Κυβερνοπόλεμος, Ασφάλεια & Στρατηγική. Δίκαιο και Ηθική. Εφαρμογές.

Η Περίπτωση της Τουρκίας.

Νικόλαος Παούνης

Ερευνητής του Επιστημονικού Οργανισμού Ε.Κ.Ε.Ο

Ιανουάριος 2019

ΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ Νο 99/2019

ΕΛΛΗΝΙΚΟ ΙΔΡΥΜΑ ΕΥΡΩΠΑΪΚΗΣ & ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Λεωφ. Βασιλίσσης Σοφίας 49, 10676, Αθήνα
Τηλ. 210 7257 110, Fax 210 7257 114, E-mail eliamep@eliamep.gr, www.eliamep.eu

ΕΛΛΗΝΙΚΟ ΙΔΡΥΜΑ ΕΥΡΩΠΑΪΚΗΣ ΚΑΙ ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ (ΕΛΙΑΜΕΠ)[1]
Λεωφ. Βασιλίσσης Σοφίας 49, 10676, Αθήνα
Τηλ: (+30) 210 7257110-1, fax: (+30) 210 7257114,
e-mail: eliamep@eliamep.gr,
url: www.eliamep.gr

Κείμενο Εργασίας Νο 99/2019

Κυβερνοπόλεμος, Ασφάλεια & Στρατηγική. Δίκαιο και Ηθική. Εφαρμογές.

Η Περίπτωση της Τουρκίας.

Νικόλαος Παούνης

Ερευνητής του Επιστημονικού Οργανισμού Ε.Κ.Ε.Ο

[1] Το ΕΛΙΑΜΕΠ δεν υιοθετεί ως ίδρυμα πολιτικές θέσεις. Καταβάλλει μάλιστα προσπάθεια να παρουσιάζονται στα πλαίσια των εκδηλώσεων του και στο μέτρο του δυνατού όλες οι υπάρχουσες απόψεις. Υπό το πρίσμα αυτό, οι αναλύσεις και οι γνώμες που δημοσιεύονται στις σειρές του θα πρέπει να αποδίδονται αποκλειστικά στους συγγραφείς και να μην θεωρούνται ότι αντιπροσωπεύουν απαραίτητα τις απόψεις του ιδρύματος, του διοικητικού συμβουλίου του, της διεύθυνσης ή των κατά περίπτωση και καθ' οιονδήποτε τρόπο συνεργαζομένων φορέων.

Σύντομο Βιογραφικό:

