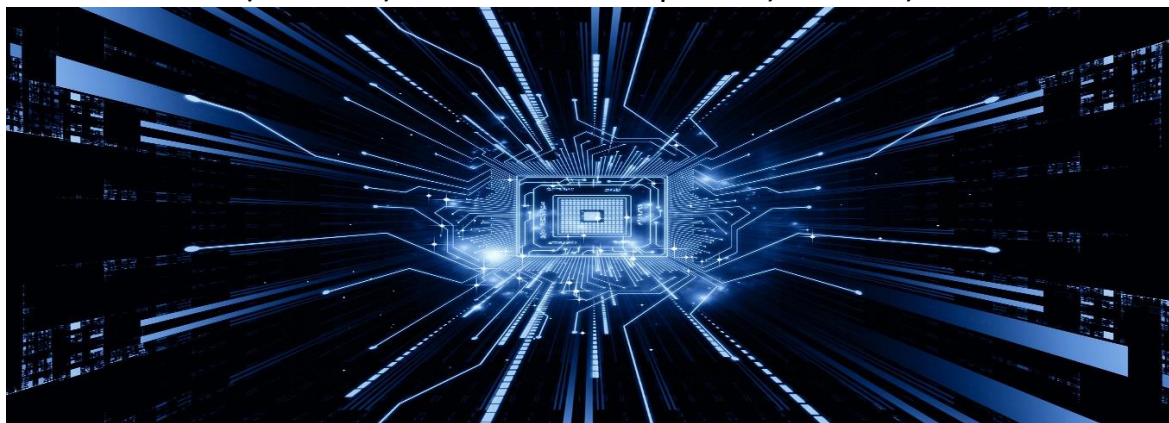




**ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

ΠΜΣ: ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ
Ειδίκευση: Διεθνές Δίκαιο και Διπλωματικές Σπουδές



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

*«Ο Κυβερνοχώρος ως Εργαλείο Προσπέλασης και Κατάλυσης
της Αρχής της Μη Επέμβασης στις Εσωτερικές Υποθέσεις Ενός
Κράτους»*

ΖΩΗ ΜΑΥΡΟΜΜΑΤΗ (ΑΜ 1218Μ029)

Επιβλέπουσα: Επίκουρη Καθηγήτρια Μαρία - Ντανιέλλα Μαρούδα

Αθήνα 20 Δεκεμβρίου 2019

Δηλώνω υπεύθυνα πως η παρούσα εργασία είναι αποτέλεσμα πρωτότυπης έρευνας και δε χρησιμοποιεί πνευματική ιδιοκτησία τρίτων χωρίς αναφορές.

Ως εκ τούτου αναλαμβάνω όλες τις νομικές και διοικητικές συνέπειες σε περίπτωση, που αποδειχθεί, ότι η εργασία μου αποτελεί προϊόν λογοκλοπής ή προϊόν τρίτων.

Copyright © Zoi Mavrommati, 2019.

Με επιφύλαξη παντός δικαιώματος. All Rights Reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να θεωρηθεί, ότι αντιπροσωπεύουν τις επίσημες θέσεις του Παντείου Πανεπιστημίου Κοινωνικών και Πολιτικών Επιστημών.

*«Η παρούσα εργασία είναι αφιερωμένη στην οικογένειά μου και
τους αγαπημένους μου ανθρώπους για την αμέριστη
συμπαράσταση και στήριξή τους...»*

Περιεχόμενα

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ	6
ΠΡΟΛΟΓΟΣ	7
ΕΙΣΑΓΩΓΗ	8
ΜΕΡΟΣ Α΄: ΤΟ ΔΙΚΑΙΪΚΟ ΠΛΑΙΣΙΩΜΑ ΕΛΕΓΧΟΥ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ	9
ΚΕΦΑΛΑΙΟ 1 ^ο : Το σύγχρονο πεδίο διεξαγωγής υβριδικών δραστηριοτήτων: βασικές έννοιες και νομική υπόσταση.....	9
ΚΕΦΑΛΑΙΟ 2ο: Το Δίκαιο της Χρήσεως Βίας και η εφαρμογή του στον Κυβερνοχώρο	12
2.1: Η αρχή της Απαγόρευσης Χρήσεως Βίας, υπό το πρίσμα της Αρχής της απαγόρευσης της επίθεσης (Άρθρο 2π4 του ΚΧ/ΗΕ).....	12
2.2: Η αρχή της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους, υπό το πρίσμα του Άρθρου 2π7 του ΚΧ/ΗΕ.	15
2.2.1.: Ο ρόλος των Ψηφισμάτων της Γενικής Συνέλευσης των Ηνωμένων Εθνών.....	17
2.2.1.a.: Προς μία ευρύτερη κατανόηση και η εισαγωγή της έννοιας του εξαναγκασμού	17
2.2.2.: Η έννοια της απαγόρευσης της επέμβασης στα ζητήματα εσωτερικής αρμοδιότητας του κράτους και η εφαρμογή της στον κυβερνοχώρο.	19
2.2.2.a: Intervention by States (Rule 66 – Tallinn Manual)	20
2.2.2.b: Intervention by the UN (Rule 67 – Tallinn Manual).....	25
2.2.3: Η έννοια του espionage στον κυβερνοχώρο	28
2.2.4.: Η έννοια της άσκησης δικαιοδοσίας και η εφαρμογή της στον κυβερνοχώρο	33
ΚΕΦΑΛΑΙΟ 3 ^ο : Η προβληματική της απόδοσης ευθύνης, ύστερα από τη διάπραξη παράνομης ενέργειας.....	42
3.1: Η εισαγωγή του όρου attribution.....	42
3.2: Η απόδοση ευθύνης στο κράτος (Responsibility of States for Internationally Wrongful Acts)	43
3.3: Ο ρόλος των μη κρατικών δρώντων και το ζήτημα της απόδοσης ευθύνης. ..	49
3.4: Η προβληματική των «ακυβέρνητων» περιοχών.....	51
ΜΕΡΟΣ Β΄: Η ΔΙΕΘΝΗΣ ΠΡΑΚΤΙΚΗ ΚΑΙ Η ΠΡΟΣΠΑΘΕΙΑ ΔΙΚΑΙΪΚΗΣ ΘΩΡΑΚΙΣΗΣ ΕΝΑΝΤΙ ΤΩΝ ΣΥΓΧΡΩΝΩΝ ΠΡΟΚΛΗΣΕΩΝ	59
ΚΕΦΑΛΑΙΟ 4 ^ο : Οι πλέον χαρακτηριστικές περιπτώσεις παραβίασης της αρχής της μη επέμβασης στην κυβερνοχώρο	59
4.1: Η Ρωσική ανάμειξη στις προεδρικές εκλογές των ΗΠΑ το 2016.....	59
4.1.1: Το χρονικό της επέμβασης	59
4.1.2: Τα νομικά ζητήματα που προκύπτουν	64

4.2: Η Ρωσική ανάμειξη στις προεδρικές εκλογές της Γαλλίας το 2017	65
4.2.1: Το χρονικό μίας επικείμενης επίθεσης	66
4.2.2: Τα νομικά ζητήματα που ανακύπτουν	68
4.3: Αποτέλεσαν αυτές οι δύο αναμετρήσεις παραβίαση της αρχής της μη επέμβασης;	69
ΚΕΦΑΛΑΙΟ 5 ^ο : Η προσπάθεια θωράκισης του κράτους αποδέκτη της επίθεσης	71
5.1: Η έννοια των αντιποίνων	71
5.2: Η έννοια των αντιμέτρων και η εφαρμογή της στον κυβερνοχώρο	72
5.3: Η έννοια των retortions	74
5.4: Η επιβολή κυρώσεων	75
5.4.1: Threat to the peace (Απειλή κατά της Διεθνούς Ειρήνης και Ασφάλειας)	76
5.4.2: Breach of the Peace (Διατάραξη της Διεθνούς Ειρήνης και Ασφάλειας):	76
5.4.3: Aggression (Επίθεση):	76
Κεφάλαιο 6 ^ο : Η θεσμική και Δικαιϊκή θωράκιση των Διεθνών Οργανισμών	79
6.1: Ο Οργανισμός Ηνωμένων Εθνών	79
6.2: Η Ευρωπαϊκή Ένωση	81
6.3: Οργανισμός Αμερικανικών Κρατών και Αφρικανική Ένωση	82
6.4: NATO	83
ΣΥΜΠΕΡΑΣΜΑΤΑ	85
ΒΙΒΛΙΟΓΡΑΦΙΑ	86

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ

ΣΥΝΤΜΗΣΗ	ΕΠΕΞΗΓΗΣΗ ΣΥΝΤΜΗΣΗΣ
Ελληνικές Συντμήσεις	
ΔΑΔ	Διεθνές Ανθρωπιστικό Δίκαιο
ΕΔΔ	Επιτροπή Διεθνούς Δικαίου
ΕΕ	Ευρωπαϊκή Ένωση
Η.Ε.	Ηνωμένα Έθνη
Η.Π.Α.	Ηνωμένες Πολιτείες Αμερικής
Ο.Η.Ε.	Οργανισμός Ηνωμένων Εθνών
ΣοΕ	Συμβούλιο της Ευρώπης
Αγγλικές Συντμήσεις	
ASR	Articles for State Responsibility
CASIC	China Aerospace Science & Industry Corporation
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDC	Cyber Defence Committee
CERT	Computer Emergency Response Team
DoD	Department of Defence
EC3	European Cybercrime Centre
EDA	European Defence Agency
EEAS	European External Action Service
ENISA	European Networks and Information Security Agency
EU	European Union
HRC	Human Rights Council
ICTs	Information and Communications Technologies
ISIS	Islamic State in Iraq and Syria
NAC	North Atlantic Council (Βορειοατλαντικό Συμβούλιο)
NATO	North Atlantic Treaty Organization (Βορειοατλαντικό Σύμφωνο)
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCRCG	National Cyber Response Coordination Group
OSCE	Organization for Security and Co-operation in Europe
RES	Resolution
UK	United Kingdom
UN	United Nations
US	United States
A/RES	Assembly General Resolution
SC/RES	Security Council Resolution
UN CHARTER	Charter of the United Nations
CoE	Council of Europe

ΠΡΟΛΟΓΟΣ

Με το πέρασμα των χρόνων η εξελικτική πορεία της τεχνολογίας διαμόρφωσε ένα νέο επιχειρησιακό πεδίο ανάπτυξης δραστηριοτήτων για τα κράτη ιδιαίτερα πολύπλοκο. Ο κυβερνοχώρος κατέστη κατ' αυτόν τον τρόπο το κομμάτι εκείνο, που συγκεντρώνει το μεγαλύτερο ενδιαφέρον ως προς τη διαμόρφωση και άσκηση πολιτικής επιρροής από τους δρώντες της διεθνούς σκακιάρας.

Το βασικότερο ερώτημα λοιπόν, το οποίο τίθεται, εστιάζει στο ποια είναι η θέση του δικαίου, και αν αυτό διαθέτει όλα εκείνα τα εργαλεία τα οποία θα το καταστήσουν κυρίαρχο σε έναν χώρο, όπου η καινοτομία ψάχνει, να βρει τρόπους προκειμένου να το θέσει στο περιθώριο. Η παρακολούθηση της Διεθνούς πραγματικότητας και οι ποικίλες αφορμές της διεθνούς πολιτικής σκηνής, αποτέλεσαν το σημαντικότερο κίνητρο για τη μελέτη και τη συγγραφή της παρούσας εργασίας, η οποία εστιάζει σε ένα ιδιαίτερο δικαϊκό κομμάτι, μία ρητή απαγόρευση του Διεθνούς Δικαίου η οποία όμως καθίσταται ιδιαίτερα ευάλωτη στον κυβερνοχώρο, λόγω κυρίως της ευκολίας τη τεχνολογίας να «σπάει» τους αυστηρούς δεσμούς, που απαγορεύουν καταστάσεις, χωρίς αυτό πολλές φορές να γίνεται αντιληπτό.

Η ρητή από το διεθνές δίκαιο απαγόρευση επέμβασης στις υποθέσεις που άπτονται της εσωτερικής δικαιοδοσίας του κράτους, αποτελεί το θεμέλιο λίθο δόμησης μίας δημοκρατικής κοινωνίας της οποίας τα μέλη καθίστανται κυρίαρχα, γεγονός που απαιτείται, να γίνεται σεβαστό από όλους.

Η επιλογή του συγκεκριμένου θέματος, βασίστηκε στην επιθυμία μου να καταστώ, μέσω της έρευνας που διεξήγαγα, κοινωνός προβληματισμών και αναζητήσεων αναφορικά με το πού μπορεί, να οδηγήσει η συνεχώς αυξανόμενη εξέλιξη των δυνατοτήτων του κυβερνοχώρου και ποια είναι η θέση του δικαίου στο πεδίο αυτό.

ΕΙΣΑΓΩΓΗ

Οι νέες μορφές παραβίασης των κανόνων που προστατεύουν τα κράτη από την ξένη επέμβαση, καθιστούν το διεθνές δικαϊκό στερέωμα ανασφαλές και πολλές φορές το θέτουν υπό αμφισβήτηση. Μετά το τέλος του Β'ΠΠ η Διεθνής κοινότητα πέρασε σε μία προσπάθεια θεμελίωσης των κανόνων εκείνων οι οποίοι θα καθιστούσαν σαφές, πως πρωταρχικός στόχος όλων των κρατών που θέλουν, να είναι μέλη της προσπάθειας αυτής, θα ήταν η με κάθε τρόπο προάσπιση της ειρήνης, η απομάκρυνση από τη χρήση μέσων που τροφοδοτούν τη βία και ο σεβασμός κάθε κράτους, ως κυρίαρχης οντότητας ίσης με όλες τις άλλες.

Όλα αυτά διατυπώθηκαν ρητώς στον καταστατικό χάρτη των Ηνωμένων Εθνών αλλά και σε μετέπειτα κείμενα, που ήρθαν για να τον πλαισιώσουν, ενώ πήραν σάρκα και οστά μέσα από τις αποφάσεις των διεθνών δικαιοδοτικών οργάνων τα οποία με τη σειρά τους διαμόρφωσαν τη διεθνή πρακτική. Όπως είπαμε και σε προηγούμενη σημείο, η εξέλιξη της τεχνολογίας άνοιξε άλλα μονοπάτια για τους διεθνείς δρώντες, προκειμένου οι ενέργειες στις οποίες καταφεύγουν, πολλές φορές να ξεπερνούν το όριο της νομιμότητας, αλλά χωρίς αυτό, να γίνεται πάντα αντιληπτό.

Η παρούσα εργασία αντλώντας την αφορμή από τις δύο εκλογικές αναμετρήσεις, αρχικά, αυτή των προεδρικών εκλογών στις Ηνωμένες Πολιτείες το 2016 και των Γαλλικών προεδρικών εκλογών το 2017, προσπαθεί, να εντοπίσει, ποια είναι τα σημεία εκείνα, όπου το δίκαιο βρίσκει εφαρμογή στο κυβερνοχώρο. Πιο συγκεκριμένα στο πρώτο μέρος μελετάται το νομικό πλαίσιο γύρω από την αρχή της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους υπό το πρίσμα του Α2π7 του ΚΧ/ΗΕ αλλά και η εφαρμογή του στον κυβερνοχώρο με έμφαση τις έννοιες της απόδοσης ευθύνης, της ύπαρξης εξαναγκασμού αλλά και τον ρόλο των μη κρατικών δρώντων σε όλο αυτό, εστιάζοντας σε κάθε πιθανή ιδιαιτερότητα της σύγχρονης πραγματικότητας. Στο δεύτερο μέρος εξετάζονται τα πραγματικά περιστατικά τα οποία ήγειραν όλα αυτά τα ερωτήματα προβαίνοντας σε ουσιαστικά συμπεράσματα.

ΜΕΡΟΣ Α΄: ΤΟ ΔΙΚΑΙΪΚΟ ΠΛΑΙΣΙΩΜΑ ΕΛΕΓΧΟΥ ΤΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΚΕΦΑΛΑΙΟ 1^ο: Το σύγχρονο πεδίο διεξαγωγής υβριδικών δραστηριοτήτων: βασικές έννοιες και νομική υπόσταση

Η έννοια του κυβερνοχώρου είναι αυτή η οποία χαρακτηρίζει ένα ευρύ δίκτυο επικοινωνιών, το οποίο χρησιμοποιεί ηλεκτρονικούς υπολογιστές. Ο Κυβερνοχώρος αποτελεί ένα νέο – σύγχρονο επιχειρησιακό πεδίο, στο οποίο τα κράτη καταφέροντας μέσω της τεχνολογικής ανάπτυξης, να εκμεταλλευτούν τις κάθε είδους δυνατότητες και ευελιξίες που διαθέτει, προβαίνουν σε ενέργειες οι οποίες έχουν ως στόχο, να βλάψουν το κράτος το οποίο δέχεται την εν λόγω επίθεση – επέμβαση.

Εδώ λοιπόν εισάγεται και ο σημαντικότερος όρος, αυτός της κυβερνοεπίθεσης – κυβερνοεπιχείρησης, cyberattack - cyberoperation, με τον οποίο εννοούμε την οργάνωση ενεργειών στον κυβερνοχώρο, στις οποίες καταφεύγουν τα κράτη, που το χρησιμοποιούν προκειμένου, να κερδίσουν το πλεονέκτημα έναντι των αντιπάλων τους και να πετύχουν το σκοπό τους. Αυτό είναι κάτι που καταφέρνουν χρησιμοποιώντας όπως προαναφέραμε όλα τα διαθέσιμα πλεονεκτήματα στον κυβερνοχώρο με σκοπό να απενεργοποιήσουν τα πληροφοριακά συστήματα της αντίπαλης πλευράς, να διεισδύσουν ή να υποκλέψουν τις απόρρητες πληροφορίες της αλλά και να προξενήσουν υλικές καταστροφές.¹ Η συστηματική κατασκοπεία, η παρακολούθηση κρατικών δομών και η απενεργοποίηση κρατικών συστημάτων ασφαλείας διαφόρων υποδομών είναι κάποια χαρακτηριστικά παραδείγματα κυβερνοεπιχειρήσεων. Χαρακτηριστικό τους γνώρισμα είναι η εύκολη διατήρηση της ανωνυμίας, η δυνατότητα διεξαγωγής με ιδιαιτέρως μεγάλη ταχύτητα αλλά και το χαμηλό επιχειρησιακό κόστος, εν συγκρίσει πάντα με την οργάνωση και υλοποίηση μίας πραγματικής επιχείρησης.

¹ International Review of the Red Cross, Volume 94 Number 886, Summer 2012, Harbert Lin, “Cyber Conflict and international humanitarian law”, p. 515

Στα τέλη Μαΐου του 2019 ο ίδιος ο Γενικός Γραμματέας του NATO Jens Stoltenberg, στο συνέδριο κυβερνοάμυνας το οποίο έλαβε χώρα στο Λονδίνο, σημείωσε, πως οι κυβερνοεπιθέσεις, μπορούν να είναι το ίδιο επιζήμιες με τις συμβατικές επιθέσεις και να θέσουν σοβαρές απειλές για τις οικονομίες των κρατών, που γίνονται αποδέκτες τους, να προκαλέσει σοβαρές ζημιές στις κρατικές υποδομές και όπως κατάδειξαν τα πρόσφατα παραδείγματα των Αμερικανικών και των Γαλλικών εκλογών, που θα αναλύσουμε παρακάτω, να υπονομεύσουν την ακεραιότητα της δημοκρατίας.² Αυτό που θα δυναμιτίσει την ασφάλεια, είναι η προσπάθεια από τα κράτη, να την ενισχύσουν, μέσω της κατανόησης κυρίως του, τί πραγματικά είναι αυτό το οποίο διεξάγεται στον κυβερνοχώρο και τί διαστάσεις μπορεί, να πάρει. Κυρίως αυτό που τονίζεται, είναι πως, θα πρέπει, να ενισχυθεί η προσπάθεια του καθορισμού της απόδοσης ευθύνης, καθώς με αυτόν τον τρόπο τα κράτη πλέον θα πρέπει, να γνωρίζουν, πως θα εντοπισθούν και θα βρεθούν υπόλογοι των ενεργειών τους.³

Προς την όλη αυτή κατεύθυνση σημαντικό έργο έχουν επιτελέσει όργανα των Ηνωμένων Εθνών αλλά διεθνείς – περιφερειακοί οργανισμοί οι οποίοι υιοθετώντας κείμενα και αποφάσεις συνδράμουν στην προσπάθεια στελέχωσης και δικαιοσύνης κάλυψης του κυβερνοχώρου. Χαρακτηριστικότερο παράδειγμα αποτελεί η σημαντική προσπάθεια μίας ομάδας επιστημόνων αλλά και ακαδημαϊκών καθηγητών στο Κέντρο Αριστείας Κυβερνοάμυνας, στο Ταλλίν της Εσθονίας οι οποίοι προσπάθησαν, να μεταφέρουν το συμβατικό Διεθνές Δίκαιο στον κυβερνοχώρο, υιοθετώντας ένα κείμενο – εγχειρίδιο, το Εγχειρίδιο του Ταλλίν περί της εφαρμογής του Διεθνούς Δικαίου στον Κυβερνοχώρο. Στο εν λόγω κείμενο, αναλύονται τα σημαντικότερα ζητήματα του διεθνούς δικαίου, που αφορούν τη Χρήση βίας, το ζήτημα της απόδοσης ευθύνης αλλά και της άσκησης δικαιοδοσίας, της μη ανάμειξης στις εσωτερικές υποθέσεις ενός κράτους, το Διεθνές Ανθρωπιστικό Δίκαιο (ΔΑΔ), τα ανθρώπινα δικαιώματα και όχι μόνο, προσφέροντας πολλές φορές ερμηνευτικές προσεγγίσεις, προκειμένου να καταστούν πιο

² North Atlantic Treaty Organization, Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, Πρόσβαση 17/12/2019, Διαθέσιμο στη Διεύθυνση https://www.nato.int/cps/en/natohq/opinions_166039.htm

³ ibid

κατανοητά τα ζητήματα, που πραγματεύεται. Χρειάζεται βέβαια, να τονίσουμε, πως δεν αποτελεί συμβατικό κείμενο, ακόμα και για το NATO, αλλά έναν λεπτομερή συμπεριφορικό κώδικα.⁴

⁴ Tallinn Manual 2.0: The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations, (...)“The focus of the original Tallinn Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict. Tallinn Manual 2.0 adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict.”(...), Πρόσβαση 17/12/2019, Διαθέσιμο στη Διεύθυνση <https://ccdcoe.org/research/tallinn-manual/>

ΚΕΦΑΛΑΙΟ 2ο: Το Δίκαιο της Χρήσεως Βίας και η εφαρμογή του στον Κυβερνοχώρο

2.1: Η αρχή της Απαγόρευσης Χρήσεως Βίας, υπό το πρίσμα της Αρχής της απαγόρευσης της επίθεσης (Άρθρο 2π4 του ΚΧ/ΗΕ).

Αν και δεν αποτελεί το βασικό αντικείμενο μελέτης της παρούσας εργασίας, κρίνεται σκόπιμο, να συμπεριληφθεί ως κομμάτι αυτής, η αρχή της απαγόρευσης της επίθεσης ή της απειλής χρήσης βίας καθώς αποτελεί τη ναυαρχίδα αξιών πάνω στην οποία στηρίχθηκε ο Καταστατικός Χάρτης των Ηνωμένων Εθνών.

Στην τέταρτη παράγραφο λοιπόν του δεύτερου άρθρου τονίζεται η υποχρέωση των κρατών, να απέχουν από την απειλή ή τη χρήση βίας η οποία βρίσκεται εκ διαμέτρου αντίθετη ως προς τις βασικές αρχές των Ηνωμένων Εθνών.⁵ Μιλάμε για τη σπουδαιότερη ρητή καταγραφή απαγόρευσης της άσκησης ένοπλης επίθεσης η οποία στην πραγμάτωσή της θα γίνει αιτία για τη διατάραξη της διεθνούς ειρήνης και ασφάλειας, η αποφυγή της οποίας αποτελεί βασική προτεραιότητα και επιθυμία των μελών του Οργανισμού των Ηνωμένων Εθνών, πολλώ δε μάλλον σε μία εποχή, που ακολούθησε της πιο βίαιης και ταραχώδους περιόδου της σύγχρονης ιστορίας. Φτάνει λοιπόν η ώρα όπου τα κράτη χρειάζεται, να καταστήσουν ακόμη πιο σαφή την ανάγκη για ρητή αποχή από επιθετικές ενέργειες, ύστερα από τη λίγο μετριοπαθέστερη στάση του Συμφώνου της Κοινωνίας των Εθνών όπου στο άρθρο 12 οριζόταν νόμιμη η προσφυγή σε πόλεμο, έπειτα από την τρίμηνη προθεσμία για εφαρμογή της αντίστοιχης απόφασης του ΔΔΔΔ ή της Διαιτησίας στην οποία θα είχαν καταφύγει τα κράτη ανάμεσα στα οποία είχε παρουσιαστεί διαφορά-ρήξη.⁶

⁵ Article 2p4 CUN: The Charter of the United Nations “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

⁶ Article 12: “The Members of the League agree that, if there should arise between them any dispute likely to lead to a rupture they will submit the matter either to arbitration or judicial settlement or to enquiry by the Council, and they agree in no case to resort to war until three months after the award by the arbitrators or the judicial decision, or the report by the

Την εμβληματικότερη περιπτώσιολογία αναφορικά με την απαγόρευση της επίθεσης αποτελεί η ερμηνεία που έδωσε το ΔΔΧ στην υπόθεση του 1986 “Military and Paramilitary activities in and against Nicaragua”. Εδώ λοιπόν το Δικαστήριο προσπαθώντας να προσδιορίσει σε ποιες περιπτώσεις ένα κράτος δέχεται ένοπλη επίθεση κάνει επίκληση του Ψηφίσματος 3314 της ΓΣ/ΗΕ περί ορισμού της επίθεσης (1974). Αυτό το Ψήφισμα ήρθε προκειμένου να αποσαφηνίσει και να κατηγοριοποιήσει τις περιπτώσεις, όπου υφίσταται ένοπλη επίθεση. Ο πίνακας των πράξεων που την καθιστούν τέτοια είναι ενδεικτικός αλλά μπορεί να μεταβάλλεται και από το ΣΑ/ΗΕ.⁷

Στο συγκεκριμένο Ψήφισμα και πιο συγκεκριμένα στο Άρθρο 1 γίνεται αναφορά μόνο στην ένοπλη επίθεση⁸, με το Άρθρο 2 να εστιάζει στο τί αποτελεί απόδειξη επιθετικής πράξης⁹, καταδεικνύοντας τη «χρήση ένοπλης δύναμης» και το Άρθρο 3 έρχεται να επιμερίσει τις περιπτώσεις που αποτελούν επίθεση.¹⁰

Έτσι λοιπόν, στην υπόθεση αυτή το Δικαστήριο προσπάθησε, να προσδιορίσει την περιπτώσιολογία, που συνιστά ένοπλη επίθεση, προκειμένου να προσδιορίσει αν ενέργειες των ΗΠΑ, μπορούν να χαρακτηριστούν ως επιθετικές. Συνεκτιμώντας τα πραγματικά περιστατικά τόσο της τοποθέτησης ναρκών στα χωρικά ύδατα της Νικαράγουα, όσο και των επιθέσεων σε πετρελαϊκές εγκαταστάσεις και ναυτικές

Council. In any case under this Article the award of the arbitrators or the judicial decision shall be made within a reasonable time, and the report of the Council shall be made within six months after the submission of the dispute.”

⁷ Ρούκουνας Εμμανουήλ, Δημόσιο Διεθνές Δίκαιο, Νομική Βιβλιοθήκη, 2015, σελ. 105

⁸ GA OR 29 (XXIX) Session Res 3314 A/9890, 14/12/1974, Article 1: “Aggression is the Use of armed force by a State against the sovereignty, territorial integrity or political independence of another State or in any other manner inconsistent with the Charter of United Nations, as set out in this Definition.”

⁹ Ibid: Article 2: The First use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.

¹⁰ Ibid: Article 3: (...) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, (...) Bombardment by the armed forces of a State (...), The blockade of the ports or coasts of a State (...), An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State, (...) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State (...).

βάσεις της χώρας, το Δικαστήριο κατέληξε στο συμπέρασμα, πως οι ενέργειες αυτές αποτελούν κατάφορη παραβίαση της αρχής της «απαγόρευσης της επίθεσης».

Εντείνοντας τη σοβαρότητα της κατάστασης το Δικαστήριο κάνει λόγο ακόμη και για πράξεις οι οποίες δεν παρουσιάζουν την αναγκαιότητα ενεργοποίησης του δικαιώματος της Νόμιμης Άμυνας, σύμφωνα με το Άρθρο 51 ΚΧ/ΗΕ, αλλά παρ' όλα αυτά περιλαμβάνουν τη χρήση βίας και γι' αυτό συνιστούν πράξεις στις οποίες το κράτος μπορεί να απαντήσει με αντίμετρα, με βάση πάντα την αρχή της αναλογικότητας.¹¹

Η κρισιμότητα των συγκεκριμένων ρυθμίσεων μας καλεί, να εστιάσουμε και σε κάτι άλλο πολύ σημαντικό. Για να μην ξεχνάμε και το βασικό υποκείμενο μελέτης μας, που δεν είναι άλλο από τον κυβερνοχώρο, χρειάζεται, να τονίσουμε, πως οι ρυθμίσεις αυτές επιδέχονται εφαρμογής και σε αυτόν, κάτι που φαίνεται να αποτελεί ιδιαίτερα σημαντική πρόκληση και θα αναλυθεί εκτενέστερα και στη συνέχεια της εργασίας μας. Σημαντικά ως προς τη θεμελίωση της άποψης αυτής συνέβαλε και μία εμβληματική γνωμοδότηση του ΔΔΧ ΤΟΥ 1996 αναφορικά με τη χρήση των πυρηνικών όπλων , η οποία διευκρίνισε με σαφήνεια ότι τα άρθρα 2(4), 42 και 51 του Χάρτη των Ηνωμένων Εθνών δεν αναφέρονται σε συγκεκριμένα όπλα και ότι εφαρμόζονται σε κάθε είδους χρήση βίας, ανεξάρτητα από το χρησιμοποιούμενο όπλο.¹² Φυσικά και η γνωμοδότηση του δικαστηρίου τη δεδομένη χρονική περίοδο αντικατόπτριζε το τεταμένο κλίμα της εποχής, παρ' όλα αυτά η χρήση της φράσης «της μη αναφοράς σε συγκεκριμένο όπλο» - “do not refer

¹¹ *Military and Paramilitary activities in and against Nicaragua (Nicaragua v. USA), Merits, Judgment I.C.J. Reports 1986, p 195*: In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law.

¹² *Legality of the threat or use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ, p. 39*: “These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter”, Ανάκτηση: 14/10/2019

to specific weapons”, αφήνει ανοιχτό το ερμηνευτικό πεδίο, ως προς το τί μπορεί να ληφθεί υπ’ όψιν ως όπλο και ποια συμπεριφορά, ως απειλή χρήσης βίας.

Κατ’ επέκταση λοιπόν, η απαγόρευση αυτή αποτυπώνεται ρητά και στο εγχειρίδιο του Ταλλίν, όπου στον Κανόνα 68 διασαφηνίζεται, πως μία ενέργεια η οποία διεξάγεται στον κυβερνοχώρο, χρησιμοποιώντας την απειλή χρήσης βίας ή τη πραγματώνοντάς τη, ενάντια στην εδαφική ακεραιότητα ή την πολιτική ανεξαρτησία ενός κράτους, είναι παράνομη. Παράλληλα, θέλοντας, να τονίσουν τις ιδιαίτερες δυνατότητές του κυβερνοχώρου, αποτυπώνουν στον κανόνα 69, την πρωτοποριακή διασαφήνιση, πως μία κυβερνητική επιχείρηση, εξομοιώνεται με τη χρήση βίας, όταν τα αποτελέσματά της είναι συγκρίσιμα με μία πραγματική κατάσταση χρήσεως ένοπλης βίας. Τέλος, ακόμη και η απειλή για πραγμάτωση μίας ενέργειας είναι παράνομη, διότι αυτή εάν πραγματώνοντας και με δεδομένο ότι θα περιελάμβανε τη χρήση βίας, έρχεται σε ρήξη με το Διεθνές Δίκαιο και αποτελεί, παράνομη χρήση βίας.¹³

2.2: Η αρχή της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους, υπό το πρίσμα του Άρθρου 2π7 του ΚΧ/ΗΕ.

