ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΙΚΩΝ & ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ ΚΑΙ ΔΙΠΛΩΜΑΤΙΚΕΣ ΣΠΟΥΔΕΣ

Διπλωματική Εργασία

«Σύγχρονες προκλήσεις στον κυβερνοχώρο: νόμιμη άμυνα και συλλογική ασφάλεια στον ευρωατλαντικό χώρο»

ΠΕΤΡΟΣ ΖΑΜΠΑΚΟΛΑΣ (Α.Μ. 1215Μ006)

Επιβλέπουσα: Μαρία-Ντανιέλλα Μαρούδα

Αθήνα, Ιανουάριος 2017

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.

Η παρούσα εργασία είναι από καρδιάς αφιερωμένη στη μικρούλα και λατρεμένη μου κόρη, για όλες εκείνες τις ώρες που στερήθηκε την παρουσία μου, την αγάπη μου και το παιχνίδι μου μαζί της.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ

ΣΥΝΤΗΜΗΣΗ	**ΕΠΕΞΗΓΗΣΗ ΣΥΝΤΜΗΣΗΣ**
Ελληνικές συντμήσεις	
ΔΑΔ	Διεθνές Ανθρωπιστικό Δίκαιο
ΔΠΔπΓ	Διεθνές ad hoc Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία
ΕΔΔ	Επιτροπή Διεθνούς Δικαίου
ΕΕ	Ευρωπαϊκή Ένωση
Η.Ε.	Ηνωμένα Έθνη
Η.Π.Α.	Ηνωμένες Πολιτείες Αμερικής
ΚΕΠΠΑ	Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας
Ο.Η.Ε.	Οργανισμός Ηνωμένων Εθνών
ΣΛΕΕ	Συνθήκη Λειτουργίας Ευρωπαϊκής Ένωσης
Αγγλικές Συντμήσεις	
ANSSI	National Network and Information Security Agency
ASR	Articles for State Responsibility
CASIC	China Aerospace Science & Industry Corporation
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDC	Cyber Defence Committee
CEPOL	European Police College
CERT	Computer Emergency Response Team
CSDF	Common Security and Defence Policy (ΚΕΠΠΑ)
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoD	Department of Defence
DoS	Denial of Service
EC3	European Cybercrime Centre
EDA	European Defence Agency
EEAS	European External Action Service
ENISA	European Networks and Information Security Agency
EP3R	European Public-Private Partnership for Resilience
EU	European Union
EUROJUST	European Justice
EUMS	European Union Military Staff
EUROPOL	European Police Office
GGE	Group of Governmental Experts
HRC	Human Rights Council
ICTs	Information and Communications Technologies
ISIS	Islamic State in Iraq and Syria
JHA	Justice and Home Affairs
MLC	Movement for the Liberation of the Congo
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

ΣΥΝΤΗΜΗΣΗ	**ΕΠΕΞΗΓΗΣΗ ΣΥΝΤΜΗΣΗΣ**
OSCE	Organization for Security and Co-operation in Europe
RES	Resolution
SCO	Shanghai Cooperation Organisation
UCC	United Cyber Caliphate
UK	United Kingdom
UN	United Nations
UNHRC	United Nations Human Rights Council
US	United States

ΠΡΟΛΟΓΟΣ

> «…Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter.…»[1] (Ban Ki-moon, Γενικός Γραμματέας Ηνωμένων Εθνών, Ιούνιος 2015)

Είναι ο κυβερνοχώρος η μεγαλύτερη πρόκληση του Διεθνούς Δικαίου στη σύγχρονη εποχή; Διαθέτει το Διεθνές Δίκαιο το απαραίτητο δικαιϊκό και θεσμικό οπλοστάσιο, ώστε να μπορεί να αντιμετωπίσει μία από τις μεγαλύτερες, κατά γενική ομολογία, σύγχρονες, ασύμμετρες απειλές που εξελίσσεται ραγδαία στο εν λόγω πεδίο, διασφαλίζοντας τη διεθνή ειρήνη και ασφάλεια στο παγκόσμιο γεωπολιτικό περιβάλλον;

Η παρούσα εργασία επιχειρεί να προσεγγίσει τις νέες αυτές προκλήσεις που αφορούν στην εφαρμογή των κανόνων εθιμικού και συμβατικού Διεθνούς Δικαίου στις περιπτώσεις εκδήλωσης επιθέσεων στο πεδίο του κυβερνοχώρου. Για τον σκοπό αυτό εξετάζονται οι υφιστάμενοι διεθνοδικαιϊκοί κανόνες που πλαισιώνουν το θεσμικό πλαίσιο της γενικότερης έννοιας της επίθεσης, της νόμιμης άμυνας και της συλλογικής ασφάλειας, τόσο σε διακρατικό επίπεδο, όσο και στο επίπεδο των κυριότερων Διεθνών Οργανισμών που δραστηριοποιούνται στον ευρω-ατλαντικό χώρο. Το Διεθνές Δίκαιο φαίνεται να καλείται να επικρατήσει σε μία διελκυστίνδα μεταξύ της εκ νέου ερμηνείας των ήδη υπαρχόντων κανόνων του και της κωδικοποίησης και δημιουργίας νέων.

Η επιλογή του συγκεκριμένου θέματος, βασίστηκε στην επιθυμία να καταστώ, μέσα από τη σχετική έρευνα που διεξήγαγα, κοινωνός των σημαντικών προβληματισμών που παράγει αυτή η σύγχρονη μορφή απειλής στον κυβερνοχώρο.

---

[1] (2016, Ιούλιος). Ενημερωτικό Δελτίο. Γραφείο για ζητήματα Αφοπλισμών των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 20, 2016, από https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/07/Information-Security-Fact-Sheet-July2016.pdf

ΕΙΣΑΓΩΓΗ

Οι επιθέσεις στον κυβερνοχώρο καθίστανται ολοένα και πιο απειλητικές, όχι μόνο για τα εκάστοτε πληροφοριακά και επικοινωνιακά συστήματα (ICTs) τα οποία αποτελούν τον κύριο «στόχο» τους, αλλά και για τον ίδιο τον άνθρωπο. Αναλόγως της έκτασης και της φύσης των συστημάτων για τα οποία προορίζονται, είναι ικανές να απειλήσουν ακόμα και την ίδια την ανθρώπινη ζωή.

Η ανάγκη να παραμείνει ο κυβερνοχώρος σταθερός και ασφαλής είναι αναμφισβήτητη, προϋποθέτει, όμως, την εξασφάλιση και περαιτέρω ανάπτυξη της διεθνούς συνεργασίας, στη βάση των κανόνων του Διεθνούς Δικαίου και των προβλέψεων του Χάρτη των Η.Ε.. Αυτό, άλλωστε, τόνισε και ο Γενικός Γραμματέας των Ηνωμένων Εθνών *Ban Ki-Moon* τον Ιούνιο του 2015, στην εισαγωγική του τοποθέτηση κατά την εξέταση της περιοδικής αναφοράς της διακυβερνητικής ομάδας εμπειρογνωμόνων των Η.Ε. (GGE) για τις εξελίξεις στο πεδίο των ICTs, στο πλαίσιο της διεθνούς ασφάλειας (βλ. σχετική δήλωσή του στην αρχή του προλόγου της παρούσας εργασίας).

Έτσι, θα εξεταστεί, πρώτα, το ισχύον θεσμικό πλαίσιο που αφορά στις έννοιες της χρήσης βίας, της επίθεσης και της νόμιμης άμυνας, ως προς το Διεθνές Δίκαιο, καθώς και τυχόν προεκτάσεις τους, στο βαθμό που αυτές θα μπορούσαν να χρησιμοποιηθούν, κατά τη διαδικασία εκτίμησης εφαρμογής των εν λόγω διεθνοδικαιϊκών κανόνων στον κυβερνοχώρο. Συναφώς, θα εξεταστεί, θεσμικά και η συλλογική ασφάλεια, στο πλαίσιο των Διεθνών Οργανισμών του ευρω-ατλαντικού στερεώματος.

Η όσο το δυνατόν, ορθότερη εκτίμηση των προεκτάσεων του Διεθνούς Δικαίου που δύνανται να εφαρμοστούν στην περίπτωση των απειλών και των επιθέσεων στο πεδίο του κυβερνοχώρου, προϋποθέτουν την όσο το δυνατόν πιο εμπεριστατωμένη κατανόηση των επιθέσεων που έχουν ήδη λάβει χώρα στο παρελθόν, ιδιαίτερα αυτών που εκδηλώθηκαν εναντίον κρίσιμων κρατικών δομών. Στο πλαίσιο αυτό, εξετάζονται οι περιπτώσεις των ιδιαίτερα σημαντικών και εκτεταμένων κυβερνοεπιθέσεων στην Εσθονία (2007) και Γεωργία (2008), καθώς και μία σειρά άλλων περιστατικών που έθεσαν σε κίνδυνο, όχι μόνο την ασφάλεια του κυβερνοχώρου, αλλά ακόμα και τη διεθνή ειρήνη και ασφάλεια.

Επίσης, για την πληρότητα της εικόνας, θα διερευνηθούν και οι υφιστάμενες στρατηγικές κυβερνοάμυνας και κυβερνοασφάλειας, τόσο σε επίπεδο εθνικό, με αναφορά στα ισχυρότερα κράτη στο υπόψη πεδίο, όσο και σε επίπεδο Διεθνών Οργανισμών, προκειμένου να γίνει κατανοητή η αντίληψη που έχουν οι παραπάνω δρώντες, όσον αφορά το μέγεθος των απειλών στον κυβερνοχώρο.

Τα προαναφερόμενα στοιχεία που πρόκειται να εξεταστούν στη συνέχεια της παρούσας εργασίας, θα αποτελέσουν, ουσιαστικά, τη βάση για την εξαγωγή των τελικών συμπερασμάτων, για αυτό το επίκαιρο ζήτημα που απασχολεί τη σύγχρονη διεθνή δικαιοταξία και ολόκληρη τη διεθνή κοινότητα.

ΜΕΡΟΣ Α' – Το θεσμικό πλαίσιο της κυβερνοάμυνας στη διεθνή δικαιοταξία

ΚΕΦΑΛΑΙΟ 1
Κυβερνοχώρος: το επιχειρησιακό πεδίο του μέλλοντος

Προτού εξεταστούν οι κανόνες εκείνοι του Διεθνούς Δικαίου, οι προεκτάσεις των οποίων ενδεχομένως να βρίσκουν εφαρμογή στον κυβερνοχώρο, κρίνεται σκόπιμο να προσδιοριστεί η έννοια του πεδίου αυτού, προκειμένου να γίνουν περισσότερο κατανοητές οι ιδιαιτερότητές του. Ο κυβερνοχώρος, λοιπόν, αποτελεί αδιαμφισβήτητα ένα σύγχρονο και ξεχωριστό πεδίο δράσεων. Σύμφωνα με τον Διεθνή Οργανισμό Τυποποίησης είναι ένα *πολύπλοκο περιβάλλον στο οποίο αλληλοεπιδρούν πρόσωπα, λογισμικά προγραμμάτων και υπηρεσίες στο διαδίκτυο, μέσω τεχνολογικών συσκευών και δικτύων που είναι συνδεδεμένα σε αυτό, το οποίο δε συναντάται σε οποιαδήποτε «φυσική μορφή»*[2]. Κατά τις Η.Π.Α., σε μία αρκετά πιο απλουστευμένη εκδοχή του εν λόγω ορισμού, αποτελεί ένα *φανταστικό περιβάλλον στο οποίο λαμβάνει χώρα επικοινωνία μεταξύ δικτύων υπολογιστών*[3]. Πλέον η χρήση υπολογιστών, πληροφοριακών και επικοινωνιακών συστημάτων και γενικότερα του διαδικτύου είναι ιδιαίτερα διαδεδομένη, όχι μόνο σε ατομικό επίπεδο, αλλά και σε κρατικές, χρηματοπιστωτικές/οικονομικές και άλλες υπηρεσίες και δραστηριότητες. Ωστόσο, η ιδιαίτερα διευρυμένη χρήση των συστημάτων αυτών, πολλαπλασίασε εν τέλει την τρωτότητά τους, καθιστώντας τις κυβερνοεπιθέσεις σημαντική απειλή όχι μόνο για την εύρυθμη λειτουργία τους, αλλά ακόμα και για την ειρήνη και ασφάλεια στο διεθνή χώρο.

Το στοιχείο της απειλής στο υπόψη πεδίο εισάγουν με αρκετή σαφήνεια τα Ηνωμένα Έθνη[4] προσδιορίζοντας τον κυβερνοχώρο ως ένα *εύθραυστο και ανασφαλές περιβάλλον, που έχει επιτρέψει σε εγκληματικές οργανώσεις να επιτίθενται και κατά περίπτωση να το καταστρέφουν, εξαιτίας της προτεραιότητας που έχει δοθεί για την ικανοποίηση συγκεκριμένων εμπορικών και αγοραστικών*

[2] Cyber Definitions. Ανάκτηση Νοέμβριος 19, 2016, από NATO Cooperative Cyber Defence Centre of Excellence, Tallin Esthonia: https://ccdcoe.org/cyber-definitions.html
[3] Ibid.
[4] Ibid.

αντικειμενικών σκοπών. Η επικινδυνότητα των αποτελεσμάτων των απειλών και των επιθέσεων στο πεδίο του κυβερνοχώρου αποτελούν, ουσιαστικά, τον βασικό πυρήνα των προβληματισμών και των προκλήσεων που καλείται να ανταποκριθεί το Διεθνές Δίκαιο και ολόκληρη διεθνής κοινότητα στη σύγχρονη εποχή.

Η επικινδυνότητα αυτή, ειδικά σε διακρατικό επίπεδο έχει ήδη επισημανθεί από πολλούς κρατικούς και διεθνείς δρώντες. Χαρακτηριστική είναι η δήλωση του τέως Γενικού Γραμματέα του ΝΑΤΟ *Anders Fogh Rasmussen*, ο οποίος είχε δηλώσει:

> «…Και οι κυβερνοεπιθέσεις είναι ένα τέλειο παράδειγμα επειδή μπορεί να προκαλέσουν καταστροφικές επιπτώσεις στην οικονομία και στις δομές ενός κράτους χωρίς ούτε ένας στρατιώτης να διασχίσει τα σύνορα. Χωρίς να ριχθεί ούτε ένας πυροβολισμός…»[5]

Η επικινδυνότητα, όμως, των κυβερνοαπειλών έχει προεκτάσεις και στην τρομοκρατία, με τον μέχρι πρότινος Πρόεδρο των Η.Π.Α. *Barack Obama* να δηλώνει:

> «…Στο σημερινό κόσμο οι τρομοκρατικές ενέργειες μπορούν να προέλθουν όχι μόνον από εξτρεμιστές με γιλέκα αυτοκτονίας, αλλά από μερικά κτυπήματα στο πληκτρολόγιο του υπολογιστή: ένα όπλο μαζικής καταστροφής…»[6]

Ιδιαίτερα μετά τις σοβαρές κυβερνοεπιθέσεις εναντίον της Εσθονίας (2007), ξεκίνησε μία παγκόσμια προσπάθεια κατανόησης των ιδιαιτεροτήτων του ξεχωριστού, αυτού, πεδίου του κυβερνοχώρου, σε διακρατικό και πολυεθνικό επίπεδο, καθόσον έγινε αντιληπτό ότι η γνώση αυτή, θα συμβάλλει ουσιαστικά στην αποτελεσματική αντιμετώπιση και αποτροπή των εν λόγω απειλών. Στο πλαίσιο των προσπαθειών αυτών, αξιοσημείωτη είναι η προσπάθεια που έγινε από μία ευρεία ομάδα έγκριτων επιστημόνων και ακαδημαϊκών καθηγητών στο Κέντρο Αριστείας Κυβερνοάμυνας στο Τάλλιν της Εσθονίας, η οποία μετά από πολλές συσκέψεις, κατέληξαν το 2013 στην εκπόνηση ενός ιδιαίτερα χρήσιμου προϊόντος, σε συνεργασία με το Πανεπιστήμιο της Οξφόρδης. Πρόκειται για το *Εγχειρίδιο του Τάλλιν περί της εφαρμογής του Διεθνούς Δικαίου στον*

[5] Κίνα και Δύση: συγκρούσεις πληκτρολογίων;. (n.d.). Ανάκτηση Νοέμβριος 20, 2016, από Δελτίο ΝΑΤΟ: http://www.nato.int/docu/review/2009/Asia/china_cyber_attacks/GR/index.htm
[6] Ibid.

Κυβερνοπόλεμο[7], γνωστό και ως *Εγχειρίδιο Τάλλιν*. Η δεύτερη, μάλιστα, έκδοση του εν λόγω εγχειριδίου, με σαφή προσανατολισμό προς τις επιχειρήσεις στον κυβερνοχώρο (*The International Law applicable to Cyber Operations*), αναμένεται να εκδοθεί μέχρι τα τέλη 2016.

Το ανωτέρω εγχειρίδιο συνιστά ένα σύνολο κανόνων (rules), οι οποίοι όμως δεν είναι νομικά δεσμευτικοί, ακόμα και για το ΝΑΤΟ, στο Κέντρο Αριστείας του οποίου προετοιμάστηκε, επεξεργάστηκε και εκπονήθηκε. Συγκεντρώνουν, ωστόσο, έναν μεγάλο αριθμό «απαντήσεων», στους περισσότερους προβληματισμούς οι οποίοι έχουν δημιουργηθεί, κατά την εξέταση εφαρμογής του Διεθνούς Δικαίου στον κυβερνοχώρο. Επίσης, εξίσου σημαντικό είναι και το ερευνητικό προϊόν το οποίο έχει παραχθεί και συνεχίζει να παράγεται την τελευταία δεκαετία, στις συσκέψεις της διακυβερνητικής ομάδας εμπειρογνωμόνων των Ηνωμένων Εθνών (GGE), όπως αναλύεται σε επόμενο κεφάλαιο της παρούσης εργασίας.

[7] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html

ΚΕΦΑΛΑΙΟ 2
Η χρήση βίας και η έννοια της επίθεσης στο Διεθνές Δίκαιο

Πριν την εξέταση των κυβερνοεπιθέσεων ως μορφή «επίθεσης» και προκειμένου να καταστεί περισσότερο ξεκάθαρη η όποια εφαρμογή του Διεθνούς Δικαίου στο πεδίο του Κυβερνοχώρου, κρίνεται σκόπιμο να γίνει πρώτα αναφορά στις έννοιες της χρήσης βίας και της επίθεσης στο Διεθνές Δίκαιο και κατόπιν να επιχειρηθεί ο όποιος συσχετισμός με τα χαρακτηριστικά εκείνα στοιχεία που πλαισιώνουν μία κυβερνοεπίθεση.

2.1 Προβλέψεις Χάρτη Ηνωμένων Εθνών.

Η σύσταση του Οργανισμού Ηνωμένων Εθνών μετά το πέρας του Β' Παγκοσμίου Πολέμου και ειδικότερα η σύσταση του Χάρτη του οργανισμού, διαμόρφωσαν έκτοτε ένα ισχυρό θεσμικό πλαίσιο κανόνων για τη διατήρηση της παγκόσμιας ειρήνης και σταθερότητας. Η εφαρμογή των κανόνων αυτών στον κυβερνοχώρο αποτελεί μία από τις σημαντικότερες προκλήσεις του Διεθνούς Δικαίου στη σύγχρονη εποχή. Σημαντικές βάσεις προς την κατεύθυνση αυτή έχουν ήδη τεθεί από το ίδιο το Διεθνές Δικαστήριο της Χάγης, το οποίο στη γνωμοδότησή του για τη *νομιμότητα απειλής ή χρήσης των πυρηνικών όπλων* (1996) διευκρίνισε με σαφήνεια ότι τα άρθρα 2(4), 42 και 51[8] του Χάρτη των Ηνωμένων Εθνών δεν αναφέρονται σε συγκεκριμένα όπλα και ότι εφαρμόζονται σε κάθε είδους χρήση βίας, ανεξάρτητα από το χρησιμοποιούμενο όπλο[9]:

> «…These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed…»

Η τοποθέτηση αυτή του Διεθνούς Δικαστηρίου ουσιαστικά νομιμοποιεί, κατά μία έννοια, το θεμελιώδες άρθρο του Χάρτη των Ηνωμένων Εθνών περί

[8] (1996, Ιούλιος). LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS. INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/95/7495.pdf (παρ. 38)
[9] Ibid. παρ. 39

απαγόρευσης απειλής ή χρήσης βίας και στον κυβερνοχώρο, ως ένα διαφορετικό «όπλο»[10]. Επίσης, ζήτημα τίθεται και ως προς την εφαρμογή ή μη του άρθρου 2(7)[11] του Χάρτη περί απαγόρευσης ανάμειξης στις εσωτερικές υποθέσεις ενός κράτους, υπό την έννοια ότι μία κυβερνοεπίθεση μπορεί να θεωρηθεί, υπό προϋποθέσεις, ως τέτοια.

2.1.1 Άρθρο 2, παρ. 4 (απαγόρευση απειλής ή χρήσης βίας)

Αναφορικά με την χρήση βίας, μετά τις αρχικές προσπάθειες της Κοινωνίας των Εθνών και το «Σύμφωνο Briand – Kellogg», ο Χάρτης των Ηνωμένων Εθνών έφερε την τελική γενική απαγόρευση της. Η αναφορά στο άρθρο 2, παρ. 4 του Χάρτη είναι σαφής:

> «…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…»[12]

Η ανωτέρω διατύπωση του εν λόγω άρθρου του Χάρτη, δεν προϋποθέτει απαραίτητα ότι οι ενέργειες που θα παραβιάζουν τις ανωτέρω προβλέψεις, θα πρέπει να αναφέρονται αποκλειστικά σε απειλή ή χρήση βίας άμεσα κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας ενός κράτους, αρκεί αυτές (οι ενέργειες) να είναι αντίθετες προς τις αρχές και τους σκοπούς του Χάρτη των Ηνωμένων Εθνών[13]. Επίσης, σύμφωνα με την απόφαση του Διεθνούς Δικαστηρίου της Χάγης στην υπόθεση *Νικαράγουα* (1986), η εν λόγω απαγόρευση αποτελεί αναμφισβήτητα κανόνα και του εθιμικού Διεθνούς Δικαίου:

---

[10] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 42-43)

[11] Ibid.

[12] (1945). Χάρτης των Ηνωμένων Εθνών. Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf (άρθρο 2, παρ.4)

[13] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 43, κανόνας 10, παρ. 2)

> «…The Court thus finds that both Parties take the view that the principles as to the use of force incorporated in the United Nations Charter correspond, in essentials, to those found in customary international law…»[14]

Η επέκταση της ισχύος της απαγόρευσης χρήσης βίας και στο εθιμικό Διεθνές Δίκαιο, πρακτικά συνεπάγεται ότι θα ισχύει και για κράτη τα οποία δεν είναι μέλη των Ηνωμένων Εθνών, στα οποία αναφέρεται άμεσα ο Χάρτης[15], σύμφωνα και με το συναφές άρθρο 2(6) αυτού[16]. Στην περίπτωση που η απειλή ή χρήση βίας ασκείται από μη κρατικούς δρώντες, το εν λόγω άρθρο δεν εφαρμόζεται, εκτός εάν οι ανωτέρω ενέργειες αποδοθούν σε συγκεκριμένο κράτος το οποίο να σχετίζεται με οποιονδήποτε τρόπο με τους σκοπούς και τις επιδιώξεις των μη κρατικών δρώντων και για το οποίο υφίσταται εκ των πραγμάτων η έννοια της κρατικής ευθύνης[17].

Το υπόψη άρθρο του Χάρτη (όπως και όλος ο Χάρτης) δεν αναφέρεται σε συγκεκριμένα κριτήρια, με βάση τα οποία να δύναται να καθοριστεί με σαφήνεια πότε μία ενέργεια αποτελεί ξεκάθαρη χρήση βίας (use of force). Το Διεθνές Δικαστήριο στην υπόθεση *Νικαράγουα*[18] επισήμανε ότι θα πρέπει να αξιολογείται κάθε φορά η φύση των εκάστοτε ενεργειών (nature of the acts), υπογραμμίζοντας, συναφώς, τη σπουδαιότητα ορθής εκτίμησης της έκτασης και των αποτελεσμάτων (scale and effects) των εν λόγω πράξεων.

Η Γενική Συνέλευση των Ηνωμένων Εθνών, στη *Διακήρυξη των αρχών του Διεθνούς Δικαίου που αφορούν στις φιλικές σχέσεις και τη συνεργασία μεταξύ των*

---

[14] (1986). CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf (παρ. 188-190)

[15] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 43, κανόνας 10, παρ. 5)

[16] «…6. The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security…»

[17] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (κανόνας 6)

[18] (1986). CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf (παρ. 195)

κρατών, σύμφωνα με τον Χάρτη των Ηνωμένων Εθνών[19] (1970) επανέλαβε το λεκτικό του άρθρου 2(4) του Χάρτη, εισάγοντας, μεταξύ άλλων, την έννοια της επιθετικότητας/επίθεσης (aggression) ως εγκληματική πράξη ενάντια στη διεθνή ειρήνη. Παράλληλα έκανε σαφή αναφορά σε ένα σύνολο άλλων ενεργειών, μικρότερης βαρύτητας, που δύνανται να αποτελούν πράξεις βίας.

2.1.2 Άρθρο 2, παρ. 7 (αρχή μη επέμβασης στο εσωτερικό άλλων κρατών)

Μία κυβερνοεπίθεση που δε θεωρείται ότι παραβιάζει την αρχή της απαγόρευσης χρήσης βίας, βάση του άρθρου 2(4) του Χάρτη των Ηνωμένων Εθνών, δύναται να θεωρηθεί ότι παραβιάζει την *αρχή της μη παρέμβασης στις εσωτερικές υποθέσεις ενός κράτους*[20], σύμφωνα με τις προβλέψεις του άρθρου 2, παρ. 7 του Χάρτη:

> «…7. 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…»[21]

Οι ανωτέρω προβλέψεις έχουν συμπεριληφθεί, σχεδόν με το ίδιο λεκτικό και στη Διακήρυξη για τις φιλικές σχέσεις και τη συνεργασία μεταξύ των κρατών (1970):

> «…The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter…»[22]

---

[19] (1970). A/RES/25/2625. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από http://www.un-documents.net/a25r2625.htm

[20] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 44, κανόνας 10, παρ. 6)

[21] (1945). Χάρτης των Ηνωμένων Εθνών. Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf (άρθρο 2, παρ.7)

[22] (1970). A/RES/25/2625. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από http://www.un-documents.net/a25r2625.htm

Επίσης, έχουν συμπεριληφθεί και στη *Διακήρυξη των Ηνωμένων Εθνών περί μη αποδοχής της παρέμβασης στις εσωτερικές υποθέσεις των κρατών και περί προστασίας της ανεξαρτησίας και της κυριαρχίας τους*[23] (1965). Στο εν λόγω κείμενο, υπάρχει σαφή αναφορά περί απαγόρευσης κάθε προσπάθειας παρέμβασης, ένοπλης ή μη, στις εσωτερικές και εξωτερικές υποθέσεις ενός κράτους, άμεσα ή έμμεσα και ανεξαρτήτου λόγου.

> «…1. No State 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 condemned…»[24]

Στην ανωτέρω διακήρυξη γίνεται, επιπλέον, αναφορά στο στοιχείο του εξαναγκασμού (coercion), υπογραμμίζοντας την υποχρέωση των κρατών να μη χρησιμοποιούν οικονομικά, πολιτικά ή άλλα μέτρα για να τον επιτύχουν, προκειμένου να διεκδικήσουν, σε οποιοδήποτε βαθμό, κυριαρχικά και μη δικαιώματα τρίτων κρατών:

> «…2. No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind…»[25]

Συναφώς, το Διεθνές Δικαστήριο της Χάγης, στην υπόθεση *Νικαράγουα* (1986), επανέλαβε τη σημασία του στοιχείου του εξαναγκασμού, ως βασικό παράγοντα για τον χαρακτηρισμό μίας παρέμβασης στις εσωτερικές υποθέσεις άλλων κρατών ως μη αποδεκτή, σύμφωνα με το Διεθνές Δίκαιο, ιδιαίτερα σε πολιτικά, οικονομικά, κοινωνικά και πολιτιστικά ζητήματα, καθώς και σε ζητήματα εξωτερικής πολιτικής:

> «…One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The

[23] (1965). A/RES/20/2131. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από http://www.un-documents.net/a20r2131.htm
[24] Ibid. παρ. 1
[25] Ibid. παρ. 2

> element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversiveor terrorist armed activities within another State…»[26]

Τέλος, στην ίδια υπόθεση, το Διεθνές Δικαστήριο επισήμανε ότι η αρχή της μη επέμβασης στο εσωτερικό άλλων κρατών [άρθρο 2(7)] αποτελεί, επίσης, αναπόσπαστο μέρος του εθιμικού Διεθνούς Δικαίου[27] («*…part and parcel of customary international law…»).*

2.2 Ψήφισμα 3314 (1974) της Γενικής Συνέλευσης των Η.Ε. περί «Επίθεσης».

Το στοιχείο της επιθετικότητας/επίθεσης (aggression), όπως αυτό αναφέρθηκε στη *Διακήρυξη των Ηνωμένων Εθνών περί των αρχών του Διεθνούς Δικαίου που αφορούν στις φιλικές σχέσεις και τη συνεργασία μεταξύ των κρατών, σύμφωνα με τον Χάρτη των Ηνωμένων Εθνών*, επεξηγήθηκε με σαφήνεια λίγα χρόνια αργότερα, με την Απόφαση 3314 (XXIX) της Γενικής Συνέλευσης (1974)[28].

Σύμφωνα με αυτή[29], επίθεση είναι *η χρήση ένοπλης δύναμης από ένα Κράτος κατά της κυριαρχίας, εδαφικής ακεραιότητας ή πολιτικής ανεξαρτησίας ενός άλλου κράτους ή κατά οποιοδήποτε τρόπο ασυμβίβαστο με τον Χάρτη των Ηνωμένων Εθνών*.

---

[26] (1986). CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf (παρ. 205)

[27] Ibid. (παρ. 202)

[28] (1974). 3314 (XXIX). Definition of Aggression. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

[29] Κρατερός, Ι. Μ., & Περράκης, Σ. Ε. (1990). Γενικό και Ειδικό Διεθνές Δίκαιο. Αθήνα-Κομοτηνή: ΣΑΚΚΟΥΛΑ. (σελ. 97-100)

> «…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 the United Nations, as set out in this Definition…»[30]

Στο δεύτερο άρθρο της εν λόγω απόφασης, επισημαίνεται ο prima facie χαρακτηρισμός της πρώτης χρήσης ένοπλης βίας από ένα κράτος, ως επιθετική πράξη:

> «…The first use of armed force by a State in contravention of the Charter shall constitute *prima facie* evidence of an act of aggression…»[31]

Στο τρίτο άρθρο της απόφασης γίνεται μία καταγραφή μίας σειράς πράξεων που θα χαρακτηρίζονται «επιθετικές», ανεξάρτητα από την κήρυξη ή μη πολέμου, η απαρίθμηση των οποίων δεν είναι εξαντλητική[32], υπό την επιφύλαξη σχετικής απόφασης του Συμβουλίου Ασφαλείας των Ηνωμένων Εθνών. Σύμφωνα με το άρθρο αυτό, οι πράξεις αυτές είναι[33]:

α. Η εισβολή ή επίθεση, από τις ένοπλες δυνάμεις ενός Κράτους, του εδάφους ενός άλλου Κράτους ή στρατιωτική κατοχή οποιασδήποτε μορφής και οσοδήποτε προσωρινή, που αυτήν την εισβολή ή επίθεση, καθώς και οποιαδήποτε προσάρτηση του εδάφους ενός άλλου κράτους ή τμήματός του με τη χρήση βίας.

β. Ο βομβαρδισμός από τις ένοπλες δυνάμεις ενός Κράτους κατά του εδάφους άλλου κράτους ή η χρήση οιωνδήποτε όπλων κατά του εδάφους άλλου κράτους.

γ. Ο αποκλεισμός των λιμένων ή των ακτών ενός Κράτους από τις ένοπλες δυνάμεις άλλου Κράτους.

δ. Η επίθεση από τις ένοπλες δυνάμεις ενός Κράτους στις χερσαίες, θαλάσσιες ή αεροπορικές δυνάμεις, ή στο στόλο πλοίων και αεροσκαφών ενός άλλου Κράτους.

---

[30] (1974). 3314 (XXIX). Definition of Aggression. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement (άρθρο 1)

[31] Ibid. άρθρο 2

[32] Ibid. άρθρο 4

[33] Κρατερός, Ι. Μ., & Περράκης, Σ. Ε. (1990). Γενικό και Ειδικό Διεθνές Δίκαιο. Αθήνα-Κομοτηνή: ΣΑΚΚΟΥΛΑ. (σελ. 99)

ε. *Η χρησιμοποίηση των ενόπλων δυνάμεων ενός κράτους που βρίσκονται στο έδαφος ενός άλλους κράτους με τη συμφωνία του τελευταίου, κατά παράβαση των όρων που προβλέπονται στη σχετική συμφωνία ή οποιαδήποτε παράταση της παραμονής τους στο έδαφος αυτό και μετά τη λήψη της συμφωνίας.*

στ. Η άδεια ενός Κράτους, το οποίο έχει θέσει το έδαφός του στη διάθεση ενός άλλου Κράτους, να χρησιμοποιηθεί το έδαφος αυτό από το τελευταίο Κράτος για την πραγματοποίηση επιθετικής πράξης κατά του τρίτου Κράτους.

ζ. Η αποστολή εκ μέρους ή για λογαριασμό ενός Κράτους ενόπλων συμμοριών, ομάδων, ατάκτων ή μισθοφόρων που πραγματοποιούν κατά άλλου Κράτους πράξεις ένοπλης βίας τέτοιας βαρύτητας ώστε είτε να ισοδυναμούν με τις πράξεις που καταγράφονται παραπάνω είτε να εμπλέκουν ουσιαστικά τέτοιες πράξεις.[34]

2.3 Κυβερνοεπίθεση.

