ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ - ΣΧΟΛΗ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΕΣΟΓΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«Διακυβέρνηση, ανάπτυξη και ασφάλεια στη Μεσόγειο»

Η ασφάλεια στον Κυβερνοχώρο και η οπτική της Ευρώπης

Security in Cyberspace and Europe's perspective

Διπλωματική εργασία του Μιχαήλ Ιωσηφίδη, Α.Μ. : 4332022007

Επιβλέπων καθηγητής

Σωτήρης Ντάλης

Μέλη Επιτροπής

Ιωάννης Σεϊμένης

Ιωάννης Φούκας

Ρόδος, Δεκέμβριος 2023

“ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ. Η εργασία που παραδίδω είναι αποτέλεσμα πρωτότυπης έρευνας και δεν χρησιμοποιώ πνευματική ιδιοκτησία τρίτων χωρίς αναφορές. Αναλαμβάνω όλες τις νομικές και διοικητικές συνέπειες που δύναμαι να αντιμετωπίσω σε περίπτωση που η εργασία μου αποδειχθεί ότι αποτελεί προϊόν λογοκλοπής, σύμφωνα με τον Κανονισμό του Ιδρύματος.”

Περιεχόμενα

Σύνοψη

Η Ευρωπαϊκή Ένωση (ΕΕ), από τις αρχές του 21ου αιώνα, έχει υιοθετήσει μια ολοκληρωμένη προσέγγιση για την ασφάλεια στον κυβερνοχώρο, κάτι το οποίο φαίνεται από τη διερεύνηση του νομικού της πλαισίου, των πρωτοβουλιών και των εταιρικών σχέσεων. Ο κανονισμός 2019/881, γνωστός ως νόμος για την ασφάλεια στον κυβερνοχώρο, αποτελεί κομβικό ορόσημο, εισάγοντας ένα πλαίσιο πιστοποίησης και ενισχύοντας τον ρόλο του ENISA. Η δέσμευση της ΕΕ για συνεργασία εκδηλώνεται μέσω της CSCG, της διεθνούς δέσμευσης και της συνεργασίας δημόσιου και ιδιωτικού τομέα. Η πρόληψη του εγκλήματος στον κυβερνοχώρο, η κατανόηση του βαθύ και σκοτεινού ιστού και η αντιμετώπιση του κυβερνοπολέμου βρίσκονται στην πρώτη γραμμή των προσπαθειών της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Η προστασία των υποδομών ζωτικής σημασίας και η εκπαίδευση στην κυβερνοασφάλεια υπογραμμίζουν περαιτέρω την ολιστική της προσέγγιση. Στην ουσία, η ΕΕ έχει διαμορφώσει ένα εξελιγμένο σύστημα κυβερνοπροστασίας.

Λέξεις κλειδιά: κυβερνοχώρος, κυβερνοασφάλεια, απειλές, έγκλημα, νομικό πλαίσιο.

Summary

The European Union (EU), since the beginning of the 21st century, has taken a comprehensive approach to cyber security, as seen by exploring its legal framework, initiatives and partnerships. Regulation 2019/881, known as the Cyber Security Law, is a key milestone, introducing a certification framework and strengthening the role of ENISA. The EU's commitment to cooperation is manifested through the CSCG, international engagement and public-private partnership. Preventing cybercrime, understanding the deep and dark web and tackling cyberwarfare are at the forefront of the EU's cyber security efforts. Critical infrastructure protection and cybersecurity training further underscore its holistic approach. In essence, the EU has developed a sophisticated system of cyber protection.

Keywords: cyberspace, cyber security, threats, crime, legal framework.

Εισαγωγή

Σε έναν ολοένα και πιο διασυνδεδεμένο και ψηφιακό κόσμο, η έννοια της κυβερνοασφάλειας έχει αναδειχθεί σε σοβαρή ανησυχία για τις κυβερνήσεις, τους οργανισμούς και τους ιδιώτες. Το παρόν κείμενο εμβαθύνει στον πολύπλευρο τομέα της κυβερνοασφάλειας, διερευνώντας τις θεμελιώδεις αρχές, τα σκιώδη πεδία του βαθύ και σκοτεινού ιστού, το ποικίλο φάσμα των απειλών στον κυβερνοχώρο και το δυναμικό τοπίο των ευρωπαϊκών πρωτοβουλιών για την κυβερνοασφάλεια μέσα από τη μελέτη της σύγχρονης βιβλιογραφίας, επιστημονικών και ηλεκτρονικών άρθρων αλλά και των κανονισμών και οδηγιών της Ευρωπαϊκής Ένωσης.

Η ανάλυση ξεκινά με μια ολοκληρωμένη εξέταση των θεμελιωδών στοιχείων της κυβερνοασφάλειας. Το Κεφάλαιο 1 διευκρινίζει τον ορισμό του κυβερνοχώρου και της κυβερνοασφάλειας, παρέχοντας ουσιαστικό πλαίσιο για τις συζητήσεις που ακολουθούν. Παρακολουθεί την εξέλιξη των εννοιών της κυβερνοασφάλειας με την πάροδο του χρόνου, αναδεικνύοντας τη διαρκώς εξελισσόμενη φύση του τομέα. Επιπλέον, το κεφάλαιο αυτό εμβαθύνει στον κομβικό ρόλο που διαδραματίζουν τα έθνη-κράτη στο πεδίο της ασφάλειας στον κυβερνοχώρο, ρίχνοντας φως στις ευθύνες και τις προκλήσεις τους.

Το κεφάλαιο 2 επιχειρεί μια περιήγηση στα βάθη του διαδικτύου, αποκαλύπτοντας τον μυστηριώδη κόσμο του βαθύ και σκοτεινού ιστού. Ρίχνει φως στις δραστηριότητες του οργανωμένου εγκλήματος σε αυτές τις κρυφές γωνιές, όπου ανθίζουν οι παράνομες επιχειρήσεις. Επιπλέον, το κεφάλαιο αυτό διερευνά την ανησυχητική παρουσία του εξτρεμισμού και της τρομοκρατίας στον κυβερνοχώρο, τονίζοντας τις προκλήσεις που θέτει για την ασφάλεια. Τέλος, περιηγείται στα ύδατα της πορνογραφίας και της διασταύρωσής της με τον κυβερνοχώρο, παρέχοντας πληροφορίες για αυτή τη συχνά παραγνωρισμένη διάσταση.

Το τρίτο κεφάλαιο διεισδύει στο πεδίο των κρατικών ανησυχιών για την κυβερνοασφάλεια - τις επιθέσεις και τις απειλές στον κυβερνοχώρο. Κατηγοριοποιεί και αναλύει διάφορους τύπους επιθέσεων στον κυβερνοχώρο, από το ransomware έως τις κρατικά χρηματοδοτούμενες επιχειρήσεις, προσφέροντας μια ολοκληρωμένη κατανόηση των διαρκώς υπαρκτών κινδύνων. Στη συνέχεια, το κεφάλαιο εμβαθύνει στο σύνθετο πεδίο του κυβερνοπολέμου, όπου ο ψηφιακός πόλεμος υπερβαίνει τα

γεωγραφικά σύνορα. Το έγκλημα στον κυβερνοχώρο είναι μια άλλη κρίσιμη πτυχή που διερευνάται, υπογραμμίζοντας τον αντίκτυπό του σε άτομα, επιχειρήσεις και έθνη. Επιπλέον, το κεφάλαιο αυτό διερευνά τους οργανισμούς και τις ενίοτε αμφιλεγόμενες πρακτικές τους στο πεδίο του κυβερνοχώρου.

Το τελευταίο κεφάλαιο μετατοπίζει την εστίαση στις ευρωπαϊκές πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο, αναδεικνύοντας την προληπτική προσέγγιση της Ευρωπαϊκής Ένωσης (ΕΕ) για τη διασφάλιση του ψηφιακού της τοπίου. Ξεκινά με την αποκάλυψη του νομικού πλαισίου που διέπει τις προσπάθειες της ΕΕ για την ασφάλεια στον κυβερνοχώρο, τονίζοντας τη σημασία της κατανόησης του νομικού καθεστώτος στην Ευρώπη. Εξετάζεται διεξοδικά η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο, με επίκεντρο την οικοδόμηση ανθεκτικότητας, και ακολουθεί η διερεύνηση του κομβικού ρόλου του ENISA στην ασφάλεια των ευρωπαϊκών δικτύων και πληροφοριών. Ο κανονισμός 2019/881, γνωστός ως νόμος για την ασφάλεια στον κυβερνοχώρο, βρίσκεται στο επίκεντρο, καθώς ενισχύει τα μέτρα ασφάλειας στον κυβερνοχώρο σε ολόκληρη την ΕΕ. Το κεφάλαιο ολοκληρώνεται με την επισήμανση της δέσμευσης της ΕΕ για την προώθηση της συνεργασίας μέσω εταιρικών σχέσεων και διαφόρων πρωτοβουλιών.

Στην καταληκτική ενότητα, η σύνθεση των διερευνηθέντων θεμάτων αποκαλύπτει την ολοκληρωμένη και συνεργατική προσέγγιση της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Υπογραμμίζει την αφοσίωση της ΕΕ στην εξασφάλιση των δικτύων, των πληροφοριών και των κρίσιμων υποδομών της, συμβάλλοντας έτσι σε ένα ασφαλέστερο και ασφαλέστερο ψηφιακό περιβάλλον για τους πολίτες και τους παγκόσμιους εταίρους της.

1. Θεμέλια της κυβερνοασφάλειας

1.1 Ορισμός του κυβερνοχώρου και της κυβερνοασφάλειας

Ο κυβερνοχώρος, που συχνά αναφέρεται ως ψηφιακός χώρος, περιλαμβάνει το τεράστιο διασυνδεδεμένο δίκτυο υπολογιστικών συστημάτων, διακομιστών, συσκευών και δεδομένων που αποτελεί τη βάση της σύγχρονης κοινωνίας. Είναι ένας τομέας όπου ανταλλάσσονται πληροφορίες, πραγματοποιούνται συναλλαγές και παρέχονται υπηρεσίες μέσω του διαδικτύου και άλλων δικτύων επικοινωνίας. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, ο κυβερνοχώρος διαδραματίζει ολοένα και πιο ζωτικό ρόλο στην καθημερινή μας ζωή, από την προσωπική επικοινωνία και τις ηλεκτρονικές αγορές μέχρι τις κρίσιμες υποδομές και την εθνική ασφάλεια.

Η κυβερνοασφάλεια, έννοια στενά συνδεδεμένη με τον κυβερνοχώρο, είναι η πρακτική της προστασίας αυτού του ψηφιακού τομέα από διάφορες απειλές και τρωτά σημεία που μπορούν να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων και των συστημάτων. Περιλαμβάνει ένα ευρύ φάσμα στρατηγικών, τεχνολογιών και πρακτικών που αποσκοπούν στην προστασία των πληροφοριών και στη διασφάλιση της ομαλής λειτουργίας των ψηφιακών υποδομών. Στην Ευρώπη, η ασφάλεια στον κυβερνοχώρο έχει καταστεί σημαντική προτεραιότητα λόγω της αυξανόμενης εξάρτησης από την τεχνολογία και των κλιμακούμενων απειλών στον κυβερνοχώρο που αντιμετωπίζουν τα άτομα, οι οργανισμοί και οι κυβερνήσεις.

Η Ευρώπη, όπως και τα περισσότερα κράτη στην υφήλιο, έχει τη δική της προοπτική για τον κυβερνοχώρο και την κυβερνοασφάλεια, η οποία προκύπτει από τη δέσμευσή της να διασφαλίσει ένα ασφαλές και ανοικτό ψηφιακό περιβάλλον στους πολίτες της. Συναφώς, οι βασικότεροι παράγοντες που συμμετέχουν στην προσέγγιση της έννοιας του κυβερνοχώρου είναι οι παρακάτω:

- Ρυθμιστικό πλαίσιο: Η θέσπιση ενός ισχυρού ρυθμιστικού πλαισίου για την ασφάλεια στον κυβερνοχώρο φαντάζει απαραίτητη τη σημερινή εποχή. Στο πλαίσιο αυτό, ο οργανισμός της ΕΕ για την κυβερνοασφάλεια, γνωστός ως ENISA (Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια), διαδραματίζει κεντρικό ρόλο στον συντονισμό και την εφαρμογή μέτρων κυβερνοασφάλειας.

Ο κανονισμός της ΕΕ του 2019[1] για τον ENISA θέτει τις βάσεις για μια εναρμονισμένη προσέγγιση της κυβερνοασφάλειας εντός της ΕΕ.

- Τοπίο απειλών: Καμία χώρα ή οργανισμός δεν είναι απρόσβλητος από τις εξελισσόμενες απειλές στον κυβερνοχώρο που ξεπερνούν τα σύνορα. Επιθέσεις στον κυβερνοχώρο, όπως το Hack της Bundestag το 2015[2] και το ξέσπασμα του ransomware WannaCry το 2017[3] κατέδειξαν την ανάγκη για προληπτικά μέτρα κυβερνοασφάλειας αλλά και την υπάρχουσα ευπάθεια σε απειλές.
- Γεωπολιτικές εκτιμήσεις: Η γεωπολιτική του κυβερνοχώρου διαμορφώνει επίσης την προοπτική των κρατών για την κυβερνοασφάλεια. Περιπτώσεις κυβερνοεπιθέσεων που χρηματοδοτούνται από έτερα κράτη, όπως η απόπειρα διακοπής του δικτύου ηλεκτροδότησης της Ουκρανίας από Ρώσους hacker[4], υπογραμμίζουν την ανάγκη διεθνούς συνεργασίας και διπλωματίας για την αντιμετώπιση των απειλών στον κυβερνοχώρο.
- Ανησυχίες για τον σκοτεινό ιστό: Τα κράτη και οι οργανισμοί αναγνωρίζουν τις προκλήσεις που θέτει ο σκοτεινός ιστός, ένα κρυφό τμήμα του διαδικτύου που χρησιμοποιείται για παράνομες δραστηριότητες και εγκλήματα στον κυβερνοχώρο.[5] Ο αντίκτυπος του σκοτεινού ιστού στη διακυβέρνηση του διαδικτύου και την ασφάλεια στον κυβερνοχώρο έχει αποτελέσει θέμα έντονης ανησυχίας.[6]
- Αποτροπή στον κυβερνοχώρο: Σημαντικοί πόροι αναλώνονται και στον τομέα που αφορά την έννοια της αποτροπής στον κυβερνοχώρο, όπως αναλύεται από τον Libicki[7]. Επιδιώκοντας να αποτρέψουν τις κυβερνοεπιθέσεις, τα Κράτη

[1] Κανονισμός ΕΕ 2019/881, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32019R0881.
[2] Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
[3] Hern A. (2017), WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017, *The Guardian*.
[4] O'Neill P.H. (2022), Russian hackers tried to bring down Ukraine's power grid to help the invasion, *MIT Technology Review*.
[5] Greenberg A. (2014), Hacker Lexicon: What is the Dark Web?, *Wired* διαθέσιμο στο https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/
[6] Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance*, No.6. Σελ. 3-7
[7] Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND corporation. Σελ. 13

αναγνωρίζουν τη σημασία της δημιουργίας αξιόπιστων μηχανισμών αποτροπής προς αποθάρρυνση των δυνητικών αντιπάλων τους.

- Συνεργασία και ανθεκτικότητα: Έμφαση στη συνεργασία μεταξύ του δημόσιου και του ιδιωτικού τομέα για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Η οικοδόμηση ενός ανθεκτικού κυβερνοχώρου αποτελεί ένα κοινό στόχο για βιομηχανία και κυβερνήσεις. [8]
- Αναδυόμενες τεχνολογίες: Εξελισσόμενες τεχνολογίες, όπως η τεχνητή νοημοσύνη και η κβαντική πληροφορική, διαδραματίζουν κρίσιμο ρόλο τόσο στις απειλές όσο και στις άμυνες στον κυβερνοχώρο. Οι τεχνολογίες αυτές προσφέρουν νέες ευκαιρίες για τους επιτιθέμενους στον κυβερνοχώρο, αλλά και καινοτόμες λύσεις για τις προκλήσεις της κυβερνοασφάλειας.
- Εκπαίδευση και ευαισθητοποίηση: Δίνεται σημασία στην εκπαίδευση των πολιτών και των οργανισμών της σχετικά με τις βέλτιστες πρακτικές κυβερνοασφάλειας. Οι πρωτοβουλίες που αποσκοπούν στην αύξηση της ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας και του ψηφιακού αλφαβητισμού αποτελούν αναπόσπαστο μέρος της ευρωπαϊκής προσέγγισης.

Συμπερασματικά, η προοπτική των κρατών και κατ' επέκταση της ΕΕ για τον κυβερνοχώρο και την κυβερνοασφάλεια χαρακτηρίζεται από μια προληπτική και συνεργατική προσέγγιση, με γνώμονα την ανάγκη προστασίας των ψηφιακών υποδομών και των πολιτών τους. Το ρυθμιστικό πλαίσιο, το τοπίο των απειλών, οι γεωπολιτικές εκτιμήσεις και η δέσμευση για έναν ανοικτό και ασφαλή κυβερνοχώρο διαμορφώνουν τη στάση τους. Με τις συνεχείς εξελίξεις στην τεχνολογία και το διαρκώς εξελισσόμενο τοπίο απειλών, εντοπίζεται μια προσήλωση στην προσαρμογή και την ενίσχυση των προσπαθειών των κρατών για την ασφάλεια στον κυβερνοχώρο με στόχο την αντιμετώπιση των προκλήσεων της νέας ψηφιακής εποχής.

1.2 Η εξέλιξη των εννοιών της κυβερνοασφάλειας

Η κυβερνοασφάλεια, στη σύγχρονη μορφή της, έχει υποστεί βαθιά μεταμόρφωση με την πάροδο των ετών. Έχει εξελιχθεί από ένα εξειδικευμένο ζήτημα σε έναν απαραίτητο πυλώνα της σύγχρονης κοινωνίας. Η εξέλιξη αυτή έχει διαμορφωθεί από

[8] Dunn Cavelty, M. , & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, 15(1), Σελ. 37-57.

έναν συνδυασμό τεχνολογικής προόδου και εξελισσόμενων τοπίων απειλών. Σε αυτή τη συζήτηση, θα εμβαθύνουμε στα κομβικά στάδια της εξέλιξης των εννοιών της κυβερνοασφάλειας.[9]

Τα πρώτα στάδια της κυβερνοασφάλειας μπορούν να εντοπιστούν στα μέσα του 20ου αιώνα, όταν η πληροφορική βρισκόταν στα σπάργανα. Κατά τη διάρκεια αυτής της περιόδου, τα συστήματα υπολογιστών ήταν σχετικά σπάνια και απομονωμένα. Οι ανησυχίες για την ασφάλεια περιστρέφονταν κυρίως γύρω από τη φυσική πρόσβαση σε αυτά τα μηχανήματα και την προστασία των διαβαθμισμένων πληροφοριών. Ο όρος "κυβερνοασφάλεια" δεν ήταν ακόμη σε κοινή χρήση και η έννοια βρισκόταν ακόμη σε αρχικό στάδιο.

Η εμφάνιση της πειρατείας στη δεκαετία του 1970 σηματοδότησε μια σημαντική καμπή στον τομέα της κυβερνοασφάλειας. Οι πρώτοι hackers[10], συχνά με γνώμονα την περιέργεια και όχι την κακόβουλη πρόθεση, άρχισαν να διερευνούν τα τρωτά σημεία των συστημάτων υπολογιστών. Έννοιες όπως η προστασία με κωδικό πρόσβασης και ο έλεγχος ταυτότητας των χρηστών απέκτησαν σημασία για τους διαχειριστές συστημάτων καθώς προσπαθούσαν να ενισχύσουν την ψηφιακή τους άμυνα.[11]

Τη δεκαετία του 1980 η απειλή στον κυβερνοχώρο, αφορούσε κυρίως κυβερνητικά δίκτυα και επικεντρωνόταν κατά κόρον στην κύβερνο-κατασκοπεία.[12] Ωστόσο παρατηρήθηκε ο πολλαπλασιασμός του κακόβουλου λογισμικού, εγκαινιάζοντας μια νέα εποχή ανησυχιών για την ασφάλεια. Η εξέλιξη αυτή κατέστησε αναγκαία τη δημιουργία λογισμικού προστασίας και την καθιέρωση της έννοιας της τακτικής ενημέρωσης των μέτρων ασφαλείας.[13]

Η ευρεία υιοθέτηση του διαδικτύου κατά τη δεκαετία του 1990 εγκαινίασε μια νέα εποχή προκλήσεων κυβερνοασφάλειας. Η διασυνδεδεμένη φύση του Παγκόσμιου Ιστού παρείχε πολυάριθμες ευκαιρίες για κυβερνοεπιθέσεις. Έννοιες όπως τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολών και η κρυπτογράφηση απέκτησαν

---

[9] Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley. Σελ. 1-10

[10] Hacker, ονομάζεται συνήθως το άτομο το οποίο εισβάλλει σε υπολογιστικά συστήματα ανεξαρτήτως πιθανού κινήτρου ή ηθικής πυξίδας. Μετέπειτα διακρίσεις σε Blackhats, Redhats, Whitehats κ.α.

[11] Denning, D. E. (1999). *Information warfare and security*. ACM Press/Addison-Wesley Publishing Co.

[12] Dunn Cavelty, M. , & Egloff, F. J. (2019). Όπ.π. Σελ. 44

[13] Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, 2016, 4 (6) Σελ. 165-176

ξεχωριστή θέση, καθώς οι οργανισμοί αγωνίζονταν να προστατεύσουν τα δικτυωμένα συστήματά τους από ένα διευρυνόμενο φάσμα απειλών.

Καθώς το ηλεκτρονικό εμπόριο και η ψηφιοποίηση των οικονομικών συναλλαγών κέρδισαν έδαφος, η εστίαση στην προστασία ευαίσθητων δεδομένων, συμπεριλαμβανομένων των πληροφοριών πιστωτικών καρτών και προσωπικών στοιχείων, εντάθηκε. Έννοιες όπως η κρυπτογράφηση δεδομένων, η τεχνολογία Secure Sockets Layer (SSL) και οι ασφαλείς πύλες πληρωμών έγιναν απαραίτητα συστατικά στοιχεία της διαδικτυακής ασφάλειας.[14]

Η δεκαετία του 2000 ήταν μάρτυρας της ανόδου δύο νέων εξελιγμένων μορφών κυβερνοεπιθέσεων. Η πρώτη αφορά μια αλλαγή εστίασης από τη θεωρητική λογική της «ημέρα της κρίσεως» (Doomsday), προς μια κυβερνοεπιθετικότητα σε συγκρούσεις μεταξύ κρατικών και μη φορέων. Με το λόγο της αλλαγής αυτής να εντοπίζεται στην ομαλοποίηση των συγκρούσεων στο κυβερνοχώρο, σταθερά σε πλαίσιο πολιτικών συγκρούσεων κάτω όμως από ένα πιθανό όριο πολέμου.[15] Η δεύτερη αφορά περισσότερη ένταση σε στοχευμένες επιθέσεις. Αφενός έχουμε την αύξηση των "hacks", δηλαδή την επιτυχή διείσδυση σε διακεκριμένους οικονομικούς ή πολιτικούς στόχους και αφετέρου την εστίαση της πολιτικής διαμάχης προηγμένες μόνιμες απειλές (Advanced Persistent Threats - APT), εξελιγμένων, μακροπρόθεσμων κυβερνοεπιθέσεων που συχνά χρηματοδοτούνται από εθνικά κράτη ή καλά χρηματοδοτούμενους οργανισμούς. Έννοιες όπως η νοημοσύνη για απειλές και το κυνήγι απειλών στον κυβερνοχώρο απέκτησαν εξέχουσα θέση, καθώς οι οργανισμοί προσπαθούσαν να ανιχνεύσουν και να ανταποκριθούν σε αυτούς τους ασύλληπτους αντιπάλους.[16]

Σε απάντηση στην αυξανόμενη συχνότητα παραβιάσεων δεδομένων και κυβερνοεπιθέσεων, οι κυβερνήσεις παγκοσμίως άρχισαν να θεσπίζουν κανονισμούς για την ασφάλεια στον κυβερνοχώρο. Αυτό οδήγησε στον πολλαπλασιασμό εννοιών όπως η προστασία δεδομένων, η συμμόρφωση και η κοινοποίηση παραβιάσεων, οι οποίες

[14] Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* HarperCollins.
[15] Dunn Cavelty, M. , & Egloff, F. J. (2019). Όπ.π. Σελ. 44-45
[16] NIST Special Publication 800-53 (2022). *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology.

κατέστησαν ζωτικής σημασίας για τους οργανισμούς που αποσκοπούσαν στην αποφυγή νομικών επιπτώσεων.[17]

Μετέπειτα, η εξέλιξη της αρχιτεκτονικής μηδενικής εμπιστοσύνης, μιας έννοιας που λειτουργεί με βάση την υπόθεση ότι οι απειλές μπορεί να υπάρχουν ήδη εντός του δικτύου, έχει αποκτήσει σημαντική απήχηση. Υπογραμμίζει τη σημασία της αυστηρής επαλήθευσης της ταυτότητας και της συνεχούς παρακολούθησης, ανεξάρτητα από το αν οι χρήστες βρίσκονται εντός ή εκτός του εταιρικού δικτύου.[18]

Η ΕΕ διαδραμάτισε σημαντικό ρόλο στη διαμόρφωση των εννοιών της κυβερνοασφάλειας, ιδίως μέσω κανονιστικών πρωτοβουλιών. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης έχει θέσει ένα παγκόσμιο πρότυπο για την προστασία των δεδομένων και της ιδιωτικής ζωής, επηρεάζοντας τις πρακτικές κυβερνοασφάλειας παγκοσμίως.[19]

Εν κατακλείδι, η εξέλιξη των εννοιών της κυβερνοασφάλειας αντικατοπτρίζει το διαρκώς εξελισσόμενο τοπίο της τεχνολογίας και των απειλών στον κυβερνοχώρο. Από την αρχή της πληροφορικής έως τη σημερινή εποχή των πολύπλοκων απειλών και των αυστηρών κανονισμών, η κυβερνοασφάλεια έχει εξελιχθεί σε απαραίτητο πυλώνα της ψηφιακής μας ύπαρξης. Οι έννοιες και οι στρατηγικές έχουν προσαρμοστεί για να αντιμετωπίσουν τις προκλήσεις που παρουσιάζει μια διασυνδεδεμένη, καθοδηγούμενη από τα δεδομένα κοινωνία. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, οι έννοιες της κυβερνοασφάλειας θα συνεχίσουν να εξελίσσονται, διασφαλίζοντας την προστασία των ψηφιακών περιουσιακών στοιχείων και τη διατήρηση της ιδιωτικής ζωής των ατόμων και των οργανισμών.[20]

1.3 Ο ρόλος των εθνικών κρατών στην ασφάλεια στον κυβερνοχώρο

Σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο που καθοδηγείται από την ψηφιακή τεχνολογία, ο ρόλος των εθνικών κρατών στην κυβερνοασφάλεια έχει καταστεί υψίστης

[17] EU General Data Protection Regulation (GDPR) (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*.

