ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΕΘΝΙΚΗ ΚΙ ΕΝΩΣΙΑΚΗ ΔΙΟΙΚΗΣΗ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

«ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ»

ΜΕΤΑΠΤΥΧΙΑΚΟΣ ΦΟΙΤΗΤΗΣ: ΤΣΑΚΩΝΑΣ ΡΑΦΑΗΛ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΠΑΚΩΝΣΤΑΝΤΗΣ ΜΑΡΚΟΣ

ΑΘΗΝΑ, ΟΚΤΩΒΡΙΟΣ 2021

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματεύεται το έγκλημα στον κυβερνοχώρο. Στις επόμενες σελίδες, αναλύεται το νομικό πλαίσιο για το κυβερνοέγκλημα, τόσο σε διεθνές όσο και ενωσιακό επίπεδο. Συγκεκριμένα, αναλύεται διεξοδικά η Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, καθώς και η Οδηγία 2013/40 της Ευρωπαϊκής Ένωσης για τις επιθέσεις κατά συστημάτων πληροφοριών. Στην συνέχεια, ερευνάται η δομή και ο ρόλος των Οργανισμών της Ευρωπαϊκής Ένωσης που έχουν επιφορτιστεί με την κυβερνοασφάλεια και κυριότερα ο Οργανισμός ENISA. Μετέπειτα, παρατίθενται οι δράσεις και οι πρωτοβουλίες της Ένωσης στον συγκεκριμένο τομέα, οι οποίες εκφράζονται κυρίως με δύο Ανακοινώσεις της Επιτροπής και με την Στρατηγική της Ευρωπαϊκής Ένωσης για την ψηφιακή δεκαετία. Βέβαια, πριν από τα ανωτέρω και για λόγους πληρότητας, κατεβλήθη προσπάθεια να παρατεθεί ο ορισμός του κυβερνοεγκλήματος, τα χαρακτηριστικά που το διαφοροποιούν από το κοινό έγκλημα, καθώς και μία σύντομη ιστορική αναδρομή.

ABSTRACT

The given master's thesis deals with cybercrime. On the following pages, the legal framework for cybercrime in both international and EU level is analyzed. More specifically, The Budapest Convention on cybercrime is thoroughly scrutinized with the Directive 2013/40 of European Union on attacks against information systems, as well. Moreover, the structure and role of the European Union Agencies in charge of cyber security is explored, and mostly the ENISA Agency. Additionally, the actions and the initiatives of the Union in this field are listed, which are mainly expressed in two Communications of the European Commission and the elaboration of strategy of the Union for the digital decade. However, before the above and for reasons of completeness, an attempt was made to cite the definition of cybercrime, the characteristics of which differentiate it from common crime, as well as a brief historical look.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η συνεχής ανάπτυξη της τεχνολογίας έχει οδηγήσει στην χρήση υπολογιστών από την συντριπτική πλειονότητα του παγκόσμιου πληθυσμού. Επακόλουθο της ραγδαίας αυτής ανάπτυξης είναι η αύξηση των εγκλημάτων που σχετίζονται με τους υπολογιστές και ειδικότερα των εγκλημάτων που διαπράττονται στον κυβερνοχώρο. Ως εκ τούτου, τόσο η παγκόσμια όσο και η ευρωπαϊκή κοινότητα δεν θα μπορούσε να παραμείνει αδιάφορη για το εν λόγω φαινόμενο. Άλλωστε, η διασυνορικότητα αποτελεί βασικό στοιχείο των εγκλημάτων στον κυβερνοχώρο, με αποτέλεσμα να καθίσταται αναγκαία η συνεργασία μεταξύ περισσότερων κρατών για την αντιμετώπιση τους.

Η Ευρωπαϊκή Ένωση, έχει αναγνωρίσει το κυβερνοέγκλημα ως μια νέα απειλή κατά της ασφάλειας, αυτής και των πολιτών της. Αυτό έχει ως συνέπεια, διατάξεις για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και για την ασφάλεια των συστημάτων πληροφοριών και δικτύων να ανευρίσκονται σε πληθώρα κειμένων, που αφορούν τις μελλοντικές προκλήσεις της Ένωσης. Άλλωστε, η αντιμετώπιση του κυβερνοεγκλήματος προβλέπεται τόσο στο πλαίσιο της στρατηγικής της Ένωσης για την Κοινή Εξωτερική Πολιτική και την Πολιτική Ασφαλείας όσο και το πλαίσιο της Ένωσης Ασφαλείας 2020 – 2025, καθώς και σε νομικά κείμενα για την ασφάλεια των δημοκρατικών θεσμών, όπως θα αναλυθεί παρακάτω.

Την ίδια στιγμή, το διαδίκτυο καθίσταται ένας χώρος που χρησιμοποιείται για την διάπραξη πληθώρας αδικημάτων που πλήττουν σοβαρά τα κράτη μέλη της Ένωσης καθώς και τα σύνορα της. Τέτοια εγκλήματα είναι για παράδειγμα η τρομοκρατία και η παιδική πορνογραφία. Πλέον, το κυβερνοέγκλημα αποτελεί μια πτυχή του οργανωμένου εγκλήματος και έχει σοβαρές συνέπειες για τις υποδομές της Ένωσης, τους πολίτες και τις επιχειρήσεις, με δυσθεώρητο οικονομικό κόστος.

Η παγκόσμια κοινότητα με την Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, καθώς και η ευρωπαϊκή κοινότητα με πληθώρα νομικών πράξεων και την ίδρυση σχετικών οργάνων και Οργανισμών, επιχειρούν την αντιμετώπιση του

φαινομένου που συνεχώς εξελίσσεται ραγδαίως, ακολουθώντας την ανάπτυξη της τεχνολογίας.

2. ΟΡΙΣΜΟΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Ένα πρωταρχικό ζήτημα που αφορά στο κυβερνοέγκλημα είναι η έλλειψη ενός ενιαίου και συγκεκριμένου ορισμού, είτε στο νόμο είτε στην θεωρία[1]. Προσπάθεια να ορίσουν το κυβερνοέγκλημα έχουν καταβάλει πολλοί ακαδημαϊκοί[2] αλλά και νομοθέτες[3], ωστόσο δεν έχει καταστεί δυνατή, έως τώρα, η εύρεση ενός ενιαίου ορισμού. Αυτό που παρατηρείται είναι ότι στα νομοθετικά κείμενα ο όρος χρησιμοποιείται ανάλογα με το εκάστοτε ρυθμιζόμενο ζήτημα, δημιουργώντας έτσι μια πληθώρα ορισμών που διαμορφώνονται σε συνάρτηση με το ρυθμιζόμενο θέμα και κατ' επέκταση τον σκοπό της ρύθμισης[4]. Κατά συνέπεια, δεν υπάρχει ένας per se ορισμός του όρου σε παγκόσμιο ή έστω σε ευρωπαϊκό επίπεδο αλλά ούτε και σε εθνικό[5].

Στην θεωρία έχουν διατυπωθεί διάφοροι ορισμοί για το κυβερνοέγκλημα. Είναι ασφαλές να ειπωθεί ότι κοινό στοιχείο όλων είναι ότι περιλαμβάνουν εγκλήματα που σχετίζονται με υπολογιστή. Έτσι, ως κυβερνοέγκλημα έχει οριστεί η πράξη που τελείται με την μεσολάβηση υπολογιστή και είτε είναι παράνομη είτε μπορεί να θεωρηθεί ως παράνομη από ορισμένα μέρη και μπορεί να τελεστεί μέσω παγκόσμιων ηλεκτρονικών δικτύων[6]. Από την άλλη πλευρά, η Ευρωπαϊκή Επιτροπή χρησιμοποιεί έναν απλό και συγκαταβατικό ορισμό της έννοιας, ορίζοντας ως κυβερνοέγκλημα κάθε έγκλημα που τελείται διαμέσου του διαδικτύου. Η πρόθεση πίσω από αυτόν τον ορισμό είναι να διευκολυνθεί η διαδικασία εναρμόνισης των

[1] YAR M., The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, European Journal of Criminology, 2005, σελ. 409

[2] Βλ. Ενδεικτικά: Pocar, F., 2004. New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, σελ. 27-37;, Thomas, D. and Loader, B., Introduction – Cybercrime: Law enforcement, security and surveillance in the information age, σε D. Thomas and B. Loader (eds), *Cybercrime: Law enforcement, security and surveillance in the information age*, London, Routledge, 2000, σελ. 3

[3] International Telecommunication Union, 2011, Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185

[4] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Vienna, February 2013, σελ. 11, διαθέσιμο σε: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf , προσπελάστηκε την 28/08/2021

[5] Proteus Manual, Prevention, Information and support to victims of online identity theft, Lisboa, APAV, 2015, σελ. 17

[6] Thomas D. και Loader B., ο.π., 2000, σελ. 3

εθνικών νομοθεσιών σε αυτά τα ζητήματα. Ωστόσο, το γεγονός ότι η Επιτροπή καθιστά την χρήση του διαδικτύου ως απαραίτητο εννοιολογικό στοιχείο του κυβερνοεγκλήματος έχει αποτελέσει αντικείμενο κριτικής[7] καθώς, εκτός των άλλων, έρχεται σε σύγκρουση με την πλειονότητα των ορισμών στην θεωρία.

Άλλοι ορισμοί που έχουν παρατεθεί από θεωρητικούς του ηλεκτρονικού εγκλήματος απαιτούν την μεσολάβηση υπολογιστή, η οποία μάλιστα θα έχει διαδραματίσει καθοριστικό ρόλο στην αξιόποινη πράξη, είτε ως εργαλείο είτε ως στόχος είτε ως τόπος του εγκλήματος[8]. Από την άλλη πλευρά, υπάρχει η γνώμη ότι για τον ορισμό του ηλεκτρονικού εγκλήματος είναι μεν απαραίτητη η ύπαρξη ηλεκτρονικού υπολογιστή, αλλά την βαρύνουσα σημασία κατέχει η προϋπόθεση ύπαρξης ενός δικτύου (network)[9].

Από τους παρατιθεμένους, ενδεικτικά αναφερόμενους, ορισμούς, αυτός που συγκεντρώνει την μεγαλύτερη αποδοχή από την θεωρία[10] και από ευρωπαϊκούς οργανισμούς[11] είναι εκείνος των Thomas D. και Loader B. Σύμφωνα με αυτόν, κυβερνοέγκλημα αποτελεί κάθε πράξη που τελείται με την μεσολάβηση υπολογιστή και είτε είναι παράνομη είτε μπορεί να θεωρηθεί ως παράνομη από ορισμένα μέρη και μπορεί να τελεστεί μέσω παγκόσμιων ηλεκτρονικών δικτύων.

Πάντως, όπως προαναφέρθηκε, δεν μπορεί να ειπωθεί ότι υπάρχει ένας ορισμός που χρησιμοποιείται καθολικά. Ενδεικτικό είναι ότι ούτε η Σύμβαση του Συμβουλίου της Ευρώπης για το Ηλεκτρονικό Έγκλημα περιλαμβάνει σχετικό ορισμό. Η προσέγγιση που επιλέγει η εν λόγω σύμβαση είναι παρόμοια με εκείνη που ακολουθεί ο Οργανισμός Ηνωμένων Εθνών στην Σύμβαση κατά της Διαφθοράς, όπου εκλείπει ο ορισμός της διαφθοράς. Από τα παραπάνω φαίνεται, τελικά, ότι ο όρος cybercrime δεν αποτελεί έναν νομικό όρο[12].

---

[7] EUCPN, Cybercrime: a theoretical overview of the growing digital threat, σε: EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network: Brussels, 2015, σελ. 9

[8] Carter D.L., Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, Volume: 64, Issue 7, σελ. 21-27, όπου αναλύει ξεχωριστά κάθε μία από τις προαναφερθείσες περιπτώσεις.

[9] Moore, R., Cybercrime: investigating high-technology computer crime, Routledge, 2015, σελ. 4

[10] Βλ. YAR, M, ο.π., 2005, σελ. 409, Castells M., The internet galaxy: Reflections on the internet, business, and society, Oxford University Press, 2002

[11] EUCPN, ο.π., 2015, σελ. 9

[12] United Nations Office on Drugs and Crime, ο.π., 2013, σελ. 12

Η έλλειψη ενός κοινώς αποδεκτού ορισμού για το κυβερνοέγκλημα, τόσο στην θεωρία όσο και στη νομοθεσία, καταδεικνύει την ανάγκη να καταγραφούν ορισμένα χαρακτηριστικά του κυβερνοεγκλήματος ώστε να καταστεί δυνατό να υπαχθεί σε αυτό κάθε πράξη που συγκεντρώνει τα σχετικά χαρακτηριστικά, ανεξαρτήτως εάν έχει οριστεί επακριβώς ως ηλεκτρονικό έγκλημα.

Η Σύμβαση της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο αποτελεί κατευθυντήρια γραμμή, καθώς υπάγει στο πρώτο τμήμα της, υπό την ονομασία Ουσιαστικό Ποινικό Δίκαιο, διάφορες πράξεις που θεωρούνται ως ηλεκτρονικό έγκλημα. Έτσι, από την Σύμβαση εξάγονται οι παρακάτω μορφές.

Παράνομη πρόσβαση σε σύστημα υπολογιστή. Αυτή η μορφή κυβερνοεγκλήματος αποδίδεται διεθνώς με τον όρο hacking. Σε αυτή την περίπτωση, ο hacker προσπαθεί να αποκτήσει κακόβουλα πρόσβαση σε ξένο δίκτυο και να ασκήσει τις εξουσίες του νόμιμου χρήστη[13].

Υποκλοπή Δεδομένων. Σε αυτή την περίπτωση, ο δράστης υποκλέπτει δεδομένα που υπάρχουν σε σύστημα υπολογιστή ή διακινούνται μέσω υπολογιστή είτε προς τον ίδιο είτε προς έτερο υπολογιστή.

Παρεμβολές σε Δεδομένα ή σε Συστήματα. Σε αυτή την κατηγορία υπάγεται η άνευ δικαιώματος βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστών ή υπολογιστικών συστημάτων[14].

Κακή χρήση συσκευών. Η περίπτωση αυτή έγκειται στην, άνευ δικαιώματος και με σκοπό την διάπραξη αξιόποινων πράξεων, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή διάθεση συσκευής ή προγράμματος υπολογιστή ή κωδικού πρόσβασης ή άλλου συναφούς δεδομένου μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση σε σύστημα υπολογιστή.

Πλαστογραφία με υπολογιστή. Έγκειται στην από πρόθεση και άνευ δικαιώματος εισαγωγή, αλλοίωση, διαγραφή ή καταστολή δεδομένων υπολογιστή, που έχει ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων, με σκοπό να

[13] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2003, σελ 41
[14] Άρθρα 4 και 5 της Σύμβασης

θεωρηθούν αυτά αυθεντικά ή να γίνουν ενέργειες με βάση αυτά σαν να είναι αυθεντικά για νόμιμους σκοπούς, ασχέτως του εάν αυτά τα δεδομένα είναι ή όχι άμεσα αναγνώσιμα ή αντιληπτά[15].

Απάτη με υπολογιστή. Στη μορφή αυτή υπάγεται η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή καθώς και της παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο[16].

Παιδική πορνογραφία. Έγκειται στην από πρόθεση και άνευ δικαιώματος: α. παραγωγή παιδικής πορνογραφίας με σκοπό την διανομή της μέσω ενός συστήματος υπολογιστή, β. προσφορά ή διάθεση παιδικής πορνογραφίας μέσω ενός συστήματος υπολογιστή, γ. διανομή ή μετάδοση παιδικής πορνογραφίας μέσω ενός συστήματος υπολογιστή, δ. προμήθεια παιδικής πορνογραφίας μέσω ενός συστήματος υπολογιστή για ιδία χρήση ή για άλλο πρόσωπο και ε. κατοχή παιδικής πορνογραφίας σε ένα σύστημα υπολογιστή ή σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή[17].

Παραβιάσεις πνευματικών δικαιωμάτων και εμπορικών σημάτων. Στις περιπτώσεις αυτές στόχος είναι ο ίδιος ο υπολογιστής και τα δεδομένα πνευματικής ή βιομηχανικής ιδιοκτησίας που υπάρχουν σε αυτόν. Ο δράστης εισέρχεται παράνομα και χωρίς δικαίωμα σε σύστημα υπολογιστή και αντιγράφει, συλλέγει, πωλεί ή διανέμει προϊόντα που είναι αντικείμενα ξένης ιδιοκτησίας όπως ευρεσιτεχνίες, εμπορικά σήματα, βιομηχανικά σχέδια, λογοτεχνικά ή καλλιτεχνικά έργα με σκοπό το εμπορικό κέρδος[18].

Παραβάσεις σχετικές με το περιεχόμενο υπολογιστή. Σε αυτή την κατηγορία θα μπορούσε να υπαχθεί για παράδειγμα η κατοχή ή αποθήκευση ή μεταφορά υλικού παιδικής πορνογραφίας, το οποίο είναι αποθηκευμένο είτε σε υπολογιστή

[15] Άρθρο 7 της Σύμβασης
[16] Άρθρο 8 της Σύμβασης
[17] Άρθρο 9 της Σύμβασης
[18] Europol, Intellectual Property Crime, διαθέσιμο σε https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime , προσπελάστηκε την 28/08/2021

είτε στο διαδίκτυο. Επιπρόσθετα, το ίδιο συμβαίνει και με την κατοχή, αποθήκευση ή διακίνηση εικόνων, ήχων, αναπαραστάσεων με περιεχόμενο λόγο μίσους, διασπορά ψευδών ειδήσεων ή υποστήριξη τρομοκρατικών πράξεων[19].

Τρομοκρατία στον κυβερνοχώρο. Πρόκειται για μία μορφή κυβερνοεγκλήματος που παρατηρείται, σταδιακά, λίγο πριν το 2001 και συνίσταται κυρίως στην οργανωμένη επίθεση κυβερνο-τρομοκρατών σε συστήματα μυστικών Υπηρεσιών και άλλων κρίσιμων κρατικών συστημάτων, με σκοπό την ανεύρεση κενών στο σύστημα ασφαλείας και κατά συνέπεια την αποδυνάμωση τους. Ακόμα και η διάδοση προπαγανδιστικού περιεχομένου ενδέχεται να υπάγεται σε αυτή την κατηγορία, όπως για παράδειγμα η αναγγελία, μέσω του κυβερνοχώρου, τρομοκρατικού χτυπήματος σε συγκεκριμένο μέρος. Αυτού του είδους η τρομοκρατία δύναται να επιφέρει σοβαρές συνέπειες στην κοινωνικο-οικονομική ζωή του κράτους-στόχου[20]. Στο ανωτέρω παράδειγμα, μία απλή αναγγελία επικείμενου τρομοκρατικού χτυπήματος μπορεί να επιφέρει καίριο πλήγμα στον τουρισμό του εν λόγω κράτους καθώς και να το οδηγήσει σε λήψη μέτρων που αναστατώνουν την κοινωνική ειρήνη και ασφάλεια. Ένας ορισμός που ανταποκρίνεται στους ορισμούς φιλελεύθερων εννόμων τάξεων για την κυβενροτρομοκρατία συνίσταται σε κάθε πράξη που συμπεριλαμβάνει τεχνολογίες υπολογιστών ή του διαδικτύου και παρακινείται από πολιτικά, θρησκευτικά ή ιδεολογικά αίτια και αποσκοπεί στην τρομοκράτηση κυβερνήσεων ή ενός τμήματος του πληθυσμού προκαλώντας σοβαρές παρεμβάσεις στις υποδομές[21].

Οι μέθοδοι που χρησιμοποιούν οι παραβάτες για τις ως άνω εγκληματικές συμπεριφορές ποικίλουν και συνεχώς εξελίσσονται με την πρόοδο της τεχνολογίας και του διαδικτύου. Το modus operandi μπορεί να αποτελείται από διάφορα μοτίβα. Ενδεικτικά αναφέρονται η διασπορά κακόβουλου λογισμικού μέσω ιών (virus),

[19] United Nations Office on Drugs and Crime, ο.π., 2013, σελ 16 και 18

[20] Χαρακτηριστικές είναι οι δηλώσεις του Β. Obama, πρόεδρου των Η.Π.Α. το 2009 στον Λευκό Οίκο όπου ανέφερε ότι «τρομοκρατικές οργανώσεις έχουν εκδηλώσει την επιθυμία να εξαπολύσουν κυβερνοεπιθέσεις στις ΗΠΑ- επιθέσεις που είναι δυσκολότερο να ανιχνευτούν και να αντιμετωπιστούν… Οι κυβερνοεπιθέσεις είναι οι πιο σοβαρές απειλές στην οικονομία και εθνική ασφάλεια που πρέπει να αντιμετωπίσουμε»

[21] Ad Ariely G., Adaptive Responses to Cyberterrorism, σε: Chen T., Jarvis L., Macdonald S. (eds) Cyberterrorism, Springer, New York, 2014, σελ. 20

δούρειων ίππων (trohan) και σκουληκιών (worms), η ανεπιθύμητη αλληλογραφία (spamming), Phising and Pharming, καθώς και το hacking ή πειρατεία λογισμικού.

Άλλωστε, το διαδίκτυο χρησιμοποιείται όχι μόνο για ευθείες προσβολές υπό την μορφή άμεσων τρομοκρατικών ενεργειών, αλλά και την υποστήριξη και ανάπτυξη της τρομοκρατίας. Αυτό συμβαίνει, όταν γίνεται χρήση διαδικτυακής προπαγάνδας και των μέσων κοινωνικής δικτύωσης, με σκοπό την στρατολόγηση μελών, την ριζοσπαστικοποίηση και την συγκέντρωση κεφαλαίων[22].

Οι παραπάνω περιπτώσεις αποτελούν διάφορες μορφές του κυβερνοεγκλήματος και μας βοηθούν να κατανοήσουμε, ελλείψει ορισμού, ποιες πράξεις θα μπορούσαν να υπαχθούν στις σχετικές διατάξεις για το κυβερνοέγκλημα. Η απαρίθμηση που προηγήθηκε είναι ενδεικτική και περιλαμβάνει τις πιο συνήθεις περιπτώσεις που συναντώνται στην πράξη. Σε καμία περίπτωση δεν μπορεί να αποκλειστεί εκ των προτέρων η υπαγωγή κι άλλων πράξεων στις διατάξεις για το κυβερνοέγκλημα. Αυτό καθίσταται εναργές, εάν ο ερευνητής λάβει υπόψη του την συνεχή εξέλιξη της τεχνολογίας και των εγκληματικών συμπεριφορών με αποτέλεσμα να δημιουργούνται συνεχώς νέα εγκλήματα, τα οποία καλούνται οι νομοθέτες να ποινικοποιήσουν.

[22] Παπακωνσταντής Μάρκος, Η τρομοκρατία στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης της Ευρωπαϊκής Ένωσης, NoB, 2019, σελ. 347

3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Το ηλεκτρονικό έγκλημα και κατ' επέκταση το κυβερνοέγκλημα διαθέτει κάποια χαρακτηριστικά τα οποία το καθιστούν ιδιαίτερο και επιβάλλουν την ξεχωριστή μεταχείριση του από το νομοθέτη σε σχέση με τα κοινά εγκλήματα. Τα χαρακτηριστικά αυτά είναι τα κάτωθι.

1.Διασυνορικότητα. Ως γνωστόν, ο κυβερνοχώρος δεν διαθέτει σύνορα με αποτέλεσμα να είναι δυνατό να διαπραχθούν εγκλήματα κατά προσώπων, φυσικών ή νομικών, ακόμα και κατά του κράτους από οπουδήποτε στην γη. Την ίδια στιγμή, είναι δυνατό οι συνέπειες των εγκληματικών πράξεων να λαμβάνουν χώρα ταυτόχρονα σε πολλούς τόπους. Το γεγονός αυτό, εγείρει, εκτός των άλλων, και ζητήματα δικαιοδοσίας καθώς τόσο οι προπαρασκευαστικές όσο και οι κύριες πράξεις είναι δυνατό να υπάγονται παράλληλα στην δικαιοδοσία περισσότερων κρατών. Επιπρόσθετα, λόγω αυτού του χαρακτηριστικού τις περισσότερες φορές δεν καθίσταται εφικτό να ταυτοποιηθεί η σύνδεση του παραβάτη με την σκηνή του εγκλήματος[23].

2.Ανωνυμία. Οι δράστες των κυβερνοεγκλημάτων εκμεταλλεύονται τις δυνατότητες που τους παρέχουν τεχνολογικά εργαλεία για να αποκρύψουν την ταυτότητα τους ή και ακόμα να παραστήσουν κάποιο διαφορετικό πρόσωπο (pseudonymity). Επιπλέον, το γεγονός ότι σε αυτού του είδους τις αξιόποινες πράξεις δεν απαιτείται φυσική παρουσία στον ίδιο χώρο του θύτη και του θύματος καθιστά ακόμα ευχερέστερη την επίτευξη της ανωνυμίας από την πλευρά του δράστη. Με αυτόν τον τρόπο, ο δράστης αισθάνεται μεγαλύτερη ασφάλεια και ενισχύεται η εγκληματική του επιθυμία. Την ίδια στιγμή, μειώνεται ο βαθμός διακινδύνευσης του δράστη και αυξάνεται ο βαθμός επιτυχημένης τέλεσης του εγκλήματος[24].

Για να επιτύχουν την ανωνυμία οι δράστες τείνουν να λειτουργούν σε χώρες ή μέσω χωρών που δεν διαθέτουν σφοδρή επιθυμία για την πάταξη του ηλεκτρονικού εγκλήματος ή δεν διαθέτουν την ικανότητα να δράσουν αποτελεσματικά για την

[23] EC3, Europol, First Year Report, σελ. 26
[24] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, IEEE, 2007, σελ. 611

εύρεση και την σύλληψη του δράστη[25]. Η χαμηλή πιθανότητα σύλληψης διευκολύνει τους δράστες να εκκινήσουν την εγκληματική πράξη και να την ολοκληρώσουν επιτυχώς[26]. Ως εκ τούτου, καθίσταται αναγκαίο όλες οι χώρες της Ευρωπαϊκής Ένωσης να λαμβάνουν τα απαραίτητα μέτρα, ώστε να παρέχουν ένα ικανοποιητικό επίπεδο πρόληψης και καταπολέμησης του κυβερνοεγκλήματος.

Χαρακτηριστικά παραδείγματα, τα οποία συναντώνται συχνά στην πράξη, αποτελούν το εμπόριο ναρκωτικών, η διακίνηση όπλων και ανθρώπων και η διαρροή στοιχείων τραπεζικών καρτών[27]. Πάντως, όλες οι κινήσεις στο διαδίκτυο δυνητικά μπορούν να εντοπιστούν ακόμα και αν χρησιμοποιούνται εργαλεία που εξασφαλίζουν σε πρώτο βαθμό την ανωνυμία ή την ψευδωνυμία. Έτσι, διατυπώνεται η άποψη ότι η ανωνυμία εξαρτάται σε απόλυτο βαθμό από την ικανότητα των διωκτικών μηχανισμών και το κατά πόσο αυτοί διαθέτουν ικανό ανθρώπινο και τεχνολογικό δυναμικό που είναι σε θέση να ανιχνεύσει τα ψηφιακά ίχνη[28].

3.Ασυμμετρία. Το χαρακτηριστικό αυτό έγκειται στην άνιση «μάχη» μεταξύ των δραστών του ηλεκτρονικού εγκλήματος και των διωκτικών αρχών. Οι πρώτοι, έχουν την δυνατότητα να εφευρίσκουν συνεχώς νέους τρόπους δράσης, όντας έτσι ένα βήμα μπροστά από τις διωκτικές αρχές. Οι δράστες εκμεταλλεύονται τις συνεχώς αυξημένες και πιο εξελιγμένες ευκαιρίες που τους παρέχει το διαδίκτυο, ενεργώντας αποτελεσματικά. Έτσι, οι αρχές αλλά και οι χρήστες καλούνται να λαμβάνουν μέτρα προστασίας για απειλές που τους είναι ακόμα άγνωστες, κάτι το οποίο είναι ιδιαίτερα δύσκολο να συμβεί. Αποτέλεσμα είναι οι χρήστες να είναι ευάλωτοι σε τέτοιου είδους εγκλήματα και οι αρχές να χάνουν πολύτιμο χρόνο, εωσότου αποκρυπτογραφήσουν την απειλή και το νέο τρόπο δράσης. Άλλωστε, αυτό που παρατηρείται είναι ότι οι δράστες επανέρχονται με βελτιωμένα λογισμικά και συστήματα συνεχίζοντας την εγκληματική τους δραστηριότητα[29].

[25] EUCPN, ο.π., 2015, σελ. 12
[26] Gosh S., Turrini, Cybercrimes: A Multidisciplinary Analysis, Springer, 2011, σελ.373
[27] EC3 Europol, The Internet Organized Crime Threat Assessment (iOcta), 2014, σελ.12
[28] Wall D.S., Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime, International Review of Law, Computers and Technology, vol. 51, 2008
[29] City of London, The implications of economic cybercrime for policing,' Research report City of London corporation, 2015, σελ. 26

4.Επεκτασιμότητα. Ένα σημαντικό πλεονέκτημα για τους δράστες των κυβερνοεγκλημάτων αποτελεί το γεγονός ότι έχουν τη δυνατότητα να πολλαπλασιάσουν τα αποτελέσματα των εγκληματικών τους πράξεων και σε σύντομο χρονικό διάστημα να πολλαπλασιάσουν τα θύματα τους, χωρίς να καταβάλλουν ιδιαίτερο πνευματικό και σωματικό κόπο[30]. Για παράδειγμα, ένας διαρρήκτης θα έπρεπε με φυσική παρουσία να αφαιρέσει το αντικείμενο, να το μεταφέρει, να διαφύγει από τον τόπο του εγκλήματος, να προσέξει μη το δουν μάρτυρες και τέλος να διαφυλάξει ή να πουλήσει το κλοπιμαίο. Αντίθετα στον κυβερνοχώρο, δεν θα ήταν υπερβολή να ειπωθεί ότι την ίδια στιγμή οι δράστες δύνανται να προσβάλλουν εκατομμύρια υπολογιστές χωρίς κανένα επιπλέον κόστος[31].

[30] Gosh, S., Turrini, E., ο.π., σελ. 373, απ' όπου εξικνείται και το ακόλουθο παράδειγμα
[31] EC3, Europol, First Year Report, σελ. 26

4. ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Στην πρώιμη έκδοση του, το κυβερνοέγκλημα εμφανίζεται αρχικά με δράστες μεμονωμένα άτομα που κατείχαν ειδικές γνώσεις προγραμματισμού και αφορούσε κυρίως την παραβίαση συστημάτων και δικτύων κινητών τηλεφώνων. Αργότερα, κατά την διάρκεια του Ψυχρού Πολέμου, οι Αμερικανικές Υπηρεσίες ανατίναξαν έναν αγωγό αερίου στην Σιβηρία εισάγοντας στο δίκτυο των υπολογιστικών συστημάτων που ήλεγχαν τον αγωγό έναν κώδικα με την ονομασία «The Logic Bomb». Αποτέλεσμα ήταν η κυβερνοεπίθεση αυτή να προκαλέσει την μεγαλύτερη έως τότε μη πυρηνική έκρηξη και να κοστίσει δισεκατομμύρια χρήματα με ανάλογες γεωπολιτικές συνέπειες.

Το 1983 ο Fred Cohen παρουσίασε ένα πρόγραμμα ικανό να εξαπλωθεί από την μία μηχανή στην άλλη ως ένα παράσιτο σε μια νόμιμη εφαρμογή. Αυτό το πρόγραμμα μπορεί ουσιαστικά να θεωρηθεί το πρώτο κακόβουλο λογισμικό σε υπολογιστή. Το 1988 δημιουργείται το πρώτο «σκουλήκι» (worm) του διαδικτύου, γνωστό με την ονομασία το Σκουλήκι του Morris, από τον δημιουργό του Rober Morris φοιτητή του Πανεπιστημίου Cornell. Παρόλο που η πρόθεση του δημιουργού του ήταν να εντοπίσει τα όρια του διαδικτύου, το σκουλήκι αυτό μόλυνε χιλιάδες υπολογιστές και προκάλεσε ζημίες που υπερβαίνουν το ποσό των δέκα εκατομμυρίων δολαρίων. Μάλιστα, ο Rober Morris κατέστη ο πρώτος που καταδικάστηκε για παράβαση του νόμου περί απάτης και κατάχρησης με υπολογιστή.

Η δεκαετία του 1990 σημαδεύτηκε από την δημιουργία και εξάπλωση παγκόσμιου δικτύου World Wide Web (WWW) και του internet με αποτέλεσμα την ανάδυση της ανάγκης για ασφάλεια των λογισμικών και του διαδικτύου. Έκτοτε, οι επιθέσεις αυξάνονται, καθώς τα αρχικά πρωτόκολλα του διαδικτύου είχαν ως κύριο μέλημα τους την χρησιμότητα και για τον λόγο αυτόν δεν υπήρξαν σκέψεις για ζητήματα ασφαλείας. Μοιραία, την έλλειψη αυτή εκμεταλλεύτηκαν εγκληματίες για να εξαπολύσουν μαζικές επιθέσεις με κορυφαία την επίθεση με το σκουλήκι Melissa όπου μόλυνε χιλιάδες υπολογιστές και προκάλεσε σοβαρή ανωμαλία στην λειτουργία των ηλεκτρονικών ταχυδρομείων. Γενικότερα, έως το 2000 το

κυβερνοέγκλημα παρατηρείται σε μεμονωμένες περιπτώσεις και όχι οργανωμένα. Παράλληλα, οι εθνικοί νομοθέτες και οι αρχές επιβολής του νόμου δεν συγκαταλέγουν στις προτεραιότητές τους την αντιμετώπιση του κυβερνοεγκλήματος καίτοι ορισμένες επιθέσεις είχαν προκαλέσει ήδη ζημιές εκατομμυρίων[32].

Την πρώτη δεκαετία του 2000 οι χρήστες του διαδικτύου ξεπέρασαν τους 300 εκατομμύρια. Η μαζική υιοθέτηση του διαδικτύου άνοιξε την πόρτα για νέες επιθέσεις, όπως το σκουλήκι I LOVE YOY στις αρχές του 2000 όπου μόλυνε περισσότερα από 50 εκατομμύρια συστήματα τις πρώτες δέκα ημέρες της δημιουργίας του. Η συνεχής αύξηση του κυβερνοεγκλήματος οδήγησε το 2001 το Συμβούλιο της Ευρώπης να προτείνει την Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα, όπου υπεγράφη από περισσότερες από 60 χώρες. Το επόμενο έτος η Ευρωπαϊκή Ένωση υιοθέτησε την Οδηγία ePrivacy, ενώ το 2003 οι Η.Π.Α. παρουσίασαν την εθνική τους στρατηγική για το κυβερνοέγκλημα με την ονομασία National Cyber Security Division.

Την δεκαετία του 2010 ο αριθμός των χρηστών του διαδικτύου αυξάνεται με εκθετικούς ρυθμούς και η κυβερνοασφάλεια αποκτά όλο και πιο κεντρικό ρόλο στις πολιτικές άμυνας και ασφάλειας των κρατών και οργανισμών. Παράλληλα, το κυβερνοέγκλημα εξελίσσεται και τα ποσοστά του αυξάνονται με δραματικούς ρυθμούς. Ενδεικτικά, το 2012 μια σειρά από οργανωμένες κυβερνοεπιθέσεις είχαν σαν αποτέλεσμα την διαρροή και υποκλοπή προσωπικών δεδομένων και δεδομένων τραπεζικών καρτών εκατομμυρίων χρηστών. Ακολούθησαν σημαντικές επιθέσεις που επηρέασαν εκατομμύρια χρήστες και έπληξαν τομείς όπως η βιομηχανία, η αγορά ακινήτων, η ακαδημαϊκή κοινότητα και η διακυβέρνηση. Οι ανωτέρω επιθέσεις εκμεταλλεύτηκαν τον πολλαπλασιασμό των συνδεδεμένων συσκευών, διαμοιράζοντας βλαβερά λογισμικά όπως το ransomware WannaCry και το botnet Mirai.