Σύμφωνα με το εγχειρίδιο του Τάλλιν[35], κυβερνοεπίθεση καλείται μία επιχείρηση στο πεδίο του κυβερνοχώρου, επιθετικού ή αμυντικού χαρακτήρα, η οποία αναμένεται ότι θα προκαλέσει τραυματισμό ή θάνατο σε ανθρώπους ή βλάβη ή καταστροφή σε αντικείμενα:

> «…A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects…»

Κατά τις Η.Π.Α.[36], κυβερνοεπίθεση είναι μία επίθεση στο πεδίο του κυβερνοχώρου που αποσκοπεί στη διακοπή, απενεργοποίηση, καταστροφή ή

[34] (1974). 3314 (XXIX). Definition of Aggression. General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement (άρθρο 3)

[35] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 106, κανόνας 30)

[36] Kissel, R. (2013). Glossary of Key Information Security Terms (NISTIR 7298, Revision 2). U.S. Department of Commerce. Ανάκτηση Νοέμβριος 19, 2016, από http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (σελ. 57)

μόλυνση με κακόβουλο λογισμικό (ιό) ενός περιβάλλοντος υπολογιστών ή στην καταστροφή ή υποκλοπή πληροφοριών, εστιάζοντας εμφανώς περισσότερο στο τεχνικό μέρος και λιγότερο στον ανθρώπινο παράγοντα, σε σχέση με τον ορισμό του εγχειριδίου του Τάλλιν:

> «…An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information…»

Εξίσου τεχνικός είναι και ορισμός που αποδίδεται από το Ηνωμένο Βασίλειο[37], κάνοντας λόγο στα πιθανά αίτια που οδηγούν στην εκδήλωση μιας κυβερνοεπίθεσης (πολιτικά ή οικονομικά), καθώς επίσης και στις επιπτώσεις στα πληροφοριακά συστήματα:

> «…The term cyber attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorised access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)…»

Ενδιαφέρον παρουσιάζει μία άλλη εκδοχή του ορισμού της κυβερνοεπίθεσης η οποία αποδόθηκε σε ένα *εγχειρίδιο κρίσιμης ορολογίας* που εκπονήθηκε μεταξύ Η.Π.Α. και Ρωσίας, στο πλαίσιο των διμερών τους σχέσεων[38]. Η εν λόγω εκδοχή του ορισμού της κυβερνοεπίθεσης, αναφέρεται σε αυτή με τον χαρακτηρισμό «κυβερνο-όπλο», η επιθετική χρήση του οποίου γίνεται με σκοπό να βλάψει έναν προκαθορισμένο στόχο:

> «…an offensive use of a cyber weapon intended to hard designated target…»

[37] Cyber Definitions. (n.d.). Ανάκτηση Νοέμβριος 19, 2016, από NATO Cooperative Cyber Defence Centre of Excellence, Tallin Esthonia: https://ccdcoe.org/cyber-definitions.html

[38] (2014). Critical Terminology Foundations 2 (Russia-U.S. Bilateral on Cybersecurity). EastWest Institute. Ανάκτηση Νοέμβριος 19, 2016, από https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

Γίνεται, λοιπόν, σαφές ότι η κυβερνοεπίθεση από τη φύση της είναι ένας ιδιαίτερος τύπος επίθεσης, που δεν εμπίπτει στις διατάξεις της προαναφερόμενης απόφασης 3314 της Γενικής Συνέλευσης των Ηνωμένων Εθνών, περί του ορισμού της επίθεσης (aggression). Μία κυβερνοεπίθεση εναντίον υπολογιστικών συστημάτων, με σκοπό την απλή υποκλοπή δεδομένων δεν μπορεί να χαρακτηριστεί ισοδύναμη με μία φυσική επίθεση εναντίον προσώπων ή αντικειμένων[39]. Μπορεί, ωστόσο, να προκαλέσει τραυματισμούς ή ακόμα και απώλειες ανθρωπίνων ζωών, χωρίς την παραμικρή βλάβη των συστημάτων που γίνονται αποδέκτες των κυβερνοεπιθέσεων. Αυτό δύναται να συμβεί, εάν π.χ. μία κυβερνοεπίθεση στοχεύσει στα συστήματα ελέγχου μίας μεγάλης εγκατάστασης φράγματος και απελευθερώσει, με τη βοήθεια κατευθυνόμενων ηλεκτρονικών εντολών από έναν μακρινό υπολογιστή, τεράστιους όγκους νερού να κινηθούν ανεξέλεγκτα, απειλώντας άμεσα ανθρώπινες ζωές. Το αποτέλεσμα θα ήταν το ίδιο στην περίπτωση που το φράγμα γινόταν στόχος βομβαρδιστικής επίθεσης. Στη δεύτερη, όμως, περίπτωση η έννοια της επίθεσης είναι περισσότερο ξεκάθαρη[40]. Αυτός είναι και ο λόγος για τον οποίο στην περίπτωση των κυβερνοεπιθέσεων, θα πρέπει να εξετάζονται ενδελεχώς το εύρος και οι επιπτώσεις των αποτελεσμάτων τους και όχι μόνο η φύση του εκάστοτε στόχου.

Στο Δίκαιο των Ενόπλων Συρράξεων και με βάση τον επίσημο σχολιασμό των Πρόσθετων Πρωτοκόλλων της 8ης Ιουνίου 1977 στις Συνθήκες της Γενεύης του 1949, επισημαίνεται ότι η έννοια της επίθεσης, κοινή για τις διεθνείς και μη συρράξεις, έχει ένα βασικό χαρακτηριστικό στοιχείο. Αυτό της χρήσης βίας (violation):

> «…'Attacks' means acts of violence against the adversary, whether in offence or defence..»[41]

Κατά συνέπεια, είναι προφανές ότι οι μη βίαιες επιχειρήσεις (non-violent operations), όπως μία κυβερνοεπίθεση που εκδηλώνεται για άσκηση ψυχολογικής

[39] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 107-108, κανόνας 30, παρ. 6)
[40] Ibid. (σελ. 107, κανόνας 30, παρ. 5)
[41] (1987). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. International Committee of the Red Cross. Ανάκτηση Νοέμβριος 19, 2016, από http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf

πίεσης (ψυχολογική κυβερνοεπίθεση) ή για κατασκοπεία (κυβερνο-κατασκοπεία) δε θεωρείται επίθεση.

Το εγχειρίδιο του Τάλλιν εξετάζει μία σειρά συγκεκριμένων παραγόντων[42] τους οποίους τα κράτη θα μπορούσαν να λάβουν υπόψη τους, προκειμένου να προβούν στις απαραίτητες εκτιμήσεις περί απόδοσης του χαρακτηρισμού της «χρήσης βίας» στις κυβερνοεπιθέσεις.

Οι ανωτέρω παράγοντες, οι οποίοι δεν αποτελούν επίσημα κριτήρια, νομικά δεσμευτικά, είναι οι παρακάτω:

α. Η σοβαρότητα (severity) της κυβερνοεπίθεσης, εξετάζοντας το σκοπό, τη διάρκεια και την ένταση των συνεπειών, καθώς και το εύρος των προκληθέντων σωματικών βλαβών και των ζημιών, σε άτομα και υλικά αντίστοιχα. Πόσοι, δηλαδή, άνθρωποι έχασαν τη ζωή τους, πόσο μεγάλο τμήμα μιας περιοχής δέχθηκε επίθεση ή πόσες ζημιές προκλήθηκαν στην εν λόγω περιοχή.

β. Η αμεσότητα (immediacy) της κυβερνοεπίθεσης, υπό την έννοια του χρονικού διαστήματος εντός του οποίου εκδηλώνεται, λαμβάνοντας υπόψη ότι μία σύντομη και μαζική κυβερνοεπίθεση, είναι πιο πιθανό και εύκολο να χαρακτηριστεί ως πράξη βίας (use of force). Σε πόσο χρόνο, δηλαδή, έγιναν αισθητά τα αποτελέσματα της κυβερνοεπίθεσης ή σε πόσο χρόνο αυτά υποχώρησαν.

γ. Η αμεσότητα (directness) της κυβερνοεπίθεσης, υπό την έννοια της άμεσης πρόκλησης των συνεπειών της, όχι από την άποψη του χρόνου, αλλά εξετάζοντας τα στάδια που μεσολαβούν από την αρχική εκδήλωση της επίθεσης μέχρι να γίνουν ορατά τα πρώτα αποτελέσματά της. Εάν ήταν, δηλαδή, η κυβερνοεπίθεση η άμεση αιτία των προκληθέντων αποτελεσμάτων ή εάν υπήρχαν επιπρόσθετες αιτίες που συνέβαλαν στην πρόκληση των συνεπαγόμενων συνεπειών.

δ. Η έκταση της εισβολής στα υπολογιστικά συστήματα-«στόχοι» από μία κυβερνοεπίθεση (invasiveness), υπό την έννοια του υφιστάμενου βαθμού δυσκολίας, για την επίτευξη της υπόψη «εισβολής» στα συγκεκριμένα συστήματα. Εάν, δηλαδή, το κυβερνο-δίκτυο που δέχτηκε την επίθεση θα έπρεπε να ήταν

[42] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 48-51, κανόνας 11, παρ. 9)

κρυπτογραφημένο/ασφαλισμένο ή εάν η κυβερνοεπίθεση προήλθε από τη χώρα στην οποία βρίσκεται ο «στόχος». Ο εν λόγω παράγοντας είναι ιδιαίτερα σημαντικός στη σύγχρονη κυβερνο-κατασκοπεία.

ε. Η δυνατότητα «μέτρησης» των αποτελεσμάτων μιας κυβερνοεπίθεσης (measurability of effects), όπως π.χ. ο όγκος των δεδομένων που διακινήθηκαν κατά τη διάρκεια της επίθεσης, ο αριθμός των εξυπηρετητών/servers που τέθηκαν εκτός λειτουργίας ή ο αριθμός των διαβαθμισμένων αρχείων τα οποία υπεκλάπησαν. Πως, δηλαδή, μπορούν να μετρηθούν τα αποτελέσματα μιας κυβερνοεπίθεσης, εάν τα αποτελέσματά της διαφέρουν από αυτά άλλων παράλληλων ή συμπληρωματικών ενεργειών ή πόσο σωστή είναι η εκτίμηση/υπολογισμός των εν λόγω συνεπειών.

στ. Ο τυχόν στρατιωτικός χαρακτήρας της κυβερνοεπίθεσης (military character), υπό την έννοια ότι μία κυβερνοεπίθεση που εκδηλώνεται παράλληλα με στρατιωτικές επιχειρήσεις, είναι πιο πιθανό και εύκολο να χαρακτηριστεί επίσης ως χρήση βίας (use of force). Εάν, δηλαδή, η κυβερνοεπίθεση εκτελέστηκε από τον στρατό ή εάν οι ένοπλες δυνάμεις ήταν ο στόχος της κυβερνοεπίθεσης. Εξάλλου, οι στρατιωτικές επιχειρήσεις από τη φύση τους συνδέονται άμεσα με την έννοια της χρήσης βίας, συμπέρασμα το οποίο προκύπτει, λαμβάνοντας υπόψη τον Χάρτη των Ηνωμένων Εθνών, τόσο στο προοίμιό του[43], όσο και στο άρθρο 44[44], στο οποίο γίνεται αναφορά στη χρήση βίας (use force), υπονοώντας σαφώς από τη συνέχεια του άρθρου τις στρατιωτικές δυνάμεις.

ζ. Ο βαθμός εμπλοκής του κράτους (state involvement), τόσο υπό την έννοια της παράλληλης εκδήλωσης δράσεων από τις ένοπλες δυνάμεις και τις υπηρεσίες πληροφοριών του εν λόγω κράτους, όσο και της ύπαρξης ξεκάθαρης σχέσης ενός ή περισσοτέρων κρατών με μία κυβερνοεπίθεση. Εάν, δηλαδή, το κράτος ενεπλάκη άμεσα ή έμμεσα στην υπόψη κυβερνοεπίθεση.

---

[43] «…to ensure, by the acceptance of principles and the institution of methods, that armed forces shall not be used, save in the common interest…» (1945). Χάρτης των Ηνωμένων Εθνών. Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf

[44] «…Art.44: When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces in fulfillment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces…» (1945). Χάρτης των Ηνωμένων Εθνών. Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf

η. Η ύπαρξη ή μη τεκμήριου νομιμότητας (presumptive legality), υπό την έννοια ότι μία πράξη που δεν απαγορεύεται επιτρέπεται, λαμβάνοντας υπόψη και το γεγονός ότι το Διεθνές Δίκαιο είναι από τη φύση του «απαγορευτικό» (Υπόθεση *Lotus*[45]). Εάν, δηλαδή, μια κυβερνοεπίθεση έχει χαρακτηριστεί ή όχι ως χρήση βίας ή αν τα μέσα που χρησιμοποιήθηκαν είναι ποιοτικά όμοια με άλλα τα οποία είναι νόμιμα κατά το Διεθνές Δίκαιο. Σε γενικές γραμμές, πράξεις οι οποίες δεν είναι παράνομες από το Διεθνές Δίκαιο (π.χ. ψυχολογικές επιχειρήσεις ή κατασκοπεία), καθίστανται πιο εύκολο να μη χαρακτηριστούν ως χρήση βίας (use of force).

[45] (1927). COLLECTION OF JUDGMENTS, THE CASE OF THE S.S. "LOTUS". PERMANENT COURT OF INTERNATIONAL JUSTICE. Ανάκτηση Νοέμβριος 19, 2016, από http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf (σελ. 19)

ΚΕΦΑΛΑΙΟ 3
Η νόμιμη άμυνα και η συλλογική ασφάλεια στο πλαίσιο Διεθνών Οργανισμών

Μετά την εξέταση της χρήσης βίας και της επίθεσης στο Διεθνές Δίκαιο, καθώς επίσης και των τυχόν προϋποθέσεων προκειμένου να χαρακτηριστεί μία κυβερνοεπίθεση ως τέτοια (χρήση βίας ή επίθεση), κρίνεται σκόπιμο να συνεξεταστούν οι αρχές της νόμιμης άμυνας και της συλλογικής ασφάλειας στο πλαίσιο των Διεθνών Οργανισμών, παράλληλα με την έννοια της κυβερνοάμυνας στη σύγχρονη εποχή.

3.1 Οργανισμός Ηνωμένων Εθνών (Άρθρο 51 Χάρτη Η.Ε.)

Η αρχή της απαγόρευσης απειλής ή χρήσης βίας, σύμφωνα με τις προβλέψεις του άρθρου 2(4) του Χάρτη των Ηνωμένων Εθνών αλλά και της Διακήρυξης *2625* των Ηνωμένων Εθνών περί φιλικών σχέσεων και συνεργασίας μεταξύ των κρατών, έχει δύο σημαντικές και νόμιμες εξαιρέσεις[46]. Η πρώτη αφορά την περίπτωση που η χρήση στρατιωτικών μέτρων είναι σύμφωνη με σχετική απόφαση του Συμβουλίου Ασφαλείας των Ηνωμένων Εθνών, σύμφωνα με τις προβλέψεις του άρθρου 39 του Χάρτη, ως προς το άρθρο 42[47]:

> «…Art.39: 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 decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security…»[48]

[46] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 43, κανόνας 10, παρ. 2)

[47] *«…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…*». (1945). Χάρτης των Ηνωμένων Εθνών. Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf (άρθρο 41)

[48] Ibid. (άρθρο 39)

Μέχρι σήμερα, δεν έχει υιοθετηθεί σχετική απόφαση του Συμβουλίου Ασφαλείας που να αφορά επίθεση στο πεδίο του κυβερνοχώρου. Η δεύτερη εξαίρεση, αφορά την εφαρμογή των προβλέψεων του άρθρου 51 του Χάρτη, σύμφωνα με το οποίο:

> «…Art.51: Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security…»[49]

Το εν λόγω, λοιπόν, άρθρο του Χάρτη, ενεργοποιεί ουσιαστικά το δικαίωμα της ατομικής ή συλλογικής άμυνας ενός κράτους, στην περίπτωση που αυτό θα δεχθεί ένοπλη επίθεση. Τι ισχύει όμως στην περίπτωση που το κράτος δεχτεί μία μη ένοπλη επίθεση, όπως είναι οι κυβερνοεπιθέσεις; Θα ισχύουν, στην περίπτωση αυτή, οι προβλέψεις του άρθρου 51; Στα ερωτήματα αυτά έχει απαντήσει ήδη το Διεθνές Δικαστήριο της Χάγης στη *γνωμοδότησή του για την νομιμότητα των πυρηνικών όπλων*[50], σύμφωνα με την οποία δεν έχει σημασία ο τύπος του όπλου (άρα και η εκδήλωση ένοπλης ή μη επίθεσης), προκειμένου να ισχύει ή όχι το εν λόγω άρθρο. Εξάλλου, το ίδιο το δικαστήριο στην υπόθεση *Νικαράγουα,* έκρινε ότι δεν ισοδυναμεί πάντα η χρήση βίας με μία ένοπλη επίθεση[51]. Έτσι μία επίθεση με χρήση ραδιολογικών, βιολογικών και χημικών ουσιών σε μεγάλη έκταση και ένταση ώστε να δύναται να θεωρηθεί ισοδύναμη με ένοπλη επίθεση, λόγω της συνεπειών που έχει στην ανθρώπινη ζωή, θα μπορούσε να ενεργοποιήσει το

[49] Ibid. (άρθρο 51)
[50] (1996, Ιούλιος). LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS. INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/95/7495.pdf (παρ. 39)
[51] (1986). CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf (παρ. 191)

δικαίωμα της νόμιμης άμυνας[52]. Με την ίδια λογική, αυτό μπορεί να συμβεί και στην περίπτωση μιας κυβερνοεπίθεσης. Απουσία συγκεκριμένων θεσμικά κριτηρίων που να χαρακτηρίζουν μία ενέργεια ως χρήση βίας, η διεθνής ομάδα εργασίας εμπειρογνωμόνων που συνέταξε το εγχειρίδιο Τάλλιν, κατέληξε στο συμπέρασμα ότι κάθε χρήση βίας που προκαλεί τον τραυματισμό ή το θάνατο στους ανθρώπους ή βλάβες ή καταστροφές σε περιουσίες, ικανοποιεί τις προϋποθέσεις που την καθιστούν αντίθετη με τις προβλέψεις περί απαγόρευσης απειλής ή χρήσης βίας[53]. Έτσι, μία κυβερνοεπίθεση που στοχεύει μία εγκατάσταση καθαρισμού πόσιμου νερού, δύναται να προκαλέσει το θάνατο σε πολλές ανθρώπινες ζωές που θα δηλητηριαστούν πίνοντας το υπόψη νερό. Στην περίπτωση αυτή, παρόλο που ο άμεσος στόχος είναι τα υπολογιστικά μηχανήματα της εγκατάστασης καθαρισμού του νερού, οι τελικές συνέπειες έχουν θανατηφόρα επίδραση σε πολλές ανθρώπινες ζωές και εάν υποτεθεί ότι ο αριθμός των απωλειών υγείας ανέλθει σε αρκετά μεγάλα ποσοστά, παρόμοια με αυτά που θα προκαλούσε κάποια εκτεταμένη ένοπλη επίθεση, τότε το δικαίωμα της νόμιμης άμυνας δύναται, κατά πάσα πιθανότητα, να ενεργοποιηθεί.

3.2 Ευρωπαϊκή Ένωση

2.1.3 Ρήτρα Αμοιβαίας Συνδρομής Ευρωπαϊκής Ένωσης (Άρθρο 42, παρ. 7 της Συνθήκης Ευρωπαϊκής Ένωσης)

Με τη Συνθήκη της Λισσαβώνας, η οποία τέθηκε σε ισχύ το 2009, επήλθαν σημαντικές τροποποιήσεις θεσμικού χαρακτήρα στον τομέα της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (ΚΕΠΠΑ), η οποία θεσμοθετήθηκε για πρώτη φορά με τη Συνθήκη του Μάαστριχτ (τέθηκε σε ισχύ το 1993). Μία από τις πιο σημαντικές αλλαγές ήταν η πρόβλεψη μίας Ρήτρας Αμοιβαίας Συνδρομής (άρθρο 42, παρ. 7 της Συνθήκης για την Ευρωπαϊκή Ένωση), σύμφωνα με την οποία:

[52] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 54-55, κανόνας 13, παρ. 3)
[53] Ibid. (σελ. 55, κανόνας 13, παρ. 6)

> «…7. Σε περίπτωση κατά την οποία κράτος μέλος δεχθεί ένοπλη επίθεση στο έδαφός του, τα άλλα κράτη μέλη οφείλουν να του παράσχουν βοήθεια και συνδρομή με όλα τα μέσα που έχουν στη διάθεσή τους, σύμφωνα με το άρθρο 51 του Καταστατικού Χάρτη των Ηνωμένων Εθνών. Αυτό δεν επηρεάζει τον ιδιαίτερο χαρακτήρα της πολιτικής ασφάλειας και άμυνας ορισμένων κρατών μελών…»[54]

Σε αντιστοιχία με το άρθρο 51 του Χάρτη των Ηνωμένων Εθνών, το οποίο και επικαλείται, το ανωτέρω άρθρο αναφέρεται στο δικαίωμα της νόμιμης άμυνας ενός κράτους, κατόπιν εκδήλωσης ένοπλης επίθεσης προς το έδαφός του.

Η εν λόγω ρήτρα, μέχρι σήμερα έχει ενεργοποιηθεί μία φορά, μετά τις τρομοκρατικές επιθέσεις της 15ης Νοεμβρίου 2015 στο Παρίσι, κατόπιν σχετικού αιτήματος για επίκληση από τη Γαλλία[55].

2.1.4 Ρήτρα Αλληλεγγύης Ευρωπαϊκής Ένωσης (Άρθρο 222 της Συνθήκης Λειτουργίας Ευρωπαϊκής Ένωσης)

Με τη Συνθήκη της Λισσαβώνας εισήχθη, επίσης, η Ρήτρα Αλληλεγγύης της Ευρωπαϊκής Ένωσης, η οποία, σύμφωνα με το άρθρο 222 της Συνθήκης Λειτουργίας της (ΣΛΕΕ) προβλέπει ότι:

> «…η Ένωση και τα κράτη μέλη της ενεργούν από κοινού, με πνεύμα αλληλεγγύης, εάν ένα κράτος μέλος δεχθεί τρομοκρατική επίθεση ή πληγεί από φυσική ή ανθρωπογενή καταστροφή. Η Ένωση κινητοποιεί όλα τα μέσα που έχει στη διάθεσή της, συμπεριλαμβανομένων των στρατιωτικών μέσων που θέτουν στη διάθεσή της τα κράτη μέλη, για:
>
> α. την πρόληψη τρομοκρατικής απειλής στο έδαφος των κρατών μελών, την προστασία των δημοκρατικών θεσμών και του άμαχου πληθυσμού από ενδεχόμενη τρομοκρατική επίθεση, την παροχή συνδρομής σε κράτος μέλος στο έδαφός του, μετά από αίτηση των πολιτικών του αρχών, σε περίπτωση τρομοκρατικής επίθεσης

[54] (2016). Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Ανάκτηση Νοέμβριος 20, 2016, από http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EL (Σελ. 39)

[55] Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (ΚΕΠΠΑ). (n.d.). Ανάκτηση Νοέμβριος 20, 2016, από ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ, Υπουργείο Εξωτερικών: http://www.mfa.gr/exoteriki-politiki/i-ellada-stin-ee/keppa.html

> β. την παροχή συνδρομής σε κράτος μέλος στο έδαφός του, μετά από αίτηση των πολιτικών του αρχών, σε περίπτωση φυσικής ή ανθρωπογενούς καταστροφής…» (παρ. 1)

Λεπτομέρειες για την εφαρμογή του εν λόγω άρθρου καθορίζονται και συντονίζονται από το Συμβούλιο της Ευρωπαϊκής Ένωσης, σύμφωνα με τις προβλέψεις των παρ. 2 και 3 του άρθρου 222 της υπόψη συνθήκης (ΣΛΕΕ).

Όπως προκύπτει από τα ανωτέρω αλλά και από την παρ.2 του ίδιου άρθρου[56], η παροχή συνδρομής προς το κράτος μέλος που δέχεται την επίθεση αφορά περιπτώσεις τρομοκρατικής απειλής και φυσικής ή ανθρωπογενούς καταστροφής. Κατά συνέπεια, με βάση των ανωτέρω διατύπωση, η πρόκληση καταστροφής λόγω κυβερνοεπίθεσης εκτιμάται ότι δεν αποκλείει την πιθανότητα επίκλησης του εν λόγω άρθρου, υπό την προϋπόθεση ότι εξεταστούν ενδελεχώς η έκταση και τα αποτελέσματά της.

3.3 ΝΑΤΟ (Άρθρο 5 Ιδρυτικής Συνθήκης Ουάσιγκτον 1949)

Στη Στρατηγική Θεώρηση (Strategic Concept) του ΝΑΤΟ το 2010, τα κράτη μέλη συμφώνησαν και αποτύπωσαν τους τρεις βασικούς άξονες (core tasks) της Συμμαχίας της Συμμαχίας: συλλογική άμυνα (collective defence), συνεργατική ασφάλεια (cooperative security) και διαχείριση κρίσεων (crisis management)[57]. Το θεμελιώδες άρθρο της συλλογικής άμυνας στην ιδρυτική συνθήκη του ΝΑΤΟ[58], είναι το άρθρο 5, σύμφωνα με το οποίο:

> «…Art.5: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and

[56] «*Σε περίπτωση που κράτος μέλος δεχθεί τρομοκρατική επίθεση ή πληγεί από φυσική ή ανθρωπογενή καταστροφή, τα υπόλοιπα κράτη μέλη του παρέχουν βοήθεια κατόπιν αιτήματος των πολιτικών του αρχών. Προς τον σκοπό αυτό, τα κράτη μέλη συντονίζονται στο πλαίσιο του Συμβουλίου*».

[57] (2010, Νοέμβριος). Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-101120-StrategicConcept.pdf (σελ. 7-8, παρ. 4)

[58] (1949). The North Atlantic Treaty. Washington D.C.: NATO. Ανάκτηση Νοέμβριος 19, 2016, από http://www.nato.int/cps/en/natohq/official_texts_17120.htm

consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security…»

Το αίτημα για ενεργοποίηση του εν λόγω άρθρου προέρχεται από το κράτος μέλος που έχει δεχτεί την επίθεση προς το ανώτατο πολιτικό όργανο της συμμαχίας που είναι το Βορειοατλαντικό Συμβούλιο (North Atlantic Council – NAC), το οποίο, αφού ακούσει την ενημέρωση από το ανωτέρω κράτος μέλος, στη συνέχεια εγκρίνει με ομοφωνία (consensus) το εν λόγω αίτημα ή όχι. Μέχρι σήμερα, από ιδρύσεως της συμμαχίας, το εν λόγω άρθρο έχει ενεργοποιηθεί μόνο μία φορά, μετά τις επιθέσεις στους «δίδυμους πύργους» στις Η.Π.Α. το 2001. Στη σχετική ανακοίνωση[59], ο τότε γενικός γραμματέας του ΝΑΤΟ *Lord Robertson* ανέφερε ως βασικό παράγοντα, που επηρέασε τη λήψη της τελικής ομόφωνης απόφασης για επίκληση του υπόψη άρθρου, το γεγονός ότι οι επιθέσεις κατευθύνθηκαν από οντότητες εκτός των συνόρων των Η.Π.Α. (directed from abroad).

Στη Σύνοδο Κορυφής του ΝΑΤΟ που διεξήχθη στη Βαρσοβία (Ιούλιος 2016), ανακηρύχθηκε επίσημα ο κυβερνοχώρος, ως επιχειρησιακό πεδίο δράσης[60], υπογραμμίζοντας ότι μία κυβερνοεπίθεση θα μπορούσε, υπό προϋποθέσεις, να ενεργοποιήσει τις προβλέψεις του ανωτέρω άρθρου 5, όπως είχε ήδη δηλώσει ο Γενικός Γραμματέας της συμμαχίας Jens Stoltenberg στις 14 Ιουνίου 2016, απαντώντας σε δημοσιογράφο στη συνέντευξη τύπου, στο περιθώριο της συνάντησης των υπουργών άμυνας των κρατών μελών της[61].

[59] Statement by NATO Secretary General, Lord Robertson. (2001). Ανάκτηση Νοέμβριος 20, 2016, από NATO On-line library: http://www.nato.int/docu/speech/2001/s011002a.htm

[60] NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. (2016, Ιούλιος 21). Ανάκτηση από CCDCOE: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

[61] Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers. (2016, Ιούνιος 14). Ανάκτηση Νοέμβριος

3.4 Κυβερνοάμυνα

Σύμφωνα με το εγχειρίδιο του Τάλλιν[62], ενεργός κυβερνοάμυνα (active cyber defence) καλείται μία σειρά προληπτικών μέτρων, με σκοπό τον εντοπισμό ή την πρόσκτηση πληροφοριών σχετικά με μία «κυβερνο-εισβολή» ή προκειμένου να καθορίσει την προέλευση μίας επιχείρησης η οποία εκδηλώνει μία προετοιμασμένη, προληπτική κυβερνο- αντιεπιχείρηση (cyber counter operation) εναντίον της πηγής.

Η.Π.Α. και Ρωσία δίνουν έναν κοινό ορισμό σε ένα διμερές εγχειρίδιο ορολογίας[63], σύμφωνα με το οποίο η κυβερνοάμυνα[64] συνιστά ένα σύνολο δυνατοτήτων για την προστασία, τον μετριασμό και την γρήγορη ανάκαμψη από τα αποτελέσματα μίας κυβερνοεπίθεσης.

Στο ίδιο μήκος κύματος η Γαλλία δίνει έναν παρόμοιο ορισμό, κατά τον οποίο η κυβερνοάμυνα συνιστά ένα σύνολο τεχνικών και μη μέτρων προκειμένου ένα κράτος να δύναται να προστατεύσει τα κρίσιμα πληροφοριακά του συστήματα υψίστης σημασίας, τα οποία διαθέτει στο πεδίου του κυβερνοχώρου[65].

Από τους παραπάνω ορισμούς, δύναται να θεωρηθεί ότι μία κυβερνοάμυνα ενεργοποιείται και «απαντά» σε μία κυβερνοεπίθεση, κατ' αντιστοιχία με τον τρόπο που η νόμιμη άμυνα και το δικαίωμα για αυτή ενεργοποιείται με την εκδήλωση ένοπλης επίθεσης και γενικά με τη χρήση βίας.

Αξίζει επίσης να επισημανθεί ότι στις στρατηγικές πολλών χωρών και Διεθνών Οργανισμών η κυβερνοάμυνα αντιμετωπίζεται παράλληλα με την έννοια της κυβερνοασφάλειας, η οποία, σύμφωνα με το προαναφερόμενο εγχειρίδιο

18, 2016, από NATO Official Web Page: http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en#top (σελ. 7)

[62] Schmitt, M. N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html (σελ. 257)

[63] (2014). Critical Terminology Foundations 2 (Russia-U.S. Bilateral on Cybersecurity). EastWest Institute. Ανάκτηση Νοέμβριος 19, 2016, από https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf (σελ. 47)

[64] «*…is organized capabilities to protect against, mitigate from and rapidly recover from the effects of cyber attack…»*

[65] *«…The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical…»,* Cyber Definitions. (n.d.). Ανάκτηση Νοέμβριος 19, 2016, από NATO Cooperative Cyber Defence Centre of Excellence, Tallin Esthonia: https://ccdcoe.org/cyber-definitions.html

κρίσιμης ορολογίας που εκπονήθηκε στο πλαίσιο των διμερών σχέσεων Η.Π.Α. – Ρωσίας, ορίζεται ως η ικανότητα αντιμετώπισης διεθνών ή/και μη απειλών και αποκατάστασης από τις συνέπειες εκδήλωσής τους.

ΚΕΦΑΛΑΙΟ 4
Ζητήματα διεθνούς ευθύνης στον Κυβερνοχώρο

4.1 Το ζήτημα της ευθύνης από κρατικούς και μη δρώντες.

Ο Κυβερνοχώρος θέτει σημαντικές προκλήσεις στη σύγχρονη εποχή, σε ότι αφορά στην εφαρμογή του Διεθνούς Δικαίου. Το ζήτημα της ευθύνης του κράτους (*State Responsibility*) και ειδικότερα της απόδοσης ευθύνης (*attribution*) συνιστούν ίσως τις πιο αξιοσημείωτες προκλήσεις στο εν λόγω πεδίο, αν λάβει κανείς υπόψη του τα κυριότερα και ιδιαίτερα χαρακτηριστικά του Κυβερνοχώρου, όπως η ανωνυμία, το χαμηλό λειτουργικό κόστος, η εύκολη πρόσβαση, η απουσία συνόρων και η ταχύτητα με την οποία δύνανται να εκτελεστούν οι εκάστοτε ηλεκτρονικές εντολές[66].

Όπως επισημαίνεται από τους Δρ. Russell Buchan και Νικόλαο Τσαγκουριά, καθηγητές Διεθνούς Δικαίου του Πανεπιστημίου του Sheffield, τα υποκείμενα του Διεθνούς Δικαίου στα οποία περιορίζεται η διεθνή ευθύνη είναι τα κράτη και οι διεθνείς οργανισμοί. Αντιθέτως, η ατομική ποινική ευθύνη έναντι του Διεθνούς Δικαίου, υφίσταται μόνο για πράξεις που αναλογούν σε διεθνές έγκλημα[67].

Η ευθύνη ενός κράτους για κάθε διεθνώς παράνομη πράξη αποτυπώνεται με σαφήνεια στα άρθρα της Επιτροπής Διεθνούς Δικαίου (International Law Commission) περί ευθύνης του κράτους (State Responsibility), τα οποία υιοθετήθηκαν από τη Γενική Συνέλευση των Ηνωμένων Εθνών στις 12 Δεκεμβρίου 2001, με το Ψήφισμα 56/83[68]. Μόλις στο πρώτο άρθρο η εν λόγω επιτροπή

[66] Buchan, R., & Tsagourias, N. (2016, Οκτωβρίου 19), σελ. 377. Journal of Conflict & Security Law. Ανάκτηση Ιανουάριος 21, 2017, από Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence και Tsagourias, N., Buchan , R., & Roscini, M. (2014, Οκτώβριος 9). State Responsibility for Cyber Operations:. Ανάκτηση Νοέμβριος 20, 2016, από http://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1

[67] Buchan, R., & Tsagourias, N. (2016, Οκτωβρίου 19), σελ. 378. Journal of Conflict & Security Law. Ανάκτηση Ιανουάριος 21, 2017, από Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence

[68] (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών*. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

καθόρισε ότι κάθε διεθνώς παράνομη πράξη ενός κράτους συνεπάγεται τη διεθνή ευθύνη του εν λόγω κράτους:

> «…Art.1 Every internationally wrongful act of a State entails the international responsibility of that State….»

Η ανωτέρω αρχή επιβεβαιώθηκε στη διεθνή νομολογία, τόσο από το Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης το 1938 στην υπόθεση *Phospates in Morocco*[69] όσο και από το Διεθνές Δικαστήριο το 1949 στην υπόθεση *Corfu Channel*[70], το 1986 στην υπόθεση *Νικαράγουα*[71] και το 1997 στην υπόθεση *Gabčíkovo-Nagymaros Project*[72], σύμφωνα με τον συναφή σχολιασμό του εν λόγω άρθρου[73].

Στο δε επόμενο άρθρο[74] η Επιτροπή Διεθνούς Δικαίου προσδιόρισε τις π ρ ο ϋ π ο θ έ σ ε ι ς υπό τις οποίες μία πράξη η παράλειψη ενός κράτους χαρακτηρίζεται ως διεθνώς παράνομη και συγκεκριμένα να δύναται να αποδοθεί σε ένα κράτος (*attributable*) κατά το Διεθνές Δίκαιο και να συνιστά παραβίαση διεθνούς υποχρέωσης του υπόψη κράτους:

> «…Art.2 Elements of an internationally wrongful act of a State
>
> There 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…»

---

[69] «…Όταν ένα κράτος προβαίνει σε μία πράξη διεθνώς παράνομη εναντίον ενός άλλου κράτους, τότε μεταξύ των δύο αυτών κρατών θα υφίσταται άμεσα διεθνής ευθύνη…» («…*international responsibility would be established immediately as between the two States…*»), (1938). *Απόφαση στην υπόθεση Phosphates in Morocco, Ιταλία/Γαλλία , No 74, Series A/B, Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης*. Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/pcij/serie_AB/AB_74/01_Phosphates_du_Maroc_Arret.pdf

[70] (1949). *Απόφαση στην υπόθεση Corfu Channel (Merits), Ηνωμένο Βασίλειο/Αλβανία, Διεθνές Δικαστήριο*. Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/1/1645.pdf

[71] (1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE*, σελ. 14, 142 (παρ. 283), 149 (παρ. 292). Ανάκτηση Νοέμβριος 18, 2016 από http://www.icj-cij.org/docket/files/70/6503.pdf

[72] (1997). Απόφαση στην υπόθεση Gabčíkovo-Nagymaros Project, Ουγγαρία/Σλοβακία, Διεθνές Δικαστήριο, σελ.7, 38 (παρ. 47). Ανάκτηση Ιανουάριος 28, 2017 από http://www.icj-cij.org/docket/files/92/7375.pdf

[73] (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, σελ.7. Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[74] (2002). Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

Οι ανωτέρω προϋποθέσεις στη διεθνή νομολογία επιβεβαιώθηκαν από το Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης στην προαναφερόμενη υπόθεση Phosphates in Morocco (1938)[75], στην οποία το δικαστήριο συνέδεσε τη δημιουργία διεθνούς ευθύνης με την τέλεση πράξης από ένα κράτος αντίθετης με τα συμβατικά δικαιώματα ενός άλλου κράτους («*…act being attributable to the State and described as contrary to the treaty right[s] of another State…*»)[76]. Επίσης, το Διεθνές Δικαστήριο το 1980 στην υπόθεση των *Ομήρων της Τεχεράνης* (*Διπλωματικό και Προξενικό Σώμα των Η.Π.Α. στη Τεχεράνη*)[77] επισήμανε ότι θα πρέπει να καθοριστεί κατά πρώτον εάν και κατά πόσο οι επίμαχες πράξεις δύνανται να αποδοθούν νομικά στο Ιρανικό κράτος και κατά δεύτερον εάν οι πράξεις αυτές είναι αντίθετες ή μη με τις υποχρεώσεις του Ιράν σύμφωνα με εν ισχύ συνθήκες ή με το Διεθνές Δίκαιο[78]:

> «…56…[f]irst, it must determine how far, legally, the acts in question may be regarded as imputable to the Iranian State. Secondly, it must consider their compatibility or incompatibility with the obligations of Iran under treaties in force or under any other rules of international law that may be applicable…»

Αντίστοιχη αναφορά συναντάται και στις προαναφερόμενες αποφάσεις του Διεθνούς Δικαστηρίου στις υποθέσεις *Νικαράγουα*[79](1986) και *Gabčíkovo-Nagymaros Project*[80](1997).