[18] Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., ... & Cobo, M. J. (2020). 20 years of scientific evolution of cyber security: A science mapping. *In International Conference on Industrial Engineering and Operations Management*. IEOM Society International. Sel. 314-325

[19] EU General Data Protection Regulation (GDPR) (2018), Όπ.π.

[20] Dunn Cavelty, M. , & Egloff, F. J. (2019). Όπ.π. Σελ. 37-57

σημασίας. Οι απειλές στον κυβερνοχώρο ξεπερνούν τα σύνορα, θέτοντας σημαντικούς κινδύνους για τις κυβερνήσεις, τις υποδομές ζωτικής σημασίας, τις επιχειρήσεις και τους ιδιώτες. Ως αποτέλεσμα, τα εθνικά κράτη διαδραματίζουν πολύπλευρους ρόλους στην άμυνα κατά των επιθέσεων στον κυβερνοχώρο, στη θέσπιση πολιτικών στον κυβερνοχώρο και στη διασφάλιση της ασφάλειας των ψηφιακών τους τομέων.

Η δεκαετία του 1990 δεν αποτέλεσε ορόσημο στην ασφάλεια του διαδικτύου μόνο για τους ιδιώτες ή τους φορείς αλλά και τα κράτη ως οντότητες. Μεγάλος αριθμός Αμερικανικών εγγράφων συνέδεσαν την εθνική ασφάλεια με πιθανές κυβερνοεπιθέσεις σε κρίσιμες δομές, όπως αεροδρόμια, σταθμούς παραγωγής ενέργειας, τράπεζες κ.α. υποστηρίζοντας έτσι την αυξανόμενη τάση κινδύνου σε έναν ηλεκτρονικό κόσμο. Αποτελούσε συνάμα σημαντικό αλλά και ανησυχητικό το γεγονός ότι ο «αντίπαλος» δεν ήταν πλέον τόσο ευδιάκριτος όσο πριν. Κατά συνέπεια, υπήρξε η τάση για αναγνώριση και εκτιμήσεις αφενός των μέσων που θα μπορούσαν να χρησιμοποιηθούν από πιθανούς αντιπάλους και αφετέρου των εσωτερικών τρωτοτήτων.[21]

Έτσι, ένας από τους πρωταρχικούς ρόλους των εθνικών κρατών στην κυβερνοασφάλεια είναι η υπεράσπιση των εθνικών τους συμφερόντων και των κρίσιμων υποδομών τους[22]. Οι κρίσιμες υποδομές, όπως τα δίκτυα ηλεκτρικής ενέργειας, τα συστήματα ύδρευσης και τα χρηματοπιστωτικά ιδρύματα, έχουν γίνει πρωταρχικός στόχος κυβερνοεπιθέσεων λόγω του ζωτικού τους ρόλου στην κοινωνία. Οι κυβερνήσεις είναι υπεύθυνες για την προστασία αυτών των βασικών υπηρεσιών από πιθανές απειλές.

Οι εθνικές υπηρεσίες κυβερνοασφάλειας και οι αμυντικοί οργανισμοί είναι επιφορτισμένοι με την ανάπτυξη και την εφαρμογή στρατηγικών για την προστασία των κρίσιμων υποδομών από απειλές στον κυβερνοχώρο. Οι στρατηγικές αυτές περιλαμβάνουν την ανίχνευση απειλών, την αντιμετώπιση περιστατικών και τον σχεδιασμό ανθεκτικότητας, ώστε να διασφαλίζεται ότι ακόμη και σε περίπτωση επίθεσης τα συστήματα μπορούν να ανακάμψουν γρήγορα. Επιπλέον, οι κυβερνήσεις συνεργάζονται με τον ιδιωτικό τομέα, καθώς πολλά στοιχεία κρίσιμων υποδομών

[21] Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, 27(5), Σελ. 781-799.

[22] CISA. (2022). Critical Infrastructure Sectors. Διαθέσιμο στο https://www.cisa.gov/critical-infrastructure-sectors

ανήκουν σε ιδιώτες, για τη θέσπιση προτύπων και βέλτιστων πρακτικών κυβερνοασφάλειας.[23]

Τα εθνικά κράτη διαθέτουν υπηρεσίες πληροφοριών που διαδραματίζουν κρίσιμο ρόλο στην ασφάλεια στον κυβερνοχώρο. Αυτές οι υπηρεσίες είναι υπεύθυνες για τη συλλογή πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο και την απόδοση κυβερνοεπιθέσεων σε συγκεκριμένους φορείς ή χώρες. Η απόδοση είναι μια πολύπλοκη διαδικασία που περιλαμβάνει την ανάλυση τεχνικών δεικτών, τακτικών, τεχνικών και διαδικασιών (TTPs), και μερικές φορές ακόμη και ανθρώπινων πληροφοριών για τον εντοπισμό της πηγής μιας κυβερνοεπίθεσης. [24]

Η εύρεση της πηγής της επίθεσης είναι ζωτικής σημασίας για την απόδοση ευθυνών στις υπεύθυνες οντότητες για τις ενέργειές τους στον κυβερνοχώρο. Επιτρέπει στις κυβερνήσεις να λαμβάνουν διπλωματικά, οικονομικά ή νομικά μέτρα ως απάντηση σε κυβερνοεπιθέσεις. Ωστόσο, η απόδοση αποτελεί συχνά πρόκληση λόγω της ανωνυμίας και των τεχνικών απόκρυψης που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου και οι κρατικά υποστηριζόμενοι φορείς. [25]

Οι κυβερνήσεις διαδραματίζουν κρίσιμο ρόλο στην ανάπτυξη και εφαρμογή πολιτικών και νομοθεσίας για την ασφάλεια στον κυβερνοχώρο[26]. Οι πολιτικές αυτές περιλαμβάνουν ένα ευρύ φάσμα θεμάτων, όπως η προστασία δεδομένων, η προστασία της ιδιωτικής ζωής, η αναφορά περιστατικών και η διεθνής συνεργασία σε θέματα κυβερνοασφάλειας. Νομοθεσία όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR) και ο νόμος των Ηνωμένων Πολιτειών για την ανταλλαγή πληροφοριών σχετικά με την κυβερνοασφάλεια (CISA) αποσκοπούν στην προστασία των δεδομένων των πολιτών και στην προώθηση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα για την αντιμετώπιση των απειλών στον κυβερνοχώρο.

Επιπλέον, οι κυβερνήσεις θεσπίζουν εθνικές στρατηγικές κυβερνοασφάλειας που περιγράφουν την προσέγγισή τους για την προστασία του κυβερνοχώρου, την ενίσχυση της ανθεκτικότητας και την αντιμετώπιση περιστατικών στον κυβερνοχώρο. Αυτές οι

---

[23] Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy, 41(1)*, Σελ. 33-54.
[24] Georgieva, I. (2020). Όπ.π.
[25] Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), Σελ. 15-32.
[26] EU General Data Protection Regulation (GDPR) (2018). Όπ.π.

στρατηγικές συχνά περιλαμβάνουν συνεργασία με διάφορους ενδιαφερόμενους φορείς, συμπεριλαμβανομένου του ιδιωτικού τομέα, του ακαδημαϊκού χώρου και της κοινωνίας των πολιτών.

Οι απειλές στον κυβερνοχώρο δεν περιορίζονται στα εθνικά σύνορα, καθιστώντας τη διεθνή συνεργασία θεμελιώδη πτυχή της ασφάλειας στον κυβερνοχώρο[27]. Τα εθνικά κράτη συμμετέχουν σε διπλωματικές προσπάθειες για τη θέσπιση κανόνων συμπεριφοράς στον κυβερνοχώρο και τη δημιουργία συμμαχιών για την αμοιβαία άμυνα κατά των απειλών στον κυβερνοχώρο. Διπλωματικές πρωτοβουλίες, όπως η Ομάδα Κυβερνητικών Εμπειρογνωμόνων των Ηνωμένων Εθνών (UN GGE) για τις εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας, επιδιώκουν να προωθήσουν την υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο.[28]

Οι διμερείς και πολυμερείς συμφωνίες για την ασφάλεια στον κυβερνοχώρο είναι επίσης απαραίτητες. Οι συμφωνίες αυτές διευκολύνουν την ανταλλαγή πληροφοριών, τον συντονισμό της αντιμετώπισης περιστατικών και τη συνεργασία στην ανταλλαγή πληροφοριών για απειλές στον κυβερνοχώρο. Οι συμμαχίες για την κυβερνοασφάλεια, όπως το Συνεργατικό Κέντρο Αριστείας για την Κυβερνοάμυνα (CCDCOE) του Οργανισμού Βορειοατλαντικού Συμφώνου (NATO), αποτελούν παράδειγμα διεθνούς συνεργασίας για την ενίσχυση της κυβερνοάμυνας.[29]

Ενώ η έμφαση δίνεται συχνά στα αμυντικά μέτρα, τα εθνικά κράτη συμμετέχουν επίσης σε επιθετικές επιχειρήσεις στον κυβερνοχώρο ως μέρος της στρατηγικής τους για την ασφάλεια στον κυβερνοχώρο. Οι επιθετικές δυνατότητες στον κυβερνοχώρο μπορούν να χρησιμοποιηθούν για να αποτρέψουν τους αντιπάλους, να διαταράξουν τα δίκτυα κυβερνοεγκληματιών ή να ανταποδώσουν επιθέσεις που χρηματοδοτούνται από το κράτος. Οι επιθετικές επιχειρήσεις μπορεί να περιλαμβάνουν δραστηριότητες όπως η εκμετάλλευση δικτύων, η συλλογή πληροφοριών ή ακόμη και η εξαπόλυση κυβερνοεπιθέσεων για τη διατάραξη της υποδομής ενός αντιπάλου.[30]

---

[27] United Nations. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Διαθέσιμο στο https://undocs.org/A/70/174

[28] Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European union and nato global cybersecurity challenges. *Prism*, *6*(2), Σελ. 126-141.

[29] Όπ.π.

[30] Libicki, M. C. (2009). Όπ.π.. Σελ. 23-39

Η χρήση επιθετικών δυνατοτήτων στον κυβερνοχώρο εγείρει ηθικά και νομικά ζητήματα και υπογραμμίζει τη σημασία σαφών κανόνων εμπλοκής και διεθνών κανόνων στον κυβερνοχώρο. Η εξεύρεση της σωστής ισορροπίας μεταξύ αμυντικών και επιθετικών επιχειρήσεων αποτελεί μια σύνθετη πρόκληση για τα εθνικά κράτη.

Οι κυβερνήσεις είναι υπεύθυνες για την οικοδόμηση εθνικών ικανοτήτων κυβερνοασφάλειας και την προώθηση μιας κουλτούρας ευαισθητοποίησης σε θέματα κυβερνοασφάλειας. Αυτό περιλαμβάνει την επένδυση σε προγράμματα εκπαίδευσης και κατάρτισης για την ανάπτυξη ενός εξειδικευμένου εργατικού δυναμικού ικανού να αντιμετωπίσει τις απειλές στον κυβερνοχώρο. Επιπλέον, οι κυβερνήσεις συχνά χρηματοδοτούν πρωτοβουλίες έρευνας και ανάπτυξης με στόχο την προώθηση τεχνολογιών και λύσεων κυβερνοασφάλειας συμβάλλουν στη συνολική ανθεκτικότητα του ψηφιακού οικοσυστήματος ενός έθνους.[31]

Σε περίπτωση περιστατικού στον κυβερνοχώρο, τα εθνικά κράτη πρέπει να διαθέτουν αποτελεσματικούς μηχανισμούς διαχείρισης κρίσεων και αντιμετώπισης. Αυτό περιλαμβάνει καλά καθορισμένα σχέδια αντιμετώπισης συμβάντων, συντονισμό μεταξύ των σχετικών υπηρεσιών και στρατηγικές επικοινωνίας για την έγκαιρη ενημέρωση των θιγόμενων μερών.[32]

Τα περιστατικά στον κυβερνοχώρο μπορεί να ποικίλλουν σε κλίμακα και επιπτώσεις, από παραβιάσεις δεδομένων μικρής κλίμακας έως κυβερνοεπιθέσεις μεγάλης κλίμακας με επιπτώσεις στην εθνική ασφάλεια. Οι κυβερνήσεις πρέπει να είναι προετοιμασμένες να ανταποκριθούν σε ένα ευρύ φάσμα σεναρίων και να προσαρμόσουν ανάλογα τις στρατηγικές τους. Ωστόσο, μετά τις αποκαλύψεις του Edward Snowden για την Αμερικανική υπηρεσία NSA (National Security Agency), έγινε γνωστό αυτό που πολλοί ερευνητές εδώ και χρόνια υποπτεύονταν: ότι οι μεγαλύτεροι παράγοντες στη «στρατηγική» χρήση του κυβερνοχώρου είναι οι Υπηρεσίες Πληροφοριών των κρατών. Εστιάζοντας εδώ και χρόνια σε πιθανά ή απίθανα καταστροφικά σενάρια κατάφεραν να διαμορφώσουν συμπεριφορές στο διαδίκτυο που έχουν γίνει αποδεκτές τις τελευταίες δεκαετίες. Οι Υπηρεσίες Πληροφοριών εκμεταλλεύονται κενά ασφαλείας σε λειτουργικά συστήματα ώστε να εκμεταλλευτούν στρατηγικές τοποθεσίες της υποδομής

[31] National Initiative for Cybersecurity Careers and Studies (NICCS), (2023). *Cybersecurity Education and Training*. Διαθέσιμο στο https://niccs.cisa.gov/education-training

[32] NIST Special Publication 800-61 (2022), *Revision 2: Computer Security Incident Handling Guide*. National Institute of Standards and Technology. Διαθέσιμο στο https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

του διαδικτύου για τους δικούς τους σκοπούς. Αυτές οι «πίσω πόρτες» (backdoors) μπορούν να χρησιμοποιηθούν για πληθώρα σκοπών, όπως παρακολούθηση, κατασκοπεία κ.λπ. ενώ παραμένουν κρυφά κατά τη διάρκεια της χρήσης τους από το θύμα. Ωστόσο, το παράδοξο είναι ότι τα κενά αυτά μειώνουν την ασφάλεια όλου του δικτύου καθώς δεν μπορεί να εγγυηθεί κανείς ότι δεν θα γίνουν αντιληπτά και δεν θα χρησιμοποιηθούν από τρίτους όπως άλλες υπηρεσίες ή εγκληματίες. Έτσι, οι κρατικοί φορείς είναι άμεσα υπεύθυνοι για την ανασφάλεια του διαδικτύου που «προσπαθούν» να ασφαλίσουν.[33]

Συμπερασματικά, ο ρόλος των εθνικών κρατών στην κυβερνοασφάλεια είναι πολύπλευρος και εκτείνεται σε διάφορους τομείς, όπως η άμυνα, οι πληροφορίες, η ανάπτυξη πολιτικής, η διπλωματία, οι επιθετικές επιχειρήσεις, η ανάπτυξη ικανοτήτων και η διαχείριση κρίσεων. Καθώς το ψηφιακό τοπίο συνεχίζει να εξελίσσεται και οι απειλές στον κυβερνοχώρο επιμένουν, ο ρόλος των εθνικών κρατών στην εξασφάλιση του κυβερνοχώρου παραμένει κρίσιμος για τη διαφύλαξη των εθνικών συμφερόντων και της παγκόσμιας σταθερότητας. Η διεθνής συνεργασία και η συνεργασία μεταξύ των κρατών είναι ζωτικής σημασίας για την αντιμετώπιση των πολύπλοκων και διαρκώς εξελισσόμενων προκλήσεων του κυβερνοχώρου.

[33] Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations. *Oxford University Press*.

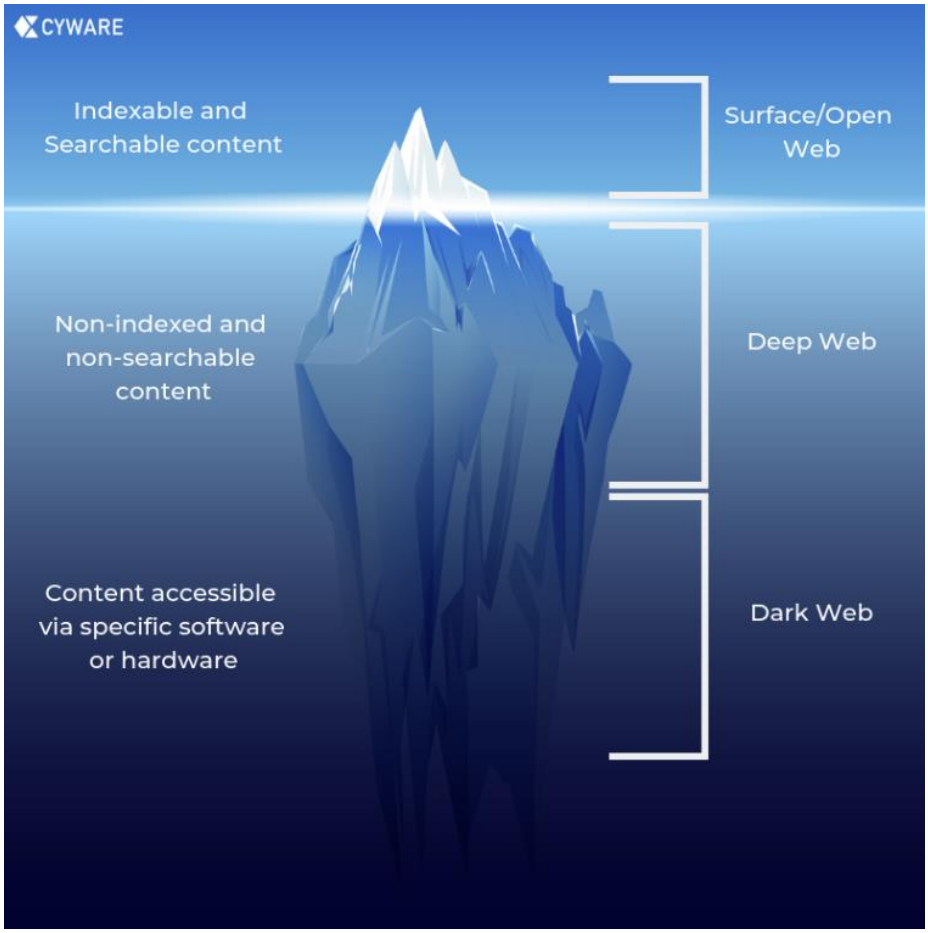
2. Ανάλυση των απειλών του Deep και Dark Web

2.1. Οργανωμένο έγκλημα

Το οργανωμένο έγκλημα έχει εξελιχθεί σημαντικά στην ψηφιακή εποχή, με τους εγκληματίες του κυβερνοχώρου να χρησιμοποιούν τον επιφανειακό, τον βαθύ και τον σκοτεινό ιστό για να διεξάγουν παράνομες δραστηριότητες. Αυτή η μεταμόρφωση αποτελεί μια σύνθετη και πολύπλευρη πρόκληση για τις υπηρεσίες επιβολής του νόμου και τους εμπειρογνώμονες ασφαλείας παγκοσμίως. Σε αυτό το σημείο της έρευνας, εμβαθύνουμε στον κόσμο του οργανωμένου εγκλήματος στο πλαίσιο του επιφανειακού, του βαθύ και του σκοτεινού ιστού, εξετάζοντας τη δυναμική του, τις μεθόδους του και τον ρόλο των δικτύων κυβερνοεγκληματιών στο σημερινό διασυνδεδεμένο ψηφιακό τοπίο.

Η τεράστια ανάπτυξη του διαδικτύου τις τελευταίες δεκαετίες οδήγησε σε μια άνευ όρων διεύρυνση του σε κάθε γωνιά της γης αλλά και σε σκοτεινές γωνιές εντός του δικτύου. Έτσι κατά μεγάλο μέρος της βιβλιογραφίας αλλά και ως, πλέον, δεδομένη γνώση, το διαδίκτυο και ο ιστός (web) δεν αποτελούν ένα ενιαίο μέρος ή κυβερνοχώρο αλλά χωρίζονται σε τρία τμήματα. Το γνωστό διαδίκτυο ή επιφανειακό διαδίκτυο (surface web), το βαθύ διαδίκτυο (deep web) και το σκοτεινό διαδίκτυο (dark web). Συχνά εμφανίζεται σε αναλογία με παγόβουνο εντός της θάλασσας (Βλ. Εικόνα 1). Το εμφανές μέρος του παγόβουνου αποτελεί το επιφανειακό διαδίκτυο, το κομμάτι που βρίσκεται κάτω από τη θάλασσα και είναι δύσκολο να παρατηρηθεί είναι το βαθύ διαδίκτυο ενώ το κομμάτι που αποτελεί το ναδίρ του παγόβουνου εντός της θάλασσας, σε βάθος όπου το φως δεν φτάνει για να το κάνει εμφανές, υπάρχει το σκοτεινό διαδίκτυο.[34]

[34] Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), Σελ. 26-27.



Εικόνα 1: Η αναλογία παγόβουνου – διαδικτύου.

Πηγή: Cyber Threat Intelligence (2019), How is Surface Web Intelligence different from Dark Web Intelligence?, CyWare διαθέσιμο στο https://cyware.com/security-guides/cyber-threat-intelligence/how-is-surface-web-intelligence-different-from-dark-web-intelligence-393c

Το διαδίκτυο αποτελεί ένα μέσο πρόσβασης σε ένα αμάλγαμα από δεδομένα. Άλλες φορές αυτά είναι εύκολα προσβάσιμα και άλλες απαιτούν συγκεκριμένα εξειδικευμένα εργαλεία για να προσπελαθούν. Ξεκινώντας από το επιφανειακό διαδίκτυο, γίνεται αντιληπτό ότι είναι εύκολα προσβάσιμο με τη χρήση μιας από τις πολλές μηχανές αναζήτησης (Google, Bing κ.λπ) και αποτελεί το κομμάτι που ο μέσος άνθρωπος χρησιμοποιεί και απολαμβάνει. Εντός αυτού βρίσκονται καθημερινές ιστοσελίδες και πληροφορίες που δεν απαιτούν καμιά περαιτέρω ερευνητική ή εξιδεικευμένη γνώση. Υπολογίζεται ότι μόλις το 4-6% του διαδικτύου ανήκει σε αυτό

το τμήμα.[35] Τα παραδοσιακά εγκλήματα στον κυβερνοχώρο, όπως το phishing, η κλοπή ταυτότητας και η απάτη με πιστωτικές κάρτες, συμβαίνουν κυρίως σε αυτό το ορατό στρώμα του ιστού. Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται ευπάθειες σε ιστότοπους, δίκτυα και λογισμικό για να κλέψουν προσωπικές και οικονομικές πληροφορίες από ανυποψίαστα θύματα.

Οι διαδικτυακές αγορές στον επιφανειακό ιστό διευκολύνουν την πώληση κλεμμένων δεδομένων, εργαλείων hacking και κακόβουλου λογισμικού. Αυτές οι αγορές λειτουργούν παρόμοια με τις νόμιμες πλατφόρμες ηλεκτρονικού εμπορίου, με τους εγκληματίες του κυβερνοχώρου να προσφέρουν προϊόντα και υπηρεσίες για παράνομους σκοπούς. Ο επιφανειακός ιστός φιλοξενεί επίσης, σε ορισμένες περιπτώσεις, fora και δωμάτια συνομιλίας όπου οι εγκληματίες του κυβερνοχώρου ανταλλάσσουν γνώσεις, συνεργάζονται σε επιθέσεις και μοιράζονται πληροφορίες σχετικά με ευάλωτους στόχους – αν και στο μεγαλύτερο μέρος τους εντοπίζονται σε βαθύτερα στρώματα του ιστού.[36]

Ο βαθύς ιστός (υπολογίζεται ότι αποτελεί πάνω από 90% του διαδικτύου), περιλαμβάνει ιστοσελίδες και δεδομένα που δεν ευρετηριάζονται από τις παραδοσιακές μηχανές αναζήτησης, παρέχει ένα κρυφό στρώμα για τις δραστηριότητες του οργανωμένου εγκλήματος. Αν και δεν είναι εγγενώς παράνομος, ο βαθύς ιστός μεταξύ άλλων φιλοξενεί πλατφόρμες, υπηρεσίες που επιτρέπουν την ανωνυμία και την εμπιστευτικότητα, καθιστώντας το ελκυστικό περιβάλλον για τους εγκληματίες του κυβερνοχώρου. Αυτό περιλαμβάνει κρυπτογραφημένες υπηρεσίες ηλεκτρονικού ταχυδρομείου, ιδιωτικά fora, διαθέσιμες βάσεις δεδομένων, επιστημονικά άρθρα και ομότιμα δίκτυα. [37]

Το AlphaBay ήταν μια εξέχουσα αγορά σκοτεινού ιστού, γνωστή για τη διευκόλυνση της πώλησης διαφόρων παράνομων αγαθών και υπηρεσιών, συμπεριλαμβανομένων ναρκωτικών, κλεμμένων δεδομένων, πλαστών εγγράφων και εργαλείων hacking. Όπως και το Silk Road[38], το AlphaBay λειτουργούσε στο Dark Web, προσφέροντας μια πλατφόρμα για τους εγκληματίες του κυβερνοχώρου να πραγματοποιούν παράνομες συναλλαγές ανώνυμα. Απέκτησε σημαντική φήμη πριν καταστραφεί από τις αρχές

[35] Ό.π.
[36] Greenberg A. (2014), Όπ.π.
[37] Όπ.π.
[38] Chertoff, M., & Simon, T. (2015). Όπ.π. Σελ. 3

επιβολής του νόμου το 2017.[39] Η κατάρριψη του AlphaBay ανέδειξε τις προκλήσεις που αντιμετωπίζουν οι υπηρεσίες επιβολής του νόμου στην καταπολέμηση των εγκληματικών δραστηριοτήτων στο Dark Web δεδομένου του ότι τόσο το Silk Road όσο και το Alphabay είχαν έσοδα εκατομμυρίων ευρώ ημερησίως και επέστρεψαν σε λειτουργία ένα μήνα και τέσσερα χρόνια μετά αντίστοιχα.[40]

Η περίπτωση του AlphaBay χρησιμεύει ως άλλη μια εικόνα του τρόπου με τον οποίο ο σκοτεινός ιστός παρέχει ένα καταφύγιο για το οργανωμένο έγκλημα, επιτρέποντας την ανταλλαγή παράνομων αγαθών και υπηρεσιών πέρα από την εμβέλεια της συμβατικής επιβολής του νόμου.

