ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ, ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΣΤΙΣ «ΔΙΕΘΝΕΙΣ ΚΑΙ ΕΥΡΩΠΑΪΚΕΣ ΣΠΟΥΔΕΣ»

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Υβριδικός πόλεμος και τρομοκρατία στο διαδίκτυο»

Παλιάτσου Θεοδώρα - Δήμητρα

Επιβλέπουσα καθηγήτρια: Μπόση Μαίρη

Αθήνα, Απρίλιος 2021

<u>Υπεύθυνη Δήλωση</u>

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις, που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι

αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από

άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν

γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου

αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

Η Δηλούσα

Παλιάτσου Θεοδώρα-Δήμητρα

Περίληψη

Σκοπός της εργασίας είναι η παρουσίαση των συγκρούσεων υβριδικού τύπου και ηλεκτρονικής τρομοκρατίας ως αποτέλεσμα της εξέλιξης της τεχνολογίας, του Διαδικτύου και του ταχύτατου ρυθμού αύξησης των προβλημάτων της Παγκοσμιοποίησης, τα οποία οδηγούν σε ένα χαοτικό περιβάλλον στον χώρο των Διεθνών Σχέσεων.

Στο πρώτο κεφάλαιο γίνεται αναφορά στην έννοια του υβριδικού πολέμου, της ασύμμετρης απειλής καθώς και στα χαρακτηριστικά αυτής της μορφής πολέμου μέσα από δημόσια διαθέσιμες πληροφορίες (internet) που περιέχονται σε επίσημα έγγραφα, επιστημονικά άρθρα και μελέτες τρίτων.

Στο δεύτερο κεφάλαιο της εργασίας αναλύονται οι έννοιες του Κυβερνοχώρου, του Κυβερνοεγκλήματος, της Τρομοκρατίας και γενικά του Οργανωμένου Ηλεκτρονικού Εγκλήματος. Γίνεται αναφορά στην Ενωσιακή Πολιτική για την καταπολέμηση του εγκλήματος-τρομοκρατίας στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών. Επιπλέον τονίζεται η μεταφορά της Ενωσιακής Νομοθεσίας για το Κυβερνοέγκλημα στην Ελληνική Νομοθεσία.

Στο τρίτο κεφάλαιο γίνεται αναφορά στον Κυβερνοπόλεμο, στην Κυβερνοασφάλεια, στις Ενωσιακές Δράσεις και Διεθνείς Συνεργασίες για την αντιμετώπιση των προκλήσεων που θέτουν σήμερα οι Κυβερνοαπειλές και καθιστούν αναγκαία την αποτελεσματική αντίδραση σε διασυνοριακό επίπεδο.

Η σημασία της προστασίας των Υποδομών Ζωτικής Σημασίας και των κοινωνικών λειτουργιών τονίζεται ιδιαίτερα, καθώς ο ρόλος τους είναι πρωταγωνιστικός στα ζητήματα κυβερνοασφάλειας σε παγκόσμιο επίπεδο.

Το Νομοθετικό Πλαίσιο της Ε.Ε. και η ασυνεπής όμως μεταφορά του στο Εθνικό Δίκαιο των κρατών μελών αποτελεί τροχοπέδη για την πλήρη εφαρμογή της Ενωσιακής Νομοθεσίας.

Στο τέταρτο κεφάλαιο αναφέρονται παραδείγματα υβριδικών πολέμων και τα συμπεράσματα της ανάλυσης που τίθενται προς συζήτηση.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1: Έννοια και περιεχόμενο υβριδικού πολέμου

Εισαγωγή

Στο σύγχρονο περιβάλλον, τα παγκόσμια προβλήματα αυξάνουν την πολυπλοκότητα της εθνικής, περιφερειακής και παγκόσμιας ασφάλειας, οι στρατιωτικοπολιτικοί, οικονομικοί και περιβαλλοντικοί παράγοντες αλλάζουν συνεχώς, ενώ οι εθνικές ,θρησκευτικές και εθνοτικές αντιπαραθέσεις γίνονται περισσότερο ορατές και έντονες[1].

Στο πλαίσιο του συστήματος των Διεθνών Σχέσεων προκύπτει μια παγκόσμια κρίση που είναι σε θέση να μεταβάλλει τα θεμελιώδη στοιχεία των σημερινών ρυθμίσεων ασφαλείας. Η παγκοσμιοποίηση έχει θέσει σε κίνηση μια διαδικασία καθολικών εκτεταμένων μεταβολών, καθώς έχει μετασχηματιστεί η μορφή του πολέμου αλλά και η έννοια της ασφάλειας. Εξαιτίας της δομής που έχει το διεθνές σύστημα, τα κράτη αλλά και η εφαρμογή των νέων τεχνολογιών, οι συγκρούσεις και ο πόλεμος έχουν προσαρμοστεί στις απαιτήσεις των καιρών. Η αύξηση της προβληματικής φύσης των διαδικασιών της παγκοσμιοποίησης παρέχει ενδείξεις σοβαρών ελλείψεων στο διεθνές σύστημα ασφάλειας[2].

Στην σφαίρα των Διεθνών Σχέσεων το κρίσιμο ζήτημα είναι η εμφάνιση του νέου- υβριδικού-τύπου συγκρούσεων με τη χρήση μη συμβατικών μέσων (πολιτικά, οικονομικά κ.α.) για την πραγμάτωση πολιτικών και στρατηγικών στόχων στον αγώνα κατά του αντιπάλου[3]. Οι ερευνητές δεν έχουν καταλήξει ακόμα στον ορισμό του φαινομένου, γιατί μολονότι η χρήση ανορθόδοξων μέσων σε μια σύγκρουση δεν συναντάται τον 21ο αιώνα για πρώτη φορά, όμως σίγουρα πρόκειται για μια πραγματικότητα, την οποία τα κράτη καλούνται να αντιμετωπίσουν. Η δράση παραστρατιωτικών ομάδων, κρατικών και μη κρατικών φορέων, τρομοκρατικών οργανώσεων και μορφωμάτων συμπίπτει με τη ραγδαία εξέλιξη τεχνικών και μεθόδων, ώστε οι συμβατικές δυνάμεις να αντιμετωπίζουν σοβαρά θεσμικά εμπόδια στην αντιμετώπιση της.

Κάποια κράτη θα αναδυθούν πιο ισχυρά -με περισσότερη επιρροή και ασφάλεια- από αυτή τη μετάβαση στην ψηφιακή εποχή, επωφελούμενα από ισχυρές συμμαχίες και έξυπνη χρήση της

[1] Manko, O., & Mikhieiev, Y. (2018). Defining the Concept of 'Hybrid Warfare' Based on the Analysis of Russia's Aggression against Ukraine. Information & Security: An International Journal, 41, 11–20.

[2] Ομοίως

[3] Ομοίως

ψηφιακής δύναμης, ενώ άλλα κράτη θα μοχθούν για να προλάβουν τις εξελίξεις και να προσαρμοστούν στις τεχνολογικές αλλαγές στο εσωτερικό τους και παγκόσμια[4].

Φιλίες, συμμαχίες και έχθρες ανάμεσα στα κράτη θα επεκταθούν και στον εικονικό κόσμο, προσθέτοντας μια νέα διάσταση στον τρόπο που παραδοσιακά σχετίζονται τα κράτη. Από πολλές απόψεις, το Διαδίκτυο μπορεί να ιδωθεί σαν την πραγματοποίηση της κλασικής θεωρίας των διεθνών σχέσεων, ενός αναρχικού και χωρίς αρχηγούς κόσμου[5].

Ορισμοί - Έννοιες

Ασύμμετρη απειλή

Γενικά, ασύμμετρος θεωρείται ο πόλεμος που διενεργείται από οργανωμένες μη-συμβατικές ομάδες, βασίζεται στην αναίρεση των κανόνων του δικαίου και του δικαίου του πολέμου, ενώ χρησιμοποιεί κυρίως χαμηλού σχετικά κόστους όπλα και επιχειρησιακή δράση που προκαλεί όμως, δυσανάλογα, μεγάλου (ασύμμετρου) κόστους αποτελέσματα στον υπέρτερο αντίπαλο, τόσο σε ανθρώπινες ζωές και υλικό επίπεδο, όσο και σε ψυχολογικό και κοινωνικό . Κύριος σκοπός του είναι η εξασθένιση/κάμψη της αποφασιστικότητας και της αποτελεσματικής χρήσης των συντελεστών ισχύος του υπέρτερου αντιπάλου.

Στις ασύμμετρες απειλές/συγκρούσεις συγκαταλέγονται ακόμη οι επιθέσεις ανταρτών, τρομοκρατικών ομάδων ή άλλων οργανωμένων οντοτήτων που ενστερνίζονται τα ανωτέρω, και μπορεί να χρησιμοποιούν από συμβατικά ή αυτοσχέδια όπλα μέχρι όπλα μαζικής καταστροφής WMD (Weapons of Mass Destruction), πχ μικρά πυρηνικά (mini πυρηνικές βόμβες πλουτωνίου), ραδιολογικά (π.χ. dirty bombs), χημικά και βιολογικά όπλα. Ιστορικά, τέτοιες μεθόδους ακολούθησαν ασθενέστερες δυνάμεις εναντίον πολύ ισχυρότερων αντιπάλων (κυβερνήσεων κρατών ή πολυεθνικών οντοτήτων, πχ συλλογικών οργανισμών άμυνας και ασφάλειας).

[4] Eric Schmidt, Jared Cohen: Η Νέα Ψηφιακή Εποχή-Οι επιπτώσεις στα Έθνη, την Επιχειρηματικότητα και τη Ζωή μας. Το Μέλλον των Κρατών Κεφ.3 σελ.118

[5] Eric Schmidt, Jared Cohen: Η Νέα Ψηφιακή Εποχή-Οι επιπτώσεις στα Έθνη, την Επιχειρηματικότητα και τη Ζωή μας. Το Μέλλον των Κρατών Κεφ.3 σελ.118

Υβριδικός Πόλεμος

Πρόκειται για συνδυασμό στοιχείων που αφορά έναν τύπο πολέμου για τον ορισμό του οποίου η διεθνής επιστημονική κοινότητα ακόμη δεν έχει καταλήξει. Ο William Lind, τονίζει ότι ο υβριδικός πόλεμος είναι στην ουσία «η επιστροφή στον τρόπο διεξαγωγής του πολέμου πριν την εμφάνιση του κυρίαρχου κράτους. Σαφώς τα μέσα και οι τεχνικές έχουν εξελιχθεί και πολλαπλασιαστεί, όμως η διάκριση μεταξύ συμμάχου και εχθρού, μαχητή και αμάχου, παραμένει δύσκολη» (Lind, 2004, σελ.14)[6]. Οι περισσότεροι αναλυτές κάνουν λόγο για παράλληλη χρήση διαφορετικών εργαλείων σε ευρύ φάσμα, όπως συμβατικές στρατιωτικές δυνάμεις, τεχνολογία, εγκληματικότητα, τρομοκρατία, άσκηση οικονομικής πίεσης, ανθρωπιστικά και θρησκευτικά μέσα, παραπληροφόρηση, σαμποτάζ. «Όλες οι παραδοσιακές, ασυνήθιστες ή καταστροφικές μορφές του πολέμου είναι μέρος ενός παράδοξου συνδυασμού με καταστροφική ικανότητα και εκτελούνται πάντοτε από κοινού ως τμήμα μιας ευέλικτης στρατηγικής που μπορεί να λάβει τη μορφή μυστικής εισβολής» (Kramer και Gordon, 2014, σελ.27)[7].

Στο διαδίκτυο ο «υβριδικός πόλεμος» ερμηνεύεται ως *«στρατιωτική στρατηγική που χρησιμοποιεί πολιτικό πόλεμο και συνδυάζει συμβατικό πόλεμο, ακανόνιστο πόλεμο και κυβερνοπόλεμο»*[8]. Ο όρος χρησιμοποιείται για να χαρακτηρίσει την περίπλοκη δυναμική του πεδίου μάχης, που προϋποθέτει την ταχεία προσαρμογή και την γρήγορη ευελιξία και ανταπόκριση.

B. Nemmet (Lieutenant Colonel of the US Marine Corps)

Θεωρεί τον «υβριδικό πόλεμο» ως ένα σύγχρονο είδος ανταρτοπόλεμου, που ενσωματώνει καινοτόμες τεχνολογίες και σύγχρονες μεθόδους κινητοποίησης.

Mc Cuen (Colonel in the US Army)

[6] https://pdfs.semanticscholar.org/6a5b/b09bc4b54074b08799be962a6da02c9b9169.pdf(accessed in 29/09/2017)

[7] https://www.nytimes.com/2014/08/28/world/europe/ukraine-russia-novoazovsk-crimea.html (accessed in 26/09/2017).

[8] https://www.academia.edu/36236087/%CE%A5%CE%B2%CF%81%CE%B9%CE%B4%CE%B9%CE%BA%CF%8C%CF%82_%CE%A0%CF%8C%CE%BB%CE%B5%CE%BC%CE%BF%CF%82_Hybrid_Warfare_

Δηλώνει ότι «ο υβριδικός πόλεμος είναι η κύρια μέθοδος των στρατιωτικών επιχειρήσεων στον ασύμμετρο πόλεμο, ο οποίος λαμβάνει χώρα σε τρεις περιοχές μάχης: μεταξύ του πληθυσμού της ζώνης συγκρούσεων, του τοπικού πληθυσμού, και της Διεθνούς Κοινωνίας.»[9]

R. Work (US Navy representative) εξηγεί ότι σε έναν «υβριδικό πόλεμο» οι εχθρικές δυνάμεις μπορούν ακόμη και να χρησιμοποιήσουν στρατιωτικούς, κρυμμένους μεταξύ του άμαχου πληθυσμού. »

David Kilcullen

Ο υβριδικός πόλεμος, κατά τον Kilcullen-Αμερικανό στρατιωτικό, θεωρητικό και συγγραφέα του βιβλίου The Accidental Guerilla (Ο Τυχαίος Αντάρτης)- αποτελεί αντιπροσωπευτικό παράδειγμα των σύγχρονων συγκρούσεων σε συνδυασμό με Αντάρτικες τακτικές, τρομοκρατικές μεθόδους, εμφύλιους πολέμους και εξεγέρσεις.

NATO[10]

Το 2009 για την διαμόρφωση ενός συνεκτικού ορισμού για τις πιθανές μελλοντικές συγκρούσεις η Διοίκηση μετασχηματισμού της νατοϊκής συμμαχίας παρουσίασε μία ερευνητική έκθεση με τίτλο “Multiple futures project – Navigating towards 2030”που δείχνει αντιλήψεις και στάσεις σε πιθανά αναπτυξιακά σενάρια του περιβάλλοντος ασφαλείας και τη φύση των πιθανών στρατιωτικών συγκρούσεων.

Μία από τις κατευθύνσεις για την ανάπτυξη των δυνατοτήτων της Συμμαχίας που αναπτύχθηκαν σε αυτή την έκθεση ήταν "η προσαρμογή στις απαιτήσεις των υβριδικών απειλών". Το σημείο ενδιαφέροντος είναι ότι ένας πιθανός εχθρός θα αποφύγει μια άμεση επαφή με τις δυνάμεις του NATO σε συμβατικές επιχειρήσεις, αντ’ αυτού θα χρησιμοποιήσει παράτυπες δυνάμεις και ασύμμετρες μορφές αντιπαράθεσης.

Ο «υβριδικός εχθρός» αναμένεται να περιλαμβάνει τακτικές και παράτυπες δυνάμεις, στοιχεία για την τρομοκρατία και το έγκλημα, τα οποία θα συνεργάζονται συνδυαστικά. Αξίζει να

[9] Jon McCuen, “Hybrid Wars,” Military Review 88, no. 2 (March-April 2008): 107-113, quote on p. 107.

[10] Manko & Mikhieiev. (2018). DEFINING THE CONCEPT OF ‘HYBRID WARFARE’ BASED ON ANALYSIS OF RUSSIA’S AGGRESSION AGAINST UKRAINE VOL 41, 11–20. https://doi.org/10.11610/isij.4107

τονιστεί ότι ο «υβριδικός εχθρός» δεν αναμένεται να τηρήσει τους διεθνείς κανόνες σύγκρουσης[11].

Daniel Lasica, Αξιωματικός της Πολεμικής Αεροπορίας των ΗΠΑ και συγγραφέας του Strategic Consequences of Hybrid Wars: The Theory of Victory εξέτασε το πληροφοριακό-ψυχολογικό στοιχείο ως βάση του υβριδικού πολέμου, ενώ η δημόσια συνείδηση (χειρισμός της κοινής γνώμης) -και όχι οι στρατιωτικές δυνάμεις ή οι υποδομές – είναι ο κύριος στόχος των εμπνευστών των πολεμικών συγκρούσεων. Επιπλέον, οι υβριδικές απειλές έχουν ασαφή χαρακτήρα, είναι δύσκολο να προσδιοριστούν, αποκτώντας ένα πολυδιάστατο χαρακτήρα[12].

William. J. Nemeth, Οι υβριδικές δυνάμεις μπορούν να ενσωματωθούν αποτελεσματικά στη στρατηγική και το δυναμικό της δομής τεχνολογικών προηγμένων συστημάτων και να χρησιμοποιηθούν αυτά τα συστήματα πέραν των προβλεπόμενων παραμέτρων χρήσης τους. Επιχειρησιακά, οι υβριδικές στρατιωτικές δυνάμεις μέσα στο περιορισμένο λειτουργικό τους φάσμα, είναι ανώτερες των Δυτικών δυνάμεων[13].

Ο Philp και ο Martin προτείνουν μια άλλη σημαντική πτυχή του υβριδικού πολέμου που ονομάζεται χρονική σύγκλιση όταν *«… η ανθρώπινη αντίληψη των γεγονότων στο χρόνο, και η αξία της γνώσης που υποτιμάται με το πέρασμα του χρόνου από την αβεβαιότητα και τις αντιθέσεις, μπορούν να καθορίσουν ένα νέο/μελλοντικό σύστημα αξιών (ή στόχων)[14] »*

Πολλοί στρατιωτικοί αναλυτές έχουν επισημάνει ότι οι μελλοντικές συγκρούσεις θα γίνονται με πολλούς διαφορετικούς τρόπους ή με πολλές παραλλαγές και δεν θα μπορούν να χαρακτηριστούν ως μια απλή μορφή πολέμου. Έτσι ζητούν μεγαλύτερη προσοχή στις συγκρούσεις που δεν έχουν ορατό χαρακτήρα και ενσωματώνουν πολλαπλές μορφές πολέμου σε συνδυασμό με την αυξανόμενη συχνότητα τους και θνησιμότητα που προκαλούν.

Αυτή η έννοια περιγράφεται συχνότερα ως «υβριδικός πόλεμος», στον οποίο ο αντίπαλος πιθανότατα θα παρουσιάζει μοναδικές συνδυαστικές ή υβριδικές απειλές που στοχεύουν

---

11 Manko & Mikhieiev. (2018). DEFINING THE CONCEPT OF 'HYBRID WARFARE' BASED ON ANALYSIS OF RUSSIA'S AGGRESSION AGAINST UKRAINE VOL 41, 11–20. https://doi.org/10.11610/isij.4107

12 Ομοίως.

13William. J. Nemeth, USMC, Future War and Chechnya: A Case for Hybrid Warfare (Monterey, CA: Naval Postgraduate School, June 2002).

14 Philp, W. R., & Martin, C. P. (2009). A philosophical approach to time in military knowledge management. Journal of Knowledge Management, 13(1), 171–183. https://doi.org/10.1108/13673270910931242

συγκεκριμένα τις αδυναμίες των ΗΠΑ. Αντί για διαφορετικούς ταραξίες με θεμελιωδώς διαφορετικές προσεγγίσεις (συμβατικές, παράτυπες ή τρομοκρατικές), μπορούμε να περιμένουμε να αντιμετωπίσουμε αντιπάλους που θα χρησιμοποιούν ταυτόχρονα όλες τις μορφές πολέμου και τακτικής. Η εγκληματική δραστηριότητα μπορεί επίσης να θεωρηθεί μέρος αυτού του προβλήματος, καθώς είτε αποσταθεροποιεί περαιτέρω την τοπική αυτοδιοίκηση είτε προκαλεί τον αντάρτη ή παράνομο πολεμιστή παρέχοντας τους επιπλέον πόρους[15].

Ένας από τους πρώτους υποστηρικτές του όρου είναι ο Frank Hoffman.[16] Με τους αντιπάλους να αναπτύσσουν όλο και περισσότερο ένα ολοκληρωμένο μείγμα συμβατικών δυνατοτήτων και παράτυπων τακτικών στο ίδιο πεδίο μάχης, ο Hoffman υποστήριξε ότι οι διακριτοί τρόποι πολεμικής μάχης, οι τρομοκρατικές ενέργειες και η εγκληματικότητα συγκλίνουν για να παράγουν μια υβριδική μορφή πολέμου. Μετά την προσάρτηση της Κριμαίας από τη Ρωσία, η ιδέα απέκτησε ευρύτερη δημοτικότητα και εισήλθε στο δυτικό στρατηγικό λεξικό. Κατά τη διαδικασία αυτή, απέκτησε μια πιο ευρεία έννοια για να αναφερθεί στη συνδυασμένη χρήση στρατιωτικών και μη στρατιωτικών, συμβατικών και μη συμβατικών, φανερών και συγκεκαλυμμένων μέσων άσκησης επιρροής[17].