Κατά την διάρκεια της πανδημίας έγινε εμφανής η έλλειψη διεθνώς συμφωνημένων κανόνων στην κυβερνοασφάλεια με αποτέλεσμα να αυξάνεται

[32] Βλ ενδεικτικά υπόθεση Morris με κόστος 10εκ $ και την υπόθεση Vladmir Levnin με το ίδιο κόστος

συνεχώς η πεποίθηση για την απαίτηση ενός τύπου «Ψηφιακής Σύμβασης της Γενεύης»[33].

[33] Ευρωπαϊκή Επιτροπή, EVOLUTION OF A MULTIFACETED DISCIPLINE, σε CYBERSECURITY, σελ. 13 - 15

5. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΚΑΤΑΣΤΟΛΗΣ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Η ανάγκη αντιμετώπισης του κυβερνοεγκλήματος καθώς και ο διασυνοριακός του χαρακτήρας κατέστησαν αναγκαία την λήψη μέτρων μεταξύ των κρατών. Τα μέτρα αυτά συναντώνται τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο. Άλλωστε, το γεγονός ότι το κυβερνοέγκλημα αποτελεί την μόνη μορφή εγκλήματος που μπορεί να λάβει διεθνικές διαστάσεις σε ταχύτατο χρονικό διάστημα καθιστά την εναρμόνιση μεταξύ των εθνικών νομοθεσιών ζωτικής σημασίας για την αποτελεσματικότητα των σχετικών ρυθμίσεων[34]. Το κυριότερο νομικό κείμενο[35] αποτελεί η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, γνωστή και ως Σύμβαση της Βουδαπέστης. Στην σύμβαση αυτή προστέθηκε αργότερα, την 28/01/2001, Πρωτόκολλο για το Κυβερνοέγκλημα. Μάλιστα, η ανωτέρω σύμβαση έχει επηρεάσει καθοριστικά το μετέπειτα νομικό πλαίσιο για το κυβερνοέγκλημα στις εθνικές και ενωσιακές πολιτικές[36]. Σε ευρωπαϊκό επίπεδο, έχουν εκδοθεί Οδηγίες για το Κυβερνοέγκλημα και τις διάφορες μορφές του.

5.1. ΔΙΕΘΝΕΣ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Στις 23 Νοεμβρίου 2001 υπεγράφη, από 26 κράτη μέλη του Συμβουλίου της Ευρώπης και 4 κράτη παρατηρητές,[37] η Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο. Αργότερα, στις 28 Ιανουαρίου 2003, συμπληρώθηκε από ένα Πρόσθετο Πρωτόκολλο για την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω υπολογιστικών συστημάτων. Ημερομηνία έναρξης ισχύος της Σύμβασης καθορίστηκε η 1η Απριλίου 2004. Η Σύμβαση της Βουδαπέστης έχει επικυρωθεί απ' όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης πλην της Ρωσίας. Η επικύρωση της Σύμβασης στην ελληνική έννομη τάξη πραγματοποιήθηκε

[34] Jonathan Clough, A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonization, Monash University Law Review (Vol 40, No 3), σελ. 700
[35] Chaikin, David, Network investigations of cyber attacks: The limits of digital evidence, Crime, Law and Social Change, 2006, σελ. 246
[36] Calderoni, Francesco, The European legal framework on cybercrime: Striving for an effective implementation, Crime, Law and Social Change, 2010, σελ 340
[37] Καναδάς, Ιαπωνία, Ν. Αφρική και Η.Π.Α

με το Ν. 4411/2016, ενώ από τα κράτη παρατηρητές την Σύμβαση δεν έχει επικυρώσει μόνο η Ν. Αφρική. Στόχος της Σύμβασης είναι να αναπτυχθεί κατά προτεραιότητα μία κοινή αντεγκληματική πολιτική που θα στοχεύει στην προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο, κυρίως με την υιοθέτηση της κατάλληλης νομοθεσίας και την ενίσχυση της διεθνούς συνεργασίας[38].

Στο πρώτο τμήμα της, η Σύμβαση της Βουδαπέστης περιέχει διατάξεις σχετικές με το ουσιαστικό ποινικό δίκαιο. Σκοπός αυτών των διατάξεων είναι η θέσπιση ελάχιστων κριτηρίων, με την πλήρωση των οποίων μία πράξη θα τιμωρείται από τις εθνικές έννομες τάξεις[39]. Με άλλες λέξεις, επιχειρείται ένα είδος εναρμόνισης των εθνικών νομοθεσιών στο πεδίο του κυβερνοεγκλήματος, θέτοντας τα ελάχιστα χαρακτηριστικά για την ποινικοποίηση της συμπεριφοράς του δράστη. Με αυτόν τον τρόπο, καταβάλλεται προσπάθεια να αποφευχθούν εμπόδια που προκύπτουν από την ύπαρξη διαφορετικών νομικών κανόνων σε κάθε κράτος. Αυτό συμβαίνει για παράδειγμα όταν η ίδια συμπεριφορά, που έχει διασυνοριακό χαρακτήρα και τελείται σε περισσότερα κράτη ταυτόχρονα, τιμωρείται από την μία έννομη τάξη και όχι από την άλλη[40].

Το πρώτο τμήμα αποτελείται από τέσσερις τίτλους, όπου κάθε ένας περιέχει επιμέρους διατάξεις για τις σχετικές εγκληματικές συμπεριφορές. Ο πρώτος τίτλος, ποινικοποιεί πράξεις που στρέφονται κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών. Οι πράξεις αυτές, κατά την Σύμβαση, συνίστανται στην παράνομη πρόσβαση[41], την υποκλοπή[42], στις παρεμβολές στα δεδομένα[43] και στα συστήματα[44], καθώς και στην κακή χρήση των συσκευών[45]. Όλες οι παραπάνω πράξεις, όπως και όλες οι πράξεις που αναφέρονται στην Σύμβαση, απαιτείται να διαπράττονται σε διεθνικό επίπεδο για να τύχει εφαρμογής η εν λόγω Σύμβαση[46].

[38] Σύμβαση της Βουδαπέστης, προοίμιο
[39] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σελ. 8
[40] Calderoni, Francesco, ο.π., σελ 342
[41] Άρθρο 2 της Σύμβασης
[42] Άρθρο 3 της Σύμβασης
[43] Άρθρο 4 της Σύμβασης
[44] Άρθρο 5 της Σύμβασης
[45] Άρθρο 6 της Σύμβασης
[46] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 39

Το εδαφικό πεδίο εφαρμογής της Σύμβασης εξαρτάται από δήλωση του κάθε συμβαλλόμενου κράτους, με την οποία ορίζεται η εδαφική επικράτεια που επιθυμεί το κράτος να ισχύουν οι διατάξεις της Σύμβασης. Ο καθορισμός γίνεται από το κράτος κατά την στιγμή της υπογραφής ή της κατάθεσης του εγγράφου κύρωσης, αποδοχής, έγκρισης ή προσχώρησης στην Σύμβαση. Η Σύμβαση, πλέον, έχει πεδίο εφαρμογής το έδαφος των κρατών που διέπονται από αυτήν.

Το άρθρο 1 της Σύμβασης παραθέτει τους απαραίτητους ορισμούς για την ορθή ερμηνεία των διατάξεων της Σύμβασης. Έτσι, «*σύστημα υπολογιστή*» νοείται μία συσκευή ή ένα σύνολο διασυνδεδεμένων ή σχετιζόμενων συσκευών, μία ή περισσότερες από τις οποίες πραγματοποιεί αυτόματη επεξεργασία δεδομένων βάσει ενός προγράμματος. «*Δεδομένα υπολογιστών*» σημαίνει αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή. «*Πάροχος υπηρεσιών*» νοείται κάθε δημόσιος ή ιδιωτικός φορέας που παρέχει στους χρήστες των υπηρεσιών του την δυνατότητα να επικοινωνούν μέσω ενός συστήματος υπολογιστή, και κάθε άλλος φορέας που επεξεργάζεται ή αποθηκεύει δεδομένα υπολογιστών είτε για λογαριασμό αυτής της υπηρεσίας επικοινωνίας, είτε των χρηστών αυτής της υπηρεσίας. «*Δεδομένα κίνησης*» νοούνται τα δεδομένα υπολογιστών που σχετίζονται με μία επικοινωνία μέσω ενός συστήματος υπολογιστή, δημιουργούμενα από ένα σύστημα υπολογιστή που αποτελούσε τμήμα της αλυσίδας επικοινωνίας, τα οποία καταδεικνύουν την προέλευση, τον προορισμό, το δρομολόγιο, το χρόνο, την ημερομηνία, το μέγεθος, τη διάρκεια ή τον τύπο της υφιστάμενης υπηρεσίας της επικοινωνίας.

Το άρθρο 2 της Σύμβασης τιμωρεί την από πρόθεση πρόσβαση σε σύστημα υπολογιστή χωρίς το σχετικό δικαίωμα. Περαιτέρω, στο δεύτερο εδάφιο του, επιτρέπει τα συμβαλλόμενα μέρη να θέσουν ως προϋπόθεση την παραβίαση ενός μέτρου ασφαλείας για τον κολασμό της πράξης. Έτσι, παρέχεται μεγαλύτερη ελαστικότητα στα κράτη να αποκλείσουν περιπτώσεις ήσσονος σημασίας[47].

[47] Calderoni, Francesco, ο.π., σελ 342

Πράγματι, θα ήταν εξαιρετικά ανεπιεικές η απλή και μόνο πρόσβαση χωρίς δικαίωμα να ποινικοποιείται. Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή του ή του συστήματος υπολογιστή[48]. Αυτή η ρύθμιση χαρακτηρίζεται ως αυστηρή καθότι τιμωρεί περιπτώσεις χωρίς να εξετάζεται αν από την χωρίς δικαίωμα πρόσβαση επιχειρείται ή προκαλείται περαιτέρω ζημιά[49]. Για τον λόγο αυτό, αναφέρεται ότι απαιτείται το σύστημα υπολογιστή να συνοδεύεται από περιορισμούς που έχουν εισαχθεί με κώδικα και κατά συνέπεια την παραβίαση αυτού του κώδικα από τον χρήστη προκειμένου να αποκτήσει πρόσβαση[50]. Πάντως, το εδάφιο έχει κατακριθεί για το γεγονός ότι με αυτή την πρόσθετη προϋπόθεση δυσχεραίνεται η εναρμόνιση[51] και δεν υπάγονται περιπτώσεις υπολογιστικών συστημάτων με ασαφή μέτρα ασφαλείας και εξουσιοδοτήσεων[52].

Το άρθρο 3 της Σύμβασης ποινικοποιεί την υποκλοπή διαβιβάσεων δεδομένων υπολογιστή που γίνεται με την χρήση τεχνικών μέσων και δεν είναι δημόσια. Η διαβίβαση μπορεί να πραγματοποιείται εντός του ίδιου υπολογιστή ή από ή προς τον υπολογιστή. Η πράξη τιμωρείται όταν διαπράττεται με πρόθεση, ενώ στο πεδίο εφαρμογής του παρόντος εμπίπτει και η περίπτωση των ηλεκτρομαγνητικών εκπομπών. Αυτό σημαίνει ότι σε αυτό το άρθρο υπάγονται οι ασύρματες διαβιβάσεις και εκπομπές καθώς και τεχνολογίες που διαβάζουν ή ανιχνεύουν οπτικές εκπομπές από οθόνες ή καλώδια οπτικών ινών ή εκπομπές μέσω τηλεφώνων, ενσύρματων ή ασύρματων, όπως τα κινητά τηλέφωνα[53]. Το άρθρο αυτό, θα μπορούσε να ειπωθεί ότι παρουσιάζει ομοιότητα με τις παραδοσιακές

[48] Δ.Π. Αγγελόπουλος, Κυβερνοχώρος - Το διεθνές «γίγνεσθαι» στο ελληνικό «είναι», ΕΛ.Ε.Σ.ΜΕ., διαθέσιμο σε http://www.elesme.gr/elesmegr/periodika/t19/t19_03.htm

[49] JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME, ITU, 2005 σελ 11

[50] Kerr Orin, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, New York University law review, 2003, σελ. 1600

[51] Mercado Kierkegaard, Sylvia, Here comes the 'cybernators!', Computer Law & Security Report, 22, 2006, σελ. 386

[52] Flanagan Anne, The law and computer crime: Reading the Script of Reform, International Journal of Law and Information Technology, 2005, σελ 110

[53] Flanagan Anne, ο.π., σελ 111

περιπτώσεις απαγόρευσης υποκλοπής τηλεφωνικών συνομιλιών, προσαρμοσμένο στη σύγχρονη πλέον εποχή της τεχνολογίας. Αναφορικά με την διάταξη του άρθρου 3, διευκρινίζεται ότι είναι απαραίτητη η χρήση τεχνικών μέσων, όπως προγράμματα υπολογιστών, κωδικών πρόσβασης και κωδικών ασφαλείας, προκειμένου να αποφεύγεται η υπερβολική διεύρυνση του πεδίου εφαρμογής[54].

Η διαβίβαση είναι δυνατό να πραγματοποιείται με ποικίλους τρόπους, όπως μέσω τηλεφώνου, τηλεομοιότυπου ή μέσω μεταφοράς αρχείων. Μια διαβίβαση χαρακτηρίζεται ως μη δημόσια όταν είναι εμπιστευτική[55]. Τέλος, αναφέρεται ότι η προϋπόθεση της μη δημόσιας διαβίβασης αφορά την διαβίβαση καθαυτή και όχι το περιεχόμενο που διαβιβάζεται. Δηλαδή, το κρίσιμο στοιχείο δεν είναι η φύση των δεδομένων που διαβιβάζονται αλλά η φύση της διαβίβασης που λαμβάνει χώρα[56]. Έτσι, δύναται να εμπίπτει στην απαγορευτική διάταξη του άρθρου 3 η διαβίβαση δημόσια προσβάσιμων δεδομένων. Ακόμη και η χρήση δημόσιων δικτύων δεν αποκλείει την εφαρμογή του παρόντος άρθρου.

Κατά την εφαρμογή του ανωτέρω άρθρου, προέκυψε το ερώτημα για το εάν εμπίπτουν στο πεδίο εφαρμογής του κι άλλες περιπτώσεις, εκτός από την παρακολούθηση των διαδικασιών μεταφοράς, όπως για παράδειγμα η παράνομη πρόσβαση πληροφοριών που βρίσκονται αποθηκευμένες σε σκληρό δίσκο. Με βάση το δεδομένο ότι το εν λόγω άρθρο απαιτεί μια διαδικασία μεταφοράς, είναι πιθανό η ανωτέρω περίπτωση να μην καλύπτεται από το άρθρο 3 της Σύμβασης[57]. Το γεγονός αυτό, αναδύει την ανάγκη να αξιολογηθούν οι υφιστάμενοι μηχανισμοί για την προστασία των πληροφοριών ώστε να καλύπτουν και τις περιπτώσεις κατασκοπείας δεδομένων που βρίσκονται αποθηκευμένα σε υπολογιστή καθώς πλέον η πλειονότητα των δεδομένων βρίσκεται αποθηκευμένη σε συστήματα υπολογιστών[58]. Άλλωστε, αναπάντητο παραμένει το ερώτημα εάν το άρθρο 3 εφαρμόζεται μόνο στην περίπτωση που ο χρήστης αποστέλλει δεδομένα, τα οποία στην συνέχεια

[54] JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, ο.π., σελ 12
[55] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 54
[56] Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU Telecommunication Development Bureau, 2012, σελ. 186
[57] Marco Gercke, ο.π., σελ. 182
[58] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, σελ. 31, διαθέσιμο σε: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

υποκλέπτονται ή το άρθρο τυγχάνει εφαρμογής και στην περίπτωση που ο παραβάτης χειρίζεται ο ίδιος τον υπολογιστή και υποκλέπτει δεδομένα. Η τελευταία περίπτωση αφορά την παράνομη απόκτηση δεδομένων υπολογιστή[59].

Αυτόδηλο είναι ότι η πρόσβαση στις πληροφορίες είναι ποινικά κολάσιμη όταν γίνεται με πρόθεση και χωρίς δικαίωμα. Κατά συνέπεια, δεν αποτελεί πρόσβαση άνευ δικαιώματος η πρόσβαση που πραγματοποιείται κατόπιν εξουσιοδότησης ή με συμφωνία των μερών που πραγματοποιούν την μεταφορά. Περαιτέρω, δεν απαγορεύεται από τις διατάξεις του άρθρου 3 η πρόσβαση που πραγματοποιείται από τις αρμόδιες αρχές για λόγους εθνικής ασφάλειας ή για την διενέργεια νόμιμων ανακριτικών πράξεων. Επίσης, η χρήση κοινών εμπορικών πρακτικών, όπως η χρήση «cookies», δεν ποινικοποιείται με το παρόν άρθρο και ως εκ τούτου δεν συνιστά πρόσβαση χωρίς δικαίωμα. Τέλος, αναφορικά με τις μη δημόσιες επικοινωνίες εργαζομένων που προστατεύονται, παρέχεται η ευχέρεια στους εγχώριους νομοθέτες να θεσπίσουν κανόνες που περιέχουν λόγους για τη νόμιμη παρακολούθηση των ανωτέρω επικοινωνιών[60].

Η Σύμβαση της Βουδαπέστης, στο τελευταίο εδάφιο του άρθρου 3, παρέχει την δυνατότητα στα συμβαλλόμενα μέρη να θέσουν ως επιπλέον προϋπόθεση για τον κολασμό της πράξης την αθέμιτη πρόθεση ή την επίτευξη της σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο. Τα κράτη που επιλέγουν να κάνουν χρήση αυτής της δυνατότητας πρέπει να ερμηνεύουν και να εφαρμόζουν αυτά τα στοιχεία σε συνδυασμό με τις υπόλοιπες έννοιες του άρθρου, όπως τις έννοιες «σκόπιμα» και «χωρίς δικαίωμα»[61].

Το άρθρο 4 της Σύμβασης απαγορεύει τις παρεμβολές σε δεδομένα, οι οποίες συνίσταντο στην άνευ δικαιώματος βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστών. Πράγματι, η εκθετικά αυξανόμενη ψηφιοποίηση του συνόλου των πληροφοριών, που υπάρχουν στις επιχειρήσεις, έχει οδηγήσει στην αποθήκευση των εν λόγω πληροφοριών με την μορφή ψηφιακών δεδομένων. Οι πληροφορίες αυτές δύνανται να αφορούν, μεταξύ άλλων, οικονομικά στοιχεία της

[59] Marco Gercke, ο.π., σελ. 185
[60] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 58
[61] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 59

επιχείρησης ή δεδομένα προσωπικού χαρακτήρα χρηστών και ως εκ τούτου οι διαχειριστές τους δεν επιθυμούν να λάβουν γνώση για το περιεχόμενο τους τρίτα άτομα. Η πρόσβαση, η διαγραφή ή η τροποποίηση των δεδομένων από μη εξουσιοδοτημένα άτομα είναι πιθανό να προκαλέσει οικονομική ζημία[62] στις επιχειρήσεις ή βλάβη στα συμφέροντα φυσικών προσώπων[63]. Έτσι, το άρθρο 4 της Σύμβασης καλύπτει το κενό που υπήρχε στην προστασία αυτών των δεδομένων και πλέον τους προσδίδει παρόμοια προστασία με αυτή που παρέχεται στα ενσώματα αντικείμενα. Επιπροσθέτως, προστατευόμενο αγαθό στο εν λόγω άρθρο είναι η ακεραιότητα και η σωστή λειτουργία ή χρήση των αποθηκευμένων σε υπολογιστή δεδομένων καθώς και των προγραμμάτων υπολογιστών[64].

Από την γραμματική ερμηνεία του άρθρου 4, συνάγεται ότι η Σύμβαση ποινικοποιεί πέντε πράξεις που σχετίζονται με τις παρεμβολές στα δεδομένα, οι οποίες όπως αναφέρθηκε παραπάνω συνίστανται στην βλάβη, διαγραφή, φθορά, αλλοίωση και την καταστολή δεδομένων υπολογιστών. Οι όροι «*βλάβη*» και «*φθορά*» αναφέρονται σε οποιαδήποτε πράξη σχετίζεται με αρνητική αλλοίωση της ακεραιότητας του περιεχομένου των πληροφοριών, δεδομένων και προγραμμάτων. Η *διαγραφή* των δεδομένων, κατά το άρθρο αυτό, ισοδυναμεί με την καταστροφή ενός ενσώματου αντικειμένου[65]. Όπως παρατηρείται, η Σύμβαση δεν πραγματοποιεί διάκριση μεταξύ των περισσότερων δυνατών τρόπων διαγραφής δεδομένων. *Καταστολή* δεδομένων υπάρχει όταν κάποιος, με ενέργεια, αποτρέπει ή τερματίζει την διαθεσιμότητα των δεδομένων στον δικαιούμενο, την πρόσβαση στον υπολογιστή ή την πρόσβαση στον φορέα που τα δεδομένα έχουν αποθηκευτεί. Τέλος, ο όρος *αλλοίωση* δεδομένων σημαίνει την τροποποίηση ήδη υφιστάμενων δεδομένων. Έτσι, η εισαγωγή κακεντρεχών κωδίκων όπως οι ιοί και οι δούρειοι ίπποι τιμωρούνται βάσει αυτής της παραγράφου, καθώς έχουν ως αποτέλεσμα την τροποποίηση δεδομένων.

---

[62] 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code, διαθέσιμο σε: www.computereconomics.com/article.cfm?id=1225

[63] Βλ. ενδεικτικά Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU Telecommunication Development Bureau, 2012, σελ. 29

[64] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 60

[65] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 61

Το άρθρο 5 της Σύμβασης ποινικοποιεί την άνευ δικαιώματος σοβαρή παρακώλυση της λειτουργίας ενός συστήματος υπολογιστή δια της εισαγωγής, διαβίβασης, βλάβης, διαγραφής, φθοράς, αλλοίωσης ή καταστολής δεδομένων υπολογιστή. Για τις παραπάνω πράξεις ο δράστης απαιτείται να ενεργεί με πρόθεση. Το παρόν άρθρο, ουσιαστικά, ποινικοποιεί πράξεις που προκαλούν σαμποτάζ στον υπολογιστή[66]. Παρατηρείται ότι η γραμματική αποτύπωση του άρθρου είναι ουδέτερη, έτσι ώστε το πεδίο εφαρμογής να καταλαμβάνει όλες τις λειτουργίες του υπολογιστή και ως εκ τούτου να τις προστατεύει[67]. Ο όρος «*παρακώληση*», αναφέρεται σε πράξεις που παρεμβαίνουν στην σωστή λειτουργία ενός υπολογιστικού συστήματος. Αυτή η παρακώληση συγκεκριμενοποιείται από το ίδιο το άρθρο που προβλέπει ότι πρέπει να συνίσταται σε εισαγωγή, διαβίβαση, βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστή. Ωστόσο, προϋπόθεση για να διωχθούν οι παραπάνω πράξεις είναι η παρακώληση να είναι σοβαρή. Η Σύμβαση δεν αναφέρει ποιες πράξεις θεωρούνται σοβαρές. Ο καθορισμός επαφίεται στην διακριτική ευχέρεια των κρατών. Κατά συνέπεια, η ίδια συμπεριφορά δύναται να χαρακτηρίζεται ως σοβαρή από μία χώρα ενώ από κάποια άλλη όχι και ως εκ τούτου να μην τιμωρείται στο δίκαιο της εν λόγω χώρας. Στην επεξηγηματική έκθεση παρατίθεται τι θα μπορούσε ενδεχομένως να χαρακτηριστεί ως σοβαρή παρακώληση. Έτσι, αναφέρεται ότι ως σοβαρή θεωρείται η παρακώληση που συνίσταται στην αποστολή δεδομένων σ' ένα συγκεκριμένο σύστημα σε τέτοια μορφή, μέγεθος ή συχνότητα με τέτοιο τρόπο ώστε να προκαλείται σημαντικά επιζήμια επίδραση στον ιδιοκτήτη ή στον χειριστή του συστήματος να χρησιμοποιήσει το σύστημα ή να επικοινωνήσει με άλλα συστήματα[68]. Τέλος, απαιτείται η παρακώληση να πραγματοποιείται χωρίς δικαίωμα. Συνηθισμένες δραστηριότητες οι οποίες αφορούν την σχεδίαση του δικτύου ή συμφυείς κοινές επιχειρησιακές ή εμπορικές πρακτικές θεωρούνται ότι γίνονται με σχετικό δικαίωμα, οπότε δεν τιμωρούνται με την ανωτέρω διάταξη. Τέτοιες δραστηριότητες θεωρούνται, για παράδειγμα, ο έλεγχος της ασφάλειας ενός υπολογιστικού

[66] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, άρθρο 5
[67] Csonka, Peter, The council of europe's convention on cyber-crime and other European initiatives, Revue internationale de droit pénal, vol. 77, no. 3-4, 2006, σελ. 485
[68] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 67

συστήματος ή η αναδιαμόρφωση του λογισμικού του συστήματος με την εγκατάσταση νέου ή την τροποποίηση του παλαιού λογισμικού, που πραγματοποιούνται μετά την έγκριση του ιδιοκτήτη ή του χειριστή του συστήματος[69]. Κατά συνέπεια, όταν υπάρχει εξουσιοδότηση η πρόσβαση γίνεται με δικαίωμα. Η σχετική εξουσιοδότηση μπορεί να πηγάζει από το νόμο, από δικαστική πράξη, από συμβόλαιο ή κατόπιν συναίνεσης ή έγκρισης ή γενικότερα να επιτρέπεται από το εσωτερικό δίκαιο.

Στο πλαίσιο του παρόντος άρθρου τιμωρείται και το spamming, δηλαδή η συνεχής και αυτόκλητη αποστολή μηνυμάτων σε μεγάλο αριθμό παραληπτών και σε μεγάλη συχνότητα για εμπορικούς ή άλλους λόγους (π.χ. προσηλυτισμός). Η πιο συνηθισμένη μορφή spamming είναι αυτή που επιχειρείται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e mails), ωστόσο μπορεί να λάβει και άλλες μορφές, όπως η αποστολή μηνυμάτων στο κινητό τηλέφωνο. Τα συμβαλλόμενα μέρη θεωρούν ότι για να ποινικοποιηθεί το spamming πρέπει αυτό να γίνεται με πρόθεση και να προκαλεί σοβαρή παρακώληση. Έτσι, επαφίεται στην διακριτική ευχέρεια των κρατών να ορίσουν τις πρακτικές εκείνες που αποτελούν σοβαρή παρακώληση, ποινικοποιώντας, ολικά ή μερικά, συγκεκριμένες πράξεις στο εσωτερικό τους δίκαιο.

Το άρθρο 6 της Σύμβασης προτρέπει το κάθε μέρος να λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος και από πρόθεση παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση μιας συσκευής, περιλαμβανομένου και ενός προγράμματος υπολογιστή, σχεδιασμένης ή προσαρμοσμένης πρωτίστως με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα άρθρα 2 έως 5, καθώς και ενός συνθηματικού ή κωδικού πρόσβασης, ή άλλου παρεμφερούς δεδομένου, με την χρήση του οποίου είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός συστήματος υπολογιστή, με πρόθεση να χρησιμοποιηθεί για τον σκοπό της διάπραξης κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω άρθρα 2 έως 5, και κατοχή ενός αντικειμένου από τα αναφερόμενα στις

[69] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 68

παραγράφους α.ι και α.ιι, με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα Άρθρα 2 έως 5.

Το εν λόγω άρθρο τιμωρεί, ουσιαστικά, την κατοχή μέσων ή εργαλείων με τα οποία πραγματοποιούνται τα εγκλήματα των άρθρων 2 – 5. Ο δικαιολογητικός λόγος του άρθρου είναι ότι με την κατοχή τέτοιων μέσων μπορεί να υποτεθεί σοβαρά ότι υπάρχει πρόθεση διάπραξης των ανωτέρω εγκλημάτων και ο κάτοχος τους έχει εγκληματικούς σκοπούς[70]. Άρα, με το παρόν άρθρο επιχειρείται η πρόληψη τέτοιων εγκλημάτων εν την γενέσει τους. Μάλιστα, με την ανάδυση του Διαδικτύου των Πραγμάτων (Internet of Things) η κακή χρήση των συσκευών αποκτά ακόμα σημαντικότερο ρόλο σε σχέση με αυτόν που κατείχε κατά τον χρόνο υπογραφής της Σύμβασης. Αυτό καθίσταται εναργές αν ο παρατηρητής λάβει υπόψη του ότι πλέον υπάρχει η δυνατότητα να χειριζόμαστε συσκευές και πράγματα από απόσταση διαμέσου άλλων συσκευών. Έτσι, οι συσκευές αυτές μπορεί να αποτελέσουν σημεία εισόδου στο δίκτυο ή να χρησιμεύσουν ως εργαλεία για κακή χρήση των συσκευών[71].

Εννοιολογικά, ο όρος διανομή αναφέρεται στην ενεργή προώθηση δεδομένων σε άλλους. Ο όρος διάθεση αναφέρεται στην τοποθέτηση ηλεκτρονικών συσκευών για χρήση από άλλους καθώς και στην δημιουργία ή συλλογική παράθεση υπερσυνδέσμων για την διευκόλυνση της πρόσβασης σε ηλεκτρονικές συσκευές. Παράλληλα, ως πρόγραμμα υπολογιστή, με το οποίο σκοπείται η διάπραξη των εν λόγω εγκληματών, νοούνται τα προγράμματα που έχουν σχεδιαστεί για να τροποποιούν ή να καταστρέφουν δεδομένα ή γενικά να παρεμβαίνουν στην λειτουργία των συστημάτων, όπως τα προγράμματα ιών.

Ζήτημα συζήτησης αποτέλεσε αν το πεδίο εφαρμογής καταλάμβανε μόνο τις συσκευές που έχουν σχεδιαστεί αποκλειστικά ή συγκεκριμένα για την διάπραξη των ανωτέρω προσβολών, αποκλείοντας έτσι από το πεδίο εφαρμογής του παρόντος άρθρου συσκευές με πολλαπλές χρήσεις. Έτσι, από την μία πλευρά υπήρξε η προοπτική να εμπίπτουν στο πεδίο εφαρμογής συσκευές με αποκλειστικά τέτοια χρήση και από την άλλη πλευρά η προοπτική να εμπίπτουν όλες ανεξαιρέτως οι

[70] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 71
[71] David Wicki-Birchler, The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?, σε Cybersecur Law Review, 2020, σελ 67

τέτοιου είδους συσκευές ακόμα και αν έχουν παραχθεί και διανεμηθεί νόμιμα. Ωστόσο, κρίθηκε ότι η πρώτη λύση στενεύει υπερβολικά το πεδίο εφαρμογής του άρθρου 6 και θα μπορούσε να οδηγήσει σε ανυπέρβλητες δυσκολίες στην ποινική διαδικασία, καθιστώντας την εφαρμογή του άρθρου σπάνια. Ως εκ τούτου, αυτή η λύση απορρίφθηκε. Την ίδια τύχη είχε και η εναλλακτική επιλογή, καθότι η εφαρμογή του άρθρου θα εξαρτώταν από το υποκειμενικό στοιχείο της πρόθεσης διάπραξης των ανωτέρω εγκλημάτων. Τελικά, υιοθετήθηκε η πλέον συμβιβαστική λύση με το πεδίο εφαρμογής του άρθρου 6 να περιορίζεται με την εισαγωγή ενός αντικειμενικού κριτηρίου. Συγκεκριμένα, στο πεδίο εφαρμογής του παρόντος εμπίπτουν οι συσκευές που αντικειμενικά σχεδιάστηκαν ή δημιουργήθηκαν με πρωταρχικό και κύριο στόχο την διάπραξη των εν λόγω προσβολών[72].

Περαιτέρω, οι πράξεις που περιγράφονται στον παρόν άρθρο πρέπει να διαπράττονται με πρόθεση και χωρίς δικαίωμα. Ωστόσο, με σκοπό την αποφυγή υπερβολικής διεύρυνσης του πεδίου εφαρμογής του παρόντος, το άρθρο 6 απαιτεί επιπλέον και πέρα από την γενική πρόθεση, ειδική πρόθεση, δηλαδή άμεσο σκοπό διάπραξης των εγκλημάτων των άρθρων 2 – 5.

Ωστόσο, καμία ποινική ευθύνη δεν υπάρχει αν η παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση ή κατοχή όπως περιγράφεται στην παράγραφο 1 του παρόντος άρθρου δεν γίνεται με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα Άρθρα 2 έως 5 της παρούσας Σύμβασης[73]. Πρόκειται για τις περιπτώσεις εκείνες που δημιουργούνται εγκεκριμένα εργαλεία για την δοκιμή του υπολογιστή ή για λόγους προστασίας. Άλλωστε, αυτές οι περιπτώσεις καλύπτονται ήδη από το γεγονός ότι οι σχετικές πράξεις διενεργούνται με δικαίωμα και ως εκ τούτου δεν πληρείται η προϋπόθεση της άνευ δικαιώματος διάπραξης.

Τέλος, τα συμβαλλόμενα κράτη διατηρούν την ευχέρεια, δυνάμει και του άρθρου 42, να μην εφαρμόσουν την παράγραφο 1 του παρόντος άρθρου. Αυτή η

[72] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 73
[73] Άρθρο 6 παρ. 2 της Σύμβασης

ευχέρεια δεν υπάρχει αν οι πράξεις αφορούν την πώληση, την διαμονή ή την διάθεση των αντικειμένων που περιγράφονται στην παράγραφο 1[74].

Ο Τίτλος 2 της Σύμβασης περιέχει δύο κατηγορίες εγκλημάτων σχετικές με υπολογιστή και συγκεκριμένα την πλαστογραφία και την απάτη σχετική με υπολογιστή. Σύμφωνα με το άρθρο 7 «*Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η από πρόθεση και άνευ δικαιώματος εισαγωγή, αλλοίωση, διαγραφή ή καταστολή δεδομένων υπολογιστή, που έχει ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων, με σκοπό να θεωρηθούν αυτά αυθεντικά ή να γίνουν ενέργειες με βάση αυτά ωσάν να είναι αυθεντικά για νόμιμους σκοπούς, ασχέτως του εάν αυτά τα δεδομένα είναι ή όχι άμεσα αναγνώσιμα ή αντιληπτά*».

Σκοπός του άρθρου είναι να αποκαταστήσει ουσιαστικά το κενό που υπήρχε στο ποινικό δίκαιο με την παραδοσιακή έννοια της πλαστογραφίας, η οποία απαιτούσε οπτική αναγνωρισημότητα του αντικειμένου της πλαστογραφίας, προϋπόθεση που δεν μπορούσε προηγουμένως να εφαρμοστεί σε ψηφιακά αποθηκευμένα δεδομένα[75]. Πρόκειται, ουσιαστικά, για την ποινικοποίηση της πλαστογραφίας που διαπράττεται με ηλεκτρονικά μέσα. Τέτοιου είδους πλαστογραφία κρίθηκε ότι μπορεί να έχει ανάλογες συνέπειες με τις παραδοσιακές μορφές πλαστογραφίας παραπλανώντας με αυτόν τον τρόπο ένα τρίτο μέρος[76].

Η πλαστογραφία του άρθρου 7 περιλαμβάνει και τις περιπτώσεις της χωρίς άδειας δημιουργίας ή αλλαγής αποθηκευμένων δεδομένων κατά τρόπο τέτοιον ώστε αυτά να αποκτούν διαφορετική αποδεικτική αξία κατά την διενέργεια των διάφορων συναλλαγών. Αυτό συμβαίνει διότι οι συναλλαγές στηρίζονται στην αυθεντικότητα των πληροφοριών που περιέχονται στα δεδομένα, τα οποία αποτελούν το αντικείμενο της εξαπάτησης[77].

Η σημασία αυτού του άρθρου καθίσταται εναργέστερη αν ληφθεί υπόψη ότι με την πρόοδο της τεχνολογίας συνεχώς αυξάνεται η παραγωγή ψηφιακών –

[74] Άρθρο 6 παρ. 3 της Σύμβασης
[75] David Wicki-Birchler, ο.π., σελ 67
[76] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 81
[77] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 81

ηλεκτρονικών νομικών εγγράφων τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα. Τέλος, η Σύμβαση παρέχει την δυνατότητα στα συμβαλλόμενα μέλη να εισάγουν στα εθνικά τους δίκαια μία επιπλέον προϋπόθεση για τον κολασμό της πλαστογραφίας σχετικής με υπολογιστές. Η προϋπόθεση αυτή έγκειται στην ύπαρξη πρόθεσης εξαπάτησης ή παρόμοιας αθέμιτης πρόθεσης.

Η απάτη σχετική με υπολογιστές προβλέπεται στο άρθρο 8 της Σύμβασης, σύμφωνα με το οποίο « *Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της α. εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή, β. παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο*».

Η πρόοδος της τεχνολογίας κατέστησε εφικτό η διαχείριση της περιουσίας να μπορεί να πραγματοποιηθεί μέσω υπολογιστικών συστημάτων. Ως εκ τούτου, αναδύθηκε η ανάγκη προστασίας των πολιτών από νέες μορφές απάτης, όπως οι απάτες με την χρήση πιστωτικών καρτών. Η πραγματικότητα έδειξε ότι υπολογιστικά συστήματα που εκπροσωπούν ή διαχειρίζονται περιουσιακά στοιχεία έχουν γίνει στόχος εγκληματιών όπως οι παραδοσιακές μορφές ιδιοκτησίας. Έτσι, σκοπός της εν λόγω διάταξης είναι η ποινικοποίηση κάθε αθέμιτης χειραγώγησης κατά την διάρκεια επεξεργασίας των δεδομένων με πρόθεση την παράνομη μεταβίβαση περιουσίας[78].

Όπως και οι παραδοσιακές μορφές απάτης, το άρθρο 8 τιμωρεί πράξεις απάτης που πραγματοποιούνται με πρόθεση εξασφάλισης παράνομου οικονομικού οφέλους για τον δράστη ή τρίτο πρόσωπο και έχουν ως αποτέλεσμα την άμεση απώλεια περιουσίας ή ιδιοκτησίας τρίτου προσώπου. Έτσι, στόχος του παρόντος άρθρου είναι η ποινικοποίηση κάθε αθέμιτης χειραγώγησης κατά την διάρκεια της επεξεργασίας των δεδομένων που πραγματοποιείται με την πρόθεση να επιφέρει παράνομη μεταβίβαση περιουσίας[79]. Χαρακτηριστικό παράδειγμα απάτης με

[78] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 86
[79] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 86

υπολογιστή αποτελεί το mail phising, το οποίο συνίσταται στην αποστολή μηνυμάτων που παριστάνουν ότι διαθέτουν έναν νόμιμο εσωτερικό ή εξωτερικό αποστολέα και αιτούνται την μεταφορά χρημάτων προς αυτόν με διάφορα προσχήματα[80].

Περαιτέρω, προκειμένου να διασφαλιστεί ότι καταλαμβάνονται από το άρθρο 8 όλες οι πιθανές προσβολές και όχι μόνο οι πράξεις της εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή, η παράγραφος 2 συμπληρώνει τις ανωτέρω προσβολές με τον γενικό όρο της παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή.

Το άρθρο 9 της Σύμβασης ποινικοποιεί την παιδική πορνογραφία. Συγκεκριμένα, επιβάλλει στα συμβαλλόμενα μέρη να λάβουν όλα τα απαραίτητα νομοθετικά μέτρα για να τιμωρούνται στο εσωτερικό τους δίκαιο η παραγωγή, η προσφορά, η διάθεση, η διανομή, η μετάδοση, η κατοχή και η προμήθεια παιδικής πορνογραφίας μέσω ενός συστήματος υπολογιστή.

Το άρθρο αυτό θεσπίστηκε στο πλαίσιο της διεθνούς τάσης για την αποτελεσματική προστασία των ανήλικων, όπως διαφαίνεται και από την υιοθέτηση, πριν την Σύμβαση της Βουδαπέστης, του προαιρετικού πρωτοκόλλου στην Σύμβαση των Ηνωμένων Εθνών για τα δικαιώματα των παιδιών, την πώληση παιδιών, την παιδική πορνεία και την παιδική πορνογραφία[81] και την πρωτοβουλία της Ευρωπαϊκής Επιτροπής για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[82].

Η ανάγκη θέσπισης του εν λόγω άρθρου γίνεται αντιληπτή εάν λάβουμε υπόψη μας ότι το 15% των συλληφθέντων για σχετική με το διαδίκτυο παιδική πορνογραφία διέθετε περισσότερες από 1.000 φωτογραφίες στον υπολογιστή του, ενώ το 80% εξ αυτών κατείχε υλικό για παιδιά ηλικίας 6 – 12 ετών[83]. Επιπλέον, η

[80] David Wicki-Birchler, ο.π., σελ 68

[81] United Nations Human Rights, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Διαθέσιμο σε https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx

[82] COMMISSION OF THE EUROPEAN COMMUNITIES, Combating trafficking in human beings and combating the sexual exploitation of children and child pornography, COM(2000) 854 final /2, 22/1/2001, διαθέσιμο σε https://ec.europa.eu/anti-trafficking/sites/default/files/com_2000_854_proposal_for_framework_decisions_en_1.pdf

[83] Wolak/ Finkelhor/ Mitchell, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, σελ. 5

παιδική πορνογραφία αποδεικνύεται ιδιαίτερα επικερδής[84] και η διενέργεια μυστικών επιχειρήσεων για την αντιμετώπιση της κρίνεται απαραίτητη[85].

Περαιτέρω, ο όρος προσφορά, που συναντάται στην παράγραφο 1 εδ. β' του παρόντος, αναφέρεται στην πρόσκληση σε άλλους να αποκτήσουν υλικό παιδικής πορνογραφίας, ενώ ο όρος διάθεση καλύπτει τις περιπτώσεις που κάποιος καθιστά προσβάσιμο υλικό παιδικής πορνογραφίας σε άλλους, όπως τα διάφορα sites. Ακόμα, ο όρος *διανομή* στο εδάφιο γ της παραγράφου 1 αναφέρεται στην ενεργή διάδοση του υλικού, ενώ ο όρος *μετάδοση* αναφέρεται στην αποστολή υλικού μέσω υπολογιστή σε ένα άλλο άτομο. Σύμφωνα με την παράγραφο 2 ο όρος *παιδική πορνογραφία* περιλαμβάνει την οπτική απεικόνιση ανηλίκου ή προσώπου που φαίνεται να είναι ανήλικο, το οποίο εμπλέκεται σαφώς σε σεξουαλική συμπεριφορά καθώς και την απεικόνιση ρεαλιστικών εικόνων που αποτυπώνουν έναν ανήλικο να εμπλέκεται σε σαφώς σεξουαλική συμπεριφορά. Η πρώτη εκ των τριών πράξεων σκοπεύει να προστατέψει ευθέως και άμεσα τους ανηλίκους από την παιδική κακοποίηση. Οι άλλες δύο πράξεις παρέχουν προστασία έναντι συμπεριφορών που, αν και δεν προκαλούν ενδεχομένως βλάβη στο παιδί που απεικονίζεται στο υλικό, καθώς μπορεί να μην υπάρχει πραγματικό παιδί, δύνανται να ενθαρρύνουν ή να παραπλανήσουν τα παιδιά να συμμετέχουν σε τέτοιες πράξεις, εκτρέφοντας με αυτόν τον τρόπο μια υποκουλτούρα που ευνοεί την παιδική κακοποίηση[86].

Τέλος, ο όρος *ανήλικος* περιλαμβάνει όλα τα πρόσωπα που δεν έχουν συμπληρώσει το 18ο έτος της ηλικίας τους, όριο που βρίσκεται σε αρμονία με το αντίστοιχο του άρθρου 1 της Σύμβασης των Ηνωμένων Εθνών για τα Δικαιώματα του Παιδιού. Σημειώνεται ότι το ανωτέρω όριο αναφέρεται σε πράξεις που μεταχειρίζονται τον ανήλικο ως σεξουαλικό αντικείμενο και δεν εμποδίζει τις εθνικές νομοθεσίες να θέτουν διαφορετικά όρια σε περιπτώσεις συναινετικής σεξουαλικής επαφής. Άλλωστε, το τελευταίο εδάφιο της παραγράφου 3 επιτρέπει στα συμβαλλόμενα μέρη να ορίσουν χαμηλότερο όριο ηλικίας, έως 16 χρονών.

[84] Walden, Computer Crimes and Digital Investigations, σελ. 66
[85] ABA, International Guide to Combating Cybercrime, σελ. 73
[86] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 102

Ο Τίτλος 4 της Σύμβασης ποινικοποιεί εγκλήματα σχετικά με παραβιάσεις συγγραφικών και συγγενικών δικαιωμάτων. Συγκεκριμένα, το άρθρο 10 προβλέπει στην παράγραφο 1 την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας υποχρεώνοντας κάθε συμβαλλόμενο μέρος να ποινικοποιεί στο εγχώριο δίκαιό του την παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας (copyright) όπως αυτά ορίζονται στο δίκαιο αυτού του Συμβαλλομένου Μέρους, σε εκτέλεση των υποχρεώσεων που έχει αναλάβει από την Πράξη του Παρισιού της 24 Ιουλίου 1971 που αναθεώρησε την Σύμβαση της Βέρνης για την Προστασία των Λογοτεχνικών και Καλλιτεχνικών Έργων (the Bern Convention for the Protection of Literary and Artistic Works), την Συμφωνία για τις Εμπορικές Πτυχές των Δικαιωμάτων Πνευματικής Ιδιοκτησίας (the Agreement on Trade - Related Aspects of Intellectual Property Rights) και την Συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας WIPO για την πνευματική ιδιοκτησία (the WIPO Copyright Treaty), με εξαίρεση τα ηθικά δικαιώματα πνευματικής ιδιοκτησίας που παρέχονται από αυτές τις συμβάσεις, στην περίπτωση που αυτές οι πράξεις διαπράττονται από πρόθεση, σε εμπορική κλίμακα και με την χρήση ενός συστήματος υπολογιστή.

Οι παραβάσεις σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας (copyright) είναι οι πιο συχνές στο διαδίκτυο και ως εκ τούτου αποτελούν πηγή ανησυχίας για τους ιδιοκτήτες των δικαιωμάτων και για τους επαγγελματίες που ασχολούνται με υπολογιστικά δίκτυα. Η κατοχή, η αναπαραγωγή και η διανομή προστατευμένων δικαιωμάτων μέσω του διαδικτύου αυξάνεται συνεχώς. Έτσι, τα μέρη υποχρεούνται να ποινικοποιήσουν τις ανωτέρω προσβολές για την προστασία των δικαιωμάτων που παρατίθενται στις προαναφερθείσες συμβάσεις και διενεργούνται μέσω υπολογιστή σε εμπορική κλίμακα.

Περαιτέρω, η παράγραφος 2 του άρθρου 10 προβλέπει ότι κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που απαιτούνται για να ποινικοποιηθεί στο εγχώριο δίκαιό του η παραβίαση των συγγενικών δικαιωμάτων, όπως αυτά ορίζονται στο δίκαιο αυτού του Συμβαλλομένου Μέρους, σε εκτέλεση των υποχρεώσεων που έχει αναλάβει από τη Σύμβαση για την Προστασία των Ερμηνευτών ή Εκτελεστών Καλλιτεχνών, των Παραγωγών Φωνογραφικών και Ραδιοτηλεοπτικών Οργανισμών (Σύμβαση της Ρώμης) (the

International Convention for the Protection of Performers , Producers of Phonograms and Broadcasting Organisations - Rome Convention), την Συμφωνία για τις Εμπορικές Πτυχές των Δικαιωμάτων Πνευματικής Ιδιοκτησίας (the Agreement on Trade - Related Aspects of Intellectual Property Rights) και την Σύμβαση για τις Ερμηνείες / Εκτελέσεις και τα Φωνογραφήματα (the WIPO Performances and Phonograms Treaty), με εξαίρεση τα ηθικά δικαιώματα που παρέχονται από αυτές τις συμβάσεις, όταν αυτές οι πράξεις διαπράττονται από πρόθεση, σε εμπορική κλίμακα και με την χρήση ενός συστήματος υπολογιστή.

Οι παραβιάσεις των πνευματικών και συγγενικών δικαιωμάτων ορίζονται στο εθνικό δίκαιο των συμβαλλόμενων μερών με την τήρηση των υποχρεώσεων που το κάθε μέρος έχει αναλάβει προς συμμόρφωση με διεθνείς συμβάσεις και όργανα[87]. Κατά συνέπεια, ο ακριβής ορισμός των παραπάνω προσβολών στα εθνικά δίκαια δύναται να διαφέρει από κράτος σε κράτος.

Η παράγραφος 3 του ίδιου άρθρου επιτρέπει στα συμβαλλόμενα μέρη να μην ποινικοποιήσουν στην εγχώρια έννομη τάξη τους, σε περιορισμένες περιπτώσεις, τις πράξεις των παραγράφων 1 και 2, υπό τον όρο ότι η έννομη τάξη διαθέτει άλλα αποτελεσματικά ένδικα βοηθήματα. Τέτοια βοηθήματα μπορεί να είναι αστικά ή διοικητικά μέτρα. Ουσιαστικά, δηλαδή, η παράγραφος αυτή παρέχει την δυνατότητα περιορισμένης εξαίρεσης από την υποχρέωση ποινικοποίησης, υπό την προϋπόθεση ότι τηρούνται οι υποχρεώσεις που έχουν αναληφθεί δυνάμει του άρθρου 61 της συμφωνίας TRIPS.

Ο τίτλος 2 κεφάλαιο 3 της Σύμβασης θεσπίζει διατάξεις διεθνούς συνεργασίας μεταξύ των συμβαλλόμενων μερών για την έκδοση προσώπων που παραβιάζουν διατάξεις της παρούσας Σύμβασης. Έτσι, το άρθρο 23 θέτει τρεις γενικές αρχές αναφορικά με την διεθνή συνεργασία. Πρώτον, προβλέπεται ότι η συνεργασία συνίσταται στην μεγαλύτερη δυνατή έκταση μεταξύ των μερών. Η εν λόγω αρχή επιτάσσει τα μέλη να συνεργάζονται εκτενώς μεταξύ τους και να μην θέτουν προσκόμματα στην ομαλή και ταχεία ανταλλαγή πληροφοριών και αποδεικτικών

[87] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 109

στοιχείων[88]. Δεύτερον, το πεδίο εφαρμογής της συνεργασίας επεκτείνεται σε όλα τα ποινικά αδικήματα που σχετίζονται με σύστημα υπολογιστών και δεδομένων καθώς και για στην συλλογή αποδεικτικών στοιχείων σε ηλεκτρονική μορφή. Βάσει αυτής της αρχής, το παρόν κεφάλαιο εφαρμόζεται τόσο σε εγκλήματα που διαπράττονται μέσω συστήματος υπολογιστή όσο και σε εγκλήματα που δεν διαπράττονται με υπολογιστή (π.χ. ανθρωποκτονία) όμως υπάρχουν γι' αυτά ηλεκτρονικά αποδεικτικά στοιχεία[89]. Βέβαια, τα άρθρα 24, 33 και 34 επιτρέπουν στα συμβαλλόμενα μέρη να θεσπίσουν διαφορετικό πεδίο εφαρμογής. Τρίτον, προβλέπεται ότι τα Συμβαλλόμενα Μέρη θα συνεργαστούν σύμφωνα με τις διατάξεις του παρόντος κεφαλαίου και την εφαρμογή των σχετικών συμφωνιών διεθνούς συνεργασίας σε ποινικά θέματα, των ρυθμίσεων που έχουν γίνει με βάση την ενιαία ή αμοιβαία νομοθεσία και τους εσωτερικούς νόμους. Η ανωτέρω ρήτρα θεμελιώνει την γενική αρχή ότι οι διατάξεις του Κεφαλαίου 3 δεν υπερέχουν ούτε αντικαθιστούν τις διατάξεις που έχουν θεσπιστεί με διεθνείς συμφωνίες σχετικά με αμοιβαία νομική συνδρομή και έκδοση ή διατάξεις του εσωτερικού δικαίου που σχετίζονται με την διεθνή συνεργασία[90]. Άλλωστε, η εν λόγω αρχή ενισχύεται σύμφωνα με τα άρθρα 25-28, 31, 33 και 34 της Σύμβασης.

Περαιτέρω, το άρθρο 24 καθορίζει την έκδοση προσώπων στο πλαίσιο της παρούσας Σύμβασης. Προκειμένου να εκδοθεί ένα πρόσωπο απαιτείται να έχει παραβιάσει κάποιο από τα άρθρα 2 -11 της Σύμβασης και επιπλέον το αδίκημα που έχει διαπράξει να τιμωρείται στα εθνικά δίκαια των εμπλεκομένων μερών με ποινή στερητικής της ελευθερίας τουλάχιστον ενός έτους[91]. Αυτόδηλο είναι ότι τον καθοριστικό ρόλο για την έκδοση δεν διαδραματίζει η ποινή που τελικά επιβλήθηκε αλλά η ποινή με την οποία απειλείται η παράβαση, ανεξάρτητα από την ποινή που τελικά επιβλήθηκε. Ωστόσο, σε περίπτωση που δυνάμει μια διεθνούς συμφωνίας ή αμοιβαίας ρύθμισης προβλέπεται κατώτερο όριο από το ένα έτος ισχύει το συμφωνηθέν κατώτατο όριο[92]. Για παράδειγμα, πολλές συμφωνίες, κυρίως μεταξύ των ευρωπαϊκών κρατών, προβλέπουν την έκδοση μόνο εάν για το αδίκημα

[88] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 242
[89] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 243
[90] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 244
[91] Άρθρο 24 παράγραφος 1 της Σύμβασης
[92] Άρθρο 24 παράγραφος 2 της Σύμβασης

απειλείται μέγιστη ποινή φυλάκισης μεγαλύτερης του ενός έτους[93]. Στις ανωτέρω περιπτώσεις τα μέρη θα συνεχίσουν να τηρούν το όριο που έχουν θέσει τα ίδια.

Η έκδοση προσώπου υπόκειται στις προϋποθέσεις που θέτει το εσωτερικό δίκαιο του συμβαλλόμενου μέρους από το οποίο ζητείται η έκδοση, μεταξύ των οποίων συμπεριλαμβάνεται και η αναφορά των λόγων για τους οποίους αιτείται η έκδοση. Έτσι, αν δεν πληρούνται οι προϋποθέσεις το κράτος μπορεί να αρνηθεί την έκδοση. Ωστόσο, σε περίπτωση που δεν πραγματοποιηθεί η έκδοση, το κράτος που την αρνήθηκε πρέπει να προχωρήσει στην εκδίκαση της υπόθεσης και να κρίνει το αδίκημα για το οποίο ζητείται η έκδοση, σύμφωνα με την αρχή «aut dedere aut judicare». Με αυτόν τον τρόπο, διασφαλίζεται ότι παρά το γεγονός ότι πολλά κράτη αρνούνται την έκδοση υπηκόων τους οι παραβάτες θα υποστούν τις απαιτούμενες κυρώσεις από τις δικαστικές αρχές του κράτους υπηκοότητας τους. Για να συμβεί, ωστόσο, αυτό πρέπει το κράτος που ζητάει την έκδοση, μετά την απόρριψη του αιτήματός του, να απευθύνει αίτημα στις αρμόδιες αρχές του κράτους από το οποίο ζητείται η έκδοση για την άσκηση ποινικής δίωξης σε βάρος του εν λόγω προσώπου[94]. Διαφορετικά, το κράτος δεν έχει υποχρέωση να προβεί σε καμία ενέργεια.

5.2. ΕΝΩΣΙΑΚΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Ακολουθώντας την Σύμβαση της Βουδαπέστης, η Ευρωπαϊκή Ένωση αντιλαμβανόμενη την ανάγκη να αναλάβει και η ίδια νομοθετική πρωτοβουλία για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο εκδίδει στις 24 Φεβρουαρίου 2005 την Απόφαση – Πλαίσιο 2005/222/ΔΕΥ για επιθέσεις κατά των συστημάτων πληροφοριών, η οποία τίθεται σε εφαρμογή την 16 Μαρτίου 2005.

Η Ευρωπαϊκή Ένωση έχει διαπιστώσει τις επαναλαμβανόμενες επιθέσεις κατά συστημάτων πληροφοριών, ιδίως στο πλαίσιο του οργανωμένου εγκλήματος και μελλοντικά της τρομοκρατίας, γεγονός που θέτει σε κίνδυνο την επίτευξη ενός

[93] Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, Οργανισμός Ηνωμένων Εθνών, σημ. 246
[94] Άρθρο 27 παράγραφος 6 της Σύμβασης

ασφαλούς Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης και ως εκ τούτου αναλαμβάνει πρωτοβουλία για την αντιμετώπιση των εν λόγω απειλών[95].

Επιπλέον, η ανάγκη για κοινή νομοθετική δράση κατά του εγκλήματος που χρησιμοποιεί προηγμένες τεχνολογίες, συμπεριλαμβάνοντας κοινούς ορισμούς, ποινικούς χαρακτηρισμούς και κυρώσεις, γίνεται εμφανής σε πληθώρα κειμένων. Τέτοια κείμενα είναι το πρόγραμμα δράσης του Συμβουλίου και της Επιτροπής όσον αφορά την άριστη δυνατή εφαρμογή των διατάξεων της συνθήκης του Άμστερνταμ για τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, το Ευρωπαϊκό Συμβούλιο του Τάμπερε της 15ης και 16ης Οκτωβρίου 1999, το Ευρωπαϊκό Συμβούλιο της Σάντα Μαρία ντα Φέιρα της 19ης και 20ής Ιουνίου 2000, ο «Πίνακας αποτελεσμάτων» της Επιτροπής και το ψήφισμά του της 19ης Μαΐου 2000 του Ευρωπαϊκού Κοινοβουλίου[96].

Έτσι, στόχος της Απόφασης είναι η προσέγγιση του ποινικού δικαίου όσον αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών για να διασφαλισθεί η μέγιστη δυνατή δικαστική και αστυνομική συνεργασία όσον αφορά τα ποινικά αδικήματα που έχουν σχέση με επιθέσεις κατά των συστημάτων πληροφοριών. Στόχο αποτελεί, επίσης, η συμμετοχή στην καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας[97].

Στην Απόφαση, παρατίθεται ένας κοινός ορισμός για το τι ονομάζεται σύστημα πληροφοριών και ηλεκτρονικά δεδομένα. Ειδικότερα, σύμφωνα με το άρθρο 1, σύστημα πληροφοριών καλείται *« οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τους υπολογιστές με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους*», ενώ ως ηλεκτρονικά δεδομένα ορίζεται η « *οποιαδήποτε παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από*

[95] Απόφαση – πλαίσιο 2005/222/ΔΕΥ, σκ. 2
[96] Απόφαση – πλαίσιο 2005/222/ΔΕΥ, σκ. 6
[97] Απόφαση – πλαίσιο 2005/222/ΔΕΥ, σκ. 8

σύστημα πληροφοριών, συμπεριλαμβανομένου ενός προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία».

Κατά συνέπεια, με την εν λόγω Απόφαση κατοχυρώνεται για πρώτη φορά στο ενωσιακό δίκαιο ένας κοινός ορισμός για όλα τα κράτη αναφορικά με το τι αποκαλείται σύστημα πληροφοριών, επιτυγχάνοντας με αυτόν τον τρόπο κοινή εφαρμογή των κανόνων της παρούσας Απόφασης και την απαιτούμενη ασφάλεια δικαίου.

Περαιτέρω, η Απόφαση τυποποιεί τρεις κατηγορίες επιθέσεων, οι οποίες κινούνται στα πλαίσια της Σύμβασης της Βουδαπέστης, αναφορικά με το περιεχόμενο τους. Πρώτον, στο άρθρο 2, τυποποιείται η παράνομη πρόσβαση σε σύστημα πληροφοριών ή μέρος αυτού. Δεύτερον, στο άρθρο 3, τιμωρείται η παράνομη παρεμβολή σε σύστημα, δηλαδή η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή, μετάδοση, ζημία, διαγραφή, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά. Τέλος, στο άρθρο 4, τιμωρείται η παράνομη παρεμβολή σε δεδομένα, η οποία συνίσταται στην διαγραφή, ζημία, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά. Αναφέρεται, ότι οι ανωτέρω πράξεις καθίστανται παράνομες όταν ο δράστης τις επιχειρεί χωρίς δικαίωμα και εκ προθέσεως.

Η Απόφαση – Πλαίσιο αντικαταστάθηκε από την Οδηγία 40/2013, η οποία αναλύεται κατωτέρω και η οποία πλέον αποτελεί το βασικό ευρωπαϊκό νομοθετικό κείμενο για την αντιμετώπιση του κυβερνοεγκλήματος. Ανατρέχοντας κανείς στα δύο σχετικά κείμενα μπορεί εύκολα να διαπιστώσει ότι το περιεχόμενο των διατάξεων τους είναι παρόμοιο. Ωστόσο, το τότε ισχύον θεσμικό πλαίσιο είχε κατακριθεί ότι δεν καλύπτει στο πεδίο εφαρμογής του όλα τα εγκλήματα που θα έπρεπε, ενώ παράλληλα δεν αντιμετωπίζεται προσηκόντως ο κίνδυνος από επιθέσεις μεγάλης κλίμακας[98].

[98] Καϊάφα – Γκμπάντι Μ., Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδραση της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 495

Έτσι, γεννάται το εύλογο ερώτημα για το ποιοι ήταν οι λόγοι που οδήγησαν την Ευρωπαϊκή Ένωση να αναλάβει εκ νέου νομοθετική πρωτοβουλία για την αντιμετώπιση του κυβερνοεγκλήματος υιοθετώντας μάλιστα ένα παρόμοιο κείμενο με την Απόφαση – Πλαίσιο.

Αρχικά, όπως και στην Απόφαση της, η Ευρωπαϊκή Ένωση κινήθηκε στο πνεύμα της Σύμβασης της Βουδαπέστης για την έκδοση της Οδηγίας. Άλλωστε, από την Σύμβαση της Βουδαπέστης δεσμεύονται ήδη όλα τα κράτη μέλη της Ένωσης. Η απάντηση στο ανωτέρω ερώτημα σχετίζεται με την μεγάλη άνοδο των κυβερνοεπιθέσεων στην Ευρώπη, μετά την έκδοση της Απόφασης, με συνεχώς πιο οργανωμένο τρόπο και ιδίως με την κακόβουλη χρήση προγραμμάτων ρομπότ (botnet) και την μορφή της άρνησης υπηρεσίας (DDOS attacks). Ειδικότερα, προέκυψαν στοιχεία που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη μέλη ή για ειδικές δραστηριότητες του δημόσιου ή του ιδιωτικού τομέα. Η τάση αυτή συνοδεύεται από την ανάπτυξη όλο και πιο εξελιγμένων μεθόδων, όπως η δημιουργία και η χρήση των αποκαλούμενων «botnet» (δίκτυα προγραμμάτων ρομπότ), η οποία περιλαμβάνει διάφορα στάδια της αξιόποινης πράξης, καθένα από τα οποία μπορεί από μόνο του να θέσει σε σοβαρό κίνδυνο το δημόσιο συμφέρον. Η παρούσα οδηγία σκοπεύει, μεταξύ άλλων, στην εισαγωγή ποινικών κυρώσεων για τη δημιουργία των «botnets», ήτοι της πράξης της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο. Μόλις δημιουργηθεί, το προσβεβλημένο δίκτυο υπολογιστών, που συνιστά το «botnet», μπορεί να ενεργοποιείται εν αγνοία των χρηστών των εν λόγω υπολογιστών, με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία συνήθως μπορεί να προκαλέσει σοβαρές ζημίες, όπως αναφέρεται στην παρούσα οδηγία[99].

Νομική βάση για την θέσπιση των σχετικών Οδηγιών στο πλαίσιο της Ευρωπαϊκής Ένωσης αποτελεί το άρθρο 83 παράγραφος 1 της Συνθήκης για την

[99] Οδηγία 40/2013/ΕΚ, σκ. 5

Λειτουργία της Ευρωπαϊκής Ένωσης. Παράλληλα, εφαρμόζεται η αρχή της επικουρικότητας καθώς οι στόχοι που τίθενται δεν μπορούν να επιτευχθούν σε ικανοποιητικό βαθμό σε επίπεδο νομοθεσίας των κρατών μελών. Η εγκληματικότητα στον κυβερνοχώρο και ειδικότερα οι επιθέσεις κατά συστημάτων πληροφοριών έχουν σημαντική διασυνοριακή διάσταση, όπως φαίνεται ιδίως σε επιθέσεις μεγάλης κλίμακας, δεδομένου ότι τα συνδετικά στοιχεία μιας επίθεσης βρίσκονται συχνά σε διαφορετικά σημεία και διαφορετικές χώρες. Κατά συνέπεια, απαιτείται η ανάληψη δράσης από την ΕΕ, ώστε να υπάρχει η δυνατότητα αντιμετώπισης της τρέχουσας τάσης για επιθέσεις μεγάλης κλίμακας στην Ευρώπη και σε παγκόσμια επίπεδο[100].

Το 2013, λοιπόν, το Ευρωπαϊκό Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο εκδίδει την υπ' αρίθμ. 40/2013 για τις επιθέσεις κατά συστημάτων πληροφοριών προς αντικατάσταση της Απόφασης-Πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, η οποία ως κύριο στόχο έχει την προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων. Στόχος αποτελεί επίσης η βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, καθώς και των αρμόδιων ειδικευμένων οργανισμών και φορέων της Ένωσης, όπως η Eurojust, η Europol και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA)[101].

Παράλληλα, οι επιθέσεις κατά των συστημάτων πληροφοριών, και ιδίως οι επιθέσεις που συνδέονται με το οργανωμένο έγκλημα, αποτελούν συνεχώς αυξανόμενη απειλή, τόσο στην Ένωση όσο και παγκοσμίως, και εντείνουν τις ανησυχίες για το ενδεχόμενο τρομοκρατικών επιθέσεων ή επιθέσεων με πολιτικά κίνητρα κατά των συστημάτων πληροφοριών που αποτελούν μέρος των υποδομών ζωτικής σημασίας των κρατών μελών και της Ένωσης. Αυτό αποτελεί απειλή για την

[100] Ευρωπαϊκή Επιτροπή, Πρόταση για Οδηγία του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών, COM(2010) 517 τελικό, 30/09/2010, διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52010PC0517&from=EN
[101] Οδηγία 40/2013/ΕΚ, προοίμιο 1

επίτευξη μιας ασφαλέστερης κοινωνίας της πληροφορίας και ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, Επομένοως, απαιτείται απάντηση στο επίπεδο της Ένωσης και βελτιωμένη συνεργασία και συντονισμός σε διεθνές επίπεδο[102].

Κατά την θέσπιση της Οδηγίας λήφθηκε μέριμνα να υπάρξουν κοινοί ορισμοί για τις έννοιες, ώστε να επιτευχθεί η ζητούμενη συνεκτική προσέγγιση μεταξύ των κρατών μελών αναφορικά με την εφαρμογή της[103]. Οι ορισμοί αυτοί αφορούν ιδίως τα εγκλήματα της παράνομης πρόσβασης σε σύστημα πληροφοριών, της παράνομης παρεμβολής σε σύστημα, της παράνομης παρεμβολής σε δεδομένα και της παράνομης υποκλοπής.

Για τους σκοπούς της Οδηγίας, ως σύστημα πληροφοριών νοείται η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους[104].

Η Οδηγία 2013/40/ΕΕ τυποποιεί πέντε κατηγορίες εγκληματικών πράξεων που διαπράττονται κατά των πληροφοριακών συστημάτων. Ειδικότερα, το άρθρο 3 απαγορεύει την παράνομη πρόσβαση σε σύστημα πληροφοριών, πράξη γνωστή στην βιβλιογραφία ως hacking. Παράνομη είναι η πρόσβαση που πραγματοποιείται με πρόθεση και χωρίς δικαίωμα σε μέρος ή στο σύνολο του πληροφοριακού συστήματος παραβιάζοντας κάποιο μέτρο ασφαλείας. Ωστόσο, σύμφωνα με το τελευταίο εδάφιο του εν λόγω άρθρου η παραβίαση πρέπει να μην είναι ήσσονος σημασίας. Ο καθορισμός των περιπτώσεων που συνιστούν ήσσονος σημασίας παραβιάσεις εναπόκειται στην ευχέρεια των κρατών μελών. Για παράδειγμα, μία περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν οι ζημίες που προκαλεί το αδίκημα ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον είναι αμελητέα ή τέτοιας φύσης,

[102] Οδηγία 40/2013/ΕΚ, προοίμιο 3
[103] Οδηγία 40/2013/ΕΚ, προοίμιο 7
[104] Άρθρο 1 εδ. α' Οδηγίας 40/2013/ΕΚ

ώστε να μην θεωρείται απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης[105]. Όπως ειπώθηκε, απαραίτητη προϋπόθεση είναι η πρόσβαση να αποκτάται με την παραβίαση κάποιου μέτρου ασφαλείας[106]. Τα πλέον συνήθη μέτρα είναι οι κωδικοί πρόσβασης, κωδικοί εισόδου και κωδικοί κρυπτογράφησης[107].

Η δεύτερη κατηγορία εγκληματικών πράξεων τυποποιείται στο άρθρο 4 της Οδηγίας και συνίσταται στην παράνομη παρεμβολή σε σύστημα. Το εν λόγω αδίκημα αφορά σε περιπτώσεις σοβαρής παρεμπόδισης ή διακοπής της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά. Η παρεμβολή για να είναι παράνομη πρέπει να γίνεται με πρόθεση και χωρίς δικαίωμα και να μην θεωρείται ήσσονος σημασίας. Η πιο γνωστή περίπτωση αυτής της κατηγορίας που αποτελεί παράνομη παρεμβολή είναι γνωστή ως επίθεση Denial of Service – DOS. Σε αυτή τη μορφή επίθεσης, ο δράστης προσπαθεί να αρνηθεί σε εξουσιοδοτημένους χρήστες την πρόσβαση σε συγκεκριμένες πληροφορίες ή σε συστήματα πληροφοριών ή και στο ίδιο το δίκτυο. Έτσι, ο δράστης καθιστά μη διαθέσιμες τις πληροφορίες στους εξουσιοδοτημένους χρήστες. Ο σκοπός αυτών των επιθέσεων μπορεί να είναι απλά η παρεμπόδιση της πρόσβασης στο συγκεκριμένο σύστημα πληροφοριών από νόμιμο χρήστη ή και η επίτευξη της πρόσβασης από μη εξουσιοδοτημένο χρήστη. Στην ανωτέρω κατηγορία, υπάγονται και οι επιθέσεις με κακόβουλα προγράμματα που μολύνουν το σύστημα, όπως οι ιοί. Ένας ιός εγκαθιστά στο πληροφοριακό σύστημα έναν κακόβουλο κώδικα, ο οποίος αρχικά αποβάλλει τον χρήστη από τις πληροφορίες του και στην συνέχεια εξάγει προς όφελος του δράστη πολύτιμες πληροφορίες που αφορούν, κατά κύριο λόγο, σε δεδομένα προσωπικού χαρακτήρα

[105] Οδηγία 40/2013/ΕΕ, προοίμιο 11

[106] Στην πρόταση της Ευρ. Επιτροπής δεν προβλεπόταν ως προϋπόθεση η παραβίαση μέτρου ασφαλείας, βλ. Ευρωπαϊκή Επιτροπή, Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, Βρυξέλλες, 2010, σελ. 15

[107] Adrian Cristian Moise, Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level, Journal of Law and Administrative Sciences, σελ. 376

του χρήστη, όπως για παράδειγμα τραπεζικοί λογαριασμοί και λογαριασμοί πιστωτικών καρτών.

Το άρθρο 5 της Οδηγίας απαγορεύει την παράνομη παρεμβολή σε δεδομένα, δηλαδή την διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα. Παρατηρείται ότι η προσβολή που τυποποιείται στο άρθρο 5 προσομοιάζει με την πράξη του άρθρου 4 της Οδηγίας. Η διαφορά των δύο άρθρων, υποστηρίζεται ότι βρίσκεται στον σκοπό τους[108]. Συγκεκριμένα, το άρθρο 4 περιλαμβάνει προσβολές σε σύστημα οι οποίες πραγματοποιούνται με την παρέμβαση στα δεδομένα του πληροφοριακού συστήματος. Από την άλλη πλευρά, το άρθρο 5 αναφέρεται σε επιθέσεις που έχουν ως μοναδικό στόχο τα δεδομένα του υπολογιστή. Λαμβάνοντας υπόψη ότι η πλειονότητα των επιθέσεων λαμβάνει χώρα στον κυβερνοχώρο, για την επιτυχία των επιθέσεων χρειάζεται ο δράστης να παρέμβει παράνομα τόσο στα δεδομένα όσο και στο σύστημα. Για τον λόγο αυτό, θα μπορούσε να ειπωθεί ότι οι προσβολές των άρθρων 4 και 5 είναι αδιαχώριστες.