Ο σκοτεινός ιστός (Dark Web) φιλοξενεί αγορές για την πώληση ναρκωτικών, πυροβόλων όπλων, πλαστών νομισμάτων και κλεμμένων προσωπικών πληροφοριών. Τα κρυπτονομίσματα όπως το Bitcoin είναι το προτιμώμενο μέσο πληρωμής, εξασφαλίζοντας ένα επίπεδο ανωνυμίας που τα παραδοσιακά χρηματοπιστωτικά συστήματα δεν μπορούν να παρέχουν[41]. Οι εγκληματικές επιχειρήσεις στον σκοτεινό ιστό χρησιμοποιούν προηγμένη κρυπτογράφηση και μέτρα ασφαλείας για την προστασία των δραστηριοτήτων και των ταυτοτήτων τους, καθιστώντας εξαιρετικά δύσκολο για τις διωκτικές αρχές να εντοπίσουν και να συλλάβουν τους εγκληματίες του κυβερνοχώρου. Κατά τους ερευνητές αποτελεί μόλις το 2-4% του διαδικτύου ενώ για τη πρόσβαση σε αυτό απαιτείται κατά κύριο λόγο εξειδικευμένο λογισμικό που εστιάζει στην ανωνυμία. Το μεγαλύτερο ποσοστό των χρηστών χρησιμοποιεί το Tor Project (συντομογραφία για The Onion Router) το οποίο αποτελεί ένα δωρεάν λογισμικό που προσφέρει ανωνυμία μέσα από στρώματα κρυπτογράφησης.[42]

Το οργανωμένο έγκλημα στον σκοτεινό ιστό δεν περιορίζεται σε μεμονωμένους δράστες- περιλαμβάνει περίπλοκα δίκτυα και συνεργασίες. Αυτά τα δίκτυα μπορεί να είναι εξαιρετικά εξελιγμένα, με ειδικούς στην πειρατεία, το ξέπλυμα χρήματος και τη διανομή. Για παράδειγμα, στις επιθέσεις ransomware συχνά εμπλέκονται πολλαπλοί

---

[39] Cimpanu, C. (2017). AlphaBay Dark Web Market Taken Down After Law Enforcement Raids. *Bleeping Computer*. Διαθέσιμο στο https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/

[40] Greenberg A. (2022), AlphaBay is taking over the dark web-again, *Wired* διαθέσιμο στο https://www.wired.com/story/alphabay-dark-web-market-ranking/

[41] Finklea, C. (2015). Dark Web. *Congressional Research Service*. Διαθέσιμο στο https://fas.org/sgp/crs/misc/R44101.pdf

[42] Chertoff, M. (2017), ό.π. Σελ. 27-28

φορείς, από τους αρχικούς hackers μέχρι τους υπεύθυνους για το ξέπλυμα των πληρωμών λύτρων.

Τα δίκτυα εγκληματιών στον κυβερνοχώρο επεκτείνονται πέρα από τα σύνορα, λειτουργώντας ως διακρατικές επιχειρήσεις. Αξιοποιούν την ανωνυμία του σκοτεινού ιστού για να διεξάγουν εγκληματικές δραστηριότητες σε όλο τον κόσμο, καθιστώντας δύσκολη την αποτελεσματική καταπολέμησή τους από οποιαδήποτε μεμονωμένη δικαιοδοσία. Τα δίκτυα αυτά προσαρμόζονται επίσης στις προσπάθειες επιβολής του νόμου, εξελίσσοντας συνεχώς τις τακτικές, τις τεχνικές και τις διαδικασίες τους για να αποφεύγουν τη σύλληψη.[43]

Η καταπολέμηση του οργανωμένου εγκλήματος στο ψηφιακό πεδίο παρουσιάζει πολλές προκλήσεις για τις υπηρεσίες επιβολής του νόμου. Η εγγενής ανωνυμία και ο παγκόσμιος χαρακτήρας των εγκληματικών δραστηριοτήτων στον κυβερνοχώρο απαιτούν διεθνή συνεργασία και συντονισμό. Οι υπηρεσίες επιβολής του νόμου συχνά συνεργάζονται με εταιρείες κυβερνοασφάλειας και διεθνείς οργανισμούς για τον εντοπισμό και την εξάρθρωση εγκληματικών δικτύων.[44]

Οι προσπάθειες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο περιλαμβάνουν πρωτοβουλίες για τον εντοπισμό των συναλλαγών κρυπτονομισμάτων, τη βελτίωση της ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας και την ενίσχυση των διεθνών νομικών πλαισίων για τη δίωξη των εγκληματιών του κυβερνοχώρου. Ωστόσο, το παιχνίδι της γάτας με το ποντίκι μεταξύ των αρχών επιβολής του νόμου και των κυβερνοεγκληματιών συνεχίζεται, με κάθε πλευρά να προσαρμόζεται στο εξελισσόμενο τοπίο του ψηφιακού εγκλήματος.[45]

Εν κατακλείδι, το οργανωμένο έγκλημα έχει βρει πρόσφορο έδαφος στην ψηφιακή εποχή, χρησιμοποιώντας τον επιφανειακό, τον βαθύ και τον σκοτεινό ιστό για τη διεξαγωγή παράνομων δραστηριοτήτων. Ο βαθύς και ο σκοτεινός ιστός παρέχουν τον μανδύα της ανωνυμίας που επιδιώκουν οι εγκληματίες του κυβερνοχώρου, καθιστώντας δύσκολη τη διακοπή αυτών των επιχειρήσεων από την επιβολή του νόμου. Τα δίκτυα εγκληματιών στον κυβερνοχώρο λειτουργούν ως πολύπλοκα οικοσυστήματα, που

[43] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). Crime in cyberspace: offenders and the role of organized crime groups, *SSRN 2211842*. Σελ. 19-25

[44] Joint Report (2019), Common challenges in combating cybercrime, as identified by Eurojust and Europol, *Europol and Eurojust Public Information* Σελ. 17-21

[45] STL Digital, (2023). The Cat and Mouse Game: A look into Cybersecurity vs Cybercrime, *STL Digital*, διαθέσιμο στο https://www.stldigital.tech/blog/the-cat-and-mouse-game-a-look-into-cybersecurity-vs-cybercrime/

επιδίδονται σε μια σειρά παράνομων δραστηριοτήτων και συνεργάζονται διασυνοριακά. Ενώ οι υπηρεσίες επιβολής του νόμου παγκοσμίως εργάζονται επιμελώς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η διαρκώς εξελισσόμενη φύση του οργανωμένου εγκλήματος στον ψηφιακό χώρο διασφαλίζει ότι η πρόκληση αυτή παραμένει στην πρώτη γραμμή των προσπαθειών για τη διατήρηση ενός ασφαλούς και αξιόπιστου ψηφιακού περιβάλλοντος.

2.2. Εξτρεμισμός και τρομοκρατία στον κυβερνοχώρο

Τα τελευταία χρόνια, το διαδίκτυο και ο κυβερνοχώρος έχουν γίνει πρόσφορο έδαφος για εξτρεμιστικές ιδεολογίες και τρομοκρατικές δραστηριότητες. Το ψηφιακό πεδίο προσφέρει μια πλατφόρμα για τη διάδοση ριζοσπαστικού περιεχομένου, τη στρατολόγηση, το συντονισμό και το σχεδιασμό τρομοκρατικών ενεργειών.[46] Το παρόν κομμάτι της εργασίας, διερευνά την ανησυχητική άνοδο του εξτρεμισμού και της τρομοκρατίας στον κυβερνοχώρο, ρίχνοντας φως στις διάφορες διαστάσεις αυτής της εξελισσόμενης απειλής. Βασιζόμενο σε ένα ευρύ φάσμα επιστημονικών αναφορών, εμβαθύνει στις μεθόδους που χρησιμοποιούν οι εξτρεμιστικές ομάδες, στο ρόλο του διαδικτύου στη ριζοσπαστικοποίηση και στις προκλήσεις που αντιμετωπίζουν οι κυβερνήσεις και οι υπηρεσίες επιβολής του νόμου για την καταπολέμηση αυτής της απειλής.

Εξτρεμιστικές ομάδες και άτομα έχουν εκμεταλλευτεί τις ευκαιρίες που προσφέρει το διαδίκτυο για να διαδώσουν τις ιδεολογίες τους σε ένα παγκόσμιο ακροατήριο.[47] Η ευκολία δημιουργίας και ανταλλαγής περιεχομένου έχει επιτρέψει σε εξτρεμιστικές οργανώσεις να δημοσιεύουν προπαγάνδα, να διανέμουν εγχειρίδια εκπαίδευσης και να εξυμνούν τρομοκρατικές πράξεις. Αυτές οι διαδικτυακές πλατφόρμες χρησιμεύουν ως εικονικά κέντρα στρατολόγησης, παρέχοντας μια αίσθηση του ανήκειν σε ευάλωτα άτομα που είναι επιρρεπή στη ριζοσπαστικοποίηση.[48]

Το εξτρεμιστικό περιεχόμενο λαμβάνει διάφορες μορφές, από γραπτές διακηρύξεις και γραφικές εικόνες μέχρι βίντεο και αναρτήσεις στα μέσα κοινωνικής δικτύωσης. Οι

[46] Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, 39(3), 195-206.
[47] Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *NCJL & Tech*., 4, 1.
[48] Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. Asian journal of criminology, 3, Σελ. 37-59.

διαδικτυακές πλατφόρμες, συμπεριλαμβανομένων των κυρίαρχων κοινωνικών δικτύων, των fora συνομιλίας και των κρυπτογραφημένων εφαρμογών ανταλλαγής μηνυμάτων, χρησιμεύουν ως αγωγοί για τη διάδοση της εξτρεμιστικής προπαγάνδας. Ενώ κάποιο περιεχόμενο είναι φανερό και εύκολα αναγνωρίσιμο, πιο διακριτικές μορφές ριζοσπαστικοποίησης συμβαίνουν μέσω διαδικτυακών θαλάμων απήχησης, όπου ομοϊδεάτες ενισχύουν ο ένας τις πεποιθήσεις του άλλου και οδηγούν στη ριζοσπαστικοποίηση.[49]

Οι πλατφόρμες κοινωνικής δικτύωσης έχουν διαδραματίσει καθοριστικό ρόλο στη διευκόλυνση της ταχείας διάδοσης εξτρεμιστικού περιεχομένου. Αυτές οι πλατφόρμες επιτρέπουν στις εξτρεμιστικές ομάδες να προσεγγίσουν ένα τεράστιο ακροατήριο, παρέχοντας παράλληλα εργαλεία δέσμευσης, όπως σχόλια, συμπάθειες και κοινοποιήσεις. Σε απάντηση στον αυξημένο έλεγχο, ορισμένες εταιρείες μέσων κοινωνικής δικτύωσης έχουν λάβει μέτρα για την αφαίρεση εξτρεμιστικού περιεχομένου και λογαριασμών. Ωστόσο, η επίμονη φύση του διαδικτύου καθιστά δύσκολη την πλήρη εξάλειψη τέτοιου υλικού.[50]

Οι τεχνολογίες κρυπτογράφησης, ιδίως η κρυπτογράφηση από άκρο σε άκρο, αποτελούν μια άλλη πρόκληση. Ενώ η κρυπτογράφηση ενισχύει την ασφάλεια και την ιδιωτικότητα των επικοινωνιών, παρέχει επίσης κάλυψη στους εξτρεμιστές για να επικοινωνούν χωρίς το φόβο της υποκλοπής.[51] Οι υπηρεσίες επιβολής του νόμου αντιμετωπίζουν το δίλημμα της εξισορρόπησης των ατομικών δικαιωμάτων προστασίας της ιδιωτικής ζωής με την ανάγκη εντοπισμού και αποδιοργάνωσης τρομοκρατικών δικτύων που δρουν στον κυβερνοχώρο.[52]

Η ριζοσπαστικοποίηση στον κυβερνοχώρο έχει γίνει ένα ανησυχητικό φαινόμενο, με άτομα να ριζοσπαστικοποιούνται αποκλειστικά μέσω της διαδικτυακής έκθεσης σε εξτρεμιστικό περιεχόμενο. Η διαδικασία συχνά ξεκινά με άτομα που καταναλώνουν προπαγάνδα και σταδιακά εξελίσσονται σε ενεργούς υποστηρικτές ή, σε ορισμένες περιπτώσεις, σε δράστες βίας. Το διαδίκτυο παρέχει μια αίσθηση ανωνυμίας που

[49] Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyberspace and the national security of the United Kingdom. Threats and Responses. *Chatham House, London*, 1(1), Σελ. 1-46.
[50] Turner, D. (2008). Symantec Global Internet Security Threat Report Trends for July–December 07, *Volume XII*
[51] US Senate Committee on Homeland Security and Governmental Affairs (2008), *Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat*
[52] Chertoff, M. (2017), ό.π. Σελ. 27-28

ενθαρρύνει τα άτομα να εξερευνήσουν εξτρεμιστικές ιδεολογίες χωρίς τον κίνδυνο άμεσης έκθεσης.[53]

Οι διαδικτυακές προσπάθειες στρατολόγησης δεν περιορίζονται σε μια συγκεκριμένη γεωγραφική περιοχή. Οι εξτρεμιστικές οργανώσεις χρησιμοποιούν το διαδίκτυο για να προσεγγίσουν πιθανούς συμπαθούντες σε παγκόσμιο επίπεδο. Οι στρατολόγοι μπορεί να εκμεταλλεύονται γεγονότα ή κρίσεις του πραγματικού κόσμου για να ενισχύσουν τις αφηγήσεις τους και να προσελκύσουν ευάλωτα άτομα στις τάξεις τους.[54]

Αποτελεί γεγονός ότι το Ισλαμικό Χαλιφάτο (ISIS/ISIL) αξιοποιεί το Dark Web για στρατολόγηση. Με ανακοίνωση του το 2015, το FBI δήλωνε ότι το ISIS χρησιμοποιούσε το Dark Web και νέες τεχνολογίες επικοινωνίας και κρυπτογράφησης για να επιτύχει διεθνή τρομοκρατικά χτυπήματα και ότι οι δυνατότητες του τότε FBI δεν αρκούσαν για να καταφέρουν να αναχαιτίσουν ή έστω να αποκρυπτογραφήσουν την ανωτέρω επικοινωνία. Αργότερα το ίδιο έτος, Τζιχαντιστές δημοσίευσαν ένα ηλεκτρονικό βιβλίο με τίτλο «Πως να επιβιώσεις στη Δύση: Ένας τζιχαντιστικός οδηγός» (How to survive in the West: A jihadist guide). Μεταξύ των κεφαλαίων ήταν «Κρύβοντας την τζιχαντιστική ιδιότητα», «πως να φτιάξεις βόμβες», «Πως να μεταφέρεις οπλισμό», «Τι να κάνεις εάν σε παρακολουθούν» κ.α. ενώ συζητά και το πως ο χρήστης μπορεί να αξιοποιήσει το Tor για να βρει τζιχαντιστικό υλικό στο σκοτεινό διαδίκτυο.[55]

Οι κυβερνήσεις παγκοσμίως αντιμετωπίζουν τις προκλήσεις που θέτει ο εξτρεμισμός και η τρομοκρατία στον κυβερνοχώρο. Οι στρατηγικές κυμαίνονται από εκστρατείες αντι-μηνυμάτων που αποσκοπούν στην απομυθοποίηση εξτρεμιστικών αφηγήσεων έως νομοθετικά μέτρα που στοχεύουν στη διαδικτυακή ρητορική μίσους και την υποκίνηση σε βία. Η διεθνής συνεργασία έχει επίσης καταστεί απαραίτητη, δεδομένης της διασυνοριακής φύσης του διαδικτύου και της παγκόσμιας εμβέλειας του εξτρεμιστικού περιεχομένου.[56]

Ωστόσο, οι προσπάθειες για την καταπολέμηση του διαδικτυακού εξτρεμισμού απαιτείται να βρίσκουν μια λεπτή ισορροπία μεταξύ της ασφάλειας και της ελευθερίας του λόγου. Η απομάκρυνση εξτρεμιστικού περιεχομένου εγείρει ανησυχίες σχετικά με

---

[53] Kimmage, D. (2010). *Al-Qaeda central and the internet*. Washington DC: New America Foundation. Σελ. 2-17

[54] Europol, T. E. S. A. T. (2010). *EU terrorism situation and trend report*. European Police Office.

[55] Weimann, G. (2016). Ό.π. Σελ. 197-199

[56] Dilipraj, E. (2014). Terror in the Deep and Dark Web. *Air Power Journal*, 9(3), Σελ. 121-140.

τη λογοκρισία και το ενδεχόμενο κατάχρησης από τις κυβερνήσεις για τη φίμωση των αντίθετων φωνών. Η εξεύρεση της σωστής ισορροπίας είναι ένα πολύπλοκο έργο που απαιτεί συνεχή βελτίωση των πολιτικών και των πρακτικών.[57]

Το τοπίο των απειλών στον κυβερνοχώρο είναι δυναμικό, με τις εξτρεμιστικές ομάδες να προσαρμόζονται στα αντίμετρα. Ορισμένες έχουν στραφεί σε κρυπτογραφημένες πλατφόρμες ανταλλαγής μηνυμάτων και στον σκοτεινό ιστό για να διατηρήσουν την επιχειρησιακή τους ασφάλεια. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, το ίδιο συμβαίνει και με τις τακτικές των εξτρεμιστικών οργανώσεων.[58]

Μια αναδυόμενη ανησυχία είναι η δυνατότητα των εξτρεμιστικών ομάδων να αξιοποιήσουν τις αναδυόμενες τεχνολογίες, όπως η τεχνητή νοημοσύνη, για αποτελεσματικότερες προσπάθειες στρατολόγησης και ριζοσπαστικοποίησης. Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για τη στόχευση ατόμων που είναι επιρρεπή στην εξτρεμιστική προπαγάνδα, προσαρμόζοντας το περιεχόμενο ώστε να εκμεταλλεύεται τα τρωτά σημεία και τις προκαταλήψεις.[59]

2.2.1. Η Περίπτωση του Reddit

Τα τελευταία χρόνια, οι διαδικτυακές πλατφόρμες (βλ. Twitter, Reddit, 4Chan κ.α.) έχουν διαδραματίσει σημαντικό ρόλο τόσο στην επικοινωνία όσο και στη διάδοση εξτρεμιστικών ιδεολογιών έως και την οργάνωση ομοϊδεατών. Το Reddit, μια δημοφιλής πλατφόρμα κοινωνικής δικτύωσης, δεν έχει μείνει ανεπηρέαστο από αυτή την τάση. Σε αυτό το κομμάτι θα διερευνηθεί η παρουσία εξτρεμιστικών κινημάτων στη περίεργη περίπτωση του Reddit, αντλώντας πληροφορίες από ακαδημαϊκές έρευνες και μελέτες που ρίχνουν φως στη δυναμική και τις επιπτώσεις αυτών των κινημάτων.

Το Reddit είναι μια τεράστια διαδικτυακή κοινότητα (forum) που αποτελείται από πολυάριθμα subreddits (μικρότερα fora), καθένα από τα οποία είναι αφιερωμένο σε συγκεκριμένα θέματα και ενδιαφέροντα. Ενώ πολλά subreddits χρησιμεύουν ως fora για υγιείς συζητήσεις και ανταλλαγή πληροφοριών, ορισμένα έχουν μετατραπεί σε εκτροφείο εξτρεμιστικών ιδεολογιών. Οι ερευνητές έχουν δείξει έντονο ενδιαφέρον για την κατανόηση των μονοπατιών και των χαρακτηριστικών που οδηγούν τον εξτρεμισμό

[57] Metz, S. (2012). Rethinking insurgency. In The Routledge handbook of insurgency and counterinsurgency. *Routledge*. Σελ. 32-44
[58] Cornish, P. (2009). *Cyber security and politically, socially and religiously motivated cyber attacks*. European Parliament Σελ. 2-37
[59] Όπ.π.

στο οικοσύστημα του Reddit, έναν κόσμο που αποτελείται από περισσότερους από 70 εκατομμύρια χρήστες ημερησίως.[60]

Έτσι, εμβάθυναν στο ζήτημα του εγχώριου εξτρεμισμού σε ανώνυμες πλατφόρμες κοινωνικής δικτύωσης, διερευνώντας δραστηριότητες κάτω από τον επιφανειακό ιστό. Η μελέτη τους ρίχνει φως στο πώς άτομα με εξτρεμιστικές απόψεις βρίσκουν ανωνυμία σε πλατφόρμες όπως το Reddit για να οργανώσουν και να διαδώσουν τις ιδεολογίες τους. Η μελέτη, επίσης, αναδεικνύει τις προκλήσεις του εντοπισμού και της αντιμετώπισης του εξτρεμισμού σε διαδικτυακούς χώρους όπου οι συμμετέχοντες συχνά κρύβονται πίσω από ψευδώνυμα. Αυτή η ανωνυμία έχει καταστήσει το Reddit μια ελκυστική πλατφόρμα για όσους επιδιώκουν να προωθήσουν εξτρεμιστικό περιεχόμενο ή να ενταχθούν σε ένα σύνολο με τα ίδια ακραία πιστεύω.[61]

Οι ερευνητές παρουσιάζουν έρευνα που εξετάζει τις ακραίες πολιτικές πεποιθήσεις και τις κοινότητες στο Reddit. Η εργασία τους υπογραμμίζει τη σημασία του Reddit στο πλαίσιο της ριζοσπαστικοποίησης και του σχηματισμού εξτρεμιστικών κοινοτήτων. Αναλύοντας τις διαδρομές μέσω των οποίων τα άτομα έλκονται προς ακραίες πολιτικές πεποιθήσεις, η μελέτη αυτή παρέχει πολύτιμες πληροφορίες για το πώς το Reddit μπορεί να χρησιμεύσει ως αγωγός για τη διαδικασία ριζοσπαστικοποίησης. Τονίζει την ανάγκη παρακολούθησης και αντιμετώπισης του εξτρεμιστικού περιεχομένου εντός της πλατφόρμας, δεδομένης της δυνητικής επιρροής του στους χρήστες.[62]

Άλλοι ερευνητές συμβάλλουν στη συζήτηση διερευνώντας το φαινόμενο της λήψης του "κόκκινου χαπιού"[63] ως μεταφορά για την υιοθέτηση εξτρεμιστικών απόψεων. Η έρευνά τους εμβαθύνει στη γλώσσα και τον λόγο που χρησιμοποιείται σε διαδικτυακές κοινότητες, συμπεριλαμβανομένου του Reddit, οι οποίες ευνοούν τον εξτρεμισμό. Η μελέτη εξετάζει τον τρόπο με τον οποίο η γλώσσα και οι αφηγήσεις μπορούν να ριζοσπαστικοποιήσουν τα άτομα και να τα οδηγήσουν σε πιο ακραίες πολιτικές πεποιθήσεις. Στο πλαίσιο του Reddit, όπου οι χρήστες μπορούν να βρουν κοινότητες

---

[60] Στατιστικά από https://www.redditinc.com/

[61] Dawson, M., Vassilakos, A., Castanon Remy, J.L. Setor, T.K. (2021) Illicit activities beneath the surface web investigating domestic extremism on anonymous social media platforms, *Holistica Journal of Business and Public Administration*, Vol.12, Iss.1, Σελ. 27-40

[62] Mann, M., Zulli, D., Foote, J., Ku, E., & Primm, E. (2023). Unsorted Significance: Examining Potential Pathways to Extreme Political Beliefs and Communities on Reddit. *Socius: Sociological Research for a Dynamic World*, 9, Σελ. 1–15.

[63] Ο όρος «Κόκκινο Χάπι» (Red pill) αναφέρεται σε μια διαδικασία με την οποία η οπτική γωνία ενός ατόμου μεταμορφώνεται δραματικά, εισάγοντάς το σε μια νέα και συνήθως διαστρεβλωμένη κατανόηση της πραγματικής φύσης μιας συγκεκριμένης κατάστασης.

ευθυγραμμισμένες με τις απόψεις τους, η έρευνα αυτή αναδεικνύει τον ρόλο των θαλάμων απήχησης στην ενίσχυση των εξτρεμιστικών ιδεολογιών.[64]

Η παρουσία εξτρεμιστικών κινημάτων στο Reddit εγείρει σημαντικές ανησυχίες τόσο για τους φορείς εκμετάλλευσης της πλατφόρμας όσο και για την κοινωνία στο σύνολό της. Παρόλο που το Reddit έχει λάβει μέτρα για την καταπολέμηση του εξτρεμιστικού περιεχομένου, η έκταση της πλατφόρμας το καθιστά δύσκολο χώρο για την αποτελεσματική αστυνόμευση. Η ανωνυμία που παρέχουν τα ψευδώνυμα και τα κρυπτογραφημένα κανάλια επικοινωνίας περιπλέκει περαιτέρω τις προσπάθειες εντοπισμού και αντιμετώπισης εξτρεμιστικών ατόμων και κοινοτήτων.

Ως απάντηση σε αυτές τις προκλήσεις, ερευνητές και οργανισμοί εργάζονται για την ανάπτυξη εργαλείων και μεθοδολογιών για την παρακολούθηση και την αντιμετώπιση του εξτρεμισμού στο Reddit και σε παρόμοιες πλατφόρμες. Ο εντοπισμός των πρώιμων προειδοποιητικών σημάτων ριζοσπαστικοποίησης, η κατανόηση της γλώσσας που χρησιμοποιείται στις εξτρεμιστικές κοινότητες και η εξεύρεση αποτελεσματικών τρόπων αντιμετώπισης αυτών των ιδεολογιών αποτελούν βασικά βήματα για την καταπολέμηση του διαδικτυακού εξτρεμισμού.[65]

Η έρευνα που παρουσιάζεται στις προαναφερθείσες μελέτες υπογραμμίζει τη σημασία της συνεχούς επαγρύπνησης και έρευνας στον τομέα αυτό. Είναι σημαντικό να παραμένουμε ενήμεροι για τη δυναμική των εξτρεμιστικών κινημάτων στο Reddit και σε άλλες διαδικτυακές πλατφόρμες όπως το 4Chan, ώστε να αναπτύξουμε στρατηγικές για την πρόληψη της ριζοσπαστικοποίησης και τον μετριασμό των επιπτώσεων του εξτρεμιστικού περιεχομένου. Καθώς το Reddit παραμένει μια εξέχουσα πλατφόρμα για συζητήσεις και κοινότητες, η αντιμετώπιση του εξτρεμισμού εντός των ψηφιακών του συνόρων αποτελεί μια συνεχή πρόκληση που απαιτεί συλλογικές προσπάθειες από ερευνητές, υπεύθυνους χάραξης πολιτικής και διαχειριστές της πλατφόρμας.[66]

---

[64] Marwick, A. E., & Furl, K. (2021). Taking The RedPill: talking about extremism. *AoIR Selected Papers of Internet Research*. Σελ. 2-5

[65] Kimmage D. (2010), Όπ.π. Σελ. 16-17

[66] Dawson, M., Vassilakos, A., Castanon Remy, J.L. Setor, T.K. (2021), Όπ.π. Σελ. 27-40

2.3. Πορνογραφία και κυβερνοχώρος: Ηθική και κρατικές παρεμβάσεις

Η έλευση του διαδικτύου μεταμόρφωσε δραματικά τον τρόπο με τον οποίο η κοινωνία καταναλώνει και παράγει περιεχόμενο. Μια από τις πιο πολυσυζητημένες και διαδεδομένες πτυχές του κυβερνοχώρου είναι η διαθεσιμότητα και η προσβασιμότητα της πορνογραφίας. Το ψηφιακό πεδίο έχει δημιουργήσει έναν μοναδικό χώρο για τη διάδοση και την κατανάλωση ρητού περιεχομένου, προκαλώντας τους παραδοσιακούς κανόνες, την ηθική και τους κανονισμούς.[67]

Το διαδίκτυο έχει καταστήσει την πορνογραφία πιο προσιτή από ποτέ, παρουσιάζοντας ένα σύνθετο τοπίο όπου η κρατική ευθύνη μπαίνει στο παιχνίδι. Λίγα πλήκτρα μπορούν να οδηγήσουν τον καθένα σε μια εκτεταμένη σειρά από υλικό, που κυμαίνεται από ερασιτεχνικό περιεχόμενο έως επαγγελματικές παραγωγές. Αυτή η άνευ προηγουμένου διαθεσιμότητα εγείρει σημαντικά ερωτήματα σχετικά με τις επιπτώσεις αυτής της εύκολης πρόσβασης και το ρόλο των κυβερνήσεων στην αντιμετώπιση των σχετικών προκλήσεων.[68]

Η ευκολία με την οποία οι άνθρωποι μπορούν να έχουν πρόσβαση στην πορνογραφία στο διαδίκτυο είναι δίκοπο μαχαίρι και τα κράτη διαδραματίζουν σημαντικό ρόλο στον καθορισμό του τρόπου ρύθμισης αυτής της πρόσβασης. Από τη μία πλευρά, δίνει τη δυνατότητα στους ενήλικες να εξερευνούν τις επιθυμίες τους ιδιωτικά και διακριτικά. Από την άλλη πλευρά, αυτή η προσβασιμότητα θέτει προκλήσεις για τους ανηλίκους και μπορεί να οδηγήσει σε ακούσια έκθεση, καθιστώντας αναγκαία τα κρατικά μέτρα για την προστασία των ευάλωτων πληθυσμών.[69] Επιπλέον, η ανωνυμία που παρέχει το διαδίκτυο μπορεί να ενθαρρύνει την επικίνδυνη συμπεριφορά και τη διάδοση μη συναινετικού ή εκμεταλλευτικού περιεχομένου, γεγονός που ωθεί τις κυβερνήσεις να αναλάβουν δράση.