Ο James Mattis, είναι ο πρώτος που χρησιμοποίησε τον όρο υβριδικός πόλεμος το Σεπτέμβριο του 2005 στο Άρλιγκτον, στο 4ο Sea Services Forum. Τον ίδιο χρόνο ο Mattis κι ο Hoffman διατύπωσαν τον υβριδικό πόλεμο ως απάντηση στη δήλωση των ΗΠΑ για την Εθνική Αμυντική Στρατηγική (NOS) όπου μία περιοχή με καταστροφικές αναταραχές απειλεί τα συμφέροντα των ΗΠΑ. Διαφώνησαν ως προς το ότι οι νέες μορφές συγκρούσεων δεν θα έχουν το χαρακτήρα του παραδοσιακού και συμβατικού πολέμου αλλά θα είναι υπό νέα μορφή που ονομάζεται υβριδικός πόλεμος. Ο Hoffman, τα επόμενα χρόνια, σε διάφορα άρθρα και βιβλία, ανέφερε ότι οι υβριδικές απειλές εμπεριέχουν μία μεγάλη ποικιλία από διαφορετικούς τρόπους πολέμου περιλαμβάνοντας συμβατικές μεθόδους, ακανόνιστες τακτικές, τρομοκρατικές ενέργειες βίας κι εξαναγκασμού κι εγκληματικότητα. Ο υβριδικός πόλεμος μπορεί να διεξαχθεί από κρατικούς και μη δρώντες. Σύμφωνα με τον Hoffman, τα βασικά χαρακτηριστικά είναι η πολλαπλών και διαφορετικών διαστάσεων δράση – multi dimensionality –, η χρήση όλων των

[15] Hoffman, F.G., "Hybrid Warfare and Challenges", Joint Forces Quarterly. 2009:52, 34–39.

[16] F. G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Warfare (Potomac Institute for Policy Studies, 2007);

[17] Sari, A. (2019). Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats. SSRN Electronic Journal, 1–24. https://doi.org/10.2139/ssrn.3315682

τομέων κι η εκμετάλλευση της πληροφορίας. Στον υβριδικό πόλεμο, χρησιμοποιούνται και προσαρμόζονται όλοι οι τρόποι συμβατικοί και μη, ώστε να κατακτηθεί ο στόχος με έμφαση στα μη συμβατικά μέσα πολέμου.

Σε άρθρο του το 2011, ο Hoffman, ανανεώνει τον ορισμό που είχε δώσει κι αναφέρεται στην εγκληματικότητα, την οποία αρκετές στρατιωτικές θεωρίες δεν αποδέχονται ως μέσο του υβριδικού πολέμου. Αναφέρει την ύπαρξη εκπαιδευτικών ιδρυμάτων που θα προάγουν τη δημιουργία και συγκρότηση δυνάμεων, ικανών να προσαρμοστούν και να αντιμετωπίσουν τις υβριδικές απειλές κι επιθέσεις.

Υπάρχει διαφορά στην πρόληψη των επιθέσεων κι στην αντιμετώπιση αυτών, καθώς χρησιμοποιείται διαφορετική μεθοδολογία στη διαδικασία της πρόληψης και διαφορετική στη διαδικασία πλέον της αντιμετώπισης.

Μετά την εδραίωση κι επισημοποίηση του όρου του υβριδικού πολέμου από τον Hoffman, θεωρείται πλέον κι ορθόδοξο μέσο πολέμου. Η χρήση της υβριδικής απειλής έχει ήδη υιοθετηθεί από το Υπουργείο Άμυνας των ΗΠΑ κι η αμυντική κοινότητα αποδέχεται αυτή τη μορφή στο σύγχρονο πόλεμο. Το ΝΑΤΟ κι η Σύνοδος Κορυφής της Ουαλίας συμφώνησε να λάβει μέτρα για την αντιμετώπιση των υβριδικών απειλών. Μελετώντας τον υβριδικό πόλεμο, μπορεί να συμπεράνει κανείς ότι στη σύγχρονη μορφή του τα βασικά χαρακτηριστικά είναι:

- Η θολή διάκριση μεταξύ πολιτικών και στρατιωτικών μέσων, η μίξη διαφορετικών μέσων από ένα ευρύ φάσμα – στρατιωτικές δυνάμεις, εγκληματικότητα, τρομοκρατία, οικονομικές πιέσεις, παραπληροφόρηση, κατασκοπεία, κοινωνικές και θρησκευτικές πιέσεις –
- Περιέχει μη κρατικούς δρώντες όπως οι παραστρατιωτικές οργανώσεις, εγκληματικές δράσεις κι ομάδες και τρομοκρατικό δίκτυο
- Σταθμίζει κάθε περίπτωση με σκοπό να χρησιμοποιηθούν παραδοσιακά και μοντέρνα μέσα ενημέρωσης για να κατασκευαστούν ειδήσεις, γεγονός που οδηγεί στον πόλεμο της πληροφορίας, τον ψυχολογικό πόλεμο μέσω της χειραγώγησης των μαζών και τον πόλεμο στο διαδίκτυο – Ρωσία-Ουκρανία, ομόφωνο παράδειγμα υβριδικού πολέμου από τη διεθνή κοινότητα.

Η στενή κατανόηση του υβριδικού πολέμου, όπως προτάθηκε αρχικά από τον Hoffman, περιγράφει μια μορφή επιχειρησιακής δράσης και, ως εκ τούτου, συνδέεται στενά με τη διεξαγωγή των εχθροπραξιών. Μοιράζεται αυτό το χαρακτηριστικό με τον ορισμό της Dunlap

για το lawfare[18]. Στην πραγματικότητα, το lawfare έχει προσδιοριστεί ως μια συγκεκριμένη υβριδική τεχνική πολέμου**[19]**. Το όφελος της στενής προοπτικής υβριδικού πολέμου είναι ότι εφιστά την προσοχή σε ορισμένες εχθρικές τακτικές. Αυτές περιλαμβάνουν την εύλογη άρνηση, τις παρεμβάσεις που δεν φθάνουν στο επίπεδο της απαγορευμένης παρέμβασης, ενεργώντας μέσω πληρεξουσίων, των επιχειρήσεων πληροφοριών και της χρήσης βίας κάτω από το όριο μιας ένοπλης επίθεσης. Αυτό εστιάζει επίσης την προσοχή σε ορισμένες νομικές δυσκολίες και τομείς του δικαίου, συμπεριλαμβανομένης της απόδοσης παράνομων πράξεων, του δικαίου των επιχειρήσεων στον κυβερνοχώρο, των αντιμέτρων, των κανόνων που διέπουν τη χρήση βίας και του δικαίου των ένοπλων συγκρούσεων**[20]**.

Ο υβριδικός πόλεμος ή αλλιώς hybrid warfare εμφανίζεται ως έννοια για πρώτη φορά στα συγγράμματα του Θουκυδίδη αναφορικά με τον Πελοποννησιακό πόλεμο και στον Σου Τσου στην «Τέχνη του πολέμου». Ο υβριδικός πόλεμος συνίσταται από την υβριδική απειλή και τη σύγκρουση. Σήμερα, λόγω της προόδου της τεχνολογίας, η ένταση και η κλίμακα αλλάζουν περιπλέκοντας την έννοια και προσδίδοντας ασάφεια στον όρο.

Ως υβριδικός πόλεμος ορίζεται η χρήση συμβατικών και μη, τακτικών και άτακτων, φανερών και συγκεκαλυμμένων μέσων και η εκμετάλλευση όλων των διαστάσεων του πολέμου, σε όλο το εύρος του για να καταπολεμηθεί η ανωτερότητα των συμβατικών όπλων, μεθόδων και τακτικών στο πεδίο της μάχης. Οι υβριδικές απειλές χρησιμοποιούν όλο το φάσμα του σύγχρονου πολέμου χωρίς να περιορίζονται στα συμβατικά μέσα και άρα στο συμβατικό πεδίο μάχης. Με τη χρήση ασύμμετρων τακτικών, οι υβριδικές απειλές εκμεταλλεύονται τις αδυναμίες του αντιπάλου, περιπλέκοντας με αυτόν τον τρόπο το πεδίο της μάχης. Συμπληρωματικά, ο υβριδικός πόλεμος είναι η σύζευξη πολλών και διαφορετικών δρώντων, μεθόδων και μεσών στο πεδίο των μαχών, μία σύρραξη κατά την οποία συμπράττουν συμβατικές και μη ένοπλες δυνάμεις για την επίτευξη ενός σκοπού. Εξακολουθεί βέβαια, να επικρατεί μία σύγχυση για τη φύση, την προέλευση και τον αντικειμενικό σκοπό της απειλής.

[18] Dunlap, C. (2008). "*Lawfare Today: A Perspective" https://www.yalejournal.org/search?q=lawfare*
«είναι η στρατηγική της χρήσης ή της κατάχρησης του δικαίου ως υποκατάστατο των παραδοσιακών στρατιωτικών μέσων για την επίτευξη ενός επιχειρησιακού στόχου».

[19] Munoz Mosquera, A. B., & Bachmann, S. D. (2016). Lawfare in Hybrid Wars: The 21st Century Warfare. Journal of International Humanitarian Legal Studies, 7(1), 63–87. https://doi.org/10.1163/18781527-00701008

[20] D. Cantwell, Hybrid Warfare: Aggression and Coercion in the Gray Zone, ASIL Insights, 29 November 2017, https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone.

Το επίπεδο εχθρότητας διατηρείται σε χαμηλότερο βαθμό απ' ότι σε έναν συμβατικό πόλεμο και η απειλή παραμένει σε μη εμπόλεμη κατάσταση. Επιτυγχάνεται η συγχρονισμένη χρήση πολλαπλών οργάνων ισχύος, εξατομικευμένα σε συγκεκριμένες αδυναμίες μέσα σε ένα μεγάλο εύρος κοινωνικών λειτουργιών για την επίτευξη κοινών στόχων[21].

Θα εξετάσουμε τη διαφορά με το συμβατικό πόλεμο, ο οποίος βάσει του διεθνούς δικαίου αναφέρεται στη σύγκρουση που διαδραματίζεται μεταξύ κυρίαρχων πολιτικών οντοτήτων – δηλαδή κρατών – ως τρόπος επίλυσης διαφορών με έσχατο τρόπο επίλυσης αυτών, τη χρήση βίας, που απαγορεύεται από τον Χάρτη των Ηνωμένων Εθνών.

Ο υβριδικός πόλεμος περιλαμβάνει ενδοκρατικές ή/και διακρατικές συγκρούσεις. Οι ενδοκρατικές συγκρούσεις διαθέτουν εγχώριους μηχανισμούς ειρηνικής επίλυσης διαφορών, χωρίς να έχουν πάντα κάποιο αποτέλεσμα, ενώ οι διακρατικές συγκρούσεις αναφέρονται σε συγκρούσεις μέσα σε διεθνή πλαίσια και καθεστώς αναρχίας με αποτέλεσμα την επιβίωση ή διάλυση του εκάστοτε κράτους.

Ο υβριδικός πόλεμος απαντάται και ως non-linear war (μη γραμμικός πόλεμος), hybrid threat (υβριδική απειλή), ή non-traditional war (μη παραδοσιακός πόλεμος).

Ο υβριδικός πόλεμος αφορά ένα είδος «αναμέτρησης» στη διάρκεια της οποίας γίνεται χρήση του συνόλου των διατιθέμενων πόρων ενός κράτους και του αποθέματος ισχύος, συνδυάζοντας συμβατικές και ανορθόδοξες επιχειρήσεις, καθώς επίσης και πολιτικά μέσα (πολιτικο-οικονομική διάσταση της σύγκρουσης). Εκτεταμένη θεωρείται και η χρήση μορφών Κυβερνοάμυνας (cyber war), καθώς επίσης και πληροφοριακών μέσων (μέσα μαζικής ενημέρωσης και κοινωνικής δικτύωσης). Αυτή ακριβώς η «συνύπαρξη» συμβατικών και ανορθόδοξων στοιχείων και τακτικών, οδήγησε στη χρήση του επιθέτου «υβριδικός». Στη διάρκεια της υβριδικής σύρραξης χρησιμοποιούνται ταυτοχρόνως δυναμικοί συνδυασμοί συμβατικών και μη τακτικών, τρομοκρατικών επιθέσεων και εν γένει εγκληματικών ενεργειών, ενώ η συγκεκριμένη έννοια μπορεί να απαντάται στις πολεμικές επιχειρήσεις ενός κρατικού ή μη κρατικού δρώντος. Συνήθως αφορά τη σύγκρουση μεταξύ κρατικών ενόπλων δυνάμεων και τρομοκρατικών/παραστρατιωτικών οργανώσεων[22].

[21] https://defencereview.gr/yvridikos-polemos-apo-ton-thoykydidi-s/

[22] Από Ανάλυση του κ. Νικολάου Παούνη Διεθνολόγου, Βαλκανιολόγου για λογαριασμό του Επιστημονικού φορέα ΕΚΕΟ (Ελληνικό Κέντρο Ελέγχου Όπλων)

Ο όρος «υβριδικός πόλεμος» εμφανίστηκε για πρώτη φορά το 2002 σε μια διατριβή του William J. Nemeth που περιγράφει τον τρόπο με τον οποίο οι Τσετσένοι αντάρτες συνδύασαν τον ανταρτοπόλεμο με τις σύγχρονες στρατιωτικές τακτικές και τη χρήση της κινητής και διαδικτυακής τεχνολογίας. Εκτός από τις εξαιρετικά ευέλικτες επιχειρησιακές τακτικές τους, οι Τσετσένοι χρησιμοποίησαν επίσης ενημερωτικές δραστηριότητες και ψυχολογικές επιχειρήσεις εναντίον των ρωσικών δυνάμεων.[23]

Ο όρος «υβριδικός πόλεμος» επίσης χρησιμοποιήθηκε για να αναφερθεί στις στρατηγικές των μη κρατικών παραγόντων, όπως η τρομοκρατική οργάνωση Χεζμπολάχ, αλλά απέκτησε νέα δυναμική μετά τις ρωσικές επιχειρήσεις στην Κριμαία και την Ανατολική Ουκρανία το 2014 όπου φάνηκε να ακολουθούν ένα σενάριο σε μεγάλο βαθμό σύμφωνα με το δόγμα του στρατηγού Valery Gerasimov του «μη γραμμικού πολέμου»[24].

Η Χεζμπολάχ, χρησιμοποίησε συμβατικό οπλοστάσιο, ασύμμετρες δυνάμεις και τακτικές ανταρτοπόλεμου, ψυχολογικές επιχειρήσεις, τρομοκρατία, εγκληματικές δραστηριότητες προκειμένου να αντιμετωπίσουν το Ισραήλ.

Η περίπτωση της Ρωσίας – Ουκρανίας, Κριμαία 2014, ξεκίνησε το Νοέμβριο του 2013 όταν Ουκρανοί διαδηλωτές ζητούσαν την προσχώρηση στην Ευρωπαϊκή σφαίρα επιρροής. Οι ρωσικές υβριδικές επιχειρήσεις χαρακτηρίζονται από:

- Προπαγάνδα: χειρισμός ΜΜΕ, αναζήτηση κι εκμετάλλευση των αδυναμιών του αντιπάλου και κινητοποίηση
- Ψυχολογικές επιχειρήσεις: επιρροή στην κοινή και διεθνή ουκρανική γνώμη, καλλιέργεια του αισθήματος κρίσης κι ηττοπάθειας
- Κυβερνοεπιθέσεις: ιός Snake, οι ηλεκτρονικοί υπολογιστές των ουκρανικών υπηρεσιών προσβλήθηκαν χωρίς να είναι δυνατή η ανίχνευση ιών στο λογισμικό για οκτώ χρόνια.
- Χρήση παραστρατιωτικών επιχειρήσεων: στρατιώτες χωρίς διακριτικά κι οικονομική ενίσχυση των στρατιωτών, εκπαίδευση κι εφοδιασμός με εξοπλισμό.

Η έννοια του «υβριδικού πολέμου» έχει επικριθεί πως ούτε νέα είναι, ούτε παρέχει μια πρόσθετη εξήγηση του σύγχρονου πολέμου. Όπως υποστηρίζει ο Damien Van Puyveld[25],

---

[23] Andras Racz. (2015). Russia' s Hybrid War in Ukraine: Breaking Enemy's Ability to Resist. FIIA Report 43, 2015, p.28, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ ukraine/

[24] Nicu Popescu, 'Hybrid tactics: Russia and the West', EUISS, October 2015, http://www.iss.europa.eu/uploads/media/Alert_46_Hybrid_Russia.pdf

[25] Daniel Van Puyveld. (2015). 'Hybrid war – does it even exist?' http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/

«κάθε απειλή μπορεί να είναι υβριδική, αρκεί να μην περιορίζεται σε μία μόνο μορφή και διάσταση του πολέμου. Όταν οποιαδήποτε απειλή ή χρήση βίας ορίζεται ως υβριδική, ο όρος χάνει την αξία του και προκαλεί σύγχυση αντί να αποσαφηνίσει την «πραγματικότητα» του σύγχρονου πολέμου»

Χαρακτηριστικά του υβριδικού πολέμου[26].

Μπορούμε να επισημάνουμε εξαρχής ως προσδιοριστικά χαρακτηριστικά του υβριδικού πολέμου (διεθνώς: H.W.) την περιπλοκότητα, την ευελιξία, τη ρευστότητα, και το «ακανόνιστο» της μορφής της απειλής, τη συνδυαστική χρήση συμβατικών και ανορθόδοξων τακτικών-μεθόδων, τη χρήση όπλων προηγμένης τεχνολογίας από παραστρατιωτικούς (που μέχρι προσφάτως εντάσσονταν αποκλειστικά στα κρατικά οπλοστάσια), ενώ ως «χώροι» διεξαγωγής της υβριδικής μάχης θεωρούνται παράλληλα το κλασσικό πεδίο αντιπαράθεσης, ο αυτόχθων πληθυσμός, πλησίον του οποίου λαμβάνει χώρα η σύγκρουση (π.χ. σε ρόλο πληροφοριοδότη, πολιτοφυλακής κ.ο.κ.), καθώς επίσης και η διεθνής κοινότητα.

Αναλυτικότερα τα χαρακτηριστικά του υβριδικού πολέμου έχουν ως εξής:

1. Ο συνδυασμός λειτουργιών: οι υβριδικές απειλές χρησιμοποιούν συνδυασμό συμβατικών και μη τακτικών μαζί με τρομοκρατία, εγκληματικές δραστηριότητες, επιθέσεις στον κυβερνοχώρο, διατάραξη της οικονομίας, της κοινωνίας και της πολιτικής εντός του εκάστοτε κράτους. Ο υβριδικός πόλεμος επεκτείνει τη χρήση βίας και άρα τον πόλεμο σε όλο το μήκος και πλάτος του.

2. Ταυτόχρονη δράση: οι υβριδικές απειλές μπορούν να χρησιμοποιήσουν διαφορετικούς τρόπους διένεξης ταυτόχρονα με τρόπο που να παρουσιάζει συνοχή. Πέραν της κάθετης κλιμάκωσης, την περεταίρω δηλαδή ένταση των στρατιωτικών επιθέσεων στο πεδίο της μάχης, η υβριδική απειλή διαθέτει και την οριζόντια κλιμάκωση· τη μεταφορά της επίθεσης από το ένα πεδίο στο άλλο ταυτόχρονα. Πολλαπλές επιθέσεις σε πολλαπλά πεδία άρα πόλεμος σε πολλαπλές διαστάσεις.

3. Συγχώνευση: μείγμα επαγγελματιών στρατιωτών, ανταρτών – μελών παραστρατιωτικών οργανώσεων – , τρομοκρατών και εγκληματιών. Για να νοείται μια

[26] https://defencereview.gr/yvridikos-polemos-apo-ton-thoykydidi-s

υβριδική απειλή, ενιαία, πρέπει να τους ενώνει ένα στοιχείο. Διαθέτουν κοινό εξατομικευμένο στόχο, ένα κοινό πολιτικό αποτέλεσμα.

4. Εγκληματικότητα: ένας υβριδικός πόλεμος δεν νοείται χωρίς εγκληματική δραστηριότητα. Οι υβριδικές απειλές δημιουργούν μία συνιστώσα διακυβέρνησης για να εγκαθιδρύσουν σταθερότητα και βιώσιμες επιχειρήσεις. Μία πολύ σημαντική μέθοδος που χρησιμοποιείται είναι η προπαγάνδα και η παροχή πληροφοριών σε περίπτωση πολέμου. Εκμεταλλεύονται τα παγκόσμια δίκτυα επικοινωνίας με σκοπό τη διάδοση του σχεδιασμού τους αλλά και ως μέθοδο εύρεσης χρηματοδότησης ή/και στρατολόγησης. Αψηφούν το διεθνές δίκαιο εν αντιθέσει με τους αντιπάλους τους – τα δυτικά κράτη – καθώς αυτό δρα περιοριστικά. Το διεθνές δίκαιο θέτει πλαίσια στον πόλεμο· ο υβριδικός πόλεμος όμως δεν έχει πλαίσια και οι κανόνες είναι διαφορετικοί για τους αντιπάλους.

