πλαισίου που προστάτευε και προστατεύει τη διεθνή κοινότητα. Για να τιθασευτεί και να τεθεί εντός κανόνων ο κυβερνοχώρος, αρκούν ορισμένες σταδιακές αλλά ταχείες τροποποιήσεις, όπου είναι εφικτό, των μέχρι τώρα σημαντικών συμβατικών κειμένων, η δημιουργία νέων και πιο λεπτομερών δεσμευτικών κειμένων, καθώς και η ερμηνεία των ήδη υπαρχόντων, με εξέχον παράδειγμα το Tallin Manual. Η αλλαγή των κανόνων σε

παγκόσμιο επίπεδο δεν είναι μια ρηξικέλευθη πρακτική των ημερών μας. Πάντοτε οι τεχνολογικές εξελίξεις επέφεραν τέτοιου είδους αλλαγές, συνήθως προς όφελος των κρατών και της κρατικής κυριαρχίας. Κάθε φόρα επεκτείνεται η ζώνη κρατικής δικαιοδοσίας και επιρροής, όπως συνέβη και με τον κυβερνοχώρο. Κάποτε η εφεύρεση του κανονιού είχε ως αποτέλεσμα την επαύξηση της ασφάλειας για τα κράτη, καθώς μπορούσαν να προστατεύονται από τους εχθρούς εξ αποστάσεως, χωρίς δηλαδή να δώσουν τα στρατεύματα τους μάχη σώμα με σώμα, περιορίζοντας με αυτόν το τρόπο τις απώλειες σε ανθρώπινο δυναμικό. Η ίδια αυτή εφεύρεση ήταν, όμως, που επέκτεινε την κρατική κυριαρχία και δημιούργησε νέα δικαιώματα για τα κράτη˙ δικαιώματα που σήμερα θεωρούμαι αναπόσπαστο κομμάτι της κρατικής υπόστασης. Η δυνατότητα του κανονιού να πλήττει μακρινούς στόχους μέσα από ένα ασφαλές περιβάλλον ήταν η αιτία δημιουργίας διάφορων ζωνών κυριαρχίας και κυριαρχικών δικαιωμάτων, όπως για παράδειγμα η αιγιαλίτιδα ζώνη στη θάλασσα. Αν αναλογιστεί κανείς, ότι μια νέα τεχνολογία -για την εποχή της- ήταν η αιτία δημιουργίας ολόκληρου του κλάδου του δικαίου της θάλασσας, μπορεί να κατανοήσει το μέγεθος των μεταβολών που δύναται να προκαλέσει μια επαναστατική, για τα δεδομένα της εποχής της, τεχνολογία. Ο κυβερνοχώρος έχει ήδη αναγνωριστεί ως πέμπτο πεδίο πολέμου. Ισχυρές χώρες με επιρροή σε μεγαλύτερη, των γεωγραφικών συνόρων τους, εμβέλεια, τον έχουν συμπεριλάβει στα στρατιωτικά τους δόγματα και κάνουν χρήση των εργαλείων του στην επίλυση των διαφορών τους. Στα πλαίσια διάφορων διεθνών και περιφερειακών οργανισμών αποτελεί ένα από τα σημαντικότερα θέματα της ατζέντας τους. Τα ΗΕ καταβάλουν σταθερή προσπάθεια διαμόρφωσης ενός πλαισίου δράσης τον κρατών μέσα στο χωρίς σύνορα και άυλο περιβάλλον του κυβερνοχώρου επισημαίνοντας τις μέχρι τώρα σταθερές αξίες της χρηστής συμπεριφοράς για την ειρηνική συνύπαρξη των κρατικών οντοτήτων και την επίλυση των διαφορών, δημιουργώντας νέες διεθνείς νόρμες, και προωθώντας, στο μέτρο του δυνατού, την διακρατική συνεργασία, αλλά και την συνεργασία με τρίτα μέρη (ιδιωτικός τομέας, ακαδημαϊκός χώρος και κοινωνία των πολιτών) στο ασφαλές περιβάλλον τόσο του ΟΗΕ όσο και άλλων περιφερειακών οργανισμών. Το ΝΑΤΟ και η ΕΕ, μάλιστα, ως πιο συνεκτικοί