Ένα από τα βασικότερα συστατικά της Διεθνούς κοινωνίας, που την καθιστούν οργανωτικά δομημένη, είναι ο σεβασμός της κρατικής κυριαρχίας και της ισότητας αυτής για όλα τα κράτη.¹⁴

Μέσω των κανόνων, που έχουν θεσπιστεί, γίνεται μία εκτεταμένη προσπάθεια τα κράτη να απέχουν από κάθε είδους παράνομες ενέργειες οι οποίες θα

¹³ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, P 329 - 339

¹⁴ «Σήμερα είναι γενικά αποδεκτό πως το κράτος είναι κυρίαρχο, επειδή υπάγεται στο ΔΔ. Αυτό το τελευταίο του εξασφαλίζει εδαφική ακεραιότητα, ισότητα, τήρηση των συμφωνημένων, μη επέμβαση στις εσωτερικές υποθέσεις και τέλος, δυνατότητα μεταβολής των διαδικασιών και των ουσιαστικών κανόνων που διέπουν τις Διεθνείς σχέσεις», Δημόσιο Διεθνές Δίκαιο, Εμμανουήλ Ρούκουνας, Νομική Βιβλιοθήκη, 2η έκδοση, Αθήνα 2015, σ.22

οδηγήσουν στα δυσάρεστα γεγονότα της δεκαετίας του 40'. Σαφέστατα ο ΚΧ/ΗΕ μιλά για σεβασμό της ισότητας της κυριαρχίας για όλα τα κράτη¹⁵ κάτι που καθίσταται ιδιαίτερα ευκρινές από την καθιέρωση στην επόμενη παράγραφο του εν λόγω άρθρου της αρχής της απαγόρευσης χρήσης βίας. Προχωρώντας ουσιαστικά στην προσπάθεια θεμελίωσης τη ειρήνης και της θέσπισης περιορισμών ως προς την ελευθερία κινήσεων για τα κράτη, οι οποίες έτειναν να έχουν ως αποτέλεσμα τη διατάραξη ή παραβίαση της διεθνούς ειρήνης και ασφάλειας, η απαγόρευση της Αρχής της Μη Επέμβασης στις Εσωτερικές Υποθέσεις ενός κράτους¹⁶ έρχεται να αποτελέσει έναν από τους θεμελιώδεις κανόνες του ΚΧ/ΗΕ.¹⁷

Μέσω αυτής της ρύθμισης θεσπίζεται η προστασία της κυριαρχίας ενός κράτους και διευκρινίζονται εκείνοι οι τομείς οι οποίοι αποτελούν κομμάτι αυστηρώς της δικής τους δικαιοδοσίας, με εξαίρεση φυσικά την «επιτρεπτή» επέμβαση από το ΣΑ/ΗΕ, υπό το κεφάλαιο VII, ακόμα κι όταν το κράτος υποστηρίζει, πως το ζήτημα για το οποίο γίνεται λόγος εμπίπτει στην εσωτερική του αρμοδιότητα, όπως θα εξετασθεί αναλυτικώς στη συνέχεια. Όπως επισημαίνεται και από τον B. Simma, οι κανόνες οι οποίοι θεσπίζονται αφορούν πρώτον τα όργανα των ΗΕ, ωθώντας τα στο σεβασμό των εσωτερικών υποθέσεων των κρατών, δεύτερον στα κράτη μέλη των ΗΕ, προκειμένου, να μη θέτουν προς συζήτηση ζητήματα τα οποία άπτονται της εσωτερικής δικαιοδοσίας άλλων κρατών μελών και τέλος τίθεται η εξαίρεση αναφορικά με την ιδιαίτερη δυνατότητα επέμβασης από το ΣΑ/ΗΕ, όπως προαναφέραμε.¹⁸ Η δεύτερη αυτή ρύθμιση έρχεται σε αντιστοιχία με ρήτρες πολυμερών και διμερών μέσων επίλυσης διαφορών, οι ρητές διατάξεις των οποίων τονίζουν, πως τα κάθε είδους όργανα επίλυσης διαφορών είναι αρμόδια μόνο για

¹⁵ Article 2p1 Charter of the UN. "The Organization is based on the principle of the sovereign equality of all its Members."

¹⁶ Article 2p7 UN Charter: "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII"

¹⁷ Bruno Simma, *The Charter of the United Nations, A Commentary*, Oxford University Press, 1995, p 143

¹⁸ Ibid: p. 149

εξέταση διακρατικών διαφορών, με βάση πάντα το δίκαιο.¹⁹ Από τα προαναφερθέντα θα μπορούσαμε, να πούμε, πως κατά κάποιον τρόπο τίθενται τα απαραίτητα εκείνα όρια, προκειμένου να επέλθει η αποτροπή, ως προς την επιθυμία αλλαγής από ένα επεμβαίνον κράτος των πολιτικών και όχι μόνο εξελίξεων στο κράτος που δέχεται την επέμβαση.

Προς την κατεύθυνση αυτή κινήθηκε και το ΔΔΧ στην Υπόθεση των «Στρατιωτικών και παραστρατιωτικών δραστηριοτήτων εντός και εκτός της Νικαράγουα» το 1986, όπου το δικαστήριο κάνοντας μνεία και το Ψήφισμα 2625 της Γενικής Συνέλευσης²⁰ διευκρινίζει πως, ένα κράτος έχει το δικαίωμα να διαχειρίζεται τις υποθέσεις του χωρίς εξωτερική παρέμβαση, μιας και ανάμεσα σε κυρίαρχα κράτη θα πρέπει, να γίνεται σεβαστή η εδαφική ακεραιότητα και η πολιτική ανεξαρτησία, ως αξίες θεμελιώδεις για το Δίκαιο που διέπει τη Διεθνή κοινωνία.²¹ Επιπρόσθετα, σε επόμενο σημείο διασαφηνίζονται οι παράγοντες εκείνοι οι οποίοι αποτελούν κομμάτι της εσωτερικής δικαιοδοσίας και δεν είναι άλλοι από το οικονομικό, το πολιτικό το κοινωνικό, τον πολιτισμό και τη διαμόρφωση της εξωτερικής πολιτικής.²²

2.2.1.: Ο ρόλος των Ψηφισμάτων της Γενικής Συνέλευσης των Ηνωμένων Εθνών

2.2.1.a.: Προς μία ευρύτερη κατανόηση και η εισαγωγή της έννοιας του εξαναγκασμού

Είναι απόλυτα λογικό το περιεχόμενο της συγκεκριμένης απαγόρευσης να έμοιαζε σε πρώτο βαθμό ιδιαίτερα ακαθόριστο, είτε γενικά να γίνει αντικείμενο παρερμηνειών και παραβλέψεων. Σταδιακά λοιπόν, φαίνεται, να επέρχεται ένα ξεκαθάρισμα ως προς τις ρυθμίσεις του εν λόγω άρθρου. Η αρχή γίνεται με το

¹⁹ *ibid*: (...) organs of dispute settlement are only competent to consider disputes under international law, p. 149

²⁰ Βλ. ενότητα 2.2.1.a

²¹ Case Military and Paramilitary activities in and against Nicaragua, Nicaragua vs United States of America, Judgment of 27 June 1986, p. 202

²² *Ibid*: p. 205

Ψήφισμα 1236 της Γενικής Συνέλευσης των Ηνωμένων Εθνών²³, όπου τα κράτη καλούνται να προασπίζουν τη διεθνή συνεργασία, να σέβονται την ισότητα της κρατικής κυριαρχίας για κάθε κράτος και να απέχουν από οποιαδήποτε ενέργεια έρχεται σε ρήξη με την αρχή της απαγόρευσης στα ζητήματα, που άπτονται της εσωτερικής αρμοδιότητας των κρατών.²⁴

Μία δεκαετία αργότερα ένα ακόμη Ψήφισμα της ΓΣ/ΗΕ, έρχεται, να διασαφηνίσει με μεγαλύτερη ακρίβεια το πλαίσιο εφαρμογής της εν λόγω ρύθμισης. Πιο συγκεκριμένα το Res 2131 (1966)²⁵, τονίζει πως κανένα κράτος δεν έχει το δικαίωμα να επεμβαίνει έμμεσα ή άμεσα, χρησιμοποιώντας βία ή οποιοδήποτε άλλο μέσο, προκειμένου να απειλήσει εν γένει την εσωτερική δομή του κράτους, την οικονομική και την πολιτική του ζωή, ακόμη και την κουλτούρα του.²⁶ Με το ψήφισμα αυτό η Γενική Συνέλευση μπορούμε να πούμε πως συγκεκριμενοποιεί τα πεδία εκείνα τα οποία άπτονται αυστηρώς στην εσωτερική δικαιοδοσία του κράτους. Ένα σημαντικό βήμα στην όλο και πληρέστερη κατανόηση του ζητήματος είναι η εισαγωγή του όρου “coercion” με τον οποίο δηλώνεται ο εξαναγκασμός ο οποίος χαρακτηρίζει τη φύση των παρεμβάσεων στις εσωτερικές υποθέσεις ενός κράτους, μίας δηλαδή κατάστασης απομακρυσμένης από την έννοια του ακώλυτου τρόπου λήψης αποφάσεων. Απαγορεύει με αυτόν τον τρόπο την υπό εξαναγκασμό

²³ Res GA/UN 1236 (1957) of December 4, “Peaceful and Neighborly Relations among States”, Διαθέσιμο στη Διεύθυνση <http://www.worldlii.org/int/other/UNGA/1957/158.pdf>

²⁴ Ibid: “(...) Realizing the need (to promote these objectives) to develop peaceful and tolerant relations among States, in conformity with the Charter, based on mutual respect and benefit, non-aggression, respect for each other’s sovereignty, equality and territorial integrity and non-intervention in one another’s internal affairs, and to fulfill the purposes and principles of the Charter, (...)”

²⁵ Res GA/UN 2131 (1966) “Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty”, Διαθέσιμο στη Διεύθυνση, [https://undocs.org/en/A/RES/2131\(XXI\)](https://undocs.org/en/A/RES/2131(XXI))

²⁶ Ibid: “No state has the right to intervene, directly or indirectly, in the internal or the external affairs (...) armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and social instructions. (...) all (other) forms of interference are condemned.

άσκησης της κρατικής κυριαρχίας²⁷. Το στοιχείο αυτό θεωρείται απαραίτητη προϋπόθεση προκειμένου, να μπορέσει να στοιχειοθετηθεί παραβίαση.²⁸

Χρειάζεται, να έχουμε πάντα κατά νου, τη βασική αρχή η οποία δομεί και κινεί το διεθνές νομικό σύστημα και δεν είναι άλλη από το σεβασμό της κυριαρχίας για όλα τα κράτη. Το Ψήφισμα 2625 της Γενικής Συνέλευσης των Ηνωμένων Εθνών έρχεται, να διευκρινίσει ορισμένες θεμελιώδεις αξίες, όπως ο διαχειρισμός κάθε είδους ζητήματος με ειρηνικά μέσα, της συνεχούς συνεργασίας, των ίσων δικαιωμάτων καθώς και του δικαιώματος στον αυτοπροσδιορισμό, αλλά τονίζεται και η ύπαρξη καθήκοντος ως προς τη μη επέμβαση σε ζητήματα, τα οποία άπτονται της δικαιοδοσίας του κράτους,²⁹ είτε χρησιμοποιώντας την ένοπλη βία, είτε κάθε άλλου είδους μέσο για την επίτευξη αυτού του σκοπού.³⁰

2.2.2.: Η έννοια της απαγόρευσης της επέμβασης στα ζητήματα εσωτερικής αρμοδιότητας του κράτους και η εφαρμογή της στον κυβερνοχώρο.

Η ιδιαιτερότητα του ζητήματός μας έγκειται ως επί τω πλείστον στην προσπάθεια εφαρμογής της εν λόγω ρύθμισης στην κυβερνοχώρο. Ένα επιχειρησιακό πεδίο το οποίο λόγω των ακαθόριστων συνόρων του, της μη ξεκάθαρης εντοπιότητας σαφών ορίων ως προς την άσκηση κυριαρχίας, γεννά συνεχώς ερωτήματα αναφορικά με τον τρόπο εφαρμογής των βασικών κανόνων του Διεθνούς Δικαίου. Παρατηρείται,

²⁷ Ibid: No state may use (...) measures to coerce another state in order to (...)

²⁸ Simma Bruno, The Charter of the United Nations: a commentary, Oxford University Press, 1995, “To intervene means to take action (...) in order to alter those matters, legally or politically, without giving the state concerned an opportunity to object to this intervention”, p 151

²⁹ Res 2625 General Assembly (1970), “(c) The duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter”, Διαθέσιμο στη Διεύθυνση

<https://unispal.un.org/DPA/DPR/unispal.nsf/0/25A1C8E35B23161C852570C4006E50AB>

³⁰ Ibid: “No State or group of States has the right to intervene directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.”

πως τα τελευταία χρόνια η εξέλιξη της τεχνολογίας και της καινοτομίας έχουν καταστήσει τον κυβερνοχώρο ένα νέο πεδίο άσκησης πιέσεων, διεξαγωγής επιθέσεων και προσπάθειας άντλησης πληροφοριών σε διακρατικό και όχι μόνο επίπεδο. Εδώ λοιπόν είναι, που χρειάζεται να δοθεί σαφέστερη απάντηση, ως προς το ποια είναι η θέση του Δικαίου εντός του νέου αυτού επιχειρησιακού πεδίου.

Στο εγχείρημα αυτό συνέβαλλαν οι εμπειρογνώμονες του NATO, δημιουργώντας το εγχειρίδιο του Tallinn προσπαθώντας, να οριοθετήσουν τις υποχρεώσεις και τα δικαιώματα ενός κράτους αναφορικά με τις ενέργειές του στον κυβερνοχώρο, καλύπτοντας ένα ευρύ πλαίσιο δράσης αναφορικά με τα πιο συνηθισμένα περιστατικά τα οποία καλούνται να αντιμετωπίσουν σε καθημερινή βάση τα κράτη, περιστατικά τα οποία φτάνουν κοντά στην χρήση ένοπλης βίας ή την απειλή αυτής. Προσδιορίζεται ακόμα και το ποια είναι επί της ουσίας η θέση του κράτους ως προς την απάντηση σε μία τέτοια ενέργεια, ως προς τη χρήση δηλαδή της νόμιμης άμυνας, των αντιμέτρων, των κυρώσεων κλπ. Έτσι λοιπόν χρειάζεται να δοθεί έμφαση τόσο στις κυβερνοεπιχειρήσεις οι οποίες λαμβάνουν χώρα σε περίοδο πολέμου αλλά και σε αυτές σε περιόδους ειρήνης. Την πρωτοβουλία για τη συγγραφή του εγχειριδίου αυτού πήρε ο Michael Schmitt από το Αμερικανικό Κολέγιο Πολεμικού Ναυτικού του Πανεπιστημίου του Exeter. Πρόκειται για μία εκτεταμένη προσπάθεια η οποία αποτελεί απόρροια της έρευνας και της διασταύρωσης των απόψεων όσων δούλεψαν γι' αυτό, ενώ τονίζεται, πως δεν αποτελεί παγιωμένη αντίληψη του οργανισμού του NATO, των Ηνωμένων Εθνών καθώς και άλλων επί μέρους κρατών.³¹

2.2.2.a: Intervention by States (Rule 66 – Tallinn Manual)

Πώς, λοιπόν εφαρμόζεται το συμβατικό Διεθνές Δίκαιο στον κυβερνοχώρο; Από την εισαγωγή του λοιπόν ο κανόνας 66 απαγορεύει ρητώς την «εξαναγκαστική

³¹ (...)The expanded edition of the Tallinn Manual, like its predecessor, represents only the views of its authors, and not of NATO, the CCDCOE, its Sponsoring Nations, or any other State or organization., *Tallinn Manual 2.:The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations*, Διαθέσιμο στη Διεύθυνση: <https://ccdcoe.org/research/tallinn-manual/>

επέμβαση»³² από ένα κράτος στις εσωτερικές και εξωτερικές υποθέσεις ενός κράτους. Και εγώ γίνεται ιδιαίτερη μνεία στην εξασφάλιση της προστασίας της βασικής αρχής, που δεν είναι άλλη από το σεβασμό της κυρίαρχης ισότητας, όπως τονίζεται και στην πρώτη παράγραφο του Άρθρου 2 του ΚΧ/ΗΕ.³³

Ως προς την κατεύθυνση αυτή κινήθηκε και το ΔΔΧ στην Υπόθεση των «στρατιωτικών και παραστρατιωτικών δραστηριοτήτων εντός και εκτός της Νικαράγουα» το 1986, όπως προαναφέραμε διευκρινίζοντας πως, ένα κράτος έχει το δικαίωμα να διαχειρίζεται τις υποθέσεις του χωρίς εξωτερική παρέμβαση, μιας και ανάμεσα σε κυρίαρχα κράτη θα πρέπει, να γίνεται σεβαστή η εδαφική ακεραιότητα και η πολιτική ανεξαρτησία, ως αξίες θεμελιώδεις για το Δίκαιο που διέπει τη Διεθνή κοινωνία. Επιπρόσθετα, σε επόμενο σημείο διασαφηνίζονται οι παράγοντες εκείνοι οι οποίοι αποτελούν κομμάτι της εσωτερικής δικαιοδοσίας και δεν είναι άλλοι από το οικονομικό, το πολιτικό το κοινωνικό, το πολιτιστικό σύστημα και τη διαμόρφωση της εξωτερικής πολιτικής.^{34 35} Παρατηρούμε δηλαδή μία διεύρυνση του προστατευόμενου πεδίου αναφορικά με την ισχύ της απαγόρευσης της αρχής της μη επέμβασης.

1

Σύμφωνα με τον εν λόγω κανόνα λοιπόν, τίθεται ρητώς η απαγόρευση της χρησιμοποίησης των οποιωνδήποτε μέσων στον κυβερνοχώρο, προκειμένου το κράτος να υιοθετήσει μία συγκεκριμένη πολιτική ή να λάβει μία απόφαση, μετά από άσκηση εξαναγκασμού και χωρίς τη θέλησή του. Η άσκηση της εν λόγω πίεσης χρειάζεται, να έχει προέλθει από κάποιον κρατικό δρώντα, προκειμένου να μπορέσει να αποδοθεί ευθύνη.³⁶ Η ομάδα των ειδικών παρατηρεί πως στον κυβερνοχώρο, η παραβίαση αυτή είναι συχνό φαινόμενο, κάτι όμως που δεν πρέπει

³² Rule 66: “This Rule prohibits coercive Intervention (...) into the internal and external affairs(...), Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p 312

³³ Article 2p1 UN Charter: “The Organization is based on the principle of the sovereign equality of all its Members.”

³⁴ *Nicaragua vs USA*, 1986, p. 202, 205

³⁵ Βλ. αναλυτικά ενότητα 2.2

³⁶ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 312 -314

να συνιστά υποβάθμιση της αξίας του κανόνα ως εθνικού.³⁷ Μη επιτρεπτή κατ' αυτόν τον τρόπο χαρακτηρίζεται και η παροχή για παράδειγμα από τον επεμβαίνον κράτος μεθόδων, όπως η παροχή τεχνολογιών για παραβίαση από αντάρτικες ομάδες των υποδομών των υπηρεσιών ασφαλείας ως προς τη διευκόλυνση των αντικυβερνητικών τους κινήσεων.³⁸ Μία τέτοιου είδους ενέργεια συνιστά παραβίαση της αρχής της μη επέμβασης στις εσωτερικές υποθέσεις του κράτους όπως αντίστοιχα σωστά θεωρήθηκε ως παραβίαση η παροχή στρατιωτικής βοήθειας, ο εξοπλισμός, η εκπαίδευση και η χρηματοδότηση των *contras*.³⁹

Η ομάδα των ειδικών διασαφηνίζει, πως υφίστανται κάποιες εξαιρέσεις αναφορικά με τον κανόνα αυτόν, οι οποίες αφορούν κυβερνοεπιχειρήσεις οι οποίες έχουν ως στόχο της συμμόρφωση του κράτους με το Διεθνές Δίκαιο, τη δημοσίευση στοιχείων τα οποία επικρίνουν απλά μία κατάσταση σε ένα κράτος, ενέργειες οι οποίες δεν εμπεριέχουν το στοιχείο του εξαναγκασμού, ενώ ακόμα και μία απλή ένδειξη ύπαρξης αυτού δεν είναι αρκετή για να οδηγήσει στη διαπίστωση ύπαρξης παραβίασης. Η έμφαση χρειάζεται, να δοθεί στην ύπαρξη συγκεκριμένου στόχου για τον επηρεασμό του αποτελέσματος, που θα είχε η πράξη αυτή αν τελούνταν χωρίς την επέμβαση του κράτους⁴⁰. Για ακόμη μία φορά και στην υπόθεση της Νικαράγουα το Δικαστήριο μίλησε παραθέτοντας συγκεκριμένες ενέργειες οι οποίες συνιστούσαν παραβίαση της αρχής της μη επέμβασης (χρηματοδότηση, εκπαίδευση κλπ.). Ομοίως και στον κυβερνοχώρο το στοιχείο αυτό είναι απαραίτητο προκειμένου να ενταχθεί η ενέργεια στον κανόνα.

Ένα ιδιαιτέρως ενδιαφέρον στοιχείο είναι αυτό το οποίο αφορά τη συμμετοχή ενός μη κυβερνητικού δρώντα στην παραβίαση, μέσω της παροχής βοήθειας σε αυτό

³⁷ Ibid: "the International Group of Experts agreed that the fact that the prohibition is often breached does not undermine the Rule as reflecting an extant principle of international law." p. 314

³⁸ Ibid p. 316

³⁹ Nicaragua vs USA Judgment: "The Court (...) Decides that the United States of America, by training, arming, equipping, financing and supplying the contra forces or otherwise encouraging, supporting and aiding military and paramilitary activities in and against Nicaragua, has acted, against the Republic of Nicaragua, in breach of its obligation under customary international law not to intervene in the affairs of another State; page 136

⁴⁰ Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 315-319

όμως απαραίτητως από κάποιο κράτος.⁴¹ Ένα πολύ πρόσφατο παράδειγμα τέτοιας ενέργειας το οποίο εμπεριέχει αυτά τα στοιχεία, μας έρχεται από τη Μέση Ανατολή. Πιο συγκεκριμένα στα μέσα Σεπτέμβρη πραγματοποιήθηκε μία μεγάλη κυβερνοεπιχείρηση η οποία είχε ως αποτέλεσμα την απενεργοποίηση των συστημάτων ασφαλείας και αναχαίτησης εχθρικών στόχων στις πετρελαϊκές εγκαταστάσεις της Aramco στη Σαουδική Αραβία. Της απενεργοποίησης των αμυντικών αυτών συστημάτων ακολούθησαν ρίψεις πυραύλων από drones οι οποίες προκάλεσαν μεγάλες ζημιές στον Σαουδαραβικό πετρελαϊκό κολοσσό. Οι υποψίες τις Δύσης αμέσως έπεσαν στο Ιράν, δεδομένης και της ήδη ταραγμένης κατάστασης ανάμεσα στους δύο σημαντικούς περιφερειακούς δρώντες. Την ευθύνη για την επίθεση ανέλαβαν όμως οι αντάρτες Χούθι της Υεμένης. Παρ' όλα αυτά οι υποψίες δεν έφυγαν από τι Ιράν, καθότι θεωρείται πως η Τεχεράνη είναι αυτή η οποία εξόπλισε τους αντάρτες, αλλά επιπρόσθετα οργάνωσε και κατηύθυνε την όλη επιχείρηση. Αποτέλεσμα, αυτής ήταν οι ζημιές που προεκλήθησαν, να προκαλέσουν ιδιαίτερα σοβαρό πρόβλημα όχι μόνο στην οικονομία του βασιλείου η οποία ως επί τω πλείστων βασίζεται στην παραγωγή και την εξαγωγή πετρελαίου, αλλά και στην παγκόσμια αγορά του μαύρου χρυσού.⁴²

Ας προσπαθήσουμε να απομονώσουμε αυτό το περιστατικό από την οπτική, που μας ενδιαφέρει, αυτήν της αρχής της μη επέμβασης, εστιάζοντας στις ενέργειες της Ιρανικής πλευράς. Ως δεδομένα πρέπει, να λάβουμε από τη μία τις ενέργειες της Σαουδικής Αραβίας η οποία τα τελευταία χρόνια εκτελούσε βομβαρδισμούς στη έδαφος της Υεμένης, στηρίζοντας την αυτοεξόριστο πλέον πρόεδρο της χώρας Χάαντι. Από την άλλη πλευρά οι αντάρτες Χούθι, δεν είναι η κυβέρνηση που ελέγχει αποτελεσματικά την Υεμένη, ενώ ταυτόχρονα ως μη κρατικοί δρώντες δεν έχουν το δικαίωμα, να χρησιμοποιούν βία ως απάντηση στις επιθέσεις της Σαουδικής Αραβίας, με χρήση δηλαδή του δικαιώματος στη Νόμιμη άμυνα.⁴³ Επιπρόσθετα, στο εσωτερικό της χώρας, η εμφύλια διαμάχη έχει πάρει εκρηκτικές διαστάσεις. Παρά

⁴¹ Ibid p. 320

⁴² DW, Drone attacks set Saudi Aramco oil facilities ablaze, Διαθέσιμο στη Διεύθυνση <https://www.dw.com/en/drone-attacks-set-saudi-aramco-oil-facilities-ablaze/a-50430391>

⁴³ EJIL: Talk, Mary Ellen O' Connell, Drone Attacks on Saudi Aramco Oil Installations, published September 17, 2019, Διαθέσιμο στη διεύθυνση <https://www.ejiltalk.org/drone-attacks-on-saudi-aramco-oil-installations/>

το ότι η Σαουδική Αραβία επενέβη μετά από πρόσκληση του νόμιμου προέδρου, εκείνος από το Μάρτιο του 2015 επί της ουσίας έχει απωλέσει τον αποτελεσματικό έλεγχο, απ' όταν η πρωτεύουσα καθώς και μεγάλο μέρος της ενδοχώρας βρίσκονται στα χέρια των Χούθις. Έτσι λοιπόν η νόμιμη κυβέρνηση η οποία έχει εξωθηθεί από άλλους εσωτερικούς παράγοντες, δεν είναι πλέον μία ισχυρή κυβέρνηση η οποία ασκεί τον αποτελεσματικό έλεγχο, που απαιτείται, και άρα δεν έχει την αρμοδιότητα «να προσκαλέσει» κάποια άλλη εξωτερική στρατιωτική βοήθεια.⁴⁴ Εάν κινηθούμε προς την κατεύθυνση της Δύσης και αποδεχθούμε, πως οι Χούθις υποστηρίζονται εν γένει από το Ιράν, το οποίο επιθυμεί μέσω αυτών, να λάβει τον πρώτο λόγο για την επόμενη μέρα στη χώρα, αλλά και το ότι ήταν η Τεχεράνη ο παράγων ο οποίος βρισκόταν πίσω από την οργάνωση και το συντονισμό των επιθέσεων στις εγκαταστάσεις της Aramco, συνθέτουμε ένα προφίλ το οποίο μας λέει, πως το Ιράν ενισχύει, εξοπλίζει και υποστηρίζει με κάθε μέσο τους αντάρτες της Υεμένης, επεμβαίνοντας σε ζητήματα, όπως είναι η διαμόρφωση της πολιτικής κατάστασης, τα οποία άπτονται της εσωτερικής δικαιοδοσίας της Υεμένης. Επιπρόσθετα, λαμβάνοντας υπόψιν τον παράγοντα «μη κρατικός δρών», προκειμένου να αποδοθεί ευθύνη στο Ιράν για τις επιθέσεις στις εγκαταστάσεις της Aramco, χρειάζεται σύμφωνα και με το Άρθρο 8, περί της ευθύνης των κρατών για Διεθνώς παράνομες πράξεις, να αποδειχθεί, πως οι Χούθις ενήργησαν κάτω από τις οδηγίες, την κατεύθυνση ή τον συγκεκριμένο έλεγχο της Ιρανικής κυβέρνησης.⁴⁵ (βλ. αναλυτικά την ενότητα 3.2)

Αν μπορούσαμε, να παραθέσουμε κάποια στοιχεία εν κατακλείδι προκειμένου, να ανακεφαλαιώσουμε τα προαναφερθέντα χρειάζεται, να εστιάζουμε στα εξής. Ακόμα και η απειλή κυβερνοεπιχείρησης, προκειμένου ένα κράτος να προβεί σε ενέργεια στην οποία δε θα προχωρούσε σε διαφορετική περίπτωση, αποτελεί απειλή για τη διεθνή ειρήνη και ασφάλεια και άρα παραβιάζει τον εν λόγω κανόνα.

⁴⁴ Ibid: "A government forced out by internal opposition forces is no longer a government in effective control. It has no authority to consent to or invite outside military assistance."

⁴⁵ Article 8, Articles on the Responsibility of States, for Internationally Wrongful Acts, βλ ενότητα 3.2

Ο εντοπισμός της έννοιας του coercion είναι απαραίτητη προϋπόθεση, ενώ παράλληλα η ενέργεια απαιτείται να αποδοθεί σε κρατικό δρώντα.⁴⁶

2.2.2.b: Intervention by the UN (Rule 67 – Tallinn Manual)

Σε αυτό το σημείο επιβάλλεται, να μιλήσουμε εκτενώς και για τις ενέργειες εκείνες οι οποίες ναι μεν αποτελούν επέμβαση, δεν αποτελούν όμως απαγορευμένη ενέργεια. Τέτοιες ενέργειες δε θα μπορούσαν, να είναι άλλες από εκείνες οι οποίες επιβάλλονται από το κυριότερο όργανο των Ηνωμένων Εθνών, το Συμβούλιο Ασφαλείας και μόνο κάτω από τις ρυθμίσεις του κεφαλαίου VII. Η ρύθμιση αυτή φυσικά αναφέρεται στην παράγραφο 2 του Άρθρου 7 του ΚΧ/ΗΗ.⁴⁷ Κατ' επέκταση ορθώς υιοθετείται με τον ίδιο τρόπο και από το εγχειρίδιο του Ταλλίν,⁴⁸ προκειμένου, να ρυθμίσει παρόμοιες ενέργειες στον κυβερνοχώρο, παρά το γεγονός πως τα κράτη εξακολουθούν, να χρησιμοποιούν την εν λόγω ρύθμιση για να αποτρέψουν ακόμη και την επέμβαση των Ηνωμένων Εθνών ιδίως όταν πρόκειται για κυβερνητικά συστήματα αλλά και εκλογές.⁴⁹ Σε αυτό το σημείο λοιπόν, χρειάζεται να προσδιορίσουμε τους τομείς εκείνους οι οποίοι άπτονται του κεφαλαίου VII του ΚΧ/ΗΕ.

Το Συμβούλιο Ασφαλείας θα αποφανθεί επί του ποια ενέργεια αποτελεί απειλή κατά της διεθνούς ειρήνης και ασφάλειας, διατάραξη αυτής ή επιθετική ενέργεια, σύμφωνα με το Άρθρο 39 του ΚΧ/ΗΕ.

⁴⁶ Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, "(...) a threat itself may violate this Rule. As with coercive acts, the threat must be coercive in nature and intrude into the internal or external affairs of another State (...) unlawful uses of force always qualify as acts of prohibited intervention. Threats of the unlawful use of force are also inherently interventions. P. 323-324"

⁴⁷ Article 2p7 UN Charter: (...) but this principle shall not prejudice the application of enforcement measures under Chapter VII.