Την τέταρτη κατηγορία προσβολών αποτελεί η παράνομη υποκλοπή, δηλαδή η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα[109]. Με άλλες λέξεις, πρόκειται για ακρόαση, επίβλεψη του περιεχομένου των επικοινωνιών και προμήθεια δεδομένων από υπολογιστή, είτε απευθείας με την πρόσβαση και χρήση του συστήματος πληροφοριών είτε έμμεσα με την χρησιμοποίηση συσκευών εγγραφής και ακρόασης. Ως τεχνικά μέσα νοούνται τόσο οι συσκευές που υπάρχουν σε σταθερές γραμμές επικοινωνίας όσο και οι συσκευές που έχουν σχεδιαστεί για να καταγράφουν και να συλλέγουν δεδομένα ασύρματα.

[108] Adrian Cristian Moise, ο.π., σελ. 377
[109] Άρθρο 6 της Οδηγίας

Στην πέμπτη και τελευταία κατηγορία προσβολών της παρούσας Οδηγίας τιμωρούνται τα εργαλεία που χρησιμοποιούνται για την διάπραξη των ανωτέρω αδικημάτων. Συγκεκριμένα, τιμωρείται η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση αφενός προγράμματος υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6· και αφετέρου συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων, μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών. Για την τιμωρία απαιτείται σύμφωνα με το γράμμα της διάταξης[110] η πρόθεση τα ανωτέρω εργαλεία να χρησιμοποιηθούν για την διάπραξη οποιουδήποτε αδικήματος που αναφέρεται στα άρθρα 3 έως 6 της παρούσας.

5.3. ΣΥΓΚΡΙΣΗ ΤΩΝ ΔΥΟ ΝΟΜΙΚΩΝ ΠΛΑΙΣΙΩΝ

Όπως αναφέρθηκε παραπάνω, η Οδηγία του 2013 στηρίχτηκε εν πολλοίς τόσο στο πνεύμα όσο και στο γράμμα της Σύμβασης της Βουδαπέστης. Επομένως, οι διαφορές μεταξύ τους δεν δύνανται να χαρακτηριστούν σημαντικές. Ειδικότερα, στο έγκλημα της παράνομης πρόσβασης η Σύμβαση αφήνει στην διακριτική ευχέρεια των συμβαλλόμενων μερών την δυνατότητα να τιμωρούν την εν λόγω πράξη, στην περίπτωση που με αυτήν (παράνομη πρόσβαση) παραβιάζεται ταυτόχρονα και κάποιο μέτρο ασφαλείας. Αντιθέτως, η Οδηγία αναφέρει ρητά ως προϋπόθεση για την τιμωρία του δράστη την παραβίαση μέτρου ασφαλείας κατά την διάπραξη του εγκλήματος.

Στο έγκλημα της παράνομης παρεμβολής σε σύστημα, το οποίο στην Σύμβαση τυποποιείται στο άρθρο 5 ενώ στην Οδηγία στο άρθρο 4, η κύρια διαφοροποίηση της Οδηγίας είναι ότι εκτός από την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ποινικοποιείται και η παρεμβολή που πραγματοποιείται, καθιστώντας έτσι τα δεδομένα του υπολογιστή απρόσιτα, δηλαδή αποκλείοντας το νόμιμο χρήστη από τα

[110] Άρθρο 7 της Οδηγίας

δεδομένα αυτά. Ωστόσο, στο σχέδιο της Σύμβασης ο νομοθέτης έχει αποδώσει στον όρο καταστολή δεδομένων, που προβλέπεται στο άρθρο 5 για το εν λόγω έγκλημα, διττό περιεχόμενο. Αφενός τιμωρείται στο πλαίσιο του όρου η διαγραφή των δεδομένων, ώστε να μην υπάρχουν αυτά πλέον διαθέσιμα και αφετέρου η παρεμπόδιση της πρόσβασης σε αυτά[111], πράξη που ρητώς τιμωρείται στην Οδηγία, όπως αναφέρθηκε.

Επιπροσθέτως, η Οδηγία θέτει ως προϋπόθεση η πράξη να μην αφορά ήσσονος σημασίας περιπτώσεις. Ωστόσο, στην εν λόγω περίπτωση αυτή η πρόβλεψη δεν συνιστά διαφοροποιητικό παράγοντα, καθώς σύμφωνα με το γράμμα της διάταξης η παρακώληση πρέπει να είναι σοβαρή. Έτσι, ερμηνευτικά προκύπτει ότι τόσο στην Οδηγία όσο και στην Σύμβαση δεν καλύπτονται από την εν λόγω διάταξη οι ήσσονος σημασίας περιπτώσεις. Σοβαρή χαρακτηρίζεται η παρακώληση της λειτουργίας ενός συστήματος με την αποστολή δεδομένων σε αυτό υπό τέτοια μορφή, μέγεθος ή συχνότητα που να επηρεάζει σημαντικά ή καθοριστικά την δυνατότητα του ιδιοκτήτη ή του χρήστη να χρησιμοποιεί το σύστημα ή να επικοινωνεί με άλλα συστήματα

Περαιτέρω, στο έγκλημα της υποκλοπής (άρθρο 3 της Σύμβασης και άρθρο 6 της Οδηγίας) η Σύμβαση της Βουδαπέστης παρέχει την δυνατότητα στα συμβαλλόμενα μέρη να εισάγουν στο εσωτερικό τους δίκαιο ως προϋπόθεση για την διάπραξη του εγκλήματος την επίτευξη σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή. Αντιθέτως, η Οδηγία δεν θέτει καμία ανάλογη προϋπόθεση. Αυτό οφείλεται στο γεγονός ότι η Οδηγία περιέχει διατάξεις για την ποινικοποίηση εγκλημάτων που στρέφονται κατά συστήματος πληροφοριών ανεξάρτητα με το αν αυτά τελούνται διαμέσου του διαδικτύου. Από την άλλη πλευρά, η Σύμβαση αναφέρεται σε εγκλήματα που τελούνται αμιγώς στον κυβερνοχώρο, δηλαδή μέσω του διαδικτύου.

Εν συνεχεία, στο έγκλημα της παρεμβολής σε δεδομένα διαφαίνεται ότι η Οδηγία καθίσταται αυστηρότερη από την Σύμβαση. Αυτό συμβαίνει διότι η

[111] Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), 2000, 19, διαθέσιμο σε: www.iwar.org.uk/law/resources/eu/cybercrime.htm

Σύμβαση[112] επιτρέπει στα μέρη να θέσουν ως προϋπόθεση για την ποινικοποίηση της πράξης την πρόκληση σοβαρής ζημίας. Αντίθετα, η Οδηγία επιτρέπει στα κράτη μέλη να μην τιμωρούν το αδίκημα, όταν πρόκειται για ήσσονος σημασίας περιπτώσεις. Έτσι, παρατηρείται ότι στο πεδίο εφαρμογής της Οδηγίας εμπίπτουν και οι περιπτώσεις που υπάρχουν μεταξύ του φάσματος της μικρής σημασίας και της σοβαρής, δηλαδή εκείνες οι περιπτώσεις που μπορούν να χαρακτηριστούν ως μέτριας σημασίας.

Γενικότερα, ο ενωσιακός νομοθέτης επέλεξε να θέσει στα αδικήματα που τιμωρεί με την Οδηγία την προϋπόθεση αυτά να μην συνιστούν ήσσονος σημασίας περιπτώσεις. Παρόμοια πρόβλεψη δεν ανευρίσκεται στην Σύμβαση, η οποία σε ορισμένες περιπτώσεις που εκτέθηκαν ανωτέρω απαιτεί την ύπαρξη σοβαρής παρακώλησης ή σοβαρής ζημίας. Ωστόσο, καίτοι η Οδηγία παραθέτει ορισμένα παραδείγματα[113] για το ποιες περιπτώσεις μπορούν να χαρακτηριστούν ως ήσσονος σημασίας, αναθέτει τελικά στο εκάστοτε κράτος να θέσει τα σχετικά όρια. Το γεγονός αυτό δύναται να θέσει σε κίνδυνο τον σκοπό της εναρμόνισης της νομοθεσίας μεταξύ των κρατών μελών, αφού κάθε κράτος έχει την δυνατότητα να θεωρεί διαφορετικές περιπτώσεις ως ήσσονος σημασίας σε σχέση με κάποιο άλλο κράτος μέλος. Σε κάθε περίπτωση, διαπιστώνεται ότι πρόκειται για μια αόριστη νομική έννοια που δύναται να προκαλέσει ανασφάλεια δικαίου, ενώ ελέγχεται και για παραβίαση της αρχής της νομιμότητας λόγω αοριστίας.

Μια ιδιαίτερα σημαντική διαφορά μεταξύ των δύο κειμένων απαντάται στα άρθρα που παραθέτουν τις προβλεπόμενες κυρώσεις[114]. Όπως παρατηρείται, τα δύο σχετικά άρθρα[115] αναφέρουν ότι οι κυρώσεις πρέπει να είναι αποτελεσματικές, ανάλογες και αποτρεπτικές. Ωστόσο, η Οδηγία προβλέπει κατώτατα όρια στερητικών

[112] Άρθρο 4 παράγραφος 2 της Οδηγίας

[113] Προοίμιο 11, το οποίο αναφέρει «Η περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης»

[114] Csonka, Peter,The council of europe's convention on cyber-crime and other European initiatives, Revue internationale de droit pénal, vol. 77, no. 3-4, 2006, σελ. 497

[115] Άρθρο 13 της Σύμβασης της Βουδαπέστης, Άρθρο 9 της Οδηγίας 40/2013/ΕΕ

της ελευθερίας ποινών. Συγκεκριμένα, προβλέπεται ότι: *«τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 τιμωρούνται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη…»*, ενώ *«οσάκις τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται εκ προθέσεως, και εφόσον έχει πληγεί σημαντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργαλείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή L 218/12 EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 14.8.2013 προσαρμοσθεί πρωτίστως για τον σκοπό αυτό, τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη…»*. Επιπλέον, *«τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον: α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της απόφασης-πλαισίου 2008/841/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή· β) προκαλούν σημαντικές ζημίες, ή γ) διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής.»* Τέλος, σύμφωνα με την παράγραφο 5 του άρθρου 9 της Οδηγίας, παρέχεται η δυνατότητα στα κράτη μέλη να θέσουν ως επιβαρυντική περίσταση την τέλεση των πράξεων των άρθρων 4 και 5 με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου με σκοπό την απόκτηση της εμπιστοσύνης τρίτων, η οποία έχεις ως αποτέλεσμα την πρόκληση ζημίας στον νόμιμο δικαιούχο της ταυτότητας, με την πρόσθετη προϋπόθεση ότι οι ανωτέρω περίσταση δεν καλύπτεται ήδη από άλλο αδίκημα που τιμωρείται σύμφωνα με το εθνικό δίκαιο.

6. ΟΡΓΑΝΙΣΜΟΙ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

6.1. ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ (ENISA)

Στις 10 Μαρτίου 2004 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εκδίδουν τον υπ' αριθμ. 460/2004 Κανονισμό για την δημιουργία ενός Ευρωπαϊκού Οργανισμού για την Ασφάλεια των δικτύων και των Πληροφοριών. Η Ευρωπαϊκή Ένωση έχοντας αντιληφθεί την σπουδαιότητα της διαφύλαξης των δικτύων και των συστημάτων πληροφοριών ιδρύει έναν Οργανισμό που ειδικεύεται στην ασφάλεια στον κυβερνοχώρο, προκειμένου να παράσχει αρωγή στα κράτη μέλη για την αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο. Η αρωγή αφορά τόσο την πρόληψη όσο και την αντιμετώπιση των ανακυπτόντων προβλημάτων σχετικά με την ασφάλεια των πληροφοριών και έχει την μορφή αφενός εξοπλιστικής ενίσχυσης και αφετέρου παροχής εξειδικευμένων γνώσεων από εμπειρογνώμονες.

Μάλιστα, η σημασία που αποδίδει η Ευρωπαϊκή Ένωση στην ασφάλεια των επικοινωνιών και των πληροφοριακών συστημάτων καθίσταται εναργής από την σύγκριση που πραγματοποιείται μεταξύ αυτών και βασικών κοινωνικών αγαθών όπως η ύδρευση και η ηλεκτροδότηση, αποδίδοντας τους ανάλογη σπουδαιότητα[116]. Έτσι, η Ευρωπαϊκή Ένωση αντιλαμβάνεται ότι λόγω της πολυπλοκότητας των συστημάτων αυτά καθίστανται ευάλωτα, τόσο σε επιθέσεις όσο και σε ατυχήματα ή σφάλματα, γεγονός που μπορεί να πλήξει ζωτικής σημασίας αγαθά για τους πολίτες και τις δομές της Ένωσης. Παράλληλα, οι συνεχώς αυξανόμενες επιθέσεις που έχουν ως αποτέλεσμα τις παραβιάσεις ασφάλειας των συστημάτων οδηγούν σε σημαντική οικονομική ζημία, πλήττοντας το ηλεκτρονικό εμπόριο και την εμπιστοσύνη των καταναλωτών και των χρηστών[117]. Ως εκ τούτου, τα ανωτέρω θέτουν σε κίνδυνο τον στόχο της Ευρωπαϊκής Ένωσης για ομαλή λειτουργία της εσωτερικής αγοράς.

Όλα τα παραπάνω, οδήγησαν την Ένωση να αναλάβει νομοθετική πρωτοβουλία ιδρύοντας έναν οργανισμό για την προστασία της ασφάλειας των

[116] Κανονισμός 460/2004, προοίμιο 1
[117] Κανονισμός 460/2004, προοίμιο 2

δικτύων και των πληροφοριών, ο οποίος «*θα λειτουργεί ως σημείο αναφοράς και θα εμπνέει εμπιστοσύνη χάρη στην ανεξαρτησία του, την ποιότητα των συμβουλών που θα παρέχει και των πληροφοριών που θα διαδίδει, τη διαφάνεια των διαδικασιών και του τρόπου λειτουργίας του, καθώς επίσης και την ταχύτητά του κατά την εκτέλεση των καθηκόντων που του έχουν ανατεθεί, θα καλύψει τις εν λόγω ανάγκες. Ο Οργανισμός θα πρέπει να έχει ως αφετηρία τις εθνικές και κοινοτικές προσπάθειες και, επομένως, να εκτελεί τα καθήκοντά του σε στενή συνεργασία με τα κράτη μέλη και να είναι ανοικτός στις επαφές με τον βιομηχανικό κλάδο και άλλους οικείους ενδιαφερόμενους. Δεδομένου ότι τα ηλεκτρονικά δίκτυα είναι, σε μεγάλο βαθμό, ιδιωτικά, ο Οργανισμός θα πρέπει να βασίζεται στη συμβολή του ιδιωτικού τομέα και στη συνεργασία με αυτόν*»[118]. Έτσι, ιδρύεται ο Οργανισμός με την ονομασία European Network and Information Security Agency (εφεξής ENISA).

Όπως ρητώς αναφέρεται στο κείμενο του Κανονισμού, ο ENISA, κατά την άσκηση των προβλεπόμενων καθηκόντων του, δεν θίγει την άσκηση αρμοδιοτήτων από τα κράτη μέλη, οι οποίες δεν υπάγονται στο πεδίο εφαρμογής της Συνθήκης ΕΚ. Τέτοιες αρμοδιότητες αποτελούν, ενδεικτικά, οι προβλεπόμενες αρμοδιότητες στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης και την ΚΕΠΠΑ. Άλλωστε, η άσκηση των αρμοδιοτήτων του Οργανισμού δεν μπορεί να θίγει την δημόσια ασφάλεια, την εθνική άμυνα και την ασφάλεια του κράτους[119].

Στις 17 Απριλίου 2019 εκδίδεται ένας νέος Κανονισμός αναφορικά με τον ENISA, ο οποίος προσαρμόζεται στις εξελίξεις και τα διδάγματα που εκμαιεύτηκαν κατά την προηγούμενη λειτουργία του Οργανισμού. Με τον Κανονισμό 881/2019 ο ENISA διαθέτει νομική προσωπικότητα και κάθε κράτος μέλος υποχρεούται να παρέχει στον Οργανισμό την ευρύτερη δυνατή νομική ικανότητα, ανάλογη με αυτή που παρέχει το εσωτερικό δίκαιο στα νομικά πρόσωπα[120]. Οι λόγοι που κατέστησαν απαραίτητη την έκδοση νέου Κανονισμού είναι, κυρίως, δύο: Πρώτον, η μεταβολή των προκλήσεων της ασφάλειας των δικτύων και πληροφοριών λόγω των τεχνολογικών και των κοινωνικοοικονομικών εξελίξεων και δεύτερον, η συνεχής

[118] Κανονισμός 460/2004, προοίμιο 11
[119] Κανονισμός 469/2004, Άρθρο 1 παρ. 3
[120] Κανονισμός 881/2019, Άρθρο 38

ανάγκη επικαιροποίησης των προτεραιοτήτων της πολιτικής της Ένωσης στον τομέα αυτόν[121].

6.1.1. ΣΤΟΧΟΣ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Στόχος του Κανονισμού, όπως αναφέρεται στο άρθρο 4, αποτελεί η καθιέρωση του ENISA ως κέντρο εμπειρογνωσίας σε θέματα κυβερνοασφάλειας χάρη στην ανεξαρτησία του, την επιστημονική και τεχνική ποιότητα των συμβουλών και της επικουρίας που παρέχει, τις πληροφορίες που διαμοιράζει, τη διαφάνεια των επιχειρησιακών διαδικασιών του, τις μεθόδους λειτουργίας και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του. Παράλληλα, ο Οργανισμός επικουρεί τα κράτη μέλη, καθώς και τα θεσμικά και λοιπά όργανα και Οργανισμούς της Ένωσης, προάγει την συνεργασία και συμβάλλει στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο Ένωσης. Τα ανωτέρω επιτυγχάνονται με την παροχή συνδρομής και πληροφοριών – συμβουλών στην Επιτροπή και τα κράτη μέλη για την αποτελεσματική άσκηση των προβλεπόμενων στον Κανονισμό αρμοδιοτήτων. Την ίδια στιγμή, ο Οργανισμός χρησιμοποιεί τις ειδικές γνώσεις που αναπτύσσουν τα μέλη του για την επίτευξη της όσο το δυνατόν ευρύτερης συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα. Πράγματι, υπάρχει η παραδοχή ότι για την διασφάλιση της εμπιστοσύνης απαιτείται οι πολίτες, οι επιχειρήσεις, καθώς και οι δημόσιες υπηρεσίες να διαθέτουν επαρκή ενημέρωση και κατάρτιση, αναφορικά με την ασφάλεια των δικτύων και των πληροφοριών. Για τον λόγο αυτό, ο νομοθέτης ενθαρρύνει τις εθνικές αρχές να πραγματοποιούν δράσεις για την ενημέρωση των μικρομεσαίων επιχειρήσεων και των πολιτών στα σχετικά θέματα, ξεκινώντας κιόλας από την δευτεροβάθμια εκπαίδευση[122].

6.1.2. ΚΑΘΗΚΟΝΤΑ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

[121] Παπακωνσταντής Μάρκος, ο.π., σελ. 352
[122] Κανονισμός 469/2004, προοίμιο 14

Σύμφωνα με το Κεφάλαιο ΙΙ του Κανονισμού 881/2019, ο Οργανισμός ασκεί καθήκοντα:

α) Για την χάραξη και εφαρμογή της πολιτικής και της νομοθεσίας της Ένωσης. Ειδικότερα, σύμφωνα με το άρθρο 5, ο ENISA συμβάλλει στη χάραξη και την εφαρμογή της πολιτικής και του δικαίου της Ένωσης, επικουρώντας και παρέχοντας συμβουλές σχετικά με τη χάραξη και την επανεξέταση της πολιτικής και του δικαίου της Ένωσης στον τομέα της κυβερνοασφάλειας και σχετικά με πρωτοβουλίες πολιτικής και δικαίου ανά τομέα. Στο πλαίσιο αυτό ο Οργανισμός επικουρεί την ορθή εφαρμογή της σχετικής νομοθεσίας με την έκδοση γνωμοδοτήσεων, κατευθυντήριων γραμμών, την παροχή συμβουλών και βέλτιστων πρακτικών. Τέλος, ο Οργανισμός στηρίζει: «*α) τη χάραξη και την εφαρμογή της ενωσιακής πολιτικής στον τομέα της ηλεκτρονικής ταυτότητας και των υπηρεσιών εμπιστοσύνης, κυρίως με την παροχή συμβουλών και την έκδοση τεχνικών κατευθυντήριων γραμμών, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών, β) την προαγωγή ενισχυμένου επιπέδου ασφάλειας των ηλεκτρονικών επικοινωνιών, μεταξύ άλλων με την παροχή συμβουλών και εμπειρογνωμοσύνης, καθώς και με τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ αρμόδιων αρχών, γ) τα κράτη μέλη στην εφαρμογή των ειδικών πτυχών κυβερνοασφάλειας της πολιτικής και του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής, παρέχοντας συμβουλευτική γνώμη στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατόπιν αιτήματος*» καθώς και «*την τακτική επανεξέταση των δραστηριοτήτων πολιτικής της Ένωσης με την εκπόνηση ετήσιας έκθεσης σχετικά με την κατάσταση εφαρμογής του αντίστοιχου νομικού πλαισίου όσον αφορά: α) πληροφορίες για τις κοινοποιήσεις συμβάντων των κρατών μελών που υποβάλλουν τα ενιαία κέντρα επαφής στην ομάδα συνεργασίας δυνάμει του άρθρου 10 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1148, β) περιλήψεις των κοινοποιήσεων παραβίασης της ασφάλειας ή απώλειας της ακεραιότητας που λαμβάνονται από παρόχους υπηρεσιών εμπιστοσύνης και που υποβάλλουν τα εποπτικά όργανα στον ENISA, δυνάμει του άρθρου 19 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (23), γ) τις κοινοποιήσεις συμβάντων σχετικών με την ασφάλεια που διαβιβάζουν οι πάροχοι δημόσιων*

ηλεκτρονικών δικτύων επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, τις οποίες υποβάλλουν οι αρμόδιες αρχές στον Οργανισμό, δυνάμει του άρθρου 40 της οδηγίας (ΕΕ) 2018/1972».

β) Επικουρικά καθήκοντα για την ανάπτυξη των ικανοτήτων. Ειδικότερα, σύμφωνα με το άρθρο 6 ο ENISA επικουρεί τα κράτη μέλη, καθώς και τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης στις προσπάθειές τους να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης, καθώς και την ικανότητα αντιμετώπισης, κυβερνοαπειλών και συμβάντων. Επίσης, επικουρεί τα κράτη μέλη για την ανάπτυξη εθνικών CSIRT[123] καθώς και στην ανάπτυξη εθνικών στρατηγικών ασφάλειας, όταν ζητούνται από τα κράτη μέλη δυνάμει της Οδηγίας 1148/2016. Τέλος, ο Οργανισμός διοργανώνει τακτικά και τουλάχιστον κάθε δύο έτη ασκήσεις κυβερνοασφάλειας σε επίπεδο Ένωσης, μετά το πέρας των οποίων διενεργεί σχετική αξιολόγηση.

γ) Επιχειρησιακή συνεργασία σε επίπεδο Ένωσης. Σύμφωνα με το άρθρο 7 του Κανονισμού «*ο ENISA συνεργάζεται σε επιχειρησιακό επίπεδο και αναπτύσσει συνέργειες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, συμπεριλαμβανομένων της CERT-EU, με τις υπηρεσίες που ασχολούνται με το κυβερνοέγκλημα και με τις εποπτικές αρχές που ασχολούνται με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα, με σκοπό την αντιμετώπιση κοινών προβλημάτων, μεταξύ άλλων μέσω: α) της ανταλλαγής τεχνογνωσίας και βέλτιστων πρακτικών, β) της παροχής συμβουλών και της έκδοσης κατευθυντήριων γραμμών για συναφή θέματα κυβερνοασφάλειας*». Επίσης ο Οργανισμός παρέχει στήριξη στα κράτη μέλη αναφορικά με την συνεργασία εντός του πλαισίου CSIRT με την παροχή συμβουλών για τον τρόπο βελτίωσης των ικανοτήτων τους να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν συμβάντα καθώς και την παροχή συνδρομής αναφορικά με την εκτίμηση και τον χειρισμό συμβάντων τα οποία έχουν σημαντικό αντίκτυπο ή για την εκ των υστέρων διερεύνηση αυτών. Τέλος, σύμφωνα με την παράγραφο 7 «*ο ENISA συμβάλλει στην ανάπτυξη μιας κοινής αντιμετώπισης, σε επίπεδο Ένωσης και κρατών μελών, των*

[123] Δίκτυο ομάδων απόκρισης συμβάντων για την ασφάλεια των υπολογιστών

μεγάλης κλίμακας διασυνοριακών συμβάντων και κρίσεων που αφορούν την κυβερνοασφάλεια, κυρίως με: α) τη συγκέντρωση και ανάλυση εκθέσεων από εθνικές πηγές οι οποίες είναι δημόσια διαθέσιμες ή ανταλλάσσονται σε εθελοντική βάση προκειμένου να συνεισφέρει στη δημιουργία κοινής επίγνωσης της κατάστασης, β) τη διασφάλιση της αποτελεσματικής ροής πληροφοριών και της πρόβλεψης μηχανισμών κλιμάκωσης ανάμεσα στο δίκτυο CSIRT και στους υπευθύνους λήψης τεχνικών και πολιτικών αποφάσεων σε επίπεδο Ένωσης, γ) τη διευκόλυνση, κατόπιν αιτήματος, του τεχνικού χειρισμού τέτοιων συμβάντων ή κρίσεων, μεταξύ άλλων ιδίως με την παροχή στήριξης για την εθελούσια ανταλλαγή τεχνικών λύσεων μεταξύ των κρατών μελών, δ) τη στήριξη των θεσμικών και λοιπών οργάνων και των οργανισμών της Ένωσης και, κατόπιν αιτήματός τους, των κρατών μελών στη δημόσια επικοινωνία σχετικά με τα εν λόγω συμβάντα ή κρίσεις».

δ) Αγορά, πιστοποίηση της κυβερνοασφάλειας και προτυποποίηση. Σύμφωνα με το άρθρο 8, ο ENISA υποστηρίζει και προάγει τη χάραξη και την εφαρμογή της πολιτικής της Ένωσης για την πιστοποίηση της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ. Επίσης, ο Οργανισμός εκδίδει κατευθυντήριες γραμμές και εκπονεί μελέτες σχετικά με ορθές πρακτικές για τις απαιτήσεις της κυβερνοασφάλειας και τα τεχνικά πεδία αυτών, αναλύοντας παράλληλα και τις εξελίξεις της διεθνούς αγοράς σε αυτόν τον τομέα. Τέλος, ο ENISA διευκολύνει την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ.

ε) Παροχή γνώσεων και πληροφοριών. Σύμφωνα με το άρθρο 9, ο ENISA διενεργεί αναλύσεις και αξιολογήσεις νέων τεχνολογιών, εκπονεί μακροπρόθεσμες στρατηγικές και παρέχει στις αρμόδιες εθνικές αρχές συμβουλές, καθοδήγηση και γνωστοποίηση των βέλτιστων πρακτικών. Παράλληλα, συλλέγει και αναλύει δημόσια διαθέσιμες πληροφορίες, σχετικά με σημαντικά συμβάντα και συντάσσει εκθέσεις με σκοπό την παροχή καθοδήγησης σε πολίτες, οργανισμούς και επιχειρήσεις στην Ένωση.

στ) Ευαισθητοποίηση και Εκπαίδευση. Ο Οργανισμός ευαισθητοποιεί το κοινό σχετικά με τους κινδύνους κυβερνοασφάλειας, διοργανώνοντας τακτικά εκστρατείες

ενημέρωσης για την κυβερνοασφάλεια και γνωστοποιώντας στις εθνικές αρχές βέλτιστες πρακτικές.

ζ) Έρευνα και Καινοτομία. Σύμφωνα με το άρθρο 11 ο Οργανισμός «*παρέχει υπηρεσίες συμβούλου στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και τα κράτη μέλη σχετικά με ερευνητικές ανάγκες και προτεραιότητες στον τομέα της κυβερνοασφάλειας, με σκοπό να καταστεί δυνατή η αποτελεσματική απόκριση στους υπάρχοντες και τους εμφανιζόμενους κινδύνους και τις κυβερνοαπειλές, μεταξύ άλλων σε σχέση με τις νέες και αναδυόμενες τεχνολογίες της πληροφορίας και των τηλεπικοινωνιών, και για την αποτελεσματική χρήση τεχνολογιών πρόληψης κινδύνων*».

η) Διεθνής Συνεργασία. Σύμφωνα με το άρθρο 12, ο ENISA συμβάλλει στις προσπάθειες της Ένωσης για συνεργασία της με τρίτες χώρες και διεθνείς οργανισμούς , για την προώθηση της διεθνούς συνεργασίας σε θέματα που αφορούν την κυβερνοασφάλεια. Για τον σκοπό αυτόν συμμετέχει ως παρατηρητής στην οργάνωση διεθνών ασκήσεων αναλύοντας τα αποτελέσματά τους και υποβάλλοντας σχετικές εκθέσεις στο διοικητικό συμβούλιο διευκολύνοντας, παράλληλα, την ανταλλαγή βέλτιστων πρακτικών με την παροχή συμβουλών και εμπειρογνωμοσύνης, κατόπιν αιτήματος της Επιτροπής.

Έτσι, στο πλαίσιο των καθηκόντων του, ο Οργανισμός έχει αναπτύξει μια πληθώρα δράσεων: Ενδεικτικά αναφέρονται:

α) *πανευρωπαϊκά προγράμματα αντιμετώπισης κρίσεων στον κυβερνοχώρο*[124], τα οποία αφορούν κυρίως την δημιουργία ασκήσεων μέσω προσομοιώσεων κρίσεων. Ειδικότερα, κάθε δύο έτη (με αρχή το 2010) ο Οργανισμός εκδίδει σενάρια κρίσεων με την ονομασία Cyber Europe[125], εμπνευσμένα από πραγματικά γεγονότα, τα οποία αφορούν σε κρίσεις μεγάλης κλίμακας και απευθύνονται τόσο σε δημόσιους όσο και σε ιδιωτικούς παράγοντες. Την ίδια στιγμή, έχει αναπτυχθεί η πλατφόρμα CEP (Cyber Exercise Platform), η οποία υποστηρίζει τη διαχείριση σύνθετων ασκήσεων, φιλοξενεί έναν ολοκληρωμένο χάρτη των επικείμενων και προηγούμενων ασκήσεων,

[124] ENISA, Cyber Exercises, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises
[125] ENISA, Cyber Europe, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

περιλαμβάνει έναν χώρο εξάσκησης με υψηλές τεχνικές προκλήσεις και αποτελεί το σημείο εισόδου σε ένα εικονικό κυβερνοχώρο που μιμείται την πραγματικότητα[126].

β) *εθνικές στρατηγικές ασφάλειας στον Κυβερνοχώρο*[127]. Ο Οργανισμός αναπτύσσει τα προγράμματα NCSS (national cybersecurity strategy) τα οποία ουσιαστικά αποτελούν σχέδια δράσης που έχουν σχεδιαστεί για να βελτιώσουν την ασφάλεια και την ανθεκτικότητα των εθνικών υποδομών και υπηρεσιών σε κυβερνοεπιθέσεις. Πρόκειται για υψηλού επιπέδου προσέγγιση που λειτουργεί από την κορυφή προς τα κάτω (level top – down), καθορίζοντας συγκεκριμένους στόχους και προτεραιότητες που πρέπει επιτευχθούν σε συγκεκριμένο χρονικό πλαίσιο. Πλέον, όλα τα κράτη μέλη διαθέτουν Εθνική Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο που αποτελεί σημαντικό σημείο της πολιτικής τους.

γ) *Ανάπτυξη συνεργασίας και ικανοτήτων.* Αρχικά, ο Οργανισμός παρέχει στους ενδιαφερόμενους λίστα με ομάδες αντιμετώπισης έκτακτων αναγκών, μέσω ενός διαδραστικού εργαλείου, δίνοντας την δυνατότητα στον εκάστοτε ενδιαφερόμενο να πραγματοποιήσει αναζήτηση βάσει χώρας, δικτύου, περιοχής ή τύπου[128]. Επιπλέον, μέσω οδηγών ο Οργανισμός καθιστά εφικτό στον χρήστη να ενημερωθεί, να βελτιώσει τις ικανότητες του, να ωριμάσει και να προετοιμαστεί κατάλληλα για την καλύτερη προστασία του[129].

δ) *Δημοσίευση εκθέσεων και μελετών για την ασφάλεια στον Κυβερνοχώρο.* Ο Οργανισμός κάθε έτος παράγει σημαντικό έργο, υπό την μορφή μελετών και εκθέσεων. Συγκεκριμένα, έχει εκπονήσει μελέτες και εκθέσεις σχετικά με την ασφάλεια στο υπολογιστικό νέφος, την προστασία των δεδομένων, τις νέες τεχνολογίες για την βελτίωση της προστασίας της ιδιωτικής και οικογενειακής ζωής, την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπίστευσης και αυθεντικότητας στις ηλεκτρονικές συναλλαγές, τον εντοπισμό απειλών στον κυβερνοχώρο κ.α.

---

[126] ENISA, Cyber Exercises Platform, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform

[127] ENISA, National Security Strategies, διαθέσιμο σε: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[128] ENISA, CSIRT Inventory, διαθέσιμο σε: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory

[129] ENISA, CSIRT Capabilities, διαθέσιμο σε: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities

Παράλληλα, ο Οργανισμός εκδίδει κάθε χρόνο το ετήσιο πρόγραμμα εργασίας του στο πλαίσιο του ελέγχου και της λογοδοσίας που απαιτείται για την δράση οργάνων και οργανισμών της Ένωσης.

ε) *Συνεργασία με έτερους Οργανισμούς της Ευρωπαϊκής Ένωσης.* Ο Οργανισμός ENISA, συνεργάζεται στενά τόσο με την Europol, όσο και με το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον Κυβερνοχώρο (European Cyber Crime Centre – EC3), αναλαμβάνοντας από κοινού δραστηριότητες έρευνας και αποτελεσματικής επικοινωνίας. Παράλληλα, παρέχει αρωγή και τεχνογνωσία για θέματα ασφάλειας στον Κυβερνοχώρο στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου (EAA), στον Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), στον Ευρωπαϊκό Οργανισμό για τη Λειτουργική Διαχείριση Μεγάλων Πληροφοριακών Συστημάτων στον Χώρο της Ελευθερίας, Ασφάλειας και Δικαιοσύνης (eu-LISA) και στον Ευρωπαϊκό Οργανισμό Ασφάλειας της Αεροπορίας (EASA).

6.1.3. ΔΟΜΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

6.1.3.1. ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ

Το Δ.Σ. του Οργανισμού απαρτίζεται από έναν εκπρόσωπο κάθε κράτους μέλους της Ένωσης καθώς και δύο εκπροσώπους που διορίζονται από την Επιτροπή, με δικαίωμα ψήφου. Στο Δ.Σ. διορίζονται και τα αναπληρωματικά μέλη. Υπό τον προ ισχύον Κανονισμό 469/2004 διοριζόταν τρεις εκπρόσωποι από το Συμβούλιο μετά από πρόταση της Επιτροπής χωρίς ωστόσο να διαθέτουν δικαίωμα ψήφου. Από τους ανωτέρω τρεις εκπροσώπους χωρίς δικαίωμα ψήφου, ο ένας προερχόταν από τον βιομηχανικό κλάδο των τεχνολογιών των πληροφοριών και των επικοινωνιών, ο άλλος από ενώσεις καταναλωτών και ο τελευταίος από πανεπιστημιακούς εμπειρογνώμονες σε θέματα ασφάλειας δικτύων και πληροφοριών.

Στο Διοικητικό Συμβούλιο του Οργανισμού παρέχονται οι απαραίτητες εξουσίες ώστε να είναι ικανό να ασκεί απρόσκοπτα τις αρμοδιότητές του, οι οποίες αφορούν:

α) *Καθορισμό των γενικών κατευθύνσεων λειτουργίας του ENISA*. Το Δ.Σ. διασφαλίζει επίσης ότι ο ENISA λειτουργεί σύμφωνα με τους κανόνες και τις αρχές που θεσπίστηκαν στον παρόντα κανονισμό· επίσης, διασφαλίζει τη συνοχή των εργασιών του ENISA με τις δραστηριότητες που διεξάγονται από τα κράτη μέλη, καθώς και σε επίπεδο Ένωσης

α) *Καθορισμό του προϋπολογισμού του*. Οι δημοσιονομικοί κανόνες που εφαρμόζονται για την λειτουργία του Οργανισμού πρέπει να συνάδουν με τον Κανονισμό 2343/2002 της Επιτροπής για τη θέσπιση δημοσιονομικού κανονιστικού πλαισίου για τους κοινοτικούς οργανισμούς και του άρθρου 185 του Κανονισμού 1605/2002 του Συμβουλίου, με τον οποίο θεσπίζεται ο δημοσιονομικός κανονισμός που εφαρμόζεται στον γενικό προϋπολογισμό των Ευρωπαϊκών Κοινοτήτων. Εξαίρεση επιτρέπεται εάν η συγκεκριμένη παρέκκλιση απαιτείται για τις ειδικές ανάγκες λειτουργίας του Οργανισμού και κατόπιν προηγούμενης συναινέσεως της Επιτροπής[130]. Άλλωστε, για την θέσπιση του προϋπολογισμού απαιτείται διαβούλευση με την Επιτροπή. Ο προϋπολογισμός εγκρίνεται με πλειοψηφία 2/3 όλων των μελών που διαθέτουν δικαίωμα ψήφου.

β) Έγκριση εσωτερικού κανονισμού και εσωτερικών κανόνων λειτουργίας. Το Δ.Σ. εγκρίνει τους εσωτερικούς κανόνες λειτουργίας και τον εσωτερικό κανονισμό του, ύστερα από πρόταση της Επιτροπής, αποφασίζοντας με την πλειοψηφία των μελών του που διαθέτουν δικαίωμα ψήφου. Για την έγκριση απαιτείται πλειοψηφία 2/3 όλων των μελών που διαθέτουν δικαίωμα ψήφου.

γ) Ορισμό των γενικών προσανατολισμών λειτουργίας. Το Δ.Σ. του Οργανισμού διασφαλίζει ότι αυτός θα λειτουργεί σύμφωνα με τα όσα ορίζονται στα άρθρα 12 – 14 και το άρθρο 23 του Κανονισμού. Παράλληλα συντονίζει σχετικές δράσεις που αναλαμβάνονται τόσο σε ενωσιακό όσο και σε εθνικό επίπεδο.

δ) Έγκριση προγράμματος εργασίας. Το Δ.Σ. έχοντας λάβει προηγουμένως την γνώμη της Επιτροπής εγκρίνει το πρόγραμμα εργασίας του Οργανισμού για το επόμενο έτος. Καθήκον του Δ.Σ. είναι να διασφαλίσει ότι το προς έγκριση πρόγραμμα συμβαδίζει με τις νομοθετικές και πολιτικές προτεραιότητες της Ένωσης, καθώς και

[130] Κανονισμός 469/2004, Άρθρο 6 παρ. 10

με τους υφιστάμενους στόχους και καθήκοντα του Οργανισμού. Για την έγκριση απαιτείται πλειοψηφία 2/3 όλων των μελών που διαθέτουν δικαίωμα ψήφου.

ε) Διορισμός και απομάκρυνση προέδρου και αντιπροέδρου. Η θητεία τους έχει διάρκεια τεσσάρων ετών[131] με δυνατότητα ανανέωσης μία φορά. Για τον διορισμό απαιτείται πλειοψηφία 2/3 όλων των μελών που διαθέτουν δικαίωμα ψήφου. Μεταξύ άλλων, καθήκον του προέδρου είναι η σύγκληση των συνεδριάσεων του Δ.Σ., το οποίο συνέρχεται σε τακτική συνεδρίαση δύο φορές ετησίως. Σε έκτακτη συνεδρίαση δύναται να συνέρχεται το Δ.Σ. με πρωτοβουλία του προέδρου ή ύστερα από αίτηση 1/3 των μελών με δικαίωμα ψήφου.

στ) Καθιέρωση διαφανών διαδικασιών εργασίας για τη λήψη αποφάσεων. Η λειτουργία του Οργανισμού διέπεται από την αρχή της Διαφάνειας. Για τον λόγο αυτό καταβάλλεται μέριμνα ώστε να παρέχονται στο κοινό και σε κάθε ενδιαφερόμενο μέρος αντικειμενικές, αξιόπιστες και εύκολα προσβάσιμες πληροφορίες, ιδίως όσον αφορά τα αποτελέσματα των εργασιών του[132]. Παράλληλα, ο Κανονισμός 1049/2001 για την πρόσβαση στα έγγραφα εφαρμόζεται και για τον παρόντα Οργανισμό[133].

ζ) Λοιπές αρμοδιότητες. Επίσης το Δ.Σ.: αζ) χαράσσει στρατηγική καταπολέμησης της απάτης ανάλογη των κινδύνων απάτης και λαμβάνοντας υπόψη την ανάλυση κόστους-οφέλους των ληπτέων μέτρων, βζ) θεσπίζει κανόνες για την πρόληψη και τη διαχείριση συγκρούσεων συμφερόντων στις οποίες εμπλέκονται τα μέλη του, γζ) εξασφαλίζει ότι δίνεται κατάλληλη συνέχεια στα πορίσματα και τις συστάσεις που προκύπτουν από τις έρευνες της Ευρωπαϊκής Υπηρεσίας Καταπολέμησης της Απάτης (OLAF) και τις διάφορες διεθνείς ή εξωτερικές εκθέσεις ελέγχου και αξιολογήσεις, δζ) όσον αφορά το προσωπικό του ENISA, ασκεί τις εξουσίες που ανατίθενται από τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων και από το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ευρωπαϊκής Ένωσης, εζ) διορίζει υπόλογο, ο οποίος μπορεί να είναι ο υπόλογος της Επιτροπής και ο οποίος λειτουργεί υπό καθεστώς πλήρους ανεξαρτησίας κατά την άσκηση των καθηκόντων του, στζ)

[131] Αυξήθηκε από τα δυόμισι έτη που προβλεπόταν στον προηγούμενο Κανονισμό.
[132] Κανονισμός 460/2004, Άρθρο 12 παρ. 2
[133] Κανονισμός 460/2004, Άρθρο 14 παρ. 1 και Κανονισμός 881/2019 άρθρο 26 σε συνδυασμό με το Άρθρο 28

λαμβάνει όλες τις αποφάσεις σχετικά με τη συγκρότηση των εσωτερικών δομών του ENISA, ζζ) εγκρίνει τη θέσπιση συμφωνιών συνεργασίας όσον αφορά το άρθρο 7, ηζ) εγκρίνει τη θέσπιση ή τη σύναψη συμφωνιών συνεργασίας σύμφωνα με το άρθρο 42.

6.1.3.2. ΕΚΤΕΛΕΣΤΙΚΟ ΣΥΜΒΟΥΛΙΟ

Το εκτελεστικό συμβούλιο αποτελείται από πέντε μέλη που διορίζονται μεταξύ αυτών που απαρτίζουν το Διοικητικό Συμβούλιο. Υποχρεωτικά, το ένα μέλος είναι ο πρόεδρος του Δ.Σ. που μπορεί να προεδρεύει και του Εκτελεστικού Συμβουλίου. Επίσης, το ένα μέλος πρέπει να είναι ο ένας από τους δύο εκπροσώπους της Επιτροπής στο Δ.Σ. Η θητεία των μελών είναι τετραετής με δυνατότητα ανανέωσης.

Το Εκτελεστικό Συμβούλιο έχει περιορισμένες αρμοδιότητες. Σύμφωνα με το άρθρο 19 του Κανονισμού, το εκτελεστικό συμβούλιο έχει αρμοδιότητα να:

α) προετοιμάζει τις αποφάσεις που λαμβάνει το διοικητικό συμβούλιο,

β) διασφαλίζει, μαζί με το διοικητικό συμβούλιο, την κατάλληλη συνέχεια στα πορίσματα και τις συστάσεις που προκύπτουν από τις έρευνες της OLAF και τις διάφορες διεθνείς ή εξωτερικές εκθέσεις ελέγχου και αξιολογήσεις,

γ) με την επιφύλαξη των αρμοδιοτήτων του εκτελεστικού διευθυντή που καθορίζονται στο άρθρο 20, επικουρεί και συμβουλεύει τον εκτελεστικό διευθυντή όσον αφορά στην εκτέλεση των αποφάσεων του διοικητικού συμβουλίου για διοικητικά και δημοσιονομικά θέματα σύμφωνα με το άρθρο 20.

6.1.3.3. ΕΚΤΕΛΕΣΤΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ

Ο Εκτελεστικός Διευθυντής διορίζεται από το Διοικητικό Συμβούλιο, μέσω της προβλεπόμενης διαδικασίας, με πλειοψηφία 2/3 όλων των μελών που διαθέτουν δικαίωμα ψήφου. Ειδικότερα, δημοσιεύεται στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης πρόσκληση για εκδήλωση ενδιαφέροντος διενεργώντας γενικό διαγωνισμό. Στην συνέχεια, η Επιτροπή προτείνει έναν κατάλογο με ενδιαφερόμενους στο Δ.Σ. οι οποίοι πληρούν τα προσόντα που έχουν τεθεί και διαθέτουν αποδεδειγμένες διοικητικές και διαχειριστικές ικανότητες καθώς και πείρα στον τομέα των δικτύων και των πληροφοριών. Έπειτα, το Δ.Σ. επιλέγει ένα

πρόσωπο από τον κατάλογο για Εκτελεστικό Διευθυντή του Οργανισμού, το οποίο καλείται πριν διοριστεί να προβεί σε δήλωση ενώπιον του Ευρωπαϊκού Κοινοβουλίου και να απαντήσει σε ερωτήσεις των μελών του. Επισημαίνεται ότι ο Εκτελεστικός Διευθυντής δύναται να καλείται για ακρόαση ενώπιον του Κοινοβουλίου και του Συμβουλίου, ύστερα από αίτηση τους, για κάθε θέμα που άπτεται των αρμοδιοτήτων του[134]. Η θητεία του διαρκεί έως πέντε έτη.

Σύμφωνα με το άρθρο 20 του Κανονισμού ο Διευθυντής είναι υπεύθυνος για τα ακόλουθα:

α) την τρέχουσα διοίκηση του ENISA,

β) την εκτέλεση των αποφάσεων που έχουν εγκριθεί από το διοικητικό συμβούλιο,

γ) την εκπόνηση του σχεδίου ενιαίου εγγράφου προγραμματισμού και την υποβολή του στο διοικητικό συμβούλιο προς έγκριση, πριν από την υποβολή του στην Επιτροπή,

δ) την εφαρμογή του ενιαίου εγγράφου προγραμματισμού και την υποβολή σχετικής έκθεσης στο διοικητικό συμβούλιο,

ε) την κατάρτιση της ενοποιημένης ετήσιας έκθεσης δραστηριοτήτων του ENISA, συμπεριλαμβανομένης της υλοποίησης του ετήσιου προγράμματος εργασίας του ENISA, και την υποβολή της στο διοικητικό συμβούλιο προς αξιολόγηση και έγκριση,

στ) την κατάρτιση σχεδίου δράσης με το οποίο δίνεται συνέχεια στα συμπεράσματα των αναδρομικών αξιολογήσεων και την υποβολή έκθεσης προόδου στην Επιτροπή ανά δύο έτη,

ζ) την κατάρτιση σχεδίου δράσης με το οποίο δίνεται συνέχεια στα πορίσματα εσωτερικών ή εξωτερικών εκθέσεων ελέγχου, καθώς και στις έρευνες της OLAF, και την υποβολή έκθεσης προόδου δύο φορές ετησίως στην Επιτροπή και ανά τακτά χρονικά διαστήματα στο διοικητικό συμβούλιο,

[134] Κανονισμός 460/2004, Άρθρο 7 παρ. 2

η) την εκπόνηση του σχεδίου των δημοσιονομικών κανόνων που εφαρμόζονται στον ENISA όπως αναφέρονται στο άρθρο 32,

θ) την κατάρτιση του σχεδίου κατάστασης προβλεπόμενων εσόδων και εξόδων του ENISA και την εκτέλεση του προϋπολογισμού του,

ι) την προστασία των οικονομικών συμφερόντων της Ένωσης, με την εφαρμογή προληπτικών μέτρων κατά της απάτης, της διαφθοράς και άλλων παράνομων δραστηριοτήτων, με αποτελεσματικούς ελέγχους και, σε περίπτωση που διαπιστωθούν παρατυπίες, με την ανάκτηση των αχρεωστήτως καταβληθέντων ποσών και, όπου είναι σκόπιμο, την επιβολή αποτελεσματικών, αναλογικών και αποτρεπτικών διοικητικών και οικονομικών κυρώσεων,

ια) τη χάραξη στρατηγικής του ENISA, για την καταπολέμηση της απάτης, και την υποβολή της στο διοικητικό συμβούλιο προς έγκριση,

ιβ) την ανάπτυξη και διατήρηση επαφών με την επιχειρηματική κοινότητα και τις ενώσεις καταναλωτών, ώστε να εξασφαλίζεται τακτικός διάλογος με τους σχετικούς συμφεροντούχους,

ιγ) την τακτική ανταλλαγή απόψεων και πληροφοριών με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης σχετικά με τις δραστηριότητές τους σχετικά με την κυβερνοασφάλεια, προκειμένου να διασφαλίζεται η συνεκτικότητα κατά την ανάπτυξη και εφαρμογή της πολιτικής της Ένωσης,

ιδ) την εκτέλεση άλλων καθηκόντων που ανατίθενται στον εκτελεστικό διευθυντή, δυνάμει του παρόντος κανονισμού.

Επιπρόσθετα, ο Διευθυντής κάθε έτος υποβάλει στο Δ.Σ. σχέδιο γενικής έκθεσης με τις δραστηριότητες του Οργανισμού κατά τον προηγούμενο χρόνο, καθώς και σχέδιο προγράμματος εργασίας, το οποίο ύστερα από έγκριση του Δ.Σ. δημοσιεύει και διαβιβάζει στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή και τα κράτη μέλη. Τέλος, ο Διευθυντής έχει την δυνατότητα να συστήνει ad hoc ομάδες εργασίας, αποτελούμενες από εμπειρογνώμονες για την διεκπεραίωση τεχνικών και επιστημονικών ζητημάτων.

6.1.3.4. ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ

Η Ομάδα συγκροτείται από το Δ.Σ. του Οργανισμού, ύστερα από πρόταση του εκτελεστικού διευθυντή και απαρτίζεται από εμπειρογνώμονες που αντιπροσωπεύουν συμφεροντούχους, οι οποίοι προέρχονται από τον κλάδο ΤΠΕ, τους παρόχους δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών για το κοινό, μικρομεσαίες επιχειρήσεις, τους φορείς εκμετάλλευσης βασικών υπηρεσιών, ομάδες καταναλωτών, τους πανεπιστημιακούς που είναι ειδικοί στον τομέα της κυβερνοασφάλειας, και εκπροσώπους των αρμόδιων αρχών. Η διάρκεια της θητείας των μελών είναι δυόμισι έτη.

Η Συμβουλευτική Ομάδα αντικαθιστά ουσιαστικά την Μόνιμη Ομάδα Ενδιαφερόμενων, η οποίο ιδρύθηκε με τον Κανονισμό 469/2004. Σε σύμπλευση με την Μόνιμη Ομάδα Ενδιαφερομένων, ο πρωταρχικός ρόλος της Συμβουλευτικής Ομάδας είναι να συμβουλεύει τον εκτελεστικό διευθυντή, κατά την άσκηση των καθηκόντων, κατά την εκπόνηση πρότασης για το πρόγραμμα εργασίας του Οργανισμού, καθώς και για την εξασφάλιση επικοινωνίας με τους οικείους ενδιαφερόμενους επί όλων των θεμάτων που αφορούν το πρόγραμμα εργασίας[135].

6.1.3.5. ΔΙΚΤΥΟ ΕΘΝΙΚΩΝ ΣΥΝΔΕΣΜΩΝ

Το Δίκτυο Συνδέσμων ιδρύθηκε αρχικά το 2004 ως ένα ανεπίσημο σημείο αναφοράς, ενώ πλέον με το άρθρο 23 αποτελεί μέρος της δομής του Οργανισμού. Το Εθνικό Δίκτυο Συνδέσμων διευκολύνει την ανταλλαγή πληροφοριών μεταξύ του ENISA και των κρατών μελών και υποστηρίζει τον ENISA στη διάδοση των δραστηριοτήτων, των πορισμάτων και των συστάσεών του στους σχετικούς ενδιαφερόμενους φορείς σε ολόκληρη την Ένωση[136]. Επίσης, διαδραματίζει σημαντικό ρόλο στην εφαρμογή του ετήσιου προγράμματος εργασίας του ENISA εντοπίζοντας ενδιαφερόμενα μέρη για την υποστήριξη του έργου του ENISA, ενημερώνοντας για τις εθνικές εξελίξεις στον κυβερνοχώρο και υποστηρίζοντας τη διάδοση δραστηριοτήτων, ευρημάτων και συστάσεων.

[135] Κανονισμός 460/2004, Άρθρο 8 παρ. 5 και Κανονισμός 881/2019 Άρθρο 21

[136] ENISA, NLO Network, διαθέσιμο σε: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office

6.2. ΕΥΡΩΠΑΪΚΟ ΚΕΝΤΡΟ ΓΙΑ ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ (EC3)

Το Ευρωπαϊκό Κέντρο Κυβερνοεγκλήματος ιδρύθηκε το 2012, ύστερα από πρωτοβουλία της Επιτροπής και έγκριση του Συμβουλίου της Ευρωπαϊκής Ένωσης και ξεκίνησε την λειτουργία του το 2013, ως μέρος της δομής της Europol, προκειμένου να συμπλεχθεί με άλλους τομείς της εγκληματικότητας[137]. Η δημιουργία του Κέντρου αποτελούσε προτεραιότητα της Ένωσης όπως προβλεπόταν στην Στρατηγική εσωτερικής ασφάλειας[138]. Σκοπός της ίδρυσης του Κέντρου ήταν να λειτουργήσει ως ένας κόμβος πληροφόρησης για το κυβερνοέγκλημα καθώς και να αποτελέσει μια ουσιαστική αντίδραση της επιβολής του νόμου στην συνεχώς αυξανόμενη άνοδο του κυβερνοεγκλήματος. Πράγματι, από την ίδρυσή του, το Κέντρο έχει συμβάλει σημαντικά στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο συμμετέχοντας σε δεκάδες επιχειρήσεις υψηλού κύρους και εκατοντάδες επιτόπου αναπτύξεις επιχειρησιακής υποστήριξης με αποτέλεσμα εκατοντάδες συλλήψεις. Παράλληλα, έχει προβεί σε ανάλυση εκατοντάδων χιλιάδων αρχείων, η συντριπτική πλειοψηφία των οποίων έχει αποδειχθεί ότι είναι κακόβουλα. Με αυτόν τον τρόπο το Κέντρο έχει παράσχει προστασία στους ευρωπαίους πολίτες, τις επιχειρήσεις και στις κυβερνήσεις από το έγκλημα στο διαδίκτυο[139].

6.2.1. ΣΤΟΧΟΙ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΕΝΤΡΟΥ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Κάθε χρόνο το Κέντρο για το έγκλημα στον Κυβερνοχώρο δημοσιεύει ετήσια έκθεση με περιεχόμενο την εκτίμηση απειλών από το οργανωμένο έγκλημα[140]. Η έκθεση αυτή παρέχει σημαντικές κατευθύνσεις στις αρχές επιβολής του νόμου και στους εθνικούς νομοθέτες αναφορικά με τις προτεραιότητες, τους στόχους και τις δράσεις που συνίσταται να αναληφθούν για την αντιμετώπιση του

[137] DigWatch, European CyberCrime Centre, διαθέσιμο σε: https://dig.watch/actors/european-cybercrime-centre

[138] Ευρωπαϊκή Επιτροπή, COM(2010)673 final, Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη

[139] Europol, European CyberCrime Centre EC-3, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[140] Για το 2021, βλ. Europol, Internet Organized Crime Threat Assessment (IOCTA) 2021, διαθέσιμο σε https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf, προσπελάστηκε την 17/02/2022

κυβερνοεγκλήματος. Στο πλαίσιο, αυτό οι κύριοι στόχοι του Κέντρου στον τομέα αυτόν είναι οι εξής:

α) Αντιμετώπιση σεξουαλικής εκμετάλλευσης παιδιών. Σεξουαλική εκμετάλλευση παιδιού αποτελεί κάθε πράξη σεξουαλικής κακοποίησης ατόμου κάτω των 18 χρονών, καθώς και η παραγωγή εικόνων τέτοιας εκμετάλλευσης και ο διαμοιρασμός τους στο διαδίκτυο[141]. Η χρήση του διαδικτύου στο εν λόγω φαινόμενο είναι εξαιρετικά συχνής και διαρκώς αυξανόμενη, καθώς οι εγκληματίες χρησιμοποιούν υπηρεσίες ανωνυμοποίησης, για να καλύπτουν τα ίχνη τους και υπηρεσίες ζωντανής σύνδεσης, όπου αποκομίζουν υψηλά οικονομικά οφέλη από χρήστες που παρακολουθούν την κακοποίηση σε πραγματικό χρόνο. Στο πλαίσιο αυτό, η Europol έχει εντοπίσει δύο κύριες απειλές: Αφενός, η χρήση δικτύων peer-to-peer και δίκτυα με ανώνυμη πρόσβαση, όπως το darknet. Τέτοια υπολογιστικά περιβάλλοντα καθίστανται οι κύριες πλατφόρμες, όπου παρατηρείται το φαινόμενο σεξουαλικής εκμετάλλευσης παιδιών, καθώς παρέχουν στους εγκληματίες το πλεονέκτημα της ανωνυμίας και της εύκολης χρήσης. Παράλληλα με το υψηλό επίπεδο ανωνυμίας, το «κρυφό» διαδίκτυο που υπάρχει κάτω από το νόμιμο, προσφέρει μεγάλες δυνατότητες διασύνδεσης (networking) μεταξύ των ατόμων που επιδίδονται σε σχετικές δραστηριότητες, με αποτέλεσμα οι εγκληματίες να αισθάνονται ασφάλεια να προβαίνουν στα εγκλήματα τους και να συζητούν μεταξύ τους τα σεξουαλικά τους ενδιαφέροντα. Αφετέρου, και σε αντίθεση με την ανωτέρω απειλή που αναφέρεται σε μη εμπορική δραστηριότητα, η δεύτερη κύρια απειλή συνίσταται στην ζωντανή μετάδοση της σεξουαλικής κακοποίησης παιδιών. Η νέα τεχνολογία παρέχει την δυνατότητα για κερδοσκοπική δραστηριότητα των εγκληματιών, όπου προβαίνουν σε πράξεις εκμετάλλευσης μπροστά σε κάμερες κατόπιν αιτήματος των πελατών.

Σε κάθε περίπτωση, το Κέντρο υποστηρίζει τις αρμόδιες αρχές για την πρόληψη και την αντιμετώπιση όλων των εγκληματικών μορφών που σχετίζονται με την σεξουαλική εκμετάλλευση παιδιών. Ειδικότερα, το Κέντρο παρέχει βοήθεια και τεχνογνωσία στην καταπολέμηση της διανομής που παράνομου περιεχομένου στο διαδίκτυο, σε κάθε μορφή διαδικτυακού περιβάλλοντος. Το περιεχόμενο αυτό,

[141] Europol, Child Sexual Exploitation, διαθέσιμο σε https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation,

ενδεικτικά, μπορεί να αφορά είτε παράνομο υλικό που παράγεται από τον ίδιο τον δράστη είτε σεξουαλικό εκβιασμό ή ζωντανή μετάδοση στο διαδίκτυο.

Για την αποτελεσματικότερη συμβολή του στην αντιμετώπιση του εν λόγω φαινομένου το Κέντρο έχει αναπτύξει διάφορες συνεργασίες με τρίτα μέρη. Έτσι, συμμετέχει στον Ευρωπαϊκό Χρηματοοικονομικό Συνασπισμό κατά της Εμπορικής Σεξουαλικής Εκμετάλλευσης Παιδιών στο Διαδίκτυο (EFC), ένα δίκτυο χρηματοδοτούμενο από την Ευρωπαϊκή Επιτροπή με συμμετοχή των αρχών επιβολής του νόμου, Μη Κυβερνητικών Οργανώσεων και ιδιωτικών ή δημόσιων φορέων. Παράλληλα, λαμβάνει μέρος στην Εικονική Παγκόσμια Ομάδα Εργασίας (VGT), μια συνεργασία των αρχών επιβολής του νόμου για την κάλυψη του ψηφιακού χάσματος σε παγκόσμιο επίπεδο, με σκοπό την αποτελεσματικότερη αντιμετώπιση της διαδικτυακής σεξουαλικής κακοποίησης παιδιών.

β) Παρακολούθηση της εξέλιξης του κυβερνοεγκλήματος. Η τεχνική καινοτομία μπορεί να αξιοποιηθεί για το κοινωνικό, καλό αλλά εξίσου εύκολα και για κακόβουλους σκοπούς. Αυτό ισχύει ακόμα περισσότερο για το έγκλημα στον κυβερνοχώρο από ότι, ίσως, σε οποιαδήποτε άλλη μορφή εγκλήματος. Οι εγκληματίες του κυβερνοχώρου γίνονται επίσης πιο επιθετικοί. Αυτός είναι ο λόγος για τον οποίο η Europol και οι οργανισμοί - εταίροι της δίνουν μάχη εναντίον τους σε όλα τα μέτωπα[142].

Όπως έχει διαπιστωθεί, οι κυβερνοεγκληματίες εκμεταλλεύονται μια πληθώρα ευκαιριών για να διαπράξουν τα εγκλήματα τους. Αυτές οι ευκαιρίες περιλαμβάνουν ιδίως την χρήση ρομπότ (botnets), τα οποία μολύνουν τα λογισμικά χωρίς να το γνωρίζουν οι χρήστες, με αποτέλεσμα οι εγκληματίες να έχουν απομακρυσμένη πρόσβαση στο μολυσμένο λογισμικό, την δημιουργία “back doors” για την κλοπή χρημάτων και δεδομένων, το ξέπλυμα παραδοσιακού και ψηφιακού χρήματος, την διάπραξη διαδικτυακών απατών μέσω τον ψηφιακών συστημάτων πληρωμών και των χρεωστικών και λοιπών καρτών, καθώς και τις διάφορες μορφές

[142] Europol, Cybercrime, διαθέσιμο σε: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime,

σεξουαλικής εκμετάλλευσης παιδιών και πώληση μέσω του διαδικτύου παράνομων προϊόντων όπως όπλα, πλαστά διαβατήρια και ναρκωτικά[143].

Στο πλαίσιο αυτό, η απάντηση της Europol πρέπει να είναι αποτελεσματική και δυναμική. Για τον λόγο αυτό, άλλωστε, δημιουργήθηκε το Κέντρο για την αντιμετώπιση του Κυβερνοεγκλήματος, με σκοπό την αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος από τις αρχές επιβολής του νόμου και την προστασία των πολιτών την Ένωσης, των κυβερνήσεων και των εταιρειών. Προς επίτευξη του ανωτέρω σκοπού, το Κέντρο δημοσιεύει την ετήσια Έκθεση για την εκτίμηση των απειλών από το οργανωμένο έγκλημα (IOCTA), ενώ φιλοξενεί και την Κοινή Ομάδα Δράσης για το κυβερνοέγκλημα (J-CAT), με αποστολή την συνεργασία για την αντιμετώπιση των κυριότερων απειλών κατά της κυβερνοασφάλειας, μέσω της διεξαγωγής διασυνοριακών ερευνών και επιχειρήσεων. Μάλιστα, η ανάπτυξη συνεργασιών αφορά και σε παράγοντες του ιδιωτικού τομέα αλλά και την Eurojust.

γ) Προστασία από τις απάτες σχετικές με τις πληρωμές. Οι εγκληματίες αρέσκονται στην διάπραξη των συγκεκριμένων εγκλημάτων, καθώς αποτελούν εγκλήματα χαμηλού ρίσκου και ταυτόχρονα υψηλού κέρδους. Η απάτη με κάρτες πληρωμών μπορεί να διακριθεί σε δύο κατηγορίες. Αφενός τις απάτες με κάρτες μέσω του διαδικτύου, χωρίς την φυσική χρήση της κάρτας. Αφετέρου, απάτες που λαμβάνουν χώρα σε μηχανήματα αυτόματης ανάληψης (ATM) ή σε λιανικές πωλήσεις με την χρήση φυσικών καρτών[144].

Το Κέντρο ασχολείται κυρίως με τις απάτες της πρώτης κατηγορίας που λαμβάνουν χώρα στο διαδίκτυο. Οι απάτες αυτές συνίστανται στην μη εξουσιοδοτημένη χρήση πιστωτικών ή χρεωστικών δεδομένων όπως αριθμό κάρτας, διεύθυνση χρέωσης, κωδικός ασφαλείας και ημερομηνία λήξης της κάρτας, για την αγορά προϊόντων στο διαδίκτυο, άνευ φυσικής παρουσίας, όπως η αγορά από ένα διαδικτυακό κατάστημα (eshop). Στις περισσότερες περιπτώσεις, τα θύματα αγνοούν

[143] IOCTA (2021), Cyber-depended crime, σελ. 19 επ., διαθέσιμο σε: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf,

[144] Europol, Payment Fraud, διαθέσιμο σε: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud,

την χρήση των καρτών από τρίτους καθώς συνεχίζουν να διατηρούν την φυσική κάρτα στην κατοχή τους.

Άλλωστε, η ραγδαία ανάπτυξη του κλάδου του ηλεκτρονικού εμπορίου έχει οδηγήσει σε αντίστοιχη ανάπτυξη των απατών με κάρτες. Το modus operandi των εγκληματιών αυτής της κατηγορίας αναμένεται να διαμορφωθεί σε συνδυασμό με τα μέτρα που λαμβάνονται συνεχώς από τον ιδιωτικό κλάδο για την προστασία των πληρωμών. Ειδικότερα, οι αναδυόμενοι εναλλακτικοί τρόποι πληρωμών όπως οι πληρωμές με χρήση επικοινωνίας κοντινού επιπέδου (NFC) ή με διπλή διαδικασία ταυτοποίησης (KYC) πρόκειται να ωθήσουν τους κυβερνοεγκληματίες στην εξεύρεση νέων τρόπων παράκαμψης των συστημάτων ασφαλείας.

Στο πλαίσιο αυτό, το Κέντρο υποστηρίζει επιχειρήσεις της Κοινής Ομάδας Δράσης για το κυβερνοέγκλημα (J-CAT), καθώς και εκατοντάδες σχετικές έρευνες. Άλλωστε, η βασική πηγή τέτοιων απατών στον ευρωπαϊκό χώρο απαντάται στον ιδιωτικό κλάδο και συχνά διευκολύνονται από κατόχους εμπιστευτικών πληροφοριών ή και με την χρήση κακόβουλων λογισμικών. Μάλιστα, τα δεδομένα των καρτών που υποκλέπτονται μέσω των ανωτέρω ενεργειών γίνονται διαθέσιμα προς αγορά από τους παραβάτες σε φόρουμ και σε παράνομα διαδικτυακά καταστήματα στο σκοτεινό διαδίκτυο.

Τέτοιου είδους απάτες λαμβάνουν χώρα σε διάφορους τομείς της οικονομικής δραστηριότητας όπως αγορά αγαθών, ενοικιάσεις αυτοκινήτων και ακινήτων καθώς και σε αεροπορικά εισιτήρια. Προς επίρρωση, η δόλια αγορά αεροπορικών εισιτηρίων με αυτόν τον τρόπο βρίσκεται στο επίκεντρο της δράσης Global Airline Action Days[145].

Οι ανωτέρω στόχοι και προτεραιότητες καθορίζονται από τον συνδυασμό συνεισφορών που προέρχονται από ειδικούς της Europol, τα κράτη μέλη, τις αρχές επιβολής του νόμου, τόσο εντός όσο και εκτός Ένωσης, καθώς και από τους συνεργάτες του ιδιωτικού τομέα, της οικονομικής δραστηριότητας και του

[145] Europol, Participants σε Global Airport Action Days (GAAD), διαθέσιμο σε: https://www.europol.europa.eu/operations-services-and-innovation/operations/global-airport-action-days-gaad,

ακαδημαϊκού χώρου. Κατόπιν τούτων, συγκεντρώνονται τα κυριότερα ευρήματα των ερευνών, καθορίζονται οι μελλοντικές απειλές και τέλος διατυπώνονται προτάσεις.

6.2.2. ΚΑΘΗΚΟΝΤΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΕΝΤΡΟΥ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Τα καθήκοντα του Κέντρου επικεντρώνονται στους ακόλουθους τομείς δραστηριότητας:

Α) Κυβερνοεγκλήματα που διαπράττονται από οργανωμένες εγκληματικές ομάδες, ιδίως όταν αποκομίζονται υψηλά κέρδη, όπως στις online απάτες

Β) Κυβερνοεγκλήματα που προκαλούν σημαντική βλάβη στο θύμα, όπως η παιδική πορνογραφία

Γ) Κυβερνοεγκλήματα ή κυβερνοεπιθέσεις που πλήττουν σημαντικές δομές και πληροφοριακά συστήματα στην Ένωση

Έτσι, τα κύρια καθήκοντα αναφορικά με τους τρεις τομείς είναι τα εξής: Πρώτον, το Κέντρο λειτουργεί ως κόμβος πληροφοριών αναφορικά με το κυβερνοέγκλημα. Δεύτερον, υποστηρίζει τις επιχειρήσεις και τις έρευνες των κρατών μελών μέσω επιχειρησιακής ανάλυσης, συντονισμού και εμπειρογνωμοσύνης. Τρίτον, παρέχει μια ποικιλία προϊόντων στρατηγικής ανάλυσης που επιτρέπουν την λήψη τεκμηριωμένων αποφάσεων στο τακτικό και στρατηγικό επίπεδο αναφορικά με την πρόληψη και καταστολή του κυβερνοεγκλήματος. Τέταρτον, καθιερώνει μια λειτουργική σύνδεση μεταξύ των αρχών επιβολής του νόμου για το κυβερνοέγκλημα και του ιδιωτικού τομέα, του ακαδημαϊκού χώρου και λοιπών, μη κρατικών, οργάνων επιβολής του νόμου. Πέμπτον, υποστηρίζει την κατάρτιση και την ανάπτυξη των ικανοτήτων των αρμόδιων αρχών των κρατών μελών. Έκτον, εξειδικεύεται στην παροχή υψηλής τεχνικής και ψηφιακής εγκληματολογικής υποστήριξης στις έρευνες και στις επιχειρήσεις. Έβδομον, εκπροσωπεί την κοινότητα επιβολής του νόμου της Ευρωπαϊκής Ένωσης στους σχετικούς τομείς.

Για την επιτυχή διεκπεραίωση της αποστολής του, το Κέντρο συνεργάζεται με τις υπηρεσίες επιβολής του νόμου, τα θεσμικά όργανα της ΕΕ, τους διεθνείς οργανισμούς, τον ιδιωτικό κλάδο, τον δημόσιο τομέα και τον ακαδημαϊκό χώρο,

αναπτύσσοντας και διατηρώντας συνεργασίες που μπορούν να συμβάλουν στην ενίσχυση των δυνατοτήτων της ΕΕ για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.

Επιπροσθέτως, το Κέντρο έχει αναπτύξει ειδικό project που ερευνά τις κυβερνητικές ρυθμίσεις και την αρχιτεκτονική του διαδικτύου ώστε να εντοπίζει εγκαίρως τυχόν ευπάθειες που εκμεταλλεύονται οι εγκληματικές ομάδες. Παράλληλα, εντοπίζει ευκαιρίες προσπαθώντας να επηρεάσει τις μελλοντικές εξελίξεις σε ζητήματα ασφαλείας και ανάπτυξης του διαδικτύου. Τέλος, ιδιαίτερα σημαντικό ρόλο διαδραματίζει η ετήσια έκθεση[146] του Κέντρου για το οργανωμένο έγκλημα στο διαδίκτυο, η οποία είναι στρατηγικής σημασίας, καθώς δημοσιοποιούνται τα κύρια ευρήματα του Κέντρου και επισημαίνονται οι αναδυόμενες απειλές και εξελίξεις στο κυβερνοέγκλημα.

6.2.3. ΔΟΜΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΕΝΤΡΟΥ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Όπως εκτέθηκε ανωτέρω, το Κέντρο λειτουργεί εντός του πλαισίου της Europol. Ως εκ τούτου, εκμεταλλεύτηκε την σταθερή βάση της Europol, αναφορικά με την οργανωτική του δομή, το νομικό πλαίσιο λειτουργίας του και τα εργαλεία επεξεργασίας πληροφοριών. Άλλωστε, υπήρχε ήδη μια ειδική Ομάδα με τεχνογνωσία και πρακτική εμπειρία στα κύρια σημεία και τις προτεραιότητες για το κυβερνοέγκλημα. Έτσι, επιλέχθηκε ο σχεδιασμός μιας απλής οργανωτικής δομής ώστε να επιτρέπεται η αποτελεσματική ανάθεση και ο συνδυασμός των καθηκόντων, με την παράλληλη διασφάλιση ισχυρής συνοχής και αποτελεσματικής επικοινωνίας εντός του Κέντρου[147].

Έτσι, η οργανωτική δομή του Κέντρου αφορούσε σε δύο κύρια επίπεδα, το επιχειρησιακό και το στρατηγικό. Το επιχειρησιακό επίπεδο περιλαμβάνει την συλλογή και διαχείριση των πληροφοριών, τα high tech εγκλήματα, την online σεξουαλική κακοποίηση παιδιών και την διαδικτυακή απάτη. Το στρατηγικό επίπεδο

[146] Europol, Internet Organize Crime Threat Assessment, διαθέσιμο σε: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

[147] Europol, EC3 First Year Report, σελ. 6, διαθέσιμο σε: https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf

περιλαμβάνει την έρευνα και υποστήριξη, τον καθορισμό της στρατηγικής και την ανάπτυξη και τέλος, την εγκληματολογική ανάλυση, στο πλαίσιο της οποίας λειτουργούν ειδικά εργαστήρια.

Παρόλο που το Κέντρο οργανωτικά ανήκει πλήρως στην Europol έχει συσταθεί, ενόψει του σύνθετο περιβάλλοντος που λειτουργεί και των πολλαπλών προκλήσεων, Συμβούλιο Προγράμματος (Programme Board). Σε αυτό το συμβούλιο εκπροσωπούνται οι βασικοί παράγοντες στον τομέα του εγκλήματος και της ασφάλειας στον κυβερνοχώρο. Συγκεκριμένα, συμμετέχει η Ευρωπαϊκή Επιτροπή, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, το Ευρωπαϊκό Συμβούλιο, καθώς και οι Eurojust, ENISA, CERT-EU, CEPOL, Interpol, EUCTF, ECTEG[148]. Το Συμβούλιο παρέχει στο Κέντρο οδηγίες για το πώς να επιτύχει τους στόχους του και να εκπληρώσει τα επίσημα καθήκοντά του, βασιζόμενο σε συνεργασίες, κοινή ευθύνη και την σύμπραξη όλων των μελών του Συμβουλίου.

Παράλληλα, καθώς το Κέντρο αποδίδει μεγάλη βαρύτητα στην συνεργασία με τον ιδιωτικό τομέα, δημιουργήθηκαν δύο ειδικές Συμβουλευτικές Ομάδες προς αρωγή του Συμβουλίου. Η μία ομάδα αφορά την Ασφάλεια στο Διαδίκτυο και η άλλη ομάδα τις χρηματοοικονομικές Υπηρεσίες. Αργότερα, δημιουργήθηκε και μία τρίτη Συμβουλευτική Ομάδα για τους Παρόχους των Επικοινωνιών[149].

Η Συμβουλευτική Ομάδα για την Ασφάλεια στο Διαδίκτυο έχει ως στόχο την επιμόρφωση των ειδικών του Κέντρου για την ασφάλεια στο διαδίκτυο, την αναβάθμιση και τον διαμοιρασμό των πληροφοριών για το κυβερνοέγκλημα, την παροχή βοήθειας στο Κέντρο σχετικά με τον καθορισμό των προτεραιοτήτων του και την ανάπτυξη κοινών δράσεων με τα μέρη που συνεργάζονται με το Κέντρο και τέλος την παροχή βοήθειας για την διατήρηση της ισορροπίας μεταξύ της πρόληψης και καταπολέμησης του κυβερνοεγκλήματος από την μία πλευρά και την έρευνα και την δίωξη από την άλλη.

[148] Europol, EC3 Programme Board, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board

[149] Europol, EC3 Partners, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners

Η Συμβουλευτική Ομάδα για Χρηματοοικονομικές Υπηρεσίες έχει τους εξής στόχους: Πρώτον, να φέρει γνώση και τεχνογνωσία στο Κέντρο σχετικά με τον αντίκτυπο του εγκλήματος στον κυβερνοχώρο στις χρηματοπιστωτικές υπηρεσίες και για το πώς αυτοί οι τομείς μπορούν να βοηθήσουν στην πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Δεύτερον, να αναβαθμίσει και να διαμοιράσει όλες τις πληροφορίες που συγκεντρώνουν τα μέλη για τα αποτελέσματα του κυβερνοεγκλήματος στις οικονομικές υπηρεσίες. Τρίτον, να βοηθήσει το Κέντρο στον καθορισμό προτεραιοτήτων για το έργο του σε αυτόν τον τομέα, συμπεριλαμβανομένης της παροχής συμβουλών για τη συνεργασία με τις χρηματοπιστωτικές υπηρεσίες και για την ανάπτυξη ιδεών για ενισχυμένη πρόληψη. Τέταρτον, να συμβουλέψει το Κέντρο σχετικά με τους τρόπους αύξησης της ανταλλαγής πληροφοριών μεταξύ των αρχών επιβολής του νόμου και χρηματοοικονομικών υπηρεσιών.

Η Συμβουλευτική Ομάδα για τους Τηλεπικοινωνιακούς Παρόχους έχει με την σειρά της τέσσερεις στόχους: Πρώτον, να προσφέρει γνώση και τεχνογνωσία στο Κέντρο σχετικά με τον αντίκτυπο κυβερνοεγκλήματος στις τηλεπικοινωνίες και για το πώς αυτός ο τομέας μπορεί να βοηθήσει στην πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Δεύτερον, να αναβαθμίσει και να διαμοιράσει όλες τις πληροφορίες που συγκεντρώνουν τα μέλη για τα αποτελέσματα του κυβερνοεγκλήματος στις τηλεπικοινωνίες. Τρίτον, να βοηθήσει το Κέντρο στον καθορισμό προτεραιοτήτων για το έργο του σε αυτόν τον τομέα, συμπεριλαμβανομένης της παροχής συμβουλών για τη συνεργασία με τις υπηρεσίες τηλεπικοινωνίας και για την ανάπτυξη ιδεών για ενισχυμένη πρόληψη. Τέταρτον, να συμβουλέψει το Κέντρο σχετικά με τους τρόπους αύξησης της ανταλλαγής πληροφοριών μεταξύ των αρχών επιβολής του νόμου και τηλεπικοινωνιακών υπηρεσιών.

Στο πλαίσιο του Κέντρου, το 2010 η Europol μαζί με την Επιτροπή και τα κράτη μέλη ίδρυσαν την European Union CYBERCRIME TASK FORCE (EUCTF). Μέλη της EUCTF είναι οι επικεφαλής των εθνικών αρχών επιβολής του νόμου, αναφορικά με το κυβερνοέγκλημα και οι εκπρόσωποι της Επιτροπής και της Eurojust. Αποστολή της είναι να αναπτύξει και να προωθήσει μια κοινή προσέγγιση εντός της Ευρωπαϊκής

Ένωσης για την εγκληματική κατάχρηση της τεχνολογίας των πληροφοριών και επικοινωνιών, καθώς και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Αρκετές φορές η EUCTF ως ομάδα εμπειρογνωμόνων έχει εμπλακεί στον καθορισμό της πολιτικής γραμμής σε επίπεδο Ένωσης (π.χ. οδηγία NIS), αξιοποιώντας τις καλές διασυνδέσεις και την κατάσταση των μελών της για να προσεγγίσει εσωτερικά τους πολιτικούς και τους νομοθέτες[150].

Αρμοδιότητες της EUCTF είναι: α) ο εντοπισμός και η πρόληψη του κυβερνοεγκλήματος, β) η προώθηση αποτελεσματικής διαδικτυακής διακυβέρνησης, γ) η καταστροφή των εγκληματικών υποδομών, δ) η πρόληψη και η καταπολέμηση της παράνομης διαδικτυακής παραοικονομίας, ε) η βελτίωση του διαμοιρασμού των πληροφοριών και η επιχειρησιακή συνεργασία, στ) η συνεργασία με τον κλάδο της ασφάλειας των πληροφοριών, ζ) η ανάπτυξη εκπαιδεύσεων, η) η παροχή συμβουλών στους θεσμούς της Ένωσης, θ) η συνεργασία με την Europol, ι) η συνεργασία με την Eurojust, κ) η προώθηση διεθνών καλών πρακτικών διερεύνησης, κα) η υποστήριξη αποτελεσματικής νομοθεσίας για την αντιμετώπιση του κυβερνοεγκλήματος.

Η EUCTF διοικείται από ένα ξεχωριστό Συμβούλιο που αποτελείται από έναν πρόεδρο, έναν αντιπρόεδρο και ένας μέλος που εκλέγονται από τα κράτη μέλη για περίοδο δύο ετών. Επιπλέον, στο Συμβούλιο αντιπροσωπεύονται επίσης από έναν εκπρόσωπο η Ευρωπαϊκή Επιτροπή και από έναν το Ευρωπαϊκό Κέντρο για το Έγκλημα στον Κυβερνοχώρο. Παράλληλα, λειτουργεί μόνιμη Γραμματεία για την υποστήριξη του έργου του.

[150] Europol, EUCTF, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf

7. ΔΡΑΣΕΙΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

7.1. ΑΞΟΝΕΣ ΓΙΑ ΤΗΝ ΟΙΚΟΔΟΜΗΣΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Στις 13 Σεπτεμβρίου 2017 με πρωτοβουλία της Ύπατη Εκπροσώπου για θέματα Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας η Επιτροπή εκδίδει Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, αναφορικά με την οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο στηριζόμενη σε τρεις βασικούς άξονες: ανθεκτικότητα, αποτροπή και διεθνή συνεργασία[151]. Στους ανωτέρω άξονες κινείται και η πιο πρόσφατη Ανακοίνωση της Επιτροπής που εκδόθηκε στις 25/07/2020 σχετικά με την στρατηγική της Ευρωπαϊκής Ένωσης για την Ένωση Ασφαλείας[152], προσαρμοζόμενη στις νεότερες εξελίξεις αναφορικά με το κυβερνοέγκλημα.

Η Επιτροπή, αντιλαμβανόμενη την σημασία των ψηφιακών τεχνολογιών για την οικονομική ευημερία των πολιτών της Ένωσης αλλά και για την λειτουργία της ίδιας της δημοκρατίας, της ελευθερίας και των αξιών της Ένωσης, συσχετίζει την ικανότητα προς απόκρουση των επιθέσεων στον κυβερνοχώρο με την μελλοντική ασφάλεια στην Ένωση. Συγκεκριμένα, η Επιτροπή τονίζει ότι τόσο οι μη στρατιωτικές υποδομές όσο και η στρατιωτική ικανότητα βασίζονται σε ασφαλή ψηφιακά συστήματα[153]. Άλλωστε, το ανωτέρω συμπέρασμα αναγνωρίζεται τόσο από Ευρωπαϊκό Συμβούλιο[154] που έλαβε χώρα τον Ιούνιο του 2017 όσο και από την στρατηγική της Ένωσης για την Εξωτερική Πολιτική και την Πολιτική Ασφαλείας[155]. Πλέον, ο κυβερνοχώρος λογίζεται ως ένα πεδίο πολεμικών επιχειρήσεων αντικαθιστώντας σταδιακά τις παραδοσιακές στρατιωτικές επιχειρήσεις για την επίτευξη γεωπολιτικών στόχων. Για παράδειγμα, έχουν εντοπιστεί φαινόμενα

[151] JOIN (2017) 450 final

[152] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας

[153] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, JOIN(2017) 450 final, σελ. 2

[154] Ευρωπαϊκό Συμβούλιο, Συμπεράσματα του Ευρωπαϊκού Συμβουλίου, EUCO 8/17, διαθέσιμο σε: http://www.consilium.europa.eu/el/press/press-releases/2017/06/23-euco-conclusions/

[155] European Union External Action Service, EU Global Strategy, διαθέσιμο σε: http://europa.eu/globalstrategy/

παρέμβασης σε εσωτερικές εκλογικές διαδικασίες καθώς και διενέργειας εκστρατειών διασποράς ψευδών ειδήσεων και παραπληροφόρησης. Για τον λόγο αυτόν, η Επιτροπή εξέφρασε με έγγραφο τον προβληματισμό της τονίζοντας τη σημασία της συνεργασίας στον τομέα της άμυνας στον κυβερνοχώρο[156].

Όπως αναφέρθηκε παραπάνω, η οικοδόμηση της κυβερνοασφάλειας στηρίζεται σε τρεις άξονες: την ανθεκτικότητα, την αποτροπή και την άμυνα. Οι άξονες αυτοί απαρτίζονται από επιμέρους δράσεις, όπως αναλύεται παρακάτω.

7.1.1. ΑΝΘΕΚΤΙΚΟΤΗΤΑ

Η οικοδόμηση της κυβερνοανθεκτικότητας αποτελεί έργο διαφόρων παραγόντων. Έτσι, απαιτείται η συμβολή όχι μόνο των κρατών μελών αλλά και των θεσμικών και λοιπών οργάνων και Οργανισμών της Ένωσης καθώς και η συμμετοχή πολλαπλών επιπέδων της διακυβέρνησης, της οικονομίας και της κοινωνίας. Πρόκειται για μία κοινή πρόκληση της κοινωνίας, η οποία σκοπείται να αντιμετωπιστεί με επιμέρους δράσεις:

7.1.1.1. ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΩΝ ΥΠΟΔΟΜΩΝ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ

Υπάρχουν ορισμένες υποδομές που είναι απαραίτητες για την καθημερινή κοινωνική και οικονομική ζωή των πολιτών, όπως η ηλεκτρική ενέργεια, τα νοσοκομεία και τα χρηματοπιστωτικά ιδρύματα. Ως εκ τούτου, η δημόσια διοίκηση οφείλει να λαμβάνει μέριμνα ώστε να εξασφαλίζει την απρόσκοπτη πρόσβαση των πολιτών σε αυτές τις υποδομές ενώ οι πολίτες έχουν δικαίωμα να προσδοκούν την πρόσβαση στις ανωτέρω παροχές απολαμβάνοντας τα οφέλη που τους παρέχουν. Εάν αυτό δεν συμβαίνει καθίσταται εξαιρετικά πιθανό να δημιουργηθεί μεγάλη αναστάτωση στο πραγματικό ή ψηφιακό κόσμο τόσο σε επίπεδο κράτους όσο και σε επίπεδο Ένωσης[157]. Έτσι, καθίσταται αναγκαία μια προσαρμογή του υπάρχοντος νομικού πλαισίου,[158] ώστε

[156] Ευρωπαϊκή Επιτροπή, Διάσκεψη για το μέλλον της Ευρώπης, διαθέσιμο σε: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_el.pdf

[157] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 8

[158] Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, Οδηγία 2008/114/ΕΚ σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους

να είναι σε θέση να αντιμετωπίσει αποτελεσματικά τους συνεχώς εξελισσόμενους κινδύνους.

Σύμφωνα με την Ένωση, οι ενεργειακές τεχνολογίες που ενσωματώνουν ψηφιακές συνιστώσες και η ασφάλεια των σχετικών αλυσίδων εφοδιασμού είναι σημαντικές για να εξασφαλίσουν τη συνέχεια των βασικών υπηρεσιών και τον στρατηγικό έλεγχο των ενεργειακών υποδομών ζωτικής σημασίας[159]. Παράλληλα, όπως ειπώθηκε ανωτέρω, οι κυβερνοεπιθέσεις δύνανται να επηρεάσουν σημαντικά τις δημοκρατικές διαδικασίες των κρατών και κατά συνέπεια να κλονίσουν τους δημοκρατικούς τους θεσμούς. Για τον λόγο αυτό η κυβερνοανθεκτικότητα αποτελεί σημαντικό παράγοντα και στα πλαίσια του ευρωπαϊκού σχεδίου δράσης για τη δημοκρατία, για τη διασφάλιση και την προώθηση ελεύθερων εκλογών, του δημοκρατικού λόγου και της πολυφωνίας των μέσων ενημέρωσης[160].

Παράλληλα, αυτό που κατέδειξαν οι τρομοκρατικές επιθέσεις των τελευταίων ετών ήταν ότι η Ένωση πρέπει να λάβει μέτρα προστασίας και για δημόσιους χώρους στην επικράτεια της. Μάλιστα, η Επιτροπή επεξεργάζεται για τον σκοπό αυτό την δημιουργία συστημάτων ανίχνευσης, πάντα με σεβασμό των θεμελιωδών ελευθεριών των πολιτών της[161].

7.1.1.2. ΕΝΙΣΧΥΣΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ (ENISA)

Όπως αναλυτικά εκτέθηκε παραπάνω ο Οργανισμός κατέχει πλέον έναν ενισχυμένο ρόλο στην προσπάθεια της Ένωσης για την ασφάλεια στον κυβερνοχώρο. Πλέον, ο Οργανισμός έχει την ικανότητα να παράσχει στήριξη στα κράτη μέλη, τις επιχειρήσεις καθώς και στα όργανα και τους οργανισμούς της Ένωσης ιδίως σχετικά με την εφαρμογή της Οδηγίας για την ασφάλεια συστημάτων δικτύων και πληροφοριών[162] και την πιστοποίηση για την ασφάλεια στον κυβερνοχώρο.

[159] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 7

[160] Ευρωπαϊκή Επιτροπή, Ανακοίνωση σχετικά με το ευρωπαϊκό σχέδιο δράσης για τη δημοκρατία, COM(2020) 790

[161] Ευρωπαϊκή Επιτροπή, COM (2020) 65, Λευκή Βίβλος Επιτροπής για Τεχνική Νοημοσύνη, 19/02/2020

[162] Οδηγία (ΕΕ) 2016/1148, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

Επιπλέον, ενισχύεται ο συμβουλευτικός ρόλος του ENISA για την ανάπτυξη και την εφαρμογή σχετικών πολιτικών, την ανάληψη πρωτοβουλιών, την ανάλυση πληροφοριών και την δημιουργία κέντρων κοινοχρησίας. Αναλυτικότερα για τον Οργανισμό και τις δράσεις του αναλύθηκαν ανωτέρω.

7.1.1.3. ΕΝΙΑΙΑ ΑΓΟΡΑ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η Επιτροπή αναγνωρίζει ως πρόσκομμα για την ανάπτυξη ενιαίας αγοράς στον τομέα της ασφάλειας στον κυβερνοχώρο την έλλειψη κοινών προτύπων και πιστοποιήσεων ασφάλειας, τα οποία θα απολαμβάνουν αναγνωρισημότητας σε ολόκληρη την ευρωπαϊκή επικράτεια[163]. Ως εκ τούτου, κρίθηκε αναγκαία η ενιαία ρύθμιση των διαδικασιών για την δημιουργία κοινών συστημάτων πιστοποίησης ασφαλείας σε προϊόντα, υπηρεσίες ή και συστήματα, είτε αυτά αφορούν υποδομές ζωτικής σημασίας είτε καταναλωτικά αγαθά. Κατά αυτόν τον τρόπο, οι επιχειρήσεις πρόκειται να αποκομίσουν σημαντικά οφέλη διότι δεν θα χρειάζεται να υποβάλλονται σε διάφορες διαδικασίες πιστοποίησης για την εκτέλεση εμπορικών συναλλαγών σε διασυνοριακό επίπεδο, περιορίζοντας με τον τρόπο αυτό το διοικητικό και οικονομικό κόστος.

Η επιβαλλόμενη ρύθμιση πραγματοποιήθηκε με τον Κανονισμό EU Cybersecurity Agency για την αναδιάρθρωση του Οργανισμού ENISA. Με την θέσπιση του Κανονισμού η Επιτροπή καλεί τους ενδιαφερόμενους να δώσουν έμφαση κυρίως σε τρεις προτεραιότητες:

Α) Ασφάλεια σε εφαρμογές κρίσιμης σημασίας ή υψηλού κινδύνου. Πρόκειται για συστήματα από τα οποία εξαρτώνται οι καθημερινές δραστηριότητες των πολιτών, όπως συστήματα αυτοκινήτων, αεροπλάνων, ηλεκτροπαραγωγής ή ιατροτεχνολογικών προϊόντων. Γίνεται αντιληπτό πλέον ότι οι καθημερινές δραστηριότητες καθίστανται όλο και περισσότερο ψηφιακές και διασυνδεδεμένες,

[163] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ. 5 - 6

οπότε αποτελεί ζήτημα μείζονος σημασίας να απολαμβάνουν το υψηλότερο επίπεδο ασφαλείας, με αυξημένες προδιαγραφές.

Β) Ασφάλεια σε ευρέως διαδεδομένα ψηφιακά προϊόντα, δίκτυα και υπηρεσίες. Πρόκειται για προϊόντα, δίκτυα και υπηρεσίες που χρησιμοποιούνται τόσο από δημόσιους όσο και από ιδιωτικούς φορείς για την προστασία από επιθέσεις κατά των συστημάτων, όπως η κρυπτογράφηση μηνυμάτων ή τα τείχη προστασίας. Ως εκ τούτου είναι απαραίτητο να διασφαλιστεί ότι η διαδεδομένη χρήση των ανωτέρω δεν θα αποτελέσει πηγή νέων κινδύνων για την ασφάλεια.

Γ) Χρήση μεθόδων «ασφάλειας εκ σχεδιασμού». Η Επιτροπή κρίνει σημαντικό τα προϊόντα χαμηλού κόστους σε ψηφιακές και διασυνδεδεμένες συσκευές στο πλαίσιο του διαδικτύου των πραγμάτων (Internet of Things) να πληρούν εκ κατασκευής τα απαραίτητα πρότυπα ασφαλείας καθώς και να υποβάλλονται σε αυστηρούς ελέγχους ασφαλείας με την δυνατότητα των πωλητών να επεμβαίνουν εκ των υστέρων στο λογισμικό σε περίπτωση απειλών ή τρωτών σημείων στην ασφάλεια.

Κατά την εφαρμογή των ανωτέρω προτεραιοτήτων συνίσταται να λαμβάνεται ειδική μέριμνα για το συνεχώς εξελισσόμενο τοπίο, αναφορικά με τις απειλές για την ασφάλεια στον κυβερνοχώρο, καθώς και για τον σημαντικό ρόλο που διαδραματίζουν βασικές υπηρεσίες που αναφέρονται σε τομείς που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας 1148/2016, όπως οι μεταφορές, η ιατροφαρμακευτική περίθαλψη, οι τράπεζες, η ενέργεια, το πόσιμο νερό, οι υποδομές των χρηματοπιστωτικών αγορών ή ψηφιακών υποδομών.

Την ίδια στιγμή, μια προσέγγιση «ασφάλειας εκ σχεδιασμού» από τους παραγωγούς θα μπορούσε να βοηθήσει στην αύξηση του επιπέδου ασφαλείας στον κυβερνοχώρο καθώς μια τέτοια προσέγγιση θα συνέβαλε δυνητικά, στηριζόμενη στην αρχή ενός καθήκοντος επιμέλειας[164], στην ανάπτυξη της συνεργασίας με την βιομηχανία, προκειμένου να μειωθούν τα τρωτά σημεία προϊόντων και λογισμικών, στην μακροχρόνια συντήρηση και χρήση ασφαλών διαδικασιών κύκλου ζωής και στην ανάπτυξη επικαιροποιήσεων και διορθώσεων σφαλμάτων για την αντιμετώπιση

[164] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ. 7

κενών ασφαλείας που ανακαλύπτονται. Στο πλαίσιο αυτό, η Επιτροπή θεωρεί σημαντικό τον ρόλο που διαδραματίζουν οι αποκαλούμενοι ερευνητές ασφαλείας τρίτων χωρών για την ανεύρεση τρωτών σημείων. Παράλληλα, η Επιτροπή θεωρεί εξίσου σημαντικό να αξιοποιηθούν οι βέλτιστες πρακτικές[165] και πρότυπα,[166] ώστε να καταστεί ευχερέστερη η δημοσιοποίηση των ανακυπτόντων τρωτών σημείων σε όλα τα κράτη μέλη. Με τον τρόπο αυτό, σκοπείται η αύξηση της εμπιστοσύνης των πολιτών – καταναλωτών στα ψηφιακά προϊόντα.

Τέλος, η ασφάλεια στον κυβερνοχώρο διαδραματίζει βαρύνοντα ρόλο στον καθορισμό της πολιτικής για το εμπόριο και τις επενδύσεις και ως εκ τούτου για την ολοκλήρωση της εσωτερικής αγοράς. Ωστόσο, ιδιαίτερα σημαντική καθίσταται η ασφάλεια στον κυβερνοχώρο και ενόψει του πλαισίου[167] για τον έλεγχο των ξένων άμεσων επενδύσεων στην Ένωση, καθώς τρίτες χώρες εξαγοράζουν κρίσιμες τεχνολογίες ασφαλείας που αποτελούν σημαντικό παράγοντα στην διασφάλιση της ασφάλειας και δημόσιας τάξης της Ένωσης. Την ίδια στιγμή, παρατηρούνταν μεγάλες δυσχέρειες στην εξαγωγή τεχνολογικών προϊόντων σε τρίτες χώρες εξαιτίας της έλλειψης των απαιτούμενων προϋποθέσεων ασφαλείας. Ως εκ τούτου, η εισαγωγή του πλαισίου για τις πιστοποιήσεις ασφάλειας στον κυβερνοχώρο ενισχύει την διεθνή ανταγωνιστική θέση της Ένωσης στην παγκόσμια αγορά.

7.1.1.4. ΠΛΗΡΗΣ ΕΦΑΡΜΟΓΗ ΤΗΣ ΟΔΗΓΙΑΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ

Η Οδηγία ΑΔΠ[168] που περιλαμβάνει μέτρα για κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών για όλη την Ένωση αποτελεί ουσιαστικά την πρώτη νομοθετική πράξη της Ένωσης για την ασφάλεια στον κυβερνοχώρο. Σκοπός της Οδηγίας είναι η δημιουργία ανθεκτικότητας που επιτυγχάνεται μέσω της βελτίωσης των ικανοτήτων σε θέματα ασφαλείας σε εθνικό επίπεδο και με την αυστηροποίηση του πλαισίου για τις επιχειρήσεις που δραστηριοποιούνται σε σημαντικούς τομείς της οικονομίας τόσο αναφορικά με την διαχείριση των κινδύνων

[165] ENISA, Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, 2016
[166] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure
[167] Ευρωπαϊκή Επιτροπή, COM (2017) 478
[168] Οδηγία (ΕΕ) 2016/1148

όσο και με την κοινοποίηση προβλημάτων ασφαλείας στις εθνικές Αρχές. Σημαντική παραμένει και η καλύτερη δυνατή συνεργασία των κρατών μελών για την επίτευξη του ανωτέρω σκοπού.

Ωστόσο, η Οδηγία δεν καλύπτει όλο το εύρος των ζητημάτων που ανακύπτουν και ως εκ τούτου η Ένωση πρέπει να εξετάσει το ενδεχόμενο συμπλήρωσης της. Ειδικότερα, η Οδηγία αναφέρεται μόνο σε βασικούς στρατηγικούς τομείς με αποτέλεσμα να θεωρείται λογικά ως επόμενο βήμα η επέκταση της Οδηγίας σε άπαντες τους ενδιαφερομένους. Επιπλέον, παρατηρείται επιφυλακτικότητα των επιχειρήσεων να επικοινωνήσουν με τις εθνικές Αρχές για την ανταλλαγή πληροφοριών σχετικά με τα τρωτά σημεία φοβούμενες την απώλεια της εμπιστευτικότητας επιχειρηματικών δεδομένων ευαίσθητου χαρακτήρα, την υποβάθμιση της φήμης τους καθώς και την παραβίαση του νόμου περί προστασίας δεδομένων προσωπικού χαρακτήρα[169]. Ως εκ τούτου, είναι επιτακτική η ανάγκη αναθεώρησης της Οδηγίας ώστε να ανταποκρίνεται στις εξελίξεις και να καλύψει τα ανωτέρω κενά[170].

7.1.1.5. ΤΑΧΕΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΤΑΣΤΑΣΕΩΝ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ

Η ταχύτητα με την οποία αντιμετωπίζονται οι διάφορες επιθέσεις στον κυβερνοχώρο αποτελεί κρίσιμο παράγοντα για δύο, κυρίως λόγους: Αρχικά, με αυτόν τον τρόπο περιορίζονται οι επιπτώσεις της επίθεσης και καθίσταται ευχερέστερη η αποκατάσταση των προκληθεισών ζημιών. Κατά δεύτερον, αποφεύγεται ο κλονισμός της εμπιστοσύνης των πολιτών και των επιχειρήσεων στην ικανότητα των δημόσιων αρχών να αντιμετωπίζουν τις κυβερνοεπιθέσεις. Άλλωστε, η αντιμετώπιση ενός ιδιαιτέρως σοβαρού περιστατικού ή σοβαρής επίθεσης στον κυβερνοχώρο αποτελεί επαρκή λόγο για την προσφυγή ενός κράτους στην ρήτρα αλληλεγγύης της Ένωσης[171].

Η ταχεία και αποτελεσματική αντιμετώπιση βασίζεται επίσης στην ύπαρξη μηχανισμού άμεσης ανταλλαγής πληροφοριών μεταξύ όλων των βασικών

[169] Cybersecurity in the European Digital Single Market, Ομάδα επιστημονικών συμβούλων υψηλού επιπέδου, Μάρτιος 2017
[170] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 13
[171] Άρθρο 222 ΣΛΕΕ

παραγόντων σε εθνικό και ενωσιακό επίπεδο, ο οποίος προϋποθέτει με τη σειρά του σαφήνεια ως προς τους αντίστοιχους ρόλους και τις σχετικές αρμοδιότητες. Για τον σκοπό αυτόν, η Επιτροπή έχει προβεί σε διαβούλευση με τα θεσμικά όργανα και τα κράτη μέλη σχετικά με την κατάρτιση προσχεδίου για την εισαγωγή μιας αποτελεσματικής διαδικασίας στο πλαίσιο της επιχειρησιακής αντιμετώπισης περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο, τόσο σε ενωσιακό επίπεδο όσο και σε επίπεδο κρατών μελών[172]. Στο εν λόγω προσχέδιο προβλέπεται δέσμη μέτρων που αναφέρονται στους υπάρχοντες μηχανισμούς αντιμετώπισης κρίσεων αλλά και μέτρα σχετικά με την αποτελεσματικότερη συνεργασία σε επίπεδο κρατών και Ένωσης.

7.1.1.6. ΔΗΜΙΟΥΡΓΙΑ ΕΥΡΩΠΑΪΚΟΥ ΚΕΝΤΡΟΥ ΕΡΕΥΝΑΣ ΚΑΙ ΙΚΑΝΟΤΗΤΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Το Κέντρο σχεδιάζεται να έχει συμπληρωματικό ρόλο με τον ENISA στον τομέα της κυβερνοανθεκτικότητας και με τον Ευρωπαϊκό Οργανισμό Άμυνας στον τομέα της κυβερνοάμυνας, συνεργαζόμενο ταυτόχρονα με τους δύο ανωτέρω Οργανισμούς. Μάλιστα, σε συνεργασία με την Ύπατη Εκπρόσωπο για θέματα ΚΕΠΠΑ, τον Ευρωπαϊκό Οργανισμό Άμυνας και την Επιτροπή, παρέχεται η δυνατότητα να εξεταστεί το ενδεχόμενο δράσης του Κέντρου για την κυβερνοασφάλεια να χρηματοδοτηθούν από το Ευρωπαϊκό Ταμείο Άμυνας.

Άλλωστε είναι στρατηγικό συμφέρον της Ένωσης η ανάπτυξη των αναγκαίων ικανοτήτων για την διασφάλιση της ψηφιακής οικονομίας, κοινωνίας και της δημοκρατίας καθώς και για την προστασία κρίσιμού λογισμικού για ζωτικές δραστηριότητες της Ένωσης και των κρατών μελών[173]. Για τους λόγους αυτούς, η Επιτροπή προτείνει την δρομολόγηση της διασύνδεσης των επιμέρους εθνικών κέντρων σε ένα μόνο δίκτυο, σε πιλοτικό στάδιο, στο πλαίσιο του προγράμματος Ορίζοντας 2020.

---

[172] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ 10

[173] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ 11

7.1.1.7. ΠΡΟΩΘΗΣΗ ΤΗΣ ΥΓΙΕΙΝΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΤΗΣ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗΣ

Ο Ανθρώπινος παράγοντας διαδραματίζει βαρύνοντα ρόλο σε ζητήματα ασφάλειας στον κυβερνοχώρο[174]. Κατά συνέπεια, κρίνεται απαραίτητο ότι πρέπει να προσαρμοστεί η συμπεριφορά των προσώπων, των επιχειρήσεων και της δημόσιας διοίκησης, ώστε να εξοπλίζονται με εργαλεία και δεξιότητες που θα τους επιτρέψουν να προστατευτούν σε περίπτωση επιθέσεων. Πρέπει δηλαδή να αναπτύξουν συνήθειες κυβερνοϋγιεινής.

Στην Οδηγία ΑΔΠ προβλέπονται οι τρεις κύριες αρμοδιότητες των κρατών μελών αναφορικά με την ανταλλαγή πληροφοριών: Πρώτον, τα κράτη μέλη πρέπει να παρέχουν τα περισσότερα δυνατά εργαλεία σε ιδιώτες και επιχειρήσεις για την ασφάλεια στον κυβερνοχώρο, με στόχο την πρόληψη[175] και τον μετριασμό των επιπτώσεων από τις επιθέσεις στους τελικούς χρήστες. Δεύτερον, τα κράτη μέλη θα πρέπει να μεριμνήσουν για την ταχύτερη χρήση περισσότερων εργαλείων ασφάλειας στον κυβερνοχώρο κατά την ανάπτυξη της ηλεκτρονικής διακυβέρνησης και να αξιοποιήσουν επιπλέον πλήρως τα οφέλη του δικτύου ικανοτήτων. Τρίτον, τα κράτη μέλη πρέπει να προβούν σε εκστρατείες ευαισθητοποίησης των πολιτών με εκστρατείες απευθυνόμενες σε σχολεία, πανεπιστήμια αλλά και στην επιχειρηματική κοινότητα και σε ερευνητικούς Οργανισμούς.

7.1.2. ΑΠΟΤΡΟΠΗ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Η αποτελεσματική αποτροπή των κυβερνοεπιθέσεων συνιστά ζήτημα κεφαλαιώδους σημασίας για την Ένωση. Ως εκ τούτου, καθίσταται απαραίτητη μια δέσμη μέτρων αποτρεπτικού χαρακτήρα τα οποία θα είναι ταυτόχρονα αποτελεσματικά. Με αυτόν τον τρόπο, οι εγκληματίες θα γνωρίζουν εκ των προτέρων ότι δεν θα έχουν να φοβηθούν μόνο την αποτυχία της επίθεσης τους αλλά και την σύλληψη και τιμωρία τους. Για την επίτευξη του ανωτέρω σκοπού, σημαντική είναι η

[174] IBM, The Cybersecurity Intelligence Index, 2014, αναφορά στο Securitymagazine.com, όπου αναφέρεται ότι περίπου το 95% των κυβερνοεπιθέσεων διευκολύνθηκε από κάποιο, εσκεμμένα ή μη, ανθρώπινο σφάλμα

[175] Βλ. για παράδειγμα την εκστρατεία NoMoreRansom της Interpol

ιχνηλάτηση και η δίωξη των εγκλημάτων του κυβερνοχώρου με ταυτόχρονη ανάπτυξη στρατιωτικών ικανοτήτων στον τομέα της κυβερνοασφάλειας[176].

Όπως αναλύθηκε ανωτέρω, ένα σημαντικό βήμα στον τομέα του ποινικού δικαίου αποτέλεσε η Οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών. Η Επιτροπή ενθαρρύνει τα κράτη μέλη για την εφαρμογή της κρίνοντας ότι δεν χρήζει τροποποίησης. Αντιθέτως, συνίσταται να γίνει χρήση όλων των δυνατοτήτων που παρέχουν οι διατάξεις της Οδηγίας[177].

Για την καθιέρωση αποτελεσματικής αποτρεπτικής ικανότητας της Ένωσης η Επιτροπή προτείνει μια σειρά δράσεων:

7.1.2.1. ΕΝΤΟΠΙΣΜΟΣ ΔΡΑΣΤΩΝ ΚΑΚΟΒΟΥΛΩΝ ΕΝΕΡΓΕΙΩΝ

Βασικός παράγοντας για τον εντοπισμό των δραστών αποτελεί η αποτελεσματική δράση της Europol με τη αρωγή των εμπειρογνωμόνων που διαθέτει. Ωστόσο, το έργο του Οργανισμού δυσχεραίνεται σημαντικά από την πρακτική των εγκληματιών να τοποθετούν χιλιάδες χρήστες στην ίδια διεύθυνση ip με αποτέλεσμα να δαπανάται χρόνος και ανθρώπινο κεφάλαιο χωρίς να καθίσταται δυνατός τελικά ο εντοπισμός των δραστών. Για τον λόγο αυτόν η Ένωση προτρέπει τα κράτη μέλη να ακολουθήσουν το παράδειγμα του Βελγίου και να υιοθετήσουν πρωτόκολλο[178] για μόνο έναν χρήστη ανά διεύθυνση ή διαφορετικά μικρό αριθμό χρηστών ανά διεύθυνση.

7.1.2.2. ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΣΕ ΕΠΙΠΕΔΟ ΕΠΙΒΟΛΗΣ ΤΟΥ ΝΟΜΟΥ

Η Επιτροπή αναγνωρίζει ότι η διερεύνηση και η δίωξη του κυβερνοεγκλήματος στην σύγχρονη εποχή επιβάλλει την διασυνοριακή συνεργασία για τον εντοπισμό των ιχνών και κατά συνέπεια των δραστών με αποτέλεσμα να παρίσταται ανάγκη για άμεση λήψη μέτρων δικονομικού χαρακτήρα και άμεσης διασυνοριακής συνεργασίας. Παράλληλα με τις δικονομικές απαιτείται η σύγκληση

[176] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ 17

[177] Ευρωπαϊκή Επιτροπή, COM (2017) 474

[178] IPv6, Internet Protocol Version 6 που αντικαθιστά το IPv4 και αποτελεί το πρωτόκολλο επικοινωνίας πάνω στο οποίο έχει χτιστεί το διαδίκτυο

μεταξύ των κρατών και στις εγκληματολογικές διαδικασίες που ακολουθούνται αναφορικά με την συλλογή και διερεύνηση των ιχνών. Έτσι, κρίνεται αναγκαία η εισαγωγή κοινών εγκληματολογικών προτύπων μεταξύ των κρατών[179]. Βέβαια, η Επιτροπή αναγνωρίζει ότι η Σύμβαση της Βουδαπέστης κινείται προς αυτό το σημείο και ενθαρρύνει τα κράτη μέλη να εστιάσουν τη νομική τους παραγωγή σε τρόπους που διασφαλίζουν την διασυνοριακή πρόσβαση σε ίχνη και όχι νέους τρόπους ποινικοποίησης των εγκλημάτων στον κυβερνοχώρο.

Η αποτελεσματική αντιμετώπιση συναντά συχνά ένα ισχυρό τοίχος στο επονομαζόμενο σκοτεινό δίκτυο[180] (darknet), όπου επιτυγχάνεται η ανωνυμοποιήση των δραστών και η χρήση του είναι ιδιαίτερα διαδεδομένη σε εγκλήματα σεξουαλικής εκμετάλλευσης παιδιών, διακίνησης ναρκωτικών και όπλων κ.α. Η Επιτροπή πρόκειται να επιχειρήσει τα επόμενα έτη να αποκτήσει ηγετικό ρόλο η Ένωση στον συντονισμό της διεθνούς δράσης για την καταπολέμηση των απειλών του σκοτεινού διαδικτύου. Ένα σημαντικό εργαλείο που πρόκειται να οδηγήσει σε αυτή την κατεύθυνση αποτελεί η αξιοποίηση της τεχνητής νοημοσύνης, καθώς παρέχει την δυνατότητα να αναλύονται μεγάλοι όγκοι πληροφοριών και να εξάγονται χρήσιμα συμπεράσματα, μοτίβα και ανωμαλίες σε μικρό χρονικό διάστημα. Για την αξιοποίηση αυτού του δυναμικού απαιτείται συγκέντρωση της έρευνας, της καινοτομίας και των χρηστών της τεχνητής νοημοσύνης με τη σωστή διακυβέρνηση και τεχνική υποδομή, και την ενεργό συμμετοχή του ιδιωτικού τομέα και των πανεπιστημίων[181]. Απαιτείται επίσης η τήρηση των θεσπισμένων προτύπων συμμόρφωσης με τα θεμελιώδη δικαιώματα των πολιτών[182], με ταυτόχρονη διασφάλιση της αποτελεσματικής προστασίας τους.

Ιδιαίτερα κρίσιμη καθίσταται η αξιοποίηση από την Ένωση της αρχιτεκτονικής του δικτύου 5G, με σεβασμό πάντοτε στην προστασία του απορρήτου των

[179] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ 19

[180] Το darknet είναι ένα δίκτυο επικάλυψης, που προσεγγίζεται μόνο με συγκεκριμένο λογισμικό, διαμορφώσεις, ή άδειες

[181] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 15

[182] Βλ. Γενικός Κανονισμός (ΕΕ) 2016/670 για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα και Οδηγία (ΕΕ) 2016/680 για την προστασία των δεδομένων από τις αρχές επιβολής του νόμου

επικοινωνιών. Έτσι, η Επιτροπή επιθυμεί την θέσπιση διεθνών προτύπων και βέλτιστων πρακτικών σε βασικούς τεχνολογικούς τομείς, ύστερα από συνεργασία της διεθνούς κοινότητας. Οι μελλοντικές προκλήσεις της τεχνολογίας είναι πολλές όπως για παράδειγμα η τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων και το blockchain.

Την ίδια στιγμή οι επαγγελματίες που εργάζονται στην επιβολή του νόμου πρέπει να βελτιώσουν τις ικανότητες τους και να προσαρμοστούν στις σύγχρονες εξελίξεις του κυβερνοεγκλήματος. Σε κάθε περίπτωση, πρέπει να διαθέτουν πρόσβαση σε νέα εργαλεία και να αναπτύσσουν εναλλακτικές τεχνικές έρευνας[183]. Πλέον, ο μεγαλύτερος αριθμός των εγκληματιών του κυβερνοχώρου χρησιμοποιεί τεχνολογίες κρυπτογράφησης. Την ίδια στιγμή η κρυπτογράφηση παρέχει πληθώρα ωφελειών στους χρήστες καθώς προστατεύει θεμελιώδη δικαίωμα τους όπως η ελευθερία της έκφρασης ενώ εξασφαλίζει παράλληλα ένα προστατευμένο περιβάλλον συναλλαγών στον ψηφιακό κόσμο. Αυτό έχει ως αποτέλεσμα να καθίσταται αναγκαία η λήψη νομικών μέτρων για την καταπολέμηση της χρήσης της κρυπτογράφησης για εγκληματικούς σκοπούς χωρίς να θίγεται ωστόσο η νόμιμη χρήση της κρυπτογράφησης και η απόλαυση των θετικών της στοιχείων.

Ωστόσο, τον σημαντικότερο ρόλο στην αντιμετώπιση του κυβερνοεγκλήματος διαδραματίζουν οι εθνικές αρχές επιβολής του νόμου καθώς και οι εισαγγελικές και δικαστικές αρχές των κρατών μελών, οι οποίες πρέπει να αναπτύξουν τις ικανότητες τους και να βελτιώσουν τους τρόπους έρευνας και δράσης τους. Οι Οργανισμοί Europol και Eurojust παρέχουν αρωγή στις εθνικές αρχές προωθώντας την συνεργασία μεταξύ των κρατών και της Ένωσης και παρέχοντας τους εξειδικευμένες οδηγίες και συμβουλές μέσω και του Κέντρου της Europol αλλά και εξειδικευμένων στα εγκλήματα στον κυβερνοχώρο εισαγγελέων.

[183] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 15

7.1.2.3. ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΠΑΡΑΝΟΜΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Εγκλήματα όπως η τρομοκρατία και η σεξουαλική κακοποίηση παιδιών καταλαμβάνουν όλο και περισσότερο χώρο στο διαδίκτυο, με αποτέλεσμα να απαιτείται συγκεκριμένη δράση για την καταπολέμηση του φαινομένου. Η χρήση του διαδικτύου για τους ανωτέρω σκοπούς εκτός από την βλάβη που επιφέρει στους πολίτες και γενικά την κοινωνία, μειώνει επιπλέον την εμπιστοσύνη των χρηστών στο διαδίκτυο και επηρεάζει τα επιχειρηματικά μοντέλα και την φήμη των θιγόμενων εταιρειών[184]. Στο πλαίσιο αυτό, είναι απαραίτητη η ανάπτυξη της συνεργασίας μεταξύ ιδιωτικού και δημόσιου τομέα στο Φόρουμ της Ευρωπαϊκής Ένωσης για το διαδίκτυο με παράλληλη υιοθέτηση της πρότασης της Επιτροπής για την διάδοση τρομοκρατικού περιεχομένου μέσω του διαδικτύου[185]. Σε διεθνές επίπεδο, απαιτείται η συνεργασία με διεθνείς παράγοντες και συμμετοχή της Ένωσης στο παγκόσμιο Φόρουμ για το διαδίκτυο και την καταπολέμηση της τρομοκρατίας. Παράλληλα, η Επιτροπή έχει αναπτύξει συγκεκριμένη στρατηγική[186] για την αντιμετώπιση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο με ταυτόχρονη υποχρέωση των εταιριών να βρίσκονται σε επαγρύπνηση και να αφαιρούν το σχετικό υλικό. Παρόμοια επαγρύπνηση των εταιρειών για την αυτόματη ανίχνευση και αφαίρεση περιεχομένου προβλέπεται και για την καταπολέμηση της υποκίνησης τρομοκρατικών πράξεων[187]. Μάλιστα, στην περίπτωση αυτή τα χρονοδιαγράμματα οφείλουν να είναι αυστηρά, με τις διάφορες πλατφόρμες να υποχρεούνται να εξηγούν με σαφήνεια στους χρήστες την πολιτική τους αναφορικά με το επιτρεπόμενο περιεχόμενο των αναρτήσεων τους[188].

Για την επίτευξη του ανωτέρω σκοπού, η Επιτροπή εκδίδει Σύσταση το 2018 που περιέχει μία δέσμη επιχειρησιακών μέτρων τα οποία οφείλουν να λάβουν οι επιχειρήσεις προκειμένου να εντείνουν την προσπάθεια αντιμετώπισης του

[184] Παπακωνσταντής Μάρκος, ο.π., σελ. 360
[185] Ευρωπαϊκή Επιτροπή, Πρόταση σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο, COM (2018) 640
[186] Ευρωπαϊκή Επιτροπή, Στρατηγική της ΕΕ για την αποτελεσματικότερη καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, COM(2020) 607
[187] Ευρωπαϊκό Συμβούλιο, Σύνοδος του Ευρωπαϊκού Συμβουλίου 22-23/06/2017, Συμπεράσματα, EUCO, 8/17
[188] Παπακωνσταντής Μάρκος, ο.π., σελ. 362

παράνομου περιεχομένου στο διαδίκτυο[189]. Η εν λόγω Σύσταση αφορά όλες τις μορφές που μπορεί να προσλάβει το παράνομο περιεχόμενο στο διαδίκτυο, από το τρομοκρατικό περιεχόμενο και την υποκίνηση του μίσους και της βίας έως και το υλικό σεξουαλικής κακοποίησης παιδιών.

7.1.2.4. ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΔΗΜΟΣΙΟΥ ΚΑΙ ΙΔΙΩΤΙΚΟΥ ΤΟΜΕΑ

Η συνεργασία των εθνικών αρχών με βιομηχανικούς παράγοντες, τον χρηματοπιστωτικό τομέα και την κοινωνία των πολιτών είναι θεμελιώδους σημασίας για την καταπολέμηση του κυβερνοεγκλήματος. Έτσι, πρέπει οι επιχειρήσεις να αναπτύξουν μια κουλτούρα συνεργασίας με τις δημόσιες αρχές σε περίπτωση κυβερνοεγκλημάτων διαβιβάζοντας και δεδομένα προσωπικού χαρακτήρα αν αυτό κρίνεται απαραίτητο, τηρώντας πάντοτε τις διατάξεις των νόμων για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Για τον σκοπό αυτό, συστήθηκε το Φόρουμ της Ευρωπαϊκής Ένωσης για το διαδίκτυο, με το οποίο πραγματοποιείται η πρόβλεψη που υπάρχει στο Ευρωπαϊκό Θεματολόγιο για την ασφάλεια. Συγκεκριμένα, προβλέπεται η συνεργασία των αρχών επιβολής του νόμου με τις εταιρείες της τεχνολογίας των πληροφοριών. Στόχος είναι η συστράτευση των αρχών επιβολής του νόμου με την κοινωνία των πολιτών ώστε να αναπτυχθεί μία κουλτούρα συνεργασίας που θα βοηθήσει στην ανάπτυξη των κατάλληλων εργαλείων για την αντιμετώπιση του παράνομου περιεχομένου του διαδικτύου. Με αυτόν τον τρόπο προωθείται μια εθελοντική συνεργασία των κρατών μελών και των παρόχων υπηρεσιών φιλοξενίας[190].

7.1.2.5. ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ

Η πανδημία που διανύουμε ανέδειξε το φαινόμενο της προσπάθειας χειραγώγησης των πληροφοριών από κρατικούς και μη κρατικούς φορείς, προκαλώντας σοβαρά προβλήματα στις υποδομές. Αυτό είχε ως αποτέλεσμα να τεθεί σε κίνδυνο η κοινωνική συνοχή και η εμπιστοσύνη των πολιτών στις δημόσιες αρχές. Στο πλαίσιο αντιμετώπισης παρόμοιων απειλών η Ένωση έχει αναπτύξει συνεργασία

[189] Ευρωπαϊκή Επιτροπή, Σύσταση ΕΕ 2018/334, Σχετικά με μέτρα για την αποτελεσματική αντιμετώπιση του παράνομου περιεχομένου στο διαδίκτυο
[190] Παπακωνσταντής Μάρκος, ο.π., σελ. 369

με το ΝΑΤΟ και την ομάδα των 7 (G7) ενώ έχει εκπονήσει συγκεκριμένη στρατηγική[191] για την αντιμετώπιση των υβριδικών απειλών υιοθετώντας τα απαραίτητα εργαλεία για την αντιμετώπιση τους. Σε επόμενη φάση, πρόκειται να δημιουργηθεί μια διαδικτυακή πλατφόρμα περιορισμένης πρόσβασης, η οποία θα έχει συμβουλευτικό και υποστηρικτικό ρόλο στα κράτη μέλη αναφορικά με την αντιμετώπιση των υβριδικών απειλών.

Βέβαια, η Επιτροπή αναγνωρίζει ότι την κύρια ευθύνη για την αντιμετώπιση υβριδικών απειλών φέρουν τα κράτη μέλη, καθότι πρόκειται για ζητήματα που άπτονται των εθνικών πολιτικών άμυνας και ασφάλειας. Ωστόσο, υπάρχουν απειλές που χαρακτηρίζονται από διασυνορικότητα και αφορούν όλα τα κράτη μέλη αλλά και την Ένωση ως Οργανισμό, όπως η στόχευση διασυνοριακών δικτύων ή υποδομών[192].

Σε κάθε περίπτωση, απαιτείται εξορθολογισμός των διάφορων ροών πληροφοριών που προέρχονται από πληθώρα πηγών, μεταξύ των οποίων τα κράτη μέλη, ο ENISA, η EUROPOL,ο FRONTEX και άλλους Οργανισμούς της Ένωσης. Τον ανωτέρω στόχο καλούνται να επιτύχουν οι αρμόδιες υπηρεσίες της Επιτροπής και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης.

7.1.2.6. ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΣΕ ΠΟΛΙΤΙΚΟ ΕΠΙΠΕΔΟ

Σύμφωνα με το Συμβούλιο της Ένωσης[193], «*η ΕΕ επιβεβαιώνει ότι τα μέτρα στο πλαίσιο της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας, συμπεριλαμβανομένων, κατά περίπτωση, των περιοριστικών μέτρων, που εγκρίνονται με βάση τις οικείες διατάξεις των συνθηκών, είναι κατάλληλα για ένα πλαίσιο κοινής διπλωματικής αντίδρασης της ΕΕ σε κακόβουλες δραστηριότητες στον κυβερνοχώρο και θα πρέπει να ενθαρρύνουν τη συνεργασία, να διευκολύνουν το μετριασμό των άμεσων και μακροπρόθεσμων απειλών και να επηρεάζουν τη συμπεριφορά των εν δυνάμει δραστών σε μακροπρόθεσμη βάση. Η ΕΕ θα επιδιώξει την περαιτέρω ανάπτυξη πλαισίου για κοινή διπλωματική αντίδραση της ΕΕ έναντι*

[191] Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών – Απόκριση της Ευρωπαϊκής Ένωσης, JOIN (2016) 18
[192] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 19
[193] Συμβούλιο της Ευρωπαϊκής Ένωσης 9916/17, 7 Ιουνίου 2017, Συμπέρασμα υπ' αριθμ. 5

κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, καθοδηγούμενη από τις εξής κύριες αρχές:

• προστασία της ακεραιότητας και της ασφάλειας της ΕΕ, των κρατών μελών της και των πολιτών τους,

• συνυπολογισμός του ευρύτερου πλαισίου των εξωτερικών σχέσεων της ΕΕ με την αφορώμενη χώρα,

• επιδίωξη της επίτευξης των στόχων της ΚΕΠΠΑ που προβλέπονται στη Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ) και στις σχετικές διαδικασίες για την επίτευξή τους,

• κοινή επίγνωση της κατάστασης σε συμφωνία με τα κράτη μέλη και ανταπόκριση στις ανάγκες που απορρέουν από συγκεκριμένες καταστάσεις,

• ενέργειες ανάλογες προς το εύρος, την κλίμακα, τη διάρκεια, την ένταση, την πολυπλοκότητα, την ιδιομορφία και τις επιπτώσεις της δραστηριότητας στον κυβερνοχώρο,

• σεβασμός του ισχύοντος διεθνούς δικαίου και των θεμελιωδών δικαιωμάτων και ελευθεριών».

7.1.2.7. ΔΗΜΙΟΥΡΓΙΑ ΑΠΟΤΡΟΠΗΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΜΕΣΩ ΤΗΣ ΑΜΥΝΤΙΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΤΩΝ ΚΡΑΤΩΝ ΜΕΛΩΝ

Η Ένωση αντιλαμβάνεται πλέον τον κυβερνοχώρο ως ένα χώρο ανάλογο με τον χερσαίο, τον εναέριο και τον θαλάσσιο χώρο ως προς την διενέργεια επιχειρήσεων. Ως εκ τούτου, η Επιτροπή καλεί τα κράτη μέλη να αναπτύξουν επαρκή αμυντική ικανότητα για τις επιθέσεις στον κυβερνοχώρο. Προς τον σκοπό αυτό, η Επιτροπή συμβάλλει στην δημιουργία συνεργιών για στρατιωτικές και μη στρατιωτικές προσπάθειες. Μάλιστα, τα προηγμένα σε αυτόν τον τομέα κράτη μπορούν, σε συνεργασία με την Ύπατη Εκπρόσωπο, να συμπεριλάβουν το ζήτημα της κυβερνοασφάλειας εντός του πλαισίου μια Μόνιμης Διαρθρωμένης Συνεργασίας.

Η Επιτροπή προσδίδει σημαντική βαρύτητα στην περαιτέρω ενσωμάτωση της ασφάλειας και της άμυνας στον κυβερνοχώρο στην Κοινή Πολιτική Ασφαλείας και Άμυνας (ΚΠΑΑ). Σκοπός είναι να αναπτυχθούν τυποποιημένες διαδικασίες και

τεχνικές ικανότητες οι οποίες θα μπορούν να υποστηρίζουν τόσο τις μη στρατιωτικές όσο και τις στρατιωτικές αποστολές και επιχειρήσεις. Στο ίδιο πλαίσιο σκοπείται η ανάπτυξη των αντίστοιχων δομών δυνατότητας σχεδιασμού και διεξαγωγής επιχειρήσεων καθώς και των παρόχων υπηρεσιών τεχνολογίας των πληροφοριών της ΕΥΕΔ[194].

7.1.3. ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ

Η Ένωση επιθυμεί να διαδραματίσει καθοριστικό ρόλο στην διεθνή συνεργασία για την αντιμετώπιση του κυβερνοεγκλήματος με στόχο την προαγωγή της παγκόσμιας σταθερότητας σε αυτόν τον τομέα και την στρατηγική αυτονομία της Ένωσης στον χώρο αυτόν. Για τον σκοπό αυτόν, η Επιτροπή ανακοινώνει τρεις δράσεις:

7.1.3.1. ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΤΟ ΠΛΑΙΣΙΟ ΤΩΝ ΕΞΩΤΕΡΙΚΩΝ ΣΧΕΣΕΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Η σύναψη στρατηγικών συμμαχιών με τρίτες χώρες καθίσταται καθοριστική και αναγκαία για την πρόληψη και την αποτροπή κυβερνοεπιθέσεων, δεδομένου ότι, πλέον, οι κυβερνοεπιθέσεις αποτελούν σημαντικό παράγοντα διεθνούς ασφάλειας και σταθερότητας. Αυτό καθίσταται εναργέστερο, εάν ληφθεί υπόψη ότι σύμφωνα με έρευνα οι επιθέσεις από ξένες χώρες αποτελούν μία από τις σημαντικότερες απειλές για την εθνική ασφάλεια των κρατών[195].

Σε διεθνές επίπεδο, η Ένωση υποστηρίζει σθεναρά ότι στον κυβερνοχώρο εφαρμόζεται το διεθνές δίκαιο και πιο συγκεκριμένα ο Χάρτης των Ηνωμένων Εθνών. Παράλληλα, η Ένωση ακολουθεί τους, μη δεσμευτικούς, κανόνες και τις αρχές υπεύθυνης κρατικής συμπεριφοράς, όπως έχουν διατυπωθεί από εμπειρογνώμονες του ΟΗΕ[196].

[194] Ευρωπαϊκή Επιτροπή, Κοινή Ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, σελ. 23
[195] Spring, Global Attitudes Survey, Pew Research Centre, 2017
[196] A/68/98 και A/70/174

Σε διμερές επίπεδο, η Ένωση έχει πραγματοποιήσει διάλογο με ορισμένα κράτη[197] για ζητήματα κυβερνοασφάλειας και στόχος είναι ο διάλογος αυτός να εμπλουτιστεί και να αναπτυχθεί περαιτέρω. Ωστόσο, λαμβάνονται τα απαραίτητα μέτρα, ώστε το έγκλημα στον κυβερνοχώρο να μην αποτελέσει πρόσχημα για την εισαγωγή νέων περιορισμών στο εμπόριο και τη οικονομία ή την καταπάτηση θεμελιωδών ελευθεριών[198].

7.1.3.2. ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΡΙΤΕΣ ΧΩΡΕΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΙΚΑΝΟΤΗΤΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Όπως έχει αναπτυχθεί πολλάκις παραπάνω, η ασφάλεια βασίζεται πρώτα απ' όλα στην ικανότητα των εθνικών αρχών να προλαμβάνουν και να λειτουργούν αποτρεπτικά στις κυβερνοεπιθέσεις. Για τον λόγο αυτό, η Ένωση πρωτοστατεί στην προσπάθεια ενίσχυσης της ανθεκτικότητας τρίτων χωρών, καθώς αυτή θα συμβάλλει στην παγκόσμια ανθεκτικότητα εν γένει. Προτεραιότητα δίνεται στις γειτονικές χώρες της Ένωσης και στις αναπτυσσόμενες χώρες, όπου παρατηρούνται συνεχώς αυξανόμενα ποσοστά συνδεσιμότητας.

7.1.3.3. ΣΥΝΕΡΓΑΣΙΑ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ - ΝΑΤΟ

Στόχος της Επιτροπής είναι η ανάπτυξη της ήδη υπάρχουσας συνεργασίας μεταξύ της Ένωσης και του ΝΑΤΟ με την προώθηση της διαλειτουργικότητας μέσω της θέσπισης κοινών προτύπων και απαιτήσεων για την ασφάλεια στον κυβερνοχώρο. Περαιτέρω, οι δύο Οργανισμοί επιτείνουν την συνεργασία τους στον τομέα της έρευνας και καινοτομίας και την ανταλλαγή πληροφοριών. Τα επόμενα έτη, σχεδιάζεται η διενέργεια κοινών ασκήσεων άμυνας στον κυβερνοχώρο με την συμμετοχή και του Συνεργατικού Κέντρου Αριστείας του ΝΑΤΟ για την Άμυνα στον Κυβερνοχώρο με έδρα το Τάλλιν.

Παράλληλα, η Ένωση και το ΝΑΤΟ διεξάγουν συντονισμένες ασκήσεις για την αντιμετώπιση υβριδικών απειλών με την συμμετοχή του ENISA και άλλων σχετικών

[197] Βλ. για παράδειγμα ΗΠΑ, Κίνα, Ιαπωνία

[198] Βλ. Συμβούλιο της Ευρωπαϊκής Ένωσης 8647/14, Κατευθυντήριες γραμμές της ΕΕ στον τομέα των ανθρωπίνων δικαιωμάτων για την ελευθερία της έκφρασης εντός και εκτός διαδικτύου, 12/05/2014

οργάνων και Οργανισμών[199]. Άλλωστε, οι δύο Οργανισμοί έχουν εκδώσει κοινή Διακήρυξη για την συνεργασία στους τομείς της ασφάλειας στον κυβερνοχώρο, των υβριδικών απειλών και της άμυνας[200].

7.2. Η ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΔΕΚΑΕΤΙΑ 2021-2030

Η Ένωση αντιλαμβανόμενη την μείζονα σημασία του κυβερνοχώρου στην απόλαυση ζωτικών αγαθών όπως οι μεταφορές, η ενέργεια, ο χρηματοοικονομικός τομέας κτλ εκπονεί στρατηγική για την κυβερνοασφάλεια σε ορίζοντα δεκαετίας προσαρμόζοντας την στις σύγχρονες εξελίξεις του κυβερνοεγκλήματος. Τις ανωτέρω θέσεις επιβεβαιώνουν τα στατιστικά και τα πορίσματα από σχετικές έρευνες. Συγκεκριμένα, οι συνδεδεμένες συσκευές υπολογίζεται έως το 2025 να ξεπερνούν τις 25 δισεκατομμύρια, αριθμός πολλαπλάσιος του συνολικού πληθυσμού της γης[201]. Άλλωστε, κατά την διάρκεια της πανδημίας το 40% των εργαζομένων πολιτών της Ένωσης υιοθέτησε την τηλεργασία, γεγονός που μπορεί να μονιμοποιηθεί[202]. Αυτά έχουν ως αποτέλεσμα να αυξάνεται η ανάγκη για κυβερνοασφάλεια, αφού αυξάνεται αντίστοιχα ο αριθμός των κυβερνοεπιθέσεων. Παράλληλα, οι πολίτες της Ένωσης δεν αισθάνονται απόλυτα προστατευμένοι από τις κυβερνοαπειλές[203]. Ειδικότερα, ένας στους τρεις πολίτες έχει λάβει τα τελευταία χρόνο δόλια μηνύματα ή κλήσεις που προσπαθούσαν να εκμαιεύσουν προσωπικά στοιχεία αλλά το 82% δεν προέβη ποτέ

[199] Βλ. CERT-EE για την Ευρωπαϊκή Ένωση και NCIRC για NATO

[200] JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION, διαθέσιμο σε: nato-eu-declaration-8-july-en-final.pdf (europa.eu)

[201] Εμπορική Ένωση Τηλεπικοινωνιών GSMA, The IoT by 2025, διαθέσιμο σε: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf

[202] Arlington, Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Tim, διαθέσιμο σε: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

[203] Ευρωπαϊκή Επιτροπή, Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας 2020, διαθέσιμο σε: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020 , https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

σε καταγγελία. Επίσης, μία στις οκτώ επιχειρήσεις έχει γίνει στόχος επιθέσεων[204] με το μέσο κόστος ανά επιχείρηση να εκτιμάται στα 3,8 εκατομμύρια ευρώ, κυρίως από απώλεια αρχείων λόγω παραβιάσεων δεδομένων[205]. Ενδεικτικό είναι επίσης ότι κατά το έτος 2020 το ετήσιο κόστος από το κυβερνοέγκλημα στην Ένωση ανέρχεται στο ποσό των 5,5 τρισεκατομμυρίων ευρώ[206], ενώ εκτιμήσεις δείχνουν την ύπαρξη 700 εκατομμυρίων νέων κακόβουλων λογισμικών, που αποτελεί τον πλέον συνήθη τρόπο εκδήλωσης των επιθέσεων[207]. Ωστόσο, το πλέον χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι το έτος 2019 σημειώθηκαν περί τις 450 επιθέσεις που είχαν ως στόχο υποδομές ζωτικής σημασίας της Ένωσης, όπως η ενέργεια και ο χρηματοπιστωτικός τομέας[208]. Ως εκ τούτου, η βελτίωση της κυβερνοασφάλειας είναι απαραίτητη, προκειμένου οι πολίτες να εμπιστεύονται, να χρησιμοποιούν και να ωφελούνται από την καινοτομία, τη συνδεσιμότητα και την αυτοματοποίηση, καθώς και για να διασφαλίζονται τα θεμελιώδη δικαιώματα και ελευθερίες, συμπεριλαμβανομένων των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και η ελευθερία έκφρασης και πληροφόρησης[209].

Από τα παραπάνω προκύπτει η αναγκαιότητα εκπόνησης της παρούσας στρατηγικής με σκοπό να αντιμετωπισθούν τα προβλήματα που αναφέρθηκαν αλλά και να προβλεφθούν νέα. Άλλωστε, η στρατηγική της Ένωσης αποτελεί βασική συνιστώσα της Διαμόρφωσης του ψηφιακού μέλλοντος της Ευρώπης[210] καθώς και του Σχεδίου Ανάκαμψης της Επιτροπής[211]. Επίσης, αποτελεί βασικό μέρος της συνολικής στρατηγικής της Ένωσης για την Εξωτερική Πολιτική και Πολιτική

[204] Δελτίο Τύπου της Eurostat, Μέτρα ασφάλειας ΤΠΕ που λαμβάνονται από τη συντριπτική πλειονότητα των επιχειρήσεων στην ΕΕ, 6/2020-13 Ιανουαρίου 2020
[205]IBM Security, Annual Cost of a Data Breach Report, 2020 Ponemon Institute, διαθέσιμο σε: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
[206] JRC, Cybersecurity – Our Digital Anchor
[207]AV-TEST, Malware, διαθέσιμο σε: https://www.av-test.org/en/statistics/malware/
[208] Ευρωπαϊκή Επιτροπή, ICT security measures taken by vast majority of enterprises in the EU, διαθέσιμο σε: https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f
[209] Ευρωπαϊκή Επιτροπή, JOIN (2020) 18 final, Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία, σελ. 4-5
[210] Ευρωπαϊκή Επιτροπή, COM (2020) 67 final
[211] Ευρωπαϊκή Επιτροπή, COM (2020) 98 final

Ασφαλείας[212], της στρατηγικής για την Ένωση Ασφαλείας 2020 – 2025[213] και του στρατηγικού Θεματολογίου του Ευρωπαϊκού Συμβουλίου 2019 – 2024[214].

Η στρατηγική κινείται σε τρεις άξονες δράσης στους οποίους θεωρεί τα τελευταία έτη η Ένωση ως απαραίτητους για την αντιμετώπιση του κυβερνοεγκλήματος: α) Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγετικός ρόλος, β) Ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντίδρασης και γ) προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου. Ειδικότερα:

7.2.1. ΑΝΘΕΚΤΙΚΟΤΗΤΑ, ΤΕΧΝΟΛΟΓΙΚΗ ΚΥΡΙΑΡΧΙΑ ΚΑΙ ΗΓΕΤΙΚΟΣ ΡΟΛΟΣ

Στόχος της Ένωσης για την επόμενη δεκαετία είναι να αποκτήσει ηγετικό ρόλο στην ανάπτυξη ασφαλών τεχνολογιών που θα εκτείνονται σε ολόκληρη την εφοδιαστική αλυσίδα. Για την επιτυχή έκβαση του ανωτέρω στόχου απαιτείται μια σειρά από επιμέρους δράσεις που θα συμβάλλουν στο επιθυμητό αποτέλεσμα.

Όπως ειπώθηκε παραπάνω, κύριο μέλημα της Ένωσης είναι η ανθεκτικότητα των υποδομών και υπηρεσιών ζωτικής σημασίας. Έτσι, πρόκειται να εισαχθούν μέτρα για τον καθορισμό κανόνων κυβερνοασφάλειας, αναφορικά με τις διασυνοριακές ροές ηλεκτρικής ενέργειας, μέτρα για αυξημένο επίπεδο ασφάλειας στον χρηματοπιστωτικό τομέα ώστε να μπορεί να αντισταθεί στις απειλές που προκύπτουν[215], μέτρα για την κυβερνοανθεκτικότητα στις μεταφορές εν γένει αλλά και για τις αεροπορικές μεταφορές ειδικότερα[216] και τέλος μέτρα για την ενίσχυση της ανθεκτικότητας των δημοκρατικών θεσμών και διαδικασιών με την ενίσχυση της πολυφωνίας στα ΜΜΕ και της ελευθερίας της έκφρασης καθώς και την προώθηση

[212] European Union External Action Service, EU Global Strategy, διαθέσιμο σε: https://eeas.europa.eu/topics/eu-global-strategy_en

[213] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας

[214] Ευρωπαϊκό Συμβούλιο, A new strategic agenda 2019-2024, διαθέσιμο σε: https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

[215] Ευρωπαϊκή Επιτροπή, Πρόταση κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014, COM/2020/595 final

[216] Εκτελεστικός κανονισμός 2019/1583 της Επιτροπής

ελεύθερων εκλογικών διαδικασιών[217]. Μελλοντικά πρόκειται να παρθούν μέτρα και για την ανθεκτικότητα του μελλοντικού διαστημικού προγράμματος της Ένωσης στα πλαίσια της στρατηγικής κυβερνοασφάλειας Galileo[218].

Περαιτέρω, κρίνεται απαραίτητο από την Επιτροπή η ανέγερση μιας ευρωπαϊκής ασπίδας στον κυβερνοχώρο. Καίριο ρόλο στην οικοδόμηση της κυβερνοασπίδας αποτελούν τα κέντρα ανταλλαγής και ανάλυσης πληροφοριών (ISAC) τα οποία επιτρέπουν σε τομεακό επίπεδο την ανταλλαγή πληροφοριών σχετικά με απειλές μεταξύ όλων των ενδιαφερόμενων μερών. Μάλιστα, αντιλαμβανόμενοι την ανάγκη για συνεχή επαγρύπνηση διάφορες επιχειρήσεις, αλλά και δημόσιοι οργανισμοί και εθνικές αρχές έχουν συστήσει ομάδες αντιμετώπισης περιστατικών κυβερνοεπιθέσεων (CSIRT). Τα εν λόγω κέντρα επιτελούν ζωτικής σημασίας ρόλο για την συλλογή αρχείων καταγραφής και την μετέπειτα απομόνωση των ύποπτων συμβάντων. Σε αυτό το πλαίσιο, η Επιτροπή προτείνει την δημιουργία δικτύου κέντρων επιχειρήσεων ασφαλείας σε ολόκληρη την Ένωση, με παράλληλη υποστήριξη των ήδη υπαρχόντων. Υποστηρικτικό ρόλο στο εγχείρημα πρόκειται να διαδραματίσει ο ENISA με την Ένωση να παρέχει περισσότερα από 300 εκατομμύρια ευρώ για την δημιουργία του δικτύου. Με τον τρόπο αυτό, θα οικοδομηθεί μια ισχυρή ασπίδα με στόχο τον έγκαιρο εντοπισμό των απειλών και την αντιμετώπιση τους πριν προκληθούν ζημιές μεγάλης κλίμακας.

Σε κάθε περίπτωση, τα κράτη μέλη έχουν δεσμευτεί να συνεργαστούν με την Επιτροπή, προκειμένου να αναπτύξουν μια ασφαλή υποδομή κβαντικής επικοινωνίας για την Ευρώπη[219]. Η υποδομή συνίσταται σε μια μορφή κρυπτογράφησης με ευρωπαϊκή τεχνολογία η οποία θα επιτρέπει στις δημόσιες αρχές την μεταβίβαση εμπιστευτικών πληροφοριών με ασφάλεια από κυβερνοεπιθέσεις. Δύο θα είναι οι κύριες συνιστώσες. Πρώτον, τα υφιστάμενα δίκτυα οπτικών ινών που συνδέουν στρατηγικές τοποθεσίες σε εθνικό και ευρωπαϊκό επίπεδο και δεύτερον, συνδεδεμένους δορυφόρους στο διάστημα που καλύπτουν

[217] Ευρωπαϊκή Επιτροπή, Ανακοίνωση σχετικά με το ευρωπαϊκό σχέδιο δράσης για τη δημοκρατία, COM(2020) 790
[218] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ 7
[219] Δήλωση EuroQCI

αφενός την επικράτεια των κρατών μελών της Ένωσης και αφετέρου τα υπερπόντια εδάφη της Ένωσης.

Άλλωστε, η Ένωση προσαρμοζόμενη στις τεχνολογικές εξελίξεις λαμβάνει μέριμνα για την αξιοποίηση των ωφελειών από τα ευρυζωνικά δίκτυα επόμενης γενιάς (5G) καθώς πλέον καθίσταται εφικτή η χρήση των πλέον προηγμένων και καινοτόμων εφαρμογών. Ως εκ τούτου, αυξάνονται οι απαιτήσεις ασφαλείας στα εν λόγω συστήματα. Για τον λόγο αυτό, η Επιτροπή από κοινού με τα κράτη μέλη και τον ENISA εξέδωσαν το 2020 την εργαλειοθήκη της Ένωσης για την αντιμετώπιση απειλών στα πλαίσια του δικτύου 5G, ώστε να επιτευχθεί η αποτελεσματικότερη επιλογή μέτρων στην εκάστοτε απειλή και να αυξηθεί η κυβερνοασφάλεια[220]. Η ανωτέρω συνεργασία μεταξύ της Επιτροπής, των κρατών μελών και του ENISA πρόκειται να ενταθεί για την εφαρμογή συγκεκριμένων στόχων και δράσεων σε αυτόν τον τομέα.

Επιπροσθέτως, η Επιτροπή έχει σκοπό να εξετάσει μια δέσμη μέτρων και οριζόντιων κανόνων για την βελτίωση της ασφάλειας όλων των συνδεδεμένων προϊόντων, συσκευών και υπηρεσιών που διατίθενται στην εσωτερική αγορά της Ένωσης[221]. Στο πλαίσιο αυτό, θα εξεταστεί η δυνατότητα εισαγωγής ενός νέου καθήκοντος μέριμνας των κατασκευαστών για την αντιμετώπιση των τρωτών σημείων του λογισμικού τους. Σε κάθε περίπτωση, η Επιτροπή σκοπεύει να εκπονήσει σχέδιο έκτακτης ανάγκης για την αντιμετώπιση σοβαρών σεναρίων που μπορούν να πλήξουν την ακεραιότητα και την διαθεσιμότητα του παγκόσμιου συστήματος ρίζας DNS. Παράλληλα, η Επιτροπή σε συνεργασία με τις αρμόδιες επιχειρήσεις και τα κράτη μέλη πρόκειται να επισπεύσει τις διαδικασίες για την εισαγωγή προτύπων IPv6 καθώς και πληρέστερων μέτρων ασφαλείας του διαδικτύου για την ασφάλεια του DNS, του ηλεκτρονικού ταχυδρομείου και της δρομολόγησης[222].

Τέλος, η Ένωση στοχεύει στην σύμπραξη δημόσιου και ιδιωτικού τομέα για την εδραίωση της ηγετικής της θέσης στο τομέα της κυβερνοασφάλειας και του

[220] Ευρωπαϊκή Επιτροπή, Εφαρμογή της εργαλειοθήκης της ΕΕ, COM(2020) 50
[221] Στα συμπεράσματα του Συμβουλίου ζητείται η λήψη οριζόντιων μέτρων για την κυβερνοασφάλεια των συνδεδεμένων συσκευών, 13629/20, 2 Δεκεμβρίου 2020
[222] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 12-13

διαδικτύου σε ολόκληρη την αλυσίδα εφοδιασμού στις ψηφιακές τεχνολογίες. Οι τεχνολογίες αυτές μπορεί να περιλαμβάνουν την ανάπτυξη επεξεργαστών επόμενης γενιάς, του υπολογιστικού νέφους και των δικτύων 6G. Καίριο ρόλο στο ανωτέρω εγχείρημα σκοπείται να επιτελέσει το προτεινόμενο βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας και το δίκτυο κέντρων συντονισμού (CCCN).

7.2.2. ΑΝΑΠΤΥΞΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΠΡΟΛΗΨΗΣ, ΑΠΟΤΡΟΠΗΣ ΚΑΙ ΑΝΤΙΔΡΑΣΗΣ

Η Ένωση επιθυμεί να στηρίξει τα κράτη μέλη στον τομέα της κυβερνοασφάλειας ώστε να είναι σε θέση να προστατέψουν τους πολίτες τους, τα οικονομικά τους συμφέροντα και την εθνική τους ασφάλεια. Για τον σκοπό αυτό έχουν δημιουργηθεί διάφορες κοινότητες, οι οποίες με την αξιοποίηση των προσφερόμενων εργαλείων είναι υπεύθυνες για την πρόληψη και αντιμετώπιση των κυβερνοαπειλών. Οι κοινότητες αυτές περιλαμβάνουν: I) αρχές NIS, όπως οι CSIRT, και την αντιμετώπιση καταστροφών, II) αρχές επιβολής του νόμου και δικαστικές αρχές, III) την κυβερνοδιπλωματία και IV) την κυβερνοάμυνα.

Για τον καλύτερο συντονισμό των εν λόγω κοινοτήτων προτείνεται μια πλατφόρμα εικονικής και φυσικής συνεργασίας με ειδίκευση στον συντονισμό των δράσεων για την αντιμετώπιση διασυνοριακών απειλών στον κυβερνοχώρο. Η πλατφόρμα προτείνεται να ονομαστεί Κοινή Μονάδα Κυβερνοχώρου και παρέχει την δυνατότητα στους ενδιαφερομένους να αξιοποιούν τα διαθέσιμα εργαλεία δημιουργώντας μια κουλτούρα «ανάγκης για ανταλλαγή»[223]. Με την δημιουργία της παραπάνω Μονάδας στοχεύεται να καλυφθούν δύο κενά που έχουν εντοπιστεί: Πρώτον, η αδυναμία των μη στρατιωτικών, διπλωματικών, αστυνομικών και αμυντικών κοινοτήτων κυβερνοασφάλειας να προωθήσουν την διαρθρωμένη συνεργασία και την επιχειρησιακή – συντονιστική συνεργασία. Δεύτερον, η αδυναμία πλήρους χρησιμοποίησης των δυνατοτήτων που προσφέρουν η επιχειρησιακή συνεργασία και η αμοιβαία συνδρομή στο πλαίσιο των υφιστάμενων δικτύων και

[223] «Μια Ένωση που επιδιώκει περισσότερα: Το πρόγραμμά μου για την Ευρώπη», πολιτικές κατευθύνσεις για την επόμενη Ευρωπαϊκή Επιτροπή 2019-2024 της υποψήφιας προέδρου της Ευρωπαϊκής Επιτροπής Ursula von der Leyen

κοινοτήτων καθώς η μη ύπαρξη πλατφόρμας που να παρέχει την δυνατότητα συνεργασίας με τον ιδιωτικό τομέα.

Η ανωτέρω Μονάδα πρόκειται να εκπληρώσει τρεις κύριους στόχους: *ετοιμότητα* των κοινοτήτων κυβερνοασφάλειας, *επίγνωση* της κατάστασης μέσω της ανταλλαγής πληροφοριών και τέλος συντονισμένη *αντίδραση* και ανάκαμψη. Για τη δημιουργία της Κοινής Μονάδας Κυβερνοχώρου προτείνονται τέσσερα βασικά στάδια[224]:

- Καθορισμός, μέσω της χαρτογράφησης των διαθέσιμων ικανοτήτων σε εθνικό και ενωσιακό επίπεδο·
- Προετοιμασία, μέσω της θέσπισης πλαισίου διαρθρωμένης συνεργασίας και συνδρομής·
- Ανάπτυξη, μέσω της εφαρμογής του πλαισίου, με βάση τους πόρους που παρέχουν οι συμμετέχοντες, έτσι ώστε να καταστεί επιχειρησιακή η Κοινή Μονάδα Κυβερνοχώρου·
- Επέκταση, μέσω της ενίσχυσης της συντονισμένης ικανότητας αντίδρασης με τη συμβολή του κλάδου και των εταίρων.

Περαιτέρω, απαιτούνται επιπλέον μέτρα για την αντιμετώπιση του κυβερνοεγκλήματος, καθώς κρίνεται επιτακτική η αναχαίτιση του όπως προβλέπεται στην Στρατηγική Ασφαλείας της Ένωσης το 2020 και το θεματολόγιο της Ένωσης για την καταπολέμηση της τρομοκρατίας[225], τα οποία συμπεριλαμβάνονται στην γενική πολιτική ασφαλείας της Ένωσης. Σε αυτό το πλαίσιο, τονίζεται ακόμη μια φορά η ανάγκη συνεργασίας και η ανταλλαγή πληροφοριών μεταξύ των παραγόντων κυβερνοασφάλειας και των εθνικών αρχών καθώς και η συνεργασία της Ένωσης με Οργανισμούς όπως ο ENISA και η Europol. Μάλιστα, η Επιτροπή προειδοποίει ότι διατίθεται να ενεργοποιήσει όλα τα διαθέσιμα μέσα[226], μεταξύ των οποίων και η διαδικασία επί παραβάσει[227],

[224] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 18
[225] Ευρωπαϊκή Επιτροπή, COM(2020) 795 final , σελ. 24 - 25
[226] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 19
[227] Άρθρα 258 ΣΛΕΕ επ.

προκειμένου να διασφαλιστεί η πλήρης και ορθή μεταφορά της Οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών στις εθνικές έννομες τάξεις των κρατών μελών. Παράλληλα, απαιτείται η έγκριση και εφαρμογή της δέσμης μέτρων για τα ηλεκτρονικά αποδεικτικά στοιχεία[228].

Σε αυτό το πλαίσιο, η Ένωση δημιουργεί, όπως προβλέπεται στο θεματολόγιο για την ασφάλεια, την Μονάδα Αναφοράς Διαδικτυακού Περιεχομένου[229]. Παράλληλα, αναλαμβάνει δράση νομοθετώντας για την παύση της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο και οργανώνει μέσω του Συ της Ευρωπαϊκής Ένωσης για το διαδίκτυο μια ευρύτερη συστράτευση των αρχών επιβολής του νόμου και της κοινωνίας των πολιτών με σκοπό την ανάπτυξη των καλύτερων δυνατών εργαλείων για την αντιμετώπιση της τρομοκρατικής προπαγάνδας στο διαδίκτυο[230].

Σημαντικό ρόλο στην πρόληψη και αντιμετώπιση του κυβερνοεγκλήματος αποδίδει η Επιτροπή στην εφαρμογή της εργαλειοθήκης της Ένωσης για την κυβερνοδιπλωματία που εκδόθηκε το 2017. Το νομικό πλαίσιο για την επιβολή στοχευμένων περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων θεσπίστηκε τον Μάϊο του 2019[231] και έκτοτε επιβλήθηκαν κυρώσεις σε έξι πρόσωπα και τρεις οντότητες που διενήργησαν ή συμμετείχαν σε κυβερνοεπιθέσεις που έπληξαν την Ένωση ή τα κράτη μέλη[232]. Άλλωστε, ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα ΚΕΠΠΑ ενθαρρύνει την δημιουργία ομάδας για ανταλλαγή πληροφοριών και στο μέλλον πρόκειται να υποβάλλει πρόταση για τον ακριβή καθορισμό της θέσης της Ένωσης για την κυβερνοαποτροπή. Επιπλέον, ο Ύπατος Εκπρόσωπος,

[228]Ευρωπαϊκή Επιτροπή, COM(2018) 225 και 226· C(2020) 2779 final

[229] European Union Internet Referral Unit (EU IRU)

[230] Παπακωνσταντής Μάρκος, ο.π., σελ. 348-349

[231] Απόφαση (ΚΕΠΠΑ) 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 13)· και Κανονισμός (ΕΕ) 2019/796 του Συμβουλίου της 17ης Μαΐου 2019, σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 1).

[232] Απόφαση (ΚΕΠΠΑ) 2020/1127 του Συμβουλίου, της 30ής Ιουλίου 2020, για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ST/9564/2020/INIT) (ΕΕ L 246 της 30.7.2020, σ. 12-17)· και εκτελεστικός κανονισμός (ΕΕ) 2020/1125 του Συμβουλίου, της 30ής Ιουλίου 2020, για την εφαρμογή του κανονισμού (ΕΕ) 2019/796 σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ST/9568/2020/INIT) (ΕΕ L 246 της 30.7.2020, σ. 4-9).

από κοινού με το Συμβούλιο και την Επιτροπή, σκοπεύει να εξετάσει πρόσθετα μέτρα στο πλαίσιο της εργαλειοθήκης για την κυβερνοδιπλωματία, συμπεριλαμβανομένης της δυνατότητας περαιτέρω επιλογών για περιοριστικά μέτρα, καθώς και της δυνατότητας ψηφοφορίας με ειδική πλειοψηφία για καταχωρίσεις στο πλαίσιο του καθεστώτος οριζόντιων κυρώσεων κατά των κυβερνοεπιθέσεων[233]. Στο πλαίσιο αυτό, η Ένωση συνίσταται να εξετάσει ακόμα την σχέση της κυβερνοδιπλωματίας με την ρήτρα αμοιβαίας άμυνας[234] και αλληλεγγύης[235] που ενυπάρχουν στις ιδρυτικές συνθήκες.

Άλλωστε, ύστερα από τον χαρακτηρισμό του κυβερνοχώρου ως πεδίο επιχειρήσεων, όπως ειπώθηκε ανωτέρω, πρέπει να εξεταστεί ο τρόπος με τον οποίο πρόκειται να πραγματοποιηθούν στον κυβερνοχώρο στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ εφόσον αυτές είναι εφικτές.

7.2.3. ΠΡΟΩΘΗΣΗ ΕΝΟΣ ΠΑΓΚΟΣΜΙΟΥ ΑΝΟΙΚΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Στο πλαίσιο αυτό η Ένωση, σύμφωνα με την παρούσα Στρατηγική πρέπει να αναλάβει τις εξής πρωτοβουλίες:

- Καθορισμός ενός συνόλου στόχων στις διεθνείς διαδικασίες τυποποίησης και να τους προωθήσει σε διεθνές επίπεδο·
- Προώθηση της διεθνούς ασφάλειας και σταθερότητας στον κυβερνοχώρο, ιδίως μέσω της πρότασης της ΕΕ και των κρατών μελών της σχετικά με πρόγραμμα δράσης για την προαγωγή της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA) στο πλαίσιο των Ηνωμένων Εθνών·
- Παροχή πρακτικής καθοδήγησης σχετικά με την εφαρμογή των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στον κυβερνοχώρο·
- Καλύτερη προστασία των παιδιών από τη σεξουαλική κακοποίηση και τη σεξουαλική εκμετάλλευση, καθώς και να παρουσιάσει στρατηγική για τα δικαιώματα του παιδιού·

[233] Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας, σελ. 21
[234] Άρθρο 42 παρ. 7 ΣΕΕ
[235] Άρθρο 222 ΣΛΕΕ

- Ενίσχυση και προώθηση της Σύμβασης της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, μεταξύ άλλων μέσω των εργασιών για το δεύτερο πρόσθετο πρωτόκολλο της Σύμβασης της Βουδαπέστης·
- Επέκταση του διαλόγου της ΕΕ με τρίτες χώρες, περιφερειακούς και διεθνείς οργανισμούς, μεταξύ άλλων μέσω άτυπου δικτύου της ΕΕ για την κυβερνοδιπλωματία·
- Ενίσχυση των ανταλλαγών με την πολυσυμμετοχική κοινότητα, ιδίως μέσω τακτικών και δομημένων ανταλλαγών με τον ιδιωτικό τομέα, την πανεπιστημιακή κοινότητα και την κοινωνία των πολιτών· και
- Πρόταση θεματολογίου της ΕΕ για την ανάπτυξη των εξωτερικών κυβερνοϊκανοτήτων και συμβούλιο της ΕΕ για την ανάπτυξη των κυβερνοϊκανοτήτων της ΕΕ .

8. ΕΠΙΛΟΓΟΣ

Η συνεχής ανάπτυξη της τεχνολογίας, αναντίρρητα, έχει ως συνέπεια την αυξημένη χρήση του διαδικτύου και την επακόλουθη αύξηση της συνδεσιμότητας δικτύων και συσκευών. Το γεγονός αυτό, ευνοεί την αύξηση του αριθμού των εγκληματιών που επιλέγουν το διαδίκτυο ως πεδίο δράσης καθώς, όπως αναφέρθηκε, βρίσκουν σε αυτό πολλά πλεονεκτήματα, όπως η δυσκολία εντοπισμού και η ανωνυμία. Το πρόβλημα αυτό εντοπίστηκε ήδη σε, σχεδόν, παγκόσμιο επίπεδο με το Συμβούλιο της Ευρώπης του Οργανισμού των Ηνωμένων Εθνών να λαμβάνει πρωτοβουλία για την υπογραφή της Σύμβασης της Βουδαπέστης, η οποία αναφέρεται στην ποινικοποίηση του κυβερνοεγκλήματος και εισάγει κοινούς ορισμούς μεταξύ των συμβαλλομένων κρατών. Το τότε αναδυόμενο πρόβλημα της αντιμετώπισης του κυβερνοεγκλήματος αντιλήφθηκε σύντομα και η Ευρωπαϊκή Ένωση, η οποία ανέλαβε με την σειρά της νομοθετική δράση, εκδίδοντας την Απόφαση – Πλαίσιο το 2002 και αντικαθιστώντας αυτή με την Οδηγία του 2013, αντιλαμβανόμενη την ανάγκη προσαρμογής στις νέες μορφές κυβερνοεγκλήματος. Έκτοτε και οι δύο Οργανισμοί αναλαμβάνουν συχνά δράσεις για την καταπολέμηση του φαινομένου.

Ωστόσο, απέχουμε πάρα πολύ από το να μπορεί κάποιος να ισχυριστεί ότι βρισκόμαστε κοντά στην ελαχιστοποίηση του φαινομένου. Αντίθετα, η εκθετικά αυξανόμενη χρήση της τεχνολογίας από πολίτες, επιχειρήσεις, κράτη και οργανισμούς, σε συνδυασμό με την βραδύτητα που κινείται η νομοθετική διαδικασία στην Ένωση, οδηγούν στην άνθιση του κυβερνοεγκλήματος. Έτσι, όλο και περισσότεροι εγκληματίες προσφεύγουν σε αυτό, εγκαταλείποντας τους παραδοσιακούς τρόπους διάπραξης εγκλημάτων. Για τον λόγο αυτό, είναι απαραίτητο τόσο τα κράτη όσο και η Ευρωπαϊκή Ένωση να δημιουργήσουν τους κατάλληλους μηχανισμούς ώστε να είναι σε θέση να προσαρμοστούν γρήγορα στις τεχνολογικές εξελίξεις.

Οι μελλοντικές προκλήσεις αναφορικά με το κυβερνοέγκλημα είναι πολλές και ποικίλουν. Αυτό έγινε σαφέστερο την εποχή της πανδημίας covid – 19, όπου το μεγαλύτερο μέρος του παγκόσμιου πληθυσμού κατέφυγε σε εργασία και

δραστηριότητες μέσω υπολογιστών και λοιπών συνδεδεμένων συσκευών. Έτσι, τα δύο τελευταία έτη διαπιστώθηκε σημαντική αύξηση στον διαμοιρασμό κακόβουλων λογισμικών μέσω sites – βιτρινών με θεματολογία σχετική με τον κορονοϊό. Παράλληλα, αυξήθηκαν οι επιθέσεις σε καίριες δομές όπως οι μεταφορές, η ενέργεια, η υγεία και η εκπαίδευση[236].

Ωστόσο, οι μελλοντικές προκλήσεις δεν περιορίζονται μόνο στα θέματα σχετικά με την πανδημία. Η άνοδος των κρυπτονομισμάτων και της τεχνολογίας του blockchain τείνει με αργά αλλά σταθερά βήματα να μετασχηματίσει την οικονομία όπως την ξέρουμε σε μία ολικώς ψηφιακή οικονομία. Ως εκ τούτου, η ανάγκη για κυβερνοασφάλεια καθίσταται ζωτικής σημασίας καθώς στο blockchain στοχεύεται να υπάρχουν όλα τα περιουσιακά στοιχεία του κάθε ατόμου, από τα χρήματα του ως τα συμβόλαια του σπιτιού του για παράδειγμα.

Την ίδια στιγμή, η ψηφιοποίηση της ζωής μας εγείρει σημαντικά θέματα προσωπικών δεδομένων και βιοηθικής. Αναφερόμενοι στην ψηφιακή ζωή, μπορούμε να σκεφτούμε το διαδίκτυο των υπηρεσιών, το διαδίκτυο των πραγμάτων ή και το ηλεκτρονικό εμπόριο καθώς και τις έξυπνες συσκευές μεταξύ άλλων. Κοινός παρονομαστής όλων αυτών είναι η καθιέρωση ενός ελάχιστου επίπεδου εμπιστοσύνης, ιδιωτικότητας και προστασίας των προσωπικών δεδομένων. Εφαρμοστής των τριών διαστάσεων είναι η κυβερνοασφάλεια, με την οποία διασφαλίζεται ότι η εμπιστοσύνη δεν αποδίδεται λανθασμένα, ότι οι ψηφιακές διαδικασίες διατηρούν την προσβασιμότητα και ακεραιότητα τους και τέλος ότι η ιδιωτικότητα και τα δεδομένα διατηρούνται με ασφάλεια[237].

Περαιτέρω, πρέπει να ληφθεί υπόψη η αναμενόμενη ανάπτυξη της Τεχνητής Νοημοσύνης και κατά συνέπεια η ανάγκη για κυβερνοασφάλεια στον τομέα αυτόν. Πολλές δραστηριότητες της καθημερινής ζωής πρόκειται να επηρεαστούν από την Τεχνητή Νοημοσύνη, όπως άλλωστε και η ίδια η κυβερνοασφάλεια. Ειδικότερα, εκτιμάται ότι θα επηρεαστούν τομείς όπως η κυβερνοάμυνα, οι νομικές διώξεις και

[236] Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ) οι επιθέσεις κατά του Οργανισμού πολλαπλασιάστηκαν επί πέντε φορές σε σχέση με την ίδια περίοδο το 2019.
[237] Ευρωπαϊκή Επιτροπή, CYBERSECURITY AT THE HEART OF SOCIETAL TRANSFORMATION, σε CYBERSECURITY, our digital anchor, σελ. 21 επ.

η ψηφιακή εγκληματολογία ενώ αναμένεται να δημιουργηθούν νέες προκλήσεις στην κυβερνοασφάλεια ιδίως με την δημιουργία νέων τύπων λογισμικών που βλάπτουν την Τεχνητή Νοημοσύνη αλλά και δόλια χρήση αυτής για εγκληματικούς σκοπούς[238].

Εν κατακλείδι, οι προκλήσεις που αναμένεται να αναδυθούν σχετικά με το έγκλημα στον κυβερνοχώρο είναι πολλές συναρτήσει, μάλιστα, της τεχνολογικής εξέλιξης. Κατά συνέπεια, όλοι οι χρήστες του διαδικτύου και εν γένει των πληροφοριακών συστημάτων οφείλουν να παρακολουθούν τις εξελίξεις και να λαμβάνουν σοβαρά υπόψη ζητήματα κυβερνοασφάλειας. Παράλληλα, τόσο η Ένωση όσο και τα κράτη μέλη οφείλουν να μεριμνήσουν για την προστασία των δικαιωμάτων των πολιτών τους. Σε κάθε περίπτωση, η διαμόρφωση κουλτούρας συνεργασίας μεταξύ των φορέων, η έρευνα και η εκπαίδευση στην κυβερνοασφάλεια και η αποτελεσματικότερη επιβολή του νόμου για το κυβερνοέγκλημα αποτελούν τρεις πυλώνες, όπου κατά την γνώμη του γράφοντος πρέπει να στηριχτεί η προσπάθεια αντιμετώπισης του κυβερνοεγκλήματος.

[238] Ευρωπαϊκή Επιτροπή, CYBERSECURITY AT THE HEART OF GIGITAL TECHNOLOGICAL DEVELOPMENT, σε CYBERSECURITY, our digital anchor, σελ. 51

9. ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ

9.1. ΕΛΛΗΝΟΓΛΩΣΣΑ

1) Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση, 2003
2) Δ.Π. Αγγελόπουλος, Κυβερνοχώρος - Το διεθνές «γίγνεσθαι» στο ελληνικό «είναι», ΕΛ.Ε.Σ.ΜΕ.
3) Καϊάφα – Γκμπάντι Μ., Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδραση της στην ελληνική έννομη τάξη, ΠοινΧρ 2011
4) Παπακωνσταντής Μάρκος, Η τρομοκρατία στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης της Ευρωπαϊκής Ένωσης, NoB, 2019

9.2. ΞΕΝΟΓΛΩΣΣΑ

5) ABA, International Guide to Combating Cybercrime
6) Ad Ariely G., Adaptive Responses to Cyberterrorism, σε: Chen T., Jarvis L., Macdonald S. (eds) Cyberterrorism, Springer, New York, 2014
7) Adrian Cristian Moise, Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level, Journal of Law and Administrative Sciences
8) Arlington, Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Tim
9) Calderoni, Francesco, The European legal framework on cybercrime: Striving for an effective implementation, Crime, Law and Social Change, 2010
10) Carter D.L., Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, Volume: 64, Issue 7
11) Chaikin, David, Network investigations of cyber attacks: The limits of digital evidence, Crime, Law and Social Change, 2006
12) City of London, The implications of economic cybercrime for policing,' Research report City of London corporation, 2015

13) Csonka, Peter, The council of europe's convention on cyber-crime and other European initiatives, Revue internationale de droit pénal, vol. 77, no. 3-4, 2006
14) Cybersecurity in the European Digital Single Market, Ομάδα επιστημονικών συμβούλων υψηλού επιπέδου, Μάρτιος 2017
15) David Wicki-Birchler, The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?, σε Cybersecur Law Review, 2020
16) Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), 2000, 19
17) EUCPN, Cybercrime: a theoretical overview of the growing digital threat, σε: EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network: Brussels, 2015
18) Flanagan Anne, The law and computer crime: Reading the Script of Reform, International Journal of Law and Information Technology, 2005
19) Global Information Security Workforce Study 2017
20) Gosh S., Turrini, Cybercrimes: A Multidisciplinary Analysis, Springer, 2011
21) Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, IEEE, 2007
22) ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008
23) Jonathan Clough, A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonization, Monash University Law Review (Vol 40, No 3)
24) JUDGE STEIN SCHJØLBERG & AMANDA M. HUBBARD, HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME, ITU, 2005
25) Kerr Orin, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, New York University law review, 2003
26) Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, ITU Telecommunication Development Bureau, 2012
27) Mercado Kierkegaard, Sylvia, Here comes the 'cybernators!', Computer Law & Security Report, 22, 2006

28) Moore, R., Cybercrime: investigating high-technology computer crime, Routledge, 2015
29) Pocar, F., 2004. New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research
30) Proteus Manual, Prevention, Information and support to victims of online identity theft, Lisboa, APAV, 2015
31) Spring, Global Attitudes Survey, Pew Research Centre, 2017
32) Spyware, Adware, Botnets, and Other malicious Code
33) Thomas, D. and Loader, B., Introduction – Cybercrime: Law enforcement, security and surveillance in the information age
34) Walden, Computer Crimes and Digital Investigations
35) Wall D.S., Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime, International Review of Law, Computers and Technology, vol. 51, 2008
36) Wolak/ Finkelhor/ Mitchell, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005
37) YAR M., The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, European Journal of Criminology, 2005
38) 2007 Malware Report: The Economic Impact of Viruses

10. ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΑΞΕΙΣ

1) Απόφαση (ΚΕΠΠΑ) 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της
2) Απόφαση (ΚΕΠΠΑ) 2020/1127 του Συμβουλίου, της 30ής Ιουλίου 2020, για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797
3) Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου, της 24ης Φεβρουαρίου 2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών

4) Γενικός Κανονισμός (ΕΕ) 2016/670 για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα
5) Κανονισμός (ΕΕ) 2019/796 του Συμβουλίου της 17ης Μαΐου 2019, σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της
6) Κανονισμός 460/2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών
7) Κανονισμός 881/2019, 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)
8) Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση
9) Οδηγία (ΕΕ) 2016/680 για την προστασία των δεδομένων από τις αρχές επιβολής του νόμου
10) Οδηγία 2008/114/ΕΚ σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους
11) Οδηγία 40/2013/ΕΚ, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

11. ΜΗ ΝΟΜΟΘΕΤΙΚΕΣ ΠΡΑΞΕΙΣ

1) COMMISSION OF THE EUROPEAN COMMUNITIES, Combating trafficking in human beings and combating the sexual exploitation of children and child pornography, COM(2000) 854 final /2, 22/1/2001
2) EC3 Europol, The Internet Organized Crime Threat Assessment (iOcta), 2014
3) EC3, Europol, First Year Report
4) Europol, Intellectual Property Crime

5) JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION
6) Εμπορική Ένωση Τηλεπικοινωνιών GSMA, The IoT by 2025
7) Ευρωπαϊκή Επιτροπή, CYBERSECURITY our digital anchor
8) Ευρωπαϊκή Επιτροπή, EVOLUTION OF A MULTIFACETED DISCIPLINE, σε CYBERSECURITY
9) Ευρωπαϊκή Επιτροπή, ICT security measures taken by vast majority of enterprises in the EU
10) Ευρωπαϊκή Επιτροπή, Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, JOIN (2017) 450 final
11) Ευρωπαϊκή Επιτροπή, Για μια πιο καθαρή και πιο ανταγωνιστική Ευρώπη, COM (2020) 98 final
12) Ευρωπαϊκή Επιτροπή, COM (2020) 605 final, Σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφαλείας
13) Ευρωπαϊκή Επιτροπή, COM (2020) 65, Λευκή Βίβλος Επιτροπής για Τεχνική Νοημοσύνη, 19/02/2020
14) Ευρωπαϊκή Επιτροπή, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, COM (2017) 474
15) Ευρωπαϊκή Επιτροπή, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of the European Union Agency for Network and Information Security (ENISA), COM (2017) 478
16) Ευρωπαϊκή Επιτροπή, Ανακοίνωση σχετικά με το ευρωπαϊκό σχέδιο δράσης για τη δημοκρατία, COM(2020) 790
17) Ευρωπαϊκή Επιτροπή, Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, COM (2020) 67 final
18) Ευρωπαϊκή Επιτροπή, Ένα νέο σχέδιο δράσης για την κυκλική οικονομία
19) Ευρωπαϊκή Επιτροπή, Εφαρμογή της εργαλειοθήκης της ΕΕ, COM(2020) 50

20) Ευρωπαϊκή Επιτροπή, Θεματολόγιο της ΕΕ για την καταπολέμηση της τρομοκρατίας: πρόβλεψη, πρόληψη, προστασία και αντιμετώπιση, COM(2020) 795 final
21) Ευρωπαϊκή Επιτροπή, Πρόταση για Οδηγία του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών, COM(2010) 517 τελικό
22) Ευρωπαϊκή Επιτροπή, Πρόταση κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014, COM/2020/595 final
23) Ευρωπαϊκή Επιτροπή, Πρόταση σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο, COM (2018) 640
24) Ευρωπαϊκή Επιτροπή, Στρατηγική της ΕΕ για την αποτελεσματικότερη καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, COM(2020) 607
25) Ευρωπαϊκή Επιτροπή, σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 και 226
26) Ευρωπαϊκή Επιτροπή, Σύσταση ΕΕ 2018/334, Σχετικά με μέτρα για την αποτελεσματική αντιμετώπιση του παράνομου περιεχομένου στο διαδίκτυο
27) Ευρωπαϊκό Συμβούλιο, Συμπεράσματα του Ευρωπαϊκού Συμβουλίου, EUCO 8/17
28) Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών – Απόκριση της Ευρωπαϊκής Ένωσης, JOIN (2016) 18
29) Συμβούλιο της Ευρωπαϊκής Ένωσης 8647/14, Κατευθυντήριες γραμμές της ΕΕ στον τομέα των ανθρωπίνων δικαιωμάτων για την ελευθερία της έκφρασης εντός και εκτός διαδικτύου
30) Συμβούλιο της Ευρωπαϊκής Ένωσης 9916/17, Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»)7 Ιουνίου 2017

12. ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΙ

1) Οργανισμός Ηνωμένων Εθνών, Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης
2) Συμβούλιο της Ευρώπης, Σύμβαση για το κυβερνοέγκλημα, European treaty series - No. 185, 2001
3) International Telecommunication Union, 2011, Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185
4) United Nations Human Rights, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
5) United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Vienna, February 2013

13. ΙΣΤΟΣΕΛΙΔΕΣ

1) DigWatch, European CyberCrime Centre, διαθέσιμο σε: https://dig.watch/actors/european-cybercrime-centre
2) ENISA, CSIRT Capabilities, διαθέσιμο σε: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities
3) ENISA, CSIRT Inventory, διαθέσιμο σε: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory
4) ENISA, Cyber Europe, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
5) ENISA, Cyber Exercises Platform, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform
6) ENISA, Cyber Exercises, διαθέσιμο σε: https://www.enisa.europa.eu/topics/cyber-exercises

7) ENISA, Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, 2016
8) ENISA, National Security Strategies, διαθέσιμο σε: https://www.enisa.europa.eu/topics/national-cyber-security-strategies
9) ENISA, NLO Network, διαθέσιμο σε: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office
10) European Union External Action Service, EU Global Strategy, διαθέσιμο σε: http://europa.eu/globalstrategy/
11) Europol, European CyberCrime Centre EC-3, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
12) Europol, Internet Organize Crime Threat Assessment, διαθέσιμο σε: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment
13) Europol, EC3 Programme Board, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board
14) Europol, EC3 Partners, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners
15) Europol, EUCTF, διαθέσιμο σε: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf
16) Europol, EC3 First Year Report, διαθέσιμο σε: https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf
17) IBM Security, Annual Cost of a Data Breach Report, 2020 Ponemon Institute, διαθέσιμο σε: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
18) IBM, The Cybersecurity Intelligence Index, 2014, αναφορά στο Securitymagazine.com
19) Ευρωπαϊκή Επιτροπή, Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας 2020, διαθέσιμο σε: https://ec.europa.eu/digital-single-market/en/news/digital-

economy-and-society-index-desi-2020 ,
https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

20) Ευρωπαϊκή Επιτροπή, Διάσκεψη για το μέλλον της Ευρώπης, διαθέσιμο σε: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_el.pdf

21) Ευρωπαϊκό Συμβούλιο, Νέο Στρατηγικό Θεματολόγιο 2019-2024, διαθέσιμο σε: https://www.consilium.europa.eu/el/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/