ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ ΑΣΦΑΛΕΙΑΣ»

Η ελληνική κυβερνοϊσχύς:
παρούσα κατάσταση, μελλοντικές προοπτικές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αχιλλέας Κουτσιούμπας

Αθήνα, 2023

Τριμελής Επιτροπή

Ανδρέας Λιαρόπουλος, Αναπλ. Καθηγητής Πανεπιστημίου Πειραιώς (Επιβλέπων)

Κωνσταντίνος Κολιόπουλος, Καθηγητής Πανεπιστημίου Πειραιώς

Χαράλαμπος Παπασωτηρίου, Καθηγητής Παντείου Πανεπιστημίου

Αφιέρωση

Στη σύζυγό μου και στα παιδιά μας, χωρίς αυτούς τίποτε δεν θα ήταν το ίδιο.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Περιεχόμενα

Κατάλογος εικόνων

Περίληψη

Το καινοφανές στοιχείο της σύγχρονης εποχής είναι ο αχαλίνωτος ρυθμός εξέλιξης της υπολογιστικής ισχύος και η διείσδυση της τεχνολογίας σε κάθε επίπεδο και πτυχή της ανθρώπινης δραστηριότητας. Ο κυβερνοχώρος, νεόκοπος όρος που πλάστηκε μόλις τη δεκαετία του ’80, από νοητικό κατασκεύασμα τείνει να αποικίσει το σύνολο του υλικού χώρου, γι’ αυτό και αναγνωρίζεται ως το πέμπτο γεωγραφικό πεδίο πολέμου.

Η κυβερνοϊσχύς, ήτοι η ικανότητα να κάνεις κάτι στρατηγικά χρήσιμο στον κυβερνοχώρο, εμπεριέχει ιδιότυπα ως προς τη διεξαγωγή πολέμου χαρακτηριστικά: την ατοπικότητα, τη μη απτότητα, την εφικτότητα διενέργειας επιχειρήσεων από μεμονωμένα άτομα ή ολιγομελείς ομάδες και πρακτικώς την από πολύ δύσκολη έως αδύνατη απόδοση ευθύνης. Στα προηγούμενα, σε αντίθεση με την κλασική στρατιωτική ισχύ, προστίθεται η δυνατότητα αδιάλειπτης προβολής της υπό τη μορφή καθημερινού πληροφοριακού πολέμου στον κυβερνοχώρο.

Για τη στρατηγική θεώρηση η ιδιαίτερη φύση της κυβερνοϊσχύος δεν εγείρει κάποιο ιδιαίτερο πρόβλημα. Ανεξαρτήτως του γεγονότος ότι δεν προκαλεί άμεση θανατηφόρα βία, η κυβερνοϊσχύς αποτελεί μια επιπλέον κατηγορία όπλου κατατασσόμενου στις ασαφείς μορφές εθνικής ισχύος. Η ίδια η κυβερνοϊσχύς μπορεί να αποτελεί σύγχρονο επίτευγμα ο λειτουργικός της ρόλος όμως δεν είναι διόλου νέος στην ιστορία της στρατηγικής. Εύκολα διαπιστώνεται η ύπαρξη μιας longue durée συναφούς έννοιας που δεν είναι άλλη παρά η πληροφορία από κοινού με την επικοινωνία της. Στρατηγικά η κυβερνοϊσχύς δεν αφορά στην τεχνολογία και στην επιστήμη. Προφανώς, δια της κυβερνοϊσχύος οι στρατηγιστές διεκπεραιώνουν αυτό που θέλουν μακράν ταχύτερα, σε μεγαλύτερες αποστάσεις και πιο κεκαλυμμένα από ότι γινόταν μέχρι την άφιξή της. Όμως, μάλλον πρόκειται για διαφορετικό είδος ισχύος από τα άλλα είδη και πιθανόν απλά να πρόκειται απλώς για έναν "ομαδικό παίκτη" στο διαρκώς εξελισσόμενο συνδεδυασμένο και πιθανώς ενοποιημένο αφήγημα διεξαγωγής πολέμου.

Στο θεσμικό επίπεδο σε παγκόσμια κλίμακα, και παρά τη φαινομενική κινητικότητα της διεθνούς κοινότητας προς διευθέτηση των προβληματικών της

κυβερνοϊσχύος, οι πλείστες εξ αυτών σχετιζόμενες με την προβολή κρατικής κυβερνοϊσχύος επί ετέρων κρατικών δρώντων, παραμένουν ανοιχτά ζητήματα, διότι οι κύριοι δρώντες του διεθνούς συστήματος εμφανίζονται από απρόθυμοι έως διστακτικοί να θεσπίσουν αυστηρά κανονιστικά όρια στον κυβερνοχώρο.

Η τρέχουσα τάση της νομικής ρύθμισης του κυβερνοχώρου lex lata, συνιστά απλώς μια κατ' επίφαση απόπειρα εφαρμογής της "κανονικότητας" Δικαίου στη "μη κανονικότητα" του κυβερνοχώρου. Προφανώς, η προβολή κυβερνοϊσχύος δεν διενεργείται σε νομικό κενό. Έως όμως τη διεθνή αποδοχή ειδικού "κυβερνοδικαίου" η προβολή κυβερνοϊσχύος θα τελεί de facto σε μια ιδιότυπη προνομιακή κατάσταση γυμνή εξουσίας, με τους κρατικούς δρώντες, εκμεταλλευόμενους τη συγκυρία, να προσπαθούν να διατηρήσουν ή να επαυξήσουν το βάθος του επιχειρησιακού τους αποτυπώματος.

Το αποτύπωμα της εθνικής κυβερνοϊσχύος είναι ευρύτερο της καθημερινής διαπάλης επίτευξης εθνικής κυβερνοασφαλείας και οι παρεχόμενες δια τις κυβερνοϊσχύος κυβερνοδυνατότητες δεν είναι τίποτε άλλο παρά περισσότερα εργαλεία στην κρατική εργαλειοθήκη. Επί του παρόντος δεν υφίσταται διεθνώς αποδεκτή αξιόπιστη μεθοδολογία αποτίμησης της εθνικής ισχύος ή των συνιστωσών της. Μια αξιοπρόσεκτη όμως προσπάθεια είναι το σύγχρονο, εκδοθέν τον Σεπτέμβριο του 2022, πολυκριτηριακό αναλυτικό μοντέλο υπολογισμού κατάταξης κυβερνοϊσχύος του Πανεπιστημίου του Harvard, το οποίο προσαρμοσμένο κατάλληλα εφαρμόσθηκε για τις ανάγκες εκπόνησης του παρόντος πονήματος. Με χρήση των δύο είδους εθνικών ενδεικτών του, πρόθεσης και δυνατοτήτων, αποτυπώθηκε αδρομερώς η τρέχουσα κατάστασης της ελληνικής κυβερνοϊσχύος, με τις προοπτικές της να παρουσιάζονται απτά ως οδικός χάρτης επιλογής επαύξησής της στην επιθυμητή κατεύθυνση, μέσω βελτίωσης των τιμών των αντιστοίχων ενδεικτών.

Λέξεις-κλειδιά: Επανάσταση της τεχνολογίας της πληροφορίας, κυβερνοχώρος, κυβερνοϊσχύς, στρατηγική, Κατάταξη Εθνικής Κυβερνοϊσχύος, ελληνική κυβερνοϊσχύς

The greek cyber power: current status, future prospects

Achilleas Koutsioumpas

Abstract

The novelty of contemporary era is the unbridled pace of the computing power development and the penetration of technology into every level and aspect of human activity. Cyberspace, a newly coined term in the 80s, from conceptual construction tends to colonize the entire physical space, which is why it is recognized as the fifth geographical domain of war.

Cyber power, or in other words the ability to do something strategically useful in cyberspace, includes idiosyncratic characteristics to warfare: the atopicallity, the intangibility, the feasibility of conducting operations by individuals or small groups, and the difficulty, rising almost to the heights of impossibility, of attributing responsibility in practice. Lastly, contrary to the classic military power, one must add cyber power's unique characteristic of being projected unceasingly in cyberspace in the form of daily information warfare.

For the general theory of strategy the special nature of cyber power does not pose a problem of any kind. Regardless of the fact that it does not inflict direct lethal force, cyber power constitutes just an additional category of weapon classified in the fuzzy forms of national power. Cyber power itself may be a contemporary achievement, but its operational role is by no means new in the history of strategy. It is easy to establish a connection within a longue durée relevant context which is none other than information together with its communication. Strategically, cyber power is not about technology and science. Indisputably, cyber power allows strategists to do what they want far faster, at greater distances, and more covertly than prior to its arrival. However, it is probably a different kind of power than the others, and probably just a "team player" in the ever-evolving connected and possibly unified narrative of warfare.

On the institutional level on a global scale, and despite the apparent mobility

of the international community to settle cyber power issues, most of them related to the projection of state cyber power on other state actors, unsolved issues remain, because the main actors of the international system appear reluctant, even hesitant, to establish strict regulatory boundaries in cyberspace.

The current trend of trying to legally regulate cyberspace lex lata is merely an apparent attempt to apply the "normality" of International Law to the "non-normality" of cyberspace. Obviously, cyber power projection does not take place in a legal vacuum. But until the international acceptance of a dedicated "cyber-law", projecting cyber power will be de facto taking place in an idiosycratic, privileged status of non-existant regulatory authority, with state actors, taking advantage of the situation, trying either to maintain or even to increase the depth of their operational footprint.

The footprint of national cyber power is broader than the day-to-day struggle to ensure national cybersecurity, and the cyber capabilities afforded by cyber power are nothing more than additional tools in the governmental toolbox. Currently, there is no internationally accepted reliable methodology for evaluating the national power or its components. However, a noteworthy effort is the recent, published in September 2022, multi-criteria analytical model for calculating the ranking of cyber power of Harvard University, which was adapted and applied for the needs of the current thesis. Using its two types of national indicators, intent and capabilities, the current state of Greek cyber power was coarsely captured whereas its prospects are presented as a tangible road map, since increasing cyber power as desired/planned can be achieved through improving the values of the corresponding indicators.

Keywords: Cyber, cyberspace, cyber power, strategy, National Cyber Power Index, greek cyber power

Εισαγωγή

Για το μεγαλύτερο μέρος της ανθρώπινης ιστορίας κάθε τεχνολογική κατάκτηση αποτελούσε την επιβράβευση επίπονης, και συνάμα επίμονης προσπάθειας, η οποία όμως προϋπέθετε εγγενώς τη διάνυση μεγάλων μεταβατικών περιόδων σταδιακών προσαρμογών. Ακόμα και οι πλέον ριζοσπαστικές καινοτομίες ήταν διαχειρίσιμες στο ήδη διαμορφωθέν εμπειρικό πλαίσιο, που προϋπήρχε της εμφάνισής τους. Έτσι λ.χ. τα ατμοκίνητα πολεμικά πλοία αξιοποιήθηκαν υπό το πρίσμα της υπάρχουσας ναυτικής πολεμικής τέχνης, ενώ τα άρματα μάχης θεωρήθηκαν μετεξέλιξη του ιππικού και αξιοποιήθηκαν με όρους θεωρίας ιππικού.

Το καινοφανές στοιχείο της σύγχρονης εποχής είναι ο αχαλίνωτος ρυθμός εξέλιξης της υπολογιστικής ισχύος και η διείσδυση της τεχνολογίας σε κάθε επίπεδο και πτυχή της ανθρώπινης δραστηριότητας. Ο κυβερνοχώρος, νεόκοπος όρος που πλάστηκε μόλις τη δεκαετία του ’80, από νοητικό κατασκεύασμα τείνει να αποικίσει το σύνολο του υλικού χώρου, γι’ αυτό και αναγνωρίζεται ως το πέμπτο γεωγραφικό πεδίο πολέμου, σε απόλυτα ισότιμη συσχέτιση με τα άλλα τέσσερα, τη ξηρά, τη θάλασσα, τον αέρα και το διάστημα (Γενικό Επιτελείο Εθνικής Άμυνας/Διεύθυνση Διακλαδικού Δόγματος [ΓΕΕΘΑ/ΔΔΔ], 2013, σ. 1-1). Ως εκ τούτου, δεν αποτελεί έκπληξη το γεγονός ότι η σύγχρονη επιχειρησιακή τέχνη τον κατατάσσει στην τριάδα των επιχειρησιακών πεδίων ενδιαφέροντος.[1]

Η απόκτηση κυβερνοϊσχύος για την επίτευξη κυριαρχίας στον κυβερνοχώρο έχει αναβιβασθεί σήμερα από τα κράτη στο σύγχρονο Άγιο Δισκοπότηρο, αφού ο φρενήρης ρυθμός τεχνολογικής ανάπτυξης επιτρέπει στην πραγματικότητα να

[1] Πιο συγκεκριμένα: "η επιχειρησιακή τέχνη εξετάζει τους σκοπούς, τους τρόπους επίτευξής τους, τα μέσα που απαιτούνται και τη διαχείριση των κινδύνων σε τρία χωριστά αλλά αλληλοσχετιζόμενα «επιχειρησιακά πεδία», το φυσικό, τον κυβερνοχώρο και το ηθικό. Επιδιώκει να καθορίσει τις διαφορετικές παραμέτρους (ενδεχόμενες καταστάσεις/κινδύνους/απειλές, πιθανότητες, αποτελέσματα και συνέπειες), που συνδέονται με κάθε ένα πεδίο μεμονωμένα αλλά και συνδυαστικά, έτσι ώστε να ληφθούν υπόψη κατά τη σχεδίαση των επιχειρήσεων. Ο επιδέξιος συνδυασμός ενεργειών στα επιχειρησιακά πεδία είναι βασικός στη δημιουργική σχεδίαση της επιχείρησης". (ΓΕΕΘΑ/Α' ΚΛΑΔΟΣ, 2012, σσ. 12-13).

αποδρά με ευκολία σε κάθε προσπάθεια επιβολής κανονιστικού πλαισίου. Δόγματα και εγχειρίδια τακτικής έχουν αποδυθεί σε έναν άνευ προηγουμένου αγώνα αναθεωρήσεων, προκειμένου να καταπολεμήσουν κάθε υποψία αναχρονισμού, που μοιραία όμως εμφιλοχωρεί σε κάθε νέα έκδοσή τους. Η αναπόδραστη αλήθεια είναι αμείλικτη, η ολοένα διογκούμενη εξάρτηση από τεχνολογίες αιχμής θα αποτελεί ανεξέλεγκτη γενεσιουργό αιτία νέων απειλών και νέων τρωτοτήτων.

Η διεξαγωγή Επιθετικών Επιχειρήσεων Κυβερνοχώρου (ΕΕΚ), η πλέον συνήθης επιλογή των κρατικών δρώντων εν ειρήνη ή εν πολέμω, μεμονωμένα ή ως μέρος συνδεδυασμένων επιχειρήσεων, για προβολή κυβερνοϊσχύος και προς επίτευξη συγκεκριμένου αντικειμενικού σκοπού, αποτελεί πλέον το μέσο επίτευξης μιας ευρείας γκάμας αποτελεσμάτων τα οποία δεν εγκλωβίζονται στα στενά όρια του ηλεκτρομαγνητικού φάσματος, δηλαδή πρόκληση δυσχέρειας διεξαγωγής επιχειρήσεων μέσω της δυσλειτουργίας του Συστήματος Διοίκησης και Ελέγχου. Θεωρητικά, στην εξελιγμένη τους μορφή, οι ΕΕΚ δύνανται να προκαλέσουν δευτερογενή αποτελέσματα τα όποια συγκρίνονται επί ίσοις όροις με αυτά ενός συμβατικού στρατιωτικού μέσου, ήτοι από τη φυσική καταστροφή υλικού έως και την απώλεια ανθρωπίνων ζωών.

Στα χαρακτηριστικά της κυβερνοϊσχύος εμπεριέχονται τρία suis generis, καινοφανή ως προς τη διεξαγωγή ενός πολέμου χαρακτηριστικά. Πρώτον, η ατοπικότητα και η μη απτότητα του κυβερνοχώρου. Πράγματι, η κυβερνοϊσχύς βρίσκεται, με όρους συμβατικής χωρικής αντίληψης, παντού και πουθενά. Δεύτερον, η ανάπτυξη και η εκτέλεση επιχειρήσεων στον κυβερνοχώρο είναι εφικτή από μεμονωμένα άτομα ή από ομάδες που δύνανται να βρίσκονται οπουδήποτε αλλού στον πλανήτη εκτός από το φυσικό σημείο προσβολής, ενώ επιπροσθέτως, η ίδια η ομάδα δύναται να έχει συγκροτηθεί μόνον ψηφιακά εντός του κυβερνοχώρου, δηλαδή τα μέλη της στον πραγματικό φυσικό κόσμο να απέχουν μεταξύ τους χιλιάδες χιλιόμετρα. Τέλος τρίτον, η απόδοση ευθύνης είναι πρακτικώς από πολύ δύσκολη έως αδύνατη. Οπότε, καθίσταται προφανές ότι αποτελεί διακύβευμα ζωτικής σημασίας για την Εθνική Άμυνα της χώρας η ασφαλής και αξιόπιστη χρήση του κυβερνοχώρου (ΓΕΕΘΑ/Διεύθυνση Κυβερνοάμυνας [ΓΕΕΘΑ/ΔΙΚΥΒ], 2014a, σ. 1].

Σε ό,τι αφορά στη συσχέτιση μεταξύ αμυντικών και επιθετικών επιχειρήσεων στον κυβερνοχώρο όσο και εάν φαίνεται παράδοξο, εκ πρώτης τουλάχιστον όψεως,

η διενέργεια αποτελεσματικής άμυνας έχει ως καθοριστική παράμετρο επιτυχίας την παράλληλη δυνατότητα διεξαγωγής ΕΕΚ. Ο κυβερνοχώρος δεν αποτελεί τίποτα λιγότερο και τίποτε περισσότερο από ένα ακόμα πεδίο αντιπαράθεσης μεταξύ των κρατικών δρώντων. Ο εγκλωβισμός σε μια παθητικού τύπου κυβερνοάμυνα, με την απεμπόλιση κάθε δυνατότητας επιθετικής ενέργειας, η οποία αποτελεί βασική Αρχή Πολέμου (Κολιόπουλος, 2010, σσ. 28, 135, 218), υποσκάπτει τελικά κάθε πιθανότητα επίτευξης τακτικού πλεονεκτήματος έναντι του επιτιθέμενου. Αυτός άλλωστε είναι και ο λόγος για τον οποίο αρκετά κράτη, ακόμη και εάν δεν αντιμετωπίζουν κάποια άμεση απειλή όπως η Ελλάδα, έχουν προδιαγράψει σε θεσμικά τους κείμενα, Εθνικές Στρατηγικές ή Δόγματα, την απαίτηση εκτέλεσης ΕΕΚ (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 3-1).

Στο σύγχρονο θολό τοπίο, που έχει επιβάλλει η κυβερνοεποχή μας, τα όρια όρων και εννοιών καθίστανται ασαφή, δυσδιάκριτα και πολλές φορές αμφίσημα. Οι κυβερνοεπιθέσεις, ή ο κυβερνοπόλεμος, ως εκφάνσεις της εθνικής κυβερνοϊσχύος, αποτελούν καταχρηστικό ευφημισμό; Ή αποτελούν μια άλλη μορφή επίθεσης, πολέμου αντίστοιχα, που σε ειρηνική περίοδο εγείρουν δικαίωμα ενεργητικής αντίδρασης στο κράτος αποδέκτη; Και εάν εγείρουν, σε ποιο επίπεδο νομιμοποιείται το κράτος να αντιδράσει; Μόνον εντός του κυβερνοχώρου ή/και σε φυσικό επίπεδο με διεξαγωγή συμβατικών πολεμικών επιχειρήσεων; Το παρόν πόνημα επιχειρεί μέσω βιβλιογραφικής (αρχειακής) έρευνας, η οποία περιλαμβάνει τη χρήση ανοικτών πηγών από το διαδίκτυο, να αναλύσει τα υφιστάμενα δεδομένα και να αναγνωρίσει τις προοπτικές ιχνηλατώντας τα μονοπάτια που θα επαυξήσουν το αποτύπωμα της εθνικής ισχύος.

Σκοπός του παρόντος πονήματος είναι μέσω της ψηλάφησης της έννοιας της κυβερνοϊσχύος και προσδιορισμού του δέοντος στρατηγικού της βάθους, της κριτικής θεώρησης των θεσμικών αντιλήψεων των διεθνών δρώντων, της ανάλυσης του υφιστάμενου νομικού πλαισίου του διεθνούς δικαίου περί προσφυγής στη βία και ενόπλων συρράξεων, ως πλαισίου αναφοράς, και τέλος της κριτικής ανάλυσης μιας μεθολογικής αποτίμησης της κυβερνοϊσχύος να ιχνηλατηθεί η παρούσα ελληνική κυβερνοϊσχύς και να διαγνωσθούν μελλοντικές προοπτικές της.

Η σύνταξη του παρόντος πονήματος έλαβε χώρα υπό το πρίσμα των κάτωθι προϋποθέσεων:

- Η Ελλάδα, ως μέλος της Ευρωπαϊκής Ένωσης (ΕΕ), θα συνεχίσει να

εναρμονίζει το εθνικό θεσμικό πλαίσιο με τις αποφάσεις των οργάνων της ΕΕ.

- Η Ελλάδα, ως μέλος του ΝΑΤΟ, θα συνεχίσει να εναρμονίζεται με τις αποφάσεις των οργάνων του και θα εφαρμόζει Πολιτικές και Συμφωνίες Τυποποίησης (ΣΤΥΠ, STANAGs).
- Η Ελλάδα, ως κράτος Δικαίου, θα συνεχίζει να εφαρμόζει τόσο το διεθνές δίκαιο όσο και το εθνικό δίκαιο, αξιοποιώντας την εθνική κυβερνοϊσχύ σε έργα ή δράσεις που δεν θα παράγουν έκνομα αποτελέσματα.

Και επιπροσθέτως υπό το πρίσμα των κάτωθι παραγόντων:

- "Ως μέσο άσκησης ασύμμετρου χαρακτήρα επιρροής και παρακώλυσης των πλέον ζωτικών λειτουργιών της χώρας ο κυβερνοπόλεμος και οι κυβερνοεπιθέσεις συνιστούν απειλή για την εθνική ακεραιότητα και την ευημερία μιας χώρας και ως τέτοιες πρέπει να αντιμετωπίζονται" (Υπουργείο Εθνικής Άμυνας [ΥΠΕΘΑ], 2015, σ. 30).
- Η επαύξηση των δυνατοτήτων στον κυβερνοχώρο είναι ένας εκ των επιχειρησιακών τομέων στους οποίους εστιάζει το ΥΠΕΘΑ (ΥΠΕΘΑ, 2015, σ. 42).
- Το ΓΕΕΘΑ/Ε5(ΔΙΚΥΒ) ενσωματώνει το πλήρες φάσμα των επιχειρήσεων των ΕΔ στον κυβερνοχώρο (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 5-1).
- Το εθνικό θεσμικό πλαίσιο επιχειρήσεων κυβερνοχώρου των ελληνικών Ενόπλων Δυνάμεων αποτελείται και οριοθετείται από:

1. Τη "Λευκή Βίβλο" (ΥΠΕΘΑ, 2015).
2. Το "Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου" (ΓΕΕΘΑ/ΔΔΔ, 2013).
3. Το "Κατευθυντήριο Πλαίσιο Ανάπτυξης Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2013).
4. Το "Τεχνικό Σχέδιο Δράσης για την Ανάπτυξη Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2014a).
5. Την "Πολιτική Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2014b).

- Η προβολή κυβερνοϊσχύος υπό τη μορφή υβριδικής απειλής[2] συνιστά σημαντική εθνική απειλή (Cullen et al., 2021, p. 28).

[2] Η ταξινομία των υβριδικών απειλών περιλαμβάνει το κυβερνοέγκλημα, τη διεξαγωγή προπαγάνδας, την κατασκοπεία, τον επηρεασμό της κοινής γνώμης, την τρομοκρατία και τον κυβερνοπόλεμο (Cullen

- Το εθνικό θεσμικό πλαίσιο ασφαλείας οριοθετείται από:

1. Την "Εθνική Στρατηγική Κυβερνοασφαλείας 2020-2025", της Εθνικής Αρχής Κυβερνοασφαλείας, του Υπουργείου Ψηφιακής Διακυβέρνησης (Υπουργείο Ψηφιακής Διακυβέρνησης/Εθνική Αρχή Κυβερνοασφαλείας, 2020).
2. Τον "Εθνικό Κανονισμό Ασφαλείας" (ΓΕΕΘΑ/Ε΄ ΚΛ, 2018).
3. Τον "Κανονισμό Προστασίας Προσωπικών Δεδομένων" της ΕΕ (ΕΕ Κανονισμός 679, 2016).
4. Τον Ν. 4411/2016, με τον οποίο κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και το Πρόσθετο Πρωτόκολλό της.

- Οι βασικοί εμπλεκόμενοι εθνικοί φορείς διαμόρφωσης εθνικής κυβερνοϊσχύος είναι (Υπουργείο Ψηφιακής Διακυβέρνησης/Εθνική Αρχή Κυβερνοασφαλείας, 2020, σσ. 23-29):

1. Η Εθνική Αρχή Κυβερνοασφαλείας.
2. Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό (CERT) (ΕΥΠ).
3. Η Διεύθυνση Κυβερνοάμυνας [ΓΕΕΘΑ/Ε5(ΔΙΚΥΒ)].
4. Η Δίωξη Ηλεκτρονικού Εγκλήματος (ΕΛ.ΑΣ)
5. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
6. Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).
7. Η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε.).
8. Κέντρο Μελετών και Ασφαλείας (Κ.Ε.Μ.Ε.Α.)

et al., 2021, p. 28).

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Κεφάλαιο πρώτο

Η διαλεκτική της κυβερνοϊσχύος με τα πεδία πολέμου

Περί εθνικής ισχύος

Ανέκαθεν η έννοια της εθνικής ισχύος υπήρξε άρρηκτα συνδεδεμένη με την έννοια εξυπηρέτησης και προαγωγής του εθνικού συμφέροντος. Ανεξαρτήτως προτιμήσεως διεθνολογικής θεώρησης η ιστορική αλήθεια είναι αδιαπραγμάτευτη: στο άναρχο και ανταγωνιστικό διεθνές σύστημα η κρατική ισχύς διεκδικεί διαχρονικά και κατ' αποκλειστικότητα το προνόμιο να αποτελεί το μόνον αποδεκτό παγκοσμίως "συναλλακτικό νόμισμα" των διεθνών σχέσεων. Ως όρος ιστορικά απετέλεσε αντικείμενο πολλαπλών προσεγγίσεων με αποτέλεσμα η διεθνής βιβλιογραφία να βρίθει εννοιολογικών ορισμών.[3] Συνεπώς, δεν αποτελεί έκπληξη ότι, καίτοι αποτελεί κεντρική έννοια των διεθνών σχέσεων, εξ ορισμού η χρήση της υποδηλώνει σύγχυση και ασάφεια (Keohane & Nye, 1989, p. 11). Παρά ταύτα, ακόμη και σήμερα στους κύκλους της εφαρμοσμένης πολιτικής, και ανεξαρτήτως ακροατηρίου, η εκφορά της και μόνον εκπέμπει κύματα μυστικής σαγήνης και ελκύει πάντοτε την προσοχή.

Σε μια πρώτη προσέγγιση η ισχύς είναι η ικανότητα να εξασφαλισθεί το επιδιωκόμενο αποτέλεσμα (Nye, 2004/2005, σ. 118). Εν προκειμένω, ο ελλοχεύων κίνδυνος είναι να παρερμηνευτεί η έννοια της ισχύος και να ταυτιστεί μόνον με όρους εξαναγκασμού και επιβολής, όμως δεν δύναται να αγνοηθεί η δυνατότητα εξυπηρέτησης του εθνικού συμφέροντος μέσω της εξαγοράς, της πειθούς ή ακόμη και της γοητείας. Άλλη προσέγγιση ορίζει την ισχύ ως τη διάδραση μεταξύ δύο

[3] Ενδεικτικά ιστορικά: ο Kautilya Ινδός λόγιος της αρχαίας Ινδίας τον 4ο π.Χ. αιώνα όρισε την ισχύ ως την κατοχή δύναμης που προκύπτει συνδυαστικά από τη γνώση, τη στρατιωτική δύναμη και την ανδρεία (Κουλουμπής, 2008, σσ. 93-94). Έναν αιώνα νωρίτερα, στο 5ο του Βιβλίο (89ο εδάφιο), ο Θουκυδίδης, στον περίφημο διάλογο Αθηναίων και Μηλίων διατυπώνει την άποψη ότι ο ισχυρός επιβάλλει ό,τι του επιτρέπει η η δύναμίς του και ο ασθενής παραχωρεί ό,τι του επιβάλλει η αδυναμία του, ενώ ο Machiavelli τον 16ο αιώνα ταύτισε την ισχύ με τον φόβο (Μακιαβέλι, 1532/2012, p. 88).

δρώντων όπου ο Α δρων έχει τη δυνατότητα να ελέγξει τη σκέψη και τις πράξεις του Β δρώντος (Κουλουμπής, 2008, σ. 94). Ενώ, μια τρίτη υποστηρίζει ότι η ισχύς είναι ο κεντρικός άξονας περιστροφής του τρόπου δράσης των κρατών και η ταξινομία της περιλαμβάνει τη λανθάνουσα ισχύ (οικονομία και τεχνολογία) και τη στρατιωτική ισχύ (Mearsheimer, 2001/2011, σ. 42). Στο περιθώριο των ακαδημαϊκών προσεγγίσεων και διενέξεων ο λιγότερο θεωρητικός και περισσότερο πρακτικός αμερικανικός Στρατός κατά τη ψυχροπολεμική περίοδο υιοθέτησε την οπτική ότι η εθνική ισχύς εδράζεται πρωτευόντως επί τεσσάρων πυλώνων ισχύος: στη Διπλωματική ισχύ, στην Πληροφοριακή, στη Στρατιωτική και στην Οικονομική.[4] Το υπόψιν μοντέλο εγκαταλείφθηκε πολύ πρόσφατα, μόλις το 2018, και στη θέση του εισήχθη η πιο διασταλτική θεώρηση πως η εθνική ισχύς εδράζεται πρωτευόντως επί οκτώ πυλώνων ισχύος, εισάγοντας πλέον των προηγουμένων τη Χρηματοοικονομική ισχύ, την ισχύ των Πληροφοριών, την ισχύ του Δικαίου και την ισχύ της Ανάπτυξης (United States/Joint Chiefs of Staff [US/JCS], 2018b, p. II-8; Aftergood, 2018).[5]

Ο Αμερικανός Καθηγητής Joseph Nye διακρίνει δύο μορφές ισχύος την ήπια και τη σκληρή, με την τελευταία να επιτυγχάνει τους στόχους της είτε με απειλή και εξαναγκασμό (μαστίγιο) είτε με χρήση ανταμοιβών (καρότο) (Nye, 2004/2005, σ. 33). Ο Nye υπεστήριξε ότι οι ΗΠΑ ήταν το ισχυρότερο κράτος της υφηλίου όχι μόνον με όρους στρατιωτικής ισχύος αλλά και με όρους ήπιας ισχύος, δηλαδή της ικανότητας να αποκομίζουν το επιδιωκόμενο όφελος δια της θέλξης, και όχι μέσω εξαναγκασμού ή εξαγοράς, άρα κατάληγε ότι η ήπια ισχύς είναι το "δεύτερο πρόσωπο της ισχύος" (Nye, 2004/2005, σ. 33). Κάποιοι εκ των σκεπτικιστών είναι επιφυλακτικοί στην ιδέα της ήπιας ισχύος, καθόσον αφενός δεν αποτελεί εγγενώς απτό εργαλείο άσκησης πολιτικής και αφετέρου ούτε μπορεί να ποσοτικοποιηθεί (Armitage & Nye, 2007, p. 9). Σ’ αυτούς ο Nye απαντά ότι μπερδεύουν το αναγκαίο με το επαρκές και ότι είναι μονοδιάστατοι παίκτες στο τριδιάστατο παίγνιο των διεθνών σχέσεων. Κατόπιν των ανωτέρω, αβίαστα προκύπτουν τα ερωτήματα τελικά ποια είναι η θέση

[4] Πρόκειται για το πασίγνωστο ακρωνύμιο DIME, ήτοι Diplomatic-Informational-Military-Economic.

[5] Πρόκειται πλέον για το ακρωνύμιο MIDFIELD, ήτοι Military-Informational-Diplomatic-Financial-Intelligence-Economic-Law-Development. Παρατηρείται ότι παρά το θόρυβο που δημιουργείται περί της κυβερνοϊσχύος απουσιάζει η ρητή αναφορά της στους πρωτεύοντες πυλώνες εθνικής ισχύος.

και ποια μπορεί να είναι μελλοντικά η θέση της κυβερνοϊσχύος ως παράγοντα εθνικής ισχύος.

Εννοιολόγηση της κυβερνοϊσχύος

Καθίσταται επιτακτική ανάγκη στο σημείο αυτό να προσδιορισθεί με τη δέουσα ακρίβεια το εννοιολογικό περιεχόμενο θεμελιωδών εννοιών, υπό το πρίσμα της στρατηγικής βεβαίως, αποφεύγοντας προσεκτικά τις παγίδες τόσο της περιττής τεχνικότητας όσο και της νομικής σχολαστικότητας. Τρεις έννοιες αποτελούν τα δομικά συστατικά στην "επανάσταση της τεχνολογίας της πληροφορίας"[6], και συγκεκριμένα ο "κυβερνοχώρος", η "κυβερνοϊσχύς" και η "κυβερνοστρατηγική" (Gray, 2013, p. 8).[7]

Καίτοι το υπόψιν γνωστικό αντικείμενο αριθμεί μόλις τέσσερις δεκαετίες ζωής έχει ήδη υποστεί τη βάσανο πολλαπλών ακαδημαϊκών, και όχι μόνον, προσεγγίσεων με αποτέλεσμα να "μαστίζεται" από πληθωρισμό ορισμών. Εξ όλων αυτών, και για τις ανάγκες του εν λόγω πονήματος, επελέγησαν οι πλέον συνεπείς και διαυγείς ορισμοί, χωρίς αυτό να σημαίνει ότι είναι οι πλέον αποδεκτοί διεθνώς ή ότι δεν φέρουν εγγενείς αδυναμίες. Τούτων λεχθέντων, ως κυβερνοχώρος ορίζεται:

> το παγκόσμιο πεδίο εντός του πληροφοριακού περιβάλλοντος, του οποίου ο διακριτός και μοναδικός χαρακτήρας οριοθετείται από τη χρήση των ηλεκτρονικών μέσων και του ηλεκτρομαγνητικού φάσματος, προκειμένου να δημιουργηθούν, αποθηκευτούν, τροποποιηθούν, ανταλλαγούν και εκμεταλλευτούν πληροφορίες, μέσω ανεξαρτήτων διασυνδεδεμένων δικτύων και με τη χρήση τεχνολογιών πληροφορικής και επικοινωνιών (Kuehl, 2009, p. 28).[8]

[6] Οι όροι "επανάσταση της τεχνολογίας της πληροφορίας" (IT revolution) ή "Εποχή της Πληροφορίας" (Information Age) ταυτίζονται εννοιολογικά με τον όρο"cyber" (Gray, 2013, p. 10). Ο τελευταίος δεν αποδίδεται ελληνιστί, καθόσον δύναται να χρησιμοποιηθεί μόνον ως πρόθεμα συνθέτων όρων.

[7] Απόδοση ελληνιστί των όρων "cyberspace", "cyber power" και "cyber strategy" αντίστοιχα.

[8] Ο υπόψιν ορισμός αγνοεί επιδεικτικά την έννοια της εθνικής διάστασης του κυβερνοχώρου (κ/χ). Η άνευ όρων υιοθέτησή του δύναται να προκαλέσει δύο σημαντικές παρερμηνείες. Αφενός, ότι ο

Σε ό,τι αφορά στην κυβερνοϊσχύ αυτή θα μπορούσε να ορισθεί ως "η ικανότητα χρήσης του κυβερνοχώρου προς δημιουργία πλεονεκτήματος και επηρεασμού των γεγονότων επί οιουδήποτε επιχειρησιακού περιβάλλοντος και επί οιουδήποτε παράγοντος ισχύος" (Kuehl, 2009, p. 38). Ή απλούστερα και εγγύτερα στη διαίσθηση, παραφράζοντας τον κλασικό θεωρητικό της αεροπορικής ισχύος Στρατηγό William (Billy) Mitchel (Gray, 2012, p. 9), κυβερνοϊσχύς είναι η ικανότητα να κάνεις κάτι στρατηγικά χρήσιμο μέσω του κυβερνοχώρου.[9]

Σε ό,τι δε αφορά στη χρήση του όρου κυβερνοστρατηγική, θα πρέπει να σημειωθεί ότι η λογική σύνθεσης του όρου, δηλαδή η παράθεση του συνθετικού "κυβερνο-" έμπροσθεν της "στρατηγικής", είναι παραπλανητική και δύναται να οδηγήσει σε επικίνδυνες παρερμηνείες. Ότι δηλαδή, η ιδιαιτερότητα της φύσης του κυβερνοχώρου είναι τέτοια που καλεί για μια διακριτού είδους στρατηγική από αυτή των υπολοίπων πεδίων. Όμως, η στρατηγική είναι στρατηγική, είτε πρόκειται για τη χερσαία ισχύ είτε για τη θαλάσσια κοκ., οπότε η ορθή διατύπωση, και όχι μόνον για λόγους συντακτικής ορθότητας, είναι "στρατηγική για τον κυβερνοχώρο" (Gray, 2013, p. 10).

Κρίνεται σκόπιμο να τονισθεί η διαφορά μεταξύ της εννοιολόγησης του όρου κυβερνοπόλεμος, και των συν αυτώ εννοιών του κυβερνομάχεσθαι, της κυβερνοεπίθεσης, της κυβερνοάμυνας, της κυβερνοεκμετάλλευσης κοκ, έναντι των προαναφερθεισών εννοιών.[10] Ο κυβερνοπόλεμος δεν προσφέρει ουδεμία

ενεργών (ο "επιτιθέμενος") δύναται να χρησιμοποιήσει τον κ/χ ως προνομιακό πεδίο αντιπαρά-θεσης για κυριαρχία ή για επίτευξη τακτικού/επιχειρησιακού/στρατηγικού αποτελέσματος χωρίς απολύτως καμία συνέπεια κατά το ΔΔ (jus ad bellum & jus in bello) και αφετέρου το αντίστροφο, ότι ο αποδέκτης (ο "αμυνόμενος") στερείται δυνατότητας επίκλησης κάθε αρχής ή κανόνα του ΔΔ. Άρα, θα μπορούσε να ωθήσει σε μια άνευ προηγουμένου ανεξέλεγκτη έκρηξη/κλιμάκωση κυβερνοπεριστατικών.

[9] Επισημαίνεται η χρήση του όρου "μέσω" αντί του όρου "στον", γιατί η κυβερνοϊσχύς βεβαίως εκπορεύεται από τον κυβερνοχώρο και εφαρμόζεται δια του κυβερνοχώρου, πλην όμως η στρατηγική δεν εγκλωβίζεται στη λογική των προκληθέντων πρωτογενώς αποτελεσμάτων, τα οποία όντως ανήκουν αποκλειστικά στη σφαίρα του κυβερνοχώρου. Η στρατηγική ενδιαφέρεται για τη σχέση αιτίας αιτιατού, και η κυβερνοϊσχύς δευτερογενώς, τριτογενώς κοκ (αδιάφορο το μήκος της αιτιακής αλυσίδας) δύναται αιτιοκρατικά να παράξει αποτελέσματα στα υπόλοιπα πεδία πολέμου.

[10] Εν προκειμένω, οι έννοιες νοηματοδοτούνται με το αυτό εννοιολογικό περιεχόμενο που φέρουν τα δεύτερα συνθετικά τους στα υπόλοιπα, φυσικά, πεδία πολέμου και όχι με το κατά το δοκούν

ακαδημαϊκού τύπου ευελιξία στη νοηματοδότησή του, καθόσον τυγχάνει επιπροσθέτως έμφορτος νομικού, πολιτικού και ηθικού βάρους. Οιαδήποτε προσθήκη ή απαλοιφή, αοριστολογία ή γενίκευση, ακούσια ή εκούσια παρερμηνεία και γενικότερα εν τέλει οιαδήποτε επιλογή στο λεκτικό του προκαλεί διαφορετικές μεν αλλά πραγματικές δε συνέπειες στον πραγματικό, φυσικό κόσμο.[11] Κυβερνοχώρος, κυβερνοϊσχύς και στρατηγική για τον κυβερνοχώρο διαθέτουν την πολυτέλεια να είναι έννοιες δεκτικές περισσότερο τεχνικού ορισμού, τη στιγμή που ο κυβερνοπόλεμος και το κυβερνομάχεσθαι, δηλαδή ο τρόπος διεξαγωγής του κυβερνοπολέμου, υπόκεινται πρωτευόντως σε υποκειμενική κρίση από κοινού με πολιτική επιλογή (Gray, 2013, p. 10).