Ο υβριδικός πόλεμος παρότι αποτελεί φαινόμενο με μακρά ιστορία από αρχαιοτάτων χρόνων, παραμένει δυναμικό ειδικά με την ανάπτυξη της τεχνολογίας που εμφανίζει νέες πτυχές του, ώστε με την πάροδο των χρόνων προστίθενται νέες διαστάσεις.

Το δόγμα Gerasimov

Το ρωσικό δόγμα γνωστό ευρέως στην Δύση και ως δόγμα Γκερασίμοφ (Gerasimov) αποτελεί ένα ολιστικό δόγμα επιχειρήσεων που εδράζεται στην καθολική θεώρηση του Πολέμου, βασισμένη στην πρότερη σοβιετική λογική του διαρκούς αγώνα τόσο εν καιρώ ειρήνης, όσο και εν καιρώ πολέμου για την επίτευξη των πολιτικών στόχων. Για τον Γκερασίμοφ και τους Ρώσους επιτελείς η σύγχρονη πολεμική σύγκρουση του 21ου αιώνα, περιλαμβάνει την συνδυαστική χρήση στρατιωτικής, πολιτικής οικονομικής και πληροφοριακής ισχύος από κρατικούς και μη κρατικούς δρώντες [27].

Το Δόγμα Γκερασίμοφ διατυπώνει μία νέα προσέγγιση στην έννοια διακρατική σύγκρουση, και αυτό γιατί θεωρεί εξ ίσου σημαντικές με τις στρατιωτικές, τις πολιτικές, οικονομικές, ανθρωπιστικές, επικοινωνιακές και άλλου είδους επιχειρήσεις[28].

[27] Κων/νος Θ. Λαμπρόπουλος, Στρατηγικός Αναλυτής και Εταίρος του Κέντρου Μελετών Ασφάλειας της Γενεύης σε συνέντευξη που δημοσιεύτηκε στις 25 Απριλίου 2019 στον ιστότοπο HuffPost Creece

[28] http://booksjournal.gr/%CE%B3%CE%BD%CF%8E%CE%BC%CE%B5%CF%82/item/2647-to-dogma-gerasimov

Στην περίπτωση της Ρωσίας, η αναθεώρηση του Αμυντικού Δόγματος στην κατεύθυνση της «ενοποιημένης χρήσης στρατιωτικών δυνάμεων και έτερων πόρων, των οποίων θα προηγείται η "προπαρασκευή" της διεθνούς κοινής γνώμης, μέσω των εφαρμογών του πληροφοριακού πολέμου», δημιούργησε την απαραίτητη βάση ώστε ο Υβριδικός Πόλεμος να θεωρείται η βάση επί της οποίας ερείδεται το σύνολο της σύγχρονης ρωσικής στρατιωτικής «σκέψης». Μετά τις επιχειρήσεις στην Τσετσενία (1994-2000) και τη Γεωργία (2008), κατέστη πασίδηλη η ανεπάρκεια της μαζικής και μονοδιάστατης χρήσης δυνάμεων ελιγμού, γεγονός το οποίο υποχρέωσε τη Ρωσική Ομοσπονδία σε γενικότερη αναδιοργάνωση των Ενόπλων Δυνάμεων. Σύντομα αλλαγές επήλθαν σε επίπεδο συμβατικών, ανορθόδοξων και πληροφοριακών επιχειρήσεων[29].

Μέθοδοι κατά Gerasimov

Διαχωρίζονται σε:

- Στρατιωτικές επιχειρήσεις εν καιρώ ειρήνης χωρίς να έχει κηρυχθεί πόλεμος
- Επιθέσεις «χειρουργικής ακρίβειας» σε πολιτικές ή στρατιωτικές υποδομές, στοχεύοντας στην στρατιωτική εξάντληση και πλήξη των οικονομικών πόρων
- Ταυτόχρονες επιθέσεις σε υπομονάδες και στρατιωτικές εγκαταστάσεις στην επικράτεια του αντιπάλου
- Ταυτόχρονη διεξαγωγή χερσαίων, θαλάσσιων κι αεροπορικών επιχειρήσεων, πληροφοριακών κι επιχειρήσεων κυβερνοπολέμου

  Ο συγχρονισμός των μέσων στοχεύει σε συγκεκριμένες αδυναμίες του αντιπάλου με διαδικασίες αυτοαξιολόγησης στις κρίσιμες λειτουργίες κι αδυναμίες κάθε τομέα.

Κβαντικές Δεξιότητες & Υβριδικός Πόλεμος

Στην μετανεωτερική εποχή, αφήνοντας πίσω μας τις βεβαιότητες της κλασσικής φυσικής, περνάμε πλέον στην κβαντική θεωρία, « έναν περίεργο κόσμο, έναν κόσμο απροσδιόριστο, του οποίου οι (σχεδόν ενοχλητικοί) νόμοι φαίνεται όχι μόνο να αναιρούν αλλά και να χλευάζουν

[29] Από Ανάλυση του κ. Νικολάου Παούνη Διεθνολόγου, Βαλκανιολόγου για λογαριασμό του Επιστημονικού φορέα ΕΚΕΟ (Ελληνικό Κέντρο Ελέγχου Όπλων)

τα παραδοσιακά όρια του χώρου, του χρόνου και της ύλης » (Zohar & Marshall, The Quantum Society, 1994)

Μια ομάδα συγγραφέων πρότεινε ότι η αρχή του εικοστού πρώτου αιώνα θα μπορούσε να ονομαστεί «Η Κβαντική Εποχή» -από τους μηχανιστικούς νόμους του Νεύτωνα της κλασικής φυσικής στις θεωρίες του χάους και της κβαντικής μηχανικής[30]. Αυτοί οι συγγραφείς υποστηρίζουν ότι οι νέες επιστήμες παρέχουν το εννοιολογικό θεμέλιο για ένα νέο σύνολο δεξιοτήτων για τους υπεύθυνους λήψης αποφάσεων - ένα σύνολο δεξιοτήτων, που μπορούν να τους επιτρέψουν να δουν τη σύγκρουση από μια νέα προοπτική , αλλά και να ανταποκριθούν στις συγκρούσεις με νέους τρόπους. Αυτή η αλλαγή επηρεάζει την άποψη των συγκρούσεων και, αντίστοιχα, των δεξιοτήτων που απαιτούνται για την αντιμετώπιση τους. Κατά τη διάρκεια των τελευταίων ετών αρκετοί συγγραφείς χρησιμοποιούν την κβαντική θεωρία στην εργασία της εκ νέου αναζήτησής τους ως μεταφορά, για την ανάπτυξη ενός νέου συνόλου δεξιοτήτων που αφορούν στους υπεύθυνους λήψης αποφάσεων, τις αποκαλούμενες κβαντικές δεξιότητες.

Η έννοια των κβαντικών δεξιοτήτων αντιστοιχεί στους στόχους της προσομοίωσης-βασισμένης μάθησης και θα χρησιμοποιηθεί από τους συντάκτες ως ακρογωνιαίος λίθος του μεθοδολογικού πλαισίου τους στον υβριδικό πόλεμο[31].

[30] Darling, J. R. (1999). Organizational excellence and leadership strategies: principles followed by top multinational executives. Leadership & Organization Development Journal, 20(6), 309–321. https://doi.org/10.1108/01437739910292625

[31] Vassileva, B., & Zwilling, M. (2018). Hybrid Warfare Simulation-based Learning: Challenges and Opportunities. Information & Security: An International Journal, 39(3), 220–234.

ΚΕΦΑΛΑΙΟ 2: Διαδίκτυο – Εγκληματικότητα - Τρομοκρατία

Εισαγωγή

Το Διαδίκτυο συγκαταλέγεται στα κορυφαία επιτεύγματα του ανθρώπου και τα οποία όμως δεν κατανοεί πλήρως. Αυτό, που ξεκίνησε, σαν ένας τρόπος μεταφοράς ηλεκτρονικών πληροφοριών από υπολογιστή σε υπολογιστή, τότε μεγέθους δωματίου, έχει μεταμορφωθεί σε ένα μέσον πανταχού παρόν, σε μια ατελεύτητη πολυεπίπεδη διέξοδο για ανθρώπινη δραστηριότητα και έκφραση. Είναι εντελώς ακανόνιστο ενώ συνεχώς μεταλλάσσεται, μεγαλώνει και γίνεται όλο και πιο πολύπλοκο.

Είναι μια πηγή απίστευτα καλού και δυνητικά τρομακτικά κακού, εξαιτίας των επιπτώσεων που θα έχει στο παγκόσμιο γίγνεσθαι.

Βασικές έννοιες του διαδικτύου

- Μία διεύθυνση IP (IP address - Internet Protocol address), είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών
- Οι δυναμικές διευθύνσεις IP/ Οι στατικές διευθύνσεις IP
- Το Πρωτόκολλο Διαδικτύου έχει δύο κύριες εκδόσεις σε χρήση, την IPv4 και την IPv6.
- Πάροχος Υπηρεσιών Διαδικτύου (Internet Service Provider) Είναι μια εταιρεία (ιδιωτική ή δημόσια), που μας παρέχει την δυνατότητα να έχουμε πρόσβαση στο Διαδίκτυο
- Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών, που χρησιμοποιούν το πρωτόκολλο IP
- Ένας διακομιστής DNS είναι ένας διακομιστής υπολογιστή που περιέχει μια βάση δεδομένων με δημόσιες διευθύνσεις IP ή και ιδιωτικές και τα αντίστοιχα ονόματα κεντρικών υπολογιστών και χρησιμεύει για την επίλυση ή τη μετάφραση αυτών των κοινών ονομάτων σε διευθύνσεις IP όπως-ζητήθηκε

Κυβερνοχώρος[32]

Το Διαδίκτυο είναι το μεγαλύτερο πείραμα σε ολόκληρη την ιστορία που περιέχει την έννοια της αναρχίας. Εκατοντάδες εκατομμύρια άνθρωποι, κάθε λεπτό, δημιουργούν και καταναλώνουν έναν ανείπωτο όγκο ψηφιακού περιεχομένου σε έναν διαδικτυακό κόσμο που είναι αδύνατο να ελεγχθεί.

Στο παγκόσμιο γίγνεσθαι, η πιο σημαντική επίπτωση της εξάπλωσης της τεχνολογίας των επικοινωνιών θα είναι ο τρόπος με τον οποίο, οι τεχνολογίες αυτές βοηθάνε να αναδιανεμηθεί η συγκέντρωση της εξουσίας μακριά από κράτη και θεσμούς, στα χέρια των ατόμων.

Καθώς αυτός ο χώρος μεγαλώνει, όλο και περισσότερο, ο τρόπος που αντιλαμβανόμαστε σχεδόν κάθε πλευράς της ζωής μας αλλάζει, από τις μικρολεπτομέρειες της καθημερινότητάς μας μέχρι τις πιο θεμελιώδεις ερωτήσεις περί ταυτότητας, σχέσεων, ακόμα και περί ασφάλειας.

Μέσω αυτής της πλατφόρμας έχει καταστεί δυνατόν, σχεδόν για όλους ,να έχουν, να αναπτύσσουν και να διαδίδουν περιεχόμενο, σε πραγματικό χρόνο, χωρίς να πρέπει να βασίζονται σε άλλους-μεσάζοντες.

Η έλλειψη όμως ελέγχου του διαδικτύου επιτρέπει τις διαδικτυακές απάτες, τις καμπάνιες εκφοβισμού, τους ιστότοπους των ομάδων μίσους και τα «δωμάτια συζητήσεων»(chat rooms) των τρομοκρατών.

Η πρόσβαση στην πληροφορία και στα νέα κανάλια επικοινωνίας σημαίνει νέες ευκαιρίες για συμμετοχή, ώστε να διατηρείται υπόλογη η εξουσία και να βελτιώνεται η ζωή του πολίτη.

Μέσα στην ιστορία, η έλευση των νέων τεχνολογιών επικοινωνίας έδωσε δύναμη σε αλλεπάλληλα ανθρώπινα κύματα, εις βάρος των παραδοσιακών φορέων της εξουσίας, είτε αυτοί ήταν ο βασιλιάς, η εκκλησία ή οι διάφορες ελίτ.

Η διάδοση της συνδεσιμότητας, ειδικά μέσω κινητών τηλεφώνων με σύνδεση στο Διαδίκτυο, είναι σίγουρα το πιο κοινό και ίσως το πιο προφανές παράδειγμα μεταφοράς της δύναμης.

Τελικά αυτή η μεταφορά δύναμης στα άτομα, θα οδηγήσει σε έναν πιο ασφαλή, ή σε έναν πιο επικίνδυνο κόσμο;

[32] Eric Schmidt, Jared Cohen: Η Νέα Ψηφιακή Εποχή-Οι επιπτώσεις στα Έθνη, την Επιχειρηματικότητα και τη Ζωή μας. Εισαγωγή σελ.15-25

Η απάντηση δεν είναι προαποφασισμένη. Το μέλλον θα διαμορφωθεί από το πώς τα κράτη , οι πολίτες, οι εταιρείες και οι θεσμοί θα χειριστούν τις νέες τους ευθύνες.

Τα κράτη ασκούν εσωτερικές και εξωτερικές πολιτικές με στόχο να μεγιστοποιήσουν την επιρροή και την ασφάλειά τους. Οι στόχοι των κρατών δεν θα αλλάξουν, οι απόψεις τους για το πώς θα εκπληρωθούν, θα αλλάξουν.

Θα πρέπει να δοκιμάσουν δύο εκδοχές των εσωτερικών και εξωτερικών πολιτικών τους - μια για τον πραγματικό, «αληθινό» κόσμο και μια για τον εικονικό κόσμο που υπάρχει στο Διαδίκτυο. Αυτές οι πολιτικές μπορεί να φαίνονται αντικρουόμενες κάποιες φορές - οι κυβερνήσεις μπορεί να παίρνουν αυστηρά μέτρα στον ένα κόσμο ενώ να επιτρέπουν συγκεκριμένες συμπεριφορές στον άλλο· μπορεί να πηγαίνουν σε πόλεμο στον κυβερνοχώρο αλλά να διατηρούν την ειρήνη στον πραγματικό κόσμο- αλλά για τα κράτη, οι πολιτικές αυτές θα είναι προσπάθειες να διαχειριστούν τις νέες απειλές και προκλήσεις που ενθαρρύνει η συνδεσιμότητα.

Σημαντικά γεγονότα συνέβησαν στον κόσμο, γεγονότα τα οποία αντικατόπτριζαν τις έννοιες και τα προβλήματα της νέας ψηφιακής εποχής. Η κινεζική κυβέρνηση εξαπέλυσε πολύπλοκες κυβερνοεπιθέσεις στη Google και σε δεκάδες άλλες αμερικανικές εταιρείες· η WikiLeaks[33] εμφανίστηκε στο προσκήνιο, και δημοσιοποίησε εκατοντάδες χιλιάδες απόρρητα έγγραφα παγκοσμίως· τεράστιοι σεισμοί σε Αϊτή και Ιαπωνία κατέστρεψαν πόλεις, αλλά γέννησαν καινοτόμες τεχνολογικές λύσεις, ως απάντηση στα προβλήματα ανοικοδόμησης· και οι επαναστάσεις της Αραβικής Άνοιξης[34] ταρακούνησαν τον κόσμο με την ταχύτητά τους, τη δυναμική τους και τη «μολυσματική» κινητοποίηση τους. Κάθε ταραχώδης εξέλιξη εισήγαγε νέες απόψεις και δυνατότητες για το μέλλον του κόσμου.

[33] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200461

[34] Αραβική Άνοιξη 2010-2014, ονομάστηκε το κύμα διαδηλώσεων και διαμαρτυριών στη Μέση Ανατολή και τη Βόρεια Αφρική, που ξεκίνησε στις 18 Δεκεμβρίου του 2010. Κοινό γνώρισμα των διαδηλώσεων ήταν οι μαζικές διαμαρτυρίες με καμπάνιες, απεργίες, πορείες, καθώς και η χρήση κοινωνικών δικτύων όπως το Facebook, το Twitter και το YouTube, για την οργάνωση, την επικοινωνία, και την ενημέρωση για τις προσπάθειες των κρατών για καταπίεση και λογοκρισία.

Οργανωμένο Έγκλημα-Τρομοκρατία

« Οργανωμένη Εγκληματική Ομάδα» σημαίνει μια δομημένη ομάδα τριών ή περισσότερων προσώπων που υφίσταται για κάποια χρονικό περίοδο και ενεργεί από κοινού με σκοπό να τελέσει ένα ή περισσότερα σοβαρά εγκλήματα ή αδικήματα που θεσπίζονται σύμφωνα με το άρθρο 2 της Σύμβασης των Ηνωμένων Εθνών(Η.Ε.), έτσι ώστε να προσπορισθεί, άμεσα ή έμμεσα, οικονομικό ή άλλο υλικό όφελος.

Οι τρομοκρατικές ομάδες[35] ενδέχεται να εμπλέκονται άμεσα στο οργανωμένο έγκλημα ή να συνδέονται με εγκληματίες και εγκληματικές ομάδες, σε τομείς όπως η παράνομη διακίνηση όπλων και ναρκωτικών, ανθρώπων, ή στην οικονομική απάτη, στη νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες και εκβιασμούς. Αν και οι στόχοι των τρομοκρατικών ομάδων μπορεί να διαφέρουν από αυτούς του οργανωμένου εγκλήματος, οι μεταξύ τους δραστηριότητες εμφανίζονται αυξανόμενες, καθώς οι τρομοκρατικές οργανώσεις χρηματοδοτούνται από εγκληματικές ενέργειες.

Ένας ορισμός για την Τρομοκρατία του 1988 από τους ακαδημαϊκούς Schmidt και Jongman, με ευρεία απήχηση και αποδοχή, έχει ως εξής: "Η τρομοκρατία είναι μια μέθοδος επαναλαμβανόμενων πράξεων βίας, στην οποία εμπλέκονται σχετικά κρυφά άτομα, ομάδες ή κρατικοί δρώντες, λόγω ιδιοσυγκρασίας, εγκληματικών ή πολιτικών λόγων, και όπου, σε αντίθεση με τη δολοφονία, οι άμεσοι στόχοι της βίας δεν αποτελούν και τον απώτερο σκοπό αυτής. Τα δε άμεσα θύματα επιλέγονται τυχαία ή μέσω συμβολικής στοχοποίησης, ως μέρος ενός ευρύτερου πληθυσμού-στόχου στον οποίο αποσκοπεί η πράξη, λειτουργώντας ως μήνυμα προς αυτόν. Έτσι, διαμέσου του θύματος, αποκαθίσταται μια επικοινωνία μεταξύ των δρώντων και του -τελούντος σε κίνδυνο- ακροατηρίου, μέσω της επιδίωξης τρομοκράτησης, της προβολής απαιτήσεων ή της έλκυσης προσοχής, ανάλογα με την τελική στόχευση, που μπορεί να είναι ο εκφοβισμός, ο πειθαναγκασμός ή η προπαγάνδα"[36].

Το νέο εγκληματικό τοπίο που εμφανίζεται σήμερα χαρακτηρίζεται από ομάδες υψηλής κινητικότητας και ευελιξίας που δρουν σε πολλές χώρες και σε πολλούς τομείς εγκληματικότητας μέσω της παράνομης και ευρείας χρήσης του Διαδικτύου[37]. Οι σημερινές

[35] COM(2011) 790 τελικό

[36]Ορίζοντας Την Τρομοκρατία: άρθρο του Θεόδωρου Μπαζίνη, Ερευνητή στο Ίδρυμα Διεθνών Σχέσεων στο Τμήμα Αμυντικών Θεμάτων. Διαδικτυακή Δημοσίευση στο https://powerpolitics.eu/

[37] COM(2011) 790 τελικό

τρομοκρατικές ενέργειες διαφέρουν από τις αντίστοιχες των δεκαετιών πριν τον Ψυχρό Πόλεμο. Η εμφάνιση των Όπλων Μαζικής Καταστροφής, η διευρυμένη συνδεσιμότητα, η υιοθέτηση νέων τεχνολογικών εργαλείων και μέσων οδηγούν σε νέες μορφές και τάσεις της τρομοκρατίας. Οι τρομοκρατικές ενέργειες δεν έχουν την μορφή πλέον συμβατικού πολέμου, θεωρούνται «ασύμμετρος πόλεμος».