---

[75] (1938). *Απόφαση στην υπόθεση Phosphates in Morocco, Ιταλία/Γαλλία , No 74, Series A/B, Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/pcij/serie_AB/AB_74/01_Phosphates_du_Maroc_Arret.pdf

[76] (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, σελ.12. Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[77] (1980). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση "Όμηροι Τεχεράνης (Διπλωματικό και Προξενικό Σώμα στην Τεχεράνη)", Η.Π.Α./Ιράν*, σελ. 29 (παρ. 56), σελ. 41 (παρ. 90). Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/64/6291.pdf

[78] (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, σελ.12. Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[79] (1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE*, σελ. 117-118 (παρ. 226). Ανάκτηση Νοέμβριος 18, 2016 από http://www.icj-cij.org/docket/files/70/6503.pdf

Όπως επισημαίνεται στον σχολιασμό των άρθρων περί ευθύνης του κράτους από την Επιτροπή Διεθνούς Δικαίου[81], το στοιχείο της απόδοσης ευθύνης (πρώτη προϋπόθεση κατά το Άρθρο 2) ορισμένες φορές χαρακτηρίζεται ως υποκειμενικό, ενώ το στοιχείο της παράβασης/παραβίασης (δεύτερη προϋπόθεση κατά το Άρθρο 2) ως αντικειμενικό. Ο χαρακτηρισμός της απόδοσης ευθύνης ως υποκειμενικό στοιχείο οφείλεται στο γεγονός ότι στηρίζεται στην πρόθεση ή γνώση περί της τέλεσης (ή παράλειψης τέλεσης) μίας πράξης από το υπόψη κράτος και τα επίσημα όργανα και υπηρεσίες του. Το στοιχείο της πρόθεσης συναντάται στη Σύμβαση για την πρόληψη και τιμωρία του εγκλήματος της Γενοκτονίας, όπου στο Άρθρο 2 αναφέρεται, μεταξύ άλλων, ότι η γενοκτονία είναι έγκλημα που διαπράττεται με πρόθεση να καταστρέψει, ολικώς ή μερικώς, μία εθνική, εθνοτική, φυλετική ή θρησκευτική ομάδα[82].

Στην περίπτωση, λοιπόν, μιας κυβερνοεπίθεσης, θα πρέπει κατά πρώτο λόγο να εξακριβωθεί το στοιχείο της απόδοσης της ευθύνης. Λαμβάνοντας υπόψη τα χαρακτηριστικά του Κυβερνοχώρου, όπως αυτά επισημάνθηκαν στην αρχή του παρόντος κεφαλαίου και τον δυνητικά υποκειμενικό χαρακτήρα της εν λόγω διαδικασίας, γίνεται αντιληπτό ότι η απόδοση ευθύνης καθίσταται ιδιαίτερα δύσκολη.

Σύμφωνα με το προαναφερόμενο Άρθρο 2 της Επιτροπής Διεθνούς Δικαίου περί ευθύνης κράτους, η διεθνής ευθύνη αποδίδεται όχι μόνο για τέλεση παραβατικής πράξης από ένα κράτος αλλά και για παραλείψεις του υπόψη κράτους. Στη διεθνή νομολογία, περίπτωση καταδίκης κράτους για παραλείψεις του συναντάται το 1949 στην υπόθεση *Corfu Channel*, όπου το Διεθνές

---

[80] (1997). *Απόφαση στην υπόθεση Gabčíkovo-Nagymaros Project, Ουγγαρία/Σλοβακία, Διεθνές Δικαστήριο*, σελ.54 (παρ. 78). Ανάκτηση Ιανουάριος 28, 2017 από http://www.icj-cij.org/docket/files/92/7375.pdf

[81] (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, σελ.12-13. Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[82] "…*In the present Convention, genocide means any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such ...*" (1948). *Σύμβαση για την Πρόληψη καιι Τιμωρία του εγκλήματος της Γενοκτονίας, που υιοθετήθηκε απο τη Γενική Συνέλευση των Ηνωμένων Εθνών.* Ανάκτηση Ιανουάριος 28, 2017, από https://treaties.un.org/doc/publication/unts/volume%2078/volume-78-i-1021-english.pdf

Δικαστήριο απέδωσε διεθνή ευθύνη στην Αλβανία, υπό την έννοια ότι ή ξ ε ρ ε ή έ π ρ ε π ε ν α γ ν ω ρ ί ζ ε ι την ύπαρξη ναρκών στα χωρικά της ύδατα και δεν προειδοποίησε σχετικά τρίτα κράτη[83]. Ομοίως έπραξε το 1980 και στην υπόθεση *Όμηροι Τεχεράνης (Διπλωματικό και Προξενικό Σώμα των Η.Π.Α. στη Τεχεράνη)*[84]. Κατά συνέπεια, στο πλαίσιο μίας κυβερνοεπίθεσης, ενδεχομένως να μπορούσε να αποδοθεί ευθύνη σε ένα κράτος, υπό την έννοια ότι αυτό δεν έλαβε όλα τα απαραίτητα μέτρα ασφαλείας στα επικοινωνιακά και πληροφοριακά του συστήματα, προκειμένου να δύναται να αποτρέψει την εκδήλωση κυβερνοεπίθεσης από το έδαφός του (π.χ. μη θεσπίζοντας σχετική εσωτερική νομολογία).

Θα πρέπει να ληφθεί υπόψη ότι το κράτος, ως μία οργανωμένη οντότητα, με νομικό πρόσωπο και πλήρη δικαιοδοσία έναντι του Διεθνούς Δικαίου, δε δρα από μόνο του. Κάθε τέλεση πράξης (ή παράλειψη), λαμβάνει χώρα μέσω του ατόμου ή μιας ομάδας ατόμων. Έτσι, το Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης, το 1923 στην υπόθεση των Γερμανών αποίκων στην Πολωνία, γνωμοδότησε ότι τα κράτη δύνανται να δρουν μόνο μέσω των υπηρεσιών και των εκπροσώπων τους[85]. Συναφώς, ο *Dionisio Anzilotti*, Ιταλός μελετητής Διεθνούς Δικαίου στον εικοστό αιώνα, είχε πει ότι κάθε πράξη ενός κράτους «δεν είναι τίποτε άλλο παρά η δραστηριότητα των ατόμων του, την οποία ο νόμος καταλογίζει στο κράτος»[86].

Όταν πρόκειται για όργανα του κράτους, τα οποία δρουν εκ μέρους του, τότε το ζήτημα της απόδοσης της ευθύνης είναι ξεκάθαρο και αποτυπώνεται στο Άρθρο 4 των άρθρων της Επιτροπής Διεθνούς Δικαίου περί ευθύνης κράτους. Σύμφωνα

---

[83] (1949). *Απόφαση στην υπόθεση Corfu Channel (Merits), Ηνωμένο Βασίλειο/Αλβανία, Διεθνές Δικαστήριο*, σελ. 22-23. Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/1/1645.pdf

[84] (1980). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση "Διπλωματικό και Προξενικό Σώμα στην Τεχεράνη", Η.Π.Α./Ιράν*, σελ. 31-32 (παρ. 63 και 67). Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/64/6291.pdf

[85] «…*States can act only by and through their agents and representatives*…», (1923). *Γνωμοδότηση Διαρκούς Δικαστηρίου Διεθνούς Δικαιοσύνης περί Γερμανών αποίκων στην Πολωνία*, σελ. 22. Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/pcij/serie_B/B_06/Colons_allemands_en_Pologne_Avis_consultatif.pdf

[86] «…*nothing but the activity of individuals that the law imputes to the State*…», Anzilotti, D. (1929). Cours de droit international και Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors.* Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

με αυτό, η συμπεριφορά των κρατικών οργάνων, ανεξάρτητα από τη θέση τους, τα καθήκοντά τους ή/και το γεωγραφικό τους ίχνος λαμβάνεται ως πράξη του υπόψη κράτους, έναντι του Διεθνούς Δικαίου:

> «…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.
>
> 2. An organ includes any person or entity which has that status in accordance with the internal law of the State…»[87]

Στη συγκεκριμένη περίπτωση, δέον όπως επισημανθεί η διαφοροποίηση που υφίσταται όταν η συμπεριφορά ενός κρατικού οργάνου έχει προσωπικό ή επίσημο χαρακτήρα. Η εν λόγω διαφοροποίηση διευκρινίστηκε με σαφήνεια σε διεθνείς, διαιτητικές αποφάσεις. Έτσι, η Γενική Επιτροπή Αποζημιώσεων μεταξύ Μεξικού και Η.Π.Α., το 1927 στην υπόθεση *Mallén*[88], αναγνώρισε την ύπαρξη κρατικής ευθύνης σε πράξη κρατικού αξιωματούχου υπό την επίσημη ιδιότητά του, ενώ αντιθέτως δεν έκανε το ίδιο σε ιδιωτική ενέργεια του ίδιου προσώπου. Όμοια, η Γενική Επιτροπή Αποζημιώσεων μεταξύ Γαλλίας και Μεξικού, το 1929 στην υπόθεση του *Jean-Baptiste Caire*[89], δεν αναγνώρισε την ύπαρξη διεθνούς ευθύνης μόνο στις πράξεις των δύο κατηγορούμενων αστυνομικών που δεν συνδεόταν με την επίσημη ιδιότητα των εν λόγω ατόμων.

Επίσης, η ευθύνη του κράτους για πράξεις των οργάνων του, εκτείνεται και στις περιπτώσεις που τα όργανα αυτά δεν ακολουθούν τις δοθείσες οδηγίες ή οι πράξεις τους βαίνουν πέραν της αρμοδιότητάς τους. Η πρόβλεψη αυτή είναι σύμφωνη με το Άρθρο 7 των άρθρων της Επιτροπής Διεθνούς Δικαίου περί ευθύνης κράτους:

---

[87] (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών.* Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[88] (1927). *Διαιτητική Απόφαση της Γενικής Επιτροπής Αποζημιώσεων Μεξικό-Η.Π.Α. στην υπόθεση Francisco Mallen*, σελ. 175. Ανάκτηση Ιανουάριος 29, 2017, από http://legal.un.org/riaa/cases/vol_IV/173-190.pdf

[89] (1929). *Διαιτητική Απόφαση της Γενικής Επιτροπής Αποζημιώσεων Γαλλίας-Μεξικού στην υπόθεση του Jean-Baptiste Caire*, σελ. 531. Ανάκτηση Ιανουάριος 29, 2017, από http://legal.un.org/docs/?path=../riaa/cases/vol_V/516-534_Caire.pdf&lang=E

> «…Article 7. Excess of authority or contravention of instructions.
>
> The conduct of an organ of a State or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions…»[90].

Η απόδοση διεθνούς ευθύνης σε ένα κράτος, για τις πράξεις ατόμων ή ομάδας ατόμων του, τα οποία δεν αποτελούν κρατικά όργανα (μη κρατικοί δρώντες), περιγράφεται στο Άρθρο 8 των υπόψη άρθρων της Επιτροπής Διεθνούς Δικαίου, το οποίο ουσιαστικά υπογραμμίζει τρία συγκεκριμένα κριτήρια. Σύμφωνα, λοιπόν, με το εν λόγω άρθρο, «η συμπεριφορά ενός ατόμου ή μιας ομάδας ατόμων, θεωρείται ως πράξη του κράτους υπό το Διεθνές Δίκαιο, εφόσον το άτομο ή η ομάδα ατόμων ενεργούν υπό τις οδηγίες, ή τη διεύθυνση ή τον έλεγχο του εν λόγω κράτους»[91]. Δεν απαιτείται η ικανοποίηση και των τριών κριτηρίων για να δύναται να αποδοθεί ευθύνη σε ένα κράτος. Αρκεί να στοιχειοθετηθεί οποιονδήποτε εκ των ανωτέρω τριών κριτηρών, σύμφωνα και με τον σχολιασμό του Άρθρου 8 της Επιτροπής Διεθνούς Δικαίου περί ευθύνης των κρατών[92].

Σε ότι αφορά στο πρώτο κριτήριο (οδηγίες/instructions), σύμφωνα με τον σχολιασμό του Άρθρου 8 από την επιτροπή ΕΔΔ[93], οι προβλέψεις του άρθρου αυτού αναφέρονται στις περιπτώσεις όπου ένα κράτος συμπληρώνει τις δράσεις του προσλαμβάνοντας ή υποκινώντας ιδιώτες ή ομάδες ιδιωτών του ως βοηθητικούς (*auxiliaries*) ή ως εθελοντές, για να φέρουν εις πέρας συγκεκριμένες αποστολές στο εξωτερικό, παραμένοντας, παράλληλα, εκτός κάθε επίσημης κρατικής δομής. Η συμπεριφορά αυτή, εκ μέρους των κρατών, λόγω των

---

[90] (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών.* Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[91] «*…Art.8 The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct…*» (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών*. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[92] (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, σελ.73, παρ. (7) . Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[93] Ibid., σελ.70, παρ. (2)

χαρακτηριστικών του Κυβερνοχώρου, είναι εύκολα εφαρμόσιμη στις περιπτώσεις κυβερνοεπιθέσεων από ένα κράτος εναντίον ενός άλλου, κατά τις οποίες «προσλαμβάνονται» άτυπα άριστοι χρήστες του διαδικτύου και προγραμματιστές (hackers) για την εκδήλωση των επιθέσεων αυτών, υπό τις οδηγίες και τις κατευθύνσεις του επιτιθέμενου κράτους. Σύμφωνα, λοιπόν , με το εν λόγω άρθρο, η ευθύνη θα πρέπει να αποδοθεί στο κράτος υπό τις οδηγίες και τις κατευθύνσεις του οποίου τίθενται οι ιδιώτες hackers.

Περαιτέρω, υπάρχουν κάποιες υποπροϋποθέσεις οι οποίες πρέπει να πληρούνται σχετικά με την εφαρμογή του πρώτου κριτηρίου[94]. Συγκεκριμένα, η μη κρατική οντότητα θα πρέπει να είναι υποκείμενη του κράτους, κατά το χρονικό διάστημα που το τελευταίο αποφασίζει να τελέσει τις επίμαχες πράξεις του. Η σχέση, βέβαια, αυτή από μόνη της δε δύναται να δικαιολογήσει την απόδοση ευθύνης στο κράτος, αν δεν υπάρχουν σχετικές επαρκείς αποδείξεις σε ότι αφορά την παροχή συγκεκριμένων οδηγιών από το τελευταίο.

Κατά συνέπεια, οι οδηγίες θα πρέπει να είναι σαφείς και να αφορούν στην υπόψη δραστηριότητα και όχι μια γενικόλογη παρότρυνση, πιθανώς βασισμένη στο συναίσθημα του πατριωτισμού και της εθνικής συσπείρωσης των υποψήφιων hackers (όπως συνέβη, σύμφωνα με ανεπιβεβαίωτες από την πλευρά της Ρωσίας θεωρίες, το 2007 στην περίπτωση των κυβερνοεπιθέσεων στην Εσθονία, όπου Ρώσοι κυβερνητικοί πράκτορες εικάζεται ότι χρησιμοποίησαν διάφορα διαδικτυακά chatrooms και φόρουμ, προκειμένου να παροτρύνουν Ρώσους «πατριώτες» hackers στο να εκδηλώσουν επιθέσεις εναντίον της Εσθονίας[95]).

Εξάλλου, το Διεθνές Δίκαιο δεν απαγορεύει την υποκίνηση παράνομης συμπεριφοράς (όπως συμβαίνει στις περιπτώσεις των εγκλημάτων γενοκτονίας και διακρίσεων). Στο συμπέρασμα αυτό καταλήγει και η Επιτροπή Διεθνούς Δικαίου στο σχολιασμό του Άρθρου 15 των άρθρων περί ευθύνης κράτους, συμπληρώνοντας ότι θα πρέπει να υπάρχει συγκεκριμένη στήριξη («*…concrete*

[94] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 415-416. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[95] Ibid.

support…») ή να υπάρχουν σαφείς αποδείξεις ότι το κράτος είχε τον έλεγχο («*…direction and control…*») της μη κρατικής οντότητας[96]. Έτσι, το Διεθνές Δικαστήριο το 1980 στην υπόθεση των *Ομήρων της Τεχεράνης (Διπλωματικό και Προξενικό Σώμα Η.Π.Α. στη* Τεχεράνη), συμπέρανε ότι η γενική παρότρυνση του τότε θρησκευτικού και πολιτικού ηγέτη του Ιράν *Ayatollah Khomeini* προς την ιρανική νεολαία εναντίον των Η.Π.Α. και του Ισραήλ («*…expand with all their might their attacks against the United States and Israel…*») δεν μπορεί να θεωρηθεί ως επίσημη άδεια από το κράτος του Ιράν για ανάληψη επιχείρησης εισβολής και κατάσχεσης στην Πρεσβεία των Η.Π.Α. [97]. Η σχετική δήλωση του εν λόγω ηγέτη, όσο «εμπρηστική» κι αν μπορεί να χαρακτηριστεί, δε συμπεριελάμβανε συγκεκριμένη αναφορά που να αναφέρεται σε επιθυμία κατάληψης της αμερικανικής Πρεσβείας. Σε ότι αφορά την παροχή συγκεκριμένων οδηγιών από το κράτος, το Διεθνές Δικαστήριο το 2007 στην υπόθεση της *Γενοκτονίας στη Βοσνία*, κατέληξε ότι οι οδηγίες θα πρέπει να δίνονται ειδικά στο πλαίσιο κάθε επιχείρησης στην οποία λαμβάνουν χώρα οι υπόψη πράξεις[98].

Επιπλέον, η ύπαρξη κοινού σκοπού μεταξύ ενός κράτους και μίας μη κρατικής οντότητας δεν αποτελεί επαρκές στοιχείο που να δικαιολογεί την απόδοση ευθύνης στο κράτος. Ως χαρακτηριστικό παράδειγμα θα μπορούσε να αναφερθεί η περίπτωση της μη κρατικής κυβερνο-οντότητας *Honker Group*[99] με

---

[96] «*…The incitement of wrongful conduct is generally not regarded as sufficient to give rise to responsibility on the part of the inciting State, if it is not accompanied by concrete support or does not involve direction and control on the part of the inciting State…*» (2012). MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25), σελ.127, παρ. (9) . Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[97] *«...it would be going too far to interpret such general declarations of the Ayatollah Khomeini to the people or students of Iran as amounting to an authorization from the State to undertake the specific operation of invading and seizing the United States Embassy…*» (1980). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση "Διπλωματικό και Προξενικό Σώμα στην Τεχεράνη", Η.Π.Α./Ιράν*, σελ. 30 (παρ. 59). Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/64/6291.pdf

[98] «*...in respect of each operation in which the alleged violations occurred…*», (2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου*, n 15 (400). Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

[99] Saporito, L., & Lewis, J. A. (2014, Μαρτίου 13). *Cyber Incidents Attributed to China.* Ανάκτηση Ιανουάριος 29, 2017, από Center for Strategic and International Studies: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130314_Chinese_hacking.pdf και Macak, K. (2016, Σεπτέμβριος 25). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors, σελ. 415.

έδρα την Κίνα, της οποίας οι στόχοι (Ινδονησία, Ταιβάν, Η.Π.Α., Ιαπωνικά ιδρύματα και ένας Θιβετιανός πολιτικός αντιφρονούντας), ευθυγραμμίζονται με τους «στόχους» της Δημοκρατίας της Κίνας. Ωστόσο, θα ήταν εσφαλμένο το συμπέρασμα να αποδοθεί ευθύνη στην Κίνα για πράξεις της υπόψη κυβερνο-οντότητας, μόνο εξαιτίας της ύπαρξης κοινών σκοπών/στόχων.

Όσον αφορά το δεύτερο κριτήριο της διεύθυνσης (direction) για την απόδοση ευθύνης σε κάποιο κράτος, η ακριβής ερμηνεία του συναντάται σε μία από τις λίγες υποθέσεις στη διεθνή νομολογία[100], όπου τα αντίδικα μέρη αναφέρθηκαν στη συγκεκριμένη έννοια του Άρθρου 8 των άρθρων περί ευθύνης κράτους της ΕΔΔ και συγκεκριμένα στην υπόθεση της *Γενοκτονίας στη Βοσνία*[101], όπου η απόδοση ευθύνης μη κρατικών δρώντων αποτέλεσε ένα από τα κεντρικά ζητήματα[102]. Στην προφορική διαδικασία ενώπιον του Διεθνούς Δικαστηρίου, ο καθηγητής *Alain Pellet*, που εκπροσωπούσε την Βοσνία και Ερζεγοβίνη, περιέγραψε την έννοια direction ως μία έννοια «λιγότερο αυστηρή» σε σχέση με τις οδηγίες/instructions («*…less rigorous term than "instructions"…*»)[103], χαρακτηρισμός για τον οποίο δεν υπήρχε αντίδραση. Ωστόσο, το Δικαστήριο κατέληξε, τελικά, στο συμπέρασμα ότι το εν λόγω κριτήριο υφίσταται όταν ένα κρατικό όργανο διευθύνει τους τελεστές μίας παράνομης πράξης κατά τρόπο ώστε να την εκτελέσουν[104], μια περιγραφή η οποία βαίνει πέραν της απλής παροχής οδηγιών και μάλιστα χωρίς περαιτέρω συνέχεια.

Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[100] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 417-418. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[101] (2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου*, n 14. Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

[102] Ibid. σελ. 396-412

[103] (2006). *Oral Proceedings, Bosnian Genocide case, ICJ, CR 2006/8*, σελ.25, παρ. 62 . Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/91/10600.pdf

[104] «*…where an organ of the State gave the instructions or provided the direction pursuant to which the perpetrators of the wrongful act acted…*», (2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου*, σελ. 171, παρ. 406. Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

Ο καθηγητής Διεθνούς Δικαίου *James Crawford*, που συμμετείχε στη σύνταξη των τελικών άρθρων περί ευθύνης κράτους της Επιτροπής Διεθνούς Δικαίου, από 1998 έως 2001 ως Ειδικός Εισηγητής, έδωσε μία παρεμφερή με το Διεθνές Δικαστήριο ερμηνεία στην έννοια της διεύθυνσης/direction, ως μία συνεχή περίοδο παροχής οδηγιών ή «σχέση» μεταξύ κράτους και μη κρατικής οντότητας, κατά τρόπο ώστε να δύναται να δικαιολογήσει την απόδοση ευθύνης στο κράτος[105]. Το στοιχείο της ύπαρξης μίας εξωθεσμικής αλλά ξεκάθαρης «σχέσης» μεταξύ κράτους και μη κρατικής οντότητας είναι και το πλέον σημαντικό στοιχείο κατά την εξέταση του παρόντος κριτηρίου, καθόσον δύναται να αποτελέσει την αιτία να αποδοθεί τελικά ευθύνη στο κράτος, ακόμα και στην περίπτωση που μπορεί να μην είχαν δοθεί συγκεκριμένες οδηγίες στη μη κρατική οντότητα.

Χαρακτηριστική περίπτωση[106] αποτελεί το παράδειγμα του κακόβουλου λογισμικού *Stuxnet*[107] , ο οποίος πρόσβαλλε το 2010, μεταξύ άλλων, εγκαταστάσεις πυρηνικού προγράμματος του Ιράν. Οι έρευνες που διεξήχθησαν κατέληξαν στο συμπέρασμα ότι η ανωτέρω κυβερνοεπίθεση εκδηλώθηκε από κράτη, με τις περισσότερες υποψίες να στρέφονται εναντίον των Η.Π.Α. και του Ισραήλ[108], τα οποία και ουδέποτε το αρνήθηκαν[109]. Σύμφωνα, μάλιστα, με τον *Alexander Klimburg*, Αυστριακό κυβερνητικό σύμβουλο στο Ατλαντικό Συμβούλιο και στο LSE[110] επί θεμάτων κυβερνοασφάλειας, η ανάπτυξη του υπόψη κακόβουλου λογισμικού έγινε τμηματικά και κατά τρόπο ώστε υπο-ομάδες προγραμματιστών να μη γνώριζαν την ύπαρξη του ευρύτερου «μεγάλου»

---

[105] «*…implies a continuing period of instruction, or a relationship between the state and a non-State entity such that suggestion or innuendo may give rise to responsibility*…» Crawford, J. (2014). *State Responsibility: The General Part*, υποσημείωση 28. Cambridge University Press.

[106] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 419. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[107] Βλέπε ενότητα 1.2.3 του Μέρους Β' της παρούσας εργασίας

[108] *Obama Order Sped Up Wave of Cyberattacks Against Iran*. (2012, Ιούνιος 1). Ανάκτηση Ιανουάριος 29, 2017, από The New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?smid=pl-share

[109] *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. (2011, Ιανουάριος 15). Ανάκτηση Ιανουάριος 29, 2017, από The New York Times: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?smid=pl-share

[110] London School of Economics and Political Science (LSE)

σχεδίου[111]. Σημαντικός αριθμός προγραμματιστών δεν είχαν διοριστεί καθ' οιονδήποτε τρόπο από τα προαναφερόμενα ύποπτα για την εκδήλωση των κυβερνοεπιθέσεων κράτη, ενώ μέρη του προγράμματος είχαν ανατεθεί σε οργανισμούς που ήταν εμπλεκόμενοι με το κυβερνοέγκλημα[112]. Έτσι, οι ομάδες προγραμματιστών που τους είχαν ανατεθεί τα εν λόγω «επίμαχα» μέρη αυτού του μακροπρόθεσμου σχεδίου, ελάμβαναν καθοδήγηση (*direction*) η οποία δεν μπορεί να αξιολογηθεί ως «οδηγίες», λόγω της συνέχειας στη λήψη σχετικών κατευθύνσεων, αλλά ούτε και ως «έλεγχος», λόγω της μη ύπαρξης θεσμικής ή εξωθεσμικής σχέσης με τα διευθύνοντα κράτη.

Το τελευταίο κριτήριο στη διατύπωση του Άρθρου 8 της ΕΔΔ είναι το στοιχείο του ε λ έ γ χ ο υ (*c o n t r o l*). Το εν λόγω κριτήριο αποτέλεσε και το βασικό ζήτημα στην υπόθεση *Νικαράγουα* (1986), όπου εξετάστηκε εάν η συμπεριφορά των *contras* μπορούσε να αποδοθεί στις Η.Π.Α. και κατά συνέπεια να αποδοθεί στους τελευταίους η ευθύνη για παραβίαση κανόνων Διεθνούς Ανθρωπιστικού Δικαίου από πράξεις που τελέστηκαν από τους *contras*. Το Διεθνές Δικαστήριο δέχτηκε[113] ότι οι Η.Π.Α. ήταν υπεύθυνες για τον σχεδιασμό, τη διεύθυνση και την υποστήριξη που παρείχαν στους contras, αλλά όχι σε τέτοιο βαθμό που να θεωρείται ότι οι τελευταίοι ενεργούσαν υπό τον πλήρη έλεγχο και εκ μέρους των Η.Π.Α., όπως ισχυρίζονταν οι εκπρόσωποι της Νικαράγουα:

> «…109. … Yet despite the heavy subsidies and other support provided to them by the United States, there is no clear evidence of the United States having actually exercised such a degree of control in al1 fields as tojustify treating the contras as acting on its behalf….»[114]

Έτσι, το Διεθνές Δικαστήριο, απουσία κατάλληλων αποδεικτικών στοιχείων περί του βαθμού ελέγχου των Η.Π.Α. επί των *contras*, αναγνώρισε ότι οι πράξεις που παραβίασαν τα ανθρώπινα δικαιώματα και το Διεθνές Ανθρωπιστικό Δίκαιο

---

[111] Klimburg, A. (2011). *Mobilising Cyber Power*. Στο A. Klimburg, Cyber Threats. Survival, σελ. 43. Ανάκτηση Ιανουάριος 29, 2017, από http://users.clas.ufl.edu/zselden/coursereading2011/klimcyber.pdf

[112] Ibid.

[113] (1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE*, σελ. 51 (παρ. 86). Ανάκτηση Νοέμβριος 18, 2016 από http://www.icj-cij.org/docket/files/70/6503.pdf

[114] Ibid. σελ. 62, παρ. 109

μπορούσαν να διαπραχθούν από μέλη των *contras*, χωρίς τον έλεγχο των Η.Π.Α. [115].

Όπως προκύπτει ανωτέρω από την υπόθεση *Νικαράγουα*, το κριτήριο του ελέγχου εξαρτάται από τον τ ύ π ο και τον β α θ μ ό ε λ έ γ χ ο υ που ασκεί το κράτος, ώστε να δύνανται οι πράξεις του να αποδοθούν σε αυτό. Ως ένα βαθμό το κράτος μπορεί να θεωρηθεί ότι ασκεί τον έλεγχο επί μη κρατικών οντοτήτων που δραστηριοποιούνται στο έδαφός του[116]. Ωστόσο, η γεωγραφική εγγύτητα δε δύναται να θεωρηθεί ως κριτήριο που να δικαιολογεί ότι το κράτος θα πρέπει να γνωρίζει κάθε παράνομη πράξη που λαμβάνει χώρα στην επικράτειά του[117] και κατά συνέπεια να δύναται να του αποδοθεί ευθύνη. Συναφώς το Διεθνές Δικαστήριο το 1949 στην υπόθεση *Corfu Channel* διευκρίνισε ότι η ανακάλυψη του ναρκοπεδίου στα χωρικά ύδατα της Αλβανίας δε σήμαινε απαραίτητα ότι η Αλβανική κυβέρνηση θα έπρεπε να γνωρίζει ποιος εναπόθεσε τις νάρκες[118]. ,

Όσον αφορά το βαθμό ελέγχου, το Διεθνές Δικαστήριο στην υπόθεση της *Γενοκτονίας στη Βοσνία* επισήμανε ότι θα πρέπει να είναι ι δ ι α ί τ ε ρ α μ ε γ ά λ ο ς («…p a r t i c u l a r l y g r e a t…»), ώστε να υπάρχει πλήρη εξάρτηση («…*complete dependence…*») του μη κρατικού δρώντα με το κράτος[119] και κατά συνέπεια η μεταξύ τους σχέση να εμπίπτει στις προβλέψεις του Άρθρου 8

---

[115] Ibid. σελ. 64-65, παρ. 115

[116] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 420. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/. Ειδικότερα βλ. Tonkin, H. (2011). *State Control over Private Military and Security Companies in Armed Conflict,* σελ. 123.

[117] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 420. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[118] «*…It is clear that knowledge of the minelaying cannot be imputed to the Albanian Government by reason merely of the fact that a minefield discovered in Albanian territorial waters caused the explosions of which the British warships were the victims…*» (1949). *Απόφαση στην υπόθεση Corfu Channel (Merits), Ηνωμένο Βασίλειο/Αλβανία, Διεθνές Δικαστήριο*, σελ. 18. Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/1/1645.pdf

[119] *«…393. However, so to equate persons or entities with State organs when they do not have that status under internal law must be exceptional, for it requires proof of a particularly great degree of State control over them, a relationship which the Court's Judgment quoted above expressly described as "complete dependence…»* (2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου*, σελ. 166, παρ. 393. Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

των άρθρων της ΕΔΔ περί ευθύνης κρατών[120]. Σε αντίθετη περίπτωση, οι εν λόγω δρώντες θα θεωρηθούν de facto κρατικά όργανα[121], εμπίπτοντας στις προβλέψεις του Άρθρου 4 των προαναφερόμενων άρθρων[122] (άρθρο περί ευθύνης κράτους για πράξεις κρατικών του οργάνων). Κατά συνέπεια, όταν ένα κράτος, προκειμένου να αντιμετωπίσει μία κυβερνοεπίθεση, προβεί στη σύσταση μίας ομάδας ειδικών, προερχόμενοι από αρμόδιες κρατικές υπηρεσίες και ιδιωτικές εταιρείες κυβερνοασφάλειας, τότε η εν λόγω ομάδα, ούσα υπό τον πλήρη έλεγχο του κράτους, θα ισοδυναμεί με κρατικό όργανο, ακόμα και αν αυτό δεν έχει γίνει θεσμικά (μέσω εσωτερικής νομοθεσίας)[123].

Ενώ, λοιπόν, ένας μη κρατικός δρώντας θα εξαρτάται πλήρως από το κράτος, όταν το τελευταίο ασκεί πλήρη έλεγχο σε αυτό («*complete dependence*»), η αντίθετη πρόβλεψη ενός ελάχιστου βαθμού ελέγχου, σύμφωνα με τον οποίο το κράτος να θεωρείται ότι ελέγχει τον μη κρατικό δρώντα, δεν είναι το ίδιο ξεκάθαρη.

Σύμφωνα με τον καθηγητή *Kubo Macak*, λέκτορα Δικαίου στο Πανεπιστήμιο του *Exeter* στο Ηνωμένο Βασίλειο[124], το Διεθνές Δικαστήριο της Χάγης, προκειμένου να καθορίσει τον απαραίτητο βαθμό ελέγχου που να αιτιολογεί επαρκώς την απόδοση ευθύνης σε ένα κράτος, διαμόρφωσε, αρχικά με την υπόθεση *Νικαράγουα* και σε συνέχεια με την υπόθεση της *Γενοκτονίας στη Βοσνία*, το λεγόμενο «τεστ του αποτελεσματικού ελέγχου (*effective control test*)», ή «τεστ της Νικαράγουα». Συγκεκριμένα, στην υπόθεση *Νικαράγουα*, το Διεθνές Δικαστήριο έκρινε ότι παρόλο που οι Η.Π.Α. χρηματοδοτούσαν, οργάνωναν, εκπαίδευαν, υποστήριζαν και εξόπλιζαν τους *contras* (μη κρατικός δρώντας), «η επιλογή στρατιωτικών ή παραστρατιωτικών στόχων και ο σχεδιασμός όλης της επιχείρησης» δεν επαρκούσε ώστε να δικαιολογεί την απόδοση ευθύνης στις Η.Π.Α. για τις πράξεις

[120] Ibid. σελ. 210, παρ. 406
[121] Ibid. σελ. 207, παρ. 397
[122] Ibid. σελ. 202, παρ. 385 και σελ. 210, παρ. 406
[123] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 420. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/
[124] Ibid. σελ. 420-421

των contras[125]. Στην ίδια υπόθεση, το δικαστήριο αναφέρθηκε στην ύπαρξη μερικής εξάρτησης (*partial dependency*), η οποία προκύπτει από την εξέταση διάφορων παραγόντων, όπως «η οργάνωση, η εκπαίδευση και ο εξοπλισμός των δυνάμεων, ο σχεδιασμός της επιχείρησης, η επιλογή των στόχων και η παρεχόμενη λειτουργική υποστήριξη»[126].

Όμοια, το Διεθνές Δικαστήριο το 2005 στην υπόθεση των *Ένοπλων δραστηριοτήτων στο έδαφος του Κονγκό*, επισήμανε ότι η στρατιωτική υποστήριξη ή η υποστήριξη σε θέματα εκπαιδεύσεως που παρείχε η Ουγκάντα στο Απελευθερωτικό Κίνημα του Κονγκό (Movement for the Liberation of the Congo - MLC), δεν επαρκούσαν για να δικαιολογήσουν ότι ήλεγχαν τον ηγέτη του MLC Jean-Pierre Bemba και τις δράσεις του, κατά τρόπο ώστε να θεωρείται (η MLC) όργανο της Ουγκάντα, ενεργοποιώντας τις προβλέψεις του Άρθρου 4 της ΕΔΔ περί ευθύνης κράτους[127]. Χαρακτηριστικό του αποτελεσματικού ελέγχου είναι ότι δεν απαιτείται ξεχωριστός έλεγχος σε κάθε πιθανή παράνομη πράξη αλλά μόνο η ύπαρξη ενός ευρύτερου σχεδίου, στο πλαίσιο του οποίου οι πράξεις αυτές δύνανται να λάβουν χώρα[128].