Για την καλύτερη στρατηγική κατανόηση της "επανάστασης της τεχνολογίας της πληροφορίας" αναγκαιεί καταρχάς να οριοθετηθούν τα τρία πλαίσια υπαγωγής της, και συγκεκριμένα αυτά της γενικής θεωρίας στρατηγικής, της γεωγραφίας και της πληροφορίας.

Η κυβερνοϊσχύς υπό τη γενική θεωρία στρατηγικής

Εξ αρχής αναγκαιεί να καταγραφεί ότι η "επανάσταση της τεχνολογίας της πληροφορίας", με τις όποιες τεχνολογικές, ψυχολογικές, πολιτικές, στρατιωτικές και άλλες πτυχές της, υπόκειται καθ’ ολοκληρίαν στην εξουσία της γενικής θεωρίας της στρατηγικής (Gray, 2013, p. 12). Λαβόντες υπόψιν ότι η στρατηγική κατάφερε να προσδώσει στρατηγικό νόημα στην ανάπτυξη, κατοχή και χρήση του πυρηνικού οπλοστασίου και να τιθασεύσει την πυρηνική απειλή, εντάσσοντας εν τέλει την πυρηνική ισχύ στο σχεδιασμό της, η κυβερνοϊσχύς δεν θα αποτελέσει λογικά γι’ αυτήν δύσκολο έργο. Θα πρέπει να γίνει αντιληπτή, για τις ανάγκες της στρατηγικής θεώρησης, ως μια επιπλέον κατηγορία όπλου, με όπλο εν προκειμένω να ορίζεται ως

αποδιδόμενο, "δημοσιογραφική αδεία", εννοιολογικό περιεχόμενο δημοσιογραφικής αρθρογραφίας.

[11] Για πληρέστερη κατανόηση στα Παραρτήματα «Β» και «Γ» παρουσιάζονται η ταξινομία των κυβερνοόπλων με τεχνικές προσβολής και η διεθνής πρακτική αντίστοιχα.

οιοδήποτε μέσο δύναται κατά τη χρήση του να προκαλέσει βλάβη στον αντίπαλο.[12] Αδιαμφισβήτητα πολύ πιο τεχνικό, πιο διαβρωτικό και ενοχλητικά πανταχού παρόν σε σχέση με τα ήδη γνωστά μας κινητικά όπλα, αλλά πάντως όπλο.

Η ιδιαίτερη φύση της κυβερνοϊσχύος δε διστάζει να προκαλέσει καλά θεμελιωμένες επί σειρά ετών συμβατικές αντιλήψεις περί στρατιωτικής στρατηγικής και πολέμου. Επί παραδείγματι, ένας εκ των επικρατούντων ορισμών στρατιωτικής στρατηγικής την ορίζει ως "την κατεύθυνση και τη χρήση βίας και την απειλή χρήσης βίας για την επίτευξη πολιτικών ΑΝΣΚ όπως αποφασίστηκαν από την πολιτική" (Gray, 2016, pp. 2, 13). Όμως, προφανώς στην περίπτωση της κυβερνοϊσχύος εκλείπει η έννοια της άσκησης φυσικής βίας, συνεπώς βάσει του ανωτέρω ορισμού δεν υπάγεται στη στρατιωτική στρατηγική! Εναλλακτικά, και προκειμένου να υπερπηδηθεί το εμπόδιο προϋπόθεσης άσκησης φυσικής βίας, θα μπορούσε να υιοθετηθεί ο ορισμός ότι "στρατιωτική στρατηγική είναι η χρήση όλων των στρατιωτικών μέσων ενός κράτους για την επίτευξη των πολιτικών αντικειμενικών σκοπών του ενόψει πραγματικής ή ενδεχόμενης σύγκρουσης" (Κολιόπουλος, 2010, σ. 44). Εν προκειμένω, ως μοναδική προϋπόθεση τίθεται η υπαγωγή της εθνικής κυβερνοϊσχύος, εν όλω ή εν μέρει, στο αρμόδιο Υπουργείο Αμύνης.

Έως και ο μεγάλος Πρώσος στοχαστής στρατηγικής δύναται σε πρώτη επιπόλαια ανάγνωση να θεωρηθεί παρωχημένος ή έστω ασύμβατος με τη χρήση της κυβερνοϊσχύος, και να κινδυνεύει με αποκαθήλωση. Και αυτό καθόσον, κατά τον Κλαούζεβιτς, ο στρατιωτικός αντικειμενικός σκοπός του πολέμου δεν είναι άλλος από τον αφοπλισμό του εχθρού και ο μοναδικός τρόπος επίτευξής του είναι η συμπλοκή,

[12] Η ίδια η φύση της κυβερνοϊσχύος, δεδομένης της εγγενούς αδυναμίας της να ασκήσει φυσική βία σε αντικείμενο με φυσική υπόσταση, αποτελεί τον κύριο λόγο έδρασης του θεμελιώδους ερωτήματος, ανοικτού επί του παρόντος από τη διεθνή νομική κοινότητα, κατά πόσον δύναται η κυβερνοϊσχύς να θεωρηθεί ως όπλο. Συναφώς, κατά πόσον η χρήση της δύναται να θεωρηθεί ως ένοπλη βία, η οποία υπό προϋποθέσεις δύναται να αναχθεί στο επίπεδο επίθεσης και να πυροδοτήσει το δικαίωμα αυτοάμυνας και συλλογικής άμυνας κρατικών δρώντων. Προφανώς, η τελική απόφαση συμπερίληψης ή όχι στη λίστα των όπλων ή εξαναγκασμού κατά το ΔΔ θα είναι εν τέλει πολιτική. Αυτό ουδόλως αποτελεί πρόβλημα για τη γενική θεωρία στρατηγικής, η οποία καλείται, διαχρονικά απαλλαγμένη από νομικά βαρίδια και πολιτικές σκοπιμότητες, να απαντά για κάθε ζήτημα το οποίο εμπίπτει στο πεδίο της "Και λοιπόν;"

η δια τον όπλων απόφαση, η οποία συνεπάγεται κατ' ανάγκην αιματοχυσία (Clausewitz, 1832/1989, book 1, ch.1, p. 75; Κολιόπουλος, 2010, σ. 156). Αλλά οι εχθροπραξίες στον κυβερνοχώρο, εγκλωβίζουν πρωτογενώς τα αποτελέσματά τους στο ψηφιακό περιβάλλον, δεν έχουν καμία επαφή με το φυσικό περιβάλλον και συνεπώς δεν δύνανται να προκαλέσουν καμία αιματοχυσία. Άρα; Τέτοιου τύπου αμφιβολίες δεν θα πρέπει επ' ουδενί να παραλύσουν τη σύγχρονη στρατηγική σκέψη. Αυτό που απαιτείται είναι να εντρυφήσει κανείς στο έργο του Πρώσου στρατηγιστή και να κατανοήσει την ουσία των γραφομένων του. Η αναμφισβήτητη αλήθεια ότι κανένας αφοπλισμός του εχθρού δεν πρόκειται να επισυμβεί και ακόμη περισσότερο κανένας πραγματικός πόλεμος δεν πρόκειται να κερδηθεί στα ψηφιακά πεδία μαχών των σύγχρονων κυβερνοστρατιωτών. Θα απαιτηθεί σε κάθε περίπτωση η διεξαγωγή συμβατικού κινητικού πολέμου, ο οποίος μπορεί να συνεπικουρείται στο έργο του από επιχειρήσεις στον κυβερνοχώρο, πλην όμως αυτές μεμονωμένα εκ φύσεως δεν κατακτούν έδαφος, δεν ασκούν θανατηφόρα φυσική βία, δεν αφοπλίζουν τον εχθρό. Συνεπώς, μεμονωμένες επιχειρήσεις αποκλειστικά στον κυβερνοχώρο δεν συνιστούν πόλεμο υπό την έννοια ότι δεν δύνανται να παράξουν αποτελέσματα πολέμου. Άρα, ο Πρώσος στοχαστής παραμένει επίκαιρος όσο ποτέ.

Άλλωστε, η μη άσκηση θανατηφόρας φυσικής βίας, ως όπλου διεξαγωγής πολέμου, δεν αποτελεί ιστορικό προνόμιο του κυβερνοπολέμου. Πολύ πριν την ανακάλυψη των πρωτοκόλλων επικοινωνιών δικτύων και των ηλεκτρονικών υπολογιστών διεξήχθησαν οικονομικοί πόλεμοι, οι οποίοι μπορεί μεν σε πρώτο χρόνο να μην επέφεραν την κλαουζεβιτσιανή αιματοχυσία, πλην όμως εδύναντο να οδηγήσουν ολόκληρους πληθυσμούς σε λιμό ή να αποστερήσουν την πολεμική βιομηχανία από τις απαραίτητες, για τη συνέχιση διεξαγωγής του πολέμου, πρώτες ύλες.

Συνεπώς, καθίσταται εκ των ανωτέρω πρόδηλο ότι η κυβερνοϊσχύς δεν εισάγει "καινά δαιμόνια" στη γενική θεωρία στρατηγικής. Απλώς, η κυβερνοϊσχύς θα είναι μία ακόμη εκ των ασαφών κατηγοριών ισχύος (Gray, 2013, p. 14). Αφού όμως, οι κυβερνοστρατιώτες χρησιμοποιούν εξοπλισμό, έστω και μη συμβατικό, με απώτερο στόχο την επίτευξη πολιτικού σκοπού, όπως ακριβώς και τα άλλα συμβατικά στρατιωτικά μέσα, η παραγόμενη ισχύς, ήτοι η κυβερνοϊσχύς, υπάγεται αυτοδικαίως στη γενική θεωρία στρατηγικής.

Ο κυβερνοχώρος ως γεωγραφικό πεδίο πολέμου

Είναι πολύ βολικό και μάλλον η πρώτη προφανής επιλογή, σε ό,τι αφορά στην αντίληψη χρήσης του κυβερνοχώρου για την ειρηνική περίοδο, την πολεμική προπαρασκευή, τον πόλεμο και την ίδια τη στρατηγική, να θεωρηθεί ότι η προσθήκη απλώς μιας επιπλέον έδρας στο τετράεδρο, κατά την κρατούσα άποψη, των πεδίων διεξαγωγής πολέμου και η ανάπλασή του πλέον σε πεντάεδρο αρκεί. Πρόκειται προδήλως για τέχνασμα, καθόσον μια τέτοια αναγωγή με γεωγραφικούς όρους είναι αντίθετη στη διαίσθηση, δεδομένης της ατοπικότητας του κυβερνοχώρου. Είναι ορθότερο ο κυβερνοχώρος να θεωρηθεί ως αυτό και μόνον αυτό που ακριβώς είναι, ήτοι μια σύνθεση δικτυωμένων χώρων οι οποίοι κατασκευάσθηκαν από τον άνθρωπο. Η άνευ όρων απλουστευτική θεώρηση ότι αποτελεί το πέμπτο γεωγραφικό πεδίο πολέμου εγκυμονεί κινδύνους. Δεδομένου ότι η ιδανική προσέγγιση του κυβερνοχώρου αποτελεί μια γνωστική εν εξελίξει εργασία και χωρίς καμία διάθεση διεκδίκησης δαφνών επιστημονικής ορθότητας εκτιμάται ότι το τέχνασμα θεώρησης του κυβερνοχώρου ως πέμπτου γεωγραφικού πεδίου είναι χρήσιμο μόνον ως μια βολική τεχνική για την τεχνητή πρόκληση στρατηγικού ενδιαφέροντος (Gray, 2013, p. 15).

Στην απόπειρα επέκτασης χρήσης του υπόψιν τεχνάσματος στο επιχειρησιακό επίπεδο ελλοχεύει υπαρκτός κίνδυνος. Συγκεκριμένα, είναι σχεδόν βέβαιο ότι αυτή η επιλογή θα οδηγήσει νομοτελειακά σε υιοθέτηση μη ορθών αναλογιών με τα υπόλοιπα επιχειρησιακά πεδία, τα οποία διαθέτουν εγγενώς πραγματικά χωρικά χαρακτηριστικά και ιδιότητες του φυσικού κόσμου. Η απουσία της φυσικής διάστασης της κυβερνοϊσχύος συνεπάγεται μια άβολη μη απτότητα σε έκφανση της στρατιωτικής ισχύος, η οποία δεν συνάδει επ’ ουδενί με την εμπεδωμένη στρατιωτική κουλτούρα του κινητικού πολέμου. Η αιθεριότητα της κυβερνοϊσχύος είναι τόσο υπερβατικά ξένη, ακόμη και σε διανοητικό επίπεδο για σκεπτόμενους με όρους κινητικού πολέμου, ώστε μοιραία αυτοί θα αποπειραθούν να τη μεταφράσουν υπό όρους πιο οικείους στη στρατιωτική τους αντίληψη από ότι στην πραγματικότητα είναι, ή μπορεί να είναι, η κυβερνοϊσχύς και ο κυβερνοχώρος. Η εξοικείωση τους θα

προκύψει μέσω αναγνώρισης υπαρκτών και κυρίως ανύπαρκτων αναλογιών με τα λοιπά πεδία πολέμου, μια διαδικασία ψυχολογικού τύπου μεροληψίας αντίστοιχη της παρειδωλίας.

Αποτελεί στοιχείο της ιστορίας της στρατηγικής ότι οι άνθρωποι αντιδρούν σε νέα ερεθίσματα, σε νέες προκλήσεις, βασιζόμενοι κυρίως επί τη βάσει στρατηγικής κατανόησης απαντήσεων σε παλαιές προκλήσεις. Το μείζον ανακύπτον θέμα είναι ότι στην περίπτωση της κυβερνοϊσχύος δεν υπάρχει ιστορικό. Επιπροσθέτως, η θεωρία της "Επανάστασης των Στρατιωτικών Υποθέσεων"[13], η οποία επιχειρεί να ερμηνεύσει το φαινόμενο σποραδικών σημαντικών μεταβολών στον χαρακτήρα της διεξαγωγής του πολέμου δεν είναι τόσο αξιόπιστη. Αυτό δεν αποτελεί κατ' ανάγκην κριτική στη θεωρία της Επανάστασης των Στρατιωτικών Υποθέσεων ή στην τρέχουσα γενική αντίληψη περί του τι εστί κυβερνοπόλεμος ή του τι συνιστά απόδειξη διεξαγωγής κυβερνοπολέμου.[14] Η πραγματικότητα είναι ότι οι τολμηρές και ελκυστικές ερμηνείες των φερόμενων ως τεραστίων στρατηγικών ιστορικών αλλαγών δεν είναι τίποτε λιγότερο και τίποτε περισσότερο από θεωρίες. Θεωρίες με προδήλως ισχυρά πειστική εξηγηματική ισχύ, αλλά παρά ταύτα ασθενή αποδεικτική ισχύ. Και αυτό γιατί η ίδια η θεωρία της Επανάστασης των Στρατιωτικών Υποθέσεων είναι μια συλλογή νοητικών κατασκευών, εκπονηθέντων από μελετητές, που συσχετίζονται με πολύπλοκες διαδικασίες στον πραγματικό κόσμο και οι οποίες όμως συνήθως δύνανται, δυστυχώς για τη θεωρία, να είναι δεκτικές πολλαπλών ευλογοφανών συσχετίσεων αιτίας αιτιατού, πλέον του κυρίαρχου αφηγήματος (Gray, 2013, p. 17).

Οι ανωτέρω επισημάνσεις επιχειρούν να καταγράψουν την ορθή στρατηγική σημασία της θεώρησης του κυβερνοχώρου ως πέμπτου γεωγραφικού πεδίου πολέμου. Όμως, καίτοι πρόκειται για ένα ριζικά διαφορετικό πεδίο πολέμου με πρωτεύοντα χαρακτηριστικά την ατοπικότητα και τη μη απτότητα, δεν θα πρέπει να διελάθει της προσοχής μας ότι εφόσον δεν πρόκειται για νοητικό κατασκεύασμα αλλά για επίτευγμα του υλικού κόσμου, τότε ως τέτοιο διαθέτει κατ' ανάγκην επισυνδέσεις, γέφυρες με τον κόσμο της ύλης, οι οποίες αναμενόμενα ενυπάρχουν στον φυσικό

[13] Απόδοση ελληνιστί του όρου "Revolution in Military Affairs" (RMA).

[14] Για πληρέστερη εικόνα της συσχέτισης Επανάστασης των Στρατιωτικών Υποθέσεων και επανάστασης της τεχνολογίας της πληροφορίας βλ. Παράρτημα «Α».

κόσμο. Πράγματι, ο κυβερνοχώρος διαθέτει, εκτός των προαναφερθέντων χαρακτηριστικών του, επιπλέον απτή, συμβατικά προσδιορισμένη χωρική διάσταση, καθόσον συντίθεται από μηχανήματα και δικτυακές υποδομές, υπηρετείται από ανθρώπους και οι συνέπειες του κυβερνοπολέμου επισυμβαίνουν, στην περίπτωση διεξαγωγής συνδεδυασμένων επιχειρήσεων, στις λοιπές γεωγραφίες, εκτός του κυβερνοχώρου.[15]

Ίσως εν τέλει, παρά τους κινδύνους που εγκυμονεί, είναι αποδεκτό να θεωρηθεί ο κυβερνοχώρος ως ένα επιπρόσθετο, μοναδικό στο είδος του, γεωγραφικό πεδίο. Η μη φυσική διάσταση του κυβερνοχώρου αποτελεί την κατ' εξοχήν τομεακή του ιδιαιτερότητα, αλλά το γεωφυσικό δεδομένο της μη απτότητάς του δεν θα πρέπει να υπερεντυπωσιάζει. Η αλήθεια είναι ότι μέχρι να ενσκύψει ο κυβερνοχώρος και η κυβερνοϊσχύς το σκεπτικό, η θεωρία, η ηθική και η νομοθεσία αφορούσε αποκλειστικά και μόνον στην ένοπλη βία. Προφανώς, ο κυβερνοχώρος και η χρήση του ηλεκτρομαγνητικού φάσματος θέτουν ασυνήθεις προκλήσεις στη στρατηγική σκέψη και στην πρακτική. Πλην όμως, η τρέχουσα εδραιωμένη αντίληψη περί του κυβερνοχώρου, αν και υπεραπλουστευτική, φαίνεται να είναι αρκούντως ορθή και λειτουργική. Ήτοι, η θεωρία ερμηνείας του κυβερνοχώρου ως γεωγραφικού πεδίου διεξαγωγής πολέμου είναι επαρκής, προκειμένου να εξυπηρετήσει τους σκοπούς της στρατηγικής εννοιολόγησης και αρκετά καλή για την άσκηση στρατηγικής (Gray, 2013, p. 18).

[15] Μερικά ενδιαφέροντα στοιχεία περί υποδομών του κυβερνοχώρου: α) Εν έτει 2023 υφίστανται 4.989 data centers κατανεμημένα σε 130 χώρες παγκοσμίως (Data Center Map, 2023; Bazzan et al. 2023). β) Τον Ιούνιο του 2021 εκ των 400 ενεργών παγκοσμίως υποθαλασσίων καλωδίων, συνολικού μήκους πλέον των $1,3*10^6$ Km, τα 18 διατλαντικά υποθαλάσσια καλώδια του Β. Ημισφαιρίου διακινούσαν το 95% των διεθνών δεδομένων. Εξ ου, ο ΓΓ του ΝΑΤΟ Jens Stoltenberg, ήδη από τον Οκτώβριο του 2020, υπογράμμισε τη σημασία της Συμμαχίας να προστατεύσει την υπόψιν υποδομή ως κρίσιμη σε περίοδο σύρραξης, με τη Ρωσική Ομοσπονδία να διαθέτει ως και πυρηνοκίνητο μη επανδρωμένο υποβρύχιο (το Poseidon) για τη διενέργεια δολιοφθορών. Μείζον θέμα ανακύπτει συνδυαστικά από το ότι η συντριπτική πλειοψηφία ανήκει σε ιδιωτικές εταιρίες (Facebook και Amazon ήλεγχαν το 2021 περίπου το 29% των καλωδίων), ότι διέρχεται από διεθνή ύδατα και ότι δεν καλύπτεται από τις υφιστάμενες νομικές πρόνοιες του Δικαίου της Θάλασσας (Wall & Morcos, 2021).

Η λειτουργική διάσταση της "επανάστασης της τεχνολογίας της πληροφορίας"

Το τρίτο πλαίσιο υπαγωγής της "επανάστασης της τεχνολογίας της πληροφορίας" είναι αυτό της πληροφορίας. Η πληροφορία ως οργανωσιακή ιδέα απελάμβανε μεγάλης δημοφιλίας τη δεκαετία του ’90. Αυτό προτού επέλθει η επίγνωση ότι η εσφαλμένη, αλλά και η ορθή χρήση της, είναι τόσο κοντά στο να τυγχάνουν πρακτικά ανοριοθέτητες εννοιολογικά, ώστε εν τέλει η πληροφορία να στερείται οιασδήποτε αποδεικτικής αξίας (Gray, 2013, p. 18). Αυτός ο εννοιολογικός υποβιβασμός της πληροφορίας, έφερε την υπογραφή στρατηγικής αποφασιστικότητας και ήταν ορθός ως επιλογή, πλην όμως δεν ήρθε χωρίς την καταβολή αναλόγου τιμήματος, το οποίο μεταξύ άλλων περιελάμβανε την κατανόηση του τι είδους "επανάσταση της τεχνολογίας της πληροφορίας" χρειαζόμαστε.

Το ότι η κυβερνοϊσχύς είναι μια νέα, μη οικεία, αχαλίνωτη, επί του παρόντος, και πολλά υποσχόμενη μορφή ισχύος είναι αν μη τι άλλο προφανές. Αυτό που δεν είναι καθόλου προφανές είναι τι σημαίνει όλη αυτή η τεχνολογική καινοτομία για τη στρατηγική. Ο μη τετριμμένος κίνδυνος, σε ό,τι αφορά τον κυβερνοχώρο, είναι η εύλογη ανησυχία, που κάποιες φορές αγγίζει τα όρια του ανείπωτου τρόμου, πως η κυβερνοϊσχύς και η διεξαγωγή κυβερνοπολέμου εκτός από μοναδικές στο είδος τους θα αποδειχθούν και υπερβατικά αποτελεσματικές. Ένας τρόπος για να διασκεδαστούν τέτοιου είδους φοβίες, για να γίνει κατανοητό τι σημαίνει επακριβώς η "επανάσταση της τεχνολογίας της πληροφορίας" και να προγνωσθεί η δυνητική ιστορική τροχιά της είναι η προσφυγή στη νοηματόδοτησή της ως προς τη λειτουργική χρήση της (Gray, 2013, p. 19). Ο σκοπός δεν είναι ούτε να υποβαθμιστεί ούτε να ευτελιστεί η έννοια, αλλά περισσότερο για να υπομνησθεί ότι ο ρόλος που διαδραματίζει δεν είναι διόλου καινοφανής στην ιστορία της στρατηγικής, καθόσον εύκολα διαπιστώνεται η ύπαρξη μιας longue durée συναφούς έννοιας. Για να καταστεί σαφέστερο το προφανές, η "επανάσταση της τεχνολογίας της πληροφορίας" αφορά στην πληροφορία και στην επικοινωνία της πληροφορίας για στρατηγικό σκοπό. Αρκούν μόνον ελάχιστες στιγμές για να αναγνωρίσει κανείς κάτι εξαιρετικά οικείο σε αυτές τις έννοιες. Κανείς δεν θα μπορούσε να αρνηθεί ότι από τεχνικής σκοπιάς κυβερνοχώρος και κυβερνοϊσχύς είναι μακράν πέραν των

συνηθισμένων. Όμως, το ίδιο ακριβώς δεν είχε συμβεί και στην περίπτωση ανακάλυψης του τηλέγραφου, τη δεκαετία του 1840; Και αργότερα το ίδιο δεν συνέβη εκ νέου, όταν το τηλέφωνο, τα ραδιοκύματα και η τηλεόραση απετέλεσαν το καθένα ξεχωριστά την αιχμή του δόρατος της τεχνολογίας της εποχής τους; Αυτό που αποτελεί απλή, αδιάψευστη ιστορική αλήθεια είναι ότι διαχρονικά οι αντίπαλες θεωρίες διαγκωνίζονται για την επικράτηση στην τριπλέτα προσέλκυση ενδιαφέροντος του κοινού - επίσημη έγκριση - χρηματοδότηση από τον αμυντικό προϋπολογισμό.

Αν μη τι άλλο, η κυβερνοϊσχύς είναι πληροφορία από κοινού με την επικοινωνία της πληροφορίας. Και ως τέτοια θα πρέπει να εκφραστεί μέσα από φυσικά δίκτυα τα οποία διαθέτουν αρχιτεκτονική στον υλικό κόσμο. Κατόπιν τούτου δεν αποτελεί ιδιαίτερη πρόκληση να αναγνωρισθεί ιστορικά η μακρόχρονη ύπαρξη της λειτουργικής χρήσης της υπό εξέταση έννοιας. Χωρίς να παύουν να είναι όντως εντυπωσιακά τα χαρακτηριστικά της, κυρίως η αστραπιαία ταχύτητα και η πανταχού παρουσία της, θα ήταν επωφελές να τοποθετηθεί η "επανάσταση της τεχνολογίας της πληροφορίας" στην ιστορική της προοπτική. Εάν πρόκειται κατ’ ουσίαν για πληροφορία τότε θα πρέπει να εκληφθεί ως απλώς η τελευταία και μόνον προσπάθεια της ανθρωπότητας να διευκολύνει τη λειτουργική χρήση της και την επικοινωνία της. Συνεπώς, η κυβερνοϊσχύς δεν αφορά σε αυτούς καθεαυτούς στους ηλεκτρονικούς υπολογιστές και σε αυτά καθεαυτά τα δίκτυά τους. αλλά στο τι δύνανται να εκτελέσουν οι δικτυωμένοι ηλεκτρονικοί υπολογιστές, σχετικά με τη διαμοίραση της πληροφορίας, και ποιες μπορεί να είναι οι συνέπειες (Gray, 2013, p. 20).

Έπεται, εκ των προαναφερθέντων, πως η "επανάσταση της τεχνολογίας της πληροφορίας" διεκπεραιώνει αυτό που θέλουν οι στρατηγιστές μακράν ταχύτερα, σε μεγάλες αποστάσεις και πιο κεκαλυμμένα από ότι γινόταν μέχρι την άφιξή της. Όμως, δεν εισάγει επ’ ουδενί καινά δαιμόνια ως προς τη λειτουργική χρήση της. Συναφώς, συνάγεται ως προς τη στρατηγική της σημασία ότι μάλλον πρόκειται για διαφορετικό είδος ισχύος από τα άλλα είδη και πιθανόν απλά να πρόκειται απλώς για έναν "ομαδικό παίκτη" στο διαρκώς εξελισσόμενο συνδεδυασμένο και πιθανώς ενοποιημένο αφήγημα διεξαγωγής πολέμου.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Κεφάλαιο δεύτερο

Θεσμικές αντιλήψεις των διεθνών δρώντων

Γενικά

Για παραπάνω από μια εικοσαετία ειδικοί και μη αναλίσκονται σε διαπιστώσεις περί του διογκούμενου κινδύνου από τις "κυβερνοαπειλές" και τις δυνητικές συνέπειες μιας επιτυχημένης "κυβερνοεπίθεσης". Η γκάμα των εξεταζόμενων σεναρίων είναι τεράστια. Εκκινεί από τη δυνατότητα εγκατάστασης κακόβουλου λογισμικού κατασκοπείας[16], το οποίο καταγράφει χρήση σε Η/Υ ή κίνηση δεδομένων σε δίκτυο, και κορυφώνεται με πλήθος καταστροφολογικών εκδοχών. Στο μενού των τελευταίων περιλαμβάνεται η διακοπή κρισίμων λειτουργιών σε εγκαταστάσεις πυρηνικών αντιδραστήρων, με στόχο την πρόκληση πυρηνικού ατυχήματος, η παραπλάνηση συστημάτων εναερίου ελέγχου κυκλοφορίας, με σκοπό την πρόκληση αεροπορικών δυστυχημάτων κτλ. Ανεξάρτητα από το πόσο κοντά στην αλήθεια βρίσκονται οι παραπάνω εκτιμήσεις κανένα από τα εσχατολογικά σενάρια δεν έχει επαληθευτεί, προς ώρας τουλάχιστον.

Πλην όμως, το σύνολο των διαπιστώσεων επαναπαύεται κυρίως σε εξαντλητικές αναλύσεις του τελικού σταδίου, ήτοι της εκτίμησης του μεγέθους της απειλής μέσω της αποτίμησης των πιθανών συνεπειών. Δεν φαίνεται να συγκεντρώνει τα φώτα της δημοφιλίας ο σκληρός πυρήνας του προβλήματος, η εννοιολογική αφετηρία, η οποία θα προσδιόριζε με τη δέουσα αυστηρότητα τα αρχέτυπα που με τη σειρά τους θα δομούσαν συνθετικά με σαφήνεια και πληρότητα το πρόβλημα. Αυτή η τυπική, με τη μαθηματική έννοια του όρου, εκκρεμότητα έχει ως λογική συνέπεια τη διαισθητική και κατά το δοκούν ερμηνεία των όρων. Επί παραδείγματι, ειδικά για την περίπτωση προβολής της κρατικής κυβερνοϊσχύος μέσω διεξαγωγής κυβερνοεπιθέσεων η διατύπωση του εννοιολογικού σκληρού πυρήνα συνίσταται στην αναγκαιότητα καθορισμού του σημασιολογικού περιεχομένου της

[16] Απόδοση ελληνιστί του όρου "spyware".

εξής απλής δυάδας ερωτημάτων: πρώτον, τι είναι κυβερνοεπίθεση και δεύτερον, ποια η ταξινομία της, εάν υπάρχει τέτοια.

Η επίλυση τέτοιων προβληματικών δεν αποτελεί κάποιου είδους υψηλού επιπέδου θεωρητική ακαδημαϊκή εκκρεμότητα προς μελλοντική διευθέτηση, καθόσον κάθε τέτοια προβληματική δεν εγκλωβίζεται μόνον σε θεωρητικό εννοιολογικό επίπεδο. Βρίσκει, απολύτως αναμενόμενα, άμεσα τη φυσική της διέξοδο και στον υλικό κόσμο, δεδομένου ότι αποτελεί τη γενεσιουργό αιτία ενός ρυθμιστικού διάκενου, ως προς τη νομιμότητα κατά το διεθνές δίκαιο ή έστω κατά τη διεθνή πρακτική η οποία επωάζει το διεθνές έθιμο. Έπεται, εν συνεχεία το προφανές, τέτοιου τύπου προβληματικές παρεισφρέουν εν είδει τροχοπέδης στην αξιοποίηση στο έπακρο της διατιθέμενης εθνικής κυβερνοϊσχύος κατά την εκπόνηση της εθνικής στρατηγικής. Ερωτήματα όπως: εάν η χρήση κυβερνοόπλων, κατά την προβολή κρατικής κυβερνοϊσχύος, θεωρείται από το διεθνές δίκαιο χρήση ένοπλης βίας τέτοιας που να μπορεί να νομιμοποιήσει την έναρξη μιας ένοπλης σύγκρουσης, εάν η νόμιμη χρήση τους, πάντα κατά το διεθνές δίκαιο, επιτρέπεται μόνον κατά την εμπόλεμη περίοδο, εάν ο κυβερνοπόλεμος αποτελεί μορφή βίας, ένοπλης βίας, είδος πολέμου ή απλώς μια νέα μορφή καταναγκασμού, όπως λ.χ. ο οικονομικός πόλεμος, οπότε η διεξαγωγή του κατά την ειρηνική περίοδο δεν είναι δυνατόν να πυροδοτήσει το άρθρο 2(4) του Καταστατικού Χάρτη του ΟΗΕ ή το άρθρο 5 της Συμφωνίας του ΝΑΤΟ, αποτελούν κεφαλαιώδους σημασίας παραμέτρους στην εκπόνηση αποτελεσματικής εθνικής στρατηγικής για τον κυβερνοχώρο. Παρά τη φαινομενική κινητικότητα της διεθνούς κοινότητας προς διευθέτηση των ανωτέρω και αντιστοίχων προβληματικών τα πλείστα εξ αυτών σχετιζόμενα με την προβολή κρατικής κυβερνοϊσχύος επί ετέρων κρατικών δρώντων παραμένουν ανοιχτά, διότι οι κύριοι δρώντες του διεθνούς συστήματος, εμφανίζονται από απρόθυμοι έως διστακτικοί να θεσπίσουν αυστηρά κανονιστικά όρια στον κυβερνοχώρο.

Στη συνέχεια παρουσιάζονται τρέχουσες θεσμικές αντιλήψεις των διεθνών δρώντων οι οποίες επιδρούν ή με οποιοδήποτε τρόπο συνδιαμορφώνουν την οικεία αντίληψη περί εθνικής κυβερνοϊσχύος και που ευθύνονται για το φαινόμενο θα μπορούσε να αποκληθεί ως "κυβερνοβαβέλ".

Ηνωμένες Πολιτείες Αμερικής

Οι ΗΠΑ, η μεγαλύτερη υπερδύναμη του πλανήτη, δεν εκφεύγουν του γενικού κανόνα της εννοιολογικής σύγχυσης, αφού πλήθος θεσμικών τους κειμένων συμβάλλουν στο διαμορφωθέν παγκοσμίως υφιστάμενο status quo. Ήδη από το 2003, στην "Εθνική Στρατηγική προς Εξασφάλιση του Κυβερνοχώρου" (The White House, 2003) υπάρχουν πλέον των 200 αναφορών στα δυνητικά αποτελέσματα των κυβερνοεπιθέσεων, χωρίς όμως να ορίζεται ποια ακριβώς πράξη συνιστά κυβερνοεπίθεση.

Στην "Εθνική Στρατιωτική Στρατηγική για τις Επιχειρήσεις στον Κυβερνοχώρο"[17] το 2006 διακηρύσσεται η αναγκαιότητα της απόκτησης και διατήρησης υπεροχής στον κυβερνοχώρο, έναντι των αντιπάλων, μέσω της ενοποίησης δικτυακής άμυνας, εκμετάλλευσης και επίθεσης (US/JCS, 2006, p. 8). Επιπροσθέτως, ορίζονται ως κυβερνοεπιθέσεις "οι επιχειρήσεις που σκοπό έχουν να αποδιοργανώσουν, αλλοιώσουν ή καταστρέψουν πληροφορίες οι οποίες βρίσκονται σε Η/Υ, δίκτυα Η/Υ ή τους ίδιους τους Η/Υ και τα δίκτυα" (US/JCS, 2006, p. G2). Ο ίδιος ορισμός κάνει την εμφάνιση του και στο Δόγμα Διακλαδικών Επιχειρήσεων το 2011 (US/JCS, 2011, p. III-26). Ο ορισμός όμως είναι προφανώς ελλιπής, αφού απουσιάζει κάθε έννοια τελολογικού κριτηρίου, με την ευρεία έννοια. Του σκοπού, με άλλα λόγια, διεξαγωγής μιας τέτοιας επίθεσης. Με αυτόν τον τρόπο μια γενικά αποδεκτή κλασικοποίηση σε κυβερνοεπιθέσεις και κυβερνοεγκλήματα καταρρέει σε μία και μοναδική κλάση, οπότε μοιραία η διεξαγωγή μιας στρατιωτικού τύπου επιχείρησης ταυτίζεται με μια κοινή κυβερνοαπάτη και το αντίστροφο.

Και σαν να μην ήταν ήδη αρκετά θολό το τοπίο, η "Εθνική Στρατηγική Ασφαλείας"[18] το 2010, η οποία αναγνωρίζει ως μια από τις προτεραιότητες της Εθνικής Ασφαλείας την προάσπιση από μεγάλης κλίμακας κυβερνοεπιθέσεις χωρίς φυσικά να ορίζει σαφώς ούτε τον ποιοτικό χαρακτηρισμό ούτε τον ίδιο τον όρο,

[17] Απόδοση ελληνιστί του λεκτικού "The National Military Strategy for Cyberspace Operations".

[18] Απόδοση ελληνιστί του λεκτικού "National Security Strategy".

εισάγει επιπροσθέτως τον όρο "κυβερνοεισβολή"[19], παραπέμποντας και σε αυτήν την περίπτωση σε διαισθητική ερμηνεία του όρου (The White House, 2010, p. 27).

Ακόμη δύο θεσμικά κείμενα, δημοσιευμένα το 2011, από τα οποία απουσιάζει οποιαδήποτε μνεία στον εννοιολογικό πυρήνα του προβλήματος είναι η "Διεθνής Στρατηγική για τον Κυβερνοχώρο" της Προεδρίας των ΗΠΑ και η "Στρατηγική για το Επιχειρείν στον Κυβερνοχώρο" του Υπουργείου Αμύνης των ΗΠΑ. Στο πρώτο απλά περιγράφεται αόριστα ως στόχος "…η δημιουργία διεθνούς περιβάλλοντος στο οποίο θα υφίστανται νόρμες υπεύθυνης συμπεριφοράς που θα καθοδηγούν τις κρατικές δράσεις, θα διατηρούν τις συνέργειες και θα υποστηρίζουν την επικράτηση του δικαίου στον κυβερνοχώρο" (The White House, 2011, p. 8). Στο δεύτερο ορίζεται ως μια από τις στρατηγικές πρωτοβουλίες η ενδυνάμωση της συλλογικής κυβερνοασφάλειας με τους διεθνείς εταίρους και συμμάχους των ΗΠΑ (US/Department of Defense [US/DoD], 2011, p. 9).

Στη συνέχεια το Διακλαδικό Δόγμα Επιχειρήσεων του 2013 εισάγει καινοφανή ταξινόμηση των στρατιωτικών επιχειρήσεων στον κυβερνοχώρο σε επιθετικές, αμυντικές και επιχειρήσεις διασφάλισης δικτύων του Υπουργείου Αμύνης, με τις επιθετικές επιχειρήσεις να αποσκοπούν "στην προβολή ισχύος μέσω επιβολής δύναμης εντός και διαμέσω του κυβερνοχώρου" (US/JCS, 2013, p. vii).

Στην "Εθνική Στρατηγική Ασφαλείας" του 2015 απουσιάζει κάθε προσπάθεια αποσαφήνισης του εννοιολογικού πλαισίου. Απλώς, με διαπιστωμένη την αδυναμία επιβολής του διεθνούς δικαίου, διατυπώνεται η ανάγκη δημιουργίας νομοθετικού πλαισίου σε επίπεδο τοπικού δικαίου. Με αυτόν τον τρόπο αναμένεται η θέσπιση επιβολής κυρώσεων σε κυβερνοδρώντες, που θα περιλαμβάνει έως και την προσαγωγή τους στις αμερικανικές δικαστικές αίθουσες, στην περίπτωση ενάσκησης παράνομης δραστηριότητας (The White House, 2015, p. 13). Φυσικά η λύση αυτή περιορίζεται σε καταλογισμό ποινικής ευθύνης σε μη κρατικούς δρώντες, καθ’ όσον προφανώς είναι αδύνατον να διαχειριστεί την περίπτωση διεξαγωγής ΕΕΚ από έτερο κρατικό δρώντα.

Στην "Εθνική Στρατηγική Ασφαλείας" του 2017 επισημαίνεται γενικά ότι οι κυβερνοεπιθέσεις υπονομεύουν την πίστη, την εμπιστοσύνη στους δημοκρατικούς

[19] Απόδοση ελληνιστί του όρου "cyber intrusion".

θεσμούς και στο παγκόσμιο οικονομικό σύστημα (The White House, 2017, p. 31), ότι η Ρωσία διεξάγει πληροφοριακές επιχειρήσεις επηρεασμού κοινής γνώμης παγκοσμίως (The White House, 2017, p. 35) και ότι οι ΗΠΑ θα αποτρέψουν, αμυνθούν και όταν παραστεί αναγκαίο θα κατανικήσουν τους κακόβουλους δρώντες του κυβερνοχώρου εξετάζοντας τις επιλογές τους κατά περίπτωση (The White House, 2017, pp. 31-32), υπονοώντας ευέλικτη ανταπόδοση ακόμη και με μέσα εκτός κυβερνοχώρου. Δεν αποτελεί έκπληξη η αναγόρευση κάθε κυβερνοπεριστατικού ως κυβερνοεπίθεση (The White House, 2017, p. 12), ενώ απευθύνεται και μια γενική προειδοποίηση για άμεσες και δαπανηρές συνέπειες προς τους κρατικούς δρώντες που διεξάγουν κυβερνοεπιθέσεις έναντι των ΗΠΑ (The White House, 2017, p. 13).