περιφερειακοί οργανισμοί, έχουν θεσπίσει την επιβολή κυρώσεων εναντίον κρατών και ιδιωτών -μόνο η ΕΕ- για κάθε κακόβουλο περιστατικό στον κυβερνοχώρο που πλήττει τα κράτη-μέλη τους, υιοθετώντας ακόμη και την μέγιστη των 'ποινών', την ενεργοποίηση των μηχανισμών συλλογικής αυτοάμυνας (άρθρο 5 της Συνθήκης της Ουάσιγκτον & άρθρο 42(7) της ΣΕΕ και 222 της ΣΛΕΕ) ως απόρροια του άρθρου 51 του Χάρτη των ΗΕ.

Δεν είναι, επομένως, άδικο να θεωρηθεί πως ένα νέο δικαίωμα των κρατών εμφανίζεται στον ορίζοντα, το οποίο θα αρθρωθεί με περισσότερη λεπτομέρεια με το πέρασμα των χρόνων. Αλλά ακόμα και αν το δικαίωμα στην κυβερνοασφάλεια δεν αποτελεί κάτι νέο, αλλά απλά μια μετεξέλιξη άλλων κλασικών δικαιωμάτων, καλύπτοντας τα θεσμικά κενά που δεν θα μπορούσαν να προβλέψουν οι συντάκτες τους, δεν μπορεί να παραβλεφθεί το γεγονός της ανάδειξης ενός νέου πεδίου δράσης και προώθησης πολιτικών σκοπιμοτήτων με ό,τι θεσμικές αλλαγές και δεσμεύσεις αυτό συνεπάγεται. Καταληκτικά, ό,τι και από τα δύο και αν συμβαίνει, ο κυβερνοχώρος φαίνεται πως ήρθε για να απασχολήσει τη διεθνή κοινότητα και να αλλάξει συλλήβδην τον τρόπο δράσης και αντίδρασης των διεθνών παικτών, είτε πρόκειται για κρατικούς είτε μη κρατικούς δρώντες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αρβανιτόπουλος, Κ., & Ήφαιστος, Π. (2003). *Ευρωατλαντικές Σχέσεις*. Εκδόσεις ΠΟΙΟΤΗΤΑ.

ΓΕΕΘΑ. (2015, Νοέμβριος 4). *Συμμετοχή των ΕΔ στο Κέντρο Αριστείας του ΝΑΤΟ για την Κυβερνοάμυνα στην Εσθονία*. https://geetha.mil.gr/6321-symmetochh-twn-ed-sto-kentro-aristeias-toy-nato-gia-thn-kybernoamyna-sthn-esthonia/

Γκίνης, Κ. (2017). Ο Κονδύλης και η Νίκη σε Έναν Ελληνοτουρκικό Πόλεμο. *ΣΤΡΑΤΗΓΙΚΟΝ*, *1*, 7–25.

Ευρωπαϊκή Ένωση. (2008). *Συνθήκη για την Ευρωπαϊκή Ένωση & Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης (2008/ C 115/01)*.

Ευρωπαϊκό Ελεγκτικό Συνέδριο. (2019). *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια*. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf

Ευρωπαϊκό Κοινοβούλιο. (2021). *Συνεργασία ΕΕ-ΝΑΤΟ στο πλαίσιο των διατλαντικών σχέσεων Ψήφισματου Ευρωπαϊκού Κοινοβουλίουτης 7ης Ιουλίου 2021 σχετικά με τη συνεργασίαΕΕ-ΝΑΤΟ στο πλαίσιο των διατλαντικών σχέσεων (2020/2257(INI))*.