Κατ' αντιστοιχία, στον τομέα του Κυβερνοχώρου, εάν ένα κράτος χρηματοδοτεί μία ιδιωτική εταιρεία για τη διασφάλιση των επικοινωνιακών και πληροφοριακών του συστημάτων έναντι πιθανής κυβερνοαπειλής/

---

[125] *«…115…. United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua…»,* (1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA). INTERNATIONAL COURT OF JUSTICE*, σελ. 54 (παρ. 115). Ανάκτηση Ιανουάριος 30, 2017 από http://www.icj-cij.org/docket/files/70/6503.pdf

[126] *«…112…This partial dependency on the United States authorities…may also be inferred from other factors, some of which have been examined by the Court, such as the organization, training and equipping of the force, the planning of operations, the choosing of targets and the operational support provided…»* Ibid. σελ. 53, παρ. 112

[127] (2005). *Απόφαση Διεθνούς Δικαστηρίου στην Υπόθεση Ένοπλων Δραστηριοτήτων στο έδαφος του Κονγκό (DRC v Ουγκάντα),* σελ. 226, παρ. 160. Ανάκτηση Ιανουάριος 30, 2017, από http://www.icj-cij.org/docket/files/116/10455.pdf

[128] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 421. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

κυβερνοεπίθεσης, παρέχοντας προστασία και ειδικές διευκολύνσεις, τότε η εν λόγω «σχέση» μεταξύ του κράτους και της εταιρείας δεν επαρκεί ώστε να υφίσταται αποτελεσματικός έλεγχος του κράτους επί της εταιρείας.

Στον αντίποδα του «τεστ της Νικαράγουα», το Διεθνές Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία (ΔΠΔπΓ) στην υπόθεση *Tadic*, πρότεινε το τεστ του «συνολικού ελέγχου (overall test)», γνωστό και ως «τεστ του Tadic»[129]. Όπως επισήμανε το ΔΠΔπΓ στην ίδια υπόθεση, πρόκειται για ένα χαμηλότερου βαθμού ελέγχου τεστ[130] (lower degree of control), σε σχέση με το «απαιτητικό» τεστ του αποτελεσματικού ελέγχου της Νικαράγουα. Το ίδιο το δικαστήριο, το 2013 στην υπόθεση *Prlic et al*, προσδιόρισε ακριβέστερα τα στοιχεία του συνολικού ελέγχου, επισημαίνοντας ότι δεν απαιτείται μόνο εξοπλισμός και χρηματοδότηση, αλλά επιπλέον συντονισμός ή συμμετοχή στον γενικότερο σχεδιασμό των στρατιωτικών δραστηριοτήτων[131].

Αξίζει να επισημανθεί η διαφοροποίηση στην οποία κατέληξε το ΔΠΔπΓ στις περιπτώσεις ομάδων με ή χωρίς συγκεκριμένη, ιεραρχική, στρατιωτική δομή, ως προς την εφαρμογή του τεστ συνολικού ή αποτελεσματικού ελέγχου. Συγκεκριμένα, στην υπόθεση *Tadic*, προσδιόρισε ότι το τεστ συνολικού ελέγχου επαρκεί μόνο σε οργανωμένες, ιεραρχικά, στρατιωτικές ομάδες[132], ενώ παράλληλα τόνισε ότι το τεστ του αποτελεσματικού ελέγχου δύναται να εφαρμοστεί σε άτομα ή ομάδες χωρίς συγκεκριμένη στρατιωτική δομή[133]. Η τελευταία επισήμανση έχει

---

[129] Ibid. σελ. 122

[130] *«…124…such practice has envisaged State responsibility in circumstances where a lower degree of control than that demanded by the Nicaragua test was exercised…»,* (1999). *Απόφαση Εφετείου Διεθνούς Ποινικού Δικαστηρίου για την πρώην Γιογκοσλαβία στην υπόθεση Prosecutor v Tadic, IT-94-1-A*, σελ. 51, παρ. 124. Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

[131] *«…86…(a)…the latter wielded overall control over the group, not merely by equipping and financing the group, but also by coordinating or providing its assistance in the overall planning of its military activities…»*, (2013). *Απόφαση Διαρκούς Ποινικού Δικαστηρίου για την πρώην Γιουγκοσλαβία στην υπόθεση Prosecutor v Prlic (Trial Judgement), IT-04-74-T*, σελ. 28, παρ. 86(a). Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/prlic/tjug/en/130529-1.pdf

[132] *«…120…Consequently, for the attribution to a State of acts of these groups it is sufficient to require that the group as a whole be under the overall control of the State. …»,* (1999). *Απόφαση Εφετείου Διεθνούς Ποινικού Δικαστηρίου για την πρώην Γιογκοσλαβία στην υπόθεση Prosecutor v Tadic, IT-94-1-A*, σελ. 49, παρ. 120. Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

[133] *«…132… individuals or groups not organized into military structures. With regard to such individuals or groups, courts have not considered an overall or general level of control to be*

ιδιαίτερο ενδιαφέρον, ως προς την εφαρμογή της στην περίπτωση του Κυβερνοχώρου, λαμβάνοντας υπόψη το γεγονός ότι στο υπόψη πεδίο δε συνηθίζεται η αυστηρά δομημένη οργάνωση των οντοτήτων που δρουν σε αυτό[134]. Τελικά, το «τεστ Tadic» απορρίφθηκε από το Διεθνές Δικαστήριο της Χάγης ως μη πειστικό[135], όσον αφορά την ικανότητά του να μπορεί να αποδώσει τυχόν ευθύνη σε κράτος.

Γενικότερα στον τομέα του Κυβερνοχώρου, η έλλειψη σχετικής πρακτικής των κρατών σε συνδυασμό με το γεγονός ότι τα άρθρα της ΕΔΔ περί ευθύνης κρατών υπολείπονται[136] προκειμένου να δύνανται να καλύψουν όλες τις περιπτώσεις, συμπεριλαμβανομένων των σύγχρονων προκλήσεων, οδηγούν στο συμπέρασμα ότι τα κράτη θα πρέπει να συμφωνήσουν, ενδεχομένως, σε νέους, συγκεκριμένους κανόνες για το εν λόγω πεδίο. Αυτό, άλλωστε, είναι σύμφωνο και με τις προβλέψεις του άρθρου 55 της ΕΔΔ (lex specialis), που προσδιορίζει ότι τα υπόψη άρθρα δεν εφαρμόζονται σε περιπτώσεις όπου το ζήτημα της απόδοσης ευθύνης για διεθνώς παράνομες πράξεις καθορίζεται από διαφορετικούς, ειδικούς κανόνες του Διεθνούς Δικαίου[137]. Συναφώς[138], ζητήματα άσκησης ελέγχου από τα κράτη θα πρέπει να επανεξεταστούν και να επικαιροποιηθούν, καθόσον, όπως

---

sufficient, but have instead insisted upon specific instructions or directives aimed at the commission of specific acts, or have required public approval of those acts following their commission..», Ibid. σελ. 56, παρ. 132

[134] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 422. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[135] (2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου*, σελ. 210, παρ. 404-406 (ειδικότερα 404). Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

[136] *«…(2)…On that basis, article 55 makes it clear that the present articles operate in a residual way…»,* (2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25)*, Σχολιασμός άρθρου 55, σελ.340. παρ. (2). Ανάκτηση Ιανουάριος 31, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

[137] *«…Art.55. These articles do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law.»,* (2002). Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[138] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 425. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

ισχύει στην περίπτωση του Κυβερνοχώρου και στο πλαίσιο του τεστ άσκησης αποτελεσματικού ελέγχου, είναι αρκετά εύκολο πλέον για τις κυβερνήσεις να αποκρύψουν πληροφορίες για πολεμικές τους επιχειρήσεις. Ενδεχομένως μία πιο ευέλικτη μορφή άσκησης ελέγχου, παρεμφερής με αυτή του συνολικού, θα συνέβαλε στην ενίσχυση της κυβερνοασφάλειας.

4.2 Η ευθύνη σε «ακυβέρνητες περιοχές»

Το μη κερδοσκοπικό ερευνητικό και αναπτυξιακό κέντρο *RAND* στις Η.Π.Α., σε έκθεση που δημοσίευσε το 2007, χαρακτήρισε ως «ακυβέρνητες περιοχές» εκείνες όπου το κράτος αντιμετωπίζει σημαντικές προκλήσεις στην άσκηση ελέγχου. Δύναται να είναι κράτη που έχουν καταρρεύσει ή είναι υπό κατάρρευση και τα οποία ελέγχουν υποτυπωδώς τα χερσαία και θαλάσσια σύνορά του, ή ακόμα και περιοχές οι οποίες γεωγραφικά βρίσκονται εντός βιώσιμων κρατών, όπου η κεντρική κυβερνητική δικαιοδοσία δεν επεκτείνεται[139]. Σύμφωνα με τον καθηγητή Διεθνούς Δικαίου κ. Νικόλαο Τσαγκουριά, αποτελούν περιοχές όπου το κράτος με γεωγραφικούς όρους και όρους δυνατότητας διακυβέρνησης έχει καταρρεύσει[140].

Οι «ακυβέρνητες περιοχές»[141], λόγω της φύσης τους, σε ότι αφορά την έλλειψη κρατικού ελέγχου, συνιστούν γόνιμο έδαφος για μη κρατικούς δρώντες που επιδιώκουν να διαπράξουν τρομοκρατικές ενέργειες, εγκλήματα και άλλες παράνομες πράξεις. Σε αυτές συμπεριλαμβάνεται, πλέον, και ο Κυβερνοχώρος, όπου οι κυβερνοεπιθέσεις δύνανται να υποκινούνται, να διευκολύνονται και να εκτελούνται. Χαρακτηριστικό παράδειγμα αποτελεί ο ISIS, που οργανώνει και εκδηλώνει τέτοιες επιθέσεις από τα εδάφη που έχει καταλάβει σε Συρία και Ιράκ, έχοντας, μάλιστα, οργανώσει το δικό του «Κυβερνοστρατό» με την ονομασία *United Cyber Caliphate (UCC)*[142]. Παρά το γεγονός ότι ο ISIS, μέχρι σήμερα, δεν

[139] *RAND Report titled "Ungoverned territories: Understanding and Reducing Terrorism Risks".* (2007), Summary, σελ. xv. Ανάκτηση Ιανουάριος 31, 2017, από http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.pdf

[140] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 458. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

[141] Ibid. , σελ. 455-456

[142] Ibid.

έχει προκαλέσει με τις κυβερνοεπιθέσεις του σημαντικές ζημιές ή ανθρώπινες απώλειες, καθόσον χρησιμοποιεί περισσότερο το διαδίκτυο για προπαγάνδα, χρηματοδότηση και στρατολόγηση νέων μαχητών, εντούτοις αυτό δε σημαίνει ότι στο μέλλον δεν δύναται να το πράξει.

Οι ακυβέρνητες περιοχές δεν αποτελούν μόνο απειλή για την ειρήνη και την ασφάλεια, αλλά και για τη διεθνή έννομη τάξη, θέτοντας σημαντικές προκλήσεις, μεταξύ άλλων, στην έννοια της κρατικής υπόστασης και της ευθύνης των κρατών.

Σύμφωνα με τον παραδοσιακό ορισμό της κρατικής υπόστασης (*statehood*) έναντι του Διεθνούς Δικαίου, όπως αυτός διατυπώθηκε στο πρώτο άρθρο της Σύμβασης για τα Δικαιώματα και τις Υποχρεώσεις των Κρατών, που υπεγράφη το 1933 στο Μοντεβίδεο[143], ένα από τα κριτήριά της είναι η α π ο τ ε λ ε σ μ α τ ι κ ή δ ι α κ υ β έ ρ ν η σ η, υπό την έννοια ότι μία εξουσία δύναται να ασκήσει αποτελεσματικό έλεγχο στο έδαφος και στους πολίτες του. Η απουσία κρατικής υπόστασης σε μία περιοχή, συνεπάγεται αδυναμία άσκησης αποτελεσματικού ελέγχου/διακυβέρνησης σε αυτήν και κατ' επέκταση αδυναμία εφαρμογής των διεθνών δεσμεύσεων που απορρέουν από διεθνείς, διμερείς ή πολυμερείς συμφωνίες στις οποίες το υπόψη κράτος παραμένει συμβαλλόμενο μέρος. Έτσι, κυβερνοεπιθέσεις που εκδηλώνονται από μη κρατικούς δρώντες, που χρησιμοποιούν υποδομές Κυβερνοχώρου σε ακυβέρνητες περιοχές, δε δύνανται να αποδοθούν σε αυτούς, έναντι του Διεθνούς Δικαίου, υπό την έννοια ότι δε δεσμεύονται από καμία διεθνή συνθήκη στις οποίες δεν έχουν δικαίωμα να προσχωρήσουν. Παράλληλα όμως, δε δύνανται να αποδοθούν ούτε και στα κράτη, υπό την έννοια ότι δεν ισχύουν τα κριτήρια του Άρθρου 8 της Επιτροπής Διεθνούς Δικαίου περί ευθύνης κρατών (οδηγίες, διεύθυνση και έλεγχος), ώστε να δικαιολογείται η απόδοση ευθύνης σε αυτά (τα κράτη) για τις παράνομες ενέργειες των μη κρατικών δρώντων.

Αντιθέτως, ευθύνη σε μη κρατικό δρώντα δύναται να αποδοθεί στο πλαίσιο του εσωτερικού ή του Διεθνούς Ποινικού Δικαίου. Ωστόσο, αυτό καθίσταται

[143] *«…Art.1. The State as a person of international law should possess the following qualifications : (a) a permanent population ; (b) a defined territory ; (c) government ; and (d) capacity to enter into relations with the other States...», Convention on Rights and Duties of States adopted by the Seventh International Conference of American States.* (1933, Δεκεμβρίου 26), . Ανάκτηση Ιανουάριος 31, 2017, από https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf

ιδιαίτερα προβληματικό, λαμβάνοντας υπόψη, εν παραδείγματι, τη δυσκολία που υφίσταται αφενός για τη Συρία να απαιτήσει την εφαρμογή της εσωτερικής νομοθεσίας στις ακυβέρνητες περιοχές της που ελέγχονται από τον ISIS και αφετέρου για τα διεθνή δικαστήρια να καλέσουν ενώπιων τους τον ISIS, ως μη κρατικό δρώντα ή υποκείμενο του Διεθνούς Δικαίου. Κατόπιν των ανωτέρω, γίνεται σαφές ότι η αποτελεσματικότητα της κρατικής υπόστασης (effective statehood) επηρεάζει άμεσα το επίπεδο απόδοσης της ευθύνης[144].

Ωστόσο, τα άρθρα της Επιτροπής Διεθνούς Δικαίου περί ευθύνης κρατών, αναφέρονται σε δύο περιπτώσεις, στις οποίες ένα κράτος δύναται να είναι υπεύθυνο για τις πράξεις μη κρατικού δρώντα, χωρίς να πρέπει να του αποδοθεί ευθύνη, υπό την έννοια των προβλέψεων του συναφούς Άρθρου 8[145]. Σύμφωνα, λοιπόν, με το Άρθρο 9 περί ευθύνης κρατών, «η συμπεριφορά ατόμου ή ομάδας ατόμων θα θεωρείται ενέργεια του κράτους, σύμφωνα με το Διεθνές Δίκαιο, εάν το άτομο ή η ομάδα ατόμων ασκεί στην πραγματικότητα στοιχεία κυβερνητικής εξουσίας σε περίπτωση απουσίας ή ανεπαρκούς λειτουργίας των επίσημων αρχών και υπό περιστάσεις τέτοιες, οι οποίες απαιτούν την άσκηση αυτών των στοιχείων εξουσίας» [146].

Στο πλαίσιο εφαρμογής του ανωτέρου άρθρου στον Κυβερνοχώρο, θα πρέπει καταρχήν να διευκρινιστούν τα στοιχεία εκείνα της κυβερνητικής εξουσίας που αναφέρονται στο σχετικό κείμενο. Η φορολόγηση, η αστυνόμευση, η άμυνα και η δικαιοσύνη συνεχίζουν, να αποτελούν μερικές από τις θεμελιώδεις λειτουργίες[147]. Ενώ η άμυνα και η αστυνόμευση υφίστανται μόνο στον «φυσικό

---

[144] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 462. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

[145] *«…Art.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…»* (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών,* Άρθρο 8. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[146] «…Art.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…», Ibid. Άρθρο 9*

[147] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 463 και υποσημείωση 31. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

κόσμο» (απαιτούν δηλαδή φυσική παρουσία και έλεγχο του μη κρατικού δρώντα), οι λειτουργίες της φορολόγησης και της δικαιοσύνης, με πρόσβαση σε αντίστοιχα κυβερνητικά λογισμικά και βάσεις δεδομένων, δύνανται να υφίστανται στον Κυβερνοχώρο.

Τι γίνεται, όμως, στην περίπτωση μη κρατικών δρώντων που διαπράττουν παράνομες δραστηριότητες, όσον αφορά το αν εμπίπτουν στις προβλέψεις του ανωτέρω άρθρου; Σύμφωνα με τον καθηγητή κ. Τσαγκουριά, δεν υπάρχει ξεκάθαρη απάντηση, ωστόσο παραβιάσεις κανόνων *jus cogens*[148] είναι αρκετές για να εξαιρέσουν τις μη κρατικές αυτές οντότητες από τις εν λόγω προβλέψεις[149]. Συναφώς, η Ανεξάρτητη Διεθνής Εξεταστική Επιτροπή για την Αραβική Δημοκρατία της Συρίας σε έκθεσή της στο Συμβούλιο Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών (UNHRC) το 2012, σημείωσε ότι, κατ' ελάχιστο, οι κανόνες *jus cogens* «δεσμεύουν κράτη, άτομα και μη κρατικές συλλογικές οντότητες, συμπεριλαμβανομένων και ένοπλων ομάδων»[150].

Γενικά, οι μη κρατικοί δρώντες που εμπίπτουν στις προβλέψεις του ανωτέρω Άρθρου 9 περί ευθύνης κρατών, έχουν ή τουλάχιστον πρέπει να έχουν δύο βασικά χαρακτηριστικά: τον προσωρινό και όχι μακροπρόθεσμο (όπως στην περίπτωση της Hezbollah) χαρακτήρα της ανάληψης των κυβερνητικών εξουσιών, καθώς την εθελοντική παρέμβασή τους, χωρίς να θέτουν εκείνοι σκόπιμα τις κυβερνητικές εξουσίες εκτός λειτουργίας, προκειμένου να τις αναλάβουν[151].

Η δεύτερη περίπτωση που η συμπεριφορά μη κρατικών δρώντων θεωρείται ενέργεια του κράτους, μη εμπίπτουσα στις προβλέψεις του Άρθρου 8 περί ευθύνης κρατών, αποτελεί το Άρθρο 10, που αφορά σε συμπεριφορά επαναστατικού ή άλλου κινήματος. Σύμφωνα με αυτό, υφίστανται δύο υποπεριπτώσεις. Πρώτον,

[148] Απαγόρευση χρήσης βίας, γενοκτονίας ή εγκλημάτων κατά της ανθρωπότητας

[149] Ibid. σελ. 463

[150] *«…the commission notes that, at a minimum, human rights obligations constituting peremptory international law (jus cogens) bind States, individuals and non-State collective entities, including armed groups…», UNHRC 'Report of the independent international commission of inquiry on the Syrian Arab Republic, A/HRC/19/69.* (2012, Φεβρουάριος 22), παρ. 106. Ανάκτηση Ιανουάριος 31, 2017, από http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session19/A-HRC-19-69_en.pdf

[151] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 464. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

όταν το επαναστατικό κίνημα εγκαθίσταται ως νέα κυβέρνηση του κράτους (θα θεωρείται ενέργεια του κράτους) και δεύτερον όταν το επαναστατικό ή άλλο κίνημα επιτυγχάνει να εγκαθιδρύσει ένα νέο κράτος σε τμήμα του εδάφους προϋπάρχοντος κράτους ή σε έδαφος υπό τη διοίκησή του (θα θεωρείται ενέργεια του νέου κράτους)[152]. Το επαναστατικό κίνημα, σύμφωνα με την Επιτροπή Διεθνούς Δικαίου και το Άρθρο 1 του Πρόσθετου Πρωτοκόλλου ΙΙ (1977)[153], είναι οργανωμένο και ασκεί τον έλεγχο εδαφικής επικράτειας, συνήθως στο ίδιο κράτος εναντίον του οποίου επαναστάτησε[154].

Ωστόσο, η διατύπωση του ανωτέρω Άρθρου 10 περί ευθύνης κρατών δημιουργεί αναπόφευκτους περιορισμούς, όσον αφορά την απόδοση ευθύνης. Έτσι, «απαλλάσσει», για πρότερες πράξεις τους, κινήματα που απέτυχαν να αναλάβουν τη διακυβέρνηση εδαφών του κράτους, καθώς και όσα συμμετέχουν σε συμφωνία συνασπισμού εξουσίας. Απαλλάσσει όμως τα υπόψη κινήματα και για πράξεις για τις οποίες δε δεσμεύονται διεθνώς. Έτσι, εν παραδείγματι, εάν ο ISIS καταφέρει να ιδρύσει νέο κράτος στη Συρία, τότε, θα ευθύνεται για προηγούμενες κυβερνοεπιθέσεις του, αλλά όχι για παραβιάσεις θεμελιωδών αρχών, όπως της απαγόρευσης μη επέμβασης ή των ανθρωπίνων δικαιωμάτων, καθόσον δε δεσμεύεται νομικά από τις σχετικές διεθνείς συμβάσεις.

Κατόπιν των ανωτέρω, διαπιστώνεται ότι υφίστανται κενά στην απόδοση ευθύνης από το Διεθνές Δίκαιο, σε ότι αφορά μη κρατικούς δρώντες που ελέγχουν

---

[152] *«…Art.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 pre-existing 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. …»* (2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών,* Άρθρο 10. Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83

[153] *«…This Protocol…shall apply to all armed conflicts… which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted mili tary operations and to implement this Protocol…», Πρόσθετο Πρωτόκολλο ΙΙ στη Σύμβαση της Γενεύης του 1949.* (1977, Ιούνιος 8). Ανάκτηση Ιανουάριος 31, 2017, από https://treaties.un.org/doc/publication/unts/volume%201125/volume-1125-i-17513-english.pdf

[154] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 464. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

ακυβέρνητες περιοχές και τις παράνομες πράξεις που λαμβάνουν χώρα σε αυτές ή από αυτές[155]. Σύμφωνα με τον καθηγητή κ. Τσαγκουριά, θα πρέπει να εξεταστούν περαιτέρω οι συνθήκες κάτω από τις οποίες θα δύναται να αποδοθούν υποχρεώσεις και ευθύνη σε μη κρατικούς δρώντες, υπό το φως της δυναμικής που διαμορφώνεται από την παρουσία και τα αποτελέσματα των πράξεων τους. Για το σκοπό αυτό, θεωρεί ότι «ένας μη κρατικός δρώντας θα πρέπει να ασκεί αποτελεσματικά την εξουσία και τον έλεγχο στο έδαφος και τους πολίτες», ώστε να δύναται να δεσμευτεί έναντι του Διεθνούς Δικαίου˙ «εξουσία είναι η δύναμη να αποφασίζει, να διατάζει, να διευθύνει, να εκπροσωπεί και να επιβάλει τη συμμόρφωση» σε κανόνες και νόμους, ενώ ο έλεγχος είναι το στοιχείο που του δίνει τη δύναμη να ασκήσει τέτοια εξουσία[156]. Προϋπόθεση για τα ανωτέρω αποτελεί η ύπαρξη οργανωμένης δομής, η οποία, μεταξύ άλλων, διαφοροποιεί τον μη κρατικό δρώντα από τα μέλη του, ώστε να δύναται να θεωρηθεί ως ανεξάρτητη νομική προσωπικότητα. Ο συσχετισμός αποτελεσματικότητας και νομικής προσωπικότητας επιβεβαιώθηκε, άλλωστε, και από το Διεθνές Δικαστήριο, στη Γνωμοδότησή του για τις Επανορθώσεις από Υπηρεσίες στα Ηνωμένα Έθνη (1949), όπου το δικαστήριο απέδωσε νομική προσωπικότητα στα Ηνωμένα Έθνη, ως μη κρατικός δρώντας, λόγω των λειτουργιών του, των δικαιωμάτων και των υποχρεώσεων που έχει, καθώς και των οργάνων που διαθέτει με ανεξάρτητη/διαφορετική αντίληψη/γνώμη, σε σχέση με τα μέλη του[157].

Ωστόσο, τα ανωτέρω δε δύνανται, κατά τον καθηγητή κ. Τσαγκουριά[158] να εφαρμοστούν στον Κυβερνοχώρο και κατ' επέκταση να δύνανται να αποτελέσουν το απαραίτητο νομικό υπόβαθρο, ώστε οι ομάδες που δραστηριοποιούνται στο πεδίο αυτό να μπορούν να αναγνωριστούν νομικές προσωπικότητες. Καταρχήν,

---

[155] Ibid. σελ. 466

[156] *«…A non-state actor should exercise effective authority and control over territory and people to trigger its international law rights, duties and responsibility. Authority is the power to decide, order, direct, delegate and enforce compliance, whereas control is the legal and material power to effectuate such authority…»,* Ibid. σελ. 467

[157] Ibid. σελ. 467 και *Advisory Opinion of 11 April 1949 on Reparation for Injuries Suffered in the Service of the United Nations.* (1949, Απρίλιος 11), σελ. 178-179. Ανάκτηση Ιανουάριος 31, 2017, από http://www.icj-cij.org/docket/files/4/1835.pdf

[158] Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, σελ. 468. Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

υφίσταται αντικειμενική δυσκολία σε ότι αφορά τη δυνατότητα άσκησης αποτελεσματικού ελέγχου επί εδάφους και ατόμων στον υπόψη ιδιαίτερο, «εικονικό» χώρο. Παράλληλα, οι κυβερνο-ομάδες δε διαθέτουν, συνήθως, οργανωμένες και ιεραρχικές δομές, ενώ η επιρροή και οι επιπτώσεις στον φυσικό κόσμο επί των μελών τους, είναι, ως επί το πλείστον, αμελητέες.

4.3 Ατομική ποινική ευθύνη – Ευθύνη ανωτέρου

Στο καινούριο Άρθρο 8bis του Καταστατικού του Διεθνούς Ποινικού Δικαστηρίου[159] της Ρώμης, καθορίζεται η έννοια του εγκλήματος της χρήσης βίας (*crime of aggression*), σύμφωνα με την οποία:

> «…means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations…» (άρθρο 8bis, παρ.1)

Παρόλο που η διατύπωση του εν λόγω άρθρου αναφέρεται σε ένα πρόσωπο, η δεύτερη έκδοση των Στοιχείων Εγκλημάτων (*Elements of Crimes*) διευκρινίζει ότι περισσότερα του ενός ατόμου δύνανται να είναι σε θέση να ασκήσουν τον απαραίτητο έλεγχο[160]. Συναφώς, το Δικαστήριο της Νυρεμβέργης το 1948, κατά την εκδίκαση της υπόθεσης *The United States of America vs. Wilhelm von Leeb et al. (High Command Trial)*[161], όπου αναγνωρίστηκε ότι ο Χίτλερ, όσο απολυταρχικός και αν ήταν, δεν μπορούσε από μόνος του να διαμορφώσει μία

[159] *Καταστατικό Διεθνούς Ποινικού Δικαστηρίου.* (1998, Ιούλιος 17), σελ.9, άρθρο 8bis, παρ.1. Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf

[160] *«… With respect to an act of aggression, more than one person may be in a position that meets these criteria…», Elements of Crimes, International Criminal Court.* (2011), σελ. 43, δεύτερη υποσημείωση (75). Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf

[161] *«… No matter how absolute his authority, Hitler alone could not formulate a policy of aggressive war and alone implement that policy by preparing, planning, and waging such a war. …», The United States of America vs. Wilhelm von Leeb et al. (HIGH COMMAND TRIAL).* (1948, Οκτώβριος 27), 11 Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No 10 (TWC), σελ 21, {485}. Ανάκτηση Ιανουάριος 31, 2017, από http://werle.rewi.hu-berlin.de/High%20Command%20Case.pdf

πολιτική επιθετικού πολέμου και κατ' επέκταση να προετοιμάσει, να σχεδιάσει και να διεξάγει έναν τέτοιο πόλεμο[162]. Το ίδιο δικαστήριο, κατά την εκδίκαση των σημαντικών εγκληματιών πολέμου (*Trial of Major War Criminals*), ήταν εξίσου σαφές, λέγοντας ότι «ο Χίτλερ, δεν μπορούσε να διεξάγει επιθετικό πόλεμο από μόνος του»[163].

Κατά συνέπεια, διεθνής ποινική ευθύνη υφίσταται στο βαθμό που το άτομο ή μια ομάδα ατόμων δύνανται να ασκήσουν αποτελεσματικό έλεγχο ή να διευθύνουν τις πολιτικές ή στρατιωτικές ενέργειες ενός κράτους κατά την τέλεση μιας πράξης χρήσης βίας. Δεν έχει δηλαδή σημασία απλά και μόνο η θέση του στην ιεραρχική αλυσίδα. Το κριτήριο του αποτελεσματικού ελέγχου, είναι και το βασικό στοιχείο, η ύπαρξη του οποίου αρκεί για να αποδώσει διεθνή ποινική ευθύνη και σε άτομα τα οποία δεν ανήκουν, απαραίτητα και άμεσα στην ανώτερη ηγεσία, ακόμα και ανήκουν σε διαφορετικούς κύκλους απασχόλησης. Σύμφωνα με το Δικαστήριο της Νυρεμβέργης, τα άτομα αυτά μπορούσαν να είναι είτε υψηλόβαθμα στελέχη στον δημοσιονομικό, βιομηχανικό ή οικονομικό τομέα μιας χώρας[164], είτε, πολιτικοί, στρατιωτικοί ηγέτες, διπλωμάτες και επιχειρηματίες[165]. Εφόσον δέχονταν να συνεργαστούν με τον Χίτλερ, καθιστούσαν εαυτούς τους μέρος του σχεδίου του[166].

Ωστόσο, η εν λόγω απόδοση προσωπικής διεθνούς ποινικής ευθύνης, σε πρόσωπα που δεν ανήκουν στην άμεση ηγεσία ενός εγκληματικού καθεστώτος, είναι ιδιαίτερα δύσκολη. Χαρακτηριστικά επισημαίνεται ότι στην υπόθεση *Krupp*, το

---

[162] Ambos, K. (2016, Αύγουστος 7). *Individual Criminal Responsibility for Cyber Aggression.* Ανάκτηση από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

[163] *«… 'Hitler could not make aggressive war by himself…», Trial of Major War Criminals before the International Military Tribunal, Vol. 22.* (1948) σελ. 468. Ανάκτηση Ιανουάριος 31, 2017, από https://www.loc.gov/rr/frd/Military_Law/pdf/NT_Vol-XXII.pdf

[164] *«… 2. Any person without regard to nationality or the capacity in which he acted, is deemed to have committed a crime… if he… held high position in the financial, industrial or economic life of any such country. …», The United States of America vs. Wilhelm von Leeb et al. (HIGH COMMAND TRIAL).* (1948, Οκτώβριος 27), 11 Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No 10 (TWC), σελ 10, άρθρο II(2). Ανάκτηση Ιανουάριος 31, 2017, από http://werle.rewi.hu-berlin.de/High%20Command%20Case.pdf

[165] *«… He [Hitler] had to have the co-operation of statesmen, military leaders, diplomats, and business men…», Trial of Major War Criminals before the International Military Tribunal, Vol. 22.* (1948), σελ. 468-469. Ανάκτηση Ιανουάριος 31, 2017, από https://www.loc.gov/rr/frd/Military_Law/pdf/NT_Vol-XXII.pdf

[166] *«… When they, with knowledge of his aims, gave him [Hitler] their co-operation, they made themselves parties to the plan he had initiated…»,*Ibid. σελ. 469

Δικαστήριο της Νυρεμβέργης, αφού αναφέρθηκε στην έννοια της ενοχής, η οποία πρέπει να είναι προσωπική[167], διευκρίνισε ότι το γεγονός και μόνο ότι ανήκε στη Διεύθυνση του Krupp ή ήταν υπάλληλος της επιχείρησης, δε δύναται να επαρκεί για να του αποδοθεί ευθύνη/ενοχή[168].

Το βασικό, λοιπόν, κριτήριο του αποτελεσματικού ελέγχου και διεύθυνσης των πολιτικών ή στρατιωτικών πράξεων ενός κράτους, κύριο χαρακτηριστικό μιας ηγεσίας, όπως αυτό διατυπώθηκε στο προαναφερόμενο άρθρο 8bis του Καταστατικού της Ρώμης, επαναλήφθηκε και στην καινούρια παράγραφο 3bis του Άρθρου 25 του εν λόγω Καταστατικού:

> «…Article 25 Individual criminal responsibility…3 bis. In respect of the crime of aggression, the provisions of this article shall apply only to persons in a position effectively to exercise control over or to direct the political or military action of a State…»[169].

Όπως προκύπτει από την ανωτέρω διατύπωση, όλα τα άτομα που δεν εμπίπτουν στην εν λόγω πρόβλεψη αλλά συμμετείχαν στο διαπραχθέν έγκλημα χρήσης βίας, εξαιρούνται ποινικής ευθύνης, το οποίο συνιστά, κατά τον *Kai Ambos,* καθηγητή Διεθνούς Ποινικού Δικαίου στο Πανεπιστήμιο του Gottingen και Δικαστή στο Περιφερειακό Δικαστήριο του Gottingen, κενό ατιμωρησίας[170].

Στην περίπτωση μιας κυβερνοεπίθεσης, η εκδήλωση της πράξης πραγματοποιείται από κάποιους προγραμματιστές (hackers). Όταν αυτή εκδηλώνεται υπό τη διεύθυνση και τον έλεγχο του κράτους, τότε, με βάση τα ανωτέρω, τα πρόσωπα της ιεραρχίας τα οποία ασκούν, πραγματικά

---

[167] *«… the Tribunal emphasized that guilt must be personal…», US v Krupp et al (Krupp case), US Military Tribunal, Case No. 58.* (1947-1948), σελ. 150, παρ. 4(viii). Ανάκτηση Ιανουάριος 31, 2017, από https://www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-10.pdf

[168] *«…The mere fact without more that a defendant was a member of the Krupp Directorate or an official of the firm is not sufficient…»*, Ibid. σελ. 150, παρ. 4(viii)

[169] *Καταστατικό Διεθνούς Ποινικού Δικαστηρίου.* (1998, Ιούλιος 17), σελ. 18, άρθρο 25, παρ. 3bis. Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf

[170] *«…In turn, all other persons participating in a crime of aggression are exempted from criminal responsibility, creating a big impunity gap…»,* Ambos, K. (2016, Αύγουστος 7). *Individual Criminal Responsibility for Cyber Aggression*, σελ. 502. Ανάκτηση από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

αποτελεσματικό έλεγχο και διεύθυνση της εν λόγω επιθετικής πράξης είναι ποινικά υπεύθυνα για αυτή, όχι όμως οι προγραμματιστές.

Σύμφωνα, μάλιστα, με την προσέγγιση του καθηγητή κ. Ambos[171], η απόδοση ποινικής ευθύνης στα ανωτέρω πρόσωπα, δεν μπορεί να επηρεαστεί/εξαρτηθεί από τα χρησιμοποιούμενα μέσα ή από τη λεπτομερή γνώση τεχνικών χαρακτηριστικών τους. Ένα υψηλά ιστάμενο πρόσωπο που διευθύνει, εκ μέρους του κράτους, πλήρως μια κυβερνοεπίθεση, κατά πάσα πιθανότητα δε γνωρίζει αλλά και δεν απαιτείται να γνωρίζει τεχνικές λεπτομέρειες των μέσων που θα χρησιμοποιηθούν. Κατά συνέπεια, η έλλειψη της συγκεκριμένης γνώσης, δε θα μπορούσε να θεωρηθεί ως ελαφρυντικό του.