⁴⁸ (...) does not include matters involving 'international peace and security', Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 325

⁴⁹ Ibid: p 325-327, Rule 67

2.2.2.b.1: Απειλή κατά της Διεθνούς Ειρήνης και Ασφάλειας (Threat to the peace)

Το ΣΑ θα εκτιμήσει πότε μία ενέργεια αποτελεί απειλή για τη διεθνή ειρήνη και ασφάλεια, όπως θα μπορούσε, να είναι για παράδειγμα μία επιθετική ενέργεια ενός κράτους σε ένα άλλο, με παραβίαση της εδαφικής ακεραιότητας του κράτους αυτού.⁵⁰

2.2.1.b.2: Διατάραξη της Διεθνούς Ειρήνης και Ασφάλειας (Breach of the peace)

Εχθροπραξίες δηλαδή ανάμεσα σε ένοπλες ομάδες δύο κρατών. (άσχετο το πότε τελειώνουν) καθώς και χρήση βίας από ή κατά μίας οντότητας, που όμως δεν αναγνωρίζεται ως κράτος (μη κρατικός δρών).⁵¹

2.2.1.b.3: Επιθετική ενέργεια (Act of Aggression)

Μελετάται η απευθείας χρήση βίας, η οποία χαρακτηρίζεται πάντα ως διατάραξη της ειρήνης, ή αλλιώς ένοπλη επίθεση σύμφωνα με το άρθρο 51 του ΚΧ/ΗΕ, δηλαδή χρήση του δικαιώματος της νόμιμης άμυνας.⁵²

το Συμβούλιο Ασφαλείας λοιπόν, μπορεί με την ενεργοποίηση του Άρθρου 40⁵³, να απαιτήσει τη συμμόρφωση των ενδιαφερόμενων μερών με προσωρινά μέτρα, όπως για παράδειγμα η απομάκρυνση στρατευμάτων των αντιμαχόμενων πλευρών πίσω από μη ακόμη διεθνώς αναγνωρισμένη συνοριακή γραμμή.⁵⁴ Πρόκειται για μέτρα, που το ίδιο ρυθμίζει, ελέγχοντας παράλληλα την εφαρμογή τους.

⁵⁰ Article 39 UN Charter: The Security Council shall determine the existence of any threat to the peace, (...)

⁵¹ Ibid: The Security Council shall determine the existence of any (...), breach of the peace (...)

⁵² Ibid: The Security Council shall determine the existence of any (...) act of aggression

⁵³ Article 40 of the Charter: In order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures.

⁵⁴ Bruno Simma, The Charter of the United Nations, a commentary, p 619

Όταν λοιπόν διαπιστωθεί, ότι τα κράτη δε συμμορφώθηκαν, το ΣΑ προχωρά στην επιβολή των μέτρων εκείνων υπό το Άρθρο 41 και 42, τα οποία μπορεί, να πάρουν τη μορφή συστάσεων, γεγονός εξαιρετικά σπάνιο. Ένα εύλογο ερώτημα, που εγείρει το ενδιαφέρον όλων, είναι κατά πόσο μία κρίση του ΣΑ για διάγνωση της υπάρχουσας κατάστασης, που σε πολλές περιπτώσεις εμπεριέχει πιθανότατα και αυξημένες δόσεις πολιτικής, αποτελούν νομιμοποιημένο κανόνα, τον οποίο τα κράτη θα πρέπει να τηρούν; Το ΣΑ λοιπόν, αποφαινεται μίας κατάστασης και προχωρά υπό το άρθρο 41⁵⁵ στην επιβολή κυρώσεων, που δεν περιλαμβάνουν τη χρήση βίας και έχουν τη μορφή που προαναφέραμε, μέτρα δηλαδή με δεσμευτικό χαρακτήρα για τα κράτη. Πιθανά τέτοια μέρη μπορεί να είναι η επιβολή εμπάργκο όπλων, το εμπάργκο πετρελαίου, η απαγορεύσεις πτήσεων, η απαγόρευση εισαγωγών εξαγωγών αλλά και οι έξυπνες κυρώσεις, αυτές δηλαδή που εφαρμόζονται δηλαδή αποκλειστικώς σε άτομα ή ομάδες ατόμων. Ένα χαρακτηριστικό παράδειγμα το οποίο έχει σχέση με την παρούσα εργασία είναι η περίπτωση του εμφυλίου πολέμου στη Λιβερία, γεγονός που άπτεται της εσωτερικής δικαιοδοσίας ενός κράτους. Στην περίπτωση αυτή όπως το ΣΑ/ΗΕ με το Ψήφισμα 788/1992⁵⁶, αποφάνθηκε πως ο πόλεμος αποτελούσε απειλή για την ειρήνη στη Δ. Αφρική και για το λόγο αυτό επέβαλλε εμπάργκο σε όλες τις μεταφορές όπλων σε όλη τη χώρα.

Πέρα όμως από το χαρακτηρισμό της κατάστασης και την υιοθέτηση των μέτρων, αυτό που έχει ιδιαίτερη σημασία και το ερώτημα, που προκύπτει, είναι, ποιός είναι ο μηχανισμός εκείνος, ο οποίος βεβαιώνει τη διεθνή κοινότητα, πως η εφαρμογή των μέτρων αυτών έχει δρομολογηθεί και άρα οι αποφάσεις τόσο του ΣΑ/ΗΕ όσο και των περιφερειακών οργανισμών τηρούνται; Το ρόλο αυτό λοιπόν αναλαμβάνουν ειδικά όργανα τα οποία εξουσιοδοτούνται από τα ΗΕ, όπως είναι

⁵⁵ Article 41 of the Charter: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations

⁵⁶ Res SC/UN 788/1992: "Decides, under Chapter VII (...)for the purposes of establishing peace and stability (...) implement a general and complete embargo on all deliveries of weapons and military equipment to Liberia until the Security Council decides otherwise.", Διαθέσιμο στη Διεύθυνση [https://undocs.org/S/RES/788\(1992\)](https://undocs.org/S/RES/788(1992))

για παράδειγμα οι ειδικές επιτροπές οι οποίες συστήνονται από το ΣΑ/ΗΕ και οι οποίες έχουν ως στόχο τους την επιτήρηση. Στο πλαίσιο αυτό τα κράτη με τη σειρά τους δεν μπορούν, να επικαλεσθούν αδυναμία εφαρμογής των μέτρων αυτών, δεν μπορούν να ισχυρισθούν ως κώλυμα την εθνική τους νομοθεσία, κάτι που τα καθιστά υπόλογα στα Ηνωμένα Έθνη. Ένα τέτοιο χαρακτηριστικό παράδειγμα κράτους, που προσπάθησε να ανακόψει την εφαρμογή των κυρώσεων ήταν οι ΗΠΑ, θεσπίζοντας νόμους, οι οποίοι παραβίαζαν τη συνθήκη για το εμπάργκο τη Ν Ροδεσία έπρεπε να το κάνουν κατά παραβίαση του ψηφίσματος και των όσων όριζε.⁵⁷

Τέλος το ΣΑ μπορεί να επιβάλει μέτρα τα οποία περιλαμβάνουν τη χρήση ένοπλης βίας υπό το Άρθρο 42 του ΚΧ/ΗΕ στην ξηρά τον αέρα και τη θάλασσα προκειμένου, να αποκατασταθεί, η διεθνής ειρήνη και ασφάλεια.⁵⁸ Ως στόχος μπορεί να τεθεί ακόμη και ο εξαναγκασμός του παραβάτη να απορρίψει την επιλογή της χρήσεως βίας ή ακόμα και να επιθεωρήσει τις ενέργειές του.⁵⁹

2.2.3: Η έννοια του espionage στον κυβερνοχώρο

Οι συνεχείς παράνομες ενέργειες, που παρατηρούνται στον κυβερνοχώρο θέτουν ιδιαίτερα σοβαρές προκλήσεις, κυρίως όσον αφορά την ασφάλεια. Η προστασία των απόρρητων κάθε είδους δεδομένων των κρατών αποτελεί τον βασικό παράγοντα θεμελίωσης της εθνικής τους ασφάλειας. Η συνεχής ανάπτυξη όμως του *innovation* προσφέρει στα κράτη εύκολους τρόπους επέμβασης μέσω της άσκησης κατασκοπείας, οι οποίοι παραβιάζουν το Διεθνές Δίκαιο και θέτουν προβληματισμούς γύρω από τα όρια, τα οποία τίθενται ως προς το σεβασμό της «αρχής της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους». Ο όρος λοιπόν

⁵⁷ Bruno Simma, *Commentary of the United Nations Charter*, Clarendon Press, 1995
Oxford University Press, "A state which cannot implement the measures to be taken according to Art. 41 because of its internal legal system is answerable to the UN.", p 626

⁵⁸ Article 42 UN Charter: (...) it may take such action (...) as may be necessary to maintain or restore international peace and security. (...)

⁵⁹ Bruno Simma, *Commentary of the United Nations Charter*, Clarendon Press, 1995
Oxford University Press, p 632

του cyber espionage, αναφέρεται σε ενέργειες οι οποίες λαμβάνουν χώρα σε περιόδους ειρήνης, μακριά από το ένοπλο επιχειρησιακό περιβάλλον μίας σύγκρουσης.

Ο ορισμός ο οποίος δίνεται για το συγκεκριμένο ζήτημα στο εγχειρίδιο του Τάλλιν, μιλά για κάθε ενέργεια που διεξάγεται με κρυφό τρόπο, είτε μέσω ψευδών προϋποθέσεων χρησιμοποιώντας κάθε είδους δυνατότητα στον κυβερνοχώρο προκειμένου να συλλέξει ή ακόμα και να διασπείρει πληροφορίες, συνήθως απόρρητες, παρανόμως και εν αγνοία του κατέχοντος την πληροφορία αυτή.⁶⁰

Προκειμένου να καταστεί το εν λόγω κεφάλαιο περισσότερο κατανοητό, χρειάζεται, να παραθέσουμε ένα σημαντικό παράδειγμα από το πρόσφατο παρελθόν. Το 2012 σε μία περίοδο, που είχε διαφανεί η αδυναμία των Ιρανικών συστημάτων να ανταποκριθούν θετικά σε ενέργειες των κακόβουλων λογισμικών Flame και Wiper (διάδοχοι Stuxnet). Πρόκειται για τα συστήματα του Υπουργείου Πετρελαίου της χώρας. Επιπρόσθετα, βρέθηκαν στο στόχαστρο η Κεντρική Τράπεζα, το Υπουργείο Πολιτισμού και πλατφόρμες γεώτρησης πετρελαίου.⁶¹

Η επίθεση αυτή στις Ιρανικές Εταιρείες Πετρελαίου, είχε ως αποτέλεσμα, να ενεργοποιηθούν οι κάμερες τα μικρόφωνα των υπολογιστών, να λαμβάνονται στιγμιότυπα οθόνης και παράλληλα, να δίνονται γεωγραφικές αναφορές για τα στοιχεία αυτά, τα οποία αποστέλλονταν στον παραβάτη μέσω Bluetooth. Τα στοιχεία έδειχναν πως πίσω από την επίθεση κρύβονταν αμερικανικές και ισραηλινές δυνάμεις. Παρ' όλα αυτά η ευθύνη επίσημα δεν αποδόθηκε ποτέ.⁶² Μία

⁶⁰ Rule 32 – Peacetime cyber espionage: 'cyber espionage' refers to any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information. It should be cautioned that the term is proffered here for the purposes of the Rule and has no independent legal significance., Michael Schmitt, *Tallinn Manual 2 on the international Law Applicable to Cyber Operations*, Cambridge University Press 2017.

⁶¹ Collin Anderson & Karim Sadjadjpour, *Iran's Cyber Threat, Espionage, Sabotage and Revenge*, Carnegie Endowment For International Peace, 2018, p. 10

⁶² Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace, Cyber Espionage and International Law (Russell Buchan)*, University of Melbourne, Edward Elgar 2017, p. 169

ακόμη σημαντική πληροφορία, η οποία ήρθε για να επιβεβαιώσει τις υποψίες ήταν οι αποκαλύψεις του Edward Snowden, πρώην υπαλλήλου της Εθνικής Υπηρεσίας Ασφαλείας, πως το Ιράν βρισκόταν στους συχνότερους στόχους στενής παρακολούθησης από τις ΗΠΑ.⁶³

Ένα από τα σημαντικότερα στοιχεία, που συνθέτουν το ζήτημα το οποίο περιγράφουμε είναι η ύπαρξη του «εξαναγκασμού», το σημαντικότερο συστατικό της αρχής της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους. Στην παραπάνω υπόθεση του 2012 που περιγράψαμε ενέχεται αυτό το στοιχείο, διότι πολύ απλά οι πληροφορίες αυτές διαρρέουν χωρίς τη σύμφωνη γνώμη του κράτους – θύματος. Δηλαδή αν ήταν στη διακριτική του ευχέρεια, οι πληροφορίες αυτές δε θα κοινοποιούνταν ποτέ.⁶⁴ Παρενθετικά χρειάζεται, να κάνουμε μία αναφορά στην πλειοψηφούσα γνώμη των ερευνητών του εγχειριδίου το Τάλλιν, οι οποίοι σημειώνουν σε αντίθεση με όσα αναφέραμε, υποστηρίζουν, πως ο κανόνας 66 αναφορικά με την απαγόρευση της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους, φαίνεται να μην έχει εφαρμογή ως προς το ζήτημα της κατασκοπείας, μια και «εκλείπει» το στοιχείο του εξαναγκασμού.⁶⁵ Ειδικότερα όταν η παραβίαση γίνεται από ξένους – αλλοδαπούς χρήστες τότε υφίσταται και παραβίαση της δικαιοδοσίας του κράτους. Το ουσιώδες ζήτημα εδώ και λαμβάνοντας υπόψιν τα απροσδιόριστα σύνορα του κυβερνοχώρου, είναι το γεγονός, πως η επιβολή κανόνων εθνικής φύσεως σε παραβάτες οι οποίοι βρίσκονται εκτός της δικαιοδοσίας του κράτους εναντίον του οποίου παρανόμησαν ή υπάρχουν υποψίες, πως θα παρανομήσουν, είναι εξαιρετικά δύσκολη.⁶⁶

Έχει διατυπωθεί και η άποψη, η οποία υποστηρίζει, πως μέσω αυτού του είδους κατασκοπίας τα κράτη έχοντας πρόσβαση σε απόρρητες πληροφορίες,

⁶³ Ibid 61: p. 58

⁶⁴ Ibid: p. 171

⁶⁵ “Cyber espionage per se, as distinct from the underlying acts that enable the espionage (...), does not qualify as intervention because it lacks a coercive element.” Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p 323

⁶⁶ Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Cyber Espionage and International Law (Russell Buchan), University of Melbourne, Edward Elgar 2017: p. 172

αντιλαμβάνονται τις προθέσεις των άλλων κρατών, αλλά παράλληλα τίθεται και η άποψη πως μέσω της τακτικής αυτής υπεισέρχεται μία ισορροπία και σε εσωτερικό επίπεδο, μιας και διαμορφώνονται σε άλλες βάσεις η εξωτερική πολιτική και η πολιτική ασφαλείας.⁶⁷ Όπως επισημάναμε όμως και σε προηγούμενο κεφάλαιο, η σύγχρονη διεθνής κοινωνία θεμελιώθηκε πάνω στην αρχή της κρατικής κυριαρχίας και της ισότητας της κυριαρχίας αυτής για όλα τα κράτη.⁶⁸ Μία αρχή η οποία συμπληρώθηκε και ενισχύθηκε μέσω και των άρθρων 2π4 για το σεβασμό της απαγόρευσης χρήσης βίας, αλλά και του 2π7 για την αρχή της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους, στην οποία και εστιάζουμε.

Αυτομάτως ο συλλογισμός μας, μας οδηγεί στην πραγμάτωση ενεργειών οι οποίες ανάλογα με την έντασή τους αποτελούν απειλή ή διατάραξη για τη διεθνή ειρήνη και ασφάλεια, όπως χαρακτηριστικά προσδιορίζει το Άρθρο 39 του ΚΧ/ΗΕ. Για το Δίκαιο λοιπόν τέτοιες μέθοδοι παραβιάζουν βασικές και θεμελιώδεις του αρχές. Από την άλλη το φλέγον ζήτημα της εθνικής ασφαλείας, μοιάζει, να θεωρεί τις μεθόδους αυτές σαν κάποιου είδους μονόδρομο προκειμένου, να προασπιστεί το εθνικό συμφέρον. Έχει διατυπωθεί η αντίληψη πως ρυθμίσεις ασφαλείας σε διεθνές επίπεδο είναι αποτέλεσμα της απομάκρυνσης, που έχει επέλθει. Κατά συνέπεια, αυτό που προτείνεται, είναι πως η χρήση της κατασκοπείας ως μέσου επίτευξης στόχων, θα οδηγήσει τους διεθνείς δρώντες σε διαπραγματεύσεις, προκειμένου να καταλήξουν σε συμβατικά κείμενα, σε ένα χώρο ιδιαιτέρως φτωχό ως προς το νομικό πλαίσιο που το καλύπτει.⁶⁹ Η απλούστερη εξήγηση που δίνεται ως προς αυτό είναι πως η προσπάθεια λήψης εμπιστευτικών πληροφοριών από τα

⁶⁷ Ibid p.173-175

⁶⁸ Article 2 p1: "The Organization is based on the principle of the sovereign equality of all its Members", UN Charter

⁶⁹ Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, American University International Law Review, Volume 19, Issue 5, Article 2, 2003, p. 1108-1112

κράτη επί της ουσίας χρησιμεύει, στο να επαληθεύσουν, αν τα κράτη που δέχονται την επέμβαση, έχουν συμμορφωθεί ή όχι με τις διεθνείς τους υποχρεώσεις.⁷⁰

Όπως προ είπαμε όμως η Διεθνής Κοινωνία όντας βασισμένη στο σεβασμό της αρχής της κυριαρχίας, χρειάζεται να καταγγείλει μέσω της αρχής της μη επέμβασης, ενέργειες όπως η διαρροή απόρρητων στοιχείων, όταν αυτό βέβαια γίνεται ενέχοντας το απαραίτητο στοιχείο του εξαναγκασμού.⁷¹ Με τον όρο coercion αναφερόμαστε σε οποιαδήποτε ενέργεια αποδεικνύεται πως είναι αποτέλεσμα χειραγώγησης –κατεύθυνσης.⁷² Κάποιοι από την άλλη πλευρά υποστηρίζουν τη μη ύπαρξη παραβίασης, από τη στιγμή που το κράτος αποδέκτης δεν έχει γνώση της πράξεως που διεξάγεται.⁷³ Αυτό σαφέστατα αποτελεί μία ιδιαίτερα περιορισμένη ερμηνεία της αρχής της μη επέμβασης.⁷⁴ Λαμβάνοντας υπόψιν την ιδιαιτερότητα του κυβερνοχώρου, είναι ιδιαίτερα αφελές, να απαιτούμε από το δέκτη της παράνομης ενέργειας την απόδοση πως έλαβε γνώση, προκειμένου να αναιρέσουμε την παράνομη φύση της ενέργειας. Εν τέλει, απαιτείται να αποδειχθεί η ύπαρξη κράτους πίσω από το δράστη, προκειμένου να αποδοθεί η ευθύνη.⁷⁵

⁷⁰ Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace, Cyber Espionage and International Law (Russell Buchan)*, University of Melbourne, Edward Elgar 2017, p. 176

⁷¹ Russell Buchan, *The International Legal Regulation of State – Sponsored Cyber Espionage, International Legal Norms, Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016, p. 73

⁷² Ibid p. 77, “Following on from this decision there seems to be near consensus within academic literature that coercion requires the imposition of ‘imperative pressure’⁶⁵ which manipulates the will of the state in order for the entity exercising coercion to realize certain objectives or, in Oppenheim’s famous and often quoted formulation, intervention is ‘dictatorial interference’”

⁷³ Ibid Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace, Cyber Espionage and International Law (Russell Buchan)*, University of Melbourne, Edward Elgar 2017 p. 183

⁷⁴ Ibid p. 183

⁷⁵ Βλ. κεφάλαιο 3, περί προσδιορισμού της έννοιας απόδοσης ευθύνης για παράνομη ενέργεια

2.2.4.: Η έννοια της άσκησης δικαιοδοσίας και η εφαρμογή της στον κυβερνοχώρο

Μιλώντας για εθνική κυριαρχία, αναφερόμαστε στη δυνατότητα του κράτους να ασκεί εξουσία επί όλων των ατόμων, που διαβιούν στην επικράτειά του. Πιο συγκεκριμένα, μιλάμε για τη δυνατότητα των κεντρικών αρχών ενός κράτους να ασκούν τις κάθε είδους δημόσιες λειτουργίες επί όλων των ατόμων που διαβιούν σε μία καθορισμένη επικράτεια.⁷⁶ Ας μη λησμονούμε και όσα προαναφέραμε μιλώντας εκτενώς για τον ορισμό ακόμα ακόμα της έννοιας του κράτους, τονίζοντας, πως ένα από τα ουσιαστικά χαρακτηριστικά, που πρέπει, να έχει προκειμένου, να θεωρείται υποκείμενο της Διεθνούς κοινωνίας και του δικαίου, είναι, να έχει μία κυρίαρχη κυβέρνηση, η οποία θα ασκεί τον απαιτούμενο αποτελεσματικό έλεγχο στα άτομα, που διαβιούν εντός της επικράτειάς του. Με βάση το εν λόγω κριτήριο, τα κράτη λοιπόν έχουν τη δυνατότητα, να ρυθμίζουν μέσω της θέσπισης νομοθεσίας τον τρόπο λειτουργίας της εν λόγω οντότητας, κανόνες οι οποίοι είναι δεσμευτικοί και απαιτείται, να γίνονται σεβαστοί από όλους⁷⁷. Επιπρόσθετα, εντοπίζεται και η δυνατότητα της δικαιοδοτικής δικαιοδοσίας η οποία έχει ως βάση της την εδαφικότητα και την ιθαγένεια του θύτη, σύμφωνα με την οποία το κράτος μπορεί, να φέρει ενώπιον της δικαιοσύνης άτομο το οποίο διέπραξε παράνομες πράξεις στο εξωτερικό, ή ενέργειες, που συνιστούν διεθνές έγκλημα.⁷⁸

Εδώ λοιπόν έγκεινται και οι δυσκολίες, που διαφαίνονται ως προς αυτό στον κυβερνοχώρο. Η καινοτομία, η ανάπτυξη της τεχνολογίας και τα ακαθόριστα σύνορα, καθιστούν μία σαφή ερμηνεία της έννοιας αλλά και της άσκησής της αδύνατη. Ποια είναι τα όρια των χρηστών του διαδικτύου. Μπορούν, να θεσπιστούν όρια σε ένα χώρο, όπου όλοι μπορούν, να έχουν πρόσβαση; Σαφέστατα δημιουργείται μία σύγχυση και τα όρια ανάμεσα στην υπακοή στον εθνικό νόμο, και το άκρο του περιορισμού της ελευθερίας σκέψης κι έκφρασης μοιάζει να

⁷⁶ Antonio Cassese, Διεθνές Δίκαιο, Αθήνα, Εκδόσεις Gutenberg, 2012, σ. 66

⁷⁷ Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015, p. 33

⁷⁸ Ibid: p. 67

βρίσκεται στο επίκεντρο της συζήτησης ανάμεσα στους online χρήστες και τα κράτη.⁷⁹

Προκειμένου, να μιλήσουμε πιο συγκεκριμένα αναφορικά με τη δικαιοδοσία στον κυβερνοχώρο χρειάζεται, να διερευνήσουμε τις αρχές που τη διέπουν. Η πρώτη φυσικά αφορά την εδαφικότητα, σχετικά με τον έλεγχο τον οποίο ασκεί στην εν λόγω επιφάνεια το κράτος με βάση την αρχή της κυριαρχίας και κατ' αυτόν τον τρόπο ορίζεται η κατανομή του ελέγχου, σε σχέση με διακρατικά συμβάντα, προκειμένου να γίνει αντιληπτό, ποιο κράτος είναι αυτό το οποίο, είναι άρρηκτα συνδεδεμένο με το γεγονός, προκειμένου να προχωρήσει η δίκαιη μεταχείριση των εμπλεκομένων, προστατεύοντας και εκπροσωπώντας τους, με τα περιστατικά ταυτόχρονων αξιώσεων διεθνούς δικαιοδοσίας να μην είναι λίγα, ούτε σπάνια.⁸⁰

Σε πρώτο βαθμό επιβάλλεται, να διασαφηνίσουμε τους τρεις τομείς άσκησης της κρατικής δικαιοδοσίας, οι οποίοι εστιάζουν ως επί τω πλείστων στην εδαφικότητα.⁸¹ Αρχικά λοιπόν, σε ένα πρώτο επίπεδο μιλάμε για τη νομοθετική ή ρυθμιστική δικαιοδοσία, η οποία δίνει τη δυνατότητα σε ένα κράτος, να θεσπίζει τους νόμους εκείνους οι οποίοι δεσμεύουν τους πολίτες οι οποίοι διαβιούν τόσο στο εσωτερικό της χώρας, τόσο και στο εξωτερικό και μπορεί να προβούν σε ενέργειες οι οποίες ενδέχεται να βλάψουν το εν λόγω κράτος.⁸² Επιβάλλεται, οι κανόνες αυτοί να μην παραβιάζουν την κυριαρχία άλλων κρατών, όπως ορίζει το άρθρο 1 του ΚΧ/ΗΕ το οποίο αναφέρεται στο σεβασμό της κυρίαρχης ισότητας ανάμεσα στα κράτη. Έπειτα, η εκτελεστική δικαιοδοσία επιτρέπει στο κράτος να λαμβάνει τα μέτρα εκείνα, κυρίως μέσω της διοίκησης, τα οποία θα φέρουν σε πέρας τη νομοθετική εντολή. Σε ένα άλλο στάδιο η δικαστική δικαιοδοσία δίνει στο

⁷⁹ Uta Kohl, Jurisdiction in cyberspace, *Research Handbook on International Law and Cyberspace*, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015, p. 30

⁸⁰ Ibid 69, "(...) looking at which State or legal system is sufficiently closely linked or connected to a transnational event (...)" p. 33

⁸¹ Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations – Cambridge University Press, 2017, "Since sovereignty is predominantly territorial under international law, the most common basis for the exercise of jurisdiction is territoriality." p 52

⁸² Antonio Cassese, Διεθνές Δίκαιο, Αθήνα, Εκδόσεις Gutenberg, 2012, σ. 66 - 67

κράτος τη δυνατότητα, να φέρει ενώπιον των εθνικών του δικαστηρίων άτομα και φορείς ώστε, να λυθούν οι προκείμενες διαφορές.

Πέραν όμως από τη θέσπιση μίας γενικής απαγόρευσης για τα κράτη, να μην μπορούν, να επεκτείνουν τη νομοθετική και δικαστική τους εξουσία σε φορείς και πρόσωπα εκτός της επικράτειάς τους, έχουν μία διακριτική ευχέρεια, η οποία περιορίζεται μόνο από απαγορευτικούς κανόνες, όπως είναι για παράδειγμα η εφαρμογή μίας απόφασης, η οποία θα αποτελεί παραβίαση της αρχής της μη επέμβασης στα εσωτερικά ενός κράτους, με τις υπόλοιπες ρυθμίσεις να επαφίενται τις οποίες θεωρεί καλύτερες και καταλληλότερες.⁸³ Κατά πόσο όμως μία θεωρία η οποία βασίζεται στο «ό,τι δεν απαγορεύεται, επιτρέπεται», μπορεί να σταθεί και να ευδοκιμήσει σε διεθνές επίπεδο;⁸⁴ Μία χαρακτηριστική υπόθεση από την εποχή ακόμα ακόμα του ΔΔΔΔ, ήταν η υπόθεση Lotus η οποία με την απόφαση η οποία πάρθηκε από το δικαστήριο δεν απέδωσε αποκλειστική αρμοδιότητα στη χώρα της οποία της σημαία έφερε το πλοίο Lotus, ως προς την παραπομπή σε δίκη για τον πλοίαρχο που ήταν επί τω έργω την ώρα του ατυχήματος, το οποίο έφερε τη Γαλλική σημαία και το οποίο έπλεε σε Διεθνή ύδατα, με το επιχείρημα πως δεν υφίσταται τέτοιος κανόνας στο Διεθνές Δίκαιο. Το Δικαστήριο λοιπόν υποστήριξε, πως «ο πρώτος και κυριότερος περιορισμός που επιβάλλεται από το διεθνές δίκαιο στο κράτος είναι ότι, δεν μπορεί να ασκήσει την εξουσία του υπό οποιαδήποτε μορφή στο έδαφος άλλου κράτους. Άρα αυτό μας οδηγεί στο συμπέρασμα, πως η δικαιοδοσία παίρνει αποκλειστική μορφή εδαφικότητας. Αυτό όμως δε σημαίνει, πως το διεθνές δίκαιο απαγορεύει σε ένα κράτος να ασκεί δικαιοδοσία στην επικράτειά του, σε σχέση με οποιαδήποτε πράξη έλαβε χώρα στο εξωτερικό. Μια τέτοια άποψη θα ήταν εφικτή μόνο, αν από το διεθνές δίκαιο υπήρχε μία ρητή απαγόρευση, ως προς την επέκταση της νομοθετικής ή δικαστικής δικαιοδοσίας τους εκτός των συνόρων τους»⁸⁵, κάτι που την περίοδο εκείνη δεν υπήρχε.

⁸³ Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015, "(...) it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; (...), p 36

⁸⁴ Ibid p. 37

⁸⁵ The Case of the SS "Lotus" (n 19) 18.

Ωστόσο, αυτό δεν συμβαίνει στο πλαίσιο του διεθνούς δικαίου, όπως ισχύει σήμερα, μιας και το 1958 με τη Σύμβαση για την Ανοιχτή Θάλασσα όπου στο Άρθρο 11 δίνεται έμφαση στο γεγονός, πως μόνο το κράτος σημαίας, ή αυτό του οποίου ο δράστης είναι υπήκοος, έχει δικαιοδοσία επί των ατόμων αναφορικά με ένα συμβάν στην ανοιχτή θάλασσα.⁸⁶ Επιπλέον, «η αρχή του κράτους σημαίας» εφαρμόστηκε και στη Σύμβαση των Ηνωμένων Εθνών για το Δίκαιο της Θάλασσας και πιο συγκεκριμένα στο Άρθρο 92.⁸⁷ Λαμβάνοντας υπόψιν την ιδιαιτερότητα του κυβερνοχώρου, εύκολα μπορούμε να σκεφτούμε, πως στην περίπτωση της «εξωεδαφικής» εφαρμογής της δικαιοδοσίας πολύ πιθανό, να προέκυπταν ζητήματα νομιμότητας.⁸⁸

Η αρχή αυτή, βασισμένη στην ενεργητική και την παθητική δικαιοδοσία εστιάζει ακόμα και στην εκδίκαση υποθέσεων, που αν και διεπράχθησαν στο εξωτερικό είναι επιβλαβή για τα εθνικά συμφέροντα ή επιδρούν σε αυτά σοβαρά.⁸⁹ Υπάρχει και η νομική κάλυψη για άσκηση οικουμενικής δικαιοδοσίας στις περιπτώσεις όπου διαπράττονται διεθνή εγκλήματα, όπως είναι αυτό της τρομοκρατίας ή του smuggling.⁹⁰ Ο Antonio Cassese έρχεται μέσω της αναφοράς του στην κατασταλτική δικαιοδοσία, να μιλήσει για ενέργειες, που άπτονται περιστατικών που λαμβάνουν χώρα στο εσωτερικό μίας χώρας. Τονίζεται λοιπόν, πως τέτοιου είδους δικαιοδοσία δεν μπορεί, να ασκηθεί από ένα κράτος εκτός της επικράτειάς του.⁹¹

Αναφορικά λοιπόν, με την εν λόγω κατάσταση η οποία φαίνεται, να βρίσκει παρόμοια εφαρμογή και στον κυβερνοχώρο το όλο ζήτημα θα πρέπει συνεπώς, να

⁸⁶ Article 11 of the Convention on the High Seas “3. No arrest or detention of the ship, even as a measure of investigation, shall be ordered by any authorities other than those of the flag State.”, Διαθέσιμη στη Διεύθυνση https://www.gc.noaa.gov/documents/8_1_1958_high_seas.pdf, ανάκτηση 15/12/2019 authorities other than those of the flag State.