Σήμερα, τον 21ο αιώνα, η τρομοκρατία σχεδόν αποτελεί μια σταθερά του κόσμου μας: δεν υπάρχει μέρα που στο ένα ή το άλλο σημείο του πλανήτη να μη γίνεται μια μικρή ή μεγάλη τρομοκρατική επίθεση, της οποίας ο αντίκτυπος να μην είναι δυνητικά αισθητός ακόμα και στο σύνολο της διεθνούς κοινότητας. Οι επιθέσεις της 11ης Σεπτεμβρίου 2001 στη Νέα Υόρκη σηματοδότησαν για πολλούς την αφετηρία μιας νέας εποχής στο ιστορικό γίγνεσθαι, ενώ καθημερινά χιλιάδες άνθρωποι στη Μέση Ανατολή, την Αφρική αλλά και στην Ευρώπη χάνουν τη ζωή τους ή πλήττονται από ενέργειες που χαρακτηρίζονται τρομοκρατικές[38].

«Η σταδιακή μετάλλαξη της τρομοκρατίας διαπιστώνεται από το τέλος του εικοστού αιώνα με τις αρχές του εικοστού πρώτου. Στην πορεία αυτών των αλλαγών παρατηρούνται ορισμένα νέα χαρακτηριστικά γνωρίσματα,[.....] τα οποία σχετίζονται με τη δυνατότητα των νέων οργανώσεων, ομάδων, μελών που χρησιμοποιούν την τρομοκρατία ως τρόπο πολιτικής έκφρασης, να χειρίζονται τη σύγχρονη τεχνολογία.

Καθώς διεθνώς πληθαίνουν οι πράξεις βίας – τρομοκρατίας από πληθώρα δραστών, είτε πρόκειται για τάσεις που πρόσκεινται σε θρησκευτικούς λόγους, είτε στην ακροδεξιά ή σε άλλες ακραίες εκφράσεις που αυτοαποκαλούνται με πληθώρα διαφορετικών ονομάτων κυρίως ενός άναρθρου πολιτικού λόγου, συναντώνται σε κοινά σημεία των πράξεων τους. Χρησιμοποιούν την απειλή αναβαθμίζοντας διαρκώς τον απειλητικό λόγο, δεν αναγνωρίζουν τους πολίτες ως αθώα θύματα, τους ενδιαφέρει ποσοτικά ο αριθμός των θυμάτων, έχουν πρόσβαση σε ποσότητες όπλων και εκρηκτικών, επιθυμούν τη διάχυση του φόβου – τρόμου, σ' όποιο σημείο του πλανήτη, επιθυμούν την προβολή τους από τα μέσα μαζικής ενημέρωσης.

Συνοπτικά, θα μπορούσε να λεχθεί ότι, η νέα εποχή της τρομοκρατίας χαρακτηρίζεται από το πέρασμα στο μαζικό στόχο-"θεαματική" δολοφονία, έναντι του πάλαι ποτέ ατομικού στόχου»[39].

[38] Λω, Ράνταλ. Ντ. ,Μεταφρ. Δήτσας, Φ. Επιστ. Επιμ. Μπόση, Μ. (2020) *Τρομοκρατία: μια παγκόσμια ιστορία*. Πανεπιστημιακές Εκδόσεις Κρήτης.

[39]Μπόση, Μ. (2019) 'Η μετάλλαξη της τρομοκρατίας', *Dikastiko.gr*. Διαθέσιμο στο : https://www.dikastiko.gr/articles/μαίρη-μπόση-η-μετάλλαξη-της-τρομοκρατ/

Σύμφωνα με την κ. Μπόση[40] σε συνέντευξη στη Liberal : « *Αυτές οι οργανώσεις δεν έχουν πλέον τα ιδεολογικά στεγανά άλλων εποχών. Εμφανίζονται με μία ακαθόριστη ιδεολογική βάση στις τοποθετήσεις τους, έτσι ώστε οι τυπικές δομές σύνθεσης να αποσύρονται και στην θέση τους να εμφανίζονται πιο ευέλικτες μορφές που είναι πολύ δύσκολο να εντοπιστούν. Δεδομένων αυτών των αλλαγών, επιτρέπεται η χρήση πολλών μέσων για να επιτευχθούν οι στόχοι, όπως και η σύμπραξη με το κοινό έγκλημα. Όσο για την στελέχωση νέων μελών, οι συνεργασίες διευρύνονται σε πολλαπλά επίπεδα και με αναζήτηση προσώπων από διάφορες κοινωνικές ομάδες*»[41].

Ηλεκτρονικό έγκλημα

Ο όρος «Ηλεκτρονικό Έγκλημα»[42] περιλαμβάνει όλες εκείνες τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση υπολογιστών και συστημάτων επεξεργασίας δεδομένων. Οι πράξεις αυτές τιμωρούνται με συγκεκριμένες ποινές από την ελληνική και τη διεθνή νομοθεσία.

Οι μορφές του ηλεκτρονικού Εγκλήματος ,ανάλογα με τον τρόπο τέλεσης, είναι οι ακόλουθες:

- Εγκλήματα με την χρήση Ηλεκτρονικών Υπολογιστών (Computer Crime) χωρίς την χρήση του διαδικτύου.
- Εγκλήματα τα οποία διαπράττονται με χρήση υπολογιστή και ειδικά μέσω διαδικτύου (Κυβερνοεγκλήματα-Cyber Crimes).

Κυβερνοέγκλημα

Η εξέλιξη του ηλεκτρονικού εγκλήματος στο Διαδίκτυο, είναι γνωστή ως Κυβερνοέγκλημα.

Δεδομένου ότι ο ορισμός του εγκλήματος στον κυβερνοχώρο δεν έχει αποτελέσει αντικείμενο συμφωνίας, οι όροι «έγκλημα στον κυβερνοχώρο», «ηλεκτρονικό έγκλημα», «έγκλημα πληροφορικής» ή «έγκλημα υψηλής τεχνολογίας» χρησιμοποιούνται συχνά αδιακρίτως.

[40] Καθηγήτρια του τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιά.

[41]Μπόση, Μ. (2019) 'Η τρομοκρατία στην Ελλάδα, δεν έχει ιδεολογία'. Διαθέσιμο στο: https://www.liberal.gr/apopsi/mairi-mposi-i-tromokratia-stin-ellada-den-echei-ideologia/273681.

[42] e-nomothesia.gr

Ο όρος «έγκλημα στον κυβερνοχώρο» νοείται ως *«αξιόποινες πράξεις που διαπράττονται με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων».*[43]

Χαρακτηριστικά

Ειδικότερα, στα χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο συμπεριλαμβάνονται και τα ακόλουθα[44]**:**

- Ευκολία - χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το | γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.
- Ταχύτητα - διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Διεθνικά στοιχεία - συνήθως εμπλέκονται θύματα και δράστες από περισσότερες διαφορετικές χώρες
- Ανωνυμία - Η διάπραξη κυβερνοεγκλημάτων εκμεταλλεύεται την σχετική ανωνυμία, που προσφέρουν ορισμένες τεχνολογικές υποδομές του διαδικτύου.
- Δυσκολία εύρεσης αποδεικτικών στοιχείων - οι αποδείξεις είναι συνήθως δεδομένα και μεταδεδομένα ψηφιακών αρχείων και ψηφιακό ίχνη που δύσκολα ανιχνεύονται
- Αστυνομική διερεύνησή γενικότερα, αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.
- Έλλειψη Επαρκούς Καταγραφής - Το μέγεθος των τελούμενων κυβερνοεγκλημάτων είναι δυσανάλογα μεγαλύτερο των καταγραφόμενων περιστατικών(e-nomothesia.gr)

Κατηγορίες

- Γνήσια πληροφορικά εγκλήματα – Κλασικά ποινικά αδικήματα, που τελούνται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών (πχ. απάτη, πλαστογραφία).
- Εγκλήματα σε σχέση με ψηφιακό περιεχόμενο – Ποινικά αδικήματα, που σχετίζονται με την διακίνηση παράνομου περιεχομένου μέσω συστημάτων πληροφοριών (πχ παιδική πορνογραφία).

[43] Επιτροπή COM (2007) 267 τελικό

[44]https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

- Εγκλήματα κατά πληροφοριακών συστημάτων–Ποινικά αδικήματα, που διαπράττονται κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων.

  Συνεπώς, βασικό στοιχείο της διάπραξης κυβερνοεγκλημάτων είναι ο διασυνδεδεμένος σε σύστημα πληροφοριών ηλεκτρονικός υπολογιστής, είτε ως στόχος της επίθεσης, είτε ως το βασικό μέσο / εργαλείο της επίθεσης, είτε τέλος ως ένα βοηθητικό μέσο / εργαλείο για τη διάπραξη της επίθεσης. Τα εγκλήματα κατά πληροφοριακών συστημάτων αποτελούν υποκατηγορία κυβερνοεγκλημάτων[45].

Μορφές διαδικτυακής εγκληματικότητας[46]

Οι βασικότερες μορφές εγκληματικής δραστηριότητας που αναπτύσσονται μέσω του διαδικτύου είναι οι ακόλουθες:

- Κακόβουλες εισβολές σε δίκτυα (hacking) η εισβολή σε ένα δίκτυο υπολογιστών αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων. Οι χάκερς συνήθως είναι προγραμματιστές, σχεδιαστές συστημάτων ή και άτομα μη επαγγελματίες που έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες είτε μόνοι τους. Αν οι ενέργειες τους είναι κακόβουλες αποκαλούνται κράκερς.
- Κακόβουλο λογισμικό
- Επιθέσεις σε δικτυακούς τόπους διακρίνονται σε δύο κατηγορίες:
- Αλλοίωσης περιεχομένου ιστοσελίδων και αντικατάστασης αυτών με αντίγραφα προπαγανδιστικού περιεχομένου ή άλλου ψευδούς.
- Άρνησης υπηρεσίας (DDoS: Distributed Denial of Service).
- Διαδικτυακή πειρατεία (παραβίαση πνευματικών δικαιωμάτων).
- Πειρατεία λογισμικού (χρήση παράνομου λογισμικού με τη χρήση crack).
- Απάτες μέσω Διαδικτύου.
- Διαδικτυακός Εκφοβισμός (cyberbullying) Ο εκφοβισμός μέσω διαδικτύου (cyberbullying) είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης,

[45] https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

[46] https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, Tablets, κινητών τηλεφώνων).

- Πορνογραφία ανηλίκων.

Κυβερνοτρομοκρατία

Ορίζεται η Κυβερνοτρομοκρατία-ο όρος υπάρχει από τη δεκαετία του ’80-ως επιθέσεις με πολιτικά ή ιδεολογικά κίνητρα σε πληροφορίες, δεδομένα χρηστών ή υπολογιστικά συστήματα, με καταστρεπτικά αποτελέσματα. (Υπάρχει μια αλληλοεπικάλυψη ανάμεσα στις τακτικές Κυβερνοτρομοκρατίας και εγκληματικού χακαρίσματος αλλά γενικώς, το κίνητρο είναι αυτό που τα διαφοροποιεί).

Είναι ξεκάθαρο ότι η τεχνολογία δίνει ίσες ευκαιρίες, παρέχοντας ισχυρά εργαλεία στους ανθρώπους ώστε να τα χρησιμοποιήσουν για τους δικούς τους σκοπούς - μερικές φορές με εντυπωσιακά δημιουργικό τρόπο αλλά και άλλες φορές προκαλώντας καταστροφή πέρα από κάθε φαντασία. Η όλο και μεγαλύτερη εξάρτηση του αναπτυγμένου κόσμου από τη συνδεσιμότητα - σχεδόν κάθε σύστημα που διαθέτουμε είναι συνδεδεμένο με κάποιο τρόπο σε ένα εικονικό δίκτυο- μας καθιστά έντονα ευάλωτους στην Κυβερνοτρομοκρατία σε όλες της τις μορφές.

Η αναπόφευκτη αλήθεια είναι ότι η συνδεσιμότητα ωφελεί επίσης τους τρομοκράτες και τους βίαιους εξτρεμιστές· και καθώς εξαπλώνεται, εξαπλώνονται και οι κίνδυνοι.

Οι τεχνικές ικανότητες των τρομοκρατών θα αυξηθούν, καθώς θα εξελίσσουν τις στρατηγικές τους για στρατολόγηση, εκπαίδευση και εκτέλεση στον εικονικό κόσμο, με την πλήρη, κατανόηση ότι οι επιθέσεις τους θα είναι πιο θεατές από ποτέ άλλοτε, εξαιτίας της τεράστιας εξάπλωσης και χρήσης των Μέσων Κοινωνικής Δικτύωσης.

Οι τρομοκρατικές ομάδες, βέβαια, θα συνεχίσουν να σκοτώνουν χιλιάδες κάθε χρόνο, με βόμβες ή άλλα μέσα. Αυτά είναι άσχημα νέα για το ευρύ κοινό, για τα κράτη που ήδη δυσκολεύονται αρκετά για να προστατεύσουν τη χώρα τους, τη φυσική της υπόσταση, αλλά και για τις εταιρείες που θα είναι όλο και περισσότερο ευάλωτες.

Καθώς η συνδεσιμότητα εξαπλώνεται σε όλο τον κόσμο, ακόμα και στα πιο απομακρυσμένα σημεία του πλανήτη, οι άνθρωποι θα έχουν μια σχετικά καλή πρόσβαση σε δίκτυα και σύγχρονες συσκευές χειρός. Πρέπει να υποθέσουμε ότι αυτές οι ομάδες θα υιοθετήσουν τις απαραίτητες τεχνικές ικανότητες για να ξεκινήσουν Κυβερνοεπιθέσεις.

Τα πλεονεκτήματα στις κυβερνοεπιθέσεις για τις εγκληματικές ομάδες είναι ξεκάθαρα, όπως λίγος η μηδενικός κίνδυνος να υποστούν σωματική βλάβη, περιορισμένοι απαιτούμενοι πόροι και τέλος ευκαιρίες να προκαλέσουν μαζικό κακό. Οι τρομοκράτες στοχεύουν τόσο σε φυσικές επιθέσεις με χρήση όπλων μαζικής καταστροφής, όσο και σε κυβερνοεπιθέσεις.

Είναι πλέον κοινός τόπος πως τόσο τα κράτη, όσο και οι μη κρατικοί παράγοντες χρησιμοποιούν υβριδικές προσεγγίσεις για να υλοποιήσουν τους πολιτικούς και στρατιωτικούς στόχους τους , συνδυάζοντας επιδέξια τις στρατιωτικές επιχειρήσεις με κυβερνοεπιθέσεις, διπλωματικές ή/και οικονομικές πιέσεις και εκστρατείες ενημέρωσης (προπαγάνδας). Κατά τη διάρκεια της τελευταίας δεκαετίας, τα μέσα κοινωνικής δικτύωσης έχουν εξελιχθεί σε έναν από τους κύριους διαύλους επικοινωνίας. Οι εικονικές πλατφόρμες επικοινωνίας έχουν γίνει αναπόσπαστο μέρος της πολεμικής στρατηγικής. Οι πρόσφατες συγκρούσεις στη Λιβύη, τη Συρία και την Ουκρανία έχουν αποδείξει ότι τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται ευρέως για τον συντονισμό των δράσεων, τη συλλογή πληροφοριών και, το σημαντικότερο, την επιρροή των πεποιθήσεων και των στάσεων του κοινού-στόχου, ακόμη και την κινητοποίηση του για δράση.[47]

Μέθοδοι - Σκοπός Επιθέσεων

Οι κυβερνοεπιθέσεις ομαδοποιούνται στις ακόλουθες κατηγορίες:

– για σκοπούς εκμετάλλευσης, όπως «προηγμένες συνεχείς απειλές»[48] για οικονομική και πολιτική κατασκοπεία (π.χ. GhostNet[49]), υποκλοπή ταυτότητας, οι πρόσφατες προσβολές κατά του συστήματος εμπορίας δικαιωμάτων εκπομπών (ETS)[50] ή κατά κρατικών/κυβερνητικών συστημάτων ΤΠ[51];

– για σκοπούς διαταραχής, όπως οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας

[47] NATO strategic communications centre of excellence: social media as a tool of hybrid warfare (May,2016). https://www.stratcomcoe.org/download/file/fid/5314

[48]Δηλ. συνεχείς και συντονισμένες επιθέσεις εναντίον κυβερνητικών οργανισμών και του δημόσιου τομέα. Καθίστανται πλέον μέλημα για τον ιδιωτικό τομέα (βλ. την έκθεση «RSA 2011 cybercrime trends report»).

[49]βλ. τις εκθέσεις του έργου Information Warfare Monitor: «Tracking GhostNet: investigating a Cyber Espionage Network» (2009) και «Shadows in the Cloud: Investigating Cyber Espionage 2.0» (2010).

[50] βλ. τις ερωταποκρίσεις στην ιστοσελίδα http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

[51] Π.χ. τις πρόσφατες επιθέσεις εναντίον της γαλλικής κυβέρνησης

(Distributed Denial of Service) ή μαζική αποστολή ανεπίκλητων μηνυμάτων (spamming) μέσω δικτύων προγραμμάτων ρομπότ (botnets, π.χ. το δίκτυο Conficker με 7 εκατομμύρια μηχανές και το εγκατεστημένο στην Ισπανία δίκτυο Mariposa με 12,7 εκατομμύρια μηχανές[52]), το Stuxnet[53] και η αποκοπή μέσων επικοινωνίας,

– για σκοπούς καταστροφής. Πρόκειται για σενάριο που δεν έχει ακόμα υλοποιηθεί, αλλά - δεδομένης της αυξανόμενης διείσδυσης των ΤΠΕ σε υποδομές ζωτικής σημασίας (π.χ. έξυπνα δίκτυα και συστήματα υδροδότησης) - δεν μπορεί να αποκλειστεί για τα επόμενα χρόνια.[54]

Οδηγίες Ε.Ε– Σύμβαση Βουδαπέστης -Ελληνική Νομοθεσία[55]

- Οδηγία 2017/541 για την καταπολέμηση της τρομοκρατίας

  Προοίμιο(6): *συμπεριφορές συνδεόμενες ιδίως με τους αλλοδαπούς τρομοκράτες μαχητές και τη χρηματοδότηση της τρομοκρατίας. Αυτές οι μορφές συμπεριφοράς θα πρέπει επίσης να τιμωρούνται όταν τελούνται μέσω του διαδικτύου, αλλά και μέσω των μέσων κοινωνικής δικτύωσης.*

  Προοίμιο (31): *η πρόληψη της ριζοσπαστικοποίησης και της στρατολόγησης στην τρομοκρατία, περιλαμβανομένης της ριζοσπαστικοποίησης μέσω του διαδικτύου,*

  Άρθρο 5: *..εκ προθέσεως, η διάδοση ή άλλη διάθεση, με οποιοδήποτε μέσο, είτε στο διαδίκτυο ή με συμβατικά μέσα, μηνύματος προς το κοινό, με πρόθεση την υποκίνηση σε τέλεση ενός από τα εγκλήματα [τρομοκρατίας]*

  Άρθρο 21 π.1,2: *η άμεση αφαίρεση διαδικτυακού περιεχομένου στην επικράτειά τους το οποίο αποτελεί δημόσια υποκίνηση σε τέλεση τρομοκρατικού εγκλήματος... φραγή της πρόσβασης στο εν λόγω περιεχόμενο στους χρήστες του διαδικτύου.*

- Οδηγία 2013/40/ΕΕ (για τις επιθέσεις κατά πληροφοριακών συστημάτων)

---

[52] Βλ. το έργο του ΟΟΣΑ/IFP «Future Global Shocks», «Reducing systemic cyber-security risks», 14 Ιανουαρίου 2011, στην ηλε-διεύθυνση

[53] http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis

[54] World Economic Forum, Global Risks 2011

[55] Αλέξανδρος-Ιωάννης Καργόπουλος(Πρωτοδίκης, εθνικός εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε.) Κυβερνο-έγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου.

Προοίμιο (15) «η σύμβαση αυτή είναι το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών. Η παρούσα οδηγία στηρίζεται στην εν λόγω σύμβαση»

- Με το Ν.4411/2016 γίνεται μεταφορά στο Ελληνικό Δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Του Συμβουλίου για τις Επιθέσεις κατά Συστημάτων Πληροφοριών η οποία περιλαμβάνει και τα εργαλεία που χρησιμοποιούνται για την τέλεση των σχετικών με τις επιθέσεις κατά συστημάτων πληροφοριών εγκλημάτων.
- Σύμβαση Συμβουλίου Ευρώπης 23/11/2001 (Βουδαπέστης) για το Κυβερνοέγκλημα, ETS 185[56]: είναι μια δεσμευτική διεθνής κατευθυντήρια γραμμή για τις χώρες που καταρτίζουν νομοθεσία για την καταπολέμηση του κυβερνοεγκλήματος. Παρέχει ένα πλαίσιο για τη διεθνή συνεργασία μεταξύ των συμβαλλομένων κρατών. Επί του παρόντος, η ΕΕ εκπροσωπείται από την Επιτροπή, το Συμβούλιο της Ευρωπαϊκής Ένωσης, την Ευρωπόλ, τον ENISA και την Eurojust[57].