Σε γενικές γραμμές, η ευθύνη ανωτέρου αποτελεί ένα ισχυρό εργαλείο για την αποτροπή εγκλημάτων πολέμου και παραβιάσεων ανθρωπίνων δικαιωμάτων[172], υπό την έννοια ότι αποδίδοντας ευθύνη σε αυτούς για πράξεις υφισταμένων τους, αναγκάζονται εκ των πραγμάτων να βρίσκονται συνέχεια σε εγρήγορση. Οι προβλέψεις περί ευθύνης ανωτέρου κωδικοποιούνται στα άρθρα 86 (*Failure to act*)[173] και 87 (*Duty of Commanders*)[174] του Πρώτου Πρόσθετου

---

[171] *«…A person in a position to issue an order to undertake an act of aggression and to effectively control the aggressive enterprise need not know the technical details of the functioning of the means employed to execute his or her order. It suffices that he/she knows that his/her order will be executed and cause harmful consequences to the persons or objects targeted …»,* Ibid. σελ. 503-504

[172] Sliedregt, E. v. (2016, Σεπτέμβριος 22). *Command Responsibility and Cyberattacks*, σελ. 510. Ανάκτηση Ιανουάριος 31, 2017, από http://jcsl.oxfordjournals.org/

[173] *«…Article 86 — Failure to act 1. The High Contracting Parties and the Parties to the conflict shall repress grave breaches, and take measures necessary to suppress all other breaches, of the Conventions or of this Protocol which result from a failure to act when under a duty to do so. 2. The fact that a breach of the Conventions or of this Protocol was committed by a subordinate does not absolve his superiors from penal or disciplinary responsibility, as the case may be, if they knew, or had information which should have enabled them to conclude in the circumstances at the time, that he was committing or was going to commit such a breach and if they did not take all feasible measures within their power to prevent or repress the breach.…», Πρώτο Πρόσθετο Πρωτόκολλο στη Συνθήκη της Γενεύης (1949).* (1977, Ιούνιος 8), σελ. 62, άρθρο 86. Ανάκτηση Ιανουάριος 31, 2017, από https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf

[174] *«…Article 87 — Duty of commanders 1. The High Contracting Parties and the Parties to the conflict shall require military commanders, with respect to members of the armed forces under their command and other persons under their control, to prevent and, where necessary, to suppress and report to competent authorities breaches of the Conventions and of this Protocol. 2. In order to prevent and suppress breaches, High Contracting Parties and Parties to the conflict shall require that, commensurate with their level of responsibility, commanders ensure that members of the armed forces under their command are aware of their obligations under the Conventions and this Protocol. 3. The High Contracting Parties and Parties to the conflict shall require any commander*

Πρωτοκόλλου στη Συνθήκη της Γενεύης (1949). Όπως προκύπτει από αυτά, υπάρχουν δύο μορφές ευθύνης ανωτέρου: η ενεργητική (ευθύνη λόγω εντολής προς υφισταμένους του να διαπράξουν κάποιο έγκλημα) και η παθητική (ευθύνη λόγω αδυναμίας αποτροπής διάπραξης εγκλήματος από τους υφισταμένους του).

Το ΔΠΔπΓ, στην υπόθεση *Hadzihasanovic*[175], έκρινε (με πλειοψηφία 3 έναντι 2) ότι ο διοικητής Kubura, δεν μπορούσε να κατηγορηθεί για πράξεις που γνώριζε πριν αναλάβει διοίκηση και για τις οποίες δεν ανέλαβε καμία ενέργεια όταν έγινε διοικητής, καθόσον ο αποτελεσματικός έλεγχος επί των υφισταμένων του έπρεπε να υφίσταται κατά τα χρόνο εκδήλωσης της επιθετικής πράξης[176].

Το Διεθνές Ποινικό Δικαστήριο στην υπόθεση *Bemba*[177], τόνισε ότι το Άρθρο 28 του Καταστατικού της Ρώμης, αποτελεί έναν τρόπο λειτουργίας, μέσω της οποίας οι ανώτεροι, δύνανται να θεωρηθούν ποινικά υπεύθυνοι για εγκλήματα που διαπράχθηκαν από τους υφισταμένους τους.

Κατόπιν των ανωτέρω και σύμφωνα με τον κ. *Elies van Sliedregt*, καθηγητή του Διεθνούς και Συγκριτικού Ποινικού Δικαίου στο Πανεπιστήμιο του Leeds, η ευθύνη ανωτέρω στοιχειοθετείται σε τρία βασικά κριτήρια/προϋποθέσεις[178]. Πρώτον, θα πρέπει να υφίσταται ιεραρχική σχέση διοίκησης μεταξύ του ανωτέρου και των υφισταμένων του. Δεύτερον, ο ανώτερος θα πρέπει να γνωρίζει την παράνομη συμπεριφορά των υφισταμένων του. Τρίτον, θα πρέπει να έχει αποτύχει ο ανώτερος να λάβει όλα εκείνα τα απαραίτητα μέτρα, προκειμένου να αποτρέψει την εκδήλωση των παράνομων πράξεων από τους υφισταμένους του.

---

who is aware that subordinates or other persons under his control are going to commit or have committed a breach of the Conventions or of this Protocol, to initiate such steps as are necessary to prevent such violations of the Conventions or this Protocol, and, where appropriate, to initiate disciplinary or penal action against violators thereof.…», Ibid. σελ. 62-63, άρθρο 87.

[175] *Prosecutor v Hadzihasanovic, Alagic and Kubura.* (2003, Ιούλιος 16), παρ. 51. Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/hadzihasanovic_kubura/acdec/en/030716.htm

[176] Sliedregt, E. v. (2016, Σεπτέμβριος 22). *Command Responsibility and Cyberattacks*, σελ. 511. Ανάκτηση Ιανουάριος 31, 2017, από http://jcsl.oxfordjournals.org/

[177] *«… Article 28 provides a mode of liability, through which superiors may be held criminally responsible for crimes...committed by his or her subordinates…», Prosecutor v Bemba (Judgment) ICC-01/05-01/08.* (2016, Μάρτιος 21), σελ. 80-81, παρ. 171. Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/CourtRecords/CR2016_02238.PDF

[178] Sliedregt, E. v. (2016, Σεπτέμβριος 22). *Command Responsibility and Cyberattacks*, σελ. 511. Ανάκτηση Ιανουάριος 31, 2017, από http://jcsl.oxfordjournals.org/

Συμπληρωματικά, όπως συμπέρανε το ΔΠΔπΓ στην υπόθεση *Blaskic*[179], επισημαίνεται ότι ο ανώτερος δεν απαιτείται να γνωρίζει τα στοιχεία των ατόμων που διέπραξαν εν τέλει τις παράνομες πράξεις, αρκεί να μπορεί να αποδειχθεί ότι υφίσταται συνδετική σχέση μεταξύ των ατόμων αυτών και των υφισταμένων του.

Τέλος, σε ότι αφορά την εφαρμογή ή μη του Διεθνούς Ανθρωπιστικού Δικαίου στην περίπτωση των ένοπλων συρράξεων, το Εφετείο του ΔΠΔπΓ στην υπόθεση *Tadic*[180], κατέληξε ότι σε μη διεθνείς ένοπλες συρράξεις, οποιαδήποτε πράξη βαίνει πέραν εσωτερικών αναταραχών ή διαδηλώσεων, ενεργοποιεί τις προβλέψεις του ΔΑΔ. Σύμφωνα με το Εγχειρίδιο του Tallinn, στην περίπτωση των κυβερνοεπιθέσεων, απαιτείται η τέλεση εχθροπραξιών ώστε να δικαιολογείται η εφαρμογή του ΔΑΔ[181]. Κατά συνέπεια, στην περίπτωση των κυβερνοεπιθέσεων στην Εσθονία (2007), όπου δε διαπράχθηκαν εχθροπραξίες, δεν μπορεί να εφαρμοστεί το ΔΑΔ. Αντιθέτως, στη Γεωργία το 2008 εφαρμόζεται, καθόσον οι κυβερνοεπιθέσεις έλαβαν χώρα παράλληλα με ένοπλες εχθροπραξίες.

[179] *Prosecutor v Blaskic (Judgment) IT-95-14-A.* (2004, Ιούλιος 29), σελ. 79-80, παρ. 217. Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/blaskic/acjug/en/bla-aj040729e.pdf
[180] Ibid. σελ. 509
[181] Ibid.

ΜΕΡΟΣ Β' – Στρατηγική θέσμιση κυβερνοάμυνας έναντι των κυβερνοεπιθέσεων στη σύγχρονη εποχή

ΚΕΦΑΛΑΙΟ 1
Η ιστορία των κυβερνοεπιθέσεων

Η ραγδαία ανάπτυξη των υπολογιστικών συστημάτων και η συνεχώς αυξανόμενη χρήση των υπηρεσιών του διαδικτύου από κρατικές και μη δομές, οδήγησαν αναπόφευκτα στην επαύξηση της εξάρτησης των υπόψη πληροφοριακών συστημάτων από τις εν λόγω υπηρεσίες. Σύντομα τα συστήματα αυτά άρχισαν να δέχονται μία σειρά επιθέσεων, οι οποίες κατάφερναν συχνά να είναι αποτελεσματικές, διατηρώντας την ανωνυμία των «επιτιθέμενων». Η νέα αυτή μορφή των κυβερνοεπιθέσεων, σε συνδυασμό με την ικανότητα διατήρησης της προαναφερόμενης ανωνυμίας, δημιούργησε καινούρια ερωτηματικά, ως προς την εφαρμογή των κανόνων του Διεθνούς Δικαίου στις περιπτώσεις αυτές.

1.1 Είδη κυβερνοεπιθέσεων.

Προκειμένου να καταστεί περισσότερο ξεκάθαρη η φύση των νέων αυτών κυβερνοεπιθέσεων, κρίνεται σκόπιμο να γίνει αναφορά στις διάφορες μορφές με τις οποίες έχουν εκδηλωθεί μέχρι σήμερα. Η εξέταση των μορφών αυτών, σε συνδυασμό με την εξέταση των καταγεγραμμένων περιπτώσεων κυβερνοεπίθεσης, ιδιαίτερα εναντίον κρατικών δομών, θα συμβάλλει περισσότερο στην εξαγωγή χρήσιμων συμπερασμάτων ως προς το στοιχείο της ενδεχόμενης ύπαρξης της ευθύνης του κράτους, το οποίο συνιστά ιδιαίτερα σημαντικό παράγοντα για την ενεργοποίηση και ορθή εφαρμογή κανόνων Διεθνούς Δικαίου.

Μία κυβερνοεπίθεση τύπου «*DoS*[182]» (*Άρνηση Υπηρεσίας – Denial of Service*), η οποία χρησιμοποιήθηκε κατά κόρον στις σοβαρές κυβερνοεπιθέσεις εναντίον Εσθονίας (2007) και Γεωργίας (2008), εκδηλώνεται με την ταυτόχρονη αποστολή ενός τεράστιου όγκου αιτημάτων για πληροφορία προς τον υπολογιστή – «στόχο», με σκοπό την απαγόρευση/άρνηση πρόσβασης σε κάθε ηλεκτρονική συσκευή, υπολογιστή, εξυπηρετητή (server) ή δίκτυο. Το γεγονός αυτό έχει ως αποτέλεσμα ο εν λόγω υπολογιστής να αδυνατεί να ανταποκριθεί σε όλα τα αιτήματα που δέχεται ή να ικανοποιεί μόνο ελάχιστα από αυτά και έτσι να καθίσταται πρακτικά ανενεργός ή μη λειτουργικός. Ο τεράστιος αυτός όγκος αιτημάτων δύναται να παράγεται με την μορφή απλών, εκτελέσιμων αρχείων, από οιονδήποτε υπολογιστή. Το φαινόμενο αυτό παρατηρείται επίσης στις περιπτώσεις απότομης αύξησης της επισκεψιμότητας σε μία συγκεκριμένη ιστοσελίδα, η οποία αδυνατώντας να ικανοποιήσει όλα τα απρόβλεπτα αυξημένα αιτήματα των χρηστών-επισκεπτών, τελικά καθίσταται ανενεργή και μη προσβάσιμη.

Εξίσου διαδεδομένος τύπος κυβερνοεπίθεσης στις περιπτώσεις της Εσθονίας και της Γεωργίας υπήρξε ο τύπος «*DDoS*[183]» (*Κατανεμημένη Άρνηση Υπηρεσίας – Distributed Denial of Service*), για την εκδήλωση της οποίας χρησιμοποιείται ένα δίκτυο πολλαπλών συστημάτων. Μπορεί να οργανωθεί από έναν μόνο προγραμματιστή (hacker), ο οποίος κατευθύνει ένα συντριπτικό αριθμό εντολών ή/και αιτήσεων προς έναν στόχο (υπολογιστή, server, δίκτυο) ή μια ομάδα στόχων. Οι επιθέσεις τύπου *DDoS* δύναται να θέσουν εκτός λειτουργίας ιστότοπους (web sites) και εξυπηρετητές (servers), να στείλουν έναν μαζικό αριθμό μηνυμάτων ηλεκτρονικής (emails) και ανεπιθύμητης (spamming) αλληλογραφίας και να διαδώσουν κακόβουλο λογισμικό (ιούς).

Οι επιθέσεις τύπου *DDoS* χρησιμοποιούν διάφορες μεθόδους για να εκδηλωθούν, με συνηθέστερη τη χρήση μικρών προγραμμάτων (*bots*[184]) τα οποία παράγουν μεγάλο αριθμό αυτοματοποιημένων και επαναλαμβανόμενων εντολών. Τα προγράμματα bots δύναται να είναι κακόβουλα ή μη, αναλόγως του σκοπού για τον οποίο χρησιμοποιούνται. Με τη χρήση των προγραμμάτων αυτών οι hackers

[182] Tikk, E., Kaska, K., & Vihul, L. (2010). INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS. Tallinn Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE). Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/publications/books/legalconsiderations.pdf (σελ. 112)
[183] Ibid.
[184] Ibid. (σελ. 111)

καταφέρνουν να πάρουν τον έλεγχο άλλων υπολογιστών (zombies), τους οποίους εν συνεχεία χρησιμοποιούν προκειμένου να εκδηλώσουν κυβερνοεπιθέσεις προς διαφορετικούς «στόχους», χωρίς να γίνονται αντιληπτοί, ακόμα και από τον κάτοχο του υπολογιστή του οποίου παίρνουν τον έλεγχο. Πρακτικά, αυτό σημαίνει ότι ένας προγραμματιστής με έδρα π.χ. τις Η.Π.Α. μπορεί να πραγματοποιήσει κυβερνοεπίθεση εναντίον μία κρατικής δομής στη Ρωσία, χρησιμοποιώντας υπολογιστή ή ομάδα υπολογιστών ακόμα και μέσα στη Ρωσία, χωρίς να γίνει αντιληπτός. Όταν ένας hacker δημιουργεί ένα δίκτυο υπολογιστών, με το οποίο και σε συνδυασμό με τη χρήση πολλών προγραμμάτων τύπου bot παίρνει ταυτόχρονα τον έλεγχο πολλών χιλιάδων υπολογιστικών μηχανημάτων, τότε το δίκτυο αυτό ονομάζεται *botnet*[185]. Με τη δημιουργία botnet οι hackers επιτυγχάνουν να εκδηλώσουν επιθέσεις τις οποίες δε θα μπορούσαν να τις πραγματοποιήσουν με τη χρήση ενός μόνο υπολογιστή. Κατά συνέπεια, χρησιμοποιούνται συνήθως σε οργανωμένες κυβερνοεπιθέσεις ευρείας κλίμακας και με πολλαπλούς «στόχους».

Μία από τις πιο απλές εντολές, που οι hackers, στις περιπτώσεις της Εσθονίας και της Γεωργίας, έστελναν ομαδοποιημένες σε τεράστιο αριθμό εναντίον ενός υπολογιστή-«στόχου» ή ομάδας «στόχων», προκειμένου να τον/τους καταστήσουν ανενεργούς, είναι η εντολή *ping*[186]. Η εντολή αυτή είναι ένα χρήσιμο δοκιμαστικό εργαλείο σε δίκτυα υπολογιστών, το οποίο στέλνεται από έναν υπολογιστή ενός δικτύου σε έναν άλλο, ώστε να διαπιστωθεί ότι επικοινωνούν μεταξύ τους. Σε περίπτωση επιτυχούς δοκιμής, επιστρέφεται ένα ανάλογο σήμα (ping) από τον υπολογιστή ο οποίος δέχτηκε την εντολή ping. Στην περίπτωση που ένας υπολογιστής λάβει ταυτόχρονα έναν τεράστιο όγκο αιτημάτων/εντολών τύπου ping, γίνεται αντιληπτό ότι καθίσταται ιδιαίτερα δύσκολο να μπορεί να απαντήσει σε όλες αυτές τις εντολές. Στην προσπάθειά του να ανταποκριθεί σε όλα τα αιτήματα αυτού του τύπου, η ταχύτητα απόδοσης αυτού του υπολογιστή γίνεται ιδιαίτερα χαμηλή, μέχρι ο υπολογιστής να καταστεί πρακτικά ανενεργός.

Τον Ιούνιο ή Ιούλιο του 2010, μία εταιρεία από τη Λευκορωσία (VirusBlockAda), ανακάλυψε για πρώτη φορά σε υπολογιστές στο Ιράν, την

[185] Ibid.
[186] Ibid. (σελ. 114)

ύπαρξη ενός ιδιαίτερου κακόβουλου λογισμικού (ιού), ο οποίος ονομάστηκε *Stuxnet*[187]. Η ιδιαιτερότητα του εν λόγω ιού, εστιάζεται στο γεγονός ότι, λόγω της πολύπλοκης κρυπτογράφησής του, δεν μπορούσε να γίνει αντιληπτός από τα προγράμματα αντιμετώπισης κακόβουλων λογισμικών (anti-virus), αναπαράγονταν και διαδίδονταν σε άλλους υπολογιστές ή δίκτυα υπολογιστών από μόνος του και εκδήλωνε αυτόματα κυβερνοεπιθέσεις εναντίον συγκεκριμένων «στόχων», μόλις τους αναγνώριζε. Αυτός ήταν και ο λόγος που χαρακτηρίστηκε ως «κυβερνοπύραυλος» (*Guided Cyber Missile*). Ένα άλλο, εξίσου σημαντικό χαρακτηριστικό του εν λόγω λογισμικού, ήταν ότι ούτε κατά τη διάρκεια της «επίθεσης» μπορούσε να γίνει αντιληπτός, καθόσον τα συστήματα ελέγχου δεν μπορούσαν να τον εντοπίσουν ώστε να εμφανίσουν στις οθόνες των χειριστών μηνύματα σφάλματος. Ο *Stuxnet* φαίνεται να χρησιμοποιήθηκε στις κυβερνοεπιθέσεις που έλαβαν χώρα το 2010 εναντίον πυρηνικών εγκαταστάσεων στο Ιράν. Οι καινοτομίες που παρουσιάζει στην αρχιτεκτονική του τον καθιστούν ένα ιδιαίτερα επικίνδυνο και αποτελεσματικό «κυβερνο-όπλο». Άλλωστε, σε σχετική έκθεση[188] που υπεβλήθη προς το Κογκρέσο των Η.Π.Α. στις αρχές του Δεκεμβρίου του 2010, επισημάνθηκε η επικινδυνότητα του εν λόγω κακόβουλου λογισμικού, κάνοντας λόγο για υφιστάμενη δυνατότητα του Stuxnet να προκαλέσει ανεπανόρθωτες βλάβες σε κρίσιμες υποδομές υψίστης σημασίας των Η.Π.Α..

1.2 Περιπτώσεις κυβερνοεπιθέσεων εναντίον κρατικών δομών.

Για να μπορέσει να γίνει περισσότερη κατανοητή η φύση των κυβερνοεπιθέσεων που στρέφονται εναντίον κρατικών και κυβερνητικών δομών, κρίνεται σκόπιμο να εξεταστούν οι περιπτώσεις κυβερνοεπιθέσεων εναντίον της Εσθονίας (2007) και της Γεωργίας (2008), λαμβάνοντας υπόψη το ευρύτερο γεωπολιτικό πλαίσιο, εντός του οποίου έλαβαν χώρα. Οι κυβερνοεπιθέσεις αυτές

[187] Farwell, J. P., & Rohozinski, R. (n.d.). Stuxnet and the Future of Cyber War. Survival. Ανάκτηση Νοέμβριος 18, 2016, από https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf

[188] Kerr, P. K., Rollins, J., & Theohary, C. A. (2010, Δεκέμβριος). The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. Congressional Research Service. Ανάκτηση Νοέμβριος 18, 2016, από http://digital.library.unt.edu/ark:/67531/metadc31393/m1/1/high_res_d/R41524_2010Dec09.pdf

αποτελούν τα πιο χαρακτηριστικά παραδείγματα μέχρι σήμερα, λόγω του τύπου και της έκτασης των επιθέσεων, της φύσης των επιλεχθέντων «στόχων» και της χρονικής τους διάρκειας. Συμπληρωματικά θα γίνει συνοπτική αναφορά και σε άλλες ενδεικτικές περιπτώσεις κυβερνοεπιθέσεων κατά κρατικών δομών, μικρότερης εμβέλειας[189].

1.2.1 Εσθονία (2007)

Στις 26 και 27 Απριλίου 2007, στο κέντρο της πρωτεύουσας της Εσθονίας (Τάλλιν) , έλαβαν χώρα εκτεταμένα επεισόδια από νεαρές εθνικιστικές ομάδες ρωσικής, κυρίως, καταγωγής (περίπου 1000 άτομα). Τα επεισόδια ήταν το αποτέλεσμα της αντίδρασης κατά της απόφασης της εσθονικής κυβέρνησης να μετακινήσει το χάλκινο άγαλμα ενός στρατιώτη το οποίο είχε τοποθετηθεί μετά το πέρας του Δευτέρου Παγκοσμίου Πολέμου (το 1947), σε κεντρικό σημείο της πόλης, σε ανάμνηση της νίκης του Σοβιετικού Στρατού κατά των ναζιστικών δυνάμεων. Αντιδράσεις υπήρξαν και από τη ρωσική κυβέρνηση, οι οποίες συνοδεύτηκαν από μία σειρά προπαγανδιστικών άρθρων, τόσο εντός όσο και εκτός της ρωσικής επικράτειας. Θα πρέπει να σημειωθεί ότι η εσθονική κυβέρνηση δικαιολόγησε την απόφασή της, προκειμένου να μετακινήσει τα οστά σοβιετικών στρατιωτών που είχαν χάσει τη ζωή τους στις μάχες για την απελευθέρωση της Εσθονίας και τα οποία φυλάσσονταν κάτω από το άγαλμα. Τελικά το άγαλμα μετακινήθηκε τη νύχτα της 27ης Απριλίου 2007 σε απροσδιόριστη τοποθεσία και τρεις μέρες αργότερα τοποθετήθηκε στο στρατιωτικό νεκροταφείο του Τάλλιν.

Η μετακίνηση του αγάλματος προκάλεσε έντονες διαμαρτυρίες έξω από την εσθονική πρεσβεία στη Μόσχα, οι οποίες κατέληξαν σε εκδήλωση φυσικής επίθεσης κατά των Εσθονών πρέσβεων, σε συνέντευξη τύπου. Ωστόσο, οι αντιδράσεις συνεχίστηκαν από το ίδιο, κιόλας, βράδυ στον κυβερνοχώρο και μάλιστα σε πρωτοφανή έκταση και βαθμό μέχρι εκείνη την εποχή[190].

[189] NATO Review Magazine. Ανάκτηση Νοέμβριος 18, 2016, από Official NATO website: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[190] Tikk, E., Kaska, K., & Vihul, L. (2010). INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS. Tallinn Estonia: Cooperative Cyber Defence Centre of Excellence (CCD

Οι κυβερνοεπιθέσεις που ακολούθησαν εκδηλώθηκαν σε δύο φάσεις, συνολικής διάρκειας τριών εβδομάδων. Η π ρ ώ τ η φ ά σ η διήρκησε τρεις μέρες (27-29 Απριλίου 2007) και στράφηκε εναντίον κυβερνητικών ιστοσελίδων και μέσων ενημέρωσης, κάθε φορά που αυτά μετέδιδαν ειδήσεις σχετικά με τις διαδηλώσεις διαμαρτυρίας και την πολιτική κατάσταση στη χώρα. Η εν λόγω φάση των κυβερνοεπιθέσεων, που επονομάστηκε *emotional response* ή *cyber riots,* εκδηλώθηκε με τον τύπο *Άρνησης της Υπηρεσίας* («Denial of Service - DoS»). Για τον σκοπό αυτό, αξίζει να επισημανθεί ότι σε διάφορα διαδικτυακά φόρουμ, ιδιαίτερα σε ρωσόφωνα, υπήρχαν συγκεκριμένες οδηγίες που προέτρεπαν και καθοδηγούσαν τους επισκέπτες να στείλουν συντονισμένα έναν μεγάλο όγκο ομαδοποιημένων εντολών.

Η δ ε ύ τ ε ρ η φ ά σ η αποτέλεσε και την κύρια φάση της κυβερνοεπίθεσης εναντίον της Εσθονίας. Εξελίχθηκε σε τέσσερα κύματα, από 30 Απριλίου έως 18 Μαΐου 2007, ήταν ευρύτερη, περισσότερο συντονισμένη και χρησιμοποιήθηκαν, όπως και στην πρώτη φάση, διαδικτυακά φόρουμ για την παροχή απλοποιημένων οδηγιών. Στο π ρ ώ τ ο κ ύ μ α (4 Μαΐου 2007) εκδηλώθηκαν πολλές και συντονισμένες επιθέσεις μέσω διαμεσολαβητών (*proxies servers*) αλλά και ομαδοποιημένου ελέγχου μεγάλου αριθμού υπολογιστών (global botnets) από ολόκληρο τον κόσμο. Στο δ ε ύ τ ε ρ ο κ ύ μ α (9-11 Μαΐου 2007), οι κυβερνοεπιθέσεις που εκδηλώθηκαν (κυρίως τύπου *Κατανεμημένης Άρνησης* Υπηρεσίας / Distributed Denial of Service - DDoS), παρουσίασαν στην έναρξή τους απότομη αύξηση κατά 150%, κατάφεραν να θέσουν ταυτόχρονα εκτός λειτουργίας, για το προαναφερόμενο χρονικό διάστημα 58 ιστοσελίδες, κυρίως επίσημες κυβερνητικές αλλά και τραπεζικές (συμπεριλαμβανομένης της κεντρικής εθνικής τράπεζας της χώρας) και έληξαν επίσης απότομα. Η ανωτέρω αύξηση των κυβερνοεπιθέσεων στις 9 Μαΐου 2007 ήταν αναμενόμενη, καθόσον η συγκεκριμένη ημέρα αποτελεί εθνική εορτή για τη Ρωσία, κατά των Ναζί. Το τ ρ ί τ ο κ ύ μ α (15 Μαΐου 2007) χαρακτηρίστηκε από μία ευρείας κλίμακας κυβερνοεπίθεση τύπου *DDoS*, για τις ανάγκες της οποίας χρησιμοποιήθηκαν *εν αγνοία των κατόχων (hacking)* περί τους 85.000 υπολογιστές, στοχοποιώντας και στην περίπτωση αυτή κυβερνητικές ιστοσελίδες, αλλά και τη δεύτερη μεγαλύτερη

COE). Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/publications/books/legalconsiderations.pdf (σελ. 14-35)

εμπορική τράπεζα στη χώρα. Στο τέταρτο και τελευταίο κύμα (18 Μαΐου 2007) εκδηλώθηκαν κυβερνοεπιθέσεις ίδιου τύπου, προέλευσης και προορισμού με το προηγούμενο κύμα.

Σε γενικές γραμμές, κατά την περίοδο της κορύφωσης των κυβερνοεπιθέσεων στην Εσθονία, διαπιστώθηκε κατακόρυφη αύξηση της διακίνησης δεδομένων και πληροφοριών στο διαδίκτυο, η οποία εκτιμήθηκε 400 φορές μεγαλύτερη από τη συνηθισμένη. Συνολικά καταγράφηκαν 128 επιθέσεις τύπου DDoS εναντίον κυβερνητικών ιστοσελίδων και διαδικτυακών τοποθεσιών δημόσιου χαρακτήρα, ενώ τέθηκε εκτός λειτουργίας ακόμα και η γραμμή έκτακτης ανάγκης (112). Πέραν των επιθέσεων τύπου *DDoS*, απεστάλη προς πάσα κατεύθυνση, εντός της χώρας, υπερμεγέθης όγκος ανεπιθύμητης αλληλογραφίας, θέτοντας εκτός λειτουργίας το ηλεκτρονικό ταχυδρομείο. Οι κυβερνητικές ιστοσελίδες που δέχτηκαν επιθέσεις ήταν αυτές της κυβέρνησης, του προέδρου της χώρας, του πρωθυπουργού, του κοινοβουλίου, όλων των υπουργείων (εκτός από αυτό του Πολιτισμού), των Σωμάτων Ασφαλείας αλλά και αυτή της αξιωματικής αντιπολίτευσης. Επίσης, σύμφωνα με το Εθνικό Κέντρο Πληροφορικής («State Informatics Centre»), οι υπολογιστές οι οποίοι συμμετείχαν καθ' οιονδήποτε τρόπο στις κυβερνοεπιθέσεις εναντίον της Εσθονίας εντοπίστηκαν κατά βάση εκτός της εδαφικής επικράτειας της χώρας και μάλιστα προερχόμενοι από 178 χώρες.

Το γεγονός που ενισχύει σε σημαντικό βαθμό τη σημασία και την απήχηση των κυβερνοεπιθέσεων στην Εσθονία, είναι η ιδιαίτερα αυξημένη εξάρτηση της εν λόγω χώρας με την ηλεκτρονική διακυβέρνηση και το διαδίκτυο γενικότερα. Αρκεί να επισημανθεί ότι ήδη από το 2007 το 95% των τραπεζικών συναλλαγών εκτελούνταν διαδικτυακά, ενώ στο 98% της εδαφικής επικράτειας της χώρας, ήταν δυνατή η με οποιονδήποτε τρόπο πρόσβαση στο ίντερνετ.

Στον απόηχο των επιθέσεων, αρκετοί πολιτικοί στην Εσθονία προσπάθησαν να παραλληλίσουν τις διεξαχθείσες κυβερνοεπιθέσεις με συμβατικές, στρατιωτικές δραστηριότητες. Ανεπιτυχής ήταν και η προσπάθεια επίκλησης του Άρθρου 5 της Ιδρυτικής Συνθήκης του ΝΑΤΟ περί συλλογικής ασφάλειας. Εν τέλει κατηγορήθηκαν και καταδικάστηκαν (με χρηματική αποζημίωση) συνολικά ένας 19χρονος Εσθονός πολίτης ρωσικής καταγωγής και ένας φοιτητής στο Τεχνολογικό Πανεπιστήμιο στο Τάλλιν.

1.2.2 Γεωργία (2008)

Οι κυβερνοεπιθέσεις εναντίον της Γεωργίας[191] εκδηλώθηκαν χρονικά μαζί με την έναρξη των στρατιωτικών επιχειρήσεων των ρωσικών δυνάμεων στο έδαφος της Γεωργίας (8 Αυγούστου 2008) και διήρκησαν τρεις εβδομάδες (8-28 Αυγούστου 2008). Οι εν λόγω επιθέσεις, όπως και στην περίπτωση της Εσθονίας, στράφηκαν κυρίως εναντίον κυβερνητικών (Πρόεδρος χώρας, κυβέρνηση, υπουργείο εξωτερικών, υπουργείο άμυνας και Κοινοβούλιο) και τραπεζικών (εθνική τράπεζα, η οποία αναγκάστηκε να θέσει εκτός λειτουργίας όλες τις διαδικτυακές συναλλαγές για δέκα ημέρες) ιστοσελίδων, καθώς επίσης και εναντίον ιστοσελίδων μέσων ενημέρωσης. Οι τύποι των κυβερνοεπιθέσεων συμπίπτουν με αυτούς που εξετάστηκαν στην περίπτωση της Εσθονίας, ενώ χρησιμοποιήθηκαν και στην περίπτωση αυτή διαδικτυακά ιστολόγια (κυρίως ρωσόφωνα) για την παροχή οδηγιών και των απαραίτητων *μολυσμένων* αρχείων εφαρμογής. Η κύρια φάση των κυβερνοεπιθέσεων διήρκησε έξι ημέρες (8-13 Αυγούστου 2008), αλλά συνεχίστηκαν έως το τέλος του ίδιου μήνα, ενώ στις 27 Αυγούστου 2008 σημειώθηκε νέα, κατακόρυφη αύξηση των επιθέσεων αυτών. Για την αμεσότερη επανενεργοποίηση των βασικών κυβερνητικών ιστοσελίδων αλλά και ιστοσελίδων μέσων ενημέρωσης, η επίσημη ιστοσελίδα της γεωργιανής κυβέρνησης και ενός διακεκριμένου τηλεοπτικού σταθμού μεταφέρθηκαν στους *εξυπηρετητές* (*servers*) μίας εταιρείας ενός Γεωργιανού υπηκόου στην Ατλάντα, ενώ οι επίσημες ιστοσελίδες των υπουργείων εξωτερικών και κυβερνητικού εκπροσώπου τύπου «φιλοξενήθηκαν» στους ιστότοπους της Εσθονικής κυβέρνησης και του Προέδρου της Πολωνίας αντίστοιχα. Κάθε μία κυβερνοεπίθεση διαρκούσε συνεχόμενα κατά μέσο όρο δύο ώρες και δεκαπέντε λεπτά, ενώ η μεγαλύτερη σε διάρκεια έφτασε και τις έξι ώρες. Την τέταρτη ημέρα των κυβερνοεπιθέσεων (11 Αυγούστου 2008) το γεωργιανό υπουργείο εξωτερικών εξέδωσε ανακοίνωση τύπου με την οποία κατηγορούσε ευθέως τη ρωσική κυβέρνηση, το οποίο και εξ' αρχής αρνήθηκε η ρωσική πλευρά.

Οι κυβερνοεπιθέσεις στη Γεωργία διέφεραν από αυτές στην Εσθονία σε δύο βασικά σημεία. Στην πρώτη περίπτωση υπήρξε ένας γενικός συντονισμός ενεργειών από την αρχή έως τη λήξη των επιθέσεων (στην περίπτωση της Εσθονίας ο συντονισμός ενεργειών χαρακτήρισε μόνο τη δεύτερη και κύρια φάση

[191] Ibid. (σελ. 66-90)

των επιθέσεων), ενώ εκδηλώθηκαν παράλληλα με τις *ένοπλες επιθέσεις* εναντίον της εδαφικής επικράτειας (της Γεωργίας από τα ρωσικά στρατεύματα). Ενώ η εκδήλωση των ένοπλων επιθέσεων αρκεί για να ενεργοποιήσει το Δίκαιο των Ενόπλων Συρράξεων, οι κυβερνοεπιθέσεις, ακόμα και όταν εκδηλώνονται παράλληλα με αυτές, δεν είναι απαραίτητο ότι συνδέονται, καθ' οιονδήποτε τρόπο με τις ένοπλες επιχειρήσεις. Στο συμπέρασμα αυτό συντείνει και το γεγονός ότι οι περισσότερες χώρες δε διαθέτουν εξειδικευμένη *δύναμη κυβερνοχώρου* (cyber force) στη στρατιωτική τους δομή διοίκησης και δυνάμεων, τέτοια που να μπορεί να δικαιολογεί κάποιου είδους διασύνδεση[192].

Τέλος, αξίζει να επισημανθούν τρεις σημαντικές παρατηρήσεις. Πρώτον, ότι η Γεωργία, σε αντίθεση με την Εσθονία, κατά την περίοδο των κυβερνοεπιθέσεων, ήταν μία χώρα με χαμηλό πληθυσμιακά δείκτη χρήσης διαδικτυακών υπηρεσιών (μόλις το 7% του πληθυσμού), ο οποίος, όμως, αυξανόταν με ταχείς ρυθμούς. Δεύτερον, οι πάροχοι διαδικτύου στη Γεωργία χρησιμοποιούσαν, ως επί το πλείστον και αναγκαστικά λόγω υφιστάμενης γειτνίασης, ενσύρματα δίκτυα από τη Ρωσία[193], γεγονός το οποίο καθιστούσε τη Γεωργία ιδιαίτερα εξαρτώμενη από τη Ρωσία στο πεδίο της χρήσης των πληροφορικών και επικοινωνιακών συστημάτων διαδικτύου. Τρίτον, οι κυβερνοεπιθέσεις στη Γεωργία δεν προκάλεσαν κάποιου είδους μόνιμης βλάβης στα υπολογιστικά συστήματα που δέχτηκαν τις επιθέσεις αυτές.

1.2.3 Λοιπές περιπτώσεις

Τον Ιούνιο του 2007 ο επίσημος λογαριασμός του υπουργείου άμυνας των Η.Π.Α. δέχτηκε «επίθεση» (hacked) από άγνωστο ξένο «εισβολέα». Η επίθεση αυτή αποτέλεσε μέρος μίας σειράς επιθέσεων που αποσκοπούσαν να αποκτήσουν πρόσβαση και να εκμεταλλευτούν τα δίκτυα του αμερικανικού πενταγώνου.