Ευρωπαϊκό Κοινοβούλιο, & Συμβούλιο της Ευρωπαϊκής Ένωσης. (2016). *ΟΔΗΓΙΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*.

Ευρωπαϊκό Κοινοβούλιο, & Συμβούλιο της Ευρωπαϊκής Ένωσης. (2019). *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/881 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξηγιατηνκυβερνοασφάλεια)*.

Ευρωπαϊκό Κοινοβούλιο, & Συμβούλιο της Ευρωπαϊκής Ένωσης. (2022). *ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 14ης Δεκεμβρίου 2022σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)*.

Ήφαιστος, Π. (2008). *ΚΟΣΜΟΘΕΩΡΗΤΙΚΗ ΕΤΕΡΟΤΗΤΑ ΚΑΙ ΑΞΙΩΣΕΙΣ ΠΟΛΙΤΙΚΗΣ ΚΥΡΙΑΡΧΙΑΣ* (Ζ. Κωτούλα, Επιμ.). Εκδόσεις Ποιότητα.

Θεοφίλης, Α. (2018). Οι κυβερνοεπιθέσεις ως Μέσο Στρατηγικής. *ΣΤΡΑΤΗΓΙΚΟΝ*, *2*, 119–132.

Καρανικολός, Κ. (2021). Ο Υβριδικός Πόλεμος στο Θαλάσσιο Πεδίο. Στο ΕΛ.Ι.Σ.ΜΕ. (Επιμ.), *ΥΒΡΙΔΙΚΟΙ ΠΟΛΕΜΟΙ* (1η έκδ., σσ. 275–334). Εκδόσεις Ινφογνώμων.

Κατσούλας, Σ. (2017). Η Έννοια της Στρατηγικής Κουλτούρας. *ΣΤΡΑΤΗΓΙΚΟΝ*, *1*, 117–142.

Κολιόπουλος, Κ. (2008). *Η ΣΤΡΑΤΗΓΙΚΗ ΣΚΕΨΗ ΑΠΟ ΤΗΝ ΑΡΧΑΙΟΤΗΤΑ ΕΩΣ ΣΗΜΕΡΑ*. Εκδόσεις ΠΟΙΟΤΗΤΑ.

Κολιόπουλος, Κ. (2011). *Η ΥΨΗΛΗ ΣΤΡΑΤΗΓΙΚΗ ΤΗΣ ΑΡΧΑΙΑΣ ΣΠΑΡΤΗΣ* (6ο έκδ.). Εκδόσεις ΠΟΙΟΤΗΤΑ.

Κονδύλης, Π. (1999). *ΘΕΩΡΙΑ ΤΟΥ ΠΟΛΕΜΟΥ* (Γ). Εκδόσεις Θεμέλιο.

Κοππά, Μ. (2017). *Η Κοινή Πολιτική Άμυνας και Ασφάλειας: Η ιστορία, οι θεσμοί, οι στρατηγικές*. Εκδόσεις Πατάκη.

Κοσμόπουλος, Α. (2021). Πρόληψη και Αντιμετώπιση Υβριδικών Απειλών: Ενοποιημένη Ανθεκτικότητα και Ολιστική Ανοσία. Στο ΕΛ.Ι.Σ.ΜΕ. (Επιμ.), *ΥΒΡΙΔΙΚΟΙ ΠΟΛΕΜΟΙ* (1η έκδ., σσ. 351–366). Εκδόσεις Ινφογνώμων.

Μαυρόπουλος, Π. (2017). Αυτοκτονία Εμπρός στο Φόβο του Θανάτου: Παρεμποδιστική Χρήση Ισχύος Ως Πολιτική Επιλογή στο Σύγχρονο Διεθνές Περιβάλλον. *ΣΤΡΑΤΗΓΙΚΟΝ*, *1*, 27–54.