[56] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[57] Η Ευρωπαϊκή Μονάδα Δικαστικής Συνεργασίας (Eurojust)

ΚΕΦΑΛΑΙΟ 3: Κυβερνοασφάλεια, προσπάθειες σε ευρωπαϊκό, παγκόσμιο και εθνικό επίπεδο

Κυβερνοπόλεμος: Παγκόσμια Ασύμμετρη Απειλή.

- Η εξάρτηση του δημόσιου και ιδιωτικού τομέα από τον κυβερνοχώρο θα αυξάνεται διαρκώς.
- Προς το παρόν, ο κυβερνοχώρος παραμένει «ευπρόσβλητος» και η απόλυτη προστασία του χαρακτηρίζεται ως «ουτοπία», καθότι αποτελεί πεδίο παγκόσμιου οικονομικού και στρατιωτικού ανταγωνισμού, ενώ η σύγχρονη τεχνολογία «αδυνατεί» να εγγυηθεί την αποτελεσματική κυβερνο-ασφάλεια.
- Η κυβερνο-απειλή είναι μια υπαρκτή παγκόσμια ασύμμετρη απειλή, που στρέφεται κατά της εθνικής ασφάλειας και της ευημερίας των χωρών.
- Η κυβερνο-επίθεση είναι φτηνή και αποτελεσματική, ενώ η κυβερνο-άμυνα είναι δαπανηρή, περίπλοκη, απαιτεί πολυμερή συνεργασία και δεν εγγυάται το αποτέλεσμα.
- Τα μέσα διεξαγωγής του κυβερνοπολέμου είναι ευρέως διαθέσιμα και αναπτύσσονται με ταχείς ρυθμούς.
- Η συντριπτική πλειοψηφία των κυβερνο-απειλών αφορούν την Κυβερνοτρομοκρατία.

Κρίσιμες Υποδομές

Προϋπόθεση του Κυβερνοπολέμου είναι η εκδήλωση Κυβερνοεπιθέσεων εναντίον στόχων αποτελεσματικών για την εξέλιξη της διαμάχης και σχετικών με τις κρίσιμες υποδομές της χώρας στόχου, στο μέτρο που αυτές είναι προσβάσιμες στους δράστες. Οι κυβερνοδυνατότητες σαν οργανωμένες δυνατότητες προσβολής στόχων μέσω της επικοινωνιακής και πληροφοριακής υποδομής του αντιπάλου αποτελούν έναν από τους παράγοντες ισχύος του δρώντος κράτους.

Οι επιθέσεις στον κυβερνοχώρο έχουν αυξηθεί σε άνευ προηγουμένου επίπεδο τεχνολογικής επιτήδευσης. Απλά πειράματα έχουν πλέον μετατραπεί σε πολύπλοκες δραστηριότητες που πραγματοποιούνται με σκοπό το κέρδος ή πολιτικούς λόγους. Οι πρόσφατες μεγάλης κλίμακας επιθέσεις στον κυβερνοχώρο εναντίον της Εσθονίας, της Λιθουανίας και της Γεωργίας είναι τα ευρύτερα γνωστά παραδείγματα μιας γενικής τάσης. Ο τεράστιος αριθμός ιών[58], ‘σκουληκιών’ και άλλες μορφές κακόβουλου λογισμικού, η επέκταση των δικτύων προγραμμάτων ρομπότ

[58] https://slideplayer.gr/slide/3644031/" title="ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ"

(botnets)[59] και η συνεχής αύξηση των ανεπίκλητων οχληρών μηνυμάτων (spam) επιβεβαιώνουν τη σοβαρότητα του προβλήματος[60].

Η υψηλή εξάρτηση από τις Υποδομές Ζωτικής Σημασίας (ΥΖΣ)[61], οι διασυνοριακές τους διασυνδέσεις και αλληλεξαρτήσεις με άλλες υποδομές, καθώς και τα ευάλωτα σημεία και οι επιβουλές που αντιμετωπίζουν ορίζουν την ανάγκη αντιμετώπισης της ασφάλειας και της ικανότητα αποκατάστασής τους σε μια συστημική προοπτική, ως πρώτη γραμμή άμυνας εναντίων αστοχιών και επιθέσεων.

Οι Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ) είναι όλο και πιο αλληλένδετες με τις καθημερινές μας δραστηριότητες. Ορισμένα από αυτά τα συστήματα, υπηρεσίες, δίκτυα και υποδομές ΤΠΕ (εν συντομία υποδομές ΤΠΕ) αποτελούν ζωτικό τμήμα της ευρωπαϊκής οικονομίας και της κοινωνίας, είτε παρέχοντας βασικά αγαθά και υπηρεσίες ή αποτελώντας την πλατφόρμα στήριξης άλλων κρίσιμων υποδομών. Κατά κανόνα θεωρούνται υποδομές πληροφοριών ζωτικής σημασίας (ΥΖΣ) δεδομένου ότι διαταραχή ή καταστροφή τους θα είχε σοβαρές επιπτώσεις στις ζωτικής σημασίας κοινωνικές λειτουργίες.

Κυβερνοασφάλεια

Κυβερνοασφάλεια[62] (cyber-security): μέτρα για την ασφάλεια των ηλεκτρονικών επικοινωνιών, των υποδομών και των υπηρεσιών, δηλαδή η ικανότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε τυχαία γεγονότα ή σε παράνομες ή κακόβουλες δράσεις που θέτουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και το απόρρητο των αποθηκευμένων ή διαβιβασμένων δεδομένων και των σχετικών υπηρεσιών που προσφέρονται ή καθίστανται προσβάσιμες από τα εν λόγω δίκτυα ή συστήματα. (άρθρο 1(3), Καν. 526/2013)

Η κυβερνοασφάλεια καλύπτει Κυβερνοεγκλήματα που αφορούν τόσο περιεχόμενο όσο και συστήματα και εκδηλώνονται με κυβερνοεπιθέσεις διαφόρων μορφών, όπως ιούς σε

[59] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets
[60] COM (2006) 688 τελικό
[61] Κρίσιμες υποδομές είναι οι φυσικές και ηλεκτρονικές υποδομές που είναι απαραίτητες για τη διασφάλιση των βασικών λειτουργιών του κράτους.
[62] Αλέξανδρος-Ιωάννης Καργόπουλος(Πρωτοδίκης, εθνικός εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε.) Κυβερνο-έγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου.

υπολογιστές, απάτες πληρωμών, διάδοση παράνομου υλικού ,εκστρατείες παραπληροφόρησης για την άσκηση επιρροής στο διαδίκτυο καθώς και παρεμβάσεις σε δημοκρατικές διαδικασίες.

Επιπλέον η Ευρωπόλ θεωρεί ότι υπάρχει σύγκλιση μεταξύ κυβερνοεγκλήματος και Τρομοκρατίας[63].

Κοινοτικές προσπάθειες

Σε μια εποχή που καθίσταται επιτακτική η προώθηση της οικονομικής ανάπτυξης, θα έχει ουσιαστική σημασία η εντατικότερη καταπολέμηση του εγκλήματος στον κυβερνοχώρο προκειμένου να διατηρηθεί η εμπιστοσύνη των πολιτών και των επιχειρήσεων στην ασφάλεια των επικοινωνιών και του εμπορίου μέσω του Διαδικτύου. Η δράση αυτή θα στηρίξει επίσης τους αναπτυξιακούς στόχους που τέθηκαν από τη στρατηγική «Ευρώπη 2020» και από το ψηφιακό θεματολόγιο για την Ευρώπη.

Η Ευρωπαϊκή Επιτροπή δρομολόγησε τον Μάρτιο 2010 την αναπτυξιακή στρατηγική «Ευρώπη 2020», για έξοδο από την κρίση και προετοιμασία της οικονομίας της Ένωσης στις προκλήσεις της επόμενης δεκαετίας. Η Ευρώπη 2020 καθορίζει ένα όραμα για την επίτευξη υψηλών επιπέδων απασχόλησης, παραγωγικότητας και κοινωνικής συνοχής, που θα υλοποιηθούν μέσω συγκεκριμένων δράσεων σε ευρωπαϊκό και σε εθνικό επίπεδο.

Η Ψηφιακή Ατζέντα 2020 (ή Ψηφιακό Θεματολόγιο) αποτελεί μια από τις επτά εμβληματικές πρωτοβουλίες (flagship initiatives) της αναπτυξιακής στρατηγικής «Ευρώπη 2020». Είναι το Ευρωπαϊκό όραμα και η βάση για να αναπτυχθούν πολιτικές και δράσεις με στόχο την εναρμονισμένη ψηφιακή πρόοδο των Ευρωπαϊκών χωρών με ορίζοντα το έτος 2020.

Ο γενικός στόχος του ψηφιακού θεματολογίου είναι «να αποκομισθούν βιώσιμα οικονομικά και κοινωνικά οφέλη από μια ενιαία ψηφιακή αγορά που θα βασίζεται σε διαδίκτυο μεγάλης και πολύ μεγάλης ταχύτητας και σε διαλειτουργικές εφαρμογές».

Οι κεντρικοί άξονες στους οποίους δίνονται προτεραιότητες από την Ευρωπαϊκή Επιτροπή είναι η:

- δημιουργία ενιαίας ψηφιακής αγοράς (ΨΗΦΙΑΚΗ ΑΓΟΡΑ)

[63] Ευρωπόλ,«Internet Organised Crime Threat Assessment 2017»

- βελτίωση του πλαισίου προϋποθέσεων για τη διαλειτουργικότητα μεταξύ προϊόντων και υπηρεσιών ΤΠΕ[64] (ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ)
- αύξηση της εμπιστοσύνης και της ασφάλειας στο διαδίκτυο (ΑΣΦΑΛΕΙΑ)
- εξασφάλιση της παροχής πολύ ταχύτερης πρόσβασης στο διαδίκτυο (ΤΑΧΥΤΗΤΑ)
- ενθάρρυνση επενδύσεων στην έρευνα και την ανάπτυξη (ΕΠΕΝΔΥΣΕΙΣ)
- ενίσχυση του ψηφιακού γραμματισμού, των δεξιοτήτων και της κοινωνικής ένταξης (ΕΚΠΑΙΔΕΥΣΗ)
- εφαρμογή των ΤΠΕ για την αντιμετώπιση κοινωνικών προβλημάτων, όπως είναι η κλιματική αλλαγή, η αύξηση του κόστους της υγειονομικής περίθαλψης και η γήρανση του πληθυσμού (ΚΟΙΝΩΝΙΑ)

Ιστορικό Δράσεων

Η ΕΕ αναγνωρίζει ότι ο κυβερνοχώρος προσφέρει σημαντικές ευκαιρίες, αλλά ταυτόχρονα θέτει συνεχώς νέες προκλήσεις για την εξωτερική δράση της ΕΕ. Η ίδια ανησυχεί σχετικά με την αυξημένη ικανότητα και προθυμία κρατικών και μη παραγόντων να επιδιώκουν τους στόχους τους μέσω κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. Οι εν λόγω δραστηριότητες είναι δυνατόν να αποτελούν παράνομες πράξεις σύμφωνα με το διεθνές δίκαιο και να χρήζουν κοινής αντίδρασης σε επίπεδο ΕΕ.

Η ΕΕ επαναλαμβάνει ότι τα κράτη δεν πρέπει εν γνώσει τους να επιτρέπουν να χρησιμοποιείται το έδαφός τους για διεθνώς παράνομες πράξεις με τη χρήση τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ).

6 Απριλίου 2016 (JOIN (2016) 18 final)

[64] Οι Τεχνολογίες των Πληροφοριών και των Επικοινωνιών (ΤΠΕ) αποτελούν σήμερα τη ραχοκοκαλιά της οικονομίας της ΕΕ και της κοινωνίας στο σύνολό της. Οι ΤΠΕ είναι ευάλωτες σε επιβουλές που δεν ακολουθούν πλέον εθνικά σύνορα και που έχουν μεταβληθεί με τις εξελίξεις στην τεχνολογία και την αγορά. Καθώς οι ΤΠΕ είναι παγκόσμιες, διασυνδεμένες και αλληλοεξαρτώμενες με άλλες υποδομές, η ασφάλεια και η ανθεκτικότητά τους δεν μπορεί να εξασφαλιστεί με αμιγώς εθνικές και ασυντόνιστες προσεγγίσεις.
Ταυτόχρονα, οι προκλήσεις που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών εξελίσσονται γρήγορα. Τα δίκτυα και τα συστήματα πληροφοριών πρέπει να προστατεύονται αποτελεσματικά από όλα τα είδη διαταραχών και αστοχιών, συμπεριλαμβανομένων των ανθρωπογενών επιθέσεων.
(https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52010PC0521)

Ευρωπαϊκή Επιτροπή / Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης ,«Κοινό πλαίσιο για την αντιμετώπιση των υβριδικών απειλών: απόκριση της Ευρωπαϊκής Ένωσης».

Καλύπτει τις κυβερνοαπειλές τόσο για τους ιδιώτες-χρήστες όσο και για τις υποδομές ζωτικής σημασίας, υπογραμμίζοντας ότι οι κυβερνοεπιθέσεις μπορούν να πάρουν και τη μορφή εκστρατειών παραπληροφόρησης στα Social Media.

19 Ιουνίου 2017

Το Συμβούλιο ενέκρινε συμπεράσματα σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»).Η ενέργεια αυτή αποτελεί μέρος της Ενωσιακής προσέγγισης για τη διπλωματία στον κυβερνοχώρο, η οποία συμβάλλει στην πρόληψη των συγκρούσεων, στον μετριασμό των απειλών για την ασφάλεια στον κυβερνοχώρο και σε αυξημένη σταθερότητα στις διεθνείς σχέσεις. Το πλαίσιο αναμένεται να ενθαρρύνει τη συνεργασία, να διευκολύνει τον μετριασμό των άμεσων και των μακροπρόθεσμων απειλών και να επηρεάσει τη συμπεριφορά των εν δυνάμει δραστών σε μακροπρόθεσμη βάση.

13 Σεπτεμβρίου 2017 (JOIN (2017) 450 final)

Ευρωπαϊκή Επιτροπή / Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης ,«Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ».

9 Οκτωβρίου 2017

Συμβούλιο της Ευρωπαϊκής Ένωσης, Τελική έκθεση του έβδομου γύρου αμοιβαίων αξιολογήσεων σχετικά με την «Πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», 12711/1/17 REV 1.

16 Απριλίου 2018

Το Συμβούλιο ενέκρινε συμπεράσματα σχετικά με τις κακόβουλες δραστηριότητες στον κυβερνοχώρο όπου υπογραμμίζεται η σημασία που έχει ένας παγκόσμιος, ανοικτός, ελεύθερος, σταθερός και ασφαλής κυβερνοχώρος, στον οποίο εφαρμόζονται πλήρως τα ανθρώπινα δικαιώματα, οι θεμελιώδεις ελευθερίες και το κράτος δικαίου. Το Συμβούλιο καταδικάζει απερίφραστα την κακόβουλη χρήση τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ), όπως στα περιστατικά με το Wannacry και το NotPetya, τα οποία έχουν προκαλέσει

σοβαρή βλάβη και οικονομική ζημία εντός και εκτός των συνόρων της ΕΕ. Τονίζει δε ότι η χρήση ΤΠΕ για δόλιους σκοπούς είναι απαράδεκτη.

18 Οκτωβρίου 2018

Το Ευρωπαϊκό Συμβούλιο ενέκρινε συμπεράσματα στα οποία ζητείται να συνεχιστούν περαιτέρω οι εργασίες για την ικανότητα αντιμετώπισης κυβερνοεπιθέσεων και αποτροπής τους με περιοριστικά μέτρα της Ένωσης, σε συνέχεια των συμπερασμάτων του Συμβουλίου της 19ης Ιουνίου 2017.

19 Νοεμβρίου 2018 (14413/18)

Πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα[65] (επικαιροποίηση 2018).

12 Απριλίου 2019

Δήλωση της Ύπατης Εκπροσώπου εξ ονόματος της ΕΕ σχετικά με τον σεβασμό της βασιζόμενης σε κανόνες τάξης στον κυβερνοχώρο.

17 Μαΐου 2019

[65] Εγκρίθηκε το 2014.

Απόφαση (ΚΕΠΠΑ)[66,67] 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της.

[66]Η θέληση των κρατών μελών να έχουν μια δυναμική παρουσία στη διεθνή πολιτική σκηνή κατέληξε στη θεσμοθέτηση της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (ΚΕΠΠΑ) που καθιερώθηκε με τη Συνθήκη του Μάαστριχτ. Η ΚΕΠΠΑ θεσπίστηκε αρχικά το 1993 με τη συνθήκη του Μάαστριχτ. Ενισχύθηκε προοδευτικά από τις επακόλουθες συνθήκες και ιδιαίτερα τη Συνθήκη της Λισαβόνας. Αφότου τέθηκε σε ισχύ η Συνθήκη της Λισαβόνας το Δεκέμβριο του 2009, η ΕΕ διαθέτει νομική προσωπικότητα (δηλ. είναι σε θέση να υπογράφει διεθνείς συνθήκες). Ένας από τους σημαντικούς λόγους που επέβαλαν την ανάπτυξη της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας-ΚΕΠΠΑ ήταν : «*Η διαμόρφωση ενός νέου διεθνούς περιβάλλοντος μετά το τέλος του Ψυχρού Πολέμου και το τέλος του διπολισμού έδινε τη δυνατότητα στην ΕΚ να προβάλει, με πιο συγκροτημένο και συνεκτικό τρόπο, τον ρόλο που θα μπορούσε να διαδραματίσει ως μια αναδυόμενη οικονομική και πολιτική δύναμη…*» (Κουσκουβέλης, 1995:150-153).

Σκοπός της ΚΕΠΠΑ είναι η διαφύλαξη των κοινών αξιών, των θεμελιωδών συμφερόντων, της ανεξαρτησίας και της ακεραιότητας της Ένωσης, η ενίσχυση της ασφάλειάς της, η διατήρηση της ειρήνης και η ενδυνάμωση της διεθνούς ασφάλειας, σύμφωνα με τις αρχές του Χάρτη των Η.Ε., την Τελική Πράξη του Ελσίνκι και τους στόχους της Χάρτας των Παρισίων, συμπεριλαμβανομένων εκείνων που αφορούν στα εξωτερικά σύνορα. Η δράση της Ε.Ε. στη διεθνή σκηνή στοχεύει στην προώθηση της δημοκρατίας, του κράτους δικαίου, του σεβασμού των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και των αρχών της ισότητας και της αλληλεγγύης.

[67] https://eur-lex.europa.eu/summary/glossary/foreign_security_policy.html?locale=el

Ασφάλεια Δικτύων -Πληροφοριών Σε Ευρωπαϊκό Επίπεδο[68]

Οι πολιτικές για την ασφάλεια δικτύων και πληροφοριών (NIS)[69] διαδραματίζουν κεντρικό ρόλο στο «Ψηφιακό θεματολόγιο για την Ευρώπη»[70](DAE)[71], μια εμβληματική πρωτοβουλία στο πλαίσιο της στρατηγικής ΕΕ 2020, για την αξιοποίηση και προώθηση του δυναμικού των ΤΠΕ και τη μετατροπή αυτού του δυναμικού σε αειφόρο ανάπτυξη και καινοτομία. Η ενθάρρυνση της αφομοίωσης των ΤΠΕ και της ενίσχυσης της εμπιστοσύνης στην κοινωνία της πληροφορίας αποτελούν βασικές προτεραιότητες του ψηφιακού θεματολογίου για την Ευρώπη.

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[72] δημιουργήθηκε αρχικά για να εξασφαλίσει ένα υψηλό και αποτελεσματικό επίπεδο ασφάλειας των δικτύων και πληροφοριών εντός της Ένωσης. Η πείρα που αποκτήθηκε στο πλαίσιο του Οργανισμού και οι προκλήσεις και απειλές υπογράμμισαν την ανάγκη εκσυγχρονισμού της εντολής του προκειμένου να ανταποκρίνεται καλύτερα στις ανάγκες της Ευρωπαϊκής Ένωσης οι οποίες οφείλονται:

---

[68] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52010PC0521

[69] Network and Information Systems (NIS): Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1-30). Προτείνει ένα ευρύ φάσμα μέτρων για την ενίσχυση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών (ασφάλεια στον κυβερνοχώρο) για την εξασφάλιση υπηρεσιών που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία της ΕΕ (Ευρωπαϊκής Ένωσης). Στόχος της είναι να εξασφαλίσει ότι οι χώρες της ΕΕ είναι καλά προετοιμασμένες και έτοιμες να χειριστούν και να αντιμετωπίσουν επιθέσεις στον κυβερνοχώρο μέσω: του διορισμού αρμόδιων αρχών, της δημιουργίας ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών(Computer Security Incident Response Teams-CSIRT) και
της υιοθέτησης εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο.
Καθορίζει επίσης τη συνεργασία σε επίπεδο ΕΕ τόσο σε στρατηγικό όσο και σε τεχνικό επίπεδο. Τέλος, εισάγει την υποχρέωση των παρόχων βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας και να ενημερώνουν τις αρμόδιες εθνικές αρχές σχετικά με σοβαρά συμβάντα. https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=CELEX%3A32016L1148

[70] COM (2010) 245 της 19.05.2010

[71] Digital Agenda for Europe

[72] Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) ιδρύθηκε το Μάρτιο του 2004 για αρχική περίοδο πέντε ετών βάσει του κανονισμού (ΕΚ) αριθ. 460/ 2004 (ΕΕ L 77 της 13.3.2004, σ. 1).