Τον Οκτώβριο του 2007 το Υπουργείο Εσωτερικής Ασφαλείας της Λαϊκής Δημοκρατίας της Κίνας ανακοίνωσε ότι ξένοι «εισβολείς» (foreign hackers)

[192] Ibid. (σελ. 80-81)
[193] Ibid. (σελ. 89)

υπέκλεψαν πληροφοριακό υλικό από κρίσιμες κρατικές δομές. Σύμφωνα με την ενημέρωση του εν λόγω υπουργείου, οι «εισβολείς» προέρχονταν κατά 42% από το Ταιβάν και κατά 25% από τις Η.Π.Α.. Ένα χρόνο νωρίτερα, από έρευνα που διεξήχθη στο εσωτερικό δίκτυο υπολογιστών της Αεροδιαστημικής, Επιστημονικής και Βιομηχανικής Εταιρείας της χώρας [China Aerospace Science & Industry Corporation (CASIC)], διαπιστώθηκε ότι στους υπολογιστές των διαβαθμισμένων τμημάτων και της ηγεσίας της εταιρείας υπήρχε προ-εγκατεστημένο λογισμικό υποκλοπής πληροφοριακού υλικού (*spyware*).

Το καλοκαίρι του 2008 υπεκλάπησαν οι βάσεις δεδομένων των εκστρατειών για τις προεδρικές εκλογές των Η.Π.Α., τόσο του Δημοκρατικού, όσο και του Ρεπουμπλικανικού κόμματος από άγνωστους ξένους «εισβολείς».

Τον Ιανουάριο του 2009 οι ισραηλινές υποδομές παροχής υπηρεσιών διαδικτύου δέχτηκαν επίθεση από άγνωστους «εισβολείς», κατά την ίδια χρονική περίοδο με τις στρατιωτικές επιχειρήσεις στη Λωρίδα της Γάζας. Οι κυβερνοεπιθέσεις εστίασαν σε κυβερνητικές ιστοσελίδες και εκτελέστηκαν με τη χρήση τουλάχιστον 5 εκατομμύρια υπολογιστών. Οι επίσημες αρχές του Ισραήλ θεώρησαν ότι οι επιθέσεις αυτές εκδηλώθηκαν από μία εγκληματική οργάνωση με έδρα ένα κράτος της πρώην Σοβιετικής Ένωσης και χρηματοδοτήθηκαν από τη Χαμάς ή τη Χεζμπολάχ.

Τον Ιανουάριο του 2010 μία ομάδα με την επωνυμία *Ιρανικός Κυβερνοστρατός* («Iranian Cyber Army») «επιτέθηκε» εναντίον της πιο δημοφιλούς μηχανής αναζήτησης στην Κίνα (*Baidu*)[194], η οποία ελέγχεται από κρατικές δομές. Κάθε φορά που οι χρήστες χρησιμοποιούσαν την εν λόγω μηχανή αναζήτησης, ανακατευθύνονταν σε μία συγκεκριμένη ιστοσελίδα με σχετικό πολιτικό μήνυμα από την εν λόγω ομάδα. Η συγκεκριμένη κυβερνοεπίθεση διήρκησε για περίπου τέσσερις ώρες. Η ίδια ομάδα, τον Δεκέμβριο του προηγούμενου έτους (2009), «επιτέθηκε» εναντίον της σελίδας κοινωνικής δικτύωσης *Twitter*, με την προβολή παρόμοιου μηνύματος για χρονικό διάστημα περίπου μίας ώρας.

[194] Beaumont, C. (2010, Ιανουάριος 12). Baidu hacked by Iranian Cyber Army. Ανάκτηση Νοέμβριος 18, 2016, από The Telegraph: http://www.telegraph.co.uk/technology/news/6974129/Baidu-hacked-by-Iranian-Cyber-Army.html

Τον Οκτώβριο του 2010 μία νέα μορφή κυβερνοεπίθεσης έκανε την εμφάνισή της με την ονομασία *Stuxnet*. Το κακόβουλο αυτό λογισμικό σχεδιάστηκε να επεμβαίνει σε βιομηχανικά συστήματα ελέγχου της εταιρείας *Siemens*[195] και εντοπίστηκε σε διάφορες χώρες, όπως Ιράν, Ινδονησία, Κίνα, Αζερμπαϊτζάν, Νότια Κορέα, Μαλαισία, Η.Π.Α., Ηνωμένο Βασίλειο, Αυστραλία, Φινλανδία και Γερμανία[196], μολύνοντας περισσότερους από 30 χιλιάδες υπολογιστές στο Ιράν και 60 χιλιάδες υπολογιστές παγκοσμίως. Σύμφωνα[197], μάλιστα, με σχετική έκθεση της εταιρείας για την ασφάλεια έναντι κακόβουλου λογισμικού *Symantec*, η αρχική μόλυνση από τον *Stuxnet* έλαβε χώρα στο Ιράν το 2009 και στη συνέχεια επεκτάθηκε στις υπόλοιπες χώρες. Η συγκεκριμένη επίθεση εκτιμήθηκε ότι επρόκειτο για μία κυβερνητική κυβερνοεπίθεση που στόχευε εγκαταστάσεις πυρηνικού προγράμματος του Ιράν. Αν και ακόμα και σήμερα διίστανται οι απόψεις ως προς τους ακριβείς στόχους του *Stuxnet*, οι περισσότερες από αυτές εστιάζονται σε δύο συγκεκριμένες πυρηνικές εγκαταστάσεις στο Ιράν (Natanz ή Bushehr[198]). Η άποψη αυτή ενισχύεται από το γεγονός ότι ο έλεγχος λειτουργίας των συγκεκριμένων εγκαταστάσεων πραγματοποιούνταν από ψηφιακά συστήματα, με τη χρήση συγκεκριμένου λογισμικού της εταιρείας *Siemens*[199], γεγονός που καθιστούσε ακόμα ευκολότερη και μεγαλύτερη την επίδραση του *Stuxnet* στα εν λόγω συστήματα. Η προσβολή των υπολογιστικών δικτύων των πυρηνικών εγκαταστάσεων του Ιράν επιβεβαιώθηκε τόσο από επίσημους αξιωματούχους της χώρας όσο και από τον ίδιο τον Πρόεδρο Αχμαντινεντζάντ, ο

[195]Shakarian, P. (2011, Απρίλιος). Stuxnet: Cyberwar Revolution in Military Affairs. Ανάκτηση Νοέμβριος 18, 2016, από Small Wars Journal: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s_eng.pdf

[196] Farwell, J. P., & Rohozinski, R. (n.d.). Stuxnet and the Future of Cyber War. Survival. Ανάκτηση Νοέμβριος 18, 2016, από https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf (σελ. 23-40)

[197][197] Broad, W. J., Markoff, J., & Sanger, D. E. (2011, Ιανουάριος 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Ανάκτηση Νοέμβριος 18, 2016, από New York Times: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

[198] Clemente, D. (2010, Σεπτέμβριος 27). Reality Approaches Hype: Critical National Infrastructure and the Stuxnet Worm. Ανάκτηση Νοέμβριος 18, 2016, από CHATHAM HOUSE The Royal Institute of International Affairs : https://www.chathamhouse.org/media/comment/view/163865#

[199] Shakarian, P. (2011, Απρίλιος). Stuxnet: Cyberwar Revolution in Military Affairs. Ανάκτηση Νοέμβριος 18, 2016, από Small Wars Journal: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s_eng.pdf

οποίος, ωστόσο, επισήμανε ότι οι εν λόγω κυβερνοεπιθέσεις δεν προξένησαν σημαντικές ή ανεπανόρθωτες βλάβες[200].

Τον Ιανουάριο του 2011 η κυβέρνηση του Καναδά ανακοίνωσε ότι δέχτηκε μία ευρείας κλίμακα κυβερνοεπίθεση εναντίον κρατικών υπηρεσιών και συμπεριλαμβανομένου του Τμήματος Αμυντικών Ερευνών το οποίο υπάγεται στο καναδικό υπουργείο άμυνας. Η επίθεση αυτή ανάγκασε την κυβέρνηση του Καναδά να αποσυνδέσει από το διαδίκτυο τις κυριότερες οικονομικές του υπηρεσίες (*Finance Department* και *Treasury Board*).

Σε ομιλία του αναπληρωτή υπουργού άμυνας των Η.Π.Α. τον Ιούλιο του 2011, σύμφωνα με το Τμήμα Στρατηγικής Κυβερνοάμυνας της χώρας, αποκαλύφθηκε ότι μία από τις συνεργαζόμενες αμυντικές βιομηχανίες δέχτηκε κυβερνοεπίθεση με αποτέλεσμα να υποκλαπούν 24 χιλιάδες αρχεία από το υπουργείο άμυνας των Η.Π.Α..

Τον Οκτώβριο του 2012, η ρωσική εταιρεία για την ασφάλεια έναντι κακόβουλου λογισμικού *Kaspersky,* αποκάλυψε ότι μία παγκόσμιας κλίμακας κυβερνοεπίθεση με την ονομασία *Κόκκινος Οκτώβριος* ήταν ήδη σε εξέλιξη και μάλιστα τουλάχιστον από το 2007. Οι επίδοξοι προγραμματιστές *hackers* συγκέντρωσαν τις απαραίτητες πληροφορίες, μέσω των τρωτών σημείων συγκεκριμένων προγραμμάτων της *Microsoft* (Word και Excel). Οι πρωταρχικοί στόχοι των εν λόγω κυβερνοεπιθέσεων φαίνεται να ήταν χώρες της Ανατολικής Ευρώπης, της πρώην Σοβιετικής Ένωσης και της Κεντρικής Ασίας, παρόλο που «θύματα» των επιθέσεων αναφέρθηκαν και στη Δυτική Ευρώπη και τη Βόρεια Αμερική. Ο υπόψη «ιός» συγκέντρωσε διάφορες πληροφορίες από πρεσβείες χωρών, εταιρείες ερευνών, στρατιωτικές εγκαταστάσεις, εταιρείες παροχής ενέργειας, πυρηνικές και άλλες υποδομές υψίστης σημασίας.

Τον Μάρτιο του 2013 τα υπολογιστικά δίκτυα χρηματοπιστωτικών ιδρυμάτων της Νότιας Κορέας και του κορεατικού τηλεοπτικού δικτύου YTN μολύνθηκαν στο πλαίσιο κυβερνοεπίθεσης η οποία θύμιζε παλιότερες συναφείς προσπάθειες από πλευράς της Βόρειας Κορέας.

[200] Albright, D., Brannan, P., & Walrond, C. (2010, Δεκέμβριος 22). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. Ανάκτηση Νοέμβριος 18, 2016, από Institute for Science and International Security: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (σελ. 1)

Τέλος, στις 8 Νοεμβρίου 2016[201] μία ευρεία σειρά κυβερνοεπιθέσεων τύπου *Κατανεμημένης Άρνησης Υπηρεσίας* (DDoS) εκδηλώθηκε για περίπου ένα 24ωρο στην ιστοσελίδα του διεθνούς μη κερδοσκοπικού οργανισμού μέσων ενημέρωσης *Wikileaks[202],* σύμφωνα με σχετική ενημέρωση από την ίδια την ιστοσελίδα. Συγκεκριμένα, όσοι χρήστες επιχειρούσαν να αποκτήσουν πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου του *John Podesta*, προέδρου της εκστρατείας της υποψηφίου *Hillary Clinton*, ελάμβαναν επανειλημμένα μηνύματα λάθους.

[201] ZILBER, A. (2016, Νοέμβριος 8). WikiLeaks comes under 'unrelenting' cyber attack that briefly prevents it from releasing more emails linked to Hillary Clinton on Election Day. Ανάκτηση Νοέμβριος 18, 2016, από DAILYMAIL.COM and ASSOCIATED PRESS: http://www.dailymail.co.uk/news/article-3917996/WikiLeaks-comes-unrelenting-cyber-attacks-briefly-prevented-releasing-emails-linked-Hillary-Clinton-Americans-polls-Election-Day.html

[202] Η Wikileaks είχε δημοσιεύσει δεκάδες χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου και έγγραφα, προερχόμενα από υποκλοπές (hacking), από τον εσωτερικό κύκλο της υποψηφίου του Δημοκρατικού Κόμματος *Hillary Clinton* για τις προεδρικές εκλογές των Η.Π.Α. του Νοεμβρίου 2016.

ΚΕΦΑΛΑΙΟ 2
Θεσμική οργάνωση κρατών και Διεθνών Οργανισμών στον Κυβερνοχώρο

Για την απόκτηση μίας ευρύτερης όσο και πλήρους εικόνας, αναφορικά με το καταλληλότερο θεσμικό πλαίσιο κανόνων δικαίου στο πεδίο του κυβερνοχώρου, κρίνεται σκόπιμο να εξεταστεί η θεσμική οργάνωση και ειδικότερα οι αντιλήψεις σημαντικών κρατικών δρώντων και διεθνών οργανισμών, όπως αυτές αποτυπώνονται σε σχετικές πολιτικές και στρατηγικές ασφαλείας. Ο τρόπος με τον οποίο αντιλαμβάνονται τα κράτη την εφαρμογή του Διεθνούς Δικαίου στον κυβερνοχώρο, τόσο σε εθνικό όσο και σε πολυεθνικό επίπεδο, δύναται να συμβάλλει σημαντικά στην εξαγωγή χρήσιμων συμπερασμάτων.

2.1 Στρατηγικές Κυβερνοάμυνας/Κυβερνοασφάλειας κρατών

2.1.1 Η.Π.Α.

Η πρώτη εθνική στρατηγική για την Κυβερνοασφάλεια εκδόθηκε το 2003 με τίτλο *The National Strategy to Secure Cyberspace*[203]. Η εν λόγω στρατηγική προσδιόριζε τρεις βασικούς αντικειμενικούς σκοπούς, ήτοι η λήψη μέτρων πρόληψης από κυβερνοαπειλές κατά υποδομών στο πεδίο του κυβερνοχώρου, η μείωση τυχόν τρωτών σημείων και η ελάττωση του χρόνου επαναφοράς των συστημάτων μετά από κυβερνοεπίθεση.

Η πρώτη, πάντως, εθνική στρατηγική στις Η.Π.Α. που έδωσε ιδιαίτερη σημασία στην αποτελεσματική αντιμετώπιση των κυβερνοαπειλών εκπονήθηκε το 2010 («2010 National Security Strategy[204]»), εστιάζοντας σε αυτές που προέρχονται από μη κρατικούς δρώντες. Η ισχύουσα Εθνική Στρατηγική

[203] (2003, Φεβρουάριος). The National Strategy to Secure Cyberspace. Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[204] (2010, Μάιος). National Security Strategy. Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Ασφαλείας, η οποία υιοθετήθηκε το 2015[205], αναγνωρίζει τον διαρκώς αυξανόμενο κίνδυνο των κυβερνοαπειλών και τις αποδιοργανωτικές έως και καταστροφικές συνέπειες των κυβερνοεπιθέσεων, υπογραμμίζοντας την ανάγκη για περαιτέρω ενίσχυση της κυβερνοασφάλειας των κρίσιμων υποδομών.

Σε ότι αφορά την αλληλεπίδραση των Η.Π.Α. με άλλους διεθνείς δρώντες στο πεδίο του Κυβερνοχώρου, εκπονήθηκε από τον Λευκό Οίκο το 2011 η *Διεθνής Στρατηγική για τον Κυβερνοχώρο*[206] («International Strategy for Cyberspace»), η οποία αποτύπωνε τις εθνικές απόψεις για ανάπτυξη σχέσεων με διεθνείς εταίρους και προώθηση των εθνικών προτεραιοτήτων. Στην εν λόγω στρατηγική γίνεται σαφές ότι η χώρα θα απαντήσει σε τυχόν εχθρικές ενέργειες στον Κυβερνοχώρο, όπως θα το έπραττε και έναντι οποιασδήποτε άλλης απειλής. Παράλληλα, τονίζεται ότι εφόσον απαιτηθεί θα χρησιμοποιηθούν όλα τα διατιθέμενα μέσα, διπλωματικά, πληροφοριακά, στρατιωτικά ή οικονομικά, σύμφωνα με το Διεθνές Δίκαιο, για την αποτελεσματικότερη άμυνα της χώρας, των συμμάχων τους, των εταίρων τους και των εθνικών συμφερόντων.

Συνοπτικά, η Διεύθυνση Εσωτερικής Ασφάλειας («Department of Homeland Security - DHS») είναι υπεύθυνη για την προστασία των κρίσιμων, κυβερνητικών, επικοινωνιακών και πληροφοριακών συστημάτων έναντι κυβερνοεπιθέσεων. Εάν η κυβερνοεπίθεση στρέφεται εναντίον στρατιωτικών υποδομών ή αμυντικών βιομηχανιών που υποστηρίζουν εθνικές στρατιωτικές επιχειρήσεις, τότε τον κεντρικό έλεγχο αναλαμβάνει το υπουργείο άμυνας («Department of Defence - DoD»).

Σε περίπτωση εθνικά σημαντικών περιστατικών[207] στο πεδίο του Κυβερνοχώρου, την ευθύνη για τον γενικό συντονισμό της προετοιμασίας, ανταπόκρισης, επαναφοράς των συστημάτων και επιχειρησιακής πληροφόρησης,

[205] (2015, Φεβρουάριος). National Security Strategy. Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

[206] (2011, Μάιος). International Strategy for Cyberspace. Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[207] (2016). National Cyber Security Organisation: UNITED STATES. Τάλλιν: Κέντρο Αριστείας Κυβερνοάμυνας. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (σελ.22)

αναλαμβάνει η *Συντονιστική Ομάδα Αντίδρασης για τον Κυβερνοχώρο* («National Cyber Response Coordination Group - NCRCG»), η οποία συγκροτείται από εκπροσώπους 19 ομοσπονδιακών διευθύνσεων και υπηρεσιών.

2.1.2 Ηνωμένο Βασίλειο

Η πρώτη εθνική στρατηγική για την Κυβερνοασφάλεια υιοθετήθηκε το 2009, εστιάζοντας στην ασφάλεια και την ανθεκτικότητα (resilience) στον κυβερνοχώρο (*Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*[208]). Το 2010, το Εθνικό Συμβούλιο Ασφαλείας, κατηγοριοποίησε τις κυβερνοεπιθέσεις από άλλα κράτη και τα κυβερνοεγκλήματα ευρείας κλίμακας ως εκ των υψηλότερων εθνικών κινδύνων ασφαλείας, λαμβάνοντας υπόψη την αυξημένη πιθανότητα και τις επιπτώσεις από ενδεχόμενη τέτοια επίθεση. Η εν λόγω κατηγοριοποίηση τοποθετεί την κυβερνοαπειλή στα υψηλότερα επίπεδα μαζί με την απειλή πυρηνικής επίθεσης, τους κινδύνους από διεθνή τρομοκρατία, μεγάλα ατυχήματα ή φυσικές καταστροφές και τις διεθνείς στρατιωτικές κρίσεις[209]. Επίσης τονίζει την συνεχώς αυξανόμενη επιρροή των κυβερνοαπειλών στην καθημερινότητα της βρετανικής κυβέρνησης, όσο η πρόσβαση στο διαδίκτυο αποτελεί ολοένα και περισσότερο «δικαίωμα παρά προνόμιο»[210].

Η εθνική στρατηγική για την κυβερνοασφάλεια αναθεωρήθηκε το 2011[211], το 2013[212], ενώ η ισχύουσα εκπονήθηκε το 2016[213]. Είναι χαρακτηριστικό ότι η

[208] (2009, Ιούνιος). Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space. Λονδίνο: UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από http://ccpic.mai.gov.ro/docs/UK_cyber_security.pdf

[209] (2010, Οκτώβριος). A Strong Britain in an Age of Uncertainty: The National Security Strategy. David Cameron, Great Britain and Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (σελ. 27)

[210] Ibid. (σελ. 29, παρ. 3.28)

[211] (2011, Νοέμβριος). The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world. UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[212] (2013, Δεκέμβριος). The National Cyber Security Strategy Our Forward Plans. UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από http://www.cyberriskinsuranceforum.com/sites/default/files/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

στρατηγική του 2011 επιβάρυνε τον κρατικό προϋπολογισμό κατά 860 εκατομμύρια λίρες, γεγονός που αποδεικνύει τη σημασία που αποδίδει το Ηνωμένο Βασίλειο στην Κυβερνοάμυνα.

Η τελευταία στρατηγική (2016) εστιάζει σε τρεις βασικούς αντικειμενικούς σκοπούς: *Άμυνα-Αποτροπή-Ανάπτυξη* («Defend-Deter_Develop»). Επίσης, η στρατηγική του 2016 επισημαίνει τις σπάνιες αλλά διαρκώς αυξανόμενες περιπτώσεις κυβερνοεπιθέσεων από άλλα κράτη ή κρατικούς φορείς, κατά κυβερνητικών, αμυντικών, οικονομικών, ενεργειακών και τηλεπικοινωνιακών υποδομών του Ηνωμένου Βασιλείου. Προσδιορίζει, μάλιστα, το εύρος των εν λόγω κυβερνοαπειλών/κυβερνοεπιθέσεων από περιπτώσεις *κυβερνοκατασκοπείας* έως και την ανάπτυξη εχθρικών και «καταστροφικών» δυνατοτήτων στο πεδίο του κυβερνοχώρου, εναντίον βρετανικών υποδομών, κατά παράβαση κανόνων του Διεθνούς Δικαίου[214]. Συναφώς τονίζεται ότι η περίπτωση κυβερνοεπίθεσης εναντίον του Ηνωμένου Βασιλείου θα αντιμετωπιστεί με την ίδια σοβαρότητα και στον ίδιο βαθμό που θα αντιμετωπιζόταν μία συμβατική επίθεση, ενεργώντας σύμφωνα με το εσωτερικό και το Διεθνές Δίκαιο:

> «…we will treat a cyber attack on the UK as seriously as we would an equivalent conventional attack and we will defend ourselves as necessary; • we will act in accordance with national and international law and expect others to do the same;…»[215]

2.1.3 Γαλλία

Από το 2008 και έκτοτε, η Γαλλία έχει εκδώσει τρία σημαντικά κείμενα τα οποία συνιστούν μία ολοκληρωμένη εθνική στρατηγική στο πεδίο του Κυβερνοχώρου:

---

[213] (2016). NATIONAL CYBER SECURITY STRATEGY 2016-2021. UK Government. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[214] Ibid. (σελ. 18, παρ. 3.7 – 3.10)

[215] Ibid. (σελ. 25, παρ. 4.5)

α. *Τη Λευκή Βίβλο για την Εθνική Άμυνα και Ασφάλεια του 2008*[216] («'Défense et Sécurité nationale: le Livre blanc»)

β. Την *εθνική Στρατηγική για τον Κυβερνοχώρο του 2011*[217] («'Défense et sécurité des systèmes d'information. Stratégie de la France»)

γ. Τη *Λευκή Βίβλο για την Εθνική Άμυνα και Ασφάλεια του 2013*[218] («'Défense et Sécurité nationale: le Livre blanc»)

Η πρώτη αναφορά στη σπουδαιότητα των κυβερνοαπειλών, ως ζήτημα εθνικής κυβερνοασφάλειας και κυβερνοάμυνας συναντάται στη *Λευκή Βίβλο* του 2008, η οποία τις χαρακτηρίζει μείζονες απειλές, επικαλούμενη απόπειρες κυβερνοεπιθέσεων από μη κρατικούς δρώντες, ακτιβιστές, hackers ή εγκληματικές οργανώσεις. Το 2009 συστάθηκε η *Υπηρεσία Εθνικής Ασφάλειας Δικτύων και Πληροφοριών* («National Network and Information Security Agency - ANSSI»), υπό τον Πρωθυπουργό και τον Γενικό Γραμματέα Άμυνας και Εθνικής Ασφάλειας. Στο πλαίσιο των αρμοδιοτήτων που της δόθηκαν, συνέταξε τον Φεβρουάριο 2011 *Εθνική Στρατηγική για τον Κυβερνοχώρο* με τίτλο «'Information systems defence and security, France's strategy[219]». Η εν λόγω στρατηγική προσδιόριζε τέσσερις βασικούς αντικειμενικούς σκοπούς:

α. Να καταστεί η Γαλλία παγκόσμια δύναμη στον κυβερνοχώρο

β. Να θωρακίσει τη δυνατότητα της χώρας να λαμβάνει αποφάσεις για την εθνική της κυριαρχία, μέσω της προστασίας της πληροφορίας

γ. Να ενισχύσει την κυβερνοασφάλεια κρίσιμων εθνικών υποδομών

δ. Να διασφαλίσει την ασφάλεια στον κυβερνοχώρο

---

[216] Jean-Claude, M. (2008). Défense et Sécurité nationale: le Livre blanc. Nicolas Sarkozy. Ανάκτηση Νοέμβριος 15, 2016, από http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf

[217] (2011). Défense et sécurité des systèmes d'information. Stratégie de la France. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Ανάκτηση Νοέμβριος 15, 2016, από https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

[218] (2013). Livre blanc: Défense et Sécurité nationale. Francois Hollande. Ανάκτηση Νοέμβριος 15, 2016, από http://fr.calameo.com/read/000331627d6f04ea4fe0e

[219] (2011). Information systems defence and security, France's strategy. Ανάκτηση Νοέμβριος 15, 2016, από https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

Αξίζει να επισημανθεί ότι η Λευκή Βίβλος του 2013[220], μεταξύ άλλων, καθορίζει με σαφήνεια ότι η ανάπτυξη «επιθετικών» δυνατοτήτων στον κυβερνοχώρο αποτελεί μέρος της εθνικής στρατηγικής στο εν λόγω πεδίο[221]. Παράλληλα, καλεί τα Ηνωμένα Έθνη να εμβαθύνουν τον διεθνή διάλογο σε καίρια ζητήματα, όπως η εφαρμογή του Άρθρου 51 του Χάρτη των Ηνωμένων Εθνών στην περίπτωση των κυβερνοεπιθέσεων και επαναλαμβάνει τον χαρακτηρισμό της προηγούμενης έκδοσης της Λευκής Βίβλου (2008) για τις κυβερνοεπιθέσεις εναντίον κρατικών πληροφοριακών υποδομών ως *μείζονες απειλές* για την ασφάλεια της χώρας και των Ευρωπαίων εταίρων της. Επίσης, σύμφωνα με την ίδια στρατηγική, η περίπτωση κυβερνοεπίθεσης από άλλο κράτος κατατάσσεται στις τρεις βασικές κατηγορίες παραγόντων που δύνανται να καθορίσουν το επίπεδο απειλής για τη χώρα[222] και ως τρίτη, κατά σειρά, απειλή εναντίον της εδαφικής ακεραιότητας και του πληθυσμού της χώρας, μετά την εκδήλωση επιθετικής ενέργειας από άλλο κράτος και την εκδήλωση τρομοκρατικών ενεργειών.

Σε συνέχεια των ανωτέρω επισημάνσεων στη Λευκή Βίβλο του 2013, το υπουργείο άμυνας της χώρας εξέδωσε τον Φεβρουάριο 2014 το *Σύμφωνο για τον Κυβερνοχώρο*[223] («Cyber Defence Pact - Pacte Défense Cyber»). Το εν λόγω κείμενο εστιάζει σε έξι βασικούς άξονες[224]:

α. Ενδυνάμωση της ασφάλειας των πληροφοριακών συστημάτων

β. Διεύρυνση της έρευνας στο πεδίο της κυβερνοασφάλειας

γ. Επιμόρφωση και εκπαίδευση, με ταυτόχρονη εξειδίκευση στο υπόψη πεδίο

---

[220] Permanent Representation of France to NATO. (2013). Ανάκτηση Νοέμβριος 15, 2016, από White Paper on Defence and National Security: http://www.rpfrance-otan.org/White-Paper-on-defence-and

[221] Ibid. («White Paper - 12 key points», ένατο σημείο, σελ. 6)

[222] Ibid. («White Paper - 12 key points», δεύτερο σημείο, σελ. 2)

[223] (2014, Φεβρουάριος). Cyber Defence Pact . Υπουργείο Άμυνας Γαλλίας. Ανάκτηση Νοέμβριος 16, 2016, από http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf

[224] National Cyber Security Organisation: France. Τάλλιν Εσθονίας: Κέντρο Αριστείας Κυβερνοάμυνας . Ανάκτηση Νοέμβριος 16, 2016, από https://ccdcoe.org/multimedia/national-cyber-security-organisation-france.html

δ. Δημιουργία μίας εθνικής κοινότητας για την κυβερνοάμυνα, βασιζόμενο σε ένα επαρκές δίκτυο εταίρων και σε ένα σύνολο εφεδρικών δικτύων.

ε. Ανάπτυξη Κέντρου Κυβερνοάμυνας στη Βρετανία για τις ανάγκες του υπουργείου άμυνας και της εθνικής κοινότητας σε θέματα κυβερνοάμυνας

στ. Ενίσχυση της διεθνούς συνεργασίας με Ευρωπαίους εταίρους.

Αξίζει, επίσης, να επισημανθεί ότι στο εν λόγω κείμενο γίνεται αναφορά στη συνεργασία με άλλους διεθνείς δρώντες και συγκεκριμένα με το ΝΑΤΟ αλλά όχι με την Ευρωπαϊκή Ένωση, ενώ υπογραμμίζεται ο διαχωρισμός μεταξύ κυβερνοασφάλειας (που αφορούν σε οικονομικές και κρίσιμες πληροφοριακές υποδομές) και κυβερνοάμυνας (που αφορούν σε στρατιωτικές υποδομές και υποδομές πληροφοριών/intelligence).

2.1.4 Κίνα

Η Κίνα αποτελεί, αποδεδειγμένα έναν λαό ο οποίος χρησιμοποιεί σε ιδιαίτερα μεγάλο βαθμό το διαδίκτυο. Αξίζει να σημειωθεί ότι σύμφωνα με στατιστικά στοιχεία, οι χρήστες του ίντερνετ που προέρχονται από την Κίνα αποτελούν το 52,2% του πληθυσμού τους, ενώ συνιστούν το 20% του συνόλου των χρηστών σε ολόκληρο τον κόσμο[225]. Το γεγονός αυτό καθιστά τη χώρα ολοένα και περισσότερο εξαρτώμενη σε διάφορα μέσα που αφορούν στον κυβερνοχώρο.

Αυτό όμως που την ξεχωρίζει από τις λοιπές «δυτικές» χώρες, είναι η απουσία μίας ολιστικής προσέγγισης στα ζητήματα κυβερνοχώρου, η οποία να αποτυπώνεται με σαφήνεια υπό τη μορφή εθνικής στρατηγικής. Κατά συνέπεια, η πολύπλοκη ιεραρχική δομή διοίκησης και τα πολλά και πολυδιάστατα επίσημα έγγραφα για ζητήματα άμυνας, διαμορφώνουν σε γενικές γραμμές μία θολή εικόνα στο υπόψη πεδίο. Ωστόσο, η επιθυμία της ηγεσίας της χώρας να διαμορφώσει μία πιο ξεκάθαρη εικόνα στα ζητήματα κυβερνοάμυνας και κυβερνοασφάλειας,

[225] 721 εκατομμύρια χρήστες επί συνόλου 3,5 δισεκατομμύρια χρηστών σε ολόκληρο τον κόσμο. Πηγή: *Internet Live Stats* το οποίο συγκεντρώνει δεδομένα από έξι μεγάλες υπηρεσίες, μεταξύ των οποίων η Μονάδα Διεθνών Τηλεπικοινωνιών («International Telecommunications Unit») και η Παγκόσμια Τράπεζα. http://www.internetlivestats.com/internet-users-by-country/ (πρόσβαση 17 Νοεμβρίου 2016)

αποτυπώθηκε στην πρόσφατη σύσταση μίας νέας υπηρεσίας (*Central Internet Security and Information Leading Group*), στην οποία έχει ανατεθεί από τον ίδιο τον Πρόεδρο της χώρας ο καθορισμός εθνικής στρατηγικής στον κυβερνοχώρο.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η αντίληψη που φαίνεται να έχει η εν λόγω χώρα, ως προς τον έλεγχο του κυβερνοχώρου. Η Διακυβερνητική Ομάδα Εμπειρογνωμόνων των Ηνωμένων Εθνών, με τη συμμετοχή, μεταξύ άλλων και εκπροσώπου από τη Λαϊκή Δημοκρατία της Κίνας, κατέληξε το 2013 στο συμπέρασμα ότι το Διεθνές Δίκαιο και οι προβλέψεις του Χάρτη των Ηνωμένων Εθνών ισχύουν και εφαρμόζονται πλήρως και στον κυβερνοχώρο. Το συμπέρασμα αυτό φανερώνει την επιρροή του εν λόγω πεδίου από ένα ευρύτατο φάσμα δρώντων (*multi-stakeholder*), όχι απαραίτητα κυβερνητικών (*intergovernmental*), σε αντίθεση, δηλαδή, με την επικρατέστερη αντίληψη στην Κίνα που αφορά στην αποκαλούμενη *κυριαρχία του κυβερνοχώρου* («cyber sovereignty»), σύμφωνα με την οποία η κυρίαρχη υπεροχή του κράτους θα πρέπει να «μεταφέρεται» και στο υπόψη πεδίο. Σύμφωνα με έκθεση της Επιτροπής Αξιολόγησης Ασφαλείας Η.Π.Α.-Κίνας («US-China Security Review Commission»), η αντίληψη του κυβερνοχώρου από πλευράς Λαϊκής Δημοκρατίας της Κίνας, εδράζεται επί δύο βασικών αξόνων:

α. Οι χρήστες του κυβερνοχώρου, τόσο εντός όσο και εκτός της εδαφικής επικράτειας της χώρας, θα πρέπει να ελέγχονται από το *φιλοξενούν έθνος* («host state»), θέση η οποία έρχεται σε πλήρη αντίθεση με τη «δυτική» αντίληψη περί ελευθερίας στον κυβερνοχώρο, με παράλληλο σεβασμό στα ανθρώπινα δικαιώματα[226]:

> «…First, states should be able to assert sovereignty in cyberspace over both their own and foreign citizens and organizations within their borders…»

β. Τα κράτη δεν θα πρέπει να αναμειγνύονται στις εσωτερικές υποθέσεις άλλων κρατών στο πεδίο του κυβερνοχώρου, χρησιμοποιώντας κρίσιμες

[226] Hsu, K. a. (2014). China and International Law in Cyberspace. Report by the U.S.-China Economic and Security. Ανάκτηση Νοέμβριος 17, 2016, από http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf (σελ.2)

υποδομές, πηγές, θεμελιώδεις τεχνολογίες και άλλα τυχόν υφιστάμενα πλεονεκτήματα, εις βάρος των δικαιωμάτων τρίτων κρατών[227]:

> «…Second, states should not interfere with the sovereignty of other states in cyberspace. States should refrain from "using their resources, critical infrastructures, core technologies and other advantages to undermine the right of other countries" to exert sovereignty within their own borders…»

Η ανωτέρω εναλλακτική αυτή αντίληψη της Κίνας παρουσιάστηκε, μαζί με τη Ρωσία και άλλες κεντροασιατικές χώρες, μέσω του Οργανισμού Συνεργασίας της Σανγκάης («Shanghai Cooperation Organisation - SCO»), για πρώτη φορά στη Γενική Συνέλευση των Ηνωμένων Εθνών το 2011 και μεταγενέστερα τον Ιανουάριο 2015[228], ως *Κώδικας Δεοντολογίας* («Code of Conduct»), χωρίς, ωστόσο, να βρίσκει επαρκή απήχηση. Ο *Κώδικας* αυτός επαναλαμβάνει, μεταξύ άλλων, την ανάγκη συμμόρφωσης με τον Χάρτη των Ηνωμένων Εθνών, με σεβασμό στην κυριαρχία και την εδαφική ακεραιότητα των κρατών και στην υποχρέωση μη χρησιμοποίησης επικοινωνιακών και πληροφοριακών συστημάτων για εχθρικές και επιθετικές ενέργειες.

Αξίζει να επισημανθεί ότι κατά μία άποψη[229] και σε αντίθεση με την επίσημη τοποθέτησή της Κίνας στο πλαίσιο της ανωτέρω ομάδας εμπειρογνωμόνων των Ηνωμένων Εθνών, η εν λόγω χώρα δε φαίνεται να θεωρεί το Διεθνές Δίκαιο ως το κυρίαρχο σύστημα κανόνων στον κυβερνοχώρο[230] (προτιμώντας ένα τέτοιο σύστημα κανόνων να διαμορφώνεται από το ίδιο το κράτος), ασκώντας κριτική και στο εγχειρίδιο του *Tallin*, ως μία προσπάθεια χειραγώγησης του κυβερνοχώρου με τη χρήση κανόνων δικαίου.

Δεν είναι, πάντως, λίγες οι φορές που επίσημοι φορείς της χώρας, ο τύπος, οι ένοπλες δυνάμεις και μέλη της ακαδημαϊκής κοινότητας, έχουν τονίσει την

---

[227] Ibid.