⁸⁷ Article 92 “ The status of Ships” of the Convention of The United Nations on the Law of the Sea, Διαθέσιμη στη Διεύθυνση https://www.https://www.gc.noaa.gov/documents/8_1_1958_high_seas.pdfun.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf Ανάκτηση 15/12/2019

⁸⁸ Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015 p 37-38

⁸⁹ Antonio Cassese, Διεθνές Δίκαιο, Αθήνα, Εκδόσεις Gutenberg, 2012 p.67

⁹⁰ Ibid

⁹¹ Ibid p. 68

εστιαστεί στην ενεργητική και την παθητική δικαιοδοσία, όπως προαναφέραμε. Με την πρώτη δηλαδή εστιάζουμε στην εδαφικότητα, το κομμάτι εκείνο εντός του οποίου διενεργείται η πράξη και την παθητική δικαιοδοσία με την οποία αναφερόμαστε στην ιθαγένεια του προσώπου του άμεσα εμπλεκόμενου. Κατ' αυτόν τον τρόπο λοιπόν μπορεί να προκύψει το φαινόμενο της διττής δικαιοδοσίας, αναφορικά με τη περιοχή στην οποία συντελείται η πράξη, αλλά με τη διαφορετική ιθαγένεια την οποία μπορεί να έχει ο θύτης. Μπορούν δηλαδή, με αυτόν τον τρόπο να ασκήσουν δικαιοδοσία επί της πράξεως αυτής πάνω από ένα κράτη.⁹²

Αυτό που κάνει τη συμβατική ερμηνεία και συζήτηση περί δικαιοδοσίας, να διαφέρει στον κυβερνοχώρο, είναι το γεγονός, πως οι κυβερνοεπιχειρήσεις μπορούν, να προέρχονται από οπουδήποτε στον πλανήτη και μέσω της μεγάλης ταχύτητας, να διαπερνούν πολύ εύκολα σύνορα και τα αποτελέσματα των ενεργειών αυτών, να επηρεάζουν πάνω από ένα κράτη. Κατ' αυτόν τον τρόπο η το ζήτημα της αναζήτησης δικαιοδοσίας αναφορικά με μία ενέργεια, αποκτά προβλήματα εντοπιότητας. Έτσι λοιπόν η Συνθήκη της Βουδαπέστης του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα, αναφέρει στο άρθρο 22 πως εκτός της υποχρέωσης που έχουν τα κράτη, να εγκαθιστούν τη δικαιοδοσία τους, τόσο στην επικράτειά τους, στα πλοία που φέρουν τη σημαία τους, στα αεροσκάφη που υπάγονται σε αυτό και όχι μόνο⁹³, σε περιπτώσεις όπου διαφαίνεται, να εμπίπτει με εκείνη άλλων κρατών επιβάλλεται, να διαλεχθεί με τα άλλα κράτη, προκειμένου να «καθορίσουν την ενδεδειγμένη δικαιοδοσία για δίωξη»⁹⁴. Αν θέλουμε λοιπόν, να φέρουμε ένα παράδειγμα το οποίο θα χαρακτήρισε αυτού του είδους την πολλαπλή δικαιοδοσία, θα μπορούσαμε να φέρουμε στο μυαλό μας έναν πολίτη με Βρετανική ιθαγένεια, που βρίσκεται στη Γαλλία και μέσω των πράξεών του χρησιμοποιεί διακομιστή ο οποίος βρίσκεται στην Ελλάδα, προκειμένου να συλλέξει απόρρητες πληροφορίες του Τουρκικού Υπουργείου

⁹² Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations – Cambridge University Press, 2017, p.52

⁹³ Article 22 of the Convention on Cybercrime, Budapest 2001, paragraph 1, Διαθέσιμη στη Διεύθυνση <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

⁹⁴ Ibid: paragraph 5, (...) the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. (...)

Εξωτερικών.⁹⁵ Σε αυτήν την περίπτωση λοιπόν η μόνη ουσιαστική λύση είναι αυτή της Διεθνούς Συνεργασίας, προκειμένου, να επέλθει η ποινική καταστολή, όπως καταδεικνύει και το κανόνας 13 του εγχειριδίου του Τάλλιν.⁹⁶

Η ομάδα εμπειρογνομόνων του εγχειριδίου του Ταλλίν ήρθαν να διασαφηνίσουν λεπτομερώς τις περιπτώσεις δικαιοδοσίας και να θέσουν τα όρια εκείνα για τη διεξαγωγή των εκάστοτε ενεργειών, μιας και λόγω της ιδιαιτερότητας του κυβερνοχώρου, ένα πιο συγκεκριμένο πεδίο εφαρμογής, μόνο θετικό θα μπορούσε να χαρακτηριστεί για τη χάραξη του τρόπου λειτουργίας από τα κράτη αναφορικά με το εν λόγω θέμα. Κάτι που χρειάζεται, να διασαφηνίσουμε είναι, πως υπάρχουν περιπτώσεις, όπως αυτές των παρόχων υπηρεσιών, οι οποίοι υποκρύπτουν την τοποθεσία τους, προκειμένου να αποφευχθεί ο εντοπισμός τους από έναν ξένο νόμο⁹⁷, οποίος μπορεί να τους θέτει υπό τη δικαιοδοσία του κράτους καταγωγής του εν λόγω νόμου, σε περιπτώσεις όπου προβαίνουν σε ενέργειες οι οποίες το επηρεάζουν. Ως προς αυτήν την κατεύθυνση απεφάνθη και το ΔΔΔΔ στην υπόθεση Lotus, λέγοντας, πως το κράτος στο οποίο η ξένη δραστηριότητα έλαβε χώρα, έχει το δικαίωμα να της επιληφθεί, ακόμη κι όταν αναφερόμαστε στο αποτέλεσμα της ενέργειας αυτής.⁹⁸

Ξεκινώντας από τη δικαιοδοσία με βάση το κριτήριο της εδαφικότητας, υπάρχουν τρεις περεταίρω παράμετροι οι οποίοι χρειάζεται, να τονιστούν σύμφωνα και με τον ένατο κανόνα του εγχειριδίου του Ταλλίν. Αρχικά λοιπόν, χρειάζεται, να τονιστεί η ταύτιση σε μεγάλο βαθμό της εδαφικότητας με την έννοια της κυριαρχίας και κατ' επέκταση της κυρίαρχης ισότητας των κρατών, αρχές θεμελιώδεις οι οποίες

⁹⁵ Η ονομαστική αναφορά στα εν λόγω κράτη, γίνεται προς διευκόλυνση κατανόησης του εν λόγω παραδείγματος.

⁹⁶ Rule 13 – International cooperation in law enforcement. (...) such cooperation may be required by the terms of an applicable treaty or other international law obligation., Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations – Cambridge University Press, 2017, p 75

⁹⁷ Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015 p 40

⁹⁸ The Case of the SS 'Lotus' "(...) to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there." 23

αναγράφονται ρητώς και στον καταστατικό χάρτη των Ηνωμένων Εθνών. Η εδαφική δικαιοδοσία λοιπόν, αναφέρεται σε φυσικά και νομικά πρόσωπα αλλά και σε δεδομένα τα οποία βρίσκονται στη συγκεκριμένη επικράτεια και έχει ισχύ ακόμη και στην ελάχιστη ανάμειξη του κράτους, που μπορεί να είναι η απλή διέλευση των δεδομένων (τα οποία μπορεί να υποκλέπτονται από κάποιον χρήστη παρανόμως σε ένα άλλο κράτος) από την επικράτειά του. Επιπρόσθετα, στην ίδια κατηγορία εναπόκεινται και οι ενέργειες οι οποίες ξεκινούν και ολοκληρώνονται εντός της επικράτειας του κράτους αυτού (αντικειμενική εδαφικότητα κανόνας 57 εγχειριδίου του Ταλλίν). Υπάρχει η πιθανότητα πολλά κράτη, να καλούνται, να ασκήσουν εδαφική δικαιοδοσία κι αυτό στις περιπτώσεις όπου η κακόβουλη ενέργεια θέτει ως στόχο μεγαλύτερο αριθμό κρατών. Η δυσκολία έγκειται στις περιπτώσεις όπου λόγω της χρήσεως των δυνατοτήτων της τεχνολογίας καθίσταται ιδιαίτερα δύσκολο, να εντοπιστεί επακριβώς κάποιο συγκεκριμένο σημείο, το οποίο να πληροί τα κριτήρια της εδαφικότητας. Ακόμα, σε επιχειρήσεις όπου εμπλέκονται ιδιώτες τρίτων κρατών των οποίων τα δικαιώματα θίγονται από τη διεξαγωγή επιθέσεων, για παράδειγμα στη βάση δεδομένων μιας εταιρείας, τα τρίτα αυτά κράτη δεν μπορούν, να θεωρήσουν, πως μπορούν, να ασκήσουν κάποιου είδους δικαιοδοσία.⁹⁹ Διαφαίνεται λοιπόν, πως διεθνείς δρώντες καταφέρνουν να απομακρύνουν από το κράτος την αποκλειστική αρμοδιότητα του ελέγχου των απόρρητων πληροφοριών.¹⁰⁰

Στη συνέχεια περνάμε σε ένα άλλο επίπεδο, πιο έμμεσης δικαιοδοσίας, αν μας επιτρέπεται, να τη χαρακτηρίσουμε έτσι, η οποία αφορά αεροσκάφη και πλοία τα οποία φέρουν τη σημαία του εν λόγω ενδιαφέροντος κράτους. Πιο συγκεκριμένα εστιάζουμε στην προσπάθεια των κρατών να «παρακολουθήσουν» τις ενέργειές τους, ακόμη κι αν βρίσκονται εκτός της επικράτειάς τους για ενέργειες οι οποίες έχουν αποτέλεσμα και πεδίο εφαρμογής εντός του κράτους. Όλα αυτά έχουν ουσία, καθώς όπως επισημαίνει η ομάδα των εμπειρογνομόνων του εγχειριδίου του Ταλλίν, χρειάζεται, να υπάρχει η απαραίτητη ισορροπία ανάμεσα στο κράτος το

⁹⁹ Ibid p. 55-60

¹⁰⁰ Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015, p. 31

οποίο θέλει, να ρυθμίζει τις δραστηριότητες στον κυβερνοχώρο και αλλά και στο μέλημα των άλλων κρατών να διατηρούν αλώβητη την κυριαρχία τους. Κατά κάποιον τρόπο λοιπόν η επέκταση άσκησης δικαιοδοσίας μπορεί, να προκαλέσει προβλήματα ως προς το σεβασμό της ισότητας της κυριαρχίας για όλα τα κράτη. Μπορεί να έχουν αποκτήσει τη δυνατότητα να επεκτείνουν τη δικαιοδοσία τους και εκτός των συνόρων τους, γεγονός που δεν καθιστά νόμιμη την επιβολή της δικαιοδοσίας τους με κάθε τρόπο. Αυτό αποτελεί μία δικλείδα ασφαλείας από το Διεθνές Δίκαιο για τα κράτη, προκειμένου να προστατεύονται από την επέμβαση τρίτων κρατών σε ζητήματα τα οποία άπτονται της δικής τους εσωτερικής δικαιοδοσίας.¹⁰¹

Σύμφωνα, λοιπόν με την παράγραφο ένα του δέκατου άρθρου το εγχειριδίου του Ταλλίν, αυτό μπορεί, να γίνει επεκτείνοντας την εσωτερική του νομοθεσία στη συμπεριφορά των υπηκόων του στο εξωτερικό, ενώ δεν είναι λίγες οι περιπτώσεις όπου τα κράτη καταφεύγουν σε αυτές τις ενέργειες και για αλλοδαπούς, που παρέμειναν για μικρό χρονικό διάστημα στο εν λόγω κράτος. Άρα σε αυτό το σημείο αντιλαμβανόμαστε τη σημασία της εθνικότητας η οποία ρυθμίζεται από τη σχέση του φυσικού και του νομικού προσώπου με το κράτος.¹⁰² Αναφερόμενοι λοιπόν στην παράγραφο ένα η οποία κάνει λόγο για ένοπλες δυνάμεις, τονίζεται, πως αυτές ως σώμα αποτελούν αναπόσπαστο κομμάτι του κράτους του οποίου φέρουν τη σημαία, ανεξαρτήτως της επιμέρους ιθαγένειας των ατόμων, που την αποτελούν. Έτσι λοιπόν το κράτος αυτό έχει τη δικαιοδοσία ελέγχου των κάθε είδους ενεργειών, όπως η οργάνωση ή η πραγμάτωση μίας κυβερνοεπιχείρησης, που θα έχει ως αφετηρία το πλοίο το οποίο φέρει τη σημαία του κράτους αυτού.¹⁰³ ¹⁰⁴ Χρειάζεται φυσικά, να τονίσουμε, πως ακόμα και το αποτέλεσμα μία πράξης, όπως για

¹⁰¹ Ibid 51-52

¹⁰² Case concerning Barcelona Traction Lights and Power Company, Ltd. P 70

¹⁰³ Ibid 104 p. 63

¹⁰⁴ Law of the Sea Convention, Art. 92(1), "Ships shall sail under the flag of one State only and save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas. A ship may not change its flag during a voyage or while in a port of call, save in the case of a real transfer of ownership or change of registry, Διαθέσιμο στη Διεύθυνση https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

παράδειγμα, ο επηρεασμός ενός εκλογικού αποτελέσματος ρυθμίζει αντίστοιχα το ζήτημα της δικαιοδοσίας.

Σε ένα άλλο σημείο ερχόμαστε στην εφαρμογή της εξωεδαφικής δικαιοδοσίας η οποία όμως σε καμία περίπτωση δεν πρέπει, να έρχεται σε ρήξη με το συμβατικό διεθνές δίκαιο. Η πλειοψηφία των περιπτώσεων αυτών πραγματώνεται μέσω ενεργειών σύμφωνα με το Δίκαιο Θαλάσσης, στην Οικονομική Αποκλειστική Ζώνη ενός κράτους και μόνο μέσω της ύπαρξης κάποιας προηγούμενης συμφωνίας για την καταπολέμηση της πειρατείας, του smuggling και όχι μόνο.¹⁰⁵ Σε κάθε περίπτωση απαιτείται η συναίνεση του άλλου κράτους. Στον κυβερνοχώρο αντίστοιχα, η έμφαση δίνεται, στο ότι κάποια κράτη επιτρέπουν την πρόσβαση σε άλλα σε δεδομένα ή άλλου είδους έγγραφα, κάτι που φυσικά χρειάζεται, να έχει συμφωνηθεί. Ανάλογα λοιπόν το ΣΑ μπορεί να ζητήσει εμπάργκο πρόσβασης στο διαδίκτυο, επιβάλλοντας για παράδειγμα κυρώσεις υπό το α 41 και τον κανόνα 76.¹⁰⁶

¹⁰⁵ Ibid p. 67

¹⁰⁶ Ibid p 68-69

ΚΕΦΑΛΑΙΟ 3^ο: Η προβληματική της απόδοσης ευθύνης, ύστερα από τη διάπραξη παράνομης ενέργειας

3.1: Η εισαγωγή του όρου attribution

Ένα από τα σημαντικότερα ζητήματα το οποίο ανακύπτει συνεχώς μετά από την εκδήλωση μίας ενέργειας στον κυβερνοχώρο, είναι αυτό της απόδοσης ευθύνης. Αυτό φυσικά και προκύπτει, βάζοντας στην άκρη ως δεδομένο, την ύπαρξη τριών βασικών υποκειμένων του ΔΔ. Αναφερόμαστε φυσικά στο κράτος, τους διεθνείς οργανισμούς αλλά και το άτομο το οποίο έχει αναδειχθεί κυρίως τα τελευταία χρόνια ως τέτοιο, μέσω της αναζήτησης ευθύνης για τέλεση πράξεων, που αφορούν διεθνή εγκλήματα.

Ο όρος attribution λοιπόν, έρχεται να δώσει ιδιαίτερη έμφαση στον καταλογισμό ευθυνών ειδικά όταν μιλάμε για πράξεις οι οποίες εγείρουν τη χρήση του δικαιώματος στη νόμιμη άμυνα από ένα κράτος. Το βασικό ερώτημα, όπως επισημαίνει και ο καθηγητής Διεθνούς δικαίου Νικόλαος Τσαγκουριάς είναι: Απέναντι σε ποιον θα ασκηθεί το δικαίωμα στο νόμιμη άμυνα;¹⁰⁷ Σαφέστατα, όπως προαναφέραμε υπάρχουν κάποια ιδιαίτερα χαρακτηριστικά, τα οποία δομούν ένα πλαίσιο γύρω από το οποίο χρειάζεται να εντοπιστεί η ιδιαιτερότητα του ζητήματος, που μελετάμε εν προκειμένω και που κυρίως έρχεται σε διαφοροποίηση με τις συνθήκες κάτω από τις οποίες αποδίδεται η ευθύνη για μία πράξη στο συμβατικό Διεθνές Δίκαιο. Η διαφοροποίηση λοιπόν αυτή έγκειται στον τρόπο με τον οποίο διεξάγεται μία ενέργεια στον κυβερνοχώρο έχοντας τα χαρακτηριστικά της ανωνυμίας, της δυνατότητας διεξαγωγής επιθέσεων πολλαπλών επιπέδων και της ταχύτητας με την οποία αυτές λαμβάνουν χώρα, της αμεσότητας και της ιδιαίτερης στόχευσης.¹⁰⁸ Ο σύνθετος αυτός και ιδιαίτερης χαρακτήρας αποδείχθηκε καταφανής και μετά τη μεγάλη κυβερνοεπίθεση στην Εσθονία, η οποία συμπεριελάμβανε τη συμμετοχή 85.000 υπολογιστών από όλο τον κόσμο. Ο

¹⁰⁷ ...against whom self-defence action will be taken. *Cyber-attacks, Self-defence and the Problem of Attribution*, *Journal of Conflict & Security Law Oxford University Press* 2012;; Ανάκτηση 13/10/2019

¹⁰⁸ Ibid, p.233

συγχρονισμός αυτός έγινε εφικτός εκμεταλλευόμενοι τη δυνατότητα μολύνσεων σε πολλαπλούς υπολογιστές μέσω των IP, κάτι που καθίσταται μη αντιληπτό από τους χρήστες. Με αυτόν τον τρόπο υφίσταται η δυνατότητα διεξαγωγής μαζικότερων επιθέσεων με περισσότερη όμως ισχύ.

Κατά συνέπεια αντιλαμβάνεται κανείς τη δυσκολία ύπαρξης αποδεικτικών στοιχείων, τα οποία όσον αφορούν την υλική υποδομή που χρησιμοποιήθηκε προκειμένου να διεξαχθεί η εν λόγω επίθεση, είναι ιδιαίτερα δύσκολο να εντοπιστούν. Κι εδώ έρχεται η επιστημονική κοινότητα, να τονίσει, πως αυτό που θα πρέπει, να λαμβάνεται ιδιαίτερα υπόψιν είναι και οι εκάστοτε επικρατούσες πολιτικές συνθήκες¹⁰⁹, προκειμένου, να γίνουν περισσότερο ευκρινή τα κίνητρα πίσω από την πράξη και άρα να μπορέσει να εντοπιστεί ο δράστης. Άρα ο προσδιορισμός της έννοιας attribution είναι αυτός ο οποίος εισάγει το συνδετικό κρίκο ανάμεσα στην πράξη αυτή καθ' εαυτή, τον δράστη – φυσικό πρόσωπο και το κράτος, που βρίσκεται πίσω από αυτόν.¹¹⁰

3.2: Η απόδοση ευθύνης στο κράτος (Responsibility of States for Internationally Wrongful Acts)

Ίσως το λιγότερο περίπλοκο ζήτημα εν προκειμένω αφορά την απόδοση ευθύνης σε ένα κράτος. Όπως γνωρίζουμε και από το συμβατικό διεθνές δίκαιο το «κυρίαρχο κράτος» είναι ο σημαντικότερος ίσως εκείνος παράγοντας οποίος λογίζεται ως το κύριο από τα υποκείμενα του διεθνούς δικαίου.¹¹¹

¹⁰⁹ Ibid: “To this end, the political climate within which the attack took place or who benefited from the attack need also to be taken into account. From the above it transpires that attribution combines technical investigation with intelligence and political assessments.” Nicholas Tsagourias, p. 234

¹¹⁰ “Attribution is about the assignment of an act to a State. Because states are abstract entities that act through physical persons, attribution establishes a link between the act, its physical author and the State. *State Responsibility for Cyber Operations*»: *International Law Issues*, British Institute of International and Comparative Law Charles Clore House, 17 Russell Square, London WC1B 5JP

¹¹¹ «Σήμερα είναι γενικά αποδεκτό πως το κράτος είναι κυρίαρχο, επειδή υπάγεται στο ΔΔ. Αυτό το τελευταίο του εξασφαλίζει εδαφική ακεραιότητα, ισότητα, τήρηση των

Ως προς τον προσδιορισμό της απόδοσης ευθύνης σε αυτό για παράνομες πράξεις, έδρασε η Επιτροπή Διεθνούς Δικαίου αποτυπώνοντας στα άρθρα τα οποία υιοθετήθηκαν από τη ΓΣ/ΗΕ με το Res 56/83 (2002)¹¹², όλες εκείνες τις ενέργειες οι οποίες μπορούν να αποδοθούν στο κράτος, καταστρώντας τις ενέργειές του παράνομες. Κατά αυτόν τον τρόπο τονίζεται καταφανώς η σπουδαιότητα της υποχρέωσης τήρησης των συμφωνηθέντων ανάμεσα στα κράτη, προκειμένου να γίνεται σεβαστή η κυριαρχία τους.

Από το πρώτο κίολας άρθρο η Επιτροπή Διεθνούς Δικαίου καθιστά σαφή την ευθύνη του κράτους για παράνομη πράξη η οποία διεξάγεται από αυτό,¹¹³ ενώ στο δεύτερο διευκρινίζονται οι προϋποθέσεις οι οποίες καθιστούν μία πράξη παράνομη και αποδίδουν την ευθύνη γι' αυτές στο κράτος.¹¹⁴

Για να μπορέσει όλο αυτό, να προσδιοριστεί καλύτερα, χρειάζεται, να δοθεί στο υποκείμενο, το οποίο από την πλευρά του εκπροσωπεί το κράτος και λειτουργεί στο όνομα αυτού.¹¹⁵ Αυτό σαφέστατα, θα δώσει τη δυνατότητα εντοπισμού της σύνδεσης του κάθε δρώντος με την κρατική οντότητα προκειμένου με τη σειρά της να πάρει σάρκα και οστά η έννοια του attribution. Οι δρώντες μπορεί, να είναι λοιπόν όργανα του κράτους, αντιπρόσωποι - εκπρόσωποι αυτού, ενώ σε ένα τρίτο επίπεδο η ευθύνη μπορεί να αποδοθεί στο κράτος λόγω της αδυναμίας ή της απροθυμίας του, να λάβει όλα εκείνα τα μέτρα, τα οποία θα οδηγήσουν σε αποτροπή από τέτοιες ενέργειες.

συμπεφωνημένων, μη επέμβαση στις εσωτερικές υποθέσεις και τέλος, δυνατότητα μεταβολής των διαδικασιών και των ουσιαστικών κανόνων που διέπουν τις Διεθνείς σχέσεις», *Δημόσιο Διεθνές Δίκαιο*, Εμμανουήλ Ρούκουνας, Νομική Βιβλιοθήκη, 2^η έκδοση, Αθήνα 2015, σ.22

¹¹² GA/UN Res 56/83 (2002), *Responsibility of States for internationally wrongful acts*,

Διαθέσιμο στη διεύθυνση

https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/56/83

¹¹³ "Article 1. Responsibility of a State for its internationally wrongful acts." Every internationally wrongful act of a State entails the international responsibility of that State."

¹¹⁴ Article 2. Elements of an internationally wrongful act of a State: here is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.

¹¹⁵ Nicholas Tsagourias, *Cyber-attacks, Self-defence and the Problem of Attribution*, *Journal of Conflict & Security Law*, Oxford University Press 2012; p. 236-242

Ας τα αποδημήσουμε όμως προκειμένου να είμαστε πιο ακριβείς. Αρχικά λοιπόν, χρειάζεται, να κάνουμε λόγο για τα *de jure* όργανα του κράτους, όπως επί παραδείγματι κάποιο στρατιωτικό τάγμα, η παράνομη πράξη του οποίου φυσικά και θα αποδοθεί στο εν λόγω κράτος, όπως ρητά ορίζει και το Άρθρο 4 περί της κρατικής ευθύνης για διεθνώς παράνομες ενέργειες.¹¹⁶ Παράλληλα ως προς αυτό το στοιχείο, επισημαίνεται πως το εν λόγω κράτος χρειάζεται να είναι έτοιμο εν προκειμένω, να γίνει αποδέκτης και της άσκησης του δικαιώματος στη νόμιμη άμυνα από το κράτος το οποίο προηγουμένως έβαλε.¹¹⁷

Τι συμβαίνει όμως στην περίπτωση, που τα εν λόγω όργανα δεν υπάγονται *de jure* σε αυτό; Αυτό σημαίνει, πως υπάρχει η πιθανότητα κρατικές ενέργειες, να δρομολογούν για λογαριασμό του κράτους, από *de facto* όργανα, που υπάγονται σε αυτό. Εδώ έγκειται και η δυσκολία τόσο στη φύση και τον προσδιορισμό των οργάνων αυτών, όσο και στο κομμάτι της απόδειξης ύπαρξης συνδετικού κρίκου μεταξύ τους. Το εν λόγω ζήτημα έχει απασχολήσει πολλές φορές τη διεθνή κοινότητα και ιδίως τα τελευταία χρόνια μετά και τη δημιουργία των φερόμενων ως “*rupture states*” τω οποίων οι αρχές είτε δρουν για λογαριασμό της Ρωσικής κυβέρνησης, είτε ελέγχονται, υποστηρίζονται και χρηματίζονται από αυτή. Οι όροι οι οποίοι πρέπει λοιπόν, να εισαχθούν τώρα είναι τα κριτήρια του αποτελεσματικού “*effective*” και ολοκληρωτικού “*overall*” ελέγχου, όροι που κάθε φορά στην προσπάθεια απόδοσης ευθύνης πρέπει να εντοπιστούν και να διασαφηνιστούν, προκειμένου να αποδοθεί ευθύνη σε κάποιο κράτος. Χαρακτηριστικό παράδειγμα ως προς αυτήν την κατεύθυνση αποτέλεσε η εμβληματική απόφαση του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου, Λοϊζίδου κατά Τουρκίας, όπου διευκρίνισε, πως η προσφεύγουσα στερούνταν του δικαιώματός της για απόλαυση της παρουσίας της λόγω της ύπαρξης στρατιωτικών δυνάμεων στη

¹¹⁶ Article 4. Conduct of organs of a State: 1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.

¹¹⁷ “(...) which (state) will then become the lawful target of the self-defense action.” *Cyber-attacks, Self-defense and the Problem of Attribution*, Journal of Conflict & Security Law Oxford University Press 2012;., Ανάκτηση 13/10/2019

διασυνοριακή περιοχή, οι οποίες ασκούσαν «γενικό έλεγχο»¹¹⁸, ενώ στη συνέχεια δίνει ακόμη μεγαλύτερη έμφαση καταδεικνύοντας την Τουρκία ως υπαίτια της κατάστασης αυτής, διευκρινίζοντας πως είναι αυτή η οποία ασκεί «ολοκληρωτικό αποτελεσματικό» έλεγχο στα εν λόγω στρατεύματα, οπότε και οι οποιεσδήποτε ενέργειές τους την καθιστούν υπεύθυνη.¹¹⁹ Σε μία ακόμη υπόθεση του ΕΔΔΑ, αναφορικά με την περιοχή της Υπερδνειστερίας, στην προσφυγή *Ilascu & Others v. Russia & Moldova*, το δικαστήριο έφερε προ των ευθυνών της τη Ρωσία καθώς είπε, πως ακόμη και ο μικρός αριθμός στρατευμάτων αρκούν για την απόδειξη ύπαρξης αποτελεσματικού ελέγχου. Όλες αυτές οι παραβιάσεις ήταν αποτέλεσμα του ελέγχου αυτού, που ασκούσε η Ρωσική Ομοσπονδία στους αντάρτες, όπως αποκαλούνται οι *de facto* αρχές και αυτονομιστές της Υπερδνειστερίας. Εκτός της οικονομικής και πολιτικής στήριξης στις αρχές αυτές, παρείχε αποδεδειγμένα και στρατιωτική στήριξη με αποτέλεσμα να βρίσκονται υπό τον πλήρη έλεγχό της, σε μία όπως τονίσαμε περιοχή, η οποία ανήκει και είναι διεθνώς αναγνωρισμένη ως επαρχία της Δημοκρατίας της Μολδαβίας.^{120 121}

Ως προς την ίδια κατεύθυνση είχε κινηθεί προηγουμένως και το ΔΔΧ όπου στην υπόθεση της Νικαράγουα μίλησε για μία σχέση απόλυτης εξάρτησης και ελέγχου

¹¹⁸ (...)The Commission found that the applicant has been and continues to be denied access to the northern part of Cyprus as a result of the presence of Turkish forces in Cyprus which exercise an overall control in the border area., *Loizidou v. Turkey*

¹¹⁹ *Ibid.* It is not necessary to determine whether, as the applicant and the Government of Cyprus have suggested, Turkey actually exercises detailed control over the policies and actions of the authorities of the "TRNC". It is obvious from the large number of troops engaged in active duties in northern Cyprus (see paragraph 16 above) that her army exercises effective overall control over that part of the island. Such control, according to the relevant test and in the circumstances of the case, entails her responsibility for the policies and actions of the "TRNC".

¹²⁰ Paragraphs 380, 382, 383, 390, *Ilascu & Others v. Russia & Moldova*

330. No joint customs posts were ever set up between the right and left banks of the river. Since 1995 Moldova has been part of the International Customs Union. Transdniestria is an integral part of Moldova, but customs control has never been exercised by Moldovan authorities over services and goods emanating from the left bank region. There has therefore never been any smuggling, formally speaking. *Ilascu & Others v. Russia & Moldova*

¹²¹ *Ibid* p. 392. All of the above proves that the "MRT", set up in 1991-1992 with the support of the Russian Federation, vested with organs of power and its own administration, remains under the effective authority, or at the very least under the decisive influence, of the Russian Federation, and in any event that it survives by virtue of the military, economic, financial and political support given to it by the Russian Federation.