- Στον κατακερματισμό των εθνικών προσεγγίσεων αντιμετώπισης των αυξανόμενων προκλήσεων·
- στην έλλειψη συνεργατικών μοντέλων υλοποίησης των πολιτικών για την ασφάλεια δικτύων και πληροφοριών·
- στο ανεπαρκές επίπεδο ετοιμότητας που οφείλεται επίσης στις περιορισμένες ικανότητες της Ευρώπης για έγκαιρη προειδοποίηση και αντίδραση·
- στην έλλειψη αξιόπιστων ευρωπαϊκών δεδομένων και στις περιορισμένες γνώσεις σχετικά με τα εξελισσόμενα προβλήματα·
- στο χαμηλό επίπεδο ευαισθητοποίησης για τους κινδύνους και τις προκλήσεις που αφορούν την ασφάλεια δικτύων και πληροφοριών·
- στην πρόκληση της ενσωμάτωσης των πτυχών ασφάλειας δικτύων και πληροφοριών στις πολιτικές για την αποτελεσματικότερη καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο.

Ορισμένες από τις τρέχουσες εξελίξεις όσον αφορά την πολιτική για την ασφάλεια δικτύων και πληροφοριών, κυρίως αυτές οι οποίες εξαγγέλθηκαν στο ψηφιακό θεματολόγιο για την Ευρώπη, αξιοποιούν τη στήριξη και την εμπειρογνωσία του ENISA.

Σε αυτές συγκαταλέγονται:

- η ενίσχυση της πολιτικής συνεργασίας για την ασφάλεια δικτύων και πληροφοριών με εντατικοποίηση των δραστηριοτήτων εντός του Ευρωπαϊκού Φόρουμ των Κρατών Μελών (European Forum of Member States-EFMS).
- η ενίσχυση της συνεργασίας και της σύμπραξης μεταξύ δημόσιου και ιδιωτικού τομέα, στηρίζοντας την Ευρωπαϊκή σύμπραξη δημόσιου-ιδιωτικού τομέα για την ανθεκτικότητα (European Public Private Partnership for Resilience-EP3R).
- η διευκόλυνση ασκήσεων ετοιμότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο σε πανευρωπαϊκό επίπεδο με τη στήριξη της Επιτροπής και τη συμβολή του ENISA, με σκοπό οι εν λόγω ασκήσεις να επεκταθούν σε μεταγενέστερο στάδιο σε διεθνές επίπεδο.
- η σύσταση μιας CERT[73] (Ομάδας Αντιμετώπισης Έκτακτων Αναγκών στην Πληροφορική - ΟΑΕΑΠ) για τα θεσμικά όργανα της ΕΕ. Η κεντρική δράση 6 του ψηφιακού θεματολογίου για

[73] CERT – Computer Emergency Response Team: Τα τελευταία χρόνια, οι CERT έχουν συσταθεί, στον δημόσιο και στον ιδιωτικό τομέα, ως μικρές ομάδες από κυβερνοεμπειρογνώμονες που είναι σε θέση - αποτελεσματικά και αποδοτικά -να αντιμετωπίσουν περιστατικά σχετικά με την ασφάλεια πληροφοριών και τις απειλές στον κυβερνοχώρο. Έχουν αναδειχθεί σε βασικό στοιχείο της αμυντικής στρατηγικής ενάντια σε αυτές τις απειλές

την Ευρώπη συνίσταται στην παρουσίαση από την Επιτροπή *«μέτρων που αποσκοπούν σε μια ενισχυμένη και υψηλού επιπέδου πολιτική ασφάλειας δικτύων και πληροφοριών, όπου συμπεριλαμβάνονται […] μέτρα τα οποία επιτρέπουν ταχύτερη αντίδραση σε περίπτωση επιθέσεων στον κυβερνοχώρο, συμπεριλαμβανομένης μιας ΟΑΕΑΠ για τα θεσμικά όργανα της ΕΕ».* Αυτό θα απαιτήσει από την Επιτροπή και τα άλλα θεσμικά όργανα της Ένωσης να αναλύσουν και να συγκροτήσουν μια Ομάδα Αντιμετώπισης Έκτακτων Αναγκών στην Πληροφορική, στην οποία ο ENISA μπορεί να παράσχει τεχνική στήριξη και εμπειρογνωσία.
Η κινητοποίηση και η στήριξη των κρατών μελών προκειμένου να ολοκληρώσουν και, όπου είναι αναγκαίο, να συγκροτήσουν εθνικές/κυβερνητικές ΟΑΕΑΠ με σκοπό να καθιερώσουν ένα αποτελεσματικό δίκτυο ΟΑΕΑΠ το οποίο θα καλύπτει ολόκληρη την Ευρώπη. Η εν λόγω δραστηριότητα θα είναι επίσης αποφασιστικής σημασίας για την περαιτέρω ανάπτυξη του Ευρωπαϊκού Συστήματος Ανταλλαγής Πληροφοριών και Έγκαιρης Προειδοποίησης (EISAS)[74] για τους πολίτες και τις ΜΜΕ.

Σχέδιο Δράσης CIIP

Στις 30 Μαρτίου 2009, η Επιτροπή εξέδωσε ανακοίνωση σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας - «Προστασία της Ευρώπης από επιθέσεις στον κυβερνοχώρο και διαταραχές μεγάλης κλίμακας: αναβάθμιση της ετοιμότητας, της ασφάλειας και της ικανότητας αποκατάστασης»[75] όπου καθορίζεται σχέδιο (το «σχέδιο δράσης για την προστασία των ΥΖΣ») με σκοπό την ενίσχυση της ανθεκτικότητας (ικανότητας αποκατάστασης) υποδομών ζωτικής σημασίας στις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ). Σκοπός ήταν να τονωθεί και να υποστηριχθεί η ανάπτυξη υψηλού επιπέδου ικανοτήτων ετοιμότητας, ασφάλειας και ανθεκτικότητας – σε εθνικό και σε ευρωπαϊκό επίπεδο. Η προσέγγιση αυτή υποστηρίχθηκε ευρύτερα από το Συμβούλιο το 2009.[76]

προλαμβάνοντας, ανιχνεύοντας και εξαλείφοντας τα τρωτά σημεία και τα κενά. Προειδοποιούν τους πελάτες τους ως προς ευπαθή σημεία ή επιβουλές και προτείνουν δράσεις για τον περιορισμό των κινδύνων. Μπορούν να βοηθήσουν στον εντοπισμό συστημάτων με ελαττώματα και επιθέσεων και λαμβάνουν κατάλληλα μέτρα για την ανάσχεση ή/και την εξάλειψή τους. Είναι στενά διασυνδεμένες μεταξύ τους, απαρτίζοντας μια κοινότητα ειδικών που αγωνίζεται για την ασφάλεια στον κυβερνοχώρο, που αποτελεί κοινή υπόθεση για όλους. https://ec.europa.eu/commission/presscorner/detail/el/IP_12_949/smo

[74] EISAS – European Information Sharing and Alert System

75 COM (2009)149

76 Ψήφισμα του Συμβουλίου, της 18ης Δεκεμβρίου 2009, για μια ευρωπαϊκή συνεργατική προσέγγιση της ασφάλειας δικτύων και πληροφοριών (2009/C 321/01)

Το σχέδιο δράσης για την προστασία των Υποδομών Ζωτικής Σημασίας-ΥΖΣ (CIIP – Critical Information Infrastructure Protection)στηρίζεται σε πέντε πυλώνες:

- ετοιμότητα και πρόληψη
- εντοπισμός και αντιμετώπιση
- άμβλυνση των επιπτώσεων και αποκατάσταση
- διεθνής συνεργασία
- κριτήρια για ευρωπαϊκές υποδομές ζωτικής σημασίας στον τομέα των ΤΠΕ.

Προσδιορίζονται οι εργασίες που πρέπει να εκτελεστούν σε κάθε πυλώνα από την Επιτροπή, τα κράτη μέλη ή/και τον κλάδο, με την υποστήριξη του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

Η ανάλυση των επιπτώσεων που συνοδεύει το σχέδιο δράσης CIIP[77], καθώς και ευρύ φάσμα αναλύσεων και εκθέσεων από ιδιωτικούς και δημόσιους ενδιαφερόμενους φορείς, δεν περιορίζονται μόνο στην υπογράμμιση των πτυχών της κοινωνικής, πολιτικής και οικονομικής εξάρτησης από τις ΤΠΕ, αλλά τονίζουν και την συνεχή αύξηση του αριθμού, του πεδίου εφαρμογής, της πολυπλοκότητας και των δυνητικών επιπτώσεων των απειλών -φυσικών ή ανθρωπογενών.

Εγκλήματα Στον Κυβερνοχώρο (EC3)

Η καταπολέμηση των εγκλημάτων στον κυβερνοχώρο, για την οποία η βασική νομική πράξη είναι η Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο[78],συνεχίζει να αποτελεί ύψιστη προτεραιότητα. Έχει περιληφθεί στον κύκλο πολιτικής της ΕΕ για το οργανωμένο και το σοβαρό διεθνές έγκλημα[79], και συνιστά αναπόσπαστο μέρος των προσπαθειών για την ανάπτυξη συνολικής στρατηγικής της ΕΕ για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Η ΕΕ έχει επίσης αναπτύξει στενές σχέσεις με διεθνείς εταίρους, για

[77] SEC (2009) 399

[78]Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο, Βουδαπέστη, 23 Νοεμβρίου 2001, που είναι επίσης γνωστή ως σύμβαση της Βουδαπέστης. Η σύμβαση συνοδεύεται από Πρόσθετο πρωτόκολλο στη σύμβαση για το έγκλημα στον κυβερνοχώρο σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης οι οποίες διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών.

[79] Ο κύκλος πολιτικής της ΕΕ για το οργανωμένο και το σοβαρό διεθνές έγκλημα καλύπτει τα έτη 2011-2013 και περιλαμβάνει οκτώ προτεραιότητες, μία εκ των οποίων είναι «Να ενταθεί η καταπολέμηση του εγκλήματος στον κυβερνοχώρο και η εγκληματική παράνομη χρήση του Διαδικτύου εκ μέρους ομάδων οργανωμένου εγκλήματος».

παράδειγμα στο πλαίσιο της υφιστάμενης ομάδας εργασίας ΕΕ-ΗΠΑ για την ασφάλεια και το έγκλημα στον κυβερνοχώρο.

Δράσεις

- Σημειώθηκε πρόοδος στην ΕΕ στο θέμα της δημιουργίας ενός ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο (EC3) και ομάδων αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα των υπολογιστών (CERT). Με την προϋπόθεση ότι θα εξασφαλιστούν οι απαραίτητοι ανθρώπινοι και οικονομικοί πόροι, ένα Ευρωπαϊκό Κέντρο για εγκλήματα στον κυβερνοχώρο θα δρα ως εστιακό σημείο στην Ευρώπη για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο, συγκεντρώνοντας εμπειρογνωμοσύνη, στηρίζοντας ποινικές έρευνες και προωθώντας λύσεις σε επίπεδο ΕΕ, με παράλληλη αύξηση της ευαισθητοποίησης σε θέματα εγκλημάτων στον κυβερνοχώρο στην Ένωση.

- Στο μέλλον, διάφορα κράτη μέλη θα πρέπει να κινηθούν κατεπειγόντως για να κυρώσουν την Σύμβαση της Βουδαπέστης η οποία παρέχει ένα πλαίσιο για τη διεθνή συνεργασία στον τομέα αυτόν.

- Τέσσερις στους δέκα πολίτες της ΕΕ πιστεύουν ότι η ΕΕ πρέπει να έχει στη διάθεσή της καλύτερα μέσα για την καταπολέμηση του οργανωμένου εγκλήματος[80]

Επανεξέταση Νομοθεσίας[81]

Από τη φύση του, το έγκλημα στον κυβερνοχώρο δεν έχει σύνορα και χαρακτηρίζεται από ευελιξία και καινοτομία. Στον τομέα της πρόληψης, του εντοπισμού και της δίωξης, η επιβολή του νόμου πρέπει να είναι σε θέση να συναγωνίζεται και να προβλέπει την εφευρετικότητα των εγκληματιών. Όσον αφορά την εγκληματικότητα στον κυβερνοχώρο, οι αρμόδιες δικαστικές αρχές πρέπει να επανεξετάσουν τον τρόπο με τον οποίον συνεργάζονται εντός της δικαιοδοσίας τους και στο πλαίσιο της ισχύουσας νομοθεσίας ώστε να διασφαλίζεται ταχύτερη διασυνοριακή πρόσβαση σε στοιχεία και πληροφορίες, λαμβάνοντας υπόψη τις τρέχουσες και μελλοντικές τεχνολογικές εξελίξεις, όπως είναι το υπολογιστικό νέφος και το διαδίκτυο των πραγμάτων. Η συγκέντρωση ηλεκτρονικών αποδεικτικών στοιχείων σε πραγματικό χρόνο από άλλες

[80] https://ec.europa.eu/commission/presscorner/detail/el/IP_11_1453

[81] COM (2015) 185 final

δικαιοδοσίες για ζητήματα όπως ιδιοκτήτες διευθύνσεων IP ή άλλα ηλεκτρονικά αποδεικτικά στοιχεία και η διασφάλιση της αποδοχής αυτών των στοιχείων ενώπιον των δικαστηρίων αποτελούν βασικά ζητήματα. Απαιτείται επίσης προσωπικό επιβολής του νόμου υψηλής ειδίκευσης που να είναι σε θέση να παρακολουθεί την τεράστια αύξηση στο πεδίο εφαρμογής, την πολυπλοκότητα και τα είδη του εγκλήματος στον κυβερνοχώρο.

Απαιτούνται σαφείς κανόνες ώστε να διασφαλίζεται η πλήρης τήρηση των αρχών προστασίας των δεδομένων, καθώς οι αρχές επιβολής του νόμου αποκτούν πρόσβαση στα στοιχεία που χρειάζονται για την προστασία της ιδιωτικής ζωής των πολιτών κατά της εγκληματικότητας στον κυβερνοχώρο και της υποκλοπής ταυτότητας. Η συνεργασία με τον ιδιωτικό τομέα έχει επίσης καίρια σημασία για την κοινή προσπάθεια καταπολέμησης του ηλεκτρονικού εγκλήματος από συμπράξεις μεταξύ δημόσιου και ιδιωτικού τομέα. Στην απόκριση στο ηλεκτρονικό έγκλημα (π.χ. ηλεκτρονικό «ψάρεμα») πρέπει να εμπλέκεται ολόκληρη η αλυσίδα: από το ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο της Ευρωπόλ[82], τις ομάδες αντιμετώπισης καταστάσεων αναγκών στην πληροφορική στα κράτη μέλη που πλήττονται από την επίθεση έως τους παρόχους υπηρεσιών διαδικτύου οι οποίοι μπορούν να προειδοποιούν τους τελικούς χρήστες και να προσφέρουν τεχνική προστασία.

Εν συντομία, το έγκλημα στον κυβερνοχώρο απαιτεί μια νέα προσέγγιση για την επιβολή του νόμου στην ψηφιακή εποχή.

Ο αρμόδιος επίτροπος για την Ένωση Ασφάλειας κ.Τζούλιαν Κινγκ[83] δήλωσε:

«Δεν μπορούμε να επιτρέψουμε σε τρομοκράτες ή εγκληματίες να βρίσκουν καταφύγιο στο διαδίκτυο καταχρώμενοι τη σύγχρονη τεχνολογία. Πρέπει να κλείσουμε τα νομικά κενά και να συνεχίσουμε από κοινού σε διεθνές επίπεδο να περιορίζουμε τον χώρο στον οποίο λειτουργούν.»

Η κ. Βέρα Γιούροβα[84], επίτροπος Δικαιοσύνης, Καταναλωτών και Ισότητας των Φύλων, δήλωσε σχετικά: *«Ενώ οι αρχές επιβολής του νόμου εξακολουθούν να εργάζονται με δύσκαμπτες μεθόδους, οι εγκληματίες χρησιμοποιούν ταχύτατες τεχνολογίες αιχμής για τη δράση τους. Πρέπει να εξοπλίσουμε τις αρχές επιβολής του νόμου με μεθόδους του 21ου αιώνα για την αντιμετώπιση*

[82]Η Ευρωπαϊκή Αστυνομική Υπηρεσία (Ευρωπόλ) άρχισε να λειτουργεί ως διακυβερνητικό όργανο σύμφωνα με τις διατάξεις σύμβασης η οποία συνήφθη μεταξύ των κρατών μελών και τέθηκε σε ισχύ το 1999. Κατ' εφαρμογή απόφασης του Συμβουλίου του 2009, η Ευρωπόλ μετατράπηκε σε οργανισμό της ΕΕ, ο οποίος χρηματοδοτείται από τον προϋπολογισμό της ΕΕ.(https://www.europol.europa.eu/about-europol)

[83] https://ec.europa.eu/commission/presscorner/detail/el/IP_19_843

[84] https://ec.europa.eu/commission/presscorner/detail/el/IP_18_3343 (Δελτίο τύπου 17/04/2018)

της εγκληματικότητας, ακριβώς όπως και οι εγκληματίες χρησιμοποιούν μεθόδους του 21ου αιώνα για να διαπράξουν τα εγκλήματά τους.»

Διεθνείς Συνεργασίες[85]

Στο πλαίσιο του EFMS εξετάστηκαν και αναπτύχθηκαν ευρωπαϊκές αρχές και κατευθυντήριες γραμμές για την ανθεκτικότητα και τη σταθερότητα του διαδικτύου. Η Επιτροπή θα εξετάσει και θα προωθήσει τις αρχές αυτές στους εκάστοτε ενδιαφερόμενους, ιδίως στον ιδιωτικό τομέα (μέσω EP3R), διμερώς με βασικούς διεθνείς εταίρους, ιδίως με τις ΗΠΑ, καθώς και πολυμερώς. Εντός των αρμοδιοτήτων της, θα προωθήσει την υπόθεση και σε άλλα βήματα, όπως την G8, τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), το NATO[86] (ιδίως βάσει της νέας στρατηγικής του που εγκρίθηκε τον Νοέμβριο του 2010 και των δραστηριοτήτων του συλλογικού κέντρου αριστείας Cooperative Cyber-defense Center of Excellence), της ITU/ΔΕΤ[87] (στο πλαίσιο της ανάπτυξης ικανοτήτων στο πεδίο της ασφαλείας στον κυβερνοχώρο), τον Οργανισμό για την Ασφάλεια και τη Συνεργασία στην Ευρώπη ΟΑΣΕ[88] (μέσω του οικείου φόρουμ για συνεργασία σε θέματα ασφάλειας)· τον ASEAN, Meridian[89], κλπ. Στόχος είναι οι εν λόγω αρχές και κατευθύνσεις να καταστούν κοινό πλαίσιο για διεθνή συλλογική προσπάθεια στην κατεύθυνση μακροπρόθεσμης ανθεκτικότητας και σταθερότητας του διαδικτύου.

Το Διαδίκτυο είναι ένα παγκόσμιο και σε μεγάλο βαθμό κατανεμημένο δίκτυο δικτύων, όπου τα κέντρα ελέγχου δεν συμπίπτουν απαραίτητα με τα εθνικά σύνορα. Προς τούτο απαιτείται ειδική, στοχοθετημένη προσέγγιση, προκειμένου να εξασφαλιστεί ικανότητα αποκατάστασης και σταθερότητα, με βάση δύο συγκλίνουσες δράσεις. Πρώτον, επίτευξη συναίνεσης ως προς τις ευρωπαϊκές προτεραιότητες για την ικανότητα αποκατάστασης της σταθερότητας του Διαδικτύου, από άποψη δημόσιας τάξης και επιχειρησιακής εξάπλωσης. Δεύτερον ,παρότρυνση της παγκόσμιας κοινότητας στην ανάπτυξη ενός συνόλου αρχών που να

[85]COM(2011) 163 τελικό,
https://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EL:HTML

[86]https://www.nato.int/

[87] International Telecommunications Union/ Διεθνής Ένωση Τηλεπικοινωνιών

[88] Αγγλικά :Organization for Security and Co-operation in Europe - OSCE

[89] Με τη διαδικασία Meridian επιδιώκεται να δοθεί στις κυβερνήσεις, σε παγκόσμια κλίμακα, ένα μέσο για την εξέταση τρόπων συνεργασίας σε επίπεδο μέτρων πολιτικής και σε θέματα προστασίας υποδομών ζωτικής σημασίας (CIIP). Βλ. http://meridianprocess.org/

αντανακλά τις βασικές αξίες της Ευρώπης, όσον αφορά την ικανότητα αποκατάστασης και τη σταθερότητα του Διαδικτύου, στο πλαίσιο τού στρατηγικού μας διαλόγου και συνεργασίας με τρίτες χώρες και διεθνείς οργανισμούς. Οι δραστηριότητες αυτές θα βασίζονται στην αναγνώριση, εκ μέρους της Παγκόσμιας Διάσκεψης Κορυφής για την Κοινωνία της Πληροφορίας[90], της καίριας σημασίας που έχει η σταθερότητα για το Διαδίκτυο.