[228] (2015, Ιανουάριος). Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Γενική Συνέλευση Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

[229] Segal, A. (2014, Οκτώβριος 14). The Deepening Divide in U.S.-China Cyber Relations. Ανάκτηση Νοέμβριος 17, 2016, από The National Interest: http://nationalinterest.org/blog/the-buzz/the-deepening-divide-us-china-cyber-relations-11568

[230] Σε συνέχεια άρθρου το οποίο δημοσιεύτηκε σε στήλη της επίσημης ιστοσελίδας των Ένοπλων Δυνάμεων της Κίνας («People's Liberation Army Daily»), βλ. άρθρο προηγούμενης υποσημείωσης

ανησυχία τους για τη διαρκώς αυξανόμενη επιρροή των Η.Π.Α. στον έλεγχο του διαδικτύου και του κυβερνοχώρου, σε παγκόσμιο επίπεδο[231]. Στο πλαίσιο αυτό, η ανωτέρω αντίληψή τους παρουσιάζεται από τους ίδιους ως εναλλακτική αλλά απαραίτητη λύση για την επίτευξη μίας εκ νέου ισοκατανομής των όρων διαχείρισης του διαδικτύου και του κυβερνοχώρου στο παγκόσμιο στερέωμα.

2.1.5 Ελλάδα

Στην Ελλάδα, την παρούσα χρονική περίοδο, τελεί υπό σύνταξη η πρώτη εθνική στρατηγική για τον κυβερνοχώρο, με τη συμμετοχή συναρμόδιων υπουργείων και φορέων.

2.2 Στρατηγικές Κυβερνοάμυνας/Κυβερνοασφάλειας Διεθνών Οργανισμών.

2.2.1 Ηνωμένα Έθνη

Το ζήτημα της Κυβερνοάμυνας/Κυβερνοασφάλειας στο πλαίσιο των Ηνωμένων Εθνών απασχολεί διαφορετικά διακυβερνητικά όργανα. Σχετικά ψηφίσματα έχουν προωθηθεί προς υιοθέτηση μόνο προς τη Γενική Συνέλευση των Ηνωμένων Εθνών, ενώ μέχρι σήμερα δεν έχει υιοθετηθεί κανένα ψήφισμα από το Συμβούλιο Ασφαλείας.

Συγκεκριμένα, τρεις από τις έξι κύριες επιτροπές της Γενικής Συνέλευσης έχουν προωθήσει προσχέδια ψηφισμάτων επί της Κυβερνοασφάλειας: η *Επιτροπή Αφοπλισμού και Διεθνούς Ασφάλειας* («Disarmament and International Security Committee»), η *Οικονομική και Δημοσιονομική Επιτροπή* («Economic and Financial Committee») και η *Κοινωνική, Ανθρωπιστική και Πολιτιστική Επιτροπή* («Social, Humanitarian and Cultural Committee»). Ενδεχομένως οι πιο αξιοσημείωτες εξελίξεις έχουν λάβει χώρα στην πρώτη εκ των προαναφερόμενων

[231] (2016). CHINA AND CYBER: ATTITUDES, STRATEGIES, ORGANISATION. Tallin: CCDCOE. Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf (σελ. 7-8)

επιτροπών, στην οποία μάλιστα συμμετέχουν συστηματικά εκπρόσωποι από τα αποκαλούμενα «ισχυρά» κράτη στον τομέα της ασφάλειας της πληροφορίας, όπως Η.Π.Α, Κίνα και Ρωσία.

Με πρωτοβουλία της Ρωσικής Κυβέρνησης εισήχθη από το 1998 στην Πρώτη Επιτροπή της Γενικής Συνέλευσης («Επιτροπή Αφοπλισμού και Διεθνούς Ασφάλειας»), σχέδιο ψηφίσματος με θέμα «Εξελίξεις στον τομέα της πληροφορίας και των τηλεπικοινωνιών, στο πλαίσιο της διεθνούς ασφάλειας», το οποίο υιοθετήθηκε από τη Γενική Συνέλευση το 1999[232]. Σχετικό ψήφισμα, υιοθετείται έκτοτε από τη Γενική Συνέλευση κάθε χρόνο.

Στο αντίστοιχο ψήφισμα που υιοθετήθηκε το 2001[233], η Ρωσία πρότεινε τη σύσταση μίας Ομάδας Κυβερνητικών Εμπειρογνωμόνων (Group of Governmental Experts – GGE), της οποίας τα μέλη, προερχόμενα από 15 κράτη, θα έχουν ως σκοπό να μελετούν τις υφιστάμενες και ενδεχόμενες απειλές στον τομέα της ασφάλειας της πληροφορίας, καθώς και πιθανά μέτρα συνεργασίας για την αποτελεσματική αντιμετώπισή τους. Η εν λόγω ομάδα συνεδρίασε τελικά για πρώτη φορά το 2004. Αξίζει να επισημανθεί ότι από την πρώτη συνεδρίαση της ανωτέρω ομάδας δεν εκπονήθηκε σχετική έκθεση, λόγω αδυναμίας επίτευξης ομοφωνίας μεταξύ των εκπροσώπων[234], ενώ στην τρίτη της σύσκεψη, *επιβεβαιώθηκε η εφαρμογή του Διεθνούς Δικαίου και ιδιαίτερα του Χάρτη των Ηνωμένων Εθνών και στον Κυβερνοχώρο*[235]. Χαρακτηριστική είναι η σχετική αναφορά του τότε και νυν Γενικού Γραμματέα των Ηνωμένων Εθνών Μπαν Κι-μουν (Ιούνιος 2013) στον πρόλογό του για την έκθεση της Ομάδας Κυβερνητικών

[232] (1999). Ψήφισμα A/RES/53/70. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf

[233] (2002). *Ψήφισμα A/RES/56/19.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-011129-ITIS.pdf

[234] Η διαφωνία αφορούσε δύο συγκεκριμένα ζητήματα: α) στο κατά πόσο το τελικό λεκτικό της έκθεσης θα έπρεπε να τονίζει τις νέες απειλές που προέρχονται από την εκμετάλλευση των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνιών για εθνικούς και στρατιωτικούς σκοπούς ασφαλείας και β) στο εάν η συζήτηση θα έπρεπε να αφορά στο περιεχόμενο των πληροφοριών ή θα έπρεπε να επικεντρωθεί στις σχετικές υποδομές πληροφοριών. Βλ. (2016, Ιούλιος). Ενημερωτικό Δελτίο. Γραφείο για ζητήματα Αφοπλισμών των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 20, 2016, από https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/07/Information-Security-Fact-Sheet-July2016.pdf

[235] (2013). Ψήφισμα A/68/98. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

Εμπειρογνωμόνων σχετικά με τις εξελίξεις στον τομέα της πληροφορίας και των επικοινωνιών, στον τομέα της διεθνούς ασφάλειας:

> «…Εκτιμώ το γεγονός ότι η έκθεση έχει εστιάσει στον κεντρικό ρόλο του Χάρτη των Ηνωμένων Εθνών και του Διεθνούς Δικαίου, καθώς επίσης και στη σημασία που επιδεικνύουν τα κράτη που έχουν τη σχετική ευθύνη. Ο προτάσεις που υποβάλλονται συνιστούν έναν μελλοντικό οδικό χάρτη για την εδραίωση των τεχνολογιών ασφάλειας της πληροφορίας και των επικοινωνιών εντός του υφιστάμενου πλαισίου του Διεθνούς Δικαίου και των συμφωνιών που διέπουν τις σχέσεις μεταξύ των κρατών και προασπίζουν τη διεθνή ειρήνη και ασφάλεια…»[236]

Η ανωτέρω ομάδα εμπειρογνωμόνων συγκροτήθηκε για τέταρτη φορά το 2014. Στις συνεδριάσεις που ακολούθησαν (Ιούλιος 2014 έως Ιούνιος 2015), και στις οποίες συμμετείχαν 20 μέλη από διάφορες χώρες[237], εξετάστηκε, μεταξύ άλλων, η ισχύς και η εφαρμογή του Διεθνούς Δικαίου στον τομέα της ασφάλειας της πληροφορίας και των επικοινωνιών. Η σχετική έκθεση[238] που συντάχθηκε και υιοθετήθηκε από τη Γενική Συνέλευση τον Δεκέμβριο 2015[239], επανεπιβεβαίωσε την εφαρμογή του Διεθνούς Δικαίου και ιδιαίτερα του Χάρτη των Ηνωμένων Εθνών στον Κυβερνοχώρο και μάλιστα ως απαραίτητο συστατικό στοιχείο για την διασφάλιση της διεθνούς ειρήνης, ασφάλειας και σταθερότητας.

Συναφώς, στην εν λόγω έκθεση, η ομάδα εμπειρογνωμόνων υπογράμμισε την αξία σεβασμού συγκεκριμένων αρχών του Διεθνούς Δικαίου και του Χάρτη των

---

[236] "*…I appreciate the report's focus on the centrality of the Charter of the United Nations and international law as well as the importance of States exercising responsibility. The recommendations point the way forward for anchoring information and communications technology security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security...*» (Μπαν Κιν-μου, Ιούνιος 2013)

[237] Η.Π.Α., Ηνωμένο Βασίλειο, Ρωσία, Κίνα, Γαλλία, Γερμανία, Ιαπωνία, Ισπανία, Εσθονία, Ισραήλ, Βραζιλία, Πακιστάν, Κολομβία, Αίγυπτος, Γκάνα, Κένυα, Μαλαισία, Μεξικό και Λευκορωσία. Βλ. (2015, Ιούλιος). Ενημερωτικό Δελτίο. Γραφείο για ζητήματα Αφοπλισμών των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

[238] (2015, Ιούλιος). Έκθεση προόδου (A/70/174). Ομάδα Κυβερνητικών Εμπειρογνωμόνων στον τομέα της Πληροφορίας και των Τηλεπικοινωνιών στο πλαίσιο της Διεθνούς Ασφάλειας. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

[239] (2015, Δεκέμβριος). Ψήφισμα A/RES/70/237. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-151223-ITIS.pdf

Ηνωμένων Εθνών και συγκεκριμένα: του σεβασμού της εδαφικής κυριαρχίας, της ειρηνικής επίλυσης των διεθνών διαφορών, της απαγόρευσης απειλής ή χρήσης βίας κατά της εδαφικής ακεραιότητας και πολιτικής ανεξαρτησίας οποιουδήποτε κράτους, του σεβασμού των ανθρωπίνων δικαιωμάτων και της μη επέμβασης στις εσωτερικές υποθέσεις των άλλων κρατών.

Σε ότι αφορά στον τρόπο εφαρμογής του Διεθνούς Δικαίου στον Κυβερνοχώρο, η ομάδα εμπειρογνωμόνων κατέγραψε τις παρακάτω απόψεις:

α. Τα κράτη έχουν δικαιοδοσία στις υποδομές πληροφοριών και επικοινωνιών εντός της εδαφικής τους επικράτειας.

β. Τα κράτη έχουν την υποχρέωση να παρακολουθούν την εφαρμογή αρχών του Διεθνούς Δικαίου στις υπόψη τεχνολογικές υποδομές, με σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών.

γ. Τα κράτη διατηρούν το εγγενές δικαίωμά τους να λαμβάνουν μέτρα που να συνάδουν με το Διεθνές Δίκαιο και τις προβλέψεις του Χάρτη των Ηνωμένων Εθνών, για την ειρηνική χρήση πληροφοριακών και επικοινωνιακών συστημάτων, αναγνωρίζοντας την ανάγκη για περαιτέρω μελέτη εν λόγω ζητήματος.

δ. Επιβεβαιώθηκε η ισχύς διεθνών νομικών αρχών, συμπεριλαμβανομένων, όπου αυτό είναι εφικτό, των αρχών του ανθρωπισμού, της αναγκαιότητας, της αναλογικότητας και της διάκρισης.

ε. Τα κράτη δε θα πρέπει να χρησιμοποιούν «διαμεσολαβητές» («proxies») κατά τη διάπραξη διεθνώς παράνομων πράξεων, μέσω πληροφοριακών και επικοινωνιακών συστημάτων. Παράλληλα, θα πρέπει να εξασφαλίζουν ότι το έδαφός τους δε θα χρησιμοποιείται από μη κρατικούς δρώντες (non state actors) για τους ανωτέρω σκοπούς.

στ. Η ένδειξη ότι μια παράνομη δραστηριότητα μέσω πληροφοριακών και επικοινωνιακών συστημάτων προέρχεται από το έδαφος ή τις υποδομές ενός κράτους μπορεί να είναι ανεπαρκής από μόνη της για να αποδώσει το αξιόποινο της εν λόγω δραστηριότητα στο κράτος αυτό, σημειώνοντας την ανάγκη για πλήρη και επαρκή τεκμηρίωση.

Ωστόσο, παρά τη διαφαινόμενη ομοφωνία απόψεων, όπως αυτή αποτυπώνεται τόσο στα ετήσια ψηφίσματα της Γενικής Συνέλευσης των

Ηνωμένων Εθνών, όσο και στις σχετικές εκθέσεις της Ομάδας Κυβερνητικών Εμπειρογνωμόνων, δεν υπάρχει ακόμα ευρέως κοινή αντίληψη ως προς τον τρόπο εφαρμογής των ισχυόντων κανόνων Διεθνούς Δικαίου στον Κυβερνοχώρο.

Η Οικονομική και Δημοσιονομική Επιτροπή («Economic and Financial Committee») έχει επίσης προωθήσει τρία ψηφίσματα (2002[240], 2003[241] και 2009[242]) σχετικά με τον Κυβερνοχώρο, εστιάζοντας, ωστόσο, στη δημιουργία μίας παγκόσμιας αντίληψης της Κυβερνοασφάλειας και στην προστασία κρίσιμων υποδομών πληροφοριών.

Η Κοινωνική, Πολιτιστική και Ανθρωπιστική Επιτροπή («Social, Cultural and Humanitarian Committee») έχει επικεντρωθεί κυρίως στα ζητήματα του Κυβερνοεγκλήματος και του δικαιώματος της ιδιωτικότητας, εστιάζοντας ιδιαίτερα στην αντιμετώπιση της εγκληματικής και ανορθόδοξης χρήσης των τεχνολογιών στον τομέα της πληροφορίας. Αξίζει να επισημανθεί ότι το 2013, η Γενική Συνέλευση υιοθέτησε το ψήφισμα «Το δικαίωμα της ιδιωτικότητας στην ψηφιακή εποχή», το οποίο, μεταξύ των άλλων, τόνιζε ότι τα ανθρώπινα δικαιώματα ισχύουν τόσο εκτός («offline»), όσο και εντός («online») του διαδικτύου/Κυβερνοχώρου. Το ίδιο ψήφισμα πρότεινε, επίσης, την εκπόνηση σχετικής αναφοράς[243] από τον Ύπατο Αρμοστή για τα Ανθρώπινα Δικαιώματα. Η σπουδαιότητα με την οποία αντιμετωπίζει το εν λόγω ζήτημα ο Οργανισμός Ηνωμένων Εθνών αποτυπώθηκε τον Μάρτιο του 2015, αποφασίζοντας τη θέσπιση ενός Ειδικού Εισηγητή για το δικαίωμα στην ιδιωτικότητα[244], με σκοπό τη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος.

---

[240] (2003, Ιανουάριος). Ψήφισμα A/RES/57/239. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOfCS.pdf

[241] (2004, Ιανουάριος). Ψήφισμα A/RES/58/199. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-031223-CultureOfCandCI.pdf

[242] (2010, Μάρτιος). Ψήφισμα A/RES/64/211. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf

[243] (2014, Ιούνιος). Έκθεση για το "Δικαίωμα της Ιδιωτικότητας στην Ψηφιακή Εποχή" (A/HRC/27/37). Γραφείο Ύπατου Αρμοστή των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-140730-RightToPrivacyReport.pdf

[244] (2015, Μάρτιος). Έκθεση για το "Δικαίωμα στην Ιδιωτικότητα στην Ψηφιακή Εποχή" (A/HRC/28/L.27). Συμβούλιο για τα Ανθρώπινα Δικαιώματα. Ανάκτηση Νοέμβριος 14, 2016, από

2.2.2 Ευρωπαϊκή Ένωση

Στο πλαίσιο της Ευρωπαϊκής Ένωσης, τα έγγραφα τα οποία σχετίζονται περισσότερο με την Κυβερνοασφάλεια είτε εκφράζουν ομόφωνη πολιτική βούληση αλλά δεν είναι νομικά δεσμευτικά (π.χ. οι ανακοινώσεις *Communications*), είτε αποτελούν διαφορετικού τύπου δράσεις, νομικά δεσμευτικές, τα οποία καθορίζουν μία σειρά υποχρεώσεων τόσο για τα κράτη μέλη της όσο και για άλλες συγκεκριμένες οντότητες. Το πρώτο συνεκτικό κείμενο το οποίο αφορούσε στην αντιμετώπιση ενός ευρέος φάσματος κυβερνοαπειλών εκδόθηκε το 2013 με τίτλο *Στρατηγική Κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης: ένας ανοιχτός, σίγουρος και ασφαλής Κυβερνοχώρος*[245] (*«Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace»*) . Στην εν λόγω στρατηγική υπογραμμίζεται ότι η Ευρωπαϊκή Επιτροπή και ο Ύπατος Εκπρόσωπος Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας, σε συνεργασία με τα κράτη μέλη της, θα υποστηρίξει την ανάπτυξη κανόνων συμπεριφοράς και μέτρων οικοδόμησης εμπιστοσύνης για τη διασφάλιση της Κυβερνοασφάλειας. Επιπρόσθετα θα διευκολύνει, μεταξύ άλλων, τον διάλογο για την εξεύρεση τρόπων εφαρμογής υφιστάμενων κανόνων Διεθνούς Δικαίου στον Κυβερνοχώρο. Αξίζει να επισημανθεί ότι η εν λόγω στρατηγική δίνει ιδιαίτερη σημασία στην πρόληψη και αντιμετώπιση τυχόν κυβερνοεπιθέσεων σε εθνικό, κατά βάση, επίπεδο, υπογραμμίζοντας ότι κεντρική εποπτεία από την ΕΕ δεν αποτελεί την ενδεικνυόμενη λύση στην αποτελεσματική αντιμετώπιση των υπόψη ζητημάτων.

Επιπρόσθετα, καθορίζει τρεις βασικούς πυλώνες για την αντιμετώπιση των κυβερνοαπειλών:

---

https://ccdcoe.org/sites/default/files/documents/UN-150324-SpecialRapporteurOnTheRightToPrivacy.pdf

[245] (2013, Φεβρουάριος). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [JOIN(2013) 1 final]. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Ευρωπαική Επιτροπή. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-130207-CSS.pdf

α. Ασφάλεια δικτύων και πληροφορίας[246], υπογραμμίζοντας τη σημασία ανάπτυξης συνεργασίας, σε διεθνές επίπεδο, με τον ιδιωτικό τομέα.

β. Επιβολή του νόμου[247], με παράλληλη υιοθέτηση Οδηγίας[248] για αντιμετώπιση επιθέσεων εναντίον πληροφοριακών συστημάτων, η οποία προϋποθέτει από τα κράτη μέλη να ενισχύσουν την εθνική τους νομοθεσία κατά του Κυβερνοεγκλήματος και να εισαγάγουν αυστηρότερες ποινικές κυρώσεις.

γ. Άμυνα[249], αναγνωρίζοντας την ανάπτυξη της αμυντικής πολιτικής και των δυνατοτήτων του Κυβερνοχώρου ως εκ των αντικειμενικών σκοπών της *Κοινής Πολιτικής Άμυνας και Ασφάλειας* («Common Security and Defence Policy - CSDF»), διαμορφώνοντας μία σειρά δράσεων, στο πλαίσιο της συνεργασίας του Ευρωπαϊκού Οργανισμού Άμυνας και των κρατών μελών της ΕΕ.

Δέον όπως επισημανθεί ότι η ανωτέρω Ευρωπαϊκή Στρατηγική για τον Κυβερνοχώρο προβλέπει ότι σοβαρό περιστατικό κυβερνοεπίθεσης εναντίον ενός κράτους μέλους της, θα μπορούσε να αποτελέσει επαρκή λόγο ώστε το κράτος αυτό να επικαλεστεί τη ρήτρα αλληλεγγύης

[246] Τα κυριότερα όργανα της ΕΕ στον εν λόγω πυλώνα είναι α) η *Ευρωπαϊκή Επιτροπή*, β) η *Ευρωπαϊκή Υπηρεσία για την Ασφάλεια των Δικτύων και της Πληροφορίας* («European Networks and Information Security Agency - ENISA»), γ) η *Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης για Υπολογιστές* («Computer Emergency Response Team – CERT EU»), δ) ένα δίκτυο αρμόδιων αρχών και ε) η Ευρωπαϊκή Εταιρική Σχέση Δημόσιου-Ιδιωτικού Τομέα για την Ανθεκτικότητα («European Public-Private Partnership for Resilience – EP3R»)

[247] Τα κυριότερα όργανα της ΕΕ στον εν λόγω πυλώνα είναι α) το *Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα* («European Cybercrime Centre – EC3»), β) η *Ευρωπαϊκή Υπηρεσία Πληροφοριών* («European Police Office - EUROPOL»), γ) η *Ευρωπαϊκή Αστυνομική Ακαδημία* («European Police College - CEPOL») και δ) η *Μονάδα Δικαστικής Συνεργασίας της ΕΕ* («European Justice - Eurojust»)

[248] (2013, Αύγουστος). DIRECTIVE 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο Ευρωπαϊκής Ένωσης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-130812-AttacksAgainstInformationSystems.pdf

[249] Τα κυριότερα όργανα της ΕΕ στον εν λόγω πυλώνα είναι α) η *Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης* («European External Action Service - EEAS»), β) το *Στρατιωτικό Επιτελείο της ΕΕ* («European Union Military Staff - EUMS»), και γ) η *Ευρωπαϊκός Οργανισμός Άμυνας* («European Defence Agency - EDA»).

της ΕΕ (άρθρο 222 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης[250]).

> "…A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)…" (σελ. 19)

Συναφώς, το Συμβούλιο της ΕΕ υιοθέτησε τον Νοέμβριο 2014 το *Πλαίσιο Εφαρμογής της Αμυντικής Πολιτικής στον Κυβερνοχώρο*[251] («EU Cyber Defence Policy Framework»), προκειμένου να παράσχει ένα χρήσιμο εργαλείο για την εφαρμογή της ανωτέρω στρατηγικής.

Επίσης, σχετικές δράσεις συμπεριλήφθηκαν από την Ευρωπαϊκή Επιτροπή:

α. στην *Ψηφιακή Ημερησία Διάταξη για την Ευρώπη*[252] («Digital Agenda for Europe»), η οποία αποτέλεσε μία από τις επτά εμβληματικές πρωτοβουλίες της *Στρατηγικής της ΕΕ για το 2020* («Europe 2020 Strategy»), που εκπονήθηκε τον Μάρτιο 2010 για να διευκολύνει την έξοδο από την κρίση και προκειμένου να προετοιμάσει την οικονομία της Ένωσης για να αντιμετωπίσει τις απειλές της επόμενης δεκαετίας (μεταξύ των οποίων και των κυβερνοαπειλών).

β. στην *Ευρωπαϊκή Ημερησία Διάταξη για την Ασφάλεια*[253] («The European Agenda on Security»), η οποία προτεραιοποίησε το κυβερνοέγκλημα ως εκ των σύγχρονων αναδυόμενων απειλών.

---

[250] (2012, Οκτώβριος). Consolidated Version of the Treaty on the Functioning of the European Union (C 326/47). Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-121026-TFEU.pdf

[251] (2014, Νοέμβριος). EU Cyber Defence Policy Framework. Συμβούλιο Ευρωπαϊκής Ένωσης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf

[252] (2010, Μάρτιος). Ψήφισμα A/RES/64/211. Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf

[253] (2015, Απρίλιος). The European Agenda on Security [COM(2015) 185 final]. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Ευρωπαϊκή Επιτροπή. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-150428-EUSecurityAgenda.pdf

2.2.3 Συμβούλιο της Ευρώπης

Η *Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα*[254] είναι η πιο σημαντική πρωτοβουλία του Οργανισμού στον τομέα του Κυβερνοχώρου, καθώς αποτέλεσε την πρώτη προσπάθεια εναρμόνισης της νομοθεσίας για την εγκληματικότητα στο υπόψη πεδίο. Η εν λόγω σύμβαση παρέχει χρήσιμες κατευθύνσεις στα κράτη που αναπτύσσουν τη δική τους εθνική νομοθεσία για την αντιμετώπιση του κυβερνοεγκλήματος, προτείνοντας παράλληλα ένα πλαίσιο διεθνούς συνεργασίας μεταξύ των κρατών που είναι συμβαλλόμενα μέρη στη συγκεκριμένη σύμβαση. Η Σύμβαση της Βουδαπέστης συμπληρώνεται από ένα πρόσθετο πρωτόκολλο[255], το οποίο υπεγράφη στο Στρασβούργο (Ιανουάριος 2003), σχετικά με την ποινικοποίηση φαινομένων ξενοφοβίας και ρατσισμού που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών. Το πρόσθετο αυτό πρωτόκολλο, μεταξύ των άλλων, καθορίζει (άρθρο 6) ως υποχρέωση των συμβαλλόμενων μερών να μη δημοσιοποιούν, μέσω των υπολογιστικών τους συστημάτων, υλικό το οποίο με τον οποιονδήποτε τρόπο να προβάλλει ή να εγκρίνει πράξεις γενοκτονίας ή εγκλημάτων κατά της ανθρωπότητας, σύμφωνα με το Διεθνές Δίκαιο:

> «…Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party…» (άρθρο 6, Πρόσθετο Πρωτόκολλο στη Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα)

[254] (2001, Νοέμβριος). Convention on Cybercrime. Βουδαπέστη: Συμβούλιο της Ευρώπης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/CoE-011123-ConventiononCybercrime.pdf

[255] (2003, Ιανουάριος). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Συμβούλιο της Ευρώπης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/CoE-030128-AdditionalProtocol.pdf

2.2.4 Οργανισμός για την ασφάλεια και τη συνεργασία στην Ευρώπη

Στο ίδιο μήκος κύματος με το Συμβούλιο της Ευρώπης κινείται και ο *Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη* («Organization for Security and Co-operation in Europe - OSCE»), εστιάζοντας περισσότερο στην αντιμετώπιση του κυβερνοεγκλήματος και της αντιτρομοκρατίας. Το 2004[256] και το 2006[257], το Υπουργικό Συμβούλιο υιοθέτησε μία σειρά αποφάσεων, προτείνοντας την ανάληψη από τα κράτη συγκεκριμένων ενεργειών, σε εθνικό επίπεδο και τη διεθνή συνεργασία για την αντιμετώπιση φαινομένων χρήσης του διαδικτύου για τρομοκρατικούς σκοπούς. Μεταγενέστερες διακηρύξεις της Κοινοβουλευτικής Ολομέλειας από το 2008, καλούν τα κράτη μέλη να λάβουν μέτρα για την καταπολέμηση του κυβερνοεγκλήματος στον Κυβερνοχώρο και την ενίσχυση της ασφάλειας στο πεδίο αυτό. Το 2013, το Μόνιμο Συμβούλιο του Οργανισμού υιοθέτησε μία αρχική δέσμη *Μέτρων Οικοδόμησης Εμπιστοσύνης για τον Κυβερνοχώρο*[258] («Confidence-Building Measures for cyberspace»), με σκοπό τη μείωση της πιθανότητας σύγκρουσης από τη χρήση των πληροφοριακών και επικοινωνιακών συστημάτων. Τον Μάρτιο 2016 υιοθετήθηκε αναθεωρημένη δέσμη μέτρων[259], η οποία, μεταξύ άλλων, επισημαίνει σαφώς την υποχρέωση συμμόρφωσης των κρατών μελών του Οργανισμού με το Διεθνές Δίκαιο, συμπεριλαμβανομένου του Χάρτη των Ηνωμένων Εθνών, της Διεθνούς Σύμβασης για τα Ατομικά και Πολιτικά Δικαιώματα («International Covenant on Civil and

[256] (2004, Δεκέμβριος). Απόφαση No 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

[257] (2006, Δεκέμβριος). 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

[258] (2013, Δεκέμβριος). 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, Permament Council. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/OSCE-131203-Confidencebuildingmeasures_0.pdf

[259] (2016, Μάρτιος). Απόφαση No. 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

Political Rights»), της Συμφωνίας του Ελσίνκι («Helsinki Final Act»[260]) και το σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών:

> «…The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms…» (Απόφαση 1202, σελ. 1)

2.2.5 NATO

Η Κυβερνοάμυνα ενσωματώθηκε για πρώτη φορά στην Ημερησία Διάταξη της συμμαχίας από τη Σύνοδο Κορυφής στην Πράγα το 2002[261], με μία λιτή αναφορά στην απόφαση των κρατών μελών να ενισχύσουν τις δυνατότητές τους για την αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων:

> «…Decided to:….f. Strengthen our capabilities to defend against cyber attacks…» (Διακήρυξη Συνόδου Κορυφής ΝΑΤΟ, Πράγα 2002)

Οι εκτεταμένες κυβερνοεπιθέσεις στην Εσθονία το 2007 ενδυνάμωσαν το ενδιαφέρον του ΝΑΤΟ στο πεδίο του Κυβερνοχώρου. Έτσι το 2008 εκπονήθηκε η πρώτη Πολιτική Κυβερνοάμυνας της συμμαχίας, ενώ το 2010, στη Σύνοδο Κορυφής στη Λισσαβώνα[262], η κυβερνοάμυνα συμπεριλήφθη στη *Στρατηγική Θεώρηση*[263] του Οργανισμού («NATO's Strategic Concept»). Τον Σεπτέμβριο 2014, στη Σύνοδο Κορυφής στην Ουαλία[264], υιοθετήθηκε μία αναθεωρημένη και ενισχυμένη Πολιτική Κυβερνοάμυνας, η οποία καθόριζε με σαφήνεια και για πρώτη

[260] (1975). FINAL ACT by CONFERENCE ON SECURITY AND CO-OPERATION IN EUROPE . Helsinki: OSCE. Ανάκτηση Νοέμβριος 14, 2016, από http://www.osce.org/helsinki-final-act?download=true

[261] (2002, Νοέμβριος). Prague Summit Declaration. NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-021121-PragueSummitDeclaration.pdf

[262] (2010, Νοέμβριος). Lisbon Summit Declaration. NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-101120-LisbonSummitDeclaration.pdf

[263] (2010, Νοέμβριος). Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-101120-StrategicConcept.pdf

[264] (2014, Σεπτέμβριος). Wales Summit Declaration. NATO. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-140905-WalesSummitDeclaration.pdf

φορά ότι μία μεγάλη, «ψηφιακή» επίθεση εναντίον ενός κράτους μέλους θα μπορούσε να ενεργοποιήσει το βασικότερο άρθρο συλλογικής ασφάλειας της συμμαχίας (άρθρο 5 της Ιδρυτικής Συνθήκης). Η αναθεωρημένη αυτή πολιτική, προωθούσε την αναγκαιότητα για ανταλλαγή πληροφοριών, την αμοιβαία συνεργασία μεταξύ των μελών της συμμαχίας, την ενίσχυση της εκπαίδευσης και την περαιτέρω συνεργασία με τη βιομηχανία. Αξίζει να σημειωθεί ότι στην επόμενη Σύνοδο Κορυφής (Βαρσοβία, Ιούλιος 2016), αναγνωρίστηκε ο Κυβερνοχώρος ως επιχειρησιακό πεδίο[265] και επιβεβαιώθηκε η εφαρμογή του Διεθνούς Δικαίου στον εν λόγω τομέα, συμπεριλαμβανομένου του Χάρτη των Ηνωμένων Εθνών, του Διεθνούς Ανθρωπιστικού Δικαίου και των Ανθρωπίνων Δικαιωμάτων:

> «…We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable…»[266]

Σε ότι αφορά στα θεσμικά όργανα του ΝΑΤΟ που είναι υπεύθυνα για θέματα Κυβερνοάμυνας, το ανώτερο συμβουλευτικό όργανο είναι από το 2014 η *Επιτροπή Κυβερνοάμυνας* («Cyber Defence Committee – CDC»). Όσον αφορά τον κεντρικό έλεγχο της τεχνικής υποστήριξης των συμμαχικών υποδομών έναντι κυβερνοαπειλών, υπεύθυνη δομή έχει καθοριστεί το κέντρο αντίδρασης για περιστατικά σε υπολογιστικά συστήματα («NATO Computer Incident Response Capability - NCIRC»), που ανήκει στην Υπηρεσία Επικοινωνιών και Πληροφοριών («NATO Communications and Information Agency - NCIA»).

Ιδιαίτερα σημαντικός, κυρίως σε θέματα εκπαίδευσης, είναι και ο ρόλος του πιστοποιημένου Κέντρου Αριστείας για την Κυβερνοάμυνα στο Τάλλιν της Εσθονίας, στο οποίο οι εκάστοτε διεξαγόμενες μελέτες παράγουν χρήσιμα προϊόντα όχι μόνο για την ίδια τη συμμαχία.

---

[265] (2016, Ιούλιος). Warsaw Summit Communiqué. NATO. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf (παρ. 70)

[266] Ibid.

ΚΕΦΑΛΑΙΟ 3
Η εφαρμογή των προβλέψεων για νόμιμη άμυνα και συλλογική ασφάλεια στον κυβερνοχώρο

Το ζήτημα της εφαρμογής του διεθνοδικαιϊκού θεσμικού πλαισίου που ισχύει για την νόμιμη άμυνα και τη συλλογική ασφάλεια στον κυβερνοχώρο, αποτελεί μία από τις σημαντικότερες (αν όχι τη σημαντικότερη) προκλήσεις του Διεθνούς Δικαίου στο υπόψη πεδίο. Υπάρχουν συγκεκριμένοι παράμετροι που δημιουργούν απροσπέλαστους προβληματισμούς, κατά την εξέταση της εφαρμογής του.

Καταρχήν, στην περίπτωση των κυβερνοεπιθέσεων, ιδιαίτερα δύσκολη, από αποδεικτικής πλευράς, είναι η απόδοση της ευθύνης (*attribution*) για την εκδήλωση των επιθέσεων αυτών και τη συνεπαγόμενη τέλεση παράνομων και αξιόποινων πράξεων στον κυβερνοχώρο, σε συγκεκριμένο κράτος (*State Responsibility*). Αυτό είναι εξαιρετικά δύσκολο, αν λάβει κανείς υπόψη του ότι στην περίπτωση των κυβερνοεπιθέσεων στην Εσθονία το 2007, χρησιμοποιήθηκαν, εξ' αποστάσεως, υπολογιστές ακόμα και μέσα στην Εσθονία, προκειμένου να ανακατευθύνουν τον τεράστιο όγκο των προκαθορισμένων εντολών προς τους «στόχους» τους, με σκοπό να τους θέσουν εκτός λειτουργίας. Η χρήση ενδιάμεσων υπολογιστικών συστημάτων (*zombies*) είναι μία ευρεία διαδεδομένη μέθοδος, κατά την εκδήλωση συντονισμένων κυβερνοεπιθέσεων, προκειμένου να δυσχεράνουν τον εντοπισμό των υπευθύνων, μέθοδος που χρησιμοποιήθηκε στην Εσθονία, καθόσον .

Δεύτερον, όπως επισημάνθηκε στο πρώτο μέρος της παρούσας εργασίας, δεν υφίστανται συγκεκριμένα κριτήρια στον Χάρτη των Ηνωμένων Εθνών, με βάση τα οποία να δύναται να χαρακτηριστεί μία ενέργεια ξεκάθαρα ως χρήση βίας, ώστε να εμπίπτει στις προβλέψεις του συναφούς άρθρου 2(4) του Χάρτη και να ενεργοποιεί, κατ' επέκταση, το δικαίωμα της νόμιμης άμυνας, σύμφωνα με το άρθρο 51. Το εγχειρίδιο του Τάλλιν απαριθμεί ένα σύνολο παραγόντων[267] που θα μπορούσαν να εξεταστούν κατά τη διαδικασία εκτίμησης μίας ενέργειας στον κυβερνοχώρο, ωστόσο δεν είναι νομικά δεσμευτικοί, ώστε να δύναται να γίνει επίκλησή τους.

[267] Βλ. παρ. 2.3/Μέρος Α' της παρούσας εργασίας

Αξίζει, ωστόσο, να επισημανθεί η προσέγγιση του καθηγητή Διεθνούς Δικαίου κ. *Kubo Macak*[268], σύμφωνα με την οποία θα πρέπει να εξετάζεται το εν λόγω ζήτημα, από την άποψη του μεγέθους και της σοβαρότητας των συνεπειών μιας κυβερνοεπίθεσης, κατά αναλογία με τις συνέπειες από μία ένοπλη επίθεση, ή πράξη χρήσης βίας, σύμφωνα με το Ψήφισμα 3314 της Γενικής Συνέλευσης των Ηνωμένων Εθνών.