Ο Νικόλαος Παούνης γεννήθηκε στην Πτολεμαΐδα Εορδαίας. Είναι αριστούχος απόφοιτος του Τμήματος Βαλκανικών, Σλαβικών και Ανατολικών Σπουδών του Πανεπιστημίου Μακεδονίας. Το 2017 εισήχθη στο Πρόγραμμα Μεταπτυχιακών Σπουδών του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών, με κατεύθυνση τις Στρατηγικές Σπουδές. Το 2018 εισήχθη στο ΠΜΣ "Δημόσιες χρήσεις της Ιστορίας" του Πανεπιστημίου Δυτικής Μακεδονίας (πρώτος επιτυχών). Το 2013 δημοσίευσε την πρώτη Διατριβή με τίτλο "Ίμια 1996", έχοντας ως κύριο θέμα διαπραγμάτευσης την ομώνυμη κρίση, αναλύοντας παράλληλα σειρά στρατιωτικών, διπλωματικών, πολιτικών και νομικών παραμέτρων. Το 2016 δημοσίευσε τη δεύτερη επιστημονική συγγραφική εργασία με τίτλο: "Ιστορική και Κριτική Προσέγγιση της Ανθρωπιστικής Επέμβασης. Περιπτωσιολογία, Νομικά και Θεωρητικά Ζητήματα. Το Κοσσυφοπέδιο". Συμμετείχε σε 4 πανεπιστημιακά συνέδρια (στο πλαίσιο των οποίων, παρουσίασε έρευνες σχετικά με γεωπολιτικά και ιστορικά ζητήματα). Επιπλέον, πραγματοποίησε επιστημονικές δημοσιεύσεις και δημοσιοποιήσεις άρθρων σε έγκυρα περιοδικά (Εκδόσεις Πανεπιστημίου Αιγαίου, Foreign Affairs, CNN, Στρατηγική κ.ά.), και άρθρων σε εφημερίδες (ΚΑΘΗΜΕΡΙΝΗ, RealNews), με θεματολογία που άπτεται της επιχειρησιακής διάστασης της σύγκρουσης Ισραήλ-Χεζμπολά στο Λίβανο (2006), τον Υβριδικό το Δικτυοκεντρικό και τον Πληροφοριοκεντρικό πόλεμο, θέματα στρατιωτικών Δογμάτων, τη διεθνοπολιτική διάσταση των ελληνοτουρκικών σχέσεων, πτυχές του Μακεδονικού προβλήματος κ.α. Το 2018 αναδημοσιεύτηκαν άρθρα στην Τουρκία (από τα εθνικά ΜΜΕ). Ήταν συνεργάτης του Ινστιτούτου Geostrategic Forecasting Corporation of Chicago. Από τον Ιούνιο του 2017 εργάζεται ως ερευνητής του επιστημονικού οργανισμού Ε.Κ.Ε.Ο. (Ελληνικό Κέντρο Ελέγχου Όπλων). Είναι συνεργάτης του ελληνικού "think tank" ΕΛΙΑΜΕΠ. Ομιλεί Αγγλικά, Τουρκικά και τη γλώσσα της Π.Γ.Δ.Μ.

Περίληψη:

Συνεχίζοντας τις θεματικές δημοσιεύσεις ως προς την εξέλιξη του Πολέμου, μετά και τη λεγόμενη «Επανάσταση στις Στρατιωτικές Υποθέσεις», αναπτύσσουμε στο παρόν κείμενο εργασίας, τον Πληροφοριοκεντρικό Πόλεμο και την Κυβερνοασφάλεια. Η Κυβερνοεπίθεση είναι μια νέα μορφή πολέμου, η οποία συμβαδίζει με τις κοινωνικοπολιτικές προεκτάσεις οι οποίες προκύπτουν από την τεχνολογική εξέλιξη. Παράλληλα τίθενται εκ νέου ζητήματα όπως η Ηθική και η εφαρμογή των διατάξεων του Διεθνούς Δικαίου. Η Εσθονία αποτέλεσε τον πρώτο Δρώντα, ο οποίος δέχτηκε μαζικά μια κυβερνοεπίθεση. Η Τουρκία προσδίδει βαρύτητα, αλλά και εφαρμόζει ήδη την προλεγόμενη μορφή Πολέμου.

Κυβερνοπόλεμος, Ασφάλεια & Στρατηγική. Δίκαιο και Ηθική. Εφαρμογές.
Η Περίπτωση της Τουρκίας.

Αδιαμφισβήτητα βιώνουμε την εποχή της πληροφορίας («information age», ευρέως γνωστή ως ψηφιακή εποχή ή περίοδος της ψηφιακής επανάστασης), την περίοδο δηλαδή όπου οι εφαρμογές της τεχνολογίας (π.χ. κινητά τηλέφωνα, υπολογιστές, tablets κ.α.), της πληροφορικής (λογισμικά συσκευών π.χ. Windows, android κτλ), βελτίωσαν ποιοτικά τη ζωή των πολιτών, καθώς η συγκέντρωση, επεξεργασία και ανταλλαγή πληροφοριών δημιούργησε ένα νέο πλαίσιο στους τομείς παροχής υπηρεσιών, έρευνας, συναλλαγών κ.ο.κ. Ο Ιστορικός του μέλλοντος θα αναφέρεται σε κοσμογονικές μεταβολές σε όλα τα πεδία της ανθρώπινης δραστηριότητας και βέβαια οι προειρημένες αλλαγές επηρεάζουν καίρια τους τομείς της εσωτερικής ασφάλειας και της εθνικής άμυνας.

