ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΕΥΡΩΠΑΙΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΕΘΝΕΣ ΔΙΚΑΙΟ ΚΑΙ ΔΙΠΛΩΜΑΤΙΚΕΣ ΣΠΟΥΔΕΣ

Η Τεχνητή Νοημοσύνη συναντά τον Κυβερνοχώρο. Αυτόματη Κυβερνοάμυνα και *jus ad bellum*

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αποστόλου Γεώργιος

Αθήνα, 2018

Τριμελής Επιτροπή:

Μαρούδα Μαρία-Ντανιέλα, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου (Επιβλέπουσα)
Περράκης Στέλιος, Ομότιμος Καθηγητής Παντείου Πανεπιστημίου
Τσαγγούριας Νικόλας, Καθηγητής Πανεπιστημίου Sheffield

Ευχαριστίες

Θερμές ευχαριστίες στην καθηγήτρια Ντ. Μαρούδα και στον ομότιμο καθηγητή Στ. Περράκη για την πολυετή συνεργασία μας. Ιδιαιτέρως, θα ήθελα να ευχαριστήσω και τον καθηγητή Ν. Τσαγγούρια για την πολύτιμη καθοδήγηση που μου προσέφερε στην εκπόνηση της παρούσας διπλωματικής εργασίας.

Περιεχόμενα

Περίληψη

Η λειτουργία της αυτόματης κυβερνοάμυνας αποσκοπεί στην εξουδετέρωση μια κυβερνοεπίθεσης. Από τη στιγμή που ένα ηλεκτρονικό σύστημα ανιχνεύσει μια κυβερνοεπίθεση, η αυτόματη απάντηση μπορεί να στοχεύει όχι μόνο στην αποτροπή της αλλά και στη δράση μέσα στο δίκτυο του επιτιθέμενου, προκειμένου να καταστήσει ανενεργό το λογισμικό που την παράγει και ταυτοχρόνως να ανακτήσει τυχών κλεμμένα δεδομένα. Σκοπός, της παρούσας διπλωματικής εργασίας, είναι να εξετάσει τη νομιμότητα της αυτόματης κυβερνοάμυνας, υπό το πρίσμα των κανόνων της χρήσης βίας στο διεθνές δίκαιο (*jus ad bellum*).

Στο πρώτο μέρος της εργασίας, αναλύεται η έννοια της κυβερνοεπίθεσης μέσα από την αναλογική ερμηνεία της παραδοσιακής επίθεσης στον κινητικό χώρο, όπως αυτή έχει διαμορφωθεί από τη διεθνή νομολογία και την πρακτική κρατών και οργανισμών. Στη συνέχεια, θα εξεταστεί το ζήτημα της απόδοσης της ευθύνης για μια κυβερνοεπίθεση, καθώς η ανωνυμία των χρηστών στο διαδίκτυο καθιστούν τη διαδικασία αυτή, κατά το διεθνές δίκαιο, συχνά προβληματική. Στο δεύτερο μέρος, αναλύεται η νομιμότητα της αυτόματης κυβερνοάμυνας κατά μιας «ένοπλης» κυβερνοεπίθεσης, βάσει των αρχών της αναγκαιότητας, αναλογικότητας και αμεσότητας. Τέλος, εξετάζεται το ζήτημα της αυτόματης κυβερνοάμυνας κατά μιας επικείμενης κυβερνοεπίθεσης όπως και κατά μη κρατικών δρώντων (ΜΚΔ), σε περίπτωση που αυτό κρίνεται απαραίτητο για την αποφυγή δυσμενών συνεπειών.

Η μεθοδολογία της εργασίας βασίστηκε στην μελέτη και ανάλυση πρωτογενών και δευτερογενών πηγών, στη νομολογία του Διεθνούς Δικαστηρίου και άλλων διεθνών δικαιοδοτικών οργάνων, σε ψηφίσματα και αποφάσεις των οργάνων των Ηνωμένων Εθνών καθώς και στην πρακτική κρατών και οργανισμών.

Λέξεις κλειδιά: κυβερνοεπίθεση, αυτόματη κυβερνοάμυνα, αναγκαιότητα, αναλογικότητα, επικείμενη κυβερνοεπίθεση, μη κρατικοί δρώντες

Artificial Intelligence meets cyberspace. Automatic cyber defence and jus ad bellum.

Author: Apostolou Georgios

ABSTRACT

The function of the automatic cyber defense is to confront a cyber-attack. Once an electronic system detects a cyber attack, the automatic response intends not only to prevent it, but also to take action within the attacker's network in order to inactivate the software that produces it and at the same time to recover the stolen data. The purpose of this thesis is to examine the legality of the automatic cyber defense, in the light of the rules of the use of force in international law (*jus ad bellum*).

In the first part of the thesis, I examine the concept of cyber attack through an analysis of the traditional attack in the kinetic world and as it has been shaped by the international jurisprudence and the practice of states and organizations. At the same time, I will examine the issue of accountability for a cyber attack, as the anonymity of internet users makes the process particularly difficult in the context of international law. In the second part, I analyze the legality of an automatic cyber defense against an "armed" cyber attack, based on the principles of necessity, proportionality and immediacy. Finally, I examine the issue of the cyber defense against an imminent cyber attack as well as against the cyber attack of non-state actors (NCAs), if this is necessary for a State in order to avoid serious consequences.

The methodology of this thesis was based upon the study and the analysis of both primary and secondary sources, the jurisprudence of the International Court of Justice and of other tribunals, resolutions of the United Nations, as well as practice of States and other organizations.

Key words: cyberspace, automatic cyber defence, cyber-attack, necessity, proportionality, immediacy, imminent cyber-attack, non-state actors.

Εισαγωγή

Η σημερινή τεχνολογική εποχή, έχει δημιουργήσει με την πάροδο των χρόνων ένα αλληλεξαρτώμενο πλέγμα ηλεκτρονικών δικτύων, μέσω της χρήσης υπολογιστών, ρυθμίζοντας τις ανάγκες των σύγχρονων κοινωνιών, σε κάθε τομέα. Για παράδειγμα, σε νοσοκομεία και επιχειρήσεις ακόμα και από χρηματοπιστωτικά ιδρύματα έως πυρηνικά εργοστάσια, το διαδίκτυο καθώς και τα επιμέρους περιφερειακά ηλεκτρονικά δίκτυα, διαδραματίζουν σημαντικό και αναγκαίο ρόλο σε επίπεδο οργάνωσης και ανταλλαγής πληροφοριών. Ο αριθμός των χρηστών του διαδικτύου αυξάνεται σταθερά κάθε χρόνο παγκοσμίως, γεγονός που αναδεικνύει ότι αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας στο κοινωνικό σύνολο.[1]

Παράλληλα, το ευρύτερο φάσμα του λεγόμενου κυβερνοχώρου, που διαμορφώνεται από την αλληλεπίδραση όλων αυτών των δικτύων, έχει δώσει τη δυνατότητα σε χρήστες να διεξάγουν παράνομες και εχθρικές δραστηριότητες μέσα σε αυτό, εκμεταλλευόμενοι, συνήθως, τα κενά ασφαλείας του διαδικτύου. Αυτές οι ενέργειες, αναφέρονται κυρίως ως κυβερνοεπιχειρήσεις ή κυβερνοεπιθέσεις. Ενδεικτικά, τέτοιες παράνομες πράξεις μπορεί να σχετίζονται με μια απλή υποκλοπή δεδομένων έως και μια πιθανή καταστροφή στις υποδομές ενός πυρηνικού εργοστασίου, όπως στην περίπτωση του πυρηνικού προγράμματος του Ιράν.[2]

Οι τρόποι που χρησιμοποιούνται για την αποδυνάμωση και την παραβίαση ενός δικτύου, μπορεί να είναι μέσω είτε της φθοράς του υλικού ('chipping' hardware) είτε του λογισμικού (software) ενός ηλεκτρονικού υπολογιστή.[3] Ακόμη, υπάρχει και η περίπτωση, κάποιος να «πλημμυρίζει» έναν ιστότοπο, μέσω της αποστολής υπερβολικού όγκου δεδομένων, αποσκοπώντας να τον καταστήσει αδύναμο να δεχτεί άλλες συνδέσεις και επομένως να μην μπορεί να εξυπηρετεί τους χρήστες του

---

[1] Για παράδειγμα, οι χρήστες τον Ιούνιο του 2018 ανέρχονταν σε 4.208.571.287 επί του παγκοσμίου πληθυσμού. Βλέπε: Internet World Stats, 'Usage and Population Statics' (30 June 2018) at: <https://www.internetworldstats.com/stats.htm> accessed 19.12.2018

[2] Για την περίπτωση της αποκάλυψης του ιού Stuxnet, το 2010, στο πυρηνικό πρόγραμμα του Ιράν βλέπε: D Kushner, 'The Real Story of Stuxnet', *IEEE Spectrum*, (26 February 2013) at: <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/> accessed 19.12.2018

[3] Η μέθοδος 'chipping' περιλαμβάνει την ενσωμάτωση μικροσκοπικών «τσιπ» στο υλικό (hardware) υπολογιστών, ώστε να δημιουργηθούν με αυτόν τον τρόπο, αδυναμίες ή ατέλειες στους σχετιζόμενους υπολογιστές και στα ηλεκτρονικά δίκτυα αυτών. Επίσης, η ανίχνευση τέτοιων «τσιπ» καθίσταται ιδιαίτερα δύσκολη. W Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994) 161-5. Πρόσφατα, Αμερικανοί αξιωματούχοι ισχυρίστηκαν ότι Κινέζοι έχουν τοποθετήσει τέτοιου είδους μικροσκοπικά «τσιπ» σε τεχνολογικά υλικά, σημαντικών αμερικανικών εταιριών που δραστηριοποιούνται στην Κίνα, μεταξύ των οποίων η Apple και η Amazon. Αυτό, κατά τα λεγόμενά τους, συνιστά απειλή κατά των Ηνωμένων Πολιτειών στον κυβερνοχώρο. T Olorunnipa and B House, 'Chip Hack a Sign of Chinese Cyber Threats to US., Official Say', *Bloomberg*, (4 October 2018) at: <https://www.bloomberg.com/news/articles/2018-10-04/chip-hack-a-sign-of-chinese-cyber-threats-to-u-s-officials-say> accessed 19.12.2018

διαδικτύου.[4] Η τελευταία μέθοδος είναι γνωστή ως 'denial of service' ('DoS') όταν προέρχεται από έναν υπολογιστή, ενώ όταν πηγάζει από περισσοτέρους, ονομάζεται 'distributed denial of service' ('DDoS'). Συχνά, μια επίθεση 'DDoS', διεξάγεται χωρίς να γίνεται αντιληπτή από τους χρήστες των ηλεκτρονικών υπολογιστών μέσω των οποίων πραγματοποιείται η κυβερνοεπίθεση. Χαρακτηριστικό παράδειγμα, είναι η περίπτωση της Εσθονίας το 2007, όπου μαζικές κυβερνοεπιθέσεις τύπου 'DDoS' μπλόκαραν δεκάδες ιστότοπους, κυβερνητικούς και μη, μεταξύ των οποίων, του κοινοβουλίου, τραπεζικών ιδρυμάτων, εφημερίδων, τηλεοπτικών δικτύων και άλλων.[5] Όσον αφορά το λογισμικό (software), υπάρχουν προγράμματα και εργαλεία που έχουν τη δυνατότητα να προκαλέσουν ζημιά μέσα σε ένα ηλεκτρονικό σύστημα ή δίκτυο. Τέτοια εργαλεία είναι, οι δούρειοι ίπποι ('trojan horses'), οι λογικές βόμβες ('logic bombs'), οι ιοί ('viruses'), τα λεγόμενα «σκουλήκια» ('worms'), καθώς και τα 'bots', τα οποία μπορούν να εγκατασταθούν σε έναν υπολογιστή ακόμη και με ένα απλό e-mail.[6]

Από τη στιγμή που μια κυβερνοεπίθεση μπορεί να επιφέρει έως και πολύ σοβαρές επιπτώσεις, είναι αναμενόμενο να μελετηθεί, αναλογικά, υπό την οπτική του διεθνούς δικαίου κατά το *jus ad bellum*, δεδομένου ότι δεν υπάρχει μια διεθνής συνθήκη που να ρυθμίζει ζητήματα χρήσης βίας στον κυβερνοχώρο. Συγκεκριμένα, τίθενται σημαντικά ερωτήματα όπως, εάν και ποιες κυβερνοεπιθέσεις μπορούν να θεωρηθούν ως χρήση βίας, υπό την έννοια της απαγόρευσης από τον Χάρτη των Ηνωμένων Εθνών, καθώς και ποιες από αυτές μπορούν να ενεργοποιήσουν το δικαίωμα στη νόμιμη άμυνα.[7]

Είναι γεγονός, ότι την εποχή που θεσπίστηκε ο Χάρτης δεν υπήρχε η έννοια του διαδικτύου και του κυβερνοχώρου. Ο άμεσος σκοπός του Χάρτη, αμέσως μετά το τέλος του Β' Παγκοσμίου, ήταν η αποφυγή της επανάληψης ενός ακόμα αιματηρού πολέμου.[8] Το πρωταρχικό ερώτημα που ανακύπτει είναι εάν ο Χάρτης μπορεί να έχει αναλογική εφαρμογή σε νέους τομείς, όπως αυτός του κυβερνοχώρου. Αρχικά, η

---

[4] Norton, 'Emerging Threats; DoS Attacks Explained' at: <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html> accessed 19.12.2018

[5] D McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News*, (27 April 2017) at: <https://www.bbc.com/news/39655415> accessed 19.12.2018

[6] Περιληπτικά, για την κάθε περίπτωση ξεχωριστά βλέπε στο CISCO, 'What is the Difference: Viruses, Worms, Trojans, and, Bots?', (14 June 2018) at: <https://www.cisco.com/c/en/us/about/security-center/virus-differences.html> accessed 19.12.2018. SPAMLAWS, 'Logic Bombs and How They Are Used', at: <https://www.spamlaws.com/how-logic-bombs-work.html> accessed 19.12.2018

[7] Charter of the United Nations (26 June 1945), 1 UNTS XVI.

[8] Στο προοίμιο, αναφέρεται συγκεκριμένα: «*Εμείς οι λαοί των Ηνωμένων Εθνών είμαστε αποφασισμένοι να σώσουμε τις ερχόμενες γενεές από τη μάστιγα του πολέμου*».

διεθνής νομολογία έχει αφήσει να εννοηθεί ότι οι κανόνες μιας σύμβασης μπορεί να έχουν μια πιο δυναμική και εξελεγκτική ερμηνεία, ανάλογα των περιστάσεων. Συγκεκριμένα, το Διεθνές Δικαστήριο στην *Υπόθεση Σχετικά με τα Δικαιώματα Πλοήγησης*, της Κόστα Ρίκα κατά της Νικαράγουα, υποστήριξε ότι «*όπου τα συμβαλλόμενα μέρη έχουν χρησιμοποιήσει γενικούς όρους σε μια συνθήκη* [...] (αυτοί) *πρέπει να θεωρηθούν, κατά γενικό κανόνα, ότι οι εν λόγω όροι έχουν σκοπό να έχουν μια εξελισσόμενη σημασία*».[9] Επιπλέον, στη *Γνωμοδότηση για τη Ναμίμπια*, το Δικαστήριο ερμήνευσε ότι «*μία διεθνής συνθήκη θα πρέπει να ερμηνεύεται και να εφαρμόζεται στο πλαίσιο ολόκληρου του νομικού συστήματος που επικρατεί κατά το χρόνο της ερμηνείας*».[10] Παράλληλα, σύμφωνα με τη Σύμβαση της Βιέννης για το Δίκαιο των Συνθηκών, μια συνθήκη, εκτός από το ίδιο της το περιεχόμενο, ερμηνεύεται και από κάθε μεταγενέστερη πρακτική εφαρμογή, από τα μέρη της,[11] όπως για παράδειγμα μέσα από έγγραφα, συμφωνίες, και άλλες δράσεις ή συμπεριφορές, οι οποίες δίνουν ένα συγκεκριμένο νόημα στη συνθήκη.[12] Με βάση τα προαναφερθέντα, μια αναλογική ερμηνεία του Χάρτη στο σύγχρονο πεδίο του κυβερνοχώρου, φαίνεται να είναι συμβατή με το διεθνές δίκαιο, γεγονός που έχει επιβεβαιώσει και ο πρώην Γενικός Γραμματέας των Ηνωμένων Εθνών, Kofi Annan, χαρακτηρίζοντάς τον ως ένα «ζωντανό» κείμενο υψηλών αρχών.[13] Παράλληλα, η πιο ευρέως αποδεκτή προσέγγιση στη μελέτη της χρήσης βίας στον κυβερνοχώρο, είναι αυτή βάσει των αποτελεσμάτων που μια κυβερνοεπίθεση επιφέρει, ώστε να μπορεί να επιχειρηθεί μια αναλογική προσέγγιση και οριοθέτηση του πλαισίου σε σχέση με τα αντίστοιχα αποτελέσματα της χρήσης βίας στον κινητικό χώρο.[14]

Στην παρούσα εργασία, θα μελετηθούν οι έννοιες της κυβερνοεπίθεσης και της κυβερνοάμυνας όπως αυτές αναλογικά θα μπορούσαν να ερμηνευτούν, βάσει των κανόνων χρήσης βίας και του Χάρτη των Ηνωμένων Εθνών. Ωστόσο, από τη στιγμή

---

[9] *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (Judgment) [2009] ICJ Rep 2009, para 66.

[10] *Legal Consequences for States of the Continued Presence of South Africa in Namibia* (South West Africa) *notwithstanding Security Council Resolution 276 (1970)* (Advisory Opinion) [1971] ICJ Rep 1971, para 53.

[11] Article 31(3)(b) of Vienna Convention on the Law of Treaties of 1969. United Nations, *Treaty Series*, (1980) Vol 1155, pp 331 ff.

[12] M Roscini, 'Cyber Operations as a Use of Force'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015), 246.

[13] K Annan, 'Secretary-General presents Annual Report to General Assembly', United Nations Press Release SG/SM/7136-GA/9596 (20 September 1999).

[14] Κατά τον Roscini, η αναλογική προσέγγιση με βάσει είτε τα μέσα διεξαγωγής μιας κυβερνοεπίθεσης είτε του στόχου αυτής, είναι ελλιπείς. Βλέπε περισσότερα στο: M Roscini, *Cyber Operations and the Use of Force in International Law*, (Oxford: Oxford University Press, 2014) 46-7.

που ο κυβερνοχώρος είναι απόρροια της τεχνολογικής προόδου, οι νέες εξελίξεις στον τεχνολογικό τομέα φέρνουν και επιμέρους προκλήσεις, όπως για παράδειγμα μέσω της ανάπτυξης της τεχνητής νοημοσύνης και των δυνατοτήτων 'machine learning'. Αυτόματες διαδικασίες σε ζητήματα κυβερνοασφάλειας χωρίς την επίδραση την επίδραση του ανθρωπίνου παράγοντα, δημιουργούν και ορισμένα νομικά ερωτήματα.

Η κύρια προβληματική στην παρούσα μελέτη, είναι κατά πόσο μπορεί να είναι εφικτή, η διαμόρφωση μιας αυτόματης κυβερνοάμυνας, στη λογική του Άρθρο 51 του Χάρτη, η οποία να είναι, ταυτοχρόνως, συμβατή με τα κριτήρια της αναγκαιότητας, της αναλογικότητας και της αμεσότητας που θέτει το διεθνές δίκαιο. Επομένως, μπορεί η επίδραση της τεχνητής νοημοσύνης στον κυβερνοχώρο μέσω αυτόματων διαδικασιών, χωρίς τον ανθρώπινο έλεγχο, να οδηγήσει σε τυχών παρερμηνείες του διεθνούς δικαίου κατά το *jus ad bellum*; Προκειμένου να απαντηθεί το ερώτημα αυτό, η παρούσα εργασία έχει χωριστεί σε δύο μέρη. Στο πρώτο μέρος, θα μελετηθούν βασικά χαρακτηριστικά του κυβερνοχώρου και η εφαρμογή του διεθνούς δικαίου σε αυτό το πεδίο, ενώ στη συνέχεια θα παρουσιαστεί ο ρόλος της τεχνητής νοημοσύνης και η συμβολή της σε θέματα κυβερνοασφάλειας. Προτού, όμως αναλυθεί η νόμιμη κυβερνοάμυνα, θα πρέπει πρώτα να μελετηθεί η έννοια της κυβερνοεπίθεσης, καθώς αυτή, πρέπει να προηγηθεί, προκειμένου να πυροδοτηθεί το δικαίωμα σε μια απάντηση. Επομένως, στη συνέχεια του πρώτου μέρους, θα οριοθετηθεί η έννοια της κυβερνοεπίθεσης, όπως αυτή αναλογικά ερμηνεύεται στο διεθνές δίκαιο κατά το *jus ad bellum*. Ωστόσο, ένα προβληματικό ζήτημα στον κυβερνοχώρο, είναι αυτό της απόδοσης της ευθύνης για μια κυβερνοεπίθεση προς ένα άλλο κράτος, λόγω των ιδιαιτεροτήτων που πεδίου αυτού, όπως για παράδειγμα της ανωνυμίας των χρηστών. Για αυτό το λόγο θα μελετηθούν, αρχικά, τα κριτήρια απόδοσης της ευθύνης για μια πράξη σε ένα κράτος κατά το διεθνές δίκαιο και, έπειτα, θα αξιολογηθεί κατά πόσο η χρήση της τεχνητής νοημοσύνης, αφού πρώτα αναγνωρίσει μια κυβερνοεπίθεση, μπορεί να συμβάλει στη διαδικασία απόδοσής της. Στο δεύτερο μέρος της παρούσα μελέτης, το κύριο ζητούμενο είναι η ανάλυση της αυτόματης κυβερνοάμυνας βάσει του Άρθρου 51 του Χάρτη. Θα πρέπει να σημειωθεί ότι η έννοια της κυβερνοάμυνας έχει δύο εκδοχές. Μπορεί να είναι είτε παθητική είτε ενεργητική. Σε παθητικό επίπεδο, ένα σύστημα προστατεύεται «περιφρουρούμενο» αμυντικά με ένα «τοίχος προστασίας», όπως, για παράδειγμα, με τα λεγόμενα'firewalls'. Αντιθέτως, στην ενεργητική άμυνα τα μέτρα απάντησης διαπερνούν το δίκτυο του επιτιθέμενου, αποσκοπώντας είτε να χτυπήσουν το κακόβουλο λογισμικό (μη επιθετική ενεργητική κυβερνοάμυνα) είτε να δράσουν περεταίρω ώστε να το αποτρέψουν από νέες

κυβερνοεπιθέσεις (επιθετική ενεργητική κυβερνοάμυνα).[15] Η παρούσα διπλωματική εργασία θα ασχοληθεί μόνο με το ζήτημα της επιθετικής ενεργητικής κυβερνοάμυνας, υπό το πρίσμα της χρήσης της τεχνητής νοημοσύνης, η οποία καθιστά τα συστήματα αυτά να λειτουργούν αυτόματα. Τέλος, θα αναλυθούν και δύο εξίσου, βασικά και επίκαιρα, ζητήματα που σχετίζονται με την κυβερνοάμυνα. Αυτά είναι η προληπτική αυτόματη κυβερνοάμυνα κατά επικείμενης κυβερνοεπίθεσης και η αυτόματη κυβερνοάμυνα κατά κυβερνοεπιθέσεων από ΜΚΔ. Όσο αφορά την προληπτική κυβερνοάμυνα, η θεωρία υποστηρίζει την ανάγκη για αντιμετώπιση της κυβερνοεπίθεσης και την αποφυγή των δυσμενών συνεπειών της, τη στιγμή που επίκειται και προτού προλάβει να ολοκληρωθεί. Από την άλλη, η κυβερνοάμυνα κατά των ΜΚΔ, δημιουργεί, ακόμη και σήμερα έντονες συζητήσεις, σχετικά με τη νομιμότητά της παρόλο που η διεθνής πρακτική φαίνεται να το αποδέχεται σε ορισμένες περιπτώσεις.

Το ζήτημα της αυτόματης κυβερνοάμυνας, δεν είναι απλώς μια θεωρητική μελέτη, αλλά ένα υπαρκτό γεγονός το οποίο βρίσκεται στα πρώτα στάδια της εξέλιξής του. Για παράδειγμα, η Μεγάλη Βρετανία, έχει δηλώσει ότι θα εφαρμόζει ενεργητική κυβερνοάμυνα (μη επιθετική) σε «*ολόκληρο τον κυβερνοχώρο της*»,[16] ενώ οι Ηνωμένες Πολιτείες και η Κίνα, φαίνεται ότι σύντομα θα αξιοποιήσουν την τεχνητή νοημοσύνη ώστε να διασφαλίσουν τα συμφέροντά τους στο πεδίο του κυβερνοχώρου και ιδίως σε θέματα κυβερνοασφάλειας.[17]

---

[15] R Dewar, 'Active Cyber Defense', *Cyber Defense Trend Analysis, Center for Security Studies (CSS), ETH Zürich*, (June 2017) 7-10.

[16] UK, National Cyber Security Strategy 2016-2021 (2016), 33, at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> accessed 19.12.2018

[17] M Sulmeyer and K Dura, 'Beyond Killer Robots: How Artificial Intelligence Can Improve Resilience in Cyber Space', *War on the Rocks*, (6 September 2018) at: <https://warontherocks.com/2018/09/beyond-killer-robots-how-artificial-intelligence-can-improve-resilience-in-cyber-space/> accessed 19.12.2018

Μέρος Α. Η ανάπτυξη της τεχνητής νοημοσύνης και η αλληλεπίδρασή της στο πεδίο του κυβερνοχώρου. Η συμβολή της στην αξιολόγηση της κυβερνοεπίθεσης

Α.1. Εισάγοντας την τεχνητή νοημοσύνη στον κυβερνοχώρο. Οι δυνατότητες για την κυβερνοασφάλεια και οι προκλήσεις στην ερμηνεία κανόνων του διεθνούς δικαίου

Η ανάλυση της χρήσης βίας στον κυβερνοχώρο μέσω της αλληλεπίδρασή της με σύγχρονα συστήματα τεχνητής νοημοσύνης είναι αρκετά πολύπλοκη. Από τη μια πλευρά, οι κανόνες που οριοθετούν το πλαίσιο της χρήσης βίας στο Χάρτη των Ηνωμένων Εθνών, θεσπίστηκαν το 1945 και είναι αρκετά παλιοί. Από την άλλη, το νέο τεχνολογικό πεδίο του κυβερνοχώρου δε φαίνεται να έχει, πρώτον, αποσαφηνιστεί επαρκώς στο διεθνές δίκαιο και, δεύτερον, να έχει συμπεριληφθεί σε κάποια διεθνή συνθήκη ώστε να ερμηνευτούν, οι όποιες «συγκρούσεις» συμβαίνουν μέσα σε αυτό. Επομένως, προτού επιχειρηθεί οποιαδήποτε ανάλυση της χρήσης βίας στο χώρο αυτό, θα πρέπει, πρώτα, να παρουσιαστούν κάποια ιδιαίτερα χαρακτηριστικά του κυβερνοχώρου καθώς και οι προκλήσεις που αναδύονται στην ερμηνεία κανόνων του διεθνούς δικαίου μέσα σε αυτόν. Στη συνέχεια, θα εξεταστεί η έννοια της τεχνητής νοημοσύνης, τα βασικά γνωρίσματά της και πώς αυτή συμβάλλει σε ζητήματα ασφάλειας και προστασίας στον κυβερνοχώρο. Κατά αυτό τον τρόπο, θα γίνει πιο κατανοητή, παρακάτω, η ανάλυση της κυβερνοεπίθεσης και της κυβερνοάμυνας, μέσω της συμβολής αυτόματων συστημάτων.

Α.1.1. Βασικά γνωρίσματα και ιδιαιτερότητες του κυβερνοχώρου.

Η ραγδαία τεχνολογική ανάπτυξη των τελευταίων δεκαετιών και η απαραίτητη, πλέον, χρήση του διαδικτύου στην καθημερινή ζωή έχουν δημιουργήσει έναν άυλο «χώρο» όπου εκτελείται πλήθος δραστηριοτήτων. Η σημερινή «Εποχή της Πληροφορίας» ή διαφορετικά της «Ψηφιακής Επανάστασης», όπως συχνά αποκαλείται, έχει οδηγήσει σε μια ιδιαίτερα αυξημένη εξάρτηση από τη χρήση των ηλεκτρονικών υπολογιστών.[18] Για παράδειγμα, χαρακτηριστικά της τεχνολογικής αυτής εποχής είναι η άμεση ψηφιακή επικοινωνία μεταξύ των ανθρώπων, η εύκολη πρόσβαση στην πληροφόρηση και γενικώς η διαμόρφωση μιας παγκοσμιοποιημένης ψηφιακής οικονομίας, όπου ιδιώτες, οργανισμοί και κράτη αλληλοεπιδρούν μέσω του

[18] V Antolin-Jenkins, 'Defining the Parameters of Cyber of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) *51 Naval L Rev 132*, 132-133.

διαδικτύου.[19] Επιπλέον, πολλοί στρατιωτικοί οργανισμοί χρησιμοποιούν το διαδίκτυο σε μεγάλο βαθμό ως βάση οργάνωσης και επικοινωνίας, γεγονός που καταδεικνύει και την έντονη διάδραση του στρατιωτικού δικτύου πληροφόρησης με τα αντίστοιχα πολιτικά δίκτυα, ιδίως από τη στιγμή που μεγάλο μέρος των στρατιωτικών πληροφοριών διοχετεύεται μέσω των συμβατικών δικτύων.[20] Ωστόσο, ο κυβερνοχώρος δίνει σε διάφορους χρήστες την ευκαιρία να διεξάγουν παράνομες δραστηριότητες, όπως, υποκλοπή δεδομένων, ηλεκτρονικές ληστείες ή άλλα περιστατικά που σκοπό έχουν να εκμεταλλευτούν ή να βλάψουν άλλα ηλεκτρονικά συστήματα.