Τρίτον, λόγω της φύσης των κυβερνοεπιθέσεων, προκύπτουν εύλογα ερωτήματα, σε ζητήματα άσκησης δικαιοδοσίας για παράνομες πράξεις στον κυβερνοχώρο. Αναλύοντας τις στρατηγικές κυβερνοάμυνας/κυβερνοασφάλειας των κρατών και των Διεθνών Οργανισμών που συμπεριλαμβάνονται στην εν λόγω εργασία, διαπιστώνεται ότι όλες υπογραμμίζουν το ρόλο του κράτους, ως προς την υποχρέωση επιτήρησης και διασφάλισης των συστημάτων του, καθώς και την άσκηση δικαιοδοσίας, όταν και αν απαιτηθεί. Ωστόσο, το ερώτημα που γεννιέται και παραμένει αναπάντητο, είναι εάν αυτή θα πρέπει να ασκηθεί από το κράτος της ιθαγένειας του προσώπου το οποίο προβαίνει στις παράνομες πράξεις στον κυβερνοχώρο, ή από το κράτος από το έδαφος του οποίου αυτές λαμβάνουν χώρα ή από το θιγόμενο κράτος.

Τέταρτον, ο άυλος χαρακτήρας του κυβερνοχώρου, ευνοεί τη δημιουργία συγκερασμών σύμφωνα με τους οποίους αυτός δεν μπορεί να θεωρηθεί ως προέκταση του εδάφους ενός κράτους και ως τέτοιος καθίσταται αρκετά δύσκολο να υφίσταται ζήτημα κρατικής κυριαρχίας στο εν λόγω πεδίο.

Πέμπτον, δεν υπάρχει προηγούμενο στη νομολογία των διεθνών δικαστηρίων. Κατά συνέπεια, τυχόν προβληματισμοί και ερωτήματα που ανακύπτουν κατά την εκδήλωση μίας κυβερνοεπίθεσης, δεν μπορούν να απαντηθούν, αξιοποιώντας παλαιότερες αποφάσεις ή σχολιασμό ενός ή περισσοτέρων διεθνών δικαστηρίων.

Όσον αφορά το ζήτημα της ενεργοποίησης των προβλέψεων περί συλλογικής ασφάλειας, στο πλαίσιο των Διεθνών Οργανισμών, αρκεί να επισημανθεί ότι και στην περίπτωση αυτή δεν υφίσταται επαρκές ιστορικό

[268] Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, σελ. 428. Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

προηγούμενο, καθόσον μόνο δύο σχετικά άρθρα έχουν ενεργοποιηθεί μέχρι σήμερα και αυτά από μία φορά έκαστο[269].

Η ομάδα διακυβερνητικών ειδικών εμπειρογνωμόνων που έχει συσταθεί από τα Ηνωμένα Έθνη επιτελεί ένα ιδιαίτερα σημαντικό και χρήσιμο έργο για την εφαρμογή του Διεθνούς Δικαίου στον κυβερνοχώρο. Φαίνεται ότι οι απόψεις διίστανται, είτε προς την κατεύθυνση της δημιουργίας νέων διεθνοδικαιϊκών κανόνων, είτε προς τη σταδιακή αποκρυστάλλωση σχετικών εθιμικών κανόνων και την εκ νέου ερμηνεία των υφιστάμενων κανόνων. Η λύση της υιοθέτησης σχετικής διεθνούς σύμβασης δεν έχει αποκλειστεί, ωστόσο η διεθνής πρακτική του παρελθόντος επιβεβαιώνει τη δυσκολία επίτευξης μίας τέτοιας συμφωνίας.

[269] Άρθρο 42(7) της Συνθήκης για την ΕΕ (τρομοκρατικές ενέργειες στο Παρίσι, 15 Νοεμβρίου 2015) και άρθρο 5 Ιδρυτικής Συνθήκης ΝΑΤΟ (επίθεση στους «δίδυμους» πύργους στις Η.Π.Α., 11 Σεπτεμβρίου 2001)

ΕΠΙΛΟΓΟΣ

Το ζήτημα της εφαρμογής του Διεθνούς Δικαίου στο ασύμμετρο πεδίο του κυβερνοχώρου, ως προς την ενεργοποίηση του δικαιώματος της νόμιμης άμυνας και της συλλογικής ασφάλειας, παραμένει μία από τις μεγαλύτερες σύγχρονες προκλήσεις, καθόσον συνεχίζει να παράγει μία σειρά από σημαντικούς προβληματισμούς. Αντίστοιχοι προβληματισμοί, όμως, ισχύουν και σε άλλα ζητήματα του Διεθνούς Δικαίου. Στην περίπτωση π.χ. του Διεθνούς Ανθρωπιστικού Δικαίου, κρίνεται επιβεβλημένη η περαιτέρω διευκρίνιση συγκεκριμένων ζητημάτων, όπως η διάκριση στον κυβερνοχώρο μεταξύ στρατιωτικών και μη στρατιωτικών στόχων, μεταξύ εμπόλεμων και ουδέτερων κρατών ή μεταξύ εμπλεκομένων στη σύρραξη και άμαχου πληθυσμού. Ερωτηματικά επίσης υπάρχουν ως προς τον τρόπο που θα διαχειριστεί μελλοντικά το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων το ζήτημα της θεμελίωσης της δικαιοδοσίας του Δικαστηρίου για παραβίαση της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα στον κυβερνοχώρο, σε περίπτωση που δε στοιχειοθετείται επαρκώς τυχόν σύνδεσμος της επίδικης συμπεριφοράς με το έδαφος συγκεκριμένου κράτους.

Αν και το πρόβλημα φαίνεται να εξελίσσεται πιο γρήγορα από το ρυθμό θεσμικής διαχείρισής του από τα κράτη, δε θα πρέπει να λησμονηθεί το ενδιαφέρον και η σημασία που τα λεγόμενα «ισχυρά κράτη» αποδίδουν στο εν λόγω ζήτημα. Ενδεικτικά επισημαίνεται ότι από τότε που συστάθηκε η ομάδα εργασίας των διακυβερνητικών εμπειρογνωμόνων στο πλαίσιο των Ηνωμένων Εθνών, μέχρι σήμερα, μετέχουν αδιάλειπτα όλα τα μόνιμα μέλη του Συμβουλίου Ασφαλείας των Η.Ε. και η Γερμανία. Σε κάθε περίπτωση, ο ρόλος του κυρίαρχου κράτους είναι καταλυτικός. Συναφώς ο καθηγητής Διεθνούς Δικαίου κ. Τσαγκουριάς επισημαίνει σε εισήγησή του[270] ότι το κράτος οφείλει να αναλαμβάνει τις ευθύνες του, όχι μόνο για τις παράνομες πράξεις του, όταν τις διαπράττει, αλλά και στην περίπτωση που δημιουργεί γόνιμο έδαφος προκειμένου να εκδηλωθούν. Η ουσιαστική βούληση των κρατών να συναινέσουν σε μία ολιστική προσέγγιση

[270] Tsagourias, N., Buchan , R., & Roscini, M. (2014, Οκτώβριος 9). State Responsibility for Cyber Operations:. Ανάκτηση Νοέμβριος 20, 2016, από http://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1

και αντιμετώπιση του εν λόγω ζητήματος που αφορά στον κυβερνοχώρο, βασισμένη στην απρόσκοπτη διακρατική συνεργασία και φυσικά στο Διεθνές Δίκαιο και στις προβλέψεις του Χάρτη των Ηνωμένων Εθνών, εκτιμάται ότι αποτελεί το κλειδί στην επίλυση των όποιων προβληματισμών, η οποία στις μέρες κρίνεται περισσότερο επιτακτική από ποτέ.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλιογραφία

Κρατερός, Ι. Μ., & Περράκης, Σ. Ε. (1990). *Γενικό και Ειδικό Διεθνές Δίκαιο.* Αθήνα-Κομοτηνή: ΣΑΚΚΟΥΛΑ.

Περράκης, Σ., & Μαρούδα, Μ.-Ν. (2016). ΔΙΕΘΝΗΣ ΔΙΚΑΙΟΤΑΞΙΑ Θεωρία και Εφαρμογή Διεθνούς Δικαίου. Ι. ΣΙΔΕΡΗΣ.

Ρούκουνας, Ε. (2015). *Διεθνές Δίκαιο.* Νομική Βιβλιοθήκη.

Brownlie, I. (1991). *International Law and the Use of Force by States.* Oxford at the Clarendon Press.

Cassese, A. (2011). *International Law .* Guremberg.

Dinstein, Y. (2011). *War, Aggression and Self-Defence.* Cambridge.

Frank, T. M. (2004). *Recourse to Force. State Action Against Threats and Armed Attacks.* Cambridge.

Harris, D. (n.d.). *Cases and Materials on International Law.* Thomson. Sweet & Maxwell.

Hensel, H. M. (2008). *THE LEGITIMATE USE OF MILITARY FORCE.* ASHGATE.

Melzer, N. (2011). *Cyberwarfare and International Law.* UNIDIR RESOURCES.

mueller, B. (2014). *The laws of war and cyberspace. On the need for a TreaTy concerning cyber conflict.* London School Of Economics and Political Science.

O'Connell, M., Arimatsu , L., & Wilmshurst , E. (2012). *Cyber Security and International Law.* CHATHAM HOUSE.

Ruys, T. (2010). *Armed Attack and Article 51 of the UN Charter.* Cambridge University Press.

SCHMITT , M. N., & VIHUL, L. (2014). *THE NATURE OF INTERNATIONAL LAW CYBER NORMS .* Tallin: CCDCOE.

Shaw, M. N. (2008). *International Law.* Cambridge.

Simma, B. (1995). *The Charter of the United Nations. A Commentary.* Oxford University Press.

Αρθρογραφία

Albright, D., Brannan, P., & Walrond, C. (2010, Δεκέμβριος 22). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. Ανάκτηση Νοέμβριος 18, 2016, από Institute for Science and International Security: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

Beaumont, C. (2010, Ιανουάριος 12). *Baidu hacked by Iranian Cyber Army*. Ανάκτηση Νοέμβριος 18, 2016, από The Telegraph: http://www.telegraph.co.uk/technology/news/6974129/Baidu-hacked-by-Iranian-Cyber-Army.html

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, Ιανουάριος 15). *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. Ανάκτηση Νοέμβριος 18, 2016, από New York Times: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

(2016). *CHINA AND CYBER: ATTITUDES, STRATEGIES, ORGANISATION.* Tallin: CCDCOE. Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf

Clemente, D. (2010, Σεπτέμβριος 27). *Reality Approaches Hype: Critical National Infrastructure and the Stuxnet Worm*. Ανάκτηση Νοέμβριος 18, 2016, από CHATHAM HOUSE The Royal Institute of International Affairs : https://www.chathamhouse.org/media/comment/view/163865#

Farwell, J. P., & Rohozinski, R. (n.d.). Stuxnet and the Future of Cyber War. Survival. Ανάκτηση Νοέμβριος 18, 2016, από https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf

NATO Review Magazine. (n.d.). Ανάκτηση Νοέμβριος 18, 2016, από Official NATO website: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Segal, A. (2014, Οκτώβριος 14). *The Deepening Divide in U.S.-China Cyber Relations*. Ανάκτηση Νοέμβριος 17, 2016, από The National Interest: http://nationalinterest.org/blog/the-buzz/the-deepening-divide-us-china-cyber-relations-11568

Shakarian, P. (2011, Απρίλιος). *Stuxnet: Cyberwar Revolution in Military Affairs*. Ανάκτηση Νοέμβριος 18, 2016, από Small Wars Journal: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s_eng.pdf

ZILBER, A. (2016, Νοέμβριος 8). *WikiLeaks comes under 'unrelenting' cyber attack that briefly prevents it from releasing more emails linked to Hillary Clinton on Election Day*. Ανάκτηση Νοέμβριος 18, 2016, από DAILYMAIL.COM and ASSOCIATED PRESS: http://www.dailymail.co.uk/news/article-3917996/WikiLeaks-comes-unrelenting-cyber-attacks-briefly-prevented-releasing-emails-linked-Hillary-Clinton-Americans-polls-Election-Day.html

Tsagourias, N., Buchan , R., & Roscini, M. (2014, Οκτώβριος 9). *State Responsibility for Cyber Operations:.* Ανάκτηση Νοέμβριος 20, 2016, από http://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1

Τσαγκουριάς, Ν. (2012). *Cyber Attacks, Self-defence and the Problem of Attribution.* Ανάκτηση από Journal of Conflict & Security Law.

Τσαγκουριάς, Ν. (2015). *The Law Applicable to Countermeasures against Low-Intensity Cyber Operations.* Ανάκτηση από Baltic Yearbook of International Law Online.

Κίνα και Δύση: συγκρούσεις πληκτρολογίων;. (n.d.). Ανάκτηση Νοέμβριος 20, 2016, από Δελτίο ΝΑΤΟ: http://www.nato.int/docu/review/2009/Asia/china_cyber_attacks/GR/index.htm

Πηγές τεκμηρίωσης

(1974). *3314 (XXIX). Definition of Aggression.* General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

(2010, Μάιος). *A Digital Agenda for Europe [COM(2010)245 final].* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Ευρωπαική Επιτροπή. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-100519-DigitalAgenda.pdf

(2010, Οκτώβριος). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* David Cameron, Great Britain and Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

(1965). *A/RES/20/2131. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.* General Assembly of United Nations . Ανάκτηση Νοέμβριος 19, 2016, από http://www.un-documents.net/a20r2131.htm

(1970). *A/RES/25/2625. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.* General Assembly of United Nations. Ανάκτηση Νοέμβριος 19, 2016, από http://www.un-documents.net/a25r2625.htm

(2003, Ιανουάριος). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through*

computer systems. Συμβούλιο της Ευρώπης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/CoE-030128-AdditionalProtocol.pdf

(1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA).* INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf

(1927). *COLLECTION OF JUDGMENTS, THE CASE OF THE S.S. "LOTUS".* PERMANENT COURT OF INTERNATIONAL JUSTICE. Ανάκτηση Νοέμβριος 19, 2016, από http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf

(1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.* International Committee of the Red Cross. Ανάκτηση Νοέμβριος 19, 2016, από http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf

(2012, Οκτώβριος). *Consolidated Version of the Treaty on the Functioning of the European Union (C 326/47).* Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-121026-TFEU.pdf

(2001, Νοέμβριος). *Convention on Cybercrime.* Βουδαπέστη: Συμβούλιο της Ευρώπης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/CoE-011123-ConventiononCybercrime.pdf

(2014). *Critical Terminology Foundations 2 (Russia-U.S. Bilateral on Cybersecurity).* EastWest Institute. Ανάκτηση Νοέμβριος 19, 2016, από https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

(2014, Φεβρουάριος). *Cyber Defence Pact .* Υπουργείο Άμυνας Γαλλίας. Ανάκτηση Νοέμβριος 16, 2016, από http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf

Cyber Definitions. (n.d.). Ανάκτηση Νοέμβριος 19, 2016, από NATO Cooperative Cyber Defence Centre of Excellence, Tallin Esthonia: https://ccdcoe.org/cyber-definitions.html

(2009, Ιούνιος). *Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space.* Λονδίνο: UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από http://ccpic.mai.gov.ro/docs/UK_cyber_security.pdf

(2013, Φεβρουάριος). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [JOIN(2013) 1 final].* JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS , Ευρωπαική Επιτροπή. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-130207-CSS.pdf

(2011). *Défense et sécurité des systèmes d'information. Stratégie de la France.* Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Ανάκτηση Νοέμβριος 15, 2016, από https://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

(2013, Αύγουστος). *DIRECTIVE 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.* Ευρωπαικό Κοινοβούλιο και Συμβούλιο Ευρωπαικής Ένωσης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-130812-AttacksAgainstInformationSystems.pdf

(2014, Νοέμβριος). *EU Cyber Defence Policy Framework.* Συμβούλιο Ευρωπαϊκής Ένωσης. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf

(1975). *FINAL ACT by CONFERENCE ON SECURITY AND CO-OPERATION IN EUROPE .* Helsinki: OSCE. Ανάκτηση Νοέμβριος 14, 2016, από http://www.osce.org/helsinki-final-act?download=true

Hsu, K. a. (2014). *China and International Law in Cyberspace.* Report by the U.S.-China Economic and Security. Ανάκτηση Νοέμβριος 17, 2016, από http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

(2011). *Information systems defence and security, France's strategy.* Ανάκτηση Νοέμβριος 15, 2016, από https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

(2011, Μάιος). *International Strategy for Cyberspace.* Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Jean-Claude, M. (2008). *Défense et Sécurité nationale: le Livre blanc.* Nicolas Sarkozy. Ανάκτηση Νοέμβριος 15, 2016, από http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010, Δεκέμβριος). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Congressional Research Service. Ανάκτηση Νοέμβριος 18, 2016, από http://digital.library.unt.edu/ark:/67531/metadc31393/m1/1/high_res_d/R41524_2010Dec09.pdf

Kissel, R. (2013). *Glossary of Key Information Security Terms (NISTIR 7298, Revision 2).* U.S. Department of Commerce. Ανάκτηση Νοέμβριος 19, 2016, από http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

(1996, Ιούλιος). *LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS.* INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/95/7495.pdf

(2015, Ιανουάριος). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* Γενική Συνέλευση Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

(2010, Νοέμβριος). *Lisbon Summit Declaration.* NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-101120-LisbonSummitDeclaration.pdf

(2013). *Livre blanc: Défense et Sécurité nationale.* Francois Hollande. Ανάκτηση Νοέμβριος 15, 2016, από http://fr.calameo.com/read/000331627d6f04ea4fe0e

National Cyber Security Organisation: France. (n.d.). Τάλλιν Εσθονίας: Κέντρο Αριστείας Κυβερνοάμυνας . Ανάκτηση Νοέμβριος 16, 2016, από https://ccdcoe.org/multimedia/national-cyber-security-organisation-france.html

(2016). *National Cyber Security Organisation: UNITED STATES.* Τάλλιν: Κέντρο Αριστείας Κυβερνοάμυνας. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf

(2016). *NATIONAL CYBER SECURITY STRATEGY 2016-2021.* UK Government. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

(2010, Μάιος). *National Security Strategy.* Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

(2015, Φεβρουάριος). *National Security Strategy.* Ουάσιγκτον: Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

Permanent Representation of France to NATO. (2013). Ανάκτηση Νοέμβριος 15, 2016, από White Paper on Defence and National Security: http://www.rpfrance-otan.org/White-Paper-on-defence-and

(2002, Νοέμβριος). *Prague Summit Declaration.* NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-021121-PragueSummitDeclaration.pdf

Schmitt, M. N. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press. Ανάκτηση Νοέμβριος 18, 2016, από https://ccdcoe.org/tallinn-manual.html

Statement by NATO Secretary General, Lord Robertson. (2001). Ανάκτηση Νοέμβριος 20, 2016, από NATO On-line library: http://www.nato.int/docu/speech/2001/s011002a.htm

(2010, Νοέμβριος). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* NATO. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-101120-StrategicConcept.pdf

(2015, Απρίλιος). *The European Agenda on Security [COM(2015) 185 final].* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Ευρωπαική Επιτροπή. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/EU-150428-EUSecurityAgenda.pdf

(2013, Δεκέμβριος). *The National Cyber Security Strategy Our Forward Plans.* UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από http://www.cyberriskinsuranceforum.com/sites/default/files/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

(2003, Φεβρουάριος). *The National Strategy to Secure Cyberspace.* Λευκός Οίκος Η.Π.Α. Ανάκτηση Νοέμβριος 15, 2016, από https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

(1949). *The North Atlantic Treaty.* Washington D.C.: NATO. Ανάκτηση Νοέμβριος 19, 2016, από http://www.nato.int/cps/en/natohq/official_texts_17120.htm

(2011, Νοέμβριος). *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world.* UK Cabinet Office. Ανάκτηση Νοέμβριος 15, 2016, από https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Tikk, E., Kaska, K., & Vihul, L. (2010). *INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS.* Tallinn Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE). Ανάκτηση Νοέμβριος 17, 2016, από https://ccdcoe.org/publications/books/legalconsiderations.pdf

(2014, Σεπτέμβριος). *Wales Summit Declaration.* NATO. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-140905-WalesSummitDeclaration.pdf

(2016, Ιούλιος). *Warsaw Summit Communiqué.* NATO. Ανάκτηση Νοέμβριος 15, 2016, από https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf

(2013, Δεκέμβριος). *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, Permament Council. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/OSCE-131203-Confidencebuildingmeasures_0.pdf

(2006, Δεκέμβριος). *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

(2004, Δεκέμβριος). *Απόφαση No 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

(2016, Μάρτιος). *Απόφαση No. 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

(2015, Μάρτιος). *Έκθεση για το "Δικαίωμα στην Ιδιωτικότητα στην Ψηφιακή Εποχή" (A/HRC/28/L.27).* Συμβούλιο για τα Ανθρώπινα Δικαιώματα. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-150324-SpecialRapporteurOnTheRightToPrivacy.pdf

(2014, Ιούνιος). *Έκθεση για το "Δικαίωμα της Ιδιωτικότητας στην Ψηφιακή Εποχή" (A/HRC/27/37).* Γραφείο Ύπατου Αρμοστή των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-140730-RightToPrivacyReport.pdf

(2015, Ιούλιος). *Έκθεση προόδου (A/70/174).* Ομάδα Κυβερνητικών Εμπειρογνωμόνων στον τομέα της Πληροφορίας και των Τηλεπικοινωνιών στο πλαίσιο της Διεθνούς Ασφάλειας. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

(2016, Ιούλιος). *Ενημερωτικό Δελτίο.* Γραφείο για ζητήματα Αφοπλισμών των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 20, 2016, από https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/07/Information-Security-Fact-Sheet-July2016.pdf

(2012). *ΕΝΟΠΟΙΗΜΕΝΗ ΑΠΟΔΟΣΗ ΤΗΣ ΣΥΝΘΗΚΗΣ ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ.* Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Ανάκτηση Νοέμβριος 19, 2016, από http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:12012E/TXT&from=el

(2016). *Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.* Επίσημη Εφημερίδα της Ευρωπαϊκής

Ένωσης. Ανάκτηση Νοέμβριος 20, 2016, από http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EL

Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (ΚΕΠΠΑ). (n.d.). Ανάκτηση Νοέμβριος 20, 2016, από ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ, Υπουργείο Εξωτερικών: http://www.mfa.gr/exoteriki-politiki/i-ellada-stin-ee/keppa.html

(1945). *Χάρτης των Ηνωμένων Εθνών.* Σαν Φραντζίσκο: Ηνωμένα Έθνη. Ανάκτηση Νοέμβριος 18, 2016, από https://treaties.un.org/doc/publication/ctc/uncharter.pdf

(1999). *Ψήφισμα A/RES/53/70.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf

(2003, Ιανουάριος). *Ψήφισμα A/RES/57/239.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-021220-CultureOfCS.pdf

(2004, Ιανουάριος). *Ψήφισμα A/RES/58/199.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-031223-CultureOfCandCI.pdf

(2010, Μάρτιος). *Ψήφισμα A/RES/64/211.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf

(2015, Δεκέμβριος). *Ψήφισμα A/RES/70/237.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-151223-ITIS.pdf

(2013). *Ψήφισμα A/68/98.* Γενική Συνέλευση Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

(2002). *Ψήφισμα A/RES/56/19.* Γενική Συνέλευση των Ηνωμένων Εθνών. Ανάκτηση Νοέμβριος 14, 2016, από https://ccdcoe.org/sites/default/files/documents/UN-011129-ITIS.pdf

Επιπρόσθετη Βιβλιο/αρθρογραφία

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.

Citron, D. K. (2009). *LAW'S EXPRESSIVE VALUE IN COMBATING CYBER GENDER HARASSMENT.* Retrieved from MICHIGAN LAW REVIEW (JSTOR).

Clopton , Z. D. (2016). *Territoriality, Technology, and National Security.* Retrieved from The University of Chicago Law Review .

Crook , J. R. (2013). *CONTEMPORARY PRACTICE OF THE UNITED STATES RELATING TO INTERNATIONAL LAW.* Retrieved from The American Journal of International Law .

Cyber warfare and international humanitarian law: The ICRC's position. (2013). Retrieved from ICRC.

Gervais, M. (2012). *Cyber Attacks and the Laws of War.* Retrieved from BERKELEY JOURNAL OF INTERNATIONAL LAW .

Graham, D. (2010). *Cyber Threats and the Law of War.* Retrieved from JOURNAL OF NATIONAL SECURITY LAW & POLICY .

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). *THE LAW OF CYBER-ATTACK.* Retrieved from California Law Revie.

HEINTSCHEL , W., & HEINEGG , V. (2015). *INTERNATIONAL LAW AND INTERNATIONAL INFORMATION SECURITY: A RESPONSE TO KRUTSKIKH AND STRELTSOV.* Retrieved from CCDCOE.

Hollis, D. B. (2011). *An e-SOS for Cyberspace.* Retrieved from Harvard International Law Journal .

Jackson, S. (2016). *NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack.* Retrieved from George Mason University .

Kanuck, S. (2010). *Sovereign Discourse on Cyber Conflict Under International Law.* Retrieved from Texas Law Review .

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.

LEWIS , J. A. (2015). *THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE.* Retrieved from CCDCOE.

NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. (2016, Ιούλιος 21). Retrieved from CCDCOE: https://ccdcoe.org/nato-recognises--cyberspace-domain-operations-warsaw-summit.html

Pihelgas , M. (n.d.). *Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks.* Retrieved from CCDCOE.

Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers. (2016, Ιούνιος 14). Retrieved Νοέμβριος 18, 2016, from NATO Official Web Page: http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en#top

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 .

RICHARDSON, J. (2011). *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield.* Retrieved from JOURNAL OF COMPUTER & INFORMATION LAW .

Roberts , S. (2014). *CYBER WARS: APPLYING CONVENTIONAL LAWS OF WAR TO CYBER WARFARE AND NON-STATE ACTORS.* Retrieved from NORTHERN KENTUCKY LAW REVIEW .

Rossini, M. (2010). *World Wide Warfare - Jus ad bellum and the use of Cyber Force.* Retrieved from Max Planck UNYB.

Schmitt , M. N. (2002). *Wired warfare: Computer network attack and jus in bello.* Retrieved from IRRC.

Schmitt , M. N., & vihul, l. (2014). *Proxy wars in cyberspace: The Evolving International Law of Attribution.* Retrieved from Fletcher Security review .

Schmitt, M. N. (2014). *THE LAW OF CYBER WARFARE: QUO VADIS?* Retrieved from STANFORD LAW & POLICY REVIEW .

Siers, R. (2014). *NORTH KOREA: THE CYBER WILD CARD.* 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.

Watts , S. (2012). *The Notion of Combatancy in Cyber Warfare.* Retrieved from CCDCOE.

Advisory Opinion of 11 April 1949 on Reparation for Injuries Suffered in the Service of the United Nations. (1949, Απρίλιος 11). Ανάκτηση Ιανουάριος 31, 2017, από http://www.icj-cij.org/docket/files/4/1835.pdf

Ambos, K. (2016, Αύγουστος 7). *Individual Criminal Responsibility for Cyber Aggression.* Ανάκτηση από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

Anzilotti, D. (1929). Cours de droit international.

Buchan, R., & Tsagourias, N. (2016, Οκτωβρίου 19). *Journal of Conflict & Security Law.* Ανάκτηση Ιανουάριος 21, 2017, από Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence.

(1986). *CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA).* INTERNATIONAL COURT OF JUSTICE. Ανάκτηση Νοέμβριος 18, 2016, από http://www.icj-cij.org/docket/files/70/6503.pdf

Convention on Rights and Duties of States adopted by the Seventh International Conference of American States. (1933, Δεκεμβρίου 26). Ανάκτηση Ιανουάριος 31, 2017, από https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf

Crawford, J. (2014). *State Responsibility: The General Part.* Cambridge University Press.

Elements of Crimes, International Criminal Court. (2011). Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf

Israeli Test on Worm Called Crucial in Iran Nuclear Delay. (2011, Ιανουάριος 15). Ανάκτηση Ιανουάριος 29, 2017, από The New York Times: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?smid=pl-share

Klimburg, A. (2011). Mobilising Cyber Power. Στο A. Klimburg, *Cyber Threats.* Survival. Ανάκτηση Ιανουάριος 29, 2017, από http://users.clas.ufl.edu/zselden/coursereading2011/klimcyber.pdf

Macak, K. (2016, Σεπτέμβριος 25). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors.* Ανάκτηση Ιανουάριος 06, 2017, από Journal of Conflict & Security Law: http://jcsl.oxfordjournals.org/

(2012). *MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS (ST/LEG/SER.B/25).* Ανάκτηση Ιανουάριος 28, 2017, από http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

Obama Order Sped Up Wave of Cyberattacks Against Iran. (2012, Ιούνιος 1). Ανάκτηση Ιανουάριος 29, 2017, από The New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?smid=pl-share

(2006). *Oral Proceedings, Bosnian Genocide case, ICJ, CR 2006/8.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/91/10600.pdf

Prosecutor v Bemba (Judgment) ICC-01/05-01/08. (2016, Μάρτιος 21). Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/CourtRecords/CR2016_02238.PDF

Prosecutor v Blaskic (Judgment) IT-95-14-A. (2004, Ιούλιος 29). Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/blaskic/acjug/en/bla-aj040729e.pdf

Prosecutor v Hadzihasanovic, Alagic and Kubura. (2003, Ιούλιος 16). Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/hadzihasanovic_kubura/acdec/en/030716.htm

RAND Report titled "Ungoverned territories: Understanding and Reducing Terrorism Risks". (2007). Ανάκτηση Ιανουάριος 31, 2017, από http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.pdf

Saporito, L., & Lewis, J. A. (2014, Μαρτίου 13). *Cyber Incidents Attributed to China.* Ανάκτηση Ιανουάριος 29, 2017, από Center for Strategic and International Studies: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130314_Chinese_hacking.pdf

Sliedregt, E. v. (2016, Σεπτέμβριος 22). *Command Responsibility and Cyberattacks.* Ανάκτηση Ιανουάριος 31, 2017, από http://jcsl.oxfordjournals.org/

The United States of America vs. Wilhelm von Leeb et al. (HIGH COMMAND TRIAL). (1948, Οκτώβριος 27). Ανάκτηση Ιανουάριος 31, 2017, από http://werle.rewi.hu-berlin.de/High%20Command%20Case.pdf

Tonkin, H. (2011). *State Control over Private Military and Security Companies in Armed Conflict.*

Trial of Major War Criminals before the International Military Tribunal, Vol. 22. (1948). Ανάκτηση Ιανουάριος 31, 2017, από https://www.loc.gov/rr/frd/Military_Law/pdf/NT_Vol-XXII.pdf

Tsagourias, N. (2016). *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts.* Ανάκτηση Ιανουάριος 31, 2017, από Journal of Conflict & Security Law : http://jcsl.oxfordjournals.org/

U.S. Cyberattacks Target ISI in a New Line of Combat. . (2016, Απριλίου 24). Ανάκτηση Ιανουάριος 31, 2017, από The New York Times: https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=1

UNHRC 'Report of the independent international commission of inquiry on the Syrian Arab Republic, A/HRC/19/69. (2012, Φεβρουάριος 22). Ανάκτηση Ιανουάριος 31, 2017, από http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session19/A-HRC-19-69_en.pdf

US v Krupp et al (Krupp case), US Military Tribunal, Case No. 58. . (1947-1948). Ανάκτηση Ιανουάριος 31, 2017, από https://www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-10.pdf

(2013). *Απόφαση Διαρκούς Ποινικού Δικαστηρίου για την πρώην Γιουγκοσλαβία στην υπόθεση Prosecutor v Prlic (Trial Judgement), IT-04-74-T.* Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/prlic/tjug/en/130529-1.pdf

(2007). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση της εφαρμογής της Σύμβασης για την πρόληψη και τιμωρία του εγκλήματος της γενοκτονίας, Βοσνία και Ερζεγοβίνη κατά Σερβίας και Μαυροβουνίου.* Ανάκτηση Ιανουάριος 29, 2017, από http://www.icj-cij.org/docket/files/91/13685.pdf

(1980). *Απόφαση Διεθνούς Δικαστηρίου στην υπόθεση "Όμηροι Τεχεράνης (Διπλωματικό και Προξενικό Σώμα στην Τεχεράνη)", Η.Π.Α./Ιράν.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/64/6291.pdf

(2005). *Απόφαση Διεθνούς Δικαστηρίου στην Υπόθεση Ένοπλων Δραστηριοτήτων στο έδαφος του Κονγκό (DRC v Ουγκάντα).* Ανάκτηση Ιανουάριος 30, 2017, από http://www.icj-cij.org/docket/files/116/10455.pdf

(1999). *Απόφαση Εφετείου Διεθνούς Ποινικού Δικαστηρίου για την πρώην Γιογκοσλαβία στην υπόθεση Prosecutor v Tadic, IT-94-1-A.* Ανάκτηση Ιανουάριος 31, 2017, από http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

(1949). *Απόφαση στην υπόθεση Corfu Channel (Merits), Ηνωμένο Βασίλειο/Αλβανία, Διεθνές Δικαστήριο.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/1/1645.pdf

(1997). *Απόφαση στην υπόθεση Gabčíkovo-Nagymaros Project, Ουγγαρία/Σλοβακία, Διεθνές Δικαστήριο.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/docket/files/92/7375.pdf

(1938). *Απόφαση στην υπόθεση Phosphates in Morocco, Ιταλία/Γαλλία , No 74, Series A/B, Διαρκές Δικαστήριο Διεθνούς Δικαιοσύνης.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/pcij/serie_AB/AB_74/01_Phosphates_du_Maroc_Arret.pdf

(1923). *Γνωμοδότηση Διαρκούς Δικαστηρίου Διεθνούς Δικαιοσύνης περί Γερμανών αποίκων στην Πολωνία.* Ανάκτηση Ιανουάριος 28, 2017, από http://www.icj-cij.org/pcij/serie_B/B_06/Colons_allemands_en_Pologne_Avis_consultatif.pdf

(1928). *Διαιτητική απόφαση στην υπόθεση Island of Palmas (Netherlands v U.S.A.),.* Ανάκτηση Ιανουάριος 31, 2017, από http://legal.un.org/riaa/cases/vol_II/829-871.pdf

(1929). *Διαιτητική Απόφαση της Γενικής Επιτροπής Αποζημιώσεων Γαλλίας-Μεξικού στην υπόθεση του Jean-Baptiste Caire.* Ανάκτηση Ιανουάριος 29, 2017, από http://legal.un.org/docs/?path=../riaa/cases/vol_V/516-534_Caire.pdf&lang=E

(1927). *Διαιτητική Απόφαση της Γενικής Επιτροπής Αποζημιώσεων Μεξικό-Η.Π.Α. στην υπόθεση Francisco Mallen.* Ανάκτηση Ιανουάριος 29, 2017, από http://legal.un.org/riaa/cases/vol_IV/173-190.pdf

Καταστατικό Διεθνούς Ποινικού Δικαστηρίου. (1998, Ιούλιος 17). Ανάκτηση Ιανουάριος 31, 2017, από https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf

Πρόσθετο Πρωτόκολλο ΙΙ στη Σύμβαση της Γενεύης του 1949. (1977, Ιούνιος 8). Ανάκτηση Ιανουάριος 31, 2017, από https://treaties.un.org/doc/publication/unts/volume%201125/volume-1125-i-17513-english.pdf

Πρώτο Πρόσθετο Πρωτόκολλο στη Συνθήκη της Γενεύης (1949). (1977, Ιούνιος 8). Ανάκτηση Ιανουάριος 31, 2017, από https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf

(1948). *Σύμβαση για την Πρόληψη καιι Τιμωρία του εγκλήματος της Γενοκτονίας, που υιοθετήθηκε απο τη Γενική Συνέλευση των Ηνωμένων Εθνών.* Ανάκτηση Ιανουάριος 28, 2017, από https://treaties.un.org/doc/publication/unts/volume%2078/volume-78-i-1021-english.pdf

(2002). *Ψήφισμα A/RES/56/83 Γενικής Συνέλευσης Ηνωμένων Εθνών.* Ανάκτηση Ιανουάριος 21, 2017, από http://www.un.org/ga/search/view_doc.asp?symbol=A/res/56/83