Η πρώιμη μορφή του Διαδικτύου απαντάται ως ARPA-NET (Advanced Research Project Agency), και αφορούσε στρατιωτική εφαρμογή την οποία ανέπτυξε στο Αμερικανικό Πεντάγωνο τη δεκαετία του 60. Η ανάγκη για την ανάπτυξη του ARPA-NET προέκυψε εξαιτίας του μεγάλου όγκου πληροφοριών που απαιτούνταν να διακινηθεί μεταξύ των Ερευνητών που εμπλέκονταν στα στρατιωτικά προγράμματα των ΗΠΑ.[2] Στις αρχές της δεκαετίας του 80, η υιοθέτηση ενός ενιαίου πρωτοκόλλου μετάδοσης πληροφοριών (TCP/IP Transmission Control Protocol/ Internet Protocol), και η απόσπαση των στρατιωτικών δραστηριοτήτων μέσω του MILNET (Military Network, σήμερα S.I.P.R.NET), συντέλεσε στη ραγδαία εξέλιξη των «ειρηνικών χρήσεων και εφαρμογών» του Διαδικτύου.[3]

Μετά το πέρας της ψυχροπολεμικής περιόδου, οι ΗΠΑ επέτρεψαν την ανάπτυξη και ευρεία χρήση του Διαδικτύου, με αποτέλεσμα τη σταδιακή δικτύωση μεταξύ ιδιωτικών επιχειρήσεων, νοικοκυριών, δημόσιων υπηρεσιών, γεγονός καθοριστικό για την αύξηση της επιρροής του Διαδικτύου στο σύνολο των ανθρώπινων δραστηριοτήτων και κατ επέκταση στην ασφάλεια. Στη σημερινή εποχή, αφενός η αλληλεξάρτηση μεταξύ κοινωνίας και υποδομών από το Διαδίκτυο αυξάνεται συνεχώς,

[2] https://www.britannica.com/topic/ARPANET

[3] http://www.differencebetween.net/technology/protocols-formats/differences-between-niprnet-and-siprnet/

αφετέρου διαχρονικά παρατηρείται ένα έλλειμμα ασφάλειας κατά τη χρήση του διαδικτύου, συνεπώς εγείρεται ζήτημα κατά πόσο υπάρχει δυνατότητα να θωρακιστούν οι οικονομικές, βιομηχανικές και κοινωφελείς υποδομές έναντι κακόβουλων λογισμικών.[4]

Οι τηλεπικοινωνίες και οι πληροφορίες αποτελούν ζωτικής σημασίας παραμέτρους για την επιτυχή διεξαγωγή πολεμικών επιχειρήσεων. Στόχος κάθε στρατιωτικής ενέργειας είναι η επικράτηση έναντι του αντιπάλου, με όσο το δυνατόν χαμηλότερες απώλειες σε σύντομο χρονικό διάστημα. Στον τομέα του «Κυβερνοπολέμου» (cyber warfare), το πεδίο της μάχης είναι ο Κυβερνοχώρος (cyber space), δηλαδή ένα πεδίο μάχης στο διαδικτυακό φάσμα χωρίς φυσικό χώρο (γεωγραφικό μήκος, πλάτος). Ως Κυβερνοχώρος νοείται η γενικότερη διαδικτύωση ανθρώπων, εταιρειών, υπηρεσιών κ.ο.κ. μέσω των Η/Υ και των τηλεπικοινωνιών, ανεξαρτήτως γεωγραφικού χώρου. Ο Κυβερνοχώρος δεν αποτελεί ένα ενιαίο πεδίο, αφού κάθε επιμέρους δίκτυο δημιουργεί το δικό του αυτοτελή κυβερνοχώρο (π.χ. Διαδίκτυο). Συμπερασματικά οι κυβερνοχώροι είναι πολυάριθμοι, ενώ η διαστρωμάτωση ενός κυβερνοχώρου διακρίνεται σε τρεις κατηγορίες **i)** το hardware (Η/Υ) **ii)** τη σημασιολογική (περιεχόμενο πληροφορίας) **iii)** τη συντακτική (software, λειτουργικά, εφαρμογές κτλ).[5]