ανάμεσα στο κράτος των ΗΠΑ και τους contras.¹²² Η εξάρτηση αυτή έφτασε σε τέτοιο βαθμό, που σύμφωνα με το δικαστήριο, θα ήταν αδύνατον οι ενέργειες αυτές των contras να πραγματοποιθούν χωρίς τη βοήθεια των ΗΠΑ.¹²³

Απαιτείται σε αυτό το σημείο, να τονίσουμε, πως απαιτείται η ύπαρξη υψηλού βαθμού ελέγχου, ο οποίος προσδιορισμός έχει ως σκοπό να βοηθήσει την εξομοίωση του de facto οργάνου αυτού με de jure του κράτους, προκειμένου εν συνεχεία να προσδιοριστεί η απόδοση ευθύνης.¹²⁴ Ο μεγάλος βαθμός ελέγχου θα μπορούσαμε, να πούμε, πως συνεπάγεται τον έλεγχο κάθε πτυχής του εν λόγω οργάνου, κάτι που δεν μπόρεσε, εν τέλει, να αποδειχθεί στην περίπτωση της Νικαράγουα.¹²⁵

Στη συνέχεια σύμφωνα με τον Καθηγητή Διεθνούς Δικαίου Νικόλαο Τσαγκουριά, περνάμε σε μία δεύτερη κατηγορία οργάνων, αυτών που δρουν κάτω από τις οδηγίες, την καθοδήγηση και τον έλεγχο του κράτους. Όλα αυτά έχουν ως σκοπό την κατά περίπτωση καθοδήγηση του οργάνου να προβεί σε μία ενέργεια στον κυβερνοχώρο, υπό τις συγκεκριμένες οδηγίες του κράτους, οι οποίες φυσικά πρέπει να σχετίζονται με την εν λόγω παράνομη ενέργεια.¹²⁶ Θα μπορούσαμε να πούμε, πως μιλάμε επί της ουσίας για την πραγμάτωση μίας συγκεκριμένης

¹²² "What the Court has to determine at this point is whether or not the relationship of the contras to the United States Government was so much one of dependence on the one side and control on the other that it would be right to equate the contras, for legal purposes, with an organ of the United States Government, or as acting on behalf of that Government.", *Nicaragua v. USA*, p 109

¹²³ "In the view of the Court it is established that the contras force has, at least at one period, been so dependent on the United States that it could not conduct its crucial or most significant military and paramilitary activities without the multi-faceted support of the United States. (...)" *Nicaragua v. USA*, p 111

¹²⁴ *Cyber-attacks, Self-defense and the Problem of Attribution*, Journal of Conflict & Security Law, Oxford University Press 2012; p 237

¹²⁵ (...)there is no clear evidence of the United States having actually exercised such a degree of control in all fields as to justify treating the contras as acting on its behalf. *Nicaragua v. USA*, p 109

¹²⁶ Instructions establish an ad hoc relationship between the entity that commits the cyber-attack and the State and, for this reason, instructions should be proven in relation to the specific cyber-attack *Cyber-attacks, Self-defense and the Problem of Attribution*, Journal of Conflict & Security Law, Oxford University Press 2012; p 237

«αποστολής».¹²⁷ Η ενέργεια αυτή θα πρέπει, να περιέχει τα χαρακτηριστικά του αποτελεσματικού ή του ολοκληρωτικού ελέγχου με την πρώτη περίπτωση να αναφέρεται σε κράτος το οποίο υποστηρίζει, χρηματοδοτεί ή προσφέρει τεχνογνωσία σε μία ομάδα, χωρίς όμως να μπορεί να αποδοθεί ευθύνη για μία συγκεκριμένη πράξη. Στο δεύτερο κριτήριο του αποτελεσματικού ελέγχου, απαιτείται η διευκρίνηση πως το συγκεκριμένο κράτος, προκειμένου να επιβαρυνθεί με την απόδοση της ευθύνης για τη συγκεκριμένη παράνομη ενέργεια, απαιτείται η απόδειξη ανάμειξης σε αυτήν την ίδια.¹²⁸ Εν τέλει, θεωρείται σημαντικό, να τονιστεί, πως και από πλευράς ΔΔΧ το κριτήριο του αποτελεσματικού ελέγχου, αποκόβεται από τον κανόνα περί κρατικής ευθύνης καθώς θέτει ιδιαίτερα αυστηρούς περιορισμούς για την απόδοσης ευθύνης.¹²⁹ Η αδυναμία απόδειξης πλήρωσης των προϋποθέσεων, αποσυνδέει την απόδοση ευθύνης στο κράτος.¹³⁰

Ένα τρίτο και τελευταίο σημείο είναι αυτό της αδυναμίας ή απροθυμίας του κράτους, να λάβει όλα εκείνα τα απαραίτητα μέτρα, προκειμένου να αποτραπεί η πραγμάτωση οποιασδήποτε παράνομης ενέργειας, ως οφείλει με βάση τους κανόνες του διεθνούς δικαίου. Η πλέον χαρακτηριστική περίπτωση είναι αυτή των Ταλιμπάν, που κατείχαν την εξουσία το 2001 στο Ιράκ. Οι τρομοκρατικές επιθέσεις από την Αλ Κάιντα εξέγειραν το ερώτημα του αν θα μπορούσε να αποδοθεί ευθύνη στο κράτος του Ιράκ, υπό το πρίσμα της αδυναμίας να φέρει σε πέρας τις διεθνείς του υποχρεώσεις και τους γεγονότος πως επέτρεψε σε έναν μη κρατικό δρώντα, μία τρομοκρατική οργάνωση να δράσει στο έδαφός του και να εξαπολύσει επιθέσεις

¹²⁷ Ibid (...) that a cyber attack carried out by a group or a person will be attributed to a State only if that State has exerted direct influence on the group or person to commit the attack or has enforced its perpetration. p. 238

¹²⁸ Ibid p. 238

¹²⁹ (...)the “overall control” test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State’s organs and its international responsibility. *Bosnia Genocide Case* p. 406.

¹³⁰ Ibid (..) The acts constituting genocide were not committed by persons or entities which, while not being organs of the FRY, were empowered by it to exercise elements of the governmental authority (Art. 5), nor by organs placed at the Respondent’s disposal by another State (Art. 6), nor by persons in fact exercising elements of the governmental authority in the absence or default of the official authorities of the Respondent (Art. 9) ; finally, the Respondent has not acknowledged and adopted the conduct of the perpetrators of the acts of genocide as its own (Art. 11)., p 116

εναντίον άλλου κράτους, γεγονός που ρητά απαγορεύεται¹³¹. Η ειδοποιός διαφορά έγκειται στην ανοχή που καταδεικνύει ένα κράτος, σε αντίθεση με την αντιμετώπιση του προβλήματος, καθώς στην περίπτωση αυτή μπορεί, να εγερθεί και το δυνατότητα χρήσης του δικαιώματος στη νόμιμη άμυνα, υπό το άρθρο 51 του ΚΧ/ΗΕ, αλλά όπως τόνισε και το ΔΔΧ στην υπόθεση “Congo vs. Uganda”, «η έλλειψη λήψης δράσεων αντιμετώπισης, δε συνιστά πάντα ανοχή της κατάστασης».¹³²

3.3: Ο ρόλος των μη κρατικών δρώντων και το ζήτημα της απόδοσης ευθύνης.

Ένα από τα καταφανώς σημαντικότερα ζητήματα ως προς την προβληματική της απόδοσης ευθύνης ύστερα από μία παράνομη ενέργεια είναι η ύπαρξη και η δράση μη κρατικών παραγόντων, οι οποίοι δυσχεραίνουν την προσπάθεια απόδοσης ευθύνης. Η προσπάθεια αυτή στη συγκεκριμένη περίπτωση έρχεται να συγκρουστεί με το συμβατικό Διεθνές Δίκαιο, που διευκρινίζει πως τα υποκείμενά του είναι τα κράτη και οι διεθνείς οργανισμοί, ενώ πλέον και το άτομο έχει καταστεί τέτοιο. Οπότε, εύκολα διερωτάται κανείς προς τα που οδηγείται η εν λόγω κατάσταση. Εναντίον ποιου, τα κράτη θύματα θα χρησιμοποιήσουν το δικαίωμα της νόμιμης άμυνας; Πώς θα μπορέσουν να δικαιολογήσουν τη χρήση αντιμέτρων;

Κατά κύριο λόγο οι ενέργειες κρατών κατά μη κρατικών δρώντων μπαίνουν σε εφαρμογή ύστερα από την τέλεση τρομοκρατικών ενεργειών από τους τελευταίους. Όπως υπογραμμίζει και η Επιτροπή Διεθνούς Δικαίου στο Άρθρο 8¹³³ για την ευθύνη του κράτους έπειτα από την τέλεση ενεργειών από όργανα, τα οποία δεν υπάγονται σε μία κρατική οντότητα, τίθενται τρεις προϋποθέσεις προκειμένου, να

¹³¹ Cyber-attacks, Self-defense and the Problem of Attribution, Journal of Conflict & Security Law, Oxford University Press 2012; p 242-243

¹³² (...) the Court cannot conclude that the absence of action by Zaire’s Government against the rebel groups in the border area is tantamount to “tolerating” or “acquiescing” in their activities. Congo vs Uganda, p. 301

¹³³ Article 8: Conduct directed or controlled by a State, “The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.” Articles on the Responsibility of States for Internationally Wrongful Acts, 2001

διασαφηνιστούν οι περιπτώσεις απόδοσης της εν λόγω ευθύνης για την παράνομη ενέργεια στο κράτος. Σύμφωνα λοιπόν με το εν λόγω άρθρο η προερχόμενη πράξη από ένα άτομο ή μία ομάδα θεωρείται ως πράξη του κράτους όταν ενεργεί υπό τις οδηγίες, τη διεύθυνση ή τον έλεγχο του κράτους αυτού, χωρίς φυσικά να απαιτείται, να πληρούνται και τα τρία κριτήρια, κάτι που γίνεται κατανοητό από τη χρήση του όρου “or” στην παράθεση των προϋποθέσεων.

Ως προς το πρώτο λοιπόν στοιχείο αυτό δηλαδή των οδηγιών και των κατευθύνσεων, η ΕΔΔ αναφέρεται στις περιπτώσεις εκείνες όπου οι δράσεις του κράτους φαίνεται να γίνονται ένα είδος αποστολής για δρώντες οι οποίοι καλούνται, να τις φέρουν σε πέρας «αποστολές για το εν λόγω κράτος μένοντας παράλληλα αποκομμένοι από τις επίσημες κρατικές δομές.¹³⁴ Έτσι λοιπόν, την ευθύνη επωμίζεται το κράτος το οποίο φιλοξενεί την οργάνωση της ενέργειας και υπάρχει η δυνατότητα, να ενεργοποιηθεί σε βάρος του το δικαίωμα νόμιμης άμυνας υπό το Α51 του ΚΧ/ΗΕ από το θύμα. ¹³⁵ Η χρήση του δικαιώματος στη νόμιμη άμυνα μπορεί να ενεργοποιηθεί τόσο σε βάρος του κράτους που φιλοξενεί τον μη κρατικό δρώντα, τόσο και σε βάρος του δρώντος αυτού καθ’ εαυτού.¹³⁶

Αναφορικά με το δεύτερο στοιχείο χρειάζεται, η εν λόγω πράξη να αποδειχθεί, πως βρισκόταν υπό τον πλήρη έλεγχο, καθοδήγηση και οργάνωση από το εν λόγω κράτος.¹³⁷ Φυσικά και εδώ όπως και σε προαναφερθείσες περιπτώσεις, όπου

¹³⁴ “Most commonly, cases of this kind will arise where State organs supplement their own action by recruiting or instigating private persons or groups who act as “auxiliaries” while remaining outside the official structure of the State.” *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, Commentary of article 8, paragraph 2.

¹³⁵ (...)an armed attack which has been perpetrated by NSAs becomes something against which a state can respond to in self-defence, it has to be shown that the NSAs concerned have been ‘sent by or on behalf’ of the state in which they are located, or that the state has been ‘substantially involved’ in the perpetration of the acts concerned. In other words, the actions of the NSA must be attributed to a state through the ‘effective control’ it exerted over them., *Non-State Actors and the Use of Force* Christian Henderson, in M. Noortmann, A. Reinisch, and C. Ryngaert, *Non-State Actors in International law* (Oxford: Hart Publishing, 2014), p 9

¹³⁶ *Non-State Actors and the Use of Force* Christian Henderson, in M. Noortmann, A. Reinisch, and C. Ryngaert, *Non-State Actors in International law* (Oxford: Hart Publishing, 2014), p 11

¹³⁷ Ibid: Such conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation.

εντάσσαμε το κριτήριο του ελέγχου ήταν απαραίτητο να διασαφηνίσουμε και βαθμό αυτού, όπως χαρακτηριστικά μας δίδαξε το ΔΔΧ στην υπόθεση της Νικαράγουα εναντίων των ΗΠΑ, τονίζοντας πως μία γενικόλογη προσέγγιση όπως δηλαδή μία γενικευμένη παρότρυνση για την τέλεση της εν λόγω παράνομης πράξης, δεν καθίσταται αρκετή. Ως προς αυτήν την κατεύθυνση κινήθηκε το ΔΔΧ το 2007 στην υπόθεση για τη γενοκτονία στη Βοσνία, διασαφηνίζοντας σε μία παράγραφο τα εξής: «Αρχικά, απαιτείται η απόδειξη απόλυτου δεσμού ανάμεσα στα άτομα και τις ομάδες με το εν λόγω κράτος καθώς και η τέλεση πράξεων υπό τον «αποτελεσματικό έλεγχο» του κράτους. Τονίζεται πως, ο εν λόγω αποτελεσματικός έλεγχος χρειάζεται να αποδειχθεί, πως ασκήθηκε για να κατευθύνει πλήρως τη συγκεκριμένη παράνομη πράξη.»¹³⁸

Με το πέρασμα του χρόνου, αν και η πρακτική έχει αποδείξει την ύπαρξη ενεργειών αυτοάμυνας οι οποίες στρέφονται μόνο κατά συγκεκριμένου δρώντος, στην περίπτωση εκείνη η οποία άλλαξε το ρου της ιστορίας και φυσικά δεν είναι άλλη από την 11/09, οι ΗΠΑ έκαναν χρήση του δικαιώματος στη Νόμιμη άμυνα, τόσο κατά του ΜΚΔ της Αλ Κάϊντα, όσο και κατά της de facto κυβέρνησης των Ταλιμπάν στο Αφγανιστάν.¹³⁹

3.4: Η προβληματική των «ακυβέρνητων» περιοχών

Ένας ιδιαίτερος ορισμός έρχεται, να βοηθήσει προκειμένου να γίνει πραγματικότητα μία προσέγγιση την οποία δυσκολευόμαστε, να προσδιορίσουμε όχι μόνο εννοιολογικά, αλλά φέρνοντας στο νου μας παραδείγματα από την υφιστάμενη κατάσταση σε πολλά σημεία της υφελίου. Το Αμερικανικό κέντρο Rand το 2007 δημοσίευσε μία μελέτη σύμφωνα με την οποία χαρακτηρίζει ως

¹³⁸ First, in this context it is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of “complete dependence” on the respondent State, (...) acted in accordance with that State’s instructions or under its “effective control”, (...) was exercised, or that the State’s instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations. , *ICJ, Bosnia & Hercegovina v. Serbia & Montenegro*, 2007, pr 400

¹³⁹ *Non-State Actors and the Use of Force* Christian Henderson, in M. Noortmann, A. Reinisch, and C. Ryngaert, *Non-State Actors in International law* (Oxford: Hart Publishing, 2014), p 13

ακυβέρνητες εκείνες τις περιοχές όπου το κράτος αντιμετωπίζει σοβαρά προβλήματα ως προς την άσκηση εξουσίας αλλά και τον έλεγχο αυτής.¹⁴⁰ Για να καταστεί ακόμη πιο κατανοητός ο συγκεκριμένος ορισμός, στην εν λόγω μελέτη παρατίθενται όλα ή τα περισσότερα εκείνα στοιχεία τα οποία συνθέτουν μία «ακυβέρνητη περιοχή». Κάποια από αυτά είναι η έλλειψη στην εν λόγω περιοχή της επίσημης κρατικής παρουσίας και κυρίως κρατικών θεσμών και υποδομών, ενώ χαρακτηριστικό γνώρισμα είναι η άνθιση της διαφθοράς, της μαύρης οικονομίας και της κοινωνικοπολιτιστικής αντίστασης. Επιπρόσθετα, τα κράτη δείχνουν ιδιαίτερη ανησυχία μπροστά στην ύπαρξη τέτοιου είδους περιοχών μιας και δεν υφίσταται το μονοπώλιο ως προς την άσκηση ένοπλης δύναμης αφού λόγω της έλλειψης ισχυρής παρουσίας από το κράτος, καθίστανται ιδανικές περιοχές για την ανάπτυξη παράνομων ένοπλων ομάδων, οι οποίες μπορούν να εξαπολύσουν τρομοκρατικές επιθέσεις κατά άλλων κρατών, διαφόρων εγκληματικών δικτύων και εν γένει να βοηθήσουν στην πρόσβαση του πληθυσμού παρανόμως στα όπλα.¹⁴¹

Όπως λοιπόν, γίνεται αντιληπτό από τα προαναφερθέντα, το ερώτημα το οποίο τίθεται, είναι, ποιος επωμίζεται την ευθύνη για μία παράνομη ενέργεια η οποία η οποία εξαπολύεται από μία τέτοια περιοχή, εναντίον ενός άλλου κράτους, πολλώ δε μάλλον όταν στις εν λόγω περιοχές δραστηριοποιούνται μη κρατικοί δρώντες. Οι παράνομες αυτές ενέργειες φυσικά και μπορούν να διενεργηθούν και στον κυβερνοχώρο. Το χαρακτηριστικότερο πλέον παράδειγμα ενός τέτοιου δρώντος είναι το ISIS, ένας μη κρατικός παράγοντας ο οποίος εξαπολύει επιθέσεις στον κυβερνοχώρο, μέσω της ομάδας Islamic Cyber Army και όχι μόνο από Συριακό και Ιρακινό έδαφος. Οι επιθέσεις αυτές είχαν ως στόχο να διασπείρουν την προπαγάνδα του ισλαμικού νόμου, τον οποία πρεσβεύει.¹⁴²

Οι ακυβέρνητες περιοχές λοιπόν θεωρούνται μία συστημική απειλή για τη διεθνή νομιμότητα καθώς σε πρώτο βαθμό αμφισβητούν την έννοια της κρατικής εξουσίας

¹⁴⁰ RAND Report "Ungoverned territories: Understanding and Reducing Terrorism Risks". (2007), Summary, σελ. Χν, 2007, Διαθέσιμο στη διεύθυνση https://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.pdf

¹⁴¹ Ibid: p. xvi

¹⁴² Tsagourias, N. "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts", p. 458, Journal of Conflict & Security Law, 2016 p.456

και σε έναν δεύτερο τους θεσμούς οι οποίοι βασίζονται στην έννοια της κρατικής εξουσίας και καθιστούν τη διεθνή νομιμότητα πραγματοποιήσιμη.¹⁴³ Αυτό που χρειάζεται, να διασαφηνίσουμε είναι η ειδοποιός διαφορά ανάμεσα στο «αποτυχημένο κράτος» και την «ακυβέρνητη περιοχή». Όπως επισημαίνει και ο καθηγητής Νικόλαος Τσαγκουριάς, ένα αποτυχημένο κράτος χαρακτηρίζεται με αυτόν τον τρόπο καθότι αδυνατεί να «σταθεί» και να ανταπεξέλθει στις υποχρεώσεις του ως ισότιμο μέλος της παγκόσμιας κοινωνίας.¹⁴⁴ Η «ακυβέρνητη περιοχή» παρουσιάζει την αδυναμία των προαναφερθέντων στοιχείων σε μία ή περισσότερες γεωγραφικές περιοχές.¹⁴⁵

Το νομικό ζήτημα λοιπόν το οποίο ανακύπτει σε αυτό το σημείο είναι αυτό της κρατικής κυριαρχίας κι αυτό, διότι αποτελεί το βασικό συστατικό δόμησης της διεθνούς κοινωνίας. Όπως έχουμε τονίσει και παραπάνω η διεθνής κοινωνία δεν έχει πολλά υποκείμενα, ένα εκ των οποίων και ίσως το σπουδαιότερο είναι το κράτος, λαμβάνοντας πάντα υπόψιν οντότητες οι οποίες μοιάζουν σε αυτό, όπως για παράδειγμα η Αγία Έδρα – Βατικανό. Έτσι λοιπόν λαμβάνουν μία νομική προσωπικότητα, η οποία τα καθιστά υποκείμενα του ΔΔ.¹⁴⁶ Τα κύρια στοιχεία τα οποία πρέπει να έχει μία οντότητα για να λογιστεί ως τέτοια είναι το έδαφος, ο λαός, μία ισχυρή κυβέρνηση, ικανή να ασκεί έλεγχο στη χώρα αλλά και να συνάπτει διπλωματικές και όχι μόνο σχέσεις με τα άλλα κράτη¹⁴⁷ και η ανεξαρτησία η οποία χαρακτηρίζει τη φύση της κυβέρνησης η οποία απαιτείται να ασκεί ανεξάρτητη,

¹⁴³ Ibid: (...) they are characterized by a lack or diminution of effective state power, which is a necessary condition for maintaining internal as well as external order and for realizing international law, p. 457

¹⁴⁴ Ibid: (...) describes a state that is 'utterly incapable of sustaining itself as a member of the international community, p. 458

¹⁴⁵ Ibid: (...) it is more inclusive by indicating a spectrum of "ungovernmentability" in geographic or governance terms.

¹⁴⁶ Το κράτος, Τα υποκείμενα του Διεθνούς Δικαίου, Άγγελος Συρίγος, Το Δίκαιο της Διεθνούς Κοινωνίας, Επιμ. Κωνσταντίνος Αντωνόπουλος, Κωνσταντίνος Μαγκλιβέρας, 3^η Έκδοση, Νομική Βιβλιοθήκη, Αθήνα 2017, p 108-110

¹⁴⁷ Article 1 Montevideo Convention on the Rights and Duties of states (26/12/1933), entered into force 23/12/1934 Διαθέσιμη στη Διεύθυνση <https://www.jus.uio.no/english/services/library/treaties/01/1-02/rights-duties-states.xml>

κυρίαρχη και αυθυπόστατη εξουσία.¹⁴⁸ Παραθέτοντας δίπλα σε αυτά τα προαναφερθέντα στοιχεία μίας ακυβέρνητης περιοχής συνειδητοποιούμε το σημαντικό έλλειμμα ως προς την ύπαρξη της ισχυρής κυβέρνησης η οποία θα ασκεί έλεγχο στην εν λόγω περιοχή, μιας και όπως τονίσαμε εκεί δραστηριοποιούνται ως επί το πλείστον μη κρατικοί δρώντες. Ακόμα, απαιτείται μία επιπρόσθετη μικρή διευκρίνιση η οποία εστιάζει στο ότι οι περιοχές αυτές δεν μπορούν να εξομοιωθούν ούτε με τα λεγόμενα puppet states - «κράτη ανδρείκελα», μιας και ο συγκεκριμένος όρος χρησιμοποιείται για να περιγράψει «κατ' όνομα κυρίαρχα κράτη, που βρίσκονται υπό ξένο έλεγχο, ιδίως στις περιπτώσεις όπου η εγκαθίδρυση του κράτους μαριονέτα, χρησιμοποιείται στην προσπάθεια νομιμοποίησης μίας κατάστασης, όπως είναι η στρατιωτική επέμβαση και η κατοχή του εν λόγω εδάφους που ακολούθησε με χαρακτηριστικό παράδειγμα τη λεγόμενη Τουρκική Δημοκρατία της Βόρειας Κύπρου.¹⁴⁹ Οι ακυβέρνητες περιοχές δεν είναι κράτη ανδρείκελα αλλά κομμάτια μιας ήδη υπάρχουσας κρατικής προσωπικότητας στα οποία η ίδια αδυνατεί να ασκήσει αποτελεσματικό έλεγχο. Αυτό είναι και το κλειδί σε όσα αναλύουμε και μελετάμε, καθώς η απουσία των κρατικών στοιχείων – θεσμών σε μία περιοχή φέρνει ως επακόλουθο την αδυναμία άσκησης αποτελεσματικού ελέγχου, διακυβέρνησης, προστασίας των πολιτών και εφαρμογής των βασικών υποχρεώσεων που απορρέουν από τα κράτη με βάση το διεθνές δίκαιο. Μία από αυτές είναι και η με κάθε τρόπο αποτροπή από το κράτος της οργάνωσης στο εσωτερικό του παράνομων ενεργειών οι οποίες στρέφονται εναντίον άλλων κρατών.

Επιπρόσθετα από όσα αναφέραμε, προκύπτει πως από τις διεθνείς αυτές υποχρεώσεις δεσμεύονται μόνο τα κράτη. Πως θα αναζητηθεί η ευθύνη για την τέλεση μίας παράνομης ενέργειας στον κυβερνοχώρο ενός μη κρατικού δρώντος, η οποία είχε ως γεωγραφική αφετηρία μία ακυβέρνητη περιοχή; Γίνεται η ευθύνη, να αποδοθεί στον εν λόγω ΜΚΔ; Σύμφωνα με το Δίκαιο, όχι. Από την άλλη ένα κράτος το οποίο έχει απωλέσει τον αποτελεσματικό του έλεγχο στη συγκεκριμένη περιοχή -

¹⁴⁸ Το κράτος, Τα υποκείμενα του Διεθνούς Δικαίου, Άγγελος Συρίγος, Το Δίκαιο της Διεθνούς Κοινωνίας, Επιμ. Κωνσταντίνος Αντωνόπουλος, Κωνσταντίνος Μαγκλιβέρας, 3η Έκδοση, Νομική Βιβλιοθήκη, Αθήνα 2017, p. 114-119

¹⁴⁹ Ibid: p. 130-132

χωρίς όμως να χάσει την κρατική του υπόσταση και διατηρώντας τη νομική του προσωπικότητα ακέραια¹⁵⁰ - και η οποία πλέον λόγω αυτού χαρακτηρίζεται ως ακυβέρνητη, επίσης δεν μπορεί να επωμιστεί την ευθύνη για την εν λόγω πράξη. Άρα ποια είναι η θέση του ΔΔ ως προς την απόδοση ευθύνης εν προκειμένω;

Σαφέστατα και η διεθνής νομολογία συντάσσεται, απατώντας στο ερώτημα που θέσαμε παραπάνω, πως ένα κράτος τίθεται προ των ευθυνών του αναφορικά με μία παράνομη πράξη, όταν στην εν λόγω περιοχή ασκεί αποτελεσματικό έλεγχο, ακόμη και όταν ασκεί αποτελεσματικό έλεγχο στα πρόσωπα τα οποία διέπραξαν την εν λόγω ενέργεια. Το ΔΔΧ μέσω της γνωμοδότησής του για τη Ναμίμπια δήλωσε, πως ο φυσικός – πραγματικός έλεγχος για μία περιοχή δηλώνει την ουσιαστική ευθύνη του κράτους και όχι ο νομικός χαρακτηρισμός της περιοχής ως μέρος – κομμάτι του εν λόγω κράτους.¹⁵¹ Επιπρόσθετα και το άρθρο 8 περί κρατικής ευθύνης σε συνέχεια παράνομης ενέργειας, τονίζουν τη σπουδαιότητα περί απόδειξης κατεύθυνσης, ύπαρξης ελέγχου ή συντονισμού της εν λόγω ενέργειας.¹⁵²

Καταφανώς λοιπόν, όταν οι ακυβέρνητες περιοχές «εγκαθίστανται» σε ένα κομμάτι της επικράτειάς του, τότε και η έκταση της αρμοδιότητάς του περιορίζεται.¹⁵³ Αυτό έχει σαν αποτέλεσμα το κράτος να μην έχει τη δυνατότητα, να ανταποκριθεί στις υποχρεώσεις που προκύπτουν από το Δεύτερο Μέρος των Άρθρων για την κρατική

¹⁵⁰ Tsagourias, N. (Non-State Actors, *Ungoverned Spaces and International Responsibility for Cyber Acts*, p. 458, Journal of Conflict & Security Law), 2016 p. 459-460

¹⁵¹ "The fact that South Africa no longer has any title to administer the Territory does not release it from its obligations and responsibilities under international law towards other States in respect of the exercise of its powers in relation to this Territory. Physical control of a territory, and not sovereignty or legitimacy of title, is the basis of State liability for acts affecting other States. *LEGAL CONSEQUENCES FOR STATES OF THE CONTINUED PRESENCE OF SOUTH AFRICA IN NAMIBIA (SOUTH WEST AFRICA) NOTWITHSTANDING SECURITY COUNCIL RESOLUTION 276 (1970)*, p.118 Διαθέσιμη στη Διεύθυνση https://www.icc-cpi.int/RelatedRecords/CR2018_04586.PDF

¹⁵² Article 8. (...) in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct., *Articles on the Responsibility of States for Internationally Wrongful Acts*

¹⁵³ (...) this is not the case when a state cannot implement or enforce international law domestically, Tsagourias, N. (Non-State Actors, *Ungoverned Spaces and International Responsibility for Cyber Acts*, p. 458, Journal of Conflict & Security Law), 2016 p. 461

ευθύνη, το οποίο αναφέρεται στις συνέπειες, που προκύπτουν από την παραβίαση των διεθνών υποχρεώσεων.¹⁵⁴

Η κατάσταση που μόλις περιγράφη αντικατοπτρίζει και τις υφιστάμενες συνθήκες στον κυβερνοχώρο. Ως μη κρατικοί δρώντες έχοντας αποκλειστεί από τη σύναψη διεθνών συνθηκών και μη όντας υποκείμενα δικαίου, δεν παραβιάζουν κάτι για το οποίο φέρουν υποχρεώσεις. Κατ' αυτόν τον τρόπο προκειμένου να καλυφθεί αυτό το καινό προστίθεται το βάρος απόδοσης της ευθύνης στο κράτος.¹⁵⁵ Όπως σωστά επισημαίνεται, κατά την απόδοση της ευθύνης διαφαίνεται και η αποτελεσματικότητα του κράτους, να ασκήσει τη διακυβέρνησή του και να καταστήσει τα όργανα εντός της επικράτειάς του είτε *de jure* είτε *de facto*, ιστάμενα σε αυτό.¹⁵⁶

Στο ζήτημα αυτό έρχεται, να απαντήσει το Άρθρο 9, αναφορικά με την ευθύνη των κρατών ως επακόλουθο παράνομης ενέργειας, το οποίο μιλά για ενέργειες οι οποίες λαμβάνουν χώρα από μη κρατικούς δρώντες και έχουν την ισχύ μίας κρατικής ενέργειας, χωρίς να λογίζονται ως τέτοιες καθότι υφίσταται η έλλειψη άσκησης κρατικής εξουσίας στην εν λόγω περιοχή, όπως προαναφέραμε και άρα υπεύθυνο ορίζεται το κράτος προκειμένου να απαιτηθεί άσκηση της εν λόγω εξουσίας.¹⁵⁷ Όπως σωστά επισημαίνεται οι βασικοί κλάδοι η φορολόγηση, η άσκηση πολιτικής η άμυνα και η δικαιοσύνη και άρα υπάρχει χώρος για μη κρατικούς δρώντες να προβούν σε τέτοιες ενέργειες; Κατά τον καθηγητή Νικόλαο Τσαγκουριά οι μη κρατικοί δρώντες μάλλον θα αποκλειστούν από την εφαρμογή του άρθρου αυτού, καθώς πρόκειται για παραβιάσεις κανόνων *ius cogens*,

¹⁵⁴ Ibid: "In other words, there is asymmetry between formal obligations and the state's material capacity to ensure respect of those obligations", p 461

¹⁵⁵ Ibid: p. 462

¹⁵⁶ Ibid: (...) the attribution standards in the law of state responsibility reflect the 'effectiveness' of statehood as an arrangement consisting of people that act on its behalf by submitting to its effective power., p. 462

¹⁵⁷ Article 9: The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority, Articles on the Responsibility of States for Internationally Wrongful Acts

θεμελιωδών κανόνων της διεθνούς κοινωνίας, μιας και το άρθρο 9 αφορά την εθελοντικώς παραδοχή κυβερνητικών αρμοδιοτήτων από μη κρατικούς φορείς και όχι καταστάσεις όπου η ανικανότητα της κυβέρνησης τους κάνει να αναλαμβάνουν τέτοιου είδους πρωτοβουλίες.¹⁵⁸ Κατ' αυτόν τον τρόπο μπορεί, να διαφανεί αυτή η ειδοποιός διαφορά η οποία στην πρώτη περίπτωση ενέχει μία δόση «ευθύνης» του κράτους, να αποτρέψει αυτούς τους μη κρατικούς δρώντες από το να προβούν σε μία παράνομη ενέργεια.

Πιο σαφές ως προς την ερμηνεία του είναι το Άρθρο 10 όπου εντάσσει στην εν λόγω συζήτηση περί απόδοσης ευθύνης ένα ευξεργετικό κίνημα το οποίο αναλαμβάνει την εξουσία και είναι υπεύθυνο και για τις πράξεις του κράτους κατά τη διάρκεια ανάληψης της εξουσίας, ενώ όταν ένα νέο κράτος δημιουργείται από ένα κίνημα, θα θεωρείται υπεύθυνο μόνο για παραβιάσεις που διαπράχθηκαν από το εν λόγω κίνημα.¹⁵⁹ Εν ολίγοις θα τεθεί υπόλογο μόνο αν καταφέρει να λάβει την εξουσία. Παρ' όλα αυτά, όπως σωστά επισημαίνεται η αδυναμία των άρθρων είναι πως εξακολουθούν να μην ανταποκρίνονται επαρκώς στις ενέργειες εκείνες οι οποίες απορρέουν από μη κρατικούς δρώντες.¹⁶⁰ Πόσο μάλλον λοιπόν μιλώντας για πράξεις, που λαμβάνουν χώρα στον κυβερνοχώρο, αν λάβουμε υπόψιν την ιδιαιτερότητα του τομέα αυτού, σε συνδυασμό με την εξέλιξη της τεχνολογίας.

Χρειάζεται να επισημάνουμε, πως πολλές φορές οι δρώντες αυτοί παρουσιάζουν μία οργανωτική δομή, ιδιαιτέρως αποτελεσματική και εδώ είναι μία χαρακτηριστική περίπτωση όπου υποστηρίζεται, πως θα πρέπει να λογίζεται ως νομική προσωπικότητα, όχι για να εξομοιωθεί με το κράτος, αλλά για να καταστεί δυνατό, να του αποδοθεί ευθύνη. Στον κυβερνοχώρο όλο αυτό είναι εξαιρετικά δύσκολο, να εφαρμοστεί καθώς δεν μπορεί, να προσδιοριστεί εύκολα η «εδαφική» υπόσταση

¹⁵⁸ Ibid 153: p. 464

¹⁵⁹ Article 10: 1. The conduct of an insurrectional movement which becomes the new Government of a State shall be considered an act of that State under international law. 2. The conduct of a movement, insurrectional or other, which succeeds in establishing a new State in part of the territory of a preexisting State or in a territory under its administration shall be considered an act of the new State under international law. 3. This article is without prejudice to the attribution to a State of any conduct, however related to that of the movement concerned, which is to be considered an act of that State by virtue of articles 4 to 9., *Articles on the Responsibility of States for Internationally Wrongful Acts*

¹⁶⁰ Ibid 52: p. 465

αλλά και η οργάνωση καθώς στην πλειοψηφία των περιπτώσεων οι οργανωτικές δομές είναι ιδιαιτέρως χαλαρές. Όλα αυτά συνηγορούν, στο ότι ένας αποτελεσματικός μη κρατικός δρών δύσκολα θα θεωρηθεί νομική προσωπικότητα, λόγω και της φύσεως των υποκειμένων που «καλύπτει» το ΔΔ.¹⁶¹

Ο μόνος ουσιαστικός τρόπος για να «πληγούν» οι δραστηριότητές τους είναι η διεθνής κοινότητα, να προβεί σε μέτρα όπως η καταφυγή σε αντίμετρα επιβολή κυρώσεων ή επιβολή κυρώσεων. Θα μπορεί να επιδιωχθεί το πάγωμα κινήσεων μη κρατικών δρώντων ποικιλοτρόπως ή ακόμη και συνθήκες αναφορικά με τον κυβερνοχώρο οι οποίες θα δεσμεύουν τόσο τα κράτη όσο και τους δρώντες αυτούς, προκειμένου να επιτευχθεί προσπάθεια, «επιβολής της ευθύνης»¹⁶²

¹⁶¹ Ibid 468-472

¹⁶² Ibid: p. 473-474

ΜΕΡΟΣ Β΄: Η ΔΙΕΘΝΗΣ ΠΡΑΚΤΙΚΗ ΚΑΙ Η ΠΡΟΣΠΑΘΕΙΑ ΔΙΚΑΙΪΚΗΣ ΘΩΡΑΚΙΣΗΣ ΕΝΑΝΤΙ ΤΩΝ ΣΥΓΧΡΩΝΩΝ ΠΡΟΚΛΗΣΕΩΝ

ΚΕΦΑΛΑΙΟ 4^ο: Οι πλέον χαρακτηριστικές περιπτώσεις παραβίασης της αρχής της μη επέμβασης στην κυβερνοχώρο

4.1: Η Ρωσική ανάμειξη στις προεδρικές εκλογές των ΗΠΑ το 2016

4.1.1: Το χρονικό της επέμβασης

Όπως χαρακτηριστικά αναφέραμε και στα προηγούμενα κεφάλαια ο κυβερνοχώρος έχει αναδειχθεί σε ένα ιδιαιτέρως πολύπλοκο αλλά την ίδια στιγμή εύχρηστο μέσο, με το οποίο τα κράτη έχουν τη δυνατότητα, να προβαίνουν σε ενέργειες προκειμένου, να προκαλέσουν κάποιο θετικό γι' αυτά αποτέλεσμα στο κράτος, το οποίο γίνεται αποδέκτης της ενέργειας αυτής. Μία από τις πλέον πολυσυζητημένες περιπτώσεις όχι μόνο υπόνοιας, αλλά ύπαρξης απτών αποδείξεων επί τούτου, αναφορικά με την παραβίαση της αρχής της μη επέμβασης στις εσωτερικές υποθέσεις ενός κράτους, είναι αυτή των αμερικανικών εκλογών το 2016. Φυσικά και το timeline της εν λόγω περίπτωσης, ξεκινάει λίγο πριν το 2015. Ακολουθώντας την πορεία των γεγονότων θα πραγματωθεί μία αναλυτική παράθεση των νομικών ζητημάτων, που ανακύπτουν.

Τον Σεπτέμβριο του 2015 το FBI, επικοινωνεί με το κόμμα των Δημοκρατικών προειδοποιώντας τους, πως τουλάχιστον ένας υπολογιστής τους έχει παραβιαστεί από Ρώσους χάκερς. Παρ' όλα αυτά το τεχνικό τμήμα το οποίο καλείται, να ερευνήσει την υπόθεση, δε βρίσκει κάτι ύποπτο και τον Νοέμβριο του ίδιου έτους το κόμμα προειδοποιείται, πως οι υπολογιστές του μεταφέρουν πληροφορίες στη Ρωσία, με τους τεχνικούς του κόμματος, να αδυνατούν, να βρουν τη δίοδο εκείνη, η οποία επέτρεψε στους Ρώσους χάκερς, να διεισδύσουν στα συστήματα των δημοκρατικών. Το αποκορύφωμα των λαθών και των λάθος χειρισμών από την ομάδα της Χίλαρι πραγματοποιείται τον Μάρτιο του 2016, όταν ο υπεύθυνος του γραφείου της λαμβάνει ένα phishing mail το οποίο τον καλούσε να αλλάξει τον

κωδικό του, διότι κάποιος άλλος χρήστης προσπάθησε, να εισέλθει σε αυτό. Ο υπεύθυνος του τεχνικού τμήματος τον οδηγεί σε λάθη¹⁶³ και έτσι δημιουργείται τον Απρίλιο του 2016 ένα ψεύτικο email. ¹⁶⁴ Χρησιμοποιώντας αυτόν τον ψεύτικο λογαριασμό, αποστέλλονται διάφορα e-mails σε πάνω από 30 άτομα της ομάδας της Χίλαρι και τα οποία περιελάμβαναν ένα link το οποίο οδηγούσε τους χρήστες σε ένα site το οποίο χειρίζονταν hackers. Με τη χρήση κακόβουλου λογισμικού κατάφερναν να έχουν πρόσβαση σε διάφορα απόρρητα αρχεία του κόμματος των δημοκρατικών τα οποία και υποκλέπτουν.

Στις 14/06/2016 αναφέρεται, ότι hackers δούλευαν για τη ρωσική κυβέρνηση, έχοντας πρόσβαση στον server των Δημοκρατικών.¹⁶⁵ Προφανώς και το Κρεμλίνο από την πλευρά του, αρνείται την οποιαδήποτε ανάμειξη, αλλά και από την πλευρά τους οι επίσημες αμερικανικές αρχές, επισημαίνουν πως οι ερευνητές της υπόθεσης δεν μπορούν ακόμη να καταλήξουν, στο ότι όντως η κυβερνοεπίθεση διενεργήθηκε από τη Ρωσία. Στις 15/06/2016, μία εταιρεία κυβερνοασφάλειας η Crowdstrike, δημοσιεύει μία ειδοποίηση, περιγράφοντας μία κυβερνοεπίθεση στην ιστοσελίδα της πολιτικής επιτροπής, από δύο ομάδες, την Cozy Bear και τη Fancy Bear. Σε απάντηση, οι χάκερ δημιουργούν ένα πρόσωπο που ονομάζεται Guccifer 2.0, ένας

¹⁶³ CNN, *2016 Presidential Campaign Hacking Fast Facts*, CNN library, Updated 1710 GMT (0110 HKT) October 31, 2019, "He shares the email with a staffer from the campaign's help desk. The staffer replies with a typo - instead of typing "This is an illegitimate email," the staffer types "This is a legitimate email." Podesta follows the instructions and types a new password, allowing hackers to access his emails." Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

¹⁶⁴ That same month, hackers use stolen credentials to access the Democratic Congressional Campaign Committee computer network, stealing data with malware. They ultimately access 33 DNC computers and anonymously register a website called DC Leaks to publicize the release of documents.

¹⁶⁵ The Washington Post, Russian Government Hackers penetrated DNC, stole opposition research on Trump, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση, https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

αυτο-περιγραφόμενος Ρουμάνος blogger που ισχυρίζεται ότι μόνο ο ίδιος διεξήγαγε την κλοπή.¹⁶⁶

Το WikiLeaks δημοσιεύει πάνω από 20.000 emails των Δημοκρατικών και το FBI με τις έρευνες που διεξάγει ανακοινώνει, ότι η επίθεση οδηγεί στη Ρωσία. Στις 27/07/2016 κατά τη διάρκεια συνέντευξης Τύπου, το Trump μιλά για τη χρήση από τον Clinton ενός ιδιωτικού διακομιστή ηλεκτρονικού ταχυδρομείου ενώ ήταν υφυπουργός και καλεί επιδεικτικά τους Ρώσους χάκερ να βρουν διαγραμμένα μηνύματα ηλεκτρονικού ταχυδρομείου.¹⁶⁷ Στις αρχές Σεπτεμβρίου του 2016, Ο Πούτιν, υποστηρίζει, πως η Ρωσική Κυβέρνηση δεν έχει καμία σχέση με το περιστατικό, λέγοντας πως το σπουδαιότερο όλων είναι η διαρροή στοιχείων, που αφορούν τους ψηφοφόρους. Στις 22 του ίδιου μήνα λέγεται από τους Δημοκρατικούς, ότι Ρώσοι οργανώνουν ένα σχέδιο προκειμένου να εμπλακούν στις επικείμενες εκλογές.

Στο debate της 26^{ης} Σεπτεμβρίου, ο Τραμπ, προσπαθώντας να θολώσει τα νερά λέει πως θα μπορούσε πίσω από αυτό να μην να κρύβεται ένα κράτος, χρηματοδοτώντας μία ομάδα χάκερ, ένας ιδιώτης, η Κίνα ή ο οποιοσδήποτε άλλος, ενώ παράλληλα εξακολουθούν, να δημοσιεύονται απόρρητα emails από τους WikiLeaks.

Στις 7 Οκτωβρίου το τμήμα ασφαλείας και πιο συγκεκριμένα το γραφείο για την ασφάλεια των εκλογών αποκάλυψε πως η ρωσική κυβέρνηση έδωσε εντολή για απόκτηση emails από Αμερικανούς πολίτες αλλά και θεσμούς. Πιο συγκεκριμένα αναφέρεται, πως σκοπός των Ρώσων, ήταν όχι μόνο να αναμειχθούν στις αμερικανικές εκλογές και να Ταχθούν υπέρ του Τραμπ, αλλά και να κλονίσουν την εμπιστοσύνη στο σύστημα.¹⁶⁸

¹⁶⁶ Crowdstrike, *Bears in the Midst: Intrusion into the Democratic National Committee*, πρόσβαση 17/12/2019, Διαθέσιμο στη Διεύθυνση <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

¹⁶⁷ "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing,"

¹⁶⁸ Homeland Security, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>

Ο Μπάρακ Ομπάμα στις 9 Δεκεμβρίου, ζητά από τους ειδικούς πράκτορες να ερευνήσουν ακόμη και τις εκλογές πίσω στο 2008 και εδώ είναι που οι σκεπτικιστές του Κρεμλίνου, ζητούν από του Αμερικανούς ερευνητές, να δημοσιεύσουν στοιχεία αναφορικά με την ενοχή των Ρώσων για «κυβερνητικώς χρηματοδοτούμενη» κατασκοπεία.¹⁶⁹ Με αφορμή αυτό το Κογκρέσο καλείται να δουλέψει για ένα μέλλον με ασφαλείς εκλογές χωρίς κυβερνοεπιθέσεις.

Οι υπηρεσίες τίθενται υπέρ της άποψης, πως υπήρξε όντως ανάμειξη των Ρώσων. Το σημείο όμως στο οποίο διαφωνούν είναι το κίνητρο της ρωσικής πλευράς ως προς την ανάμειξη αυτή. Ως προς αυτό η CIA υποστήριζε, πως σκοπός της ανάμειξης αυτής ήταν να εκλεγεί ο Ρεπουμπλικανός υποψήφιος έναντι της Χίλαρι, ενώ το FBI αδυνατούσε να το διασαφηνίσει.¹⁷⁰

Στις 29 Δεκεμβρίου ανακοινώνονται τα μέτρα που έλαβε ο τότε Αμερικανός πρόεδρος με τη μορφή κυρώσεων έναντι της Ρωσίας, διατάσσοντας μεταξύ άλλων την αποπομπή 35 Ρώσων διπλωματών, ενώ στις αρχές Ιανουαρίου του νέου έτους γίνεται συνάντηση των αρμόδιων της υπηρεσίας που διεξήγαγε την έρευνα με τους Τραμπ και Ομπάμα και τους ανακοινώθηκε, πως οι Ρώσοι δεν επενέβησαν στα μηχανήματα της εκλογικής αναμέτρησης. Αντί αυτού το Κρεμλίνο διέταξε μια πολύπλευρη εκστρατεία επιρροής η οποία περιελάμβανε τη διάδοση της προπαγάνδας αλλά και την υποκλοπή των απόρρητων εγγράφων. σύμφωνα με την έκθεση. Επιπρόσθετα, σε περίπτωση νίκης των Δημοκρατικών οι Ρώσοι ήταν έτοιμοι να προωθήσουν το hashtag “#DemocracyRIP” στη νύχτα των εκλογών. Μετά τις αποκαλύψεις αυτές ο Ντόναλντ Τραμπ κάνοντας δηλώσεις λέει πως όντως οι Ρώσοι επενέβησαν στα αρχεία των δημοκρατικών, όχι όμως στα εκλογικά μηχανήματα, κάτι που σημαίνει, πως τα αποτελέσματα των εκλογών δεν επηρεάστηκαν. Στη

¹⁶⁹ CNN, Tal Kopan, Kevin Liptak and Jim Sciutto, *Obama orders review of Russian election-related hacking*, Πρόσβαση 17/11/2019, Διαθέσιμο στη διεύθυνση <https://edition.cnn.com/2016/12/09/politics/obama-orders-review-into-russian-hacking-of-2016-election/>

¹⁷⁰ CNN, Evan Perez, Manu Raju and Deirdre Walsh, *Gap on Russia hacking conclusions between intelligence, FBI, Updated 1632 GMT (0032 HKT) December 12, 2016* *Russia hacking Donald Trump spicer smerconish_00000000*, Πρόσβαση 17/11/2019, διαθέσιμο στη διεύθυνση <https://edition.cnn.com/2016/12/11/politics/russia-hacking-conclusions-donald-trump/index.html>

συνέχεια τονίζει, πως επιθυμεί τη σύσφιξη των σχέσεων με τη Ρωσία. Από την πλευρά του ο Πούτιν λέει ότι οι κυβερνοεπιθέσεις αυτές, μπορεί να πραγματοποιήθηκαν από πατριώτες Ρώσους πολίτες που αισθάνονται υποχρεωμένοι να ανταποκριθούν σε αντιληπτές αδυναμίες κατά της Ρωσίας από την Αμερική.¹⁷¹ Κατά τη διάρκεια μιας συνέντευξης ημέρες αργότερα, ο Πούτιν λέει, ότι «ένα παιδί θα μπορούσε εύκολα να διαπράξει την κυβερνοεπίθεση αυτή».

Στις 17/05/2017 ο αναπληρωτής Γενικός Εισαγγελέας Rod Rosenstein ορίζει τον πρώην διευθυντή του FBI Robert Mueller ως ειδικό σύμβουλο για να διεξαγάγει έρευνα για την ξένη ανάμειξη στις εκλογές, η οποία θα μπορούσε, να οδηγήσουν σε ποινικές διώξεις. Στις 21 Ιουνίου, κατά τη διάρκεια ακρόασης της Γερουσίας, ο αρμόδιος υπουργός Εσωτερικής Ασφάλειας λέει, ότι οι χάκερ που συνδέονται με τη ρωσική κυβέρνηση στοχεύουν σε συστήματα ψηφοφορίας σε 21 κράτη.¹⁷²

Ο Τραμπ καταφέρνει να εξομαλύνει τις Αμερικανικές κυρώσεις, παρ' όλα αυτά ο Πούτιν με τη σειρά του σε απάντηση προς τις αμερικανικές, ανακοινώνει, ότι 755 υπάλληλοι των Αμερικανικών αποστολών στη Ρωσία, θα απομακρυνθούν από τη χώρα.

Στις 16 Φεβρουαρίου 2018, Το Υπουργείο Δικαιοσύνης ανακοινώνει ότι ο Mueller ανέφερε 13 Ρώσους υπηκόους και τρεις ρωσικές οντότητες για δήθεν εμπλοκή στις εκλογές του 2016, που τους απαγγέλλει συνωμοσία για να εξαπατήσουν τις Ηνωμένες Πολιτείες.¹⁷³

Στις 18 Ιουλίου 2018, η Επιτροπή Πληροφοριών της Γερουσίας εκδίδει μια έκθεση, που καταλήγει στο συμπέρασμα ότι η εκτίμηση της εκλογικής παρέμβασης της κοινότητας των υπηρεσιών πληροφοριών του Ιανουαρίου 2017 ήταν ακριβής.

¹⁷¹ BBC, *Putin: Patriotic Russians may be involved in hacking*, Πρόσβαση 17/11/2019, Διαθέσιμο στη διεύθυνση <https://www.bbc.com/news/technology-40122943>

¹⁷² CNN, Tal Kopan, *DHS officials: 21 states potentially targeted by Russia hackers pre-election*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html>

¹⁷³ In the United States District Court for the District of Columbia, p 2, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2018/02/16/politics/mueller-indictment-13-russian-nationals/index.html>

Σύμφωνα με τη σύνοψη, οι υπηρεσίες πληροφοριών ήταν σωστές στο να διαπιστώσουν ότι ο στόχος της παρεμβολής στις εκλογές ήταν να βοηθήσει το Trump και όχι απλά να δημιουργήσει σύγχυση.

13 Ιουλίου 2018 - Το υπουργείο Δικαιοσύνης ανακοινώνει ενδείξεις εναντίον 12 μελών της ρωσικής υπηρεσίας πληροφοριών, GRU, στο πλαίσιο της διεξαγόμενης έρευνας του Mueller. Το κατηγορητήριο κατηγορεί τους Ρώσους ότι θα συμμετάσχουν σε μια "διαρκή προσπάθεια" για να χάσουν μηνύματα ηλεκτρονικού ταχυδρομείου και δίκτυα ηλεκτρονικών υπολογιστών που συνδέονται με το Δημοκρατικό Κόμμα κατά τη διάρκεια της προεκλογικής εκστρατείας του 2016.¹⁷⁴

Με τη δημοσίευση των εγγράφων του Mueller τον Απρίλιο 2019 αλλά και το δεύτερο τόμο τρεις μήνες μετά αρχίζουν, να βγαίνουν στο φως ακόμη περισσότερα στοιχεία αναφορικά με τη Ρωσική ανάμειξη, γεγονότα, που δρομολογούν εκ νέου έρευνες από πλευράς FBI.

4.1.2: Τα νομικά ζητήματα που προκύπτουν

Αυτό που χρειαζόταν να γίνει ρητώς, ήταν η επίσημη απόδοση ευθύνης στο Ρωσικό κράτος. Χρειαζόταν, να βρεθεί ο συνδετικός αυτός κρίκος ανάμεσα στην ενέργεια η οποία διεξήχθη και το Ρωσικό κράτος.¹⁷⁵ Η ομάδα η οποία ενήργησε σε βάρος του αμερικανικού κράτους θα έπρεπε να αποδειχθεί ότι αποτελούσε de jure όργανο του Ρωσικού κράτους, σύμφωνα και με το άρθρο 4 περί ευθύνης κρατών για διεθνώς παράνομες ενέργειες. Έπειτα, θα απαιτούνταν η απόδειξη της πλήρωσης των κριτηρίων του ολοκληρωτικού – overall, ή του αποτελεσματικού – effective ελέγχου, από το κράτος αναφορικά με την εν λόγω ενέργεια. Επιπρόσθετα και με το άρθρο 5 και 6 για την ευθύνη των κρατών μετά από την πραγμάτωση παράνομων ενεργειών, που επιφέρουν τη διεθνή ευθύνη τονίζεται, πως το όργανο αυτό ενεργεί ως

¹⁷⁴ CNN, Katelyn Polantz and Stephen Collinson, *12 Russians indicted in Mueller investigation*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html>

¹⁷⁵ Cyber-attacks, Self-defence and the Problem of Attribution, *Journal of Conflict & Security Law*, Nicholas Tsagourias, Oxford University Press 2012; p. 236-242

εξουσιοδοτημένο για λογαριασμό του κράτους, ενώ τέλος με το Άρθρο 8 διασαφηνίζεται, πως στην περίπτωση που ο θύτης είναι μη κρατικός δρων, αυτός χρειάζεται, να ενεργεί υπό την κατεύθυνση και τον έλεγχο του κράτους, αλλά αναφορικά με τη συγκεκριμένη ενέργεια κι όχι εν γένει, χωρίς φυσικά χωρίς να απαιτείται, να πληρούνται και τα δύο κριτήρια ταυτοχρόνως.¹⁷⁶

4.2: Η Ρωσική ανάμειξη στις προεδρικές εκλογές της Γαλλίας το 2017

Όπως αναλύσαμε και σε προηγούμενα κεφάλαια, ένα από τα σημαντικότερα ζητήματα που ανακύπτουν μετά από τη διεξαγωγή μίας επίθεσης στον κυβερνοχώρο, είναι το ποιος θα μπορούσε, να είναι ο τρόπος απάντησης του κράτους το οποίο βάλλεται. Θα μπορούσε μία κυβερνοεπίθεση, να αποτελέσει αιτία για την άσκηση του δικαιώματος στη νόμιμη άμυνα, ή στη χρήση των αντιμέτρων; Και αν προχωρήσουμε και εστιάσουμε στις ενέργειες εκείνες οι οποίες δεν αποτελούν επίθεση με τον τρόπο, που την έχουμε ορίσει στο Διεθνές Συμβατικό Δίκαιο, αλλά πρόκειται για κινήσεις που ως στόχο έχουν, να προκαλέσουν ζημία, όχι χρησιμοποιώντας ένοπλη βία, αλλά προβαίνοντας σε ενέργειες ως προς τον επηρεασμό κάποιου αποτελέσματος εσωτερικής δικαιοδοσίας στο κράτος το οποίο βάλλεται. Σε αυτήν την περίπτωση, ποια είναι η μορφή η οποία μπορεί να ασκηθεί, δεδομένου, ότι επιβάλλεται να πληρείται το κριτήριο της αναλογικότητας. Μία λοιπόν χαρακτηριστική υπόθεση η οποία μας δίδαξε σχετικά με τον εν λόγω προβληματισμό, είναι αυτή της Ρωσικής και πάλι επέμβασης στις προεδρικές εκλογές της Γαλλίας στο 2017.

Σημαντικό κριτήριο ως προς την οποιαδήποτε προσέγγιση θα πρέπει να είναι η ιδιαιτερότητα του κυβερνοχώρου ως προς το ακαθόριστο των συνόρων του, της ανωνυμίας που υφίσταται αλλά και της δυσκολίας να αποδοθεί η ευθύνη, σε ένα κράτος ακόμη και όταν υπάρχουν σοβαρές ενδείξεις για την ενοχή του.

Ποιο είναι εκείνο το στοιχείο το οποίο μπορεί να καταστήσει μία δύναμη η οποία δέχεται επίθεση, ικανή να αντισταθεί και να απαντήσει; Αν και αυτό το ερώτημα

¹⁷⁶ Βλ. εν 3.1

άπτεται κυρίως του τομέα των στρατηγικών αναλύσεων και όχι τόσο του δικαίου, αξίζει, να γίνει μία ιδιαίτερη αναφορά σε αυτό μιας και η δυνατότητα αντίστασης ήταν αυτή η οποία έκανε την επίθεση της βραδιάς των Γαλλικών εκλογών να διαφέρει από εκείνη των Αμερικανικών ένα χρόνο πριν. Η ομάδα του Εμμάνουελ Μακρόν, όντας πολύ καλά προετοιμασμένη, κατάφερε με πολύ προσεκτικό τρόπο, να περιμένει την εκδήλωση της Ρωσικής επίθεσης, προκειμένου με αυτόν τον τρόπο να σταματήσει την εξάπλωσή της και στη συνέχεια να σταματήσει την εξάπλωσή της επίθεσης, απατώντας.¹⁷⁷

4.2.1: Το χρονικό μίας επικείμενης επίθεσης

Η ρωσική ανάμειξη και το ενδιαφέρον του Κρεμλίνου, δεν άρχισαν ξαφνικά μία ημέρα πριν από τις Γαλλικές εκλογές. Το χρονικό της Ρωσικής ανάμειξης εντοπίζεται μερικά χρόνια πριν, όταν το ακροδεξιό κόμμα του Εθνικού Μετώπου, του οποίου τώρα επικεφαλής είναι η Μαρίν Λε Πέν, βρισκόταν στα πρόθυρα της κατάρρευσης, τόσο πολιτικά, όσο και σε οικονομικό επίπεδο. Την περίοδο εκείνη λοιπόν το κόμμα υποστηρίχθηκε από δύο μυστηριώδη δάνεια ύψους 2 και 9 εκατομμυρίων ευρώ, ποσά προερχόμενα από τράπεζες οι οποίες φαίνεται να έχουν στενούς δεσμούς με την KGB αλλά και Ρώσους επενδυτές. Επιπρόσθετα, είναι αξιοσημείωτο, το ότι το κόμμα του “Front National (FN)” υπήρξε το μοναδικό Γαλλικό κόμμα το οποίο υποστήριξε την προσάρτηση της Κριμαίας στη Ρωσία, χαρακτηρίζοντας μάλιστα το Κριμαϊκό δημοψήφισμα – παρωδία, «αναμφισβήτητο»¹⁷⁸.

¹⁷⁷ The Strategy Bridge, “Cybersecurity as Attack-Defense: What the French Election Taught Us About Fighting Back”, Youri Cormier, September 12, 2018, “Time, as we shall see below, is indeed one of the greatest tools at the disposition of the counter-cyber strategist, but it is by no means to be equated with waiting around idly. In fact, it’s quite the opposite. One must engage hackers as though in a duel: deflect, hit back, and in doing so, occupy their space and their time to limit their reach and contain the potential damage they might wreak.” Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση https://thestrategybridge.org/the-bridge/2018/9/12/cybersecurity-as-attack-defense-what-the-french-election-taught-us-about-fighting-back?fbclid=IwAR0dC2tQZZGIX3CCHJoCSEvMAdFQLoLlQ_QMRpl4WZkZbvo72HjysTf_yCU

¹⁷⁸ Le Monde, “Visites, financement: le Front national et la Russie, une idylle qui dure, La rencontre officielle entre Marine Le Pen et Vladimir Poutine, le 24 mars, est l’aboutissement de plusieurs années de prises de position prorusses du parti d’extrême droite.” Laura Motet,

Η γλώσσα προγραμματισμού η οποία χρησιμοποιήθηκε, έδειξε σημάδια κωδικοποίησης και επεξεργασίας σε ρωσικούς υπολογιστές.¹⁷⁹ Το σημαντικότερο στοιχείο είναι πως η ομάδα του Μακρόν ήταν προετοιμασμένη, λόγω κυρίως και της προηγηθείσας Αμερικανικής εμπειρίας.¹⁸⁰ Έτσι λοιπόν, μέσω της δημιουργίας ψεύτικων λογαριασμών με μαζικό τρόπο, κατάφεραν, να επιβραδύνουν τους Χάκερς¹⁸¹. Επιπρόσθετα, με τη σειρά της μία Ιαπωνική εταιρεία, η Trend Micro, έφερε στο φως μία έκθεση, η οποία περιελάμβανε 160 καταγεγραμμένες απόπειρες ηλεκτρονικής κατασκοπείας, οι οποίες είχαν ως στόχο την ομάδα του Ε. Μακρόν.¹⁸² Η ομάδα των Γάλλων χρησιμοποιώντας πραγματικά ονόματα ανθρώπων της ομάδας του Μακρόν στους ψεύτικους αυτούς λογαριασμούς, κατάφερε να προσελκύσει τους Χάκερς, οι οποίοι κατάφεραν να υποκλέψουν 5 γραμματοκιβώτια ηλεκτρονικού ταχυδρομείου. Έτσι λοιπόν τους έδωσαν πρόσβαση σε λογαριασμούς και υλικό το οποίο ήταν ψεύτικο και αληθοφανές, σε χιλιάδες έγγραφα δηλαδή «παγίδες», προκειμένου να κερδίσουν τον απαραίτητο χρόνο και να απαντήσουν.¹⁸³

18/11/2016, Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση https://www.lemonde.fr/les-decodeurs/article/2016/11/18/le-front-national-et-la-russie-une-idylle-qui-dure_5033857_4355770.html

¹⁷⁹ The New York Times, “Hackers Came, but the French Were Prepared” Adam Nossiter, David E. Sanger, Nicole Perlroth, 09/05/2017, Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση <https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html>

¹⁸⁰ ibid

¹⁸¹ Ibid: Mr. Mahjoubi: “We created false accounts, with false content, as traps. We did this massively, to create the obligation for them to verify, to determine whether it was a real account. I don’t think we prevented them. We just slowed them down. Even if it made them lose one minute, we’re happy.” (...) “ (...)the Russians did a poor job of covering their tracks (...)”

¹⁸² AP NEWS, Researchers: “Russia – linked hackers targeted Macron campaign, Raphael Satter”, 25/04/2017, Πρόσβαση 18/11/2019, “Trend Micro’s report, which was produced independently of the Macron campaign and lists 160 attempts at electronic espionage across a series of targets, adds a measure of evidence to the claim, saying hackers set up a bogus website to harvest the passwords of Macron campaign staffers.” Διαθέσιμο στη Διεύθυνση <https://apnews.com/0fda6547810540699f009a2875c73b1d/Researchers:-Russia-linked-hackers-targeted-Macron-campaign%20;%20https://www.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html>

¹⁸³ The Strategy Bridge, “Cybersecurity as Attack-Defense: What the French Election Taught Us About Fighting Back”, Youri Cormier, September 12, 2018, Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση <https://thestrategybridge.org/the-bridge/2018/9/12/cybersecurity-as-attack-defense-what-the-french-election-taught-us->

Έτσι λοιπόν τα αρχεία περιείχαν ακόμη και ρωσικούς χαρακτήρες και διέρρευσαν ακόμη και μέσω WikiLeaks, ενώ δεν ήταν αυθεντικά με τους υπεύθυνους της πλατφόρμας, να προσπαθούν να αποκαταστήσουν την εγκυρότητα και την αξιοπιστία τους.¹⁸⁴

4.2.2: Τα νομικά ζητήματα που ανακύπτουν

Η ύπαρξη απλών στοιχείων τα οποία καταδεικνύουν την προέλευση της ανάμειξης δεν επαρκούν, προκειμένου, να αποδοθεί η ευθύνη η οποία ως επακόλουθο, θα είχε νομικές συνέπειες για τον θύτη. Στην περίπτωση της Γαλλίας, η άκρως καλά προετοιμασμένη ομάδα του Εμμανουέλ Μακρόν κατάφερε, συνθέτοντας το παζλ των στοιχείων, που κατείχε, να βρει έναν κρίκο που φαίνεται, να συνδέει την Μαρίν Λεπέν με τη ρωσική πλευρά. Αυτό που δεν κατέστη εφικτό ήταν να συνδεθεί επίσημα και με αδιάσειστα στοιχεία η ενέργεια των Χάκερς με το Ρωσικό κράτος και πιο συγκεκριμένα με τη ρωσική κυβέρνηση. Χρειάζεται δηλαδή, να εντοπιστεί οντότητα η οποία θα συνδέεται με το κράτος και η σύνδεση αυτή θα είναι αδιαμφισβήτητη.¹⁸⁵ Αρχικά, όπως αναλύσαμε και σε προηγούμενο κεφάλαιο, θα έπρεπε η ομάδα αυτή να αποδειχθεί πως αποτελεί de jure όργανο του Ρωσικού κράτους, σύμφωνα και με το άρθρο 4 περί ευθύνης κρατών για διεθνώς παράνομες ενέργειες. Σε ένα άλλο στάδιο στην περίπτωση που η εν λόγω ομάδα – όργανο – άτομο αποτελεί de facto όργανο του ρωσικού κράτους, θα χρειαζόταν, να αποδειχθεί πως πληρούνται τα κριτήρια του ολοκληρωτικού – overall, ή του αποτελεσματικού – effective ελέγχου από τη ρωσική κυβέρνηση, όπως χαρακτηριστικά ανέλυσε το ΔΔΧ στις υποθέσεις της Νικαράγουα αλλά και της γενοκτονίας στη Βοσνία. Επιπρόσθετα και με το άρθρο 5 και 6 για την ευθύνη των κρατών μετά από την πραγμάτωση παράνομων ενεργειών, που επιφέρουν τη

[about-fighting-back?fbclid=IwAR0dC2tQZZGIX3CCHJoCSEvMAdFQLoLlQ_QMRpl4WZkZbvo72HjysTf_yCU](#)

¹⁸⁴ Ibid: “Even if any of it were true or damaging, they could easily be denied. Wikileaks saw its credibility crippled for having shared the dubious hack and, treading nervously, they reminded their followers the documents had not been listed on their website, merely shared on Twitter.”

¹⁸⁵ Cyber-attacks, Self-defence and the Problem of Attribution, Journal of Conflict & Security Law, Nicholas Tsagourias, Oxford University Press 2012; p. 236-242

διεθνή ευθύνη τονίζεται, πως το όργανο αυτό ενεργεί ως εξουσιοδοτημένο για λογαριασμό του κράτους, ενώ τέλος με το Άρθρο 8 διασαφηνίζεται, πως όταν αναφερόμαστε σε μη κρατικό παράγοντα, αυτός χρειάζεται, να ενεργεί υπό την κατεύθυνση και τον έλεγχο του κράτους, αλλά αναφορικά με τη συγκεκριμένη ενέργεια κι όχι εν γένει και φυσικά χωρίς να απαιτείται, να πληρούνται και τα δύο κριτήρια ταυτοχρόνως.¹⁸⁶

Χρειάζεται, να τονίσουμε λοιπόν, πως η απόδοση ευθύνης είναι προσκολλημένη στην απόδειξη εξάρτησης του δρώντος, κρατικού και μη στο κράτος, λόγω της σοβαρότητας που φέρει η θέση του ως υποκειμένου στο Διεθνές Δίκαιο. Παρόλα αυτά αντιλαμβανόμαστε, πως το Διεθνές Δίκαιο φαίνεται, να έχει μείνει στάσιμο και να μην εξελίσσει την εφαρμογή του, με τον ίδιο ρυθμό με τον οποίο εξελίσσει τις δυνατότητές της η τεχνολογία. Έτσι, κρατικοί και μη δρώντες εκμεταλλευόμενοι την ιδιαιτερότητα του κυβερνοχώρου και τις «διευκολύνσεις» τις οποίες προσφέρει, προβαίνουν σε παράνομες ενέργειες έναντι άλλων κρατικών αποδεκτών καταφέροντας, να αποφεύγουν τη λογοδοσία έναντι της διεθνούς κοινότητας.

4.3: Αποτέλεσαν αυτές οι δύο αναμετρήσεις παραβίαση της αρχής της μη επέμβασης;

Οι περισσότεροι αναλυτές και νομικοί υποστηρίζουν, πως και στις δύο προαναφερθείσες περιπτώσεις, δεν υπήρξε παραβίαση αναφορικά με τη αρχή της μη επέμβασης στα ζητήματα, που άπτονται της εσωτερικής δικαιοδοσίας ενός κράτους κι αυτό διότι φάνηκε, να εκλείπει το στοιχείο του εξαναγκασμού. Όπως αναλύσαμε και σε προηγούμενο κεφάλαιο ο εξαναγκασμός είναι το στοιχείο αυτό το οποίο καταδεικνύει τη συγκεκριμένη τροπή την οποία έλαβαν τα γεγονότα, παρά τη θέληση του ενδιαφέροντος κράτους. Οι μελετητές λοιπόν οι οποίοι υποστηρίζουν, πως δεν υπήρξε παραβίαση του Α2 π7 του ΚΧ/ΗΕ μάλλον εστιάζουν στο γεγονός πως δεν επηρεάστηκαν στα εκλογικά συστήματα, ως προς το τεχνικό τους κομμάτι. Πράγματι, κάτι τέτοιο δεν συνέβη. Αν σταθούμε σε μία τόσο στενή

¹⁸⁶ Βλ. εν 3.1

ανάλυση των γεγονότων, τότε σίγουρα δε θα δούμε πουθενά την παραβίαση. Όπως επισημαίνει ο καθηγητής Νικόλαος Τσαγκουριάς, η ουσία έγκειται αλλού και αυτό το άλλο δεν είναι καθόλου απροσδιόριστο. «Η διαμόρφωση μιας πολιτικής εξουσίας είναι ελεύθερη, μόνο όταν η διαδικασία ως προς αυτό είναι ελεύθερη»¹⁸⁷. Εδώ λοιπόν αντιλαμβανόμαστε, πως πρόκειται για μία ενέργεια η οποία παραβιάζει κατάφορα την αρχή της αυτοδιάθεσης. Η επέμβαση μετατοπίζεται στα άτομα και τη διαμόρφωση της θέλησης. Η χειραγώγηση γίνεται στην πηγή, με την άσκηση προπαγάνδας. Κατ' αυτόν τον τρόπο τα πράγματα διαμορφώνονται με βάση τη θέληση του παρεμβαίνοντος.¹⁸⁸

Κατανοούμε λοιπόν, πως απαιτείται σε τέτοιου είδους περιπτώσεις η προσέγγιση να γίνεται με πιο λεπτομερή, πιο έμμεσο τρόπο. Χρειάζεται, να υπεισερχόμαστε στην ουσία, να εστιάζουμε στον εξαναγκασμό, που ασκείται στη βάση της δημιουργίας του εν λόγω ζητήματος, προβληματισμού και κατ' επέκτασιν παραβίασης. Η χειραγώγηση της κοινής γνώμης έρχεται σε ρήξη με το σεβασμό της αρχής της αυτοδιάθεσης και του αυτοπροσδιορισμού αλλά και της ανεπηρέαστης επιλογής του τρόπου διακυβέρνησης.

¹⁸⁷ Nicholas Tsagourias, EJIL: Talk!, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, Yet, a government's authority and will remains free only when its sourcing is also free. Διαθέσιμο στη διεύθυνση <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/>, Πρόσβαση 19/12/2019

¹⁸⁸ Ibid: "Where coercion as control can manifest itself more acutely is when a state's authority and will are manipulated at its source; in the process of their formation." (...) "when a state interferes in the electoral process, for example through disinformation or 'hack and leak' operations, it interferes with the structures but also with the environment that condition and facilitate the formation of authority (...) the intervening state controls not only the peoples' cognitive environment within which authority and will are formed but also their choices."

ΚΕΦΑΛΑΙΟ 5^ο: Η προσπάθεια θωράκισης του κράτους αποδέκτη της επίθεσης

Το ιδιαίτερα ενδιαφέρον κομμάτι των επεμβάσεων αυτών είναι η αντίδραση του κράτους, που δέχεται την επίθεση κι αυτό διότι, αυτού του είδους οι επεμβάσεις οι οποίες δεν περιλαμβάνουν τη χρήση βίας. Κατ' αυτόν τον τρόπο αντιλαμβανόμαστε λοιπόν, πως οι δυνατότητες αντίδρασης του κράτους είναι ιδιαιτέρως περιορισμένες και εστιάζουν κυρίως στη χρήση αντιμέτρων, κυρώσεων και άλλων ειρηνικών μέσων επίλυσης των διαφορών.

5.1: Η έννοια των αντιποίνων

Φέρνοντας ξανά στο νου μας την υπόθεση των στρατιωτικών και παραστρατιωτικών δραστηριοτήτων στο εσωτερικό και κατά της Νικαράγουα, το Δικαστήριο έκανε μία ιδιαιτέρως σημαντική διάκριση ανάμεσα στη χρήση βίας η οποία αγγίζει τα όρια του απλού μεθοριακού επεισοδίου και της χρήσης βίας, που αγγίζει όμως τα όρια της ένοπλης επίθεσης και άρα συνιστά ενεργοποίηση του Α51 και του δικαιώματος στη νόμιμη άμυνα.¹⁸⁹

Αρχικά ετέθη στη διεθνή πρακτική ο όρος «νόμιμα αντίποινα». Αν και τα αντίποινα ως έννοια θεωρούνται παράνομες μιας και παραβιάζουν την απαγόρευση χρήσης βίας, υπό κάποιες προϋποθέσεις αίρεται ο παράνομος χαρακτήρας τους. Πρόκειται δηλαδή για πράξεις, που περιλαμβάνουν τη χρήση στρατιωτικής δύναμης, η οποία αποτελεί «απάντηση» σε προηγούμενη παράνομη ενέργεια του αντίπαλου κράτους. Για να αρθεί ο παράνομος χαρακτήρας τους απαιτείται η έγκριση του ΣΑ/ΗΕ, το οποίο όμως μέχρι σήμερα δεν έχει νομιμοποιήσει τη χρήση αντιμέτρων. Το 1970 η ΓΣ/ΗΕ στο RES 2625 μίλησε για ειρηνική επίλυση των διαφορών ανάμεσα στα κράτη αλλά και στο καθήκον των κρατών να απέχουν από ενέργειες οι οποίες

¹⁸⁹ Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, Judgement I.C.J. 1986, p. 195

περιλαμβάνουν τη χρήση βίας.¹⁹⁰ Όσα προαναφέραμε λοιπόν μας οδηγούν στο συμπέρασμα, πως ο μόνος τρόπος προκειμένου τα κράτη να έχουν τη δυνατότητα να προβούν στη χρήση αντιμέτρων είναι η έγκριση του ΣΑ αλλά και η εναρμόνισή τους με τις ανάγκες που επιτάσσει η άσκηση του δικαιώματος στη νόμιμη άμυνα υπό το Α51 του ΚΧ/ΗΕ.

5.2: Η έννοια των αντιμέτρων και η εφαρμογή της στον κυβερνοχώρο

Το ΔΔΧ στην υπόθεση της Νικαράγουα ανέφερε, πως «η επέμβαση στα εσωτερικά άλλου κράτους δεν συνιστά αιτιολόγηση για συλλογικά αντίμετρα με τη χρήση ένοπλης βίας», με το Δικαστήριο, να βρίσκει τις πράξεις για τις οποίες κατηγορείται η Νικαράγουα, πως «δεν δικαιολογούν τη λήψη αντιμέτρων από τρίτο μέρος και εν προκειμένω τις ΗΠΑ και άρα δεν μπορεί να δικαιολογηθεί επέμβαση με τη χρήση βίας.»¹⁹¹

Ένας πολύ σημαντικός προβληματισμός ο οποίος ετέθη από τον σπουδαίο Δικαστή του ΔΔΧ, Bruno Simma αναφορικά με την αποτυχία του Δικαστηρίου, να διευθετήσει το ζήτημα των αντιμέτρων και της χρήσεως βίας, εστίαζε στο «Πως ένα κράτος θα μπορούσε, να απαντήσει στη χρήση βίας, η οποία δεν ανάγεται στο επίπεδο της ένοπλης επίθεσης;» στο ερώτημα αυτό απάντησε υποστηρίζοντας την αντίληψη της αμυντικής στρατιωτικής ενέργειας, η οποία όμως δεν ανάγεται στο επίπεδο της πλήρους αυτοάμυνας (full-scale self-defence).¹⁹²

Κατηγορία λοιπόν των μέτρων απάντησης σε παράνομη ενέργεια, η οποία είναι περισσότερο συμβατική με το είδος των επεμβάσεων, που μελετάμε δεν είναι άλλη

¹⁹⁰ AG/RES 2625, 24/10/1970 “Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations”, Διαθέσιμο στη Διεύθυνση <https://unispal.un.org/DPA/DPR/unispal.nsf/0/25A1C8E35B23161C852570C4006E50AB>

¹⁹¹ Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, Judgement I.C.J. 1986, p 246-249.

¹⁹² Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America) 2003, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://www.icj-cij.org/files/case-related/90/9745.pdf>

από τα αντίμετρα. Με τον όρο αυτό, εννοούμε κατά βάση παράνομες πράξεις οι οποίες δεν περιλαμβάνουν τη χρήση βίας και οι οποίες μπορούν να νομιμοποιηθούν υπό συγκεκριμένες προϋποθέσεις, αλλά παράλληλα θα πρέπει απαραίτητως, να αποτελούν απάντηση σε προηγούμενη παράνομη ενέργεια.¹⁹³ Για τη χρήση τους οι προϋποθέσεις οι οποίες πρέπει, να πληρούνται, είναι διαβεβαίωση εξάντλησης όλων των άλλων ειρηνικών μέσων για την επίλυση της διαφοράς, η προειδοποίηση στον εν λόγω κράτος πως αν δεν επιστρέψει στη νομιμότητα θα υποστεί τις συνέπειες των αντιμέτρων, η έγκριση από το ΣΑ/ΗΕ, η τήρηση της αρχής της αναλογικότητας, η στόχευση κατά του κράτους το οποίο προέβη στην προηγούμενη παράνομη ενέργεια, η απαγόρευση αντιμέτρων, που παραβιάζουν του κανόνες *ius cogens*, αλλά και η μη υπέρβαση του σκοπού εφαρμογής τους, που δεν είναι άλλος από την επιστροφή του παραβάτη στη νομιμότητα.

Ως προς την εφαρμογή των αντιμέτρων στον κυβερνοχώρο το εγχειρίδιο του Ταλλίν διασαφηνίζει στον κανόνα 20, πως ένα κράτος έχει τη δυνατότητα, να καταφύγει στη λύση των αντιμέτρων είτε μέσω του κυβερνοχώρου είτε όχι, κάτι που είναι ιδιαίτερος σημαντικό, προκειμένου, να απαντήσει σε μία παράνομη ενέργεια σε βάρος του. Τονίζεται, πως χρειάζεται τα μέτρα αυτά, να λαμβάνονται από κυβερνητικά όργανα, ή κυβερνητικές δομές στον κυβερνοχώρο, ενώ φυσικά τα αντίμετρα δεν αποτελούν διαθέσιμο μέσο απάντησης σε πράξη η οποία προέρχεται από μη κρατικό δρών, αλλά έχουν εφαρμογή μόνο αν η παράνομη ενέργεια αποδοθεί στο κράτος.¹⁹⁴ Στη συνέχεια κατά κάποιον τρόπο επαναλαμβάνονται οι θεμελιώδεις εκείνες αξίες οι οποίες θα πρέπει να εφαρμόζονται ανεξαιρέτως και στον κυβερνοχώρο και εστιάζουν στην ανάγκη, να λαμβάνονται αλλά μόνο για να επαναφέρουν το κράτος, που παρανομεί, στη νομιμότητα, να μην περιλαμβάνουν

¹⁹³ Article 22: *State's Responsibility for Internationally wrongful acts* "Countermeasures in respect of an internationally wrongful act. The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of part three."

¹⁹⁴ Rule 20: Countermeasure (General Principle), N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* – Cambridge University Press, 2017, p. 113 "It is important to emphasize that countermeasures are not available in response to a cyber operation conducted by a non-State actor unless the operation is attributable to a State."

ενέργειες οι οποίες έρχονται σε ρήξη με τις θεμελιώδεις αρχές σεβασμού των ανθρωπίνων δικαιωμάτων ενώ φυσικά απαιτείται, να έχουν εξαντληθεί όλα εκείνα τα λοιπά μέτρα για την επαναφορά του κράτους, που παρανομεί στη νομιμότητα. Τέλος επιβάλλεται, να γίνεται σεβαστή η αρχή της αναλογικότητας ως προς την εφαρμογή τους.¹⁹⁵

5.3: Η έννοια των *retortions*

Η έννοια αυτή έρχεται, να διαφοροποιήσει λίγο την προσέγγιση ως προς το ποια είναι εκείνα τα επιτρεπτά από το Διεθνές Δίκαιο μέτρα τα οποία συνίστανται ως προς τη χρήση τους για απάντηση μετά από παράνομη ενέργεια. Σύμφωνα λοιπόν με την Επιτροπή Διεθνούς Δικαίου (ΕΔΔ) είναι νόμιμες αλλά μη φιλικές ενέργειες ενός κράτους προς ένα άλλο, χωρίς όμως να είναι αντίθετες με τις διεθνείς υποχρεώσεις του.¹⁹⁶ Θα μπορούσαμε να πούμε πως ως προς τη μορφή που μπορούν να πάρουν μοιάζουν με τις κυρώσεις, μιας και περιλαμβάνουν την άσκηση εμπάργκο, την επιβολή δασμών, τον περιορισμό εισαγωγών και εξαγωγών και όχι μόνο. Και σε αυτήν την περίπτωση φυσικά τα μέτρα επιβάλλεται, να παύουν όταν τερματίζεται η παράνομη ενέργεια. Στον ίδιο διευκρινιστικό τόνο ως προς τη φύση τους κινήθηκαν και οι εμπειρογνώμονες του εγχειριδίου του Ταλλίν, θέλοντας να διασαφηνίσουν τη νομιμότητα των μέτρων αυτών.¹⁹⁷

¹⁹⁵ Ibid Rules 21-23, p 116-130

¹⁹⁶ Thomas Giegerich, *Retorsion*, Oxford Public International Law, March 2011, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983>

¹⁹⁷ Rule 20: Countermeasure (General Principle), N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* – Cambridge University Press, 2017, p. 112 “The fact that countermeasures involve acts that would otherwise be unlawful also distinguishes them from retorsion. Retorsion refers to the taking of measures that are lawful, albeit ‘unfriendly’. A State may, for instance, employ an access control list to prevent communications from another State because the former enjoys sovereignty over the cyber infrastructure on its territory (Rule 2). The action would be lawful even if detrimental to the interests of the latter so long as it violates no treaty obligation or applicable customary law norm.”

5.4: Η επιβολή κυρώσεων

Η εφαρμογή των μέτρων αυτών ξεφεύγει από το κρατικό επίπεδο και ανάγεται σε ένα ευρύτερο επίπεδο καταστολής παράνομων ενεργειών και υπεισέρχεται σε ένα ευρύτερο πεδίο εφαρμογής αποφάσεων που λαμβάνονται τόσο από το ΣΑ/ΗΕ όσο και από διεθνείς οργανισμούς. Οι κυρώσεις λοιπόν, δεν συνεπάγονται χρήση βίας (A41). Στο πλαίσιο του ΣΑ και ως προς αυτήν την κατεύθυνση ιδρύονται οι Επιτροπές Κυρώσεων (Committees of Sanctions). Σε ένα δεύτερο βαθμό, συνεπάγονται χρήση βίας, κατά το A42 όπου περιλαμβάνεται ένοπλη επέμβαση από ξηράς, αέρος, θαλάσσης κι από δυνάμεις που προσφέρουν τα κράτη ή οι διεθνείς οργανισμοί. Η δεύτερη αυτή κατηγορία δεν άπτεται του ενδιαφέροντος των ενεργειών, που να αναλογούν σε παράνομες ενέργειες οι οποίες παραβιάζουν την αρχή της μη επέμβασης.

Χρειάζεται, να εστιάσουμε στα μέτρα εκείνα με τη μορφή κυρώσεων υπό το Άρθρο 41, τα οποία μπορούν, να διαμορφωθούν ως εξής: Εμπάργκο όπλων και άλλου εξοπλισμού, εμπάργκο πετρελαίου, απαγόρευση πτήσεων, μερική διακοπή διπλωματικών σχέσεων, ολική διακοπή οικονομικών σχέσεων, πάγωμα τραπεζικών λογαριασμών, απαγόρευση οποιασδήποτε μεταβίβασης κεφαλαίων, απαγόρευση ταξιδιών, απαγόρευση εισαγωγών – εξαγωγών ή παραγωγής συγκεκριμένων προϊόντων, έξυπνες κυρώσεις – Κυρώσεις κατά μη κρατικών δρώντων, ατόμων και οντοτήτων, σύσταση ad hoc δικαστηρίου ή παραπομπή υπόθεσης στο ΔΠΔ, σύστημα επανόρθωσης ζημίας που προκλήθηκε μετά από επίθεση.

Προκειμένω, να κατανοηθεί το συγκεκριμένο ζήτημα οφείλουμε να αναφερθούμε στο πότε, ενεργοποιείται το πεδίο δράσης τους. Αρχικά, λοιπόν, εναπόκειται στο Συμβούλιο Ασφαλείας, να διευκρινίσει την υπάρχουσα κατάσταση υπό το κεφάλαιο VII και να αναγνωρίσει την ύπαρξη κάποιας παραβίασης από κράτος, πράξη η οποία αποτελεί απειλή κατά της διεθνούς ειρήνης και ασφάλειας, διατάραξη αυτής ή επιθετική ενέργεια, σύμφωνα με το Άρθρο 39 του ΚΧ/ΗΕ.¹⁹⁸

¹⁹⁸ **Article 39 of the Charter:** The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or

5.4.1: Threat to the peace (Απειλή κατά της Διεθνούς Ειρήνης και Ασφάλειας)

Το ΣΑ θα εκτιμήσει πότε μία ενέργεια αποτελεί απειλή για τη διεθνή ειρήνη και ασφάλεια, όπως θα μπορούσε, να είναι για παράδειγμα μία επιθετική ενέργεια ενός κράτους σε ένα άλλο, με παραβίαση της εδαφικής ακεραιότητας του κράτους αυτού.

5.4.2: Breach of the Peace (Διατάραξη της Διεθνούς Ειρήνης και Ασφάλειας):

Εχθροπραξίες δηλαδή ανάμεσα σε ένοπλες ομάδες δύο κρατών. (άσχετο το πότε τελειώνουν) καθώς και χρήση βίας από ή κατά μίας οντότητας, που όμως δεν αναγνωρίζεται ως κράτος.

5.4.3: Aggression (Επίθεση): Μελετάται η απευθείας χρήση βίας, η οποία χαρακτηρίζεται πάντα ως διατάραξη της ειρήνης, ή αλλιώς ένοπλη επίθεση σύμφωνα με το άρθρο 51 του ΚΧ/ΗΕ.

Σε αυτό το σημείο χρειάζεται, να επισημάνουμε πως το A39 δίνει ξεκάθαρα τη δικαιοδοσία στο ΣΑ για εγκατάσταση στην επικράτεια άλλου κράτους ένοπλης δύναμης, με την επίκληση του A42.¹⁹⁹

Το Συμβούλιο, συνεπικουρούμενο από τα υπόλοιπα μέλη των ΗΕ, αλλά και εκπροσώπους της Κοινωνίας των Πολιτών ξεκίνησε μια ευρεία συζήτηση σχετικά με τις συνέπειες των κυρώσεων, σε μια προσπάθεια να καταστούν αποδοτικότερες και λιγότερο επιβλαβείς στις αδύναμες ομάδες του πληθυσμού.

Ένα από τα πρώτα μέτρα που ελήφθησαν για τη βελτίωση της αποτελεσματικότητας των κυρώσεων, ήταν ο σχηματισμός ανεξάρτητων ειδικών επιτροπών και μηχανισμών ελέγχου για την εφαρμογή τους. Το 2000, ο τότε Υπουργός Εξωτερικών του Καναδά, Lloyd Axworthy, κάλεσε το ΣΑ/ΗΕ σε μια ειδική σύνοδο, όπου αποφασίστηκε η καθιέρωση της «Άτυπης Ομάδας Εργασίας σχετικά με Γενικά

decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

¹⁹⁹ Article 42 UN Charter: "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

Ζητήματα Κυρώσεων», με την εντολή να υποβάλλει προτάσεις για τη βελτίωση της αποτελεσματικότητας των κυρώσεων, όταν αυτά λαμβάνονται, προσπαθώντας, όπως προαναφέραμε, να ασκήσουν τις απαραίτητες πιέσεις στη πηγή του προβλήματος.²⁰⁰

Η συζήτηση σε αυτό το πλαίσιο ήταν ιδιαίτερα αποδοτική και συνέβαλε αποφασιστικά στη βελτίωση των μηχανισμού αυτού, έτσι ώστε οι πιο πρόσφατες Αποφάσεις τόσο του ΣΑ/ΗΕ όσο και των περιφερειακών οργανισμών, που επιβάλλουν το μέτρο των κυρώσεων, να χρησιμοποιούν όλο και περισσότερο τις αποκαλούμενες «έξυπνες κυρώσεις» (smart sanctions), οι οποίες στοχεύουν στην άσκηση πίεσης στο εκάστοτε καθεστώς του κράτους – παραβάτη παρά στους λαούς εν γένει. Οι συζητήσεις είναι ακόμα εν εξελίξει σε σημαντικά ζητήματα, όπως ο ανθρωπιστικός αντίκτυπος των κυρώσεων, η πολιτική διάσταση της εφαρμογής και των χρονικών ορίων τους, καθώς και η καθιέρωση των προϋποθέσεων για την κατάργησή τους.

Τα τελευταία χρόνια, παρατηρούμε έντονα μερικές περιπτώσεις στοχοθετημένων οικονομικών κυρώσεων σε άτομα – πυλώνες επικίνδυνων καθεστώτων, σε επιχειρήσεις και όχι μόνο. Περιλαμβάνουν μέτρα, όπως το πάγωμα των ξένων περιουσιακών στοιχείων συγκεκριμένων ατόμων, κρατικών επιχειρήσεων και κυβερνήσεων, ενώ χρησιμοποιούνται ως οϊωνός για επιβολή άλλων μέτρων.

Οι έξυπνες κυρώσεις εμπεριέχουν μία περαιτέρω διάκριση, η οποία υφίσταται μεταξύ των "στοχοθετημένων - targeted" και "επιλεκτικών - selective" κυρώσεων. Οι "επιλεκτικές" κυρώσεις, οι οποίες είναι λιγότερο ευρείες από τις συνολικές απαγορεύσεις, συνεπάγονται περιορισμούς για συγκεκριμένα προϊόντα ή χρηματοοικονομικές ροές. Οι «στοχοθετημένες» κυρώσεις επικεντρώνονται σε συγκεκριμένες ομάδες ή άτομα στη χώρα-στόχο και στοχεύουν στην άμεση επίπτωση αυτών των ομάδων. Οι δύο αυτές έννοιες επικαλύπτονται. Παραδείγματα

²⁰⁰ Permanent Mission of Greece to the UN, Sanctions Διαθέσιμο στη διεύθυνση <https://www.mfa.gr/missionsabroad/en/un-en/greece-in-organization/peace-and-security.html?page=5>

στοχοθετημένων μέτρων είναι τα εμπάργκο Όπλων, η απαγόρευση ταξιδιών και το πάγωμα λογαριασμών.²⁰¹

Αυτό που έχει σημασία να διασαφηνίζουμε καταληκτικά σε αυτήν την ενότητα, είναι το γεγονός, πως πρόκειται για νόμιμα μέτρα τα οποία λαμβάνονται από τα όργανα των ΗΕ και πιο συγκεκριμένα από το σπουδαιότερο όλων, όπως είναι το ΣΑ, σε αντίθεση με τα αντίμετρα, τα οποία είναι παράνομες ενέργειες των οποίων αίρεται ο παράνομος χαρακτήρας και περνούν στη νομιμότητα, προκειμένου, να εξασφαλιστεί η διεθνής ειρήνη και ασφάλεια.

²⁰¹ Peterson Institute for International Economics February 23, 2000, *Targeted Sanctions: A Policy Alternative?*, "Targeted Measures: Arms Embargoes, Travel Bans and Asset Freezes" διαθέσιμο στη σελίδα, <https://piie.com/commentary/speeches-papers/targeted-sanctions-policy-alternative>

Κεφάλαιο 6^ο: Η Θεσμική και Δικαιϊκή Θωράκιση των Διεθνών Οργανισμών

6.1: Ο Οργανισμός Ηνωμένων Ηνωμένων Εθνών

Προσπαθώντας να εντοπίσουμε τον τρόπο με τον οποίο είναι δομημένο το σύστημα καταγραφής και νομικής θωράκισης του κυβερνοχώρου, χρειάζεται, να εστιάσουμε στο έργο το οποίο επιτελούν τα διάφορα όργανά του. Με το Συμβούλιο Ασφαλείας για ευνόητους λόγους, να μην έχει υιοθετήσει κανένα σχετικό ψήφισμα το κέντρο βάρους μας πέφτει στη Γενική Συνέλευση και στις επιμέρους επιτροπές της. Λίγο πριν την αλλαγή της χιλιετίας, ετέθη στο τραπέζι μία ιδιαιτέρως σημαντική πρωτοβουλία από ρωσικής πλευράς η οποία αφορούσε τη σύνταξη ενός σχεδίου ψηφίσματος το οποίο θα αφορούσε τις εξελίξεις στον τομέα της Πληροφορίας και των Τηλεπικοινωνιών, αναφορικά με τη διεθνή ασφάλεια. Το εν λόγω ψήφισμα υιοθέτησε η ΓΣ/ΗΕ το 1999.²⁰² Το σπουδαιότερο κατόρθωμα αναφορικά με τις κατά καιρούς υιοθετήσεις κειμένων από τη ΓΣ/ΗΕ είναι το γεγονός, πως το συμβατικό Διεθνές Δίκαιο έχει βρει την πλήρη του εφαρμογή και στον κυβερνοχώρο. Πιο συγκεκριμένα και με το πρόσφατο Ψήφισμα της Γενικής Συνέλευσης 73/27 διασαφηνίζεται η σπουδαιότητα του σεβασμού των βασικών αρχών του Διεθνούς Δικαίου αναφορικά με την εφαρμογή του στον κυβερνοχώρο, αναφορικά με το σεβασμό της εδαφικής κυριαρχίας, της ειρηνικής επίλυσης των διεθνών διαφορών, της εδαφικής ακεραιότητας, του σεβασμού της πολιτικής ανεξαρτησίας, του σεβασμού των ανθρωπίνων δικαιωμάτων αλλά και της απαγόρευσης απειλής ή χρήσεως βίας αλλά και της απαγόρευσης επέμβασης στις υποθέσεις οι οποίες άπτονται της εσωτερικής δικαιοδοσίας ενός κράτους.²⁰³ Καλούνται δηλαδή τα κράτη σε πλήρη σεβασμό των αρχών που πρεσβεύει ο καταστατικός χάρτης των Ηνωμένων Εθνών.

Ας μην ξεχνάμε, πως το ζήτημα της ασφάλειας στην κυβερνοχώρο βρίσκεται στην ημερήσια ατζέντα ήδη από το 1998, όταν η Ρωσική Ομοσπονδία έθεσε το

²⁰² A/RES/53/70 1990. Γενική Συνέλευση των Ηνωμένων Εθνών, Πρόσβαση 18/12/2019 Διαθέσιμο στη Διεύθυνση <https://undocs.org/en/A/RES/53/70>

²⁰³ A/RES/73/27 2018. Γενική Συνέλευση των Ηνωμένων Εθνών, 05/15/2018, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση, <https://undocs.org/pdf?symbol=en/A/RES/73/27>

συγκεκριμένο ζήτημα ως καίριας σημασίας με την υιοθέτηση όπως προαναφέραμε του πρώτου σχετικού ψηφίσματος, το οποίο ανανεώνεται κάθε χρόνο. Ομάδες εμπειρογνομόνων συστάθηκαν προκειμένου, να μελετούν συστηματικά τις νέες απειλές, που εντοπίζονται κυρίως με την ανάπτυξη της τεχνολογίας και της καινοτομίας στον κυβερνοχώρο. Επιπρόσθετα με το Ψήφισμα 70/237, «τα κράτη καλούνται να καθοδηγήσουν τη χρήση των τεχνολογιών, των πληροφοριών και των επικοινωνιών, μετά και την έκθεση της επιτροπής των εμπειρογνομόνων, που αναφέραμε το 2015.²⁰⁴

Η ομάδα των εμπειρογνομόνων σε ένα από τα report της αναφέρεται στην άμεση ανάγκη τα μέλη των Ηνωμένων Εθνών, να συμβάλουν στην προώθηση της συνεργασίας και της δημιουργίας ενός ασφαλούς περιβάλλοντος. Επιπρόσθετα, είναι ιδιαίτερως σπουδαίας σημασίας η συνεργασία του ΟΗΕ με άλλους περιφερειακούς οργανισμούς, προκειμένου η προσπάθεια αυτή να λάβει εκ των πραγμάτων παγκόσμια τροχιά. Ακόμα, τονίζεται ο σεβασμός στις νόρμες του διεθνούς δικαίου, στην κυριαρχία και την πολιτική ακεραιότητα των κρατών, αλλά και την ανάγκη για ουσιαστικό καταμερισμό ευθύνης μετά την πραγμάτωση διεθνώς παράνομων πράξεων.²⁰⁵

Από την πλευρά της η Οικονομική και Δημοσιονομική Επιτροπή, έχει προβεί στην υιοθέτηση κειμένων αναφορικά με την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Ένα χαρακτηριστικό παράδειγμα αποτελεί, το Ψήφισμα 64/211 το οποίο υιοθετήθηκε από τη Γενική Συνέλευση στις 17/03/2010 αναφορικά με τη δημιουργία «παγκόσμιας κουλτούρας» στην κυβερνοασφάλεια, καλώντας τα κράτη,

²⁰⁴ United Nations, Office of the Disarmament Affairs, *Developments in the field of information and telecommunications in the context of international security*, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση <https://www.un.org/disarmament/ict-security/>

²⁰⁵ United Nations, General Assembly, A/RES/68/98, 24/06/2013, *Developments in the Field of information and telecommunications in the context of international security, Group of Experts on Developments in the field of Information and Telecommunications in the context of International Security*, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://undocs.org/A/68/98>

να αναπτύξουν και να υιοθετήσουν τις στρατηγικές εκείνες οι οποίες θα βελτιώσουν τη ασφάλειά τους από τις επικείμενες απειλές.²⁰⁶

6.2: Η Ευρωπαϊκή Ένωση

Φεύγοντας από το πεδίο του ΟΗΕ, η Ευρωπαϊκή Ένωση αποτελεί με τη σειρά της σημαντικό πυλώνα ως προς τη θέσπιση κειμένων αναφορικά με την προώθηση της ασφάλειας στον κυβερνοχώρο. Το πρώτο σημαντικό κείμενο υιοθετήθηκε το 2013 με τίτλο *Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace* όπου και εδώ δίνεται έμφαση στην ανάγκη εφαρμογής και σεβασμού των υπάρχουσών αρχών του Διεθνούς Δικαίου.²⁰⁷

Κρίνεται ακόμη απαραίτητο, να αναφερθούμε σε κάποια από τα όργανα του Οργανισμού τα οποία ασχολούνται με το κυβερνοέγκλημα. Κάποιες από αυτές είναι η Ευρωπαϊκή Υπηρεσία για την Ασφάλεια των Δικτύων και της Πληροφορίας “European Networks and Information Security Agency – ENISA”, η Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης για Υπολογιστές “Computer Emergency Response Team – CERT EU”, το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα “European Cybercrime Centre – EC3”, η Ευρωπαϊκή Υπηρεσία Πληροφοριών “European Police Office - EUROPOL», η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης «European External Action Service – EEAS”, το Στρατιωτικό Επιτελείο της ΕΕ “European Union Military Staff – EUMS”, και γ) η Ευρωπαϊκός Οργανισμός Άμυνας “European Defence Agency – EDA” και όχι μόνο.

Θα ήταν σημαντική μας παράλειψη η μη αναφορά στον σημαντικότερο ίσως πυλώνα του Ευρωπαϊκού Οικοδομήματος, το Συμβούλιο της Ευρώπης (ΣοΕ), που με

²⁰⁶ United Nations, General Assembly, A/RES/64/211, 17/03/2010, Resolution Adopted by the General Assembly on 21 December 2009, *Creation of global culture of cybersecurity and taking stock of National efforts to protect critical information infrastructures*, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση <https://undocs.org/A/RES/64/211>

²⁰⁷ European Union, European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>

σειρά κειμένων τα οποία υιοθετεί, θωρακίζει το Ευρωπαϊκό Οικοδόμημα. Ένα λοιπόν από τα σημαντικότερα κείμενα τα οποία υιοθέτησε είναι η Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα (The Budapest Convention on Cybercrime)²⁰⁸ η οποία συμπληρώνεται και από το πρόσθετο Πρωτόκολλο²⁰⁹, ενάντια στην ξеноφοβία και το Ρατσισμό. Πρόκειται για μία συνθήκη, η οποία δίνει ιδιαίτερη έμφαση στην ενίσχυση και την προώθηση εύρεσης τρόπων για τη στελέχωση της εθνικής νομοθεσίας ενός κράτους, δίνοντας επιπλέον ιδιαίτερη προσοχή στην ανάπτυξη της διεθνούς συνεργασίας για την όλο και αποτελεσματικότερη αντιμετώπιση των απειλών στην κυβερνοχώρο.

6.3: Οργανισμός Αμερικανικών Κρατών και Αφρικανική Ένωση

Στην προσπάθειά μας να κατανοήσουμε το πόσο οικουμενική έχει καταστεί η ανάγκη για ενίσχυση της γενικότερης δομής που αποτελεί, περιβάλλει και στηρίζει τον κυβερνοχώρο, αξίζει, να κάνουμε μία μικρή έστω αναφορά στο ότι και ο Οργανισμός Αμερικανικών Κρατών αλλά και η Αφρικανική Ένωση έχουν υπογράψει συνθήκες αναφορικά με την ενίσχυση της υποδομής και της ασφάλειας στον κυβερνοχώρο. Πιο συγκεκριμένα ο Οργανισμός Αμερικανικών κρατών έχει υιοθετήσει πληθώρα κειμένων αναφορικά με διάφορα ζητήματα, που άπτονται της ασφάλειας του τραπεζικού συστήματος από παράνομες δραστηριότητες και όχι μόνο.²¹⁰

Αναφορικά με την Αφρικανική Ένωση, στις 27/07/2014 υιοθετήθηκε η Σύμβαση για την Κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων, στην οποία αποτυπώνονται ρητώς οι πολιτικές της ένωσης αναφορικά με τα εν λόγω ζητήματα

²⁰⁸ European Union, Council of Europe, “The Budapest Convention on Cybercrime”, 2001, Πρόσβαση 3/10/2019, Διαθέσιμο στη Διεύθυνση https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_7_conv_budapest_en.pdf

²⁰⁹ Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg 28/01/2003, Πρόσβαση 3/10/2019, Διαθέσιμο στη Διεύθυνση <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f>

²¹⁰ Organization of American States, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp>

πάντα δίνοντας έμφαση στο σεβασμό των ανθρωπίνων δικαιωμάτων και των κανόνων του διεθνούς δικαίου.²¹¹

6.4: NATO

Το NATO είναι ένας οργανισμός ο οποίος έχει δώσει ιδιαίτερως μεγάλη έμφαση τόσο στην κυβερνοάμυνα όσο και εν γένει στη διερεύνηση των δυνατοτήτων του κυβερνοχώρου. Έχει εντάξει όλο αυτό το ζήτημα στην ημερήσια ατζέντα του, κάτι που φαίνεται ιδιαίτερως λογικό για έναν στρατιωτικό οργανισμό ο οποίος μάλιστα έχει χαρακτηρίσει τον κυβερνοχώρο ως το νέο επιχειρησιακό πεδίο. Δίνει έμφαση στην προάσπιση των συμφερόντων του κράτους από κυβερνοεπιθέσεις στον αέρα την ξηρά και τη θάλασσα. Επιπρόσθετα, ο οργανισμός εστιάζει τόσο στην πρόληψη και την αντιμετώπιση των κυβερνοεπιθέσεων, όσο και στην άμεση αποκατάσταση των ζημιών που προκαλούνται αλλά και την ανοικοδόμηση των ψηφιακών συστημάτων.²¹² Υπεύθυνα όργανα αναφορικά με θέματα του κυβερνοχώρου είναι η Επιτροπή Κυβερνοάμυνας “Cyber Defense Committee CDC” αλλά και το “NATO Computer Incident Response Capability – NCIRC” που αποτελεί μέρος της Υπηρεσίας Επικοινωνιών και Πληροφοριών “NATO Communications and Information Agency – NCIA”. Εν τέλη, θα ήταν παράβλεψη από μέρους μας η μη αναφορά μας στο κέντρο Αριστείας για την Κυβερνοάμυνα στο Ταλλίν της Εσθονίας με αξιοσημείωτο εκπαιδευτικό έργο. Η μεγάλης ισχύος κυβερνοεπίθεση της Ρωσίας έναντι της Εσθονίας το 2007 αποτέλεσε σημείο αναφοράς για το NATO μιας και θα λέγαμε πως το κομβικό αυτό σημείο έκανε τον Οργανισμό περισσότερο ενεργό ως προς τη βελτίωση των τεχνικών υποδομών αλλά και των «νομικών» σπουδαιότερα έγγραφα, είναι τα δύο εγχειρίδια του Ταλλίν στα οποία οι εμπειρογνώμονες του NATO προσπάθησαν να αποτυπώσουν λεπτομερώς κάθε έκφανση του Συμβατικού Διεθνούς Δικαίου στον κυβερνοχώρο, προκειμένου να καταστεί ακόμη πιο σαφής

²¹¹ African Union Convention on Cyber Security and Personal Data Protection, 27/06/2014, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση [https://au.int/sites/default/files/treaties/29560-treaty-0048 -_african union convention on cyber security and personal data protection e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

²¹² North Atlantic Treaty Organization, Cyber Defence, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση https://www.nato.int/cps/en/natohq/topics_78170.htm

ανάγκη για τον απόλυτο σεβασμό σε κάθε περίπτωση των θεσμικών κανόνων, που διέπουν τη διεθνή κοινωνία.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Έχοντας διανύσει όλο αυτό το ερευνητικό μονοπάτι, καταφέραμε να εντρυφήσουμε σε εκείνα τα σημεία τα οποία μας έκαναν, να κατανοήσουμε ακόμη περισσότερο το πως είναι δομημένο το διεθνές σύστημα αναφορικά με την ερμηνεία αλλά και την προστασία ενός κράτους από παράνομες ενέργειες, που το αναγκάζουν, να δέχεται επέμβαση στα ζητήματα, που άπτονται της αποκλειστικής δικαιοδοσίας τους.

Έτσι λοιπόν το ζήτημα της εφαρμογής του Διεθνούς Δικαίου στον κυβερνοχώρο εγείρει αρκετούς προβληματισμούς λόγω της ιδιαιτερότητάς του η οποία εστιάζει στο ακαθόριστο των συνόρων, στα όρια άσκησης δικαιοδοσίας και όχι μόνο, συμβάντα που στο συμβατικό δίκαιο δεν τίθενται κατ' αυτόν τον τρόπο υπό αμφισβήτηση. Αυτό που εύκολα παρατηρούμε όμως είναι προσκόλληση του Δικαίου στο κράτος. Φυσικά και δεν είναι κάτι το οποίο θα πρέπει, να αμφισβητείται, μόνο που με το πέρασ του χρόνου και την ανάπτυξη όλων αυτών των τεχνολογικών διευκολύνσεων, έρχεται η στιγμή, που ο εκσυγχρονισμός του δικαίου και η εναρμόνισή του με την εμφάνιση όλων αυτών των νέων δρώντων, σίγουρα θα το καταστήσει πιο αποτελεσματικό. Επιπρόσθετα, αυτό το οποίο απαιτείται, όπως προείπαμε και σε προηγούμενο σημείο της εργασίας μας, είναι ο εντοπισμός της παραβίασης και η αναζήτησή του εκεί που ουσιαστικά είναι η πηγή του. Εκεί, όπου διαμορφώνεται η κοινή γνώμη και γεννάται η επιθυμία για διαμόρφωση του τρόπου με τον οποίο οι πολίτες επιθυμούν, να διοικούνται.

Τόσο ο Οργανισμός των Ηνωμένων Εθνών, όσο και οι υπόλοιποι Διεθνείς Οργανισμοί αλλά και τα κράτη, που λαμβάνουν μέρος σε αυτά, επιβάλλεται να ενισχύσουν τις μεθόδους προστασίας τους από τέτοιου είδους ενέργειες, ενώ παράλληλα κρίνεται σκόπιμο θα θωρακισθεί το νομικό πλαίσιο το οποίο περικλείει τον κυβερνοχώρο, προκειμένου, να πάψει, να αποτελεί ένα όχι και τόσο χαρτογραφημένο πεδίο, όπου δύσκολα εναρμονίζονται με τη νομιμότητα.

Μόνο έτσι το Δίκαιο θα μπορέσει, να καταστεί ουσιαστικός και αποτελεσματικός συνοδοιπόρος μας για το μέλλον.

BIBΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΟΓΛΩΣΣΗ

- Αντωνόπουλος, Κ., Μαγλιβέρας, Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Β' Έκδοση, Νομική Βιβλιοθήκη
- Antonio Cassese, Διεθνές Δίκαιο, Αθήνα, Εκδόσεις Gutenberg, 2012
- Περράκης Στέλιος, Μαρούδα Μαρία Ντανιέλλα, Διεθνής Δικαιοταξία, Θεωρία και Εφαρμογή Διεθνούς Δικαίου, Τόμος Α', 2η Έκδοση, Εκδόσεις Σιδέρη Αθήνα, 2016
- Περράκης Στέλιος, Μαρούδα Μαρία – Ντανιέλλα, Έννοπλες συρράξεις και Διεθνές Ανθρωπιστικό Δίκαιο, Εκδόσεις Σάκκουλα, 2001
- Ρούκουνας Εμμανουήλ, Διεθνές Δίκαιο, Τεύχος πρώτο, Σχέσεις Εσωτερικού Διεθνούς Δικαίου – Τρόποι παραγωγής του Διεθνούς Δικαίου, Β' Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή, 1997
- Ρούκουνας Εμμ, Δημόσιο Διεθνές Δίκαιο, Νομική Βιβλιοθήκη, 2015

ΞΕΝΟΓΛΩΣΣΗ

- Bruno Simma, The Charter of the United Nations, A Commentary, Oxford University Press, 1995
- Christopher D. Baker, Tolerance of International Espionage: A Functional Approach, 2003 , American University International Law Review
- Christopher D. Baker, Tolerance of International Espionage: A Functional Approach, American University International Law Review, Volume 19, Issue 5, Article 2, 2003, p. 1108-1112
- Collin Anderson & Karim Sadjadpour, Iran's Cyber Threat, Espionage, Sabotage and Revenge, Carnegie Endowment For International Peace, 2018

- EJIL: Talk, Mary Ellen O'Connell, Drone Attacks on Saudi Aramco Oil Installations, published September 17, 2019
- Gray Cristine. International law and the Use of Force, 3d edition, New York, Oxford University Press, 2008
- Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer International Publishing Switzerland 2017
- Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017
- Mary Ellen O'Connell, Cyber Security without Cyber War, Journal of Conflict & Security Law Oxford University Press 2012;
- Nicholas Tsagourias, Russel Buchan Research Handbook on International Law and Cyberspace, Edward Elgar, 2015
- Non-State Actors and the Use of Force Christian Henderson, in M. Noortmann, A. Reinisch, and C. Ryngaert, Non-State Actors in International law (Oxford: Hart Publishing, 2014)
- Peterson Institute for International Economics February 23, 2000, Targeted Sanctions: A Policy Alternative?, "Targeted Measures: Arms Embargoes, Travel Bans and Asset Freezes"
- Shaw Malcolm, International Law, 6th edition, Cambridge, Cambridge University Press, 2008
- RAND Report "Ungoverned territories: Understanding and Reducing Terrorism Risks". (2007), Summary
- Robert Mueller, Special Counsel, Report On the Investigation Into the Russian In the 2016 Presidential Election, Volume I of II, March 2019

- Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume II: Russia's Use of Social Media with additional views
- Russell Buchan, The International Legal Regulation of State – Sponsored Cyber Espionage, International Legal Norms, Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016
- State Responsibility for Cyber Operations»: International Law Issues, British Institute of International and Comparative Law Charles Clore House, 17 Russell Square, London WC1B 5JP
- Thomas Giegerich, *Retorsion*, Oxford Public International Law, March 2011
- Uta Kohl, Jurisdiction in cyberspace, Research Handbook on International Law and Cyberspace, Nicholas Tsagourias, Russell Buchan, Edward Elgar Publishing Limited, UK, 2015
- Vladyslav Lanovoy, The Use of Force by Non State Actors and the Limits of Attribution of Conduct, The European Journal of International Law, Vol 28, no 2, 2017, published by Oxford University Press

ΣΥΜΒΑΤΙΚΑ ΚΕΙΜΕΝΑ: ΨΗΦΙΣΜΑΤΑ - ΣΥΜΒΑΣΕΙΣ

- African Union Convention on Cyber Security and Personal Data Protection, Διαθέσιμη στη διεύθυνση <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
- Assembly General, Resolution 3314 (XXIX) 1974, Definition of Aggression, United Nations Διαθέσιμο στη διεύθυνση <http://hrlibrary.umn.edu/instreet/GAres3314.html>
- Assembly General Resolution 1236 (1957) of December 4, “Peaceful and Neighborly Relations among States”, Διαθέσιμο στη Διεύθυνση <http://www.worldlii.org/int/other/UNGA/1957/158.pdf>
- Assembly General Resolution 2131 (1966) “Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty”, Διαθέσιμο στη Διεύθυνση, [https://undocs.org/en/A/RES/2131\(XX\)](https://undocs.org/en/A/RES/2131(XX))
- Assembly General, Resolution 2625, 24/10/1970 “Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations”, Διαθέσιμο στη διεύθυνση <https://legal.un.org/avl/ha/dpilfrscun/dpilfrscun.html>
- Assembly General, Res 56/83 (2002), Responsibility of States for internationally wrongful acts, United Nations, Διαθέσιμο στη Διεύθυνση [https://www.investorstatelawguide.com/documents/documents/OTI-0104%20-%20Responsibility%20of%20States%20for%20Internationally%20Wrongful%20Acts,%20UNGA%20Resolution56-83%20\(2002\)%20\(citation%20and%20source\).pdf](https://www.investorstatelawguide.com/documents/documents/OTI-0104%20-%20Responsibility%20of%20States%20for%20Internationally%20Wrongful%20Acts,%20UNGA%20Resolution56-83%20(2002)%20(citation%20and%20source).pdf)

- Assembly General Resolution 53/70 1990. Γενική Συνέλευση των Ηνωμένων Εθνών, Πρόσβαση 18/12/2019 Διαθέσιμο στη Διεύθυνση <https://undocs.org/en/A/RES/53/70>
- Assembly General Resolution 73/27 2018. Γενική Συνέλευση των Ηνωμένων Εθνών, 05/15/2018, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση, <https://undocs.org/pdf?symbol=en/A/RES/73/27>
- Assembly General Resolution 68/98, 24/06/2013, Developments in the Field of information and telecommunications in the context of international security, Group of Experts on Developments in the field of Information and Telecommunications in the context of International Security, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://undocs.org/A/68/98>
- Assembly General Resolution 64/211, 17/03/2010, Resolution Adopted by the General Assembly on 21 December 2009, Creation of global culture of cybersecurity and taking stock of National efforts to protect critical information infrastructures, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση <https://undocs.org/A/RES/64/211>
- Convention of The United Nations on the Law of the Sea, Διαθέσιμη στη Διεύθυνση https://www.un.org/depts/los/convention_agreements/texts/unclos/unclose.pdf
- Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2008, United Nations, Διαθέσιμο στη διεύθυνση https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
- European Union, European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,

Διαθέσιμο στη Διεύθυνση <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001>

- European Union, Council of Europe, “The Budapest Convention on Cybercrime”, 2001, Πρόσβαση 3/10/2019, Διαθέσιμο στη Διεύθυνση https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
- European Union, Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg 28/01/2003, Πρόσβαση 3/10/2019, Διαθέσιμο στη Διεύθυνση <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f>
- International Law Commission: Responsibility of States for Internationally Wrongful Acts, United Nations 2001, Διαθέσιμο στη Διεύθυνση <https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/International%20Law%20Commission%202001%20Draft%20Articles%20on%20State%20Responsibility.pdf>
- United Nations, General Assembly, A/RES/64/211, 17/03/2010, Resolution Adopted by the General Assembly on 21 December 2009, Creation of global culture of cybersecurity and taking stock of National efforts to protect critical information infrastructures, Διαθέσιμο στη Διεύθυνση http://emsa.europa.eu/e-learning/cybersec/AMC001/story_content/external_files/un091221.pdf
- The Charter of the United Nations, San Francisco 1945, Διαθέσιμο στη Διεύθυνση <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>
- Organization of American States, Cyber Policy Portal, updated May 2019

- Security Council Resolution Res SC/UN 788/1992: Διαθέσιμο στη Διεύθυνση [https://undocs.org/S/RES/788\(1992\)](https://undocs.org/S/RES/788(1992))
- ΟΑΣΕ: Οργανισμός για την ασφάλεια και τη συνεργασία στη Ευρώπη (κυβερνοέγκλημα και τρομοκρατία)
 1. Απόφαση Νο 3/04 COMBATING THE USE OF THE INTERNET FOR TERRORIST PURPOSES. Σόφια: OSCE. Ανάκτηση Νοέμβριος 14, 2016, από <https://ccdcoe.org/sites/default/files/documents/OSCE-041207-CombatingUseofInternet.pdf>
 2. Απόφαση 7/06 COUNTERING THE USE OF THE INTERNET FOR TERRORIST PURPOSES. Βρυξέλλες: OSCE. Ανάκτηση Νοέμβριος 14, 2016, από <https://ccdcoe.org/sites/default/files/documents/OSCE-061205-CounteringUseofInternet.pdf>
 3. Απόφαση 1106 INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. OSCE, Permanent Council. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/OSCE-131203-Confidencebuildingmeasures_0.pdf
 4. 2016, Μάρτιος). Απόφαση Νο. 1202 OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. OSCE, Permanent Council. Ανάκτηση Νοέμβριος 14, 2016, από <https://ccdcoe.org/sites/default/files/documents/OSCE-160310-NewCBMs.pdf>

ΑΠΟΦΑΣΕΙΣ ΔΙΚΑΣΤΗΡΙΩΝ

- Bosnia & Hergegovina v. Serbia & Montenegro, Application of the Convention on the Prevention and punishment of the crime of Genocide, 2007, Διαθέσιμο στη διεύθυνση <https://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-00-EN.pdf>
- Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America) 2003, Διαθέσιμο στη Διεύθυνση <https://www.icj-cij.org/files/case-related/90/090-20031106-JUD-01-00-EN.pdf>
- Case Concerning Armed Activities on the territory of Congo (Democratic Republic of the Congo v. Uganda), 19/12/2005, Διαθέσιμο στη διεύθυνση <https://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf>
- European Court of Human Rights, case of Loizidou v. Turkey, 23/03/1995, Διαθέσιμο στη διεύθυνση [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57920%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57920%22]})
- European Court, of Human Rights, Case of Ilascu & Others v. Moldova & Russia, Strasburg 08/07/2004, Διαθέσιμο στη Διεύθυνση [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-61886%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61886%22]})
- Legal consequences for States of the Continued Presence of South Africa In Namibia (South West Africa) Notwithstanding security council Resolution 276 (1971) Διαθέσιμο στη διεύθυνση <https://www.icj-cij.org/files/case-related/53/053-19710621-ADV-01-00-EN.pdf>
- Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion 08/07/1996, Διαθέσιμο στη διεύθυνση <https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>

- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 27/06/1986, Διαθέσιμο στη Διεύθυνση
<https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>
- Permanent, Court of International Justice, The Case of the SS “Lotus”, France v. Turkey 07/09/1927, Διαθέσιμο στη Διεύθυνση
http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm

ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

- AP NEWS, Researchers: “Russia – linked hackers targeted Macron campaign, Raphael Satter”, 25/04/2017, Πρόσβαση 18/11/2019,
<https://apnews.com/0fda6547810540699f009a2875c73b1d/Researchers:-Russia-linked-hackers-targeted-Macron-campaign%20;%20https://www.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html>
- BBC, *Putin: Patriotic Russians may be involved in hacking*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση
<https://www.bbc.com/news/technology-40122943>
- CNN, Tal Kopan, Kevin Liptak and Jim Sciutto, *Obama orders review of Russian election-related hacking*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση
<https://edition.cnn.com/2016/12/09/politics/obama-orders-review-into-russian-hacking-of-2016-election/>
- CNN, Evan Perez, Manu Raju and Deirdre Walsh, *Gap on Russia hacking conclusions between intelligence, FBI, Updated 1632 GMT (0032 HKT) December 12, 2016*
- CNN, *2016 Presidential Campaign Hacking Fast Facts*, CNN library, Updated 1710 GMT (0110 HKT) October 31, 2019,
<https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

- CNN, Tal Kopan, *DHS officials: 21 states potentially targeted by Russia hackers pre-election*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html>
- CNN, Katelyn Polantz and Stephen Collinson, *12 Russians indicted in Mueller investigation*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html>
- Crowdstrike, *Bears in the Midst: Intrusion into the Democratic National Committee*, πρόσβαση 17/12/2019, Διαθέσιμο στη Διεύθυνση <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
- DW, *“Drone attacks set Saudi Aramco oil facilities ablaze”*, Διαθέσιμο στη Διεύθυνση <https://www.dw.com/en/drone-attacks-set-saudi-aramco-oil-facilities-ablaze/a-50430391>
- EJIL: Talk, Mary Ellen O’ Connell, *“Drone Attacks on Saudi Aramco Oil Installations”*, published September 17, 2019, Διαθέσιμο στη διεύθυνση <https://www.ejiltalk.org/drone-attacks-on-saudi-aramco-oil-installations/>
- EJIL: Talk!, Nicholas Tsagourias, *“Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace”*, published August 26, 2019 Διαθέσιμο στη διεύθυνση <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/>

- European Union, European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *“Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”*, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>
- Homeland Security, *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>
- In the United States District Court for the District of Columbia, p 2, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2018/02/16/politics/mueller-indictment-13-russian-nationals/index.html>
- Permanent Mission of Greece to the UN, Sanctions Διαθέσιμο στη Διεύθυνση <https://www.mfa.gr/missionsabroad/en/un-en/greece-in-organization/peace-and-security.html?page=5>
- Peterson Institute for International Economics February 23, 2000, Targeted Sanctions: A Policy Alternative?, *“Targeted Measures: Arms Embargoes, Travel Bans and Asset Freezes”* Διαθέσιμο στη Διεύθυνση, <https://piie.com/commentary/speeches-papers/targeted-sanctions-policy-alternative>
- RAND Report *“Ungoverned territories: Understanding and Reducing Terrorism Risks”*. (2007), Summary, σελ. Xv, 2007, Διαθέσιμο στη Διεύθυνση https://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.pdf
- *Russia hacking Donald Trump spicer smerconish_00000000*, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση <https://edition.cnn.com/2016/12/11/politics/russia-hacking-conclusions-donald-trump/index.html>
- The Washington Post, *“Russian Government Hackers penetrated DNC”*, stole opposition research on Trump, Πρόσβαση 17/11/2019, Διαθέσιμο στη Διεύθυνση, <https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/>

research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

- The Strategy Bridge, “Cybersecurity as Attack-Defense: What the French Election Taught Us About Fighting Back”, Youri Cormier, September 12, 2018, https://thestrategybridge.org/the-bridge/2018/9/12/cybersecurity-as-attack-defense-what-the-french-election-taught-us-about-fighting-back?fbclid=IwAR0dC2tQZZGIX3CCHJoCSEvMAdFQLoLIq_QMRpl4WZkZbvo72HjysTf_yCU
- Le Monde, “Visites, financement: le Front national et la Russie, une idylle qui dure, La rencontre officielle entre Marine Le Pen et Vladimir Poutine, le 24 mars, est l’aboutissement de plusieurs années de prises de position prorusses du parti d’extrême droite.” Laura Motet, 18/11/2016, Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση https://www.lemonde.fr/les-decodeurs/article/2016/11/18/le-front-national-et-la-russie-une-idylle-qui-dure_5033857_4355770.html
- North Atlantic Treaty Organization, Cyber Defence, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση https://www.nato.int/cps/en/natohq/topics_78170.htm
- North Atlantic Treaty Organization, Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, Πρόσβαση 17/12/2019, Διαθέσιμο στη Διεύθυνση https://www.nato.int/cps/en/natohq/opinions_166039.htm
- United Nations, Office of the Disarmament Affairs, “Developments in the field of information and telecommunications in the context of international security”, Πρόσβαση 18/12/2019, Διαθέσιμο στη διεύθυνση <https://www.un.org/disarmament/ict-security/>

- The New York Times, *“Hackers Came, but the French Were Prepared”*, Adam Nossiter, David E. Sanger, Nicole Perlroth, 09/05/2017, Πρόσβαση 18/11/2019, Διαθέσιμο στη Διεύθυνση <https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html>
- Thomas Giegerich, *Retorsion*, Oxford Public International Law, March 2011, Πρόσβαση 18/12/2019, Διαθέσιμο στη Διεύθυνση <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e983>

ΕΠΙΠΡΟΣΘΕΤΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Abele, D. (2016). *Cyberwar, International Politics, and Institutional Design*. Retrieved from The University of Chicago Law Review.
- Austin, G. (2016). *International Legal Norms in Cyberspace: Evolution of China’s National Security Motivations*. Retrieved from CCDCOE.
- Gervais, M. (2012). *Cyber Attacks and the Laws of War*. Retrieved from BERKELEY JOURNAL OF INTERNATIONAL LAW.
- KILOVATY, I. (2015). *RETHINKING THE PROHIBITION ON THE USE OF FORCE IN THE LIGHT OF ECONOMIC CYBER WARFARE: TOWARDS A BROADER SCOPE OF ARTICLE 2(4) OF THE UN CHARTER*. Retrieved from JOURNAL OF LAW AND CYBER WARFARE.
- Simma, B. (n.d.). *NATO, the UN and the Use of Force: Legal Aspects*. Retrieved from EJIL.

- Obama Order Sped Up Wave of Cyberattacks Against Iran. (2012, Ιούνιος 1).
Ανάκτηση Ιανουάριος 29, 2017, από The New York Times:
<https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?smid=pl-share&mtrref=undefined&gwh=3C2B0AA2834ED1CE04C54180C9ECB281&gw-t=pay&assetType=REGIWALL>
- *Prosecutor v Bemba (Judgment) ICC-01/05-01/08*. (2016, Μάρτιος 21).
Διαθέσιμο στη Διεύθυνση https://www.icc-cpi.int/CourtRecords/CR2016_02238.PDF
- *Prosecutor v Blaskic (Judgment) IT-95-14-A*. (2004, Ιούλιος 29). Διαθέσιμο στη Διεύθυνση <http://www.icty.org/x/cases/blaskic/aciug/en/bla-aj040729e.pdf>
- Remus, T. (2013). *Cyber-attacks and International law of armed conflicts; a “jus ad bellum” perspective*. Retrieved from Journal of International Commercial Law and Technology .
- Tonkin, H. (2011). *State Control over Private Military and Security Companies in Armed Conflict*.
- Watts, S. (2012). *“The Notion of Combatancy in Cyber Warfare”*. Retrieved from CCDCOE.