Ούτε το τρέχον Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου αντιμετωπίζει με ενάργεια το φαινόμενο. Αντιθέτως, εισάγει νεολογισμούς, επίθεση κυβερνοχώρου αντί κυβερνοεπίθεση, εκμετάλλευση κυβερνοχώρου αντί κυβερνοεκμετάλλευση κοκ, αποφεύγοντας κάθε μνεία σε κυβερνοπόλεμο ή στο κυβερνομάχεσθαι (US/JCS, 2018a, p. GL4). Επισημαίνει ότι το ΥΠΑΜ διενεργεί επιχειρήσεις κυβερνοχώρου οι οποίες συμμορφώνονται μεν με το εθνικό δίκαιο και το διεθνές δίκαιο, αλλά και τις εκάστοτε πολιτικές δε (US/JCS, 2018, pp. xiv, III-11). Έτερη πρωτοτυπία του είναι ο "χρωματισμός" του παγκόσμιου κυβερνοχώρου[20] με τις Ένοπλες Δυνάμεις να οφείλουν να υπερασπισθούν τον "εθνικό" κυβερνοχώρο, αλλά να δύνανται να επιχειρούν και εκτός αυτού ως στον λοιπό κυβερνοχώρο να μην υφίσταται η αρχή της εθνικής κυριαρχίας. Οπότε, ορίζει πως όταν δυνάμεις των ΗΠΑ διενεργούν κυβερνοεπιχειρήσεις εκτός οικείων δικτύων, μετά από εξουσιοδότηση, γενικά θα περιορίζονται στον γκρι και στον κόκκινο κυβερνοχώρο, εκτός εάν ενεργοποιηθούν άλλοι κανόνες εμπλοκής (US/JCS, 2018, pp. xiv, III-11).

Το 2018 ο Λευκός Οίκος εκδίδει την "Εθνική Κυβερνοστρατηγική των ΗΠΑ", σε συνέχεια της "Εθνικής Στρατηγικής Ασφαλείας", επισημαίνοντας τη σημασία της κυβερνοϊσχύος στη διαμόρφωση της εθνικής στρατηγικής. Σύμφωνα με αυτήν η εθνική κυβερνοστρατηγική εδράζεται σε τέσσερις πυλώνες και συγκεκριμένα στην

[20] Ο κυβερνοχώρος, πλέον του εθνικού, χαρακτηρίζεται αμφιμονοσήμαντα με έναν εκ των τριών χρωματισμών: μπλε, κόκκινο και γκρι. Πιο συγκεκριμένα, στο συμμαχικό κυβερνοχώρο ανατίθεται ο μπλε χρωματισμός, στον εχθρικό ο κόκκινος και στον υπόλοιποι ο γκρι.

προστασία των ανθρώπων και του αμερικανικού τρόπου ζωής, την προώθηση της αμερικανικής ευημερίας, τη διατήρηση της ειρήνης μέσω ενδυνάμωσης της κυβερνοϊσχύος και την προαγωγή της αμερικανικής επιρροής. Για πρώτη φορά, σε θεσμικό κείμενο στρατηγικού επιπέδου, οι ΗΠΑ δηλώνουν ότι θα προωθήσουν ένα πλαίσιο καθορισμού συνόλου κανόνων μη δεσμευτικών και σε εθελοντική βάση, εν καιρώ ειρήνης και επί τη βάσει του διεθνούς δικαίου, περί υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο, προς απομείωση του κινδύνου σύγκρουσης ένεκα κακόβουλης χρήσης του κυβερνοχώρου (The White House, 2018, p. 20). Κατά τα λοιπά και πολύ "βολικά" αποφεύγεται οιαδήποτε μνεία σε όρους κυβερνοεπίθεση, κυβερνοπόλεμος κτλ.

Τέλος, και η τρέχουσα "Εθνική Στρατηγική Ασφαλείας" του 2022 ακολουθεί πιστά την πεπατημένη αποφεύγοντας να διακρίνει ταξινομία των κυβερνοπεριστατικών, συνεπώς κάθε συμβάν στον κυβερνοχώρο εξακολουθεί θα αντιμετωπίζεται ως κυβερνοεπίθεση (The White House, 2022, p. 34). Ο κυβερνοχώρος πλέον θεωρείται ως στρατιωτικό πεδίο αντιπαράθεσης (The White House, 2022, p. 22), σε απόλυτη ισοτιμία με τέσσερα άλλα γεωγραφικά πεδία. Ρωσία και Κίνα ονοματίζονται ως επικίνδυνοι ανταγωνιστές, με την Κίνα να διαθέτει τόσο τους απαραίτητους συντελεστές ισχύος όσο και την πρόθεση για την αναμόρφωση της παγκόσμιας τάξης (The White House, 2022, p. 23), ενώ καταγράφεται ρητά πως η Ρωσία διεξάγει κυβερνοεπιθέσεις εναντίων των εθνικών δικτύων κρισίμων υποδομών (The White House, 2022, p. 32). Επιβεβαιώνεται η βούληση, που διατυπώθηκε επί Προεδρίας Trump, περί τήρησης νόρμας υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο, στο πλαίσιο του ΟΗΕ όμως αυτή τη φορά, και με την επισήμανση ανεπιφύλακτης, χωρίς αστερίσκους, αναγνώρισης της εφαρμοσιμότητας του διεθνούς δικαίου στον κυβερνοχώρο (The White House, 2022, p. 34).

Εν κατακλείδι, η τρέχουσα θεσμική οπτική των ΗΠΑ περί κυβερνοϊσχύος δύναται να συνοψισθεί ως εξής:

- Η τεχνολογία διαδραματίζει κεντρικό ρόλο στον γεωπολιτικό ανταγωνισμό και στο μέλλον της εθνικής ασφάλειας, οικονομίας και δημοκρατίας.

- Ρωσία και Κίνα ονοματίζονται ως επικίνδυνοι ανταγωνιστές, με την Κίνα να διαθέτει τόσο τους απαραίτητους συντελεστές ισχύος όσο και την πρόθεση για την αναμόρφωση της παγκόσμιας τάξης.
- Αποτυγχάνει να οριοθετήσει διαχωριστικές γραμμές μεταξύ μορφών προβολής κυβερνοϊσχύος (κυβερνοεπίθεσης, κυβερνοεγκλήματος, κυβερνοεκμετάλλευσης κοκ) και πηγών προέλευσης (κρατικών και μη δρώντων), με τον όρο κυβερνοεπίθεση να είναι επικίνδυνα υπερπεριληπτικός[21].
- Δεν υφίσταται καν μνεία στους όρους κυβερνοπόλεμος και κυβερνομάχεσθαι.
- Στα ύψιστα θεσμικά κείμενα δεν ορίζονται τυπικά μεν χρησιμοποιούνται όμως άφοβα δε, με τη διαισθητική τους προφανώς έννοια, οι όροι κυβερνοχώρος και κυβερνοεπιχειρήσεις.
- Διατυπώνεται η βούληση περί τήρησης νόρμας υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο.
- Αναγνωρίζεται η εφαρμοσιμότητα του διεθνούς δικαίου κατά την προβολή κυβερνοϊσχύος στον κυβερνοχώρο.

ΝΑΤΟ

Με δεδομένη τη θεσμική οπτική των ΗΠΑ δεν αποτελεί έκπληξη το γεγονός ότι το ΝΑΤΟ, χωρίς να ταυτίζεται, δεν αποκλίνει αισθητά από αυτήν, οπότε μοιραία εμφανίζει τις ίδιες αδυναμίες. Πρέπει να σημειωθεί όμως ότι δεν υπάρχει ολοκληρωμένη ενιαία δεσμευτική θεώρηση για τα κράτη μέλη της Συμμαχίας, πχ μια Συμφωνία Τυποποίησης.

[21] Ο τρέχων ορισμός της κυβερνοεπίθεσης είναι: "η εισχώρηση σε Η/Υ που έχει ως αποτέλεσμα την υποβάθμιση, άρνηση ή καταστροφή της πληροφορίας ή του Η/Υ" (US Army/Cyber Command, 2022). Ένας τέτοιος ορισμός στον οποίο απουσιάζει κάθε έννοια τελολογικού κριτηρίου αναβιβάζει ακόμη και τα κοινά κυβερνοεγκλήματα στο επίπεδο της κυβερνοεπίθεσης και της απειλής για την Εθνική Ασφάλεια.

Εν πάσει περιπτώσει, ως σημαντικοί σταθμοί στη θεσμική οπτική του ΝΑΤΟ θεωρούνται η αναγνώριση του κυβερνοχώρου ως πεδίου επιχειρήσεων κατά την έννοια της ξηράς, του αέρα και της θάλασσας στη Σύνοδο Κορυφής στη Βαρσοβία το 2016[22], με ό,τι αυτό συνεπάγεται, και η υπογραφή το ίδιο έτος της Τεχνικής Συμφωνίας Κυβερνοάμυνας μεταξύ ΝΑΤΟ και ΕΕ με σκοπό την εμβάθυνση στη μεταξύ τους συνεργασία, εκπαίδευση και έρευνα (NATO, 2022a). Είχε βεβαίως προηγηθεί στη Σύνοδο Κορυφής της Ουαλίας το 2014 η θεμελιώδης αναγνώριση ότι ο κυβερνοχώρος αποτελεί πεδίο εφαρμογής του διεθνούς δικαίου, συμπεριλαμβανομένων του Διεθνούς Ανθρωπιστικού Δικαίου και του Καταστατικού Χάρτη του ΟΗΕ[23]. Η εφαρμοσιμότητα του διεθνούς δικαίου στον κυβερνοχώρο επανεπιβεβαιώθη και στο κείμενο "NATO 2022 Strategic Concept", της πρόσφατης Συνόδου Κορυφής το 2022 στη Μαδρίτη (NATO, 2022b, para. 25).

Τέλος, αξίζει μνείας η ύπαρξη του ΝΑΤΟϊκού Κέντρου Αριστείας στο Ταλίν της Εσθονίας[24] το οποίο εκπονεί μη δεσμευτικές για τα κράτη μέλη δημοσιεύσεις, οι οποίες μεταξύ άλλων πραγματεύονται και την εφαρμοσιμότητα του διεθνούς δικαίου στον κυβερνοχώρο[25].

[22] Το ακριβές λεκτικό προσθήκης του κυβερνοχώρου στα λοιπά φυσικά πεδία επιχειρήσεων, με το οποίο δύναται να πυροδοτηθούν τα οικεία άρθρα του Συμφώνου περί συλλογικής άμυνας, ήταν το εξής: "Τώρα, στη Βαρσοβία, επιβεβαιώνουμε την αμυντική εντολή [mandate] του ΝΑΤΟ και αναγνωρίζουμε τον κυβερνοχώρο ως πεδίο επιχειρήσεων στο οποίο το ΝΑΤΟ πρέπει να αμυνθεί τόσο αποτελεσματικά όσο αμύνεται και στον αέρα, στη ξηρά και στη θάλασσα" (NATO/Warsaw Summit, 2016, para. 70).

[23] "Η πολιτική μας αναγνωρίζει επίσης ότι το διεθνές δίκαιο, συμπεριλαμβανομένου του Διεθνούς Ανθρωπιστικού Δικαίου και του Χάρτη του ΟΗΕ, εφαρμόζεται στον κυβερνοχώρο" NATO/Wales Summit, 2014, para. 72).

[24] Τυπικά: "NATO Cooperative Cyber Defence Centre of Excellence" [NATO CCDCOE].

[25] Κορωνίδα της όλης προσπάθειας εφαρμοσιμότητας του ΔΔ lex lata, καίτοι συνιστά ίσως ανυπέρβλητη πρόκληση η διαπραγμάτευση νέων εννοιών με χρήση παλαιών όρων, αποτελεί η έκδοση δύο εγχειριδίων γνωστών στη νομική κοινότητα ως Tallinn I και II, (Schmitt, 2013, p. 19; Schmitt, 2017, p. 3).

Συμβούλιο της Ευρώπης

Το Συμβούλιο της Ευρώπης[26], μέλος του οποίου είναι και η Ελλάς, έχει υιοθετήσει μια πιο πρακτική θεσμική οπτική. Αντιλαμβανόμενο εγκαίρως αφενός το μέγεθος του προβλήματος και αφετέρου το πεπερασμένο των θεσμικών του δυνατοτήτων, προτίμησε την επιλογή άσκησης μιας συγκεκριμένου εύρους, αλλά αποδοτικής κυβερνοπολιτικής, από τη διατύπωση μιας υπερφιλόδοξης διακρατικής στρατηγικής κυβερνοχώρου. Χάραξε από πολύ νωρίς μια πρωτοποριακή, για την εποχή της, πολιτική ασφαλείας, ασφυκτικά εγκλωβισμένης όμως, στο περιοριστικό πλαίσιο αντιμετώπισης των κυβερνοεγκλημάτων.

Πράγματι από το 2001 στο Συνέδριο της Βουδαπέστης το Συμβούλιο της Ευρώπης εξέδωσε τη "Σύμβαση για το Κυβερνοέγκλημα"[27], γνωστή και ως "Σύμβαση της Βουδαπέστης"[28]. Η Συνθήκη ορίζει τα ποινικώς κολάσιμα αδικήματα[29] από το εκάστοτε εθνικό ποινικό δίκαιο, τα οποία δύνανται να διαπραχθούν με τη χρήση υπολογιστικών συστημάτων και μέσω του διαδικτύου και τα οποία δύνανται να προκαλέσουν ζημία σε ιδιώτες και επιχειρήσεις, όχι τις επιθέσεις που δύνανται να διεξαχθούν στα υπολογιστικά συστήματα, δηλαδή ορίζει το κυβερνοέγκλημα (Council of Europe, 2001, p. 4). Αποφεύγει με αυτόν τον τρόπο πολύ βολικά τη μνεία σε κρατικούς δρώντες, οι οποίοι εν τέλει είναι οι αυτουργοί τέλεσης των κυβερνοεπιθέσεων ή του κυβερνοπόλεμου.

[26] Το Συμβούλιο της Ευρώπης (Council of Europe), ο παλαιότερος Οργανισμός με όραμα την ενοποίηση της Ευρώπης, είναι Διεθνής διακυβερνητικός Οργανισμός με έτος ίδρυσης το 1949, στο οποίο μετέχουν 47 ευρωπαϊκά κράτη. Δεν θα πρέπει να συγχέεται με το Ευρωπαϊκό Συμβούλιο (European Council) ούτε με το Συμβούλιο της ΕΕ (Council of the European Union), τα οποία αποτελούν όργανα της Ευρωπαϊκής Ένωσης.

[27] Απόδοση ελληνιστί του όρου "Convention on Cybercrime".

[28] Μεταξύ των κρατών τα οποία έχουν επικυρώσει τη Συνθήκη προηγούμενα της Ελλάδος είναι και η Τουρκία, την 29/9/2014 με ημερομηνία έναρξης εφαρμογής την 1/1/2015. (Council of Europe, 2014).

[29] Απόδοση ελληνιστί του όρου "offences".

Ευρωπαϊκή Ένωση

Σε ό,τι αφορά την ΕΕ αυτή, ως μια κατ' εξοχήν οικονομική - πολιτική ένωση ανεξαρτήτων κρατών μελών, τηρεί μια μάλλον αποστασιοποιημένη θεώρηση των πραγμάτων, προσανατολισμένη πρωτευόντως στην εμπέδωση πολιτικών κυβερνοασφάλειας. Το 2008 εκδίδεται η Κοινοτική Οδηγία 2008/114/ΕΚ[30], σχετικά με την αξιολόγηση και προστασία των ευρωπαϊκών υποδομών ζωτικής σημασίας (ΕΥΖΣ), που όμως "επικεντρώνεται στους τομείς ενέργειας και μεταφορών" και στην οποία ορίζεται ρητά ότι "η πρωταρχική και ύπατη ευθύνη για την προστασία των ΕΥΖΣ ανήκει στα κράτη μέλη και στους κύριους/διαχειριστές των υποδομών αυτών" (ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης, 2008, σ. L 345/75).

Το 2013 εκδίδει τη "Στρατηγική της ΕΕ για την Ασφάλεια στον Κυβερνοχώρο"[31]. Στο υπόψιν θεσμικό κείμενο διατυπώνεται εμφατικά ότι η υπόψη στρατηγική "αποσαφηνίζει τις αρχές που πρέπει να καθοδηγούν την πολιτική ασφαλείας στον κυβερνοχώρο εντός της ΕΕ αλλά και διεθνώς" (ΕΕ/Ευρωπαϊκή Επιτροπή, 2013, σ. 4) και ορίζεται ότι "σε περίπτωση επέκτασης ενόπλων συγκρούσεων στον κυβερνοχώρο, εφαρμόζονται το Διεθνές Ανθρωπιστικό Δίκαιο, και κατά περίπτωση, τα νομικά μέσα του δικαίου των ανθρωπίνων δικαιωμάτων" (ΕΕ/Ευρωπαϊκή Επιτροπή, 2013, σ. 19). Επιπροσθέτως, ξεκαθαρίζει ρητώς ότι:

> εάν το συμβάν φαίνεται να συνδέεται με ηλεκτρονική κατασκοπεία ή κρατικά υποστηριζόμενη επίθεση ή ότι έχει επιπτώσεις στην εθνική ασφάλεια, οι εθνικές αρχές ασφαλείας και άμυνας θα κινητοποιήσουν τους εκάστοτε ομολόγους τους, έτσι ώστε να ενημερωθούν πως υφίστανται επίθεση και εάν είναι σε θέση να αμυνθούν (ΕΕ/Ευρωπαϊκή Επιτροπή, 2013, σ. 23),

με άλλα λόγια η ευθύνη διαχείρισης των κυβερνοπεριστατικών βαραίνει τα κράτη μέλη, τα οποία όμως προτρέπονται για συνεργασία.

Το 2016 η ΕΕ εμφανίζεται να προσπαθεί να εμπλουτίσει το πεδίο των πολιτικών κυβερνοασφαλείας αναγνωρίζοντας την ύπαρξη υβριδικών απειλών, "που

[30] Η Οδηγία ενσωματώθηκε στο ελληνικό δίκαιο ως Προεδρικό Διάταγμα υπ' αριθμ. 39 το 2011.

[31] Απόδοση ελληνιστί από την ίδια την ΕΕ του όρου "Cybersecurity Strategy of the European Union".

επιδιώκουν να εκμεταλλευτούν τα τρωτά στοιχεία μιας χώρας και συχνά επιδιώκουν να υπονομεύσουν τις θεμελιώδεις δημοκρατικές αξίες και ελευθερίες", και με ζητούμενο όχι φυσικά την ενίσχυση της εθνικής άμυνας των κρατών-μελών, ή έστω πιο απροσωποποιημένα της ευρωπαϊκής άμυνας, αλλά "...τη βελτίωση της ανθεκτικότητας των συστημάτων επικοινωνιών και πληροφοριών... για την υποστήριξη της ψηφιακής ενιαίας αγοράς" (ΕΕ/Ευρωπαϊκή Επιτροπή, 2016, σ. 4). Για τη σωστή αντίληψη της κατάστασης και την αξιολόγηση κινδύνων εκδηλώνει ενέργειες αντίδρασης και, μεταξύ άλλων, συμπράττει με το ΝΑΤΟ στην ίδρυση ενός Κέντρου Αριστείας (Hybrid CoE) στο Ελσίνκι της Φινλανδίας. Και σ' αυτήν την περίπτωση όμως δεν υφίσταται ουδεμία αναφορά σε κυβερνοπόλεμο, ο όρος επίθεση στον κυβερνοχώρο χρησιμοποιείται υπερπεριληπτικά, προκειμένου να συμπεριλάβει το οργανωμένο έγκλημα, την τρομοκρατία από μη κρατικούς δρώντες κτλ, ενώ ως είθισται για άλλη μια φορά προτρέπει τα μέλη κράτη σε συνεργασία στην περίπτωση εμφάνισης περιστατικού, σε εθελοντική πάντως βάση (ΕΕ/Ευρωπαϊκή Επιτροπή, 2016, σ. 12).

Τέλος, το 2018 στην επικαιροποίηση του "Πλαισίου Πολιτικής Κυβερνοάμυνας της ΕΕ" αναγνωρίζεται ο κυβερνοχώρος ως το πέμπτο πεδίο επιχειρήσεων (ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης, 2018, σ. 4), ενώ στο κείμενο "Μια Στρατηγική Πυξίδα για την Ασφάλεια και την Άμυνα" το 2022 απλώς αναγνωρίζεται η ανάγκη ανάπτυξης "στάσης της Ένωσης στον κυβερνοχώρο"[32] για την αντιμετώπιση των κυβερνοεπιθέσεων (ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022, σ. 23). Τα λοιπά θεσμικά κείμενα της ΕΕ, που κατά καιρούς έχουν εκδοθεί, είτε ως εσωτερικές κανονιστικές οδηγίες είτε ως Κοινοτικές Οδηγίες, αναλίσκονται σε πολιτικές ασφαλείας και αποφεύγουν επιδέξια κάθε εμπλοκή με έννοιες όπως ο κυβερνοπόλεμος ή οι κυβερνοεπιθέσεις.

ΟΗΕ

[32] Απόδοση ελληνιστί από την ίδια την ΕΕ του όρου "cyber posture".

Ο ΟΗΕ ενέταξε στην ατζέντα του το θέμα υπό το πρίσμα της "ασφάλειας πληροφοριών"[33], ήδη από το μακρινό 1998, κατόπιν πρότασης της Ρωσικής Ομοσπονδίας[34]. Από το 2004 έως σήμερα έχουν συσταθεί έξι ομάδες Κυβερνητικών Ειδικών που μελετούν τις απειλές στο πλαίσιο της διεθνούς ασφαλείας με ευκταίο στόχο την εμπέδωση νορμών υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο. Η πρόοδος είναι αθροιστική και οι αναφορές 4 ομάδων έχουν γίνει αποδεκτές από όλα τα κράτη μέλη του Οργανισμού.[35]

Στην τελευταία αναφορά τα κράτη προτρέπονται να συνεχίσουν τον διάλογο, για επαύξηση της αμοιβαίας κατανόησης, αποφυγή παρανοήσεων, υιοθέτηση υπεύθυνης συμπεριφοράς και περαιτέρω ανταλλαγή απόψεων για τον τρόπο εφαρμογής του διεθνούς δικαίου. Τέλος, με Ψήφισμά της η ΓΣ/ΟΗΕ το 2020 (UN/GA, 2020) δημιούργησε μια νέα 5ετή Ομάδα Εργασίας για θέματα ασφαλείας από και στη χρήση τεχνολογιών πληροφοριών και επικοινωνίας[36].

Ελλάδα

Η Ελλάς παρά το μικρό αποτύπωμα ισχύος της, συγκρινόμενη με τους παγκόσμιους δρώντες, και παρά την υπερδεκαετή πλέον ενσκύψασα εν έτει 2010 οικονομική κρίση, εμφανίζει θεσμική, κατ' ελάχιστον, κινητικότητα. Κατά τα έτη 2013 και 2014 μέσω του ΓΕΕΘΑ, και συγκεκριμένα μέσω της Διεύθυνσης Διακλαδικού Δόγματος και της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ [νυν ΓΕΕΘΑ/Ε5 (ΔΙΚΥΒ)], εκπονεί το "Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου" (ΓΕΕΘΑ/ΔΔΔ, 2013), το "Κατευθυντήριο Πλαίσιο Ανάπτυξης Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2013), το "Τεχνικό Σχέδιο Δράσης για την Ανάπτυξη Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2014b) και την "Πολιτική Κυβερνοάμυνας στις ΕΔ" (ΓΕΕΘΑ/ΔΙΚΥΒ, 2014a) που

[33] Απόδοση ελληνιστί του όρου "information security".

[34] Η πρόταση υιοθετήθηκε από τη ΓΣ άνευ ψήφου (UN/GA, 1998).

[35] Οι τέσσερις (4) αναφορές οι οποίες έχουν γίνει δεκτές είναι οι: 2009-2011 A/65/201, 2012-2013 A/68/98, 2014-2015-A/70/174 και 2019-2021-A/76/174 (UN/Office for Disarmament Affairs, n.d.)

[36] Πιο συγκεκριμένα η Ομάδα Εργασίας είναι τύπου Open Ended WorkGroup (OEWG).

απετέλεσαν συνδυαστικά τον πρώτο οδικό χάρτη για την ανάπτυξη εθνικής στρατηγικής για τον κυβερνοχώρο και επιχειρησιακό οδηγό για τις ελληνικές ΕΔ. Είχε προηγηθεί βεβαίως από το 2003 το νομικό πλαίσιο το οποίο καθόριζε ως Τεχνικής Φύσεως Αρχή Ασφαλείας Πληροφοριών (INFOSEC) αρμόδια Διεύθυνση της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ) (ΠΔ 325, 2003)[37].

Το 2015 εκδίδεται από το ΥΠΕΘΑ η τρέχουσα "Λευκή Βίβλος" η οποία ορίζει ρητά ότι ο κυβερνοπόλεμος αποτελεί μια εκ των "κυρίων απειλών υπονόμευσης της ασφάλειας της χώρας" (ΥΠΕΘΑ, 2015, σ. 134), καθώς "κυβερνοπόλεμος και κυβερνοεπιθέσεις συνιστούν πράγματι απειλή για την εθνική ακεραιότητα και την ευημερία μιας χώρας και ως τέτοιες πρέπει να αντιμετωπίζονται" (ΥΠΕΘΑ, 2015, σ. 30). Επιπλέον, στο ίδιο θεσμικό κείμενο αναφέρεται πως ένας από τους επιχειρησιακούς τομείς στους οποίους εστιάζει το ΥΠΕΘΑ, δεδομένων των απειλών στη ΝΑ Μεσόγειο, είναι "η επαύξηση των δυνατοτήτων… στον κυβερνοχώρο" (ΥΠΕΘΑ, 2015, σ. 42). Υπό το πρίσμα αυτής της θεώρησης δεν προξενεί έκπληξη το γεγονός ότι το ΥΠΕΘΑ, μέσω της Εθνικής Αμυντικής Βιομηχανικής Στρατηγικής, όρισε ως έναν από τους τομείς σύγκλισης των ερευνητικών δραστηριοτήτων τις τεχνολογίες κυβερνοάμυνας και κυβερνοεπίθεσης (ΥΠΕΘΑ, 2015, σ. 100).

Παρά ταύτα αναφύονται στο υφιστάμενο θεσμικό πλαίσιο και για τις επιχειρήσεις στον κυβερνοχώρο δύο τουλάχιστον σημεία, τα οποία χρήζουν ιδιαίτερης μνείας. Πρώτα από όλα, σε εννοιολογικό επίπεδο πραγματοποιείται σημασιολογικό άλμα με την ταύτιση του όρου επιθετική επιχείρηση στον κυβερνοχώρο με τον όρο κυβερνοεπίθεση[38] (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 3-1), τη στιγμή που διεθνώς αναγνωρίζονται τουλάχιστον άλλες δύο διακριτές μορφές επιθετικών επιχειρήσεων, η κυβερνοεκμετάλλευση, με πιο αναγνωρίσιμη μορφή της την

[37] Η ίδια πρόνοια νόμου επαναδιατυπώθηκε και το έτος 2008 (Ν. 3649, 2008).

[38] Αγγλιστί οι όροι αποδίδονται ως "offensive cyberspace operation" (OCO) και "computer network attack" (CNA) αντίστοιχα.

κυβερνοκατασκοπεία, και η ενεργητική άμυνα[39]. Στην τελευταία βέβαια γίνεται αναφορά, χωρίς όμως να της προσδίδεται το ανάλογο εννοιολογικό περιεχόμενο στο πλήρες εύρος της, απλά ως προαπαιτούμενο αποτελεσματικής κυβερνοάμυνας και προς αντιμετώπιση των κυβερνοεπιθέσεων (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 4-3).

Το δεύτερο σημείο είναι ότι η προσπάθεια καθορισμού ευκρινών ορίων στον καθορισμό αρμοδιοτήτων στον κυβερνοπόλεμο καταλήγει σε λογικά παράδοξα, ακριβώς εξαιτίας της εννοιολογικής σύγχυσης. Πιο συγκεκριμένα, ο αρμόδιος εθνικός φορέας εμφανίζεται στα πλαίσια ανάθεσης ευθυνών και αρμοδιοτήτων που καθορίζονται στο οικείο Διακλαδικό Δόγμα να έχει ως βασική αποστολή τον σχεδιασμό, τη διεύθυνση και τη διεξαγωγή [συνολικά] των επιθετικών επιχειρήσεων κυβερνοχώρου (ΕΕΚ) (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 5-1). Στο ίδιο θεσμικό κείμενο ορίζεται ότι οι ΕΕΚ είναι "οι ενέργειες που αναλαμβάνονται με σκοπό την υπεροχή – έλεγχο του κυβερνοχώρου του αντιπάλου" (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 3-1). Ακόμα, ορίζεται ως ένας από τους σκοπούς των κυβερνοεπιθέσεων "η καταστροφή ενός δικτύου ή ενός συστήματος (ανεξάρτητα από το εάν είναι διασυνδεδεμένο ή όχι", με την απαίτηση όμως "οι επιθετικές επιχειρήσεις [να] βασίζονται στη χρήση της υπάρχουσας τεχνολογικής υποδομής (λογισμικό – υλικό) ως όπλο για την εκτέλεση μιας επίθεσης"[40] (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 3-1).

Συνεπώς, προκύπτει το λογικό παράδοξο του τύπου της επιχείρησης, λ.χ. μια επιχείρηση δολιοφθοράς με ΑΝΣΚ την ανατίναξη ενός πληροφοριακού συστήματος ή ο βομβαρδισμός με Μη Επανδρωμένα Αεροσκάφη (ΜΕΑ) ενός δικτύου οπτικών ινών, που πληρούν τις απαιτήσεις του ορισμού των ΕΕΚ ως επίσης και το σκοπό διεξαγωγής, αλλά παραβαίνουν την επιβληθείσα απαίτηση διεξαγωγής των επιχειρήσεων αποκλειστικά με χρήση όπλων (υλικού-λογισμικού), με γραμματική ερμηνεία των

[39] Αγγλιστί οι όροι αποδίδονται ως "cyber network exploitation" (CNE) και active defence, αντίστοιχα. Αν και στο ισχύον δόγμα η κυβερνοκατασκοπεία, αναφέρεται ως τρωτότητα του κυβερνοχώρου εκλείπει κάθε άλλη αναφορά σε αυτήν (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 4-3). Αντ' αυτής εισάγεται στο Κεφάλαιο 8, Ορισμοί-Ορολογία, ο όρος «παθητική επίθεση» (passive attack) ο οποίος ορίζει την παρακολούθηση/καταγραφή πληροφορίας χωρίς αλλαγή της κατάστασής της ως είδος επίθεσης (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 8-4).

[40] Το κατά πόσον νομικά δύνανται τα κυβερνοόπλα να θεωρούνται όντως όπλα και η χρήση τους να συνιστά πράξη ένοπλης βίας αποτελεί ανοικτό πρόβλημα της νομικής κοινότητας.

ορισμών να μη θεωρούνται σύμφωνα με το Δόγμα ως ΕΕΚ. Οπότε, ο αρμόδιος εθνικός φορέας να μην αναλαμβάνει το σχεδιασμό, τη διεύθυνση και τη διεξαγωγή της όλης επιχείρησης.

Όμως, μια εκ του αποτελέσματος προσέγγιση θεώρηση οδηγεί στο ακριβώς αντίθετο συμπέρασμα. Η επιβολή απαίτησης στη χρήση όπλου δεν αποτελεί κριτήριο του είδους της επίθεσης, διότι νομικά "τα χαρακτηριστικά εκείνα που καθιστούν όπλο ένα αντικείμενο, μια συσκευή ή ένα σύστημα δεν είναι τα εκ της κατασκευής ή κατά τον προορισμό χαρακτηριστικά του ή η συνήθης χρήση του, αλλά οι προθέσεις και οι επιδιώξεις με τις οποίες χρησιμοποιείται και τα αποτελέσματα της χρήσης αυτής"[41] (Μακρής, 2011, σ. 40). Υπό το πρίσμα αυτής της θεώρησης, επειδή η πρόθεση στο βομβαρδισμό με ΜΕΑ ενός δικτύου οπτικών ινών εμπίπτει στον ορισμό των ΕΕΚ αλλά και επειδή το αποτέλεσμα της χρήσης οδήγησε στην καταστροφή του δικτύου, δηλαδή στην εκπλήρωση του σκοπού εκδήλωσης μιας κυβερνοεπίθεσης, η όλη επιχείρηση βομβαρδισμού είναι σαφώς ΕΕΚ και το ίδιο το ΜΕΑ, για την υπόψη επιχείρηση, κυβερνοόπλο[42]. Τότε, όμως, από τον καθορισμό αρμοδιοτήτων, σύμφωνα με το Δόγμα, ο αρμόδιος εθνικός φορέας θα πρέπει να αναλάβει το σχεδιασμό, τη διεύθυνση και τη διεξαγωγή της όλης επιχείρησης!

Ο τελευταίος σημαντικός σταθμός στη διαμόρφωση της εθνικής θεσμικής αντίληψης περί κυβερνοχώρου είναι η έκδοση το 2020 της "Εθνικής Στρατηγικής Κυβερνοασφαλείας 2020-2025", με εκδούσα αρχή την Εθνική Αρχή Ασφαλείας, του Υπουργείου Ψηφιακής Διακυβέρνησης. Αν και η έκδοσή της σίγουρα αποτελεί θετικό και αναγκαίο βήμα προς τη σωστή κατεύθυνση, θα πρέπει να επισημανθεί ότι, όπως προκύπτει αβίαστα και από διατύπωση των αρχών και του οράματος της, αφορά αποκλειστικά σε πολιτικές ασφαλείας, καθόσον αποσκοπεί στην προστασία των πολιτών, δομών και φορέων ως και στην προστασία της ψηφιακής διακυβέρνησης και

[41] Αυτή είναι η νομική συλλογιστική, η ερμηνεία πρόκλησης ισοδυνάμου αποτελέσματος, με την οποία χαρακτηρίζεται λ.χ. μια ληστεία με μαχαίρι ως ένοπλη ληστεία. Το μαχαίρι, σε αυτήν την περίπτωση, δεν θεωρείται ως εργαλείο κοπής, αλλά ως όπλο, αφού ως τέτοιο χρησιμοποιήθηκε από τον θύτη προκειμένου να απειλήσει τη ζωή του θύματος.

[42] Αποτελεί οξύμωρο σχήμα το γεγονός ότι τα θεσμικά κείμενα υιοθετούν αυτή ακριβώς τη θεώρηση χαρακτηρίζοντας τις τεχνικές χρήσης λογισμικού και υλισμικού ως κυβερνοόπλα, αλλά την απορρίπτουν «δογματικά» στην υπόψη περίπτωση.

ευημερίας της χώρας (Υπουργείο Ψηφιακής Διακυβέρνησης/Εθνική Αρχή Κυβερνοασφαλείας, 2020, σσ. 22-23). Υπό αυτό το πρίσμα είναι αδύνατο να συλλάβει τις δομικές έννοιες για την εθνική άμυνα κυβερνοϊσχύς, κυβερνοπόλεμος[43] και στρατηγική για τον κυβερνοχώρο. Επιπροσθέτως, αν και ορίζει τους βασικούς εμπλεκόμενους εθνικούς φορείς και περιγράφει τα καθήκοντά τους δεν προσδιορίζει κάποιου είδους κάθετη δομή διοίκησης στη διαχείριση των κυβερνοπεριστατικών, οπότε αναμενόμενα θα ανακύψουν θέματα αναποτελεσματικής διαχείρισης. Εν κατακλείδι, η Ελλάς δεν εκφεύγει του κανόνα της εννοιολογικής σύγχυσης του Δυτικού κόσμου και επιπλέον θεσμικά καταγράφεται ως εκκρεμότητα η εκπόνηση της τόσο αναγκαίας Εθνικής Στρατηγικής για τον Κυβερνοχώρο.

Οργανισμός Συνεργασίας της Σαγκάης

Ο "Οργανισμός Συνεργασίας της Σαγκάης"[44] υιοθετεί μια εναλλακτική προσέγγιση, που απηχεί εν ολίγοις την οπτική των μειζόνων κρατικών δρώντων Κίνας και Ρωσίας. Στο πλαίσιο της εν ισχύι Συμφωνίας του Εκατερίνεμπουργκ το 2009 στο πεδίο της Διεθνούς Ασφαλείας Πληροφοριών, και πρακτικά επαναλαμβάνοντας τα συμφωνηθέντα σε αντίστοιχη Συμφωνία του 2008, αναγνωρίζονται στο προοίμιό της οι "απειλές που υφίστανται εξαιτίας της ασύμβατης χρήσης τεχνολογιών και μέσων ως προς τη διεθνή ασφάλεια και σταθερότητα τόσο σε πολιτικό, όσο και σε στρατιωτικό επίπεδο" (CIS Legislation, 2009). Ο Οργανισμός δεν χρησιμοποιεί

[43] Ενδεικτικά, ο κυβερνοπόλεμος στο πλαίσιο της υπόψιν Στρατηγικής θεωρείται μορφή του κυβερνοεγκλήματος, από κοινού με την κυβερνοτρομοκρατία και τις επιθέσεις άρνησης υπηρεσιών (DOS) (Υπουργείο Ψηφιακής Διακυβέρνησης/Εθνική Αρχή Κυβερνοασφαλείας, 2020, σ. 16).

[44] Αγγλιστί "Shanghai Cooperation Organisation" (SCO). Ο υπόψιν Οργανισμός ιδρύθηκε το έτος 2001 ως μετεξέλιξη του Shanghai Five, ο οποίος ιδρύθηκε το έτος 1996, με γενικότερο σκοπό την πολιτική, στρατιωτική και οικονομική συνεργασία μεταξύ των κρατών. Ιδιαιτέρως όμως εστιάζει σε θέματα περιφερειακής ασφαλείας και πιο συγκεκριμένα στη τριάδα περιφερειακή τρομοκρατία, εθνοτικό διαχωρισμό και θρησκευτικό εξτρεμισμό (UN/Political and Peacebuilding Affairs, n.d.) Περιλαμβάνει πλέον τα εξής οκτώ κράτη: Κίνα, Ρωσική Ομοσπονδία, Ινδία, Πακιστάν, Καζακστάν, Κιργιστάν, Τατζικιστάν και Ουζμπεκιστάν (Shanghai Cooperation Organisation, 2022).

καθόλου τους όρους ΕΕΚ, κυβερνοπόλεμος κτλ, αλλά ακολουθώντας μια διασταλτική συλλογιστική ταυτίζει τον κυβερνοπόλεμο με τον Πληροφοριακό Πόλεμο. Ο τελευταίος οριζόταν ήδη από την αντίστοιχη Συμφωνία του 2008 ως "η μαζική ψυχολογική πλύση εγκεφάλου με σκοπό την αποσταθεροποίηση κοινωνίας και κράτους, αλλά και πειθαναγκασμού λήψης αποφάσεων από το κράτος προς εξυπηρέτηση συμφερόντων αντίπαλου μέρους" (Hathway et al., 2012, p. 826). Επιπλέον, ο Οργανισμός αναγνωρίζει τη διάχυση της πληροφορίας ως επιβλαβή σε "κοινωνικοπολιτικές, κοινωνικοοικονομικές, πνευματικές, ηθικές και πολιτισμικές σφαίρες των ετέρων κρατών" και ως μια από τις πρωτεύουσες απειλές της πληροφοριακής ασφαλείας (Hathway et al., 2012, pp. 826-827).[45]

Η διαφορετικότητα στην οπτική μεταξύ Δυτικού Κόσμου και SCO είναι εμφανής. Η ερμηνεία της όμως είναι παραπάνω από προφανής, καθώς το παρελθόν ολοκληρωτισμού στις πρώην Σοβιετικές Δημοκρατίες, αλλά και το κομμουνιστικό παρόν της Κίνας, εκλαμβάνουν ως δυνητική απειλή υποσκαφής του υφιστάμενου πολιτικού καθεστώτος, το οποίο φυσικά αναγορεύεται ταυτόσημο με το εθνικό συμφέρον, κάθε νεωτερισμό ακόμα και εάν αυτός αφορά τεχνολογικά επιτεύγματα. Εξ ου και η εμφανής υπερμεγέθυνση των πιθανών συνεπειών του κυβερνοπολέμου και ο de jure αφορισμός του ως αποσταθεροποιητικού παράγοντα της κοινωνίας.

Βεβαίως, η ταύτιση οπτικής στο στρατηγικό επίπεδο, μεταξύ των μειζόνων δρώντων του Οργανισμού Κίνας και Ρωσικής Ομοσπονδίας, περί των δυνητικών απειλών κατά την προβολή κυβερνοϊσχύος στον κυβερνοχώρο, δεν θα πρέπει να παρερμηνευθεί ότι επεκτείνεται σε επιχειρησιακό και σε τακτικό επίπεδο, καθόσον πρόκειται για δύο εντελώς διαφορετικές στρατηγικές κουλτούρες. Επί παραδείγματι, στον κυβερνοπόλεμο[46] οι κλαουζεβιτσιανής κοσμοθεωρίας Ρώσοι επενδύουν πρωτευόντως στη τέχνη της χειραγώγησης με τη χρήση της αντίστροφης ψυχολογίας μέσω μη κρατικών δρώντων και με στόχο την επίτευξη συγκεκριμένου πολιτικού ΑΝΣΚ ή την ακύρωση της θεωρίας της νίκης του αντιπάλου, ενώ οι Κινέζοι επιχειρούν

[45] Η θεσμική αντίληψη η οποία διαπνέει τη Συμφωνία του Εκατερίνεμπουργκ επανεπιβεβαιώθη στη Σύσκεψη Κορυφής στην Ούφα τον Ιούλιο του 2015 αλλά και στη Συνάντηση Γραμματειών Εθνικών Συμβουλίων Ασφαλείας του SCO στο Πεκίνο τον Μάιο του 2018 (CCDCOE, 2023).

[46] Ο όρος χρησιμοποιείται διαισθητικά χωρίς οιαδήποτε τυπική νομική αυστηρότητα.

συνδυαστικά με την τριάδα: ψυχολογικές επιχειρήσεις, επιχειρήσεις επηρεασμού της κοινής γνώμης και νομικό πόλεμο (Cullen et al., 2021, pp. 18-22; Wirtz, 2015, pp. 36-37).

Πέραν όμως των κοινών συστημικών καταβολών του SCO δεν θα πρέπει να αγνοηθεί και η παράμετρος του μελλοντικού σχεδιασμού. Ίσως δεν θα πρέπει να αποκλειστεί και η πιθανότητα η ανωτέρω διατύπωση να μην αποτελεί τίποτε άλλο από ένα ιντερλούδιο στην επιβολή λογοκρισίας στο διαδίκτυο για τα κράτη του SCO. Άλλωστε δεν θα πρέπει να προκαλεί εντύπωση ότι "οι μείζονες κρατικοί δρώντες το πιθανότερο είναι να έχουν διαφορετικές οπτικές…καθώς αντιλαμβάνονται διαφορετικά σύνολα στρατηγικών κινδύνων και ευκαιριών" (Waxman, 2011, pp. 458-459). Παρά ταύτα, θα πρέπει να αναγνωρισθεί στη Ρωσική Ομοσπονδία το γεγονός, όπως ήδη προανεφέρθη ανωτέρω, πως πρώτη αυτή από το 1998 είχε θέσει στον ΟΗΕ το ζήτημα σύναψης διεθνούς ελέγχου των κυβερνοόπλων και είχε επισημάνει την ανάγκη θέσπισης κανονιστικού πλαισίου.

Εν τέλει, η υφιστάμενη οπτική του Οργανισμού Συνεργασίας της Σαγκάης περί προβολής κυβερνοϊσχύος, κυβερνοχώρου και κυβερνοπολέμου δύναται να συνοψισθεί ως εξής:

- Ο κυβερνοπόλεμος διασταλτικά ταυτίζεται με τον Πληροφοριακό Πόλεμο.
- Υιοθετεί προσέγγιση βασισμένη στο απώτερο σκοπό διεξαγωγής, όπου ως τέτοιος θεωρείται η αποσταθεροποίηση της κοινωνίας και του κράτους και η λήψη αποφάσεων αντίθετων στο εθνικό συμφέρον.
- Αποτυγχάνει να οριοθετήσει διαχωριστικές γραμμές μεταξύ των μορφών επιχειρήσεων του κυβερνοχώρου (κυβερνοεπίθεση, κυβερνοεκμετάλλευση κτλ).

Κεφάλαιο τρίτο
Το νομικό πλαίσιο της προβολής κυβερνοϊσχύος
κατά το jus ad bellum και το jus in bello

Γενικά

Η νομική προσπάθεια τιθάσευσης της προβολής κυβερνοϊσχύος στον κυβερνοχώρο, είτε αφορά σε ΕΕΚ είτε σε ενεργητική άμυνα, δια της απευθείας υπαγωγής lex lata στο εν ισχύι πλαίσιο διεθνούς δικαίου, τόσο για το δίκαιο προσφυγής στη βία (jus ad bellum) όσο και για το δίκαιο ενόπλων συρράξεων (jus in bello), παρουσιάζει ανυπέρβλητες δυσκολίες, εξαιτίας συνδυαστικά των suis generis χαρακτηριστικών κυβερνοϊσχύος και κυβερνοχώρου, με αποτέλεσμα να αποτελεί ακόμη ανοικτό

πεδίο.[47] Ιδιαίτερη πρόκληση συνιστά η διαχείριση των ΕΕΚ οι οποίες δεν επιφέρουν οι ίδιες κάποιο φυσικό αποτέλεσμα στον υλικό κόσμο, αλλά θα μπορούσαν να διευκολύνουν πολεμικές επιχειρήσεις κινητικού πολέμου όπως λ.χ. κυβερνοεπιθέσεις τύπου Διοίκησης και Ελέγχου[48]. Η πηγή του προβλήματος είναι απλό να εντοπισθεί, αλλά φαντάζει αδύνατο να υπερκερασθεί, το μοντέλο του διεθνούς δικαίου είναι βεστφαλιανό τη στιγμή που η κυβερνοτεχνολογία αμφισβητεί τα ίδια των κρατοκεντρικά θεμέλια του διεθνούς δικαίου (Kessler & Werner, 2013, p. 795).

Μέχρι σήμερα πάντως κανένας κρατικός δρων δεν έχει ισχυρισθεί ότι η προβολή κυβερνοϊσχύος στον κυβερνοχώρο δια της διενέργειας ΕΕΚ, και ακόμα ειδικότερα οι κυβερνοεπιθέσεις, συνιστούν "ένοπλη επίθεση", γεγονός το οποίο θα τους επέτρεπε να επικαλεστούν το δικαίωμα αυτοάμυνας όπως αυτό προσδιορίζεται σύμφωνα με το άρθρο 51 του Καταστατικού Χάρτη του ΟΗΕ. Αλλά ακόμη περισσότερο ούτε ποτέ κάποιο κράτος υποστήριξε ότι γενικά κάθε διεξαγωγή κυβερνοεπίθεσης συνιστά απαγορευμένη χρήση βίας (Hathway, 2012, p. 842; Schmitt, 2022), με μοναδική ίσως εξαίρεση την περίπτωση της Εσθονίας το 2007, που μετά τις αρχικές δηλώσεις περί ισοδύναμου αποτελέσματος με "ναυτικό

[47] Επί παραδείγματι, ποιο το εννοιολογικό περιεχόμενο του όρου "κρατική κυριαρχία" στον "κυβερνοχώρο" ενός κράτους; [Βλ. ενδεικτικά: (Tsagourias, 2020, p. 7)]. Ισχύει η έννοια της κρατικής κυριαρχίας και αντίστοιχα της κρατικής ευθύνης για την αποθήκευση δεδομένων στο "νέφος" και την "υπολογιστική στο νέφος"; Υπάρχει η έννοια απόδοσης ευθύνης Δκσης σε ημιαυτόνομο ή πλήρως αυτόνομο κυβερνοόπλο; κτλ [Βλ. ενδεικτικά (Buchan & Tsagourias, 2020, p. 673)]. Άλλωστε, ο ίδιος ο Καθηγητής Μ. Schmitt, η "ψυχή" του ΝΑΤΟϊκού CCDCOE στο Ταλίν, και υπέρμαχος στο ΝΑΤΟ της ερμηνείας του διεθνούς δικαίου lex lata είχε πραγματευτεί σε νομικό άρθρο του τις αντικειμενικές δυσκολίες εφαρμογής του δικαίου ενόπλων συρράξεων lex lata, και συγκεκριμένα για την αρχή της διάκρισης, της συμμετοχής στις εχθροπραξίες και των κυβερνοεπιχειρήσεων ως ένοπλη σύρραξη. Στο εν λόγω άρθρο κατέληγε ότι πραγματεύτηκε επιδερμικά χωρίς να επιλύει τρία εκ των πολλών υφισταμένων θεμάτων εφαρμογής του δικαίου ενόπλων συρράξεων στις κυβερνοεπιχειρήσεις (Schmitt, 2011, p. 106).

[48] Απόδοση ελληνιστί του όρου "Command and Control" (C2).

αποκλεισμό"[49] ανέκρουσε πρύμναν και περιόρισε τις αντιδράσεις της αποκλειστικά σε επικοινωνιακό επίπεδο.

Παρά ταύτα, υφίστανται ισχυρές ενδείξεις ότι οι ΕΕΚ παραβιάζουν το διεθνές δίκαιο (Hathway, 2012, p. 845), και αυτό διότι:

- Τα κράτη δεν εμπλέκονται ανοικτά, προφανώς για την αποφυγή ανάθεσης ευθύνης, επιλέγοντας την ασφαλέστερη οδό ανάθεσης του υπόψιν έργου σε διαμεσολαβητικούς δρώντες[50].
- Για κράτη που υπήρξαν θύματα τέτοιων επιθέσεων οι σύμμαχοι τους αποδοκίμασαν τις επιθέσεις με δημόσιες τοποθετήσεις.
- Το ΝΑΤΟ δημοσίως έχει ήδη αποδεχθεί την εφαρμοσιμότητα του διεθνούς δικαίου στον κυβερνοχώρο και έχει υποδείξει ότι η εκδήλωση κυβερνοεπίθεσης σε μέλος κράτος της Συμμαχίας δύναται να πυροδοτήσει το άρθρο 4[51], αφήνοντας υπονοούμενα ακόμη και για το άρθρου 5[52], του Καταστατικού Χάρτη του ΝΑΤΟ.

[49] Σύμφωνα με την Απόφαση 3314 του 1974 της ΓΣ του ΟΗΕ περί "Ορισμού της Επιθέσεως "στο άρθρο 3 (c) καθορίζεται ότι ο αποκλεισμός λιμένων και ακτών κράτους συνιστά εκδήλωση επίθεσης και εμπίπτει στις διατάξεις του άρθρου 2 του Χάρτη του Οργανισμού (UN/GA, 1974).

[50] Όπως τέθηκε πολύ εύστοχα: "το να ψεύδονται για τα πραγματικά γεγονότα…. είναι το τίμημα που πληρώνουν οι παραβατικές κυβερνήσεις για την παραβίαση των διεθνών τους υποχρεώσεων" (Franck, 2005, p. 73).

[51] Κατά τον Έλληνα κυρωτικό νομοθέτη: "τα Συμβαλλόμενα Μέρη θέλουσι συσκέπτεσθαι από κοινού οσάκις κατά τη γνώμη οιουδήποτε εξ αυτών, απειλείται η εδαφική ακεραιότης, πολιτική ανεξαρτησία ή ασφάλεια ενός οιουδήποτε των Μερών" (Ν. 1989, 1952, σ. 227).

[52] Κατά τον Έλληνα κυρωτικό νομοθέτη: "τα Συμβαλλόμενα Μέρη συμφωνούν ότι, ένοπλος επίθεσις εναντίον ενός ή πλειόνων εξ αυτών εν Ευρώπη ή Βορείω Αμερική, θέλει θεωρηθή ως επίθεσις εναντίον απάντων και, συνεπώς συμφωνούν ότι, εν περιπτώσει ταύτης ενόπλου επιθέσεως, έκαστον εξ αυτών, εν τη ασκήσει του άρθρου 51 του Χάρτου των Ηνωμένων Εθνών αναγνωριζομένου δικαιώματος της ατομικής ή συλλογικής αυτοαμύνης θα συνδράμη τα υφιστάμενα της επίθεση εν ή πλείονα Μέρη δια της αμέσου λήψεως, τόσο ατομικώς όσο και από του συμφώνου μετά των ετέρων Μερών, των μέτρων άτινα θεωρεί αναγκαία, περιλαμβανομένη της χρήσεως ενόπλου βίας, προς αποκατάστασιν και διατήρησιν της ασφαλείας της περιοχής του Βορείου Ατλαντικού"(Ν. 1989, 1952, σ. 227).

Προβολή κυβερνοϊσχύος κατά το jus ad bellum

Στο τρέχον υποκεφάλαιο εξετάζονται οι αρχές και οι παραδοχές οι οποίες διέπουν το δίκαιο προσφυγής στη βία (jus ad bellum) ως προς την προβολή κυβερνοϊσχύος στον κυβερνοχώρο. Αποδεικνύεται ότι το πεδίο παραμένει ακόμα ανοικτό, καθώς η τεχνολογική εξέλιξη ωθεί την ερμηνεία των υφιστάμενων νομικών εννοιών lex lata στα απώτατα όρια τους.

Το υπάρχον νομικό πλαίσιο, το οποίο ορίζει με περιοριστικό τρόπο το πότε και με ποιόν τρόπο εγείρεται το δικαίωμα αυτοάμυνας οριοθετείται, κατά φθίνουσα σειρά βαρύτητας[53], έχει ως εξής:

1. Καταστατικός Χάρτη του ΟΗΕ[54] και συγκεκριμένα:
    α. Το άρθρο 2(4)[55],
    β. Το άρθρο 39[56],

[53] Παράθεση επί τη βάσει του Καταστατικού του Διεθνούς Δικαστηρίου της Χάγης (International Court of Justice, ICJ) (ICJ, 2023, Article 38.1).

[54] Ο Καταστατικός Χάρτης του ΟΗΕ εισήχθη στο ελληνικό δίκαιο ως κυρωτικός αναγκαστικός νόμος (Α.Ν. 585, 1945).

[55] Κατά τον Έλληνα κυρωτικό νομοθέτη: "πάντα τα Μέλη θα απέχωσι εις τας διεθνείς αυτών σχέσεις της απειλής ή χρήσεως βίας κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οιουδήποτε κράτους ή καθ' οιονδήποτε άλλον τρόπον ασυμβίβαστον προς τους σκοπούς των Ηνωμένων Εθνών" (Α.Ν. 585, 1945, σ. 1213).

[56] Κατά τον Έλληνα κυρωτικό νομοθέτη: "το Συμβούλιον Ασφαλείας θα αποφαίνεται περί της υπάρξεως απειλής κατά της ειρήνη, ή επιθετικής πράξεως και θα προβαίνη εις συστάσεις ή θα αποφασίζη περί των ληπτέων μέτρων συμφώνως προς τα άρθρα 41 και 42 προς διατήρησιν ή αποκατάστασιν της διεθνούς ειρήνης και ασφαλείας"(Α.Ν. 585, 1945, σ. 1216).

γ. Το άρθρο 51[57]

2. Εθιμικός κανόνας jus cogens[58] απαγόρευσης χρήσης βίας ή απειλής χρήσης βίας.

3. Νόρμα εθιμικού Διεθνούς Δικαίου περί μη ανάμιξης στα εσωτερικά άλλων κρατών[59].

4. Διακηρύξεις του ΟΗΕ, ότι το άρθρο 2(4) αναφέρεται μόνον σε ένοπλη βία:

α. "Declaration of Friendly Relations" (UN/GA, 1970).

β. "Declaration of Non-Use of Force" (UN/GA, 1987).

5. Απόφαση του Διεθνούς Δικαστηρίου της Χάγης στην υπόθεση Nicaragua v. USA, στην οποία το Δικαστήριο στην παράγραφο 228 εμμέσως πλην σαφώς αναγνώρισε πως η ανάμιξη των ΗΠΑ, χρήση όπλου μη κινητικής ενεργείας (εν προκειμένω η παροχή εκπαίδευσης και εξοπλισμού στους Contras), δύναται να αξιολογηθεί ως απειλή ή χρήση βίας, οπότε να συνιστά παραβίαση του άρθρου 2(4) του ΟΗΕ (ICJ, 1986, p. 118).

---

[57] Κατά τον Έλληνα κυρωτικό νομοθέτη: "ουδέν εκ των διαλαμβανομένων εν τω παρόντι Χάρτη θα παρεμποδίζη το φυσικό δικαίωμα ατομικής νομίμου αμύνης εις περίπτωσιν καθ' ήν Μέλος τι των Ηνωμένων Εθνών υποστή έπίθεσιν ένοπλον, μέχρι ου το Συμβούλιον Ασφαλείας λάβη τα αναγκαία μέτρα προς διατήρησιν της διεθνούς ειρήνης και ασφαλείας. Τα υπό των Μελών λαμβανόμενα μέτρα, εν τη ασκήσει του δικαιώματος τούτου νομίμου αμύνης, θα αναφέρωνται αμέσως εις το Συμβούλιον Ασφαλείας και κατ' ουδέν θα θίγουν την εξουσίαν και την υποχρέωσιν του Συμβουλίου Ασφαλείας συμφώνως τω παρώντι Χάρτη όπως αναλάβη οποτεδήποτε οίαν δράσιν ήθελε κρίνει αναγκαίαν προς διατήρησιν ή αποκατάστασιν της διεθνούς ειρήνης και ασφαλείας"(Α.Ν. 585, 1945, σ. 1217). Επισημαίνεται ότι η διατύπωση περί «νομίμου αμύνης» έλκει προφανώς την προέλευση της από την έκδοση του κειμένου στη γαλλική γλώσσα (legitime defence), ενώ στην αγγλική έκδοση αναφέρεται ως «αυτοάμυνα» (selfdefence). Συνεπώς, και οι δύο όροι όπου χρησιμοποιούνται στην συνέχεια θεωρούνται ως ταυτόσημοι.

[58] Το jus cogens (αναγκαστικό δίκαιο) δεσμεύει κάθε κράτος ανεξάρτητα από το εάν είναι μέλος του ΟΗΕ.

[59] Η υπόψη νόρμα έχει ληφθεί υπόψη και στον Χάρτη του ΟΗΕ στο άρθρο 2(7), όπου κατά τον Έλληνα κυρωτικό νομοθέτη: "ουδεμία διάταξις εκ των διαλαμβανομένων εις τον παρόντα Χάρτην θα παρέχη το δικαίωμα εις τα Ηνωμένα Έθνη να επεμβαίνωσιν εις ζητήματα ανήκοντα ουσιαστικώς εις την εσωτερικήν δικαιοδοσίαν οιουδήποτε Κράτους ή θα υποχρεοί τα Μέλη να υποβάλλωσιν παρόμοια ζητήματα προς διακανονισμόν κατά τον παρόντα Χάρτην". (Α.Ν. 585, 1945, σ. 1213).

6. Γνωμοδότηση του Διεθνούς Δικαστηρίου της Χάγης, περί της "Νομιμότητας της απειλής ή χρήσης των πυρηνικών όπλων", στην οποία το Δικαστήριο στην παράγραφο 39 απεφάνθη ότι τα άρθρα 2(4), 42[60] και 51 του Χάρτη του ΟΗΕ δεν αναφέρονται σε συγκεκριμένα όπλα, εφαρμόζονται σε κάθε χρήση βίας και ανεξαρτήτως των χρησιμοποιούμενων όπλων (ICJ, 1996, p. 244).

7. Ψήφισμα της ΓΣ/ΟΗΕ περί του "Ορισμού της Επίθεσης" (UN/GA, 1974).

8. Απόφαση το 2001 του ΣΑ/ΟΗΕ, με την οποία το Συμβούλιο αναγνώρισε στις ΗΠΑ το "φυσικό δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας, σύμφωνα με το Χάρτη" για τις επιθέσεις της 11ης Σεπτεμβρίου 2001, όπου ως "όπλα" χρησιμοποιήθηκαν πολιτικά επιβατικά αεροσκάφη (UN/Security Council, 2001).

9. Δίκαιο Διεθνούς Ευθύνης[61] (UN/International Law Commission, 2001).

Το κανονιστικό νομικό πλαίσιο, ήτοι το άρθρο 2(4) του Χάρτη του ΟΗΕ και το εθιμικό δίκαιο, παρουσιάζει δύο κυρίαρχα χαρακτηριστικά, εν πρώτοις η διατύπωσή του εδράζεται σε αμιγώς απαγορευτικό περιεχόμενο, οπότε δεν διατυπώνεται καμία ρύθμιση για αποκατάσταση σε status quo ante και εν δευτέροις δεν καθορίζει τη φύση και το εύρος των ενεργειών σε περίπτωση παραβίασής του (Μακρής, 2011, σ. 36). Οι τελευταίες διέπονται από τους κανόνες άσκησης του νόμιμου δικαιώματος αυτοάμυνας και το Δίκαιο Διεθνούς Ευθύνης, ενώ ανατίθενται εν λευκώ στο ΣΑ/ΟΗΕ, όταν αυτό αποφασίσει χρονικά να επέμβει και αναλαμβάνοντας δράσεις ad hoc.

Δεδομένου ότι η συζήτηση για τα όρια εφαρμογής των άρθρων 2(4) και 51 του Χάρτη του ΟΗΕ παραμένει ανοικτή (Hathway et al., 2012, p. 844), η απάντηση στο ερώτημα εάν η προβολή κυβερνοϊσχύος στον κυβερνοχώρο συνιστά εκδήλωση χρήσης βίας (force) ή εκδήλωση επίθεσης (aggression), ήτοι εκδήλωση ένοπλης βίας

[60] Κατά τον Έλληνα κυρωτικό νομοθέτη: "εάν το Συμβούλιον Ασφαλείας ήθελε θεωρήσει τα προβλεπόμενα υπό του άρθρου 41 μέτρα μη τελέσφορα ή ήθελον ταύτα αποδειχθή μη τελέσφορα θα δύναται να αναλάβη από αέρος, θαλάσσης ή δια στρατιωτικών δυνάμεων της ξηράς, την δράσιν ήτις θα είναι αναγκαία όπως διατηρηθή ή αποκατασταθή η διεθνής ειρήνη και ασφάλεια. Παρομοία δράσις θα δύναται να περιλαμβάνη στρατιωτικάς επιδείξεις, αποκλεισμόν και άλλας επιχειρήσεις από αέρος θαλάσσης ή ξηράς υπό Μελών των Ηνωμένων Εθνών"(Α.Ν. 585, 1945, σ. 1213).

[61] Το Δίκαιο Διεθνούς Ευθύνης δεν αποτελεί Σύμβαση και δεν δεσμεύει καθ' οιονδήποτε τρόπο τα κράτη, αν και υπάρχουν πιέσεις προς αυτήν την κατεύθυνση. Παρά ταύτα τυγχάνει ευρείας αποδοχής στον νομικό κόσμο και εφαρμόζεται πρακτικά ακόμη και από το ICJ (Crawford, 2012).

(armed force) ή ακόμα περισσότερο ένοπλης επίθεσης (armed attack), αποτελεί ύψιστη πρόκληση διερεύνησης των απωτάτων ορίων ενός κειμένου που συνετάχθη ογδόντα περίπου χρόνια πριν[62]. Η γραμματική ερμηνεία του όρου "βία" καλύπτει αναντίρρητα τη περίπτωση συμβατικής στρατιωτικής βίας, ενώ ανοίγει διάπλατα το παράθυρο για την κάλυψη και ετέρων μορφών καταναγκασμού. Συντακτικά ο όρος δεν συνοδεύεται από τον επιθετικό προσδιορισμό ένοπλος. Αυτή η "παράλειψη" δεν αποτελεί επ' ουδενί αβλεψία ή λάθος του νομοθέτη, διότι ο ίδιος έχει φροντίσει επιμελώς στα άρθρα 41 και 46 να χρησιμοποιείται ο επιθετικός προσδιορισμός, ενώ στο άρθρο 44 γίνεται σαφές ότι αφορά στρατιωτική βία και μόνον. Η τελολογική ερμηνεία του άρθρου ωθεί μερίδα μελετητών να υποστηρίζουν ότι οι ερμηνείες των όρων ένοπλη βία και βία θα πρέπει να αποδοθούν συστολικά, καθόσον σκοπός του Χάρτη είναι, σύμφωνα με το προοίμιο του, "όπως σώσωμεν τας επερχόμενας γενεάς από την μάστιγα του πολέμου". Συνεπώς, κατά τον διαπρεπή Γερμανό νομικό Randelzhofer, δεν αποτελεί σκοπό του Χάρτη ο περιορισμός εντός νομικού πλαισίου όλων των μορφών και τρόπων καταναγκασμού, οι οποίοι είναι δυνατόν να χρησιμοποιηθούν μεταξύ των κρατών στις διεθνείς τους σχέσεις (Μακρής, 2011, σ. 37).

Η τελευταία οπτική φαίνεται να είναι και η επικρατούσα αφού τόσο στις προπαρασκευαστικές εργασίες της Διάσκεψης του San Francisco το 1945, όσο και στις Διακηρύξεις της ΓΣ του ΟΗΕ, οι οποίες αναφέρονται ανωτέρω, αποκαλύπτεται η βούληση της πλειοψηφίας διεθνώς ότι "βία" δεν σημαίνει "ένοπλη βία" (Silver, 2002,

[62] Καίτοι οι όροι επίθεση και ένοπλη επίθεση καταχρηστικά στην κοινή αντίληψη ταυτίζονται, κατά το διεθνές δίκαιο υφίσταται ουσιώδης νομική διάκριση. Εκδήλωση επίθεσης συνεπάγεται παραβίαση του άρθρου 2, σύμφωνα με το άρθρο 3 του Ψηφίσματος της ΓΣ/ΟΗΕ περί του "Ορισμού της Επίθεσης", αλλά δεν συνεπάγεται απαραίτητα ενεργοποίηση του άρθρου 51 του Χάρτη του ΟΗΕ. Αντίθετα, εκδήλωση ένοπλης επίθεσης πυροδοτεί το δικαίωμα ενεργοποίησης του άρθρου 51.

pp. 80-81).[63] Επιπλέον, στην ίδια γραμμή κινείται και η απόφαση του Διεθνούς Δικαστηρίου της Χάγης στην υπόθεση Nicaragua v. USA, όπου θεωρήθηκε ότι η χρηματοδοτική υποστήριξη των ανταρτών, η οποία με τη σειρά της χρησιμοποιήθηκε για πράξεις βίας, δεν συνιστά χρήση βίας εκ μέρους των ΗΠΑ (Silver, 2002, p. 81).

Οπότε, άμεσα προκύπτει ότι προκειμένου να θεωρηθεί η προβολή κυβερνοϊσχύος ως άσκηση ένοπλης βίας θα πρέπει να εξετασθεί το κατά πόσον η εκδήλωση της συνιστά ένοπλη βία ή ένοπλη επίθεση, καθώς το άρθρο 51 του Χάρτη του ΟΗΕ επιτρέπει την αυτοάμυνα ρητά μόνον εναντίον ενόπλου επιθέσεως. Αυτό με τη σειρά του συνεπάγεται την ανάγκη καθορισμού της έννοιας "όπλο". Η τρέχουσα νομική αντίληψη του όρου είναι πως ως όπλο ορίζεται "κάθε μέσο για διεξαγωγή επιθετικής ή αμυντικής μάχης, ή οποιοδήποτε άλλο μέσο που μπορεί να χρησιμοποιηθεί ή που αποσκοπεί στην καταστροφή, κατανίκηση ή τραυματισμό του εχθρού" (Black, 1968, p. 1762). Συνεπώς, κάθε αντικείμενο ή μέσο δυνητικά είναι όπλο, άρα και μια επιχείρηση κυβερνοχώρου δύναται να θεωρηθεί ως όπλο, αρκεί η χρήση του ως τέτοιο να συνοδεύεται και από την πρόθεση αυτού που το φέρει ή το χρησιμοποιεί[64].

Όμως, με δεδομένο ότι, το άρθρο 2(4) του Χάρτη απαγορεύει μεν τη χρήση βίας, αλλά το άρθρο 51 του Χάρτη επιτρέπει τη νόμιμη εκδήλωση αυτοάμυνας μόνον εφόσον η ένοπλη βία αναχθεί σε ένοπλη επίθεση, συνάγεται κατά Randelzhofer (Μακρής, 2011, σ. 39) και κατά Dinstein (Hathway et al., 2012, p. 847) ότι υφίσταται ένα ρυθμιστικό διάκενο ανάμεσα στην κατωφλίωση εκδήλωσης ένοπλης βίας και

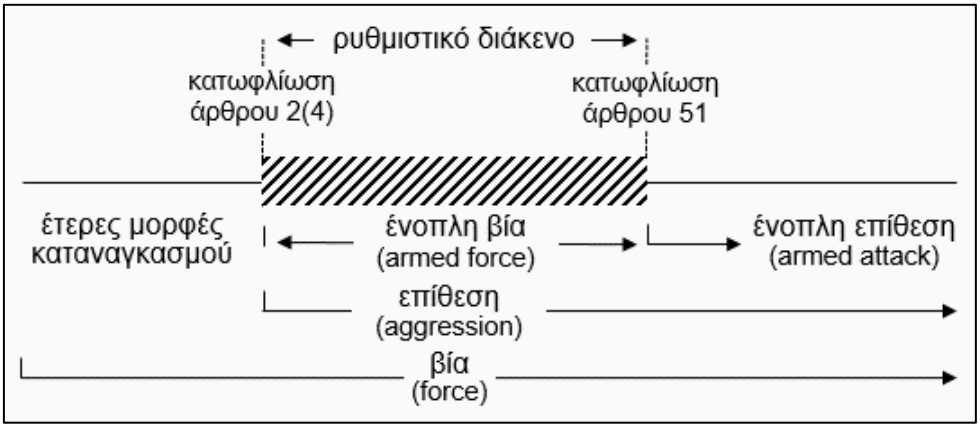
[63] Ίσως τελικά αποτελέσει θεία νέμεση το γεγονός ότι, ενώ μέχρι σήμερα τα αδύναμα κράτη πίεζαν προς την κατεύθυνση διασταλτικής ερμηνείας του άρθρου 2(4), αλλά τα ισχυρά κράτη αρνούνταν σκοπίμως να την αποδεχθούν, οι ΕΕΚ, που με πολύ μικρό κόστος είναι σε θέση να παράξουν ασύμμετρα υπερμεγέθη αποτελέσματα, οδηγήσουν τα ισχυρά, πλην όμως ευάλωτα πλέον, κράτη να αναθεωρήσουν τη στάση τους και να "συνθηκολογήσουν" (Hathway et al., 2012, p. 844). Ακόμη κι έτσι όμως, παραμένει ανοικτό ερώτημα η έκταση ερμηνείας του άρθρου 2(4) στις περιπτώσεις άσκησης μη-στρατιωτικής φυσικής βίας, όπως η πρόκληση πυρκαγιάς ή πλημμύρας (Silver, 2002, pp. 82-83).

[64] Αυτή άλλωστε είναι και η οπτική η οποία υιοθετήθηκε από το ΣΑ/ΟΗΕ με την Απόφαση S/RES/1373/28-09-2001, τα επιβατικά αεροπλάνα θεωρήθηκαν όπλα στα χέρια των τρομοκρατών, άρα δεν αποτελεί έκπληξη η υιοθέτηση ανάλογης οπτικής για την προβολή κυβερνοϊσχύος και τις ΕΕΚ στον κυβερνοχώρο στους κόλπους του ΝΑΤΟ.

στην κατωφλίωση εκδήλωσης ένοπλης επίθεσης[65]. Εντός αυτού του διακένου, στη νοητή βαθμίδα κλιμάκωσης βίας, το κράτος μπορεί να χρησιμοποιήσει άλλα μέτρα αντίδρασης, σε καμία περίπτωση όμως δεν δύναται να ασκήσει την αναγκαία ανάλογη βία στα πλαίσια αυτοάμυνας. Τα ανωτέρω οπτικοποιούνται στην κάτωθι εικόνα:

Εικόνα 1

Το ρυθμιστικό διάκενο μεταξύ των άρθρων 2(4) και 51 του Χάρτη ΟΗΕ



Προσεγγίσεις υπαγωγής στο jus ad bellum

Όπως ήδη τεκμαίρεται εκ των ανωτέρω δεν συνιστά νομικά, κατά το διεθνές δίκαιο, ένοπλη επίθεση κάθε έκφανση προβολής κυβερνοϊσχύος στον κυβερνοχώρο. Επιπλέον, αποτελεί ακόμα πεδίο ακαδημαϊκής διαμάχης ο τρόπος αξιολόγησης των ΕΕΚ, προκειμένου να εξαχθεί γνήσιο υποσύνολο αυτών, οι οποίες χαρακτηρισμένες ως ένοπλες επιθέσεις πλέον να πυροδοτούν το δικαίωμα της νόμιμης αυτοάμυνας.˙ Η τελευταία υπόκειται ανελαστικά στις αρχές της αναγκαιότητας, της αναλογικότητας

[65] Και η πρακτική του Διεθνούς Δικαστηρίου της Χάγης ενισχύει την υπόψη θεώρηση, καθώς υποδεικνύει ότι μικρής κλίμακας μεθοριακές εισβολές συνιστούν "μεθοριακά επεισόδια" και όχι ένοπλες επιθέσεις. Οπότε, εισάγει de facto την υιοθέτηση του κριτηρίου κλίμακας-αποτελέσματος (scale and effects) προκειμένου να νομιμοποιήσει τη χρήση του δικαιώματος νόμιμης αυτοάμυνας (Hathway et al., 2012, p. 847).

και της αμεσότητας που επιβάλλει το εθιμικό διεθνές δίκαιο.[66] Οι οπτικές προσέγγισης δύνανται να ομαδοποιηθούν σε τρεις κυρίαρχες κατηγορίες: στην προσέγγιση με βάση το μέσο, στην προσέγγιση με βάση το στόχο και στην προσέγγιση με βάση το αποτέλεσμα (Hathway et al., 2012, p. 848).

Η *προσέγγιση με βάση το μέσο* συνιστά την παραδοσιακή οπτική στην αντίληψη περί ενόπλου επιθέσεως. Κατ' αυτήν η προβολή κυβερνοϊσχύος δια διενέργειας ΕΕΚ συνιστά ένοπλη χρήση βίας αποκλειστικά και μόνον εφόσον χρησιμοποιεί στρατιωτικά όπλα κινητικής τροχιάς. Οπότε, επί παραδείγματι, ο βομβαρδισμός με πολεμικά Α/Φ εξυπηρετητών δικτύου ή καλωδιώσεων διαδικτύου συνιστά χρήση ένοπλης βίας, η οποία δύναται να υπερβεί την κατωφλίωση της ένοπλης επίθεσης υπό την ανελαστική προϋπόθεση της πλήρωσης του κριτηρίου επαρκούς κλίμακας στη βαρύτητα των επιφερομένων αποτελεσμάτων της (Hathway et al., 2012, p. 848). Προφανής αχίλλειος πτέρνα της υπόψη προσέγγισης είναι η αδυναμία της να κατατάξει ως ένοπλη βία οιαδήποτε ενέργεια εκδηλώνεται μέσω του κυβερνοχώρου, αφού από αυτήν εκλείπουν τα φυσικά χαρακτηριστικά τα οποία θα τη χαρακτήριζαν ως τέτοια. Ο ΟΗΕ τόσο στον Καταστατικό Χάρτη του όσο και στην Απόφαση περί «Ορισμού της Επίθεσης» υιοθετεί την υπόψη προσέγγιση, παρά το γεγονός ότι πληθώρα έγκριτων ακαδημαϊκών την έχουν απορρίψει ως επικίνδυνα αναχρονιστική (Hathway et al., 2012, pp. 848-849).

Αντιθέτως, στην *προσέγγιση με βάση το στόχο* κριτήριο αναγωγής της προβολής κυβερνοϊσχύος στο επίπεδο ενόπλου επιθέσεως αποτελεί η στοχοποίηση επαρκώς σημαντικού πληροφοριακού συστήματος. Με άλλα λόγια, αρκεί η εκδήλωση ενέργειας κατά κρισίμου συστήματος εθνικής πληροφοριακής υποδομής, ανεξαρτήτως από την πρόκληση υλικής ζημίας ή τυχόν ανθρωπίνων απωλειών, προκειμένου να νομιμοποιηθεί το"θύμα" να αναλάβει ενέργειες οι οποίες υπάγονται στο πλαίσιο νόμιμης αυτοάμυνας. Προφανώς η υιοθέτηση της υπόψη προσέγγισης εγκυμονεί τον κίνδυνο της ανεξέλεγκτης κλιμάκωσης βίας (Hathway et al., 2012, p. 849).

Τέλος, η *προσέγγιση με βάση το αποτέλεσμα* επιχειρεί να ταξινομήσει την προβολή κυβερνοϊσχύος δια διενέργειας ΕΕΚ ως ένοπλη επίθεση με χρήση του

[66] Απόδοση ελληνιστί των όρων "necessity", "proportionality" και "immediacy" αντίστοιχα.

κριτηρίου του ισοδυνάμου αποτελέσματος. Η υπόψη θεώρηση, η οποία τυγχάνει της ευρύτερης αποδοχής όλων, είναι διαισθητικά ορθή και υιοθετεί τα θετικά στοιχεία των προηγουμένων προσεγγίσεων, ενώ αποσυμπλέκεται ευέλικτα από τα μειονεκτήματά τους. Η δική της αχίλλειος πτέρνα υποκρύπτεται αφενός στην αναγκαιότητα της de jure διαμόρφωσης ex ante κοινά αποδεκτής τυπολογίας αποτελεσμάτων, τα οποία θα νομιμοποιούσαν την προσφυγή στη νόμιμη αυτοάμυνα και αφετέρου στη de facto "νομιμοποίηση" της χαμηλής έντασης βίας (Hathway et al., 2012, p. 849).

Κατά καιρούς έχουν προταθεί διάφορες βαριάντες κριτηρίων με πλέον διάσημη αυτή του εισηγητή της υπόψη προσέγγισης ακαδημαϊκού και νομικού Michael Schmitt. Η δική του οπτική εστιάζει στην εξέταση της ενέργειας υπό το πρίσμα έξι κριτηρίων και συγκεκριμένα: της σφοδρότητας, της χρονικής αμεσότητας, της αιτιακής αμεσότητας, της διεισδυτικότητας, της μετρησιμότητας και της έλλειψης νομιμότητας (Schmitt, 1999, pp. 914-915).[67] Προφανώς στην πρότασή του, και προκειμένου να αποφεύγονται ανεξέλεγκτες κλιμακώσεις, θα μπορούσε να προστεθεί άλλο ένα κριτήριο, αυτό της απόδοσης της κρατικής ευθύνης. Πάντως, είναι πρόδηλο ότι κάθε κριτήριο εισάγει αθόρυβα την απαίτηση θέσπισης οικείου ορίου κατωφλίωσης.

Στην πλέον απλή εκδοχή της προσέγγισης με βάση το αποτέλεσμα, αρκεί η εξέταση μόνον δύο κριτηρίων, αυτών της προβλεψιμότητας και της σφοδρότητας (Hathway et al., 2012, pp. 850-851). Με άλλα λόγια, μια προβολή κυβερνοϊσχύος στον κυβερνοχώρο δια διενέργειας ΕΕΚ νομιμοποιεί την εκδήλωση ενεργειών αυτοάμυνας μόνον εφόσον η σφοδρότητα των αναμενόμενων συνεπειών προσομοιάζει με αυτές άσκησης ένοπλης βίας. Η υπόψιν παραλλαγή θυσιάζει την ακαδημαϊκή πληρότητα των κριτηρίων Schmitt στο βωμό της απλότητας και της ευκολίας. Παράλληλα όμως, εξασφαλίζει ότι μόνον μια κατάλληλη κρίσιμη μάζα ΕΕΚ θα χαρακτηρισθεί ως ένοπλη βία, αποφεύγοντας με αυτόν τον τρόπο τον κίνδυνο επιπολασμού ανεξέλεγκτης κλιμάκωσης της βίας.

[67] Απόδοση ελληνιστί των όρων severity, immediacy, directness, invasiveness, measurability και presumptive legitimacy αντίστοιχα.

Προβολή κυβερνοϊσχύος κατά το jus in bello

Καίτοι έως σήμερα δεν υφίσταται καμία ιστορική καταγραφή ΕΕΚ, η οποία να απετέλεσε αυτοτελώς την αιτία, ή έστω την αφορμή, για την έναρξη ένοπλης σύγκρουσης συμβατικού πολέμου, έχουν εξαπολυθεί κατά καιρούς ΕΕΚ μεταξύ εμπολέμων είτε μεμονωμένα είτε συνδυαστικά με συμβατικές πολεμικές επιχειρήσεις, ως ανταπόδοση σε κλασικής μορφής προκλήσεις. Συνεπώς, για λόγους πληρότητας απαιτείται να καταγραφεί η οπτική του νομικού πλαισίου, που διέπει σε εμπόλεμη περίοδο το διεθνές δίκαιο.

Αυτό που σήμερα καλείται Διεθνές Ανθρωπιστικό Δίκαιο ή Δίκαιο Ενόπλων Συρράξεων ή Δίκαιο του Πολέμου ή Δίκαιο της Χάγης ή επί το λατινικότερο jus in bello, αφορά στο μεικτό δίκαιο το οποίο προέκυψε μετά τη συνένωση του Δικαίου της Χάγης και του Δικαίου της Γενεύης (Μαρούδα, 2014, σ. 736). Το πρώτο συνιστούσε το κανονιστικό πλαίσιο για ό,τι αφορούσε στα μέσα διεξαγωγής της μάχης, στην κατοχή και στην ουδετερότητα. Ενώ, το δεύτερο, ήδη γνωστό και ως ανθρωπιστικό δίκαιο, διαμόρφωνε το δικαιικό κανονιστικό πλέγμα των προστατευτικών διατάξεων για τα θύματα των ενόπλων συρράξεων, ήτοι τραυματίες, ασθενείς, ναυαγούς, αιχμαλώτους πολέμου, άμαχο πληθυσμό και γενικά όσων συνέδραμαν τα θύματα. Η διάκριση των δύο κατηγοριών δικαίου σταδιακά αμβλύνθηκε ιδιαίτερα μετά την υιοθέτηση, το 1977, των δύο Προσθέτων Πρωτοκόλλων, με αποτέλεσμα σήμερα να αντιμετωπίζονται από τη διεθνή νομική βιβλιογραφία και πρακτική ως ταυτόσημες έννοιες. Η προβληματική του εν λόγω δικαίου, ως προς τις καινοφανείς προκλήσεις αξιολόγησης της νομιμότητας επιχειρήσεων κυβερνοχώρου εν πολέμω, ανάγεται στο πρώτο επίπεδο στην επιμέρους εξέταση συσχετίσεων της προβολής κυβερνοϊσχύος με τις πέντε κυρίαρχες αρχές που το διέπουν, ήτοι της διάκρισης, της απαγόρευσης πρόκλησης μη αναγκαίου πόνου, της αναγκαιότητας, της αναλογικότητας και της ουδετερότητας.[68]

[68] Σειριακά αγγλιστί: principle of distinction, principle of prohibition of unnecessary suffering, principle of necessity, principle of proportionality, principle of neutrality. Οι δε δύο πρώτες αποτελούν τις βασικές αρχές του jus in bello, κατά το Διεθνές Δικαστήριο της Χάγης (ICJ, 1996, p. 257 - para. 78).

Η *αρχή της διάκρισης* αποτελεί πεδίο έγερσης μεγάλων προκλήσεων στην αξιολόγηση της νομιμότητας κατά την προβολή κυβερνοϊσχύος εν πολέμω. Η αρχή επιβάλλει ότι τα όπλα, άρα και τα κυβερνοόπλα, θα πρέπει να χρησιμοποιούνται με τέτοια ακρίβεια χρήσης, ώστε να είναι δυνατή η διάκριση μεταξύ πολιτικού τύπου και στρατιωτικών αντικειμενικών σκοπών. Στο πνεύμα αυτό στο άρθρο 54(2) του Προσθέτου Πρωτοκόλλου του 1977 (UN, 1977, p. 267) καθορίζεται κατά τον Έλληνα κυρωτικό νομοθέτη ότι "απαγορεύεται η επίθεση, καταστροφή, απομάκρυνση ή αχρήστευση αστικών αντικειμένων απαραίτητων στην επιβίωση τους αμάχου πληθυσμού, όπως τρόφιμα [και] παροχές πόσιμου νερού" (Ν. 1786, 1988, σ. 2452). Διασταλτικά η αρχή απαγορεύει επιχειρήσεις στον κυβερνοχώρο που θα είναι ανεξέλεγκτες, απρόβλεπτες και δεν θα είναι σε θέση να στοχοποιούν αυστηρά στρατιωτικούς και μόνον ΑΝΣΚ. Όμως, δεδομένης πλέον της παράλληλης χρήσης, πολλαπλών υποδομών και υπηρεσιών, τίθεται εύλογα προβληματισμός ως προς τη ρεαλιστική εφαρμογή της. Στην ίδια αρχή υπάγεται και η παράμετρος εξέτασης του προσωπικού που νομιμοποιείται να διεξάγει κυβερνοεπιχειρήσεις (Hathway et al., 2012, pp. 857-859). Πρόδηλα, η επιλογή κρατικού δρώντα να εμπλέξει μη στρατιωτικό προσωπικό, μέσω ανάθεσης σε διαμεσολαβητικούς δρώντες, με πρόθεση την εύκολη άρνηση εμπλοκής του και την αποκήρυξη της όποιας ευθύνης του, συνιστά παραβίαση του jus in bello. Όμως, ακόμη και ο καθορισμός αρμοδιοτήτων του στρατιωτικού προσωπικού που νομιμοποιείται να διεξάγει κυβερνοεπιχειρήσεις συνιστά νομικά επικίνδυνο ναρκοπέδιο, με προφανή επιλογή την καθετοποιημένη διοίκηση με αυστηρά κεντρικό έλεγχο. Εξ ου και στο εν ισχύι Διακλαδικό Δόγμα ορίζεται στις ελληνικές Ένοπλες Δυνάμεις, και για ό,τι τις αφορά, συγκεκριμένος εθνικός Φορέας ο οποίος είναι υπεύθυνος, μεταξύ άλλων, για τον σχεδιασμό, την εκτέλεση, και τον συντονισμό συνολικά των επιχειρήσεων στον κυβερνοχώρο (ΓΕΕΘΑ/ΔΔΔ, 2013, σ. 5-1).

Η *αρχή της απαγόρευσης πρόκλησης μη αναγκαίου πόνου* αποτελεί απαράβατη αρχή του διεθνούς εθιμικού δικαίου και η πρώτη της αναφορά

εντοπίζεται στο Προοίμιο της Διακήρυξης της Αγίας Πετρούπολης το 1868[69]. Αντιμετωπίζει προκλήσεις παρόμοιες με αυτές της διενέργειας συμβατικών επιχειρήσεων, με την επισήμανση όμως ότι κατά κοινή αποδοχή η αναφορά σε πόνο αφορά συγκεκριμένα σε φυσικό πόνο. Συνεπώς, κάθε άλλη επιχείρηση που προκαλεί μη φυσικό πόνο θεωρείται γενικά ως νόμιμη, πχ ψυχολογικές επιχειρήσεις. Προφανώς όμως, αποτελεί ανοικτό πρόβλημα ο συνυπολογισμός δευτερογενών αποτελεσμάτων επιχειρήσεων του κυβερνοχώρου, εφόσον βεβαίως αυτά συνιστούν πηγή πρόκλησης φυσικού πόνου.

Σύμφωνα με την *αρχή της αναγκαιότητας,* θα πρέπει η διενέργεια οιασδήποτε πολεμικής επιχείρησης να συσχετίζεται άμεσα με την προσπάθεια απόκτησης στρατηγικού πλεονεκτήματος εκ μέρους του ενεργούντος. Συνεπώς, μια μεμονωμένη διενέργεια επιθετικής ενέργειας στον κυβερνοχώρο είναι δυνατόν να βρεθεί ακάλυπτη και εκτός διακαιϊκού πλαισίου διεξαγωγής του πολέμου, εάν δεν προωθεί με απτό τρόπο κάποιον συγκεκριμένο στρατιωτικό αντικειμενικό σκοπό. Η εξέταση της νομιμότητας διενέργειας κυβερνοεπιχειρήσεων, ως προς την υπόψη αρχή, αντιμετωπίζει προκλήσεις παρόμοιες με αυτές της διενέργειας συμβατικών επιχειρήσεων και δεν παρουσιάζει κάποια διακριτή ιδιαιτερότητα (Hathway et al., 2012, p. 853).

Σε αντίθεση με τις δύο προηγούμενες αρχές, η *αρχή της αναλογικότητας* ωθείται στα όρια ερμηνείας της. Και αυτό διότι, σύμφωνα με το άρθρο 51(5)(β) του Προσθέτου Πρωτοκόλλου Ι της Γενεύης, απαγορεύεται η "επίθεση η οποία δύναται να αναμένεται να προκαλέσει απώλειες και τραυματισμούς ανάμεσα σε ιδιώτες, ως παρεπόμενον αυτής ζημίες σε αστικούς στόχους ή ένα συνδυασμό αυτών, τα οποία θα ήσαν υπερβολικά σε σχέση με το συγκεκριμένο και άμεσο στρατιωτικό πλεονέκτημα που αναμένετο" (Ν. 1786, 1988, σ. 2452). Επισημαίνεται βεβαίως ότι λαμβάνοντας υπόψη συνδυαστικά τα άρθρα 51(5)(β), 54 και 57(2)(α)(ιιι) του υπόψιν Πρωτοκόλλου Ι, δεν απαγορεύεται κάθε χρήση ένοπλης βίας η οποία αναμένεται να

[69] Συμπεριελήφθη ως κανόνας Δικαίου στο πρόσθετο Πρωτόκολλο Ι το 1977 με το άρθρο 35(2), σύμφωνα με το οποίο κατά τον Έλληνα κυρωτικό νομοθέτη: "απαγορεύεται η χρήση όπλων, βλημάτων και υλικού και μεθόδων πολέμου τέτοιας φύσης ώστε να προκαλούν περιττά τραύματα και μη απαραίτητα πόνο" (Ν. 1786, 1988, σ. 2449).

επιφέρει τις περιγραφόμενες στο άρθρο 51(5)(β) συνέπειες. Επιβάλλεται όμως μια κατωφλίωση νομιμότητας, η οποία προσδιορίζεται, έστω και αφηρημένα, από την επίτευξη του αναμενόμενου στρατιωτικού πλεονεκτήματος (Hathway et al., 2012, p. 854).

Όμως, τα άμεσα, ή αλλιώς πρωτογενή αποτελέσματα, διεξαγωγής των ΕΕΚ είναι ασφυκτικά εγκλωβισμένα εντός του άυλου κυβερνοχώρου, συνήθως εξαντλούμενα σε προσωρινή, με την έννοια της χρονικής διάστασης, αδυναμία λειτουργίας των κρισίμων συστημάτων, των οποίων φυσικά γνήσιο υποσύνολο αποτελούν τα συστήματα κρισίμων υποδομών. Παραμένει δυσεπίλυτο ανοικτό πρόβλημα η αξιολόγηση, στο πλαίσιο μιας ανάλυσης αναλογικότητας, της χρονοεξαρτώμενης επιβολής δυσλειτουργίας των υπολογιστικών συστημάτων.[70]

Τέλος, σύμφωνα με την *αρχή της ουδετερότητας* αποτελεί κυριαρχικό δικαίωμα του ουδετέρου κράτους το απαραβίαστο, ενώ κυριαρχικές υποχρεώσεις είναι η αποχή και η αμεροληψία, αντιστρόφως αποτελεί χρέος κάθε εμπόλεμου να σεβασθεί το πρώτο ως και να επιμείνει στα τελευταία (Hathway et al., 2012, p. 859). Όπως καθίσταται εύλογα προφανές, η αρχή της ουδετερότητας εφαρμόζεται μόνο στην περίπτωση διεθνών ενόπλων συγκρούσεων. Πλην όμως και αυτή η αρχή αντιμετωπίζει ουσιαστικές, ως προς τον ίδιο τον πυρήνα της, προκλήσεις εφαρμογής. Επί παραδείγματι, πως θα διαχειριστεί το jus in bello την περίπτωση που κράτος διακηρύττει μεν την ουδετερότητά του αλλά υπολογιστικά συστήματα που εντοπίζονται χωρικά στην επικράτειά του συμμετέχουν σε επιχειρήσεις κυβερνοχώρου; Άμεσα ανακύπτουν τα επόμενα ερωτήματα. Το κράτος αποδέκτης

[70] Και σαν να μην ήταν αυτό αρκετό στην προβληματική αξιολόγησης έρχεται συνακόλουθα να προστεθεί και το ερώτημα μέχρι ποιου βάθους θα πρέπει να συνυπολογίζονται τα μη πρωτογενή αποτελέσματα. Επί παραδείγματι, η προσωρινή διακοπή λειτουργίας νοσοκομειακών υποδομών θα μπορούσε να προκαλέσει απώλειες ανθρωπίνων ζωών και να συνδεθεί ευθέως, αν και αποτελεί δευτερογενές αποτέλεσμα, με μια κυβερνοεπίθεση. Όμως, η προσωρινή διακοπή λειτουργίας Συστήματος Εναερίου Ελέγχου, η οποία θα έχει ως συνέπεια τη μη έγκαιρη διακομιδή ασθενούς σε νοσοκομείο, με συνέπεια την κατάληξη του, είναι απώλεια ζωής η οποία θα πρέπει να καταλογισθεί ως αποτέλεσμα της κυβερνοεπίθεσης; Ίσως τελικά τέτοιου τύπου ερωτήματα ωθήσουν σε διαφορετική αντίληψη εφαρμογής του άρθρου 2(4) σε ό,τι αφορά τις προσωρινές, μη θανατηφόρες πρωτογενείς συνέπειες άσκησης βίας (Hathway et al., 2012, p. 854).

των αποτελεσμάτων οφείλει να σεβασθεί τη δεδηλωμένη ουδετερότητα; Ποια είναι τα κριτήρια και ποια η κατωφλίωση στην ανάθεση ευθύνης ώστε να τεκμαίρεται εμπλοκή του κράτους και άρα να αίρεται η υποχρέωση στο άλλο κράτος σεβασμού της ουδετερότητας του πρώτου; Τέτοιου είδους καινοφανείς προκλήσεις δεν θα είναι πια οι εξαιρέσεις, που διερευνούν τα όρια εφαρμογής του jus in bello, αλλά μάλλον ο κανόνας. Ως εκ τούτου, de facto το jus in bello αναμένεται να ωθηθεί στα όρια ερμηνείας του.

Κυβερνοϊσχύς και διεθνές δίκαιο, κατακλείδα

Λαμβάνοντας υπόψιν το σύνολο των ανωτέρω αναγραφομένων πρόδηλα προκύπτει ότι η σύγχρονη τάση της νομικής ρύθμισης του κυβερνοχώρου lex lata, συνιστά απλώς μια κατ’ επίφαση απόπειρα εφαρμογής της "κανονικότητας" Δικαίου στη "μη κανονικότητα" του κυβερνοχώρου. Προφανώς, οι κυβερνοεπιχειρήσεις δεν διενεργούνται σε νομικό κενό. Πλην όμως, έως την κατάρτιση και τη διεθνή αποδοχή ειδικού "κυβερνοδικαίου" η προβολή κυβερνοϊσχύος στον κυβερνοχώρο θα τελεί de facto σε μια ιδιότυπη προνομιακή κατάσταση γυμνή εξουσίας, με τους κρατικούς δρώντες, εκμεταλλευόμενους τη συγκυρία, να προσπαθούν να διατηρήσουν ή να επαυξήσουν το βάθος του επιχειρησιακού τους αποτυπώματος (Janssens, 2022, p. 2116). Η Ελλάδα οφείλει να ακολουθεί το διεθνές υπόδειγμα και να εξελίσσει τις δυνατότητες της ελληνικής κυβερνοϊσχύος με τέτοιον τρόπο, ώστε χωρίς να παραβιάζει το διεθνές δίκαιο να εκμεταλλεύεται με τον καλύτερο δυνατό τρόπο το momentum προς εξυπηρέτηση των εθνικών συμφερόντων.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Κεφάλαιο τέταρτο

Περί αποτίμησης της εθνικής κυβερνοϊσχύος

Γενικά

Δεδομένου ότι η έννοια της ισχύος είναι συνυφασμένη με την έννοια της επιβολής, δεν αποτελεί έκπληξη το γεγονός ότι η εφαρμοσμένη πολιτική θέλγεται διαχρονικά από την ιδέα αποτίμησης τόσο των επιμέρους παραγόντων εθνικής ισχύος όσο και της ίδιας της εθνικής ισχύος συνθετικά, ει δυνατόν με όρους απόλυτων αριθμητικών τιμών. Η κεντρική ιδέα είναι ότι ιδανικά η ισχύς με όρους μέσων/δυνατοτήτων μεταφράζεται σε ισχύ με όρους αποτελέσματος απρόσκοπτα και επαναλαμβανόμενα ως να αποτελεί κάθε φορά εφαρμογή κάποιου φυσικού νόμου. Πράγματι, μια τέτοια προοπτική θα αναδιαμόρφωνε το σύνολο των διεθνών σχέσεων, όπως το γνωρίζουμε σήμερα, και θα άλλαζε τη φύση διεξαγωγής του ίδιου του πολέμου. Προικισμένες με ισχύ χώρες θα αρκούσε να επισείσουν το χαρτί της ισχύος τους σε λιγότερο προικισμένες χώρες και αυτές αναίμακτα θα υπέκυπταν υπό το συντριπτικό βάρος μιας βέβαιης σε περίπτωση σύγκρουσης επερχόμενης ήττας. Ένα τέτοιο σενάριο είναι βεβαίως ουτοπικό, καθόσον η εθνική ισχύς συνίσταται, μεταξύ άλλων, από ποιοτικούς, μη μετρήσιμους, μη ποσοτικοποιήσιμους παράγοντες, από παράγοντες οι οποίοι μπορεί να είναι μετρήσιμοι αλλά να μην μπορούν να ποσοτικοποιηθούν και επιπλέον ο ακριβής προσδιορισμός της συσχέτισης μεταξύ των επιμέρους συνιστωσών της αποτελεί πάντοτε έναν ανεπίλυτο γρίφο. Η σημαντικότερη προβληματική του όμως είναι ότι αγνοεί παντελώς την έννοια της στρατηγικής. Άλλωστε, έχει εκπονηθεί μελέτη η οποία εξετάζοντας τις στρατιωτικές δυνατότητες, υπό το πρίσμα της εθνικής ισχύος προ της έναρξης του πολέμου, διεπίστωσε ότι οι στρατιωτικά ισχυρότεροι αντίπαλοι κατά την χρονική περίοδο από το έτος 1816 έως το έτος 1976 βγήκαν νικητές λιγότερο από τις μισές φορές (Wayman et al., 1983).

Στο ερώτημα εάν είναι εφικτό να θεμελιωθεί μια αναλυτική μέθοδος υπολογισμού της απόλυτης, ή της σχετικής, εθνικής ισχύος και συνακόλουθα των συνθετικών παραγόντων της, άρα και της κυβερνοϊσχύος, ως πρώτο αναγκαίο βήμα

προβάλει η επανανοηματοδότηση της ίδιας της αφετηριακής έννοιας, ήτοι της ισχύος, με όρους αποτίμησης. Στη διεθνή βιβλιογραφία φαίνεται να έχει επικρατήσει η εξής τριπλέτα επιλογών στην προσέγγιση του όρου: η πρώτη είναι να θεωρηθεί η ισχύς ως κάποιου είδους "διαμοίραση πόρων", η δεύτερη ως η "ικανότητα χρήσης αυτών των πόρων ως μέσα", υπονοώντας την ύπαρξη κάποιου κεντρικού σχεδιασμού, και η τρίτη είναι η "αντίσταση σε αντίθετη θέληση" (Tellis et al., 2000, pp. 13-14). Αυτή η οπτική εισάγει με άλλα λόγια την απλούστατη ταξινομία πόροι, στρατηγική, αποτέλεσμα. Πώς όμως η ισχύς μετουσιώνεται σε εθνική ισχύ; Λίγες γραμμές πιο πάνω κατεγράφη ότι η διαισθητική προσέγγιση της απευθείας μετάφρασης των μέσων σε αποτελέσματα φαίνεται να μην είναι συνεπής. Παρά ταύτα, δεν σημαίνει ότι θα πρέπει να απορριφθεί, καθώς το ελλείπον συστατικό είναι απλώς η προσέγγιση της έννοιας της εθνικής ισχύος εντός συγκεκριμένου πλαισίου κάθε φορά (Tellis et al., 2000, p. 18). Συνεπώς, η ιδέα της ανάπτυξης μιας γενικής μετρικής, απόλυτης ή σχετικής, της εθνικής ισχύος είναι σκόπιμη και χρήσιμη, υπό την ανελαστική προϋπόθεση η ερμηνεία της να μην είναι απλοϊκή αλλά επαναξιολογούμενη εντός του εκάστοτε πλαισίου αναφοράς.

Κατά τη διάρκεια του 20ου αιώνα έχουν προταθεί αρκετές μεθοδολογικές προσεγγίσεις στην αποτίμηση της εθνικής ισχύος είτε μονοκριτηριακές, ήτοι προσεγγίσεις που ταυτίζουν την εθνική ισχύ με μία εκ των παραμέτρων της στρατιωτικής ή της οικονομικής ισχύος (πχ εξοπλιστικές δαπάνες), είτε πολυκριτηριακές, οι οποίες εισάγουν πολυπλοκότητα στη μετρική ισχύος δια της εισαγωγής αρκετών παραμέτρων με αντίτιμο την αξιόπιστη προσέγγιση μιας γενικής αλήθειας (Tellis et al., 2000, pp. 25-30). Ανάμεσα στις πλέον ευρέως αναγνωρίσιμες μετρικές είναι η μη γραμμική πολυκριτηριακή σχέση του Cline:

$$P_p=(C+E+M)*(S+W)$$[71]

Αντίστοιχα με την εθνική ισχύ προσπάθειες έχουν καταβληθεί και για τον

[71] Όπου: P_p η αντιληπτή ισχύς, *C* η κρίσιμη μάζα (περιλαμβάνει πληθυσμό και έκταση), *E* οι οικονομικές δυνατότητες (περιλαμβάνει εισόδημα, ενέργεια, ορυκτούς πόρους, βιομηχανία, τρόφιμα και εμπόριο), *M* οι στρατιωτικές δυνατότητες (περιλαμβάνει στρατηγικό ισοζύγιο, δυνατότητες εμπλοκής και πριμοδότηση της προσπάθειας), *S* ο εθνικός συντελεστής στρατηγικής και *W* η εθνική πρόθεση (περιλαμβάνει το επίπεδο εθνικής ολοκλήρωσης, τη δύναμη και τη συνάφεια της εθνικής στρατηγικής με το εθνικό συμφέρον). (Tellis et al., 2000, p. 30).

καθορισμό μετρικής της κυβερνοϊσχύος. Εν προκειμένω, διακρίνονται τρεις κυρίαρχες αντιλήψεις αναλόγως της οπτικής ως προς τον τρόπο εισφοράς της στη διαμόρφωση της εθνικής ισχύος. Πιο συγκεκριμένα ότι: αποτελεί ανεξάρτητο παράγοντα εθνικής ισχύος (οπότε στα μοντέλο DIME ή MIDFIELD αναγκαιεί να προστεθεί και το γράμμα C), δεν αποτελεί ανεξάρτητο παράγοντα ισχύος αλλά άθροισμα των επιμέρους επεκτάσεων των υφιστάμενων παραγόντων στον κυβερνοχώρο και τρίτον ότι δεν είναι τίποτα από τα προηγούμενα αλλά αποτελεί το προτιμώμενο επίπεδο επικοινωνίας της ανθρώπινης διάδρασης με την πραγματικότητα (Van Vuuren & Leenen, 2019, pp. 100-101). Ανεξαρτήτως πάντως αντίληψης, η επικρατούσες μετρικές είναι κατά κύριο λόγο μη γραμμικές πολυκριτηριακές σχέσεις, παραλλαγές αυτής του Cline (Van Vuuren & Leenen, 2019, pp. 116-119). Τη διαφορά στις θεωρήσεις μετρικής φαίνεται να κάνει μια πρόσφατη, πολύ πιο ολοκληρωμένη, αναλυτική και εμβριθής πρόταση από το διάσημο Πανεπιστήμιο του Harvard, η οποία και θα αναλυθεί στη συνέχεια. Η πρόταση αποφεύγει να εγκλωβιστεί στη θεωρητική διαμάχη περί της φύσης της κυβερνοϊσχύος και υιοθετεί ευέλικτα την προσέγγιση επίτευξης στόχου, ήτοι ότι κυβερνοϊσχύς είναι η μορφή της ισχύος με την οποία μπορούν να επιτευχθεί σύνολο συγκεκριμένων ΑΝΣΚ. Τέλος, ούσα πραγματικά αναλυτική δύναται να χρησιμοποιηθεί και ως μεθοδολογικό εργαλείο κατάστρωσης οδικού χάρτη για την επαύξηση εθνικής κυβερνοϊσχύος.

Το μοντέλο αποτίμησης εθνικής κυβερνοϊσχύος του Πανεπιστημίου Harvard (*NCPI-22*)

Σαράντα περίπου χρόνια πριν μια διεπιστημονική ομάδα διαπρεπών ακαδημαϊκών και ερευνητών του Πανεπιστημίου του Harvard, μεταξύ τους οι Nye και Allison, συνένωσαν τις δυνάμεις τους προκειμένου να αποσοβήσουν τη μεγαλύτερη ψυχροπολεμική απειλή, τον κίνδυνο ενός πυρηνικού πολέμου.[72] Το 2020 συστήθηκε εκ νέου μια ακαδημαϊκή ομάδα και πάλι στο Harvard με σκοπό όμως αυτή τη φορά

[72] Πρόκειται για το "Avoiding Nuclear War Project", με ένα εκ των παραγώγων του το πολύ γνωστό βιβλίο "Hawks, Doves, and Owls: An Agenda for Avoiding Nuclear War" (Allison et al., 1986).

να προσεγγίσει και να αποσοβήσει μια καινοφανή απειλή: τον κυβερνοπόλεμο. Τα θέματα που θα πρέπει να αντιμετωπιστούν με ενάργεια είναι και ουσιώδη και μεγάλου εύρους. Μεταξύ αυτών διακρίνονται: η προστασία των κρισίμων υποδομών στον κυβερνοχώρο, η οργάνωση κατάλληλα εκπαιδευμένης στρατιωτικής δύναμης με στόχο την επικράτηση στα ψηφιακά πεδία μάχης, η αποτροπή τρομοκρατικών ενεργειών, η μείωση της εθνικής επιφάνειας προσβολής για τους επιτιθέμενους στον κυβερνοχώρο, μέσω μόχλευσης συνδυαστικά νομικών εργαλείων και πολιτικών επιλογών, και όλα αυτά με παρεμβάσεις οι οποίες δεν θα ανασχέσουν την καινοτομία.

Η κυρίαρχη τρέχουσα αντίληψη περί κυβερνοϊσχύος περιορίζεται στο να εστιάζει συνδυαστικά κυρίως στις δυνατότητες καταστροφής που παρέχουν, εάν πράγματι παρέχουν, τα κυβερνοόπλα για συγκεκριμένους κρατικούς δρώντες και στην αποτύπωση μιας κατάταξης της κυβερνοϊσχύος των υπόψιν δρώντων, από αμφίβολης όμως αξιοπιστίας ποσοτικούς ή ποιοτικούς δείκτες. Φαίνεται να μην είναι σε θέση να διακρίνει τη διαφορά μεταξύ πραγματικών δυνατοτήτων προβολής κυβερνοϊσχύος και προθέσεων προβολής, ενώ επιπροσθέτως η διαδικασία αυτή καθεαυτή δεν παρέχει την παραμικρή ένδειξη διαφορών στην προβολή ισχύος σε διαφορετικές περιπτώσεις, ή ισοδύναμα η απόσταση που χωρίζει δύο αξιολογούμενους είναι ομοιόμορφα ίδια για κάθε τους δυνατότητα. Αυτό που απαιτείται είναι μια ολιστική προσέγγιση στη δημιουργία μιας κατάταξης κυβερνοϊσχύος με πρωτεύοντα χαρακτηριστικά την ενάργεια και τη μεθοδολογική αξιοπιστία, ώστε να αποτυπώνεται αμερόληπτα η υπάρχουσα κατάσταση αλλά και οι τυχόν υποβόσκουσες τάσεις, προς άντληση αξιοποιήσιμων πληροφοριών.

Η πρώτη προσπάθεια το έτος 2020, η οποία τιτλοφορήθηκε "Κατάταξη Εθνικής Κυβερνοϊσχύος 2020: Μεθοδολογία και αναλυτικές θεωρήσεις"[73], αφορούσε στην κατάταξη δέκα (10) κρατών ως προς την ικανότητα (που χωρίς τυπική αυστηρότητα αποτελούσε παράγωγο μέγεθος δύο μεταβλητών και συγκεκριμένα της δυνατότητας και της πρόθεσης) επίτευξης επτά (7) ΑΝΣΚ (Voo et al., 2020, pp. 2, 30). Η δεύτερη προσπάθεια το 2022, που τιτλοφορήθηκε "Κατάταξη Εθνικής

[73] Απόδοση ελληνιστί του "National Cyber Power Index: Methodology and Analytical Considerations".

Κυβερνοϊσχύος 2022" (NCPI) αφορούσε στην κατάταξη τριάντα (30) κρατών ως προς την ικανότητα επίτευξης οκτώ (8) ΑΝΣΚ[74].

Απώτερος στόχος του έργου της διεπιστημονικής ομάδας ήταν να γίνει κατανοητό ότι το αποτύπωμα της κυβερνοϊσχύος είναι ευρύτερο της καθημερινής διαπάλης επίτευξης εθνικής κυβερνοασφαλείας και πως η βέλτιστη αξιοποίησή της απαιτεί μια εκ βάθρων επαναπροσέγγιση, καθόσον οι κυβερνοδυνατότητες δεν είναι τίποτε άλλο παρά ένα ακόμη εργαλείο στην κρατική εργαλειοθήκη (Voo et al., 2022, p. 1). Αυτή η οπτική συνεπάγεται ότι αφενός η Ελλάδα θα πρέπει να διοχετεύει κατάλληλα τις πηγές κυβερνοϊσχύος της, προς εξυπηρέτηση των τεθέντων από την Πολιτεία εθνικών ΑΝΣΚ και αφετέρου ότι ο κυβερνοχώρος θα πρέπει να αναπλαστεί κατάλληλα, μέσω νορμών, για οριοθέτηση των διεθνών εμπλοκών. Το οξύμωρο της σήμερον ημέρας είναι πως ενώ οι κρατικοί δρώντες φαίνεται να αντιλαμβάνονται τον κρίσιμο ρόλο ανάπτυξης και αποτελεσματικής χρήσης της κυβερνοϊσχύος, στην κατεύθυνση της παροχής κυβερνοασφάλειας, και ενώ η τεχνολογία εμποτίζει όλο και βαθύτερα την κοινωνική σφαίρα, παρά ταύτα ολοένα και αυξάνονται σε απόλυτους αριθμούς και σε βαρύτητα τα κυβερνοπεριστατικά που λαμβάνουν χώρα στον

[74] Αυτοί είναι: α) Επιτήρηση και παρακολούθηση εγχώριων ομάδων, περιλαμβάνει την ύπαρξη νομικού πλαισίου για την παρακολούθηση πολιτών εντός συνόρων και αντικατασκοπεία. β) Ενδυνάμωση και ενίσχυση εθνικής κυβερνοάμυνας, περιλαμβάνει ενεργητική άμυνα, κυβερνοασφάλεια και προώθηση πολιτικών κυβερνο-υγιεινής. γ) Έλεγχος και χειραγώγηση πληροφοριακού περιβάλλοντος, περιλαμβάνει αλλαγή αφηγήματος εγχώρια και στο εξωτερικό, παραπληροφόρηση προπαγάνδα και στοχοποίηση ομάδων (πχ τρομοκρατών) εκτός εδαφικής διακαιοδοσίας. δ) Συλλογή πληροφοριών εκτός συνόρων για λόγους Εθνικής Ασφαλείας. ε) Επαύξηση εθνικής ικανότητας στον κυβερνοχώρο και στην εμπορική τεχνολογία, περιλαμβάνει τη χρήση νόμιμων ή έκνομων μέσων (πχ βιομηχανική κυβερνοκατασκοπεία) εκτός συνόρων και την ενίσχυση της κυβερνοασφάλειας στο εσωτερικό. στ) Καταστροφή ή απενεργοποίηση υποδομών και δυνατοτήτων του εχθρού, περιλαμβάνει διεξαγωγή επιθετικών επιχειρήσεων κυβερνοχώρου για αποτροπή, διάβρωση, υποβάθμιση του αντιπάλου να μάχεται στον κυβερνοχώρο ή στα άλλα συμβατικά πεδία. ζ) Καθορισμός νορμών και τεχνικών προτύπων. η) Συσσώρευση πλούτου ή/και εξόρυξη κρυπτονομισμάτων, περιλαμβάνει την κλοπή δια της χρήσης κυβερνομέσων (ransomware, εκβιασμοί με δεδομένα από κυβερνοεπιθέσεις ή διαρροές κτλ) (Voo et al., 2022, pp. 5-6).

κυβερνοχώρο[75]. Η ωμή αλήθεια είναι πως όσο περισσότερο διασυνδεδεμένοι γινόμαστε, τόσο πιο ελκυστικές θα γίνονται οι κυβερνοεπιθέσεις από τα κράτη προκειμένου να επαυξήσουν την κυβερνοϊσχύ τους.

Σύμφωνα με την οπτική του Harvard η αφηρημένη θεωρητική έννοια της εθνικής κυβερνοϊσχύος δύναται να καταστεί απτή νοηματοδοτούμενη ως σύνθεση της ικανότητας επίτευξης από τους κρατικούς δρώντες εντός και μέσω του κυβερνοχώρου των οκτώ (8) προαναφερθέντων απολύτως διακριτών ΑΝΣΚ (Voo et al., 2022, p. 2). Αυτό που πρέπει να καταστεί σαφές είναι ότι οι κρατικοί δρώντες μέσω της προβολής της κυβερνοϊσχύος τους δεν επιδιώκουν αποκλειστικά να καταστρέψουν ή να αχρηστεύσουν τις υποδομές και τις δυνατότητες του αντιπάλου. Μια τέτοια οπτική είναι ίσως μερικώς σωστή και μόνον εν πολέμω, εν ειρήνη όμως είναι περιοριστική και παραπλανητική. Η προβολή κυβερνοϊσχύος μπορεί επιπλέον να αφορά σε ενδυνάμωση και σε ενίσχυση της εθνικής κυβερνοάμυνας, στη συλλογή πληροφοριών, στην επαύξηση της εθνικής ανταγωνιστικότητας στην κυβερνοτεχνολογία, στην επαύξηση της εθνικής εμπορικής ανταγωνιστικότητας, στο έλεγχο και στη χειραγώγηση του πληροφοριακού περιβάλλοντος και τέλος στην επέκταση της επιρροής τους μέσω καθορισμού τεχνικών προδιαγραφών και διεθνών νορμών στον κυβερνοχώρο.

Στην "Κατάταξη Εθνικής Κυβερνοϊσχύος 2022" έχουν καθοριστεί συνολικά εικοσιεννέα (29) ενδείκτες δυνατοτήτων και τριάντα δύο (32) ενδείκτες πρόθεσης επί των οκτώ (8) ΑΝΣΚ. Πρέπει να επισημανθεί, προς αποφυγή τυχόν παρερμηνειών, ότι το όλο σχήμα κατάταξης της εθνικής κυβερνοϊσχύος βασίζεται σε δημόσια διαθέσιμα και μόνον στοιχεία (Voo et al., 2022, p. 3). Κι αυτό διότι όταν ένας κρατικός δρων διενεργεί κυβερνοεπιθέσεις, εκμεταλλευόμενος την ανωνυμία του κυβερνοχώρου, επισήμως πάντοτε αρνείται κάθε ανάμιξη, καθώς εάν μεν η επίθεση απέτυχε δεν

[75] Ίσως το πλέον γνωστό πρόσφατο κυβερνοπεριστατικό είναι το "Colonial Pipeline Ransomware Attack" το οποίο είναι το σοβαρότερο διαχρονικά περιστατικό, εκ των ανακοινωθέντων τουλάχιστον, προσβολής υποδομών στις ΗΠΑ. Ο αγωγός καυσίμου (βενζίνης), ο οποίος ετέθη εκτός λειτουργίας συνεπεία της προσβολής από 7-12/5/2021, τροφοδοτούσε το νοτιανατολικό τμήμα των ΗΠΑ. Η ιδιοκτήτρια εταιρεία αναγκάσθηκε να καταβάλει λύτρα αξίας 4,4 εκ. $ στους εισβολείς αφού προεκλήθη έλλειψη καυσίμου σε έξι (6) Πολιτείες. Ο Πρόεδρος Biden εξέδωσε στις 12/5/2021 Διάταγμα, περί προληπτικών μέτρων ενίσχυσης της κυβερνοασφάλειας (Kerner, 2022).

θέλει να του χρεωθεί έστω και υποψία αδυναμίας, ενώ εάν είναι επιτυχημένη η αποποίηση της ανάληψης ευθύνης ισοδυναμεί με αποφυγή επιβολής οιασδήποτε νομικής συνέπειας. Το αντίστροφο ισχύει από την πλευρά του αποδέκτη της επιθετικής ενέργειας. Άρα, η υπόθεση εργασίας είναι πως τα παγκοσμίως δημόσια διαθέσιμα στοιχεία εκτός από ενδεικτικά είναι και αναλογικά αντιπροσωπευτικά των εθνικών δυνατοτήτων και προθέσεων. Είναι η κορυφή μόνον του παγόβουνου για έναν κρατικό δρώντα, αλλά αφού ισχύει για όλους τότε είναι αρκετό προκειμένου να εξαχθεί μια αξιόπιστη διεθνής κατάταξη και να παραχθούν χρήσιμα συμπεράσματα για τους λήπτες αποφάσεων.

Μεθοδολογία υπολογισμού του μοντέλου *NCPI-22*

Μεθοδολογικά η αποτίμηση της εθνικής πρόθεσης στην επιδίωξη επίτευξης κάθε ΑΝΣΚ συνάγεται ως συνεκτίμηση των εκδοθέντων εθνικών στρατηγικών, της δημόσιας ρητορικής και της ευλογοφανούς υποψίας ανάμιξης σε διενεργηθείσες κυβερνοεπιχειρήσεις (Voo et al., 2022, p. 7). Άμεσα συνάγεται ότι υπολογισμός χαμηλής επίδοσης στην πρόθεση επίτευξης ενός ΑΝΣΚ συνεπάγεται ότι η επιδίωξη επίτευξής του είναι χαμηλής προτεραιότητας από τον δρώντα. Αντίστοιχα με την εθνική πρόθεση και η αποτίμηση εθνικών δυνατοτήτων εκτιμάται ανά ΑΝΣΚ. Οι αντίστοιχοι ενδείκτες είτε εισφέρουν απευθείας στην εθνική κυβερνοϊσχύ είτε αντιπροσωπεύουν δύσκολα αποτιμώμενες δυνατότητες. Στο σημείο αυτό επισημαίνεται ότι η όλη διαδικασία, άρα και η τελική κατάταξη, δεν αποτιμά τεχνικές δυνατότητες και δεν λαμβάνει με κανέναν τρόπο το πόσο προηγμένη τεχνολογικά είναι μια κυβερνοεπίθεση και αυτό γιατί τελικά η πολυπλοκότητά της εξαρτάται από το στόχο (Voo et al., 2022, p. 8). Επιπλέον, το μοντέλο είναι σε θέση να συνεκτιμήσει περιπτώσεις που τα κράτη επιδιώκουν περισσότερους από έναν ΑΝΣΚ στην ίδια κυβερνοεπιχείρηση, ενώ επιπροσθέτως η έννοια του βάρους, δηλαδή της σταθμισμένης συμμετοχής των δυνατότητων ανά ΑΝΣΚ στο τελικό αποτέλεσμα

επιτυγχάνεται εμμέσως από τις τιμές της εθνικής πρόθεσης.[76, 77] Τελικά, ο τύπος υπολογισμού "Κατάταξης Εθνικής Κυβερνοϊσχύος 2022" (*NCPI*) είναι ο:[78]

$$(NCPI) = \frac{1}{8}\sum_{i=1}^{8} \text{Δυνατότητες}_x \times \text{Πρόθεση}_x$$

Η εθνική κυβερνοϊσχύς στο μικροσκόπιο του μοντέλου *NCPI-22*

Όπως έχει ήδη αναφερθεί ανωτέρω το μοντέλο χρησιμοποιεί υποσύνολα από δύο δεξαμενές ενδεικτών, συγκεκριμένα από τριάντα δύο (32) ενδείκτες πρόθεσης και εικοσιεννέα (29) ενδείκτες δυνατοτήτων, επί οκτώ (8) ΑΝΣΚ και επί συγκεκριμένου συνόλου υπό εξέταση κρατικών δρώντων, προκειμένου να υπολογίσει τη μεταξύ τους κατάταξη ως προς την κατοχή κυβερνοϊσχύος. Πλέον όμως της εξαγόμενης λίστας κατάταξης, η οποία αποτελούσε τον ευθύς εξαρχής κεντρικό στόχο, είναι σε θέση να παράξει επιπλέον τα εξής προϊόντα ανάλυσης: αποτελέσματα κατάταξης προθέσεων των δρώντων ανά ΑΝΣΚ (Voo et al., 2022, pp. 29-30), αποτελέσματα κατάταξης δυνατοτήτων των δρώντων ανά ΑΝΣΚ (Voo et al., 2022, pp. 27-28), αποτελέσματα

[76] Προκειμένου να προκύψουν τα στοιχεία που θα αποτελέσουν τις "εθνικές μεταβλητές" του τύπου ακολουθούνται επιπλέον οι εξής συμβάσεις: όταν λείπουν στοιχεία, τότε συμπληρώνονται εκτιμώμενες τιμές τους από παρόμοια κράτη (ως μέτρα ομοιότητας χρησιμοποιούνται ο πληθυσμός, το μέγεθος, η οικονομική δύναμη και η γεωγραφία), αλλιώς οι ενδείκτες εξαιρούνται. Στους ενδείκτες εκ κατασκευής μεγαλύτερη τιμή τους αντιστοιχεί με μεγαλύτερη επίδοση κυβερνοϊσχύος. Τα σύνολα των αρχικώς υπολογισθέντων τιμών για τους ενδείκτες δυνατοτήτων για όλα τα κράτη ανάγονται ανά ενδείκτη σε νέα σύνολα τιμών ενδεικτών δυνατοτήτων κατόπιν μαθηματικής min - max κανονικοποίησης με νέο διάστημα ανάθεσης τιμών το [0,1]. Εν συνεχεία, για κάθε κράτος υπολογίζεται ο μέσος όρος των κανονικοποιημένων ενδεικτών δυνατοτήτων ανά ΑΝΣΚ. Τέλος, αυτός ο μέσος όρος ανά ΑΝΣΚ και ανά κράτος εισάγεται στον τύπο και πολλαπλασιάζεται με την πρόθεση ανά ΑΝΣΚ του υπόψιν κράτους (Voo et al., 2022, pp. 18-20).

[77] Επισημαίνεται ότι ο μετρικός χώρος του υπόψιν μοντέλου δεν έχει τις ιδιότητες του Ευκλείδειου χώρου, δηλαδή ο λόγος δύο μετρικών δεν έχει φυσικό νόημα. Οπότε λ.χ. διπλάσια εξαγώμενη αποτίμηση δεν συνεπάγεται διπλάσια κυβερνοϊσχύ, με παρόμοια λογική που οι 2°C δεν είναι διπλάσια θερμοκρασία από τον 1°C, είναι απλώς μεγαλύτερη κατά ένα βαθμό της κλίμακας °C.

[78] Παρέλκει η επισήμανση ότι πρόκειται για το φαινότυπο της εθνικής κυβερνοϊσχύος. Μόνον ο ίδιος ο εθνικός δρων γνωρίζει τις πραγματικές του προθέσεις και δυνατότητες σε δεδομένη χρονική στιγμή.

κατανομής της εθνικής κυβερνοϊσχύος με γραφήματα τύπου ραντάρ ανά δρώντα (Voo et al., 2022, pp. 20-25) και διάγραμμα διασποράς στο οποίο αποτυπώνονται οι διαφορές κυβερνοϊσχύος των κρατικών δρώντων με άξονες ανάλυσης δυνατότητες έναντι πρόθεσης (Voo et al., 2022, p. 26). Αποτελεί εκ κατασκευής ανελαστική απαίτηση για λειτουργική χρήση του μοντέλου ο καθορισμός συνόλου κρατικών δρώντων.[79]

Όμως ένα τόσο πολυκριτηριακό αναλυτικό μοντέλο υπολογισμού θα μπορούσε να χρησιμοποιηθεί εκ παραλλήλου και ως οδηγός για την αποτύπωση της τρέχουσας κατάστασης της εθνικής κυβερνοϊσχύος και εν συνεχεία ως οδικός χάρτης για την επαύξησή της στην επιθυμητή κατεύθυνση μέσω βελτίωσης των τιμών των αντιστοίχων ενδεικτών. Στα Παραρτήματα «Δ» και «Ε» παρατίθενται στοιχεία τα οποία συνελέγησαν από δημόσια διαθέσιμα πηγές, και σύμφωνα με τον εν λόγω μοντέλο, για την αποτύπωση της ελληνικής πραγματικότητας.[80] Λόγω του μεγάλου πλήθους των ενδεικτών θα παρατεθούν εν συνεχεία επιλεκτικά οι σημαντικότεροι εξ αυτών, ήτοι αυτοί που παρέχουν σημαντικά περιθώρια βελτίωσης, αυτοί που φέρουν ήδη υψηλές τιμές και θα πρέπει να τις διατηρήσουν και αυτοί που έχουν κρίσιμο ειδικό βάρος.

Σε ό,τι αφορά στον ενδείκτη περί "επίγνωσης της κυβερνοασφάλειας και του ψηφιακού αναλφαβητισμού", ο οποίος εν ολίγοις αποτυπώνει τις πρακτικές κυβερνοϋγιεινής του γενικού πληθυσμού, η Ελλάδα κατατάσσεται 41^{η} παγκοσμίως με τον δείκτη να επιβαρύνεται από τις αστοχίες του εκπαιδευτικού συστήματος και της αγοράς εργασίας, που κατατάσσονται 47^{ο} και 48^{η} αντίστοιχα στις ανάλογες κλίμακες αξιολόγησης (OliverWymanForum.com, 2021). Ενδεικτικό της κατάστασης στην κυβερνοϋγιεινή για τον ελληνικό κυβερνοχώρο αποτελεί το γεγονός ότι το "ποσοστό των μολυσμένων με κακόβουλο λογισμικό Η/Υ" το 2022 άγγιξε το εντυπωσιακό

[79] Κατά παρέκκλιση και εκφυλιστικά, κατ' εκτίμηση του γράφοντος, θα μπορούσε ίσως να χρησιμοποιηθεί το μοντέλο για έναν (1) κρατικό δρώντα με εισαγωγή διαχρονικών στοιχείων του, προκειμένου να διαπιστωθούν διαχρονικές τάσεις ή μεταβολές της οικείας κυβερνοϊσχύος.

[80] Το μοντέλο περιλαμβάνει σημαντικό αριθμό ενδεικτών οι οποίοι στην περίπτωση της εν λόγω δημοσίευσης υπολογίστηκαν οίκοθεν. Αυτοί οι ενδείκτες δεν συμπεριελήφθησαν στα υπόψιν Παραρτήματα, καθόσον εκτιμάται ότι η καθορισμός τους εκφεύγει του σκοπού του παρόντος πονήματος.

11,80% ωθώντας την Ελλάδα στη 10η θέση της σχετικής παγκόσμιας κατάταξης (SecureList.com, 2022). Κι αυτό τη στιγμή που ενδείκτης "ποσοστό % του πληθυσμού που χρησιμοποιεί το διαδίκτυο" και ο ενδείκτης "ποσοστό % του πληθυσμού που χρησιμοποιεί μέσα κοινωνικής δικτύωσης" έχουν σκαρφαλώσει στο 78,49% (The World Bank, 2023d) και στο 72,3% (datareportal.com, 2023, p. 168), αρκετά πάνω από το Μέσο Όρο, καθιστώντας το γενικό πληθυσμό εύκολο στόχο σε εκστρατείες παραπληροφόρησης και κυβερνοκατασκοπείας. Προφανή μέτρα βελτιώσεως των δεικτών συνιστούν διαρκείς εκστρατείες ενημέρωσης και ευαισθητοποίησης του γενικού πληθυσμού και η εισαγωγή αντιστοίχων αντικειμένων εκπαίδευσης σε όλες τις βαθμίδες Εκπαιδεύσεως ως και στους χώρους εργασίας.

Σε ό,τι αφορά τον ενδείκτη "νομοθεσίας περί προσωπικών δεδομένων και ψηφιακής διακυβέρνησης", ο οποίος τυγχάνει να αποτελεί ενδείκτη πρόθεσης αλλά και δυνατοτήτων, η Ελλάδα δια του ΕΚ 679/2016, γνωστού και ως Κανονισμού GDPR, ανήκει ήδη στο κλειστό προνομιακό κλαμπ χωρών με πολύ αυστηρό νομοθετικό πλαίσιο προστασίας (DLAPIPER, 2023).

Από την άλλη, ο ενδείκτης "ηλεκτρονικού εμπορίου ως ποσοστού του ΑΕΠ", ακόμη και κατά την περίοδο της ενσκύψασας πανδημίας του COVID19, ήταν πολύ κάτω του Μέσο Όρου του Δυτικού Κόσμου στο 6,8%, ενδεικτικά την ίδια περίοδο το Ηνωμένο Βασίλειο ήταν στο 31,7% (IMF.org, 2022). Συνεπώς, η τάση στο άμεσο μέλλον είναι άνευ απροόπτου να αγγίξει διψήφια νούμερα. Εάν η βελτίωση της κυβερνοϋγιεινής δεν αποτελέσει άμεση προτεραιότητα των εφαρμοζόμενων πολιτικών ασφαλείας τότε αναπόφευκτα θα υπάρξει αύξηση του ποσοστού των "μολυσμένων" με κακόβουλο λογισμικό Η/Υ, με συνεπακόλουθη μείωση των ενδεικτών κυβερνοασφαλείας στον εθνικό κυβερνοχώρο.

Από τη λίστα των διαχρονικά εξεταζόμενων εβδομήντα (70) χωρών για την κατάταξή τους ως προς την "ελευθερία στο διαδίκτυο" απουσιάζει η Ελλάδα. Πλην όμως, θα μπορούσαμε να εικάσουμε ευλογοφανώς, βάσει των αναγραφομένων στην οικεία Έκθεση Αναφοράς, ότι η αποδιδόμενη τιμή για την Ελλάδα είναι πέριξ των τιμών 73-74 της κλίμακας μέτρησης (statista, 2023). Ένας τέτοιος δείκτης, περίπου στο Μέσο Όρο του Δυτικού Κόσμου, δεικνύει μειωμένες δυνατότητες ελέγχου στην πληροφοριακή ροή του διαδικτύου από το κράτος. Ακόμη όμως κι αν αυτό αποτελεί απολύτως συνειδητή πολιτική ή ιδεολογική επιλογή, αναγκαιεί για λόγους Εθνικής

Ασφαλείας (αποφυγή εργαλειοποίησης του διαδικτύου για πληροφοριακό πόλεμο από τον εχθρό, διοχέτευση εθνικού αφηγήματος κτλ) ο σχεδιασμός ελέγχου για την ενεργοποίησή του σε περιόδους θερμών κρίσεων ή πολέμου.

Αρκεί μια προσεκτική παρατήρηση στον ενδείκτη "ήπιας ισχύος" για να διαπιστώσει οποιοσδήποτε ότι η Ελλάδα με τιμή κλίμακας 40 υπολείπεται της Τουρκίας, ακόμη και του Κατάρ, τη στιγμή που οι μεσογειακές Ισπανία και Ιταλία φλερτάρουν με το 55 (BrandFinance, 2023). Εξωστρέφεια, προώθηση τουριστικού προϊόντος και πολιτισμού αποτελούν μέρος μόνον των δράσεων με τις οποίες η Ελλάδα δύναται να αναβαθμίσει τη θέση της.

Στους πιο απαιτητικούς ενδείκτες του "ποσοστού των προϊόντων υψηλής τεχνολογίας επί του συνόλου των εξαγωγών" και του "ποσοστού των προϊόντων Τεχνολογίας Πληροφορικής και Επικοινωνιών"[81] οι τιμές 6,11% (The World Bank, 2023a) και 5,6% (The World Bank, 2023b), με διαχρονική τάση ανόδου, αντίστοιχα από κοινού με τα φτωχά ευρήματα του ενδείκτη "κατοχύρωσης διπλωμάτων ευρασιτεχνίας" (The World Bank, 2023c), μόλις 400 το έτος 2020, δεν αφήνουν περιθώρια για εφησυχασμό. Αποδεικνύουν τον υψηλό βαθμό εξάρτησης σε προϊόντα υψηλής τεχνολογίας από τρίτους, γεγονός το οποίο εξωθεί σε κίνδυνο αναστολής των εθνικών κυβερνοδυνατοτήτων, απομείωση επιλογών από εθνικές δεξαμενές υψηλής τεχνολογίας και τρωτότητα των εθνικών κυβερνοϋποδομών από πιθανώς κακόβουλο μη εθνικό προμηθευτή. Αποκαλυπτικό της δυσχερούς κατάστασης είναι το γεγονός δεν υπάρχει ούτε μια ιδιωτική ελληνικών συμφερόντων εταιρία, σύμφωνα με τον αντίστοιχο ενδείκτη, που να παρέχει δυνατότητες επιτήρησης στον κυβερνοχώρο. Η προσπάθεια ανάταξης οφείλει να αποτελεί κεντρικό πολιτικό σχεδιασμό και να περιλαμβάνει κατ΄ελάχιστον ενίσχυση της υγιούς επιχειρηματικότητας στην υπόψιν κατεύθυνση, προώθηση συμπαραγωγής προϊόντων υψηλής τεχνολογίας τους κορυφαίους του χώρου και μεθόδευση αντισταθμιστικού οφέλους ει δυνατόν σε κάθε κρατική προμήθεια.

Σε ό,τι αφορά στον ενδείκτη ύπαρξης "Εθνικής Διοίκησης Κυβερνοχώρου", προκειμένου ως κεντρικοποιημένη Αρχή να προσδώσει στην ελληνική Πολιτεία την ικανότητα να χαλιναγωγήσει τις πολλαπλές εθνικές κυβερνοδυνατότητες και να

[81] Απόδοση ελληνιστί του όρου Information and Communications Technology (ICT).

εμπλέξει στρατιωτικά μέσα όταν απαιτηθεί η απάντηση είναι αρνητική. Η Ελλάδα δεν διαθέτει στρατιωτική Διοίκηση Κυβερνοχώρου, αλλά μια επιπέδου Διεύθυνσης σε Επιτελείο οντότητα της οποίας το κύριο έργο είναι επιτελικό σε επιχειρησιακό επίπεδο και όχι σε στρατηγικό.

Σε ό,τι αφορά στους ενδείκτες πρόθεσης, δεν έχει αποδοθεί κυβερνοεπίθεση στην Ελλάδα (Council on Foreign Relations, 2023). Ο στρατηγικός σχεδιασμός αναγνωρίζει ότι το κράτος έχει δυνατότητες να ελέγξει και χειραγωγήσει το πληροφοριακό περιβάλλον, ενώ η Ελλάδα διαθέτει στρατιωτική μονάδα για τον κυβερνοχώρο με την οποία συμμετέχει σε πολυμερείς ασκήσεις, όμως δεν ανευρέθησαν αναφορές σε ανοιχτές πηγές για την εκπόνηση σχεδίου ενεργητικής άμυνας. Επιπροσθέτως, αν και η Ελλάδα την τελευταία δεκαετία εξέδωσε πλήθος θεσμικών κειμένων μεγάλο μέρος του χρήζει επικαιροποίησης, ενώ σημαντικό θεσμικό έλλειμμα συνιστά η μη κατάρτιση Εθνικής Στρατηγικής Κυβερνοχώρου. Τέλος, η Ελλάδα είναι μέλος σε διάφορα τεχνικά φόρα, δεν συμμετέχει όμως σε υψηλού επιπέδου τεχνικές επιτροπές (UNIDIR, 2017, p. 17; Internet Governance Forum, 2023; GFCE, 2023; ISO.org, 2023; ITU, 2023; CommonCriteria.org, 2023; IECEE.ord, 2023).

Συμπεράσματα

Στα χαρακτηριστικά της κυβερνοϊσχύος εμπεριέχονται καινοφανή ως προς τη διεξαγωγή ενός πολέμου χαρακτηριστικά. Η ατοπικότητα και η μη απτότητα του κυβερνοχώρου, η εφικτότητα εκτέλεσης επιχειρήσεων ακόμη και από μεμονωμένα άτομα και η πρακτικώς από πολύ δύσκολη έως αδύνατη απόδοση ευθύνης. Στα προηγούμενα, σε αντίθεση με την κλασική στρατιωτική ισχύ, προστίθεται η δυνατότητα προβολής της υπό τη μορφή καθημερινού πληροφοριακού πολέμου στον κυβερνοχώρο. Οπότε, καθίσταται προφανές ότι αποτελεί διακύβευμα ζωτικής σημασίας για την Εθνική Άμυνα της χώρας η ασφαλής και αξιόπιστη χρήση του κυβερνοχώρου.

Για τη στρατηγική θεώρηση, η ιδιαίτερη φύση της κυβερνοϊσχύος, ανεξαρτήτως του ότι δεν προκαλεί άμεση θανατηφόρα βία, αποτελεί μια επιπλέον κατηγορία όπλου, αφού ως τέτοιο ορίζεται οιοδήποτε μέσο δύναται κατά τη χρήση του να προκαλέσει βλάβη στον αντίπαλο. Αδιαμφισβήτητα πολύ πιο τεχνικό, πιο διαβρωτικό και ενοχλητικά πανταχού παρόν σε σχέση με τα ήδη γνωστά κινητικά όπλα, αλλά πάντως όπλο κατατασσόμενο στις ασαφείς μορφές εθνικής ισχύος.

Καίτοι η κυβερνοϊσχύς είναι μια εντυπωσιακή, μη οικεία και πολλά υποσχόμενη μορφή ισχύος ο λειτουργικός της ρόλος δεν είναι διόλου καινοφανής στην ιστορία της στρατηγικής. Εύκολα διαπιστώνεται η ύπαρξη μιας longue durée συναφούς έννοιας που δεν είναι άλλη παρά η πληροφορία από κοινού με την επικοινωνία της. Συνεπώς, λειτουργικά η κυβερνοϊσχύς δεν αφορά σε αυτούς καθεαυτούς στους ηλεκτρονικούς υπολογιστές και στα δίκτυά τους αλλά είναι στο τι δύνανται να εκτελέσουν οι δικτυωμένοι ηλεκτρονικοί υπολογιστές ως προς τη διαμοίραση της πληροφορίας και ποιες μπορεί να είναι οι συνέπειες.

Στρατηγικά η κυβερνοϊσχύς δεν αφορά στην τεχνολογία και στην επιστήμη. Και αυτό γιατί κατά τον Κλαούζεβιτς ο πόλεμος δεν συμβαίνει για αυτά καθεαυτά τα χαρακτηριστικά του αλλά συνεπεία της πολιτικής. Συνεπώς, το αντικείμενο της στρατηγικής είναι ο ίδιος ο πόλεμος όχι τα μέσα διεξαγωγής. Άρα, η κυβερνοϊσχύς δεν αφορά στην τεχνολογία και στην επιστήμη, όπως και η αεροπορική ισχύς δεν

αφορά την αεροναυτική και η πυρηνική ισχύς δεν αφορά στην κβαντική φυσική. Και οι τρεις πρόσφατες Επαναστάσεις στις Στρατιωτικές Υποθέσεις, αεροπορική ισχύς - πυρηνική ισχύς - κυβερνοϊσχύς, σχετίζονται με την πολιτική και τις παραγόμενες πολιτικές.

Έπεται ότι δια της κυβερνοϊσχύος οι στρατηγιστές διεκπεραιώνουν αυτό που θέλουν μακράν ταχύτερα, σε μεγαλύτερες αποστάσεις και πιο κεκαλυμμένα από ότι γινόταν μέχρι την άφιξή της. Συναφώς, ως προς τη στρατηγική της σημασία συνάγεται ότι μάλλον πρόκειται για διαφορετικό είδος ισχύος από τα άλλα είδη και πιθανόν απλά να πρόκειται απλώς για έναν "ομαδικό παίκτη" στο διαρκώς εξελισσόμενο συνδεδυασμένο και πιθανώς ενοποιημένο αφήγημα διεξαγωγής πολέμου.

Στο θεσμικό επίπεδο σε παγκόσμια κλίμακα, και παρά τη φαινομενική κινητικότητα της διεθνούς κοινότητας προς διευθέτηση των προβληματικών της κυβερνοϊσχύος, οι πλείστες εξ αυτών σχετιζόμενες με την προβολή κρατικής κυβερνοϊσχύος επί ετέρων κρατικών δρώντων παραμένουν ανοιχτά ζητήματα, διότι οι κύριοι δρώντες του διεθνούς συστήματος εμφανίζονται από απρόθυμοι έως διστακτικοί να θεσπίσουν αυστηρά κανονιστικά όρια στον κυβερνοχώρο.

Η τρέχουσα τάση της νομικής ρύθμισης του κυβερνοχώρου lex lata, συνιστά απλώς μια κατ’ επίφαση απόπειρα εφαρμογής της "κανονικότητας" Δικαίου στη "μη κανονικότητα" του κυβερνοχώρου. Προφανώς, η προβολή κυβερνοϊσχύος δεν διενεργείται σε νομικό κενό, έως όμως τη διεθνή αποδοχή ειδικού "κυβερνοδικαίου" η προβολή κυβερνοϊσχύος θα τελεί de facto σε μια ιδιότυπη προνομιακή κατάσταση γυμνή εξουσίας, με τους κρατικούς δρώντες, εκμεταλλευόμενους τη συγκυρία, να προσπαθούν να διατηρήσουν ή να επαυξήσουν το βάθος του επιχειρησιακού τους αποτυπώματος. Η Ελλάδα οφείλει να ακολουθεί το διεθνές υπόδειγμα και να εξελίσσει τις δυνατότητες της ελληνικής κυβερνοϊσχύος με τέτοιον τρόπο, ώστε χωρίς να παραβιάζει το διεθνές δίκαιο να εκμεταλλεύεται με τον καλύτερο δυνατό τρόπο το momentum προς εξυπηρέτηση των εθνικών συμφερόντων.

Το αποτύπωμα της κυβερνοϊσχύος είναι ευρύτερο της καθημερινής διαπάλης επίτευξης εθνικής κυβερνοασφαλείας και οι παρεχόμενες δια τις κυβερνοϊσχύος κυβερνοδυνατότητες δεν είναι τίποτε άλλο παρά περισσότερα εργαλεία στην κρατική εργαλειοθήκη. Η Ελλάδα οφείλει να διοχετεύει κατάλληλα τις πηγές κυβερνοϊσχύος της, προς εξυπηρέτηση των τεθέντων από την Πολιτεία εθνικών ΑΝΣΚ.

Χρησιμοποιώντας το πολυκριτηριακό αναλυτικό μοντέλο υπολογισμού κατάταξης κυβερνοϊσχύος του Πανεπιστημίου του Harvard δύναται να αποτυπωθεί η τρέχουσα κατάστασης της ελληνικής κυβερνοϊσχύος και εν συνεχεία να καταρτισθεί οδικός χάρτης για την επαύξησή της στην επιθυμητή κατεύθυνση, μέσω βελτίωσης των τιμών των αντιστοίχων ενδεικτών.

Σε μια πρώτη προσέγγιση διεγνώσθησαν κίνδυνοι, τρωτότητες αλλά και ευκαιρίες. Διεγνώσθη η ανάγκη εκδήλωσης συντονισμένων στοχευμένων πολιτικών παρεμβάσεων τόσο σε θεσμικό επίπεδο, αναψηλάφηση κειμένων και εκπόνηση Εθνικής Στρατηγικής Κυβερνοχώρου για την επίτευξη εθνικής συναντίληψης, όσο και σε επίπεδο πρακτικών πολιτικών, λ.χ. ενδεικτικά δημιουργία καθετοποιημένης Αρχής Κυβερνοχώρου με αποκεντρωμένη δομή και κεντρικό έλεγχο, ενισχυμένη παρουσία σε διεθνή fora και Οργανισμούς τυποποίησης και διαμόρφωσης του κυβερνοχώρου, ενίσχυση επιχειρηματικότητας προϊόντων υψηλής τεχνολογίας προς την κατεύθυνση τεχνολογικής αυτονομίας κτλ. Τέλος, απαιτείται η τακτή διενέργεια εκστρατειών ενημέρωσης και επιμόρφωσης του γενικού πληθυσμού.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Πηγές -βιβλιογραφία

Πηγές

Α΄ Νόμοι - Θεσμικά κείμενα

ΓΕΕΘΑ/Α' ΚΛΑΔΟΣ. (2012). *Επιχειρησιακή Σχεδίαση (ΔΚ 2-1).* Τυπογραφείο Ελληνικού Στρατού.

ΓΕΕΘΑ/ΔΔΔ. (2013). *Διακλαδικό Δόγμα Επιχειρήσεων Κυβερνοχώρου.* Τυπογραφείο Ελληνικού Στρατού.

ΓΕΕΘΑ/ΔΙΚΥΒ. (2013). *Κατευθυντήριο Πλαίσιο Ανάπτυξης Κυβερνοάμυνας στις ΕΔ.* Τυπογραφείο Ελληνικού Στρατού.

ΓΕΕΘΑ/ΔΙΚΥΒ. (2014a). *Πολιτική Κυβερνοάμυνας στις ΕΔ.* Τυπογραφείο Ελληνικού Στρατού.

ΓΕΕΘΑ/ΔΙΚΥΒ. (2014b). *Τεχνικό Σχέδιο Δράσης για την Ανάπτυξη της Κυβερνοάμυνας στις ΕΔ.* Τυπογραφείο Ελληνικού Στρατού.

ΓΕΕΘΑ/Ε΄ ΚΛ. (2018). *Εθνικός Κανονισμός Ασφαλείας.* Τυπογραφείο Ελληνικού Στρατού.

ΕΕ. Κανονισμός 679/2016. *Κανονισμός Προστασίας Προσωπικών Δεδομένων.* https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR

ΕΕ/Ευρωπαϊκή Επιτροπή. (2013). *Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο*. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

ΕΕ/Ευρωπαϊκή Επιτροπή. (2016). *Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών: Απόκριση της Ευρωπαϊκής Ένωσης.* https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης. (2008). *Σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους.* [Οδηγία]. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=%20CELEX:32008L0 114&from=EN

ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης. (2018). *Πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση 2018).* https://data.consilium. europa.eu/ doc/document/ST-14413-2018-INIT/el/pdf

ΕΕ/Συμβούλιο της Ευρωπαϊκής Ένωσης. (2022). *Στρατηγική πυξίδα για την ασφάλεια και την άμυνα.* https://data.consilium.europa.eu/doc/ document/ST-7371-2022-INIT/el/pdf

Α.Ν. 585/1945-ΦΕΚ 242/Α΄/29-09-1945. *Περί κυρώσεως του εν Αγίω Φραγκίσκω υπογραφέντος Χάρτου των Ηνωμένων Εθνών.*

Ν. 1989/1952-ΦΕΚ 124/Α΄/19-02-1952. *Περί κυρώσεως της Συνθήκης του Βορείου Ατλαντικού.*

Ν. 1786/1988-ΦΕΚ 125/Α΄/08-06-1988. Κ*ύρωση προσθέτου Πρωτοκόλλου Ι στις Συμβάσεις της Γενεύης της 12ης Αυγούστου 1949 που αναφέρονται στην προστασία των θυμάτων ενόπλων συγκρούσεων.*

Ν. 3649/2008-ΦΕΚ 39/Α΄/03.03.2008. *Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις.*

Ν. 4411/2016-ΦΕΚ 142/Α΄/03.08.2016. *Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.*

ΠΔ 325/2003-ΦΕΚ 273 Α΄/01.12.2003. *Πρόβλεψη των καταλλήλων μέτρων για τη διευκόλυνση υλοποίησης και τήρησης της Απόφασης του Συμβουλίου της Ευρωπαϊκής Ένωσης στις 19.03.2001 "Περί Εγκρίσεως των Κανονισμών Ασφαλείας του Συμβουλίου" (2001/264/ΕΚ).*

Υπουργείο Εθνικής Άμυνας (ΥΠΕΘΑ). (2015). *Λευκή Βίβλος (White Paper).* Τυπογραφείο Ελληνικού Στρατού.

Υπουργείο Ψηφιακής Διακυβέρνησης/Εθνική Αρχή Κυβερνοασφαλείας. (2020). *Εθνική Στρατηγική Κυβερνοασφαλείας 2020-2025*. Υπουργείο Ψηφιακής Διακυβέρνησης. https://mindigital.gr/wp-content/uploads/2022/11/EL-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf

CIS-Legislation. (2009). T*he agreement between the governments of state members of*

the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security. https://cis-legislation. com/document.fwx?rgn=28340

Council of Europe. (2001). *Convention on Cybercrime CETS No.: 185.* [International Treaty].

ICJ. (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).* (Judgment). https://www.icj-cij.org/ public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

ICJ. (1996). *Legality Of The Threat Or Use Of Nuclear Weapons.* (Advisory Opinion). https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

The White House. (2003). *The National Strategy to Secure Cyberspace.* The White House. https://georgewbush-whitehouse.archives.gov/ pcipb/

The White House. (2010). *National Security Strategy.* The White House. http://nssarchive.us/?page_id=8

The White House. (2011). *International Strategy for Cyberspace.* The White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

The White House. (2015). *National Security Strategy.* The White House. http://nssarchive.us/?page_id=1310

The White House. (2017). *National Security Strategy.* The White House. http://nssarchive.us/wp-content/uploads/2020/04/2017.pdf

The White House. (2018). *National Cyber Strategy.* The White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/ National-Cyber-Strategy.pdf

The White House. (2022). *National Security Strategy.* The White House. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

UN. (1977). *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I).* [United Nations — Treaty Series]. 1125. 1-17512. https://www.un.org/en/ genocideprevention/documents/atrocity-crimes/ Doc.34_AP-I-EN.pdf

UN/International Law Commission. (2001). *Responsibility of States for Internationally Wrongful Acts.* https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

UN/GA. A/RES/2625(XXV)/24-10-1970. *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.* https://digital library.un.org/record/202170

UN/GA. A/RES/3314(XXIX)/14-12-1974. *Definition of Aggression.* https://legal.un.org/avl/pdf/ha/da/da_e.pdf

UN/GA. A/RES/42/22/18-11-1987. *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations.* https://digitallibrary.un.org/record/ 152626

UN/GA. A/RES/53/70/4-12-1998. *Developments in the field of information and telecommunications in the context of international security. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement*

UN/GA. A/RES/75/240/31-12-2020. *Developments in the field of information and telecommunications in the context of international security.* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement.

UN/Security Council. S/RES/1373/28-09-2001. *Resolution 1373/adopted by the Security Council at its 4385th meeting, on 28 September 2001.* https://digital library.un.org/record/449020?ln=en

US/Department of Defense. (2011). *Strategy For Operating in Cyberspace.* Department of Defence. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyber space.pdf

US/Joint Chiefs of Staff. (2006). *The National Military Strategy for Cyberspace Operations.* Joint Chiefs of Staff. https://www.hsdl.org/?view&did=35693

US/Joint Chiefs of Staff. (2011). *Joint Operations.* Joint Chiefs of Staff. https://www.benning.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/JP%203-0.pdf

US/Joint Chiefs of Staff. (2013). *Cyberspace Operations.* Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_12r.pdf

US/Joint Chiefs of Staff. (2018a). *Cyberspace Operations.* Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_12.pdf

US/Joint Chiefs of Staff. (2018b). *Strategy (1-18).* Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/ jdn1_ 18.pdf

Β΄ Ιστοσελίδες

Aftergood, S. (2018, April 30). Strategy: Directing the Instruments of National Power. *Federation of American Scientists (FAS).* https://fas.org/blogs/secrecy/2018/04/strategy-jcs/ (πρόσβαση στις 23/03/2023).

Bazzan, B., Colombo, A., Giordano, M., Misto, G., Piro, L., & Stojsic, I. (2023, n.d.). The Physical Internet. *Politecnico Milano 1863.* https://densitydesign.github.io/teaching-dd15/course-results/es01/group04/ (πρόσβαση στις 22/03/2023).

BrandFinance. (2023, n.d.). *Global soft power index.* https://brandirectory.com/softpower/ (πρόσβαση στις 27/03/2023).

Britannica. (Encyclopedia). (2022, December 15). *Cyberwar.* https://www.britannica.com/topic/cyberwar (πρόσβαση στις 01/01/2023).

CCDCOE. (2023, n.d.). *Shanghai Cooperation Organization.* https://ccdcoe.org/organisations/sco/ (πρόσβαση στις 21/03/2023).

CommonCriteria.org. (2023, n.d.). *Members of the CCRA.* https://www.commoncriteriaportal.org/ccra/members/ (πρόσβαση στις 27/03/2023).

comparitech. (2022, September 26). *Which countries have the worst and the best cybersecurity?.* https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ (πρόσβαση στις 27/03/2023).

Council of Europe. (2014, September 29). *News.* https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/turkey-ratifies-budapest-convention (πρόσβαση στις 17/03/2023).

Council on Foreign Relations. (2023, n.d.). *Cyber Operations Tracker*. https://www.cfr.org/cyber-operations/ (πρόσβαση στις 27/03/2023).

Crovitz, G. L. (2011, June 06). *China Goes Phishing: Google uncovers Beijing's*

escalating cyber warfare. [Opinion article]. in The Wall Street Journal 6 June 2011. https://www.wsj.com/articles/SB10001424052702303657404576363374283504838 (πρόσβαση στις 01/01/2023).

Cybil. (2022, n.d.). *The Knowledge Portal for Cyber Capacity Building:Greece.* https://cybilportal.org/?s=greece (πρόσβαση στις 27/03/2023).

Data Center Map. (2023, n.d.). *Colocation Data Centers.* https://www.datacentermap.com/datacenters.html (πρόσβαση στις 23/03/2023).

datareportal.com. (2023, n.d.). *Global Overview Report*. https://datareportal.com/?utm_source=Statista&utm_medium=Data_Citation_Hyperlink&utm_campaign=Data_Partners&utm_content=Statista_Data_Citation (πρόσβαση στις 27/03/ 2023).

DLAPIPER. (2023, n.d.). *Data protection laws of the world.* https://www.dlapiperdataprotection.com/ (πρόσβαση στις 27/03/2023).

GFCE. (2023, n.d.). *Our Members.* https://thegfce.org/member-overview/ (πρόσβαση στις 27/03/2023).

Google. (2010, January 12). *A new approach to China*. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (πρόσβαση στις 01/01/2023).

Google. (2023, n.d.). *Transparency Report: Government requests to remove content - Greece.* https://transparencyreport.google.com/government-removals/government-requests/GR (πρόσβαση στις 27/03/2023).

ICJ. (2023, n.d.). *Statute of the International Court of Justice.* https://www.icj-cij.org/statute#CHAPTER_II (πρόσβαση στις 24/03/2023).

IECEE.ord. (2023, n.d.). *Member Bodies* (MB's). https://www.iecee.org/members/member-bodies (πρόσβαση στις 27/03/2023).

IMF.org. (2022, January 28). *E-commerce During Covid: Stylized Facts from 47 Economies.* https://www.imf.org/en/Publications/WP/Issues/2022/01/28/E-commerce-During-Covid-Stylized-Facts-from-47-Economies-512014 (πρόσβαση στις 27/03/2023).

Internet Governance Forum. (2023, n.d.). *MAG 2018 Members*. https://www.intgovforum.org/en/content/mag-2018-members (πρόσβαση στις 27/03/2023).

ISO.org. (2023, n.d.). *Technical Commitees: ISO/IEC JTC 1-Information technology.*

https://www.iso.org/committee/45020.html (πρόσβαση στις 27/03/2023).

ITU. (2023, n.d.). *ITU-T Study Groups (Study Period 2017-2021)*. https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx (πρόσβαση στις 27/03/2023).

Kerner, S. M. (2022, April 26). Colonial Pipeline hack explained: Everything you need to know. *WhatIs.com.* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (πρόσβαση στις 28/03/2023).

NATO. (2022a, April 01). *Cyber Defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm (πρόσβαση στις 14/03/2023).

NATO. (2022b, n.d.). *NATO 2022 Strategic Concept.* https://www.nato.int/strategic-concept/ (πρόσβαση στις 13/03/2023).

NATO/Wales Summit. (2014, September 05). *Wales Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. https://www.nato.int/cps/en/natohq/official_texts_112964.htm (πρόσβαση στις 14/03/2023).

NATO/Warsaw Summit. (2016, July 09). *Warsaw Summit Communiqué.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (πρόσβαση στις 15/03/2023).

OliverWymanForum.com. (2021, n.d.). *Cyber Risk Literacy and Education Index: Greece.* https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html#Greece (πρόσβαση στις 27/03/2023).

SecureList.com. (2022, August 15). *IT threat evolution in Q2 2022. Non-mobile statistics*. https://securelist.com/it-threat-evolution-q2-2022/107099/ (πρόσβαση στις 27/03/2023).

Shanghai Cooperation Organisation. (2022, October 05). *Member states of the Shanghai Cooperation Organisation.* https://eng.sectsco.org/20221005/915167.html (πρόσβαση στις 21/03/2023).

Schmitt, M. N. (2022, July 28). Cyber Symposium - The evolution of cyber jus ad bellum thresholds. *West Point-Lieber Institute.* https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/ (πρόσβαση στις 23/03/2023).

Shodan. (2023, n.d.). *Shodan Report:Greece.* https://www.shodan.io/search/report?query=greece (πρόσβαση στις 27/03/2023).

statista. (2023, February 10). *Degree of internet freedom in selected countries according to the Freedom House Index in 2022.* https://www.statista.com/statistics/272533/degree-of-internet-freedom-in-selected-countries/ (πρόσβαση στις 27/03/ 2023).

The World Bank. (2023a, n.d.). *High Technology exports (% of manufactured exports).* https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?view=map (πρόσβαση στις 27/03/2023).

The World Bank. (2023b, n.d.). *ICT goods imports (% total goods imports).* https://data.worldbank.org/indicator/TM.VAL.ICTG.ZS.UN (πρόσβαση στις 27/03/2023).

The World Bank. (2023c, n.d.). *Patent applications, residents.* https://data.worldbank.org/indicator/IP.PAT.RESD?end=2020&start=2020&view=map (πρόσβαση στις 27/03/2023).

The World Bank. (2023d, n.d.). *Individuals using the Internet (% of population).* https://data.worldbank.org/indicator/IT. NET.USER.ZS? view=map (πρόσβαση στις 27/03/2023).

UN/Office for Disarmament Affairs. (n.d.). *Developments in the field of information and telecommunications in the context of international security*. https://www.un.org/disarmament/ict-security/ (πρόσβαση στις 26/03/2023).

UN/Political and Peacebuilding Affairs. (n.d.). *Shanghai Cooperation Organisation*. https://dppa.un.org/en/shanghai-cooperation-organization (πρόσβαση στις 21/03/2023).

US Army/Cyber Command. (2022, November 10). *Cyberspace Terminology.* https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2686075/cybersecurity-terminology/ (πρόσβαση στις 14/03/2023).

Wall C., & Morcos P. (2021, June 11). Invisible and Vital: Undersea Cables and Transatlan tic Security. *Center for Strategic & International Studies.*

https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security (πρόσβαση στις 22/03/2023).

Βιβλιογραφία

Ελληνόγλωσση

Κολιόπουλος, Κ. (2010). *Η στρατηγική σκέψη από την αρχαιότητα έως σήμερα.* Ποιότητα.

Κουλουμπής, Θ. (2008). *Διεθνείς Σχέσεις: Ισχύς και Δικαιοσύνη.* Παπαζήσης.

Μακιαβέλι, Ν. (2012). *Ο Ηγεμόνας* (επιμ. Π. Σταύρου & μτφρ. Ν. Καζαντζάκης). Καζαντζάκη. (Το πρωτότυπο έργο εκδόθηκε το έτος 1532 μ.Χ.).

Μακρής, Β. Γ. (2011). *Η επίθεση σε δίκτυα Η/Υ και η χρήση βίας κατά το Διεθνές Δίκαιο.* (Διπλωματική εργασία). Δημοκρίτειο Πανεπιστήμιο. http://www.militaryjustice.gr/wp-content/uploads/2018/03/epithesi_diktia_yh.pdf.

Μαρούδα, Ντ. Μ. (2014). Ανθρωπιστικό Δίκαιο που εφαρμόζεται σε ένοπλες συρράξεις. Στο Κ. Μαγκλιβέρα & Κ. Αντωνόπουλου (επιμ.), *Δίκαιο Διεθνούς Κοινωνίας* (σ. 727-777). Νομική Βιβλιοθήκη.

Mearsheimer, J. J. (2011). *Η τραγωδία της πολιτικής των μεγάλων Δυνάμεων* (επιμ. Π. Ήφαιστος & μτφρ. Κ. Κολιόπουλος). Ποιότητα. (Το πρωτότυπο έργο εκδόθηκε το έτος 2001).

Nye, J. (2005). *Ήπια ισχύς: Το μέσο επιτυχίας στην παγκόσμια πολιτική* (επιμ. Σ. Ντάλης & μτφρ. Ε. Μπαρτζινόπουλος). Παπαζήσης. (Το πρωτότυπο έργο εκδόθηκε το έτος 2004).

Ξενόγλωσση

Allison, G. T., Carnesale, A., & Nye, J. S. (Eds.) (1986). *Hawks, Doves, and Owls: An Agenda for Avoiding Nuclear War*. WW Norton & Company.

Armitage, R. L., & Nye, J. S. (2007). *CSIS commission on smart power: a smarter, more secure America.* CSIS Press.

Black, H. C. (1968). *Black's Law Dictionary.* (4th Edition). West Publishing Corporation.

Britz, M. (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson PLC.

Brodie, B. (Ed.) (1946). *The Absolute Weapon: Atomic Power and World Order*. Harcourt, Brace and Company.

Buchan, R., & Tsagourias, N. (2020). Autonomous Cyber Weapons and Command Responsibility. *International Law Studies,* 96, 645 - 673.

Clausewitz, C. von. (1989). *On War* (Eds. transl. M. Howard & P. Paret). Princeton University Press. (Το πρωτότυπο έργο εκδόθηκε το 1832).

Crawford, J. (2012). Articles on responsibility of states for international wrongful acts. *United Nations Audiovisual Library of International Law.* https://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_e.pdf

Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J., & Schroefl, J. (2021). *The landscape of Hybrid Threats: A Conceptual Model (Public Version)*. G. Giannopoulos, H. Smith & M. Theocharidou (Eds.), EUR 30585 EN, Publications Office of the European Union. doi:10.2760/419776.

ENISA. (2018). *Reference Incident Classification Taxonomy Task Force Status and Way Forward*. ENISA.

Franck, T. M. (2005). Legitimacy after Kosovo and Iraq. In V. Crnić-Grotić & M. Matulović (Eds), *International law and the use of force at the turn of centuries: Essays in honour of V. D. Degan*, (pp. 69-86). University of Rijeka.

Gray, C. S. (1982). *Strategic Studies and Public Policy: The American Experience.* University Press of Kentucky.

Gray, C. S. (2010). *The Strategic Bridge: Theory for Practice.* Oxford University Press.

Gray, C. S. (2012). *Airpower for Strategic Effect.* Air University Press.

Gray, C. S. (2013). *Making Strategic Sense of Cyber Power: Why the sky is not falling.* Strategic Studies Institute, US Army College.

Gray, C. S. (2016). *Perspectives on Strategy.* Oxford University Press.

Hathway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 100, 4, 817-885.

Janssens, P. C., & Wouters, J. (2022). Informal international law-making: A way around the deadlock of international humanitarian law?. In *International Review of the Red Cross (2022)*, (pp. 2111-2130). Cambridge University Press.

Keohane, R. O., & Nye, J. S. (1989). *Power and Interdepedence*. HarperCollins.

Kessler, O., & Werner, W. G. (2013). Expertise,Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden Journal of International Law*, 793-810.

Krepinevich, A. F. (2012). *Cyber Warfare: A "Nuclear Option"?.* Center for Strategic and Budgetary Assessments.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, H. S. Starr & L. K. Wentz (Eds), *Cyberpower and National Security* (pp. 24-42). National Defence University Press.

Menn, J. (2010). *Fatal Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet.* Public Affairs.

Richards, J. (2009). Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. *International Affairs Review*, 18, 2 http://www.iar-gwu.org/node/65

Sackelfords, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, 27, 1, 192-251.

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *The Columbia Journal of Transnational Law*, 37, 885-937.

Schmitt, M. (2011). Cyber Operations and the Jus in Bello: Key Issues, *International Law Studies*, 87, 89-110.

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

Schmitt, M. (Ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Silver, D. B. (2002). Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. In M. N. Schmitt & T. O'Donell (Eds), *Computer Network Attack and International Law,* (pp. 73-97). US Naval War College Publishing.

Tanenbaum, A. S. (2009). *Modern Operating Systems* (3rd Edition). Pearson Prentice Hall.

Tellis, A. J., Bially, J., Layne, C., & McPherson, M. (2000). *National power in the*

postindustrial age. RAND. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1110/RAND_MR1110.pdf

Tsagourias, N. (2020). Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace. *ESIL Reflections COVID-19 Series*, 9, 4, 1-7.

UNIDIR. (2017). *The United Nations, Cyberspace and International Peace and Security* UNIDIR. https://unidir.org/sites/default/ files/publication/pdfs//the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Voo, J., Hemani, I., Jones, S., Desombre, W., Cassidy, D., & Schwarzenbach, A. (2020). *National Cyber Power Index: Methodology and Analytical Considerations.* (Belfer Center Report). Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2020-09/ NCPI_20 20.pdf

Voo, J., Hemani, I., & Cassidy, D. (2022). *National Cyber Power Index 2022.* (Belfer Center Report). Harvard Kennedy School. https://www.belfercenter.org/publication/national-cyber-power-index-2022

Van Vuuren, J. J., & Leenen, L. (2019). Building blocks and measurement of national cyberpower. In M. Sarfraz (Ed). *Developments in information security and cybernetic wars.* (pp. 97-120). IGI Global.

Wayman, F., Singer, D. J., & Goertz, G., (1983). Capabilities, Allocations, and Success in Militarized Disputes and Wars: 1816–1976. *International Studies Quarterly*, 27, 4, 497–515.

Waxman, M. C. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law*, 36, 2, 421-459.

Wirtz, J. J. (2015). Cyber war and strategic culture: The russian integration of cyber power into grand strategy. In K. Geers (Ed.), *Cyber war in perspective: russian aggression against Ukraine*, (pp. 29-37). NATO CCD COE Publications.

Παράρτημα Α

Θεωρία της Επανάστασης στις Στρατιωτικές Υποθέσεις και "επανάσταση της τεχνολογίας της πληροφορίας"

Αποτελεί κοινή πεποίθηση ότι η "τεχνολογία της πληροφορίας"[82] έχει πυροδοτήσει και ενεργοποιήσει στρατηγικές αλλαγές σε τέτοιο βαθμό που αυτοδίκαια έχει κερδίσει τον χαρακτηρισμό επαναστατική. Μάλιστα θεωρείται ότι η Επανάσταση στις Στρατιωτικές Υποθέσεις, την οποία ενεργοποίησε η τεχνολογία της πληροφορίας, είτε έχει ήδη επισυμβεί είτε εξελίσσεται σε πραγματικό χρόνο (Gray, 2013, p. 21). Πλην όμως, σε ό,τι αφορά τη στρατηγική το θέμα δεν είναι αυτή καθεαυτή η διαμόρφωση νέας πραγματικότητας στον κυβερνοχώρο ή η δυναμική περαιτέρω τεχνικών βελτιώσεων της υφιστάμενης κατάστασης. Η στρατηγική, όπως έπραττε διαχρονικά έτσι και τώρα αναζητά την απάντηση στη θεμελιώδη ερώτηση: "Και λοιπόν;"

Τα πρώτα αχνά ίχνη της τεχνολογίας της πληροφορίας ανιχνεύονται περίπου στα μέσα της δεκαετίας του ’80. Από τότε, δειλά στην αρχή και με ολοένα επιταχυνόμενο ρυθμό στη συνέχεια, καταλήξαμε στη σημερινή εκτυφλωτική λάμψη της που θαμπώνει ειδικούς και μη με τις τεχνικές της δυνατότητες, όμως η στρατηγική κατανόηση εκλείπει, έχει είτε παραμεληθεί ή απλά αναβληθεί. Με άλλα λόγια, ενώ η τεχνολογία της πληροφορίας "ευλογήθηκε" πολιτικά και υπήρξε η έξαψη να συναρμοστεί άμεσα στην καθημερινότητα, παράλληλα με τη ραγδαία εξέλιξή της, δεν απεφεύχθη η δυσαρμονία συναρμογής της με το στρατηγικό επίπεδο. Δεν είναι η πρώτη φορά στη σύγχρονη ιστορία που η στρατηγική διαπιστώνεται εμφατικά απούσα από τις εξελίξεις (Gray, 2013, p. 22). Μάλιστα η σύγχρονη ανωριμότητα στη στρατηγική σκέψη της τεχνολογίας της πληροφορίας παραλληλίζεται ευθέως με την πρώιμη πυρηνική στρατηγική (Krepinevich, 2012, pp. 4-5). Οι υποψίες για τον υπαίτιο αυτής της κατάστασης εύλογα κατευθύνονται στη θεωρία της Επανάστασης στις Στρατιωτικές Υποθέσεις. Αυτό που συνέβη είναι ότι η στρατιωτική κοινότητα, μη εξαιρουμένων των ΗΠΑ, παραδόθηκε στην επιστήμη και στην τεχνολογία εστιάζοντας στην αχαλίνωτη εξέλιξη στο τεχνικό μέρος έχοντας τη θεμελιωμένη ιστορική

[82] Απόδοση ελληνιστί του όρου "Information Technology" (IT).

πεποίθηση ότι θα έρθει κάποια μέρα στο μέλλον που είτε εμείς είτε κάποιος άλλος θα είναι σε θέση να ερμηνεύσει τι σημαίνει στρατηγικά το τεχνολογικό άλμα της χρήσης των ηλεκτρονικών υπολογιστών.

Στρατηγικά οι συνέπειες των μεγάλων επιστημονικών και τεχνικών αλλαγών σπανίως είναι εξ αρχής προβλέψιμες σε όλη την έκτασή τους. Ο σιδηρόδρομος, τα ραδιοκύματα, το αεροπλάνο και τα πυρηνικά όπλα δεν έγιναν στρατηγικά κατανοητά με την εμφάνισή τους. Σε κάθε τέτοια αλλαγή ο χρόνος είναι πάντοτε αντίπαλος, η κρίσιμη παράμετρος που μπορεί να αναδείξει τον νικητή, με το διακύβευμα να κυμαίνεται μεταξύ της επικράτησης και της επιβίωσης. Ακόμη και στην περίπτωση των πυρηνικών όπλων, της μεγαλύτερης απειλής που ενέσκυψε μέχρι σήμερα στην ανθρώπινη ιστορία, απαιτήθηκε να παρέλθει διάστημα περίπου εικοσαετίας από την άφεση της πρώτης πυρηνικής βόμβας[83] έως ότου να μορφοποιηθεί κατάλληλη στρατηγική θεώρησή τους[84]. Γιατί λοιπόν η "επανάσταση της τεχνολογίας της πληροφορίας" να διαφέρει; Αποτελεί ανοιχτό ερώτημα σε ποιο χρονικό σημείο ωρίμανσης της στρατηγικής σκέψης στην "επανάσταση της τεχνολογίας της πληροφορίας" εκτιμάται ότι βρισκόμαστε σήμερα, κατ’ αναλογίαν με το αντίστοιχο πυρηνικό χρονοδιάγραμμα.

Η ανάγκη για τη θεμελίωση στρατηγικής κοινής λογικής στον κυβερνοχώρο είναι παραπάνω από επιτακτική. Πλην όμως, πολιτική και Δημόσια Διοίκηση είναι εθισμένες, εκ της αποστολής τους, να προσδιορίζουν τόσο το βάθος του χρονικού ορίζοντα όσο και τη λεπτομέρεια της πρόβλεψης υπό τους όρους της έννοιας του "προβλεπτού μέλλοντος", κάτι που δυστυχώς ανάγεται στη σφαίρα του φανταστικού (Gray, 2013, p. 25). Το μέλλον δεν είναι αδύνατο να προσεγγιστεί, υπό την έννοια όμως του "αναμενόμενου μέλλοντος", δηλαδή ως μια αδρομερής πρόβλεψη που αποφεύγει επιμελώς τις λεπτομέρειες. Η πρακτική πρόκληση είναι να γίνει κατανοητό

[83] Θα ήταν σημαντική παράλειψη να μην επισημανθεί η συμβολή του στρατηγιστή Bernard Brodie, του επονομαζόμενου "Αμερικανού Κλαούζεβιτς", στη θεμελίωση της στρατηγικής σκέψης περί των πυρηνικών όπλων, ο οποίος ήδη από το 1946 δήλωνε ότι: "Μέχρι σήμερα ο κύριος σκοπός του στρατού ήταν να κερδίζει πολέμους. Από εδώ και πέρα ο κύριος σκοπός του θα είναι να τους αποτρέπει. Δεν μπορεί να έχει σχεδόν κανέναν άλλο χρήσιμο σκοπό" (Brodie, 1946, p. 62).

[84] Η πραγματικά "χρυσή περίοδος" στρατηγικής σκέψης περί της πυρηνικής απειλής ήταν η δεκαετία 1955-1966, οπότε και το αντικείμενο εξαντλήθηκε στρατηγικά (Gray , 1982, pp. 44-58).

πως να αξιοποιηθεί με βέλτιστο τρόπο, με τη στρατηγική του σημασία, αυτό που νομίζουμε ότι γνωρίζουμε, με υψηλό βαθμό αξιοπιστίας, για το μέλλον της "επανάστασης της τεχνολογίας της πληροφορίας".

Οι ΗΠΑ τη δεκαετία του ’00 προσπαθούσαν να κατανοήσουν τη στρατηγική σημασία των "εξωτικών" δυνατοτήτων που παρείχε η κυβερνοϊσχύς και να συγκεκριμενοποιήσουν τις πιθανές απειλές των αντίστοιχων δυνατοτήτων των αντιπάλων τους. Οι στρατηγιστές τους από την άλλη αναζητούσαν την επόμενη "μεγάλη ιδέα", με την "επανάσταση της τεχνολογίας της πληροφορίας" να βρίσκεται μεταξύ των υποψηφίων (Gray, 2013, p. 26). Η υπόσχεση της ψηφιακής αλλαγής θεωρήθηκε η προφανής τρέχουσα Επανάσταση στις Στρατιωτικές Υποθέσεις και σχεδόν άμεσα ο αμερικανικός στρατός ξεκίνησε τον μετασχηματισμό του για την ενσωμάτωση της. Τότε ανέκυψαν οι πραγματικές συρράξεις στο Αφγανιστάν και στο Ιράκ, και αυτό που έγινε απτό από την πρώτη στιγμή ήταν ότι η ένταση της τεχνικής αλλαγής στη ψηφιοποίηση είχε προσπεράσει τη στρατηγική της σημασία (Gray, 2013, p. 27). Αποδείχθηκε ότι σκοποί, μέσα και υποθέσεις δεν είχαν ολιστική συνοχή. Όσο συναρπαστικά κι αν είναι τα διατιθέμενα μέσα και οι τρόποι εμπλοκής τους εάν αυτά δεν συνδεθούν ευφυώς για την επίτευξη συνετών πολιτικών σκοπών, η στρατηγική δεν μπορεί να λειτουργήσει.[85] Το λάθος ήταν ότι η θεωρία της Επανάστασης στις Στρατιωτικές Υποθέσεις μπέρδεψε τη μονομερή μαχητική ισχύ με την αποτελεσματικότητα, η οποία είναι αυτή που παράγει τα αποτελέσματα στη στρατηγική ιστορία (Gray, 2010, p. 167).

Στο σημείο αυτό αξίζει να σημειωθεί ότι σε κανένα μεγάλο πόλεμο της σύγχρονης Ιστορίας δεν υφίσταται αποκλειστικού τύπου αιτιώδης συνάφεια μεταξύ τεχνολογικής κατωτερότητας και ήττας. Και αντιστρόφως, η τεχνολογική ανωτερότητα δεν απετέλεσε, ιστορικά, άνευ όρων εγγύηση νίκης[86]. Ο πόλεμος και η

[85] Θα ήταν τουλάχιστον αφελές να θεωρηθεί ότι η κριτική αδικεί τον αμερικανικό Στρατό, δεδομένου ότι βασίζεται σε a posteriori γνώση. Το επιχειρησιακό περιβάλλον του Αφγανιστάν ήταν a priori γνωστό, όπως προβλεπτή ήταν και η φύση του πολέμου στις άνυδρες ορεινές εκτάσεις του και τέλος δεν αποτελούσε μυστικό η ιστορική του διαδρομή ως "νεκροταφείο Αυτοκρατοριών".

[86] Ένα εκ των στρατηγικών θεωρητικών προβλημάτων είναι ποια η συσχέτιση ποσότητας έναντι της ποιότητας. Εν προκειμένω ο Β΄ ΠΠ προσφέρει πληθώρα διδαγμάτων. Ένα εξ αυτών είναι οι νίκες της Λουτβάφε επί της Κόκκινης Αεροπορίας στην αρχική φάση του πολέμου, οι οποίες επετεύχθησαν

διεξαγωγή του δεν δύνανται να "εγκλωβιστούν" εννοιολογικά και φυσικά σε ερμηνευτικό πλαίσιο το οποίο χρησιμοποιεί αποκλειστικά όρους εξοπλισμού, οργάνωσης και διατιθέμενων στρατιωτικών μέσων ενός εκ των εμπολέμων, παραλείποντας οτιδήποτε άλλο. Αυτό ακριβώς επιβεβαιώθηκε άλλη μια φορά στην πράξη όταν η μοναδική υπερδύναμη του πλανήτη, η οποία εντρυφούσε επί σχεδόν μια δεκαετία στη θεωρία Επανάστασης στις Στρατιωτικές Υποθέσεις και στον συνεπαγόμενο μετασχηματισμό των Ενόπλων Δυνάμεών της, ταπεινώθηκε από υποδεέστερους, φτωχά εξοπλισμένους, πλην όμως ευπροσάρμοστους, αντιπάλους της στους πολέμους του Ιράκ και του Αφγανιστάν. Οι ΗΠΑ αποδείχθηκε ότι ήταν ένας παραπληροφορημένος σύγχρονος Γολιάθ με τις επαναστατικές θεωρήσεις τους για τη μετεξέλιξη του πολέμου να είναι απλώς ακατάλληλες για το είδος του πολέμου που επέλεξαν να εμπλακούν. Κι αυτό διότι υπολείπονταν εξ αρχής της ποιοτικής συνιστώσας της στρατηγικής. Η έλλειψη στρατηγικού περιεχομένου αντάξιου της πολλά υποσχόμενης στρατιωτικής μετεξέλιξης είχε επισημανθεί στη βιβλιογραφία, αλλά αυτό ήταν κάτι αναμενόμενο να συμβεί. Η ίδια η θεωρία δεν ήταν λανθασμένη σε ολόκληρη την έκτασή της, απλώς μάλλον δεν μπορούσε να φιλοδοξεί ότι επαρκούσε αυτοτελώς να περιλάβει την ολότητα της πολιτικής και του πολέμου (Gray, 2013, p. 29).

Χρόνια τώρα ο μεγάλος Πρώσος στρατηγιστής μας έχει επισημάνει ότι ο πόλεμος και η διεξαγωγή του αφενός περιλαμβάνουν αιματοχυσία (Clausewitz, 1832/1989, book 1, ch. 1, p. 75) και αφετέρου αποτελούν το κατ’ εξοχήν πεδίο κινδύνου και εντατικής φυσικής προσπάθειας (Clausewitz, 1832/1989, book 2, ch. 3, p. 149), αβεβαιότητας (Clausewitz, 1832/1989, book 1, ch. 6, pp. 117-118) και τύχης (Clausewitz, 1832/1989, book 1, ch. 3-8, pp. 100-123). Πλην όμως, ο ίδιος ο πόλεμος δεν συμβαίνει για αυτά καθ’ εαυτά τα χαρακτηριστικά του αλλά συνεπεία της πολιτικής, η οποία ως μήτρα τον τίκτει (Clausewitz, 1832/1989, book 1, ch. 1, pp. 80-81 & book 1, ch. 1, pp. 86-89 & book 8, ch. 6, pp. 603-610). Συνεπώς, το αντικείμενο

συνεπεία της ποιοτικής υπεροχής της. Όταν όμως η ΕΣΣΔ έφθασε να παράγει αεροσκάφη με αναλογία 4:1 έναντι της Γερμανίας, η ωμή αριθμητική υπεροχή των Ρώσων απέναντι στους εμμονικούς με την ποιοτική ανωτερότητα Γερμανούς στοίχισε στους τελευταίους τη νίκη (Κολιόπουλος, 2010, σσ. 244-245).

της στρατηγικής είναι ο ίδιος ο πόλεμος όχι η διεξαγωγή του. Προφανώς, τα μέσα διεξαγωγής έχουν τη σημασία τους και θα πρέπει να λαμβάνονται υπόψιν στο σχεδιασμό (Clausewitz, 1832/1989, book 8, ch. 6, pp. 608-609), όμως αν αυτά αποτελούν τη γραμματική του πολέμου η λογική του είναι η ζήτημα της πολιτικής (Clausewitz, 1832/1989, book 8, ch. 6, p. 605). Οι ορισμοί της στρατηγικής δεν αφήνουν κανένα περιθώριο αμφισημίας: η στρατιωτική στρατηγική είναι η η χρήση ή η απειλή χρήσης βίας για επίτευξη πολιτικών αντικειμενικών σκοπών οι οποίοι αποφασίζονται από την εκάστοτε πολιτική ηγεσία. Άρα, η "επανάσταση στην τεχνολογία της πληροφορίας", ως Επανάσταση στις Στρατιωτικές Υποθέσεις, και η παραγόμενη κυβερνοϊσχύς δεν αφορά στην τεχνολογία και στην επιστήμη, όπως και η αεροπορική ισχύς δεν αφορά την αεροναυτική και η πυρηνική ισχύς δεν αφορά στην κβαντική φυσική (Gray, 2013, p. 30). Και οι τρεις πρόσφατες Επαναστάσεις στις Στρατιωτικές Υποθέσεις, αεροπορική ισχύς - πυρηνική ισχύς - κυβερνοϊσχύς, σχετίζονται με την πολιτική και τις παραγόμενες πολιτικές. Το τεχνικό μέρος και η τακτική χρήση είναι χρήσιμα, πλην όμως δεν αποτελούν αντικείμενο της στρατηγικής θεώρησης.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Παράρτημα Β

Ταξινομία κυβερνοόπλων - τεχνικές προσβολής

Στη συνέχεια παρουσιάζονται οι κυριότερες τεχνικές προσβολής συστημάτων και δικτύων, οι οποίες μπορούν να υιοθετηθούν κατά τη διενέργεια διεξαγωγής επιθετικών επιχειρήσεων κυβερνοχώρου[87]. Στην ουσία κάθε μια εξ' αυτών αποτελεί μια κλάση κυβερνοόπλων, οπότε προκύπτει εμμέσως και μια ταξινομία τους, αν και πρακτικά πλέον τα εξελιγμένα κυβερνοόπλα αναπτύσσονται με τη δυνατότητα ενσωμάτωσης πολλαπλών τεχνικών προσβολής στα επίπεδα[88] που διενεργούνται. Και τα τρία επίπεδα είναι ευάλωτα κατά τη διεξαγωγή κυβερνοπολέμου, επειδή όμως επίθεση στο φυσικό επίπεδο εμπλέκει κυρίως τεχνικές συμβατικού πολέμου (σαμποτάζ, βομβαρδισμό κτλ), οι τεχνικές οι οποίες παρουσιάζονται στη συνέχεια στρέφονται εναντίον του συντακτικού και του εννοιολογικού επιπέδου[89].

[87] Η παγκόσμια βιβλιογραφία βρίθει προτεινόμενων ταξινομιών. Προς αποφυγή περιττών τεχνικοτήτων υιοθετήθηκε οπτική η οποία προσομοιάζει με αυτήν του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA, 2018).

[88] Είναι γνωστό ότι ο κυβερνοχώρος δομείται σε τρία επίπεδα, το φυσικό (physical), το συντακτικό (syntactic) και το εννοιολογικό (semantic). Το φυσικό επίπεδο συνίσταται από το υλισμικό, το συντακτικό επίπεδο από το λογισμικό, το οποίο απαιτείται προκειμένου να καταστεί λειτουργικό το φυσικό επίπεδο, π.χ. υλικολογισμικό (firmware), ενώ στο εννοιολογικό επίπεδο εδράζεται το σύνολο της ψηφιακής πληροφορίας υπό τη μορφή δεδομένων (Britannica, 2022).

[89] Γενικά, τα κυβερνοόπλα εναντίον του συντακτικού επιπέδου εκμεταλλεύονται κάποια τρωτότητα του λογισμικού, σε επίπεδο πρωτοκόλλου επικοινωνίας ή λειτουργικού συστήματος ή υλικολογισμικού, Αντίθετα, τα κυβερνοόπλα εναντίον του σημασιολογικού επιπέδου αποσκοπούν συνήθως στη χειραγώγηση του ανθρωπίνου παράγοντα, γι' αυτό και είναι γνωστά ως κοινωνική μηχανική (social engineering). Χρησιμοποιούνται δε κυρίως για κυβερνοαπάτες και κατασκοπεία (Britannica, 2022).

Ως κυβερνοεπίθεση τύπου *DOS* καλείται η αδρανοποίηση του υπολογιστικού συστήματος[90], χωρίς κατ' ανάγκην την επίτευξη μεμακρυσμένου ελέγχου του ή πρόσβασης σε δεδομένα του, είτε μέσω της παρεμπόδισης της εξουσιοδοτημένης πρόσβασης νόμιμων χρηστών σε πόρους του είτε δια της επιβολής στο σύστημα χρονικής υστέρησης σε χρονοεξαρτώμενες κρίσιμες λειτουργίες του (Britz, 2013, p. 80). Επιτυγχάνεται μέσω καταιγισμού στο υπολογιστικό σύστημα μεγάλου πλήθους νομιμοφανών αιτημάτων πληροφοριών που υπερβαίνουν το σχεδιασθέν όριο κατωφλίωσης εξυπηρέτησης. Και ενώ, η τεχνική DOS δύναται να εκτελεσθεί μέσω ενός και μόνον Η/Υ, η πλέον συνήθης βαριάντα της είναι η τεχνική Κατανεμημένης Άρνησης Υπηρεσιών[91].

Μια άλλη προσφιλής τεχνική προσβολής συστήματος είναι το *κακόβουλο λογισμικό*[92]. Πρόκειται για λογισμικό, το οποίο εισάγεται στο υπολογιστικό σύστημα εν αγνοία του νόμιμου διαχειριστή του, συνήθως συγκεκαλυμμένα, με σκοπό να υποβαθμίσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των δεδομένων, των εφαρμογών ή και του ίδιου του λειτουργικού προγράμματος του συστήματος (Britz, 2013, p. 80; Tanenbaum, 2009, pp. 665-666). Το τμήμα του πηγαίου κώδικα το οποίο ευθύνεται για την κακόβουλη συμπεριφορά του λογισμικού καλείται φορτίο (payload) (Tanenbaum, 2009, p. 671). Οι πλέον δημοφιλείς μορφές του είναι ο ιός, το ηλεκτρονικό σκουλήκι, ο δούρειος ίππος, το πολυμορφικό κακόβουλο λογισμικό, το μεταμορφικό κακόβουλο λογισμικό, η λογική βόμβα και η βόμβα χρονικής καθυστέρησης.

Στο επίπεδο της κοινωνικής μηχανικής ο επιτιθέμενος πλαστογραφεί την πραγματική του ιδιότητα εμφανιζόμενος στον ανυποψίαστο χρήστη ως νόμιμος διαχειριστής ιστοσελίδας πλαστογραφώντας την αυθεντική IP διεύθυνση με σκοπό είτε την εγκατάσταση κακόβουλου λογισμικού στην περίπτωση της *παραπλάνησης* (IP

[90] Το εννοιολογικό περιεχόμενο του όρου υπολογιστικό σύστημα ή πληροφοριακό σύστημα, ή απλά σύστημα, περιλαμβάνει τις περιπτώσεις του προσωπικού Η/Υ, του μεμονωμένου (stand alone) Η/Υ, του εξυπηρετητή (server), του προσωπικού δικτύου (Personal Area Networks, PAN), του τοπικού δικτύου Η/Υ (Local Area Network, LAN) και του δικτύου ευρείας περιοχής (Wide Area Network, WAN). Στο τελευταίο δίκτυο συγκαταλέγεται και το διαδίκτυο (internet).

[91] Απόδοση ελληνιστί του όρου "Distributed Denial of Service" (DDOS).

[92] Απόδοση ελληνιστί του όρου "malicious software", "malware".

spoofing) (Britz, 2013, p. 104) είτε την υποκλοπή προσωπικών δεδομένων στην περίπτωση *ψαρέματος* (phising) (Britz, 2013, p. 133).

Τέλος, στη βιβλιογραφία αναφέρεται και η περίπτωση *κακόβουλων ενεργειών σε επίπεδο ολοκληρωμένων κυκλωμάτων* (chip level actions ή chiping). Φυσικός αυτουργός είναι ο ίδιος ο κατασκευαστής ο οποίος σκόπιμα ενσωματώνει τρωτότητες στο υλισμικό σε επίπεδο ολοκληρωμένων κυκλωμάτων[93]. Αντικειμενικός σκοπός είναι η δημιουργία ηλεκτρονικής κερκόπορτας, μέσω της οποίας κακόβουλος τρίτος απόκτα δυνατότητες μεμακρυσμένου ελέγχου επί του συστήματος.

[93] Πιο συγκεκριμένα, δύναται να υλοποιηθεί με δύο τρόπους είτε σε επίπεδο υλισμικού με την ύπαρξη, ή την ενσωμάτωση ελαττωματικού υποσυστήματος, είτε σε επίπεδο λογισμικού με την προσθήκη κατάλληλου προγράμματος.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Παράρτημα Γ

Περί επιχειρήσεων στον κυβερνοχώρο - διεθνής πρακτική

Το 2007 η *Εσθονία*, η πλέον διασυνδεδεμένη χώρα της Ευρώπης, γίνεται στόχος της σφοδρότερης σε ένταση και πλέον εκτεταμένης σε χρονική διάρκεια κυβερνοεπίθεσης, τύπου DDOS, που έχει σημειωθεί έως σήμερα[94]. Εκτιμάται ότι στις επιθέσεις συμμετείχαν περισσότεροι από ένα εκατομμύριο Η/Υ zombie από 178 χώρες (Menn, 2010, p. 213). Ο ΥΠΑΜ της Εσθονίας έκανε λόγο για «αποκλεισμό» της χώρας[95] και η χώρα αιτήθηκε, ως μέλος του ΝΑΤΟ, την ενεργοποίηση του Οργανισμού σύμφωνα με το άρθρο 5. Όμως, το ΝΑΤΟ εκτίμησε ότι δεν υπήρχε έδαφος εφαρμογής του άρθρου και απλά απέστειλε τεχνική βοήθεια, ενώ επισημαίνεται ότι ο ΟΗΕ δεν ασχολήθηκε καν (Sackelfords, 2009, pp. 210, 238).

Ένα χρόνο αργότερα, τον Αύγουστο του 2008, τα στρατεύματα της Ρωσικής Ομοσπονδίας εισέβαλαν στη *Γεωργία* διεξάγοντας συμβατικές πολεμικές επιχειρήσεις. Οι ρωσικές στρατιωτικές επιθέσεις συνοδεύτηκαν από μεγάλης κλίμακας κυβερνοεπιθέσεις τύπου DDOS. Μάλιστα, ενώ η Ρωσία αποκήρυττε οιαδήποτε συσχέτιση με τις κυβερνοεπιθέσεις, αυτές κατά περίεργο τρόπο, και εξαιρετικά βολικά για το Κρεμλίνο, προηγούνταν των ρωσικών αεροπορικών επιδρομών (Menn, 2010, p. 214). Μπορεί να εξαχθεί απαγωγικά ότι στη Γεωργία επιχειρήθηκε μια επιτυχής σύζευξη της τρέχουσας αντίληψης των στρατιωτικών δογμάτων με νέα τεχνολογικά επιτεύγματα προκειμένου να δημιουργηθούν οι

[94] Η διάρκειας 3 εβδομάδων επίθεση, η οποία πέτυχε να παραλύσει τη χώρα, ξεκίνησε την 27η Απριλίου του 2007 στις 10 πμ (Richards, 2009). Ως αιτία θεωρείται η κυβερνητική απόφαση μετεγκατάστασης στην πρωτεύουσα Ταλίν μνημείου πολέμου, το οποίο είχε ανεγερθεί από τους Σοβιετικούς σε ανάμνηση της απελευθέρωσης της Εσθονίας από τη ναζιστική κατοχή του Β΄ ΠΠ.

[95] Σύμφωνα με το άρθρο 3(c) της Απόφασης της ΓΣ/ΟΗΕ του 1974 υπό τον τίτλο «Ορισμός της Επίθεσης» ο αποκλεισμός λιμένων και ακτών κράτους συνιστά εκδήλωση επίθεσης και εμπίπτει στις διατάξεις του άρθρου 2 του Χάρτη του Οργανισμού (UN/GA, 1974).

συνθήκες για αυτό που οι θεωρητικοί στις επιστήμες αποκαλούν μετατόπιση υποδείγματος[96].

Μια από τις πλέον γνωστές κυβερνοεπιχειρήσεις είναι η εκστρατεία κυβερνοκατασκοπείας με το κωδικό όνομα *Titan Rain*, η οποία ενορχηστρώθηκε και εξαπολύθηκε το 2002 από τη Λαϊκή Δημοκρατία της Κίνας[97]. Η όλη εκστρατεία συγκέντρωνε πολύ υψηλού επιπέδου τεχνολογικά χαρακτηριστικά, που την κατηγοριοποιούσαν στην κλάση των προηγμένων επίμονων απειλών[98], ενώ και το εκτελεστικό της τμήμα διεξήχθη με μαεστρική δεξιοτεχνία. Η εκστρατεία Titan Rain τερματίστηκε με την καθοριστική συμβολή των ΗΠΑ πέντε χρόνια αργότερα.

Κάποια στιγμή το καλοκαίρι του 2009 η Λαϊκή Δημοκρατία της Κίνας εξαπολύει νέα κυβερνοεκστρατεία κατασκοπείας, γνωστή με το κωδικό όνομα *Aurora.* Και αυτή η κυβερνοεκστρατεία αξιολογήθηκε ως APT. Στα μέσα του Ιανουαρίου του 2010 ο κολοσσός της πληροφορικής Google ανακοινώνει δημόσια ότι εντόπισε κυβερνοεπίθεση προερχόμενη από την Κίνα, η οποία αφού διείσδυσε επιτυχώς στα συστήματα του, κατόρθωσε να υποκλέψει πληροφορίες (Google, 2010)[99]. Η Google δεν βίωσε μόνη της αυτήν την περιπέτεια καθώς και άλλες εταιρείες κολοσσοί υπήρξαν θύματα της υπόψη εκστρατείας κυβερνοκατασκοπείας, αποδεικνύοντας την ευρύτητα των ενδιαφερόντων της Κίνας.

Το πλέον εξελιγμένο κακόβουλο λογισμικό πάντως, το οποίο γνωρίζουμε, είναι επίτευγμα υπηρεσιών είτε του Δυτικού Κόσμου είτε του Ισραήλ· και το όνομα αυτού είναι *Stuxnet* (Krepinevich, 2012, p. 62). Το "ηλεκτρονικό σκουλήκι" Stuxnet ανακαλύφθηκε τον Ιούλιο του 2010. Χαρακτηρίστηκε ως στρατιωτικού επιπέδου «κυβερνοπύραυλος», αφού μόλυνε σε παγκόσμια κλίμακα συστήματα που ήλεγχαν βιομηχανικές διαδικασίες, τα λεγόμενα "Συστήματα Εποπτικού Ελέγχου και Συλλογής

[96] Μετατόπιση υποδείγματος (paradigm shift) καλείται μια δομική αλλαγή στη θεώρηση ή στις βασικές παραδοχές που διαμορφώνουν μια θεωρία.

[97] Το όνομα αποδίδεται στο ομώνυμο λογισμικό σάρωσης, το οποίο διερευνούσε σε παγκόσμια κλίμακα την ύπαρξη τρωτοτήτων λογισμικού σε δίκτυα Η/Υ που συσχετίζονταν, άμεσα ή έμμεσα είτε με την εθνική ασφάλεια είτε με τη βιομηχανία υψηλής τεχνολογίας (Menn, 2010, p. 218).

[98] Απόδοση ελληνιστί του όρου "Advanced Persistent Threat" (APT).

[99] Ανάλογη ανακοίνωση εξέδωσε εκ νέου η Google ενάμιση χρόνο αργότερα με την οποία γνωστοποιούσε ότι εκατοντάδες εργαζόμενοί της έπεσαν θύματα επιχείρησης ψαρέματος (Crovitz, 2011).

Δεδομένων"[100]. Παρότι το Stuxnet εξαπλώθηκε σε ολόκληρη την υφήλιο υπάρχουν ισχυρές ενδείξεις, οι οποίες συγκλίνουν στη διαπίστωση, πως αποκλειστικός στόχος ήταν οι πυρηνικές εγκαταστάσεις του Ιράν (Britz, 2013, p. 163). Εν κατακλείδι, τεχνικά το Stuxnet ήταν ένα «υπερ-κυβερνοόπλο», το οποίο απέδειξε ότι είναι δυνατόν να διεξαχθούν κυβερνοεπιθέσεις χειρουργικής ακρίβειας, αποσείοντας πιθανές αναστολές ανεπιθύμητων δευτερογενών παρενεργειών.

[100] Απόδοση ελληνιστί του όρου "Supervisory Control And Data Acquisition systems" (SCADA).

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

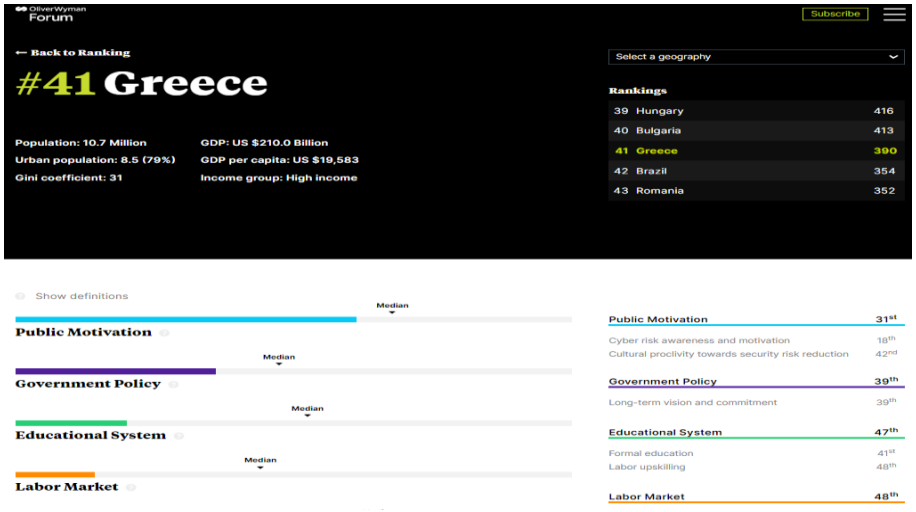
Παράρτημα Δ

Στοιχεία ενδεικτών δυνατοτήτων ελληνικής κυβερνοϊσχύος

κατά το *NCPI* -22 μοντέλο

Εικόνα Δ1

Επίγνωση κυβερνοασφαλείας και ψηφιακός αναλφαβητισμός



Σημείωση: Από *Cyber Risk Literacy and Education Index: Greece* by OliverWymanForum.com, 2021, Ανακτήθηκε στις 27/03/23, https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index. html#Greece.

Εικόνα Δ2

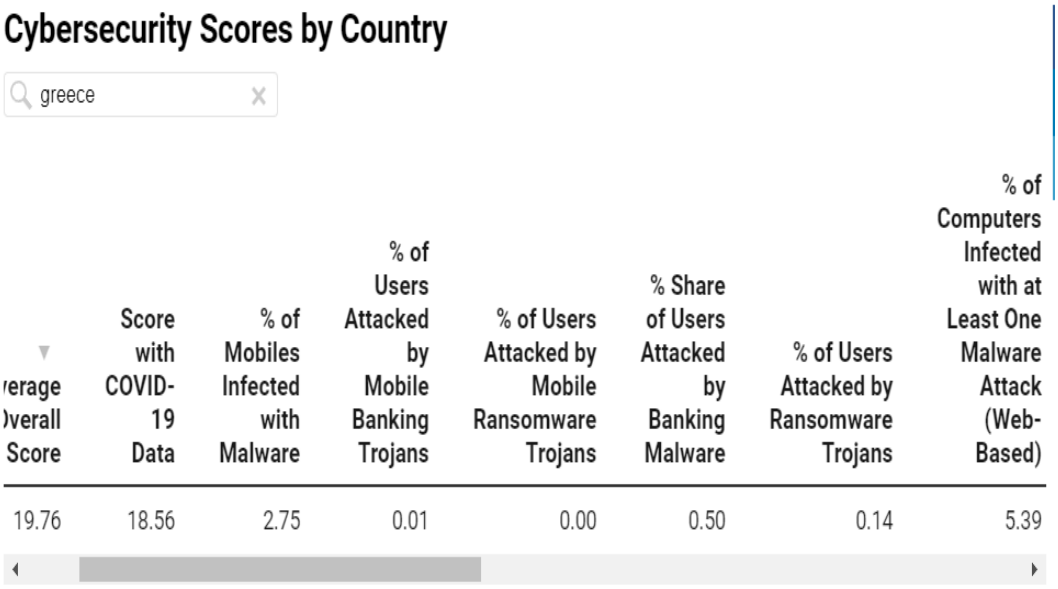
Ποσοστό μολυσμένων Η/Υ (2022)

	Country or territory*	%**
1	Taiwan	26.07
2	Hong Kong	14.60
3	Algeria	14.40
4	Nepal	14.00
5	Tunisia	13.55
6	Serbia	12.88
7	Sri Lanka	12.41
8	Albania	12.21
9	Bangladesh	11.98
10	Greece	11.86
11	Palestine	11.82
12	Qatar	11.50
13	Moldova	11.47

Σημείωση: Από *IT threat evolution in Q2 2022. Non-mobile statistics* by SecureList.com, 2022, Ανακτήθηκε στις 27/03/23, https://securelist.com/it-threat-evolution-q2-2022/107099/.

Εικόνα Δ3

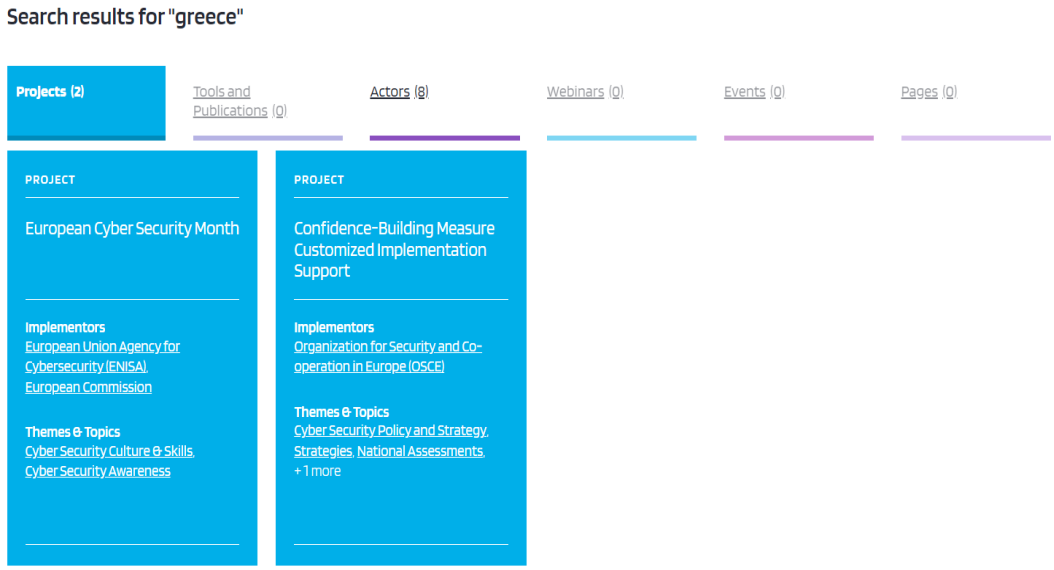
Ποσοστό μολυσμένων Η/Υ και κινητών συσκευών (2020)



Σημείωση: Από *Which countries have the worst and the best cybersecurity?* by comparitech, 2022, Ανακτήθηκε στις 27/03/23, https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

Εικόνα Δ4

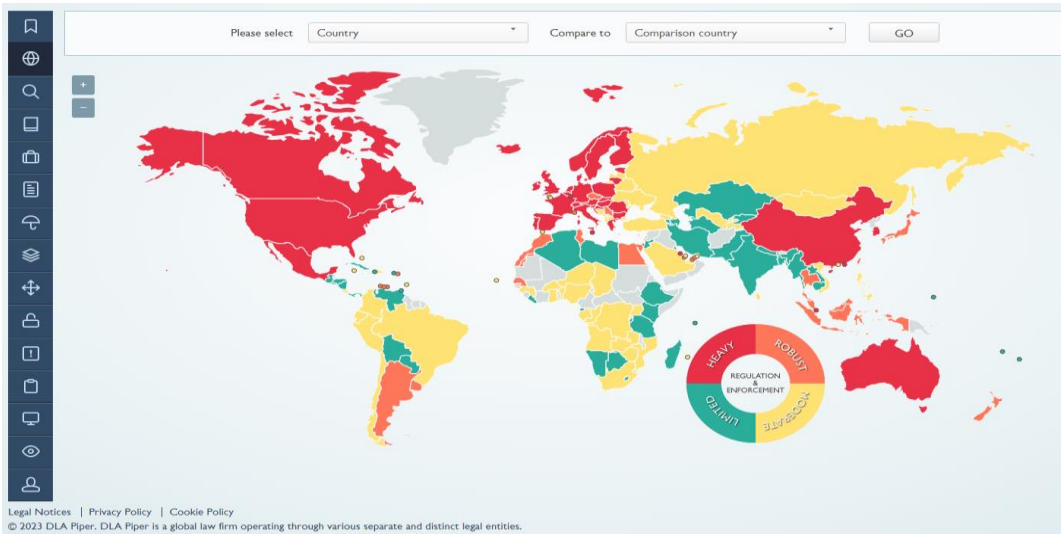
Συμμετοχή σε έργα ανάπτυξης ικανοτήτων κυβερνοχώρου ως βοήθεια στο εξωτερικό



Σημείωση: Από *The Knowledge Portal for Cyber Capacity Building:Greece* by Cybil, 2022, Ανακτήθηκε στις 27/03/23, https://cybilportal.org/?s=greece.

Εικόνα Δ5

Ισχύς νομοθεσίας προστασίας προσωπικών δεδομένων και Ψηφιακή Διακυβέρνηση



Σημείωση: Από *Data protection laws of the world* by DLAPIPER*, 2023,* Ανακτήθηκε στις 27/03/23, https://www.dlapiperdataprotection.com/.

Εικόνα Δ6

Ηλεκτρονικό εμπόριο ως ποσοστό του ΑΕΠ (2021)

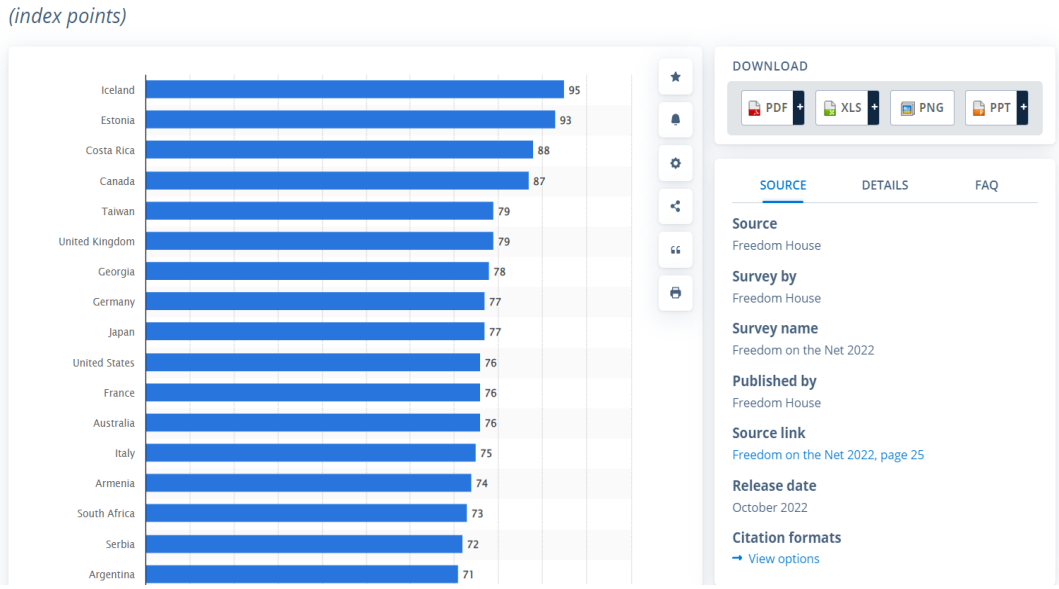
Table 1. Online Share During COVID in all Economies in the Sample

Economy	2019 average	Crisis peak (Peak year/month)	Latest	Latest minus pre-COVID trend
Bahrain	21.2	38.7 (2021/05)	34.1	10.0
Jamaica	33.1	45.8 (2021/09)	43.1	8.3
New Zealand	28.3	39.2 (2020/04)	29.0	5.1
Norway	18.2	23.4 (2021/09)	19.7	4.2
United Kingdom	28.4	39.8 (2021/01)	31.3	3.7
Singapore	27.6	43.5 (2021/09)	34.7	3.2
Australia	28.6	32.7 (2021/09)	32.1	2.0
Brazil	6.7	10.4 (2021/03)	9.5	0.9
Malaysia	11.7	19 (2021/08)	15.8	0.9
Russia	13.2	21.9 (2020/12)	20.8	0.8
India	4.4	7.4 (2021/05)	6.5	0.8
Croatia	1.5	4.1 (2020/12)	3.0	0.8
Zimbabwe	0.9	2.2 (2021/07)	1.9	0.8
Ecuador	3.9	6 (2021/04)	4.6	0.7
Sweden	10.4	12 (2020/12)	11.0	0.7
Montenegro	1.2	3.2 (2020/11)	2.6	0.6
Italy	5.7	9.9 (2020/11)	6.5	0.5
Egypt	6.4	10.5 (2020/06)	10.1	0.5
Slovenia	1.2	2.9 (2020/12)	1.7	0.4
Romania	3.6	7 (2020/11)	5.9	0.4
Serbia	1.2	2.4 (2021/09)	2.0	0.3
Slovakia	2.0	3.7 (2020/12)	2.5	0.2
Argentina	4.3	5.2 (2021/05)	3.9	0.1
United Arab Emirates	13.1	16.6 (2021/02)	16.6	0.1
Austria	3.5	7.7 (2020/11)	4.2	0.1
Hungary	5.8	9.9 (2021/03)	8.5	0.0
Thailand	9.4	13.7 (2021/08)	11.9	0.0
Cambodia	1.0	1.4 (2021/07)	1.2	0.0
Czech Republic	5.4	11.7 (2021/03)	8.0	0.0
Greece	4.8	8.6 (2021/08)	6.8	-0.1
Bulgaria	3.2	4.9 (2021/03)	4.3	-0.1
Lithuania	3.2	4.8 (2020/12)	3.6	-0.1
Canada	24.4	33.1 (2021/04)	27.0	-0.2
Poland	2.7	4.1 (2020/11)	3.8	-0.2
Germany	7.1	12.2 (2020/12)	7.9	-0.2

Σημείωση: Από *E-commerce During Covid: Stylized Facts from 47 Economies* by IMF.org, 2022, Ανακτήθηκε στις 27/03/23, https://www.imf.org/en/Publications/WP/Issues/2022/01/28/E-commerce-During-Covid-Stylized-Facts-from-47-Economies-512014.

Εικόνα Δ7

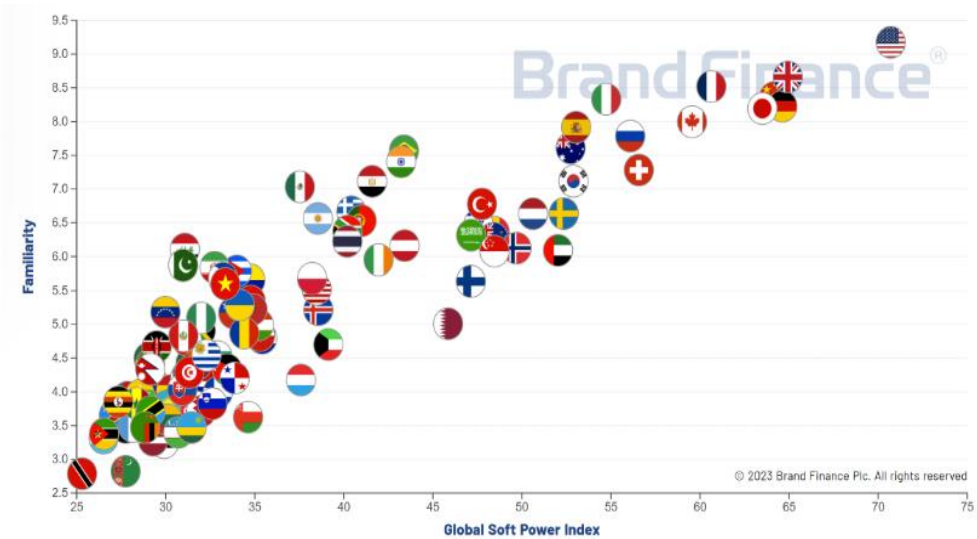
Ενδείκτης ελευθερίας στο διαδίκτυο (2022)



Σημείωση: Από *Degree of internet freedom in selected countries according to the Freedom House Index in 2022* by statista, 2023, Ανακτήθηκε στις 27/03/23, https://www.statista.com/statistics/272533/degree-of-internet-freedom-in-selected-countries/.[101]

Εικόνα Δ8

Κατάταξη ήπιας ισχύος

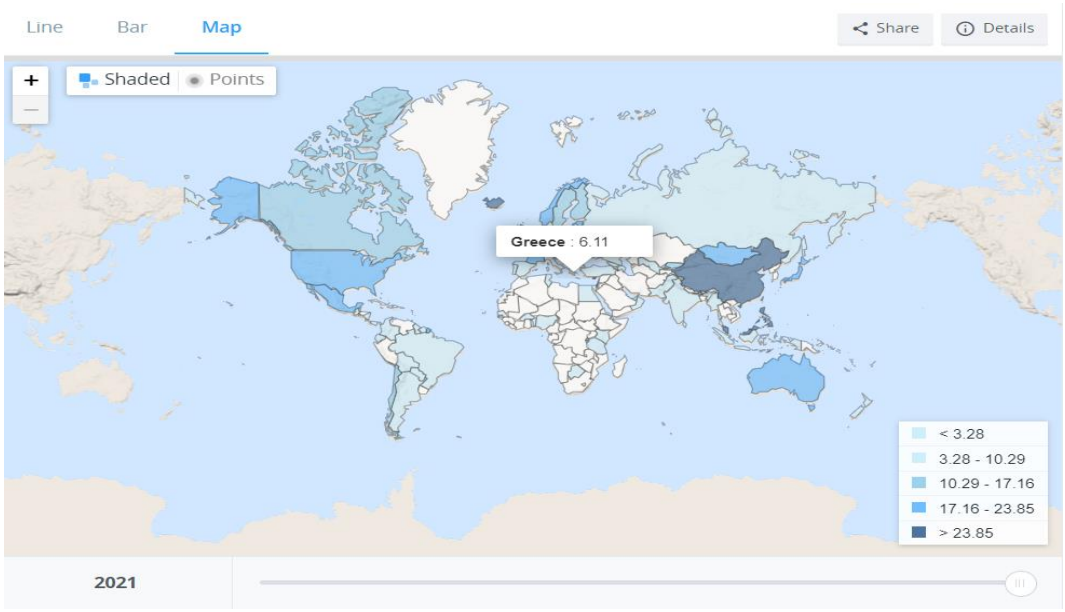


Σημείωση: Από *Global soft power index* by BrandFinance, 2023, Ανακτήθηκε στις 27/03/23, https://brandirectory.com/softpower/.

[101] Η Ελλάδα απουσιάζει από τη λίστα των διαχρονικά εξεταζόμενων εβδομήντα (70) χωρών, πλην όμως θα μπορούσαμε να εικάσουμε ευλογοφανώς, βάσει των αναγραφομένων στην Έκθεση αναφοράς, ότι ο ενδείκτης της είναι πέριξ του 73-74.

Εικόνα Δ9

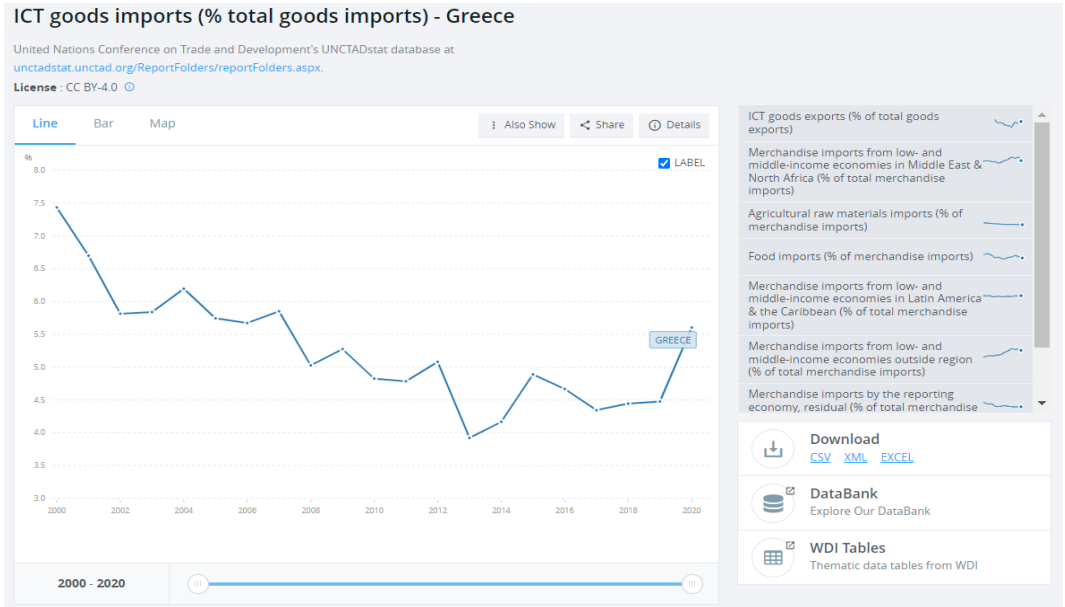
Ποσοστό των προϊόντων υψηλής τεχνολογίας επί του συνόλου εξαγωγών (2021)



Σημείωση: Από *High Technology exports (% of manufactured exports)* by The World Bank, 2023a, Ανακτήθηκε στις 27/03/23, https://data.worldbank.org/indicator/TX. VAL.TECH.MF.ZS?view =map.

Εικόνα Δ10

Ποσοστό προϊόντων ICT επί των γενικών εισαγωγών των αγαθών



Σημείωση: Από *ICT goods imports (% total goods imports)* by The World Bank, 2023b, Ανακτήθηκε στις 27/03/23, https://data.worldbank.org/indicator/TM.VAL.ICTG.ZS.UN.

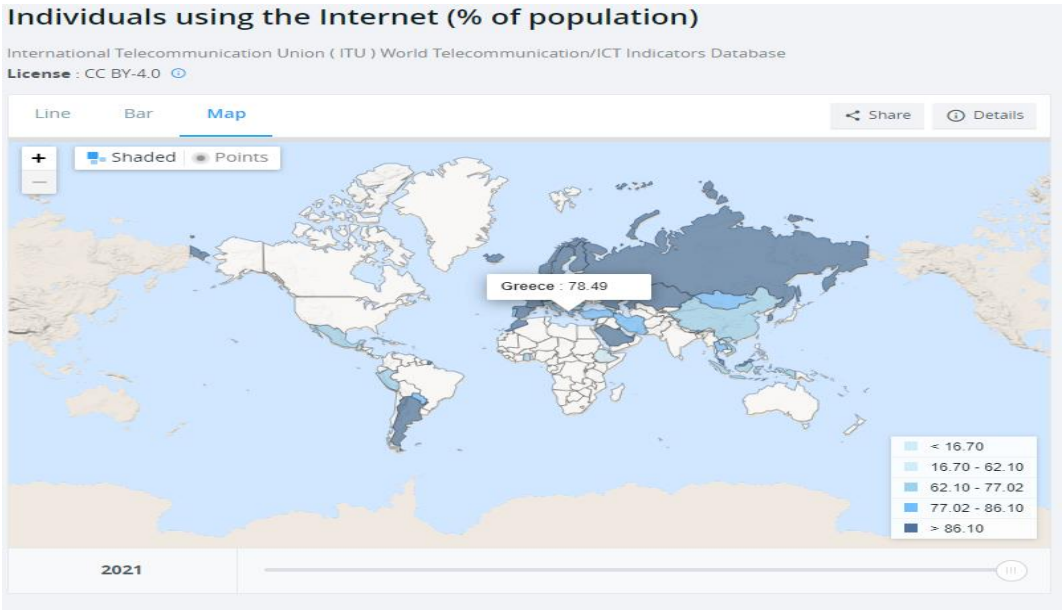
Εικόνα Δ11

Κατοχυρώσεις διπλωμάτων ευρασιτεχνίας (2020)

Σημείωση: Από *Patent applications, residents* by The World Bank, 2023c, Ανακτήθηκε στις 27/03/23, https://data. worldbank.org/indicator/IP.PAT.RESD?end=2020&start=2020&view=map.

Εικόνα Δ12

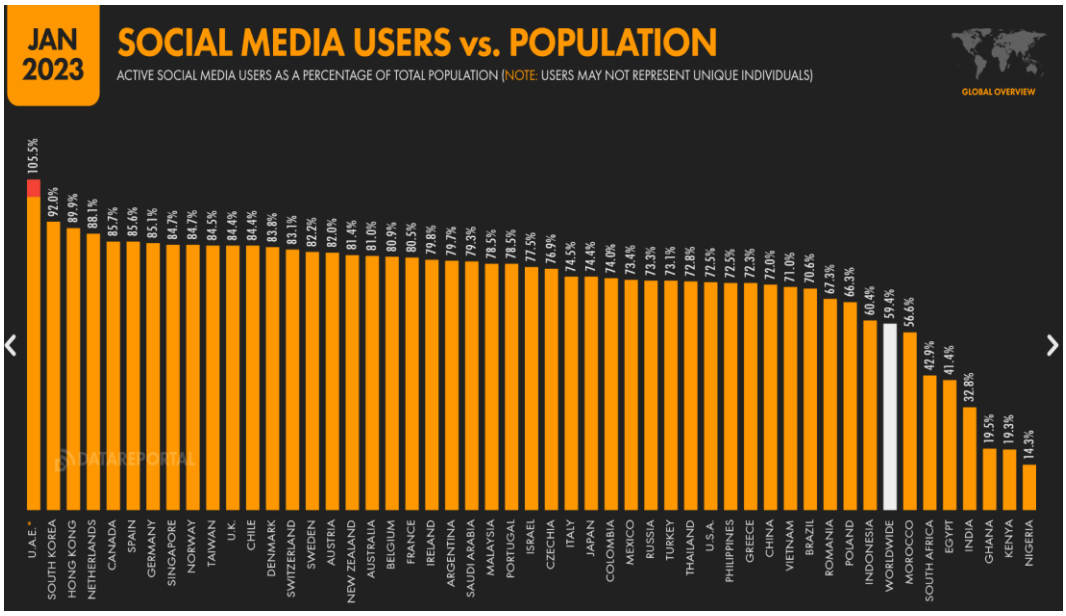
Ποσοστό του πληθυσμού που χρησιμοποιεί το διαδίκτυο (2021)



Σημείωση: Από *Individuals using the Internet (% of population)* by The World Bank, 2023d, Ανακτήθηκε στις 27/03/23, https://data.worldbank.org/indicator/IT.NET.USER.ZS? view=map.

Εικόνα Δ13

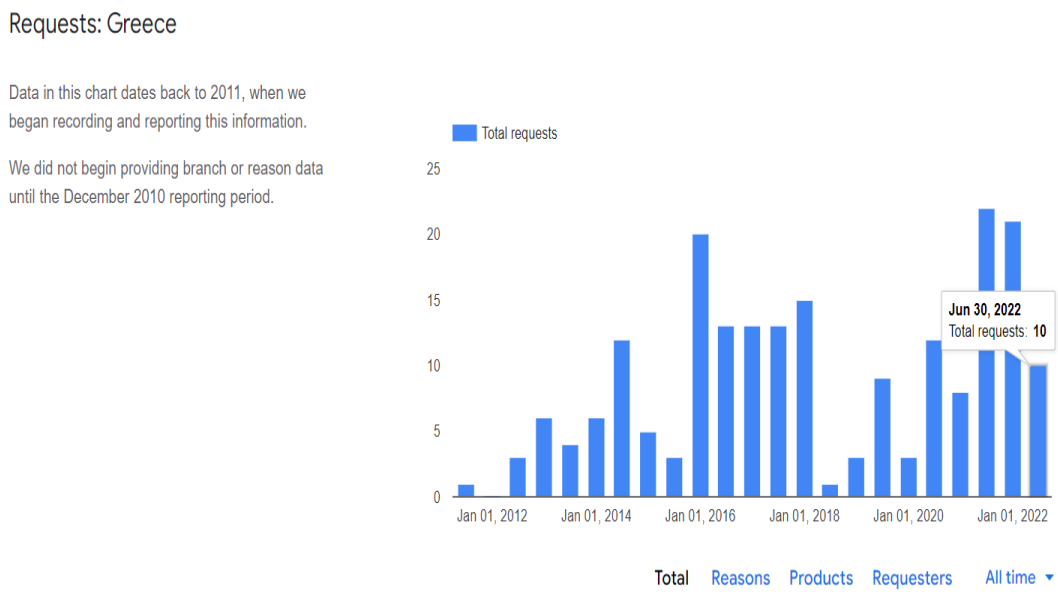
Ποσοστό του πληθυσμού που χρησιμοποιεί Μέσα Κοινωνικής Δικτύωσης (2023)



Σημείωση: Από *Global Overview Report* by datareportal.com, 2023, (p. 168), Ανακτήθηκε στις 27/03/23, https://datareportal.com/?utm_source=Statista&utm_medium=Data_Citation_Hyperlink&utm_campaign=Data_Partners&utm_=Statista_Data_Citation.

Εικόνα Δ14

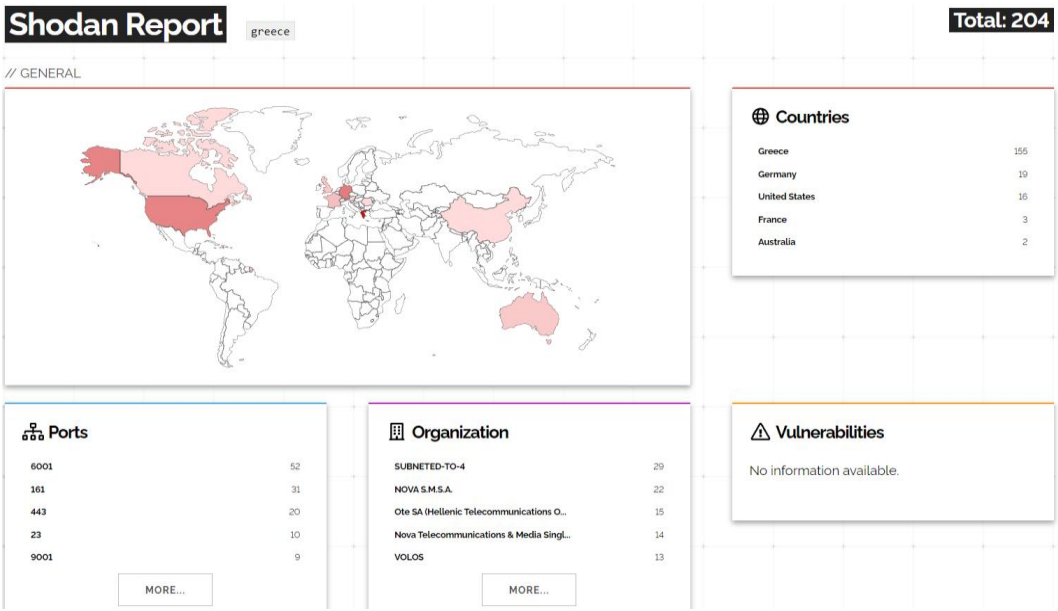
Επιτυχείς αιτήσεις απόσυρσης περιεχομένου από τη Google (2022)



Σημείωση: Από Trans*parency Report: Government requests to remove content - Greece* by Google, 2023, Ανακτήθηκε στις 27/03/23, https://transparencyreport.google.com/government-removals/government-requests/GR.

Εικόνα Δ15

Αναφορά αθροιστικών τρωτοτήτων εθνικών υποδομών



Σημείωση: Από *Shodan Report: Greece* by Shodan, 2023, Ανακτήθηκε στις 27/03/23, https://www.shodan.io/search/report?query=greece.

Παράρτημα Ε

Στοιχεία ενδεικτών πρόθεσης ελληνικής κυβερνοϊσχύος

κατά το *NCPI* -22 μοντέλο

Εικόνα Ε1

Αποδιδόμενες κυβερνοεπιθέσεις κατά το έτος 2022

Σημείωση: Από *Cyber Operations Tracker* by Council on Foreign Relations, 2023, Ανακτήθηκε στις 27/03/23, https://www.cfr.org/cyber-operations/.

Εικόνα Ε2

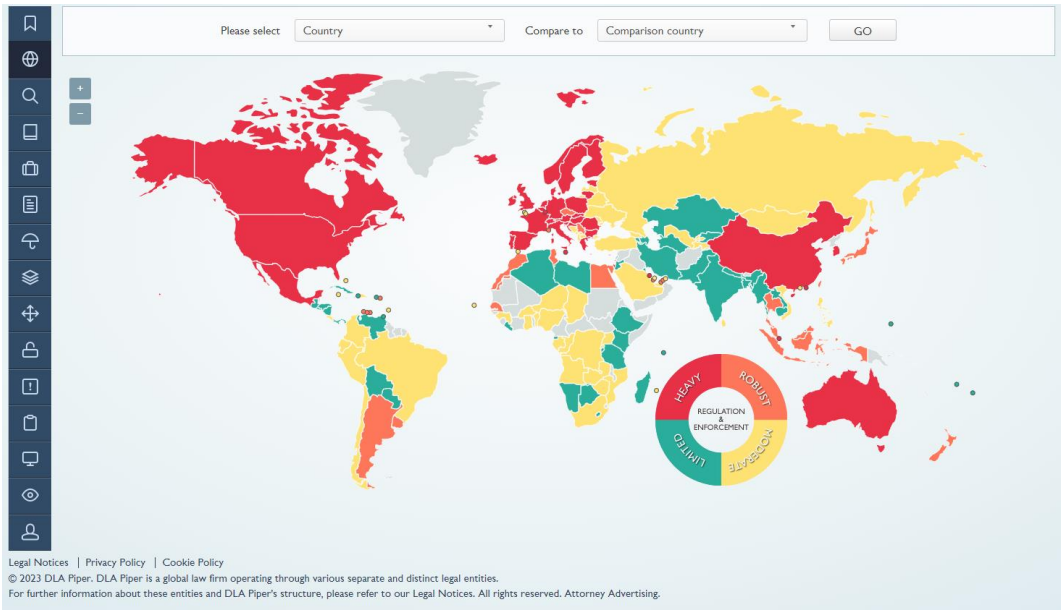
Συμμετοχή κρατών στο (UN) Internet Governance Forum (IGF) το έτος 2018

Σημείωση: Από *MAG 2018 Members* by Internet Governance Forum, 2023, Ανακτήθηκε στις 27/03/23,

https://www.intgovforum.org/en/content/mag-2018-members. [102]

Εικόνα Ε3

Ισχύς νομοθεσίας προστασίας προσωπικών δεδομένων και Ψηφιακή Διακυβέρνηση



Σημείωση: Από *Data Protection Laws of the World* by DLAPIPER, *2023,* Ανακτήθηκε στις 27/03/23, https://www.dlapiperdataprotection.com/.

Εικόνα Ε4

Συμμετοχή κρατών στα UN Cyber Government Groups of Experts (GGE)

[102] Η Ελλάδα δε συμμετέχει.

Σημείωση: Από *The United Nations, Cyberspace and International Peace and Security* by UNIDIR, 2017, (p. 17), Ανακτήθηκε στις 27/03/23, https://unidir.org/sites/default/files/publication/pdfs//the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Εικόνα Ε5

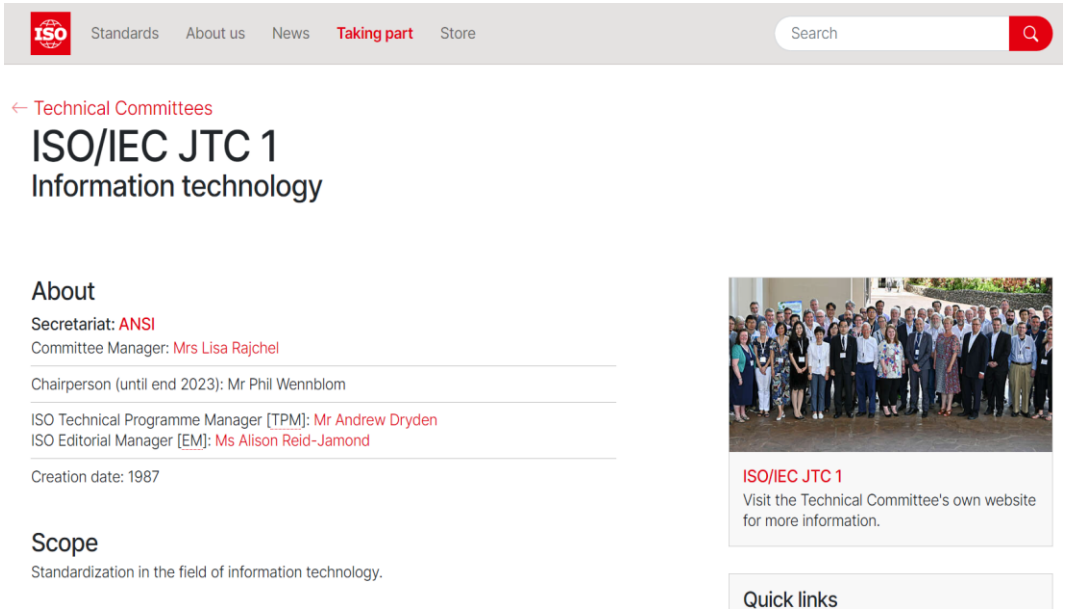
Αλφαβητικά συμμετοχές στο Global Forum for Cyber Expertise

Deloitte	DAI	Dominica	Dominican Republic
Economic Community of Central African States (ECCAS)	Economic Community of West African States (ECOWAS)	ESET	Estonia
Ethiopia	European Union	Europol	Finland
France	FS-ISAC	Gabon	Germany
Ghana	Guatemala	Hewlett Packard	Huawei
Hungary	International Association of Prosecutors (IAP)	IBM	International Chamber of Commerce (ICC)

Σημείωση: Από *Our Members* by GFCE, 2023, Ανακτήθηκε στις 27/03/23, https://thegfce.org/ member-overview/.

Εικόνα Ε6

Συμμετοχές σε ISO /IEC Joint Technical Commitees for Information Technology



Σημείωση: Από *Technical Commitees: ISO/IEC JTC 1-Information technology* by ISO.org, 2023, Ανακτήθηκε στις 27/03/23, https://www.iso.org/committee/45020.html.[103]

Εικόνα Ε7

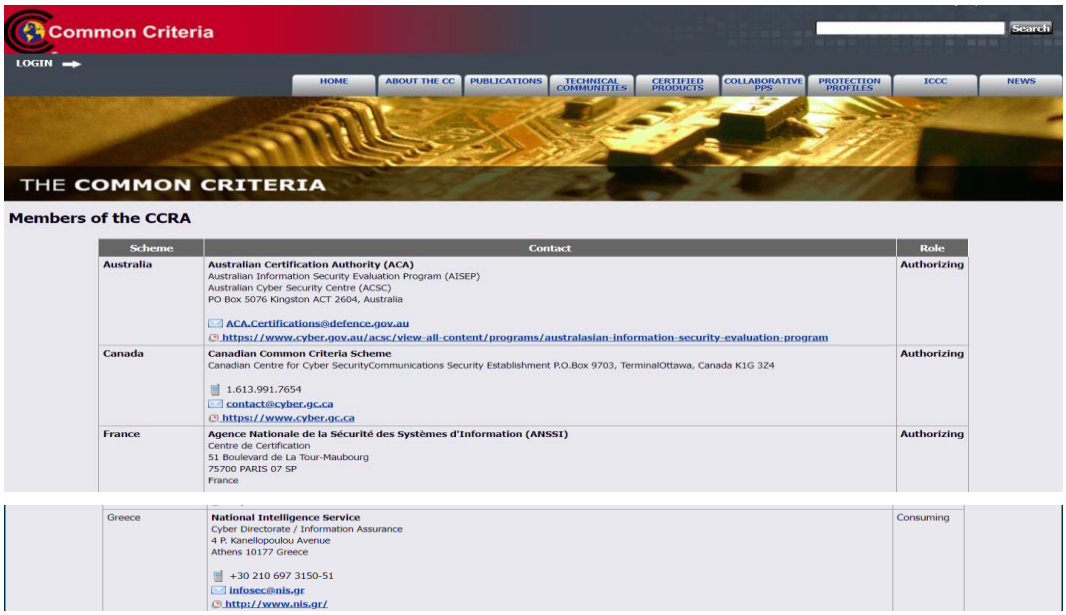
Συμμετοχές στο ITU-T Study Groups

Σημείωση: Από *ITU-T Study Groups (Study Period 2017-2021)* by ITU, 2023, Ανακτήθηκε στις 27/03/23, https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx.

Εικόνα Ε8

[103] Δεν ανευρέθη συμμετοχή της Ελλάδος σε κάποιες από τις 22 Τεχνικές Επιτροπές του Οργανισμού.

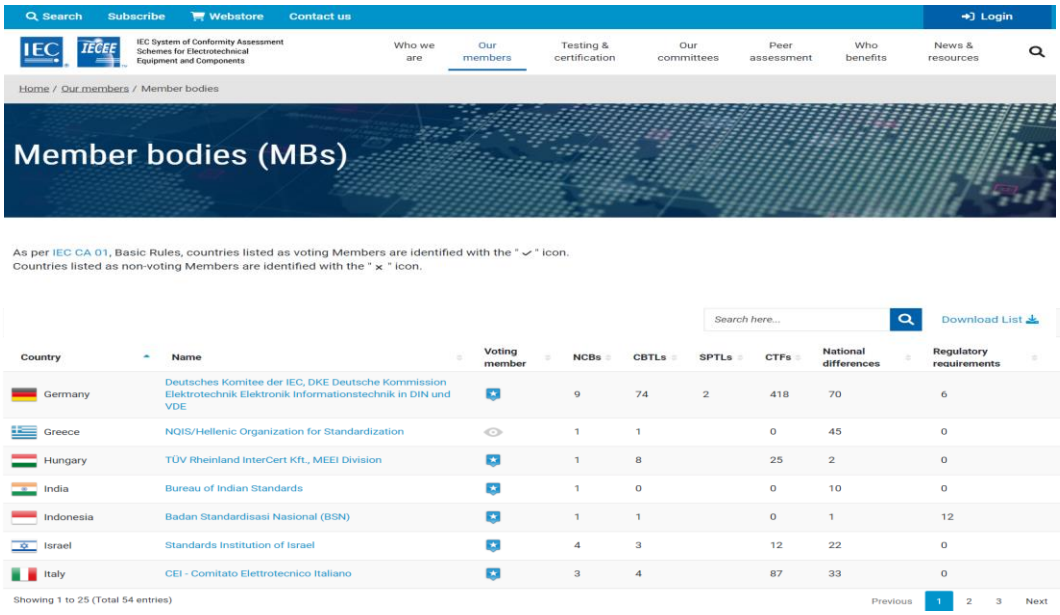
Συμμετοχή της Ελλάδος (ΕΥΠ) στο CCRA



Σημείωση: Από *Members of the CCRA* by CommonCriteria.org, 2023, Ανακτήθηκε στις 27/03/23, https://www.commoncriteriaportal.org/ccra/members/.

Εικόνα Ε9

Συμμετοχή της Ελλάδος, με καθεστώς παρατηρητή, στο IECEE



Σημείωση: Από *Member Bodies (MB's)* by IECEE.ord, 2023, Ανακτήθηκε στις 27/03/23, https://www.iecee.org/members/member-bodies.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