Μήτσιος, Β. (2021). Υβριδικός Πόλεμος: Η Αμφισβήτηση της Ορθόδοξης Ανάλυσης και των Προκαταλήψεων. Στο ΕΛ.Ι.Σ.ΜΕ. (Επιμ.), *ΥΒΡΙΔΙΚΟΙ ΠΟΛΕΜΟΙ* (1η έκδ., σσ. 59–92). Εκδόσεις Ινφογνώμων.

Μπαζίνης, Θ. (2021). Ο Υβριδικός Πόλεμος ως Όπλο του Αδυνάτου. Στο ΕΛ.Ι.Σ.ΜΕ. (Επιμ.), *ΥΒΡΙΔΙΚΟΙ ΠΟΛΕΜΟΙ* (1η έκδ., σσ. 247–274). Εκδόσεις Ινφογνώμων.

NATO. (1949). *Η Συνθήκη Του Βόρειου Ατλαντικού*. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=el

NATO. (2008). *Bucharest Summit Declaration*.

Οργανισμός Ηνωμένων Εθνών. (1945). *Χάρτης των Ηνωμένων Εθνών* [ΟΗΕ]. https://unric.org/el/%CF%87%CE%B1%CF%81%CF%84%CE%B7%CF%83-%CE%BF%CE%B7%CE%B5/

Παπασωτηρίου, Χ. (2011). *Βυζαντινή Υψηλή Στρατηγική* (7ο έκδ.). Εκδόσεις ΠΟΙΟΤΗΤΑ.

Πιπύρος, Κ., & Μήτρου, Λ. (2018). Κυβρνοεπίθεση ή Κυβερνοπόλεμος; *FORUM*, *2*.

ΣΟΥΝ ΤΣΟΥ. (2008). *Η ΤΕΧΝΗ ΤΟΥ ΠΟΛΕΜΟΥ* (Χ. Παπαβασιλείου & Έ. Καλλιφατίδου, Επιμ.). ΕΚΔΟΣΕΙΣ ΟΞΥ.

Συμβούλιο της Ευρωπαϊκής Ένωσης. (2017a). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')*.

Συμβούλιο της Ευρωπαϊκής Ένωσης. (2017b). *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*.

Συμβούλιο της Ευρωπαϊκής Ένωσης. (2019a). *ΑΠΟΦΑΣΗ (ΚΕΠΠΑ) 2019/797 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της*.

Συμβούλιο της Ευρωπαϊκής Ένωσης. (2019b). *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2019/796 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 17ης Μαΐου 2019 σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της*.

Συρίγος, Ά. (2014). Το κράτος. Στο Κ. Αντωνόπουλος & Κ. Μαγκλιβέρας (Επιμ.), *Το Δίκαιο της Διεθνούς Κοινωνίας* (2ο έκδ., σσ. 101–140). ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ.

Συρίγος, Ά. (2018). *Ελληνοτουρκικές Σχέσεις* (3ο έκδ.). Εκδόσεις Πατάκη.

Bachmann, S.-D., & Gunneriusson, H. (2015a). HYBRID WARS: THE 21st - CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY. *Scientia Militaria, South African Journal of Military Studies*, *43*(1), 77–98.

Bachmann, S.-D., & Gunneriusson, H. (2015b). HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY. *Scientia Militaria - South African Journal of Military Studies*, *43*(1). https://doi.org/10.5787/43-1-1110

BDI. (2022). *Towards an NIS 2 Directive that is implementable for Europe's industry Developing a holistic approach from the European Commission's, Euro-pean Parliament's and European Council's positions*. https://english.bdi.eu/publication/news/nis-2-co-legislators-proposals-for-trilogue-cybersecurity-it-data

Boot, M. (2008). *The Corps should look to its small-wars past*. http://www.afji.com/2006/03/1813950http://www.afji.com/2006/03/1813950

Brent, L. (2019, Φεβρουάριος 12). *NATO's role in cyberspace*.

Cassese, A. (2012). *Διεθνές Δίκαιο* (Φ. Παζαρτζή, Επιμ.). Εκδόσεις Gutenberg.