Εξαιτίας των νέων δεδομένων που προέκυψαν, αναπτύχθηκε μια καινοφανής στρατηγική αντίληψη περί του λεγόμενου «Πληροφοριοκεντρικού Πολέμου» (Info Based Warfare).[6] Ο Πληροφοριοκεντρικός (ή Πληροφοριακός) Πόλεμος – όπως και ο Δικτυοκεντρικός – έχει ως βασικό πυρήνα τις δραστηριότητες γύρω από την έννοια της «πληροφορίας», μπορεί δε να ενταχθεί σ' ένα πλαίσιο «Μη Γραμμικού Πολέμου», προκειμένου ένας δρών (Κράτος, Διεθνής Οργανισμός, παραστρατιωτική οργάνωση, πολιτοφυλακή, τρομοκρατική ομάδα κ.α.), να επιβληθεί έναντι του αντιπάλου με τρόπο αιφνίδιο και αποτελεσματικό. Ο Πληροφοριακός Πόλεμος επικεντρώνεται, ωστόσο, στη συλλογή, αξιολόγηση και διανομή της πληροφορίας, χωρίς να περιλαμβάνει τις περαιτέρω προεκτάσεις του Δικτυοκεντρικού πολέμου (π.χ. διακίνηση δεδομένων από τα κέντρα επιχειρήσεων προς τα μέσα κρούσης). Μια «ειδικότερη υποκατηγορία» του Πληροφοριοκεντρικού πολέμου, θεωρείται ο Κυβερνοπόλεμος.

Οι σκοποί στη διάρκεια ενός «Κυβερνοπολέμου» συνοψίζονται ως εξής: Κυβερνοάμυνα: δηλαδή **α)** προστασία ημέτερων πληροφοριακών συστημάτων και πληροφοριών από εχθρική κυβερνοεπίθεση, **β)** αποσιώπηση εχθρικών πληροφοριών. Στο πλαίσιο μιας Κυβερνοεπίθεσης, οι στόχοι είναι οι κάτωθι: **α)** πρόσβαση και εκμετάλλευση πληροφοριών του εχθρού **β)** προσβολή εχθρικών πληροφοριακών συστημάτων **γ)** διασπορά ειδήσεων μέσω του διαδικτύου και των ΜΜΕ με περιεχόμενο που θα μπορούσε να επηρεάσει αρνητικά το ηθικό των πολιτών και των στρατευμάτων της αντιμαχόμενης χώρας, οργάνωσης κτλ. Οι επιθέσεις αυτές μπορούν να γίνουν μέσω της χρήσης κακόβουλων λογισμικών (ιούς, Trojan Horse etc), ή μέσω της εσκεμμένης αποστολής

[4] Sreltsov. International Information Security. Description and Legal Aspects. Disarmament Forum.Vol.3.p 4,5.

[5] Libicki Martin: Conquest in Cyberspace.p.8-28

[6] Γρίβας Κ. Ο Πόλεμος στον 21ο Αιώνα. Σελ.28.

μεγάλου όγκου πληροφοριών σ' ένα σύστημα (αδυναμία επεξεργασίας και κατάρρευση ή προβληματική λειτουργία του συστήματος). Τα προειρημένα θεωρούνται ως τα όπλα μιας κυβερνοεπίθεσης (cyber attack).[7]