NATO – ΕΕ.

Το ΝΑΤΟ ως μία αμιγώς στρατιωτική συμμαχία δεν θα μπορέσει να αντιμετωπίσει όλο το φάσμα των απειλών που συναντάμε σε έναν υβριδικό πόλεμο. Το ΝΑΤΟ χρειάζεται να αποκτήσει μία πιο ευέλικτη στρατηγική για την αντιμετώπιση των απειλών με μεγαλύτερο εύρος οργάνων, μεθόδων και μεσών. Μετά την έναρξη του πολέμου στην Κριμαία το 2014, εγκαινιάστηκε μία νέα συνεργασία με την ΕΕ για μία διαφορετική και πιο ευέλικτη στρατηγική με βασικό στόχο την πρόληψη κι αντιμετώπιση του υβριδικού πολέμου. Η ΕΕ είναι ο καταλληλότερος οργανισμός για να συμπληρώσει και να συνεργαστεί με το ΝΑΤΟ, καθώς προκύπτει ένα υβρίδιο σκληρής κι ήπιας ισχύος με περισσότερα μέσα, μεθόδους και δρώντες – πολιτικοί και στρατιωτικοί – για την αντιμετώπιση κι ανίχνευση των υβριδικών απειλών.

Το ψήφισμα 2151 του Συμβουλίου Ασφαλείας των Ηνωμένων Εθνών είχε σκοπό την πρόληψη του υβριδικού πολέμου με την υιοθέτηση μέτρων από τα ευάλωτα κράτη για τη σταθεροποίηση τους και άρα τον περιορισμό τρωτότητας τους από τις υβριδικές απειλές. Μέρος του ψηφίσματος ήταν και η ενίσχυση της ικανότητας κάθε κράτους να προβάλλει τη δημόσια ασφάλεια και προστασία του κράτους δικαίου συνδυαστικά με διαφάνεια κι υπευθυνότητα.

Το ΝΑΤΟ έχει αναπτύξει μία στρατηγική βασισμένη στο σκεπτικό της μετατροπής της στρατηγικής στα δεδομένα του σήμερα, πιο ευέλικτη και προσαρμόσιμη. Τα τρία στάδια αυτής είναι:

- Προετοιμασία: το ΝΑΤΟ μαζεύει κι επεξεργάζεται πληροφορίες για να αναγνωρίσει και να ανιχνεύσει υβριδικές απειλές.
- Αποτροπή: το ΝΑΤΟ είναι σε θέση να δράσει άμεσα για να αποτρέψει οποιαδήποτε υβριδική απειλή. Προσπάθεια για βελτίωση και της πολιτικής ανταπόκρισης.

[90]Θεματολόγιο της Τύνιδας για την Κοινωνία της πληροφορίας, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

- Άμυνα: σε περίπτωση που αποτύχει η αποτροπή, το ΝΑΤΟ είναι σε θέση να υπερασπιστεί κάθε σύμμαχο εναντίον κάθε υβριδικής απειλής.

  Οι τρόποι αντιμετώπισης από ΕΕ και ΝΑΤΟ, εάν δεν κρίνονται αποτελεσματικοί – δεν αποτράπηκε η προσάρτηση της Κριμαίας στη Ρωσία – κρίνονται μερικώς αποτελεσματικοί, διότι ίσως προλάβουν άλλες τέτοιες υβριδικές απειλές σε γειτονικά κράτη και περιοριστεί με τον τρόπο αυτό μία σειρά αλληλένδετων εξελίξεων με αφετηρία την Κριμαία. Στο πεδίο μάχης της Συρίας, ο ISIS, έχει περιοριστεί σημαντικά όμως αυτό δεν είναι αποτέλεσμα που προκύπτει μόνο από τη δράση του ΝΑΤΟ αλλά από συνδυασμό των κρατικών δρώντων.

Κρατικό Επίπεδο

Ό,τι αφορά το κρατικό επίπεδο, υπάρχουν πλέον κι οι μη κρατικοί δρώντες που ασκούν βία με αποτέλεσμα, για να μπορέσει το κράτος να αντιμετωπίσει αυτό το φαινόμενο, οφείλει να χαράξει εθνική πολιτική αντιμετώπισης με στόχο να διατηρήσει την ασφάλεια εντός των συνόρων του. Η ανάγκη για πρόληψη και καταστολή του φαινομένου κρίνεται επιτακτική. Τα κράτη θα πρέπει να αναπτύξουν εθνική πολιτική αντιμετώπισης του υβριδικού πολέμου κι αυτή να συντονιστεί με την εθνική πολιτική των γειτονικών κρατών. Ο συντονισμός καθίσταται πιο αποτελεσματικός από τη μεμονωμένη κρατική δράση. Το κράτος πρέπει να αναγνωρίσει τις λειτουργίες της απειλής και τα τρωτά της σημεία· να τα ανιχνεύσει στο σύνολο της κοινωνίας όπου θα μπορούσαν να αναπτυχθούν και να προσπαθήσει να τα επουλώσει. Παράλληλα, οφείλει να συγχρονίσει και να εκσυγχρονίσει όλα τα μέσα που διαθέτει – στρατιωτικά, διπλωματικά, τεχνολογικά, οικονομικά – και να στοχεύσει στα τρωτά σημεία της απειλής.

Για το συντονισμό διαφορετικών κρατών σε μία κοινή δράση, απαιτείται η διαρκής κι ειλικρινής επικοινωνία μεταξύ των διαφορετικών πολιτικών ηγεσιών, όπως κι η ανταλλαγή πληροφοριών με κοινό στόχο, την αντιμετώπιση των υβριδικών απειλών και πολέμου.

Ο υβριδικός πόλεμος είναι ένα δυναμικό φαινόμενο που παρουσιάζει σημαντική εξέλιξη. Συνιστά μία μορφή αντίδρασης των δρώντων που έχουν λιγότερη ισχύ από τους άλλους. Σήμερα, είναι η αντίδραση ορισμένων μη κρατικών αλλά και κρατικών δρώντων, κυρίως της Μέσης Ανατολής στο συμβατικό πόλεμο, ώστε να χαθεί το πλεονέκτημα της Δύσης στο συμβατικό πεδίο μάχης. Είναι το εργαλείο του αδύναμου δρώντα, όμως ορισμένες φορές χρησιμοποιείται και από Μεγάλες Δυνάμεις για να επιτευχθούν κεκαλυμμένα πολιτικά αποτελέσματα όπως συνέβη για παράδειγμα στην Κριμαία.

Οι υβριδικές επιθέσεις είναι διεθνές ζήτημα κι απαιτούνται διεθνή πλαίσια συνεργασίας συντονισμού για την εξάλειψη τους.

Το Ηνωμένο Βασίλειο κι η Νορβηγία, συνεργάστηκαν σε διεθνές πρότζεκτ για τον εντοπισμό και την αντιμετώπιση του υβριδικού πολέμου, με τη χρηματοδότηση του νορβηγικού Υπουργείου Άμυνας.

Πλέον, ο υβριδικός πόλεμος τείνει να θεωρείται ορθόδοξο μέσο πολέμου. Στη σύγκρουση μεταξύ Ρωσίας – Ουκρανίας, εισήχθη επίσημα το μοντέλο του υβριδικού πολέμου με τη χρήση του διαδικτύου.

Από τη δεκαετία του 1990, η διεθνής κοινότητα αναρωτιέται για το αν έχει αλλάξει και ποια είναι η μορφή του πολέμου. RMA: Revolution in Military Affairs, Military Transformation. Μετά τη 9/11 η Δύση κι ειδικά οι ΗΠΑ ξεκίνησαν ένα διαφορετικού είδους πόλεμο στη Μέση Ανατολή, το Αφγανιστάν κι άλλες περιοχές που ονομάζεται Global War against Terrorism (GWOT).

Εμφανίζεται η ασύμμετρη απειλή, 4ης γενιάς πόλεμος κι η κυριαρχία πλήρους φάσματος που καλύπτουν τις διαστάσεις του υβριδικού πολέμου με τη Ρωσία – Ουκρανία να είναι και πάλι παράδειγμα της νέας μορφής πολέμου χωρίς τη χρήση συμβατικών μέσων.

Ψηφιακή επιτήρηση[91]

Σε μία εποχή που αποκαλείται «Αιώνας της Πληροφόρησης» και χαρακτηρίζεται από την παγκοσμιοποίηση και τη ραγδαία ανάπτυξη της τεχνολογίας, όπου παλιές και νέες απειλές συνυπάρχουν, ενώ εμφανίζονται νέες προκλήσεις, ευκαιρίες και κίνδυνοι, οι σύγχρονες δημοκρατίες μέσω των υπηρεσιών πληροφοριών και ασφαλείας τους προσπαθούν να παρέχουν ασφάλεια στις κοινωνίες τους. Παράλληλα, αναζητούν τρόπους προστασίας των δημοκρατικών ελευθεριών, των ανθρωπίνων δικαιωμάτων και της ιδιωτικότητας, καθώς και τρόπους τήρησης των ηθικών αξιών τους. Η ανάγκη για την επίτευξη ασφάλειας σε ένα άναρχο διεθνές σύστημα, όπου δεν υπάρχει παγκόσμιος Λεβιάθαν, θέτει επιτακτικά τα διλήμματα που ανέλυσε ο Τζωρτζ Όργουελ στο κλασικό βιβλίο του 1984: Ο Μεγάλος Αδελφός καλεί τις ηγεσίες των σύγχρονων δημοκρατικών κρατών να βρουν τη χρυσή τομή μεταξύ δημοκρατίας, ανθρωπίνων

[91] Σαμαράς Ν., Α. *και άλλοι.* 'Βιβλίο Συνόψεων Κοινωνία της επιτήρησης: Από την Κυβερνοασφάλεια στα Fake News| Μέσα| Μηνύματα| Στρατηγικές', στο. *7ο Επιστημονικό Συνέδριο Εργαστήριο στρατηγικής Επικοινωνίας και Μέσων Ενημέρωσης Συνδιοργάνωση: Εργαστήριο Πληροφόρησης και Κυβερνοασφάλειας. Εισαγωγικό σημείωμα: Ανδρέας Λιαρόπουλος, Επίκουρος Καθηγητής, Τμήμα Διεθνών & Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς, Διευθυντής Εργαστηρίου Πληροφόρησης και Κυβερνοασφάλειας.*

δικαιωμάτων, ιδιωτικότητας και ασφάλειας. Η διασπορά ψευδών ειδήσεων, οι αποκαλύψεις των Edward Snowden και των WikiLeaks περί ψηφιακής επιτήρησης, καθώς και οι υβριδικές απειλές που παρουσιάστηκαν στην κρίση της Ουκρανίας αναδεικνύουν τον φόβο μετατροπής των σύγχρονων δημοκρατιών σε «ψηφιακά κράτη επιτήρησης».

Υβριδική Πολιτική Ασφάλειας

Σύμφωνα με τον κ. Κωνσταντόπουλο[92], για την αντιμετώπιση του υβριδικού πολέμου και των υβριδικών απειλών απαιτείται μια ολιστική προσέγγιση μία "υβριδική πολιτική ασφάλειας", ένα δόγμα αντιμετώπισης τους και ένα κέντρο λήψης αποφάσεων όπου εμπλέκεται η κυβέρνηση σε εθνικό και τοπικό επίπεδο, ο ιδιωτικός τομέας ,και ολόκληρη η κοινωνία. Λαμβάνοντας υπόψη την ολιστική αυτήν προσέγγιση, η Πληροφόρηση αποτελεί πραγματικά ένα κρίσιμο και σημαντικό εργαλείο για την αντιμετώπιση του υβριδικού πολέμου και των υβριδικών απειλών, καθώς και οι τέσσερις λειτουργίες της (συλλογή, ανάλυση, αντιπληροφόρηση, μυστική δράση) είναι κατάλληλες για το σκοπό αυτόν. […] Επειδή διαθέτουν ένα συγκριτικό πλεονέκτημα, τη μυστικότητα, η οποία αποτελεί το κυριότερο χαρακτηριστικό τους. Δηλαδή, χρησιμοποιούν μυστικά μέσα και μεθόδους που δεν διαθέτει καμία άλλη δημόσια ή ιδιωτική υπηρεσία και έχουν διαμορφώσει και μία διακριτή κουλτούρα πληροφόρησης.

Η πρόκληση για τις υπηρεσίες πληροφοριών είναι να αναγνωρίσουν το εύρος των υβριδικών απειλών και τους παράγοντες που τις διαφοροποιούν από τις συμβατικές απειλές. Ούτως ειπειν, οι στόχοι είναι οι κοινωνίες και όχι οι στρατοί και διάφορα εργαλεία χρησιμοποιούνται ταυτόχρονα και στρατηγικά, έτσι ώστε να αποφέρουν το μέγιστο αποτέλεσμα προς όφελος των δρώντων που καταφεύγουν στις υβριδικές απειλές και στον υβριδικό πόλεμο. Επίσης, η διάσταση του κυβερνοπολέμου μαζί με τα κοινωνικά μέσα (social media) και την εικονική πραγματικότητα (virtual realms), προσφέρουν φθηνά εργαλεία επίθεσης. Το εναρκτήριο σημείο αντιμετώπισης των υβριδικών απειλών είναι να εντοπιστούν όσο το δυνατόν νωρίτερα τα σήματα που δείχνουν την προετοιμασία ή την διεξαγωγή εχθρικών υβριδικών δράσεων.

[92] Κωνσταντόπουλος, Ι. 'Στόχοι των υβριδικών απειλών είναι οι κοινωνίες και όχι οι στρατοί'. *HuffPost Greece*, 25 Απρίλιος 2019. https://www.huffingtonpost.gr/entry/ioannes-konstantopoelos-stochoi-ton-evridikon-apeilon-einai-oi-koinonies-kai-ochi-oi-stratoi_gr_5cbee6ffe4b0f7a84a74b9e2.

Η καλύτερη άμυνα απέναντι σε πρακτικές υβριδικού πολέμου αποτελεί, πρώτον, η διαμόρφωση της αντίληψης της απειλής και η κατανόηση του υβριδικού πολέμου και των υβριδικών απειλών, δεύτερον, η προσπάθεια ενδυνάμωσης της ανθεκτικότητας μίας κοινωνίας, έτσι ώστε σε περίπτωση που δεχθεί ένα υβριδικό χτύπημα να μπορέσει σύντομα να αναδιοργανωθεί και να αντιδράσει, ενώ θα έχει ελαχιστοποιήσει όσο είναι δυνατόν τις ζημιές, τρίτον, η δημιουργία και η συνεχιζόμενη ανάπτυξη των μέσων αντίδρασης και τέταρτον, η δημιουργία ενός θεσμικού πλαισίου συνεργασίας μεταξύ των διάφορων κρατικών υπηρεσιών (πολιτικών και στρατιωτικών), καθώς και του ιδιωτικού τομέα, που θα πρέπει να συνεργάζονται προκειμένου να αντιμετωπιστούν οι υβριδικές απειλές.

RuNet 2020 και το Δόγμα Ασφάλειας Πληροφοριών[93].

Η Ρωσία θεωρεί το διαδίκτυο ως μια άμεση απειλή της ρωσικής πολιτισμικής ταυτότητας και της πολιτικής της ανεξαρτησίας καθώς η ελεύθερη διακίνηση της πληροφορίας και κατ ’επέκταση η παραπληροφόρηση αποτελεί όπλο ξένων δυνάμεων. Μετά την αναγνώριση από το ΝΑΤΟ του κυβερνοχώρου ως πεδίο επιχειρήσεων το 2016,η Ρωσία ανακοίνωσε ότι μέχρι το 2020,το RunNet – το ρωσικό τμήμα του διαδικτύου – θα μπορεί να αποκοπεί από το παγκόσμιο διαδίκτυο. . Σύμφωνα με το Δόγμα Ασφάλειας Πληροφοριών, που υπεγράφη από τον Πρόεδρο Vladimir Putin στις 5 Δεκεμβρίου του 2016, η Ρωσία στοχεύει να αναπτύξει ένα σύστημα ελέγχου το οποίο θα διαχειρίζεται το ρωσικό τμήμα του διαδικτύου.Οι πολιτικές προστασίας της ιδιωτικότητας από εταιρίες όπως η Google,το Facebook και το Twitter κρίνονται σαν απειλή της ψηφιακής της κυριαρχίας και κατ ‘επέκταση της εθνικής της ασφάλειας. Σκοπός της Ρωσίας εξαιτίας των παραπάνω είναι να δημιουργήσει ένα κρατικά ελεγχόμενο και ανεξάρτητο δίκτυο, το οποίο θα εξασφαλίζει καλύτερη προστασία εναντίον ξένων απειλών. Το RuNet 2020 είναι βασισμένο στο εγχείρημα «καθαρό διαδίκτυο», το οποίο ξεκίνησε το 2012 και είναι ένα σύστημα αυτό-λογοκρισίας που φιλοδοξεί να προσφέρει στους χρήστες του ένα πιο ασφαλές δίκτυο. Το Δόγμα Ασφάλειας Πληροφοριών είναι η τελευταία εξέλιξη στη Ρωσική προσπάθεια να εξασφαλίσει και να εθνικοποιήσει την πληροφοριακή σφαίρα. Επίσης η θέσπιση σειράς νόμων που ενισχύουν την κυβερνητική εποπτεία και λογοκρίνουν την πληροφορία, ελέγχοντας την διαδικτυακή κίνηση μέσα στο κράτος,

[93] Λιαρόπουλος, Α. (2020) ‘Ρωσικές Πληροφοριακές Επιχειρήσεις: Κυριαρχώντας στο Πληροφοριακό Περιβάλλον’, *Ναυτική Επιθεώρηση*, 612(180), σ.σ. 68–81.

περιορίζουν τις ξένες επενδύσεις σε ρωσικά μέσα ενημέρωσης καθώς και την εξάρτηση των εγχώριων βιομηχανιών από ξένες πληροφοριακές τεχνολογίες προωθώντας την ανάπτυξη αντίστοιχων ρωσικών τεχνολογιών. Το Δόγμα Ασφάλειας Πληροφοριών αναφέρεται επίσης σε στρατηγικές συνεργασίες που στοχεύουν στη εξασφάλιση της ρωσικής πληροφοριακής σφαίρας.

Το επιχείρημα ότι το RuNet 2020 θα προστατεύει τους πολίτες από επιβλαβείς πληροφορίες και ψευδείς ειδήσεις είναι ένα αφήγημα το οποίο πολλά κράτη ενδέχεται να υιοθετήσουν, με σκοπό να αποσυνδεθούν από το διαδίκτυο. Εάν γίνει αυτό και το παράδειγμα της Ρωσίας ακολουθήσουν και άλλα κράτη που ανήκουν στην Κοινοπολιτεία Ανεξαρτήτων Κρατών και αναπτύξουν ένα εναλλακτικό διαδίκτυο, αυτό θα αποτελέσει μεγάλη ιδεολογική νίκη για τη Ρωσία και θα οδηγήσει στον κατακερματισμό της αρχιτεκτονικής του παγκόσμιου διαδικτύου αμφισβητώντας έτσι τον τρόπο με τον οποίο λειτουργούν οι δημοκρατίες. Η Δύση θα έρθει αναπόφευκτα αντιμέτωπη με το δίλημμα να αγνοήσει την εξέλιξη αυτή ή να εφαρμόσει αντίμετρα με σκοπό τον περιορισμό των αδυναμιών της. Η προσαρμογή σε ένα κλειστό εθνικό μοντέλο θα σήμαινε ότι η Δύση αμφισβητεί την αξία ενός παγκόσμιου και ανοιχτού διαδικτύου και επομένως παραδέχεται ότι το μοντέλο της έχει αποτύχει. Η Μόσχα θα χάσει το τωρινό της συγκριτικό πλεονέκτημα αν η Δύση ακολουθήσει το παράδειγμα της Ρωσίας και μετατρέψει τον εθνικό της κυβερνοχώρο σε πιο κλειστό και ελεγχόμενο.