Η ιδιάζουσα φύση και τα ιδιαίτερα γνωρίσματα του κυβερνοχώρου καθιστούν την ερμηνεία του διεθνούς δικαίου στο πεδίο αυτό ενίοτε δυσχερή, ιδίως στην περίπτωση της παρούσας μελέτης η οποία σχετίζεται με τη χρήση βίας κατά το *jus ad bellum*. Επομένως, προτού επιχειρηθεί οποιαδήποτε ανάλυση για τη χρήση βίας στον κυβερνοχώρο θα πρέπει πρώτα να παρουσιαστούν κάποια ιδιαίτερα χαρακτηριστικά του χώρου αυτού. Αρχικά, όσον αφορά στην ορολογία, υπάρχουν πολλές σύνθετες λέξεις με το πρόθεμα «κυβερνο-» ('cyber') που χρησιμοποιούνται για να περιγράψουν σχεδόν οτιδήποτε έχει να κάνει με δίκτυα και υπολογιστές, ιδίως στον τομέα της ασφάλειας. Ενδεικτικά, συναντώνται συχνά οι έννοιες όπως: κυβερνοασφάλεια, κυβερνοεπίθεση, κυβερνοάμυνα και άλλες. Ωστόσο, στο σημείο αυτό, θα πρέπει να τονιστεί η απουσία ενός διεθνούς κοινά αποδεκτού ορισμού από τα κράτη, που να οριοθετεί το πεδίο του κυβερνοχώρου στο διεθνές δίκαιο καθώς και τα αποτελέσματα των όποιων συγκρούσεων μέσα σε αυτό.[21] Ενδεικτικά, το *Εγχειρίδιο του Ταλλίν* ορίζει τον κυβερνοχώρο ως «*το περιβάλλον που σχηματίζεται από φυσικά και μη συστατικά, χαρακτηρίζεται από τη χρήση ηλεκτρονικών υπολογιστών και ηλεκτρομαγνητικού φάσματος, αποθηκεύει, τροποποιεί και ανταλλάσσει δεδομένα χρησιμοποιώντας δίκτυα ηλεκτρονικών υπολογιστών*».[22] Παρόμοια περιγραφική προσέγγιση του κυβερνοχώρου δίνεται, για παράδειγμα, και από το διακλαδικό «Λεξικό Στρατιωτικών και Συναφών Όρων» του Υπουργείου Εθνικής Άμυνας των ΗΠΑ που ορίζει τον κυβερνοχώρο ως *«ένα παγκόσμιο πεδίο μέσα στο περιβάλλον της πληροφόρησης, που αποτελείται από το αλληλεξαρτώμενο δίκτυο υποδομών τεχνολογίας, πληροφοριών και δεδομένων ιδιωτών,*

---

[19] M Castells, *The Information Age. Economy, Society, and Culture* Vol 1, (2nd edn, New Jersey: Blackwell Publishing Ltd, 2010) 77-8.

[20] Οπ. π., υποσημείωση 18.

[21] NATO CCDCOE, 'Cyberspace: Definition and Implications' at: <https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html> accessed 19.12.2018

[22] M Schmitt (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013) 258 (*Tallin Manual*).

συμπεριλαμβανομένου του Διαδικτύου, των τηλεπικοινωνιακών δικτύων, των συστημάτων πληροφορικής και των ενσωματωμένων επεξεργαστών και ελεγκτικών μηχανισμών».[23] Επίσης, αντίστοιχες προσεγγίσεις στην έννοια του κυβερνοχώρου επιχειρούνται και από άλλα κράτη.[24] Από τους παραπάνω ορισμούς προκύπτει ότι ο κυβερνοχώρος πέρα από τις απαραίτητες υλικοτεχνικές εγκαταστάσεις που περικλείει, δημιουργεί, πρωτίστως, ένα παγκόσμιο «εικονικό πεδίο» όπου λαμβάνουν χώρα όλες οι δραστηριότητες μέσω του διαδικτύου. Επομένως, με βάση τα παραπάνω, ο κυβερνοχώρος δομείται σε τρεις παράλληλες και αλληλεξαρτώμενες διαστάσεις· την φυσική που περιλαμβάνει όλες τις υλικοτεχνικές υποδομές, την διάσταση του λογισμικού που συμπεριλαμβάνει τα δίκτυα, τις εφαρμογές και τα απαραίτητα λογισμικά συστήματα και τη διάσταση που περιλαμβάνει τα δεδομένα όπως αυτά διαμορφώνονται υπό την ανθρώπινη επίδραση.[25]

Αυτός ο τομέας, όπως είναι εύκολα αντιληπτό, διαπερνά, κατά μια έννοια, τα σύνορα των κρατών, δημιουργώντας ένα παγκόσμιο πλέγμα ροής και ανταλλαγής δεδομένων. Η απουσία και η αδυναμία προσδιορισμού ευδιάκριτων συνόρων, όπως το αντιλαμβανόμαστε υπό την έννοια της εδαφικής οριοθέτησης, έχουν δημιουργήσει ερωτήματα στο κατά πόσο ο κυβερνοχώρος υπόκειται στο διεθνές δίκαιο και επιπλέον αν τίθεται ζήτημα κυριαρχίας και δικαιοδοσίας των κρατών σε αυτό. Το Ινστιτούτο Διεθνούς Ανθρωπιστικού Δικαίου αναφέρει ότι αυτό το πλασματικό περιβάλλον του κυβερνοχώρου βρίσκεται πέρα από τη δικαιοδοσία οποιουδήποτε κράτους, καθιστώντας έτσι δύσκολο τον προσδιορισμό μιας εχθρικής πράξης και πρόθεσης αντίστοιχα.[26] Σε μια άλλη προσέγγιση, το Υπουργείο Εθνικής Άμυνας των ΗΠΑ, το 2005, είχε συμπεριλάβει στα Παγκόσμια Κοινά (Global Commons) και τον κυβερνοχώρο, λογική που υποστηρίζεται και από μερίδα συγγραφέων.[27] Στην περίπτωση αυτή, όμως, δε θα μπορούσε να ασκηθεί κρατική κυριαρχία ούτε και να

---

[23] US Department of Defence, 'Dictionary of Military and Associated Terms', Joint Publication 1-02 (8 November 2010, as amended through 15 February 2016), 58 at: <https://fas.org/irp/doddir/dod/jp1_02.pdf> accessed 19.12.2018

[24] Βλέπε στο λεξικό του NATO CCDCOE, τον όρο "cyberspace" και επεξηγηματικά τις προσεγγίσεις που αναφέρονται από τα κράτη. At: < https://ccdcoe.org/cyber-definitions.html> accessed 19.12.2018

[25] US Joint Chiefs of Staff, 'Cyberspace Operations', Joint Publication 3-12, (8 June 2018) I-2 at: <https://fas.org/irp/doddir/dod/jp3_12.pdf> accessed 19.12.2018. L Robert and S Rahman, 'Analytic of China Cyberattack', *The International Journal of Multimedia & Its Applications*, (2012) Vol 4 No 3, 37-56.

[26] International Humanitarian Law Institute, *Rules of Engagement Handbook* (September 2009), 15.

[27] US Department of Defence, 'Strategy for Homeland Defense and Civil Support' (June 2005), 12. Maj Gen M Barret, D Bedford, E Skinner, E Vergles, *Assured Access to the Global Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization (Norfolk, Virginia USA, April 2011) xvi, at: <https://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf> accessed 19.12.2018

νοείται η χρήση βίας από κράτος κατά άλλου, γεγονός που θα έκανε την ερμηνεία των όποιων παράνομων ενεργειών στο πεδίο αυτό ιδιαίτερα δυσχερή κατά το διεθνές δίκαιο. Ωστόσο, η παρούσα μελέτη δεν θεωρεί ότι υπάρχουν ζητήματα αμφιβολίας καθώς ο κυβερνοχώρος, κατά κοινή ομολογία, φαίνεται να υπάγεται, πλέον, στο διεθνές δίκαιο και τα κράτη μπορούν να εγείρουν ζητήματα δικαιοδοσίας και κρατικής κυριαρχίας μέσα σε αυτό.[28] Για παράδειγμα, η έκθεση για την ανάπτυξη στο πεδίο των πληροφοριών και των τηλεπικοινωνιών, της Ομάδας Κυβερνητικών Εμπειρογνώμων των Ηνωμένων Εθνών (United Nations Group of Governmental Experts), επιβεβαιώνει ότι το διεθνές δίκαιο και ιδίως ο Χάρτης των Ηνωμένων Εθνών εφαρμόζεται και στον κυβερνοχώρο.[29] Η θέση αυτή εκφράστηκε και στη Σύνοδο Κορυφής του NATO το 2014, όπου κατά την επίσημη δήλωσή του ανέφερε πως «*αναγνωρίζει επίσης ότι το διεθνές δίκαιο, συμπεριλαμβανομένου του διεθνούς ανθρωπιστικού δικαίου και του Χάρτη των Ηνωμένων Εθνών, εφαρμόζεται στον κυβερνοχώρο*».[30] Επιπλέον, η κρατική κυριαρχία καθώς και οι διεθνείς κανόνες και αρχές που πηγάζουν από αυτή, ισχύουν κατά τη διεξαγωγή των όποιων σχετικών δραστηριοτήτων από τα κράτη στο τεχνολογικό πεδίο της πληροφόρησης και της επικοινωνίας (Information and Communication Technology) καθώς και στη δικαιοδοσία των κρατών επί των τεχνολογικών υποδομών εντός της επικράτειάς τους.[31] Συνεπώς, οποιαδήποτε θεώρηση «αποκοπής» του κυβερνοχώρου από το διεθνές δίκαιο θα δημιουργούσε, επικίνδυνα, ένα δυσεπίλυτο νομικό κενό όσον αφορά την προσπάθεια ερμηνείας εννοιών όπως της κυβερνοεπίθεσης και της κυβερνοάμυνας καθώς και ως προς τις όποιες έννομες συνέπειες αυτών.

Μια κυβερνοεπίθεση μπορεί να ενεργοποιήσει το δικαίωμα της νόμιμης κυβερνοάμυνας, όπως θα αναλυθεί σε επόμενο κεφάλαιο. Ωστόσο, προτού γίνει αυτό, θα πρέπει η πηγή και ο δημιουργός της επίθεσης να έχουν προσδιοριστεί με σαφήνεια. Η φύση του κυβερνοχώρου, όμως, κάνει το ζήτημα της απόδοσης ευθυνών για πράξεις

---

[28] N Tsagourias, 'The Legal Status of Cyberspace'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015), 13.

[29] UN GA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98, paras 19-20. Η ομάδα των εμπειρογνωμόνων συστήθηκε από τον Γενικό Γραμματέα των Ηνωμένων Εθνών βάσει του Ψηφίσματος 66/24 της Γενικής Συνέλευσης, για να επανεξετάσει τις υπάρχουσες αλλά και δυνητικές απειλές στη σφαίρα του κυβερνοχώρου. Developments in the field of information and telecommunications in the context of international security, GA Res 66/24, (2 December 2011) UN Doc A/RES/66/24.

[30] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales (5 September 2014), para 72 at: <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm> accessed 19.12.2018

[31] Οπ. π., υποσημείωση 29. Βλέπε επίσης: *Tallin Manual*, 15-8.

που συμβαίνουν μέσα σε αυτόν ιδιαίτερα δυσχερή. Συγκεκριμένα, η ανωνυμία, οι επιθέσεις από πολλαπλά στάδια (multi-stage cyber attacks) και η ταχύτητα με την οποία αυτές εκτελούνται, αποτελούν τους κύριους παράγοντες που καθιστούν την απόδοση μιας πράξης προς τον δημιουργό της προβληματική.[32] Η ανωνυμία στο διαδίκτυο μπορεί να είναι είτε «αληθινή ανωνυμία» ("true anonymity") είτε «ψευδής» αντίστοιχα, ("pseudo-anonymity") μέσω της παραπλάνησης. Στην πρώτη περίπτωση, η ανίχνευση του σήματος και της θέσης του χρήστη δεν μπορεί να γίνει σε καμία περίπτωση, ενώ στη δεύτερη, η ανίχνευση μπορεί να οδηγήσει εσκεμμένα σε ψευδή χρήστη.[33] Επιπλέον, η απόδοση ευθυνών γίνεται ακόμη πιο δύσκολη λόγω των κυβερνοεπιθέσεων από πολλαπλά στάδια, όπως είναι για παράδειγμα οι επιθέσεις 'DDoD'. Συγκεκριμένα, οι επιθέσεις αυτού του τύπου διεξάγονται μέσω τρίτων υπολογιστών οι οποίοι με τη σειρά τους μπορούν να χρησιμοποιήσουν επιπλέον και άλλους υπολογιστές ώστε να συνεχιστεί η αρχική κυβερνοεπίθεση.[34] Στην παραπάνω λογική για παράδειγμα, ένας υπολογιστής Α διεισδύει στον υπολογιστή Β, ο οποίος χρησιμοποιείται ως πλατφόρμα για τη διείσδυση στον υπολογιστή Γ, ο οποίος με τη σειρά του επιτίθεται στον υπολογιστή Δ.[35] Εάν αυτό το «πλέγμα» υπολογιστών συμπεριλαμβάνει εκατοντάδες μεμονωμένους υπολογιστές, είναι εμφανές ότι μια τέτοια κυβερνοεπιχείρηση μπορεί να επιφέρει σημαντικά αρνητικά αποτελέσματα. Βάσει των παραπάνω δεδομένων, είναι επίσης εμφανές ότι η ευελιξία παράνομης δραστηριοποίησης των χρηστών στον κυβερνοχώρο είναι τέτοια που θέτει πολλούς περιορισμούς στον εντοπισμό των ιθυνόντων και στον καταλογισμό ευθυνών.

Α.1.2. Η τεχνητή νοημοσύνη στην κυβερνοασφάλεια.

Στο παρόν κεφάλαιο, θα αναλυθεί η έννοια της τεχνητής νοημοσύνης καθώς και η επιρροή της στον τομέα της κυβερνοάμυνας. Απώτερος στόχος της ανάλυσης των παραπάνω ορισμών είναι η αποσαφήνιση και η βαθύτερη κατανόηση της αυτόματης κυβερνοάμυνας όπως αυτή θα αναλυθεί εκτενέστερα στο δεύτερο μέρος της παρούσας μελέτης.

---

[32] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', *Journal of Conflict &Security Law*, (2012) Vol 17 No 2, 233-234.

[33] M Chawki, 'Anonymity in Cyberspace: Finding the Balance between Privacy and Security', (July 2006) at: <http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf> accessed 19.12.2018

[34] D Clark and S Landau, 'The Problem isn't attribution: It's Multi-Stage Attacks' in Proceeding of a workshop on Re-Architecting the Internet, (2010) No. 11, ACM.

[35] Ibid

Η τεχνητή νοημοσύνη αποτελεί ένα ταχύτατα εξελισσόμενο τεχνολογικό τομέα. Προσανατολισμένη στο να κάνει τα σύγχρονα συστήματα ακόμα πιο "ευφυή", αξιολογεί την ικανότητα ενός συστήματος να εντοπίζει τις καλύτερες επιλογές εκτέλεσης μιας πράξης για την επίτευξη των στόχων του, σε ένα ευρύ φάσμα διαφορετικών περιβαλλοντικών συνθηκών.[36] Ο όρος «τεχνητή νοημοσύνη» χρησιμοποιείται επιμελώς όταν μια μηχανή μιμείται τις «γνωστικές» λειτουργίες των ανθρώπων, όπως «μάθηση» και «επίλυση προβλημάτων», μέσα από εμπειρικές διαδικασίες που επιτρέπουν να λειτουργήσει και να αντιδράσει όπως ένας άνθρωπος.[37] Η τεχνολογία αυτή επιτρέπει ουσιαστικά στα εν λόγω συστήματα να εκπαιδεύονται μέσω μιας διαδικασίας συνεχούς έκθεσης και προσαρμογής σε νέα δεδομένα, ώστε να μπορούν να αναλύουν μεγάλο όγκο δεδομένων, εντοπίζοντας τάσεις και μοτίβα συμπεριφορών (patterns) στο διαδίκτυο. Η δυνατότητα προηγμένων υπολογισμών παράγει ιδιαίτερα αξιόπιστα αποτελέσματα, γεγονός που αναδεικνύει την ανάγκη υιοθέτησής της σε συνεχώς περισσότερους τομείς, από την αυτοκινητοβιομηχανία και την υγειονομική περίθαλψη έως την άμυνα και το εμπόριο.[38] Οι διαφορετικές προσεγγίσεις έρευνας και η ταχύτητα εξέλιξης του πεδίου αυτού δεν έχουν επιτρέψει τη δημιουργία ενός κοινώς αποδεκτού ορισμού περί της τεχνητής νοημοσύνης. Στο πλαίσιο αυτό, όμως, η Επιτροπή Ενέργειας και Εμπορίου σε συνεργασία με άλλες σχετικές επιτροπές της Βουλής των Αντιπροσώπων των ΗΠΑ, σε νομοσχέδια που κατέθεσαν το Δεκέμβριο του 2017, ορίζουν την τεχνητή νοημοσύνη ως «*κάθε τεχνητό σύστημα που εκτελεί καθήκοντα υπό διαφορετικές και απρόβλεπτες συνθήκες, χωρίς σημαντική ανθρώπινη εποπτεία ή που μπορεί να μάθει από την εμπειρία και να βελτιώσει τις επιδόσεις του* [...] *Μπορεί να επιλύσει καθήκοντα που απαιτούν ανθρώπινη αντίληψη, γνώση, σχεδιασμό, μάθηση, επικοινωνία ή φυσική δράση*».[39]

Η διαδικασία ψηφιοποίησης των περισσότερων επιχειρήσεων, βάσεων δεδομένων, αρχείων και λειτουργικών συστημάτων, σήμερα, δίνει στους χάκερς περισσότερες ευκαιρίες για παράνομη δραστηριοποίηση ενάντια στα ψηφιακά οικοσυστήματα. Η πολυπλοκότητα των σύγχρονων κυβερνοεπιθέσεων καθιστά τον ανθρώπινο παράγοντα και τους παραδοσιακούς τρόπους κυβερνοάμυνας ανεπαρκή και

---

[36] A Graham, 'Artificial Intelligence in Cyber Security', *IT Governance Blog* (22 March 2018) at: <https://www.itgovernance.co.uk/blog/artificial-intelligence-in-cyber-security> accessed 19.12.18

[37] Ibid

[38] SAS Institute, 'Analytics and Data Insights' at: <https://www.sas.com/en_gb/insights/analytics/machine-learning.html> accessed 19.12.18

[39] D Hoadley and N Lucas, 'Artificial Intelligence and National Security', *Congressional Research Service*, (26 April 2018) at: <https://fas.org/sgp/crs/natsec/R45178.pdf> accessed 19.12.18

αναδεικνύει την ανάγκη ενσωμάτωσης εξελιγμένων μηχανισμών αντιμετώπισης περιστατικών ασφαλείας, ικανών να περιορίσουν όσο το δυνατόν πιο γρήγορα και διεξοδικά τους διαδικτυακούς κινδύνους.[40]

Το Αμερικανικό Ινστιτούτο Αεροναυτικής και Αστροναυτικής υποστηρίζει ότι η επόμενη γενιά των προϊόντων κυβερνοασφάλειας θα επιτύχει αποδοτικότερα και ασφαλέστερα επίπεδα κρυπτογράφησης με την ενσωμάτωση πιο εξελιγμένων τεχνολογιών τεχνητής νοημοσύνης και μηχανικής μάθησης (machine learning).[41] Οι τελευταίες εξελίξεις στο χώρο της τεχνητής νοημοσύνης έχουν δημιουργήσει πιο ευφυή συστήματα αυτόματης κυβερνοάμυνας, ικανά να εκπαιδεύονται μέσω της διαδικασίας μηχανικής μάθησης.[42] Ειδικότερα, οι αλγόριθμοι που χρησιμοποιούνται, έχοντας την ικανότητα να οριοθετούν τι θεωρείται κανονική ή μη δραστηριότητα, μπορούν να ανιχνεύουν οποιαδήποτε διαταραχή ή ακανόνιστη συμπεριφορά ενός μοτίβου. Στη συνέχεια, η εξέταση αυτών των ασυνήθιστων γεγονότων, μπορεί να οδηγήσει στον εντοπισμό κυβερνοεπιθέσεων. Άλλος τρόπος εντοπισμού απειλών κατά του συστήματος, είναι μέσω αλγορίθμων που εντοπίζουν απειλές στις οποίες έχουν εκπαιδευτεί, όπως για παράδειγμα ένα προηγμένο κακόβουλο λογισμικό που αποτελεί νεότερη ή μεταλλαγμένη έκδοση ενός παλαιότερου λογισμικού.[43] Η διεκπεραίωση των εν λόγω λειτουργιών γίνεται με διαδικασίες σχεδόν αυτόματες από τα συστήματα τεχνητής νοημοσύνης, κάτι που λόγω όγκου και ταχύτητας δεδομένων, είναι εξαιρετικά δύσκολο και χρονοβόρο να πραγματοποιηθεί επιτυχώς από τον άνθρωπο.[44]

Υποστηρίζεται ότι η χρήση συστημάτων τεχνητής νοημοσύνης μπορεί να μειώσει σημαντικά τον απαιτούμενο χρόνο εντοπισμού μιας ανώμαλης συμπεριφοράς, ειδοποιώντας άμεσα το αρμόδιο τεχνικό προσωπικό ('Information Technology').[45] Η εφαρμογή, λόγου χάρη, 'QRadar Advisor with Watson' της αμερικανικής εταιρείας τεχνολογιών υπολογιστών IBM, αποτελεί χαρακτηριστικό παράδειγμα χρήσης τεχνολογίας τεχνητής νοημοσύνης που συμβάλλει στον εντοπισμό απειλών στον

---

[40] V Vasudevan, 'How AI Is Transforming Cyber Defense', Forbes, (24 July 2018) at: <https://www.forbes.com/sites/forbestechcouncil/2018/07/24/how-ai-is-transforming-cyber-defense/#67448e593bb2> accessed 19.12.18

[41] American Institute of Aeronautics and Astronautics, 'Artificial Intelligence for Cybersecurity', at: <https://www.aiaa.org/protocolAI/> accessed 19.12.18

[42] Οπ. π., υποσημείωση 40.

[43] Οπ. π., υποσημείωση 40.

[44] CISCO Systems, Annual Cybersecurity Report, (2018) 49 at: <https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2> accessed 19.12.18

[45] Οπ. π., υποσημείωση 41.

κυβερνοχώρο.[46] Με την αρωγή του εν λόγω «έξυπνου» λογισμικού ανάλυσης 'big data'[47], η διαδικασία της σύνθετης έρευνας και του εντοπισμού κενών ασφαλείας φτάνει να είναι εξήντα φορές ταχύτερη από τον παραδοσιακό τρόπο αναζήτησης, μειώνοντας έτσι τον απαιτούμενο χρόνο από μία ώρα σε λιγότερο από ένα λεπτό.[48]

Ανακριβείς πληροφορίες και εσφαλμένες ειδοποιήσεις για ζητήματα ασφαλείας στον κυβερνοχώρο, πολύ συχνά έχουν σημαντικές οικονομικές συνέπειες. Στην προσπάθειά τους να αντιμετωπίσουν τέτοια περιστατικά, οργανισμοί και επιχειρήσεις υπολογίζεται ότι ξοδεύουν έως και 1.3 εκατομμύρια δολάρια ετησίως.[49] Συστήματα, όμως, που χρησιμοποιούν τεχνολογία μηχανικής μάθησης, εκπαιδεύονται στο να αναλύουν τεράστιους όγκους πληροφοριών και να εντοπίζουν τα έκτοπα μοτίβα συμπεριφορών, ακόμα και κατά τη διάρκεια μιας κυβερνοεπίθεσης, διασφαλίζοντας, παράλληλα, την προστασία και τον έλεγχο της πρόσβασης σε απόρρητες πληροφορίες.[50] Ουσιαστικά, έχουν εκπαιδευτεί να μιμούνται την ανθρώπινη αντίληψη σε κάθε διαδικτυακή αλληλεπίδραση, με στόχο την απομάκρυνση μιας ασυνήθιστης δραστηριότητας μέσα από εκατομμύρια άλλες, ώστε στη συνέχεια να επιθεωρηθεί από ανθρώπινο παράγοντα. Η μείωση του απαιτούμενου χρόνου εντοπισμού ενός κενού ασφαλείας είναι ιδιαίτερα κρίσιμης σημασίας, ειδικά αν σκεφτούμε ότι ο μέσος χρόνος εύρεσης μιας παραβίασης ξεπερνά τις 260 μέρες.[51]

Η συνεχής ψηφιοποίηση των σύγχρονων επιχειρήσεων θέτει την αύξηση του ετήσιου προϋπολογισμού για θέματα κυβερνοασφάλειας στην κορυφή της ατζέντας. Οι περισσότερες εταιρείες αναζητούν την εγκατάσταση τεχνολογιών μηχανικής μάθησης, τεχνητής νοημοσύνης και αυτόματων συστημάτων ανάλυσης δεδομένων. Εξ αυτών, το 53% αναφέρει πως προσέφυγε σε αναγκαστική αύξηση δαπανών για την

---

[46] Αναλυτικότερα βλέπε στο: IBM, 'IBM QRadar Advisor with Watson' at: <https://www.ibm.com/us-en/marketplace/cognitive-security-analytics/details> accessed 19.12.18

[47] Ο όρος 'big data' αναφέρεται στο μεγάλο όγκο δεδομένων που μια επιχείρηση διαχειρίζεται καθημερινά. Αλλά αυτό που έχει μεγαλύτερη σημασία, εν προκειμένω, δεν είναι ο όγκος αυτός καθαυτός, αλλά οι διαδικασίες διαχείρισης από τούς οργανισμούς. Η ανάλυση των 'big data' παράγει ιδέες που μπορούν να οδηγήσουν σε καλύτερες αποφάσεις και στρατηγικές επιχειρηματικές κινήσεις. Αναλυτικότερα βλέπε: SAS Institute, 'Big Data· What it is and why it matters', at: <https://www.sas.com/en_us/insights/big-data/what-is-big-data.html> accessed 19.12.2018

[48] IBM, 'Artificial Intelligence and Cybersecurity FAQ Handbook' at: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?%3B=&%3Bdd=yes&htmlfid=10016710USEN> accessed 30.09.18

[49] Οπ. π., υποσημείωση 41.

[50] K Lamb, 'Challenges of Digitalisation in the Aerospace and Aviation Sectors', *Centre for Digital Built Britain*, (March 2018) 8, at:

<https://www.repository.cam.ac.uk/bitstream/handle/1810/278896/CDBB_REP_002_Lamb.pdf?sequence=1&isAllowed=y> accessed 19.12.18

[51] Οπ. π., υποσημείωση 41.

εγκατάσταση πιο σύγχρονων μηχανισμών ασφαλείας τον τελευταίο χρόνο, ενώ το 65% προβλέπει περαιτέρω αύξηση του σχετικού προϋπολογισμού για το 2019.[52] Ο επιχειρηματικός κόσμος γνωρίζει πλέον ότι το κόστος αποτυχίας από μια απλή κυβερνοεπίθεση μπορεί να αποδειχτεί ιδιαίτερα υψηλό. Σε μια πρόσφατη επίθεση, μια ινδική τράπεζα έχασε 944 εκατομμύρια ρουπίες μετά την εγκατάσταση κακόβουλου προγράμματος στον διακομιστή αυτόματων αναλήψεων (ATM), που επέτρεψε στους χάκερς να κάνουν παράνομες αναλήψεις σε 28 χώρες.[53]

Οι προαναφερθείσες εξελίξεις στο πεδίο του κυβερνοχώρου και η αυξανόμενη χρήση της τεχνητής νοημοσύνης, εγείρουν πολλαπλές προκλήσεις με σημαντικές νομικές προεκτάσεις. Μία από αυτές, είναι η περίπτωση που μια πράξη αυτόματης κυβερνοάμυνας, χωρίς την επιρροή του ανθρώπινου παράγοντα, μπορεί να προκαλέσει την επίκληση του δικαιώματος στη νόμιμη άμυνα, βάσει του Άρθρου 51 του Χάρτη των Ηνωμένων Εθνών. Ωστόσο, προτού αναλυθεί κατά πόσο μια τέτοια διαδικασία είναι σύμφωνη με τους κανόνες του διεθνούς δικαίου, θα πρέπει πρώτα να προσδιοριστεί η έννοια της επίθεσης στον κυβερνοχώρο και να εξεταστεί κατά πόσο η τεχνητή νοημοσύνη διαθέτει την ικανότητα να κρίνει ότι μια τέτοια πράξη είναι αποδοτέα προς το κράτος που φέρει την ευθύνη.

Α.2. Η έννοια της επίθεσης στον κυβερνοχώρο και το πρόβλημα της απόδοσης ευθυνών. Μπορούν τα «έξυπνα» αυτόματα συστήματα να συμβάλλουν στην έγκαιρη αναγνώρισή της;

Η έννοια της επίθεσης στο διεθνές δίκαιο, δεν ήταν επαρκώς προσδιορισμένη κατά τον Χάρτη των Ηνωμένων Εθνών, καθώς δεν εμπεριέχει κάποιο νομικό ορισμό. Θα χρειαστούν να περάσουν αρκετά χρόνια έως ότου η Γενική Συνέλευση καταλήξει στο Ψήφισμα 3314, το 1974, με το οποίο θα ορίσει την έννοια της Επίθεσης. Σημαντικό ρόλο στη διαμόρφωση αυτής θα διαδραματίσει, παράλληλα, και η διεθνής νομολογία, όπως θα αναφερθεί στη συνέχεια. Ωστόσο, σε καμία περίπτωση, δε θα μπορούσε εκείνη την εποχή να νοηθεί η έννοια της κυβερνοεπίθεσης όπως αυτή αναφέρεται, συχνά, στη σημερινή τεχνολογική εποχή. Η ιδιαίτερη φύση του κυβερνοχώρου και το γεγονός ότι τα αποτελέσματα των όποιων κυβερνοεπιθέσεων μπορεί να μην είναι

---

[52] Ernst & Young, 'Is Cybersecurity about more than protection?' *EY Global Information Security Survey 2018-2019*, 8, at: <https://assets.ey.com/content/dam/ey-sites/ey-com/global/topics/advisory/GISS-2018-19-low-res.pdf> accessed 19.12.18

[53] R Jadhav, 'Indian Bank Loses $13,5m in Global Attack', *Reuters*, (14 August 2018) at: <https://www.reuters.com/article/cyber-heist-india/indias-cosmos-bank-loses-13-5-mln-in-cyber-attack-idUSL4N1V551G> accessed 19.12.18

πάντοτε εμφανή, καθιστούν τον προσδιορισμό και την ερμηνεία της επίθεσης στο πεδίο αυτό ενίοτε δυσχερή. Επιπλέον, στην εξαίρετη περίπτωση επίκλησης του δικαιώματος της νόμιμης άμυνας στον κυβερνοχώρο, και ιδίως μέσω αυτόματων διαδικασιών τεχνητής νοημοσύνης, εγείρονται, εύλογα, οι ακόλουθοι προβληματισμοί. Αρχικά, η δυνατότητα ενός «έξυπνου» συστήματος να αναγνωρίσει ένα περιστατικό που ισοδυναμεί με «ένοπλη επίθεση», χωρίς την επίδραση του ανθρωπίνου παράγοντα, και δεύτερον, ο εντοπισμός του ίχνους της επίθεσης με στόχο την αποκάλυψη της ταυτότητας του δράστη, ώστε να αποδοθεί η ευθύνη της πράξης σε ένα κράτος. Επομένως, στην παρούσα ενότητα θα επιχειρηθεί ο προσδιορισμός της έννοιας της κυβερνοεπίθεσης, καθώς και η διαδικασία αναγνώρισης και απόδοσης αυτής σε ένα κράτος, υπό το πρίσμα των τεχνολογικών συστημάτων που κάνουν χρήση της τεχνητής νοημοσύνης.

Α2.1. Εννοιολογικός προσδιορισμός της επίθεσης: χρήση συναφών όρων υπό το πρίσμα του Χάρτη των Ηνωμένων Εθνών και της διεθνούς νομολογίας.

Εννοιολογικά, ο όρος «Επίθεση» αναφέρεται μέσω ομοειδών εκφράσεων στο Χάρτη των Ηνωμένων Εθνών καθώς δεν περικλείει κάποιο συγκεκριμένο νομικό ορισμό.[54] Για παράδειγμα, το Άρθρο 1(1), το οποίο ορίζει τους σκοπούς των Ηνωμένων Εθνών, αναφέρει την έκφραση «επιθετικές ενέργειες» ('acts of aggression') ενώ το Άρθρο 2(4) που απαγορεύει τη βία, αναφέρει την γενικευμένη έκφραση «χρήση βίας» ('use of force').[55] Χαρακτηριστικό, επίσης, είναι και το Άρθρο 39 του Χάρτη το οποίο ορίζει: «*Το Συμβούλιο Ασφαλείας θα αποφαίνεται αν υπάρχει απειλή για την ειρήνη, διατάραξη της ειρήνης ή επιθετική ενέργεια και θα κάνει συστάσεις ή θα αποφασίζει ποια μέτρα θα λαμβάνονται σύμφωνα με τα Άρθρα 41 και 42, για να διατηρηθεί ή να αποκατασταθεί η διεθνής ειρήνη και ασφάλεια*». Βάσει του παραπάνω, υπάρχει και η άποψη ότι η σειρά των τριών όρων στο Άρθρο 39 («απειλή για την ειρήνη, παραβίαση της ειρήνης ή επιθετική ενέργεια») είναι προοδευτική και επομένως η έννοια της «επιθετικής ενέργειας» να θεωρείται είναι πιο βαρύνουσας σημασίας.[56]

---

[54] United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI.

[55] Το Άρθρο 2(4) αναφέρει: «*Όλα τα Μέλη στις διεθνείς τους σχέσεις θα απέχουν από την απειλή ή τη χρήση βίας, που εκδηλώνεται εναντίον της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους είτε με οποιαδήποτε άλλη ενέργεια ασυμβίβαστη προς τους Σκοπούς των Ηνωμένων Εθνών*».

[56] Το Άρθρο 51 αναφέρει: «Καμιά διάταξη αυτού του Χάρτη δε θα εμποδίζει το φυσικό δικαίωμα της ατομικής ή συλλογικής νόμιμης άμυνας, σε περίπτωση που ένα Μέλος των Ηνωμένων Εθνών δέχεται ένοπλη επίθεση, ως τη στιγμή που το Συμβούλιο Ασφαλείας θα πάρει τα αναγκαία μέτρα για να διατηρήσει τη διεθνή ειρήνη και ασφάλεια. Τα μέτρα που θα παίρνουν τα Μέλη των Ηνωμένων Εθνών κατά την άσκηση αυτού του δικαιώματος της νόμιμης άμυνας θα ανακοινώνονται αμέσως στο

Παράλληλα, το Άρθρο 51, που ορίζει το δικαίωμα στη νόμιμη άμυνα ενός κράτους, αναφέρει την έννοια της επίθεσης ως «ένοπλη επίθεση» ('armed attack'). Η επίκληση, δηλαδή, του δικαιώματος αυτού δεν συμπεριλαμβάνει οποιαδήποτε επιθετικότητα ή χρήση βίας αλλά μόνο αυτή της «ένοπλης». Όπως θα αναλυθεί στο επόμενο υποκεφάλαιο, η «ένοπλη επίθεση» είναι μεγαλύτερης βαρύτητας και ξεχωρίζει από τις υπόλοιπες βίαιες πράξεις λόγω της έντασης και των αποτελεσμάτων που μπορεί να προκαλέσει. Αξίζει, ωστόσο, να σημειωθεί ότι στην επίσημη αυθεντική γαλλική μετάφραση, του Άρθρου 51, δεν γίνεται αναφορά ως «ένοπλη επίθεση» αλλά ως «ένοπλη επιθετικότητα» ('aggression armée'). Παράλληλα, όπως διαπιστώνεται από τη διεθνή πρακτική, το Συμβούλιο Ασφαλείας του ΟΗΕ σε αρκετές αποφάσεις του, κατά το παρελθόν, έχει καταδικάσει επίθεση κράτους κατά άλλου χρησιμοποιώντας, και σε αυτή την περίπτωση, συναφείς εκφράσεις. Ενδεικτικά, το 1985 καταδίκασε την στρατιωτική επιχείρηση της Νότιας Αφρικής κατά της Μποτσουάνα ως μια «*επιθετική ενέργεια εναντίον αυτής της χώρας και μιας σοβαρής παραβίασης της εδαφικής ακεραιότητας και της εθνικής κυριαρχίας*» ('acts of aggression').[57] Αντιστοίχως, κατά την ίδια χρονιά, καταδίκασε τον αεροπορικό βομβαρδισμό του Ισραήλ στην εδαφική επικράτεια της Τυνησίας ως μια «*ένοπλη επιθετική ενέργεια*» ('act of armed aggression').[58] Από τα παραπάνω, προκύπτει ότι οι συναφείς εννοιολογικοί προσδιορισμοί της «Επίθεσης» δεν έχουν διασαφηνιστεί επαρκώς ούτε από νομικά κείμενα ούτε από την πρακτική των κρατών, με αποτέλεσμα να αποτελούν συχνά αντικείμενο νομικής διαμάχης.[59] Κατά το Ruys, υπάρχει μια καθοδική σχέση στις έννοιες «βία» ('force'), «επιθετικότητα» ('aggression') και «ένοπλη επίθεση» ('armed attack'), με την τελευταία να είναι η πιο ισχυρή, με αποτέλεσμα να ενεργοποιεί το δικαίωμα στη νόμιμη άμυνα.[60]

Αξίζει, επιπλέον, να σημειωθεί, ότι παράλληλα υπάρχει και η συζήτηση μεταξύ των νομικών αν η έννοια της «χρήσης βίας», κατά το Άρθρο 2(4), είναι ευρύτερη

Συμβούλιο Ασφαλείας, και σε καμία περίπτωση δε θα θίγουν την εξουσία και την υποχρέωση που έχει το Συμβούλιο Ασφαλείας, σύμφωνα με αυτόν το Χάρτη, να αναλαμβάνει οποτεδήποτε τη δράση που κρίνει αναγκαία για τη διατήρηση ή για την αποκατάσταση της διεθνούς ειρήνης και ασφάλειας».

[57] UN Security Council Resolution 568, UN Doc S/RES/568 (21 June 1985). Βλέπε αντίστοιχα επίσης: UN Security Council Resolution 602, S/RES/602 (25 November 1987) και UN Security Council Resolution 577, UN Doc S/RES/577 (6 December 1985).

[58] UN Security Council Resolution 573, UN Doc S/RES/573 (4 October 1985).

[59] O Dörr and A Randelzhofer, 'Ch. I Purposes and Principles, Article 2 (4)' in: B Simma, D-E Khan, G Nolte and A Paulus (ed) *The Chapter of the United Nations: A Commentary*, (3rd edn, Oxford: Oxford University Press, 2012) 206-08.

[60] T Ruys, *'Armed Attack' and Article 51 of the UN Charter*, (Cambridge: Cambridge University Press, 2010), 136-9.

απαγορεύοντας οποιαδήποτε βία ή αν ερμηνεύεται πιο συσταλτικά στη βάση του απώτερου σκοπού του Χάρτη.[61] Οι προπαρασκευαστικές εργασίες, έδειξαν ότι οι συγγραφείς του Χάρτη δεν είχαν πρόθεση να συμπεριλάβουν στο περιεχόμενο της βίας τον οικονομικό εξαναγκασμό ή την άσκηση πολιτικής πίεσης.[62] Το αποτέλεσμα, ωστόσο, θα πρέπει να περιέχει οπωσδήποτε χρήση (ή απειλή) βίας ανεξαρτήτως με ποια μέσα αυτή θα ασκηθεί, δηλαδή κινητικά είτε ηλεκτρονικά, στη σημερινή εποχή.[63] Είναι, εμφανές, από τα παραπάνω ότι η έννοια της «Επίθεσης» κατά τα προηγούμενα χρόνια αναφερόταν πρωτίστως στον κινητικό χώρο. Ακόμη και όταν, το 1974, ορίστηκε η έννοια της «Επίθεσης» από τη Γενική Συνέλευση των Ηνωμένων Εθνών με το Ψήφισμα 3314, ο προσδιορισμός αυτής δε θα μπορούσε να συμπεριλάβει ή να προβλέψει το πεδίο του κυβερνοχώρου καθώς την τότε εποχή ήταν υποτυπώδες.[64] Επομένως, στη συνέχεια της παρούσας μελέτης πρέπει, πρώτα, να προσδιοριστεί η έννοια της χρήσης βίας στον κυβερνοχώρο και έπειτα οι πράξεις για τις οποίες μπορεί μια κυβερνοεπίθεση να θεωρηθεί ως «ένοπλη επίθεση» σε σχέση πάντοτε με την αλληλεπίδραση «έξυπνων» συστημάτων τεχνητής νοημοσύνης.

Α.2.2. Οι κυβερνοεπιχειρήσεις ως «χρήση βίας». Η περίπτωση της κυβερνοεπίθεσης ως ένοπλη επίθεση.

Η απουσία σαφούς ορισμού, όπως προαναφέρθηκε, της έννοιας της «χρήσης βίας» οδηγεί αντίστοιχα και στη δυσκολία προσδιορισμού αυτής στον κυβερνοχώρο. Η προσπάθεια οριοθέτησής της, στο άυλο αυτό πεδίο, επιχειρείται μέσω μιας αναλογικής προσέγγισης των αποτελεσμάτων που οι κυβερνοεπιχειρήσεις μπορεί να επιφέρουν.[65] Οι επιθετικές ενέργειες, δηλαδή, στο πεδίο του κυβερνοχώρου που θα προκαλέσουν καταστροφή περιουσίας ή τραυματισμό ανθρώπων, αναλογούν σε χρήση βίας και, επομένως, απαγορεύονται βάσει του Άρθρου 2(4) του Χάρτη των Ηνωμένων

---

[61] M Roscini, *Cyber Operations and the Use of Force in International Law*, 45-6. Από το προοίμιο του Χάρτη των Ηνωμένων Εθνών, όπως προαναφέρθηκε, συμπεραίνεται ότι ο απώτερος σκοπός του οργανισμού είναι η αποφυγή ενός πολέμου.

[62] T Ruys, *'Armed Attack' and Article 51 of the UN Charter*, 56.

[63] Y Dinstein, *War, Aggression and Self-Defense*, (5th edn, Cambridge: Cambridge University Press, 2012) 88.

[64] Definition of Aggression, GA Res 3314 (XXIX),14 December 1974. Βλέπε για παράδειγμα, το Άρθρο 3, το οποίο παραθέτει συγκεκριμένες επιθετικές ενέργειες. Είναι αντιληπτό ότι αφορούν τον κινητικό χώρο.

[65] M Roscini, *Cyber Operations and the Use of Force in International Law*, 47-8. Η προσέγγιση αυτή φαίνεται να είναι κοινώς αποδεκτή. Για παράδειγμα, βλέπε και τον Κανόνα 11 στο *Εγχειρίδιο του Τάλλιν*. Όπως αναφέρει ο Roscini, άλλες προσεγγίσεις βάσει των μέσων ή του στόχου, φαίνονται ανεπαρκείς στην ερμηνεία της χρήσης βίας στον κυβερνοχώρο.

Εθνών.[66] Την άποψη αυτή επιβεβαίωσε το 2012 και ο νομικός σύμβουλος του Υπουργείου Εξωτερικών των ΗΠΑ, καθηγητής H. Koh, όπου χαρακτηριστικά ανέφερε σε ομιλία του ότι «*οι δραστηριότητες στον κυβερνοχώρο που σχεδόν προκαλούν θάνατο, τραυματισμό ή σημαντική καταστροφή θα θεωρούνται ενδεχομένως ως χρήση βίας*».[67] Για παράδειγμα, μια κυβερνοεπίθεση θα μπορούσε να προκαλέσει την καταστροφή ενός πυρηνικού αντιδραστήρα, μέσω του ηλεκτρονικού δικτύου του, ενώ το ίδιο αποτέλεσμα, παραδοσιακά, θα μπορούσε να είχε επιτευχθεί μέσω ενός βομβαρδισμού με συμβατικά όπλα. Συνεπώς, τέτοιες κυβερνοεπιθέσεις θεωρούνται ως χρήση βίας και βάσει του Άρθρου 2(4) του Χάρτη των Ηνωμένων Εθνών, απαγορεύονται.[68] Ωστόσο, οι κυβερνοεπιχειρήσεις που στοχεύουν στην παράνομη μεν εκμετάλλευση υπολογιστών, υποκλέβοντας για παράδειγμα μόνο κάποια στοιχεία, δε θεωρούνται ως χρήση βίας εάν ταυτόχρονα δεν προκαλούν φθορά, τροποποίηση ή διαγραφή στα δεδομένα αυτά.[69] Από την άλλη πλευρά, ορισμένες κυβερνοεπιχειρήσεις μπορεί να προκαλούν φθορά σε διάφορα συστήματα και εγκαταστάσεις χωρίς να υπάρχουν εμφανή αποτελέσματα καταστροφής ή τραυματισμού ανθρώπων. Στην περίπτωση, όμως, που κυβερνοεπιθέσεις προκαλούν ουσιαστική ζημιά σε δίκτυα κρίσιμων υποδομών ενός κράτους, επηρεάζοντας παράλληλα και την καθημερινότητα της κοινωνίας, τότε αυτές εμπίπτουν στην έννοια της χρήσης βίας.[70] Για παράδειγμα, οι μαζικές κυβερνοεπιθέσεις στα χρηματοπιστωτικά ιδρύματα μιας χώρας θα μπορούσαν, ενδεχομένως, να προκαλέσουν μια προσωρινή απορρύθμιση της αγοράς καθώς και να σπείρουν ένα κλίμα πανικού στην κοινωνία.

Ο προσδιορισμός, ωστόσο, των «κρίσιμων υποδομών» ('critical infrastructures') ενός κράτους, είναι ένα σημαντικό ερώτημα προτού μια κυβερνοεπίθεση χαρακτηριστεί ως χρήση βίας σε αυτούς τους τομείς. Σύμφωνα με την 2001 PATRIOT Act των ΗΠΑ, ως «κρίσιμες υποδομές» νοούνται «*τα συστήματα και τα περιουσιακά στοιχεία, φυσικά και εικονικά, που είναι τόσο ζωτικά για τις Ηνωμένες Πολιτείες, που ανικανότητα ή η καταστροφή τέτοιων συστημάτων και περιουσιακών*

---

[66] R Buchan, 'Cyber Attacks: Unlawful Uses of Force or prohibited Interventions?', *Journal of Conflict & Security Law*, (2012) Vol 17 No 2, 212

[67] H Koh, 'International Law in Cyberspace; remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012'. *Harvard International Law Journal*, (December 2012) Vol 54, 3-4.

[68] Ibid

[69] M Roscini, 'Cyber Operations as a Use of Force'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace*, 240.

[70] K Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict', *Military Law and the Law of War review,* (2010) Vol 49, 74-5.

στοιχείων θα είχε εξασθενητικό αντίκτυπο στην ασφάλεια, την εθνική οικονομική ασφάλεια, την εθνική δημόσια υγεία ή σε οποιονδήποτε συνδυασμό αυτών των τομέων».[71] Παρόμοια προσέγγιση, δίνει και το Συμβούλιο της Ευρωπαϊκής Ένωσης σε Οδηγία του, το 2008, ορίζοντας τις «κρίσιμες υποδομές» ως «*ένα περιουσιακό στοιχείο, ένα σύστημα ή μέρος αυτού που βρίσκεται στα κράτη μέλη και το οποίο είναι ουσιώδες για τη διατήρηση των ζωτικών κοινωνικών λειτουργιών, την υγεία, την προστασία, την ασφάλεια, την οικονομική ή κοινωνική ευημερία των ανθρώπων και των οποίων η διακοπή ή καταστροφή θα είχε σημαντικές επιπτώσεις σε ένα κράτος μέλος ως αποτέλεσμα της αδυναμίας διατήρησης αυτών των λειτουργιών*».[72] Λαμβάνοντας υπόψη και τις προσεγγίσεις άλλων κρατών, μπορεί να ειπωθεί ότι οι «κρίσιμες υποδομές» ενός κράτους, περικλείουν, ενδεικτικά, τους τομείς της ενέργειας, των τηλεπικοινωνιών, των μεταφορών, των αναγκαίων αγαθών, του τραπεζικού συστήματος, της δημόσιας υγείας, του υδρευτικού δικτύου καθώς επίσης και οτιδήποτε άλλο σχετίζεται με την εθνική ασφάλεια.[73] Για παράδειγμα, σύμφωνα με τη λίστα του Υπουργείου Εσωτερικών των ΗΠΑ, ο τομέας των επικοινωνιών αποτελεί μια σημαντική κατηγορία «κρίσιμης υποδομής».[74] Για αυτό το λόγο, η παρουσία ρωσικών υποβρυχίων σε περιοχές όπου βρίσκονται κεντρικά καλώδια τηλεπικοινωνιών στην ανοιχτή θάλασσα προκαλεί ιδιαίτερη ανησυχία στις ΗΠΑ και το ΝΑΤΟ.[75] Μια πιθανή καταστροφή, σε συγκεκριμένα κομβικά σημεία, θα είχε οδυνηρές συνέπειες στις τηλεπικοινωνίες καθώς επίσης, θα επηρέαζε, εμμέσως, και τη διακίνηση του παγκόσμιου εμπορίου και κεφαλαίου. Επομένως, είναι εμφανές ότι οι κυβερνοεπιθέσεις σε «κρίσιμους τομείς» επηρεάζουν όχι μόνο την λειτουργία ενός κρατικού τομέα αλλά και μέρος της καθημερινότητας του κοινωνικού συνόλου. Για αυτό το λόγο, παρόλο που τέτοιου τύπου κυβερνοεπιθέσεις δεν προκαλούν κάποια φυσική καταστροφή ή τραυματισμό, αυτές εμπίπτουν στην έννοια της «χρήσης βίας».

---

[71] Public Law 107-56, (26 October 2001) Section 1016(e). Βλέπε αντίστοιχα και τις Προεδρικές Οδηγίες των ΗΠΑ όπου δείχνουν την σημασία προστασίας των κρίσιμων υποδομών, για τις ΗΠΑ, από απειλές του κυβερνοχώρου: 'US President Policy Directive/PPD-20' (October 2012) and 'US President Policy Directive'/PPD-21 (February 2015).

[72] European Council Directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, (23.12.2018) L/345/75.

[73] Αναλυτικότερα, για την προσέγγιση που δίνουν διάφορα κράτη στην έννοια «κρίσιμες υποδομές» βλέπε στο: M Roscini, *Cyber Operations and the Use of Force in International Law*, 55-63

[74] US Department of Homeland Security, 'Critical Infrastructure Sectors' at: <https://www.dhs.gov/critical-infrastructure-sectors> accessed 19.10.2018

[75] D E Sanger and E Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *New York Times*, (25 October 2015) at: <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0> accessed 19.10.2018

Παράλληλα, το *Εγχειρίδιο του Ταλλίν*, κατά την ίδια αντίληψη με τα προαναφερθέντα, επιχειρεί μια πιο ευρεία ερμηνεία της «χρήσης βίας». Αρχικά, οι συγγραφείς του εγχειριδίου, ερμηνεύοντας αναλογικά και την *Υπόθεση Νικαράγουα* του 1986, προτείνουν ότι μια κυβερνοεπιχείρηση συνιστά χρήση βίας λόγω της έντασης και των αποτελεσμάτων της.[76] Το Διεθνές Δικαστήριο, ωστόσο, είχε ερμηνεύσει ότι η «απλή οικονομική υποστήριξη» ανταρτών δεν θεωρείται ως χρήση βίας ενώ ο «εξοπλισμός και η εκπαίδευση» αυτών, που συμμετέχουν στις εχθροπραξίες κατά άλλου κράτους, είναι.[77] Αναλογικά επομένως, κατά το *Εγχειρίδιο*, η απλή χρηματοδότηση μιας ομάδας χάκερ που συμμετέχουν σε κυβερνοεπιχειρήσεις, κατά άλλου κράτους, δεν μπορεί να χαρακτηριστεί ως χρήση βίας. Αντιθέτως, ο εφοδιασμός τέτοιων ομάδων με υλικοτεχνικό εξοπλισμό και λογισμικό, για τη συμμετοχή τους στις κυβερνοεχθροπραξίες, την συνιστά.[78] Ωστόσο, οι έννοιες «ένταση και αποτελέσματα» είναι αρκετά γενικές ως προς τον χαρακτηρισμό μιας κυβερνοεπιχείρησης ως χρήση βίας. Για αυτό το λόγο, οι συγγραφείς του εγχειριδίου έχουν προτείνει, ενδεικτικά, μερικούς παράγοντες που ένα κράτος είναι πιθανό να εξετάσει και να δώσει βαρύτητα προκειμένου να αξιολογήσει εάν μια κυβερνοεπίθεση μπορεί να θεωρηθεί ως χρήση βίας.[79] Αυτοί οι παράγοντες είναι: η σοβαρότητα της πράξης (δηλαδή της καταστροφής ή του τραυματισμού που αυτή επιφέρει), η αμεσότητα (η ταχύτητα με την οποία οι συνέπειες εκδηλώνονται), η ευθύτητα (ο βαθμός σύνδεσης της κυβερνοεπιχείρησης σε σχέση με τα αποτελέσματα που προκύπτουν), η διεισδυτικότητα (ο βαθμός που μια κυβερνοεπιχείρηση διεισδύει μέσα στο στοχοποιημένο σύστημα), η μετρησιμότητα των συνεπειών, ο στρατιωτικός χαρακτήρας της κυβερνοεπιχείρησης, η συμμετοχή του κράτους και η τεκμαιρόμενη νομιμότητα αυτής.

Η υποκειμενική ερμηνεία των παραπάνω παραγόντων καθώς και τα διαφορετικά περιστατικά κυβερνοεπιθέσεων, έχουν πυροδοτήσει μια συζήτηση μεταξύ των συγγραφέων σχετικά με την πληρότητα των παραπάνω κριτηρίων. Ενδεικτικά, για παράδειγμα, η Ziolkowski θεωρεί ότι τα κριτήρια της αμεσότητας και της ευθύτητας μη ικανοποιητικά λόγω της πολυπλοκότητας των σύγχρονων ηλεκτρονικών συστημάτων.[80] Όπως αναφέρει, οποιαδήποτε ένδειξη δυσλειτουργίας ενός συστήματος

---

[76] *Tallin Manual*, 45-52

[77] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v USA*) (Merits) [1986] ICJ Rep 14, para 228 (*Nicaragua Case*).

[78] *Tallinn Manual*, 46

[79] Ibid

[80] Αναλυτικότερα βλέπε στο: K Ziolkowski, '*Jus ad Bellum* in Cyberspace- Some Thoughts on the "Schmitt-Criteria" for Use of Force'. 4th International Conference on Cyber Conflict, (NATO CCD COE

δε θα μπορεί να κριθεί εύκολα και άμεσα ως αποτέλεσμα μιας κυβερνοεπίθεσης καθώς πρώτα πρέπει να διερευνηθεί η πιθανότητα αστοχίας του ίδιου του συστήματος σε επίπεδο υλικού (hardware) ή λογισμικού (software) και αυτή να εξεταστεί, πρώτα, από τους αρμόδιους κατασκευαστές. Ενώ, όπως επισημαίνει και ο Τσαγγούριας, μπορεί να υπάρχουν διακεκομμένα στάδια κατά διεξαγωγή μιας κυβερνοεπίθεσης, όπως στην περίπτωση του Stuxnet. Δηλαδή, πρώτα να γίνει η ηλεκτρονική εισαγωγή του ιού, έπειτα να επέλθει μια περίοδος παύσης, στη συνέχεια να φορτωθεί το κακόβουλο λογισμικό στο σύστημα και τέλος να εκδηλωθούν, σταδιακά, οι όποιες συνέπειες.[81] Επομένως, τα κριτήρια, για παράδειγμα, της αμεσότητας και της ευθύτητας περιπλέκουν, ενίοτε, οποιαδήποτε αξιολόγηση, καθώς οι συνέπειες μιας κυβερνοεπίθεσης μπορεί να εκτελούνται κατά έμμεσο τρόπο χωρίς να προκαλούν άμεσα εμφανή αποτελέσματα. Παράλληλα, τα αποτελέσματα αυτής μπορεί να επηρεάζουν, μακροπρόθεσμα, άλλα συνδεδεμένα περιφερειακά συστήματα, προκαλώντας σε αυτά σημαντικά προβλήματα.[82] Επιπλέον, και το κριτήριο της μετρησιμότητας των συνεπειών είναι σχετικό, καθώς δεν μπορεί για παράδειγμα να εκτιμηθεί συνολικά το κατά πόσο η περίπτωση του Stuxnet επηρέασε ολόκληρο το πυρηνικό πρόγραμμα του Ιράν.[83] Τέλος, και το κριτήριο της συμμετοχής του κράτους, είναι λόγω της φύσης του κυβερνοχώρου και της ανωνυμίας που προσφέρει, ιδιαίτερα προβληματικό και δύσκολο να αποδοθεί στην πράξη, όπως θα αναφερθεί σε επόμενο κεφάλαιο. Αντιστοίχως, εφαρμόζοντας τα παραπάνω κριτήρια στην περίπτωση της Εσθονίας, το 2007, είναι δύσκολο να χαρακτηριστεί η κυβερνοεπίθεση που δέχτηκε ως χρήση βίας, καθώς η σοβαρότητα όσο αφορά τη διάρκεια και το σκοπό της, είναι περιορισμένη και επιπλέον η απόδοση αυτής προς κάποιο κράτος δεν αποδείχθηκε ποτέ.[84] Όμως, στην περίπτωση του Stuxnet, ενδεχομένως, να μπορούσε να θεωρηθεί ως χρήση βίας καθώς ο ιός φαίνεται να προκάλεσε υλικές ζημιές στο πυρηνικό πρόγραμμα του Ιράν. Σύμφωνα με το Ινστιτούτο για την Επιστήμη και τη Διεθνή Ασφάλεια, το Ιράν αντικατέστησε 1,000 φυγοκεντρωτές σε εργοστάσιο εμπλουτισμού,

---

Publications, 2012), 295-309, at: <http://www.ccdcoe.org/publications/2012proceedings/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf>, accessed 17.10.2018

[81] N Tsagourias, 'Chapter 2: The Tallin Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II-The Use of Force', *Yearbook of International Humanitarian Law*, Vol 15, 23-5.

[82] Ibid

[83] Ibid

[84] Ibid. Βλέπε επίσης: R Buchan, 'Cyber Attacks: Unlawful Uses of Force or prohibited Interventions?', 218-9.

αριθμός αρκετά μεγάλος ώστε να πιστεύεται ότι είναι αποτέλεσμα του κακόβουλου λογισμικού.[85]

Τα κριτήρια χαρακτηρισμού μιας κυβερνοεπιχείρησης ως χρήση βίας, είναι όπως προαναφέρθηκε, ως ένα βαθμό υποκειμενικά λόγω της φύσεως και των περιστάσεων στον κυβερνοχώρο. Η συμβολή, ωστόσο, της τεχνολογίας μέσω των αυτόματων συστημάτων τεχνητής νοημοσύνης θα ήταν καθοριστική στον προσδιορισμό και χαρακτηρισμό των όποιων κυβερνοεπιχειρήσεων ως χρήση βίας. Με τη εφαρμογή, δηλαδή, ενός «έξυπνου» λογισμικού το οποίο εγκαθίσταται σε υπολογιστές ή δίκτυα, θα ανιχνεύεται αυτομάτως αν έχει εισέλθει στο σύστημα κάποιο κακόβουλο λογισμικό και, στη συνέχεια, θα κρίνεται ποια λειτουργικά συστήματα επηρεάζονται ή πρόκειται να επηρεαστούν. Συνολικά, προηγμένα τεχνολογικά προγράμματα μπορούν να αναγνωρίσουν μια κυβερνοεπίθεση και να μετρήσουν την κλίμακα της βλάβης που αυτή προκάλεσε ή πρόκειται να προκαλέσει.[86] Επομένως, με αυτό τον τρόπο, γίνεται και ένα είδους ποσοτικοποίησης των επιπτώσεων της επίθεσης από τα αυτοματοποιημένα συστήματα, κάτι που από μόνος του ο ανθρώπινος παράγοντας αδυνατεί, συνήθως, να κάνει αφού οι συνέπειες δεν είναι πάντοτε εμφανείς. Κατά τη γνώμη μου, η χρήση συστημάτων τεχνητής νοημοσύνης για την αναγνώριση μιας κυβερνοεπίθεσης είναι απαραίτητη. Οι υπολογιστές έχουν τη δυνατότητα να επεξεργάζονται στιγμιαία την τεράστια και συνεχή ροή δεδομένων που διαχέονται μέσα στα ηλεκτρονικά δίκτυα.[87] Ο σκοπός είναι να διαγνωστεί όσο το δυνατόν έγκαιρα μια κυβερνοεπίθεση, προτού αυτή έχει ολοκληρώσει τον κύκλο της, έχοντας περιορίσει έτσι τις συνέπειες που θα επέλθουν, στον ελάχιστο βαθμό. Για παράδειγμα, στην περίπτωση του Stuxnet, το κακόβουλο λογισμικό εικάζεται ότι είχε εισαχθεί στο δίκτυο των υπολογιστών αρκετό καιρό προτού εκδηλωθούν οι λεγόμενες

---

[85] D Albright, P Brannan and C Walrond, 'Reports. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment', *Institute for Science and International Security*, (22 December 2018) at: <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/> accessed 19.12.2018. Το Ιράν, παρόλα αυτά, δεν έδωσε πολιτική έκταση στο συμβάν και δεν παραδέχθηκε ευθέως την φθορά που προκάλεσε το κακόβουλο λογισμικό στο πυρηνικό του πρόγραμμα. Για αυτό, κατά την άποψη μου, η περίπτωση του Stuxnet δεν φαίνεται, να αποτελεί ένα ιδανικό πρακτικό παράδειγμα μελέτης της χρήση βίας στο πεδίο του κυβερνοχώρου. Αναλυτικότερα βλέπε στο: G D Brown, 'Why Iran Didn't Admit Stuxnet Was an Attack', *Joint Force Quarterly*, (4th quarter 2011) Issue 63, at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485181?> accessed 19.12.2018

[86] N Tsagourias and R Buchan, 'Automatic Cyber Defence and the Laws of War', *German Yearbook of International Law*, (2017) Vol 60, 6-7.

[87] Βλέπε περισσότερα στην παρούσα εργασία, το υποκεφάλαιο Α.1.2.

επιπτώσεις στους φυγοκεντρωτές.[88] Επομένως, ο ανθρώπινος παράγοντας θα βρίσκεται συνήθως σε δυσχερή θέση όσον αφορά την έγκαιρη αναγνώριση και το χαρακτηρισμό μιας κυβερνοεπιχείρησης ως χρήση βίας, και για αυτό το λόγο θεωρώ τη συνδρομή των «έξυπνων» λειτουργικών συστημάτων, πλέον, απαραίτητη.

Από τη στιγμή που μια κυβερνοεπίθεσης αναγνωριστεί και αξιολογηθεί από τα συστήματα τεχνητής νοημοσύνης ως χρήση βίας, μια αυτόματη απάντηση από αυτά στο πλαίσιο της ενεργητικής κυβερνοάμυνας θα μπορούσε να έχει δύο ενδεχόμενα. Είτε να είναι ως νόμιμη κυβερνοάμυνα υπό το Άρθρο 51 του Χάρτη εφόσον η κυβερνοεπίθεση συνιστά «ένοπλη επίθεση» ή σε διαφορετική περίπτωση, να είναι με τη μορφή κυβερνοαντιμέτρων. Η παρούσα μελέτη θα εξετάσει μόνο την πρώτη περίπτωση, δηλαδή το δικαίωμα της νόμιμης άμυνας στον κυβερνοχώρο μέσω της συμβολής «έξυπνων» συστημάτων. Όσο αφορά τα κυβερνοαντίμετρα, οι συγγραφείς του *Εγχειριδίου του Ταλίν* καταλήγουν ότι υφίσταται το δικαίωμα του θιγόμενου κράτους να χρησιμοποιήσει αναλογικά κυβερνοαντίμετρα κατά του κράτους που διεξήγαγε την παράνομη διεθνή πράξη.[89]

Α.2.2.1. *Η κυβερνοεπίθεση ως «ένοπλη επίθεση».*

Σύμφωνα με το Άρθρο 51, ένα κράτος μπορεί να επικαλεστεί το δικαίωμα της νόμιμης άμυνας σε περίπτωση που δεχθεί ένοπλη επίθεση από ένα άλλο κράτος. Ωστόσο, η έννοια της «ένοπλης επίθεσης» θα ερμηνευτεί αρκετά χρόνια αργότερα, το 1986, από το Διεθνές Δικαστήριο στην *Υπόθεση Νικαράγουα*. Το Δικαστήριο, αρχικώς, απεφάνθει ότι πρέπει να γίνει διάκριση μεταξύ «*των ακραίων μορφών χρήσης βίας (αυτών που συνιστούν ένοπλη επίθεση) και άλλων λιγότερο ακραίων μορφών*».[90] Με αναφορά στη Διακήρυξη των Φιλικών Σχέσεων,[91] το Δικαστήριο παραθέτει ορισμένες μορφές χρήσης βίας, που θεωρούνται λιγότερο σοβαρές, όπως για παράδειγμα η υποχρέωση των κρατών να μη προσφεύγουν σε αντίποινα καθώς και στην απειλή ή χρήση βίας προκειμένου να παραβιάζουν υπάρχοντα διεθνή σύνορα. Στη συνέχεια, ξεχώρισε τις πράξεις που συνιστούν «ένοπλη επίθεση» βάσει των κριτηρίων της

---

[88] J Finkle, 'Researchers say Stuxnet was deployed against Iran in 2007', *Reuters*, (26 February 2013) at: <https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226> accessed 19.12.2018

[89] *Tallin Manual*, 36-41.

[90] *Nicaragua Case*, para 191. Την ερμηνεία αυτή επανέλαβε, αργότερα, και στην Υπόθεση Εξεδρών Πετρελαίου το 2003. *Case Concerning Oil Platforms* (*Islamic Republic of Iran v. USA*) (Merits) [2003] ICJ Rep 161, para 51 (*Oil Platform Case*).

[91] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), 24 October 1970.

«*έντασης και των αποτελεσμάτων*» ("*scale and effects"*) τους.[92] Η «ένταση» μπορεί να εξαρτάται από την ποσότητα της χρησιμοποιούμενης βίας, τη διάρκεια της επίθεσης ή την τοποθεσία της, ενώ τα «αποτελέσματα» χαρακτηρίζονται από τη ζημιά ή τα θύματα που η επίθεση έχει επιφέρει.[93] Ως προς το τελευταίο, πιθανοί παράγοντες μπορεί να συμπεριλαμβάνουν και την πρόθεση του δράστη (εάν η επίθεση είναι σκόπιμη ή τυχαία) καθώς και τα κίνητρα του (εάν έγινε για παράδειγμα για λόγους εδαφικής κατάκτησης ή για την αλλαγή ενός καθεστώτος).[94] Επιπλέον, μια επίθεση μπορεί να μην διεξάγεται πάντοτε υπό την παραδοσιακή αντίληψη ενός, για παράδειγμα, τακτικού εχθρικού στρατού ο οποίος διαπερνά τα σύνορα ενός άλλου αντίπαλου κράτους. Το Δικαστήριο έχει ερμηνεύσει, επικαλούμενο και το Άρθρο 3 (ζ) του Ορισμού της Επίθεσης,[95] ότι η δράση εκ μέρους ή για λογαριασμό του κράτους, ενόπλων ομάδων που δραστηριοποιούνται στο έδαφος άλλου κράτους θα συνιστά ένοπλη επίθεση για το πρώτο, σε περίπτωση που οι πράξεις αυτών πληρούν τα κριτήρια της «έντασης» και των «αποτελεσμάτων».[96] Ωστόσο, όπως θα αναλυθεί στο επόμενο κεφάλαιο, θα πρέπει παράλληλα να υφίσταται και ο «αποτελεσματικός έλεγχος του κράτους» για να του αποδοθούν οι πράξεις αυτές.

Αναλογικά, βάσει των παραπάνω, μια κυβερνοεπίθεση που προκαλεί σοβαρό ανθρώπινο τραυματισμό ή και υλική ζημιά θα θεωρείται ότι συνιστά «ένοπλη επίθεση» και, επομένως, θα πυροδοτεί το δικαίωμα της νόμιμης κυβερνοάμυνας από το θιγόμενο κράτος.[97] Η θεώρηση αυτή είναι σύμφωνη, επίσης, και με τη *Γνωμοδότηση για τη Νομιμότητα της Απειλής ή της Χρήσης Πυρηνικών Όπλων*, του Διεθνούς Δικαστηρίου, το 1996. Ουσιαστικά, το Δικαστήριο υποστήριξε ότι τα Άρθρα 2(4), 51 και 42 του Χάρτη των Ηνωμένων Εθνών «*δεν αναφέρονται σε συγκεκριμένα όπλα*» και οι διατάξεις των παραπάνω άρθρων «*ισχύουν για κάθε χρήση βίας, ανεξάρτητα από τα χρησιμοποιούμενα όπλα*».[98] Επομένως, η επιλογή των μέσων για τη διεξαγωγή μιας επίθεσης είναι άσχετη από το ζήτημα εάν αυτή συνιστά «ένοπλη επίθεση». Επιπλέον,

---

[92] *Nicaragua Case*, para 195.

[93] T Ruys, *'Armed Attack' and Article 51 of the UN Charter*, 139.

[94] Ibid

[95] Οπ. π., υποσημείωση 64.

[96] *Nicaragua Case*, para 195.

[97] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 231. M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', (2010) *Max Planck Yearbook of United Nations Law,* Vol 14, 114-9. K Kittichaisaree, *Public International Law of Cyberspace*, (Springer International Publishing Switzerland, 2017) Governance and Technology Series Vol 32, 166-8. *Tallin Manual*, 54-8.

[98] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion of 8 July 1996) [1996] ICJ Rep 226, paras 38-9. (*Nuclear Weapons*)

η χρήση μη κινητικών όπλων όπως των βιολογικών ή χημικών, θεωρείται κοινώς αποδεκτή ως «χρήση βίας» ενώ το επίπεδο της «έντασης και των αποτελεσμάτων» τους, μπορεί να συνιστά μια «ένοπλη επίθεση» η οποία να πυροδοτήσει στη συνέχεια το δικαίωμα της νόμιμης άμυνας.[99] Ωστόσο, το «κενό» μεταξύ του Άρθρου 2(4) και του Άρθρου 51 δεν απαραιτήτως ευρύ, καθώς το Διεθνές Δικαστήριο στην *Υπόθεση Εξεδρών Πετρελαίου*, δεν απέκλειε την «*πιθανότητα, η καταστροφή και ενός μόνο πλοίου από νάρκη, να είναι επαρκής για να ενεργοποιηθεί το 'φυσικό δικαίωμα της νόμιμης άμυνας'*».[100] Το *Εγχειρίδιο του Ταλλίν*, επιβεβαιώνει την, παραπάνω, αναλογική ερμηνεία της χρήση βίας στον κυβερνοχώρο βάσει της σοβαρότητας των αποτελεσμάτων που μια κυβερνοεπίθεση μπορεί να επιφέρει.[101] Για παράδειγμα, όπως αναφέρθηκε προηγουμένως, μια κυβερνοεπίθεση θα μπορούσε να προκαλέσει έκρηξη σε ένα πυρηνικό αντιδραστήρα, τροποποιώντας τα δεδομένα στο ηλεκτρονικό του σύστημα με σκοπό να λειτουργήσει εκτός των προβλεπόμενων ορίων. Αυτό θα επέφερε, ενδεχομένως, και τον άμεσο τραυματισμό ή θάνατο ανθρώπων, πέρα από τις σοβαρές υλικές ζημιές. Επιπροσθέτως, η τυχόν διαρροή ραδιενέργειας στην ευρύτερη περιοχή θα επηρέαζε την υγεία, περεταίρω ατόμων καθώς επίσης θα επιβάρυνε και το ίδιο το περιβάλλον. Συνεπώς, μια τέτοιου τύπου κυβερνοεπίθεση συνιστά, αναλογικά, μια «ένοπλη επίθεση» κατά το Άρθρο 51 του Χάρτη.

Ένα κρίσιμο, ωστόσο, ερώτημα γεννάται στο κατά πόσο η διεξαγωγή μιας κυβερνοεπίθεσης σε κρίσιμες υποδομές ενός κράτους, που δεν προκαλεί φυσική ζημιά ή τραυματισμό, μπορεί να θεωρηθεί ως μια ένοπλη επίθεση, ενεργοποιώντας το δικαίωμα για νόμιμη άμυνα από το θιγόμενο κράτος. Κατά τον Τσαγγούρια, μια κυβερνοεπίθεση σε κρίσιμες υποδομές που «*παραλύει ή μαζικά διαταράσσει τις δομές ενός κράτους πρέπει να εξομοιώνεται με ένοπλη επίθεση, ακόμη και αν δεν προκαλεί άμεση ανθρώπινη βλάβη ή υλική ζημιά*».[102] Η άποψη αυτή επιβεβαιώνεται, κατά τη γνώμη μου, αν λάβουμε υπόψη τα αλυσιδωτά αποτελέσματα που μια κυβερνοεπίθεση σε τέτοιους κρίσιμους τομείς, μπορεί να επιφέρει. Για παράδειγμα, μια κυβερνοεπίθεση θα μπορούσε να στοχεύει στην κατάλυση των δικτύων των τραπεζικών συστημάτων μιας χώρας καθώς και στο ίδιο το χρηματιστήριο. Σε περίπτωση που η πράξη είναι υψηλής έντασης και μακράς διάρκειας, θα προκαλούσε, ενδεχομένως, σοβαρά

[99] I Brownlie, *International Law and the Use of Force by States*, (Oxford: Clarendon Press, 1963), 362-3. M Roscini, *Cyber Operations and the Use of Force in International Law*, 50.

[100] *Oil Platform Case*, para 72.

[101] *Tallin Manual*, 54-5.

[102] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 231.

προβλήματα στην κίνηση του κεφαλαίου και στο εμπόριο ενώ γενικότερα θα συνέβαλε στην απορρύθμιση της αγοράς, επηρεάζοντας άμεσα την καθημερινή ζωή των ανθρώπων μιας κοινωνίας. Συνεπώς, μια κυβερνοεπίθεση μπορεί να μην επιφέρει άμεση υλική ζημιά ή τραυματισμό αλλά να επηρεάζει δυσμενώς την λειτουργία του κράτους καθώς και την καθημερινότητα των πολιτών και επομένως να ισοδυναμεί, αντίστοιχα, με μια «ένοπλη επίθεση».

Η συμβολή της τεχνολογίας και των αυτόματων συστημάτων στην διαδικασία χαρακτηρισμού κυβερνοεπιθέσεων ως «ένοπλη επίθεση», είναι ιδιαίτερα σημαντική, ιδίως στις περιπτώσεις που τα αποτελέσματα αυτών δεν είναι άμεσα εμφανή. Στο παράδειγμα που μόλις ανέφερα, θεωρώ ότι ο ανθρώπινος παράγοντας θα είναι, πάντοτε, σε μειονεκτική θέση να αντιληφθεί και να αξιολογήσει εγκαίρως τις πολλαπλές και παράλληλες κυβερνοεπιθέσεις που έχουν ως στόχο τα χρηματοπιστωτικά ιδρύματα μιας χώρας και γενικότερα το οικονομικό σύστημα του ίδιου του κράτους. Επομένως, χωρίς την αξιοποίηση της τεχνητής νοημοσύνης, είναι πιθανό η ανθρώπινη εκτίμηση να γίνεται προ τετελεσμένων γεγονότων, έχοντας δηλαδή η κυβερνοεπίθεση ολοκληρώσει το σκοπό της και έχοντας πραγματοποιήσει την όποια ζημιά στην «αγορά». Για αυτό το λόγο, η χρήση «έξυπνων αλγορίθμων» μέσω των αυτόματων συστημάτων θα μπορούν εγκαίρως να επεξεργάζονται, λόγω ταχύτητας, τα ηλεκτρονικά δεδομένα τη στιγμή της επίθεσης, να αναγνωρίζουν ποια αλληλεξαρτώμενα δίκτυα θα επηρεαστούν και τέλος να εκτιμούν ποιοι γενικότεροι τομείς επηρεάζονται, συνεκτιμώντας παράλληλα και τις επιπτώσεις που το ίδιο το κοινωνικό σύνολο ενδέχεται να δεχθεί.

Αφού αναγνωριστεί μια κυβερνοεπιχείρηση ως χρήση βίας, τα «έξυπνα» συστήματα θα μπορούν προχωρήσουν σε μια αυτόματη νόμιμη κυβερνοάμυνα εφόσον η κυβερνοεπίθεση συνιστά μια «ένοπλη επίθεση». Ωστόσο, προτού επιχειρηθεί οποιαδήποτε ενέργεια απάντησης από το θιγόμενο κράτος, θα πρέπει, πρώτα, να γίνει απόδοση της ευθύνης για την παράνομη πράξη σε κάποιο κράτος. Όπως θα αναλυθεί στη συνέχεια, η διαδικασία αυτή αποτελεί ένα δύσκολο κομμάτι στην περίπτωση του κυβερνοχώρου λόγω των ιδιαίτερων γνωρισμάτων του.

Α.2.3. Το πρόβλημα της απόδοσης ευθυνών στον κυβερνοχώρο.

Τα ιδιαίτερα γνωρίσματα του κυβερνοχώρου, όπως αναφέρθηκε και στο πρώτο κεφάλαιο της παρούσας μελέτης, θέτουν εμπόδια στη διαδικασία εντοπισμού του προσώπου ή των ατόμων που διεξάγουν μια κυβερνοεπίθεση, καθώς επίσης και στην απόδοση της πράξης αυτής σε κάποιο κράτος. Συγκεκριμένα, η ανωνυμία των χρηστών

στο διαδίκτυο, η διεξαγωγή επιθέσεων πολλαπλών σταδίων μέσω τρίτων υπολογιστών και η ταχύτητα ροής των δεδομένων, κάνουν ιδιαιτέρα δυσχερή τη διαδικασία εντοπισμού του ιθύνοντος. Για παράδειγμα, στην περίπτωση της Εσθονίας το 2007 οι κυβερνοεπιθέσεις (τύπου 'DDoS') ενέπλεξαν 80.000 τρίτους υπολογιστές ('botnets') από 178 χώρες, καθιστώντας την αναγνώριση του πραγματικού σχεδιαστή της επίθεσης εμφανώς δύσκολη.[103] Στο σημείο αυτό, είναι σημαντικό να αναφερθεί ότι η απόδοση της ευθύνης στον κυβερνοχώρο δεν καθορίζεται μόνο από την ταυτοποίηση του ατόμου ή της ομάδας ατόμων που τελούν μια πράξη κυβερνοεπίθεσης. Σύμφωνα, μάλιστα, με το *Εγχειρίδιο του Ταλλίν*, το γεγονός της κυβερνοεπίθεσης από μόνο του, παρόλο που μπορεί να φαίνεται ότι προέρχεται από κυβερνητικές δομές ενός συγκεκριμένου κράτους, δεν αποτελεί επαρκή απόδειξη για την απόδοση της ευθύνης στο κράτος αυτό, αλλά ένδειξη πιθανής εμπλοκής του.[104] Επιπλέον, η απουσία συγκεκριμένου νομικού πλαισίου περί της ευθύνης στον κυβερνοχώρο, αφήνει περιθώρια συνεκτίμησης επιπλέον παραγόντων, συμπεριλαμβανομένου και πολιτικών.[105]

Η έκθεση για την ανάπτυξη στο πεδίο των πληροφοριών και των τηλεπικοινωνιών, της Ομάδας Κυβερνητικών Εμπειρογνώμων των Ηνωμένων Εθνών, αναφέρει ότι:

> «τα κράτη πρέπει να τηρούν τις διεθνείς υποχρεώσεις τους όσον αφορά τις διεθνείς παράνομες πράξεις που τους αποδίδονται. Τα κράτη δεν πρέπει να χρησιμοποιούν διακομιστές για να διαπράττουν διεθνείς παράνομες πράξεις. Τα κράτη πρέπει να επιδιώξουν να διασφαλίσουν ότι τα εδάφη τους δεν χρησιμοποιούνται από μη κρατικούς δρώντες για την παράνομη χρήση της τεχνολογίας των πληροφοριών και των επικοινωνιών».[106]

Δεδομένου, λοιπόν, ότι δεν έχει θεσπιστεί κάποιο ειδικό καθεστώς ευθύνης στο πεδίο του κυβερνοχώρου, οι ισχύοντες κανόνες είναι αυτοί που περιλαμβάνονται στα Άρθρα περί Ευθύνης των Κρατών για Διεθνείς Παράνομες Πράξεις, οι οποίοι υιοθετήθηκαν από την Επιτροπή Διεθνούς Δικαίου το 2001 και αργότερα από τη Γενική Συνέλευση του ΟΗΕ.[107] Σύμφωνα με το διεθνές δίκαιο, υπάρχουν τρεις κατηγορίες απόδοσης ευθύνης για μια παράνομη διεθνή πράξη σε ένα κράτος. Πρώτον, η ευθύνη να

---

[103] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 233

[104] *Tallin Manual*, Κανόνας 7.

[105] C Antonopoulos, 'State Responsibility in Cyberspace'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace*, 63.

[106] Οπ. π., υποσημείωση 29.

[107] Βλέπε τα Άρθρα στο: 'Report of the Commission to the General Assembly on the work of its fifty-third session', *Yearbook of the International Law Commission*, (2001) Vol II, 26-30 (Articles on State Responsibility). UN General Assembly, 'Responsibility of States for Internationally Wrongful Acts', A/RES/56/589 (26 November 2001).

καταλογίζεται στα όργανα του κράτους, δεύτερον, να οφείλεται σε πρόσωπα που δεν έχουν επίσημη ιδιότητα αλλά δρουν για λογαριασμό του κράτους και, τρίτον, να προκύπτει για διεθνώς παράνομες πράξεις ιδιωτών στην περίπτωση που το κράτος αναγνωρίζει ή υιοθετεί τη συμπεριφορά αυτών.[108] Σε οποιαδήποτε από τις παραπάνω περιπτώσεις, το δικαίωμα της νόμιμης κυβερνοάμυνας μπορεί να ασκηθεί κατά του επιτιθέμενου κράτους.

Στον κυβερνοχώρο, το *Εγχειρίδιο του Ταλλίν* επιχειρεί, μια ανάλογη προσέγγιση, όσον αφορά τις περιπτώσεις απόδοσης της ευθύνης, για παράνομες πράξεις, σε ένα κράτος.[109] Αντιστοίχως, είναι προφανές ότι η διεξαγωγή μιας κυβερνοεπίθεσης από *de jure* όργανα του κράτους, είναι αυτομάτως αποδοτέα σε αυτό και, επομένως, μπορεί να εγερθεί το δικαίωμα της νόμιμης άμυνας από το θιγόμενο μέρος, εφόσον η κυβερνοεπίθεση ισοδυναμεί με μια «ένοπλη επίθεση».[110] Ωστόσο, οι πληροφορίες σχετικά με την δυνατότητα ενός κράτους να εκτελέσει κυβερνοεπιχειρήσεις είναι, συνήθως, διαβαθμισμένες και μη προσβάσιμες στο ευρύ κοινό.[111] Είναι όμως γεγονός, ότι αρκετά κράτη έχουν δημιουργήσει αρμόδια τμήματα ή τομείς για θέματα κυβερνοασφάλειας. Ενδεικτικά, οι ΗΠΑ έχουν από το 2009 θεσπίσει το United States Cyber Command (USCYBERCOM) με σκοπό να κατευθύνει, να συγχρονίζει και να συντονίζει τον προγραμματισμό και τις επιχειρήσεις στον κυβερνοχώρο καθώς και να μπορεί να υπερασπίζει και να προωθεί τα εθνικά συμφέροντα σε συνεργασία με εγχώριους και διεθνείς εταίρους.[112] Αντίστοιχα, και το Ηνωμένο Βασίλειο δίνει ιδιαίτερη έμφαση στο τομέα της κυβερνοασφάλειας, αναβαθμίζοντας και επενδύοντας σημαντικά κεφάλαια στο Cyber Security Operation Centre, προκειμένου να ανταπεξέλθει στις σύγχρονες προκλήσεις που εγείρονται στον κυβερνοχώρο.[113]

Επιπλέον, υπάρχει και η περίπτωση, το κράτος να φέρει ευθύνη για παράνομες πράξεις ενός προσώπου ή ομάδας ατόμων που δεν αποτελούν κρατικά όργανα, αλλά ασκούν συγκεκριμένες κυβερνητικές αρμοδιότητες (governmental authority),

---

[108] Αναλυτικότερα βλέπε στο: Ε Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (2η έκδοση, Αθήνα: Νομική Βιβλιοθήκη, 2015) 457-461.

[109] *Tallinn Manual*, 30-1.

[110] Articles on State Responsibility, Article 4.

[111] M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', 97-8.

[112] U.S. CYBER COMMAND, 'Mission' at: <https://www.cybercom.mil/About/Mission-and-Vision/> accessed 19.12.2018

[113] UK Ministry of Defense, 'Defence Secretary announces £40m Cyber Security Operations Centre' (1 April 2016) at: <https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre> accessed 19.12.2018

εξουσιοδοτούμενοι από νόμο.[114] Σύμφωνα με το σχολιασμό των Άρθρων περί Διεθνούς Ευθύνης των Κρατών, το εύρος αυτών των αρμοδιοτήτων δεν καθορίζεται ακριβώς διότι «*πέρα από ένα συγκεκριμένο όριο, αυτό που θεωρείται ως 'κυβερνητικό' εξαρτάται από το συγκεκριμένο κοινωνικό περιβάλλον, την ιστορία και τις παραδόσεις του*».[115] Όσον αφορά τον κυβερνοχώρο, πρακτική εφαρμογή του ανωτέρω Άρθρου, αποτελεί η περίπτωση των ιδιωτικών εταιριών που παρέχουν υπηρεσίες κυβερνοασφάλειας στις κρατικές αρχές. Για παράδειγμα, τέτοια αποτελεί η 'National Computer Emergency Response Teams' η οποία παρέχει τις υπηρεσίες της, ως ιδιωτικός φορέας, για την αντιμετώπιση κυβερνοεπιθέσεων, συντονίζοντας παράλληλα τις δράσεις της με τους σχετιζόμενους κυβερνητικούς θεσμούς.[116] Στο σημείο αυτό, αξίζει να αναφερθεί ότι ακόμα και η υπέρβαση των αρμοδιοτήτων που οι σχετικές ιδιωτικές εταιρίες έχουν εξουσιοδοτηθεί να εκτελούν, εγείρει την ευθύνη του κράτους.[117]

Η απόδοση της ευθύνης για την διεξαγωγή μιας κυβερνοεπίθεσης σε ένα κράτος, είναι πιο περίπλοκη στην περίπτωση που αυτή διεξάγεται από άτομα ή ομάδες ατόμων που το ίδιο το κράτος «εκπαιδεύει», «ελέγχει» ή «καθοδηγεί».[118] Η έννοια της «εκπαίδευσης» ερμηνεύεται ως η ύπαρξη μιας σχέσης μεταξύ του κράτους και του δράστη σε κάθε πράξη, μεμονωμένα, που εκτελεί. Αυτό σημαίνει ότι, οι οδηγίες ενός κράτους πρέπει να αποδειχθούνε ότι υφίστανται πίσω από κάθε συγκεκριμένη κυβερνοεπίθεση, προκειμένου αυτή να αποδοθεί σε αυτό.[119] Αντιστοίχως, η ίδια λογική διέπει και την έννοια της «καθοδήγησης».[120] Η δυσκολία έγκειται στον προσδιορισμό του βαθμού του «ελέγχου» που το κράτος ασκεί σε αυτά τα άτομα, καθώς η ίδια η νομολογία του Διεθνούς Δικαστηρίου έχει δώσει, κατά περιπτώσεις, διαφορετικές ερμηνείες. Συγκεκριμένα, το Δικαστήριο στην *Υπόθεση Νικαράγουα* υποστήριξε ότι για να αποδειχθεί η ευθύνη των ΗΠΑ για την δράση των αντικαθεστωτικών 'contras', δεν

---

[114] Article on State Responsibility, Article 5.

[115] Articles on State Responsibility, 43.

[116] Αναλυτικότερα βλέπε στο: M Roscini, *Cyber Operations and the Use of Force in International Law*, 35-6. *Tallin Manual*, 30.

[117] Article on State Responsibility, Article 7.

[118] *Tallinn Manual*, 32. Η θεώρηση αυτή πηγάζει από τα Άρθρα για τη Διεθνή Ευθύνη και συγκεκριμένα από το Άρθρο 8 που αναφέρει ότι: «*Η συμπεριφορά ενός προσώπου ή μιας ομάδας προσώπων θεωρείται πράξη του κράτους βάσει του διεθνούς δικαίου, εάν το πρόσωπο ή η ομάδα προσώπων ενεργεί πράγματι κατόπιν εντολής ή υπό τη διεύθυνση ή τον έλεγχο του εν λόγω κράτους κατά την εκτέλεση του συμπεριφορά*», Articles on State Responsibility, Article 8.

[119] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia)* [2007] ICJ Rep 43, para 400 (*Bosnia Genocide Case*).

[120] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 237.

αρκεί μόνο η χρηματοδότησή τους, η εκπαίδευση και η παροχή προμηθειών και εξοπλισμού, αλλά θα πρέπει να υπάρχει ένας «αποτελεσματικός έλεγχος» ('effective control') στις στρατιωτικές ή παραστρατιωτικές τους επιχειρήσεις.[121] Πρόκειται, συνεπώς, για ένα υψηλό και αυστηρό κριτήριο, για την απόδειξη της ευθύνης του κράτους στον έλεγχο των ενόπλων ομάδων που δρουν στο έδαφος άλλου κράτους. Το Δικαστήριο, επιβεβαίωσε αυτό το υψηλό κριτήριο και στην *Υπόθεση Γενοκτονίας* και συμπλήρωσε ότι ο «αποτελεσματικός έλεγχος» σημαίνει ότι κράτος καθοδηγεί κάθε πράξη των ατόμων ή ομάδων που διαπράττουν τις παραβιάσεις.[122] Αντιθέτως, το ad hoc Διεθνές Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία στην *Υπόθεση Tadic*, υιοθέτησε ένα λιγότερο αυστηρό κριτήριο, όσο αφορά τον έλεγχο επί των ατόμων, μιλώντας για «συνολικό έλεγχο» του κράτους. Αρχικώς, υποστήριξε, ότι ο βαθμός ελέγχου μπορεί να διαφοροποιείται ανάλογα με τα πραγματικά περιστατικά της κάθε περίπτωσης.[123] Στη συνέχεια, όμως, αποφάνθηκε ότι ένα κράτος «*ασκεί γενικό έλεγχο επί των ομάδων, όχι μόνο με τον εξοπλισμό και τη χρηματοδότηση αυτών, αλλά και με το συντονισμό ή τη συνδρομή στο γενικό σχεδιασμό της στρατιωτικής τους δραστηριότητας* […] *χωρίς να είναι απαραίτητο, επιπλέον, το Κράτος να εκδίδει, είτε στον επικεφαλή είτε στα μέλη της ομάδας, οδηγίες για τη διεξαγωγή συγκεκριμένων πράξεων που αντιβαίνουν το διεθνές δίκαιο*».[124] Επομένως, ο «συνολικός έλεγχος» καλύπτει την περίπτωση όπου ένα κράτος ασκεί μια γενική επιρροή σε μια ομάδα ανθρώπων και στις δραστηριότητές αυτών. Για παράδειγμα, με βάσει τα παραπάνω δεδομένα που αφορούν το κριτήριο του συνολικού ελέγχου, ένα κράτος θα μπορούσε θεωρηθεί υπεύθυνο για την διεξαγωγή μιας κυβερνοεπίθεσης από μια ομάδα ατόμων στην περίπτωση που τους παρέχει τεχνική υποστήριξη και γενικώς οργανώνει κάθε δράση τους.[125] Αξίζει, όμως, να σημειωθεί ότι το ad hoc Δικαστήριο υποστήριξε ότι το κριτήριο του «συνολικού ελέγχου» εφαρμόζεται μόνο στην περίπτωση «*μιας οργανωμένης και ιεραρχικά δομημένης ομάδας ατόμων, όπως μιας στρατιωτικής ομάδας, είτε σε οργανωμένους μη τακτικούς μαχητές ή αντάρτες, σε περίπτωση πολέμου*

---

[121] *Nicaragua Case*, paras 115-7. Βλέπε και στο: Στ Περράκης, Μ-Ντ Μαρούδα, Διεθνής Δικαιοταξία, Θεωρία και Εφαρμογή του Διεθνούς Δικαίου, (2η εκδ, Αθήνα: Σιδέρης), 250-1.

[122] *Bosnia Genocide Case*, para 400. Επιπροσθέτως, το Δικαστήριο έκανε λόγο για «αυστηρό έλεγχο» ή για ένα «υψηλό βαθμό ελέγχου του Κράτους», δείχνοντας, με αυτό τον τρόπο, ότι η έννοια του «αποτελεσματικού ελέγχου» συνιστά μια στενή σχέση εξάρτησης μεταξύ κράτους και μη κρατικών δρώντων που ελέγχει. *Bosnia Genocide Case*, paras 391,393.

[123] *Prosecutor v Duško Tadić*, (Appeal) ICTY-94-1-A (15 July 1999), para 117 (*Tadić* Appeal).

[124] *Tadić* Appeal, para 131.

[125] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 238

ή εμφύλιας σύρραξης».[126] Στον κυβερνοχώρο, όμως, ομάδες «χάκερ επαναστατών», οι οποίες να είναι οργανωμένες και ιεραρχικά δομημένες δεν φαίνεται να υπάρχουν στην παρούσα στιγμή.[127]

Το Διεθνές Δικαστήριο, ωστόσο, στην *Υπόθεση Γενοκτονίας* άσκησε κριτική στο κριτήριο του «συνολικού ελέγχου» και επαναβεβαίωσε αυτό του «αποτελεσματικού ελέγχου» που είχε ερμηνεύσει στην *Υπόθεση Νικαράγουα*.[128] Για αυτό το λόγο, η τέλεση της γενοκτονίας δεν αποδόθηκε στη Σερβία καθώς δεν υπήρχε ο «αποτελεσματικός έλεγχος», δηλαδή αυτή η στενή σύνδεση μεταξύ του κράτους και των ενόπλων ομάδων που τέλεσαν τις εγκληματικές πράξεις.[129] Στο σημείο αυτό, όμως, τίθενται δύο σημαντικά ζητήματα. Εάν, αρχικά, το κριτήριο του «αποτελεσματικού ελέγχου» μπορεί να εφαρμοστεί στην περίπτωση του κυβερνοχώρου και, δεύτερον, εάν η συμβολή της τεχνητής νοημοσύνης μπορεί να πετύχει μια αυτόματη διαδικασία απόδοσης της ευθύνης, κατά την παραπάνω νομική προσέγγιση, και χωρίς την επίδραση του ανθρωπίνου παράγοντα.

Η εφαρμογή ενός τόσο αυστηρού κριτηρίου στον κυβερνοχώρο θα καθιστούσε, κατά τη γνώμη μου, τη διαδικασία απόδοσης ευθυνών πολλές φορές αδύνατη, όπως για παράδειγμα, στην περίπτωση που ένα κράτος καθοδηγεί μια ομάδα χάκερ ώστε να διεξάγουν κυβερνοεπιθέσεις κατά άλλου κράτους. Ο «αποτελεσματικός έλεγχος» θα σήμαινε, λόγου χάρη, ότι το κράτος τους παρέχει εκπαίδευση, χρήματα, λογισμικό (software), υλικό (hardware) και καθοδήγηση, σε κάθε πράξη κυβερνοεπίθεσης που αυτοί διεξάγουν. Όμως, το διαδίκτυο, προσφέρει έφορο έδαφος για ανωνυμία και, επομένως, μπορεί πολύ εύκολα να διεκπεραιωθεί οποιαδήποτε συναλλαγή και διακίνηση δεδομένων, χωρίς να αποκαλυφθεί η ταυτότητα των χρηστών.[130] Με τον τρόπο αυτό, ένα κράτος μπορεί ανώνυμα να συνδιαλέγεται με μια ομάδα χάκερ, παρέχοντάς τους οικονομική ενίσχυση, λογισμικό και οδηγίες για την επιλογή των στόχων, χωρίς να φανερωθεί ποτέ, η στενή, μεταξύ τους σχέση. Συνεπώς, η ιδιάζουσα φύση του κυβερνοχώρου καθιστά το κριτήριο του «αποτελεσματικού ελέγχου» αρκετά προβληματικό ώστε να αποδειχθεί η ευθύνη που φέρει ένα κράτος για τις πράξεις του, μέσα στο πεδίο αυτό. Επομένως, δημιουργούνται δυσχέρειες, όσον αφορά στην ενεργοποίηση του δικαιώματος της νόμιμης άμυνας, από το θιγόμενο μέρος. Για την

---

[126] *Tadić* Appeal, para 120.

[127] M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', 100.

[128] *Bosnia Genocide Case*, paras 402-6.

[129] *Bosnia Genocide Case*, paras 395, 413-5.

[130] J A Wood, 'The Darknet: A Digital Copyright Revolution', *Richmond Journal of Law & Technology*, Vol XVI, Issue 4, 18 at: <http://jolt.richmond.edu/jolt-archive/v16i4/article14.pdf> accessed 19.12.2018

αντιμετώπιση αυτού του ζητήματος, θεωρώ απαραίτητη την ύπαρξη ενός πιο ελαστικού κριτηρίου που αφορά το βαθμό «ελέγχου» του κράτους σε μια ομάδα ατόμων χάκερ, στην προκειμένη περίπτωση. Το σκεπτικό αυτό, δεν μπορεί να θεωρηθεί αντίθετο προς τη διεθνή νομολογία που προαναφέρθηκε, καθώς τα διεθνή δικαιοδοτικά όργανα, στην εκάστοτε περίπτωση, ερμήνευσαν το κριτήριο αυτό, υπό διαφορετικό πρίσμα. Για παράδειγμα, το Διεθνές Δικαστήριο στην *Υπόθεση Νικαράγουα*, αναζήτησε την διεθνή ευθύνη των ΗΠΑ για τις στρατιωτικές και παραστρατιωτικές τους δραστηριότητες μέσα από το βαθμό ελέγχου στους αντικαθεστωτικούς 'contras', ενώ το ad hoc Διεθνές Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία, χρησιμοποίησε το ήπιο κριτήριο του «συνολικού ελέγχου» με σκοπό να ορίσει εάν η σύρραξη είναι διεθνής ή μη.[131] Επιπροσθέτως, και τα Άρθρα περί Διεθνούς Ευθύνης των κρατών αναγνωρίζουν ειδικές κατηγορίες στο διεθνές δίκαιο οι οποίες διέπονται από δικούς τους κανόνες διεθνούς ευθύνης ('lex specialis'), όπως στην περίπτωση του ανθρωπιστικού δικαίου.[132] Αναλογικά, λοιπόν, στο πεδίο του κυβερνοχώρου θα ήταν προτιμότερο να εξεταστεί κατά περίπτωση και να χρησιμοποιηθεί ένα αντίστοιχο πιο ήπιο κριτήριο, όπως αυτό του «συνολικού ελέγχου» για να μπορεί να υπάρξει καταλογισμός ευθύνης στο κράτος εφόσον αυτό έχει εμπλοκή στις δράσεις των ομάδων χάκερ, χωρίς όμως την ύπαρξη μιας, απαραίτητα, στενής σχέσης αλληλεξάρτησης, η οποία εκ των πραγμάτων είναι σχεδόν αδύνατη να αποδειχθεί.[133] Ωστόσο, σε περίπτωση διεξαγωγής κυβερνοεπίθεσης από αυτόνομα ηλεκτρονικά συστήματα, με τη χρήση τεχνητής νοημοσύνης, είναι δύσκολο να εξεταστεί το οποιοδήποτε κριτήριο, όταν ο ανθρώπινος παράγοντας δεν έχει καμία επίδραση σε αυτά, γεγονός που δημιουργεί δυσχέρειες στην απόδοση ευθυνών κατά το διεθνές δίκαιο. Η έννοια του «αποτελεσματικού» ή «συνολικού» ελέγχου ενός κράτους, δεν μπορεί να ερμηνευθεί στην περίπτωση των ηλεκτρονικών συστημάτων που λειτουργούν αυτόνομα με τη χρήση τεχνητής νοημοσύνης και 'machine learning'. Για αυτό το λόγο, ως εναλλακτική προσέγγιση θα εξεταστεί, στο δεύτερο μέρος της

---

[131] *Nicaragua Case* para 1, *Tadić* Appeal, paras 88, 97-8.

[132] Articles on State Responsibility, Article 55. Βλέπε για παράδειγμα το Άρθρο 91 του Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), (8 June 1977) 1125 UNTS 3· εισάγει ένα αυστηρό επίπεδο ευθύνης για το κράτος σε περίπτωση που μέλη των ενόπλων δυνάμεών του διαπράξουν παραβιάσεις ανθρωπιστικού δικαίου. Βλέπε επίσης: N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 239.

[133] Από την άλλη πλευρά, ο Roscini ισχυρίζεται ότι ένα πολύ ήπιο και ελαστικό κριτήριο θα μπορούσε να δημιουργήσει προϋποθέσεις ώστε τα κράτη να αλληλοκατηγορούνται επιπόλαια για επιθέσεις στον κυβερνοχώρο (ιδίως εάν το θιγόμενο μέρος κάνει λόγο για το δικαίωμα στη νόμιμη άμυνα). M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', 100.

παρούσας εργασίας, και η νομιμότητα της αυτόματης κυβερνοάμυνας κατά κυβερνοεπίθεσης που προέρχεται από ΜΚΔ από το έδαφος άλλου κράτους ως αυτόνομη πηγή χρήσης βίας και όχι κατά του ίδιου του κράτους.

Τέλος, υπάρχει και η περίπτωση όπου το κράτος φέρει ευθύνη, για διεθνώς παράνομες πράξεις ιδιωτών, στην περίπτωση που αναγνωρίζει ή υιοθετεί τη συμπεριφορά αυτών.[134] Χαρακτηριστικό παράδειγμα είναι η *Υπόθεση* του *Διπλωματικού και Προξενικού Προσωπικού των ΗΠΑ στην Τεχεράνη*, όπου το Διεθνές Δικαστήριο υποστήριξε ότι το Ιράν μπορεί να μην είχε αρχικώς ευθύνη για τις πράξεις των «εξεγερμένων φοιτητών» αλλά υπείχε στη συνέχεια ευθύνη καθώς επικρότησε τη συμπεριφορά αυτών.[135] Ωστόσο, αυτή η περίπτωση ευθύνης είναι πιο δύσκολο να συναντηθεί στον κυβερνοχώρο καθώς οι χρήστες μπορούν να δρουν ανώνυμα χωρίς να αφήνουν ίχνη της ταυτότητάς τους, όπως αναφέρθηκε προηγουμένως.

Με βάση τα παραπάνω, κρίσιμο είναι και το ερώτημα εάν η συμβολή της τεχνητής νοημοσύνης μπορεί να καταλήξει «αυτόματα» σε ένα ασφαλές συμπέρασμα και να καταλογίσει την ευθύνη των όποιων παράνομων κυβερνοπράξεων σε ένα κράτος, χωρίς την επιρροή του ανθρωπίνου παράγοντα. Αντίστοιχα, και σε αυτή την περίπτωση, η φύση του κυβερνοχώρου και οι παράγοντας της ανωνυμίας των χρηστών και της παραπλάνησης, κάνουν την διαδικασία αυτή εξαιρετικά δύσκολη. Ακόμα και αν ανιχνευθεί, με κάποιο τρόπο, η διαδρομή του σήματος και βρεθεί ο χρήστης που διεξήγαγε τις παράνομες κυβερνοπράξεις, για να γίνει η απόδοση των πράξεών του στο κράτος θα πρέπει να συντρέχουν οι προϋποθέσεις της διεθνούς ευθύνης που αναφέρθηκαν παραπάνω. Η περίπτωση, όμως, λανθασμένου καταλογισμού θα επέφερε σοβαρά νομικά και πολιτικά προβλήματα στα κράτη. Για αυτό το λόγο, όπως αναφέρουν και οι Τσαγγούριας και Buchan, προκειμένου μια αυτόματη κυβερνοάμυνα να είναι αποδοτική, η αναγνώριση του πραγματικού δράστη μέσω τεχνικών μέσων και πληροφοριών είναι ιδιαίτερα σημαντική και ενδεχομένως, χρειάζεται παράλληλα, και η ανθρώπινη επιρροή.[136]

---

[134] Articles on State Responsibility, Article 11.

[135] *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* [1980] ICJ Rep 3, para 74.

[136] N Tsagourias and R Buchan, 'Automatic Cyber Defence and the Laws of War', *German Yearbook of International Law*, 9.

Μέρος Β. Η προσέγγιση της αυτόματης νόμιμης άμυνας στον κυβερνοχώρο. Σύγχρονες εξελίξεις και προκλήσεις στην εφαρμογή του διεθνούς δικαίου

Β.1. Η ερμηνεία του Άρθρου 51 του Χάρτη των Ηνωμένων Εθνών στο σύγχρονο πεδίο του κυβερνοχώρου και η νομιμότητα της αυτόματης κυβερνοάμυνας στο διεθνές δίκαιο.

Η απαγόρευση της «χρήσης βίας» ('use of force'), όπως αναλύθηκε στο Α' Μέρος της παρούσας εργασίας υπόκειται σε δύο, βασικές, εξαιρέσεις σύμφωνα τις διατάξεις του Κεφαλαίου VII, του Χάρτη των Ηνωμένων Εθνών. Πρώτον, στο δικαίωμα της νόμιμης άμυνας, κατά το Άρθρο 51, ως μια άμεση, αναγκαία και αναλογική απάντηση κατά μιας «ένοπλης επίθεσης» ('armed attack'). Δεύτερον, στην ανάληψη δράσης από το Συμβούλιο Ασφαλείας, όπου κατά το Άρθρο 42 έχει τη δυνατότητα, σε περίπτωση απειλής, να εξουσιοδοτεί κράτη μέλη του Οργανισμού να αναλάβουν δράση για τη διατήρηση ή την αποκατάσταση της διεθνούς ειρήνης και ασφάλειας. Στο παρόν κεφάλαιο, θα μελετηθεί η πρώτη περίπτωση εξαίρεσης του κανόνα της απαγόρευσης της χρήσης βίας, όπως αυτή ερμηνεύεται αναλογικά στον κυβερνοχώρο υπό το φως των σύγχρονων εξελίξεων. Κύριο ερώτημα είναι εάν η χρήση του δικαιώματος της νόμιμης κυβερνοάμυνας, κατά τη λογική του Άρθρου 51, μέσω αυτόματων συστημάτων χωρίς την επιρροή του ανθρωπίνου παράγοντα, μπορεί να είναι συμβατή με τα κριτήρια της αναγκαιότητας και της αναλογικότητας και της αμεσότητας.

Β.1.1. Επισκόπηση του δικαιώματος της νόμιμης άμυνας.

Η νόμιμη άμυνα προβλέπεται στο Άρθρο 51 του Χάρτη των Ηνωμένων Εθνών το οποίο συγκεκριμένα αναφέρει:

> «Καμιά διάταξη αυτού του Χάρτη δε θα εμποδίζει το φυσικό δικαίωμα της ατομικής ή συλλογικής νόμιμης άμυνας, σε περίπτωση που ένα Μέλος των Ηνωμένων Εθνών δέχεται ένοπλη επίθεση, ως τη στιγμή που το Συμβούλιο Ασφαλείας θα πάρει τα αναγκαία μέτρα για να διατηρήσει τη διεθνή ειρήνη και ασφάλεια. Τα μέτρα που θα παίρνουν τα Μέλη των Ηνωμένων Εθνών κατά την άσκηση αυτού του δικαιώματος της νόμιμης άμυνας θα ανακοινώνονται αμέσως στο Συμβούλιο Ασφαλείας, και σε καμία περίπτωση δε θα θίγουν την εξουσία και την υποχρέωση που έχει το Συμβούλιο Ασφαλείας, σύμφωνα με αυτόν το Χάρτη, να αναλαμβάνει οποτεδήποτε τη δράση που κρίνει αναγκαία για τη διατήρηση ή για την αποκατάσταση της διεθνούς ειρήνης και ασφάλειας».

Είναι αξιοσημείωτο, ότι η νόμιμη άμυνα αναφέρεται ως φυσικό δικαίωμα στη συγκεκριμένη διάταξη του Χάρτη. Αυτό σημαίνει, ότι δεν είναι κάτι πρωτόγνωρο αλλά φαίνεται να προϋπάρχει της δημιουργίας του Χάρτη ως απόρροια της κυριαρχίας των

κρατών.[137] Η λογική αυτή θα επιβεβαιωθεί, αρχικά, από το Διεθνές Δικαστήριο στην απόφαση για την *Υπόθεση Νικαράγουα*, ερμηνεύοντας ότι το Άρθρο 51 του Χάρτη «*έχει νόημα μόνο στη βάση ότι υπάρχει ένα 'φυσικό' ή 'έμφυτο' δικαίωμα νόμιμης άμυνας και ο εθιμικός του χαρακτήρας δεν δύναται να αμφισβητηθεί ακόμα και εάν το παρόν περιεχόμενο έχει επιβεβαιωθεί και επηρεαστεί από το Χάρτη*».[138] Στη συνέχεια, επιβεβαιώνεται και στη *Γνωμοδότηση για τη Νομιμότητα της Απειλής ή της Χρήσης Πυρηνικών Όπλων*, όπου το Δικαστήριο χαρακτηρίζει ως «*θεμελιώδες το δικαίωμα του κράτους προς επιβίωση, και επομένως και του δικαιώματός του στη νόμιμη άμυνα, σύμφωνα με το Άρθρο 51 του Χάρτη, όταν απειλείται η επιβίωσή του»*.[139] Παράλληλα, το Ινστιτούτο Διεθνούς Δικαίου στη διακήρυξή του, το 2017, στο πλαίσιο της συνδιάσκεψής του στο Σαντιάγκο, επιβεβαιώνει, και αυτό με τη σειρά του, ότι το Άρθρο 51 συμπληρώνεται από το εθιμικό δίκαιο.[140]

Όπως αναφέρθηκε στο Α' Μέρος της παρούσας εργασίας, το Άρθρο 2(4) του Χάρτη, απαγορεύει την «χρήση βίας» ('use of force') στις διακρατικές σχέσεις. Η ύπαρξη, ωστόσο, χρήσης βίας δεν προϋποθέτει και την ύπαρξη «ένοπλης επίθεσης» ('armed attack').[141] Σύμφωνα με το Διεθνές Δικαστήριο μόνο οι ακραίες μορφές χρήσης βίας οι οποίες λόγω της «έντασης» και «αποτελεσμάτων» τους, δύναται να συνιστούν μια ένοπλη επίθεση. Επομένως, η επίκληση του δικαιώματος της νόμιμη άμυνας έχει ως *condition sine qua non* την ύπαρξη μιας ένοπλης επίθεσης, σύμφωνα με το Δικαστήριο.[142] Επιπλέον, το Διεθνές Δικαστήριο, έκανε σαφές ότι η νόμιμη άμυνα υφίσταται όταν υπάρχει πράγματι μια ένοπλη επίθεση και όχι όταν ένα κράτος την επικαλείται για την προστασία συμφερόντων ασφαλείας του από τυχόν κίνδυνο.[143] Είναι σημαντικό, επίσης, να αναφερθεί ότι το Διεθνές Δικαστήριο στην *Υπόθεση Εξεδρών Πετρελαίου,* ερμήνευσε ότι «*το βάρος της απόδειξης των πραγματικών περιστατικών που αποδεικνύουν την ύπαρξη*» ένοπλης επίθεσης, έγκειται στο κράτος που ασκεί το δικαίωμα της νόμιμης άμυνας.[144] Παράλληλα, οποιαδήποτε απάντηση σε μια επίθεση, τελεί πάντοτε υπό την αίρεση λήψης μέτρων από το Συμβούλιο

---

[137] Y Dinstein, *War, Aggression and Self-Defense*, 191-2.

[138] *Nicaragua Case*, para 176.

[139] *Nuclear Weapons*, para 96. Βλέπε επίσης: *Oil Platform Case*, para 72.

[140] Institute De Droit International, 'Present Problems of the Use of Armed Force in International Law; A. Self-defence', (27 October 2007) 10A Resolution, para 1.

[141] Βλέπε το Κεφάλαιο Α.2.2.

[142] Nicaragua Case, para 195.

[143] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda)* [2005] ICJ Rep 168, para 148 (*Congo v Uganda*).

[144] *Oil Platform Case*, para 57.

Ασφαλείας, σύμφωνα με το Άρθρο 51 του Χάρτη. Με βάσει τα παραπάνω, και υπό το πρίσμα μιας θετικιστικής ερμηνείας, η νόμιμη άμυνα, κατά μια άποψη, ισχύει μόνο στην περίπτωση που μια ένοπλη επίθεση έχει εξαπολυθεί κατά άλλου κράτους, γεγονός που δεν επιτρέπει την επίκληση του δικαιώματος σε προληπτικό επίπεδο ή κατά επίθεσης μη κρατικών δρώντων ως αυτόνομη πηγή χρήσης βίας. Αντιθέτως, σε επόμενο υποκεφάλαιο θα εξεταστούν και οι θεωρίες που υποστηρίζουν την ενεργοποίηση της νόμιμης άμυνας και σε τέτοιες περιπτώσεις.

Η άσκηση του δικαιώματος της νόμιμης άμυνας, υπόκειται, σε δύο κύριες προϋποθέσεις, σε αυτή της αναγκαιότητας και της αναλογικότητας. Τα δύο, αυτά, κριτήρια είναι βαρύνουσας σημασίας και αποτελούν τον πυρήνα της νόμιμης άμυνας. Οι ρίζες τους πηγάζουν ήδη από τον Ιούλιο του 1842, μέσα από την αλληλογραφία μεταξύ του τότε Υπουργού Εξωτερικών Daniel Webster και του ομολόγου του, Lord Ashburton, των Ηνωμένων Πολιτειών, που αφορούσε το περιστατικό 'Caroline'. Κατά τον Webster, προκειμένου ένα κράτος να επικαλεστεί το δικαίωμα της νόμιμης άμυνας, χρειάζεται να:

> «επιδείξει την ανάγκη της νόμιμης άμυνας, άμεσα, αποφασιστικά, χωρίς να επιτρέπει καθόλου περιθώρια και μέσα για συζήτηση. Θα χρειαστεί, επίσης, να δείξει ότι [...] δεν έκανε τίποτα παράλογο ή υπερβολικό· δεδομένου ότι η πράξη, δικαιολογημένη από την ανάγκη για νόμιμη άμυνα, πρέπει να περιοριστεί σε αυτή την αναγκαιότητα και να διατηρηθεί με σαφήνεια μέσα σε αυτήν».[145]

Η αναγκαιότητα και η αναλογικότητα αποτελούν, πλέον, διεθνές εθιμικό δίκαιο[146], και τα κριτήρια αυτά έχουν, επίσης, τονιστεί σε σημαντικές αποφάσεις του Διεθνούς Δικαστηρίου.[147] Αρχικά, η αναγκαιότητα, κοινώς ερμηνεύεται ως η απαίτηση να μην δύναται καμία άλλη δυνατή εναλλακτική απάντηση, τη στιγμή εκείνη, πέρα από αυτή της νόμιμης άμυνας.[148] Η έννοια της αναλογικότητας, σχετίζεται με την ένταση της απάντησης, το είδος αυτής, τον στόχο της και άλλους παράγοντες όπως ακόμα και γεωγραφικοί, οι οποίοι λαμβάνονται υπόψη προκειμένου να εκτιμηθεί συνολικά η αναλογικότητα της πράξης.[149] Η εκτίμηση, ωστόσο αυτή, πρέπει να διαμορφώνεται

---

[145] See Letter from the British Minister to the United States Lord Alexander Baring Ashburton to Secretary of State Daniel Webster, (28 July 1842) at: <http://avalon.law.yale.edu/19th_century/br-1842d.asp>accessed 19.12.2018

[146] C Gray, *International Law and the Use of Force*, (3rd edn, Oxford: Oxford University Press, 2008), 148-50. *Nuclear Weapons* para 41.

[147] *Nicaragua Case* paras 194, *Υπόθεση Εξεδρών Πετρελαίου* para 43, *Congo v Uganda* para 147, *Nuclear Weapons* paras 41-4.

[148] J Gardam, *Necessity, Proportionality and the Use of Force by States,* (Cambridge: Cambridge University Press, 2004) 149.

[149] Ibid, 159-163. Το Διεθνές Δικαστήριο, στην *Υπόθεση Εξεδρών Πετρελαίου*, εφάρμοσε την αρχή της αναγκαιότητας προκειμένου να διαπιστώσει εάν ένας στόχος μπορεί να χτυπηθεί για τους σκοπούς της νόμιμης άμυνας ενώ έκρινε, με βάση την αρχή της αναλογικότητας, εάν το μέτρο αυτό ήταν ανάλογης βαρύτητας σε σχέση με το επιτιθέμενο χτύπημα. Βλέπε: *Oil Platform Case*, paras 76-7. Ένα επίσης

προκειμένου η χρήση βίας ως απάντηση, κατά παράνομης πράξη άλλου κράτους, να μην είναι υπερβολική σε σχέση με το σκοπό της, ο οποίος είναι η υποβάθμιση ή η διακοπή της επανάληψης της εχθρικής επίθεσης.[150] Παράλληλα, η αναγκαιότητα και η αναλογικότητα, ως προϋποθέσεις της νόμιμης άμυνας, εξετάζονται μεμονωμένα από το Διεθνές Δικαστήριο. Ωστόσο, όπως αναφέρει και η Gray, στην πράξη, αυτά τα δύο κριτήρια δεν μπορούν να λειτουργήσουν ξεχωριστά καθώς, εάν μια πράξη χρήσης βίας δεν είναι αναγκαία τότε αυτή δε μπορεί να θεωρηθεί και αναλογική ενώ αντιστρόφως, αν μια πράξη δεν είναι αναλογική είναι δύσκολο να εξεταστεί κατά πόσο αυτή είναι και αναγκαία.[151] Τα δύο αυτά κριτήρια θα αναλυθούν εκτενέστερα σε επόμενο υποκεφάλαιο. Υπάρχει, τέλος, και ένα τρίτο κριτήριο, αυτό της «αμεσότητας», το οποίο παρόλο που δεν έχει εκφραστεί στη νομολογία του διεθνούς δικαστηρίου, προβλέπεται και αυτό με τη σειρά του από το διεθνές εθιμικό δίκαιο.[152] Αυτό σημαίνει, ότι δεν πρέπει να υπάρχει μια αδικαιολόγητη χρονική υστέρηση μεταξύ της ένοπλης επίθεσης και της άσκησης του δικαιώματος της νόμιμης άμυνας, προκειμένου αυτό να μπορεί να θεωρηθεί νόμιμο.[153]

Β.1.2. Αυτόματη νόμιμη άμυνα στον κυβερνοχώρο.

Το παρόν κεφάλαιο, θα εξετάσει την περίπτωση της νόμιμης άμυνας στον κυβερνοχώρο ως απάντηση σε μια κυβερνοεπίθεση η οποία συνιστά ένοπλη επίθεση κατά το Άρθρο 51 του Χάρτη. Η παραπάνω ανάλυση, θα επιχειρηθεί υπό την χρήση συστημάτων τεχνητής νοημοσύνης, σε ηλεκτρονικούς υπολογιστές και δίκτυα, τα οποία συντελούν στην διεξαγωγή μιας αυτόματης κυβερνοάμυνας χωρίς την επίδραση του ανθρωπίνου παράγοντα.

Αρχικά, για να υπάρξει το δικαίωμα της νόμιμης άμυνας στο ευρύτερο πεδίο του κυβερνοχώρου απαιτείται ως προϋπόθεση η ύπαρξη μιας κυβερνοεπίθεσης. Το *Εγχειρίδιο του Ταλλίν* επί του ζητήματος αυτού αναφέρει: «*Ένα Κράτος που είναι στόχος μιας κυβερνοεπιχείρησης, η οποία ανέρχεται στο επίπεδο της ένοπλης επίθεσης,*

χαρακτηριστικό παράδειγμα, αντλείται μέσα από την *Υπόθεση Congo v Uganda*. Το Δικαστήριο έκρινε ότι δεν υπάρχουν οι προϋποθέσεις ώστε να ασκηθεί το δικαίωμα της νόμιμης άμυνας από την Ουγκάντα κατά του Κονγκό και για αυτό το λόγο δεν εξέτασε τα κριτήρια της αναγκαιότητας και της αναλογικότητας. Ωστόσο, ερμήνευσε ότι η κατάληψη αεροδρομίων και πόλεων αρκετά χιλιόμετρα μακριά από τις διασυνοριακές εχθροπραξίες δε φαίνεται να είναι αναγκαία και αναλογικά στο πλαίσιο της ισχυριζόμενης νόμιμης άμυνας. Βλέπε: *Congo v Uganda*, para 147.

[150] A Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*, (Athens: Sakkoulas Publishing, 2000) 161-2.

[151] C Gray, *International Law and the Use of Force*, 150.

[152] Y Dinstein, *War, Aggression and Self-Defense*, 230-1.

[153] Ibid, 233.

θα μπορεί να ασκήσει το φυσικό δικαίωμα της νόμιμης άμυνας. Εάν μια κυβερνοεπιχείρηση συνιστά μια ένοπλη επίθεση, αυτό εξαρτάται από την ένταση και τα αποτελέσματά της».[154] Όπως αναλύθηκε στο πρώτο μέρος της παρούσας εργασίας, μια κυβερνοεπίθεση μπορεί να συνίσταται, εάν αυτή προκαλεί σοβαρές υλικές ζημιές ή τραυματισμό ή θάνατο ανθρώπων.[155] Για παράδειγμα, μια κυβερνοεπίθεση που θα αποσκοπούσε στην απενεργοποίηση του ηλεκτρικού συστήματος ενός νοσοκομείου, πέρα από τις υλικοτεχνικές ζημιές που θα επέφερε, θα προκαλούσε ενδεχομένως και την επιβάρυνση της υγείας μερικών ασθενών είτε ακόμη και θάνατο σε εξαιρετικές περιπτώσεις. Ωστόσο, μια τέτοιου τύπου επίθεση μπορεί να μη προκαλεί πάντοτε εμφανή και άμεσα αποτελέσματα, όπως στο παραπάνω παράδειγμα. Οι κυβερνοεπιθέσεις, μπορούν να προκαλέσουν, επίσης, και έμμεσες αλυσιδωτές συνέπειες όπως στην περίπτωση που στοχεύουν τις «κρίσιμες υποδομές» ενός κράτους. Όπως προαναφέρθηκε, στο πρώτο μέρος, οι κυβερνοεπιθέσεις, για παράδειγμα, που στοχεύουν τα χρηματοπιστωτικά ιδρύματα μιας χώρας, μπορεί να επιφέρουν αποσταθεροποίηση της αγοράς, δημιουργώντας κλίμα πανικού και αβεβαιότητας, επηρεάζοντας, παράλληλα, τόσο την εύρυθμη λειτουργία του ίδιου του κράτους όσο και την καθημερινότητα των ανθρώπων της κοινωνίας.

Η φύση του κυβερνοχώρου συνιστά την διαδικασία απόδοσης ευθυνών, κατά το διεθνές δίκαιο, ιδιαίτερα δύσκολη.[156] Ακόμη και η χρήση «έξυπνων» αυτόματων συστημάτων δε φαίνεται να είναι σε θέση να φέρουν εις πέρας αυτή τη διαδικασία ορθά χωρίς την εμπλοκή του ανθρωπίνου παράγοντα, όπως εξετάστηκε. Ωστόσο, ακόμα και αν μια κυβερνοεπίθεση αξιολογηθεί από τους «έξυπνους» αλγόριθμους ως μια ένοπλη επίθεση και αποδοθεί σε ένα κράτος, η αυτόματη κυβερνοάμυνα προκειμένου να είναι νόμιμη θα πρέπει να είναι υπόκειται στις προϋποθέσεις της αναγκαιότητας και της αναλογικότητας.[157]

Β.1.2.1. ***Αναγκαιότητα.***

Το κριτήριο της αναγκαιότητας, κατά το *jus ad bellum*, χαρακτηρίζεται από δύο παράγοντες οι οποίοι εφαρμόζονται αναλογικά και στον κυβερνοχώρο. Πρώτον, ερμηνεύεται ως η ανάγκη να μην δύναται άλλη εναλλακτική απάντηση προς μια επιτιθέμενη πράξη τη δεδομένη στιγμή, πέρα της νόμιμης άμυνας, γεγονός που

---

[154] *Tallin Manual*, Rule 13.

[155] Βλέπε το υποκεφάλαιο Α.2.2.1.

[156] Βλέπε το υποκεφάλαιο Α.2.3.

[157] *Tallin Manual*, Κανόνας 14.

καταδεικνύει και τον αυστηρά αμυντικό της σκοπό.[158] Δεύτερον, η αναγκαιότητα σημαίνει παράλληλα και ένα είδους «έσχατης λύσης» χρήσης βίας, προκειμένου να απωθήσει την επίθεση, όταν τα υπόλοιπα μέσα δεν επαρκούν για αυτό.[159] Παράλληλα, σύμφωνα και με το *Εγχειρίδιο του Ταλλίν*, αυτό δε σημαίνει ότι η απάντηση στην κυβερνοεπίθεση είναι η μοναδική λύση διότι μπορούν να συνυπάρχουν και άλλα μη βίαια μέτρα, όπως η διπλωματία και οι οικονομικές κυρώσεις.[160] Η αρχή της αναγκαιότητας στο τεχνολογικό πεδίο, διαφαίνεται και μέσα από τις προσεγγίσεις διαφόρων κρατών.[161] Ενδεικτικά, οι Ηνωμένες Πολιτείες υποστηρίζουν ότι στην περίπτωση του κυβερνοχώρου «*η χρήση βίας στο πλαίσιο της νόμιμης άμυνας, πρέπει να περιορίζεται σε αυτό που είναι αναγκαίο για την αντιμετώπιση μιας επικείμενης ή πραγματική ένοπλης επίθεσης και πρέπει να είναι ανάλογη με την απειλή που αντιμετωπίζει*».[162] Αντιστοίχως, η λογική αυτή επιβεβαιώνεται, για παράδειγμα, και από την Ολλανδία, όπου κατόπιν αξιολόγησης των ερωτημάτων που είχε θέσει προς μελέτη για τον κυβερνοπόλεμο στο Advisory Council on International Affairs (AIV) και στην Advisory Committee on Issues of Public International Law (CAVV), υιοθέτησε, μεταξύ άλλων, ότι η νόμιμη άμυνα κατά μιας κυβερνοεπίθεσης πρέπει να είναι συμβατή με τις αρχές της αναγκαιότητας και της αναλογικότητας.[163]

Οι επιθέσεις στον κυβερνοχώρο, εξαπολύονται, συνήθως, σε ελάχιστο χρονικό διάστημα, χωρίς να γίνονται εύκολα αντιληπτές από τον άνθρωπο, παρά μόνο όταν έχουν εκδηλωθεί οι όποιες συνέπειες. Αυτό δημιουργεί ερωτήματα, στο κατά πόσο μια ενέργεια ανταπόδοσης στο πλαίσιο της νόμιμης άμυνας μπορεί να είναι συμβατή με την αρχή της αναγκαιότητας, εφόσον η κυβερνοεπίθεση έχει, αφενός, λήξει και έχοντας, αφετέρου, μεσολαβήσει, στη συνέχεια, κάποιο χρονικό διάστημα μέχρι αυτή να διαπιστωθεί και να αποδοθεί προς ένα άλλο κράτος.[164] Η διεθνής πρακτική, κατά την παραδοσιακή αντίληψη της νόμιμης άμυνας, δείχνει ότι υπάρχει μια σιωπηρή

---

[158] Οπ. π., υποσημείωση 148.

[159] M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', 119.

[160] *Tallin Manual*, 62.

[161] M Roscini, *Cyber Operations and the Use of Force in International Law*, 88-90.

[162] UN GA 'Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary General', (15 July 2011) UN Doc A/66/152.

[163] Government response to the AIV/CAVV Report on Cyber Warfare, 5 at: <http://docplayer.net/25408344-Government-response-to-the-aiv-cavv-report-on-cyber-warfare.html> accessed 19.12.2018. Για το περιεχόμενο της έκθεσης του AIV/CAVV βλέπε στο: Cyber Warfare, AIV (No 22)/CAVV (December 2011) at: <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf> accessed 19.12.2018

[164] F Grimal and J Sundaram, 'Cyber Warfare and Autonomous Self-defence', *Journal on the Use of Force and International Law*, (2017) Vol 4 No2, 340-2.

ανοχή μεταξύ των κρατών, όσο αφορά στη χρονική καθυστέρηση που συνήθως υφίσταται μεταξύ της ένοπλη επίθεσης και της άσκησης του δικαιώματος της νόμιμης άμυνας.[165] Αξίζει, όμως, να σημειωθεί, ότι το Διεθνές Δικαστήριο έχει επικρίνει τη μεσολάβηση μεγάλου χρονικού διαστήματος στην ενεργοποίηση του δικαιώματος της νόμιμης άμυνας. Συγκεκριμένα, στην *Υπόθεση Νικαράγουα*, το Δικαστήριο υποστήριξε ότι ακόμα και αν οι Ηνωμένες Πολιτείες ενεργούσαν νομότυπα στην άσκηση του συλλογικού δικαιώματος της νόμιμης άμυνας υπέρ του Ελ Σαλβαδόρ, αυτό δεν θα μπορούσε να ήταν συμβατό με το κριτήριο της αναγκαιότητας καθώς η ένοπλη επίθεση της Νικαράγουα κατά του Ελ Σαλβαδόρ είχε απωθηθεί αρκετούς μήνες πριν την δράση των ΗΠΑ.[166] Συνεπώς, οι όποιες στρατιωτικές και παραστρατιωτικές δραστηριότητες των Ηνωμένων Πολιτειών κατά της Νικαράγουα, δεν πληρούσαν την αρχή της αναγκαιότητας και της αμεσότητας.

Η διεξαγωγή νόμιμης κυβερνοάμυνας, από τον ανθρώπινο παράγοντα κατά μιας κυβερνοεπίθεσης, θα απαιτούσε ένα κρίσιμο χρονικό διάστημα μέχρι αυτή να αποφασιστεί. Αρχικά, θα πρέπει πρώτα να αναλυθεί και να αξιολογηθεί εάν η επίθεση εμπίπτει στο επίπεδο μιας «ένοπλης επίθεσης», ενώ στη συνέχεια, θα πρέπει να αποκαλυφθεί η ταυτότητα του δράστη και, τέλος, να αποδοθεί σε κάποιο άλλο κράτος. Η διαδικασία αυτή όπως αναφέρθηκε σε προηγούμενο κεφάλαιο είναι ιδιαίτερα δύσκολη, χρονοβόρα και απαιτητική στην περίπτωση του κυβερνοχώρου. Επομένως, η καθυστερημένη άσκηση κυβερνοάμυνας, κατά μιας κυβερνοεπίθεσης που έχει ήδη λήξει, θα μπορούσε ίσως να θεωρηθεί και ως πράξη ένοπλων αντιποίνων, γεγονός που δε συνάδει με τους κανόνες του διεθνούς δικαίου.[167] Η περίπτωση της αυτόματης κυβερνοάμυνας φαίνεται, σε ορισμένες περιπτώσεις, να μπορεί να μειώσει το χρόνο αντίδρασης και, επομένως, να μην αφήνει περιθώριο αμφισβήτησης της αρχής της αναγκαιότητας. Για παράδειγμα, στην περίπτωση μιας μαζικής κυβερνοεπίθεσης, τύπου 'DDoS', κατά ιστοσελίδων και κρίσιμων υποδομών, τα «έξυπνα» συστήματα θα μπορούν να επεξεργάζονται και να αναλύουν τη ροή των δεδομένων άμεσα. Στιγμιαία, θα απαντούν αυτόματα, στο πλαίσιο της νόμιμης άμυνας, διεξάγοντας, αντιστοίχως, τις

---

[165] A Cassese, 'Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law', *European Journal of International Law*, (2001) Vol 12 No 5, 995-998.

[166] *Nicaragua Case,* para 237.

[167] Κατά την παραδοσιακή αντίληψη της νόμιμης άμυνας, ο Cassese υπενθυμίζει ότι ο σκοπός της είναι η απώθηση της επίθεσης. Ένα από τα προβλήματα που αφορούν το στόχο της νόμιμης άμυνας είναι και η χρονική στιγμή που αυτή θα ενεργοποιηθεί. Εάν αυτή δεν διεξαχθεί άμεσα, τίθενται αμφιβολίες κατά πόσο αυτή είναι συμβατή με το διεθνές δίκαιο, εάν, δηλαδή, πληροί την αρχή της αναγκαιότητας. Σε διαφορετική περίπτωση, η μεγάλη χρονική καθυστέρηση απάντησης σε μια επίθεση, ως νόμιμη άμυνα, θα μπορούσε να θεωρηθεί και ως ένα είδος ένοπλων αντιποίνων. Βλέπε αναλυτικότερα όπ. π., υποσημείωση 165.

απαιτούμενες ενέργειες προκειμένου η κυβερνοεπίθεση να απωθηθεί ή να εξαλειφθεί.[168] Αυτό, όμως, προϋποθέτει ότι η επιλογή της αυτόματης ενεργητικής νόμιμης χρησιμεύει ως «έσχατη λύση» ανάγκης, δεδομένου ότι άλλοι τρόποι αποτροπής δεν επαρκούν, όπως λόγου χάρη η προστασία σε επίπεδο παθητικής άμυνας με τη χρήση 'firewalls'. Υπάρχουν, ωστόσο και οι περιπτώσεις όπου λόγω του είδους της κυβερνοεπίθεσης, μεσολαβεί μεγάλο χρονικό διάστημα μεταξύ της κυβερνοεπίθεσης και του χρόνου αντίδρασης, καθώς εξελιγμένοι ιοί μπορούν να διεισδύσουν σε λειτουργικά συστήματα και να δρουν χωρίς αυτό να γίνεται αντιληπτό. Χαρακτηριστικό παράδειγμα βάσει της παραπάνω λογικής αποτελεί ο ιός Stuxnet στο Ιράν. Όπως αναφέρθηκε και στο πρώτο μέρος, ο ιός φαίνεται να επηρέασε δεκάδες φυγοκεντρωτές, του πυρηνικού προγράμματος του Ιράν, χωρίς να έχει γίνει αντιληπτός για μεγάλο χρονικό διάστημα. Σε αυτές τις περιπτώσεις, τέτοιου τύπου επιθέσεις είναι δύσκολο τόσο να αποκαλυφθούν όσο και να αποδοθούν με ακρίβεια προς κάποιο κράτος, καθώς η όλη διαδικασία είναι ιδιαίτερα χρονοβόρα ακόμα και για τα πιο εξελιγμένα «έξυπνα» συστήματα, ενώ για τη νομική διάσταση της απόδοσης της ευθύνης η ανθρώπινη παρέμβαση κρίνεται απαραίτητη.[169] Συνεπώς, με βάσει τα προαναφερθέντα, στην περίπτωση της αυτόματης κυβερνοάμυνας, δεν μπορεί να θεωρηθεί δεδομένο ότι το κριτήριο της αναγκαιότητα καλύπτεται επαρκώς.

Β.1.2.2. ***Αναλογικότητα.***

Η αρχή της αναλογικότητας συνδέεται άρρηκτα με αυτή της αναγκαιότητας, οι οποίες έχουν χαρακτηριστεί από τον Ago ως οι δύο πλευρές ενός νομίσματος.[170] Η αναλογικότητα, συγκεκριμένα, απάντα στο ερώτημα «πόση χρήση βίας», συμπεριλαμβανομένου και των κυβερνοεπιχειρήσεων, είναι επιτρεπτή από τη στιγμή που η άσκησή της κρίνεται απαραίτητη.[171] Επομένως, εξαρτάται από την κλίμακα, το σκοπό, τη διάρκεια και την ένταση της αμυνόμενης πράξης που λαμβάνει χώρα, στο πλαίσιο της νόμιμης άμυνας.[172] Η αρχή της αναλογικότητας, επιδέχεται διαφόρων ερμηνειών στον ακαδημαϊκό κόσμο[173] Το δίλλημα που τίθεται, ενίοτε, είναι εάν η

---

[168] N Tsagourias and R Buchan, 'Automatic Cyber Defence and the Laws of War', *German Yearbook of International Law*, 9-10.

[169] Ibid

[170] R Ago, 'Addendum to the Eighth Report on State Responsibility', *Yearbook of the International Law Commission*, (1980) Vol II (1), 69.

[171] *Tallin Manual*, 62-3.

[172] Ibid

[173] Η παρούσα μελέτη αναφέρεται και ασχολείται μόνο υπό το πρίσμα του *jus ad bellum*. Υπάρχουν και άλλα νομικά πλαίσια που ερμηνεύουν υπό άλλη σκοπιά αυτή την αρχή, όπως το διεθνές ανθρωπιστικό

αναλογικότητα ερμηνεύεται ως η χρήση βίας που εξισορροπεί την «ένταση» και τα «αποτελέσματα» της αντίπαλης ένοπλης επίθεσης ή εάν ερμηνεύεται υπό το γενικότερο σκοπό απώθησης της επίθεσης αυτής.[174] Ευρύτερη αποδοχή φαίνεται να έχει η δεύτερη περίπτωση, καθώς όπως έχει επισημάνει ο Ago, η δράση που απαιτείται για την εξουδετέρωση της επίθεσης, μπορεί να επιφέρει και δυσανάλογα μέτρα μέσα από την αυστηρή ερμηνεία της αρχής της αναλογικότητας. Προκειμένου να υλοποιηθεί ο γενικότερος σκοπός της απώθησης μιας επίθεσης, επισημαίνει, ότι αυτό που έχει σημασία, είναι το αποτέλεσμα να επιτευχθεί μέσω «αμυντικής» δράσης και όχι μόνο μέσω, του περιεχομένου και της ουσίας της αντίπαλης δύναμης, καθ' αυτής.[175] Επομένως, υπό το γενικότερο πλαίσιο της απώθησης μιας επίθεσης, είναι πιθανό να ληφθούν και ηπιότερα μέτρα χρήσης βίας, σε περίπτωση που αυτά είναι επαρκή για την επίτευξη αυτού του σκοπού.[176]

Εφαρμόζοντας την παραπάνω ερμηνεία, της αρχής της αναλογικότητας, στην αυτόματη κυβερνοάμυνα, δημιουργούνται ορισμένες αμφιβολίες σχετικά με τη νομιμότητά της στο διεθνές δίκαιο. Προηγουμένως, αναφέρθηκε ότι ο γενικότερος σκοπός της είναι η ανάσχεση και η απώθηση μιας αντίπαλης ένοπλης επίθεσης, μέσα από μια αμυντική δράση. Ωστόσο, η περίπτωση της αυτόματης άμυνας, στην παρούσα μελέτη, εξετάζεται υπό το πρίσμα της ενεργητικής κυβερνοάμυνας. Αυτό σημαίνει ότι τα μέτρα που λαμβάνονται διαπερνούν τα «σύνορα» του αμυνόμενου καθώς αποσκοπούν να προσβάλλουν τα δίκτυα και τα ηλεκτρονικά συστήματα του επιτιθέμενου, προκειμένου να παύσει η κυβερνοεπίθεση. Επομένως, αν θεωρηθεί ότι ο σκοπός της αναλογικότητας είναι μόνο η ανάσχεση μιας κυβερνοεπίθεσης καθαυτής, τότε η αυτόματη ενεργητική κυβερνοάμυνα δεν πληροί τα κριτήριο της αναλογικότητας καθώς τα μέτρα που θα ληφθούν μπορεί να «ξεπεράσουν» αυτά της κυβερνοεπίθεσης, προκειμένου να την καταστήσουν ανενεργή.[177] Ενώ, αν η αυτόματη κυβερνοάμυνα διεξάγεται υπό το γενικότερο πλαίσιο του σκοπού της αποτροπής και προστασίας του αμυνόμενου, τότε τα μέτρα που θα παρθούν ικανοποιούν το κριτήριο

δίκαιο. Βλέπε στο: Ντ Μαρούδα, *Διεθνές Ανθρωπιστικό Δίκαιο*, (Αθήνα: Σιδέρης, 2015), 171-3 και N Tsagourias and A Morrison, *International Humanitarian Law. Cases, Materials and Commentary*, (Cambridge: Cambridge University Press, 2018) 49-54.

[174] M Roscini, *Cyber Operations and the Use of Force in International Law*, 90.

[175] Οπ. π., υποσημείωση 173. Επιπλέον, η Δικαστής Higgins, επιβεβαιώνει την άποψη του Ago στη *Διιστάμενη Γνώμη* του στη *Γνωμοδότηση για τη Νομιμότητα της Απειλής ή της Χρήσης Πυρηνικών Όπλων*. *Nuclear Weapons*, Separate Opinion of Judge Higgins, para 5.

[176] Ibid

[177] N Tsagourias and R Buchan, 'Automatic Cyber Defence and the Laws of War', *German Yearbook of International Law*, 13.

της αναλογικότητας. Επομένως, η αρχή της αναλογικότητας, μπορεί να θεωρηθεί, κατά μία άλλη άποψη, και «ελαστική», καθώς εξαρτάται από την οπτική που η κυβερνοάμυνα λαμβάνει χώρα. Εάν δηλαδή, συμβαίνει για να απωθηθεί μια επίθεση, ή για να αποτραπούν νέες ή για να εξαλειφθούν οι πηγές της απειλής.[178] Ωστόσο, το Διεθνές Δικαστήριο έχει υποστηρίξει ότι η αρχή της αναγκαιότητας και της αναλογικότητας είναι κριτήρια «αυστηρά και αντικειμενικά».[179] Μετά τα γεγονότα της 11ης Σεπτεμβρίου το 2001, τα κράτη έχουν προχωρήσει σε πιο ευρύτερες ερμηνείες όσον αφορά στο δικαίωμα της νόμιμης άμυνας και κατ' επέκταση και τις αρχές τις αναγκαιότητας και της αναλογικότητας. Η οπτική αυτή, μέσα από την αυτόματη άμυνα, καθώς και οι προκλήσεις που τίθενται στο διεθνές δίκαιο, θα μελετηθούν σε αμέσως επόμενο κεφάλαιο.

Τέλος, ένα άλλο ζήτημα που αφορά την αρχή της αναλογικότητας στον κυβερνοχώρο, σχετίζεται με την δυσκολία της «μετρησιμότητας» της χρήσης βίας στο πεδίο αυτό.[180] Αδιαμφισβήτητα, είναι δύσκολο για τον ανθρώπινο παράγοντα να μπορεί να αξιολογήσει και να ποσοτικοποιήσει μια κυβερνοεπίθεση που θα οδηγήσει σε ανάληψη δράσεων κυβερνοάμυνας, χωρίς αυτές να έχουν δυσανάλογο χαρακτήρα. Παράδειγμα αποτελεί ο ιός Stuxnet ο οποίος φαίνεται να δρούσε για μήνες προτού αποκαλυφθεί, ενώ οι συνέπειές αυτού δεν ήταν εύκολο να αξιολογηθούν και ποσοτικοποιηθούν άμεσα. Στο σημείο αυτό, λοιπόν, η ταχύτητα και ικανότητα ανάλυσης δεδομένων των συστημάτων τεχνητής νοημοσύνης, θεωρούνται ιδιαίτερα κρίσιμες στο στάδιο αξιολόγησης των συνεπειών μιας κυβερνοεπίθεσης, μειώνοντας σημαντικά τις πιθανότητες απόδοσης δυσανάλογων δραστηριοτήτων κυβερνοάμυνας.

Β.2. Η αυτόματη κυβερνοάμυνα ως προπομπός εξελίξεων στο διεθνές δίκαιο. Η χρήση της για την αντιμετώπιση επικείμενης κυβερνοεπίθεσης. Η ανάγκη για αυτόματη άμυνα κατά κυβερνοεπίθεσης από μη κρατικούς δρώντες.

Στην προηγούμενη ενότητα, αναλύθηκε η αυτόματη κυβερνοάμυνα υπό το πρίσμα της παραδοσιακής αντίληψης της νόμιμης άμυνας στον κινητικό χώρο. Αυτό σημαίνει, ότι για να ενεργοποιηθεί αυτό το δικαίωμα θα πρέπει, πρώτον, να έχει εκδηλωθεί η κυβερνοεπίθεση, η οποία να εμπίπτει στο επίπεδο της «ένοπλης επίθεσης» και,

[178] N Tsagourias, 'Chapter 2: The Tallin Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II-The Use of Force', 34.

[179] *Oil Platform Case*, para 73.

[180] M Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-defense', *Boston College International and Comparative Law Review*, (2009) Vol 32 Issue 2, 452.

δεύτερον, αυτή να είναι αποδοτέα προς ένα άλλο κράτος.[181] Παράλληλα, υπάρχει και η θεωρία της προληπτικής νόμιμης άμυνας κατά μιας ένοπλης επίθεσης που πρόκειται να συμβεί ή που μόλις έχει πυροδοτηθεί, χωρίς όμως αυτή να έχει αναπτυχθεί πλήρως. Η θεωρία υποστηρίζεται από μερίδα κρατών και ακαδημαϊκών και αποτελεί, διαχρονικά, ένα ζήτημα έντονης συζήτησης, σχετικά με τη νομιμότητά της στο διεθνές δίκαιο.[182]

Στη συνέχεια, θα αναλυθεί η έννοια της προληπτικής άμυνας στον κυβερνοχώρο και ειδικότερα η διεξαγωγή της αυτόματης προληπτικής κυβερνοάμυνας, κατά ερμηνεία του Άρθρου 51 του Χάρτη, μέσω της χρήσης της τεχνητής νοημοσύνης. Η έννοια της προληπτικής αυτόματης κυβερνοάμυνας, κατά την παρούσα ανάλυση, θα ερμηνευτεί υπό τη λογική της 'anticipatory self-defense', δηλαδή, κατά μιας κυβερνοεπίθεσης η οποία επίκειται άμεσα να συμβεί ή έχει μόλις αρχίσει να εξελίσσεται χωρίς, όμως, να έχει φτάσει το επίπεδο της «ένοπλης επίθεσης» και, επομένως, χωρίς να έχουν εκδηλωθεί οι όποιες σοβαρές συνέπειες. Σε διαφορετική περίπτωση, η διεξαγωγή 'preemptive self-defense', σε αόριστο χρόνο θέτει ερωτήματα σχετικά με τη νομιμότητά της στο διεθνές δίκαιο,[183] καθώς, τόσο η διαβαθμισμένη φύση των πληροφοριών σχετικά με τις δυνατότητες ενός κράτους να διεξάγει κυβερνοεπιχειρήσεις, όσο και οι ενδείξεις των όποιων προθέσεων για την μελλοντική διεξαγωγή εχθροπραξιών στον κυβερνοχώρο, είναι εκ των πραγμάτων αδύνατη.[184] Συνεπώς, η ανάλυση που θα ακολουθήσει σχετίζεται με την έννοια της 'anticipatory self-defense' καθώς σε διαφορετική περίπτωση, δημιουργείται το ενδεχόμενο

---

[181] Στην *Υπόθεση Congo v Uganda*, το Δικαστήριο παρόλο που θα μπορούσε να εξετάσει το ενδεχόμενο της νομιμότητας της προληπτικής άμυνας για την Ουγκάντα, τελικώς δεν το έπραξε καθώς η τελευταία υποστήριξε πως οι δράσεις της ήταν κατά ένοπλης επίθεσης που ήδη είχε συμβεί. Ωστόσο, ορισμένες πράξεις της Ουγκάντα κατά του Κονγκό, χαρακτηρίστηκαν 'preventive' από το Δικαστήριο, το οποίο στη συνέχεια αρκέστηκε να τονίσει μόνο ότι «*το Άρθρο 51 του Χάρτη μπορεί να δικαιολογήσει την χρήση βίας λόγω νόμιμης άμυνας, μόνο εντός των αυστηρών ορίων που καθορίζονται μέσα σε αυτό*». Βλέπε: *Congo v Uganda*, paras 143, 148. Αντιστοίχως, το ζήτημα της προληπτικής νόμιμης δεν εγέρθηκε και στην *Υπόθεση Nicaragua* και για αυτό το λόγο το Δικαστήριο δεν προχώρησε στην εξέταση του ζητήματος. *Nicaragua Case*, para 194.

[182] International Law Association, 'Final Report on Aggression and the Use of Force', Sydney Conference Use of Force, (2018) 13. T Ruys, '*Armed Attack' and Article 51 of the UN Charter*, 255-6.

[183] Είθισται, η προληπτική άμυνα, κατά μιας επικείμενης επίθεσης, να εκφράζεται με τον όρο 'anticipatory' ή και 'pre-emptive' όταν η επίθεση έχει αρχίσει να εξελίσσεται ή πρόκειται άμεσα να συμβεί, ενώ με τον 'preventive' όταν υπάρχουν βάσιμοι λόγοι ότι αυτή θα πραγματοποιηθεί, μελλοντικά, προκαλώντας σημαντική ζημιά. Βλέπε αναλυτικότερα στο: A. Sofaer, *The Best Defense? Legitimacy of Preventive Force*, (Stanford: Hoover Institution Press, 2010) 9-10.

[184] Αντιθέτως, στον κινητικό χώρο οι ενδείξεις μιας, ενδεχομένως, επικείμενης επίθεσης είναι πιο οφθαλμοφανείς. Για παράδειγμα, η μεγάλη συγκέντρωση στρατού ή και στόλου στα χερσαία και θαλάσσια σύνορα μεταξύ δύο χωρών, μπορεί να είναι οιωνός εξελίξεων, δεδομένου και ενός τεταμένου πολιτικού κλίματος αντιπαλότητας.

επικίνδυνων ερμηνειών στον κανόνα εξαίρεσης της χρήσης βίας του Άρθρου 51 του Χάρτη των Ηνωμένων Εθνών.

Β.2.1. Η προληπτική αυτόματη κυβερνοάμυνα κατά επικείμενης κυβερνοεπίθεσης.

Η δικαιολόγηση της προληπτικής άμυνας, πηγάζει ήδη από την εποχή του περιστατικού 'Caroline' που αναφέρθηκε προηγουμένως. Η δράση της Μεγάλης Βρετανίας κατά του πλοίου, έλαβε χώρα προληπτικά χωρίς να έχει προηγηθεί κάποια επίθεση από αυτό. Κατά την λογική του Webster για να δικαιολογήσει την πράξη της η Μεγάλη Βρετανία, έπρεπε να αποδείξει ότι η απειλή ήταν «*στιγμιαία, συντριπτική, χωρίς να αφήνει περιθώρια για συζήτηση*».[185] Αυτό, εκλαμβάνεται από ορισμένους ακαδημαϊκούς, ότι η 'anticipatory self-defense' υπάγεται στο διεθνές εθιμικό δίκαιο, αποτελώντας το φυσικό δικαίωμα της νόμιμης άμυνας ('*inherent right of self-defense*') που αναφέρεται στο Άρθρο 51, δικαίωμα δηλαδή, το οποίο προϋπάρχει του Χάρτη και, επομένως, δεν επηρεάζεται από αυτόν.[186] Το Διεθνές Δικαστήριο, δεν έχει ερμηνεύσει κατά πόσο η λογική της προληπτικής νόμιμης άμυνας του περιστατικού '*Caroline*', έχει ισχύ μετά την έλευση του Χάρτη, γεγονός που επιτρέπει να υπάρχουν διαφορετικές απόψεις επί του ζητήματος.[187] Τελικώς, όμως, φαίνεται η έννοια της προληπτικής νόμιμης άμυνας να αποτελεί διεθνές εθιμικό δίκαιο κατά τη γνώμη πολλών επιφανών συγγραφέων.[188] Την άποψη αυτή, επιβεβαιώνει η έκθεση του UN High-Level Panel on Threats, Challenges and Change, επισημαίνοντας ότι ένα απειλούμενο κράτος, σύμφωνα με το καθιερωμένο διεθνές δίκαιο, μπορεί να αναλάβει αναλογική στρατιωτική δράση εφόσον τίθεται ζήτημα επικείμενης επίθεσης και δεν μπορεί να την εκτρέψει με κανένα άλλο μέσο.[189] Ενώ από την πλευρά του, ο Γενικός Γραμματέας των Ηνωμένων Εθνών έχει αναφέρει σε έκθεσή του ότι «*οι επικείμενες απειλές καλύπτονται πλήρως από το Άρθρο 51, το οποίο διασφαλίζει το φυσικό δικαίωμα των κυρίαρχων κρατών να υπερασπίζονται τον εαυτό τους ενάντια σε ένοπλη επίθεση. Οι νομικοί έχουν αναγνωρίσει εδώ και καιρό ότι αυτό καλύπτει μια επικείμενη επίθεση*».[190]

---

[185] Οπ. π., υποσημείωση 145.

[186] K Kittichaisaree, *Public International Law of Cyberspace*, 172-3.

[187] Ibid, οπ. π., υποσημείωση 156.