Η παρουσία της πορνογραφίας στον κυβερνοχώρο επηρεάζει επίσης τις στενές σχέσεις, απαιτώντας σε ορισμένες περιπτώσεις κρατικές παρεμβάσεις. Ορισμένοι υποστηρίζουν ότι μπορεί να βελτιώσει τις σεξουαλικές εμπειρίες των ζευγαριών, καθώς χρησιμεύει ως μια μορφή σεξουαλικής εκπαίδευσης και διέγερσης, ενώ άλλοι υποστηρίζουν ότι η

[67] Αγγελής, Ι. (2005). *Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης*. Ποινική Δικαιοσύνη, 23-40.
[68] Αλεξανδροπούλου- Αιγυπτιάδου Ε. (2002), *Ζητήματα από το Δίκαιο της Πληροφορικής*, Αθήνα-Κομοτηνή: Εκδόσεις Σάκκολυα
[69] Αλεξανδρίδου, Ε. (2010). *Το Δίκαιο του Ηλεκτρονικού Εμπορίου*. Αθήνα: Εκδόσεις Σάκκουλα.

υπερβολική κατανάλωση πορνογραφίας μπορεί να οδηγήσει σε μη ρεαλιστικές προσδοκίες, απευαισθητοποίηση και δυσαρέσκεια εντός των σχέσεων. Ο πολλαπλασιασμός της πορνογραφίας στον κυβερνοχώρο έχει προκαλέσει πολυάριθμες ηθικές συζητήσεις, περιπλέκοντας περαιτέρω το ζήτημα, και οι κυβερνήσεις συχνά διαδραματίζουν ρόλο στη διαμόρφωση του ηθικού και νομικού πλαισίου που περιβάλλει αυτές τις συζητήσεις.[70]

Μια από τις κεντρικές ηθικές ανησυχίες περιστρέφεται γύρω από ζητήματα συναίνεσης και εκμετάλλευσης στη βιομηχανία ψυχαγωγίας ενηλίκων, τα οποία μπορεί να οδηγήσουν σε κρατική παρέμβαση. Περιπτώσεις εξαναγκασμού, εμπορίας ανθρώπων και εκμετάλλευσης είναι καλά τεκμηριωμένες, εγείροντας ερωτήματα σχετικά με τις ηθικές επιπτώσεις της κατανάλωσης τέτοιου περιεχομένου, ακόμη και από ενήλικες που συναινούν. Σε απάντηση, οι κυβερνήσεις μπορούν να θεσπίσουν νομοθεσία και κανονισμούς για να διασφαλίσουν την προστασία των εμπλεκομένων στη βιομηχανία και των καταναλωτών.[71]

Οι τεχνολογικοί κολοσσοί και οι διαδικτυακές πλατφόρμες διαδραματίζουν επίσης καθοριστικό ρόλο στη διανομή πορνογραφίας, η οποία απαιτεί κρατική εποπτεία. Πρέπει να περιηγηθούν σε μια λεπτή ισορροπία μεταξύ της προστασίας της ελεύθερης έκφρασης και της πρόληψης της βλάβης, και σε αυτό το σημείο μπαίνουν στο προσκήνιο οι κυβερνητικοί κανονισμοί και οι πολιτικές συγκράτησης του περιεχομένου. Εταιρείες όπως η Google, το Facebook και το Twitter έχουν αντιμετωπίσει επικρίσεις και ελέγχους σχετικά με τις πολιτικές τους για τη συγκράτηση του περιεχομένου και τον βαθμό στον οποίο επιτρέπουν το σχετικό υλικό. Οι κρατικές αρχές οφείλουν, κατά τους ειδικούς, να παρακολουθούν και, εάν είναι απαραίτητο, να ρυθμίζουν αυτές τις πλατφόρμες για να διασφαλίσουν ότι τηρούν τα νομικά και ηθικά πρότυπα.[72]

Η πλοήγηση στο νομικό τοπίο της πορνογραφίας στον κυβερνοχώρο είναι ένα πολύπλοκο εγχείρημα, καθώς περιλαμβάνει την εξισορρόπηση της ελευθερίας του λόγου με την ανάγκη προστασίας των ευάλωτων πληθυσμών και την καταπολέμηση των παράνομων δραστηριοτήτων, όπου τα κράτη διαδραματίζουν κεντρικό ρόλο.

---

[70] Βλαχόπουλος, Κ. (2007). *Ηλεκτρονικό Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.
[71] Ιγγλεζάκης, Ι. (2018). *Δίκαιο πληροφορικής*. Αθήνα: Εκδόσεις Σάκκουλα
[72] Αλεξανδροπούλου- Αιγυπτιάδου, Ε. (2007). *Η πλοήγηση των ανηλίκων στο διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων*. Αρμενόπουλος ΞΑ,12-35.

Διαφορετικές χώρες έχουν διαφορετικούς ορισμούς της αισχροκέρδειας και αυτό που θεωρείται νόμιμο σε μια δικαιοδοσία μπορεί να είναι παράνομο σε μια άλλη. Αυτή η νομική ασάφεια περιπλέκει τις διεθνείς προσπάθειες για τη ρύθμιση του περιεχομένου στο διαδίκτυο, προτρέποντας τις κυβερνήσεις να συνεργαστούν και να εναρμονίσουν τις προσεγγίσεις τους.[73]

Μία από τις πιο πιεστικές νομικές προκλήσεις είναι ο εντοπισμός και η απομάκρυνση της παιδικής πορνογραφίας, όπου οι κρατικές αρχές πρέπει να αναλάβουν ταχεία δράση. Οι εταιρείες τεχνολογίας και οι υπηρεσίες επιβολής του νόμου πρέπει να συνεργαστούν για την καταπολέμηση της διανομής τέτοιου υλικού, σεβόμενοι παράλληλα την ιδιωτική ζωή και τα δικαιώματα των ατόμων. Αυτό απαιτεί νομοθεσία, πόρους και διεθνή συνεργασία για την αποτελεσματική αντιμετώπιση του ζητήματος.

Η διαδικτυακή κατανάλωση πορνογραφικού υλικού μπορεί να εγείρει σημαντικά ζητήματα προστασίας της ιδιωτικής ζωής και της ασφάλειας, γεγονός που καθιστά αναγκαία τη λήψη κρατικών μέτρων προστασίας. Πολλοί ιστότοποι που φιλοξενούν ρητό περιεχόμενο συλλέγουν δεδομένα χρηστών, συχνά χωρίς ρητή συγκατάθεση. Τα δεδομένα αυτά μπορεί να είναι ευάλωτα σε παραβιάσεις και διαρροές, εκθέτοντας ενδεχομένως τα άτομα σε αμηχανία, εκβιασμό ή βλάβη. Οι κυβερνήσεις επιχειρούν να θεσπίσουν και να επιβάλουν νόμους για την προστασία των δεδομένων ώστε να διασφαλίσουν την ιδιωτική ζωή των χρηστών.[74]

Ακόμη, οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν συχνά την πορνογραφία ως όχημα για τη διανομή κακόβουλου λογισμικού και τη διενέργεια επιθέσεων ηλεκτρονικού "ψαρέματος", γεγονός που υπογραμμίζει τη σημασία της κρατικής συμμετοχής στην κυβερνοασφάλεια. Οι ανυποψίαστοι χρήστες μπορούν να θέσουν ακούσια σε κίνδυνο τις προσωπικές τους πληροφορίες και την ασφάλειά τους. Οι κυβερνήσεις απαιτείται να επενδύσουν σε μέτρα κυβερνοασφάλειας και να ευαισθητοποιήσουν για τις διαδικτυακές απειλές.[75]

Ένα μεγάλο μέρος της διαμοιραζόμενης πορνογραφίας στο διαδίκτυο, αφορά ανηλίκους. Παρά τις εξοντωτικές ποινές παγκοσμίως και το «κυνήγι μαγισσών» που

[73] Άντρη, Ε. (2013). Το φαινόμενο τον διαδικτυακού εθισμού στο σύγχρονο άνθρωπο. *Cyprus Nursing Chronicles, 14(3)*. Σελ. 2-5

[74] Δαγτόγλου, Π. (2012). *Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*. Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

[75] Βλαχόπουλος, Κ. (2013). *Ηλεκτρονικό έγκλημα: Μορφές, πρόληψη, αντιμετώπιση*. Αθήνα: Νομική Βιβλιοθήκη

Κράτη και οργανισμοί έχουν εξαπολύσει κατά των διακινητών αυτού του υλικού, η ζήτηση και προσφορά του στο σκοτεινό διαδίκτυο παραμένει σε υψηλά επίπεδα και απασχολεί διαρκώς τις υπηρεσίες επιβολής του νόμου.[76]

Τα προβλήματα που αντιμετωπίζουν οι αρχές είναι σημαντικά. Εκτός της προφανής δυσκολίας στον εντοπισμού του δράστη μέσω δαιδαλωδών διαδρομών και κρυπτογραφημένων δεδομένων στο διαδίκτυο, ομοίως δύσκολη είναι και η προσπάθεια μη περαιτέρω θυματοποίησης των ανήλικων θυμάτων.[77] Τα κράτη και κατ' επέκταση οι αρχές επιβολής του νόμου έχουν να αντιμετωπίσουν εκτός από την αναζήτηση και παύση της διακίνησης του υλικού αυτού στο κόσμο του διαδικτύου και τις μετέπειτα συνέπειες που αυτό έχει στη ψυχοσύνθεση και ζωή των ανήλικων θυμάτων εκτός αυτού. Οι ανήλικοι μάρτυρες-θύματα σεξουαλικής κακοποίησης, βρίσκουν τους εαυτούς τους σε μια δεινή κατάσταση, κατά την οποία υποχρεώνονται να εξιστορήσουν το γεγονός της κακοποίησης τους σε άγνωστους σε αυτούς, κοινωνικούς λειτουργούς, ανακριτικούς υπαλλήλους, δικαστικούς λειτουργούς κ.α., δίχως να γνωρίζουν το γιατί και το αν αυτή η πράξη θα έχει όφελος ή είναι ακόμα ένας εξαναγκασμός. Βιώνοντας ντροπή και ενοχή ανακαλούν τα γεγονότα, διογκώνοντας τον ψυχικό τραυματισμό τους και καθυστερώντας την επούλωση του.[78]

Η αντιμετώπιση των πολύπλοκων ζητημάτων που αφορούν την πορνογραφία και ιδιαίτερα των ανηλίκων στον κυβερνοχώρο απαιτεί μια πολύπλευρη προσέγγιση που περιλαμβάνει εκστρατείες εκπαίδευσης και ευαισθητοποίησης.[79]

Η διδασκαλία δεξιοτήτων ψηφιακού αλφαβητισμού μπορεί να βοηθήσει τα άτομα, ιδίως τους νέους, να αξιολογούν κριτικά και να περιηγούνται σε ρητό περιεχόμενο στο διαδίκτυο. Η εκπαίδευση των ατόμων σχετικά με τους πιθανούς κινδύνους και τις συνέπειες των διαδικτυακών τους δραστηριοτήτων είναι ζωτικής σημασίας.[80]

Η προώθηση ανοιχτών και ειλικρινών συζητήσεων σχετικά με την ενήλικη πορνογραφία και τις επιπτώσεις της μπορεί να μειώσει το στίγμα και τη ντροπή. Οι

---

[76] Macilotti, G. (2020). Online child pornography: Conceptual issues and law enforcement challenges. *In Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support*. IGI Global. Σελ. 226-247

[77] Θεμελή Ο. (2017), Η αναζήτηση της ουσιαστικής αλήθειας και ο κίνδυνος της νομικής πλάνης κατά τη διερεύνηση των ισχυρισμών των ανηλίκων θυμάτων σεξουαλικής κακοποίησης, στον *Τιμητικό Τόμο για τον Α. Μαγγανά*, Σελ. 669-686

[78] Πανάγος Κ. (2019), Η δικανική εξέταση ανηλίκων σε υποθέσεις σεξουαλικής κακοποίησης: Νεότερα νομοθετικά δεδομένα, *The Art of Crime*

[79] Gottfried, E. D., Shier, E. K., & Mulay, A. L. (2020). Child pornography and online sexual solicitation. *Current psychiatry reports*, *22*, Σελ. 1-8.

[80] Δαλακούρας, Θ. (2019). *Ηλεκτρονικό Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.

διάλογοι αυτοί θα πρέπει να περιλαμβάνουν θέματα όπως η συναίνεση, οι υγιείς σχέσεις και η υπεύθυνη χρήση του διαδικτύου.[81]

Η επικράτηση της πορνογραφίας στον κυβερνοχώρο είναι ένα πολύπλευρο ζήτημα που αγγίζει πολλές πτυχές της κοινωνίας, συμπεριλαμβανομένης της ηθικής, του δικαίου, της ιδιωτικής ζωής και των σχέσεων. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, το ίδιο θα συμβεί και με τις προκλήσεις και τις συζητήσεις γύρω από το ρητό περιεχόμενο στο διαδίκτυο. Η πλοήγηση σε αυτά τα αμφιλεγόμενα ύδατα απαιτεί μια διαφοροποιημένη και μελετημένη προσέγγιση που σέβεται τα ατομικά δικαιώματα, ενώ παράλληλα αντιμετωπίζει τις πιθανές βλάβες και τις ηθικές ανησυχίες που προκύπτουν στην ψηφιακή εποχή.[82]

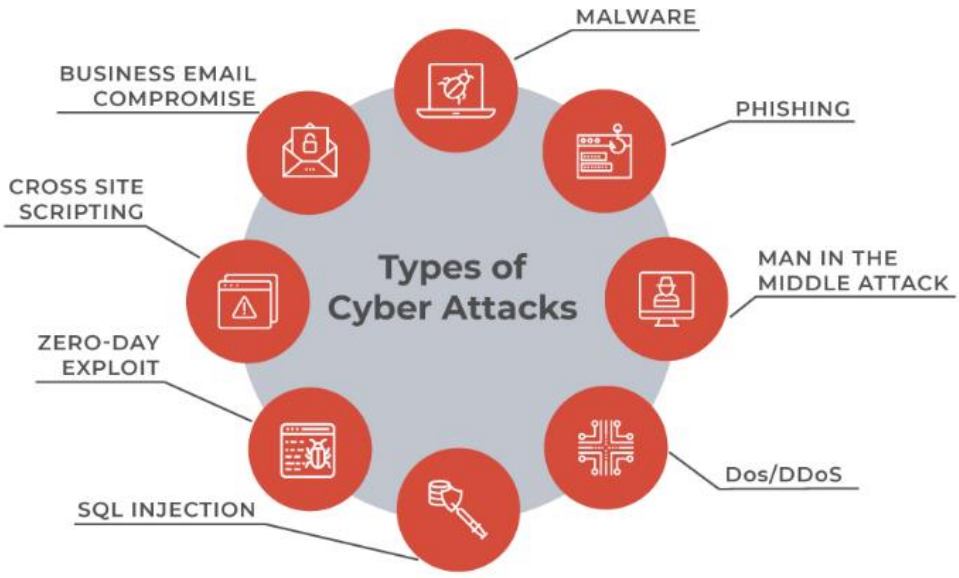
[81] Ιγγλεζάκης, Ι. (2020). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019).* Αθήνα: Interactive Books

[82] Καϊάφα- Γκμπάντι, Μ. (2012). *Διαδικτυακές προσβολές της ανηλικότητας*. ΠοινΧρ., 171.

3. Κυβερνοεπιθέσεις και απειλές

3.1. Είδη κυβερνοεπιθέσεων

Η ασφάλεια στον κυβερνοχώρο αποτελεί αναμφισβήτητα κρίσιμη ανησυχία στον σημερινό ψηφιακά συνδεδεμένο κόσμο, και καθώς η τεχνολογία συνεχίζει να εξελίσσεται, το ίδιο συμβαίνει και με τις μεθόδους και τις τακτικές που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να θέσουν σε κίνδυνο τα συστήματα, να κλέψουν ευαίσθητες πληροφορίες και να διαταράξουν τις λειτουργίες. Όπως αναφέρθηκε σε προηγούμενα κεφάλαια, έχουμε διερευνήσει διάφορες πτυχές των απειλών στον κυβερνοχώρο. Εδώ, θα εμβαθύνουμε σε ορισμένες επαναλαμβανόμενες απειλές και τις επιπτώσεις τους.



Εικόνα 2: Συνήθης τύποι κυβερνοεπιθέσεων

Πηγή: Team Ecosystm (2019), Things you need to know about Cyber Attacks, Threats and Risks, *Ecosystm* διαθέσιμο στο https://blog.ecosystm.io/cyber-attacks-threats-risks/

Το κακόβουλο λογισμικό (Malware), όπως αναφέρθηκε προηγουμένως, είναι μια ευρεία κατηγορία απειλών στον κυβερνοχώρο που περιλαμβάνει worms, ιούς, trojans και πρόσφατα κακόβουλα λογισμικά όπως spyware (λογισμικό υποκλοπής) και ransomware (λογισμικό λύτρων). Αυτές οι επιθέσεις περιλαμβάνουν την εισαγωγή κακόβουλου κώδικα στο σύστημα του θύματος, συχνά με σκοπό την απόκτηση μη

εξουσιοδοτημένης πρόσβασης, την κλοπή δεδομένων ή την πρόκληση διαταραχών του συστήματος.[83]

Οι επιθέσεις κακόβουλου λογισμικού αποτελούν μια διάχυτη και επίμονη απειλή στο ψηφιακό τοπίο καθώς αυτό αναπαράγεται ή εξαπλώνεται όταν αλληλοεπιδρά με άλλα συστήματα ή συσκευές. Μόλις εισέλθει σε ένα σύστημα, το κακόβουλο λογισμικό μπορεί να εκτελέσει μια σειρά επιβλαβών ενεργειών, όπως η διαρροή δεδομένων, η χειραγώγηση του συστήματος ή η δημιουργία backdoors για μελλοντική εκμετάλλευση με αποτελέσματα παραβιάσεις δεδομένων, οικονομικές απώλειες, βλάβη της φήμης και διακοπή λειτουργίας.[84] Οι επιθέσεις Ransomware περιλαμβάνουν την κρυπτογράφηση των δεδομένων του θύματος και την απαίτηση λύτρων για το κλειδί αποκρυπτογράφησης. Αυτές οι επιθέσεις μπορούν να διαταράξουν κρίσιμες λειτουργίες και να θέσουν σε κίνδυνο ευαίσθητες πληροφορίες.

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" είναι παραπλανητικές τακτικές που χρησιμοποιούνται από εγκληματίες του κυβερνοχώρου για να εξαπατήσουν τα άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, στοιχεία πιστωτικών καρτών ή προσωπικά στοιχεία ταυτότητας. Οι επιθέσεις αυτές συχνά περιλαμβάνουν απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου, ιστότοπους ή μηνύματα που έχουν σχεδιαστεί για να φαίνονται νόμιμα.

Η κοινωνική μηχανική είναι μια ευρύτερη κατηγορία που περιλαμβάνει τεχνικές χειραγώγησης που χρησιμοποιούνται για την εκμετάλλευση της ανθρώπινης ψυχολογίας. Το "ψάρεμα" είναι μία από τις πιο κοινές τεχνικές κοινωνικής μηχανικής.[85] Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται την εμπιστοσύνη και τα συναισθηματικά ερεθίσματα για να εξαπατήσουν τα άτομα ώστε να προβούν σε ενέργειες που ωφελούν τον επιτιθέμενο.

Οι επιθέσεις DDoS αποσκοπούν στην υπερφόρτωση ενός συστήματος ή δικτύου-στόχου με υπερβολικό όγκο κίνησης, καθιστώντας το απρόσιτο για τους νόμιμους

---

[83] Saravanan, A., & Bama, S. S. (2019). A review on cyber security and the fifth generation cyberattacks. Oriental journal of computer science and technology, 12(2), Σελ. 50-56.

[84] Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive survey on petya ransomware attack. In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) IEEE Σελ. 122-125

[85] Small, G. W., Moody, T. D., Siddarth, P., & Bookheimer, S. Y. (2009). Your brain on Google: patterns of cerebral activation during internet searching. American Journal of Geriatric Psychiatry, 17(2), 116-126. https://doi.org/10.1097/JGP.0b013e3181953a02

χρήστες. Αυτές οι επιθέσεις συχνά περιλαμβάνουν δίκτυα παραβιασμένων συσκευών (botnets) που συντονίζονται για να κατακλύσουν τον στόχο με κίνηση.

Οι επιπτώσεις των επιθέσεων DDoS μπορεί να είναι σοβαρές. Διακόπτουν τις διαδικτυακές υπηρεσίες και προκαλούν οικονομικές απώλειες. Ο μετριασμός των επιθέσεων DDoS απαιτεί ισχυρή υποδομή δικτύου, φιλτράρισμα της κυκλοφορίας και παρακολούθηση σε πραγματικό χρόνο για τον εντοπισμό και τον αποκλεισμό της κακόβουλης κυκλοφορίας.[86]

Η Structured Query Language Injection είναι μια συνηθισμένη επίθεση, η οποία βασίζεται στην αρχιτεκτονική των βάσεων δεδομένων που χρησιμοποιούν SQL. Συνήθως ο εισβολέας χρησιμοποιεί έναν κώδικα ο οποίος αναγκάζει τις βάσεις δεδομένων να του δώσουν πληροφορίες που υπό κανονικές συνθήκες δεν θα εμφάνιζαν. Συνήθως αυτό συμβαίνει με την εισδοχή του κώδικα στο πεδίο της αναζήτησης μιας ιστοσελίδας.[87]

Οι επιθέσεις τύπου MitM (Man in the Middle) συμβαίνουν όταν ο επιτιθέμενος παρεμβαίνει μεταξύ δύο συναλλασσόμενων υπολογιστών. Έτσι, κάθε συναλλαγή ή δεδομένο περνάει από τον εισβολέα πριν μεταφερθεί από το σημείο Α στο σημείο Β. Οι κίνδυνοι που ελλοχεύουν εστιάζουν τόσο στη κλοπή των δεδομένων όσο και στη δυνατότητα αλλαγής τους. Σε κάποιες περιπτώσεις τα δεδομένα κλέβονται απευθείας ενώ σε άλλες, ο επιτιθέμενες εγκαθιστά πρώτα κακόβουλο λογισμικό.[88]

Μια ευπάθεια Zero-day είναι ένα κενό ασφάλειας σε ένα σύστημα ή μια συσκευή που έχει αποκαλυφθεί αλλά δεν έχει ακόμη επιδιορθωθεί. Ένα exploit (πρόγραμμα που προσπαθεί να εκμεταλλευτεί μια ευπάθεια) που επιτίθεται σε μια ευπάθεια Zero-day ονομάζεται Zero-day Exploit. Το κενό ασφάλειας επιτρέπει στους επιτιθέμενους να κλέψουν ευαίσθητα δεδομένα, να εγκαταστήσουν κακόβουλο λογισμικό ή να θέσουν σε κίνδυνο ολόκληρα συστήματα.[89]

Οι τελευταίες δύο, αποτελούν Προηγμένες Διαρκείς Απειλές (Advanced Persistent Threats, APT) και είναι εξαιρετικά εξελιγμένες και στοχευμένες επιθέσεις στον

---

[86] OWASP (2023), Denial of Service, OWASP Foundation διαθέσιμο στο https://owasp.org/www-community/attacks/Denial_of_Service

[87] OWASP (2023), SQL Injection, OWASP Foundation διαθέσιμο στο https://owasp.org/www-community/attacks/SQL_Injection

[88] Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance,* 28, 24-31.

[89] Trend (2023), Zero-Day Vulnerability, Trend Micro Bussiness, διαθέσιμο στο https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability

κυβερνοχώρο, οι οποίες συνήθως ενορχηστρώνονται από κράτη-έθνη ή καλά χρηματοδοτούμενες εγκληματικές οργανώσεις. Οι δράστες APT χρησιμοποιούν διάφορες τακτικές, όπως spear-phishing, ευπάθειες μηδενικής ημέρας (zero-day exploits) και μυστική παραμονή σε παραβιασμένα συστήματα.[90]

Οι επιπτώσεις των APT είναι σοβαρές, ιδίως στον τομέα της εθνικής ασφάλειας και της εταιρικής κατασκοπείας. Οι επιθέσεις αυτές μπορεί να οδηγήσουν στην κλοπή ευαίσθητων κυβερνητικών ή εταιρικών δεδομένων, στην κλοπή πνευματικής ιδιοκτησίας και σε μακροχρόνιες παραβιάσεις κρίσιμων υποδομών. Η ανίχνευση και η άμυνα κατά των APTs απαιτεί προηγμένες πληροφορίες για τις απειλές, συνεχή παρακολούθηση και ισχυρά σχέδια αντιμετώπισης περιστατικών.

Οι επιθέσεις XSS πραγματοποιούνται με την έγχυση ενός κακόβουλου κώδικα σε μια κατά τα άλλα αξιόπιστη τοποθεσία. Όταν το θύμα επισκέπτεται τη συγκεκριμένη τοποθεσία, ο browser του δεν έχει τρόπο να γνωρίζει αν ο κώδικας που του αποστέλλεται δεν είναι αξιόπιστος, αποκτώντας πρόσβαση σε πληθώρα δεδομένων. Η ευπάθεια που χρησιμοποιείται για τις επιθέσεις XSS είναι αρκετά διαδεδομένη και μπορεί να συμβεί οπουδήποτε.[91]

Η κυβερνοασφάλεια είναι ένας διαρκώς εξελισσόμενος τομέας με ένα συνεχώς μεταβαλλόμενο τοπίο απειλών. Παρόλο που εξετάσαμε διάφορους τύπους επιθέσεων στον κυβερνοχώρο σε αυτή την ανασκόπηση, είναι σημαντικό να αναγνωρίσουμε ότι αναδύονται συνεχώς νέοι φορείς και τεχνικές επιθέσεων. Η συνεχής ενημέρωση σχετικά με τις τελευταίες απειλές και η εφαρμογή προληπτικών μέτρων ασφαλείας είναι ζωτικής σημασίας για τα άτομα και τους οργανισμούς ώστε να προστατεύονται στον ψηφιακό κόσμο.