CCDCEO. (χ.χ.). *CCDCEO - Our mission & vision*. Ανακτήθηκε 14 Μάιος 2023, από https://ccdcoe.org/about-us/

CISA. (2022). *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a

Codagnone, C., Liva, G., & Rodriguez Las Heras Ballell, T. DE. (2022). *Identification and assessment of existing and draft EU legislation in the digital field*. http://www.europarl.europa.eu/supporting-analyses

Corbett, J. (2020). *Some Principles of Maritime Strategy*. GUTENBERG EBOOK. https://www.gutenberg.org/cache/epub/15076/pg15076-images.html

Council of the European Union. (2021). *China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory*.

Cyber Security in Estonia 2021. (2021). file:///C:/Users/L%CE%B5no%CE%BDo/Downloads/Cyber-Security-in-Estonia-2021%20(1).pdf

del Mar Negreiro Achiaga, M. (2023). *REVIEW OF THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATIONSYSTEMS - Q4 2020*. https://www.europarl.europa.eu/legislative-train/carriage/review-of-the-nis-directive/report?sid=6901

Digital Watch. (χ.χ.). *UN OEWG*. Digital Watch. Ανακτήθηκε 15 Μάιος 2023, από https://dig.watch/processes/un-gge

Digital Watch. (2016). *Cyber Defence Pledge*. https://dig.watch/resource/nato-cyber-defence-pledge

Dill, D. (χ.χ.). *The Boiled Frog Syndrome: or How You Can Behave Unethically Without Realizing It*.

DoD, D. of D. (2016). *Law of War Manual*.

Douhet, J. (χ.χ.). *The Command of the Air* (D. Budjenska, Επιμ.). Air University Press. Ανακτήθηκε 15 Μάιος 2023, από https://apps.dtic.mil/sti/pdfs/AD1122179.pdf

English Oxford Company. (χ.χ.). *Definition of Cyberwarfare in English*. Oxford University Press. Ανακτήθηκε 14 Μάιος 2023, από https://www.oxfordlearnersdictionaries.com/definition/english/cyberwarfare

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN (2013) 1 final*. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building – A Playbook*.

European Commission. (2020). *Proposal for directive on measures for high common level ofcybersecurity across the Union*. https://digital-strategy.ec.europa.eu/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

European Commission. (2022a). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 - COM(2022) 454 final2022/0272 (COD)*.

European Commission. (2022b, Σεπτέμβριος 15). *EU Cyber Resilience Act*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (2023a). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - COM(2023) 209 final2023/0109 (COD)*. https://www.ibm.com/reports/data-breach

European Commission. (2023b, Απρίλιος 18). *The EU Cyber Solidarity Act*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

FBI, & CISA. (2021). *Compromise of Microsoft Exchange Server*. https://www.cisa.gov/tlp/.

France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, Republic of Korea, Republic of Moldova, Republic of North Macedonia, UnitedKingdom, & EU. (2020). *The future of discussions on ICTs and cyberspace at the UN Summary of the Proposal: explore establishment of a Programme of Action for advancing responsible State behaviour in cyberspace with a view to ending the dual track discussions (GGE/OEWG) and establishing a permanent UN forum to consider the use of ICTs by States in the context of international security*. https://www.un.org/disarmament/convarms/salw/programme-of-action/

GGE. (2010). *General A/65/201 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

GGE. (2015). *General A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

GGE. (2021). *General A/76/135 Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* Summary*.

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Quarterly*, *4*(3), 102–135. https://doi.org/10.2307/26269789

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Source: Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.2307/26463926

Hoffman, F. (2007). Preparing for Hybrid Wars What will be the future Marine Corps capability. *Marine Corps Gazette*.

Hoffman, F. (2009). Hybrid Warefare and Challenges. *JFQ*, *52*.

Hybrid Warfare. (2009). http://www.gao.gov/.

International Court of Justice. (1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA)*.

Jackson, R., & Sørensen, G. (2006). *ΘΕΩΡΙΑ ΚΑΙ ΜΕΘΔΟΛΟΓΙΑ ΤΩΝ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ* (1η έκδ.). GUTENBERG.

Kant, I. (1893). *Perpetual Peace and other Essays on Politics, History and Morals* (T. Humphrey, Επιμ.). Hackett Publishing Company.

Kastelic, A. (2022). *Non-Escalatory Attribution of International Cyber Incidents*. www.unidir.org

Kennedy, P. (1990). *Η ΑΝΟΔΟΣ ΚΑΙ Η ΠΤΩΣΗ ΤΩΝ ΜΕΓΑΛΩΝ ΔΥΝΑΜΕΩΝ* (τ. 2). Εκδόσεις ΑΞΙΩΤΕΛΛΗΣ.

Kikk, Eneken., Kaska, Kadri., & Vihul, Liis. (2010). *International cyber incidents: legal considerations*. Cooperative Cyber Defence of Excellence (CCD COE).

Kononenko, V. (2021). *Improving the common level of c ybersecurity across the EU*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662606/EPRS_BRI(2021)662606_EN.pdf

Lasconjarias, G., & Larsen, J. A. (2015). *General Philip Breedlove Supreme Allied Commander Europe*.

Lella, I., Theocharidou, M., Tsekmezoglou, E., Svetozarov Naydenov, R., Ciobanu, C., Malatras, A., & European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022.* (Lella Ifigeneia, Tsekmezoglou Eleni, Svetozarov Naydenov Rossen, Ciobanu Cosmin, Malatras Apostolos, & Theocharidou Marianthi, Επιμ.).

Machiavelli, N. (2013). *Ο Ηγεμόνας*. Εκδόσεις Εκάτη.

Maigre, M. (2022). *Cyber threat actors: how to build resilience to counter them*.

Mattis, J., & Hoffman, F. (2005). Future Warfare: The Rise of Hybrid Wars. *U.S. NAVAL INSTITUTE*, *132*.

Microsoft. (2022a). *An overview of Russia's cyberattack activity in Ukraine*.

Microsoft. (2022b). *Microsoft Digital Defense Report 2022 Illuminating the threat landscape and empowering a digital defense.*

Microsoft. (2022c). *Microsoft Digital Defense Report 2022 Executive Summary*.

Microsoft Exchange & F5 Critical Vulnerabilities. (2021, Μάρτιος 12). *State Bank Commissioner of Kansa*. https://www.osbckansas.org/microsoft-exchange-f5-critical-vulnerabilities/

Morgenthau, H. J. (2018). *Η Πολιτική μεταξύ των Εθνών* (Κολιόπουλος Κωμσταντίνος, Επιμ.). Εκδόσεις ΠΟΙΟΤΗΤΑ.

Mumford, A. (2013). Proxy warfare and the future of conflict. *RUSI Journal*, *158*(2), 40–46. https://doi.org/10.1080/03071847.2013.787733

Nations, U. (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Note by the Secretary-General*.

NATO. (2002). *PRAGUE SUMMIT 2002*. https://www.nato.int/docu/0211prague/speeches-e.pdf

NATO. (2008). *Bucharest Summit Declaration*. https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2014). *Wales Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016a). *Cyber Defence Pledge*. https://www.nato.int/cps/su/natohq/official_texts_133177.htm

NATO. (2016b). *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Nye, J. S. (1990). Soft Power. *Foreign Policy*, *80*, 153. https://doi.org/10.2307/1148580

OEWG. (2021). *Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report-A/AC.290/2021/CRP.2*. https://www.un.org/disarmament/open-ended-

OEWG. (2022). *First annual progress report of the open-ended working groupon security of and in the use of information and communications technologies 2021–2025 - Report A/77/275*.

Office of Disarmament Affairs. (χ.χ.). *Group of Governmental Experts*.

OSCE. (χ.χ.). *Transnational Threats Department Cyber/ICT Security*.

OSCE. (2013). *DECISION No. 1106 INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES*.

OSCE. (2016). *DECISION No. 1202 OSCE CONFIDENCE-BUILDING MEASURES TOREDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES*.

Overview of F5 vulnerabilities. (2021, Μάρτιος). https://my.f5.com/manage/s/article/K02566623

Paganini, P. (2022). Another nation-state actor exploits Microsoft Follina to attack European and US entities. *Security Affairs*.

Pawlak, P. (2015). *At a glance*.

Pawlak, P., & Biersteker, T. (2019). *Guardian of the Galaxy: EU cyber sanctions and norms in cyberspace*. Publications Office of the European Union.

Phillips, M. (2010). National Will from a Threat Perspective. *MILITARY REVIEW*, 33–39.

Pipyros, K. (2019). *A new systematic modelling methodology for improving cyber-attack evaluation on states' Critical Information Infrastructure (CII) Kosmas Pipyros* [Ph.D.]. Athens University of Economics and Business.

Pipyros, K., Mitrou, L., & Gritzalis, D. (2017, Σεπτέμβριος). Evaluating the effects of cyber-attacks on critical infrastructures in the context of Tallinn Manual. *2nd Conference on Cyber Security in Maritime Domain*.

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyber operations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare. *Information and Computer Security*, *24*(1), 38–52. https://doi.org/10.1108/ICS-12-2014-0081

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016, Σεπτέμβριος). Cyber-Attacks Evaluation Using Simple Additive Weighting Method on the Basis of Schmitt' s Analysis. *10th Mediterranean Conference on Information Systems (MCIS-2016)*. http://aisel.aisnet.org/mcis2016http://aisel.aisnet.org/mcis2016/41

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers and Securitys*, *74*(Special), 371–383. https://doi.org/10.1016/j.cose.2017.04.007

Possen, B. (1984). The Sources of Military Doctrine: France, Britain, and Germany between the World Wars. Στο *The Sources of Military Doctrine* . Cornell University Press. https://www.jstor.org/stable/10.7591/j.ctt1287fp3

Pronk, D. (2021). *Fifty Shades of Grey 21 st century strategic competition with Russia and China Strategic Alert*.

Rantapelkonen, J., & Salminen, M. (2013). *THE FOG OF CYBER DEFENCE*.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Ringsmose, Jens., & Rynning, S. (2011). *NATO's new strategic concept: a comprehensive assessment*. Danish Institute for International Studies.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers and Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of Transnational Law37*, *37*, 885–937.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge University Press.

Smith, B. (2022). *Defending Ukraine: Early Lessons from the Cyber War*.

The White House. (2021, Ιούλιος 18). *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*. THE WHITE HOUSE.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & Mccue, M. (2018). *Addressing Hybrid Threats*.

United Nations -GA. (2021). *A/RES/75/240- Developments in the field of information and telecommunications in the context of international security*.

United Nations-GA. (2022). *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security-A/C.1/77/L.73*.

Von Klausewitz, K. (1999). *ΠΕΡΙ ΤΟΥ ΠΟΛΕΜΟΥ* (Ξεπουλιά, Νατάσα). ΕΚΔΟΣΕΙΣ ΒΑΝΙΑΣ.

Warden, J. A. (1995). The Enemy as a System. *Airpower Journal*, *9*(1), 40–55. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf

Watson, A. (2010). *Η ΕΞΕΛΙΞΗ ΤΗΣ ΔΙΕΘΝΟΥΣ ΚΟΙΝΩΝΙΑΣ* (Παπασωτηρίου Χαράλαμπος & Ήφαιστος Παναγιώτης, Επιμ.; 4ο έκδ.). Εκδόσεις ΠΟΙΟΤΗΤΑ.

What is a DDoS attack? (χ.χ.). CLOUDFLARE. Ανακτήθηκε 15 Μάιος 2023, από https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

WILPF. (2022). *ADVANCING A GLOBAL CYBER PROGRAMME OF ACTION: Options and priorities*.