[188] N Tsagourias, 'Chapter 2: The Tallin Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II-The Use of Force', 35.

[189] 'A More Secure World: Our Shared Responsibility', Report of the High-level Panel on Threats, Challenges and Change, UN Doc A/59/565, (2004) para 188.

[190] 'In larger freedom: Towards Development, Security and Human Rights for All', Report of the Secretary General. UN Doc A/59/2005, (2005) para 122.

Επιπροσθέτως, όσο αφορά το Άρθρο 51 του Χάρτη, ο Roscini θεωρεί ότι η ερμηνεία του θα πρέπει γίνεται, λαμβάνοντας υπόψη και το Άρθρο 32 της Σύμβασης της Βιέννης για το Δίκαιο των Συνθηκών.[191] Αυτό σημαίνει ότι η ερμηνεία του κανόνα, δε θα πρέπει να «*οδηγεί σε ένα αποτέλεσμα που είναι προφανώς παράδοξο και παράλογο*».[192] Επομένως, δε μπορεί να θεωρηθεί ρεαλιστικό σε, ορισμένες περιπτώσεις, για τα κράτη να περιμένουν, πρώτα, την ολοκλήρωση μιας επίθεσης, ώστε αυτά στη συνέχεια να μπορέσουν να αντιδράσουν.[193] Από τα παραπάνω, η έννοια της προληπτικής νόμιμης άμυνας φαίνεται να είναι συμβατή με το διεθνές δίκαιο, ιδίως από τη στιγμή που μια ένοπλη επίθεση ενδέχεται να προκαλέσει ανεπανόρθωτη ζημιά σε ένα κράτος.

Στην περίπτωση του κυβερνοχώρου, η προληπτική νόμιμη άμυνα κατά μιας «ένοπλης» κυβερνοεπίθεσης υποστηρίζεται και από το *Εγχειρίδιο του Ταλλίν*.[194] Συγκεκριμένα, η πλειοψηφία των συγγραφέων του, θεωρεί ότι παρόλο που το Άρθρο 51 δεν επιτρέπει την προληπτική νόμιμη άμυνα, ένα κράτος δεν χρειάζεται άπραγα να περιμένει μια επικείμενη κυβερνοεπίθεση, που να αναλογεί σε «ένοπλη επίθεση».[195] Η υψηλή ταχύτητα και ο μεγάλος όγκος των δεδομένων και πληροφοριών που διακινούνται στα ηλεκτρονικά δίκτυα φαίνεται να πληρούν τα κριτήρια της προληπτικής άμυνας κατά τη λογική του Webster καθώς η απειλή είναι «*στιγμιαία*» και δεν «*αφήνει περιθώρια συζήτησης*».[196] Το *Εγχειρίδιο του Ταλλίν*, διακρίνει την εισαγωγή μιας 'logic bomb' σε ένα ηλεκτρονικό σύστημα ή δίκτυο σε σχέση με την τοποθέτηση ενός κακόβουλο λογισμικού με δυνατότητα απομακρυσμένης ενεργοποίησης. Η 'logic bomb', σχετίζεται με ένα μέρος του λογισμικού, το οποίο θα εκτελέσει την κυβερνοεπίθεση βάσει συγκεκριμένων, προκαθορισμένων παραγόντων, χωρίς την ύπαρξη εξωτερικής εντολής. Εάν οι συνθήκες ενεργοποίησής είναι πιθανό να τεθούν σε λειτουργία, τότε αυτό συνιστά μια επικείμενη ένοπλη επίθεση, γεγονός που στον κινητικό χώρο, αντιστοιχεί, για παράδειγμα, με την τοποθέτηση θαλασσίων ναρκών στα χωρικά ύδατα ενός κράτους.[197] Αντιθέτως, η περίπτωση της απλής τοποθέτησης ενός κακόβουλου λογισμικού, το οποίο απαιτεί απομακρυσμένη ενεργοποίηση, δεν συνιστά μια επικείμενη κυβερνοεπίθεση, παρά μόνο τη στιγμή που

---

[191] M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', 32.

[192] Article 32 of Vienna Convention on the Law of Treaties of 1969.

[193] W Elizabeth. 'The Chatham House Principles of International Law on the Use of Force in Self-Defence'. *International and Comparative Law Quarterly*, (2006) Vol 55 No 4, 965.

[194] *Tallinn Manual*, 63-5.

[195] Ibid

[196] Οπ. π., υποσημείωση 145.

[197] *Tallin Manual*, 65.

οι διαχειριστές του αποφασίσουν να τον θέσουν σε λειτουργία.[198] Αντιστοίχως, και η απλή τοποθέτηση ενός κακόβουλου λογισμικού που να επιτρέπει, παρανόμως, τη μη εξουσιοδοτημένη πρόσβαση σε ένα ηλεκτρονικό σύστημα δε συνιστά μια επικείμενη επίθεση που να ενεργοποιεί το δικαίωμα σε μια νόμιμη άμυνα.[199]

Αξίζει να αναφερθεί ότι η ερμηνεία της προληπτικής κυβερνοάμυνας, κατά το *Εγχειρίδιο*, δε γίνεται υπό το πρίσμα του χρονικού κριτηρίου αλλά υπό τη γενικότερη θεώρηση της κυβερνοάμυνας ως «*τελευταίο εφικτό παράθυρο ευκαιρίας*», διότι σε περίπτωση κυβερνοεπίθεσης, η υψηλή ταχύτητα των δεδομένων φέρνει το κράτος προ τετελεσμένων γεγονότων.[200] Αυτό σημαίνει ότι, εάν μια επερχόμενη εχθρική επίθεση, είτε κινητική είτε στον κυβερνοχώρο, δεν μπορεί να αντιμετωπιστεί σε περίπτωση διεξαγωγής της, τότε το θιγόμενο κράτος θα πρέπει να αναλάβει δράση ακόμα και αν η επίθεση καθυστερήσει να ενεργοποιηθεί. Κατά τη γνώμη μου, η παραπάνω λογική της προληπτικής κυβερνοάμυνας κατά κυβερνοεπίθεσης που δεν επίκεται άμεσα, είναι πιο κοντά στην έννοια της 'preventive' νόμιμης άμυνας, η οποία διευρύνει το Άρθρο 51, ενδεχομένως, πέρα από τα επιτρεπτά όρια του διεθνούς δικαίου. Ειδικότερα, όπως αναφέρθηκε προηγουμένως, στον κυβερνοχώρο οι οπτικές ενδείξεις διεξαγωγής μιας κυβερνοεπίθεσης είναι σχεδόν μηδαμινές, ενώ οι πληροφορίες σχετικά με τα μέσα και τις δυνατότητες διεξαγωγής κυβερνοεπιχειρήσεων από ένα κράτος είναι συνήθως διαβαθμισμένες και δύσκολο να επιβεβαιωθούν.[201] Επομένως, αυτού του είδους η προληπτική κυβερνοάμυνα για να διεξαχθεί, θα πρέπει να στηρίζεται σε συγκεκριμένη πληροφόρηση που να αφορά στο στόχο της επικείμενης κυβερνοεπίθεσης καθώς και σε στοιχεία για την ένταση και τη διάρκεια αυτής, γεγονός που πάντοτε θα εγείρει ερωτήματα σχετικά με την εγκυρότητα και την αξιοπιστία της. Αξίζει για παράδειγμα να αναλογιστεί κανείς, τα καταστροφικά αποτελέσματα που θα μπορούσε να επιφέρει η λογική της προληπτικής νόμιμης άμυνας στο πλαίσιο εκατέρωθεν απειλών για όπλα χρήση όπλων μαζικής καταστροφής μεταξύ δύο κρατών, χωρίς, όμως, την ύπαρξη σαφών ενδείξεων επίθεσης, αλλά στηριζόμενα μόνο κάποιου είδους πληροφόρησης.[202] Αυτό θα μπορούσε να ανοίξει ένα φαύλο κύκλο εχθροπραξιών με οδυνηρές συνέπειες σε περίπτωση κλιμάκωσης και χρήσης πυρηνικών όπλων από τα κράτη. Συνεπώς,

---

[198] Ibid

[199] H Dinniss, *Cyber Warfare and the Laws of War*, (Cambridge: Cambridge University Press, 2012) 90.

[200] Οπ. π., υποσημείωση 194.

[201] N Tsagourias, 'Chapter 2: The Tallin Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II-The Use of Force', 36.

[202] M Waxman, 'Regulating Resort to Force: Form and Substance of the UN Charter Regime', *European Journal of International Law*, (2013) Vol 24 No1, 160.

θεωρώ ότι η προληπτική δράση κατά κυβερνοεπίθεσης που δεν έχει πυροδοτηθεί ή δεν πρόκειται να ενεργοποιηθεί άμεσα, απειλεί να δημιουργήσει παρερμηνείες σχετικά με την εφαρμογή του Άρθρου 51 του Χάρτη, και της πληρότητας των κριτηρίων της αναγκαιότητας και της αναλογικότητας.[203]

Οι σχολιαστές του *Εγχειριδίου του Ταλλίν*, όπως προαναφέρθηκε, δεν στηρίζουν την έννοια της προληπτικής νόμιμης άμυνας, έναντι μιας κυβερνοεπίθεσης, στο χρονικό κριτήριο, λόγω της υψηλής ταχύτητας και ροής που τα δεδομένα κινούνται στο διαδίκτυο. Είναι προφανές ότι η 'anticipatory self-defense' μέσα στον κυβερνοχώρο, τη στιγμή που ενεργοποιείται η κυβερνοεπίθεση, είναι πολύ δύσκολο να εφαρμοστεί, καθώς ο ανθρώπινος παράγοντας δεν είναι σε θέση να αντιληφθεί, να κρίνει και να απαντήσει προς μια τέτοια επίθεση, στον ελάχιστο χρόνο που αυτή χρειάζεται για να ολοκληρωθεί.

Η αυτόματη κυβερνοάμυνα μέσω της χρήσης τεχνητής νοημοσύνης, θα μπορούσε να συμβάλει καθοριστικά στην αντιμετώπιση μιας επικείμενης επίθεσης, τη στιγμή που αυτή ενεργοποιείται. Όπως αναφέρθηκε στο πρώτο μέρος της παρούσας εργασίας, η τεχνητή νοημοσύνη και οι δυνατότητες 'machine learning' έχουν δημιουργήσει ήδη ευφυή και αποτελεσματικά συστήματα παθητικής αυτόματης κυβερνοάμυνας.[204] Η τεχνολογική εξέλιξη, επιφέρει όλο και πιο εξελιγμένα αυτόματα συστήματα που άπτονται της κυβερνοασφάλειας, η χρήση των οποίων φαίνεται να είναι όλο και πιο απαραίτητη.[205] Επομένως, σύντομα η χρήση αυτής της «έξυπνης» τεχνολογίας θα μπορούσε να συνδράμει αποτελεσματικά και σε μια αυτόματη ενεργητική 'anticipatory self-defense' προκειμένου να αντιμετωπίσει μια

---

[203] Η παρούσα εργασία μελετά το ζήτημα της κυβερνοάμυνας κατά μιας κυβερνοεπίθεσης μεμονωμένα. Ωστόσο, οι κυβερνοεπιθέσεις μπορεί να αποτελούν μέρος ενός γενικότερου πεδίου εχθροπραξιών μεταξύ δύο κρατών στο κινητικό πεδίο ή να συμβαίνουν, δηλαδή, υπό το γενικότερο πλαίσιο ενός υβριδικού πολέμου. Σε τέτοια περίπτωση η δικαιολόγηση προληπτικών ενεργειών, χωρίς να έχει ενεργοποιηθεί η κυβερνοεπίθεση φαίνεται να είναι δικαιολογημένη, υπό συγκεκριμένες προϋποθέσεις. Σε προηγούμενο παράδειγμα, αναφέρθηκε ότι η συγκέντρωση στρατευμάτων στα σύνορα και ένα τεταμένο πολιτικό κλίμα μεταξύ των δύο κρατών, μπορεί να είναι οιωνός για την εξέλιξη εχθροπραξιών. Σε αυτή την περίπτωση, η διεξαγωγή μιας προληπτικής κυβερνοεπίθεσης σε συστήματα επικοινωνίας ή και στο κέντρο ελέγχου των πτήσεων, φαίνεται να λειτουργεί αποτρεπτικά έναντι της επερχόμενης ένοπλης επίθεσης. Επομένως, παρόλο που δεν έχει ενεργοποιηθεί κάποια κυβερνοεπίθεση από την αντίπαλη πλευρά, η προληπτική νόμιμη κυβερνοάμυνα, σε αυτή την περίσταση, φαίνεται να είναι συμβατή με το διεθνές δίκαιο καθώς και με την άποψη που εκφράζεται στο *Εγχειρίδιο του Ταλλίν*. Βλέπε επίσης: N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 232. D Cantwel, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone', *The David D. Caron Fund*, (29 November 2017) Vol 21 Issue 14, at:<https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone> accessed 19.12.18

[204] Οπ. π., υποσημείωση 40.

[205] J Hayes, 'Cyber Defense Automation', BlackRidge Technology at: <https://www.blackridge.us/images/site/pagecontent/BlackRidge_Cyber_Defense_Automation_white_paper.pdf> accessed 12.12.2018

κυβερνοεπίθεση τη στιγμή που πυροδοτείται. Από τα παραπάνω, φαίνεται, λοιπόν, ότι η έννοια της αυτόματης προληπτικής νόμιμης άμυνας ('anticipatory') μέσα στον κυβερνοχώρο, μπορεί να είναι εφικτή και σύμφωνη με τους κανόνες του διεθνούς δικαίου έναντι μιας αντίστοιχης 'preventive self-defense', η οποία θα μπορούσε να εγείρει σημαντικούς νομικούς προβληματισμούς και παρερμηνείες.

Τέλος, στην περίπτωση της αυτόματης προληπτικής κυβερνοάμυνας κατά επικείμενης κυβερνοεπίθεσης, η οποία πρόκειται άμεσα να ενεργοποιηθεί, τίθεται και το ερώτημα κατά πόσο πληρείται το κριτήριο της αναγκαιότητας και της αναλογικότητας. Μετά τα γεγονότα της 11ης Σεπτεμβρίου το 2001, ξεκινά να υπάρχει μια πιο ευρεία ερμηνεία σχετικά με το σκοπό της νόμιμης άμυνας.[206] Η προληπτική χρήση βίας, θεωρείται ότι πληροί εν μέρη τα κριτήρια υπό ένα γενικότερο πλαίσιο προστασίας των κρατών, προκειμένου αυτά να αποφύγουν τις συνέπειες μιας ένοπλης επίθεσης καθώς και να αποτρέψουν τις όποιες μεταγενέστερες.[207]

Β.2.2 Αυτόματη κυβερνοάμυνα κατά κυβερνοεπίθεσης από μη κρατικούς δρώντες.

Το ζήτημα της νόμιμης άμυνας κατά ΜΚΔ σχετίζεται και με το πεδίο του κυβερνοχώρου, καθώς μέσα σε αυτό υποκινούνται και διεξάγονται κυβερνοεπιθέσεις που σκοπό έχουν να προκαλέσουν καταστροφή στα κράτη ή στην κοινωνία αυτών. Το ερώτημα που τίθεται, είναι κατά πόσο μια αυτόματη «έξυπνη» κυβερνοάμυνα από κράτος κατά κυβερνοεπίθεσης από ΜΚΔ στο έδαφος άλλου κράτους, μπορεί να συμβατή με το διεθνές δίκαιο, όταν αυτοί δεν δρουν είτε εκ μέρους του κράτους ή υπό τον «αποτελεσματικό έλεγχό» του, ώστε αυτό να φέρει διεθνή ευθύνη για τις πράξεις τους.

Αρχικά, υπό από μία οπτική, το Άρθρο 51 του Χάρτη δεν αναφέρει ότι η νόμιμη άμυνα που ασκείται από το θιγόμενο κράτος, πρέπει να είναι μόνο κατά άλλου κράτους. Δεδομένου, όμως, ότι οι ΜΚΔ δεν αποτελούσαν για καιρό υποκείμενα του διεθνούς δικαίου και λαμβάνοντας υπόψη τη νομολογία του Διεθνούς Δικαστηρίου, η παραδοσιακή αντίληψη έχει διαμορφωθεί στη λογική ότι το Άρθρο 51 αφορά μόνο τα κράτη.[208]

---

[206] T Gill, 'The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy', *Journal of Conflict & Security Law*, (2006) Vol 11 No 3, 367

[207] M Schmitt, 'Counter-Terrorism and the Use of Force in International Law', *George C. Marshall. European Center for Security Studies*, (November 2005) No 5, 65-66.

[208] Στη *Γνωμοδότηση για το Παλαιστινιακό Τοίχος*, το Δικαστήριο ανέφερε χαρακτηριστικά ότι το «*Άρθρο 51 του Χάρτη, αναγνωρίζει την ύπαρξη του φυσικού δικαιώματος της νόμιμης άμυνας στη*

Υπάρχει, από την άλλη πλευρά, η άποψη που υποστηρίζει ότι το Άρθρο 51 δεν αποκλείει το δικαίωμα στην άσκηση νόμιμης άμυνας κατά των ΜΚΔ, καθώς αυτό πηγάζει ήδη από το περιστατικό *Caroline*.[209] Αντίθετοι, με την παραδοσιακή ερμηνεία της νόμιμης άμυνας είναι και ορισμένοι δικαστές του Διεθνούς Δικαστηρίου, οι οποίοι έχουν εκφράσει μέσα από τις ατομικές και διιστάμενες γνώμες τους, το δικαίωμα άσκησης της νόμιμης άμυνας και κατά ΜΚΔ.[210] Αξίζει κυρίως να αναφερθεί η ατομική γνώμη του Δικαστή Kooijmans, που θεωρεί ότι και οι ΜΚΔ ενός κράτους δύναται να διεξάγουν ένοπλες επιθέσεις, υπό την έννοια του Άρθρου 51, προς μια γειτονική επικράτεια, ακόμα και αν οι πράξεις τους δεν είναι αποδοτέες προς κάποιο κράτος. Επομένως, καταλήγει ότι, «*θα ήταν παράλογο να αρνηθεί το επιτιθέμενο κράτος το δικαίωμα στη νόμιμη άμυνα απλώς και μόνο επειδή δεν υπάρχει ένα επιθετικό κράτος και ο Χάρτης δεν το προβλέπει*».[211] Επιπροσθέτως, το δικαίωμα στη νόμιμη άμυνα, υποστηρίζεται ότι πυροδοτείται από την πράξη καθ' αυτή, και όχι από το δημιουργό της, γεγονός που διαφαίνεται και μέσα από την πρακτική των κρατών.[212] Ενδεικτικά, τέτοιες περιπτώσεις είναι η δράση του Ισραήλ, ως νόμιμη άμυνα, κατά της οργάνωσης Hezbollah στο Λίβανο και κατά του ISIS στη Συρία, όπως αντιστοίχως και της Τουρκίας κατά κουρδικών ένοπλων ομάδων στο Ιράκ, ή των Ηνωμένων Πολιτειών κατά της Al-Qaeda στο Αφγανιστάν.[213]

Συγκρίνοντας το Άρθρο 2(4) του Χάρτη σε σχέση με το Άρθρο 51, είναι προφανές ότι ο σκοπός του πρώτου (η απαγόρευση της χρήσης βίας) περιορίζεται ρητώς στις διακρατικές σχέσεις ενώ, αντιθέτως, το Άρθρο 51 δεν το ορίζει συγκεκριμένα, όπως προαναφέρθηκε. Υπάρχει και η άποψη, επομένως, ότι το Άρθρο 51 έχει εφαρμογή, ως *argumentum a contrario*, και στις ένοπλες επιθέσεις από μη

περίπτωση ένοπλης επίθεσης, από ένα κράτος κατά ενός άλλου κράτους». *Legal Consequences of the Construction of a Wall in the Palestinian Occupied Territory* (Advisory Opinion) [2004] ICJ Rep 2004, para 139 (*Palestinian Wall*). Επιπλέον, και στην *Υπόθεση Congo v Uganda*, το Δικαστήριο απέρριψε τον ισχυρισμό της άσκησης νόμιμης άμυνας από την Ουγκάντα κατά του Κονγκό, καθώς δεν υπήρχε κάποια απόδειξη που να συνέδεε ότι η δράση των ΜΚΔ γινόταν υπό τον άμεσο ή έμμεσο έλεγχο του Κονγκό. Το Δικαστήριο, είχε τη ευκαιρία να εξετάσει το ζήτημα της νόμιμης άμυνας κατά ΜΚΔ, ωστόσο δεν προχώρησε σε αυτή τη διαδικασία καθώς είχε ήδη απορρίψει τον ισχυρισμό της Ουγκάντας προηγουμένως. Συνεπώς, φαίνεται η ερμηνεία του Δικαστηρίου να επιβεβαιώνει την παραδοσιακή αντίληψη ερμηνείας του Άρθρου 51. *Congo v Uganda*, para 146-7.

[209] H Dinniss, *Cyber Warfare and the Laws of War*, 102-104.

[210] *Palestinian Wall*, Separate Opinion of Judge Higgins, para 33. *Palestine Wall*, Declaration of Judge Buergenthal, para 6. *Palestine Wall*, Separate Opinion of Judge Kooijmans, para 35.

[211] *Congo v Uganda,* Separate Opinion of Judge Kooijmans, para 30· άποψη με την οποία συμφωνεί και ο Δικαστής Simma. Ibid, Separate Opinion of Judge Simma, paras 10-11.

[212] International Law Association, 'Final Report on Aggression and the Use of Force', 14-5.

[213] Ibid

κρατικούς δρώντες.[214] Αυτό το συμπέρασμα, είναι επίσης συμβατό με το σκοπό του Άρθρου 51, ο οποίος είναι το κράτος να μπορεί να προστατευτεί έναντι μιας ένοπλης επίθεσης, στη περίπτωση που το Συμβούλιο Ασφαλείας αδρανήσει και δεν λάβει μέτρα για τη διατήρηση της ειρήνης και της ασφάλειας. Επομένως, υπό μια τελεολογική σκοπιά, δεν έχει σημασία εάν μια ένοπλη επίθεση προέρχεται από κράτος ή ΜΚΔ, αλλά το κράτος να μπορέσει να την αντιμετωπίσει έγκαιρα, ώστε να προστατευτεί.[215]

Υπό μια άλλη προσέγγιση, ένα κράτος καθίσταται υπεύθυνο όταν δε θέλει ή αδυνατεί να καταπολεμήσει επιθετικές πράξεις, που διεξάγουν ΜΚΔ από το έδαφός του κατά άλλων κρατών. Αρχικά, αξίζει να αναφερθεί ότι, σύμφωνα με το διεθνές δίκαιο, η επικράτεια ενός κράτους δε θα πρέπει να χρησιμοποιείται «*αντίθετα με τα δικαιώματα άλλων λαών*».[216] Επιπλέον, ήδη από το 1872, η διαιτησία μεταξύ Ηνωμένων Πολιτειών και Μεγάλης Βρετανίας στην *Υπόθεση Alabama*, έδειξε ότι η εδαφική επικράτεια δε θα πρέπει να χρησιμοποιείται και για την ενίσχυση στρατιωτικών ενεργειών κατά άλλου κράτους.[217] Αναλογικά, στον κυβερνοχώρο, η παραπάνω προσέγγιση έχει εκφραστεί και από τον επικεφαλή του US Cyber Command, στρατηγό Keith Alexander, ο οποίος έχει επισημάνει ότι κάθε κυβέρνηση είναι υπεύθυνη για τις πράξεις που προέρχονται μέσα από τη χώρα της.[218] Η έκθεση για την ανάπτυξη στο πεδίο των πληροφοριών και των τηλεπικοινωνιών, της Ομάδας Κυβερνητικών Εμπειρογνώμων των Ηνωμένων Εθνών έχει αναφέρει, μεταξύ άλλων, ότι τα «*κράτη θα πρέπει να επιδιώξουν να εξασφαλίσουν ότι τα εδάφη τους δεν θα χρησιμοποιούνται από ΜΚΔ για παράνομη χρήση του κυβερνοχώρου*».[219] Οι συγγραφείς του *Εγχειριδίου του Ταλλίν* επιβεβαιώνουν, αυτή τη λογική. Σύμφωνα με το *Εγχειρίδιο*, «*ένα κράτος δεν θα επιτρέπει εν γνώση του οι υποδομές του κυβερνοχώρου του, που βρίσκονται στην επικράτειά του ή υπό τον κυβερνητικό του έλεγχο, να χρησιμοποιούνται για πράξεις που επηρεάζουν αρνητικά και παράνομα άλλα κράτη*».[220] Συνεπώς, σύμφωνα

---

[214] A Zimmerman, 'The Second Lebanon War: *Jus ad Bellum, Jus in Bello* and the Issue of Proportionality', *Max Planck Yearbook of United Nations Law*, (2007) Vol 11, 117.

[215] Ibid. Αντιθέτως, υπάρχει και η άποψη που δεν αποδέχεται το δικαίωμα της νόμιμης άμυνας κατά ΜΚΔ σε περίπτωση που το κράτος δε θέλει ή δεν μπορεί να δράσει, όπως για παράδειγμα αυτή εκφράζεται μέσω της ενυπόγραφης έκκλησης, περισσοτέρων των 200 νομικών από όλο τον κόσμο. Βλέπε αναλυτικότερα: O Corten, 'A Plea against Abusive Invocation of Self-defence a Response to Terrorism', *EJIL Talk!*, (14 July 2016) at: <https://www.ejiltalk.org/a-plea-against-the-abusive-invocation-of-self-defence-as-a-response-to-terrorism/> accessed 19.12.2018

[216] *Corfu Case,* para 22.

[217] E Chadwick, 'The British view of neutrality in 1872'. In: P. Lottaz and H. Reginbogin (eds), *Notions of Neutralities*. (Lexington Press, 2018), 95-97.

[218] M Roscini, *Cyber Operations and the Use of Force in International Law*, 81.

[219] Οπ. π., υποσημείωση 29.

[220] *Tallinn Manual*, 26.

με την παρούσα προσέγγιση, εάν ένα κράτος δε δύναται να αντιμετωπίσει τις πράξεις των ΜΚΔ που διεξάγονται από το έδαφός του, προς άλλα κράτη, φέρει διεθνή ευθύνη λόγου παράλειψης της γενικής υποχρέωσης του due diligence.[221] Αυτό για παράδειγμα, ερμηνεύεται, αναλογικά, ότι σε περίπτωση κυβερνοεπίθεσης, το θιγόμενο κράτος μπορεί να απαντήσει με αυτόματη κυβερνοάμυνα κατά των ΜΚΔ, όταν το κράτος παραμένει απρόθυμο στη δράση τους. Διαφορετικά, δημιουργείται ένα «κενό» μεταξύ της ένοπλης επίθεσης των ΜΚΔ και της δυνατότητας αντιμετώπισής τους, καθώς υπό την παραδοσιακή θεώρηση, θα πρέπει να αποδειχθεί ότι το κράτος τους ελέγχει αποτελεσματικά, προκειμένου να ενεργοποιηθεί το δικαίωμα στη νόμιμη άμυνα. Όπως αναφέρει και ο Τσαγγούριας, εάν η υποχρέωση του due diligence υπάρχει για να διασφαλίσει βασικές παγκόσμιες αξίες όπως η ασφάλεια και η ειρήνη, ή για να επιβάλει ορισμένες σημαντικές υποχρεώσεις όπως η μη χρήση βίας, τότε θα ήταν παράλογο να μην επιτρέπει στο θιγόμενο κράτος να υπερασπιστεί την ακεραιότητά του έναντι μιας ένοπλης επίθεσης.[222] Η νόμιμη άμυνα κατά ΜΚΔ αποτυπώνεται, επίσης, και από το Ινστιτούτο Διεθνούς Δικαίου στη διακήρυξή του, το 2017, στο πλαίσιο της συνδιάσκεψής του στο Σαντιάγκο.[223]

Η πρακτική των κρατών στην καταπολέμηση της διεθνούς τρομοκρατίας δείχνει να επιβεβαιώνει την παραπάνω αντίληψη, ιδίως μετά τα γεγονότα της 11ης Σεπτεμβρίου, το 2001. Χαρακτηριστικό, είναι το παράδειγμα της δράσης των Ηνωμένων Πολιτειών κατά της Al-Qaeda, στην περιοχή του Αφγανιστάν. Η χρήση βίας, κατά τρομοκρατών, δικαιολογήθηκε ως νόμιμη άμυνα[224] λόγω της απροθυμίας του καθεστώτος των Ταλιμπάν, να πάψουν να παρέχουν ασφαλές καταφύγιο στην τρομοκρατική οργάνωση, έχοντας ήδη προηγηθεί αυστηρές συστάσεις από το Συμβούλιο Ασφαλείας.[225] Εξίσου, η Ρωσία επικαλέστηκε το δικαίωμα της νόμιμης άμυνας κατά των Τσετσένων ανταρτών που δραστηριοποιούνταν σε περιοχή της Γεωργίας, ισχυριζόμενη ότι η τελευταία, δεν μπορούσε ή δεν ήθελε να αποτρέψει αυτές

---

[221] N Tsagourias, 'Self-defense against Non-state Actors: The Interaction between self-Defence as a Primary Rule and Self-Defense as a Secondary Rule', *Leiden Journal of International Law*, (2006) Vol 29, 817.

[222] N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', 22.

[223] Institute De Droit International, 'Present Problems of the Use of Armed Force in International Law; A. Self-defence', para 10.

[224] Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, (7 October 2001) UN Doc S/2001/946. Την θέση των ΗΠΑ και το δικαίωμα στην ατομική και συλλογική νόμιμης άμυνας κατά της ένοπλης επίθεσης του ΜΚΔ (Al-Qaeda), λόγω της 11ης Σεπτεμβρίου, διαφαίνεται και μέσα από τα Ψηφίσματα 1368 και 1373 του Συμβουλίου Ασφαλείας. UN SC Res 1368, (12 September 2001) UN Doc S/Res1368 (2001). UN SC Res 1373, (28 September 2001) UN Doc S/Res/1371(2001).