3.2. Κυβερνοπόλεμος

Στην ψηφιακή εποχή, ο πόλεμος έχει ξεπεράσει τα παραδοσιακά όρια και έχει περάσει στο πεδίο του κυβερνοχώρου. Ο κυβερνοπόλεμος, ή κυβερνοσυγκρούσεις, περιλαμβάνει τη χρήση ψηφιακών τεχνικών και τεχνολογιών για την παραβίαση συστημάτων υπολογιστών, δικτύων και κρίσιμων υποδομών για στρατηγικούς,

[90] Kaspersky (2023), What is an APT?, *Kaspersky*, διαθέσιμο στο https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[91] OWASP (2023), Cross Site Scripting (XSS), OWASP Foundation, διαθέσιμο στο https://owasp.org/www-community/attacks/xss/

πολιτικούς ή στρατιωτικούς σκοπούς. Αυτό το δοκίμιο διερευνά το εξελισσόμενο τοπίο του κυβερνοπολέμου, τις μεθόδους, τα κίνητρα και τον κρίσιμο ρόλο της κυβερνοάμυνας σε έναν διασυνδεδεμένο κόσμο.

Θα πρέπει πρώτα να γίνει αντιληπτό ότι ο κυβερνοπόλεμος αποτελεί κατά τη βιβλιογραφία και τις στρατηγικές σπουδές, ασύμμετρη απειλή. Οι ασύμμετρες απειλές, γνωστές επίσης ως ασύμμετρος πόλεμος, αντιπροσωπεύουν μια ιδιαίτερη μορφή σύγκρουσης στην οποία ένα μέρος, συνήθως ένας ασθενέστερος ή μη κρατικός φορέας, υιοθετεί μη συμβατικές στρατηγικές και τακτικές για να υπερνικήσει τις δυνάμεις ενός ισχυρότερου αντιπάλου, συχνά ενός έθνους-κράτους. Αυτές οι απειλές χαρακτηρίζονται από την εγγενή ανισορροπία στις στρατιωτικές και οικονομικές δυνατότητες, καθιστώντας την ασθενέστερη πλευρά να βασίζεται σε καινοτόμες και μη παραδοσιακές μεθόδους για να αμφισβητήσει την ισχυρότερη δύναμη.[92] Οι ασύμμετρες απειλές έχουν συγκεντρώσει αυξανόμενη προσοχή στις σύγχρονες μελέτες ασφάλειας και στρατιωτικών σπουδών λόγω της επικράτησής τους στις σύγχρονες συγκρούσεις. Τα βασικά χαρακτηριστικά των ασύμμετρων απειλών περιλαμβάνουν:

- Ανισορροπία ισχύος και πόρων: Στο επίκεντρο των ασύμμετρων απειλών βρίσκεται μια ουσιαστική ανισορροπία ισχύος, πόρων και δυνατοτήτων μεταξύ των αντιμαχόμενων μερών. Η ανισότητα αυτή μπορεί να προκύπτει από τη διαφορά στη στρατιωτική ισχύ, την οικονομική ικανότητα ή την τεχνολογική πρόοδο.
- Μη συμβατικές τακτικές: Αυτές οι τακτικές μπορεί να περιλαμβάνουν ανταρτοπόλεμο, αντάρτικο, τρομοκρατία, επιθέσεις στον κυβερνοχώρο, προπαγάνδα και χρήση μη ένστολων μαχητών.
- Προσαρμοστικότητα: Η ικανότητά τους να προσαρμόζουν γρήγορα την τακτική τους και να εκμεταλλεύονται τα τρωτά σημεία στην προσέγγιση του εχθρού μπορεί να αποδειχθεί σημαντικό πλεονέκτημα.
- Χρήση μη κρατικών φορέων: Γίνεται χρήση ομάδων ανταρτών, πολιτοφυλακών ή τρομοκρατικών οργανώσεων. Οι ομάδες αυτές δρουν εκτός του παραδοσιακού στρατιωτικού πλαισίου και χρησιμοποιούν τη γνώση του τοπικού εδάφους, τα δίκτυα υποστήριξης και τις μη συμβατικές στρατηγικές τους.

[92] Lele, A. (2014). Asymmetric Warfare: A State vs Non-State Conflict. OASIS, (20), Universidad Externado de Colombia. Σελ. 97-111.

- Ψυχολογικός πόλεμος: Η ψυχολογική χειραγώγηση και η προπαγάνδα είναι κοινά εργαλεία στο οπλοστάσιο των ασύμμετρων δρώντων. Στόχος είναι η διάβρωση του ηθικού της ισχυρότερης δύναμης, η συγκέντρωση υποστήριξης από τον τοπικό πληθυσμό ή η υποκίνηση φόβου.
- Πολυπλοκότητα και ασάφεια: Οι ασύμμετρες συγκρούσεις εκτυλίσσονται συχνά σε πολύπλοκα και ασαφή περιβάλλοντα, όπου τα όρια μεταξύ μαχητών και μη μαχητών είναι θολά. Αυτή η πολυπλοκότητα μπορεί να περιπλέξει τη λήψη αποφάσεων και για τα δύο μέρη και καθιστά δύσκολο για τους ισχυρότερους δρώντες να εντοπίσουν και να εξουδετερώσουν τις απειλές.[93]

Ωστόσο, Σε αντίθεση με τον παραδοσιακό πόλεμο, μία από τις μοναδικές προκλήσεις του κυβερνοπολέμου, όπως ήδη αναφέρθηκε, είναι η δυσκολία της απόδοσης ή του προσδιορισμού της πηγής μιας κυβερνοεπίθεσης. Η πρόκληση αυτή υπογραμμίζει την ανάγκη διεθνούς συνεργασίας και συμφωνιών για τη θέσπιση κανόνων και κανόνων στον κυβερνοχώρο.[94]

Ο κυβερνοπόλεμος έχει αποκτήσει εξέχουσα σημασία τα τελευταία χρόνια, καθώς τα έθνη αναγνωρίζουν τις δυνατότητες του κυβερνοχώρου ως πεδίου μάχης. Η δημιουργία της Διοίκησης Κυβερνοχώρου των ΗΠΑ το 2009 αποτέλεσε σημαντικό ορόσημο, σηματοδοτώντας τη θεσμοθέτηση των δυνατοτήτων κυβερνοπολέμου. Η εξέλιξη αυτή υπογράμμισε την ανάγκη για ειδικά μέτρα άμυνας στον κυβερνοχώρο και την αναγνώριση του κυβερνοχώρου ως τομέα στρατιωτικών επιχειρήσεων.[95]

Ο κυβερνοπόλεμος περιλαμβάνει ένα ευρύ φάσμα μεθόδων και τακτικών, συχνά σχεδιασμένων για την επίτευξη συγκεκριμένων στόχων. Αυτές οι μέθοδοι περιλαμβάνουν την ανάπτυξη κακόβουλου λογισμικού για την απόκτηση μη εξουσιοδοτημένης πρόσβασης, την απομόνωση δεδομένων ή τη διακοπή επιχειρήσεων. Επιπλέον, οι επιτιθέμενοι χρησιμοποιούν παραπλανητικές τακτικές όπως το phishing και η κοινωνική μηχανική για να εξαπατήσουν άτομα ή οργανισμούς ώστε να

[93] Brzica, N. (2018). Understanding Contemporary Asymmetric Threats. Croatian International Relations Review, 24(83), Σελ. 34-51.
[94] Wang, M., Callaghan, V., Bernhardt, J., White, K., & Peña-Rios, A. (2018). Augmented reality in education and training: pedagogical approaches and illustrative case studies. Journal of Ambient Intelligence and Humanized Computing, 9(5), Σελ. 1391-1402.
[95] U.S. Cybercom. (n.d.). Command History. Retrieved December 22, 2019, from https://www.cybercom.mil/About/History/.

αποκαλύψουν ευαίσθητες πληροφορίες.[96] Οι επιθέσεις άρνησης παροχής υπηρεσιών (DDoS) κατακλύζουν τα συστήματα-στόχους με υπερβολική κίνηση, καθιστώντας τα απρόσιτα για τους χρήστες. Οι Προηγμένες Διαρκείς Απειλές (Advanced Persistent Threats - APTs) είναι εξελιγμένες, μακροχρόνιες εκστρατείες στον κυβερνοχώρο που ενορχηστρώνονται από εθνικά κράτη ή καλά χρηματοδοτούμενες ομάδες για να διεισδύσουν σε συστήματα, να κλέψουν δεδομένα ή να διατηρήσουν κρυφή πρόσβαση. Οι επιθέσεις στην αλυσίδα εφοδιασμού θέτουν σε κίνδυνο την αλυσίδα εφοδιασμού για την εισαγωγή κακόβουλου κώδικα ή στοιχείων υλικού σε προϊόντα λογισμικού ή υλικού.[97]

Τα κίνητρα πίσω από τον κυβερνοπόλεμο είναι ποικίλα και μπορεί να περιλαμβάνουν πολιτικές, οικονομικές, στρατιωτικές, ή ιδεολογικές προθέσεις. Ορισμένα κοινά κίνητρα περιλαμβάνουν την κατασκοπεία, όπου τα έθνη-κράτη συλλέγουν πληροφορίες για τις δραστηριότητες άλλων χωρών. Το σαμποτάζ περιλαμβάνει τη στόχευση κρίσιμων υποδομών για τη διακοπή των επιχειρήσεων και την πρόκληση οικονομικής ή κοινωνικής ζημίας. Οι επιχειρήσεις επιρροής (PsyOp)[98] χρησιμοποιούν τεχνικές στον κυβερνοχώρο για να χειραγωγήσουν την κοινή γνώμη, να σπείρουν τη διχόνοια ή να παρέμβουν στις πολιτικές διαδικασίες άλλων εθνών.

Καθώς η σημασία του κυβερνοπολέμου αυξάνεται, τα ισχυρά μέτρα κυβερνοάμυνας έχουν καταστεί επιτακτικά. Οι αποτελεσματικές στρατηγικές άμυνας στον κυβερνοχώρο περιλαμβάνουν μέτρα ασφαλείας δικτύου, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και κρυπτογράφηση.[99] Η εκπαίδευση των χρηστών διαδραματίζει κρίσιμο ρόλο στη μείωση του κινδύνου επιτυχημένων επιθέσεων, εκπαιδεύοντας τα άτομα και τους υπαλλήλους σχετικά με τις απειλές στον κυβερνοχώρο, την ασφαλή διαδικτυακή συμπεριφορά και την αναγνώριση των προσπαθειών phishing. Τα σχέδια αντιμετώπισης περιστατικών, τα οποία

[96] Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. European journal of operational research, 146(2), Σελ. 241-257.
[97] Harknett R. & Smeets M., (2022). Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 45:4, Σελ. 534-567
[98] Οι Ψυχολογικές Επιχειρήσεις (PSYOP) είναι λειτουργίες για τη μετάδοση επιλεγμένων πληροφοριών και δεικτών στο κοινό για να επηρεάσουν τα κίνητρα και την αντικειμενική τους λογική και τελικά τη συμπεριφορά κυβερνήσεων, οργανισμών, ομάδων και μεγάλων ξένων δυνάμεων.
[99] Wang, M., Callaghan, V., Bernhardt, J., White, K., & Peña-Rios, A. (2018). Όπ.π.

αναπτύσσονται και εφαρμόζονται από τους οργανισμούς, επιτρέπουν την ταχεία και αποτελεσματική αντίδραση όταν σημειώνονται επιθέσεις στον κυβερνοχώρο.[100]

Η προοπτική κυβερνοσυγκρούσεων εγείρει επίσης ερωτήματα σχετικά με τους κανόνες εμπλοκής και την εφαρμογή του διεθνούς δικαίου. Οι παραδοσιακές αρχές της ένοπλης σύγκρουσης, όπως η αναλογικότητα και η διάκριση μεταξύ μαχητών και μη μαχητών, πρέπει να προσαρμοστούν στον ψηφιακό τομέα.[101]

Σε απάντηση στην αυξανόμενη απειλή του κυβερνοπολέμου, πολλά έθνη έχουν αναγάγει την ασφάλεια στον κυβερνοχώρο σε εθνική προτεραιότητα. Αυτό περιλαμβάνει όχι μόνο την ενίσχυση των αμυντικών δυνατοτήτων, αλλά και την επένδυση σε επιθετικές κυβερνοδυνατότητες ως αποτρεπτικό μέσο.[102]

Ο κυβερνοπόλεμος έχει αναδειχθεί σε καθοριστική πρόκληση της ψηφιακής εποχής. Οι μέθοδοι, τα κίνητρα και οι επιπτώσεις του συνεχίζουν να εξελίσσονται, παρουσιάζοντας σύνθετες και δυναμικές απειλές για έθνη, οργανισμούς και άτομα. Ενώ η επιτακτική ανάγκη της κυβερνοάμυνας είναι σαφής, η αντιμετώπιση των μοναδικών προκλήσεων που την χαρακτηρίζουν και της προσαρμογής των διεθνών κανόνων παραμένει μια συνεχής προσπάθεια.[103]

3.3. Κυβερνοέγκλημα

Το έγκλημα στον κυβερνοχώρο, το οποίο χαρακτηρίζεται από παράνομες δραστηριότητες που διεξάγονται μέσω δικτύων υπολογιστών και του διαδικτύου, έχει καταστεί σημαντική απειλή για άτομα, οργανισμούς και έθνη παγκοσμίως.

Περιλαμβάνει ένα ευρύ φάσμα παράνομων δραστηριοτήτων που αξιοποιούν την τεχνολογία και το διαδίκτυο για την επίτευξη εγκληματικών στόχων με απεριόριστο αριθμό πιθανών θυμάτων, αποτελώντας σημαντική πρόκληση για τις υπηρεσίες

[100] Walther, G. (2015). Printing insecurity? The security implications of 3d-printing of weapons. *Science and engineering ethics*, 21(6), Σελ. 1435-1445

[101] Wang, M., Callaghan, V., Bernhardt, J., White, K., & Peña-Rios, A. (2018). Όπ.π.

[102] Wang, P., Dawson, M., & Williams, K. L. (2019). Improving cyber defense education through national standard alignment: case studies. In National Security: Breakthroughs in Research and Practice IGI Global. Σελ. 78-91

[103] Ward, C., Polglase, K., Shukla, S., Mezzofiore, G., & Lister, T. (2020). How Russian meddling is back before 2020 vote. *CNN.* Διαθέσιμο στο https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

επιβολής του νόμου και τους επαγγελματίες της κυβερνοασφάλειας.[104] Τα κυβερνοεγκλήματα χαρακτηρίζονται από:

- Το παράνομο της δραστηριότητας: Περιλαμβάνουν διάφορες μορφές όπως η πειρατεία, η κλοπή ταυτότητας, η απάτη, η διαδικτυακή παρενόχληση και η διανομή κακόβουλου λογισμικού.
- Την Ψηφιακή μορφή: Καθώς λαμβάνουν χώρα κυρίως στο ψηφιακό πεδίο, βασιζόμενα στα δίκτυα υπολογιστών, το λογισμικό και το διαδίκτυο ως βασικά εργαλεία για το σχεδιασμό και την εκτέλεση.
- Την Παγκόσμια εμβέλεια: οι κυβερνοεγκληματίες μπορούν να δρουν σχεδόν από οπουδήποτε στον κόσμο, γεγονός που καθιστά δύσκολο τον εντοπισμό και τη δίωξη των δραστών.
- Εξελισσόμενες τεχνικές: Οι δράστες προσαρμόζονται και αναπτύσσουν συνεχώς νέες τεχνικές, εκμεταλλευόμενοι τα τρωτά σημεία της τεχνολογίας και της ανθρώπινης συμπεριφοράς για να επιτύχουν τους στόχους τους.[105]

Στην αρχή του κεφαλαίου έγινε αναφορά στους πιο διαδεδομένους τρόπους με τους οποίους διαπράττεται το έγκλημα στον κυβερνοχώρο, ενώ νωρίτερα τα χαρακτηριστικά του. Θα πρέπει όμως να γίνει μια παρουσίαση και στα κίνητρα. Ορισμένα από αυτά είναι:

- Οικονομικό κέρδος: Ίσως το πιο διαδεδομένο κίνητρο στο πλαίσιο των εγκλημάτων. Σκοπός είναι η πρόσβαση σε χρηματικά ποσά ή δεδομένα με στόχο το εύκολο κέρδος μέσω απάτης.
- Hacktivism – Πολιτικός ή Κοινωνικός ακτιβισμός: Ο χακτιβισμός είναι μια δραστηριότητα που περιλαμβάνει ανώνυμους οργανισμούς που εισβάλλουν στην υποδομή πληροφορικής ενός οργανισμού για πολιτικούς ή κοινωνικούς λόγους. Συχνοί στόχοι αποτελούν κυβερνήσεις και πολιτικοί φορείς.
- Διανοητική πρόκληση: Πολλές επιθέσεις σε στόχους γίνονται στα πλαίσια προσωπικής ικανοποίησης ή εύρεσης τρωτών σημείων με σκοπό την μετέπειτα επισκευή τους από εργολαβικές ομάδες.

[104] Aman Gupta, A. A. (2017). Ethical Hacking and Hacking Attacks. *International Journal Of Engineering And Computer Science*, 6(4), Σελ. 21042- 21050.
[105] Joshi, D. M. (2021). Cyber Pornography: An Interdisciplinary study of technology led crime against women and children. International Journal of Creative Research Thoughts (IJCRT), 9(12), Σελ. 297- 301.

- Κατασκοπεία: Κλοπή απόρρητων πληροφοριών από οργανισμούς ή Εθνικά Κράτη.
- Οργανωμένο έγκλημα: Το ψηφιακό πεδίο παρέχει μια πλατφόρμα για επέκταση των εγκληματικών δραστηριοτήτων των οργανωμένων ομάδων.
- Αποσταθεροποίηση: Στόχος η διαταραχή της λειτουργίας επιχειρήσεων ή υποδομών ζωτικής σημασίας με σκοπό, συνήθως, την πρόκληση οικονομικής ζημιάς.[106]

Η έξαρση του εγκλήματος στον κυβερνοχώρο θέτει διάφορες προκλήσεις για τα άτομα, τους οργανισμούς και την κοινωνία στο σύνολό της:

- Διάδοση: Το έγκλημα στον κυβερνοχώρο επηρεάζει άτομα όλων των ηλικιών και υποβάθρων, καθιστώντας το μια διάχυτη απειλή.
- Ταχεία εξέλιξη: Οι εγκληματίες του κυβερνοχώρου προσαρμόζουν συνεχώς τις τακτικές τους, καθιστώντας δύσκολο για τα μέτρα κυβερνοασφάλειας να συμβαδίσουν.
- Οικονομικός αντίκτυπος: Το έγκλημα στον κυβερνοχώρο έχει ως αποτέλεσμα σημαντικές οικονομικές απώλειες για άτομα και οργανισμούς, επηρεάζοντας τις οικονομίες σε παγκόσμιο επίπεδο.
- Ανησυχίες για την προστασία της ιδιωτικής ζωής: Η κλοπή και η κατάχρηση προσωπικών πληροφοριών εγείρουν σημαντικές ανησυχίες για την προστασία της ιδιωτικής ζωής και διαβρώνουν την εμπιστοσύνη στις διαδικτυακές δραστηριότητες.
- Νομική δικαιοδοσία: Ο καθορισμός της νομικής δικαιοδοσίας για υποθέσεις εγκλημάτων στον κυβερνοχώρο που αφορούν διεθνείς δράστες μπορεί να είναι πολύπλοκος.[107]

Καθώς οι εκδηλώσεις του εγκλήματος στον κυβερνοχώρο συνεχίζουν να εξελίσσονται, τα άτομα και οι οργανισμοί πρέπει να παραμένουν σε εγρήγορση και να εφαρμόζουν ισχυρά μέτρα κυβερνοασφάλειας για την προστασία από αυτή την αυξανόμενη απειλή. Σε έναν κόσμο που διασυνδέεται όλο και περισσότερο με την τεχνολογία, η

[106] Paquet-Clouston, M., & García, S. (2022). On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime*, Σελ. 1-30.
[107] Όπ.π.

καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι μια συνεχής προσπάθεια ζωτικής σημασίας για την ασφάλεια και την ευημερία όλων. [108]

3.4. Οργανώσεις και αμφιλεγόμενες πρακτικές

Η ενσωμάτωση των οργανισμών και των αμφιλεγόμενων πρακτικών στο πλαίσιο της ευρύτερης συζήτησης για την ασφάλεια στον κυβερνοχώρο και τις υπηρεσίες πληροφοριών στον κυβερνοχώρο μπορεί αρχικά να φαίνεται ανομοιογενής. Ωστόσο, είναι σημαντικό να αναγνωρίσουμε ότι τα στοιχεία αυτά διασταυρώνονται μέσα στο πολύπλευρο τοπίο της ψηφιακής ασφάλειας. Ενώ η ασφάλεια στον κυβερνοχώρο επικεντρώνεται κυρίως στη διαφύλαξη των ψηφιακών περιουσιακών στοιχείων και στον μετριασμό των απειλών στον κυβερνοχώρο, οι οργανισμοί διαδραματίζουν συχνά καθοριστικό ρόλο στον τομέα της ασφάλειας στον κυβερνοχώρο. Η παρούσα ενότητα ρίχνει φως στις λιγότερο συζητημένες αλλά σημαντικές ηθικές και δεοντολογικές διαστάσεις που αφορούν τους οργανισμούς και τις πρακτικές τους στο πλαίσιο της κυβερνοασφάλειας και των υπηρεσιών πληροφοριών στον κυβερνοχώρο.

Στον σημερινό διασυνδεδεμένο κόσμο, οι οργανισμοί δεν είναι μόνο καταναλωτές των μέτρων κυβερνοασφάλειας αλλά και αναπόσπαστοι συντελεστές του εξελισσόμενου κυβερνοτοπίου. Είναι υπεύθυνοι για την ασφάλεια των συστημάτων τους και των δεδομένων που διαχειρίζονται, τα οποία συχνά περιλαμβάνουν ευαίσθητες πληροφορίες που ανήκουν σε ιδιώτες και οντότητες.[109]

Ένας από τους κρίσιμους τομείς στους οποίους οι οργανισμοί διασταυρώνονται με την κυβερνοασφάλεια είναι το απόρρητο των δεδομένων. Σε μια εποχή όπου τα δεδομένα αποτελούν πολύτιμο αγαθό, οι οργανισμοί έχουν την ηθική ευθύνη να χειρίζονται τα δεδομένα με τη μεγαλύτερη δυνατή προσοχή και σύμφωνα με τους σχετικούς κανονισμούς. Η κακή χρήση ή ο κακός χειρισμός των δεδομένων μπορεί να οδηγήσει σε παραβιάσεις της ιδιωτικής ζωής, οι οποίες, με τη σειρά τους, μπορεί να έχουν σημαντικές ηθικές επιπτώσεις και νομικές συνέπειες. Μόλις το Μάιο του 2023 η Ιρλανδική Επιτροπή Προστασίας Δεδομένων επέβαλε το ιστορικό πρόστιμο των 1,2 δισεκατομμυρίων ευρώ στον Αμερικανικό τεχνολογικό κολοσσό Meta για παραβιάσεις

[108] Altwairqi F.A. (2019). Four Most Famous Cyber Attacks for Financial Gains. *International Journal of Engineering and Advanced Technology (IJEAT),* 9(2), 2131-2139.
[109] Denning, D. E. (2015). A Framework for Ethical Decision Making in Cybersecurity. *IEEE Security & Privacy*, 13(1), Σελ. 84-88

των ιδιωτικών δεδομένων των χρηστών[110] ενώ λίγο αργότερα το Δεκέμβριο του 2023 έγινε γνωστό ότι Κυβερνήσεις παίρνουν στοιχεία χρηστών όπως δεδομένα ειδοποιήσεων από την Google και την Apple εδώ και χρόνια προκειμένου να ταυτοποιούν τους χρήστες.[111]

Μια μελέτη της Ilina Georgieva διερευνά τον απρόβλεπτο ρόλο των υπηρεσιών πληροφοριών στον κυβερνοχώρο. Χρησιμεύει ως ένα εύστοχο παράδειγμα του τρόπου με τον οποίο οι οργανισμοί, ιδίως όσοι ασχολούνται με τις υπηρεσίες πληροφοριών και την ασφάλεια στον κυβερνοχώρο, πρέπει να περιηγηθούν σε σύνθετα ηθικά και δεοντολογικά διλήμματα.[112]

Οι υπηρεσίες πληροφοριών διαδραματίζουν ζωτικό ρόλο στη διασφάλιση των συμφερόντων ενός έθνους στον κυβερνοχώρο, λειτουργώντας συχνά στη σκιά και χρησιμοποιώντας εξελιγμένες τεχνικές στον κυβερνοχώρο. Οι ηθικές και δεοντολογικές διαστάσεις των ενεργειών τους βρίσκονται υπό συνεχή έλεγχο. Η μελέτη υπογραμμίζει τη σημασία της τήρησης ηθικών προτύπων, όχι μόνο στις δραστηριότητες των υπηρεσιών πληροφοριών, αλλά και στις διεθνείς σχέσεις και τη διπλωματία στο πλαίσιο του κυβερνοπολέμου.

Επιπλέον, η εξέταση πραγματικών περιπτώσεων, όπως οι αποκαλύψεις του Snowden, παρέχει πολύτιμα διδάγματα τόσο για τους οργανισμούς όσο και για τις υπηρεσίες πληροφοριών. Οι ηθικοί προβληματισμοί γύρω από την επιτήρηση, τη συλλογή δεδομένων και την προστασία της ιδιωτικής ζωής κατέστησαν κεντρικοί μετά τις αποκαλύψεις αυτές. Υπογραμμίζεται η σημασία της διαφάνειας, της λογοδοσίας και της τήρησης ηθικών προτύπων στο πεδίο των πληροφοριών και της ασφάλειας στον κυβερνοχώρο.[113]

Εν κατακλείδι, ενώ η κυβερνοασφάλεια αφορά κυρίως την προστασία των ψηφιακών περιουσιακών στοιχείων και την αντιμετώπιση των απειλών στον κυβερνοχώρο, οι οργανισμοί και οι πρακτικές τους είναι εγγενείς σε αυτόν τον τομέα. Η προστασία της ιδιωτικής ζωής των δεδομένων και η διαφάνεια είναι βασικά στοιχεία που οι οργανισμοί θα πρέπει να θέτουν ως προτεραιότητα στις προσπάθειές τους για την

[110] Milmo D. (2023), Facebook owner Meta fined €1.2bn for mishandling user information, *The Guardian* διαθέσιμο στο https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta

[111] Couts A. & Newman L.H (2023), Police can spy on your iOS and Android Push Notifications, *Wired*, διαθέσιμο στο https://www.wired.com/story/apple-google-push-notification-surveillance/

[112] Georgieva, I. (2020). Όπ.π., Σελ. 33-54.

[113] Smith, S. W. (2021). Cybersecurity and Cyberwarfare: An *Introduction*. Routledge.