Μέσω μιας κυβερνοεπίθεσης, είθισται να επιδιώκεται εναλλακτικά **α)** η διακοπή της λειτουργίας του συστήματος (επίθεση σε υποδομές π.χ. δίκτυο διανομής ηλεκτροδότησης) **β)** ο αποκλεισμός χρηστών από την πρόσβαση σ' ένα σύστημα (π.χ. απαγόρευση χρήσης υπηρεσιών) **γ)** η κυβερνοκατασκοπεία (συλλογή απόρρητων πληροφοριών) και **δ)** η αλλοίωση των δεδομένων που διακινούνται σ' ένα σύστημα (λ.χ. καταστροφή ή μεταβολή περιεχομένου ιστοσελίδων στο πλαίσιο ΨΕΠ). Οι στόχοι αυτοί δύναται να περιλαμβάνουν τις εχθρικές τηλεπικοινωνίες, το δίκτυο ύδρευσης, τα χρηματοπιστωτικά ιδρύματα, τις μεταφορές, τις τραπεζοασφαλιστικές και ταχυδρομικές υπηρεσίες και, τέλος, τις στρατιωτικές εγκαταστάσεις. Το πλεονέκτημα του Κυβερνοπολέμου έγκειται στο γεγονός ότι η επίθεση σχεδόν ανέξοδα, χωρίς την εμπλοκή συμβατικών μέσων κρούσης (αεροσκάφη, πυραύλους κτλ), μπορεί δε να επιφέρει σχεδόν ίδιας σημασίας πλήγματα σε εγκαταστάσεις ζωτικής σημασίας, και να οδηγήσει στην κατάρρευση του αντίπαλου κράτους. Επίσης, μπορεί να προλειάνει το έδαφος για μια δεύτερη επίθεση με συμβατικά όπλα. Η «μη γραμμικότητα» της επίθεσης, μπορεί να προκαλέσει χάος, αποσυντονισμό των υπηρεσιών του κράτους και καταβαράθρωση του ηθικού του λαού.

Οι αθέμιτες πράξεις μπορεί να εκπορεύονται από μεμονωμένους hackers, ή ολιγομελείς εγκληματικές οργανώσεις, όπου συνήθως η πρόθεση είναι η υπεξαίρεση περιουσιακών στοιχείων των θυμάτων, να προσελκύσει την προσοχή των ΜΜΕ κ.α. Στον αντίποδα μπορεί να βρίσκονται οργανωμένες στρατιωτικές υπηρεσίες Κυβερνοπολέμου μιας χώρας, εθνικές μυστικές υπηρεσίες ή διεθνείς τρομοκρατικές-παραστρατιωτικές οργανώσεις, όπου στην περίπτωση αυτή πρόθεση μπορεί να αποτελεί η επίτευξη συγκεκριμένων στρατιωτικών στοχεύσεων, ο μαζικός εκφοβισμός του πληθυσμού της αντίπαλης χώρας κτλ. Ωστόσο, η προειρημένη κατηγοριοποίηση δεν είναι απολύτως εφικτή εξαιτίας των δυσδιάκριτων ορίων μεταξύ μιας πράξης Κυβερνοπολέμου και Κυβερνοεγκλήματος.

Το γεγονός ότι κυβερνοεπιθέσεις ενορχηστρώνονται από κρατικές υπηρεσίες μιας χώρας και στοχεύουν τις υποδομές ενός έτερου κράτους συνεπάγεται εχθρική πράξη, δηλαδή είναι μια πολεμική ενέργεια, και φυσικά έχει αντίκτυπο στις διμερείς σχέσεις, συνεπώς δύναται να αποτελέσει αντικείμενο μελέτης των Διεθνών Σχέσεων. Επίσης, θα πρέπει να διέπεται από τους κανόνες του Διεθνούς Δικαίου και του Δικαίου Ενόπλων Συρράξεων (Συμβατικό και Εθιμικό). Ο Πόλεμος και η Κοινωνία εξελίσσονται, οπότε απαιτείται αναπροσαρμογή των έως σήμερα ισχυόντων κανόνων.

[7] Woods Ben, Wired, 09/05/2017: https://www.wired.co.uk/article/ransomware-viruses-trojans-worms

Δίκαιο και Ηθική στον Κυβερνοπόλεμο

Ο ΟΗΕ μέσω άρθρων του Καταστατικού Χάρτη[8], απαγορεύει τη χρήση βίας στις διακρατικές σχέσεις, πλην της νόμιμης αυτοάμυνας και της λήψης σχετικής απόφασης από το Σ.Α. Περαιτέρω διευκρινήσεις ως προς το τι συνιστά επίθεση έδωσε το ψήφισμα 3314 του ΟΗΕ (A/RES/29/3314) της 14ης Δεκεμβρίου 1974, σύμφωνα με το οποίο: «*Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition. *Explanatory note: In this Definition the term "State":(**a**) Is used without prejudice to questions of recognition or to whether a State is a member of the United Nations, (**b**) Includes the concept of a "group of States" where appropriate*».[9]

Από τον ορισμό συνάγεται το συμπέρασμα ότι αφορά την κρατική χρήση ένοπλης βίας έναντι μιας άλλης κρατικής οντότητας. Επομένως γεννώνται ερωτήματα όπως αν μια κυβερνοεπίθεση μπορεί να υπαχθεί στις εχθρικές ενέργειες **i)** εφόσον εκτελείται από μια παραστρατιωτική οργάνωση **ii)** εφόσον δεν χρησιμοποιούνται υλικά μέσα στη διάρκεια της **iii)** εφόσον δεν στοχεύει στην εδαφική επικράτεια του αντιπάλου αλλά στις υποδομές κ.α. Δηλαδή αν υφίσταται το περίφημο ***Jus ad Bellum*** (Δικαίωμα προσφυγής στη χρήση βίας σύμφωνα με τα παρακάτω κριτήρια: δίκαια υπόθεση, νόμιμη δικαιοδοσία, καλές προθέσεις, πιθανότητα επιτυχίας, έσχατο μέσο και αναλογικότητα.). Στο σημείο αυτό επιχειρείται μια ταξινόμηση βάσει 3 κριτηρίων. **α)** βαθμός εμπλοκής κρατικών υπηρεσιών του επιτιθέμενου μέρους **β)** μέσα επιθέσεως και **γ)** αποτέλεσμα. Οι δυσχέρειες που προκύπτουν είναι σχεδόν ανυπέρβλητες διότι είναι δύσκολο να αποκαλυφθεί από πού εκπορεύεται μια κυβερνοεπίθεση (π.χ. εκτέλεση από μεμονωμένους hackers που προσελήφθησαν από μια κυβέρνηση). Επίσης η προσβολή μονάδων του συστήματος υγείας (νοσοκομεία, ΜΕΘ, Κέντρα Υγείας κτλ), αν και «άυλη» θα μπορούσε να προκαλέσει εκατόμβη θυμάτων. Τέλος προκύπτει δικαίωμα αντεπίθεσης κατόπιν μιας κυβερνοεπίθεσης, και αν ναι με συμβατικά μέσα εφόσον δεν υπάρχει αντίστοιχη επάρκεια στον κυβερνοπόλεμο;

Το έτος 2001 η Ευρωπαϊκή Ένωση με τη Σύμβαση της Βουδαπέστης[10], προσπάθησε να κανονικοποιήσει ορισμένα ανάλογα ζητήματα και να θεσπίσει κοινή πολιτική μεταξύ των Κρατών-Μελών για την αντιμετώπιση των εγκλημάτων του Κυβερνοχώρου. Ωστόσο, η Σύμβαση εστιάζει περισσότερο στην εναρμόνιση των κρατικών νομοθεσιών για την αντιμετώπιση τρομοκρατικών ενεργειών στον κυβερνοχώρο, παρά στις διακρατικές κυβερνοδιενέξεις. Με αφορμή την επίθεση κατά

[8] Άρθρα 2,39,41 και 51.

[9] http://www.un-documents.net/a29r3314.htm

[10] Council of Europe. European Treaty Series No 185. Convention on Cybercrime. Budapest 23/10/2001.http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

της Εσθονίας το 2007, εντός του ΝΑΤΟ προκλήθηκε η συζήτηση για τυχόν τροποποιήσεις του άρθρου 5 ώστε να συμπεριληφθούν οι κυβερνοεπιθέσεις στις κατηγορίες επιθέσεων που δύναται να προκαλέσουν την ενεργοποίηση της αμοιβαίας συνδρομής μεταξύ των μελών της Συμμαχίας.

Όσον αφορά την Ηθική διάσταση του Πολέμου, εξετάζονται δύο θεμελιώδη ερωτήματα. Το ηθικό της προσφυγής στη χρήσης βίας, και τι είναι ηθικά επιτρεπτό στη διάρκεια του Πολέμου. Στον κυβερνοπόλεμο οι απαντήσεις στα ερωτήματα είναι εκ πρώτης όψεως αυτονόητες και προσδιορίσιμες, καθώς οι επιθέσεις μπορούν να περιοριστούν σε έκταση (δυσκολότερο να επιτευχθεί με κλασικά επιθετικά μέσα), τα αποτελέσματα μπορούν να είναι στοχευμένα και αναίμακτα (ηθική διάσταση). Η αποφυγή του ανθρώπινου πόνου ικανοποιεί τους υποστηρικτές της θεωρίας του Ωφελιμισμού (utilitarianism), αλλά και προσδίδει ισχύ ανυπολόγιστης αξίας, πάγιο στόχο σύμφωνα με τη θεωρία του Ρεαλισμού.

Εσθονία 2007

Στις 27 Απριλίου 2007 η εσθονική κυβέρνηση απομάκρυνε ένα μνημείο της σοβιετικής περιόδου από κεντρικό σημείο του Talin, με αποτέλεσμα να προκληθεί ένταση στις ρωσοεσθονικές σχέσεις. Την ίδια μέρα εξαπολύθηκε μαζική κυβερνοεπίθεση κατά δικτυακών τόπων, όπως του Κοινοβουλίου, των υπουργείων, των δημοσίων υπηρεσιών, κατά των έξι μεγάλων τραπεζών και των ιδιωτικών επιχειρήσεων. Ο Τύπος έκανε λόγο για τον πρώτο κυβερνοπόλεμο. Ο Υπουργός Άμυνας της χώρας, Jaak Aaviksoo, έκανε λόγο για επιθέσεις από ένα εκατομμύριο υπολογιστές «ζόμπι», δηλαδή «μολυσμένες» συσκευές χωρίς να το γνωρίζει ο κάτοχος, οι οποίοι μετατράπηκαν σε πιόνια. Επίσης συμπλήρωσε ότι οι διευθύνσεις IP αντιστοιχούσαν σε Η/Υ της Ρωσίας. Ο εκπρόσωπος της ρωσικής κυβέρνησης απέρριψε κάθε εμπλοκή στην υπόθεση. Στη διάρκεια των επιθέσεων παρατηρήθηκε αλλοίωση ιστοσελίδων και αδυναμία χρήσης διαδικτύου σε ορισμένες περιπτώσεις. Η μεταγενέστερη έρευνα εντόπισε τις πηγές επίθεσης σε ΗΠΑ, Ρωσία, Λατινική Αμερική, αλλά και στο εσθονικό έδαφος.

Οι ανακοινώσεις της Εσθονικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, δεικνύουν τον πολύ υψηλό βαθμό δικτύωσης της χώρας. Οι τραπεζικές συναλλαγές γίνονταν σε ποσοστό 98% διαδικτυακά, ενώ η χρήση ίντερνετ άγγιζε το 66% του πληθυσμού. Επιθέσεις δέχτηκε το Κοινοβούλιο, τα πολιτικά κόμματα, Υπουργεία, Τράπεζες και δημοφιλείς οργανισμοί ειδήσεων.[11]

[11] Σπηλιωτόπουλος Δ. Η έννοια και ο ορισμός του φαινομένου του Κυβερνοπολέμου, μέσα από μια ανάλυση των πληροφοριών των ψηφιακών Μέσων ενημέρωσης. Σελ.58,59.

Τουρκία και Κυβερνοπόλεμος.

Αρχές Οκτωβρίου, ο Πρόεδρος **Recep Tayyip Erdoğan**, μιλώντας στην Άγκυρα, επισήμανε την ανάγκη μετασχηματισμού του τουρκικού εκπαιδευτικού συστήματος, σύμφωνα με τις απαιτήσεις της ψηφιακής κοινωνίας διότι τούτο είναι ζωτικής σημασίας για το λαμπρό και ασφαλές μέλλον της χώρας, ενώ σε μια αποστροφή του λόγου του υπερτόνισε τη σημασία της ασφάλειας στον κυβερνοχώρο και τις πληροφορίες, ενώ σημείωσε ότι οι μελλοντικοί πόλεμοι θα γίνονται με κυβερνοεπιθέσεις και όχι με συμβατικά όπλα.[12]

Η Τουρκία εξαπέλυσε μαζικές κυβερνοεπιθέσεις κατά του δικτύου τηλεπικοινωνιών του YPG, στη διάρκεια της επιχείρησης «Κλάδος Ελαίας/Zeytin Dali». Το αποτέλεσμα ήταν άμεσο καθώς παρέλυσε κάθε μορφή συνεννόησης μεταξύ των μαχητών της κουρδικής πολιτοφυλακής. Τα επιχειρησιακά πλεονεκτήματα εμφανή. Η Τουρκική Αεροπορία δεν σπατάλησε πόρους (προσωπικό, καύσιμα, πυρομαχικά) για να καταστρέψει το δίκτυο (κεραίες, σταθμούς αναμετάδοσης κτλ). Το δίκτυο κατέρρευσε άμεσα, και κάθε δυνατότητα συνεννόησης κατέστη ανέφικτη.[13]

[12] **Daily Sabah. 03/10/2018: https://www.dailysabah.com/politics/2018/10/04/turkey-sees-strengthening-education-system-with-reforms-innovation-essential-for-digital-future**

[13] Παούνης Νικόλαος. Ανασκόπηση της δράσης των ΤΕΔ στο Αφρίν. Defencereview (24/03/18).

ΠΗΓΕΣ:

- Daily Sabah: https://www.dailysabah.com/politics/2018/10/04/turkey-sees-strengthening-education-system-with-reforms-innovation-essential-for-digital-future
- Featherly Kevin. Britannica Encyclopedia. ARPANET. U.S. Defense Program.
- Geers. Cyberspace and the Changing Nature of Warfare. Hakin9. Magazine (6).
- Libicki Martin: Conquest in Cyberspace. Cambridge University Press. 2007.
- Sreltsov. International Information Security. Description and Legal Aspects. Disarmament Forum.Vol.3.2007.
- Watts S. Combatant Status and Computer Network Attack. Virginia Journal of International Law (2010).
- Woods Ben. Wired: Viruses, Trojans, Malware, Warms. What's the difference? 09/05/2017
- Γρίβας Κωνσταντίνος: Ο Πόλεμος τον 21ο Αιώνα. Εκδόσεις Επικοινωνίες Α.Ε. (1999).
- Καραμπελιάς Γ. Κοινωνιολογία και Ένοπλες Δυνάμεις. Νομική Βιβλιοθήκη (2009).
- Ντόκος Θ. και Τσάκωνας Π. Στρατηγική Εθνικής Ασφαλείας. Εκδόσεις Παπαζήση, Αθήνα (2005).
- Παούνης Ν. Ανασκόπηση της Δράσης των Τ.Ε.Δ. στο μέτωπο του Αφρίν. Συνέντευξη στο Defencereview. 24 Μαρτίου 2018.

- Σπηλιωτόπουλος Δ. Η έννοια και ο ορισμός του φαινομένου του Κυβερνοπολέμου, μέσα από μια ανάλυση των πληροφοριών των ψηφιακών Μέσων ενημέρωσης: Οι περιπτώσεις του BBC και του CNN. Πάντειο Πανεπιστήμιο. Σχολή Κοινωνικών και Πολιτικών Επιστημών (2012).