[225] UN SC Res 1267, (15 October 1999) UN Doc S/Res/1267(1999)

τις επιθέσεις από το έδαφός της.[226] Η νόμιμη άμυνα κατά ένοπλης επίθεσης ΜΚΔ, υποστηρίχθηκε, σχετικά πρόσφατα, και στον πόλεμο κατά του ISIS/ISIL στη Συρία από τις Ηνωμένες Πολιτείες, την Αυστραλία και την Τουρκία, ενώ εμμέσως, την προσέγγιση αυτή ακολούθησαν το Ηνωμένο Βασίλειο και η Γαλλία.[227] Σημαντικό είναι και το γεγονός, ότι οι επιθέσεις του δυτικού συνασπισμού δεν έτυχαν κριτικής ή καταδίκης από το Συμβούλιο Ασφαλείας ως παραβίαση της εδαφικής κυριαρχίας της Συρίας,[228] παρόλο που η τελευταία δήλωσε ότι επιθέσεις στην εδαφική της επικράτεια κατά των τρομοκρατικών οργανώσεων χωρίς προηγούμενη συνεννόηση με το κυβερνητικό καθεστώς, θα συνιστούν παραβίαση της κυριαρχίας τους.[229]

Αναλογικά, με βάση την ήδη υπάρχουσα θεωρία και πρακτική, υποστηρίζεται από τα κράτη, το δικαίωμα της κυβερνοάμυνας κατά μιας «ένοπλης» κυβερνοεπίθεσης προερχόμενη από ΜΚΔ. Ενδεικτικά, οι Ηνωμένες Πολιτείες θεωρούν ότι στον κυβερνοχώρο το «*δικαίωμα της νόμιμης άμυνας κατά επικείμενης ή ένοπλης επίθεσης εφαρμόζεται είτε ο επιτιθέμενος είναι κράτος είτε μη κρατικό δρώντας*»[230] Παράλληλα, στο *Εγχειρίδιο του Ταλλίν*, η πλειοψηφία των συγγραφέων του, συμφωνεί με το δικαίωμα της νόμιμης άμυνας κατά κυβερνοεπιθέσεων από ΜΚΔ, λαμβάνοντας υπόψη τη διεθνή πρακτική, μετά τα γεγονότα της 11ης Σεπτεμβρίου του 2001.[231] Συνεπώς, με βάση τα παραπάνω, θεωρώ ότι η περίπτωση της αυτόματης κυβερνοάμυνας μέσω της χρήσης, τεχνητής νοημοσύνης, κατά ΜΚΔ, φαίνεται να μπορεί να έχει εφαρμογή και να είναι συμβατή με το διεθνές δίκαιο, υπό συγκεκριμένες περιστάσεις. Το ζητούμενο, ωστόσο, δεν είναι κάθε είδους κυβερνοεπίθεση να απαντάται, αντίστοιχα, με νόμιμη κυβερνοάμυνα, παρακάμπτοντας τη διαδικασία απόδοσης της ευθύνης. Η περίπτωση της αυτόματης κυβερνοάμυνας σε κυβερνοεπιθέσεις ΜΚΔ, πρέπει να χρησιμοποιείται, αρχικά, εφόσον οφείλεται σε υποχρέωση due diligence ενός κράτους, όπως αναφέρθηκε προηγουμένως. Δεύτερον, στην περίπτωση που μια κυβερνοεπίθεση είναι τόσο ισχυρή σε ένταση και αποτελέσματα, ώστε τα μέσα παθητικής προστασίας να

---

[226] Letter dated 11 September 2002 from the Permanent Represented of the Russian Federation to the United Nations addressed to the Secretary-General, (12 September 2002) UN Doc S/2002/1012.

[227] N Tsagourias, 'Self-defense against Non-state Actors: The Interaction between self-Defence as a Primary Rule and Self-Defense as a Secondary Rule', *Leiden Journal of International Law*, 808.

[228] 'Statement by the President of the UN Security Council', (19 September 2014) UN Doc S/PRST/2014/20.

[229] The Guardian, 'Syria offers to help fight Isis but warns against unilateral air strikes', (26 August 2018) at: <https://www.theguardian.com/world/2014/aug/26/syria-offers-to-help-fight-isis-but-warns-against-unilateral-air-strikes> accessed 15.12.2018

[230] UN GA 'Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary General', (15 July 2011) UN Doc A/66/152, 18.

[231] *Tallinn Manual*, 58-9.

καθίστανται ανεπαρκή να την αποτρέψουν, ενώ παράλληλα να μην δύναται η πολυτέλεια του χρόνου για περεταίρω διερεύνηση, όσον αφορά στη διαδικασία απόδοσης ευθυνών ή και την όποια διαβούλευση με το κράτος από το οποίο πηγάζει. Επομένως, θεωρώ ότι η αυτόματη κυβερνοάμυνα κατά ΜΚΔ θα πρέπει να διεξάγεται με αυστηρά κριτήρια και να ερμηνεύεται συσταλτικά και όχι διευρυμένα, καθώς αλόγιστη χρήση της, θα μπορούσε να οδηγήσει, ενδεχομένως, σε επικίνδυνη παρερμηνεία του δικαιώματος της εξαίρεσης στη χρήση βίας, κατά τον Χάρτη.

Συμπεράσματα

Η παρούσα μελέτη ανέλυσε το ζήτημα της χρήσης βίας, όπως αυτό ερμηνεύεται αναλογικά μέσα στον κυβερνοχώρο, εστιάζοντας στη νόμιμη άμυνα και στη διαμόρφωση αυτής, μέσω των σύγχρονων τεχνολογικών καινοτομιών, όπως της τεχνητής νοημοσύνης. Η κύρια προβληματική της μελέτης είναι, εάν η διεξαγωγή μιας αυτόματης ενεργητικής κυβερνοάμυνας στη λογική του Άρθρου 51, χωρίς την ανθρώπινη επίδραση, μπορεί να είναι συμβατή με τους κανόνες του διεθνούς δικαίου. Τόσο οργανισμοί, ιδιωτικοί και μη, όσο και κράτη, φαίνεται ήδη να οδηγούνται, προς την αξιοποίηση της σύγχρονης τεχνολογίας σε επίπεδο κυβερνοασφάλειας. Σε παθητικό επίπεδο, όπως για παράδειγμα μέσω της χρήσης ‘firewalls’, η κυβερνοασφάλεια καθίσταται ήδη αποδοτικότερη υπό την επίδραση της τεχνητής νοημοσύνης και των δυνατοτήτων ‘machine learning’. Αξίζει να σημειωθεί, ότι ήδη οι πρώτες σκέψεις και για ενεργητική αυτόματη κυβερνοάμυνα είναι ήδη προ των πυλών, γεγονός που θα δημιουργήσει προκλήσεις στην ερμηνεία του διεθνούς δικαίου, στο άμεσο μέλλον.

Η απάντηση στην κύρια προβληματική της παρούσας εργασίας, δίνεται ουσιαστικά μέσα από τη μελέτη του κάθε σταδίου, χωριστά, έως ότου φτάσουμε στην ενεργοποίηση του δικαιώματος της αυτόματης κυβερνοάμυνας και τα αποτελέσματα αυτής. Για το λόγο αυτό, πρώτα επιχειρήθηκε η αναλογική ερμηνεία της χρήσης βίας, στο ευρύτερο πεδίο του κυβερνοχώρου, διακρίνοντας, αρχικά, τις κυβερνοεπιθέσεις που συνιστούν μια «ένοπλη επίθεση». Τέτοιες κυβερνοεπιθέσεις, προκειμένου να καλύπτονται από το Άρθρο 51, πρέπει να προκαλούν κάποια υλική καταστροφή ή τραυματισμό ανθρώπων ή να παραλύουν κρίσιμες υποδομές σε ένα κράτος. Είναι εμφανές, λοιπόν, ότι οι κυβερνοεπιθέσεις που στρέφονται, για παράδειγμα, κατά νοσοκομείων, υδροηλεκτρικών φραγμάτων ή πυρηνικών εργοστασίων, ερμηνεύονται ως «ένοπλες επιθέσεις», λόγω των εκτεταμένων συνεπειών που μπορούν να επιφέρουν. Ωστόσο, από τη στιγμή που ο Χάρτης έχει θεσπιστεί αρκετές δεκαετίες πριν, η

αναλογική αυτή ερμηνεία της κυβερνοεπίθεσης βάσει των αποτελεσμάτων της, δεν είναι πάντοτε εύκολη σε σχέση με τον παραδοσιακό κινητικό χώρο όπου η χρήση βίας είναι εμφανής και εκφραζόμενη με κινητικά μέσα. Για αυτό το λόγο, η αξιοποίηση της τεχνητής νοημοσύνης, είναι ιδιαίτερα σημαντική στην περίπτωση του κυβερνοχώρου, καθώς μπορεί να συμβάλει στην έγκαιρη αναγνώριση και αξιολόγηση μιας κυβερνοεπίθεσης, ιδίως όταν αυτή δεν έχει άμεσα και εμφανή αποτελέσματα.

Η ενεργητική αυτόματη κυβερνοάμυνα, βρίσκεται στα πρώτα της στάδια και, κατά τη γνώμη μου, θα έχει άμεση εφαρμογή από τα κράτη στο προσεχές μέλλον.[232] Θα πρέπει όμως, τα κράτη να είναι εκ των προτέρων προετοιμασμένα ώστε εάν μια τέτοια «απάντηση» ενεργοποιηθεί, αυτή θα πρέπει να υπόκειται στις βασικές αρχές της αναγκαιότητας, της αναλογικότητας και της αμεσότητας, όπως έχει προαναφερθεί. Η όποια απάντηση, επομένως, θα πρέπει να δίνεται άμεσα προς την πηγή, ως έσχατη λύση ανάγκης και αναλογικής «βίας». Τα αυτόματα «έξυπνα» συστήματα φαίνεται να έχουν τη δυνατότητα να πληρούν με μια πιο διευρυμένη ερμηνεία αυτά τα κριτήρια, ιδίως της αναλογικότητας, κάτι που για τον ανθρώπινο παράγοντα είναι ιδιαίτερα δύσκολο, καθώς μια κυβερνοεπίθεση, συνήθως, δεν είναι ούτε εμφανής και ούτε εύκολο να ποσοτικοποιηθεί.[233]

Ένα σημαντικό θέμα, ιδιαίτερα προβληματικό στον κυβερνοχώρο είναι το ζήτημα της απόδοσης ευθυνών. Η ανωνυμία που προσφέρει το διαδίκτυο έχει ως αποτέλεσμα, να μη γίνονται εμφανή τα όποια απαραίτητα αποδεικτικά στοιχεία για να ανιχνευθούν οι χρήστες που ευθύνονται για την παράβαση, ώστε να μπορεί, στη συνέχεια, να αξιολογηθεί η απόδοση της παράνομης πράξης σε ένα κράτος, είτε μέσω των οργάνων του είτε μέσω του βαθμού ελέγχου που αυτό μπορεί να ασκεί στις ομάδες χάκερ. Όπως αναλύθηκε και προηγουμένως, το ζήτημα παραμένει εξίσου «προβληματικό», με τη χρήση της τεχνητής νοημοσύνης να μην φαίνεται να επαρκεί από μόνης της, στη διαδικασία της απόδοσης της ευθύνης, γεγονός που καθιστά στη παρούσα φάση απαραίτητη και την συνεκτίμηση του ανθρωπίνου παράγοντα. Υπάρχει, ωστόσο, και η θεωρία, της χρήσης βίας, κατά ΜΚΔ, όπως αναλύθηκε στο τελευταίο κεφάλαιο. Η αυτόματη ενεργητική κυβερνοάμυνα κατά κυβερνοεπίθεσης από ΜΚΔ μπορεί να δικαιολογηθεί στο διεθνές δίκαιο είτε μέσα από μια ευρεία ερμηνεία του

---

[232] Οι προβλέψεις, για παράδειγμα, κάνουν λόγο για εξελιγμένα αυτόνομα όπλα μετά το 2025. Γεγονός που δείχνει τους ρυθμούς με τους οποίους εξελίσσεται η τεχνολογία στα οπλικά συστήματα. Για περισσότερα σχετικά με την εξέλιξη της αυτονομία των όπλων στο μέλλον βλέπε: Human Rights Watch, 'Losing Humanity: The Case Against Killer Robots, (2012) 7-9 at: https://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf accessed 19.12.2018

[233] Όπως για παράδειγμα η περίπτωση του Stuxnet

Άρθρου 51 του Χάρτη, είτε μέσω παραβίασης της υποχρέωσης due diligence για ένα κράτος. Θεωρώ, λοιπόν, ότι όταν υπάρχουν εξαιρετικά σοβαρές κυβερνοεπιθέσεις, προερχόμενες από ΜΚΔ, οι οποίες δεν μπορούν αποδοθούν στο κράτος και δεν αφήνουν περιθώρια ευελιξίας και προστασίας, θα πρέπει να αντιμετωπίζονται μέσω της αυτόματης κυβερνοάμυνας κατευθείαν στην πηγή τους. Όπως, όμως, ανέφερα, αυτό θα πρέπει να λαμβάνει χώρα μέσα από μια αυστηρά συσταλτική ερμηνεία ως λύση ανάγκης, τη δεδομένη εκείνη στιγμή, και με γνώμονα την απώθηση της κυβερνοεπίθεσης και της αποτροπής των σοβαρών συνεπειών που αυτή ενδέχεται να προκαλέσει. Τυχών ασύστολη χρήση βίας, μέσω της αυτόματης κυβερνοάμυνας, κατά των κυβερνοεπιθέσεων ΜΚΔ θα μπορούσε να οδηγήσει σε σοβαρές παρερμηνείες του Άρθρου 51 του Χάρτη, ανοίγοντας το δρόμο και για αντίστοιχες περεταίρω θεωρήσεις και στον κινητικό χώρο.

Βιβλιογραφία

Συνθήκες

Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945,1 UNTS XVI.

Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, in force 7 December 1979, 1125 UNTS 3.

Vienna Convention on the Law of Treaties of 1969. United Nations, *Treaty Series*, (1980) Vol 1155

United Nations Resolutions

General Assembly

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Res, 24 June 2013, UN Doc A/68/98.

Developments in the field of Information and Telecommunications in the Context of International Security. Report of the Secretary. General Assembly Res, 2 December 2011, UN Doc A/RES/66/24.

Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary General', (15 July 2011) UN Doc A/66/152.

Definition of Aggression, GA Res 3314 (XXIX), 14 December 1974.

Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), 24 October 1970.

Responsibility of States for Internationally Wrongful Acts, GA Res, 26 November 2001, UN Doc A/RES/56/589.

Security Council

UN Security Council Resolution 568, UN Doc S/RES/568 (21 June 1985)

UN Security Council Resolution 602, UN Doc S/RES/602 (25 November 1987)

UN Security Council Resolution 577, UN Doc S/RES/577 (6 December 1985)

UN Security Council Resolution 573, UN Doc S/RES/573 (4 October 1985)

UN Security Council Resolution 1267 (1999), UN Doc S/RES/1267 (1999)

UN Security Council Resolution 1268 (1999), UN Doc S/RES/1269 (1999)

UN Security Council Resolution 1368 (2001), UN Doc S/RES/1368 (2001)

UN Security Council Resolution 1371 (2001), UN Doc S/RES/1371 (2001)

UN Security Council Resolution 1373 (2001), UN Doc S/RES/1373 (2001)

Other Documents

United Nations

'A More Secure World: Our Shared Responsibility', Report of the High-level Panel on Threats, Challenges and Change, UN Doc A/59/565, (2004).

'In larger freedom: Towards Development, Security and Human Rights for All', Report of the Secretary General. UN Doc A/59/2005, (2005).

K Annan, 'Secretary-General presents Annual Report to General Assembly', United Nations Press Release SG/SM/7136-GA/9596 (20 September 1999).

Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, (7 October 2001) UN Doc S/2001/946.

Letter dated 11 September 2002 from the Permanent Represented of the Russian Federation to the United Nations addressed to the Secretary-General, (12 September 2002) UN Doc S/2002/1012.

‘Report of the Commission to the General Assembly on the work of its fifty-third session’, *Yearbook of the International Law Commission*, (2001) Vol II.

‘Statement by the President of the UN Security Council’, (19 September 2014) UN Doc S/PRST/2014/20.

National Security Strategies

‘US President Policy Directive/PPD-20’ (October 2012).

‘US President Policy Directive’/PPD-21 (February 2015).

US Department of Defence, ‘Strategy for Homeland Defense and Civil Support’ (June 2005)

UK, National Cyber Security Strategy 2016-2021 (2016), at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>

NATO

NATO CCDCOE, ‘Cyberspace: Definition and Implications’ at: <https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html>

Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales (5 September 2014), at: <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm>

Νομολογία

Διεθνές Δικαστήριο

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda) [2005] ICJ Rep 168.

Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia) [2007] ICJ Rep 43.

Case Concerning Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v USA*) (Merits) [1986] ICJ Rep 14.

Case Concerning Oil Platforms (*Islamic Republic of Iran v. USA*) (Merits) [2003] ICJ Rep 161.

Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua) (Judgment) [2009] ICJ Rep 2009.

Legal Consequences of the Construction of a Wall in the Palestinian Occupied Territory (Advisory Opinion) [2004] ICJ Rep 2004

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) *notwithstanding Security Council Resolution 276 (1970)* (Advisory Opinion) [1971] ICJ Rep 1971.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion of 8 July 1996) [1996] ICJ Rep 226.

United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) [1980] ICJ Rep 3.

Διεθνές Ποινικό Δικαστήριο για την πρώην Γιουγκοσλαβία

Prosecutor v Duško Tadić, (Appeal) ICTY-94-1-A (15 July 1999)

European Union

European Council Directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, (23.12.2018) L/345/75.

Βιβλιογραφία

Ελληνική βιβλιογραφία

Κ Αντωνόπουλος και Κ Μαγκλιβέρας (επ.), *Το Δίκαιο της Διεθνούς Κοινωνίας*. (2η εκδ, Αθήνα: Νομική Βιβλιοθήκη, 2014)

Ε Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (2η έκδοση, Αθήνα: Νομική Βιβλιοθήκη, 2015)

Ντ Μαρούδα, *Διεθνές Ανθρωπιστικό Δίκαιο*, (Αθήνα: Σιδέρης, 2015)

Στ Περράκης, Μ-Ντ Μαρούδα, *Διεθνής Δικαιοταξία, Θεωρία και Εφαρμογή του Διεθνούς Δικαίου*, (2η εκδ, Αθήνα: Σιδέρης).

Ξενόγλωσση

A Cassese, *International Law,* 2th edition, (2nd edn, Oxford: Oxford University Press, 2005)

A Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter*, (Athens: Sakkoulas Publishing, 2000)

I Brownlie, *International Law and the Use of Force of by States*, (Oxford: Oxford University Press, 1963)

A Sofaer, *The Best Defense? Legitimacy of Preventive Force*, (Stanford: Hoover Institution Press, 2010)

C Gray, *International Law and the Use of Force*, (3rd edn, Oxford: Oxford University Press, 2008)

J Gardam, *Necessity, Proportionality and the Use of Force by States,* (Cambridge: Cambridge University Press, 2004)

H Dinniss, *Cyber Warfare and the Laws of War*, (Cambridge: Cambridge University Press, 2012)

I Brownlie, *International Law and the Use of Force by States*, (Oxford: Clarendon Press, 1963)

K Kittichaisaree, *Public International Law of Cyberspace*, (Springer International Publishing Switzerland, 2017) Governance and Technology Series Vol 32.

M Castells, *The Information Age. Economy, Society, and Culture* Vol 1, (2nd edn, New Jersey: Blackwell Publishing Ltd, 2010)

M Roscini, *Cyber Operations and the Use of Force in International Law*, (Oxford University Press, 2014)

N Tsagourias and A Morrison, *International Humanitarian Law. Cases, Materials and Commentary*, (Cambridge: Cambridge University Press, 2018)

N Tsagourias and R Buchan (eds), Research Handbook on International Law and Cyberspace (Cheltenham: Edward Elgar Publishing, 2015)

W Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994)

T Ruys, *'Armed Attack' and Article 51 of the UN Charter*, (Cambridge University Press, 2010)

Y Dinstein, *War, Aggression and Self-Defense*, (5th edn, Cambridge University Press, 2012)

Κεφάλαια σε τόμους

C Antonopoulos, 'State Responsibility in Cyberspace'. In: N Tsagourias and R Buchan (eds), Research Handbook on International Law and Cyberspace (Cheltenham: Edward Elgar Publishing, 2015)

E Chadwick, 'The British view of neutrality in 1872'. In: P. Lottaz and H. Reginbogin (eds), *Notions of Neutralities*. (London: Lexington Press, 2018)

M Roscini, 'Cyber Operations as a Use of Force'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015)

N Tsagourias, 'The Legal Status of Cyberspace'. In: N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015),

O Dörr and A Randelzhofer, 'Ch. I Purposes and Principles, Article 2 (4)' in: B Simma, D-E Khan, G Nolte and A Paulus (ed) *The Chapter of the United Nations: A Commentary*, (3rd edn, Oxford University Press, 2012)

Εγχειρίδια

International Humanitarian Law Institute, *Rules of Engagement Handbook* (September 2009).

M Schmitt (ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press, 2013)

Άρθρα-Μελέτες

A Zimmerman, 'The Second Lebanon War: *Jus ad Bellum, Jus in Bello* and the Issue of Proportionality', *Max Planck Yearbook of United Nations Law*, (2007) Vol 11.

A Cassese, 'Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law', *European Journal of International Law*, (2001) Vol 12 No 5.

CISCO Systems, Annual Cybersecurity Report, (2018) at: <https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2>

D Albright, P Brannan and C Walrond, 'Reports. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment', *Institute for Science and International Security*, (22 December 2018) at: <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>.

D Cantwel, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone', *The David D. Caron Fund*, (29 November 2017) Vol 21 Issue 14, at:<https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone>.

D Clark and S Landau, 'The Problem isn't attribution: It's Multi-Stage Attacks' in Proceeding of a workshop on Re-Architecting the Internet, (2010) No. 11, ACM

D Hoadley and N Lucas, 'Artificial Intelligence and National Security', *Congressional Research Service*, (26 April 2018) at: <https://fas.org/sgp/crs/natsec/R45178.pdf>

Ernst & Young, 'Is Cybersecurity about more than protection?' *EY Global Information Security Survey 2018-2019*, 8, at: <https://assets.ey.com/content/dam/ey-sites/ey-com/global/topics/advisory/GISS-2018-19-low-res.pdf>

F Grimal and J Sundaram, 'Cyber Warfare and Autonomous Self-defence', *Journal on the Use of Force and International Law*, (2017) Vol 4 No2.

G D Brown, 'Why Iran Didn't Admit Stuxnet Was an Attack', *Joint Force Quarterly*, (4th quarter 2011) Issue 63.

H Koh, 'International Law in Cyberspace; remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012'. *Harvard International Law Journal*, (December 2012) Vol 54.

Human Rights Watch, 'Losing Humanity: The Case Against Killer Robots, (2012) 7-9 at: <https://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf>.

J A Wood, 'The Darknet: A Digital Copyright Revolution', *Richmond Journal of Law & Technology*, Vol XVI, Issue 4.

Institute De Droit International, 'Present Problems of the Use of Armed Force in International Law; A. Self-defence', (27 October 2007) 10A Resolution.

International Law Association, 'Final Report on Aggression and the Use of Force', Sydney Conference Use of Force, (2018).

K Lamb, 'Challenges of Digitalisation in the Aerospace and Aviation Sectors', *Centre for Digital Built Britain*, (March 2018) 8, at:

<https://www.repository.cam.ac.uk/bitstream/handle/1810/278896/CDBB_REP_002_Lamb.pdf?sequence=1&isAllowed=y>

K Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict', *Military Law and the Law of War review,* (2010) Vol 49.

K Ziolkowski, '*Jus ad Bellum* in Cyberspace- Some Thoughts on the "Schmitt-Criteria" for Use of Force'. 4th International Conference on Cyber Conflict, (NATO CCD COE Publications, 2012).

M Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-defense', *Boston College International and Comparative Law Review*, (2009) Vol 32 Issue 2.

M Roscini, 'World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force', (2010) *Max Planck Yearbook of United Nations Law,* Vol 14, 114-9

L Robert and S Rahman, 'Analytic of China Cyberattack', *The International Journal of Multimedia & Its Applications*, (2012) Vol 4 No 3.

Maj Gen M Barret, D Bedford, E Skinner, E Vergles, *Assured Access to the Global Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization (April 2011), at: <https://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf>.

M Schmitt, 'Counter-Terrorism and the Use of Force in International Law', *George C. Marshall. European Center for Security Studies*, (November 2005) No 5.

M Waxman, 'Regulating Resort to Force: Form and Substance of the UN Charter Regime', *European Journal of International Law*, (2013) Vol 24 No1.

O Corten, 'A Plea against Abusive Invocation of Self-defence a Response to Terrorism', *EJIL Talk!*, (14 July 2016) at: <https://www.ejiltalk.org/a-plea-against-the-abusive-invocation-of-self-defence-as-a-response-to-terrorism/>.

R Ago, 'Addendum to the Eighth Report on State Responsibility', *Yearbook of the International Law Commission*, (1980) Vol II (1).

R Buchan, 'Cyber Attacks: Unlawful Uses of Force or prohibited Interventions?', *Journal of Conflict & Security Law*, (2012) Vol 17 No 2.

R Dewar, 'Active Cyber Defense', Cyber Defense Trend Analysis, Center for Security Studies (CSS), ETH Zürich, (June 2017).

V. Antolin-Jenkins, 'Defining the Parameters of Cyber of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) *51 Naval L Rev 132*.

N Tsagourias, 'Chapter 2: The Tallin Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II-The Use of Force', *Yearbook of International Humanitarian Law*, Vol 15.

N Tsagourias and R Buchan, 'Automatic Cyber Defence and the Laws of War', *German Yearbook of International Law*, (2017) Vol 60.

N Tsagourias, 'Cyber attacks, self-defense and the problem of attribution', *Journal of Conflict &Security Law*, (2012) Vol 17 No 2.

N Tsagourias, 'Non-State Actors, Ungoverned Spaces and International responsibility for Cyber Acts', *Journal of Conflict & Security Law*,(2016) Vol 21 Issue 3.

N Tsagourias, 'Self-defense against Non-state Actors: The Interaction between self-Defence as a Primary Rule and Self-Defense as a Secondary Rule', *Leiden Journal of International Law*, (2006) Vol 29.

T. Gill, 'The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy', *Journal of Conflict & Security Law*, (2006) Vol 11 No 3.

W Elizabeth. 'The Chatham House Principles of International Law on the Use of Force in Self-Defence'. *International and Comparative Law Quarterly*, (2006) Vol 55 No 4.

Ειδησεογραφικά άρθρα

American Institute of Aeronautics and Astronautics, 'Artificial Intelligence for Cybersecurity', at: <https://www.aiaa.org/protocolAI/>

A Graham, 'Artificial Intelligence in Cyber Security', IT Governance Blog (22 March 2018) at: <https://www.itgovernance.co.uk/blog/artificial-intelligence-in-cyber-security>

CISCO, 'What is the Difference: Viruses, Worms, Trojans, and, Bots?', (14 June 2018) at: <https://www.cisco.com/c/en/us/about/security-center/virus-differences.html

D E Sanger and E Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *New York Times*, (25 October 2015) at: <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0>.

D McGuinness, 'How a Cyber Attack Transformed Estonia', BBC News, (27 April 2017) at: <https://www.bbc.com/news/39655415>

D Kushner, 'The Real Story of Stuxnet', IEEE Spectrum, (26 February 2013) at: <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/>

J Finkle, 'Researchers say Stuxnet was deployed against Iran in 2007', *Reuters*, (26 February 2013) at: <https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226>.

J Hayes, 'Cyber Defense Automation', BlackRidge Technology at: <https://www.blackridge.us/images/site/pagecontent/BlackRidge_Cyber_Defense_Automation_white_paper.pdf>.

IBM, 'Artificial Intelligence and Cybersecurity FAQ Handbook' at: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?%3B=&%3Bdd=yes&htmlfid=10016710USEN>

IBM, 'IBM QRadar Advisor with Watson' at: <https://www.ibm.com/us-en/marketplace/cognitive-security-analytics/details>

Internet World Stats, 'Usage and Population Statics' (30 June 2018) at: <https://www.internetworldstats.com/stats.htm>

M Chawki, 'Anonymity in Cyberspace: Finding the Balance between Privacy and Security', (July 2006) at: <http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf>

M Sulmeyer and K Dura, 'Beyond Killer Robots: How Artificial Intelligence Can Improve Resilience in Cyber Space', *War on the Rocks*, (6 September 2018) at: <https://warontherocks.com/2018/09/beyond-killer-robots-how-artificial-intelligence-can-improve-resilience-in-cyber-space/>

Norton, 'Emerging Threats. DOS Attacks Explained' at: <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html>

R Jadhav, 'Indian Bank Loses $13,5m in Global Attack', Reuters, (14 August 2018) at: <https://www.reuters.com/article/cyber-heist-india/indias-cosmos-bank-loses-13-5-mln-in-cyber-attack-idUSL4N1V551G>

SAS Institute, 'Analytics and Data Insights' at: <https://www.sas.com/en_gb/insights/analytics/machine-learning.html>

SAS Institute, 'Big Data· What it is and why it matters', at: <https://www.sas.com/en_us/insights/big-data/what-is-big-data.html>

SPAMLAWS, 'Logic Bombs and How They Are Used', at: <https://www.spamlaws.com/how-logic-bombs-work.html>

T Olorunnipa and B House, 'Chip Hack a Sign of Chinese Cyber Threats to US., Official Say', *Bloomberg*, (4 October 2018) at: <https://www.bloomberg.com/news/articles/2018-10-04/chip-hack-a-sign-of-chinese-cyber-threats-to-u-s-officials-say>

V Vasudevan, 'How AI Is Transforming Cyber Defense', Forbes, (24 July 2018) at: <https://www.forbes.com/sites/forbestechcouncil/2018/07/24/how-ai-is-transforming-cyber-defense/#67448e593bb2>

Διάφορα

Cyber Warfare, AIV (No 22)/CAVV (December 2011) at: <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>.

Government response to the AIV/CAVV Report on Cyber Warfare, at: <http://docplayer.net/25408344-Government-response-to-the-aiv-cavv-report-on-cyber-warfare.html>.

Letter from the British Minister to the United States Lord Alexander Baring Ashburton to Secretary of State Daniel Webster, (28 July 1842) at: <http://avalon.law.yale.edu/19th_century/br-1842d.asp>.

UK Ministry of Defense, 'Defence Secretary announces £40m Cyber Security Operations Centre' (1 April 2016) at: <https://www.gov.uk/government/news/defence-secrtary-announces-40m-cyber-security-operations-centre>

US Department of Defence, 'Dictionary of Military and Associated Terms', Joint Publication 1-02 (8 November 2010, as amended through 15 February 2016), 58 at: <https://fas.org/irp/doddir/dod/jp1_02.pdf>

US Joint Chiefs of Staff, 'Cyberspace Operations', Joint Publication 3-12, (8 June 2018) I-2 at: <https://fas.org/irp/doddir/dod/jp3_12.pdf>

United States, 2001 PATRIOT Act, Public Law 107-56, (26 October 2001) Section 1016(e).

US Department of Homeland Security, 'Critical Infrastructure Sectors' at: <https://www.dhs.gov/critical-infrastructure-sectors>.

U.S. CYBER COMMAND, 'Mission' at: <https://www.cybercom.mil/About/Mission-and-Vision/