ασφάλεια στον κυβερνοχώρο. Η μελέτη της Ilina Georgieva (2020) χρησιμεύει ως υπενθύμιση ότι ακόμη και στον κρυφό κόσμο των υπηρεσιών πληροφοριών και του κυβερνοπολέμου, τα ηθικά πρότυπα και οι ηθικές εκτιμήσεις πρέπει να καθοδηγούν τις δράσεις. Αυτές οι ηθικές διαστάσεις δεν είναι ζωτικής σημασίας μόνο για τους οργανισμούς και τις υπηρεσίες πληροφοριών, αλλά είναι επίσης κεντρικής σημασίας για τις διεθνείς σχέσεις και τη διπλωματία στην εποχή της κυβερνοασφάλειας.

4. Ευρωπαϊκές πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο

4.1. Νομικό πλαίσιο: Κατανόηση του νομικού καθεστώτος στην Ευρώπη

Η Ευρώπη είναι μια ήπειρος που χαρακτηρίζεται από την ποικιλομορφία της, και η ποικιλομορφία αυτή επεκτείνεται στα νομικά συστήματα και πλαίσια. Το νομικό τοπίο στην Ευρώπη είναι ένα πολύπλοκο μωσαϊκό από εθνικούς νόμους, περιφερειακές συμφωνίες και κανονισμούς της Ευρωπαϊκής Ένωσης (ΕΕ).

Το νομικό καθεστώς στην ΕΕ αντλεί από διάφορες πηγές, καθεμία από τις οποίες συμβάλλει στην ανάπτυξη και την εφαρμογή των νόμων σε ολόκληρη την ήπειρο. Οι πηγές αυτές περιλαμβάνουν:

- Εθνικοί νόμοι: Κάθε ευρωπαϊκή χώρα έχει το δικό της νομικό σύστημα, το οποίο επηρεάζεται από ιστορικούς, πολιτιστικούς και κοινωνικούς παράγοντες ρυθμίζοντας ένα ευρύ φάσμα θεμάτων.
- Περιφερειακές συμφωνίες: Το νομικό τοπίο της ΕΕ διαμορφώνεται από περιφερειακές συμφωνίες, όπως η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ) και η Συμφωνία Σένγκεν.
- Δίκαιο της Ευρωπαϊκής Ένωσης: Το δίκαιο της ΕΕ αποτελείται από πρωτογενές και δευτερογενές δίκαιο, συμπεριλαμβανομένων συνθηκών, κανονισμών, οδηγιών και αποφάσεων.[114]
- Νομολογία: Οι αποφάσεις των ευρωπαϊκών δικαστηρίων, όπως το Ευρωπαϊκό Δικαστήριο (ΔΕΚ) και το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΑΔ), συμβάλλουν στην ανάπτυξη των νομικών αρχών και στην ερμηνεία των νόμων σε ολόκληρη την ΕΕ.

Το ευρωπαϊκό νομικό πλαίσιο περιλαμβάνει διάφορα βασικά στοιχεία, καθένα από τα οποία εξυπηρετεί έναν συγκεκριμένο σκοπό:

[114] European Union. (2023). *Law*. Διαθέσιμο στο https://european-union.europa.eu/institutions-law-budget/law_en

- Συνθήκες: Οι συνθήκες είναι διεθνείς συμφωνίες μεταξύ των κρατών μελών της ΕΕ που καθορίζουν τους στόχους, τα θεσμικά όργανα και τους τομείς αρμοδιότητας της ΕΕ.
- Κανονισμοί: Οι κανονισμοί είναι άμεσα εφαρμοστέοι νόμοι της ΕΕ που έχουν άμεση νομική ισχύ και δεσμευτικότητα για όλα τα κράτη μέλη.[115]
- Οδηγίες: Οι οδηγίες θέτουν συγκεκριμένους στόχους για τα κράτη μέλη που πρέπει να επιτύχουν εντός συγκεκριμένου χρονικού πλαισίου με σκοπό την εναρμόνιση στο Ευρωπαϊκό πλαίσιο.[116]
- Αποφάσεις: Οι αποφάσεις είναι δεσμευτικές για τα συγκεκριμένα μέρη ή κράτη μέλη στα οποία απευθύνεται η απόφαση. Χρησιμοποιούνται για θέματα που απαιτούν εξατομικευμένες ή ακριβείς ενέργειες.[117]
- Νομολογία: Οι αποφάσεις των ευρωπαϊκών δικαστηρίων, ιδίως του ΔΕΕ, ερμηνεύουν το δίκαιο της ΕΕ και επιλύουν διαφορές μεταξύ κρατών μελών, θεσμικών οργάνων και ατόμων.[118]
- Εθνικοί νόμοι: Τα εθνικά νομικά συστήματα συνυπάρχουν με το δίκαιο της ΕΕ και συνεχίζουν να εφαρμόζονται σε τομείς που δεν καλύπτονται από την αρμοδιότητα της ΕΕ λειτουργώντας συμπληρωματικά.
- Μηχανισμοί επιβολής: Τα θεσμικά όργανα της ΕΕ και τα κράτη μέλη συνεργάζονται για να διασφαλίσουν τη συμμόρφωση με το δίκαιο της ΕΕ. Αυτό περιλαμβάνει τον ρόλο της Ευρωπαϊκής Επιτροπής στην παρακολούθηση και την επιβολή των κανονισμών της ΕΕ.

Ενώ το ευρωπαϊκό νομικό πλαίσιο αποτελεί πρότυπο συνεργασίας και ολοκλήρωσης, αντιμετωπίζει αρκετές προκλήσεις:

- Ποικιλομορφία των νομικών συστημάτων: Η νομική ποικιλομορφία της ΕΕ, δημιουργεί προκλήσεις στην εναρμόνιση των νόμων μεταξύ των κρατών μελών.
- Brexit: Η αποχώρηση του Ηνωμένου Βασιλείου από την ΕΕ, γνωστή ως Brexit, έχει εγείρει πολύπλοκα νομικά ζητήματα σχετικά με το εμπόριο, τα δικαιώματα

[115] European Union. (2023). *Types of legislation*. Διαθέσιμο στο https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
[116] Όπ.π.
[117] Όπ.π.
[118] European Union. (2023). *Law*. Όπ.π.

των πολιτών και το πρωτόκολλο της Βόρειας Ιρλανδίας προκαλώντας περίπλοκες νομικές διαπραγματεύσεις.[119]

- Κράτος δικαίου: Οι ανησυχίες σχετικά με το κράτος δικαίου σε ορισμένα κράτη μέλη της ΕΕ, ιδίως όσον αφορά την ανεξαρτησία της δικαιοσύνης και την ελευθερία των μέσων ενημέρωσης, έχουν προκαλέσει συζητήσεις σχετικά με την ικανότητα της ΕΕ να προασπίσει τις θεμελιώδεις αξίες της.[120]
- Ψηφιοποίηση: Η ψηφιακή εποχή παρουσιάζει νέες νομικές προκλήσεις, όπως η προστασία των δεδομένων, η κυβερνοασφάλεια και η ρύθμιση των ψηφιακών πλατφορμών. Η προσαρμογή των υφιστάμενων νόμων στις προκλήσεις αυτές είναι μια συνεχής διαδικασία.[121]
- Μετανάστευση: Η διαχείριση των μεταναστευτικών ροών εντός της ΕΕ και ο χειρισμός των αιτούντων άσυλο έχουν δημιουργήσει νομικές διαφορές και πολιτικές εντάσεις μεταξύ των κρατών μελών.

Το νομικό πλαίσιο στην ΕΕ είναι ένα πολύπλοκο και δυναμικό σύστημα που αντλεί από διάφορες πηγές και ενώ έχει επιτύχει ένα σημαντικό βαθμό εναρμόνισης και ολοκλήρωσης, οι προκλήσεις εξακολουθούν να υφίστανται, από τα διαφορετικά νομικά συστήματα των κρατών μελών έως τρέχοντα ζητήματα όπως το Brexit, το κράτος δικαίου και η ψηφιοποίηση της κοινωνίας. Το νομικό καθεστώς της ΕΕ συνεχίζει να εξελίσσεται, διαμορφωμένο από τη δέσμευσή της στις κοινές αξίες, τη συνεργασία και το κράτος δικαίου.

4.2. Οικοδόμηση ανθεκτικότητας: Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο

Σε έναν όλο και πιο διασυνδεδεμένο κόσμο, η Ευρωπαϊκή Ένωση (ΕΕ) αναγνωρίζει την κρίσιμη σημασία της ασφάλειας στον κυβερνοχώρο. Με την ψηφιοποίηση να διαπερνά όλες τις πτυχές της κοινωνίας, η ΕΕ έχει αναπτύξει μια ολοκληρωμένη στρατηγική

[119] European Commission. (2023). *The EU-UK Trade and Cooperation Agreement*. Διαθέσιμο στο https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en
[120] European Union (2023). *Rule of Law*. Διαθέσιμο στο https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en
[121] European Union Agency for Cybersecurity. (ENISA) (2023). *NIS Directive*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/nis-directive

κυβερνοασφάλειας για την προστασία των ψηφιακών υποδομών, των δεδομένων και των πολιτών της από τις απειλές στον κυβερνοχώρο.

Η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο είναι ένα πλαίσιο που περιγράφει την προσέγγιση της ΕΕ για τη διασφάλιση της ασφάλειας και της ανθεκτικότητας του κυβερνοχώρου της. Η στρατηγική, η οποία παρουσιάστηκε για πρώτη φορά το 2013, επικαιροποιήθηκε το 2020 και τροποποιήθηκε το 2023, αποσκοπεί στην αντιμετώπιση του εξελισσόμενου τοπίου των απειλών και των τρωτών σημείων στον κυβερνοχώρο.[122] Περιλαμβάνει τρεις βασικές συνιστώσες:

- Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγεσία στον κυβερνοχώρο:

  Η ΕΕ εστιάζει στην ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο των υποδομών ζωτικής σημασίας, των οργανισμών και των ατόμων. Η ανθεκτικότητα στον κυβερνοχώρο περιλαμβάνει την ικανότητα αντίστασης, αντίδρασης και ανάκαμψης από επιθέσεις στον κυβερνοχώρο, διατηρώντας παράλληλα τη διαθεσιμότητα και την ακεραιότητα των συστημάτων και των δεδομένων. Στοχεύει σε τεχνολογική κυριαρχία ενθαρρύνοντας και επενδύοντας στην έρευνα και την καινοτομία στον τομέα της ασφάλειας.[123]

- Επιχειρησιακή ικανότητα πρόληψης αποτροπής και αντίδρασης:

  Η στρατηγική υπογραμμίζει την ανάγκη για ένα ισχυρό πλαίσιο αποτροπής και αντίδρασης που θα αποτρέπει τους κακόβουλους φορείς από το να επιδίδονται σε κυβερνοεπιθέσεις κατά των κρατών μελών της ΕΕ. Αυτό περιλαμβάνει την ικανότητα απόδοσης κυβερνοεπιθέσεων και ανάλογης αντίδρασης αλλά και απάντησης σε στρατηγικό αλλά και επιχειρησιακό επίπεδο.

- Συνεργασία για την προώθηση ενός παγκόσμιου και ανοιχτού κυβερνοχώρου:

  Προβλέπει τη προώθηση παγκόσμιων κανόνων για την αντιμετώπιση των κυβερνοαπειλών μέσα από τη διεθνή συνεργασία. Αναγνωρίζοντας τον παγκόσμιο χαρακτήρα των απειλών στον κυβερνοχώρο, η ΕΕ συνεργάζεται με διεθνείς εταίρους για την προώθηση κανόνων, αρχών και κανόνων για υπεύθυνη συμπεριφορά στον κυβερνοχώρο. Έτσι, η ΕΕ προσπαθεί να διαμορφώσει διεθνείς νόρμες και κανόνες για υπεύθυνη συμπεριφορά στον κυβερνοχώρο. Υποστηρίζει

[122] European Commission. (2023). *The Cybersecurity Strategy*. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[123] European Commission. (2023). *Enhancing EU Resilience*. Διαθέσιμο στο https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3992

την τήρηση αρχών όπως η προστασία των υποδομών ζωτικής σημασίας και η ειρηνική επίλυση των διαφορών.[124]

Στο πλαίσιο αυτό, η ΕΕ επιδιώκει να ενισχύσει το νομικό της πλαίσιο με την επικαιροποίηση και την εναρμόνιση της νομοθεσίας για την ασφάλεια στον κυβερνοχώρο σε όλα τα κράτη μέλη. Αυτό περιλαμβάνει τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) και την οδηγία για τα Συστήματα Δικτύων και Πληροφοριών (NIS και NIS2).[125]

Η φιλοδοξία της να δημιουργήσει έναν ασφαλή και προστατευμένο κυβερνοχώρο επεκτείνεται στο ρόλο της ως διεθνούς ηγέτη στον τομέα της ασφάλειας στον κυβερνοχώρο. Η ανθεκτικότητα, σε αυτό το πλαίσιο, αναφέρεται στην ικανότητα απορρόφησης, προσαρμογής και αποτελεσματικής ανάκαμψης από επιθέσεις στον κυβερνοχώρο. Σηματοδοτεί τη δέσμευση της ΕΕ όχι μόνο να προστατεύσει τα δικά της ψηφιακά περιουσιακά στοιχεία, αλλά και να συμβάλει στην παγκόσμια ανθεκτικότητα της κυβερνοασφάλειας. Αναλαμβάνοντας ηγετικό ρόλο, η ΕΕ προωθεί ενεργά μια συλλογική προσέγγιση για την ασφάλεια στον κυβερνοχώρο στη διεθνή σκηνή.[126]

Η έρευνα της Sarah Backman, όπως παρουσιάζεται στο "Risk vs. threat-based cybersecurity: the case of the EU", αναδεικνύει την προσέγγιση της ΕΕ για την αξιολόγηση και την αντιμετώπιση των προκλήσεων της κυβερνοασφάλειας. Η διάκριση μεταξύ της ασφάλειας στον κυβερνοχώρο με βάση τον κίνδυνο - και της ασφάλειας στον κυβερνοχώρο με βάση τις απειλές, είναι ζωτικής σημασίας για την κατανόηση της στρατηγικής της ΕΕ. Η προσέγγιση με βάση τον κίνδυνο αξιολογεί τα τρωτά σημεία και τις πιθανές επιπτώσεις τους, εστιάζοντας στην πρόληψη και τον μετριασμό. Η ΕΕ, όπως προκύπτει από την έρευνα της Backman, τείνει να δώσει έμφαση σε μια προσέγγιση που βασίζεται στην απειλή, η οποία λαμβάνει υπόψη τις πραγματικές απειλές στον κυβερνοχώρο και τους αντιπάλους. Η προσέγγιση αυτή επιτρέπει στην ΕΕ να προσαρμόζει τα αμυντικά της μέτρα, να δίνει προτεραιότητα στις αναδυόμενες απειλές και να κατανέμει τους πόρους αποτελεσματικότερα. Με την υιοθέτηση ενός μοντέλου

---

[124] European Union External Action. (2023). *EU cyber diplomacy*. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[125] European Commission. (2018). *Regulation (EU) 2018/1724* of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012. Διαθέσιμο στο https://eur-lex.europa.eu/eli/reg/2018/1724/oj

[126] Dunn Cavelty, M. (2013). A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers*, 23.

βασισμένου στις απειλές, η ΕΕ μεγιστοποιεί την ετοιμότητα και τις δυνατότητες αντίδρασής της απέναντι στους εξελισσόμενους κινδύνους στον κυβερνοχώρο.[127]

Η ΕΕ συμμετέχει ενεργά σε συνεργατικές προσπάθειες με διεθνείς εταίρους, οργανισμούς και ενδιαφερόμενους φορείς για την ενίσχυση της παγκόσμιας κυβερνοασφάλειας. Συμμετέχοντας σε κοινές πρωτοβουλίες και συμφωνίες ανταλλαγής πληροφοριών, η ΕΕ επεκτείνει την εμβέλεια και την επιρροή της στη διαφύλαξη του κυβερνοχώρου. Η έμφαση σε μια προσέγγιση με πολλούς ενδιαφερόμενους φορείς, στην οποία συμμετέχουν κυβερνήσεις, ο ιδιωτικός τομέας, η κοινωνία των πολιτών και ο ακαδημαϊκός κόσμος, επιτρέπει μια ολιστική και χωρίς αποκλεισμούς στρατηγική. Η ΕΕ αναγνωρίζει ότι η συλλογική ασφάλεια στον κυβερνοχώρο μπορεί να επιτευχθεί μόνο μέσω της συνολικής συνεργασίας και δέσμευσης με όλους τους σχετικούς φορείς.

Η έρευνα της Backman επισημαίνει τη σημασία της καινοτομίας στην κυβερνοασφάλεια. Οι επενδύσεις της ΕΕ στην έρευνα και την ανάπτυξη ευθυγραμμίζονται με αυτή την προοπτική. Με την προώθηση της καινοτομίας, η ΕΕ προάγει συνεχώς τις ικανότητές της στον τομέα της κυβερνοασφάλειας. Αυτή η εστίαση σε τεχνολογίες, πρακτικές και λύσεις αιχμής διασφαλίζει ότι η ΕΕ παραμένει πρωτοπόρος της ασφάλειας στον κυβερνοχώρο. Η συνεργασία μεταξύ του ακαδημαϊκού χώρου, του ιδιωτικού τομέα και των κυβερνητικών ιδρυμάτων οδηγεί σε καινοτόμες λύσεις που μπορούν να αντιμετωπίσουν αποτελεσματικά τις νέες και αναδυόμενες απειλές στον κυβερνοχώρο.[128]

4.3. ENISA - Διασφάλιση των ευρωπαϊκών δικτύων και πληροφοριών

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) διαδραματίζει κρίσιμο ρόλο στην ασφάλεια των ευρωπαϊκών δικτύων και πληροφοριών σε έναν ολοένα εξελισσόμενο κόσμο. Ο ENISA ιδρύθηκε το 2004, τη παρούσα στιγμή εδρεύει στο Χαλάνδρι Αττικής στην Ελλάδα και έχει εξελιχθεί σε βασικό παράγοντα για την ενίσχυση της ανθεκτικότητας της Ευρωπαϊκής Ένωσης (ΕΕ) και των κρατών μελών της στον κυβερνοχώρο.

---

[127] Backman S. (2023) Risk vs. threat-based cybersecurity: the case of the EU, *European Security*, 32:1, Σελ. 85-103

[128] Όπ.π.

Ένας από τους πρωταρχικούς στόχους του ENISA είναι η παροχή εμπειρογνωμοσύνης και υποστήριξης στα κράτη μέλη της ΕΕ για την ενίσχυση των ικανοτήτων τους στον τομέα της κυβερνοασφάλειας. Ο ENISA συνεργάζεται στενά με τις εθνικές αρχές, τους ενδιαφερόμενους φορείς του κλάδου και άλλους οργανισμούς κυβερνοασφάλειας για να διευκολύνει τη συνεργασία και την ανταλλαγή πληροφοριών. Αυτή η συνεργατική προσέγγιση επιτρέπει την ανάπτυξη αποτελεσματικών στρατηγικών και πρακτικών κυβερνοασφάλειας που ωφελούν ολόκληρη την κοινότητα της ΕΕ.[129]

Το έργο του ENISA περιλαμβάνει διάφορους τομείς της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των πληροφοριών σχετικά με τις απειλές, της διαχείρισης κινδύνων, της αντιμετώπισης περιστατικών και της προστασίας των υποδομών ζωτικής σημασίας. Παραμένοντας στην πρώτη γραμμή των αναδυόμενων απειλών και τρωτών σημείων στον κυβερνοχώρο, ο ENISA βοηθά τα κράτη μέλη να προσαρμόζονται και να ανταποκρίνονται αποτελεσματικά στις εξελισσόμενες προκλήσεις.[130]

Ένας άλλος κρίσιμος ρόλος του ENISA είναι η προώθηση και η διευκόλυνση της ευαισθητοποίησης και της ανταλλαγής γνώσεων στον τομέα της κυβερνοασφάλειας σε ολόκληρη την ΕΕ. Αυτό περιλαμβάνει τη διοργάνωση εργαστηρίων, εκπαιδευτικών σεμιναρίων και εκστρατειών ευαισθητοποίησης που απευθύνονται τόσο στους επαγγελματίες της κυβερνοασφάλειας όσο και στο ευρύ κοινό. Με την ευαισθητοποίηση και την παροχή εκπαιδευτικών πόρων, ο ENISA συμβάλλει σε μια πιο ενημερωμένη και προσεκτική ευρωπαϊκή κοινωνία.[131]

Ο ENISA διαδραματίζει επίσης ζωτικό ρόλο στην ανάπτυξη και εφαρμογή των πολιτικών και της νομοθεσίας της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Η εμπειρογνωμοσύνη του οργανισμού συμβάλλει στη δημιουργία κανονιστικών πλαισίων που ενισχύουν την ασφάλεια στον κυβερνοχώρο σε ολόκληρη την ΕΕ. Για παράδειγμα, ο ENISA διαδραμάτισε σημαντικό ρόλο στη θέσπιση της οδηγίας για τα συστήματα δικτύων και πληροφοριών (NIS), η οποία καθορίζει απαιτήσεις κυβερνοασφάλειας για

[129] European Union Agency for Cybersecurity (ENISA). (2023). *About ENISA*. Διαθέσιμο στο https://www.enisa.europa.eu/about-enisa

[130] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. Διαθέσιμο στο https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[131] European Union Agency for Cybersecurity (ENISA). (2021). *Raising awareness of Cybersecurity*. Διαθέσιμο στο https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών.[132]

Επιπλέον, ο ENISA χρησιμεύει ως κόμβος πληροφοριών και βέλτιστων πρακτικών για την ασφάλεια στον κυβερνοχώρο. Ο οργανισμός διατηρεί ένα αποθετήριο πόρων, κατευθυντήριων γραμμών και εκθέσεων που βοηθούν οργανισμούς και άτομα να βελτιώσουν τη στάση τους στον τομέα της κυβερνοασφάλειας. Οι πόροι αυτοί καλύπτουν ένα ευρύ φάσμα θεμάτων, από την αντιμετώπιση περιστατικών έως την ασφαλή υπολογιστική νέφους.[133]

Τα τελευταία χρόνια, ο ENISA έχει επεκτείνει την εστίασή του για να αντιμετωπίσει τις αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας, όπως το Διαδίκτυο των πραγμάτων (IoT) και τα δίκτυα 5G. Με τον πολλαπλασιασμό των συσκευών IoT και την ανάπτυξη υποδομών 5G, αναδύθηκαν νέοι κίνδυνοι για την κυβερνοασφάλεια. Ο ENISA παρέχει καθοδήγηση και συστάσεις για τη διασφάλιση της ασφαλούς υιοθέτησης αυτών των τεχνολογιών, διασφαλίζοντας τα ευρωπαϊκά δίκτυα και τις πληροφορίες.[134]

Η δέσμευση του ENISA για την ασφάλεια των ευρωπαϊκών δικτύων και πληροφοριών υποστηρίζεται από τη στενή συνεργασία του με τους ενδιαφερόμενους φορείς τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Αυτή η πολυμερής προσέγγιση προάγει ένα ολιστικό και χωρίς αποκλεισμούς οικοσύστημα κυβερνοασφάλειας που μπορεί να ανταποκριθεί αποτελεσματικά στις απειλές και τις προκλήσεις.[135]

Αξίζει επίσης να σημειωθεί ότι το τοπίο απειλών του ENISA χρησιμεύει ως ακρογωνιαίος λίθος του ετήσιου στρατηγικού χάρτη πορείας του ENISA. Περιγράφει τις κορυφαίες απειλές, τα τρωτά σημεία και τους αναδυόμενους κινδύνους στον κυβερνοχώρο που είναι πιθανό να αντιμετωπίσει η ΕΕ κατά το συγκεκριμένο έτος. Με τον εντοπισμό αυτών των προκλήσεων, ο ENISA είναι καλύτερα εξοπλισμένος για τη διαμόρφωση των προτεραιοτήτων του, την κατανομή των πόρων και την ανάπτυξη στρατηγικών που ενισχύουν την ανθεκτικότητα της Ευρωπαϊκής Ένωσης (ΕΕ) και των

---

[132] European Union Agency for Cybersecurity (ENISA). (2023). *NIS Directive*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/nis-directive

[133] European Union Agency for Cybersecurity (ENISA). (2023). *Publications*. Διαθέσιμο στο https://www.enisa.europa.eu/publications

[134] European Union Agency for Cybersecurity (ENISA). (2023). *Emerging Technologies*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

[135] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. Όπ.π.

κρατών μελών της στον κυβερνοχώρο.
Η δημοσίευση παρέχει μια βαθιά εμβάθυνση στους βασικούς τομείς εστίασης που ο ENISA προτίθεται να αντιμετωπίσει κατά το αντίστοιχο έτος. Αυτοί οι τομείς εστίασης είναι απαραίτητοι για την κατανόηση των επιχειρησιακών και πολιτικών στόχων του οργανισμού. Περιλαμβάνουν ένα ευρύ φάσμα απειλών στον κυβερνοχώρο, όπως οι αναδυόμενες τεχνολογίες, οι υποδομές ζωτικής σημασίας, η ανταλλαγή πληροφοριών και η αντιμετώπιση περιστατικών.
Το τοπίο απειλών του ENISA αξιοποιεί τις πληροφορίες για τις απειλές στον κυβερνοχώρο για να προσφέρει πολύτιμες πληροφορίες σχετικά με τις τακτικές, τις τεχνικές και τις διαδικασίες που χρησιμοποιούν οι κακόβουλοι φορείς. Αναλύοντας το εξελισσόμενο τοπίο απειλών, ο ENISA μπορεί να παρέχει στην ΕΕ και τα κράτη μέλη της κρίσιμες πληροφορίες σχετικά με τους δυνητικούς αντιπάλους στον κυβερνοχώρο, τα κίνητρά τους και τα εργαλεία που είναι πιθανό να χρησιμοποιήσουν. Αυτές οι πληροφορίες είναι ζωτικής σημασίας για την ανάπτυξη ισχυρών στρατηγικών άμυνας και την προληπτική αντιμετώπιση των απειλών στον κυβερνοχώρο.
Ένα από τα βασικά συμπεράσματα από το τοπίο απειλών του ENISA είναι ο αντίκτυπός του στην ανάπτυξη πολιτικής και στη διεθνή συνεργασία. Το έγγραφο υπογραμμίζει τη σημασία της συνεργασίας μεταξύ της ΕΕ, των κρατών μελών της και των διεθνών εταίρων για την αποτελεσματική αντιμετώπιση των προκλήσεων της κυβερνοασφάλειας. Θέτει τα θεμέλια για τη δημιουργία πλαισίων συνεργασίας, την ανταλλαγή βέλτιστων πρακτικών και τη διασφάλιση συντονισμένης αντιμετώπισης των απειλών στον κυβερνοχώρο σε παγκόσμια κλίμακα.
Το τοπίο απειλών του ENISA διαδραματίζει επίσης ζωτικό ρόλο στην ευαισθητοποίηση του κοινού και στην εκπαίδευση των ενδιαφερομένων σχετικά με τις εξελισσόμενες απειλές στον κυβερνοχώρο. Χρησιμεύει ως πολύτιμη πηγή για τους υπεύθυνους χάραξης πολιτικής, τους ηγέτες του κλάδου, τους επαγγελματίες της ασφάλειας και το ευρύ κοινό, παρέχοντας σαφή κατανόηση των πιεστικών ζητημάτων κυβερνοασφάλειας και των μέτρων που λαμβάνονται για την αντιμετώπισή τους.[136]
Συνεπώς, το ENISA Threat Landscape 2023 αποτελεί απαραίτητο εργαλείο για τις προσπάθειες της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας. Αυτές οι ετήσιες δημοσιεύσεις προσφέρουν πολύτιμες γνώσεις, καθοδήγηση πολιτικής και

[136] Όπ.π.

πληροφορίες για την αντιμετώπιση του ταχέως μεταβαλλόμενου τοπίου ψηφιακών απειλών. Παραμένοντας συντονισμένοι με αυτές τις εκθέσεις, η ΕΕ και τα κράτη μέλη της μπορούν να ενισχύσουν συλλογικά την άμυνά τους στον κυβερνοχώρο και να παραμείνουν ανθεκτικοί στις ολοένα αυξανόμενες απειλές.

Εν κατακλείδι, ο ENISA διαδραματίζει ζωτικό ρόλο στη διασφάλιση των ευρωπαϊκών δικτύων και πληροφοριών παρέχοντας εμπειρογνωμοσύνη, προωθώντας τη συνεργασία, αυξάνοντας την ευαισθητοποίηση και διαμορφώνοντας τις πολιτικές της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Οι συνεισφορές του είναι ουσιαστικές για την ενίσχυση της ανθεκτικότητας των κρατών μελών της ΕΕ στις απειλές στον κυβερνοχώρο και τη διασφάλιση της προστασίας των υποδομών ζωτικής σημασίας και των ψηφιακών υπηρεσιών. Να σημειωθεί ότι τον Απρίλιο του 2023 προτάθηκε από την Επιτροπή η απόδοση μεγαλύτερων ευθυνών στον ENISA μέσω τροποποίησης του «Ευρωπαϊκού νόμου για την ασφάλεια στον Κυβερνοχώρο» επιτρέποντας τη μελλοντική έγκριση ευρωπαϊκών συστημάτων πιστοποίησης για τις «διαχειριζόμενες υπηρεσίες ασφάλειας» που θα καλύπτουν τομείς όπως η αντιμετώπιση συμβάντων, οι δοκιμές διείσδυσης και οι έλεγχοι ασφάλειας.[137]

4.4. Κανονισμός 2019/881: Ενίσχυση των μέτρων κυβερνοασφάλειας

Ο κανονισμός (ΕΕ) 2019/881, γνωστός και ως "νόμος για την ασφάλεια στον κυβερνοχώρο", αποτελεί σημαντικό βήμα προς τα εμπρός για την ενίσχυση των μέτρων ασφάλειας στον κυβερνοχώρο εντός της Ευρωπαϊκής Ένωσης (ΕΕ). Ο εν λόγω κανονισμός, που τέθηκε σε ισχύ το 2019, αποσκοπεί στην ενίσχυση της ανθεκτικότητας της ΕΕ στον κυβερνοχώρο και στη βελτίωση της ικανότητάς της να ανταποκρίνεται αποτελεσματικά σε απειλές και περιστατικά στον κυβερνοχώρο.[138]

Μία από τις βασικές πτυχές του κανονισμού 2019/881 είναι η δημιουργία ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας. Το πλαίσιο αυτό παρέχει μια τυποποιημένη προσέγγιση για την πιστοποίηση της ασφάλειας των προϊόντων,

[137] Ευρωπαϊκή Επιτροπή, (2023), *Η πράξη της ΕΕ για την ασφάλεια στον Κυβερνοχώρο*, διαθέσιμο στο https://digital-strategy.ec.europa.eu/el/policies/cybersecurity-act

[138] European Parliament and Council. (2019). *Regulation (EU) 2019/881* of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Διαθέσιμο στο https://eur-lex.europa.eu/eli/reg/2019/881/oj

υπηρεσιών και διαδικασιών τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ). Με την εισαγωγή ενός κοινού ευρωπαϊκού πλαισίου, ο κανονισμός απλοποιεί τη διαδικασία πιστοποίησης, προάγει την εμπιστοσύνη στα προϊόντα και τις υπηρεσίες ΤΠΕ και διευκολύνει το διασυνοριακό ψηφιακό εμπόριο.[139]

Ωστόσο, η εστίαση του εν λόγω κανονισμού εκτείνεται πέρα από τις πιστοποιήσεις κυβερνοασφάλειας. Υπογραμμίζει την επιτακτική ανάγκη για ενισχυμένη συνεργασία και συντονισμό μεταξύ των κρατών μελών της ΕΕ και των αρχών επιβολής του νόμου για την αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας μεγάλης κλίμακας. Για την επίτευξη αυτού του στόχου, η ΕΕ έχει δρομολογήσει τη δημιουργία κοινών μονάδων κυβερνοασφάλειας, συγκεντρώνοντας τεχνογνωσία από όλα τα κράτη μέλη. Οι εν λόγω μονάδες διαδραματίζουν κρίσιμο ρόλο στην αντιμετώπιση σημαντικών περιστατικών στον κυβερνοχώρο, διασφαλίζοντας την ενιαία και συντονισμένη προσέγγιση στη διαχείριση και τον μετριασμό των απειλών.[140][141]

Ένα αξιοσημείωτο παράδειγμα αυτής της πρωτοβουλίας είναι η δημιουργία της κοινής μονάδας για τον κυβερνοχώρο. Η μονάδα αυτή αποτελεί κρίσιμη συνιστώσα της συνολικής στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, με στόχο την αντιμετώπιση σημαντικών περιστατικών ασφάλειας. Λειτουργεί με πρωταρχικό στόχο την ταχεία και αποτελεσματική αντιμετώπιση απειλών και επιθέσεων μεγάλης κλίμακας στον κυβερνοχώρο. Η Κοινή Κυβερνομονάδα αξιοποιεί τις συλλογικές γνώσεις και τους πόρους των κρατών μελών, ενισχύοντας έτσι τη συνολική στάση της ΕΕ στον τομέα της κυβερνοασφάλειας.[142]

Επιπλέον, η οδηγία 2022/2555 (NIS2 Directive) περιγράφει το πλαίσιο συνεργασίας μεταξύ των κρατών μελών της ΕΕ και των αρχών επιβολής του νόμου για την αντιμετώπιση των απειλών στον κυβερνοχώρο και τη διασφάλιση της ασφάλειας στον κυβερνοχώρο. Η εν λόγω οδηγία παρέχει τη νομική βάση για τη σύσταση και τη

---

[139] European Union Agency for Cybersecurity (ENISA). (2023). *Certification*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/certification

[140] Cimpanu C. (2021), EU announces joint cyber unit to respond to large-scale security incidents. *The Record.* Διαθέσιμο στο https://therecord.media/eu-announces-joint-cyber-unit-to-respond-to-large-scale-security-incidents

[141] European Parliament and Council. (2022) *Directive (EU) 2022/2555* of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1697797857660

[142] Ευρωπαϊκή Επιτροπή, (2023*), Κοινή Κυβερνομονάδα*. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/el/policies/joint-cyber-unit

λειτουργία βασικών οντοτήτων, όπως οι ομάδες-κόμβοι των αρχών επιβολής του νόμου για την ασφάλεια στον κυβερνοχώρο (EU CyCLONe) και οι ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT)[143]. Η EU CyCLONe[144] συμβάλλει καθοριστικά στο συντονισμό των δραστηριοτήτων επιβολής του νόμου σε ολόκληρη την ΕΕ και στην ενίσχυση της συνεργασίας για την αντιμετώπιση διαφόρων προκλήσεων στον τομέα της ασφάλειας στον κυβερνοχώρο. Αποτελείται από εκπροσώπους των αρχών διαχείρισης κρίσεων των κρατών-μελών, ενώ σε περιστατικά μαζικής κλίμακας κυβερνοασφάλειας ή σημαντικού αντικτύπου, συμμετέχει και η ίδια η Επιτροπή. Σε διαφορετικές περιπτώσεις, η Επιτροπή έχει το ρόλο του παρατηρητή. Τα κύρια καθήκοντα της EU CyCLONe εντοπίζονται:

- στην υποστήριξη της συντονισμένης διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας σε επιχειρησιακό επίπεδο,
- στην τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των θεσμών και αρχών των κρατών-μελών,
- στη εκπόνηση προτάσεων για το μετριασμό των επιπτώσεων
- στο συντονισμό της διαχείρισης περιστατικών και κρίσεων στο κυβερνοχώρο
- στην υποστήριξη λήψης αποφάσεων σε πολιτικό επίπεδο σε σχέση με περιστατικά και κρίσης κυβερνοασφάλειας μέσω πραγματογνωμοσύνης
- συζητήσεις και προτάσεις κατόπιν αιτήματος κράτους-μέλους για εθνικά σχέδια μεγάλης κλίμακας για περιστατικά κυβερνοασφάλειας και διαχείρισης κρίσεων.[145]

Ακολούθως, οι CSIRT διαδραματίζουν ζωτικό ρόλο στην ενίσχυση της ασφάλειας στον κυβερνοχώρο παρέχοντας υπηρεσίες αντιμετώπισης περιστατικών και μετριασμού των επιπτώσεων. Χρησιμεύουν ως κεντρικός πόρος για τους οργανισμούς και τις αρχές για την ανταλλαγή πληροφοριών, τη διαχείριση και την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοασφάλειας. Βασική λειτουργία τους είναι η συντονισμένη αναγνώριση και αποκάλυψη τρωτών σημείων που θα μπορούσαν να επιφέρουν ένα σημαντικό αντίκτυπο σε οντότητες ή φορείς σε περισσότερα από ένα κράτη-μέλη. Η σύσταση και λειτουργία των CSIRT στα κράτη μέλη της ΕΕ είναι αναπόσπαστο μέρος

[143] Computer Security Incident Response Team
[144] European cyber crisis liaison organization network (EU-CyCLONe)
[145] European Union Agency for Cybersecurity (ENISA). (2022*). EU CyCLONe*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/incident-response/cyclone

της ευρύτερης στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο, διασφαλίζοντας ότι τα περιστατικά κυβερνοασφάλειας αντιμετωπίζονται συνολικά και συνεργατικά.[146]

Συμπερασματικά, ο κανονισμός (ΕΕ) 2019/881, μαζί με την οδηγία 2022/2555, υπογραμμίζει τη δέσμευση της ΕΕ να ενισχύσει τις ικανότητές της στον τομέα της κυβερνοασφάλειας και να βελτιώσει την ανθεκτικότητά της έναντι των απειλών στον κυβερνοχώρο. Αυτά τα νομοθετικά μέτρα, σε συνδυασμό με πρωτοβουλίες όπως η Κοινή Κυβερνομονάδα, το CyCLONE και οι CSIRT, σηματοδοτούν μια ολοκληρωμένη προσέγγιση για την ασφάλεια στον κυβερνοχώρο, δίνοντας έμφαση στη συνεργασία, τον συντονισμό και την ταχεία αντίδραση για την προστασία του ψηφιακού τοπίου της ΕΕ.[147]

4.5. Προώθηση της συνεργασίας: Συμπράξεις και πρωτοβουλίες της ΕΕ

Η προώθηση της συνεργασίας αποτελεί κεντρικό στοιχείο της προσέγγισης της Ευρωπαϊκής Ένωσης (ΕΕ) για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Απέναντι στις εξελισσόμενες απειλές και προκλήσεις στον κυβερνοχώρο, η ΕΕ έχει συμμετάσχει ενεργά σε συμπράξεις και πρωτοβουλίες για την προώθηση της συνεργασίας μεταξύ των κρατών μελών, των διεθνών οργανισμών και του ιδιωτικού τομέα.

Μία από τις κύριες πρωτοβουλίες της ΕΕ για την προώθηση της συνεργασίας και της εμπιστοσύνης είναι η Ομάδα Συνεργασίας της ΕΕ για την Κυβερνοασφάλεια (CSCG). Η CSCG χρησιμεύει ως κεντρικό φόρουμ για τα κράτη μέλη προκειμένου να ανταλλάσσουν πληροφορίες, βέλτιστες πρακτικές και να συντονίζουν τις αντιδράσεις τους σε περιστατικά στον κυβερνοχώρο. Διαδραματίζει κρίσιμο ρόλο στην ενίσχυση

[146] CSIRTs Network (2023), *Intro*, διαθέσιμο στο https://csirtsnetwork.eu/#:~:text=The%20mission%20of%20the%20European,exchange%20best%20practices%20in%20incident

[147] Cyberwatching.eu. (n.d.). *European Commission Sets Up Joint Cyber Unit to Respond to Large-Scale Cyber Incidents.* Διαθέσιμο στο https://www.cyberwatching.eu/news-events/news/european-commission-sets-joint-cyber-unit-respond-large-scale-cyber-incidents

της επίγνωσης της κατάστασης και στη διευκόλυνση της ενιαίας αντίδρασης της ΕΕ στις απειλές στον κυβερνοχώρο[148].

Επιπλέον, η ΕΕ προωθεί τη συνεργασία μέσω της δέσμευσής της με διεθνείς εταίρους. Η ΕΕ συμμετέχει ενεργά σε διαλόγους και πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο σε παγκόσμιο επίπεδο. Ένα αξιοσημείωτο παράδειγμα είναι η συνεργασία της ΕΕ με την ομάδα κυβερνητικών εμπειρογνωμόνων των Ηνωμένων Εθνών για τις εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας (UN GGE). Η ΕΕ συμβάλλει στη διαμόρφωση διεθνών κανόνων και κανόνων για υπεύθυνη συμπεριφορά στον κυβερνοχώρο μέσω τέτοιων πρωτοβουλιών.[149]

Ακόμη, οι προσπάθειες συνεργασίας της ΕΕ επεκτείνονται σε συμπράξεις δημόσιου και ιδιωτικού τομέα. Η ΕΕ αναγνωρίζει τον ζωτικό ρόλο του ιδιωτικού τομέα στην ασφάλεια στον κυβερνοχώρο και συνεργάζεται ενεργά με τους ενδιαφερόμενους φορείς του κλάδου για την ενίσχυση της ανθεκτικότητας των υποδομών ζωτικής σημασίας και των ψηφιακών υπηρεσιών. Οι πρωτοβουλίες συνεργασίας με τη βιομηχανία περιλαμβάνουν την ανταλλαγή πληροφοριών, την ανταλλαγή πληροφοριών σχετικά με απειλές και κοινές ασκήσεις κυβερνοασφάλειας.[150]

Η ΕΕ υποστηρίζει επίσης την έρευνα και την καινοτομία ως μέρος της στρατηγικής της για τη συνεργασία. Μέσω προγραμμάτων όπως το Horizon Europe, η ΕΕ χρηματοδοτεί ερευνητικά έργα για την ασφάλεια στον κυβερνοχώρο που προωθούν την καινοτομία και την ανάπτυξη τεχνολογιών αιχμής. Οι συνεργατικές ερευνητικές προσπάθειες φέρνουν σε επαφή ακαδημαϊκούς, βιομηχανικούς και δημόσιους οργανισμούς για την αντιμετώπιση αναδυόμενων προκλήσεων στον τομέα της κυβερνοασφάλειας.[151]

Μια άλλη κρίσιμη πτυχή της προώθησης της συνεργασίας είναι η δέσμευση της ΕΕ για τη δημιουργία ικανοτήτων. Η ΕΕ συνεργάζεται με τις χώρες εταίρους, ιδίως εκείνες που βρίσκονται στη γειτονιά της, για να ενισχύσει τις ικανότητές τους στον τομέα της κυβερνοασφάλειας. Αυτό περιλαμβάνει την παροχή τεχνικής βοήθειας, την κατάρτιση

---

[148] European Union Agency for Cybersecurity (ENISA). (2021). *Cyber Crisis Cooperation*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/cyber-crisis-cooperation

[149] European Union External Action. (2023). *EU cyber diplomacy*. Όπ.π.

[150] European Union Agency for Cybersecurity (ENISA). (2023). *Public-Private Partnerships*. Διαθέσιμο στο https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps

[151] European Commission. (2023). *Horizon Europe*. Διαθέσιμο στο https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

και την ανταλλαγή εμπειρογνωμοσύνης για να βοηθήσει τις χώρες εταίρους να ενισχύσουν την ανθεκτικότητά τους στον κυβερνοχώρο.[152]

Επιπλέον, η ΕΕ δίνει μεγάλη έμφαση στην προώθηση της ανάπτυξης διεθνών κανόνων και μέτρων οικοδόμησης εμπιστοσύνης. Οι προσπάθειες αυτές αποσκοπούν στη μείωση του κινδύνου συγκρούσεων στον κυβερνοχώρο και στην ενίσχυση της σταθερότητας. Υποστηρίζει αρχές όπως η προστασία των υποδομών ζωτικής σημασίας, η ειρηνική επίλυση των διαφορών και η υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο.[153]

Συνεχίζοντας τη διερεύνηση των διεθνών συμπράξεων στον τομέα της ασφάλειας στον κυβερνοχώρο, η Ευρωπαϊκή Ένωση (ΕΕ) βρίσκεται στην πρώτη γραμμή των προσπαθειών για την ενίσχυση της παγκόσμιας άμυνας στον κυβερνοχώρο. Η δέσμευση της ΕΕ για την προώθηση της διεθνούς συνεργασίας εκτείνεται πέρα από τα σύνορά της και περιλαμβάνει συνεργασίες με βασικούς διεθνείς οργανισμούς, όπως τον Οργανισμό του Βορειοατλαντικού Συμφώνου (NATO).[154]

Η εταιρική σχέση ΕΕ-NATO στον τομέα της ασφάλειας στον κυβερνοχώρο εδράζεται στην πεποίθηση ότι με τη συνεργασία τους οι δύο οντότητες μπορούν να ενισχύσουν την ανθεκτικότητα και την ασφάλεια των κρατών μελών τους αλλά και της ευρύτερης διεθνούς κοινότητας. Η στρατηγική ευθυγράμμιση μεταξύ της ΕΕ και του NATO είναι ζωτικής σημασίας για την αποτελεσματική αντιμετώπιση των πολύπλοκων και εξελισσόμενων απειλών στον κυβερνοχώρο.[155]

Στο πλαίσιο αυτής της εταιρικής σχέσης, έχουν αναδειχθεί διάφοροι βασικοί τομείς συνεργασίας. Οι τομείς αυτοί περιλαμβάνουν την ανταλλαγή πληροφοριών σχετικά με απειλές, την επίγνωση της κατάστασης, την αντιμετώπιση περιστατικών και την ανάπτυξη κοινών στρατηγικών για την αντιμετώπιση απειλών στον κυβερνοχώρο. Με την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών, η ΕΕ και το NATO στοχεύουν στη βελτίωση της συνολικής τους στάσης στον κυβερνοχώρο και στην ενίσχυση της ικανότητάς τους να ανταποκρίνονται γρήγορα σε περιστατικά στον κυβερνοχώρο.

---

[152] European Union External Action. (2023). *EU cyber diplomacy*. Όπ.π.

[153] Council of the European Union. (2023). *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox.* Διαθέσιμο στο https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

[154] Strategic Communications. (2023). European Union and NATO intensify cooperation in addressing cyber threats. *European External Action Service* Διαθέσιμο στο https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en

[155] Lete B., Pernik P. (2017), EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions, *Policy Brief GMF*. Διαθέσιμο στο https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf

Επιπλέον, η συνεργασία αυτή επεκτείνεται σε προσπάθειες δημιουργίας ικανοτήτων με στόχο να βοηθηθούν οι χώρες εταίροι, ιδίως εκείνες που βρίσκονται στη γειτονιά της ΕΕ, να ενισχύσουν την ανθεκτικότητά τους στον κυβερνοχώρο. Η τεχνική βοήθεια, τα προγράμματα κατάρτισης και οι πρωτοβουλίες ανταλλαγής γνώσεων αποτελούν βασικά στοιχεία αυτής της προσέγγισης για την ανάπτυξη ικανοτήτων. Η ΕΕ και το ΝΑΤΟ συνεργάζονται για να βοηθήσουν τις χώρες να αναπτύξουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας, συμβάλλοντας έτσι σε ένα ασφαλέστερο ψηφιακό περιβάλλον.

Η εταιρική σχέση μεταξύ της ΕΕ και του ΝΑΤΟ ευθυγραμμίζεται επίσης στενά με τις προσπάθειές τους να προωθήσουν διεθνείς κανόνες και υπεύθυνη συμπεριφορά στον κυβερνοχώρο. Με τη συνεργασία τους, οι δύο οργανισμοί μπορούν να υποστηρίξουν καλύτερα παγκόσμιες αρχές όπως η προστασία των υποδομών ζωτικής σημασίας, η ειρηνική επίλυση διαφορών και η υπεύθυνη κρατική συμπεριφορά στον ψηφιακό τομέα.[156]

Συμπερασματικά, η προώθηση της συνεργασίας με Οργανισμούς και Κράτη βρίσκεται στον πυρήνα της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Η συνεργατική προσέγγιση μεταξύ της ΕΕ και του ΝΑΤΟ αποτελεί μέρος μιας ευρύτερης δέσμευσης για την προώθηση της διεθνούς κυβερνοασφάλειας και της αμυντικής συνεργασίας. Με την ενεργό συνεργασία με διεθνείς εταίρους, την ανταλλαγή ζωτικών πληροφοριών, την στήριξη της έρευνας και της καινοτομίας, την ανάπτυξη διεθνών κανόνων και την υποστήριξη πρωτοβουλιών για την ανάπτυξη ικανοτήτων, η ΕΕ και το ΝΑΤΟ συμβάλλουν στις παγκόσμιες προσπάθειες διεθνούς σταθερότητας.

[156] NATO. (2023). *Cyber Defence*. Διαθέσιμο στο https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en

Συμπεράσματα

Στον τομέα της ασφάλειας στον κυβερνοχώρο, η Ευρωπαϊκή Ένωση (ΕΕ) έχει κάνει σημαντικά βήματα προόδου τα τελευταία χρόνια, αναγνωρίζοντας την ανάγκη να διασφαλίσει τα δίκτυα, τις πληροφορίες και τις ψηφιακές υποδομές της. Αυτή η ολοκληρωμένη διερεύνηση του τοπίου κυβερνοασφάλειας της ΕΕ υπογραμμίζει την πολύπλευρη προσέγγιση που έχει υιοθετήσει για την αντιμετώπιση των διαρκώς εξελισσόμενων κυβερνοαπειλών και προκλήσεων της ψηφιακής εποχής. Μέσω ενός συνδυασμού κανονισμών, πολιτικών, συμπράξεων και πρωτοβουλιών, η ΕΕ έχει επιμείνει στη δέσμευσή της για τη δημιουργία ενός πιο ασφαλούς και ανθεκτικού κυβερνοχώρου.

Ο κανονισμός 2019/881, κοινώς γνωστός ως νόμος για την ασφάλεια στον κυβερνοχώρο, αποτελεί ακρογωνιαίο λίθο των προσπαθειών της ΕΕ να ενισχύσει την άμυνά της στον κυβερνοχώρο. Με την εισαγωγή ενός ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας και την ενίσχυση του ρόλου του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), ο κανονισμός αυτός αποσκοπεί στην ενίσχυση της αξιοπιστίας των προϊόντων και υπηρεσιών τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ). Ανοίγει το δρόμο για μια εναρμονισμένη προσέγγιση στην πιστοποίηση της κυβερνοασφάλειας σε όλα τα κράτη μέλη της ΕΕ και εξορθολογίζει το διασυνοριακό ψηφιακό εμπόριο. Επιπλέον, η διευρυμένη εντολή του ENISA, συμπεριλαμβανομένου του ρόλου του στο συντονισμό των δραστηριοτήτων κυβερνοασφάλειας σε επίπεδο ΕΕ καθώς και η θεσμοθέτηση ομάδων όπως η EU CyCLONe και οι CSIRTs, συμβάλλουν σημαντικά στην προώθηση της μεγαλύτερης συνεργασίας, συνεννόησης και τελικά ασφάλειας μεταξύ των κρατών μελών.

Η δέσμευση της ΕΕ για την προώθηση της συνεργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο είναι εμφανής μέσω διαφόρων πρωτοβουλιών και συμπράξεων. Η ομάδα συνεργασίας της ΕΕ για την κυβερνοασφάλεια (CSCG) χρησιμεύει ως άξονας για τα κράτη μέλη για την ανταλλαγή πληροφοριών, βέλτιστων πρακτικών και τον συντονισμό των αντιδράσεων σε περιστατικά στον κυβερνοχώρο. Επιπλέον, η ΕΕ συνεργάζεται ενεργά με διεθνείς εταίρους, όπως η ομάδα κυβερνητικών εμπειρογνωμόνων των Ηνωμένων Εθνών, για τη διαμόρφωση παγκόσμιων κανόνων και κανόνων για υπεύθυνη συμπεριφορά στον κυβερνοχώρο. Αναγνωρίζοντας τον αναντικατάστατο ρόλο του ιδιωτικού τομέα στην ασφάλεια στον κυβερνοχώρο και

συνεργάζεται στενά με τους ενδιαφερόμενους φορείς του κλάδου. Η έρευνα και η καινοτομία, η δημιουργία ικανοτήτων και η ανάπτυξη διεθνών κανόνων υπογραμμίζουν περαιτέρω την πολύπλευρη προσέγγιση της ΕΕ στη συνεργασία.

Στον τομέα του εγκλήματος στον κυβερνοχώρο, η ΕΕ έχει επίσης λάβει σημαντικά μέτρα για την καταπολέμηση των αυξανόμενων απειλών κατά των πολιτών, των επιχειρήσεων και των υποδομών ζωτικής σημασίας. Το νομικό πλαίσιο της ΕΕ, συμπεριλαμβανομένου του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ), χρησιμεύει ως ισχυρή άμυνα κατά των παραβιάσεων των δεδομένων και των παραβιάσεων της ιδιωτικής ζωής. Επιπλέον, η ΕΕ έχει υιοθετήσει προληπτική στάση κατά του εγκλήματος στον κυβερνοχώρο, υποστηρίζοντας την έρευνα, την εκπαίδευση και τις εκστρατείες ευαισθητοποίησης. Η εταιρική σχέση της ΕΕ με τον ιδιωτικό τομέα είναι καθοριστικής σημασίας για την ενίσχυση της ανθεκτικότητας της κυβερνοασφάλειας.

Η κατανόηση του περιγράμματος του deep web και του dark web παρέχει πληροφορίες σχετικά με τις προκλήσεις που θέτουν οι παράνομες δραστηριότητες και οι απειλές στον κυβερνοχώρο που ευδοκιμούν σε αυτές τις κρυφές γωνιές του διαδικτύου. Παρόλο που ο σκοτεινός ιστός εξακολουθεί να αποτελεί πρόσφορο έδαφος για εγκληματίες του κυβερνοχώρου και παράνομες δραστηριότητες, είναι σημαντικό να αναγνωριστεί ότι δεν είναι όλες οι δραστηριότητες σε αυτό το πεδίο εγγενώς κακόβουλες. Ο βαθύς ιστός, ο οποίος αποτελεί ένα τεράστιο τμήμα του διαδικτύου, αποτελείται κυρίως από νόμιμο και μη ευρετηριασμένο περιεχόμενο. Η πλοήγηση στις πολυπλοκότητες αυτών των κρυφών χώρων απαιτεί μια διαφοροποιημένη προσέγγιση που κάνει διάκριση μεταξύ κακόβουλων φορέων και νόμιμων χρηστών.

Ο κυβερνοπόλεμος θέτει ένα μοναδικό σύνολο προκλήσεων στην ψηφιακή εποχή, υπερβαίνοντας τα γεωγραφικά σύνορα και τα συμβατικά πολεμικά παραδείγματα. Τα έθνη υποχρεώνονται να παλέψουν με τις πολυπλοκότητες της αποτροπής στον κυβερνοχώρο, της απόδοσης και των πιθανών συνεπειών των επιθετικών επιχειρήσεων στον κυβερνοχώρο. Για την πλοήγηση σε αυτό το εξελισσόμενο τοπίο, η διεθνής συνεργασία, η ανάπτυξη κανόνων και η ενίσχυση των αμυντικών δυνατοτήτων φαντάζει επιτακτική ανάγκη. Η Ευρωπαϊκή Ένωση έχει συμμετάσχει ενεργά στη συζήτηση γύρω από τον κυβερνοπόλεμο, συμβάλλοντας στις διεθνείς προσπάθειες για

τη θέσπιση κανόνων εμπλοκής και την προώθηση της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο.

Οι υποδομές ζωτικής σημασίας αποτελούν τη ραχοκοκαλιά της σύγχρονης κοινωνίας, γεγονός που τις καθιστά ελκυστικό στόχο για κυβερνοεπιθέσεις. Η ΕΕ έχει αναγνωρίσει την ανάγκη προστασίας αυτών των ζωτικών συστημάτων μέσω της οδηγίας για την προστασία των υποδομών ζωτικής σημασίας και της συνεργασίας με τον ιδιωτικό τομέα. Προσδιορίζοντας και ορίζοντας οντότητες ζωτικής σημασίας, η ΕΕ διασφαλίζει ότι αυτές τηρούν ισχυρά πρότυπα κυβερνοασφάλειας, μειώνοντας τα τρωτά σημεία και ενισχύοντας την ανθεκτικότητα.

Στο ευρύτερο πλαίσιο της εκπαίδευσης και κατάρτισης στον τομέα της κυβερνοασφάλειας, η ΕΕ δίνει μεγάλη έμφαση στον εξοπλισμό του εργατικού δυναμικού της με τις δεξιότητες και τις γνώσεις που απαιτούνται για την άμυνα έναντι των απειλών στον κυβερνοχώρο.

Εν κατακλείδι, η προσέγγιση της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο χαρακτηρίζεται από τις πολύπλευρες, συνεργατικές και προνοητικές στρατηγικές της. Αναγνωρίζει την περίπλοκη φύση του ψηφιακού τοπίου και την ανάγκη ολιστικής αντιμετώπισης. Μέσω κανονισμών, συμπράξεων, διεθνούς δέσμευσης και εστίασης στην εκπαίδευση και την ευαισθητοποίηση, η ΕΕ τοποθετείται ως προληπτικός και ανθεκτικός πυλώνας στο διαρκώς εξελισσόμενο πεδίο του κυβερνοχώρου. Καθώς ο ψηφιακός κόσμος συνεχίζει να εξελίσσεται, η δέσμευση της ΕΕ για τη διασφάλιση των δικτύων, των πληροφοριών και των κρίσιμων υποδομών της παραμένει ακλόνητη, εξασφαλίζοντας ένα ασφαλέστερο ψηφιακό περιβάλλον για τους πολίτες και τους εταίρους της παγκοσμίως.

Βιβλιογραφία

Ελληνόγλωσση

Αγγελής, Ι. (2005). *Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης*. Ποινική Δικαιοσύνη, 23-40.

Αλεξανδρίδου, Ε. (2010). *Το Δίκαιο του Ηλεκτρονικού Εμπορίου*. Αθήνα: Εκδόσεις Σάκκουλα.

Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002). *Ζητήματα από το Δίκαιο της Πληροφορικής*. Αθήνα – Κομοτηνή: Εκδόσεις Σάκκουλα.

Αλεξανδροπούλου- Αιγυπτιάδου, Ε. (2007). *Η πλοήγηση των ανηλίκων στο διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων*. Αρμενόπουλος ΞΑ,12-35.

Άντρη, Ε. (2013). Το φαινόμενο τον διαδικτυακού εθισμού στο σύγχρονο άνθρωπο. *Cyprus Nursing Chronicles*, 14(3). Διαθέσιμο στο https://cncjournal.cyna.org/wp-content/uploads/2019/07/CNC-14-3.6-11.pdf

Βλαχόπουλος, Κ. (2007). *Ηλεκτρονικό Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.

Βλαχόπουλος, Κ. (2013). *Ηλεκτρονικό έγκλημα: Μορφές, πρόληψη, αντιμετώπιση*. Αθήνα: Νομική Βιβλιοθήκη

Δαγτόγλου, Π. (2012). Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα. *Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα.*

Δαλακούρας, Θ. (2019). *Ηλεκτρονικό Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.

Θεμελή Ο. (2017), Η αναζήτηση της ουσιαστικής αλήθειας και ο κίνδυνος της νομικής πλάνης κατά τη διερεύνηση των ισχυρισμών των ανηλίκων θυμάτων σεξουαλικής κακοποίησης, στον Τιμητικό Τόμο για τον Α. Μαγγανά, Σελ. 669-686 διαθέσιμο στην ιστοσελίδα http://pandemos.panteion.gr/index.php?lang=el&op=record&type&q&page=0&pid=iid%3A18581&fbclid=IwAR2m0YkEB_5l5PjA0MtruXfyTW_AV3j2fdjpxAzGDVzfBgvs7sJMvxfe1HQ

Ιγγλεζάκης, Ι. (2018). *Δίκαιο πληροφορικής*. Αθήνα: Εκδόσεις Σάκκουλα

Ιγγλεζάκης, Ι. (2020). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019). *Αθήνα: Interactive Books*

Καϊάφα- Γκμπάντι, Μ. (2012). *Διαδικτυακές προσβολές της ανηλικότητας*. ΠοινΧρ., 171.

Πανάγος Κ. (2019), Η δικανική εξέταση ανηλίκων σε υποθέσεις σεξουαλικής κακοποίησης: Νεότερα νομοθετικά δεδομένα, *The Art of Crime* διαθέσιμο στο: https://theartofcrime.gr/%CE%B7-%CE%B4%CE%B9%CE%BA%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%B5%CE%BE%CE%AD%CF%84%CE%B1%CF%83%CE%B7-%CE%B1%CE%BD%CE%B7%CE%BB%CE%AF%CE%BA%CF%89%CE%BD-%CF%83%CE%B5-%CF%85%CF%80%CE%BF%CE%B8%CE%AD%CF%83/

Ευρωπαϊκή Επιτροπή, (2023), Κοινή Κυβερνομονάδα. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/el/policies/joint-cyber-unit

Ευρωπαϊκή Επιτροπή, (2023), Η πράξη της ΕΕ για την ασφάλεια στον Κυβερνοχώρο, διαθέσιμο στο https://digital-strategy.ec.europa.eu/el/policies/cybersecurity-act

Κανονισμός ΕΕ 2019/881, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32019R0881.

Οδηγία ΕΕ 2022/2555, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2), *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022L2555&qid=1697797857660

Ξενόγλωσση

Aidan, J. S., & Garg, U. (2018). Advanced Petya ransomware and mitigation strategies. στο *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 23-28). IEEE.

Aman Gupta, A. A. (2017). Ethical Hacking and Hacking Attacks. International *Journal Of Engineering And Computer Science*, 6(4), 21042- 21050.

Altwairqi, F.A. (2019). Four Most Famous Cyber Attacks for Financial Gains. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(2), 2131-2139.

Backman S. (2023) Risk vs. threat-based cybersecurity: the case of the EU, *European Security*, 32:1, 85-103, DOI: 10.1080/09662839.2022.2069464

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance,* 28, 24-31.

Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *NCJL & Tech*., 4, 1.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). Crime in cyberspace: offenders and the role of organized crime groups, *SSRN 2211842*. Διαθέσιμο στο https://www.academia.edu/download/39890872/Crime_in_Cyberspace_Offenders_and_the_Ro20151110-17776-op46wg.pdf

Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations. *Oxford University Press.*

Brzica, N. (2018). Understanding Contemporary Asymmetric Threats. *Croatian International Relations Review*, 24(83), 34-51. Διαθέσιμο στο https://www.researchgate.net/publication/328633110_Understanding_Contemporary_Asymmetric_Threats

Cadwalladr, C. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Διαθέσιμο στο https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [τελευταία πρόσβαση 9/11/2023]

Carroll, A. B. (1999). Corporate social responsibility. *Business & Society*, 38(3), 268-295.

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26-27.

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security. *Global Commission on Internet Governance*, No.6.

Cimpanu, Catalin (2017). AlphaBay Dark Web Market Taken Down After Law Enforcement Raids. *Bleeping Computer*, διαθέσιμο στο https://www.bleepingcomputer.com/news/security/alphabay-dark-web-market-taken-down-after-law-enforcement-raids/ [τελευταία πρόσβαση 9/11/2023]

Cimpanu C. (2021), EU announces joint cyber unit to respond to large-scale security incidents., *The Record*, Διαθέσιμο στο https://therecord.media/eu-announces-joint-cyber-unit-to-respond-to-large-scale-security-incidents [τελευταία πρόσβαση 9/11/2023]

Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. Asian journal of criminology, 3, 37-59.

Macilotti, G. (2020). Online child pornography: Conceptual issues and law enforcement challenges. In Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support. IGI Global. Σελ. 226-247

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. *HarperCollins*.

Cornish, P. (2009). Cyber security and politically, socially and religiously motivated cyber attacks. *European Parliament* διαθέσιμο στο https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyberspace and the national security of the United Kingdom. Threats and Responses. *Chatham House, London*, 1(1), 1-46.

Council of the European Union. (2023). Revised Implementing Guidelines of the Cyber Diplomacy Toolbox. Διαθέσιμο στο https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

Couts A. & Newman L.H (2023), Police can spy on your iOS and Android Push Notifications, *Wired*, διαθέσιμο στο https://www.wired.com/story/apple-google-push-notification-surveillance/ [τελευταία πρόσβαση 07/12/2023]

CSIRTs Network (2023), Intro, διαθέσιμο στο https://csirtsnetwork.eu/#:~:text=The%20mission%20of%20the%20European,exchange%20best%20practices%20in%20incident

Cyberwatching.eu. (n.d.). European Commission Sets Up Joint Cyber Unit to Respond to Large-Scale Cyber Incidents. Διαθέσιμο στο https://www.cyberwatching.eu/news-events/news/european-commission-sets-joint-cyber-unit-respond-large-scale-cyber-incidents [τελευταία πρόσβαση 9/11/2023]

Dawson, M., Vassilakos, A., Castanon Remy, J.L. Setor, T.K. (2021) Illicit activities beneath the surface web investigating domestic extremism on anonymous social media platforms, *Holistica Journal of Business and Public Administration*, Vol.12, Iss.1, pp.27-40

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), 15-32.

Denning, D. E. (1999). Information warfare and security. *ACM Press/Addison-Wesley Publishing Co.*

Denning, D. E. (2015). A Framework for Ethical Decision Making in Cybersecurity. *IEEE Security & Privacy*, 13(1), 84-88. DOI: 10.1109/MSP.2014.49

Dilipraj, E. (2014). Terror in the Deep and Dark Web. *Air Power Journal*, 9(3), 121-140.

Dingledine, R., Mathewson, N., & Syverson, P. (2004), Tor: The Second-Generation Onion Router. Διαθέσιμο στο https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router

Dunn Cavelty, M. (2013). A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers*, 23.

Dunn Cavelty, M. , & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, 15(1), 37-57.

Strategic Communications. (2023). European Union and NATO intensify cooperation in addressing cyber threats. *European External Action Service* Διαθέσιμο στο https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en [τελευταία πρόσβαση 9/11/2023]

EU General Data Protection Regulation (GDPR) (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and

on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*.

European Union. (2023). Law. Διαθέσιμο στο https://european-union.europa.eu/institutions-law-budget/law_en

European Union. (2023). Types of legislation. Διαθέσιμο στο https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

European Union. (2023). Rule of Law. Διαθέσιμο στο https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en

European Commission. (2023). The EU-UK Trade and Cooperation Agreement. Διαθέσιμο στο https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en

European Commission. (2023). The Cybersecurity Strategy. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission. (2023). Enhancing EU Resilience. Διαθέσιμο στο https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3992

European Comission. (2021). Migration and Asylum. Διαθέσιμο στο https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/new-pact-migration-and-asylum_en

European Commission. (2018). Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012. Διαθέσιμο στο https://eur-lex.europa.eu/eli/reg/2018/1724/oj

European Parliament and Council. (2022) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1697797857660

European Parliament and Council. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Διαθέσιμο στο https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Union External Action. (2023). EU cyber diplomacy. Διαθέσιμο στο https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Union Agency for Cybersecurity (ENISA). (2023). About ENISA. Διαθέσιμο στο https://www.enisa.europa.eu/about-enisa

European Union Agency for Cybersecurity (ENISA). (2021). Raising awareness of Cybersecurity. Διαθέσιμο στο https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

European Union Agency for Cybersecurity (ENISA). (2023). Public-Private Partnerships. Διαθέσιμο στο https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps

European Union Agency for Cybersecurity (ENISA). (2023). EU CyCLONe. Διαθέσιμο στο https://www.enisa.europa.eu/topics/incident-response/cyclone

European Union Agency for Cybersecurity (ENISA). (2023). NIS Directive. Διαθέσιμο στο https://www.enisa.europa.eu/topics/nis-directive

European Union Agency for Cybersecurity (ENISA). (2023). Publications. Διαθέσιμο στο https://www.enisa.europa.eu/publications

European Union Agency for Cybersecurity (ENISA). (2023). Emerging Technologies. Διαθέσιμο στο https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

European Union Agency for Cybersecurity (ENISA). (2023). Certification. διαθέσιμο στο https://www.enisa.europa.eu/topics/certification

Europol, T. E. S. A. T. (2010). EU terrorism situation and trend report. *European Police Office*

Finklea, C. (2015). Dark Web. *Congressional Research Service*. Διαθέσιμο στο https://fas.org/sgp/crs/misc/R44101.pdf [τελευταία πρόσβαση 9/11/2023]

Ferrell, O. C., Fraedrich, J., & Ferrell, L. (2013). Business ethics: Ethical decision making and cases. *Cengage Learning*.

Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., ... & Cobo, M. J. (2020). 20 years of scientific evolution of cyber security: A science mapping. *In International Conference on Industrial Engineering and Operations Management*. IEOM Society International. Sel. 314-325

Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy*, 41(1), 33-54. DOI: 10.1080/13523260.2019.1677389.

Greenberg A. (2014), Hacker Lexicon: What is the Dark Web?, *Wired*. διαθέσιμο στο https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ [τελευταία πρόσβαση 9/11/2023]

Greenberg A. (2022), AlphaBay is taking over the dark web-again, *Wired* διαθέσιμο στο https://www.wired.com/story/alphabay-dark-web-market-ranking/ [τελευταία πρόσβαση 9/11/2023]

Gottfried, E. D., Shier, E. K., & Mulay, A. L. (2020). Child pornography and online sexual solicitation. *Current psychiatry reports*, *22*, Σελ. 1-8.

Harknett R. & Smeets M., (2022). Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*, 45:4, 534-567

Hazle, M. (2013,). CREDIT CARD SECURITY BREACH AT TARGET. *University of Southern California*: http://viterbi.usc.edu/news/news/2013/credit-card-security.htm [τελευταία πρόσβαση 9/11/2023]

Hern A. (2017), WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017, *The Guardian*. διαθέσιμο στο https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware#:~:text=The%20WannaCry%20outbreak%20had%20shut,handle%20any%20more%20emergency%20cases [τελευταία πρόσβαση 9/11/2023]

Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European union and nato global cybersecurity challenges. *Prism*, *6*(2), Σελ. 126-141

Joint Report (2019), Common challenges in combating cybercrime, as identified by Eurojust and Europol, *Europol and Eurojust Public Information* διαθέσιμο στο https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf

Joshi, D. M. (2021). Cyber Pornography: An interdisciplinary study of technology led crime against women and children. *International Journal of Creative Research Thoughts* (IJCRT), 9(12), b297- b301.

Kaspersky (2023), What is an APT?, *Kaspersky*, διαθέσιμο στο https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kimmage, D. (2010). Al-Qaeda central and the internet, *Washington DC: New America Foundation.*

Lele, A. (2014). Asymmetric Warfare: A State vs Non-State Conflict. *OASIS*, (20), 97-111. Universidad Externado de Colombia. Διαθέσιμο στο https://www.redalyc.org/pdf/531/53163822007.pdf

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. *RAND corporation*.

Mann, M., Zulli, D., Foote, J., Ku, E., & Primm, E. (2023). Unsorted Significance: Examining Potential Pathways to Extreme Political Beliefs and Communities on Reddit. *Socius: Sociological Research for a Dynamic World*, 9, 1–15. DOI: 10.1177/23780231231174823

Marwick, A. E., & Furl, K. (2021). Taking The RedPill: talking about extremism. AoIR Selected Papers of Internet Research. Σελ. 2-5. DOI: 10.5210/spir.v2021i0.12207

Metz, S. (2012). Rethinking insurgency**.** In The Routledge handbook of insurgency and counterinsurgency. *Routledge*. Σελ. 32-44

Milmo D. (2023), Facebook owner Meta fined €1.2bn for mishandling user information, *The Guardian* διαθέσιμο στο https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta [τελευταία πρόσβαση 21/11/2023]

NATO. (2023), Cyber Defence. Διαθέσιμο στο https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en [τελευταία πρόσβαση 9/11/2023]

National Initiative for Cybersecurity Careers and Studies (NICCS), (2023). *Cybersecurity Education and Training*. Διαθέσιμο στο https://niccs.cisa.gov/education-training [τελευταία πρόσβαση 9/11/2023]

NIST Special Publication 800-53 (2022). Security and Privacy Controls for Information Systems and Organizations. *National Institute of Standards and Technology.*

NIST Special Publication 800-61 (2022), Revision 2: Computer Security Incident Handling Guide. *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [τελευταία πρόσβαση 9/11/2023]

O'Neill P.H. (2022), Russian hackers tried to bring down Ukraine's power grid to help the invasion, *MIT Technology Review* διαθέσιμο στο https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/#:~:text=Hackers%20believed%20to%20be%20working,using%20malware%20known%20as%20Industroyer. [τελευταία πρόσβαση 9/11/2023]

OWASP (2023), Denial of Service, OWASP Foundation διαθέσιμο στο https://owasp.org/www-community/attacks/Denial_of_Service [τελευταία πρόσβαση 21/11/2023]

OWASP (2023), Cross Site Scripting (XSS), OWASP Foundation, διαθέσιμο στο **https://owasp.org/www-community/attacks/xss/** [τελευταία πρόσβαση 21/11/2023]

OWASP (2023), SQL Injection, OWASP Foundation διαθέσιμο στο https://owasp.org/www-community/attacks/SQL_Injection [τελευταία πρόσβαση 21/11/2023]

Paquet-Clouston, M., & García, S. (2022). On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime*, Σελ. 1-30.

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Saravanan, A., & Bama, S. S. (2019). A review on cyber security and the fifth generation cyberattacks. *Oriental journal of computer science and technology*, 12(2), 50-56.

Schneier, B. (2000). Secrets and lies: Digital security in a networked world. *Wiley*.

Smith, S. W. (2021). Cybersecurity and Cyberwarfare: An Introduction. *Routledge*.

STL Digital, (2023). The Cat and Mouse Game: A look into Cybersecurity vs Cybercrime, *STL Digital*, διαθέσιμο στο https://www.stldigital.tech/blog/the-cat-and-mouse-game-a-look-into-cybersecurity-vs-cybercrime/ [τελευταία πρόσβαση 21/11/2023]

Trend (2023), Zero-Day Vulnerability, Trend Micro Bussiness, διαθέσιμο στο https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability [τελευταία πρόσβαση 21/11/2023]

Turner, D. (2008). Symantec Global Internet Security Threat Report Trends for July–December 07, *Volume XII*, διαθέσιμο στο https://docs.broadcom.com/doc/istr-08-april-exec-sum-en [τελευταία πρόσβαση 21/11/2023]

Lete B., Pernik P. (2017), EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions, *Policy Brief GMF* Διαθέσιμο στο https://www.gmfus.org/sites/default/files/EU-NATO%2520Cybersecurity%2520and%2520Defense%2520Cooperation%2520edit.pdf [τελευταία πρόσβαση 9/11/2023]

United Nations. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://undocs.org/A/70/174 [τελευταία πρόσβαση 9/11/2023]

U.S. Cybercom. (2023). Command History. Διαθέσιμο στο https://www.cybercom.mil/About/History/. [τελευταία πρόσβαση 9/11/2023]

Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. *European journal of operational research*, 146(2), 241-257.

US Senate Committee on Homeland Security and Governmental Affairs (2008), Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat διαθέσιμο στο https://www.govinfo.gov/content/pkg/CHRG-

110shrg44123/html/CHRG-110shrg44123.htm [τελευταία πρόσβαση 21/11/2023]

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, 27(5), 781-799.

Walther, G. (2015). Printing insecurity? The security implications of 3d-printing of weapons. *Science and engineering ethics*, 21(6), 1435-1445.

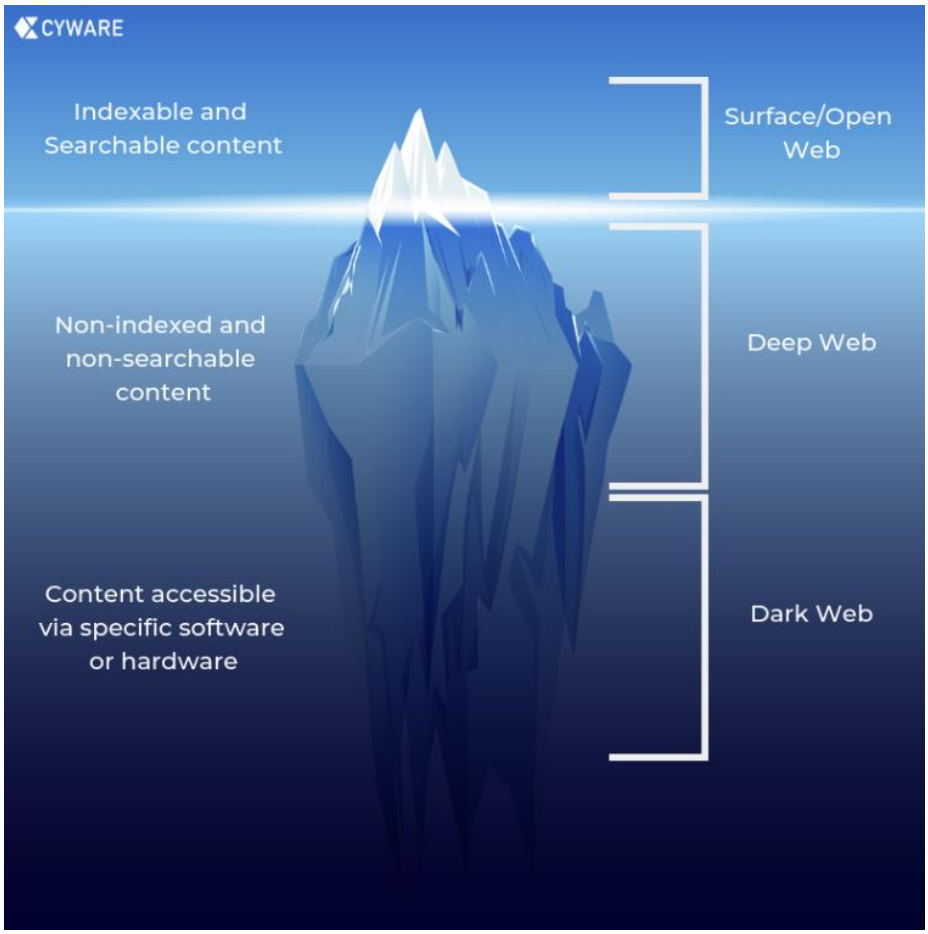
Wang, M., Callaghan, V., Bernhardt, J., White, K., & Peña-Rios, A. (2018). Augmented reality in education and training: pedagogical approaches and illustrative case studies. *Journal of Ambient Intelligence and Humanized Computing*, 9(5), 1391-1402.

Wang, P., Dawson, M., & Williams, K. L. (2019). Improving cyber defense education through national standard alignment: case studies. *In National Security: Breakthroughs in Research and Practice* (pp. 78-91). IGI Global.

Ward, C., Polglase, K., Shukla, S., Mezzofiore, G., & Lister, T. (2020). How Russian meddling is back. CNN, διαθέσιμο στο https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html [τελευταία πρόσβαση 21/11/2023]

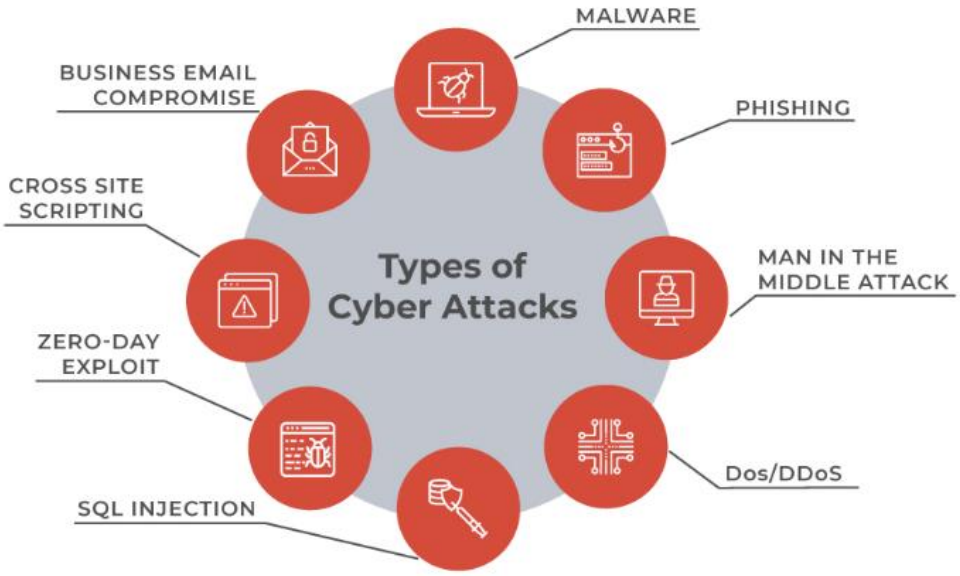
Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, 39(3), 195-206.

Παράρτημα



Εικόνα 1: Η αναλογία παγόβουνου – διαδικτύου.

Πηγή: Cyber Threat Intelligence (2019), How is Surface Web Intelligence different from Dark Web Intelligence?, CyWare διαθέσιμο στο https://cyware.com/security-guides/cyber-threat-intelligence/how-is-surface-web-intelligence-different-from-dark-web-intelligence-393c



Εικόνα 2: Συνήθης τύποι κυβερνοεπιθέσεων

Πηγή: Team Ecosystm (2019), Things you need to know about Cyber Attacks, Threats and Risks, *Ecosystm* διαθέσιμο στο https://blog.ecosystm.io/cyber-attacks-threats-risks/