Case Studies

- Αμερικανική Επανάσταση (1776): παρατηρείται μία σύμπραξη μεταξύ του Ηπειρωτικού Στρατού (Continental Army) – συμβατικός στρατός – με την Πολιτοφυλακή – μη συμβατικός στρατός – εναντίον του συμβατικού αποικιακού στρατού.
- Ναπολεόντειοι Πόλεμοι (1803-1815): η φάση όπου οι βρετανικές συμβατικές δυνάμεις επιτέθηκαν σε πόλεις της Ισπανίας, οι οποίες τελούσαν υπό γαλλικό έλεγχο, σε συνδυασμό με Ισπανούς αντάρτες, οι οποίοι με άτακτες μεθόδους επιτέθηκαν στις γραμμές επικοινωνίας του γαλλικού στρατού.
- Αντιστασιακές οργανώσεις που δημιουργήθηκαν κατά τη διάρκεια του Β΄ Παγκοσμίου Πολέμου σε όλα τα κράτη υπό γερμανική κατοχή με κοινό στόχο την απελευθέρωση τους. Τις οργανώσεις αυτές τις χρηματοδοτούσε η Μεγάλη Βρετανία που μαζί με το συμμαχικό στρατό και τις αντιστασιακές οργανώσεις επιτέθηκαν στον κοινό αντίπαλο, τη Γερμανία.
- Ο πόλεμος στο Βιετνάμ (1955-1975): εμπλοκή συμβατικών στρατών – στρατός των ΗΠΑ, οργανωμένος στρατός Νότιου Βιετνάμ – εναντίον μη συμβατικών στρατών – σύμπραξη

άτακτου στρατού Βόρειου Βιετνάμ με αντάρτες από το Νότιο Βιετνάμ, τους Βιετκόνγκ – η χρήση του ανταρτοπόλεμου στέφθηκε με επιτυχία.

- Πόλεμος Ισραήλ – Λιβάνου εναντίον Χεζμπολάχ (2006): αναδείχτηκε το πόσο επιτυχημένος και επικίνδυνος μπορεί να είναι ένας μη-κρατικός δρώντας και απέδειξε ότι έχει την ικανότητα να επιβιώσει και να αναπτυχθεί στο σύγχρονο κρατοκεντρικού τύπου σύστημα. Κατά τη διάρκεια του πολέμου, αποκεντρωμένοι πυρήνες σιιτικής πολιτικής και στρατιωτικής οργάνωσης, υποκινούμενοι από το Ιράν, συνδύαζαν αντάρτες, συμβατικές ένοπλες δυνάμεις, μη επανδρωμένα αεροσκάφη και μη συμβατική αστική εκστρατεία κατά του συμβατικού στρατού του Ισραήλ. Ενδιαφέρον παρουσιάζει το γεγονός ότι το Ισραήλ αν και δεν ηττήθηκε στο συμβατικό πεδίο μάχης, κατάφερε να αλλάξει ελάχιστα πράγματα στο στρατηγικό περιβάλλον του Λιβάνου κι έχασε τη μάχη των ΜΜΕ καθώς η πλειοψηφία της διεθνούς κοινότητας πίστευε πως το Ισραήλ ηττήθηκε από τη Χεζμπολάχ.
- Πόλεμος στην Κριμαία (2014): μεταξύ συμβατικών ουκρανικών ενόπλων δυνάμεων και ρωσόφωνων αντιστασιακών ομάδων σε συνδυασμό με ενεργειακό εμπάργκο από τη Ρωσία κι επιθέσεις στον κυβερνοχώρο. Επανήλθε στο προσκήνιο ο υβριδικός πόλεμος κι αποτέλεσε κινητήριο δύναμη για τη Δύση για να προβεί σε ενέργειες για την αντιμετώπιση του.
- Πόλεμος στη Συρία (2011-σήμερα): διαδραματίζεται μεταξύ συριακών συμβατικών ενόπλων δυνάμεων – συριακή κυβέρνηση – πολλές παραστρατιωτικές ομάδες, τουρκικές ένοπλες δυνάμεις, ρωσικές, αμερικανικές και γαλλικές αεροπορικές επιδρομές, τζιχαντιστές (ISIS) και πολύ μεγάλο εύρος μεσών και μεθόδων κυρίως από τις μη συμβατικές δυνάμεις που έχουν κάνει την απειλή δυσδιάκριτη και μη αντιμετωπίσιμη· στην περίπτωση του ISIS, στρατολόγηση μέσω διαδικτύου.

  Το παράδειγμα της Συρίας κρίνεται αντιπροσωπευτικό για τη μορφή του υβριδικού πολέμου καθώς δεν αφήνει αμέτοχη καμία διάσταση του πολέμου.

Συμπεράσματα

Τα τελευταία χρόνια ,καθώς ο κυβερνοχώρος στρατιωτικοποιείται ολοένα και περισσότερο και προσαρμόζεται για πολεμική χρήση, δεν αντιλαμβανόμαστε ακόμα τις συνέπειες -πολιτικές πολιτιστικές και ψυχολογικές-της καινούργιας αυτής ικανότητας μας να εκμεταλλευόμαστε τη φυσική και συναισθηματική απόσταση ,ώστε να απομακρύνουμε τον ανθρώπινο παράγοντα από τον πόλεμο, σε τέτοιο βαθμό. Ιστορικά ο πόλεμος από απόσταση έχει ξανασυμβεί με τη χρήση πυραύλων, αλλά στο μέλλον θα είναι κοινά αποδεκτό να υπάρχει ακόμα μεγαλύτερη

απόσταση ανάμεσα στον επιτιθέμενο και το πεδίο της μάχης. Με περισσότερες επιλογές στη σύγκρουση ,που δεν θα ξεσηκώνουν τη δημόσια γνώμη ,οι κυβερνήσεις μπορούν να πετύχουν τους στόχους τους, χωρίς να χρειαστεί να εμπλέξουν τα στρατεύματα τους και με αυτόν τον τρόπο να μειώσουν εντελώς την πιθανότητα ενός ανοιχτού πολέμου.

Μικρότερες απώλειες σε ανθρώπινες ζωές, λιγότερες παράπλευρες απώλειες και μειωμένος κίνδυνος τραυματισμών είναι καλοδεχούμενα αποτελέσματα αλλά η στροφή σε ένα πιο αυτοματοποιημένο πεδίο μάχης θα φέρει νέες προκλήσεις και προβλήματα, όπως αυτό της κυβερνοασφάλειας. Κυρίαρχη πρόκληση θα είναι η διατήρηση της κυβερνοασφάλειας των εξοπλισμών και των συστημάτων.

Ο υβριδικός πόλεμος είναι σχεδιασμένος ώστε να αναδεικνύει τα τρωτά σημεία του αντιπάλου και να επιτίθεται με μη συμβατικά μέσα.

Ο αυτοματοποιημένος πόλεμος μελλοντικά θα οδηγήσει σε περισσότερες κυβερνοεπιθέσεις, δύσκολα ανιχνεύσιμες καθώς και στην ανάπτυξη νέων κυβερνοόπλων για την υποβάθμιση ή καταστροφή των δικτύων επικοινωνίας του αντιπάλου. Ο περιορισμός της ζημιάς αυτών των επιθέσεων προϋποθέτει συστήματα ολοκληρωτικά «αδιαπέραστα», πράγμα αδύνατο από τη στιγμή που οι ίδιοι οι κατασκευαστές και ειδικοί ασφάλειας δεν μπορούν να αντιμετωπίσουν τα ελαττώματά τους.

Οι ασύμμετρες απειλές στις συγκρούσεις θα συνεχίσουν να θέτουν απρόβλεπτα προβλήματα ακόμα και για τις πιο εξεζητημένες τεχνολογίες που με αυτόν τον τρόπο αναγκάζονται να προσαρμόζουν συνεχώς τα προϊόντα τους.

Ο υβριδικός πόλεμος συνιστά την κύρια αιτία ανησυχίας του Δυτικού κόσμου, διότι είναι απρόβλεπτος, πολύπλευρος και ταχύτατα εξελισσόμενος. Η διεθνής πραγματικότητα οδηγείται σε ένα νέο επίπεδο, στο οποίο η στρατιωτική υπεροχή, η εξασφάλιση συμμάχων και οι δεινές διαπραγματευτικές ικανότητες των κρατών δεν μπορούν να εγγυηθούν την εσωτερική, περιφερειακή και εν τέλει παγκόσμια ασφάλεια, αφού λιγότερο ισχυροί δρώντες επιλέγουν τη χρήση μη παραδοσιακών μέσων και τεχνικών.

Οι χρονοβόρες προσπάθειες των ερευνητών να προσδιορίσουν τη μορφή και τα χαρακτηριστικά του ξεπερνιούνται από την εμφάνιση νέων μέσων και μεθόδων, διευρύνοντας έτσι το πεδίο έρευνας και περιορίζοντας το χρονικό περιθώριο ανάπτυξης αμυντικών μηχανισμών. Παραστρατιωτικές ομάδες, μη κρατικοί δρώντες, τρομοκρατικές οργανώσεις και άλλοι υβριδικοί φορείς δρουν απρόσμενα, χρησιμοποιούν ανορθόδοξους πόρους,

υπογραμμίζοντας κατά αυτόν τον τρόπο τα θεσμικά εμπόδια που αντιμετωπίζουν φορείς της διεθνούς κοινότητας, όπως η Βόρειο-Ατλαντική Συμμαχία, η Ευρωπαϊκή Ένωση και τα Ηνωμένα Έθνη, στην προσπάθειά τους να ανταποκριθούν έγκαιρα στις υβριδικές απειλές.

Ένας υβριδικός πόλεμος μπορεί να διαφέρει από έναν άλλον εξαιτίας της ποικιλίας των υβριδικών απειλών και της έντονης πολυμορφίας που επεκτείνει το εύρος του πολέμου. Η περιπλοκότητα του φαινομένου προκύπτει από τα πολλά και διαφορετικά είδη υβριδικών απειλών που υπάρχουν. Οι μέθοδοι αντιμετώπισης των δυτικών θεσμών – ΝΑΤΟ, ΕΕ – κρίνονται μερικώς αποτελεσματικοί, καθώς δεν προσαρμόζονται γρήγορα στις μεταβολές του φαινομένου. Τα κράτη οφείλουν να αναπτύξουν εθνική πολιτική αντιμετώπισης του υβριδικού πολέμου και να συντονίσουν τη δράση τους με άλλα κράτη για την πιο αποτελεσματική αντιμετώπισή του. Η πολυμορφία του υβριδικού πολέμου οδηγεί και στην πολυμορφία των τρόπων αντιμετώπισης.

Ανακεφαλαιώνοντας, η διεξαγωγή υβριδικών επιχειρήσεων σημαίνει και το τέλος των συγκρούσεων με την ιστορική μορφή που ήταν γνωστή. Πλέον αποκτούν ολοένα και περισσότερα υβριδικά χαρακτηριστικά, εξέλιξη αναμενόμενη, αφού έτσι εξυπηρετούνται πιο αποτελεσματικά οι επιδιώξεις των υβριδικών δρώντων. Η αναχαίτιση δράσεων που απειλούν την παγκόσμια ασφάλεια έγκειται στην αποφασιστική αντιμετώπιση από διεθνείς φορείς. Ωστόσο, δεν θα πρέπει να επιδιώκεται μόνο η ενίσχυση στρατιωτικής ισχύος, διότι δεν θα ήταν αποτελεσματική έναντι απρόβλεπτων και καινοτόμων δράσεων. Η προσαρμογή στις νέες τεχνικές και η ανάπτυξη υβριδικών μέσων είναι οι τρόποι που θα σηματοδοτήσουν τη θωράκιση της απειλούμενης διεθνούς κοινότητας, βήματα που επιτυγχάνονται μέσα από ουσιαστική μεταξύ των χωρών συνεργασία, στην οποία κι η Ελλάδα καλείται να συμμετάσχει, ανταποκρινόμενη στα νέα πλέον παγκόσμια δεδομένα των υβριδικών πολέμων.

Βιβλιογραφία

Ελληνική

Κουσκουβέλης, Η.(1995) Διπλωματία και Στρατηγική της Ευρωπαϊκής Ένωσης,. Αθήνα :Εκδόσεις Παπαζήση

Κωνσταντόπουλος, Ι. (2019) 'Στόχοι των υβριδικών απειλών είναι οι κοινωνίες και όχι οι στρατοί', *HuffPost Greece*. Διαθέσιμο στο : https://www.huffingtonpost.gr/entry/ioannes-konstantopoelos-stochoi-ton-evridikon-apeilon-einai-oi-koinonies-kai-ochi-oi-stratoi_gr_5cbee6ffe4b0f7a84a74b9e2

Λιαρόπουλος, Α. (2020) 'Ρωσικές Πληροφοριακές Επιχειρήσεις: Κυριαρχώντας στο Πληροφοριακό Περιβάλλον', *Ναυτική Επιθεώρηση*, 612(180), σ.σ. 68–81.

Λω, Ράνταλ. Ντ. ,Μεταφρ. Δήτσας, Φ. Επιστ. Επιμ. Μπόση, Μ. (2020) *Τρομοκρατία: μια παγκόσμια ιστορία*. Πανεπιστημιακές Εκδόσεις Κρήτης. Διαθέσιμο στο: https://osdelnet.gr/book/1273882.

Μπόση, Μ. (2019a) 'Η μετάλλαξη της τρομοκρατίας', *Dikastiko.gr*. Διαθέσιμο στο: https://www.dikastiko.gr/articles/μαίρη-μπόση-η-μετάλλαξη-της-τρομοκρατ/.

Μπόση, Μ. (2019b) 'Η τρομοκρατία στην Ελλάδα, δεν έχει ιδεολογία'. Διαθέσιμο στο: https://www.liberal.gr/apopsi/mairi-mposi-i-tromokratia-stin-ellada-den-echei-ideologia/273681.

Μπόση, Μ. (2018). Οι όψεις της διεθνούς αφάλειας. Αθήνα: Εκδόσεις Ποιότητα.

Μπόση, Μ. (2014). Η διεθνής ασφάλεια στον μεταψυχροπολεμικό κόσμο. Οι αραβικές εξεγέρσεις και η περίπτωση της Συρίας. Αθήνα: Εκδόσεις Ποιότητα.

Μπόση, Μ. (2000). Περί του ορισμού της τρομοκρατίας, [Επιμέλεια: Στ. Κράτσης] Αθήνα: Εκδόσεις Τραύλος.

Μπόση, Μ. (1999). Ζητήματα ασφάλειας στη νέα τάξη πραγμάτων. [Πρόλογος: Γ. Πανούσης] Αθήνα: Εκδόσεις Παπαζήσης.

Σαμαράς Ν., Α. *και άλλοι.* 'Βιβλίο Συνόψεων_ Κοινωνία της επιτήρησης: Από την Κυβερνοασφάλεια στα Fake News| Μέσα| Μηνύματα| Στρατηγικές', στο: *7ο Επιστημονικό Συνέδριο Εργαστήριο στρατηγικής Επικοινωνίας και Μέσων Ενημέρωσης Συνδιοργάνωση: Εργαστήριο Πληροφόρησης και Κυβερνοασφάλειας. Εισαγωγικό σημείωμα: Ανδρέας*

Λιαρόπουλος, Επίκουρος Καθηγητής, Τμήμα Διεθνών & Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς, Διευθυντής Εργαστηρίου Πληροφόρησης και Κυβερνοασφάλειας.

Τσαρδανίδης, Χ. (2008) Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (ΚΕΠΠΑ).Ν. Μαραβέγιας (επιμέλεια) Ευρωπαϊκή Ένωση: Δημιουργία, Εξέλιξη, Προοπτικές. Εκδόσεις Κριτική (2016).

Eric Schmidt, Jared Cohen (2014): Η Νέα Ψηφιακή Εποχή-Οι επιπτώσεις στα Έθνη, την Επιχειρηματικότητα και τη Ζωή μας.

Σορμάς Στέφανος (2015): Διπλωματική Εργασία με θέμα: «Υβριδικός πόλεμος: Η νέα πρόκληση για την ασφάλεια της Ευρώπης» Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στις Διεθνείς Σχέσεις και Ασφάλεια, Ανώτατη Διακλαδική Σχολή Πολέμου, Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών Τμήμα Βαλκανικών, Σλαβικών και Ανατολικών Σπουδών (Πανεπιστήμιο Μακεδονίας).

Ξενόγλωσση

Andr as Racz. (2015). *Russia's Hybrid War in Ukraine: Breaking Enemy's Ability to Resist*. http://www.fiia.fi/en/publication/514/

Cyber Crime: Critical View. (2016). *International Journal of Science and Research (IJSR)*, *5*(1), 85–87. https://doi.org/10.21275/v5i1.nov152579

D. Cantwell. (2017). Cantwell, Hybrid Warfare: Aggression and Coercion in the Gray Zone. *ASIL Insights*, *21*(14), 1–10. https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone

Daniel Van Puyveld. (2015). *'Hybrid war–does it even exist?'* http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/

Darling, J. R. (1999). Organizational excellence and leadership strategies: principles followed by top multinational executives. Leadership & Organization Development Journal, 20(6), 309–321. https://doi.org/10.1108/01437739910292625

Hoffman, F.G., "Hybrid Warfare and Challenges", Joint Forces Quarterly. 2009:52, 34–39.

Hoffman, F. G., Conflict in the 21st Century: The Rise of Hybrid Warfare (Potomac Institute for Policy Studies, 2007);

Kramer, Andrew, και Michael Gordon. 2014. «Ukraine Reports Russian Invasion on a New Font.» The New York Times, 27 August.

Lind, William S. 2004. «Understanding the Fourth Generation War.» Military Review 14.

McCuen, J. "Hybrid Wars," Military Review 88, no. 2 (March-April 2008): 107-113, quote on p. 107.

Manko, O., & Mikhieiev, Y. (2018). Defining the Concept of 'Hybrid Warfare' Based on the Analysis of Russia's Aggression against Ukraine. *Information & Security: An International Journal*, *41*, 11–20. https://doi.org/10.11610/isij.4107

Munoz Mosquera, A. B., & Bachmann, S. D. (2016). Lawfare in Hybrid Wars: The 21st Century Warfare. *Journal of International Humanitarian Legal Studies*, *7*(1), 63–87. https://doi.org/10.1163/18781527-00701008

Nemeth J. William., USMC, Future War and Chechnya: A Case for Hybrid Warfare (Monterey, CA: Naval Postgraduate School, June 2002).

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE (Ed.). (2016, May). *SOCIAL MEDIA AS A TOOL OF HYBRID WARFARE*. https://www.stratcomcoe.org/download/file/fid/5314

Nicu Popescu. (2015, October). *Hybrid tactics: Russia and the West*. http://www.iss.europa.eu/uploads/media/Alert_46_Hybrid_Russia.pdf

Philp, W. R., & Martin, C. P. (2009). A philosophical approach to time in military knowledge management. *Journal of Knowledge Management*, *13*(1), 171–183. https://doi.org/10.1108/13673270910931242

Sari, A. (2019). Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats. *SSRN Electronic Journal*, 1–24. https://doi.org/10.2139/ssrn.3315682

Stupples, D. (2015, November 26). *The next war will be an information war, and we're not ready for it*. The Conversation. https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218

Vassileva, B., & Zwilling, M. (2018). Hybrid Warfare Simulation-based Learning: Challenges and Opportunities. *Information & Security: An International Journal*, *39*(3), 220–234. https://doi.org/10.11610/isij.3919

Νομικό περιεχόμενο (https://eur-lex.europa.eu/)

COM (2007) 267, Ανακοίνωση της Επιτροπής «Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο» (22.5.2007)

COM (2012) 149, Ανακοίνωση της Ευρωπαϊκής Επιτροπής σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας, «Προστασία της Ευρώπης από επιθέσεις στον κυβερνοχώρο και διαταραχές μεγάλης κλίμακας: αναβάθμιση της ετοιμότητας, της ασφάλειας και της ικανότητας αποκατάστασης» (30.3.2009)

COM (2010) 521 τελικό, Κανονισμός Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου σχετικά με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) (30.9.2010)

COM(2010) 245 :Ψηφιακό θεματολόγιο για την Ευρώπη (26.8.2010)

COM (2011) 163 τελικό, Ανακοίνωση της Ευρωπαϊκής Επιτροπής σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας, «Επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο» (31.3.2011)

COM (2012) 140, Ανακοίνωση της Ευρωπαϊκής Επιτροπής για την αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο (28.3.2012)

COM(2013) 173 final Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον οργανισμό της Ευρωπαϊκής Ένωσης για τη συνεργασία και την κατάρτιση στον τομέα της επιβολής του νόμου (Ευρωπόλ) και για την κατάργηση των αποφάσεων 2009/371/ΔΕΥ και 2005/681/ΔΕΥ

COM (2015) 185 τελικό, Ανακοίνωση της Ευρωπαϊκής Επιτροπής για «Το ευρωπαϊκό θεματολόγιο για την ασφάλεια» (28.3.2012)

Ιστολόγια

https://scholar.google.com/citations?user=wKWyhzcAAAAJ&hl=el&fbclid=IwAR3tV0z6Si60a-O7s96dHHx4Zdf4F2gk-LwV6ATMn9SZiknRvbAuwbuyVr8

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52011DC0790

https://ec.europa.eu/commission/presscorner/detail/el/IP_18_3343

https://ec.europa.eu/commission/presscorner/detail/el/IP_19_843

https://ec.europa.eu/commission/presscorner/detail/el/IP_11_1453

https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

https://defencereview.gr/yvridikos-polemos-apo-ton-thoykydidi-s/

https://www.europol.europa.eu/about-europol

https://www.cepol.europa.eu/

https://www.eurojust.europa.eu/

https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020

https://slideplayer.gr/slide/3644031/" title="ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ"

Working papers

Αλέξανδρος-Ιωάννης Καργόπουλος (Πρωτοδίκης, εθνικός εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε.) Κυβερνο-έγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου.