ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΡΌΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΚΑΤΕΥΘΥΝΣΗ «ΕΘΝΙΚΗ ΚΑΙ ΕΝΩΣΙΑΚΗ ΔΙΟΙΚΗΣΗ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Έγκλημα στον Κυβερνοχώρο εντός του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης της Ευρωπαϊκής Ένωσης

Λιόκουρας Γ. Μιχαήλ
(Α.Μ.: 7118Μ008)

Επιβλέπων Καθηγητής:
Δονάτος Παπαγιάννης

Αθήνα, Νοεμ. 2019 – Μάιος 2020

<u>Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ</u>
<u>ΓΙΑ ΤΗ ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ</u>

Επιβλέπων Καθηγητής: Δονάτος Παπαγιάννης

Μέλος: Πολυξένη Παπαδάκη

Μέλος: Μάρκος Παπακωνσταντής

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον καθηγητή μου κο Μάρκο Παπακωνσταντή για τον χρόνο που διέθεσε προκειμένου να με καθοδηγήσει και να προσφέρει την πολύτιμη βοήθεια του στην επιμέλεια της παρούσας εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τον Διευθυντή του τμήματος «Δημόσια Διοίκηση» κο Δονάτο Παπαγιάννη και όλους τους καθηγητές και καθηγήτριες για την υποστήριξη και την αλληλεγγύη που επέδειξαν καθ' όλη τη διάρκεια σύνταξης της παρούσας εργασίας.

ΑΚΡΩΝΥΜΙΑ – ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Ελληνόγλωσσες

ΕΑΑ	Ευρωπαϊκή Αστυνομική Ακαδημία
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΑ	Επιτροπή Εσωτερικής Ασφαλείας
ΕΖΕΣ	Ευρωπαϊκή Ζώνη Ελευθέρων Συναλλαγών
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΕΥΕΔ	Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης
ΚΕΠΠΑ	Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας
ΚΠΑΑ	Κοινή Πολιτική Ασφαλείας και Άμυνας
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΣΕΕ	Συνθήκη για την Ευρωπαϊκή Ένωση
ΣΕΚ	Συνθήκη Ευρωπαϊκών Κοινοτήτων
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΤΠΕ	Τεχνολογία Πληροφοριών και Επικοινωνίας

Ξενόγλωσσες

ACDC	Advanced Cyber Defence Centre
ASEAN	Association of South East Asian Nations
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEPOL	European Police College
CERT/EU	Computer Emergency Response Team for the EU Institutions, bodies and agencies
CIP-PSP	Policy Support Programme of Critical Infrastructure Protection
CSDP	Common Security and Defense Policy
CSIRT	Computer Security Incident Response Team
DG CNECT	DG for Communication, Network, Content and Technology

EC3	European Cybercrime Center
ECRIS	European Criminal Records Information System
EDA	European Defence Agency
EEAS	European External Action Service
EFTA	European Free Trade Association
EJN	European Judicial Network
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Network an Information Security Agency
EP3R	European Public-Private Partnership for Resilience
EUCPN	European Crime Prevention Network
EUROSUR	European Border Surveillance System
FRONTEX	Frontieres Exterieures (FR) – European Border and Coast Guard Agency (ENG)
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
INSAFE	European Network of Awareness Centres
JRC	Joint Research System
NIS	Network and Information Systems
NRA	National Risk Assessment
OSCE	Organization for Security and Co-operation in Europe
SIS	Schengen Information System
SOCTA	Serious and Organised Crime Threat Assessment
TDL	Trust in Digital Life
VIS	Visa Information System
UNHCR	United Nations High Commissioner for Refugees

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ 8

1 ΣΥΓΚΡΟΤΗΣΗ ΤΟΥ ΧΩΡΟΥ ΕΛΕΥΘΕΡΙΑΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗΣ….9

1.1 Νομικό πλαίσιο του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης **……..... 9**

1.1.1 Η Συνθήκη του Άμστερνταμ……...9

1.1.2 Η Συνθήκη της Νίκαιας…….13

1.1.3 Η Συνθήκη της Λισαβόνας……... 14

1.2 Πολιτικό πλαίσιο του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης…… 17

1.2.1 Το Πρόγραμμα του Τάμπερε ……..…….. 18

1.2.2 Το Πρόγραμμα της Χάγης……..... 20

1.2.3 Το Πρόγραμμα της Στοκχόλμης…….……. 22

1.2.4 Οι στρατηγικές κατευθυντήριες γραμμές στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης…… 24

2 ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΩΣ ΑΠΕΙΛΗ ΤΟΥ ΧΩΡΟΥ ΕΛΕΥΘΕΡΙΑΣ, ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗΣ ……25

2.1 Συστατικά στοιχεία του Ηλεκτρονικού Εγκλήματος……..... 27

2.2 Κατηγορίες Ηλεκτρονικού Εγκλήματος……... 27

2.3 Μορφές Ηλεκτρονικού Εγκλήματος……. 30

2.3.1 Γνήσια Ηλεκτρονικά Εγκλήματα…….. 31

2.3.2 Μη Γνήσια Ηλεκτρονικά Εγκλήματα.……... 34

3 ΕΝΩΣΙΑΚΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ….. ……..... 36

3.1 Εξέλιξη του παραγώγου δικαίου για την καταπολέμηση του Κυβερνοεγκλήματος στην Ε.Ε……36

3.2 Η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά των Συστημάτων Πληροφοριών…….…….....37

3.3 Η Οδηγία 2011/92/ΕΕ για την καταπολέμηση της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας…….…….……41

3.4 Η Οδηγία 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση……..…….…47

4 ΕΠΙΠΕΔΑ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΟΡΓΑΝΙΣΜΟΙ ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ……. 54

4.1 Τομέας ασφάλειας, δικτύων και πληροφοριών…….... 55

4.1.1 Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)…….55

4.1.2 Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης στην Πληροφορική / CERT-EU (Computer Emergency Response Team)……..59

4.1.3 Ευρωπαϊκή Κοινοπραξία Δημοσίου – Ιδιωτικού Τομέα για την Ανθεκτικότητα - EP3R (European Public-Private Partnership For Resilience) …….60

4.2 Τομέας επιβολής του νόμου……..……....60

4.2.1 Ευρωπαϊκό Κέντρο για τα εγκλήματα στον Κυβερνοχώρο EC3 (European Cybercrime Center) ……...61

4.2.2 Europol…….66

4.2.3 Οργανισμός της Ευρωπαϊκής Ένωσης για την κατάρτιση στον τομέα της επιβολής του νόμου (European Police College- Cepol) ……..……...67

4.2.4 Eurojust …….…...68

4.3 Τομέας άμυνας……..…….……69

4.3.1 Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης - ΕΥΕΔ (European External Action Service - EEAS) ……..… 69

4.3.2 Ευρωπαϊκή Υπηρεσία Άμυνας (European Defence Agency- EDA) …….... 70

4.4 Συνεργασία αρμοδίων αρχών, φορέων και οργάνων ……....……71

5 Η ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ Ε.Ε…….……..71

5.1 Επίτευξη ανθεκτικότητας σχετικά με την ασφάλεια στον Κυβερνοχώρο……..…….. 72

5.2 Δραστική μείωση του Ηλεκτρονικού Εγκλήματος ……..…….74

5.3 Επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον Κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)……...…….….81

5.4 Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων με στόχο την ασφάλεια στον Κυβερνοχώρο ……..82

5.5 Θέσπιση συνεκτικής διεθνούς πολιτικής στον Κυβερνοχώρο για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της ΕΕ ……...……..87

ΣΥΜΠΕΡΑΣΜΑΤΑ……91

ΕΙΣΑΓΩΓΗ:

Η τεχνολογία είναι το αποτέλεσμα της εφαρμογής της θεωρητικής επιστημονικής γνώσης με σκοπό τη δημιουργία υλικού ή άϋλου αντικειμένου με πρακτικό όφελος για τον άνθρωπο. Αναπτύσσεται διαρκώς και η εξέλιξη της είναι ραγδαία. Αρχικά ο άνθρωπος χρησιμοποίησε την τεχνολογία για να μετατρέψει τις πρώτες ύλες σε χρήσιμα για αυτόν εργαλεία. Σήμερα ο άνθρωπος χρησιμοποιεί την τεχνολογία αδιαλείπτως αφού αυτή έχει κατακλύσει την ζωή του παρέχοντας του τη δυνατότητα να βελτιώνει τη ζωή του σε πολλούς τομείς όπως η υγεία, η βιομηχανία, οι μεταφορές, οι πληροφορίες, η επικοινωνία κλπ. Ο ηλεκτρονικός υπολογιστής και το διαδίκτυο, δύο από τα πιο σπουδαία επιτεύγματα της τεχνολογίας, και γενικότερα η ανάπτυξη του τομέα της πληροφορίας είναι τα στοιχεία που συνέβαλαν κατά κύριο λόγο στη βελτίωση της ποιότητας της καθημερινής ζωής του ανθρώπου και γενικά της κοινωνικής και οικονομικής ανάπτυξης. Η ψηφιακή ανάπτυξη που έχει επέλθει δεν βελτίωσε μόνο την καθημερινή ζωή των ανθρώπων σε τομείς όπως η εκπαίδευση, η επικοινωνία, η επιστήμη κ.α., αλλά και τις κοινωνικές, πολιτικές και οικονομικές συνθήκες διαβίωσης αφού πλέον υπάρχει δυνατότητα να πραγματοποιούνται συναλλαγές ανά πάσα ώρα και στιγμή καθημερινά, διευκολύνοντας έτσι τόσο τη ζωή των πολιτών όσο και την οικονομική ζωή της χώρας αφού συναλλαγές με το Δημόσιο ή τους ιδιώτες διεκπεραιώνονται μέσω των ηλεκτρονικών συστημάτων των τραπεζών (e-banking), χωρίς να είναι ανάγκη να απουσιάσει ο εργαζόμενος από την εργασία του.

Οι ηλεκτρονικοί υπολογιστές και γενικότερα τα πληροφοριακά συστήματα είναι χρήσιμα εργαλεία για τους ανθρώπους αρκεί αυτοί να ανακαλύπτουν και να εκμεταλλεύονται όλες τις παρεχόμενες δυνατότητες και να συμβάλλουν στην εξέλιξή τους, ώστε να τις προετοιμάζουν για τις επόμενες απαιτήσεις της ζωής τους. Αυτά τα συστήματα όμως δεν είναι άτρωτα. Υπάρχουν σημεία τα οποία κακόβουλοι χρήστες τα εκμεταλλεύονται προκειμένου να βλάψουν άλλους χρήστες γεγονός που δημιουργεί νέες μορφές εγκληματικότητας. Γνώστες της τεχνολογίας και μεθόδων προγραμματισμού με κακόβουλη διάθεση αντλούν στοιχεία που πληκτρολογούνται από τους χρήστες όπως κωδικοί πρόσβασης, φωτογραφίες, διευθύνσεις κατοικίας ή εργασίας κ.α και με χρήση ή επεξεργασία αυτών προβαίνουν στην τέλεση αξιόποινων πράξεων εναντίον τους. Με αυτό τον τρόπο οι χρήστες γίνονται θύματα του εργαλείου που βελτίωσε και βελτιώνει αξιοσημείωτα τη ζωή τους.

Επιχειρώντας μία ιστορική αναδρομή, το πρώτο καταγεγραμμένο ηλεκτρονικό έγκλημα χρονολογείται το έτος 1820 όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η συσκευή αυτή επέτρεπε την επανάληψη μίας σειράς όμοιων βημάτων κατά την ύφανση συγκεκριμένου είδους υφασμάτων. Οι υπάλληλοί του νιώθοντας φόβο από την συσκευή αυτή διότι θεωρούσαν ότι απειλούσε την εργασία τους, προκαλούσαν συχνά ζημιά στο μηχάνημα. Με τις δολιοφθορές τους επεδίωκαν την απομάκρυνση του Jacquard από την νέα τεχνολογία.

Επιστρέφοντας στη σημερινή εποχή, η Ευρωπαϊκή Ένωση, στο πλαίσιο του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης, αντιλαμβανόμενη τους κινδύνους που ελλοχεύει η ανάπτυξη της τεχνολογίας κατέληξε στο συμπέρασμα ότι η προστασία των χρηστών των υπολογιστικών συστημάτων και του διαδικτύου είναι επιτακτική. Έτσι προέβη στη θέσπιση νομοθετικών πράξεων που εξειδικεύουν εγκλήματα τα οποία τελούνται μέσω ηλεκτρονικών υπολογιστών και διαδικτύου αφού τα ήδη υπάρχοντα εγκλήματα που αφορούσαν για παράδειγμα την απάτη ή την παραβίαση προσωπικών

δεδομένων δεν έβρισκαν πάντα πρόσφορο πεδίο εφαρμογής μέσω επεκτάσεων στον τομέα της τεχνολογίας. Με αυτό τον τρόπο επιχειρείται η οριοθέτηση ενός συγκεκριμένου πλαισίου δυνατοτήτων των χρηστών του διαδικτύου και επιτυγχάνεται ο έλεγχος της κοινωνίας της πληροφορίας προτού αυτή γίνει ανεξέλεγκτη και προκαλέσει χάος και ανομία. Η νομοθεσία που υπάρχει σε ενωσιακό επίπεδο θα αποτελέσει το κύριο αντικείμενο της παρούσας εργασίας. Ωστόσο, προτού καταπιαστούμε με την εννοιολογική προσέγγιση του εγκλήματος στον κυβερνοχώρο, χρήσιμο θα ήταν να πραγματοποιηθεί μία αναδρομή της εξέλιξης της οικοδόμησης του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης της Ένωσης, που το ηλεκτρονικό έγκλημα απειλεί.

1. ΣΥΓΚΡΟΤΗΣΗ ΤΟΥ ΧΩΡΟΥ ΕΛΕΥΘΕΡΙΑΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗΣ

Η οικοδόμηση της εσωτερικής αγοράς αν και συνιστά το σημαντικότερο βήμα στο δρόμο για την ευρωπαϊκή ολοκλήρωση, δεν είναι αρκετό για την ενίσχυση του αισθήματος των ευρωπαίων πολιτών ότι ανήκουν σε μία μεγάλη πολιτική κοινότητα κοινών αξιών, αρχών, αντιλήψεων και συμφερόντων. Και αυτό γιατί πρωταρχικός στόχος της ευρωπαϊκής ολοκλήρωσης δεν θα έπρεπε να είναι ο homo oeconomicus, αλλά ο πολίτης της Ένωσης.

Έτσι, σταδιακά συνειδητοποιήθηκε ότι η ομαλή και απρόσκοπτη λειτουργία της εσωτερικής αγοράς προϋποθέτει έναν Χώρο ελευθερίας, όπου η ελεύθερη κυκλοφορία τόσο των εργαζομένων ειδικότερα, όσο και των ευρωπαίων πολιτών γενικότερα, θα διεξάγεται χωρίς εμπόδια, δηλαδή με κατάργηση των συνοριακών ελέγχων, έναν Χώρο ασφαλείας όπου όλοι οι ευρωπαίοι πολίτες θα μπορούν να απολαμβάνουν την ελευθερία τους χωρίς κινδύνους από την εγκληματικότητα και έναν Χώρο δικαιοσύνης, όπου θα κυριαρχεί η ασφάλεια δικαίου, με ελεύθερη πρόσβαση στη δικαιοσύνη και που θα διασφαλίζεται η προστασία κυρίως από το διασυνοριακό έγκλημα.

1.1 Νομικό πλαίσιο της συγκρότησης του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης

1.1.1 Η Συνθήκη του Άμστερνταμ

Η δημιουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης[1] αποτελεί σύλληψη που ενσωματώθηκε για πρώτη φορά σε κείμενο πρωτογενούς κοινοτικού και ενωσιακού δικαίου με τη Συνθήκη του Άμστερνταμ, όπου επιτεύχθηκε ένας δύσκολος συμβιβασμός με τα θέματα αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις να ρυθμίζονται σε ενωσιακό επίπεδο και στη βάση διακυβερνητικής συνεργασίας (αρθρ. 29 – 45 ΣΕΕ), ενώ τα θέματα που αφορούν στην ελεύθερη κυκλοφορία των προσώπων, τους συνοριακούς ελέγχους, τις θεωρήσεις εισόδου, το άσυλο, τη μετανάστευση αλλά και τη δικαστική συνεργασία στις αστικές υποθέσεις να ρυθμίζονται από το κοινοτικό δίκαιο (αρθρ. 61 – 69 ΣΕΚ).

Αν και στη Συνθήκη δεν υπάρχει σαφής οριοθέτηση του Χώρου και του ακριβούς εύρους του περιεχομένου του, Ανακοίνωση[2] της Επιτροπής τονίζει ότι η έννοια

[1] Παπαγιάννης Δον., Ο ευρωπαϊκός χώρος ελευθερίας, ασφάλειας και δικαιοσύνης Εκδόσεις Σάκκουλα, (2001).
[2] Ανακοίνωση της Επιτροπής «προς μία ζώνη ελευθερίας, ασφάλειας και δικαιοσύνης» COM (1998) 459 τελ.

του Χώρου περιλαμβάνει αξίες και αντιλήψεις που απορρέουν από τις δημοκρατικές παραδόσεις των κρατών - μελών και από το «κράτος δικαίου», όπως νοηματοδοτείται σε αυτά. Άλλωστε, η Ανακοίνωση σημειώνει ότι «*η ελευθερία θα χάνει μεγάλο μέρος της σημασίας της, αν δεν μπορεί να βιωθεί μέσα σε ασφαλές περιβάλλον, με πλήρη υποστήριξη ενός συστήματος δικαιοσύνης, στο οποίο μπορούν να έχουν πρόσβαση όλοι οι πολίτες της Ένωσης και όσοι διαμένουν σε αυτή*».

Εν τούτοις, με την εν λόγω Συνθήκη προστίθενται στους στόχους της Ένωσης, μεταξύ άλλων, η διατήρηση και ανάπτυξη της Ένωσης ως Χώρου «*ελευθερίας, ασφάλειας και δικαιοσύνης, μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των προσώπων σε συνδυασμό με κατάλληλα μέτρα όσον αφορά στους ελέγχους στα εξωτερικά σύνορα, το άσυλο, τη μετανάστευση και την πρόληψη και καταστολή της εγκληματικότητας*» (αρθ.2 ΣΕΕ). Η βούληση δε των κρατών μελών στην επίτευξη του συγκεκριμένου στόχου είναι ισχυρή, καθώς στο προοίμιο της Συνθήκης εκφράζουν την αποφασιστικότητα τους να εγκαθιδρύσουν τον Χώρο ώστε να «*διευκολύνουν την ελεύθερη κυκλοφορία των προσώπων, διαφυλάσσοντας ταυτόχρονα την ασφάλεια και την προστασία των λαών τους*». Η συμπερίληψη του στόχου αυτού για πρώτη φορά στο κείμενο μιας συνθήκης δεν είναι τυχαία, καθώς προτίθεται να σηματοδοτήσει την προσπάθεια δημιουργίας μιας Ένωσης η οποία θέτει την ανάδειξη του πολίτη στο επίκεντρο της ευρωπαϊκής ολοκλήρωσης και για χάρη του οποίου δημιουργείται ή τουλάχιστον αναλαμβάνεται η προσπάθεια να δημιουργηθεί ο συγκεκριμένος Χώρος[3]. Η πρόθεση ενίσχυσης του Χώρου βρίσκεται έκτοτε σε όλες τις μετέπειτα Συνθήκες της ΕΕ. Προκειμένου δε να επιτευχθεί η ελεύθερη κυκλοφορία των προσώπων, το κεκτημένο Σένγκεν ενσωματώνεται στη Συνθήκη μέσω ενός πρωτοκόλλου που προσαρτάται στο κείμενο της τελευταίας.

Η δημιουργία ενός Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης (άρθ. 2 ΣΕΕ) αντικαθιστά τον στόχο της εγκαθίδρυσης ενός χώρου δικαιοσύνης και εσωτερικών υποθέσεων τον οποίο είχε εισαγάγει η Συνθήκη του Μάαστριχτ (αρθ. 2 ΣΕΕ). Ο νέος στόχος εισάγεται με το Άμστερνταμ προκειμένου ο Ευρωπαίος πολίτης να απολαμβάνει την ελεύθερη κυκλοφορία μέσα σε ένα ασφαλές περιβάλλον και με την υποστήριξη ενός συστήματος δικαιοσύνης. Η δημιουργία του Χώρου συνιστά ένα σύνθετο εγχείρημα καθώς επιχειρεί να συναρθρώσει πολιτικές που αγγίζουν πτυχές του σκληρού πυρήνα του κράτους[4]. Η αναφορά στον Χώρο ελευθερίας καλύπτει τον στόχο της ελεύθερης κυκλοφορίας των προσώπων, της προστασίας των θεμελιωδών δικαιωμάτων και της κατάργησης κάθε είδους διακρίσεων. Η αναφορά στον Χώρο ασφάλειας καλύπτει τον στόχο καταπολέμησης της εγκληματικότητας στους τομείς που καθορίζονται στο άρθρο 29 ΣΕΕ, ενώ με την αναφορά στον Χώρο δικαιοσύνης, αποτυπώνεται η υποχρέωση για διευκόλυνση της πρόσβασης των πολιτών στη δικαιοσύνη και για συνεργασία μεταξύ των δικαστικών αρχών σε ποινικές υποθέσεις.[5]

---

[3] Παπαγιάννης Δον., Ο χώρος ελευθερίας, ασφάλειας και δικαιοσύνης μετά τη Συνθήκη της Λισαβόνας, ΕΕΕυρΔ 3:2010, σελ. 345

[4] Περράκης Σ., Ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης στην ΕΕ, στο Κ. Στεφάνου – Α. Φατούρος (επιμ.), Εισαγωγή στις ευρωπαϊκές σπουδές, Εκδόσεις Σάκκουλας, (2007), τ. Α', σ. 371.

[5] Νάσκου – Περράκη Π., Θεωρήσεις, άσυλο, μετανάστευση και άλλες πολιτικές σχετικές με την ελεύθερη κυκλοφορία των προσώπων, στο Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Ερμηνεία συνθηκών για την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα, σσ 621-622. Για μια περιγραφή του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, βλ. Επιτροπή των Ευρωπαϊκών Κοινοτήτων, προς μία ζώνη ελευθερίας, ασφάλειας και δικαιοσύνης, COM (1998) 459 τελικό, 14.09.1998.

Στο κείμενο της Συνθήκης ο όρος ελευθερίας μνημονεύεται για πρώτη φορά μόνος του, δίχως οποιονδήποτε πρόσθετο προσδιορισμό, δεδομένου ότι τα προηγούμενα κείμενα των Συνθηκών τον συνέδεαν πάντοτε με την κυκλοφορία των προσώπων, των υπηρεσιών, των εμπορευμάτων και των κεφαλαίων.[6] Το δικαίωμα στην ελεύθερη κυκλοφορία αναγνωρίζεται ως το προνόμιο του Ευρωπαίου πολίτη να ζει σε ένα ευνομούμενο περιβάλλον, πεπεισμένος ότι οι εθνικές αρχές χρησιμοποιούν όλη την ατομική και συλλογική τους ισχύ προκειμένου να προλαμβάνουν και να καταστέλλουν οποιοδήποτε φαινόμενο κατάχρησης της ελευθερίας. Συνεπώς, με τη Συνθήκη του Άμστερνταμ έχουμε ένα διευρυμένο δικαίωμα, η άσκηση του οποίου διασφαλίζεται με εθνικά και κοινοτικά μέσα. Εν τούτοις, ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης δεν είναι αυστηρά προσδιορίσιμος και η έννοια του είναι αναγκαστικά γενική. Ωστόσο, ο Χώρος θα μπορούσε να προσδιοριστεί ως ο εσωτερικός χώρος της Ένωσης εντός του οποίου διασφαλίζονται η πρωταρχία των δικαιϊκών κανόνων και οι Ευρωπαίοι πολίτες, όπως επίσης και εκείνοι των τρίτων χωρών που βρίσκονται νόμιμα στο Χώρο, κυκλοφορούν χωρίς συνοριακούς ελέγχους, δίχως να διακινδυνεύεται η ασφάλεια τους αλλά και η ασφάλεια των κρατών – μελών και όπου η πρόσβαση στη δικαιοσύνη είναι ελεύθερη σε όλους.[7] Ως εκ τούτου, ο Χώρος προϋποθέτει έλεγχο των εξωτερικών συνόρων, συνεργασία μεταξύ των εθνικών αρχών δίωξης του εγκλήματος, την αναγνώριση των δικαστικών αποφάσεων, καθώς και κατοχυρωμένη τη πρόσβαση στη δικαιοσύνη.

Χαρακτηριστική περιγραφή του βαθμού αλληλεξάρτησης των εννοιών της ελευθερίας, της ασφάλειας και της δικαιοσύνης δίνεται στο πρόγραμμα δράσης του Συμβουλίου και της Επιτροπής αναφορικά με την άριστη εφαρμογή των διατάξεων της Συνθήκης του Άμστερνταμ.[8] Σύμφωνα με το κείμενο αυτό, οι έννοιες της ελευθερίας, της ασφάλειας και της δικαιοσύνης συνδέονται τόσο στενά μεταξύ τους, ώστε να μην είναι εφικτή η υλοποίηση της μιας χωρίς να πραγματωθούν οι άλλες δύο. Η ελευθερία κυκλοφορίας καθίσταται σχεδόν κενή περιεχομένου εάν ο πολίτης δεν μπορεί να απολαύσει σε ένα ασφαλές περιβάλλον, με την πλήρη υποστήριξη ενός συστήματος δικαιοσύνης το οποίο να μπορούν να εμπιστεύονται όλοι οι πολίτες της Ένωσης και οι νομίμως διαμένοντες σε αυτή. Κατά τον τρόπο αυτό, οι τρείς έννοιες έχουν κοινό παρανομαστή τον πολίτη και καμία από αυτές δεν μπορεί να πραγματωθεί χωρίς τις άλλες.

Για την αποτελεσματική λειτουργία του νέου Χώρου ένα σημαντικό τμήμα του τρίτου πυλώνα του Μάαστριχτ μετακινείται στον πρώτο και υπάγεται στην κοινοτική αρμοδιότητα. Με τον τρόπο αυτό αντιμετωπίζεται το πρόβλημα της συγκέντρωσης ετερόκλητων τομέων δράσης υπό την ίδια θεσμική στέγη που χαρακτηρίζει τον τρίτο πυλώνα του Μάαστριχτ. Έτσι, με τη Συνθήκη του Άμστερνταμ ο παλαιός τίτλος VI «διατάξεις σχετικά με τη συνεργασία στους τομείς της δικαιοσύνης και των εσωτερικών υποθέσεων» διασπάται αφενός στον τίτλο ΙΙΙ της Συνθήκης για την Ευρωπαϊκή Κοινότητα «Θεωρήσεις, άσυλο, μετανάστευση και άλλες πολιτικές σχετικές με την ελεύθερη κυκλοφορία των προσώπων»[9], αφετέρου στον τίτλο VI της Συνθήκης για την

---

[6] Χριστογιαννόπουλος Ν., Θεωρήσεις, άσυλο, μετανάστευση και άλλες πολιτικές σχετικές με τη ελεύθερη κυκλοφορία των προσώπων, Ερμηνεία κατ' άρθρο της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για την ίδρυση της Ευρωπαϊκής Κοινότητας, Δ. Γκουλούσης – Γ. Κρεμλής (επιμ.), σ. 376

[7] Παπαγιάννης Δον., Ο χώρος ασφάλειας στην ΕΕ, Εκδόσεις Σάκκουλα, (2008), σελ. 31

[8] 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 – Κείμενο εγκριθέν από το Συμβούλιο «Δικαιοσύνη και Εσωτερικές Υποθέσεις» της 3ης Δεκεμβρίου 1998, ο.π., σ.2.

[9] Άρθρα 61-69 ΣΕΚ

ΕΕ «διατάξεις για την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις»[10]. Δηλαδή, τα ζητήματα θεωρήσεων, ασύλου, μετανάστευσης και άλλες πολιτικές που άπτονται της ελεύθερης κυκλοφορίας των προσώπων, όπως η δικαστική συνεργασία σε αστικές υποθέσεις, μεταφέρονται από τον τρίτο πυλώνα της ΕΕ στον πρώτο πυλώνα, ενώ οι διατάξεις σχετικά με την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις παραμένουν στον τρίτο πυλώνα της ΕΕ. Η αλλαγή του πλαισίου λειτουργίας και η διάσπαση του τρίτου πυλώνα έχει ιδιαίτερη σημασία και επιβάλλεται για τρεις λόγους. Πρώτον, για να καταστεί αποτελεσματικότερη μία συνεργασία σε ένα πεδίο όπου η ΕΕ εμφανίζεται να απέχει από τις προσδοκίες των πολιτών της. Δεύτερον, για να δημιουργηθεί ένα θεσμικό πλαίσιο ανάληψης δράσης από τα κράτη μέλη στους αλληλένδετους τομείς της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις παρέχοντας κατ' αυτόν τον τρόπο περισσότερη ασφάλεια στους πολίτες αλλά και προασπίζοντας τα συμφέροντα της ΕΕ. Τρίτον, για να για να δοθεί μία δυναμική στη δημιουργία ενός πλέγματος κανόνων ενόψει της διεύρυνσης της ΕΕ με κράτη της Ανατολικής Ευρώπης, τα οποία διακρίνονται για τα σαθρά ποινικά τους συστήματα[11].

Με τη Συνθήκη του Άμστερνταμ το θεματικό περιεχόμενο του τρίτου πυλώνα περιορίζεται σε δύο πεδία, ήτοι στα θέματα της αστυνομικής συνεργασίας και σε αυτά της δικαστικής συνεργασίας σε ποινικές υποθέσεις. Η Συνθήκη λαμβάνει υπόψη τη Σύμβαση της Europol που είχε ήδη εφαρμοστεί και αναμενόταν να εφαρμοστεί από τις αρχές του Οκτωβρίου 1998 και την ανάγκη για ένα καθορισμένο πλαίσιο δικαστικής συνεργασίας. Στόχος της Συνθήκης δεν καθίσταται η δημιουργία ενός ευρωπαϊκού Χώρου ασφαλείας, με την έννοια μιας κοινής επικράτειας στην οποία όλες οι ευρωπαϊκές υπηρεσίες επιβολής του νόμου στην Ευρώπη που χειρίζονται θέματα ασφαλείας εφαρμόζουν ομοιόμορφες διαδικασίες έρευνας και καταστολής, αλλά η λειτουργία ενός χώρου συνεργασίας στο συγκεκριμένο πεδίο[12].

Η ανάπτυξη της από κοινού δράσης των κρατών μελών στον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις και, ειδικότερα, η πρόληψη και η καταπολέμηση της εγκληματικότητας, του οργανωμένου εγκλήματος, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο, της τρομοκρατίας, της εμπορίας ανθρώπων, της παράνομης διακίνησης ναρκωτικών και όπλων, της δωροδοκίας και της απάτης[13], συμβάλλουν στην πραγμάτωση του στόχου της ΕΕ να παρέχει στους Ευρωπαίους πολίτες ένα υψηλό επίπεδο προστασίας εντός του Χώρου ελευθερίας, ασφάλειας και δικαιοσύνης (αρθ. 29 ΕΕ).

1.1.2 Η Συνθήκη της Νίκαιας

Η σύγκλιση της διακυβερνητικής διάσκεψης του 2000 ανταποκρίνεται στην ανάγκη να επιλυθούν όσα θεσμικά ζητήματα δεν διευθετήθηκαν στο Άμστερνταμ και τα οποία επιβάλλονταν να ρυθμιστούν πριν από την τότε επερχόμενη διεύρυνση της ΕΕ

[10] Άρθρα 29-42 ΣΕΕ

[11] Παπακωνσταντής Μ., Η τρομοκρατία στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης της Ευρωπαϊκής Ένωσης, Νομική Βιβλιοθήκη, (2019) σελ. 208-209.

[12] Ομοίως, σελ. 209.

[13] Σύμφωνα με την καθηγήτρια Παρούλα Νάσκου-Περράκη πρόκειται για ενδεικτική απαρίθμηση που στόχο έχει να τονίσει τις μορφές εγκλημάτων που εμφανίζονται συχνότερα βλ., Π. Νάσκου – Περράκη, τίτλος VI, Διατάξεις για την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις, Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Ερμηνεία συνθηκών για την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα, σελ. 104.

με δέκα νέα κράτη μέλη. Τον Δεκέμβριο του 1999 το Ευρωπαϊκό Συμβούλιο του Ελσίνκι καθορίζει την ημερήσια διάταξη της διακυβερνητικής διάσκεψης καταλείποντας ανοιχτό ένα παράθυρο καθορισμό και άλλων ζητημάτων.

Η Συνθήκη της Νίκαιας υπογράφεται στις 26 Φεβρουαρίου 2001 και τίθεται σε ισχύ την 1η Φεβρουαρίου 2003. Η θεσμική μεταρρύθμιση που πραγματοποιείται στη Νίκαια χαρακτηρίζεται ως τεχνική και περιορισμένη καθώς αρκείται στο να επιφέρει προσαρμογές αναφορικά με τη λειτουργία και τη σύνθεση των θεσμικών οργάνων και τις ενισχυμένες συνεργασίες.

Στον τίτλο VI σχετικά με τις διατάξεις για την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις οι αλλαγές που επέρχονται δεν είναι σημαντικές. Στη σύνοδο κορυφής στο Τάμπερε[14] αποφασίζεται η ενίσχυση της καταπολέμησης των σοβαρών μορφών οργανωμένου εγκλήματος, συμπεριλαμβανομένου και του εγκλήματος στον κυβερνοχώρο, με την ίδρυση της μονάδας Eurojust με καθήκον τη διευκόλυνση του συντονισμού των εθνικών εισαγγελικών αρχών και την υποστήριξη των ποινικών ερευνών στις περιπτώσεις οργανωμένου εγκλήματος. Η Συνθήκη της Νίκαιας αναδεικνύει την Eurojust και την Europol από κοινού, ως κεντρικό συντονιστικό όργανο για την συντεταγμένη κινητοποίηση της ποινικής καταστολής.

Ο στόχος παροχής στους Ευρωπαίους πολίτες ενός Χώρου ελευθερίας, ασφάλειας και δικαιοσύνης επιτυγχάνεται με την πρόληψη και την καταπολέμηση της εγκληματικότητας, του οργανωμένου εγκλήματος, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο, της τρομοκρατίας, της εμπορίας ανθρώπων, της παράνομης διακίνησης ναρκωτικών και όπλων, της δωροδοκίας και της απάτης. Ως μέσο επίτευξης επιλέγεται η στενότερη συνεργασία μεταξύ εθνικών αστυνομικών και άλλων αρμοδίων εθνικών αρχών, τόσο απ' ευθείας όσο και μέσω της Europol, καθώς και η στενότερη συνεργασία μεταξύ δικαστικών και άλλων αρμοδίων αρχών των κρατών μελών, συμπεριλαμβανομένης της συνεργασίας μέσω της Eurojust (αρθ. 29 ΣΕΕ). Η τελευταία αναλαμβάνει την ενίσχυση της συνεργασίας μεταξύ των αρμόδιων υπουργείων και των δικαστικών αρχών. Ο ρόλος αυτός ενθαρρύνεται από το Συμβούλιο καθώς επιτρέπει στην Eurojust να συμβάλλει στον αποτελεσματικό συντονισμό μεταξύ των εθνικών διωκτικών αρχών των κρατών μελών, ευνοεί τη συμμετοχή της Eurojust στις έρευνες σχετικά με θέματα σοβαρής διασυνοριακής εγκληματικότητας, ιδίως στην περίπτωση του οργανωμένου εγκλήματος, λαμβανομένων μεταξύ άλλων υπόψη των αναλύσεων που πραγματοποιεί η Europol και διευκολύνει τη στενή συνεργασία της Eurojust με το ευρωπαϊκό δικαστικό δίκτυο κυρίως στην εκτέλεση αιτήσεων δικαστικής συνδρομής και αιτήσεων έκδοσης (αρθ. 31 παρ.2 ΣΕΕ).

Κάνοντας έναν σύντομο απολογισμό για τη Συνθήκη της Νίκαιας αναφορικά με το πεδίο του τρίτου πυλώνα, συμπεραίνεται ότι η συμβολή στην εξέλιξη των πολιτικών του συγκεκριμένου πεδίου είναι θετική προς δύο κατευθύνσεις. Αφενός αναθέτει στην Eurojust τον ρόλο του συντονιστή της καταπολέμησης του οργανωμένου εγκλήματος στην ΕΕ, αφετέρου ενισχύει και διευκολύνει την εφαρμογή του μηχανισμού της ενισχυμένης συνεργασίας, καθώς δεν επιτρέπει πλέον σε ένα κράτος μέλος να αντιτάσσεται στη θέσπιση ενισχυμένης συνεργασίας, όπως προέβλεπε η Συνθήκη του Άμστερνταμ. Με τον τρόπο αυτό γίνεται πιο εφικτή μία ελαστικότερη πορεία προς την εξέλιξη

[14] Δελτίο ΕΕ 10-1999, σημ. Ι.14.46.

των πολιτικών του τρίτου πυλώνα (αρθ. 40 ΣΕΕ). Στα αρνητικά της Συνθήκης μπορούμε να επισημάνουμε ότι το νομικό πλαίσιο για το μεγαλύτερο μέρος της ποινικής νομοθεσίας χαρακτηρίζεται από μία σειρά αδυναμιών, όπως απαίτηση ομοφωνίας, διαβούλευση μόνο με το Ευρωπαϊκό Κοινοβούλιο και ανυπαρξία διαδικασίας επί παραβάσει ενώπιον του ΔΕΚ με σκοπό τον έλεγχο της προσήκουσας εφαρμογής από μέρους των κρατών μελών των διατάξεων του τρίτου πυλώνα. Ωστόσο, ακόμα και μετά τη Συνθήκη της Νίκαιας, δεν εφαρμόζεται κανένα σχέδιο ενισχυμένης συνεργασίας.

1.1.3 Η Συνθήκη της Λισαβόνας

Η Συνθήκη της Λισαβόνας επέφερε κρίσιμες αλλαγές σε ό, τι αφορά τη δημιουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης. Η έννοια του Χώρου, απροσδιόριστη σε όλες τις εκφάνσεις της, καταλείπει ευρέα περιθώρια διάπλασης στα ενωσιακά όργανα. Αυτή τη διάπλαση διευκολύνει πλέον αισθητά η Συνθήκη της Λισαβόνας, αφού εντάσσει τα θέματα του Χώρου στον κανόνα της συνήθους νομοθετικής διαδικασίας, καταργώντας το πυλωνικό σύστημα. Το σύστημα αυτό δυσχέραινε σε σημαντικό βαθμό τη λήψη αποφάσεων, ιδίως στους τομείς της δικαστικής συνεργασίας σε ποινικές υποθέσεις και την αστυνομική συνεργασία[15].

Η πλέον θεαματική και ταυτόχρονα ουσιώδης αλλαγή στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης αφορά προφανώς στην κατάργηση των πυλώνων. Την κατάργηση αυτή προέβλεπε και η Συνταγματική Συνθήκη, μία κρίσιμη επιλογή που διατηρήθηκε και στη Συνθήκη της Λισαβόνας.[16] Ο τρίτος πυλώνας, από τον οποίο προβλεπόταν η δημιουργία του Χώρου σε μεγάλο βαθμό, αφού σε αυτόν είχε προβλεφθεί η αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις, καταργείται.

Η διχοτόμηση[17] των σχετικών ρυθμίσεων που είχε προβλεφθεί με τη Συνθήκη του Άμστερνταμ, όπου τα υπόλοιπα θέματα που εντάσσονταν στη δημιουργία του Χώρου είχαν ενταχθεί στον πρώτο πυλώνα, διασπούσε την ενότητα των σχετικών ρυθμίσεων και συνέβαλε αρνητικά στο αίτημα για διαφάνεια και απλοποίηση του ευρωπαϊκού οικοδομήματος. Πέραν αυτού, οι διαφοροποιήσεις ως προς την τυπολογία των ενωσιακών πράξεων, την ένταση του δικαστικού ελέγχου και τη συμμετοχή των ενωσιακών οργάνων, οι ειδικότερες ρυθμίσεις για το κεκτημένο του Schengen με τη μη συμμετοχή κρατών μελών, αλλά και με τη συμμετοχή μη κρατών μελών, συνέτειναν στη δημιουργία ενός αληθινού χάους, ενός κυκεώνα ρυθμίσεων.

Καθώς πια οι πυλώνες καταργούνται, όλα τα θέματα που ανάγονται στη δημιουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης εντάσσονται στον κανόνα, στην κοινοτική μέθοδο και οργανώνονται σε πέντε κεφάλαια υπό τον γενικό τίτλο V, που φέρει ως επικεφαλίδα «Ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης», όπου το Κεφάλαιο 1 έχει ως αντικείμενο «Γενικές Διατάξεις», το Κεφάλαιο 2 «Πολιτικές σχετικά με τους ελέγχους στα σύνορα, το άσυλο και τη μετανάστευση», το Κεφάλαιο 3 την «Δικαστική συνεργασία σε αστικές υποθέσεις», το Κεφάλαιο 4 την

[15] Παπαγιάννης Δον., Ο χώρος ελευθερίας, ασφάλειας και δικαιοσύνης μετά τη Συνθήκη της Λισαβόνας, ΕΕΕυρΔ 3:2010, σελ. 345

[16] Βλ. σχετ. Schiffauer P., Zum Verfassungzustand der Europaischen Union nach Unterzeichnung des Vertrages von Lissabon , EuGRZ (2008), σελ.1

[17] Muller – Graff P.Chr (Hrsg.) Der Raum der Freiheit, der Sicherheit und des Rechts, 2005, S.Peers, EU Justice and Home Affairs 2. Aufl. (2006).

«Δικαστική προστασία σε ποινικές υποθέσεις» και το Κεφάλαιο 5 την «Αστυνομική συνεργασία».

Με το νέο άρθρο 67 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) οργανώνονται συνολικά οι γενικές στοχεύσεις των πολιτικών, μέσω των οποίων επιχειρείται η δημιουργία του Χώρου. Σύμφωνα με αυτό «*Η Ένωση συγκροτεί Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης, με σεβασμό των θεμελιωδών δικαιωμάτων και των διαφορετικών νομικών συστημάτων και παραδόσεων των κρατών μελών*».

Οι επιμέρους τρεις επόμενες παράγραφοι του εν λόγω άρθρου προσδιορίζουν τις γενικές επιδιώξεις σε τρεις τομείς, στον τομέα ελεύθερης διακίνησης των προσώπων, της ασφάλειας και της πρόσβασης στη δικαιοσύνη. Αναφορικά με τον πρώτο τομέα, *η Ένωση εξασφαλίζει την απουσία ελέγχων των προσώπων στα εσωτερικά σύνορα και αναπτύσσει κοινή πολιτική ασύλου, της μετανάστευσης και του ελέγχου των εξωτερικών συνόρων, η οποία βασίζεται στην αλληλεγγύη μεταξύ των κρατών μελών και είναι δίκαιη έναντι των υπηκόων τρίτων χωρών.*

Στον τομέα της Ασφάλειας, η ένωση καταβάλλει προσπάθεια για να εξασφαλίζει υψηλό επίπεδο προσπάθειας με τη θέσπιση μέτρων πρόληψης και καταπολέμησης της εγκληματικότητας, του ρατσισμού και της ξενοφοβίας, μέτρων συντονισμού και συνεργασίας μεταξύ αστυνομικών και δικαστικών αρχών και των λοιπών αρμοδίων αρχών καθώς και με την αμοιβαία αναγνώριση των δικαστικών αποφάσεων σε ποινικές υποθέσεις και, εάν χρειάζεται, την προσέγγιση των ποινικών νομοθεσιών.

Τέλος, η Ένωση διευκολύνει την πρόσβαση στη δικαιοσύνη, ιδίως με την αρχή της αμοιβαίας αναγνώρισης των δικαστικών και εξώδικων αποφάσεων σε αστικές υποθέσεις.

Η κατάργηση των πυλώνων έχει ως αποτέλεσμα να ισχύει πλέον και για τα θέματα του Χώρου η συνήθης νομοθετική διαδικασία με την έκδοση ενωσιακών πράξεων, όπως Κανονισμού, Οδηγίας και Απόφασης.

Η συνολική αναδιατύπωση διάσπαρτων πολιτικών και στοχεύσεων που παρατηρούνταν στο προηγούμενο καθεστώς υπό τη Συνθήκη του Άμστερνταμ αποτελεί αναμφίβολα πρόοδο, καθιστά την Ένωση αποτελεσματικότερη στην αντιμετώπιση των ευαίσθητων αυτών θεμάτων. Η ρύθμιση είναι πλέον προφανώς πιο διαφανής και πιο απλή.

Ευκρίνεια ικανοποιητικού βαθμού αποκτάται και ως προς την ακριβή φύση της αρμοδιότητας που αναγνωρίζεται στην Ένωση. Σύμφωνα με το άρθρο 4 παρ. 2 ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης ανάγεται στις συντρέχουσες αρμοδιότητες της Ένωσης. Άμεση συνέπεια αυτού του ρητού χαρακτηρισμού της συγκεκριμένης αρμοδιότητας ως συντρέχουσας είναι η εφαρμογή της αρχής της επικουρικότητας και κατ' επέκταση η εμπλοκή των εθνικών κοινοβουλίων.

Οι αλλαγές που φέρει η Συνθήκη της Λισαβόνας ως προς τις κατ' ουσία ρυθμίσεις του Χώρου, μολονότι δεν θα μπορούσαν να χαρακτηριστούν ως θεαματικές, είναι παρά ταύτα σημαντικές. Το μεγάλο πλεονέκτημα εντοπίζεται στην αντιμετώπιση των

εν λόγω πολιτικών, οι οποίες ενώ με το προϊσχύσαν καθεστώς[18] αντιμετωπίζονταν αποσπασματικά και πιο εξειδικευμένα, πλέον διαθέτουμε μια συνολική θεώρηση των σχετικών πολιτικών και μια προσπάθεια για συνολική αντιμετώπιση των αναφυόμενων προβλημάτων. Έτσι, η νέα Συνθήκη δεν διστάζει να χρησιμοποιήσει τους όρους «κοινή πολιτική» συνολικά για το άσυλο, την μεταναστευτική πολιτική, την επικουρική προστασία, την προσωρινή προστασία.

Ειδικά ως προς τους ελέγχους στα σύνορα, η πολιτική της Ένωσης στοχεύει στην εξάλειψη των ελέγχων στα εσωτερικά σύνορα και την αποτελεσματική εποπτεία και ο έλεγχος κατά τη διέλευση των εξωτερικών συνόρων. Ο απώτερος στόχος εδώ είναι η προοδευτική δημιουργία ενός ολοκληρωμένου συστήματος διαχείρισης εξωτερικών συνόρων.

Συνολική προβλέπεται πλέον η ανάπτυξη της κοινής πολιτικής στους τομείς του ασύλου, όπως επίσης της επικουρικής και προσωρινής προστασίας, με στόχο να παρέχεται το κατάλληλο καθεστώς σε οποιονδήποτε υπήκοο τρίτης χώρας χρήζει διεθνούς προστασίας. Ως βασικός στόχος εδώ αναδεικνύεται η δημιουργία ενός ενιαίου καθεστώτος ασύλου για τους υπηκόους τρίτων χωρών. Σύμφωνα μάλιστα με το άρθρο 78 παρ.3 ΣΛΕΕ, σε περίπτωση που κράτος μέλος αντιμετωπίζει επείγουσα κατάσταση λόγω αιφνίδιας εισροής υπηκόων τρίτων χωρών, μπορούν να ληφθούν από την πλευρά της Ένωσης προσωρινά μέτρα.

Ρητά προβλέπεται πλέον και η «μεταναστευτική πολιτική» ως κοινή πολιτική της Ένωσης.[19] Αξιοσημείωτη είναι η ρύθμιση του άρθρου 79 παρ. 4 ΣΛΕΕ, κατά την οποία, με βάση τη συνήθη νομοθετική διαδικασία μπορούν να θεσπίζονται μέτρα ενθάρρυνσης και στήριξης δράσεων των κρατών μελών που στοχεύουν στη διευκόλυνση ένταξης των υπηκόων τρίτων χωρών και οι οποίοι διαμένουν νόμιμα στο έδαφος τους. Σε κάθε περίπτωση πάντως δεν θίγεται το δικαίωμα των κρατών μελών να ορίζουν αποκλειστικά μόνα τους τον όγκο των εισερχομένων υπηκόων τρίτων χωρών στο έδαφος τους για αναζήτηση εργασίας.

Βασική αρχή που πλαισιώνει το σύνολο αυτών των πολιτικών συνιστά η αρχή της αλληλεγγύης και της δίκαιης κατανομής των ευθυνών μεταξύ των κρατών μελών και στο οικονομικό επίπεδο, οι οποίες ορίζονται ρητά στο άρθρο 80 ΣΛΕΕ.

Η δικαστική συνεργασία σε αστικές υποθέσεις διέπεται από τη βασική αρχή της *αμοιβαίας αναγνώρισης των δικαστικών και εξωδίκων αποφάσεων*, η οποία καθιερώνεται ρητά πλέον στο άρθρο 81 παρ. 1 ΣΛΕΕ. Η Συνθήκη αναδεικνύει ως πρωταρχικούς στόχους στον εν λόγω τομέα επιπρόσθετα τη διασφάλιση της ουσιαστικής πρόσβασης στη δικαιοσύνη, την ανάπτυξη εναλλακτικών μεθόδων επίλυσης των διαφορών, την υποστήριξη της κατάρτισης των δικαστών και των άλλων λειτουργών και υπαλλήλων του τομέα απονομής της δικαιοσύνης. Ειδικά για τα λαμβανόμενα μέτρα που έχουν διασυνοριακές επιπτώσεις και αφορούν το οικογενειακό δίκαιο προβλέπεται, όχι η συνήθης, αλλά η ειδική νομοθετική διαδικασία.

[18] Νικολακοπούλου–Στεφάνου Η., Οι πολιτικές μετανάστευσης και ασύλου της Ευρωπαϊκής Ένωσης, σε Ν. Μαραβέγια/Μ. Τσινισιζέλη (επιμ.), Η νέα Ευρωπαϊκή Ένωση. Οργάνωση και Πολιτικές, σ. 422.
[19] Στεφάνου Κ./Καταπόδης Γ. , Οι ευρωπαϊκές συνθήκες μετά την αναθεώρηση της Λισαβόνας, Εκδόσεις Σάκκουλας, (2008) σελ.24.

Ο τομέας της δικαστικής συνεργασίας σε ποινικές υποθέσεις είναι ο τομέας που υφίσταται την πλέον σημαντική μεταρρύθμιση, αφού μεταφέρεται συνολικά στον κανόνα της συνήθους νομοθετικής διαδικασίας. Η αλλαγή αυτή επέβαλε την ανάγκη να συνεκτιμώνται οι διαφορές μεταξύ των νομικών συστημάτων και παραδόσεων των κρατών μελών, κατά την έκδοση Οδηγιών με τις οποίες εναρμονίζεται η αμοιβαία αναγνώριση των δικαστικών αποφάσεων και διαταγών, κατά το άρθρο 82 παρ. 2 ΣΛΕΕ. Ωστόσο, προβλέπεται η δυνατότητα κράτους μέλους να ασκήσει βέτο και να ζητήσει να παραπεμφθεί το θέμα στο Ευρωπαϊκό Συμβούλιο.

Η Ένωση αποκτάει τέλος την αρμοδιότητα να θεσπίζει μέτρα ενθάρρυνσης στον τομέα πρόληψης του εγκλήματος, αποκλειομένης όμως της εναρμόνισης των νομοθετικών διατάξεων των κρατών μελών.

Στο άρθρο 86 ΣΛΕΕ προβλέπεται έκδοση Κανονισμού για την ίδρυση της Ευρωπαϊκής Εισαγγελίας από την Eurojust για την καταπολέμηση των αδικημάτων που θίγουν τα οικονομικά συμφέροντα της Ένωσης. Η Εισαγγελία θα είναι αρμόδια για την καταζήτηση, τη δίωξη και την παραπομπή ενώπιον της δικαιοσύνης των δραστών εις βάρος των οικονομικών συμφερόντων της Ένωσης.

Ο δεύτερος τομέας του τρίτου πυλώνα, δηλαδή η αστυνομική συνεργασία υπάγεται και αυτή πλέον στον κανόνα της συνήθους νομοθετικής διαδικασίας και τώρα πια είναι δυνατή με βάση την ειδική νομοθετική διαδικασία η θέσπιση μέτρων για την επιχειρησιακή συνεργασία μεταξύ των αρμοδίων αρχών των κρατών μελών. Ρητά επίσης προβλέπεται και η δυνατότητα ανάληψης δράσης των αστυνομικών αρχών στο έδαφος άλλου κράτους μέλους, όπου οι σχετικές προϋποθέσεις αποφασίζονται με βάση την ειδική νομοθετική διαδικασία (άρθρο 89 ΣΛΕΕ).

Σύμφωνα με το άρθρο 88 ΣΛΕΕ ο μέχρι πρότινος διεθνής οργανισμός της Europol ρυθμίζεται με Κανονισμούς και με βάση τη συνήθη νομοθετική διαδικασία, με συνέπεια να απωλέσει τον διεθνικό της χαρακτήρα και να ενταχθεί ως οργανισμός στα πλαίσια της Ένωσης. Αποστολή της είναι η στήριξη και η ενίσχυση της δράσης των αστυνομικών αρχών, καθώς και η αμοιβαία συνεργασία τους στην πρόληψη και καταπολέμηση των σοβαρών εγκλημάτων που έχουν διασυνοριακές επιπτώσεις, συμπεριλαμβανομένων των εγκλημάτων στον κυβερνοχώρο.

Εν κατακλείδι, η κατάργηση των πυλώνων είχε ευεργετικά αποτελέσματα δεδομένου ότι αποκατέστησε τη συμμετοχή των οργάνων στα κλασικά πρότυπα της «κοινοτικής λειτουργίας». Η Επιτροπή πλέον διαδραματίζει τον παραδοσιακό της ρόλο για την εκπόνηση και εκτέλεση των πολιτικών, το κοινοβούλιο ανακτά τον νομοθετικό και ελεγκτικό του ρόλο, όπως επίσης το Δικαστήριο τον δικαστικό έλεγχο.

1.2 Πολιτικό πλαίσιο της συγκρότησης του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης

Η Συνθήκη του Άμστερνταμ θέτει για πρώτη φορά μεταξύ των προτεραιοτήτων της ΕΕ τη σταδιακή ανάπτυξη ενός Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης, ικανοποιώντας τη προσδοκία των πολιτών για πλήρη ελευθερία κίνησης και δράσης μέσα σε ένα περιβάλλον ασφάλειας χωρίς συμβιβασμούς στον σεβασμό των θεμελιωδών δικαιωμάτων τους. Για την επίτευξη του στόχου αυτού δημιουργεί τις προϋποθέσεις παραγωγής κανόνων και αποτελεσματικών μέσων και μηχανισμών. Οι μετέπειτα

ενωσιακές συνθήκες εξελίσσουν τη συνεργασία στον Χώρο στηριζόμενες στο στέρεο έδαφος του κεκτημένου που είχε δημιουργηθεί από το Άμστερνταμ και ενσωματώνουν απαντήσεις στα ερωτήματα που θέτουν η εξέλιξη της ενωσιακής συνεργασίας, οι προκλήσεις από έναν συνεχώς μετεξελισσόμενο κόσμο και οι εξωγενείς παράγοντες που λόγω της εδραίωσης της παγκοσμιοποίησης επιδρούν στις προτεραιότητες της ΕΕ[20].

Η ελευθερία, ασφάλεια και δικαιοσύνη αποτελούν θεμέλιους λίθους για την επίτευξη της ευημερίας και της ειρήνης στην ΕΕ. Η οικοδόμηση της αναγκαίας ικανότητας για τη διαφύλαξη των θεμελιωδών αυτών αξιών δεν μπορεί να πραγματοποιηθεί από τη μια μέρα στην άλλη, αλλά αποτελεί ένα έργο μακρόπνοο το οποίο οφείλει να διαθέτει αφενός την τήρηση ενός αταλάντευτου προγραμματισμού για την υλοποίηση των τιθέμενων στόχων, αφετέρου την απαραίτητη ευελιξία ώστε ο ενωσιακός μηχανισμός να ανταποκρίνεται σε απρόβλεπτα γεγονότα.

Η οικοδόμηση και λειτουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης επιδιώκεται μέσα από τέσσερα διαδοχικά προγράμματα, ήτοι το Πρόγραμμα του Τάμπερε (2000-2004), το Πρόγραμμα της Χάγης (2005 – 2009), το Πρόγραμμα της Στοκχόλμης (2010 – 2014) και των Στρατηγικών Κατευθυντήριων Γραμμών (2015 – 2019). Το κάθε κείμενο χαράσσει ένα πενταετές πλάνο πολιτικής με προτεραιότητες και μετρήσιμους στόχους, οι οποίο στη συνέχεια μετατρέπονται σε πρωτοβουλίες από την Επιτροπή και ενέργειες από το Συμβούλιο. Κάθε πρόγραμμα προσπαθεί να παγιώσει τα κεκτημένα που δημιουργεί το προηγούμενο, να προάγει τη συνεργασία και να ενσωματώσει πολιτικές που εξελίσσουν αυτές του συγκεκριμένου Χώρου. Πλέον υφίσταται ένας προγραμματισμός ο οποίος καλείται να καλύψει συγκεκριμένες ανάγκες οι οποίες αξιολογούνται ως προτεραιότητες για την Ένωση. Εν τούτοις, είκοσι χρόνια σχεδόν μετά το πρώτο πρόγραμμα δράσης του Τάμπερε, οι προτεραιότητες για την ορθή λειτουργία του Χώρου παραμένουν οι ίδιες, ήτοι η οικοδόμηση ενός πραγματικού ευρωπαϊκού χώρου δικαιοσύνης και η ενίσχυση του αγώνα ενάντια σε όλες τις σοβαρές μορφές εγκληματικότητας, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο, που απειλούν την εσωτερική ασφάλεια της Ένωσης[21]. Το γεγονός αυτό μαρτυρά αφενός τη συντονισμένη προσπάθεια που απαιτείται διαρκώς για τη μεγιστοποίηση των αποτελεσμάτων της συνεργασίας μεταξύ των κρατών μελών σε τομείς που αγγίζουν τον σκληρό πυρήνα του κράτους, αφετέρου τη διαρκή μετεξέλιξη των απειλών που θέτουν σε κίνδυνο την ασφάλεια του Χώρου.

1.2.1 Το Πρόγραμμα του Τάμπερε

Ενώ η Συνθήκη του Άμστερνταμ καθορίζει ένα σαφές νομικό πλαίσιο εντός του οποίου οφείλει να αναπτυχθεί ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης, δεν προτείνει τον τρόπο και τα μέσα επίτευξης αυτού του εγχειρήματος. Το Ευρωπαϊκό Συμβούλιο, στο πλαίσιο του ρόλου του να καθορίζει τους στρατηγικούς προσανατολισμούς της ΕΕ, αναλαμβάνει αυτόν τον ρόλο. Έτσι, στο Ευρωπαϊκό Συμβούλιο του Πόρτσαχ, στις 24 και 25 Οκτωβρίου 1998, τα κράτη μέλη συμφωνούν να συγκαλέσουν μία ειδική σύνοδο η οποία θα ασχοληθεί αποκλειστικά με τη δρομολόγηση της λειτουργίας του Χώρου. Πράγματι, η σύνοδος αυτή λαμβάνει χώρα έναν χρόνο αργότερα

[20] Παπακωνσταντής Μ., Η τρομοκρατία στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης της Ευρωπαϊκής Ένωσης, Νομική Βιβλιοθήκη, (2019), σελ. 239.
[21] Conseil de l' Europeenne, Vivre dans un espace de liberte, securite et justice, ο.π., σ.11.

στις 15 και 16 Οκτωβρίου 1999 στο Τάμπερε της Φινλανδίας[22], πέντε μήνες μετά την έναρξη της ισχύος της Συνθήκης του Άμστερνταμ.

Έτσι, σε αυτή τη συνεδρίαση του Ευρωπαϊκού Συμβουλίου δόθηκε ουσιαστική ώθηση στη δημιουργία του Χώρου, όπου εκδηλώθηκε η αποφασιστικότητα να αναπτυχθεί η Ένωση ως Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης[23], στέλνοντας ένα ηχηρό πολιτικό μήνυμα για την επιβεβαίωση της πρωταρχικής σημασίας του στόχου αυτού[24]. Για την υλοποίηση, μάλιστα, της αναληφθείσας δέσμευσης αρχικά χαράσσεται μία μεθοδολογία εργασίας και, εν συνεχεία, οι επί μέρους δράσεις οι οποίες συνοδεύονται από ένα συγκεκριμένο χρονοδιάγραμμα. Παράλληλα, ζητείται από την Επιτροπή να προτείνει έναν τρόπο παρακολούθησης της επιτευχθείσας προόδου κατά την εφαρμογή των απαιτούμενων μέτρων που θα πρέπει να ληφθούν εντός μιας περιόδου πέντε ετών σύμφωνα με τα όσα καθορίζονται στη Συνθήκη του Άμστερνταμ και το Σχέδιο Δράσης της Βιέννης.

Ειδικότερα, αναφορικά με τη δημιουργία του Χώρου ασφάλειας, εκδηλώθηκε από το Ευρωπαϊκό Συμβούλιο η βούληση του να ενισχύσει την καταπολέμηση του οργανωμένου εγκλήματος, μέρος του οποίου συνιστά και το έγκλημα στον κυβερνοχώρο, σε διεθνές επίπεδο, στοχεύοντας σε μια ισορροπημένη ανάπτυξη σε όλη την Ένωση μέτρων κατά του εγκλήματος με ταυτόχρονη προστασία της ελευθερίας των πολιτών της και όσων διαμένουν σε αυτή, ενώ σχετικά με την πρόληψη του εγκλήματος στο επίπεδο της Ένωσης, κρίθηκε ότι θα πρέπει να αναπτυχθούν ανταλλαγές των βέλτιστων πρακτικών, να ενισχυθεί το δίκτυο των εθνικών αρχών που είναι αρμόδιες για την πρόληψη του εγκλήματος και να διερευνηθεί η δυνατότητα δημιουργίας ενός προγράμματος με κοινοτική χρηματοδότηση που θα αποσκοπεί στην επίτευξη των ίδιων στόχων, με έμφαση στην εγκληματικότητα των νέων, των πόλεων και την εγκληματικότητα σχετικά με τα ναρκωτικά.

Μάλιστα, απευθύνθηκε έκκληση για την άμεση σύσταση κοινών ερευνητικών ομάδων με στόχο την καταπολέμηση του λαθρεμπορίου ναρκωτικών, της εμπορίας ανθρώπων, καθώς και της τρομοκρατίας, ενώ έμφαση δόθηκε στη συμφωνία κοινών ορισμών κατηγοριών και κυρώσεων για ορισμένα εγκλήματα, όπως η εκμετάλλευση γυναικών, η σεξουαλική εκμετάλλευση παιδιών, η εμπορία ανθρώπων, η εγκληματικότητα υψηλής τεχνολογίας, η περιβαλλοντική εγκληματικότητα και το λαθρεμπόριο ναρκωτικών.

Επιπρόσθετα, καθώς κατά τη σύνοδο του Τάμπερε η Europol έχει συμπληρώσει τρεις μήνες λειτουργίας, το Ευρωπαϊκό Συμβούλιο καλεί το Συμβούλιο να της παράσχει την αναγκαία υποστήριξη και τους αναγκαίους πόρους που θα διευκολύνουν τη λειτουργία της και θα επεκτείνουν την αρμοδιότητα της στην πάταξη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, ανεξάρτητα από τον τύπο του αδικήματος από τον οποίο προέρχονται τα έσοδα. Παράλληλά αναφέρει ότι ο ρόλος της Europol θα πρέπει να ενισχυθεί με τη συλλογή επιχειρησιακών δεδομένων από τα κράτη μέλη και με την παροχή της δυνατότητας να τους ζητά να αρχίζουν να διεξάγουν ή να συντονίζουν έρευνες ή να δημιουργούν κοινές ερευνητικές ομάδες σε ορισμένους τομείς

[22] Δελτίο ΕΕ 10-1999, σημ. 1.1.-1.7.22.
[23] Elsen C., L' esprit et les ambitions de Tampere, une ere nouvelle pour la cooperation dans le domaine de la justice et les affaires interiures, RMCUE,659.
[24] Ευρωπαϊκό Συμβούλιο Tampere 1999, Συμπεράσματα Προεδρίας, βλ. και NJW 2000, 339.

εγκληματικών δραστηριοτήτων με πλήρη σεβασμό των συστημάτων δικαστικού ελέγχου των κρατών μελών.

Περαιτέρω, για την ενίσχυση του αγώνα κατά του σοβαρού οργανωμένου εγκλήματος, το Ευρωπαϊκό Συμβούλιο συμφώνησε να ιδρύσει τη Μονάδα Δικαστικής Συνεργασίας της ΕΕ (Eurojust) αποτελούμενη από εισαγγελείς, δικαστές και αξιωματικούς αστυνομίας με έργο τη διευκόλυνση του αποτελεσματικού συντονισμού των εθνικών εισαγγελικών ερευνών και την υποστήριξη των ποινικών ερευνών σε υποθέσεις οργανωμένου εγκλήματος.

Η Ευρωπαϊκή Αστυνομική Ακαδημία, γνωστή ως CEPOL, αποτελεί το δεύτερο προϊόν των εργασιών του Ευρωπαϊκού Συμβουλίου της φινλανδικής προεδρίας. Τα κράτη μέλη αποφασίζουν την ίδρυση μιας αρχής η οποία θα λειτουργεί ως δίκτυο υφισταμένων εθνικών ιδρυμάτων κατάρτισης. Ειδικότερα, η Ευρωπαϊκή Αστυνομική Ακαδημία υποστηρίζει, εφαρμόζει και συντονίζει την κατάρτιση των λειτουργιών επιβολής του νόμου, ιδίως στους τομείς της πρόληψης και της καταπολέμησης σοβαρών μορφών εγκληματικότητας, καθώς και της τρομοκρατίας.

Επιχειρώντας έναν γενικό απολογισμό του πενταετούς Προγράμματος του Τάμπερε εξάγεται το συμπέρασμα ότι η αρχική φιλοδοξία σύνταξης ενός πολυδιάστατου ολοκληρωμένου προγράμματος σταδιακά ενίοτε εξασθενεί από εμπόδια νομικού και θεσμικού χαρακτήρα, ενώ άλλες φορές λόγω ανεπαρκούς πολιτικής συμφωνίας. Τα πεδία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης συνιστούν ένα νέο κεφάλαιο στη συνεργασία των κρατών μελών και είναι αναμενόμενο ότι δεν μπορούν να αποδώσουν άμεσα καρπούς. Μέσα, όμως, από την εφαρμογή του Προγράμματος αποδεικνύεται ότι η σταδιακή προσέγγιση μεταξύ των εταίρων συνιστά μονόδρομο προκειμένου να σημειωθεί πρόοδος σε θέματα που άπτονται του σκληρού πυρήνα του κράτους.

1.2.2 Πρόγραμμα της Χάγης

Κατά τη διαδικασία της δημιουργίας του Χώρου υπό τις γενικές κατευθύνσεις που χαράχθηκαν στο Τάμπερε, παρατηρήθηκαν αστοχίες και αδικαιολόγητες καθυστερήσεις, με αποτέλεσμα το Ευρωπαϊκό Συμβούλιο του Ιουνίου 2004 να δρομολογήσει την αναζωογόνηση της οικοδόμησης του[25]. Σημειώνει μάλιστα ότι το πρόγραμμα που θα διαδεχτεί αυτό του Τάμπερε θα πρέπει να είναι ανάλογο με το μέγεθος της πρόκλησης και των προσδοκιών των Ευρωπαίων πολιτών, να είναι πρακτικό και σύμφωνο με τις εργασίες που έχουν δρομολογηθεί με βάση το Πρόγραμμα του Τάμπερε και με την αξιολόγηση των μέτρων της πρώτης γενιάς, να σέβεται τις αρχές της επικουρικότητας, της αναλογικότητας και της αλληλεγγύης και να αποτελεί πραγματική και ουσιώδη πρόοδο προς την κατεύθυνση της ενίσχυσης της αμοιβαίας εμπιστοσύνης, της προώθησης κοινών πολιτικών και της έμπρακτης συνεργασίας προς όφελος όλων των Ευρωπαίων πολιτών

Έτσι, τον Νοέμβριο του 2004 εγκρίνεται στο Ευρωπαϊκό Συμβούλιο το Πρόγραμμα της Χάγης, με το οποίο καταστρώθηκε μία συνολική στρατηγική για την ενδυνάμωση του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης. Με βάση το εν λόγω

[25] Συμβούλιο της Ευρωπαϊκής Ένωσης, Ευρωπαϊκό Συμβούλιο Βρυξελλών 17 και 18 Ιουνίου 2004, εγγρ. 10679/04, Βρυξέλλες, 18 Ιουνίου 2004.

πρόγραμμα, η Επιτροπή με Ανακοίνωση[26] της δίνει έμφαση για την προσεχή πενταετία στην ενίσχυση των θεμελιωδών δικαιωμάτων και της ιθαγένειας, στην καταπολέμηση της τρομοκρατίας, στον καθορισμό μιας ισόρροπης αντιμετώπισης της μετανάστευσης, στη θέσπιση κοινής διαδικασίας σε θέματα ασύλου, στη μεγιστοποίηση των ωφελειών από τη μετανάστευση, στη διαμόρφωση πλήρους διαχείρισης των εξωτερικών συνόρων της Ένωσης, στην επίτευξη ικανοποιητικής ισορροπίας μεταξύ της προστασίας του ιδιωτικού βίου και της ασφάλειας κατά τη διαβίβαση των πληροφοριών, στη διαμόρφωση στρατηγικής αντίληψης αναφορικά με το οργανωμένο έγκλημα, στην εγγύηση ενός πραγματικού ευρωπαϊκού χώρου δικαιοσύνης και η μέριμνα για την αλληλεγγύη.

Από τα δέκα ανωτέρω σημεία, εκείνα που ενδιαφέρουν πρωτίστως τον Χώρο αναφορικά με τον τομέα της Ασφάλειας, είναι η καταπολέμηση της τρομοκρατίας και η διαμόρφωση στρατηγικής σχετικά με το οργανωμένο έγκλημα, μέρος του οποίου συνιστά και το έγκλημα στον κυβερνοχώρο. Ως προς την καταπολέμηση της τρομοκρατίας η Επιτροπή επικεντρώνεται στην πρόληψη της τρομοκρατίας, στην ανταλλαγή πληροφοριών, στις πτυχές της στρατολόγησης και της χρηματοδότησης της, καθώς και στην ανάλυση των κινδύνων. Αναφορικά με την καταπολέμηση του οργανωμένου εγκλήματος, η Επιτροπή εστιάζει στη βελτίωση της συνεργασίας μεταξύ των υπηρεσιών επιβολής του νόμου των κρατών – μελών, όπως η αστυνομία και τα τελωνεία ως βασική προϋπόθεση για την αποτελεσματική αντιμετώπιση του. Βασικό χαρακτηριστικό των πολιτικών που περιλαμβάνονται σε αυτή την ενότητα συνιστά η αποσύνδεση του ζητήματος της ασφάλειας από τη σφαίρα της κρατικής κυριαρχίας και η αναγωγή του στο διακρατικό και το υπερκρατικό επίπεδο.

Αναφορικά με την αστυνομική συνεργασία, το Ευρωπαϊκό Συμβούλιο τονίζει ότι για την αποτελεσματική καταπολέμηση του διασυνοριακού εγκλήματος και των άλλων σοβαρών εγκλημάτων, μεταξύ των οποίων και του εγκλήματος στον κυβερνοχώρο, απαιτείται η εντατικοποίηση της συνεργασίας μεταξύ των αστυνομικών και τελωνειακών αρχών των κρατών μελών και της Europol, καθώς και η καλύτερη αξιοποίηση των σχετικών υφισταμένων μέσων. Το Ευρωπαϊκό Συμβούλιο προτρέπει τα κράτη μέλη να παράσχουν τη δυνατότητα στην Europol, σε συνεργασία με την Eurojust, να διαδραματίζει βασικό ρόλο στην καταπολέμηση του οργανωμένου εγκλήματος, μέρος του οποίου συνιστά και το έγκλημα στον κυβερνοχώρο, προβαίνοντας στην αποτελεσματική εφαρμογή των απαιτουμένων νομικών πράξεων μέχρι τα τέλη του 2004, στην έγκαιρη παροχή κάθε απαιτούμενης πληροφορίας υψηλής διαβάθμισης στην Europol και στην ενθάρρυνση της καλής συνεργασίας μεταξύ των αρμοδίων εθνικών αρχών και της Europol.

Σχετικά με τη δικαστική συνεργασία στο πλαίσιο της Eurojust, το Ευρωπαϊκό Συμβούλιο τονίζει ότι για την αποτελεσματική καταπολέμηση του οργανωμένου εγκλήματος, μέρος του οποίο είναι και το έγκλημα στον κυβερνοχώρο, απαιτείται συνεργασία και συντονισμός των ανακρίσεων και στοχευμένες διώξεις από την Eurojust με τη συνδρομή της Europol. Το Ευρωπαϊκό Συμβούλιο παροτρύνει τα κράτη μέλη να διευκολύνουν το έργο της Eurojust εφαρμόζοντας την απόφαση του Συμβουλίου για τη

[26] Ανακοίνωση της Επιτροπής στο Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο της 10ης Μαΐου 2005, «Το πρόγραμμα της Χάγης: δέκα προτεραιότητες για την προσεχή πενταετία. Μια εταιρική σχέση για την ευρωπαϊκή ανανέωση στον τομέα της ελευθερίας, της ασφάλειας και της δικαιοσύνης». COM (2005) 184 τελ.

σύσταση του εν λόγω φορέα και εξασφαλίζοντας την πλήρη συνεργασία μεταξύ των αρμόδιων εθνικών τους αρχών και της Eurojust.

Σε συνέχεια της παραπάνω Ανακοίνωσης, το Συμβούλιο και η Επιτροπή εξέδωσαν Σχέδιο Δράσης για την εφαρμογή του εν λόγω προγράμματος[27], το οποίο λειτουργεί ως πλαίσιο αναφοράς για τις εργασίες της Επιτροπής και του Συμβουλίου κατά την περίοδο 2004 – 2009.

1.2.3 Πρόγράμμα της Στοκχόλμης

Το Πρόγραμμα της Στοκχόλμης (2010 – 2014), διάδοχος των προγραμμάτων του Τάμπερε (1999 – 2004) και της Χάγης (2004 – 2009) θέτει ως προτεραιότητες στο πλαίσιο του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης, την προώθηση των δικαιωμάτων των πολιτών της Ένωσης, τη βελτίωση της καθημερινότητας τους, τη προστασία των πολιτών, την πρόσβαση στο ευρωπαϊκό χωρικό κεκτημένο, καθώς και την αλληλεγγύη σε θέματα μετανάστευσης και ασύλου.

Ως προς τη λειτουργία, λοιπόν, των θεμελιωδών δικαιωμάτων των πολιτών της Ένωσης, αναλαμβάνονται πρωτοβουλίες αναφορικά με την προσχώρηση της ΕΕ στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), ενώ παράλληλα υπογραμμίζεται η αναγκαιότητα της απόκτησης του δικαιώματος διανομής βάσει του δικαίου της ΕΕ για τους Ευρωπαίους πολίτες καθώς και τις οικογένειες αυτών, δικαίωμα που απορρέει από την άσκηση του δικαιώματος της ελεύθερης κυκλοφορίας των προσώπων. Με το εν λόγω δικαίωμα δεν στοχεύεται η καταστρατήγηση των κανόνων της μετανάστευσης εφόσον και καθόσον η ελεύθερη κυκλοφορία απαντάται σε μία αμφίδρομη σχέση τόσο δικαιωμάτων όσο και υποχρεώσεων.

Αναφορικά με τη λειτουργία της δικαστικής συνεργασίας, τονίζεται πως η αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων συνιστά θεμέλιο λίθο αυτής. Ο Χώρος Δικαιοσύνης πρέπει να επιτρέπει στους πολίτες πλήρη διεκδίκηση των δικαιωμάτων τους στην ολότητα του ευρωπαϊκού κεκτημένου με τη δέουσα διευκόλυνση τους στη πρόσβαση στη δικαιοσύνη. Σύμφωνα με το εν λόγω Πρόγραμμα επιδιώκεται περαιτέρω η δημιουργία ενός πλήρους συστήματος συγκέντρωσης αποδεικτικών στοιχείων επί υποθέσεων διασυνοριακού εγκλήματος, ενώ παράλληλα η ηλεκτρονική δικαιοσύνη (e – Justice) παρουσιάζεται ως ιδανική ευκαιρία για τη διευκόλυνση της πρόσβασης στη δικαιοσύνη[28].

Στο πεδίο της προστασίας των Ευρωπαίων πολιτών, δίνεται έμφαση στον καθορισμό και την οριοθέτηση μιας συνολικής στρατηγικής εσωτερικής ασφαλείας της ΕΕ, ενώ η παρακολούθηση, η τήρηση και η εφαρμογή καθίσταται ένα από τα κύρια καθήκοντα της Επιτροπής Εσωτερικής Ασφαλείας (ΕΕΑ). Το εν λόγω Πρόγραμμα εστιάζει στην ανάγκη δημιουργίας ευρωπαϊκής κουλτούρας κυριαρχίας του δικαίου, στην ενίσχυση της δραστηριοποίησης του μηχανισμού πολιτικής προστασίας, στην α-

[27] Σχέδιο δράσης του Συμβουλίου και της Επιτροπής για την εφαρμογή του προγράμματος της Χάγης, (ΕΕ 2005 C 198/1) και Ανακοίνωση της Επιτροπής για την εφαρμογή του προγράμματος της Χάγης και τη μελλοντική πορεία COM (2006) 331 τελ.

[28] Επίσημος Διαδικτυακός ιστότοπος Ευρωπαϊκού Χώρου Δικαιοσύνης, Ελευθερίας και Ασφάλειας, http://www.mfa.gr/ brussels / monimi – antiprosopeia – ee / ellada - sten-ee/europaikos-khoros-dikaiosunes-eleutherias-kai-asfaleia.html?page=3, (πρόσβαση 22-10-2019).

ντιμετώπιση θεμάτων «Δημόσιας Τάξης» και στη διαμόρφωση μιας ενοποιημένης πολιτικής κατά της εμπορίας ανθρώπων. Μάλιστα, έμφαση δίνεται στη βέλτιστη υλοποίηση ενός αποτελεσματικού επιπέδου συνεργασίας τόσο των αστυνομικών όσο και των δικαστικών αρχών των κρατών μελών (Europol και Eurojust), ουσιαστικότερη αξιοποίηση του EUCPN[29] (Ευρωπαϊκό Δίκτυο Πρόληψης Εγκληματικότητας), της CEPOL (Ευρωπαϊκή Αστυνομική Ακαδημία), του SaCen (Κέντρο Διαχείρισης Κρίσεων), όπως και της εφαρμογής ECRIS[30] (Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου). Ειδικότερη μνεία γίνεται και αναφορικά με τη λήψη μέτρων κατά των ναρκωτικών, της τρομοκρατίας και της παιδικής σεξουαλικής εκμετάλλευσης του ηλεκτρονικού εγκλήματος, θέμα το οποίο θα αναλύσουμε διεξοδικότερα κατωτέρω.

Αναφορικά με τη πρόσβαση στο ευρωπαϊκό χωρικό κεκτημένο, η Ένωση, ως μήτρα του δημοκρατικού πολιτεύματος και της αρχής του Κράτους Δικαίου, παρέχει διευκολύνσεις για την απρόσκοπτη πρόσβαση στην επικράτεια των κρατών μελών, πάντα με εργαλείο τα κατάλληλα μέτρα για την αντιμετώπιση της παράνομης μετανάστευσης καθώς και του διασυνοριακού εγκλήματος. Οι συνοριακοί έλεγχοι δεν θα πρέπει να εμποδίζουν την πρόσβαση σε συστήματα ασφαλείας σε άτομα που έχουν δικαίωμα να επωφεληθούν από αυτά (πχ ευρωπαϊκή ιθαγένεια). Για αυτό το σκοπό το Πρόγραμμα της Στοκχόλμης εστιάζει στην ανάγκη ενίσχυσης του ρόλου της FRONTEX[31] (επεξεργασία σαφών κοινών επιχειρησιακών διαδικασιών για τις κοινές επιχειρήσεις στη θάλασσα, συνεργασία με χώρα διέλευσης και προέλευσης) και του EUROSUR[32] (Ευρωπαϊκό Σύστημα Προστασίας Συνόρων). Ιδιαίτερη μνεία γίνεται στην έναρξη λειτουργίας του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς – SIS[33] II όπως και στη λειτουργία του Συστήματος Πληροφοριών για τις Θεωρήσεις (VIS[34]) ως κύριος στόχος του Προγράμματος.

Σχετικά με τη λειτουργία της αλληλεγγύης σε θέματα μετανάστευσης και ασύλου, λαμβάνονται υπόψη οι μακροπρόθεσμες συνέπειες της μετανάστευσης, οι οποίες συνδέονται με την κοινωνική ενσωμάτωση καθώς και στην αγορά εργασίας. Πρακτικές λύσεις αναζητούνται οι οποίες θα αποδώσουν αύξηση στην ποσόστωση της συνοχής μεταξύ της μεταναστευτικής πολιτικής και λοιπών πολιτικών (πολιτικές απασχόλησης, υγείας, εμπορίου και εκπαίδευσης). Στο Πρόγραμμα δίδεται επιπλέον έμφαση στις αρχές που περιλαμβάνονται στη σφαιρική προσέγγιση της μετανάστευσης καθώς και στο Ευρωπαϊκό Σύμφωνο για τη Μετανάστευση και το Άσυλο, ενώ τονίζεται η ανάγκη ενσωμάτωσης και υιοθέτησης της μεταναστευτικής πολιτικής στην εξωτερική πολιτική της ΕΕ. Με στόχο τη διασύνδεση της μετανάστευσης με την ανάπτυξη, προτείνεται πλαίσιο μέτρων για την ασφαλή και χαμηλού κόστους μεταφορά εμβασμάτων, για την ενεργότερη συνεργασία με εκπροσώπους της διασποράς, καθώς και την αναβάθμιση και διεύρυνση του ρόλου της κυκλικής μετανάστευσης[35]. Ως προς την έκφανση της νομίμου μετανάστευσης, το Ευρωπαϊκό Συμβούλιο αναγνωρίζει ότι η μετανάστευση εργατικού δυναμικού από μια περιοχή προς μια άλλη και η αποτελεσματική ένταξη

[29] European Crime Prevention Network
[30] European Criminal Records Information System
[31] Frontieres Exterieures (FR) – European Border and Coast Guard Agency (ENG)
[32] European Border Surveillance System
[33] Schengen Information System
[34] Visa Information System
[35] Επίσημος Διαδικτυακός ιστότοπος Ευρωπαϊκού Χώρου Δικαιοσύνης, Ελευθερίας και Ασφάλειας, http://www.mfa.gr/ brussels / monimi – antiprosopeia – ee / ellada - sten-ee/europaikos-khoros-dikaiosunes-eleutherias-kai-asfaleia.html?page=3, (πρόσβαση 22-10-2019).

των νομίμως διαμενόντων υπηκόων τρίτων χωρών δύναται να συμβάλλει στην οικονομική ανάπτυξη. Μείζονος σημασίας προτεραιότητας παραμένει η καταπολέμηση της εμπορίας ανθρώπων, η παράνομη συμπεριφορά μεταναστών, καθώς και η προστασία των ανηλίκων. Αναφορικά με το Άσυλο υπογραμμίζεται η άμεση ανάγκη στενής συνεργασίας με την Ύπατη Αρμοστεία του ΟΗΕ για τους πρόσφυγες (UNHCR)[36], καθώς και τα Προγράμματα περιφερειακής προστασίας, ενώ παράλληλα εμφαίνεται προσπάθεια ενθάρρυνσης εθελοντικής συμμετοχής των κρατών μελών της ΕΕ στο κοινό πρόγραμμα επανεγκατάστασης της ΕΕ[37].

Τέλος, στο πλαίσιο του Προγράμματος της Στοκχόλμης στο οποίο κυοφορείται η εξωτερική διάσταση του Τομέα Ελευθερίας, Ασφάλειας και Δικαιοσύνης, γίνεται επισήμανση της ανάγκης σύναψης συμφωνιών με τρίτες χώρες, ιδίως όσον αφορά στη δικαστική συνεργασία, καθώς και στον τομέα του Αστικού Δικαίου. Σε θέματα Ελευθερίας, Ασφάλειας και Δικαιοσύνης, αναφορικά με τα Δυτικά Βαλκάνια και την Τουρκία, παρουσιάζεται η δέουσα αναφορά, ενώ παράλληλα τονίζεται η σπουδαιότητα της προσφοράς της Ευρωπαϊκής Πολιτικής Γειτονίας, η οποία δύναται να λειτουργήσει με τρόπο συντονισμένο και αποτελεσματικό.

1.2.4 Οι Στρατηγικές Κατευθυντήριες Γραμμές στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης

Η Συνθήκη της Λισαβόνας ορίζει ότι η ΕΕ συγκροτεί έναν Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων. Ανατθέτει δε στο Ευρωπαϊκό Συμβούλιο να προσδιορίσει στον τομέα αυτό τις στρατηγικές κατευθυντήριες γραμμές για τον νομοθετικό και επιχειρησιακό σχεδιασμό (αρθ. 68 ΣΛΕΕ).

Έτσι, τον Ιούνιο του 2014 το Ευρωπαϊκό Συμβούλιο καθόρισε τις στρατηγικές κατευθυντήριες γραμμές στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης για την περίοδο 2015 – 2019 [38]. Οι κατευθυντήριες γραμμές βασίζονται στην πρόοδο του Προγράμματος της Στοκχόλμης και του πολυετούς προγράμματος για τη δικαιοσύνη και τις εσωτερικές υποθέσεις για την περίοδο 2010 – 2014. Με τον νέο πολιτικό προγραμματισμό δίνεται πλέον έμφαση στην εφαρμογή και στην ενοποίηση των υφιστάμενων νομικών πράξεων και των μέτρων πολιτικής που αφορούν στη λειτουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης. Το Ευρωπαϊκό Συμβούλιο εκτιμά ότι η απάντηση σε πολλές από τις προκλήσεις που αντιμετωπίζει ο Χώρος εντοπίζονται στις σχέσεις με τρίτες χώρες, γεγονός το οποίο καθιστά αναγκαία τη διασύνδεση ανάμεσα στην εσωτερική και την εξωτερική πολιτική της ΕΕ. Παράλληλα, υπογραμμίζει ότι θέματα με παγκόσμιο χαρακτήρα, όπως η μετανάστευση και το άσυλο, η καταπολέμηση της τρομοκρατίας και η προστασία των προσωπικών δεδομένων, πρέπει να αντιμετωπίζονται τόσο εντός της ΕΕ, όσο και μέσα από τις σχέσεις της τελευταίας με τις τρίτες χώρες.

---

[36] United Nations High Commissioner for Refugees

[37] Επίσημος Διαδικτυακός ιστότοπος Ευρωπαϊκού Χώρου Δικαιοσύνης, Ελευθερίας και Ασφάλειας, http://www.mfa.gr/ brussels / monimi – antiprosopeia – ee / ellada - sten-ee/europaikos-khoros-dikaiosunes-eleutherias-kai-asfaleia.html?page=3, (πρόσβαση 22-10-2019).

[38] Ευρωπαϊκό Συμβούλιο 26/27 Ιουνίου 2014 – Συμπεράσματα, εγγρ. EUCO 79/14, Βρυξέλλες, 27 Ιουνίου 2014, διαθέσιμα στον επίσημο Διαδικτυακό ιστότοπο του Ευρωπαϊκού Συμβουλίου http:// data.consilium.europa.eu/doc/document/ST-79-2014-INIT/el/pdf (πρόσβαση στις 10-11-2019).

Στο πεδίο του οργανωμένου εγκλήματος, μέρος του οποίου συνιστά και το έγκλημα στον κυβερνοχώρο, το Πρόγραμμα αναφέρει ότι επιβάλλεται μία αποτελεσματική πολιτική αντιμετώπισης, στο πλαίσιο της οποίας θα συνεργάζονται στενά όλοι οι εμπλεκόμενοι φορείς και η οποία θα ενσωματώνει τόσο τις εσωτερικές όσο και τις εξωτερικές πτυχές της καταπολέμησης του φαινομένου. Στον αγώνα κατά του οργανωμένου εγκλήματος, το Ευρωπαϊκό Συμβούλιο αναφέρει ότι η Ένωση θα πρέπει να στηρίζει τις εθνικές αρχές, κινητοποιώντας όλα τα μέσα δικαστικής και αστυνομικής συνεργασίας και ενισχύοντας τον συντονιστικό ρόλο της Europol και της Eurojust αναφορικά με την επανεξέταση και ενημέρωση της στρατηγικής της εσωτερικής ασφάλειας ως τα μέσα του 2015, στη βελτίωση της διασυνοριακής ανταλλαγής πληροφοριών και στην περαιτέρω ανάπτυξη μιας ολοκληρωμένης προσέγγισης της ασφάλειας και της εγκληματικότητας στον κυβερνοχώρο.

Μάλιστα, αναφορικά με τη διαδικτυακή τρομοκρατία που συνιστά ένα από τα εγκλήματα στο κυβερνοχώρο στο οποίο εστίασαν οι στρατηγικές κατευθυντήριες γραμμές στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης για την περίοδο 2015 – 2019, δημιουργήθηκε τον Δεκέμβριο του 2016 το Φόρουμ της ΕΕ για το διαδίκτυο με σκοπό την αντιμετώπιση του προβλήματος με το τρομοκρατικό υλικό που διακινείται μέσω του διαδικτύου. Η Μονάδα της ΕΕ για την αναφορά διαδικτυακού περιεχομένου (EU IRU) που λειτουργεί από το 2015 στο πλαίσιο της Europol συμβάλλει στη μείωση του όγκου του τρομοκρατικού υλικού που κυκλοφορεί στο διαδίκτυο.

2. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΩΣ ΑΠΕΙΛΗ ΤΟΥ ΧΩΡΟΥ ΕΛΕΥΘΕΡΙΑΣ, ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗΣ

Η ανάπτυξη της τεχνολογίας με τη δημιουργία των ηλεκτρονικών υπολογιστών και του διαδικτύου προκάλεσε την ανάπτυξη νέων μορφών εγκληματικότητας που σχετίζονται με αυτά. Τα ορισμένα - μέχρι την ενσωμάτωση των επιτευγμάτων αυτών - εγκλήματα δεν ήταν σε θέση να «καλύψουν» τα ηλεκτρονικά εγκλήματα και αυτό γίνεται εύκολα αντιληπτό εάν αναλογιστεί κανείς πως η έννοια του ηλεκτρονικού εγκλήματος παρέμενε άγνωστη. Έτσι παρουσιάστηκε η ανάγκη ορισμού του.

Έγιναν πολλές απόπειρες ορισμού του ηλεκτρονικού εγκλήματος μέχρις ότου να βρεθεί η καταλληλότερη και μεταξύ τους αυτές οι προσπάθειες διέφεραν λόγω διαφορετικής οπτικής με την οποία αντιμετωπιζόταν το πρόβλημα. Η πρώτη προσπάθεια έγινε από τον Donn Parker ο οποίος με τη μελέτη του ″Crime by Computer″ όρισε ότι «*κατάχρηση υπολογιστή συνιστά κάθε συμβάν που σχετίζεται άμεσα με την τεχνολογία των υπολογιστών κατά το οποίο ένα θύμα υπέστη ή μπορούσε να υποστεί απώλεια και ο δράστης σκόπιμα απέκτησε ή μπορούσε να αποκομίσει κέρδος*[39]». Έπειτα το 1994 οι T. Forester και P. Morisson[40] όρισαν το ηλεκτρονικό έγκλημα ως «*μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της*». Από την άλλη το 2000 ο Αγγελής[41] υιοθέτησε μία τριπλή προσέγγιση ώστε να ερμηνεύσει το ηλεκτρονικό έγκλημα. Βάσει της δικής του οπτικής το ηλεκτρονικό έγκλημα:

[39] Λάζος Γ., *«Πληροφορική και Έγκλημα»*, Νομική Βιβλιοθήκη, (2001), σελ 38 επ.
[40] Forester T. and Morisson P. (1994) , *« Computer ethics: Cautionary Tales and ethical dilemmas in computing »*, Massachusetts Institute of Technology.
[41] Αγγελής Ι, *«Διαδίκτυο και Ποινικό Δίκαιο, Έγκλημα στον Κυβερνοχώρο »* (2000), σελ. 675 επ.

• είναι μία νέα μορφή εγκλήματος η οποία λαμβάνει χώρα με τη χρήση των ηλεκτρονικών υπολογιστών

• είναι μία παραλλαγή των ήδη υπαρχόντων εγκλημάτων που τιμωρούνται από τον Ποινικό Κώδικα και άλλους ειδικούς ποινικούς νόμους με τη διαφορά ότι στην περίπτωση αυτή τα εγκλήματα διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών.

• είναι μία εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής συμμετέχει με οποιοδήποτε τρόπο.

Το 2011 οι Debarati Halder και Dr. K. Jaiskhanskar[42] όρισαν τα εγκλήματα στον κυβερνοχώρο ως τα εγκλήματα τα οποία διαπράττονται εις βάρος άλλων ατόμων με σκοπό είτε να βλάψουν τη φήμη τους είτε να προκαλέσουν σε αυτά σωματική ή ψυχική βλάβη με τη χρήση των σύγχρονων δικτύων. Η Δίωξη Ηλεκτρονικού Εγκλήματος η οποία είναι το τμήμα το οποίο αντιμετωπίζει τα ηλεκτρονικά εγκλήματα εκπροσωπώντας την Ελληνική Αστυνομία ως ηλεκτρονικό έγκλημα θεωρεί «*τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία*[43]».

Τέλος αναφορικά με τον όρο του ηλεκτρονικού εγκλήματος αξίζει να σημειωθεί ότι αυτό εκφράζεται με ποικίλους τρόπους. Αντί για τον όρο «ηλεκτρονικό έγκλημα» πολλές φορές στην ελληνική γλώσσα χρησιμοποιούνται οι όροι «διαδικτυακό έγκλημα» και «έγκλημα στον κυβερνοχώρο» ενώ οι αγγλικές ορολογίες που χρησιμοποιούνται για το ηλεκτρονικό έγκλημα είναι οι: «e-crime», «cybercrime», «computer crime», «internet related crime» και «hi-tech-crime»[44].

Ωστόσο, το ηλεκτρονικό έγκλημα διακρίνεται από το διαδικτυακό (cyber crime), καθώς το δεύτερο παρουσιάζει ποιοτικά σημαντικές διαφοροποιήσεις από το πρώτο λόγω των ιδιαίτερων χαρακτηριστικών του Διαδικτύου, που συνοψίζονται στη δυνατότητα ανταλλαγής δεδομένων και προγραμμάτων μεταξύ όλων των συνδεδεμένων υπολογιστών. Ειδικότερα, η σχέση που συνδέει το ηλεκτρονικό με το διαδικτυακό έγκλημα είναι σχέση γένους προς είδος. Το ηλεκτρονικό έγκλημα είναι έννοια γένους που περιλαμβάνει εννοιολογικά και το διαδικτυακό έγκλημα χωρίς όμως να ταυτίζεται με αυτό. Το διαδικτυακό έγκλημα είναι δηλαδή μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος.

Κατά τον ορισμό του Donn Parker «το διαδικτυακό έγκλημα ή αλλιώς κυβερνοέγκλημα (cyber-crime), είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, αυτό για την τέλεση του οποίου ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο. Σχετίζεται με την οιονδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το Διαδίκτυο».

---

[42] Halder, D. και Jaishankar K., *« Cybercrime and the Victimization of Women: Laws Rights, and Regulations »*, Hershey:IGI Global, (2011).

[43] Επίσημος Διαδικτυακός ιστότοπος βοηθητικών νομικών κειμένων/ηλεκτρονικό έγκλημα - https://www.lawspot.gr/ nomikes-plirofories/voithitika-kemena/ilektroniko-egklima (πρόσβαση στις 5-10-2019).

[44] Επίσημος Διαδικτυακός ιστότοπος Ηλεκτρονικού Εγκλήματος - https://sites.google.com / site / elektronikoenklema 2012 / ti-einai-elektroniko-enklema (πρόσβαση 5-10-2019).

2.1 Συστατικά στοιχεία του Ηλεκτρονικού Εγκλήματος

Τα ηλεκτρονικά εγκλήματα αποτελούν μία ιδιαίτερη κατηγορία εγκλημάτων λόγω των χαρακτηριστικών που τα διακρίνουν από τα κλασσικά εγκλήματα του ποινικού κώδικα. Τα γνωρίσματα αυτά είναι:

i. Η ευκολία και η ταχύτητα, στοιχεία τα οποία συνδέονται άμεσα μεταξύ τους διότι ο δράστης χωρίς καν να μετακινηθεί από το σημείο στο οποίο βρίσκεται μέσα σε ελάχιστα δευτερόλεπτα μπορεί να τελέσει κάποιο έγκλημα μέσω ηλεκτρονικού υπολογιστή και διαδικτύου με τον απλούστατο τρόπο, πατώντας πλήκτρα στον υπολογιστή του προκαλώντας ζημιά οπουδήποτε και σε οποιονδήποτε θέλει.

ii. Ο διασυνοριακός χαρακτήρας του αφού για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτείται πολλές φορές η συνεργασία περισσοτέρων του ενός κρατών δεδομένου ότι ο δράστης λόγω των ανοιχτών συνόρων του διαδικτύου μπορεί να τελέσει αξιόποινη πράξη εναντίον κάποιου που βρίσκεται σε άλλο κράτος ή ακόμα και ήπειρο. Στην περίπτωση αυτή προκαλούνται πολλές φορές προβλήματα σχετικά με τη νομιμότητα της πράξης που τελεί ο δράστης αφού αυτή μπορεί να είναι σύμφωνη με τη νομοθεσία της χώρας στην οποία βρίσκεται, ενώ ταυτόχρονα να θεωρείται παράνομη για την χώρα στην οποία είναι το θύμα, πρόβλημα που οφείλεται στις ποικίλες και διαφορετικές νομοθεσίες ανά χώρα οι οποίες δεν είναι εναρμονισμένες μεταξύ τους.

iii. Η ανωνυμία και η δυσκολία εξεύρεσης αποδεικτικών στοιχείων, αφού το διαδίκτυο είναι απρόσωπο, μέσω ορισμένων τεχνολογικών υποδομών και προγραμμάτων ελεύθερου λογισμικού χάρη στα οποία οι δράστες είτε εισβάλλουν σε δίκτυα και υπολογιστικά συστήματα ευκολότερα είτε διευκολύνονται στη διαγραφή και την καταστροφή των ιχνών τους.

iv. Οι εξειδικευμένες και διαρκώς εξελισσόμενες γνώσεις των χάκερς (hackers), οι οποίοι χάρη στην προηγμένη τεχνολογία και τα κενά που δημιουργούνται από την εξέλιξη που δεν καλύπτονται όλα με την πρώτη έκδοση που κυκλοφορεί εισβάλλουν και διαπράττουν τα ηλεκτρονικά εγκλήματα. Η διαλεύκανση αυτών των εγκλημάτων δημιουργεί νέες ανάγκες στις Αστυνομικές και Εισαγγελικές Αρχές, οι οποίες για να μπορέσουν να ακολουθήσουν τον ειρμό της σκέψης και της δράσης των δραστών ώστε να φτάσουν στην εξιχνίαση του εγκλήματος, πρέπει να διαθέτουν τουλάχιστον ίδιες γνώσεις προγραμματισμού και δικτύων με αυτούς.

2.2 Κατηγορίες Ηλεκτρονικού Εγκλήματος

Τα ηλεκτρονικά εγκλήματα διακρίνονται σε πολλές κατηγορίες βάσει των ειδικών. Η πρώτη άποψη όσον αφορά σε αυτές τις κατηγορίες διατυπώθηκε περί το 1980 από ένα ανεξάρτητο σώμα το οποίο είχε ως σκοπό από την πρώτη στιγμή της ίδρυσής του να εξακριβώσει την έκταση που είχε πάρει το ηλεκτρονικό έγκλημα τόσο στον

δημόσιο όσο και στον ιδιωτικό τομέα, την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας[45]. Αυτή διέκρινε τα εγκλήματα που τελούνται μέσω ηλεκτρονικών υπολογιστών σε οκτώ κατηγορίες:

i. Απάτη για προσωπική ωφέλεια μέσω αλλοίωσης των εισαγομένων δεδομένων με νόμιμο τρόπο, καταστροφής, συμπίεσης, ακαταλληλότητας εκροών, αλλοίωσης των δεδομένων του ηλεκτρονικού υπολογιστή, αλλοίωσης ή κακής χρήσης των προγραμμάτων με εξαίρεση τις προσβολές από τους ιούς.

ii. Κλοπή είτε δεδομένων είτε λογισμικού.

iii. Χρήση λογισμικού χωρίς άδεια, δηλαδή χρήση παράνομων αντιγράφων.

iv. Ιδιωτική εργασία μέσω της χρήσης των δυνατοτήτων των υπολογιστικών συστημάτων του οργανισμού με σκοπό την αποκομιδή κέρδους ή για προσωπικό όφελος.

v. Χάκινγκ (hacking) δηλαδή η ελεύθερη πρόσβαση σε ένα σύστημα ηλεκτρονικού υπολογιστή, η οποία κατά βάση γίνεται με τη χρήση των δυνατοτήτων επικοινωνίας.

vi. Σαμποτάζ δηλαδή η διαμεσολάβηση με τη πρόκληση ζημιάς στον τρέχοντα κύκλο ή εξοπλισμό.

vii. Εισαγωγή υλικού πορνογραφικού περιεχομένου.

viii. Ιοί δηλαδή η διάχυση ενός προγράμματος προκειμένου να ματαιωθεί η τρέχουσα εφαρμογή.

Ο Neil Barret από την άλλη περιόρισε την ανωτέρω κατηγοριοποίηση της Εξεταστικής Επιτροπής της Μ. Βρεττανίας διακρίνοντας μόνο δύο κατηγορίες[46]:

i. Τα εγκλήματα τα οποία στρέφονται κατά των ηλεκτρονικών υπολογιστών και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός ηλεκτρονικού υπολογιστή, η εισβολή σε ηλεκτρονικά αρχεία, ο ψηφιακός βανδαλισμός και η διασπορά καταστρεπτικών ιών.

ii. Τα εγκλήματα τα οποία υποστηρίζονται από ηλεκτρονικούς υπολογιστές στα οποία ανήκουν η πορνογραφία, η πειρατεία λογισμικού, οι ηλεκτρονικές απάτες και το ξέπλυμα μαύρου χρήματος μέσω διαδικτύου.

Ωστόσο, ο Αργυρόπουλος[47] διέκρινε το ηλεκτρονικό έγκλημα σε τρείς κατηγορίες:

---

[45] Furnell Steven , « Κυβερνοέγκλημα, καταστρέφοντας την κοινωνία της πληροφορίας », Εκδ. Παπαζήση, (2006), σελ. 26 - 28.
[46] https://stevinews.wordpress.com/2015/06/25/ηλεκτρονικό-έγκλημα-χάκερ-διαδίκτυο/ (Πρόσβαση 15-03-2020).
[47] Αργυρόπουλος Α. Δ. (2001), «Ηλεκτρονική εγκληματικότητα», Εκδ. Αντ. Ν. Σάκκουλα.

i. Τα εγκλήματα τα οποία διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Στην κατηγορία αυτή εντάσσονται εγκλήματα όπως είναι η συκοφαντική δυσφήμηση ή η εξύβριση που είναι δυνατό να διαπραχθεί και σε διαδικτυακό περιβάλλον όπως για παράδειγμα η ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο και η υβριστική επίθεση εις βάρος κάποιου, μέσω των μέσων κοινωνικής δικτύωσης.

ii. Τα εγκλήματα τα οποία τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς αυτός να είναι συνδεδεμένος στο διαδίκτυο. Χαρακτηριστικό παράδειγμα είναι η παράνομη αντιγραφή λογισμικού και η παράνομη πρόσβαση σε απόρρητα.

iii. Τα εγκλήματα τα οποία σχετίζονται αποκλειστικά με το διαδίκτυο. Τα εγκλήματα αυτά είναι γνωστά ως « διαδικτυακά εγκλήματα ». Συνηθισμένες επιθέσεις τέτοιου είδους είναι η διασπορά κακόβουλου λογισμικού και η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή.

Ο Donald Pipkin εν έτει 2003 αναφερόμενος στα ηλεκτρονικά εγκλήματα τα κατέταξε σε τέσσερις κατηγορίες:

i. Η πρώτη κατηγορία περιλαμβάνει τα παραδοσιακά εγκλήματα τα οποία τελούνται με τη χρήση ηλεκτρονικού υπολογιστή όπως είναι η απάτη και η κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και ηλεκτρονικής ταυτότητας.

ii. Η δεύτερη περιέχει τα ειδικά εγκλήματα των ηλεκτρονικών υπολογιστών θεωρώντας ως τέτοια την άρνηση της παροχής υπηρεσιών, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.

iii. Η τρίτη κατηγορία αφορά τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί.

iv. Η τέταρτη κατηγορία σχετίζεται με τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

Σύμφωνα με τη Διεθνή Συνθήκη για το Κυβερνοέγκλημα[48] που υπογράφηκε το 2001 ψηφιακά - ηλεκτρονικά εγκλήματα είναι:

i. Παράνομη πρόσβαση,
ii. Παράνομη υποκλοπή,
iii. Παρεμβολή σε δεδομένα,
iv. Παρεμβολή σε συστήματα,
v. Κακή χρήση συσκευών,
vi. Κλοπή που σχετίζεται με υπολογιστή,
vii. Απάτη που σχετίζεται με υπολογιστή,
viii. Παιδική πορνογραφία
ix. Κλοπή πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών.

[48] Βλ. Convention on Cybercrime, Budapest, 23.XI.2001, διαθέσιμη στον ιστότοπο http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Πρόσβαση 15-03-2020).

Η Σύμβαση για το Έγκλημα στον Κυβερνοχώρο, γνωστή ως Σύμβαση της Βουδαπέστης του 2001, χρησιμοποιεί έναν ορισμό για το κυβερνοέγκλημα που βασίζεται στο ποια εγκλήματα θα έπρεπε να συμπεριληφθούν σε αυτόν, αντί να δώσει έναν ακριβή ορισμό[49]. Σε αυτόν περιλαμβάνονται:

i. Εγκλήματα ενάντια στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα ψηφιακών δεδομένων και συστημάτων, όπως παράνομη πρόσβαση, υποκλοπή, παρέμβαση σε δεδομένα και συστήματα.

ii. Εγκλήματα που τελούνται με χρήση υπολογιστών, όπως πλαστογραφία ή απάτη με τη χρήση ηλεκτρονικών υπολογιστών.

iii. Εγκλήματα σχετικά με το περιεχόμενο, όπως πορνογραφία ανηλίκων.

iv. Εγκλήματα σχετικά με την παραβίαση πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων.

Ωστόσο, επειδή η Σύμβαση της Βουδαπέστης αφορά σε κείμενο που γράφτηκε το 2001, πολλές μορφές κυβερνοεγκλήματος που έχουν εμφανιστεί έκτοτε, δεν δύνανται να ενταχθούν στις τέσσερις προαναφερθείσες κατηγορίες.

Ως εκ τούτου, η Ευρωπαϊκή Επιτροπή το 2007 έδωσε έναν νέο ορισμό για το κυβερνοέγκλημα, στον οποίο περιλαμβάνονται τρεις μεγάλες κατηγορίες:

i. Παραδοσιακά εγκλήματα, όπως η απάτη και η πλαστογραφία, που τελούνται με τη χρήση ψηφιακών μέσων και διαμέσου δικτύων επικοινωνιών.

ii. Παράνομο περιεχόμενο που μεταδίδεται από ψηφιακά μέσα, όπως υλικό σεξουαλικής εκμετάλλευσης ανηλίκων ή ρατσιστικός λόγος.

iii. Εγκλήματα που τελούνται αποκλειστικά σε ψηφιακό περιβάλλον, όπως επιθέσεις εναντίον πληροφοριακών συστημάτων, επιθέσεις άρνησης παροχής υπηρεσιών και το hacking.

2.3 Μορφές Ηλεκτρονικού Εγκλήματος

Απαραίτητη προϋπόθεση για την τέλεση ηλεκτρονικού εγκλήματος είναι η ύπαρξη και κατ' επέκταση η χρήση συσκευής επεξεργασίας δεδομένων όπως είναι ο ηλεκτρονικός υπολογιστής, το κινητό τηλέφωνο κλπ. Ο ρόλος του ηλεκτρονικού υπολογιστή όσον αφορά τα ηλεκτρονικά εγκλήματα είναι σημαντικός καθώς:

i. μπορεί να είναι το θύμα μίας επίθεσης,

ii. μπορεί να αποτελεί το μέσο τέλεσης της επίθεσης για να επιτύχει ο δράστης τον εγκληματικό σκοπό του

iii. μπορεί να αποτελεί υποστηρικτικό μέσο για τη διάπραξη ενός εγκλήματος.

[49] Γερμανός Γ., Παπαθανασίου Αν. «Νομοθεσία για το Έγκλημα στον Κυβερνοχώρο και την Ψηφιακή Εγκληματικότητα, Εκδόσεις Σάκκουλα (2017)

Τα ηλεκτρονικά εγκλήματα εντάσσονται σε δύο κατηγορίες ανάλογα με το ρόλο που διαδραματίζει ο ηλεκτρονικός υπολογιστής:

i. τα γνήσια ηλεκτρονικά εγκλήματα η ύπαρξη των οποίων συμπίπτει με την ύπαρξη των ηλεκτρονικών υπολογιστών και του διαδικτύου, δηλαδή χωρίς αυτά δεν θα υπήρχε έγκλημα, αποτελούν «καινούριο» έγκλημα

ii τα μη γνήσια ηλεκτρονικά εγκλήματα, δηλαδή παραδοσιακά ή συμβατικά εγκλήματα που υπήρχαν ήδη πριν από την δημιουργία των ηλεκτρονικών υπολογιστών και του διαδικτύου αλλά τώρα με την παρουσία και τη συμβολή αυτών έχουν προκύψει νέοι τρόποι τέλεσής τους.

2.3.1 Γνήσια Ηλεκτρονικά Εγκλήματα[50]

Τα γνήσια ηλεκτρονικά εγκλήματα πολλές φορές εκφράζονται και με τον όρο «εγκλήματα του κυβερνοχώρου», όρος που προκύπτει από πιστή μετάφραση της αντίστοιχης αγγλικής ορολογίας «cybercrime». Θεωρείται όμως πως ο πιο ακριβής όρος για την εν λόγω κατηγορία των ηλεκτρονικών εγκλημάτων είναι ο όρος «διαδικτυακά εγκλήματα» αφού για την τέλεση τους είναι απαραίτητη η ύπαρξη και χρήση του διαδικτύου και συνεπώς και ενός υπολογιστικού συστήματος. Τα κυριότερα διαδικτυακά εγκλήματα είναι:

i. *Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε ηλεκτρονικό υπολογιστή (hacking, cracking)*

Στην περίπτωση αυτή ο δράστης έχει ως στόχο την απομακρυσμένη διαχείριση επί του επιτιθέμενου συστήματος προς επιδίωξη υποκλοπών ή άλλων παράνομων πράξεων. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει ζημιά ή να αποκομίσει οικονομικό όφελος χαρακτηρίζεται hacker ενώ σε κάθε αντίθετη περίπτωση ονομάζεται cracker.

ii. *Επιθέσεις άρνησης εξυπηρέτησης (DoS, Denial of Service)*

Με τις επιθέσεις άρνησης εξυπηρέτησης ο δράστης αποσκοπεί στην εξάντληση των πόρων ενός υπολογιστή ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό πολλές φορές συνεπάγεται τη διακοπή λειτουργίας μιας υπηρεσίας ή ακόμα και ενός συνόλου υπηρεσιών που προσφέρονται από έναν διακομιστή γεγονός που πολλές φορές προκαλεί δυσμενείς συνέπειες για έναν οργανισμό.

iii. *Κακόβουλο λογισμικό (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)*

Πρόκειται για ένα από τα πιο συνήθη ηλεκτρονικά εγκλήματα. Αφορά σε ένα πρόγραμμα ηλεκτρονικού υπολογιστή – έναν κακόβουλο κώδικα – το οποίο δημιουργείται με σκοπό να προκαλέσει ζημιά σε άλλο υπολογιστή ή να εισχωρήσει σε αυτόν με σκοπό την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τρεις επί μέρους κατηγορίες:

[50] Βλαχόπουλος Κων., *«Ηλεκτρονικό Έγκλημα: μορφές, πρόληψη, αντιμετώπιση»* Νομική Βιβλιοθήκη (2007).

α) Ιοί - Viruses: Πρόκειται για ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγράφει χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του.

β) Σκουλήκια - Worms: Προσομοιάζουν στους ιούς με τη διαφορά ότι πολλαπλασιάζονται χωρίς κάποια ενέργεια του δράστη, διαδίδονται μέσω του διαδικτύου και μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία και να στείλουν αντίγραφα[51].

γ) Δούρειοι Ίπποι – Trojan Horses: Πρόκειται για ένα πρόγραμμα ηλεκτρονικού υπολογιστή το οποίο ενώ φαίνεται ότι λειτουργεί κανονικά στην πράξη εκτελεί και άλλες αφανείς λειτουργίες με ζημιογόνα και καταστροφικά για άλλα προγράμματα και αρχεία του υπολογιστή αποτελέσματα.

iv. *Ανεπιθύμητη αλληλογραφία (spamming)*

Με τον όρο «Ανεπιθύμητη Αλληλογραφία» ή «Spam» γίνεται αναφορά στη χρήση οποιουδήποτε ηλεκτρονικού μέσου για μαζική αποστολή ανεπιθύμητων μηνυμάτων, κατά κανόνα διαφημιστικών, σε πολύ μεγάλες ποσότητες. Ο όρος αυτός χρησιμοποιείται ακόμα και για οποιοδήποτε μήνυμα που παραλαμβάνει κάποιος αρκεί να το θεωρεί ενοχλητικό.

v. *Επιθέσεις σε διαδικτυακούς τόπους*

Οι επιθέσεις σε διαδικτυακό τόπο γίνονται από τους δοκιμαζόμενους βάνδαλους και αποτελούν συνηθισμένη και διαρκώς αυξανόμενη μορφή ηλεκτρονικού εγκλήματος στις μέρες μας. Στην πράξη οι βάνδαλοι αποσκοπούν στην αλλοίωση του περιεχομένου του διαδικτυακού στόχου που είναι ο στόχος της επίθεσης με χιουμοριστικό, προπαγανδιστικό ή και προσβλητικό τρόπο. Συνήθως οι επιθέσεις σε διαδικτυακούς τόπους στρέφονται κατά κυβερνητικών οργανισμών και υπηρεσιών και τα αποτελέσματα τους είναι αναστρέψιμα αλλά απαιτείται χρόνος για την επαναφορά στην αρχική κατάσταση της ιστοσελίδας. Χαρακτηριστικό παράδειγμα της εποχής μας αποτελούν οι Anonymous οι οποίοι προβαίνουν σε διαδικτυακές επιθέσεις μεγάλης κλίμακας όπως σε κυβερνητικά δίκτυα, τράπεζες και υπηρεσίες με σκοπό την προβολή της ιδεολογίας τους και την προσωρινή διακοπή της λειτουργίας των εν λόγω ιστοσελίδων.

vi. *Πειρατεία ονομάτων χώρου (domain names piracy)*

Το φαινόμενο αυτό της πειρατείας ονομάτων χώρου παρουσιάστηκε κατά κύριο λόγο με τη δημιουργία του διαδικτύου και στην πρώτη περίοδο αυτού προτού δηλαδή προλάβουν να κατοχυρωθούν οι διευθύνσεις από τις εταιρείες. Οι επιτήδειοι προλάβαιναν τις διευθύνσεις αυτές και στη συνέχεια είτε τις πωλούσαν στις εταιρείες έναντι μεγάλων χρηματικών ποσών είτε προσποιούμενοι μία εταιρεία και αξιοποιώντας το κύρος της προέβαιναν σε προσβλητικές δημοσιεύσεις. Ο κυβερνοσφετερισμός (cybersquatting) όπως ονομάστηκε το αδίκημα αυτό στην ουσία τελείται όταν κάποιος χρήστης του διαδικτύου κατοχυρώνει για εμπορικούς λόγους το όνομα χρήστη (domain name) που περιέχει την επωνυμία μίας επιχείρησης ή το λογότυπο αυτής, προκαλώντας βλάβη στη φήμη στους όντες δικαιούχους και ενδεχομένως τον αποκλεισμό τους από το διαδίκτυο με την επωνυμία τους και πολλές φορές εάν δεν πληρώσουν

[51] Ένα από τα πιο καταστροφικά σκουλήκια ήταν το Code Red II που τον Αύγουστο του 2001 μόλυνε μέσα σε 14 ώρες 359.000 υπολογιστές προκαλώντας ζημιά κόστους μεγαλύτερου των 2 δις. δολαρίων

αστρονομικά θα έλεγε κανείς ποσά για αυτό που τους ανήκει νόμιμα δηλαδή την ιστοσελίδα τους.

vii. *Ηλεκτρονικό « ψάρεμα » (phising)*

Με το phising ή « ηλεκτρονικό ψάρεμα » επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος προκειμένου να χρησιμοποιηθούν σε άλλες παράνομες πράξεις. Τέτοιες πληροφορίες μπορεί να είναι τα στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού, κωδικοί πρόσβασης κλπ.

viii. *Πειρατεία λογισμικού*

Αυτή η μορφή ηλεκτρονικού εγκλήματος αναφέρεται στην αναπαραγωγή ή διάθεση προγραμμάτων υπολογιστή τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων χωρίς να υπάρχει γραπτή συναίνεση του δημιουργού τους. Οι κυριότερες μορφές πειρατείας λογισμικού είναι η χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της άδειας χρήσης και η πλαστογράφηση ή πλήρης απομίμηση του προϊόντος.

ix. *Πειρατεία ονομάτων χώρου*

Το φαινόμενο αυτό της πειρατείας ονομάτων χώρου παρουσιάστηκε κατά κύριο λόγο με τη δημιουργία του διαδικτύου και στην πρώτη περίοδο αυτού προτού δηλαδή προλάβουν να κατοχυρωθούν οι διευθύνσεις από τις εταιρίες. Οι επιτήδειοι προλάβαιναν τις διευθύνσεις αυτές και στη συνέχεια είτε τις πωλούσαν στις εταιρείες έναντι μεγάλων χρηματικών ποσών είτε προσποιούμενοι μία εταιρία και αξιοποιώντας το κύρος της προέβαιναν σε προσβλητικές δημοσιεύσεις. Ο κυβερνοσφετερισμός (cybersquatting) όπως ονομάστηκε το αδίκημα αυτό στην ουσία τελείται όταν κάποιος χρήστης του διαδικτύου κατοχυρώνει για εμπορικούς λόγους το όνομα χρήστη (domain name) που περιέχει την επωνυμία μίας επιχείρησης ή το λογότυπο αυτής, προκαλώντας βλάβη στη φήμη στους όντες δικαιούχους και ενδεχομένως τον αποκλεισμό τους από το διαδίκτυο με την επωνυμία τους και πολλές φορές εάν δεν πληρώσουν αστρονομικά θα έλεγε κανείς ποσά για αυτό που τους ανήκει νόμιμα δηλαδή την ιστοσελίδα τους.

x. *Εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας*

Αυτή η μορφή ηλεκτρονικού εγκλήματος αναφέρεται στη βιομηχανική κατασκοπεία και τον διαμοιρασμό περιεχομένου που προστατεύεται από τη νομοθεσία περί πνευματικής ιδιοκτησίας, χωρίς σχετική άδεια, όπως εικόνες, μουσική ή ταινίες.

xi. *Μη εξουσιοδοτημένη χρήση συστημάτων τηλεφωνικής επικοινωνίας (phreaking)*

Αυτή η μορφή ηλεκτρονικού εγκλήματος αποσκοπεί είτε στην πραγματοποίηση δωρεάν τηλεφωνικών κλήσεων, είτε στην ανώνυμη επικοινωνία μεταξύ μελών μίας εγκληματικής οργάνωσης.

xii. *Δορυφορική πειρατεία*

Αυτή η μορφή ηλεκτρονικού εγκλήματος αναφέρεται σε παράνομες αποκρυπτογραφήσεις σήματος δορυφορικών τηλεοπτικών μεταδόσεων.

2.3.2 Μη Γνήσια Ηλεκτρονικά Εγκλήματα[52]

Μη γνήσια ηλεκτρονικά εγκλήματα ονομάζονται τα εγκλήματα τα οποία δεν εμφανίστηκαν με την δημιουργία του ηλεκτρονικού υπολογιστή και του διαδικτύου αλλά υπήρχαν και πριν από αυτά όπως και σήμερα μπορούν να υπάρχουν και χωρίς να γίνονται μέσω ηλεκτρονικού υπολογιστή και διαδικτύου. Είναι τα εγκλήματα τα οποία ο Ποινικός Κώδικας τα τιμωρεί και ανεξάρτητα από την εμπλοκή του ηλεκτρονικού υπολογιστή. Στην ουσία τα μη γνήσια ηλεκτρονικά εγκλήματα χρησιμοποιούν τον υπολογιστή σαν βοηθητικό μέσο για την τέλεση των ήδη υπαρχόντων εγκλημάτων. Ο υπολογιστής χρησιμοποιείται ποικιλοτρόπως καθώς βοηθάει :

i. Στην αποθήκευση προσωπικών δεδομένων και καταστάσεων παράνομων δραστηριοτήτων

ii. Στην εύρεση και εκμαίευση πληροφοριών παράνομων δραστηριοτήτων

iii. Στη διάδοση πληροφοριών ιδιαίτερα εάν αυτές έχουν συκοφαντικό περιεχόμενο

iv. Στην ηλεκτρονική αγορά με τη χρήση κλεμμένων πιστωτικών καρτών (που κλάπηκαν με φυσικό τρόπο),

v. Στη διάδοση παράνομου οπτικοακουστικού υλικού.

Στις δύο τελευταίες χρήσεις του ο υπολογιστής συνεργάζεται με το διαδίκτυο.

Οι κυριότερες μορφές μη γνήσιων ηλεκτρονικών εγκλημάτων είναι:

i. *Η απάτη στο διαδίκτυο*

Η απάτη στο διαδίκτυο είναι η εξέλιξη της συμβατικής μορφής της απάτης διότι το αδίκημα είναι ακριβώς το ίδιο, μόνο που τελείται σε ηλεκτρονικό περιβάλλον. Το διαδίκτυο αποτελεί πρόσφορο έδαφος για τους εγκληματίες ώστε να εκμεταλλευτούν τα χαρακτηριστικά του (ανωνυμία) και να εξαπατήσουν ανυποψίαστους χρήστες του. Η απάτη στο διαδίκτυο μπορεί να τελεστεί με τους εξής τρόπους:

α. *Απάτη με e-mail:* Στην απάτη με e-mail οι δράστες παραπλανούν τους παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου και παριστάνουν ότι είναι κάποιος άλλος, συνήθως αποστολέας φαίνεται κάποια τράπεζα η οποία ζητάει επιβεβαίωση των κωδικών του e - banking του χρήστη. Οι δράστες αποσκοπούν στην εκμαίευση χρηματικών ποσών από το θύμα. Χαρακτηριστικό είναι το παράδειγμα της Νιγηριανής Απάτης όπου ο δράστης προσποιούμενος κάποιο υψηλό πρόσωπο του καθεστώτος της Νιγηρίας ζητάει από τον παραλήπτη του e-mail να τον βοηθήσει να βγάλει από τη χώρα κάποιο χρηματικό ποσό με αντάλλαγμα μέρος αυτού. Ο ανυποψίαστος παραλήπτης αφού συμφωνήσει, προβαίνει σε υπογραφή εντύπων γεγονός που καθιστά τη συμφωνία

[52] Βλαχόπουλος Κων., *«Ηλεκτρονικό έγκλημα, μορφές, πρόληψη, αντιμετώπιση»* Νομική Βιβλιοθήκη, (2007).

«μαϊμού» αξιόπιστη στα μάτια του θύματος και μετά του ζητείται η καταβολή κάποιου χρηματικού ποσού ή τα στοιχεία του λογαριασμού τραπέζης του για έξοδα μεταφοράς που προκύπτουν. Όταν το θύμα καταβάλει τα εν λόγω ποσά ή στοιχεία τότε ο δράστης εξαφανίζεται και χρεώνει τον λογαριασμού του θύματος με υπέρογκα ποσά[53].

β. *Απάτη με ιστοσελίδες:* Στην εν λόγω απάτη ιστοσελίδες που είναι όμοιες με αυτές τις οποίες παριστάνουν προσπαθούν να αντλήσουν στοιχεία του θύματος. Συχνό είναι το φαινόμενο όπου μέσω e-mail ζητείται η επιβεβαίωση στοιχείων, συνήθως τραπεζών, πατώντας σε σύνδεσμο που περιέχεται στο e-mail ο οποίος παραπέμπει σε ιστοσελίδα που προσποιείται αυτή της τράπεζας. Το περιβάλλον τόσο του e-mail όσο και της ιστοσελίδας είναι πιστό αντίγραφο του αληθινού περιβάλλοντος της τράπεζας γεγονός που καθιστά δυσδιάκριτο τον κίνδυνο που κρύβεται.

γ. *Απάτη με πιστωτικές κάρτες:* Λόγω της σημερινής οικειότητας με το διαδίκτυο, το ηλεκτρονικό εμπόριο διαρκώς αυξάνεται. Οι κακόβουλοι χρήστες του διαδικτύου εκμεταλλευόμενοι την άνθιση του ηλεκτρονικού εμπορίου και την ανωνυμία του πωλητή εξαπατούν τους αγοραστές υποκλέπτοντας τα στοιχεία της πιστωτικής κάρτας που καταχωρούν στην ιστοσελίδα από την οποία αγοράζουν. Η άντληση των στοιχείων της πιστωτικής κάρτας μπορεί να γίνει και αυτόματα μέσω ειδικής τεχνολογίας.

δ. *Απάτη με επιταγές:* Αυτή η μορφή απάτης λαμβάνει χώρα κατά κύριο λόγο σε δικτυακές δημοπρασίες στις οποίες ο δράστης-αγοραστής συμφωνεί με τον πωλητή η αγορά να γίνει μέσω επιταγής. Οι τράπεζες στις συναλλαγές με επιταγές πιστώνουν το ποσό στον πωλητή προτού ελέγξουν την γνησιότητα της επιταγής (εάν είναι πλαστή ή ακάλυπτη) ο οποίος αποστέλει το προϊόν που αγοράστηκε. Όταν η τράπεζα προβαίνει σε έλεγχο της επιταγής και διαπιστώνει ότι δεν μπορεί να εξαργυρωθεί αφαιρεί το χρηματικό ποσό που πίστωσε στον πωλητή με αποτέλεσμα αυτός πλέον να μην έχει ούτε το προϊόν ούτε τον συμφωνηθέν με τον απατεώνα αγοραστή αντίτιμό του.

ii. *Το ξέπλυμα χρήματος*

Το ξέπλυμα χρήματος είναι η διαδικασία με την οποία κάποιος αποκρύπτει χρήματα τα οποία περιήλθαν παράνομα στην κατοχή του. Ο εγκληματίας της εν λόγω περίπτωσης προσπαθεί να μετατρέψει τα παράνομα αυτά χρήματα σε όσο το δυνατόν λιγότερο ύποπτη μορφή. Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί συνήθως τρία στάδια: την τοποθέτηση, τη στρωματοποίηση και την ενσωμάτωση.

iii. *Διακίνηση πορνογραφικού υλικού – Παιδική πορνογραφία*

Η δημιουργία και η διακίνηση πορνογραφικού υλικού είναι μία διαδικασία που προϋπήρχε η οποία σήμερα διευκολύνεται μέσω του διαδικτύου. Το πορνογραφικό υλικό συναντάται σε μορφή φωτογραφιών, βίντεο και οποιαδήποτε άλλη μορφή πολυμέσων. Το διαδίκτυο βοηθά στην εξάπλωση του πορνογραφικού υλικού, καθώς οποιοσδήποτε μπορεί πολύ εύκολα να ανακτήσει πορνογραφικό υλικό και παράλληλα διευκολύνει τον εγκληματία καθώς λόγω της ανωνυμίας που του προσφέρει καθίσταται δύσκολος ο εντοπισμός του. Στην Ελλάδα σήμερα, όμως, η παιδική πορνογραφία προβληματίζει έντονα τις διωκτικές αρχές διότι διαρκώς καταγγέλλονται νέα περιστατικά

[53] Το έγκλημα αυτό ονομάζεται και « 419 » διότι τιμωρείται σύμφωνα με το Άρθρο 419 του Νιγηριανού Ποινικού Κώδικα.

τα οποία ευτυχώς προέρχονται από μεμονωμένα άτομα και όχι οργανωμένα κυκλώματα.

iv. *Διαδικτυακή τρομοκρατία*

Η διαδικτυακή τρομοκρατία είναι ένα είδος τρομοκρατίας η οποία εκδηλώνεται αποκλειστικά μέσω διαδικτύου. Η κυβερνοτρομοκρατία[54], όπως λέγεται αλλιώς, στην ουσία είναι μία μορφή ηλεκτρονικού εγκλήματος με την οποία χρησιμοποιείται το διαδίκτυο για την εκδήλωση τρομοκρατικών επιθέσεων. Ο κυβερνοπόλεμος περιλαμβάνει πολεμικές επιθέσεις ενάντια στο στρατιωτικό σώμα ενός έθνους και επιθέσεις έναντι άμαχου πληθυσμό.

v. *Επιθέσεις παρενόχλησης*

Οι επιθέσεις παρενόχλησης (cyberbullying) είναι μία εγκληματική συμπεριφορά με την οποία ο επιτιθέμενος με την χρήση ηλεκτρονικών μέσων επικοινωνίας όπως είναι δηλαδή το διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματα του για διάφορους λόγους. Τέτοιοι λόγοι μπορεί να είναι η εκδίκηση, η επίλυση προσωπικών διαφορών κ.α.

3. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΕ ΕΝΩΣΙΑΚΟ ΕΠΙΠΕΔΟ

3.1 Εξέλιξη του νομικού πλαισίου του κυβερνοεγκλήματος στην Ε.Ε.

Το κυβερνοέγκλημα ως φαινόμενο και ως αντικείμενο νομικής έρευνας προηγείται χρονικά της άνθησης του Ίντερνετ. Αξιοσημείωτη είναι η σύσταση του Συμβουλίου της Ευρώπης του 1989[55], η οποία προέβη σε βασικές διακρίσεις μεταξύ των διαφόρων μορφών έκφρασης του εγκλήματος στον κυβερνοχώρο και, κατά συνέπεια, θα μπορούσε να αναγορευτεί ως προάγγελος της Σύμβασης της Βουδαπέστης.

Πράγματι, η Σύμβαση για το έγκλημα στον κυβερνοχώρο της 23ης Νοεμβρίου 2001[56], η οποία υπογράφτηκε στη Βουδαπέστη, βασίζεται κατά ένα ουσιώδες μέρος στην ανωτέρω σύσταση. Η Σύμβαση προτείνει ένα νέο ενιαίο νομικό πλαίσιο του εγκλήματος στον κυβερνοχώρο σε διεθνές επίπεδο, αρκετά απλό και συναινετικό ώστε να μπορέσει να αποσπάσει τη συμμετοχή πολλών κρατών – μελών του Συμβουλίου της Ευρώπης και όχι μόνο. Παράλληλα, και άλλοι οργανισμοί καταπιάστηκαν με το νομικό πλαίσιο του εγκλήματος στον κυβερνοχώρο, όπως ο ΟΗΕ και ο ΟΟΣΑ.

Ωστόσο, η Σύμβαση της Βουδαπέστης για δύο λόγους συνιστά την απαρχή κάθε συζήτησης σχετικά με το έγκλημα στον κυβερνοχώρο αφενός γιατί θέτει σε διεθνές επίπεδο τις βάσεις για μια εναρμόνιση του ουσιαστικού ποινικού δικαίου της πληροφορικής, αφετέρου γιατί έχει κυρωθεί, όχι μόνο από όλα τα κράτη που είναι μέλη

[54] Το FBI ορίζει την κυβερνοτρομοκρατία ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι άμαχων στόχων από υπερεθνικές ομάδες και μυστικούς πράκτορες.
[55] Council of Europe Recommendation on computer –related crimes, No R. (89) 9, 13 Σεπτεμβρίου 1989
[56] Council of Europe, Budapest Convention on Cybercrime of 23 November 2001, CET.185.

του Συμβουλίου της Ευρώπης, αλλά και πολλά άλλα κράτη, όπως οι ΗΠΑ, ο Καναδάς, η Νότια Αφρική, η Ιαπωνία κ.α.

Στην ουσία, η Σύμβαση διακρίνει τέσσερις κατηγορίες κυβερνοεγκλημάτων: τα αδικήματα κατά του προσωπικού χαρακτήρα και της ακεραιότητας των δεδομένων και των πληροφοριακών συστημάτων, τα αδικήματα σχετικά με υπολογιστές, τα αδικήματα σχετικά με το περιεχόμενο μιας επικοινωνίας και τα αδικήματα αναφορικά με την προσβολή της διανοητικής ιδιοκτησίας. Δηλαδή, η Σύμβαση δεν αναφέρεται αποκλειστικά στο κυβερνοέγκλημα με την στενή έννοια, καθώς φιλοδοξεί να προσφέρει ένα οριζόντιο εργαλείο εναρμόνισης.

Αναφορικά με το κυβερνοέγκλημα με την στενή έννοια, διακρίνονται και ορίζονται τρία βασικά αδικήματα που αποτελούν τον πυρήνα του θέματος, ήτοι η παράνομη πρόσβαση σε πληροφοριακό σύστημα, η παράνομη παρέμβαση σε πληροφοριακό σύστημα και η παράνομη παρέμβαση σε δεδομένα. Το καθεστώς αυτό με τα τρία αδικήματα, μαζί με τα αδικήματα της υποκλοπής και της διάδοσης εργαλείων για σκοπό πειρατείας, θα υιοθετηθεί και από τον ενωσιακό νομοθέτη και θα ενσωματωθεί στο ενωσιακό δίκαιο υπό την κατηγορία των κυβερνοεπιθέσεων.

Η διαδικασία υλοποιήθηκε με την Απόφαση – Πλαίσιο 2005/222 /ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005[57]. Η νομοθεσία του 2005 είναι προφανώς εμπνευσμένη από τη Σύμβαση της Βουδαπέστης, αλλά δεν στοχεύει μόνο στην αναγνώριση της Σύμβασης σε ενωσιακό επίπεδο. Μάλιστα, ο ενωσιακός νομοθέτης είχε ήδη αρχίσει από το 2000 να μελετά την ανάγκη ενός ενιαίου πλαισίου ρύθμισης του κυβερνοεγκλήματος. Ωστόσο, από το 2008[58] έγινε αντιληπτό ότι η εξέλιξη σε τεχνολογικό επίπεδο της πειρατείας απαιτεί μία αντίστοιχη νομοθετική μεταρρύθμιση και η Απόφαση – Πλαίσιο του 2005 καταργήθηκε από την Οδηγία 2013/40/ΕΕ αναφορικά με τις «επιθέσεις κατά συστημάτων πληροφοριών»[59], η οποία και την αντικαθιστά.

3.2 Η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών[60]

Η εν λόγω Οδηγία, κατά το άρθρο 1, αποσκοπεί στην προσέγγιση και σύγκλιση του ποινικού δικαίου των κρατών – μελών στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών, ενώ με τους ορισμούς του άρθρου 2 ως σύστημα πληροφοριών νοείται η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία 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 συντήρηση τους, ορολογία που κληρονομείται από τη Σύμβαση της Βουδαπέστης. Ο νομοθέτης, μάλιστα, αποφεύγει να κάνει αναφορά σε υπολογιστές ή σε

[57] Council Framework Decision 2005/222/JHA of 24 Febraury 2005 on attacks against information systems.
[58] Commission Report to the Council on Article 12 of the Council Framework Decision of 24 Febraury 2005 on attacks against information systems.
[59] Οδηγία 2013/40/ΕΕ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.
[60] Βλ. πλήρες κείμενο της Οδηγίας στον επίσημο Διαδικτυακό ιστότοπο της Ευρωπαϊκής Ένωσης - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013L0040&from=EL (πρόσβαση 21-10-2019).

δίκτυο, παρέχοντας με τον τρόπο αυτό μια αναγκαία ευελιξία σε έναν τομέα όπου η τεχνολογική εξέλιξη δεν παύει να εκπλήσσει. Έτσι, ο χαρακτηρισμός ως σύστημα πληροφοριών δεν περιορίζεται σε ηλεκτρονικούς υπολογιστές αλλά επεκτείνεται και σε κινητά τηλέφωνα ή έξυπνες συσκευές.

Σύμφωνα με την εν λόγω Οδηγία, οι μορφές επίθεσης στο πληροφοριακό σύστημα διακρίνονται σε παράνομη πρόσβαση και παράνομη παρεμβολή. Ως εκ τούτου, στο άρθρο 3 αυτής ορίζεται ότι τα κράτη - μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις. Μάλιστα, ο ορισμός της παράνομης πρόσβασης ως παράβασης ενός μέτρου ασφαλείας συνιστά καινοτομία καθώς δεν περιλαμβανόταν στις προηγούμενες νομοθεσίες[61]. Ως εκ τούτου, αποκλείονται από το πεδίο εφαρμογής πολλές περιπτώσεις μη εξουσιοδοτημένης χρήσης οι οποίες στο παρελθόν είχαν αντιμετωπιστεί ως κυβερνοεπιθέσεις. Επίσης, άμεση συνέπεια της αναφοράς σε παραβίαση ενός πληροφοριακού συστήματος είναι ο αποκλεισμός των συστημάτων από τον θεσμό, εφόσον δεν διαθέτουν καμία μορφή τεχνικής προστασίας[62].

Αντίστοιχα, στο άρθρο 4 αυτής προστίθεται ότι τα κράτη - μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή 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, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις. Το αδίκημα της παράνομης παρεμβολής διαφέρει από το αδίκημα της παράνομης πρόσβασης σε δύο σημεία. Καταρχάς, μπορεί ο χρήστης να διαθέτει μία νόμιμη πρόσβαση ή ακόμα και να αποκτήσει πρόσβαση χωρίς πρόθεση στο σύστημα, αλλά από τη στιγμή που το χρησιμοποιεί, δηλαδή όταν εισάγει στοιχεία, αλλοιώνει την ακεραιότητα του πληροφοριακού συστήματος ή διαγράφει δεδομένα με αποτέλεσμα τη σοβαρή παρεμπόδιση ή διακοπή λειτουργίας του συστήματος πληροφοριών, διαπράττει το αδίκημα του άρθρου 4. Επιπλέον, το αδίκημα της παράνομης παρεμβολής σε σύστημα διακρίνεται από το αδίκημα της παράνομης πρόσβασης σε σύστημα καθώς σε ορισμένες περιπτώσεις μπορεί να γίνει παρεμβολή χωρίς πρόσβαση. Σε νομικό επίπεδο, κανένα εμπόδιο δεν υφίσταται για την ποινική καταστολή αυτού του φαινομένου, καθώς στην εν λόγω διάταξη προβλέπεται ότι η παρεμβολή γίνεται όχι μόνο με την εισαγωγή δεδομένων στο σύστημα, αλλά επίσης με τον αποκλεισμό της πρόσβασης στα δεδομένα.

Με την εν λόγω Οδηγία, δεν προβλέπεται μόνο προστασία του πληροφοριακού συστήματος, αλλά και των ίδιων των πληροφοριών του συστήματος. Έτσι, κατά το άρθρο 5 της Οδηγίας, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις. Περαιτέρω, με το άρθρο 6 της Οδηγίας προβλέπεται ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν

[61] Miguel P., Freitas F. & Goncalves N., Illegal access to information systems.
[62] Jougleux Philippe, Ευρωπαϊκό δίκαιο του διαδικτύου – Νομικές πτυχές του διαδικτύου στην Ευρώπη, Εκδόσεις Σάκκουλα., σελ. 116.

ότι η υποκλοπή με τεχνικά μέσα, μη δημοσίων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις. Έτσι, το αδίκημα της υποκλοπής ψηφιακών δεδομένων διαφέρει από τα αδικήματα της παράνομης επέμβασης και πρόσβασης σε σύστημα στο ότι προστατεύει ένα πολύ διαφορετικό έννομο αγαθό, την ιδιωτική ζωή.

Όσον αφορά στην παράνομη υποκλοπή, το άρθρο 6 της εν λόγω Οδηγίας προβλέπει ότι τα κράτη μέλη οφείλουν να λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι 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, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Αναφορικά με την ποινικοποίηση των προπαρασκευαστικών πράξεων, το άρθρο 7 της Οδηγίας προβλέπει ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των ανωτέρω αδικημάτων, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις: α) πρόγραμμα υπολογιστή, που έχει σχεδιαστεί ή προσαρμοστεί κατά κύριο λόγο με σκοπό τη διάπραξη οποιουδήποτε εκ των ανωτέρω αδικημάτων, β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης μέσω των οποίων δύναται να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών. Το αδίκημα διακρίνεται καθώς δεν διώκεται εδώ μια ζημιογόνος συμπεριφορά ούτε μια δραστηριότητα, η οποία είναι per se επικίνδυνη για την κοινωνία, αλλά μια συγκεκριμένη πράξη, ήτοι η διανομή εργαλείων hacking ή ιών. Με άλλα λόγια, η ποινικοποίηση αυτής της δραστηριότητας έχει ως μοναδικό σκοπό την αποτροπή και την πρόληψη των κυβερνοεπιθέσεων. Συμπληρωματικά στο άρθρο 7, το άρθρο 8 της εν λόγω Οδηγίας συμβάλλει στην πρόληψη των επιθέσεων καθώς ποινικοποιείται η *ηθική αυτουργία, υποβοήθηση και συνέργεια προς διάπραξη των ανωτέρω αδικημάτων.*

Το άρθρο 8 αναφορικά με την ηθική αυτουργία, υποβοήθηση, συνέργεια και απόπειρα προβλέπει ότι τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι η ηθική αυτουργία, ή η υποβοήθηση και η συνέργεια, προς διάπραξη των παραπάνω αδικημάτων τιμωρούνται ως ποινικό αδίκημα. Μάλιστα, τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης των ανωτέρω αδικημάτων τιμωρείται ως ποινικό αδίκημα.

Αναφορικά με τις κυρώσεις, το άρθρο 9 της Οδηγίας προβλέπει ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα ανωτέρω αδικήματα τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις και πιο συγκεκριμένα ότι τιμωρούνται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη. Σχετικά με τα αδικήματα των άρθρων 4 και 5 της Οδηγίας, που διαπράττονται εκ προθέσεως και εφόσον έχει πληγεί μεγάλος αριθμός συστημάτων πληροφοριών με τη χρήση εργαλείου αναφερόμενο στο άρθρο 7, αυτά πρέπει να τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη. Επιπλέον, αναφορικά με τα αδικήματα των άρθρων 4 και 5 τα κράτη μέλη πρέπει να εξασφαλίσουν ότι αυτά θα τιμωρούνται με

στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον είτε διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης, είτε προκαλούν σημαντικές ζημιές, είτε διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής. Τέλος, εφόσον τα αδικήματα των άρθρων 4 και 5 της εν λόγω Οδηγίας διαπράττονται με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων και ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να εξασφαλίσουν ότι το γεγονός αυτό να μπορεί να εκλαμβάνεται ως επιβαρυντική περίσταση.

Αναφορικά με την ευθύνη νομικών προσώπων, το άρθρο 10 της εν λόγω Οδηγίας προβλέπει ότι τα κράτη μέλη οφείλουν να λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τα νομικά πρόσωπα είναι δυνατόν να υπέχουν ευθύνη για τα ανωτέρω αδικήματα τα οποία έχουν τελεσθεί προς όφελός τους από οιοδήποτε πρόσωπο, ενεργώντας είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου και το οποίο κατέχει ιθύνουσα θέση εντός του νομικού αυτού προσώπου, βάσει εξουσίας εκπροσώπησης του νομικού προσώπου, εξουσίας λήψης αποφάσεων για λογαριασμό του νομικού προσώπου και εξουσίας άσκησης ελέγχου εντός του νομικού προσώπου. Μάλιστα, τα κράτη μέλη οφείλουν να λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα μπορούν να θεωρούνται υπεύθυνα οσάκις η έλλειψη εποπτείας ή ελέγχου εκ μέρους ενός από τα ανωτέρω πρόσωπα έχει επιτρέψει τη διάπραξη οποιουδήποτε εκ των ανωτέρω αδικημάτων προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που τελεί υπό την εξουσία του. Περαιτέρω, η ευθύνη των νομικών προσώπων δεν αποκλείει την ποινική δίωξη φυσικών προσώπων που είναι αυτουργοί ή ηθικοί αυτουργοί ή συνεργοί στη διάπραξη ανωτέρω αδικημάτων.

Αναφορικά με τις κυρώσεις κατά νομικών προσώπων, το άρθρο 11 της εν λόγω Οδηγίας προβλέπει *ότι* τα κράτη μέλη οφείλουν να λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 της παρούσας Οδηγίας, τιμωρείται με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και οι οποίες μπορούν να περιλαμβάνουν και άλλες κυρώσεις, όπως αποκλεισμό από δημόσιες παροχές ή ενισχύσεις, προσωρινή ή οριστική απαγόρευση της άσκησης εμπορικών δραστηριοτήτων, θέση υπό δικαστική εποπτεία, δικαστική εκκαθάριση και προσωρινό ή οριστικό κλείσιμο των εγκαταστάσεων που χρησιμοποιήθηκαν για τη διάπραξη του αδικήματος.

Σχετικά με τη δικαιοδοσία, το άρθρο 12 της εν λόγω Οδηγίας, προβλέπει ότι τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα ανωτέρω αδικήματα, εφόσον το αδίκημα έχει διαπραχθεί εν όλω ή εν μέρει στο έδαφος τους, ή από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί. Επιπλέον, προβλέπεται ότι το κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμφωνα με τα ανωτέρω, εξασφαλίζει ότι διαθέτει δικαιοδοσία, οσάκις ο δράστης διέπραξε το αδίκημα, όταν ευρίσκετο στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του, ή το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός του ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα ευρίσκετο στο έδαφός του. Περαιτέρω, προβλέπεται ότι το κράτος μέλος ενημερώνει σχετικά την Επιτροπή οσάκις αποφασίζει να θεμελιώσει δικαιοδοσία για τα ανωτέρω αδικήματα, τα οποία διαπράττονται εκτός του εδάφους του, οσάκις, μεταξύ άλλων ο δράστης του αδικήματος έχει τη συνήθη

κατοικία του στο έδαφος του, ή το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του.

Αναφορικά με την ανταλλαγή πληροφοριών, το άρθρο 13 της εν λόγω Οδηγίας προβλέπει ότι για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα ανωτέρω αδικήματα, τα κράτη μέλη εξασφαλίζουν ότι διαθέτουν ένα λειτουργικό εθνικό σημείο επαφής και κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας. Τα κράτη μέλη εξασφαλίζουν επίσης ότι διαθέτουν διαδικασίες ώστε, σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής. Επιπλέον, προβλέπεται ότι τα κράτη μέλη ενημερώνουν την Επιτροπή για το σημείο επαφής που έχουν ορίσει κατά τα αναφερόμενα ανωτέρω. Η Επιτροπή διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη και τους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης. Περαιτέρω, προβλέπεται ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να εξασφαλίσουν ότι διατίθενται οι κατάλληλοι δίαυλοι αναφοράς προκειμένου να διευκολυνθεί η υποβολή αναφορών χωρίς αδικαιολόγητη καθυστέρηση σχετικά με τα ανωτέρω αδικήματα στις αρμόδιες εθνικές τους αρχές.

Τέλος, αναφορικά με την παρακολούθηση και τις στατιστικές, το άρθρο 14 της εν λόγω Οδηγίας προβλέπει ότι τα κράτη μέλη εξασφαλίζουν ότι ένα σύστημα ευρίσκεται σε ετοιμότητα για την καταγραφή, την παραγωγή και την παροχή στατιστικών στοιχείων για τα ανωτέρω αδικήματα. Μάλιστα, τα ανωτέρω αναφερόμενα στατιστικά στοιχεία καλύπτουν κατ' ελάχιστον τα υφιστάμενα δεδομένα ως προς τον αριθμό των ανωτέρω αδικημάτων, τα οποία καταγράφονται από τα κράτη μέλη, καθώς και τον αριθμό των προσώπων τα οποία διώχθηκαν και καταδικάστηκαν για τα ανωτέρω αδικήματα. Τέλος, προβλέπεται ότι τα κράτη μέλη διαβιβάζουν στην Επιτροπή τα στοιχεία που συγκεντρώνουν σύμφωνα με τα ανωτέρω αναγραφόμενα. Η Επιτροπή μεριμνά ώστε να δημοσιεύεται και να υποβάλλεται στους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης συγκεντρωτική επισκόπηση αυτών των στατιστικών εκθέσεων.

Η εν λόγω Οδηγία αντικατέστησε την απόφαση - πλαίσιο 2005/222/ΔΕΥ και τα κράτη μέλη ανέλαβαν την υποχρέωση να την ενσωματώσουν στα εθνικά τους δίκαια έως τις 4 Σεπτεμβρίου 2015.

3.3 Η Οδηγία 2011/92/ΕΕ για την καταπολέμηση της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[63]

Μέχρι την ψηφιακή επανάσταση, η προστασία των ανηλίκων αποτελούσε ένα γνωστό αλλά από νομική άποψη εύκολο θέμα. Πράγματι, κόμικς, εφημερίδες, και τηλεοράσεις μπορούσαν να ελέγξουν το περιεχόμενο τους και οι εκδότες οι ίδιοι ευθύνονταν για τις επιλογές τους. Στο πλαίσιο αυτό, φαινόμενα όπως η παιδική πορνογραφία περιοριζόταν de facto σε πολύ ειδικούς κύκλους μετάδοσης. Αντίθετα, το διαδίκτυο συγκεντρώνει όλες τις μορφές και όλους τους τύπους επικοινωνίας σε έναν μοναδικό ιστό και, καθώς δεν νοείται να απομονωθεί και να απομακρυνθεί ο ανήλικος από αυτή

[63] Βλ. πλήρες κείμενο της Οδηγίας στον επίσημο διαδικτυακό ιστότοπο της Ευρωπαϊκής Ένωσης - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013L0040&from=EL (πρόσβαση: 25-10-2019).

την τεχνολογία, η ανεύρεση μιας αποτελεσματικής προστασίας του ανηλίκου σε τεχνικό και νομικό επίπεδο συνεχίζει να προβληματίζει τους νομοθέτες, τους οργανισμούς προστασίας και όλους τους γονείς.

Το διαδίκτυο μεταμόρφωσε εκ βάθους τον τρόπο τέλεσης του εγκλήματος. Ενώ στο παρελθόν ο εγκληματίας έκρυβε την αρρώστια του από την κοινωνία και ζούσε σε μια ψυχολογική απομόνωση, η άνθιση των κοινωνικών δικτύων είχε ως αποτέλεσμα να προσφερθεί στους παιδόφιλους η δυνατότητα δημιουργίας κύκλων. Με άλλα λόγια, το διαδίκτυο συνέβαλε στην προώθηση της δικτύωσης των παιδόφιλων με άμεση συνέπεια να ενθαρρύνονται, να αλληλοβοηθούνται και να προστατεύονται καλύτερα, καθώς οι πιο έμπειροι δίνουν συμβουλές κρυπτογράφησης στους άλλους.

Η Σύμβαση της Βουδαπέστης δημιούργησε ένα νέο ποινικό αδίκημα το οποίο ορίζει την παιδική πορνογραφία μέσω πληροφοριακού συστήματος. Η Σύμβαση ενέπνευσε τον ενωσιακό νομοθέτη να θεσπίσει ένα παρόμοιο καθεστώς με την Απόφαση Πλαίσιο 2004/68/ΔΕΥ. Η ραγδαία εξέλιξη της τεχνολογίας και η μεγαλύτερη ευαισθητοποίηση της κοινής γνώμης στους κινδύνους στους οποίους εκτίθενται οι ανήλικοι στο διαδίκτυο οδήγησε, ωστόσο, το νομοθέτη στην κατάργηση της Απόφασης – Πλαισίου, η οποία αντικαταστάθηκε από την Οδηγία 2011/92/ΕΕ της 13ης Δεκεμβρίου 2011 σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας.

Η εν λόγω Οδηγία θεσπίζει ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των κυρώσεων στον τομέα της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών, της παιδικής πορνογραφίας και της άγρας παιδιών για σεξουαλικούς σκοπούς. Σύμφωνα με τους ορισμούς του άρθρου 2 αυτής, ως παιδί χαρακτηρίζεται κάθε πρόσωπο ηλικίας κάτω των 18 ετών, ως ηλικία σεξουαλικής συναίνεσης, η ηλικία κάτω της οποίας, σύμφωνα με το εθνικό δίκαιο, απαγορεύεται η τέλεση σεξουαλικών πράξεων με παιδί, ενώ ως υλικό παιδικής πορνογραφίας ορίζεται κάθε υλικό στο οποίο απεικονίζεται παιδί να επιδίδεται σε πραγματική ή προσομοιωμένη πράξη σαφούς σεξουαλικού χαρακτήρα, καθώς και κάθε απεικόνιση των γεννητικών οργάνων παιδιού[64], προς σεξουαλικούς κυρίως σκοπούς. Δηλαδή προσφέρονται δύο εναλλακτικοί ορισμοί είτε βάσει της σεξουαλικής δραστηριότητας του παιδιού, είτε βάσει της απεικόνισης των γεννητικών οργάνων για σεξουαλικούς σκοπούς.

Σύμφωνα με το άρθρο 3, αναφορικά με τα αδικήματα σεξουαλικής κακοποίησης, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τιμωρούνται με συγκεκριμένα πλαίσια ποινών, οι εκ προθέσεως τελούμενες πράξεις του εξαναγκασμού, προς σεξουαλικούς σκοπούς, παιδιού που δεν έχει φθάσει την ηλικία σεξουαλικής συναίνεσης να γίνει μάρτυρας σεξουαλικών πράξεων και κακοποίησης, ακόμα και αν δεν συμμετέχει σε αυτές, της σεξουαλικής πράξης με παιδί που δεν έχει φθάσει την ηλικία σεξουαλικής συναίνεσης, της σεξουαλικής πράξης με παιδί, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, όταν, είτε γίνεται κατάχρηση αναγνωρισμένης θέσης εμπιστοσύνης, εξουσίας ή επιρροής επάνω στο παιδί, είτε γίνεται κατάχρηση μιας ιδιαίτερα ευάλωτης κατάστασης του παιδιού, κυρίως λόγω διανοητικής ή σωματικής αναπηρίας ή κατάστασης εξάρτησης, είτε γίνεται χρήση εξα-

[64] Βλ. άρθρο 2 της Οδηγίας 2011/92/ΕΕ.

ναγκασμού, βίας ή απειλής, καθώς και της χρήσης εξαναγκασμού, βίας ή απειλής προκειμένου να τελέσει το παιδί, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, σεξουαλική πράξη με τρίτο πρόσωπο.

Σύμφωνα με το άρθρο 4, αναφορικά με τα αδικήματα σεξουαλικής εκμετάλλευσης, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τιμωρούνται με συγκεκριμένα πλαίσια ποινών, οι εκ προθέσεως τελούμενες πράξεις της πρόκλησης της συμμετοχής παιδιού, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, σε πορνογραφικές παραστάσεις ή της στρατολόγησής του προκειμένου να συμμετάσχει σε αυτές ή της αποκόμισης κέρδους από παιδί ή της εκμετάλλευσής του με άλλους τρόπους προς τον σκοπό αυτό, της χρήσης εξαναγκασμού ή βίας προκειμένου να συμμετάσχει παιδί, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, σε πορνογραφικές παραστάσεις ή της χρήσης απειλής απέναντί του προς τον σκοπό αυτό, της εν γνώσει παρακολούθησης πορνογραφικών παραστάσεων στις οποίες συμμετέχουν παιδιά, ακόμα και αν έχουν υπερβεί την ηλικία σεξουαλικής συναίνεσης, της πρόκλησης της συμμετοχής παιδιού, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, σε παιδική πορνεία ή της στρατολόγησής του προκειμένου να συμμετάσχει σε αυτήν όπως και της αποκόμισης κέρδους από το παιδί ή της εκμετάλλευσής του με άλλους τρόπους προς τον σκοπό αυτό, της χρήσης εξαναγκασμού ή βίας προκειμένου να συμμετάσχει το παιδί, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, σε παιδική πορνεία ή της χρήσης απειλής απέναντί του προς τον σκοπό αυτό και της τέλεσης σεξουαλικών πράξεων με παιδί, ακόμα και αν έχει υπερβεί την ηλικία σεξουαλικής συναίνεσης, εάν πραγματοποιείται μέσω παιδικής πορνείας.

Αναφορικά με τα διαδικτυακά αδικήματα παιδικής πορνογραφίας, κατά το άρθρο 5 της εν λόγω Οδηγίας, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τιμωρούνται με ένα συγκεκριμένο πλαίσιο ποινών τα εκ προθέσεως αδικήματα παιδικής πορνογραφίας, ήτοι η απόκτηση ή κατοχή υλικού παιδικής πορνογραφίας, η εν γνώσει απόκτηση πρόσβασης σε παιδική πορνογραφία μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, η διανομή, διάδοση ή μετάδοση υλικού παιδικής πορνογραφίας, η προσφορά, παροχή ή διάθεση υλικού παιδικής πορνογραφίας, καθώς και η παραγωγή υλικού παιδικής πορνογραφίας.

Επιπλέον, κατά το άρθρο 6 της Οδηγίας αναφορικά με την άγρα παιδιών για σεξουαλικούς σκοπούς, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τιμωρείται με ένα συγκεκριμένο πλαίσιο ποινών η εκ προθέσεως πρόταση, μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, από μέρους ενηλίκου να συναντήσει παιδί που δεν έχει φτάσει στην ηλικία σεξουαλικής συναίνεσης, με σκοπό τη διάπραξη του αδικήματος της σεξουαλικής πράξης ή της παραγωγής υλικού παιδικής πορνογραφίας, όταν η εν λόγω πρόταση ακολουθείται από πράξεις που οδηγούν σε μια τέτοια συνάντηση, καθώς και η δια της τεχνολογίας πληροφοριών και επικοινωνιών απόπειρα διάπραξης των αδικημάτων της απόκτησης ή κατοχής υλικού παιδικής πορνογραφίας και της εν γνώσει απόκτησης πρόσβασης σε αυτή, από ενήλικα που προσεγγίζει παιδί το οποίο δεν έχει φτάσει στην ηλικία της σεξουαλικής συναίνεσης για την παραγωγή παιδικής πορνογραφίας που απεικονίζει το παιδί αυτό.

Ωστόσο, ανακύπτει το νομικό ζήτημα πως μπορεί να διευκρινιστεί ότι το άτομο που απεικονίζεται είναι όντως παιδί, ειδικά όταν ο προσδιορισμός των ηλικιών πλησίον των 18 ετών είναι δύσκολος και η διαφοροποίηση των ηλικιών δυσδιάκριτη. Το ζήτημα

αυτό προσφέρει θεωρητικά ένα ισχυρό μέσο άμυνας στον κατηγορούμενο και στην ουσία η αβεβαιότητα αυτή κινδυνεύει να εξουδετερώσει την εφαρμογή του νομικού πλαισίου. Αυτό που απασχόλησε περισσότερο είναι αν θα ισχύει η φαινομενική ή η πραγματική ηλικία. Η εν λόγω Οδηγία λύνει το θέμα αυτό οριστικά καθώς έκρινε ότι δεν αποτελεί μέτρο η πραγματική ηλικία, αλλά η εμφάνιση όταν χρειάζεται για σκοπούς καλύτερης εφαρμογής του θεσμού. Με άλλα λόγια, λαμβάνεται υπόψη η πιο μικρή ηλικία από την ηλικία που φαίνεται και την ηλικία που ισχύει στην πραγματικότητα[65].

Εν τούτοις, ο ενωσιακός νομοθέτης καταλείπει ένα περιθώριο, αφού στο άρθρο 5 της εν λόγω Οδηγίας δίνει τη διακριτική ευχέρεια στα κράτη μέλη, εάν το επιθυμούν, να καθιερώσουν ένα μέσο άμυνας όταν αποδεικνύεται ότι τελικά αυτό το άτομο που έμοιαζε με παιδί ήταν στην πραγματικότητα άνω των 18 ετών. Με τον ίδιο τρόπο, αναφορικά με την παραγωγή, απόκτηση και κατοχή πορνογραφικού υλικού, το άρθρο 8 της Οδηγίας επιτρέπει στον εθνικό νομοθέτη, να προβλέπει μια εξαίρεση στην καταστολή όταν το παιδί έχει φτάσει στην ηλικία σεξουαλικής αυτοδιάθεσης.

Ωστόσο, περιορίζει αυτό το ενδεχόμενο μέσω της καθιέρωσης κάποιων προϋποθέσεων, όπως η συγκατάθεση του παιδιού, η ιδιωτική χρήση του πορνογραφικού υλικού, στο μέτρο που οι πράξεις αυτές δεν περιλαμβάνουν οποιαδήποτε κακοποίηση.

Επιπρόσθετα, σύμφωνα με το άρθρο 8 της εν λόγω Οδηγίας αναφορικά με τις συναινετικές σεξουαλικές δραστηριότητες, εξαρτάται από τη διακριτική ευχέρεια των κρατών μελών το κατά πόσον εφαρμόζεται το άρθρο 3 της εν λόγω Οδηγίας στις συναινετικές σεξουαλικές δραστηριότητες μεταξύ προσώπων που έχουν παρόμοια ηλικία και βαθμό ψυχολογικής και σωματικής ανάπτυξης ή ωριμότητας, εφόσον οι εν λόγω πράξεις δεν περιελάμβαναν οποιαδήποτε κακοποίηση. Ομοίως, εξαρτάται από τη διακριτική ευχέρεια των κρατών μελών το κατά πόσον η παράγραφος 4 του άρθρου 4 εφαρμόζεται σε πορνογραφική παράσταση που πραγματοποιείται στο πλαίσιο συναινετικών σχέσεων εάν το παιδί έχει φθάσει την ηλικία της σεξουαλικής συναίνεσης ή μεταξύ προσώπων που έχουν παρόμοια ηλικία και βαθμό ψυχολογικής και σωματικής ανάπτυξης ή ωριμότητας, εφόσον οι πράξεις δεν συνεπάγονταν οποιαδήποτε κακοποίηση ή εκμετάλλευση και δεν προσφέρθηκαν χρήματα ή άλλου είδους ανταλλάγματα ή ανταπόδοση ως αμοιβή για την πορνογραφική παράσταση. Τέλος, εξαρτάται από τη διακριτική ευχέρεια των κρατών μελών το κατά πόσον το άρθρο 5 της εν λόγω Οδηγίας εφαρμόζεται στην παραγωγή, απόκτηση ή κατοχή υλικού στην οποία εμφανίζονται παιδιά που έχουν φθάσει την ηλικία της σεξουαλικής συναίνεσης, εφόσον η παραγωγή και κατοχή του εν λόγω υλικού πραγματοποιείται με τη συναίνεση των παιδιών αυτών και μόνο προς ιδία χρήση από τα συγκεκριμένα πρόσωπα, στον βαθμό που οι πράξεις δεν περιελάμβαναν οποιαδήποτε κακοποίηση.

Επίσης, η Οδηγία επιλύει ένα ακόμα δύσκολο νομικό ζήτημα σχετικά με τον ορισμό του υλικού παιδικής πορνογραφίας. Πράγματι, το άρθρο 2 περιλαμβάνει μια περίπτωση στον ορισμό του, σύμφωνα με την οποία υλικό παιδικής πορνογραφίας συνιστούν ρεαλιστικές εικόνες παιδιού όπου απεικονίζεται να επιδίδεται σε πράξη σαφούς σεξουαλικού χαρακτήρα ή ρεαλιστικές εικόνες των γεννητικών οργάνων παιδιού, προς σεξουαλικούς κυρίως σκοπούς. Η αναφορά στη «ρεαλιστική» εικόνα σημαίνει ότι

[65] Philippe Jougleux, Ευρωπαϊκό δίκαιο του διαδικτύου – Νομικές πτυχές του διαδικτύου στην Ευρώπη, Εκδόσεις Σάκκουλα, σελ. 145.

ενσωματώνονται στη λίστα των πορνογραφικών υλικών και πλασματικές εικόνες όπως ζωγραφιές, σκηνές ηλεκτρονικού παιχνιδιού ή κινούμενα σχέδια. Η εικονική απεικόνιση ανηλίκου έχει προβληματίσει τα δικαστήρια εφόσον σε αυτή τη περίπτωση δεν μπορεί κάποιος να ισχυριστεί ότι πρόκειται για την εκμετάλλευση πραγματικού παιδιού. Δηλαδή, στο φως της ανθρωπιστικής προσέγγισης, δεν παραβιάζεται η προσωπικότητα ενός ατόμου. Για αυτόν τον λόγο, στην Αμερική, τα δικαστήρια έχουν κρίνει ότι σε αυτή τη περίπτωση πρέπει να υπερισχύει η ελευθερία έκφρασης[66], ώστε, αντιστοίχως, να υπαναχωρήσει η ποινική καταστολή. Αντίθετα, στην ευρωπαϊκή προσέγγιση επικρατεί η αντίληψη ότι μετράει η αντικοινωνική συμπεριφορά του κατηγορουμένου και σε αυτή τη λογική είναι αδιάφορο το κατά πόσο οι εικόνες είναι πραγματικές ή πλασματικές, εφόσον πρόκειται για ρεαλιστικές εικόνες[67].

Ωστόσο, το άρθρο 5 της εν λόγω Οδηγίας περιορίζει την πλήρη εναρμόνιση του νομικού πλαισίου σε αυτό το θέμα, καθώς το αφήνει στην τελική και διακριτική εκτίμηση του εθνικού νομοθέτη. Βέβαια, ο περιορισμός αυτός εφαρμόζεται μόνο στην περίπτωση των πράξεων πρόσβασης ή παραγωγής, όταν το εικονικό υλικό έχει δημιουργηθεί για ιδιωτική χρήση και μόνο. Η διάταξη βασίζεται στην ιδέα ότι, εφόσον δεν πρόκειται για αληθινό παιδί και εφόσον δεν υπάρχει μια ενεργή επικοινωνία του υλικού που θα τροφοδοτούσε μια αγορά, η συμπεριφορά δεν ενέχει κίνδυνο για την κοινωνία και δεν δικαιολογείται πλέον η καταστολή.

Περαιτέρω, το άρθρο 9 της Οδηγίας προβλέπει κάποιες επιβαρυντικές περιστάσεις, ήτοι την εκμετάλλευση ενός ιδιαίτερα ευάλωτου παιδιού, όπως για παράδειγμα παιδιού με διανοητική ή σωματική αναπηρία, τη διάπραξη του αδικήματος από άτομο της οικογένειας ή το οποίο διαμένει στον ίδιο χώρο ή κατέχει μια θέση εξουσίας, τη διάπραξη από κοινού του αδικήματος, τη διάπραξη του αδικήματος στο πλαίσιο εγκληματικής οργάνωσης[68], την περίπτωση της υποτροπής, την περίπτωση όπου η πράξη έθεσε σε κίνδυνο τη ζωή του παιδιού, και, τέλος, όταν το αδίκημα περιελάμβανε σοβαρή βία ή προκάλεσε σοβαρή βλάβη στο παιδί.

Μάλιστα, κατά το άρθρο 10 της εν λόγω Οδηγίας, αναφορικά με την ακαταλληλότητα λόγω καταδίκης, για να αποφευχθεί ο κίνδυνος επανάληψης των αδικημάτων, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν τη δυνατότητα να επιβάλλεται σε φυσικό πρόσωπο που έχει καταδικαστεί για τα ανωτέρω αδικήματα σε προσωρινή ή μόνιμη απαγόρευση άσκησης τουλάχιστον επαγγελματικών δραστηριοτήτων που περιλαμβάνουν τακτικές επαφές με παιδιά. Επιπλέον, τα κράτη μέλη λαμβάνουν τα απαραίτητα μέτρα για να διασφαλίζουν ότι οι εργοδότες, όταν προσλαμβάνουν ένα πρόσωπο για επαγγελματικές ή οργανωμένες δραστηριότητες εθελοντικού χαρακτήρα που περιλαμβάνουν τακτικές επαφές με παιδιά, δικαιούνται να ζητούν πληροφορίες, σύμφωνα με το εθνικό δίκαιο και με κάθε πρόσφορο τρόπο, όπως η πρόσβαση κατόπιν αιτήματος ή μέσω του οικείου προσώπου, για καταχωρισμένες στο ποινικό μητρώο καταδικαστικές αποφάσεις που αφορούν σε οποιοδήποτε από τα ανωτέρω αδικήματα ή για την ύπαρξη οποιασδήποτε απαγόρευσης άσκησης δραστηριοτήτων

[66] Ο αμερικανικός νόμος κρίθηκε για αυτόν τον λόγο, και για άλλους επίσης, ως αντισυνταγματικός. Βλ. Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002) και United States v. American Library Association, 539 U.S 194 (2003).

[67] Philippe Jougleux, Ευρωπαϊκό δίκαιο του διαδικτύου – Νομικές πτυχές του διαδικτύου στην Ευρώπη, Εκδόσεις Σάκκουλα., σελ. 147.

[68] Όπως ορίζεται στην Απόφαση – Πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου, της 24ης Οκτωβρίου 2008 για την καταπολέμηση του οργανωμένου εγκλήματος.

που περιλαμβάνουν άμεσες και τακτικές επαφές με παιδιά λόγω αυτών των καταδικαστικών αποφάσεων.

Επίσης, κατά το άρθρο 11 της παρούσας Οδηγίας σχετικά με την κατάσχεση και δήμευση, τα κράτη μέλη λαμβάνουν τα απαραίτητα μέτρα ώστε να διασφαλίσουν ότι οι αρμόδιες αρχές τους έχουν τη δυνατότητα να προβαίνουν σε κατασχέσεις και δημεύσεις των οργάνων και προϊόντων που προέρχονται από τα ανωτέρω αδικήματα.

Επιπρόσθετα, σύμφωνα με το άρθρο 12 της παρούσας Οδηγίας αναφορικά με την ευθύνη των νομικών προσώπων, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι μπορούν να υπέχουν ευθύνη νομικά πρόσωπα για τα ανωτέρω αδικήματα που διαπράττονται προς όφελός τους από οποιοδήποτε πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου νομικού προσώπου και κατέχει ιθύνουσα θέση εντός του νομικού προσώπου, με βάση την εξουσία αντιπροσώπευσης του νομικού προσώπου, το δικαίωμα λήψης αποφάσεων για λογαριασμό του νομικού προσώπου και το δικαίωμα άσκησης ελέγχου εντός του νομικού προσώπου. Μάλιστα, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι μπορούν να υπέχουν ευθύνη νομικά πρόσωπα στις περιπτώσεις όπου η απουσία εποπτείας ή ελέγχου από τα ανωτέρω πρόσωπα κατέστησαν δυνατή τη διάπραξη οποιουδήποτε από τα εν λόγω αδικήματα προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που ενεργεί υπό τη δικαιοδοσία του.

Περαιτέρω, σύμφωνα με το άρθρο 13 της παρούσας Οδηγίας σχετικά με τις κυρώσεις εις βάρος νομικών προσώπων, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν την τιμωρία νομικών προσώπων που υπέχουν ευθύνη βάσει του προηγούμενου άρθρου 12 με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή διοικητικά πρόστιμα και, ενδεχομένως, άλλες κυρώσεις, όπως ο αποκλεισμός από δημόσιες παροχές ή ενισχύσεις, η προσωρινή ή οριστική απαγόρευση της άσκησης εμπορικής δραστηριότητας, η δικαστική εποπτεία, η δικαστική εκκαθάριση ή το προσωρινό ή οριστικό κλείσιμο των εγκαταστάσεων που χρησιμοποιήθηκαν για τη διάπραξη του αδικήματος.

Ωστόσο, κατά το άρθρο 14 της παρούσας Οδηγίας αναφορικά με τη μη άσκηση δίωξης ή μη επιβολή ποινών στα θύματα, τα κράτη μέλη, σύμφωνα με τις βασικές αρχές των νομικών συστημάτων τους, λαμβάνουν τα απαραίτητα μέτρα ώστε να παρέχουν στις αρμόδιες εθνικές αρχές τις εξουσίες για μη άσκηση δίωξης ή μη επιβολή ποινών σε ανήλικα θύματα σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης λόγω της συμμετοχής τους σε εγκληματικές δραστηριότητες, τις οποίες εξαναγκάστηκαν να διαπράξουν ως άμεση συνέπεια του γεγονότος ότι υπέστησαν οιαδή- ποτε των πράξεων που περιγράφονται ανωτέρω.

Επιπλέον, σύμφωνα με το άρθρο 15 της εν λόγω Οδηγίας σχετικά με την ποινική έρευνα και δίωξη, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι τα αδικήματα που περιγράφονται ανωτέρω, εφόσον έχει χρησιμοποιηθεί παιδική πορνογραφία υπό την έννοια του άρθρου 2 της εν λόγω Οδηγίας, διώκονται για ικανό χρονικό διάστημα μετά την ενηλικίωση του θύματος και ότι η δίωξη αυτή είναι ανάλογη με τη σοβαρότητα του διαπραχθέντος αδικήματος. Επίσης, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να τεθούν στη διάθεση των προσώπων, των μονάδων ή των υπηρεσιών που έχουν αρμοδιότητα διερεύνησης ή δίωξης των ανωτέρω αδικημάτων αποτελεσματικά εργαλεία έρευνας, όπως αυτά που

χρησιμοποιούνται σε περιπτώσεις οργανωμένου εγκλήματος ή άλλων σοβαρών μορφών εγκληματικότητας. Εξάλλου, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να δοθεί η δυνατότητα στις ερευνητικές μονάδες ή υπηρεσίες να επιχειρούν την ταυτοποίηση των θυμάτων των ανωτέρω αδικημάτων, ειδικότερα μέσω ανάλυσης υλικού παιδικής πορνογραφίας, όπως φωτογραφίες και οπτικοακουστικές εγγραφές που μεταδίδονται ή καθίστανται διαθέσιμες μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών.

Τέλος, το άρθρο 25 της Οδηγίας αποτελεί μία από τις πιο σημαντικές καινοτομίες στο πεδίο προστασίας του παιδιού. Η ιδέα είναι να δοθεί προτεραιότητα στην εξαφάνιση της κυκλοφορίας υλικού παιδικής πορνογραφίας στο διαδίκτυο και για αυτόν τον σκοπό δίνονται στο δικαστήριο νέες εξουσίες. Σύμφωνα με το άρθρο αυτό τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να διασφαλίζουν την κατάργηση ιστοτόπων που περιέχουν ή διαδίδουν υλικό παιδικής πορνογραφίας και φιλοξενούνται στο έδαφος τους, καθώς και να προσπαθούν να εξασφαλίζουν την κατάργηση τέτοιου είδους σελίδων που φιλοξενούνται εκτός του εδάφους τους. Παράλληλα, τα κράτη μέλη δύνανται να λάβουν μέτρα για τη φραγή της πρόσβασης σε ιστοσελίδες που περιλαμβάνουν ή διαδίδουν παιδική πορνογραφία στους χρήστες του Διαδικτύου στην επικράτεια τους. Τα μέτρα αυτά πρέπει να καθορίζονται με διαφανείς διαδικασίες και να παρέχουν επαρκείς εγγυήσεις, ειδικότερα για να εξασφαλίζεται ότι η φραγή περιορίζεται στις απαραίτητες και αναλογικές προς τον επιδιωκόμενο σκοπό ενέργειες και ότι οι χρήστες θα ενημερώνονται για τους λόγους μιας τέτοιας απαγόρευσης. Στις εν λόγω εγγυήσεις περιλαμβάνεται επίσης και η δυνατότητα άσκησης δικαστικής προσφυγής.

Όπως προαναφέρθηκε, η εν λόγω Οδηγία αντικατέστησε την Απόφαση Πλαίσιο 2004/68/ΔΕΥ, ενώ τα κράτη μέλη, κατά το άρθρο 27 αυτής, ανέλαβαν την υποχρέωση να θέσουν σε ισχύ όλες τις νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με την λόγω Οδηγία το αργότερο έως τις 18 Δεκεμβρίου 2013.

3.4 Η Οδηγία 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

Το μέγεθος, η συχνότητα και ο αντίκτυπος των συμβάντων ασφάλειας αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Τα συστήματα αυτά μπορούν επίσης να αποτελέσουν στόχο σκόπιμων επιζήμιων ενεργειών που έχουν σκοπό να προκαλέσουν βλάβες στα συστήματα ή να διακόψουν τη λειτουργία τους. Τέτοια συμβάντα μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σημαντική ζημία στην οικονομία της Ένωσης.

Τα συστήματα δικτύου και πληροφοριών, και κυρίως το διαδίκτυο, διαδραματίζουν ένα ουσιώδη ρόλο στη διευκόλυνση της διασυνοριακής κυκλοφορίας αγαθών, υπηρεσιών και προσώπων. Λόγω του διακρατικού τους χαρακτήρα, ενδεχόμενη σημαντική διατάραξη των συστημάτων αυτών, εσκεμμένη ή μη και ανεξαρτήτως του τόπου όπου εκδηλώνεται, μπορεί να επηρεάσει ατομικά κράτη μέλη και την Ένωση στο σύνολό της. Η ασφάλεια των συστημάτων δικτύου και πληροφοριών είναι επομένως ουσιώδης για την ομαλή λειτουργία της εσωτερικής αγοράς.

Η Ευρωπαϊκή Ένωση, λαμβάνοντας υπ' όψιν το ζωτικό ρόλο που διαδραματίζουν για την κοινωνία και την οικονομία τα συστήματα δικτύου και πληροφοριών και εκτιμώντας την σοβαρότητα της βλάβης που προκαλείται από σκόπιμες επιζήμιες ενέργειες στην οικονομία της Ένωσης και γενικότερα στην κοινωνία, θεσπίζει κοινό πλαίσιο κανόνων για όλα τα κράτη μέλη, ώστε να επιτευχθεί ένα ελάχιστο κοινό επίπεδο ασφάλειας και ενθαρρύνει τη συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[69] ώστε να υπάρχει και ενιαία στρατηγική αντιμετώπισης των κινδύνων.

Τα μέτρα αφορούν Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και Παρόχους Ψηφιακών Υπηρεσιών, όπως η ενέργεια, οι μεταφορές, οι τράπεζες, ο τομέας της υγείας, η διανομή νερού, η ψηφιακή υποδομή, αλλά και υπηρεσίες επιγραμμικής (online) αγοράς, μηχανής αναζήτησης και νεφοϋπολογιστικής (cloud computing).

Ο ορισμός της έννοιας των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και των Παρόχων Ψηφιακών Υπηρεσιών μετά τη διαπίστωση ότι υπάρχει διαφοροποίηση εντός της Ένωσης στο επίπεδο προστασίας καταναλωτών και επιχειρήσεων, θεσπίζεται με κοινό τρόπο, με τον σαφή προσδιορισμό για ορισμένες κοινές παραμέτρους και αφήνοντας τα κράτη μέλη να ορίσουν τις συγκεκριμένες τιμές τους σε εθνικό επίπεδο, χωρίς να αποκλείεται η θέσπιση και επιπλέον παραμέτρων από τα κράτη μέλη ή επιπλέον κανόνων ασφάλειας.

Οι κανόνες μπορεί να οριστούν τόσο από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Παρόχους Ψηφιακών Υπηρεσιών, όσο και από τα κράτη μέλη.

Η εν λόγω Οδηγία αποσκοπεί στο να αποτελέσει ένα ελάχιστο μέσο σύγκλισης των νομοθεσιών των κρατών - μελών της Ε.Ε., όσον αφορά στην εφαρμογή της Οδηγίας NIS, στον τομέα της ασφάλειας συστημάτων δικτύων και πληροφοριών.

Σύμφωνα με το άρθρο 1, η εν λόγω οδηγία θεσπίζει μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης, με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς. Για τον σκοπό αυτό, προβλέπει τις υποχρεώσεις να θεσπιστεί εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κράτη μέλη, δημιουργεί ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, καθώς και την ανάπτυξη της εμπιστοσύνης και της αξιοπιστίας μεταξύ τους, δημιουργεί δίκτυο ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών («δίκτυο CSIRT»), προκειμένου να συμβάλλει στην ανάπτυξη της αξιοπιστίας και εμπιστοσύνης μεταξύ των κρατών μελών και να προωθήσει την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία, θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών και προβλέπει τις υποχρεώσεις των κρατών μελών να ορίζουν εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

[69] European Network Information Security Agency

Ωστόσο, η εν λόγω οδηγία δεν θίγει τα μέτρα που λαμβάνουν τα κράτη μέλη για τη διαφύλαξη των ουσιωδών κρατικών λειτουργιών τους και ιδίως για τη διαφύλαξη της εθνικής ασφάλειας, συμπεριλαμβανομένων των μέτρων για την προστασία πληροφοριών των οποίων τη διάδοση τα κράτη μέλη θεωρούν αντίθετη προς τα ουσιώδη συμφέροντα ασφάλειάς τους, καθώς και για τη διατήρηση του νόμου και της τάξης και ιδίως για τη διευκόλυνση της διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων. Μάλιστα, σύμφωνα με το άρθρο 3 της Οδηγίας, τα κράτη μέλη δύνανται να θεσπίζουν ή να διατηρούν διατάξεις με στόχο την επίτευξη υψηλότερου επιπέδου ασφαλείας των συστημάτων δικτύου και πληροφοριών.

Κατά τους ορισμούς του άρθρου 4 της εν λόγω Οδηγίας, το σύστημα δικτύου και πληροφοριών μπορεί να συνιστά είτε ένα δίκτυο ηλεκτρονικών επικοινωνιών, είτε κάθε συσκευή ή ομάδα διασυνδεδεμένων συσκευών, οι οποίες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από δίκτυα ηλεκτρονικών επικοινωνιών ή ομάδα διασυνδεδεμένων συσκευών για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησης τους. Επιπρόσθετα, η ασφάλεια συστημάτων δικτύου και πληροφοριών είναι η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία.

Σύμφωνα με το άρθρο 5 της Οδηγίας, τα κράτη μέλη προσδιορίζουν για κάθε τομέα που αναφέρεται στο παράρτημα ΙΙ αυτής τους φορείς εκμετάλλευσης βασικών υπηρεσιών που είναι εγκατεστημένοι στην επικράτεια τους, τα δε κριτήρια για τον προσδιορισμό φορέων εκμετάλλευσης βασικών υπηρεσιών συνιστούν η οντότητα που παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών και οικονομικών δραστηριοτήτων, η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφοριών και τυχόν συμβάν που θα προκαλούσε σοβαρή διατάραξη της παροχής της εν λόγω υπηρεσίας. Σε τακτική δε βάση, ανά διετία τουλάχιστον, τα κράτη μέλη επανεξετάζουν, και εφόσον απαιτείται, επικαιροποιούν τον κατάλογο των προσδιορισμένων φορέων εκμετάλλευσης βασικών υπηρεσιών.

Κατά το άρθρο 6 της εν λόγω Οδηγίας σχετικά με τη σοβαρή διατάραξη της παροχής των υπηρεσιών, αναφέρεται ότι κατά τον προσδιορισμό της σοβαρότητας της διατάραξης, τα κράτη μέλη θα πρέπει να λαμβάνουν υπόψη παράγοντες που αφορούν στον αριθμό των χρηστών που εξαρτώνται από την υπηρεσία που παρέχεται από την οικεία οντότητα, στον αντίκτυπο που θα μπορούσαν να έχουν τα συμβάντα, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια, στο μερίδιο αγοράς της εν λόγω οντότητας, στο γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα συμβάν και στη σημασία του φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας.

Περαιτέρω, το άρθρο 7 της Οδηγίας προβλέπει ότι κάθε κράτος μέλος θεσπίζει εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών, στην οποία καθορίζονται οι στρατηγικοί στόχοι και τα κατάλληλα μέτρα πολιτικής και κανονιστικής ρύθμισης με σκοπό την επίτευξη και διατήρηση υψηλού επιπέδου ασφαλείας συστημάτων δικτύου και πληροφοριών. Η εθνική στρατηγική για την ασφάλεια συ-

στημάτων δικτύου και πληροφοριών αφορά στους στόχους και προτεραιότητες της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών, στο πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του ρόλου και των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμοδίων φορέων, στον προσδιορισμό των μέτρων ετοιμότητας, παρέμβασης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στον δημόσιο και ιδιωτικό τομέα, στην αναφορά των σχεδίων έρευνας και ανάπτυξης, καθώς και των προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών, στο σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό των κινδύνων και τέλος, στον κατάλογο των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών.

Μάλιστα, τα κράτη μέλη δύνανται να αιτούνται τη συνδρομή του ENISA για την ανάπτυξη των εθνικών στρατηγικών ασφαλείας συστημάτων δικτύου και πληροφοριών, ενώ ταυτόχρονα είναι υποχρεωμένα να κοινοποιούν την εθνική στρατηγική τους για την ασφάλεια συστημάτων δικτύου και πληροφοριών στην Επιτροπή εντός τριών μηνών από την έγκριση της, διαθέτοντας ωστόσο τη δυνατότητα εξαιρούν από την κοινοποίηση αυτή στοιχεία της στρατηγικής που συνδέονται με την εθνική ασφάλεια.

Σύμφωνα δε με το άρθρο 8 της εν λόγω Οδηγίας, αναφορικά με τις εθνικές αρμόδιες αρχές και το ενιαίο κέντρο επαφής, κάθε κράτος μέλος ορίζει μία ή περισσότερες εθνικές αρμόδιες αρχές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, που καλύπτουν τουλάχιστον τους τομείς που αναφέρονται στην Οδηγία, με αρμοδιότητα να παρακολουθούν την εφαρμογή της εν λόγω Οδηγίας σε εθνικό επίπεδο. Παράλληλα, κάθε κράτος μέλος ορίζει ένα εθνικό ενιαίο κέντρο επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, το οποίο ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών μελών, καθώς και με τις αρμόδιες αρχές άλλων κρατών μελών, στην περίπτωση δε που οριστεί μία μόνο αρμόδια αρχή, η εν λόγω αρμόδια αρχή αποτελεί και το ενιαίο κέντρο επαφής. Τα κράτη μέλη είναι υποχρεωμένα να εξασφαλίζουν επαρκείς πόρους για τις αρμόδιες αρχές και τα ενιαία κέντρα επαφής, ώστε να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους ανατίθενται και να επιτυγχάνουν, με τον τρόπο αυτό, τους στόχους της εν λόγω Οδηγίας. Οι αρμόδιες αρχές και το ενιαίο κέντρο επαφής διαβουλεύονται και συνεργάζονται με τις αρμόδιες εθνικές αρχές επιβολής του νόμου και τις εθνικές αρχές προστασίας δεδομένων. Τέλος, κάθε κράτος μέλος είναι υποχρεωμένο να κοινοποιεί στην Επιτροπή, χωρίς καθυστέρηση, τον ορισμό της αρμόδιας εθνικής αρχής και του ενιαίου κέντρου επαφής, τα καθήκοντα τους, καθώς και κάθε μεταγενέστερη τροποποίηση.

Περαιτέρω, κατά το άρθρο 9 της εν λόγω Οδηγίας, αναφορικά με τις ομάδες απόκρισης για συμβάντα που αφορούν στην ασφάλεια των υπολογιστών (CSIRT)[70], κάθε κράτος μέλος δύναται να ορίζει μία ή περισσότερες CSIRT, που είναι υπεύθυνες για τον χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας. Οι CSIRT δύνανται να είναι συγκροτημένες ακόμα και εντός της αρμόδιας αρχής, ενώ τα κράτη μέλη είναι υποχρεωμένα να εξασφαλίζουν ότι διαθέτουν επαρκείς πόρους για

[70] Computer Secutity Incident Response Team

την αποτελεσματική εκτέλεση των καθηκόντων τους και παράλληλα μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των CSIRT στο πλαίσιο του δικτύου CSIRT. Τέλος, τα κράτη μέλη μεριμνούν ώστε οι CSIRT να έχουν πρόσβαση σε μία ανθεκτική, κατάλληλη και ασφαλή υποδομή επικοινωνιών σε εθνικό επίπεδο, ενημερώνουν την Επιτροπή σχετικά με την εντολή και τα βασικά στοιχεία της διαδικασίας χειρισμού συμβάντων από τις CSIRT και δύνανται να αιτούνται τη συνδρομή του ENISA για την ανάπτυξη των εθνικών CSIRT.

Επιπλέον, κατά το άρθρο 10 της Οδηγίας, αναφορικά με τη συνεργασία σε εθνικό επίπεδο, η αρμόδια αρχή, το ενιαίο κέντρο επαφής και οι CSIRT του ίδιου κράτους μέλους εφόσον αυτά είναι διαφορετικά, συνεργάζονται ως προς την τήρηση των υποχρεώσεων που προβλέπονται στην εν λόγω Οδηγία. Τα κράτη μέλη είναι υποχρεωμένα να εξασφαλίζουν ότι είτε οι αρμόδιες αρχές είτε οι CSIRT λαμβάνουν τις κοινοποιήσεις που υποβάλλονται σύμφωνα με την εν λόγω Οδηγία, σε περίπτωση δε που κράτος μέλος αποφασίσει ότι οι CSIRT δεν λαμβάνουν κοινοποιήσεις, χορηγείται σε αυτές, στον βαθμό που είναι αναγκαίο για την εκπλήρωση των καθηκόντων τους, πρόσβαση σε δεδομένα σχετικά με συμβάντα που κοινοποιούνται από τους φορείς εκμετάλλευσης βασικών υπηρεσιών ή από παρόχους ψηφιακών υπηρεσιών. Τέλος, τα κράτη μέλη υποχρεούνται να διασφαλίζουν ότι οι αρμόδιες αρχές ή οι CSIRT ενημερώνουν τα ενιαία κέντρα επαφής σχετικά με κοινοποιήσεις συμβάντων που υποβάλλονται σύμφωνα με την εν λόγω Οδηγία.

Κατά το άρθρο 11 της Οδηγίας, προβλέπεται η συγκρότηση ομάδας συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, την ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης, καθώς και την επίτευξη ενός κοινού υψηλού επιπέδου ασφαλείας συστημάτων δικτύου και πληροφοριών στην Ένωση. Η ομάδα συνεργασίας, η οποία απαρτίζεται από αντιπροσώπους των κρατών μελών, της Επιτροπής και του ENISA, εκτελεί τα καθήκοντα της βάσει διετών προγραμμάτων εργασιών, συμφώνων προς τους στόχους της εν λόγω Οδηγίας. Τα καθήκοντα της ομάδας συνεργασίας συνίστανται στην παροχή στρατηγικής καθοδήγησης για τις δραστηριότητες του δικτύου CSIRT, στην ανταλλαγή βέλτιστων πρακτικών για την ανταλλαγή πληροφοριών που αφορούν την κοινοποίηση συμβάντων, στην ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών, στην αρωγή στα κράτη μέλη αναφορικά με την ανάπτυξη ικανοτήτων στον τομέα της ασφάλειας συστημάτων δικτύου και πληροφοριών, στη συζήτηση για τις δυνατότητες και την ετοιμότητα των κρατών μελών, στην αξιολόγηση των εθνικών στρατηγικών ασφάλειας συστημάτων δικτύου και πληροφοριών και της αποτελεσματικότητας του CSIRT, στην ανταλλαγή πληροφοριών και βέλτιστων πρακτικών σχετικά με την ευαισθητοποίηση και την κατάρτιση, καθώς και την έρευνα και την ανάπτυξη για την ασφάλεια συστημάτων δικτύου και πληροφοριών, στην ανταλλαγή εμπειριών για θέματα ασφάλειας συστημάτων δικτύου και πληροφοριών με τα αρμόδια θεσμικά και λοιπά όργανα της Ένωσης και με τους αρμόδιους οργανισμούς της, στη συλλογή πληροφοριών για βέλτιστες πρακτικές σχετικά με κινδύνους και συμβάντα, στη συζήτηση για τις εργασίες που πραγματοποιούνται σε επίπεδο ασκήσεων σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, των εκπαιδευτικών προγραμμάτων και κατάρτισης, συμπεριλαμβανομένων των εργασιών που έγιναν από τον ENISA και στην ανταλλαγή βέλτιστων πρακτικών σχετικά με τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών από τα κράτη μέλη.

Κατά το άρθρο 12 της εν λόγω Οδηγίας, προβλέπεται η δημιουργία δικτύου εθνικών CSIRT, με σκοπό τη συμβολή στην ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης μεταξύ των κρατών μελών και την προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας. Το δίκτυο CSIRT απαρτίζεται από αντιπροσώπους των CSIRT των κρατών μελών και την CERT- EU[71], ενώ η Επιτροπή συμμετέχει σε αυτό ως παρατηρητής. Το δίκτυο CSIRT διαθέτει καθήκοντα ανταλλαγής πληροφοριών σχετικά με τις υπηρεσίες, τις δραστηριότητες και τις δυνατότητες συνεργασίας των CSIRT, ανταλλαγής και διάθεσης σε εθελούσια βάση με εμπιστευτικών πληροφοριών για μεμονωμένα συμβάντα, υποστήριξης των κρατών μελών για την αντιμετώπιση διασυνοριακών συμβάντων βάσει της εθελούσιας αμοιβαίας συνδρομής τους, συζήτησης, διερεύνησης και καθορισμού περαιτέρω μορφών επιχειρησιακής συνεργασίας, συμπεριλαμβανομένων μεταξύ άλλων και τα σχετικά με τις κατηγορίες κινδύνων και συμβάντων, τις έγκαιρες προειδοποιήσεις και την αμοιβαία συνδρομή, ενημέρωσης της ομάδας συνεργασίας σχετικά με τις δραστηριότητες του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται, της συζήτησης των διδαγμάτων που αντλούνται από ασκήσεις σχετικά με τη ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων μεταξύ άλλων και από εκείνες που οργανώνει ο ENISA, της συζήτησης των δυνατοτήτων και της ετοιμότητας συγκεκριμένου CSIRT, κατόπιν αιτήματος του και της ανταλλαγής και συζήτησης μη ευαίσθητων από εμπορικής άποψης πληροφοριών που σχετίζονται με συγκεκριμένο συμβάν και συναφείς κινδύνους, κατόπιν αιτήματος αντιπροσώπου CSIRT κράτους μέλους που ενδέχεται να επηρεάζεται από αυτό το συμβάν.

Περαιτέρω, η Οδηγία 2016/1148/ΕΕ προβλέπει την ασφάλεια των συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών. Σύμφωνα με το άρθρο 14 αυτής, αναφορικά με τις απαιτήσεις ασφαλείας και τη κοινοποίηση συμβάντων, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών λαμβάνουν τα κατάλληλα, αναλογικά, τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητες τους, με έμφαση στη λήψη κατάλληλων μέτρων για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή αυτών των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της συνέχειας τους και τη χωρίς αδικαιολόγητη καθυστέρηση κοινοποίηση από τους φορείς εκμετάλλευσης βασικών υπηρεσιών στην αρμόδια αρχή ή τη CSIRT συμβάντων με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν. Για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη ο αριθμός των χρηστών που επηρεάζεται από τη διατάραξη της βασικής υπηρεσίας, η διάρκεια του συμβάντος και το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν. Βάσει των πληροφοριών που παρέχονται στην κοινοποίηση από τον φορέα εκμετάλλευσης βασικών υπηρεσιών, η αρμόδια αρχή ή η CSIRT ενημερώνει τυχόν επηρεαζόμενα κράτη μέλη, αν το συμβάν έχει σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών στο εν λόγω κράτος μέλος. Στο πλαίσιο της ενημέρωσης αυτής, η αρμόδια αρχή ή η CSIRT, διαφυλάσσει την ασφάλεια και τα εμπορικά συμφέροντα του φορέα εκμετάλλευσης βασικών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί στην κοινοποίηση του. Το ενιαίο κέντρο επαφής από την πλευρά του, κατόπιν αιτήματος της αρμόδιας αρχής ή της CSIRT, διαβι-

[71] The Computer Emergency Response Team for the EU Institutions, bodies and agencies.

βάζει τις ανωτέρω κοινοποιήσεις στα ενιαία κέντρα επαφής των επηρεαζόμενων κρατών μελών. Κατόπιν διαβούλευσης με τον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, η αρμόδια αρχή ή η CSIRT δύναται να ενημερώνει το κοινό σχετικά με μεμονωμένα συμβάντα, σε περίπτωση που η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη.

Η εν λόγω Οδηγία προβλέπει ομοίως την ασφάλεια των συστημάτων δικτύου και πληροφοριών των παρόχων ψηφιακών υπηρεσιών. Σύμφωνα με το άρθρο 16 αυτής, αναφορικά με τις απαιτήσεις ασφαλείας και τη κοινοποίηση συμβάντων, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι πάροχοι ψηφιακών υπηρεσιών λαμβάνουν τα κατάλληλα, αναλογικά, τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά στην ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στο πλαίσιο παροχής υπηρεσιών, με έμφαση στη λήψη κατάλληλων μέτρων για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή αυτών των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της συνέχειας τους και στη χωρίς αδικαιολόγητη καθυστέρηση κοινοποίηση από τους παρόχους ψηφιακών υπηρεσιών στην αρμόδια αρχή ή τη CSIRT συμβάντων με σοβαρό αντίκτυπο στη παροχή της υπηρεσίας, που προσφέρουν εντός της Ένωσης. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα ανωτέρω μέτρα οφείλουν να εξασφαλίζουν ένα επίπεδο ασφαλείας των συστημάτων δικτύου και πληροφοριών, ανάλογο προς τον εκάστοτε κίνδυνο, συνεκτιμώντας την ασφάλεια των συστημάτων και των εγκαταστάσεων, τη διαχείριση των συμβάντων και της επιχειρησιακής συνέχειας, την παρακολούθηση, τις επιθεωρήσεις και τις δοκιμές, καθώς και τη συμμόρφωση με διεθνή πρότυπα. Για να προσδιοριστεί αν ο αντίκτυπος ενός συμβάντος είναι σημαντικός, λαμβάνονται υπόψη ο αριθμός των χρηστών που επηρεάζεται από το συμβάν, η διάρκεια του συμβάντος, το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν, η έκταση της διατάραξης της λειτουργίας της υπηρεσίας και η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες. Βάσει των πληροφοριών που παρέχονται στην κοινοποίηση από τον πάροχο ψηφιακών υπηρεσιών, η αρμόδια αρχή ή η CSIRT ενημερώνει τυχόν κράτη μέλη που επηρεάζονται από το συμβάν. Στο πλαίσιο της ενημέρωσης αυτής, η αρμόδια αρχή, η CSIRT και τα ενιαία κέντρα επαφής διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα του παρόχου ψηφιακών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί στην κοινοποίηση του. Κατόπιν διαβούλευσης με τον ενδιαφερόμενο πάροχο ψηφιακών υπηρεσιών, η αρμόδια αρχή ή η CSIRT δύνανται να ενημερώνουν το κοινό σχετικά με τα μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή σε περίπτωση που η αποκάλυψη του συμβάντος είναι προς το δημόσιο συμφέρον.

Σύμφωνα με το άρθρο 17 της εν λόγω Οδηγίας, αναφορικά με την εφαρμογή και επιβολή, προβλέπεται ότι τα κράτη μέλη διασφαλίζουν την ανάληψη δράσης από τις αρμόδιες αρχές, εάν είναι αναγκαία, με εκ των υστέρων εποπτικά μέτρα, όταν τους παρέχονται στοιχεία που αποδεικνύουν ότι πάροχος ψηφιακών υπηρεσιών δεν πληροί τις απαιτήσεις που ορίζονται ανωτέρω. Τα εν λόγω αποδεικτικά στοιχεία μπορούν να υποβάλλονται από μια αρμόδια αρχή άλλου κράτους μέλους στο οποίο παρέχεται η υπηρεσία. Για τον ανωτέρω σκοπό, οι αρμόδιες αρχές διαθέτουν τις αναγκαίες εξουσίες και μέσα ώστε να απαιτούν από τους παρόχους ψηφιακών υπηρεσιών να παρέχουν

τις απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και πληροφοριών τους, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών ασφάλειας, να αποκαθιστούν οποιαδήποτε παράλειψη συμμόρφωσης προς τις απαιτήσεις που ορίζονται ανωτέρω. Μάλιστα, εάν ένας πάροχος ψηφιακών υπηρεσιών έχει την κύρια εγκατάστασή του ή αντιπρόσωπο σε ένα κράτος μέλος, αλλά τα συστήματα δικτύου και πληροφοριών του βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, η αρμόδια αρχή του κράτους μέλους της κύριας εγκατάστασης ή του αντιπροσώπου και οι αρμόδιες αρχές των άλλων κρατών μελών συνεργάζονται και παρέχουν αμοιβαία συνδρομή, εφόσον απαιτείται. Η συνδρομή και η συνεργασία μπορεί να καλύπτουν ανταλλαγές πληροφοριών μεταξύ των σχετικών αρμοδίων αρχών και αιτήματα για τη λήψη εποπτικών μέτρων που αναφέρονται ανωτέρω.

Σύμφωνα με το άρθρο 18 της εν λόγω Οδηγίας, αναφορικά με τη δικαιοδοσία και την εδαφικότητα, ένας πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο έχει την κύρια εγκατάστασή του. Ένας πάροχος ψηφιακών υπηρεσιών θεωρείται ότι έχει την κύρια εγκατάστασή του σε κράτος μέλος όταν έχει την έδρα του στο εν λόγω κράτος μέλος. Επιπλέον, ένας πάροχος ψηφιακών υπηρεσιών που δεν είναι εγκατεστημένος στην Ένωση αλλά προσφέρει υπηρεσίες εντός της Ένωσης ορίζει αντιπρόσωπο στην Ένωση. Ο αντιπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη μέλη στα οποία προσφέρονται οι υπηρεσίες. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο αντιπρόσωπος. Ο ορισμός ενός αντιπροσώπου από τον πάροχο ψηφιακών υπηρεσιών δεν θίγει τις νομικές ενέργειες οι οποίες μπορούν να αναληφθούν κατά του ίδιου του παρόχου ψηφιακών υπηρεσιών.

Αναφορικά με τη μεταφορά της εν λόγω Οδηγίας στο εθνικό δίκαιο, κατά το άρθρο 25 αυτής, τα κράτη μέλη ήταν υποχρεωμένα να θεσπίσουν και να δημοσιεύσουν έως τις 9 Μαΐου 2018 τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις ώστε να συμμορφωθούν με αυτή.

4. ΕΠΙΠΕΔΑ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΟΡΓΑΝΙΣΜΟΙ ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Λόγω της διασυνδεσιμότητας του ψηφιακού κόσμου, τα συμβάντα παραβίασης της Ασφάλειας Δικτύων και Πληροφοριών δεν σταματούν στα σύνορα κάθε κράτους μέλους της Ευρωπαϊκής Ένωσης. Για την αποτελεσματική αντιμετώπιση συμβάντων και κινδύνων, όλοι οι φορείς, από τις αρμόδιες αρχές για την Ασφάλεια Δικτύων και Πληροφοριών, τις ομάδες CERT, τις αρχές επιβολής του Νόμου ως και τη βιομηχανία, πρέπει να αναλαμβάνουν ευθύνη τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο και να εργάζονται από κοινού για την ενίσχυση της κυβερνοασφάλειας. Καθώς όμως διαφορετικά νομοθετικά πλαίσια και διαφορετικού βαθμού δικαιοδοσίες εμπλέκονται στην προσπάθεια καταπολέμησης των περιστατικών παραβίασης της ασφάλειας στον κυβερνοχώρο, μεγάλη πρόκληση για την Ευρωπαϊκή Ένωση αποτελεί η αποσαφήνιση των ρόλων και των αρμοδιοτήτων των φορέων που συμμετέχουν στην προσπάθεια αυτή. Δεδομένης, λοιπόν, της πολυπλοκότητας του θέματος και του μεγάλου φάσματος των φορέων που συμμετέχουν, η κεντρική ευρωπαϊκή εποπτεία δεν είναι η απάντηση. Οι εθνικές κυβερνήσεις είναι οι καταλληλότερες για την οργάνωση της πρόληψης και της αντιμετώπισης περιστατικών και επιθέσεων στον κυβερνοχώρο, αλλά και για τη δημιουργία επαφών και δικτύων επικοινωνίας με τον ιδιωτικό τομέα και το ευρύ

κοινό. Παρόλα αυτά, λόγω της παγκόσμιας φύσης των κινδύνων του κυβερνοχώρου, μια αποτελεσματική εθνική απάντηση απαιτεί συχνά και τη συμμετοχή σε επίπεδο ΕΕ.

Για την αντιμετώπιση των συμβάντων κυβερνοασφάλειας με έναν αποτελεσματικό τρόπο και για την ανάπτυξη μιας ολοκληρωμένης προσέγγισης, οι αντίστοιχες δράσεις θα πρέπει να εκτείνονται πάνω σε τρεις βασικούς τομείς-κλειδιά, της Ασφάλειας Δικτύων και Πληροφοριών, της επιβολής του νόμου και της άμυνας. Σε κάθε έναν από τους τομείς αυτούς έχουμε και τους αρμόδιους φορείς και τις αρχές, που εκτελούν το δικό τους έργο, ερευνητικό, συμβουλευτικό αλλά συνεργάζονται και μεταξύ τους.

4.1 Τομέας Ασφάλειας Δικτύων και Πληροφοριών

4.1.1 Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA - European Network And Information Security Agency)

Ο Κανονισμός (ΕΕ) 526/2013[72] αναδιοργανώνει και εξελίσσει τη λειτουργία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)[73] , καταργώντας σχετικές διατάξεις του μέχρι τότε ισχύοντος (ΕΕ) 460/2004 Κανονισμού για τη λειτουργία του ENISA. Με τον εν λόγω Κανονισμό αναγνωρίζονται και διαφυλάσσονται τα μέχρι σήμερα επιτεύγματα του ENISA σε τομείς όπως οι ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT – Computer Emergency Response Team)[74] στα κράτη μέλη και οι σημαντικού κύρους ασκήσεις ασφάλειας στον κυβερνοχώρο, όπως η Cyber Europe 2012 με 600 συμμετέχοντες από όλη την Ευρώπη. Βασικά σημεία του νέου Κανονισμού συνιστούν, αφενός ότι ο ENISA αποκτά διασύνδεση με το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο της Europol και αφετέρου ότι παγιώνεται ο συμβουλευτικός και υποστηρικτικός ρόλος του στις χώρες της ΕΕ και στα όργανα της Ένωσης.

Σύμφωνα με το άρθρο 1 του εν λόγω Κανονισμού αναφορικά με το αντικείμενο και το πεδίο εφαρμογής αυτού, ιδρύεται Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), με σκοπό να συμβάλλει σε ένα υψηλό επίπεδο ασφαλείας των δικτύων και των πληροφοριών εντός της Ένωσης, να ευαισθητοποιήσει την κοινωνία και να αναπτύξει και να προωθήσει μια αντίληψη ασφάλειας των δικτύων και των πληροφοριών, προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα στην Ένωση, συμβάλλοντας έτσι στην εγκαθίδρυση και στην εύρυθμη λειτουργία της εσωτερικής αγοράς. Αναφορικά με τους ορισμούς του εν λόγω Κανονισμού, ως «ασφάλεια δικτύου και πληροφοριών» νοείται η ικανότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται σε τυχαία γεγονότα ή σε παράνομες ή κακόβουλες δράσεις που θέτουν σε κίνδυνο

[72] Βλ. πλήρες κείμενο του Κανονισμού στον επίσημο Διαδικτυακό ιστότοπο της Ευρωπαϊκής Ένωσης - https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0526&from=el (πρόσβαση στις 27-10-2019).

[73] Γιαννόπουλος Γ., Η ευθύνη των παρόχων υπηρεσιών στο Internet, Νομική Βιβλιοθήκη (2003) σελ. 297.

[74] Για τις ομάδες CERT του ENISA βλ επίσημο Διαδικτυακό ιστότοπο του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών - https://www.enisa.europa.eu / activities / cert

τη διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα και το απόρρητο των αποθηκευμένων ή διαβιβασμένων δεδομένων και των σχετικών υπηρεσιών που προσφέρονται ή καθίστανται προσβάσιμες από τα εν λόγω συστήματα ή δίκτυα.

Κατά το άρθρο 2 του Κανονισμού στόχοι του ανωτέρω Οργανισμού είναι η ανάπτυξη και διατήρηση υψηλού επιπέδου εμπειρογνωσίας, η αρωγή των θεσμικών και λοιπών οργάνων, των υπηρεσιών και οργανισμών της Ένωσης στην ανάπτυξη πολιτικών για την ασφάλεια των δικτύων και πληροφοριών, η αρωγή των οργάνων, υπηρεσιών, οργανισμών της Ένωσης και των κρατών μελών στην υλοποίηση των πολιτικών που απαιτούνται για την εκπλήρωση των νομικών και ρυθμιστικών απαιτήσεων σχετικά με την ασφάλεια των δικτύων και πληροφοριών, τόσο στις ισχύουσες όσο και στις μελλοντικές νομικές πράξεις της Ένωσης, συμβάλλοντας έτσι στην ορθή λειτουργία της εσωτερικής αγοράς, η αρωγή της Ένωσης και των κρατών μελών στη βελτίωση και την ενίσχυση της ικανότητας και της ετοιμότητας τους ώστε να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν προβλήματα και περιστατικά που αφορούν στην ασφάλεια δικτύων και πληροφοριών και η χρησιμοποίηση της εμπειρογνωσίας του προκειμένου να ενισχύσει την ευρεία συνεργασία μεταξύ φορέων του δημοσίου και ιδιωτικού τομέα.

Κατά το άρθρο 3 αναφορικά με τα καθήκοντα του, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) υποστηρίζει τη χάραξη της πολιτικής και της νομοθεσίας της Ένωσης, παρέχοντας τόσο βοήθεια και συμβουλές για όλα τα θέματα που αφορούν την πολιτική και τη νομοθεσία της Ένωσης για την ασφάλεια των δικτύων και πληροφοριών, όσο και προπαρασκευαστικό έργο, συμβουλές και αναλύσεις σχετικά με την ανάπτυξη και την επικαιροποίηση της πολιτικής και της νομοθεσίας της Ένωσης στον τομέα της ασφάλειας των δικτύων και των πληροφοριών, καθώς και αναλύοντας τις δημόσια διαθέσιμες στρατηγικές για την ασφάλεια των δικτύων και πληροφοριών και προωθώντας τη δημοσίευση τους. Επιπλέον, υποστηρίζει την ανάπτυξη ικανότητας, επικουρώντας τα κράτη μέλη, μετά από σχετικό αίτημα τους, στις προσπάθειες τους να αναπτύξουν και να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης προβλημάτων και συμβάντων σχετικά με την ασφάλεια δικτύων και πληροφοριών και διαθέτοντας τους τις απαιτούμενες γνώσεις και υποστηρίζοντας την αύξηση επιπέδου ικανότητας των εθνικών και ενωσιακών CERT, μεταξύ άλλων με την προώθηση του διαλόγου και της ανταλλαγής πληροφοριών, προκειμένου να εξασφαλίζεται ότι, όσον αφορά τη στάθμη της τεχνικής, κάθε CERT διαθέτει ένα κοινό σύνολο ελάχιστων ικανοτήτων και λειτουργεί με βάση τις βέλτιστες πρακτικές. Περαιτέρω, υποστηρίζει την εθελοντική συνεργασία μεταξύ αρμόδιων εθνικών αρχών και μεταξύ των άμεσα ενδιαφερομένων από τον δημόσιο και ιδιωτικό τομέα, συμπεριλαμβανομένων πανεπιστημίων και ερευνητικών κέντρων στην Ένωση, προωθώντας τη συνεργασία μεταξύ εθνικών και κυβερνητικών CERT ή ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT) και διευκολύνοντας τον διάλογο και τις προσπάθειες για την ανάπτυξη και την ανταλλαγή βέλτιστων πρακτικών. Επιπρόσθετα, υποστηρίζει την έρευνα, την ανάπτυξη και την τυποποίηση, διευκολύνοντας την καθιέρωση και χρήση ευρωπαϊκών και διεθνών προτύπων για τη διαχείριση κινδύνου και την ασφάλεια ηλεκτρονικών προϊόντων, συστημάτων, δικτύων και υπηρεσιών και παρέχοντας υπηρεσίες συμβούλου στην Ένωση και τα κράτη μέλη σχετικά με ερευνητικές ανάγκες στον τομέα της ασφάλειας δικτύου και πληροφοριών, με σκοπό να καταστεί δυνατή η ουσιαστική αντίδραση στους υπάρχοντες και τους εμφανιζόμενους κινδύνους και απειλές για την ασφάλεια των δικτύων

και των πληροφοριών σε σχέση με τις εμφανιζόμενες νέες τεχνολογίες της πληροφορίας και των τηλεπικοινωνιών και για την αποτελεσματική χρήση τεχνολογιών πρόληψης κινδύνων. Επίσης, συνεργάζεται με τα θεσμικά και λοιπά όργανα, τις υπηρεσίες και τους οργανισμούς της Ένωσης, συμπεριλαμβανομένων εκείνων που ασχολούνται με το ηλεκτρονικό έγκλημα και την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, με σκοπό την αντιμετώπιση κοινών προβλημάτων, ανταλλάσσοντας τεχνογνωσία και βέλτιστες πρακτικές και παρέχοντας συμβουλές για τις σχετικές πτυχές της ασφάλειας δικτύων και πληροφοριών, με στόχο την ανάπτυξη συνεργειών. Τέλος, συμβάλλει στις προσπάθειες της Ένωσης για συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς σε θέματα που αφορούν την ασφάλεια δικτύων και πληροφοριών, συμμετέχοντας ως παρατηρητής, καθώς και σε οργανωτικό επίπεδο, στην οργάνωση διεθνών ασκήσεων, αναλύοντας τα αποτελέσματα τους και υποβάλλοντας σχετικές εκθέσεις, διευκολύνοντας την ανταλλαγή βέλτιστων πρακτικών μεταξύ των σχετικών οργανισμών και παρέχοντας εμπειρογνωσία στα θεσμικά όργανα της Ένωσης.

Σύμφωνα με το άρθρο 4 του εν λόγω Κανονισμού αναφορικά με τη σύνθεση του, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) απαρτίζεται από το Διοικητικό Συμβούλιο, τον εκτελεστικό διευθυντή, το προσωπικό και τη μόνιμη ομάδα ενδιαφερομένων. Κατά το άρθρο 5 του Κανονισμού δε, το Διοικητικό Συμβούλιο ορίζει τις γενικές κατευθύνσεις λειτουργίας του Οργανισμού, διασφαλίζει ότι αυτός λειτουργεί με τους κανόνες και τις αρχές της διαφάνειας και της τήρησης του απορρήτου, καθώς και τη συνοχή των εργασιών του με τις δραστηριότητες που διεξάγονται από τα κράτη μέλη, καθώς και σε επίπεδο Ένωσης. Επίσης, εγκρίνει το ετήσιο και το πολυετές πρόγραμμα εργασιών του Οργανισμού, καθώς και την ετήσια έκθεση δραστηριοτήτων του, την οποία διαβιβάζει στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή και το Ελεγκτικό Συνέδριο. Επιπλέον, χαράσσει στρατηγική καταπολέμησης της απάτης ανάλογη των κινδύνων απάτης και λαμβάνοντας υπόψη την ανάλυση κόστους - οφέλους των λαμβανομένων μέτρων, ενώ παράλληλα εξασφαλίζει ότι δίνεται κατάλληλη συνέχεια στα συμπεράσματα και τις συστάσεις που προκύπτουν από τις έρευνες της Ευρωπαϊκής Υπηρεσίας Καταπολέμησης της Απάτης (OLAF)[75]. Επιπρόσθετα, θεσπίζει κανόνες για την πρόληψη και τη διαχείριση συγκρούσεων συμφερόντων. Περαιτέρω, διορίζει τον εκτελεστικό διευθυντή και μπορεί να παρατείνει τη θητεία του ή ακόμα και να τον απαλλάξει από τα καθήκοντα του. Τέλος, εγκρίνει τόσο τον εσωτερικό κανονισμό όσο και τους δημοσιονομικούς κανόνες που ισχύουν για τον Οργανισμό.

Σύμφωνα δε με το άρθρο 6 του Κανονισμού αναφορικά με τη σύνθεση του Διοικητικού Συμβουλίου, αυτό απαρτίζεται από έναν εκπρόσωπο από κάθε κράτος μέλος και δύο εκπροσώπους που διορίζονται από την Επιτροπή με κριτήριο τη γνώση τους σχετικά με τα καθήκοντα και τους στόχους του Οργανισμού, ενώ λαμβάνονται επίσης υπόψη οι ικανότητες διεύθυνσης, διοίκησης και δημοσιονομικής διαχείρισης που είναι συναφείς με την εκτέλεση των καθηκόντων τους. Η θητεία των μελών του Διοικητικού Συμβουλίου είναι τετραετής, άπαξ ανανεώσιμη και όλα τα μέλη έχουν δικαίωμα ψήφου.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) διοικείται από τον εκτελεστικό διευθυντή του, ο οποίος ενεργεί ανεξάρτητα από την άσκηση των καθηκόντων του και είναι υπεύθυνος, σύμφωνα με

[75] European Anti-Fraud Office.

το άρθρο 11 του Κανονισμού, για την τρέχουσα διοίκηση του Οργανισμού, την εκτέλεση των αποφάσεων που έχουν εγκριθεί από το Διοικητικό Συμβούλιο, την προετοιμασία και εφαρμογή του ετήσιου προγράμματος εργασιών και του πολυετούς προγράμματος, καθώς και την υποβολή σχετικής έκθεσης στο διοικητικό συμβούλιο, την προστασία των οικονομικών συμφερόντων της Ένωσης, με την εφαρμογή προληπτικών μέτρων κατά της απάτης και της διαφθοράς, τη χάραξη στρατηγικής του Οργανισμού για την καταπολέμηση της απάτης, καθώς και την ανάπτυξη και διατήρηση επαφών τόσο με τα θεσμικά και λοιπά όργανα, τις υπηρεσίες και τους οργανισμούς της Ένωσης, όσο και με την επιχειρηματική κοινότητα και τις ενώσεις καταναλωτών, ώστε να εξασφαλίζεται διάλογος με τους άμεσα ενδιαφερομένους. Μάλιστα, σύμφωνα με το άρθρο 24 του Κανονισμού, ο εκτελεστικός διευθυντής προσλαμβάνεται ως έκτακτος υπάλληλος του Οργανισμού και διορίζεται από το διοικητικό συμβούλιο, από κατάλογο υποψηφίων που προτείνει η Επιτροπή, με ανοιχτή και διαφανή διαδικασία. Η θητεία του είναι πενταετής και παρατείνεται άπαξ για διάστημα που δεν υπερβαίνει την πενταετία. Τέλος, ο εκτελεστικός διευθυντής μπορεί να απαλλαγεί από τα καθήκοντα του με απόφαση του διοικητικού συμβουλίου.

Σύμφωνα δε με το άρθρο 12 του εν λόγω Κανονισμού, το Διοικητικό Συμβούλιο, κατόπιν προτάσεως του εκτελεστικού διευθυντή, συγκροτεί μία μόνιμη ομάδα ενδιαφερομένων η οποία απαρτίζεται από εμπειρογνώμονες αναγνωρισμένου κύρους που αντιπροσωπεύουν τους σχετικούς άμεσα ενδιαφερομένους, όπως τον κλάδο ΤΠΕ[76], τους παρόχους δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών για το κοινό, τις ομάδες καταναλωτών και τους πανεπιστημιακούς που είναι ειδικοί στην ασφάλεια δικτύων και πληροφοριών και αντιπροσώπους των εθνικών ρυθμιστικών αρχών. Οι διαδικασίες, ιδίως όσον αφορά τον αριθμό, τη σύνθεση και τον διορισμό των μελών της μόνιμης ομάδας ενδιαφερομένων από το διοικητικό συμβούλιο κατόπιν πρότασης του εκτελεστικού διευθυντή, καθώς και τη λειτουργία της ομάδας, καθορίζονται στους εσωτερικούς κανόνες λειτουργίας του Οργανισμού και δημοσιοποιούνται. Πρόεδρος της μόνιμης ομάδας ενδιαφερομένων είναι ο εκτελεστικός διευθυντής ή πρόσωπο διορισμένο από τον εκτελεστικό διευθυντή. Η διάρκεια της θητείας των μελών της μόνιμης ομάδας ενδιαφερομένων είναι δυόμισι έτη, ενώ τα μέλη του διοικητικού συμβουλίου δεν επιτρέπεται να είναι μέλη της μόνιμης ομάδας ενδιαφερομένων. Οι εμπειρογνώμονες της Επιτροπής και των κρατών μελών έχουν δικαίωμα να παρίστανται στις συνεδριάσεις της μόνιμης ομάδας ενδιαφερομένων και να συμμετέχουν στις εργασίες της. Η μόνιμη ομάδα ενδιαφερομένων παρέχει συμβουλές στον Οργανισμό σχετικά με την εκτέλεση των δραστηριοτήτων του. Παρέχει ειδικότερα συμβουλές στον εκτελεστικό διευθυντή κατά την κατάρτιση πρότασης για το πρόγραμμα εργασίας του Οργανισμού και για τη διασφάλιση της επικοινωνίας με τους σχετικούς άμεσα ενδιαφερόμενους επί όλων των θεμάτων που σχετίζονται με το πρόγραμμα εργασίας.

Ως προς τη λειτουργία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), σύμφωνα με το άρθρο 13 του Κανονισμού αναφορικά με το πρόγραμμα εργασίας αυτού, ο Οργανισμός εκτελεί τις εργασίες του σύμφωνα με το ετήσιο και το πολυετές πρόγραμμα εργασίας του, που περιλαμβάνει όλες τις προγραμματισμένες δραστηριότητες του. Το πρόγραμμα εργασίας περιλαμβάνει εξειδικευμένους δείκτες επιδόσεων που επιτρέπουν την αποτελεσματική αξιολόγηση των αποτελεσμάτων που επιτυγχάνονται όσον αφορά στους στόχους. Ο εκτελεστικός διευθυντής είναι υπεύθυνος για την κατάρτιση του σχεδίου του προγράμματος

[76] Τεχνολογία Πληροφοριών και Επικοινωνίας.

εργασίας του Οργανισμού κατόπιν προηγούμενης διαβούλευσης με τις υπηρεσίες της Επιτροπής και υποβάλλει το σχέδιο προγράμματος εργασίας του επόμενου έτους, που περιλαμβάνει τις πολυετείς προοπτικές, στο διοικητικό συμβούλιο, το οποίο εγκρίνει, αφού λάβει προηγουμένως τη γνωμοδότηση της Επιτροπής. Το διοικητικό συμβούλιο διασφαλίζει ότι το πρόγραμμα εργασίας συνάδει με τους στόχους του Οργανισμού, καθώς και με τις νομοθετικές και πολιτικές προτεραιότητες της Ένωσης στο πεδίο της ασφάλειας δικτύων και πληροφοριών. Το πρόγραμμα εργασίας διαρθρώνεται σύμφωνα με την αρχή διαχείρισης βάσει δραστηριοτήτων και εναρμονίζεται με τη δήλωση εκτίμησης εσόδων και εξόδων του Οργανισμού και τον προϋπολογισμό αυτού για το ίδιο οικονομικό έτος. Τέλος, ο εκτελεστικός διευθυντής διαβιβάζει το πρόγραμμα εργασίας, μετά την έγκριση του από το διοικητικό συμβούλιο, στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Επιτροπή και τα κράτη μέλη, και το δημοσιεύει.

Σύμφωνα με το άρθρο 35 του Κανονισμού, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) διαδέχεται τον Οργανισμό που συστάθηκε δυνάμει του Κανονισμού υπ' αριθ. 460/2004 όσον αφορά σε όλα τα δικαιώματα ιδιοκτησίας, τις συμφωνίες, τις νομικές υποχρεώσεις, τις συμβάσεις εργασίας, τις οικονομικές δεσμεύσεις και ευθύνες. Αναφορικά με τη διάρκεια λειτουργίας του Οργανισμού, το άρθρο 36 του Κανονισμού προβλέπει ότι αυτός ιδρύεται στις 19 Ιουνίου 2013 για θητεία επτά ετών.

4.1.2 Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης στην Πληροφορική / CERT-EU (Computer Emergency Response Team)

Οι νέες και τεχνολογικά πιο εξελιγμένες απειλές στον κυβερνοχώρο μπορούν να διαταράξουν ή να καταστρέψουν ζωτικές κοινωνικές και οικονομικές λειτουργίες. Επίσης, τα κενά σε θέματα Ασφάλειας Δικτύων και Πληροφοριών εξακολουθούσαν να υπάρχουν σε ολόκληρη την ΕΕ, κυρίως όσον αφορά στις ικανότητες των εθνών, το συντονισμό σε περιπτώσεις συμβάντων που εκτείνονται πέρα από τα σύνορα, τη συμμετοχή και ετοιμότητα του ιδιωτικού τομέα. Έτσι το 2012 καθιερώνεται η Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης στην Πληροφορική, υπεύθυνη για την ασφάλεια των συστημάτων πληροφορικής της ΕΕ, των ιδρυμάτων, των οργανισμών και των φορέων (CERT-EU). Αποτελεί υποχρέωση όλων των κρατών μελών να ιδρύσουν εύρυθμα λειτουργούσες ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) που να συμμορφώνονται με τις βασικές απαιτήσεις, ώστε να διασφαλίζονται αποτελεσματικές και συμβατές ικανότητες για την αντιμετώπιση συμβάντων και κινδύνων και να εξασφαλίζεται αποτελεσματική συνεργασία σε ενωσιακό επίπεδο. Οι απαιτήσεις και τα καθήκοντα της CERT είναι επαρκώς και σαφώς καθορισμένα και στηρίζονται από εθνική πολιτική και κανονιστική ρύθμιση.

Η CERT εξασφαλίζει ευρεία διαθεσιμότητα των υπηρεσιών επικοινωνιών της αποφεύγοντας αστοχίες και προσφέρει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους. Οι δίαυλοι επικοινωνίας πρέπει να είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στην κοινότητα και στους εταίρους της συνεργασίας. Επιπλέον, εφαρμόζει και διαχειρίζεται μέτρα ασφάλειας για να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα των πληροφοριών που λαμβάνει και χειρίζεται, ενώ παράλληλα τα γραφεία της και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους. Περαιτέρω, συστήνεται σύστημα ποιότητας διαχείρισης υπηρεσιών για την παρακολούθηση των ε-

πιδόσεων της CERT και για την εξασφάλιση διαρκούς διαδικασίας βελτίωσης. Βασίζεται σε σαφώς καθορισμένα κριτήρια μέτρησης που περιλαμβάνουν επίσημα επίπεδα παρεχόμενων υπηρεσιών και βασικούς δείκτες επιδόσεων. Τέλος, αναφορικά με τη συνέχεια της επιχειρηματικής δραστηριότητας, η CERT είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων, είναι επαρκώς στελεχωμένη ώστε να εξασφαλίζεται η διαθεσιμότητα ανά πάσα στιγμή και βασίζεται σε υποδομή, η συνέχεια της οποίας είναι διασφαλισμένη. Για το σκοπό αυτό, συστήνονται πλεονάζοντα συστήματα και εφεδρικές περιοχές εργασίας για τη CERT, ώστε να εξασφαλίζεται διαρκής πρόσβαση στους τρόπους επικοινωνίας.

Στα καθήκοντα της CERT περιλαμβάνονται η παρακολούθηση συμβάντων σε εθνικό επίπεδο, η παροχή έγκαιρης προειδοποίησης, ειδοποιήσεων επαγρύπνησης, ανακοινώσεων και διάδοσης των πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα, η απόκριση σε συμβάντα, η παροχή δυναμικής ανάλυσης κινδύνου και συμβάντων και επίγνωση της κατάστασης, η ανάπτυξη ευρείας ευαισθητοποίησης του κοινού σχετικά με τους κινδύνους που συνδέονται με δραστηριότητες στο διαδίκτυο, καθώς και η διοργάνωση εκστρατειών ευαισθητοποίησης για την Ασφάλεια Δικτύων και Πληροφοριών. Επιπλέον, η CERT εγκαθιδρύει σχέσεις συνεργασίας με τον ιδιωτικό τομέα. Προς διευκόλυνση της συνεργασίας, η CERT προωθεί την υιοθέτηση και χρήση κοινών ή τυποποιημένων πρακτικών για διαδικασίες χειρισμού συμβάντων ή κινδύνου, συστήματα ταξινόμησης συμβάντων, κινδύνου και πληροφοριών, ταξινομήσεις για συστήματα μέτρησης, μορφότυπους ανταλλαγής πληροφοριών σχετικά με κινδύνους, συμβάντα, καθώς και συμβάσεις ονοματοδοσίας συστημάτων.

Οι εθνικές CERT από την πλευρά τους, πρέπει να αποτελούν μέρος ενός αποτελεσματικού δικτύου στο οποίο ανταλλάσσονται πληροφορίες σύμφωνα με τα απαραίτητα πρότυπα εμπιστοσύνης και εμπιστευτικότητας (http://www.enisa.europa.eu).

4.1.3 Ευρωπαϊκή Κοινοπραξία Δημοσίου – Ιδιωτικού Τομέα για την Ανθεκτικότητα - EP3R (European Public-Private Partnership For Resilience)

Οι εθνικές αρμόδιες αρχές Ασφάλειας Δικτύων και Πληροφοριών είναι εκείνες που πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες με άλλα ρυθμιστικά όργανα, όπως με τις αρχές προστασίας προσωπικών δεδομένων και με τις αρχές επιβολής του νόμου σε περίπτωση εντοπισμού σοβαρής εγκληματικής ενέργειας. Επίσης, πρέπει να δημοσιεύουν τακτικά στον κοινό ιστότοπο μη διαβαθμισμένες πληροφορίες σχετικά με τις έγκαιρες προειδοποιήσεις και τις συντονισμένες αποκρίσεις για περιστατικά και κινδύνους Ασφάλειας Δικτύων και Πληροφοριών.

Για την ενίσχυση, όμως, των επιπέδων ασφαλείας και την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών, κρίνεται απαραίτητη η ανάπτυξη συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα. Η σύσταση της Ευρωπαϊκής Κοινοπραξίας Δημόσιου-Ιδιωτικού Τομέα για την Ανθεκτικότητα (EP3R), μιας αξιόπιστης και έγκυρης πλατφόρμας σε επίπεδο ΕΕ, ήταν ορόσημο για τη συμμετοχή του ιδιωτικού τομέα στη βελτίωση του επιπέδου ασφάλειας του ψηφιακού περιβάλλοντος και στην ανάπτυξη μιας αξιόπιστης αγοράς για την ασφάλεια των πληροφοριών στην Ευρώπη. Η Επιτροπή έχει σκοπό να ενισχύσει τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα σε στόχους ασφάλειας και ικανότητας αποκατάστασης, βασικές απαιτήσεις, ορθή πρα-

κτική μέτρων και πολιτικής. Το κύριο βάρος της EP3R αφορά στην ευρωπαϊκή διάσταση προοπτικών στρατηγικού και τακτικού/επιχειρησιακού χαρακτήρα, όπως η βιομηχανική ανάπτυξη. Η EP3R πρέπει να στηρίζεται και να συμπληρώνει τις υπάρχουσες εθνικές πρωτοβουλίες και τις επιχειρησιακές δραστηριότητες του ENISA.

4.2 Τομέας επιβολής του Νόμου

Η καταπολέμηση των εγκλημάτων στον κυβερνοχώρο, η οποία αποτελεί ύψιστη προτεραιότητα, ως βασική νομική πράξη έχει τη Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο που έγινε στη Βουδαπέστη στις 23 Νοεμβρίου 2001(γνωστή και ως σύμβαση της Βουδαπέστης). Η σύμβαση συνοδεύεται από πρόσθετο πρωτόκολλο στη σύμβαση για το έγκλημα στον κυβερνοχώρο σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, οι οποίες διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών.

Παρά την πρόοδο που είχε σημειωθεί στο θέμα της ασφάλεια για το έγκλημα στον κυβερνοχώρο ως το 2012, υπήρχαν ακόμη αρκετά εμπόδια που δυσκόλευαν την αποτελεσματική διερεύνηση των εγκλημάτων στον κυβερνοχώρο και τη δίωξη των δραστών σε ευρωπαϊκό επίπεδο. Κάποια από αυτά ήταν τα όρια της δικαιοδοσίας, οι ανεπαρκείς ικανότητες στον τομέα της ανταλλαγής πληροφοριών, οι τεχνικές δυσχέρειες στην ανίχνευση της προέλευσης των δραστών, οι διαφορετικές ερευνητικές και εγκληματολογικές ικανότητες, η έλλειψη ειδικευμένου προσωπικού και μη τακτική συνεργασία με άλλους αρμόδιους φορείς για την ασφάλεια στον κυβερνοχώρο.

Επιπρόσθετα, η ΕΕ είχε να αντιμετωπίσει τις ταχέως εξελισσόμενες διεθνείς απειλές στις αναπτυσσόμενες και στις ευρισκόμενες σε μεταβατικό στάδιο χώρες, όπου συχνά απουσιάζουν οι απαιτούμενες ικανότητες για την καταπολέμηση του οργανωμένου εγκλήματος στον κυβερνοχώρο.

Για να αντιμετωπίσει τις προκλήσεις, η Ευρωπαϊκή Επιτροπή εξέδωσε στις 28 Μαρτίου του 2012 την ανακοίνωσή της προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο με τίτλο: «Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: Ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο». Το EC3 ξεκίνησε να λειτουργεί τον Ιανουάριο του 2013.

4.2.1 Το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον Κυβερνοχώρο EC3 (European Cybercrime Center)

Το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3), εστιάζει στους ακόλουθους βασικούς άξονες εγκλημάτων στον κυβερνοχώρο τηρώντας συγχρόνως την αρχή της επικουρικότητας:

(i) εγκλήματα στον κυβερνοχώρο που διαπράττονται από ομάδες οργανωμένου εγκλήματος, ιδίως εγκλήματα που αποφέρουν τεράστια κέρδη όπως η επιγραμμική απάτη.

(ii) εγκλήματα στον κυβερνοχώρο που προκαλούν σοβαρές βλάβες στα θύματά τους, όπως η επιγραμμική σεξουαλική εκμετάλλευση παιδιών.

(iii) εγκλήματα στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο, που επηρεάζουν βασικά συστήματα υποδομών και πληροφοριών στην Ένωση.

Λαμβάνοντας υπόψη την αδιάλειπτα εξελισσόμενη φύση των εγκλημάτων στον κυβερνοχώρο, το εν λόγω Κέντρο είναι σε θέση να αναλαμβάνει δράση ανταποκρινόμενο σε αιτήματα κρατών μελών, και να αντιμετωπίζει την εμφάνιση νέων απειλών για την Ένωση στον τομέα των εγκλημάτων στον κυβερνοχώρο.

Το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο (EC3) εκπληρώνει τέσσερις βασικές λειτουργίες:

α) *Χρησιμεύει ως ευρωπαϊκό εστιακό σημείο πληροφοριών για τα εγκλήματα στον κυβερνοχώρο*.

Η λειτουργία της συγχώνευσης πληροφοριών διασφαλίζει τη συλλογή πληροφοριών για εγκλήματα στον κυβερνοχώρο από το ευρύτερο δυνατό φάσμα δημόσιων, ιδιωτικών και ανοικτών πηγών, εμπλουτίζοντας τα διαθέσιμα στοιχεία της αστυνομίας. Με τον τρόπο αυτό καλύπτονται προοδευτικά τα σημερινά κενά στις πληροφορίες που παρέχονται από τις κοινότητες που είναι υπεύθυνες για την ασφάλεια και την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο. Οι συλλεγόμενες πληροφορίες αφορούν σε δραστηριότητες, μεθόδους και υπόπτους στον τομέα των εγκλημάτων στον κυβερνοχώρο. Η λειτουργία χρησιμεύει τόσο στη βελτίωση των γνώσεων για τα εγκλήματα στον κυβερνοχώρο και την πρόληψη, την ανίχνευση και τη δικαστική του ς δίωξη, όσο και στην προώθηση κατάλληλων συνδέσμων μεταξύ των αρχών επιβολής του νόμου, της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και των εμπειρογνωμόνων ασφάλειας των τεχνολογιών της πληροφορίας και επικοινωνίας που υπάγονται στον ιδιωτικό τομέα. Κατά την ανταλλαγή πληροφοριών τα διάφορα μέρη τηρούν τους κανόνες και τις συμφωνίες περί εμπιστευτικότητας. Η λειτουργία της συγχώνευσης πληροφοριών είναι επίσης χρήσιμη για τη βελτίωση της υποβολής αναφορών για το έγκλημα στον κυβερνοχώρο και της ανταλλαγής πληροφοριών. Επιθυμία της Επιτροπής είναι η επιβολή από τα κράτη μέλη υποχρέωσης αναφοράς των σοβαρών αδικημάτων στον κυβερνοχώρο στις εθνικές αρχές επιβολής του νόμου. Με τον τρόπο αυτό οι εθνικές αστυνομικές υπηρεσίες είναι σε θέση να παρέχουν συστηματικότερα πληροφορίες για σοβαρά αδικήματα στον κυβερνοχώρο στο εν λόγω Κέντρο (EC3), το οποίο με τη σειρά του διαβιβάζει τις εν λόγω πληροφορίες ούτως ώστε να ενημερώνονται συνάδελφοι σε άλλα κράτη μέλη που επιδιώκουν τον ίδιο στόχο και να επωφελούνται από τις πληροφορίες που συγκεντρώνουν οι συνάδελφοί τους στις έρευνες. Ο στόχος είναι να αποκρυσταλλωθεί με την πάροδο του χρόνου μια σαφέστερη εικόνα για τα εγκλήματα στον κυβερνοχώρο στην Ευρώπη, ούτως ώστε να εκπονούνται υψηλής ποιότητας στρατηγικές εκθέσεις σχετικά με τις τάσεις και τις απειλές, να αποκτηθούν βαθιές γνώσεις βασισμένες σε ολοκληρωμένα αριθμητικά στοιχεία για τα εγκλήματα και να βελτιωθούν οι επιχειρησιακές πληροφορίες που θα προέρχονται από βάση η οποία αντλεί τα δεδομένα από ευρύ φάσμα πηγών[77].

[77] Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https:// register. consilium.europa.eu/doc/srv?l=EL&f=ST%208543% 202012%20INIT (πρόσβαση στις 13-11-2019).
.

β) Συγκεντρώνει την ευρωπαϊκή εμπειρογνωμοσύνη στον τομέα των εγκλημάτων στον κυβερνοχώρο προκειμένου να ενισχυθούν τα κράτη μέλη στην ανάπτυξη ικανοτήτων.

Το εν λόγω Κέντρο (EC3) συνδράμει τα κράτη μέλη παρέχοντας εμπειρογνωμοσύνη και κατάρτιση ούτως ώστε να περιοριστούν τα εγκλήματα στον κυβερνοχώρο. Ο κύριος στόχος είναι η επιβολή του νόμου, αλλά πρέπει επίσης να παρασχεθεί κατάρτιση στις δικαστικές αρχές. Οι ήδη αναληφθείσες πρωτοβουλίες της Europol, της CEPOL και των κρατών μελών εκσυγχρονίστηκαν μετά από μια εις βάθος ανάλυση των αναγκών για την εξασφάλιση μεγαλύτερου συντονισμού και συμπληρωματικότητας. Η κατάρτιση αυτή καλύπτει από εξειδικευμένη τεχνική εμπειρογνωμοσύνη έως ευρύτερη ανάπτυξη ικανοτήτων για αστυνομικούς, εισαγγελείς και δικαστές για τον χειρισμό υποθέσεων σχετικών με εγκλήματα στον κυβερνοχώρο.

Δημιουργείται γραφείο συνδρομής (helpdesk) για την ανταλλαγή βέλτιστων πρακτικών και γνώσεων και για τις επαφές με τα κράτη μέλη και τις διεθνείς αρχές επιβολής του νόμου, τις δικαστικές αρχές, τον ιδιωτικό τομέα και τις οργανώσεις της κοινωνίας των πολιτών και για να δίδονται απαντήσεις στα ερωτήματά τους, για παράδειγμα, σε περίπτωση επιθέσεων στον κυβερνοχώρο ή νέων μορφών απατών στο Διαδίκτυο.

Το γραφείο αυτό στηρίζει τις δραστηριότητες ομάδων εμπειρογνωμόνων για εγκλήματα στον κυβερνοχώρο και παρέχει συμβουλές σε αυτές, καθώς και στην ομάδα δράσης της Ευρωπαϊκής Ένωσης για τα εγκλήματα στον κυβερνοχώρο και σε εμπειρογνώμονες για την καταπολέμηση της επιγραμμικής σεξουαλικής εκμετάλλευσης παιδιών. Συνεργάζεται επίσης με το αναπτυσσόμενο δίκτυο κέντρων αριστείας για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο, όπως το «2Centre», καθώς και με την κοινότητα των ερευνητών.

Το Κέντρο (EC3) βοηθήσει τα κράτη μέλη στην ανάπτυξη και εγκατάσταση επιγραμμικής εφαρμογής για τις αναφορές εγκλημάτων στον κυβερνοχώρο, με βάση συμφωνηθέντα πρότυπα, προκειμένου να συνδεθεί η ροή αναφορών από μια σειρά παράγοντες (εταιρείες, εθνικές/κυβερνητικές ομάδες αντιμετώπισης εκτάκτων αναγκών στην πληροφορική - CERT, πολίτες κ.λπ) στους εθνικούς φορείς επιβολής του νόμου και από τους εθνικούς φορείς επιβολής του νόμου στο EC3.

Το Κέντρο (EC3) διευκολύνει επίσης την ανταλλαγή βέλτιστων πρακτικών σε επίπεδο ποινικής δικαιοσύνης και επιβολής του νόμου. Η αποτελεσματική συμμετοχή των δικαστικών αρχών στην αντιμετώπιση του εγκλήματος στον κυβερνοχώρο έχει καθοριστική σημασία για τη βελτίωση της δίωξης των σοβαρών εγκλημάτων στον κυβερνοχώρο στα κράτη μέλη[78].

γ) Στηρίζει τις έρευνες των κρατών μελών για τα εγκλήματα στον κυβερνοχώρο.

[78] Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https:// register. consilium.europa.eu/doc/srv?l=EL&f=ST%208543% 202012%20INIT (πρόσβαση στις 14-11-2019).

Το EC3 παρέχει επιχειρησιακή στήριξη σε έρευνες για εγκλήματα στον κυβερνοχώρο, ενθαρρύνοντας για παράδειγμα τη σύσταση κοινών ομάδων ερευνών για εγκλήματα στον κυβερνοχώρο και την ανταλλαγή επιχειρησιακών πληροφοριών για τις έρευνες που βρίσκονται σε εξέλιξη.

Επίσης, παρέχει υψηλής στάθμης βοήθεια σε επίπεδο ανάλυσης (διευκολύνσεις, αποθήκευση, εργαλεία) και εμπειρογνωμοσύνη στον τομέα της κρυπτογράφησης για έρευνες εγκλημάτων στον κυβερνοχώρο.

δ) Καθίσταται η συλλογική φωνή των ευρωπαίων διενεργούντων έρευνες εγκλημάτων στον κυβερνοχώρο στο επίπεδο του δικαστικού τομέα και του τομέα της επιβολής του νόμου

Το εν λόγω Κέντρο (EC3) λειτουργεί ως σημείο συσπείρωσης για ευρωπαίους διενεργούντες έρευνες εγκλημάτων στον κυβερνοχώρο, εξασφαλίζοντάς τους ενιαία φωνή στις συζητήσεις με τη βιομηχανία των ΤΠΕ και άλλες επιχειρήσεις του ιδιωτικού τομέα καθώς και με την κοινότητα των ερευνητών, τις ενώσεις χρηστών και τις οργανώσεις της κοινωνίας των πολιτών σχετικά με τους καλύτερους τρόπους αποτροπής των εγκλημάτων στον κυβερνοχώρο και τον συντονισμό εστιασμένων δραστηριοτήτων ερευνών.

Το Κέντρο (EC3) συνιστά το φυσικό σημείο επαφής για τις δραστηριότητες καταπολέμησης εγκλημάτων στον κυβερνοχώρο της Interpol και άλλων διεθνών αστυνομικών μονάδων καταπολέμησης των εν λόγω εγκλημάτων. Συντονίζει επίσης τις συνεισφορές στις υφιστάμενες πρωτοβουλίες διακυβέρνησης του Διαδικτύου και στην ανοικτή διακυβερνητική ομάδα εμπειρογνωμόνων του ΟΗΕ για την εγκληματικότητα στον κυβερνοχώρο.

Το εν λόγω Κέντρο (EC3) συνεργάζεται επίσης με φορείς, όπως το INSAFE[79], στο πλαίσιο της διοργάνωσης εκστρατειών ευαισθητοποίησης του κοινού, προσαρμόζοντάς τις στις μεταβολές που εντοπίζει το Κέντρο στις αναλύσεις των εγκλημάτων στον κυβερνοχώρο, ούτως ώστε να ενθαρρυνθεί η συνετή και ασφαλής επιγραμμική συμπεριφορά[80].

Το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο αποτελεί μέρος της Europol και εδρεύει στις υπάρχουσες εγκαταστάσεις της. Τούτο παρέχει σημαντικά πλεονεκτήματα καθώς ο ρόλος της Europol είναι αναγνωρισμένος μεταξύ των κρατών μελών και των λοιπών ενδιαφερομένων φορέων, συμπεριλαμβανομένης της Interpol και των διεθνών αρχών επιβολής του νόμου, ενώ διαθέτει ήδη εντολή να λάβει μέτρα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος[81]. Κύριο καθήκον της Europol είναι να συμβάλει σε μια ασφαλέστερη Ευρώπη προς όφελος όλων των πολιτών, στηρίζοντας τις υπηρεσίες επιβολής του νόμου της ΕΕ μέσω της ανταλλαγής και επεξεργασίας πληροφοριών ποινικού χαρακτήρα.

[79] European Network of Awareness Centres - Ευρωπαϊκό Δίκτυο Κέντρων Ευαισθητοποίησης που προωθούν την ασφαλή, υπεύθυνη χρήση του διαδικτύου και κινητών συσκευών από τους νέους.
[80] Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https:// register. consilium.europa.eu/doc/srv?l=EL&f=ST%208543% 202012%20INIT (πρόσβαση στις 14-11-2019).
[81] Απόφαση του Συμβουλίου (2009/371/ΔΕΥ) της 6 Απριλίου 2009 για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας, άρθρο 4 παράγραφος 1 σε συνδυασμό με παράρτημα.

Καθίσταται σαφές ότι η ίδρυση του Ευρωπαϊκού Κέντρου για εγκλήματα στον Κυβερνοχώρο έχουν επιφέρει αύξηση των πόρων καθώς απαιτήθηκαν επιπλέον αποσπάσεις υπαλλήλων από κράτη μέλη. Η Επιτροπή, κατά την αξιολόγηση των αναγκών σε πόρους, έχει λάβει υπόψη τρία στοιχεία: πρώτον, τη μέτρια αύξηση του συνολικού αριθμού των υποθέσεων εγκλημάτων στον κυβερνοχώρο και όχι μια μαζική αύξηση των εν λόγω εγκλημάτων· δεύτερον, την ενίσχυση των ικανοτήτων των κρατών μελών για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο και τρίτον, την εστίαση του εν λόγω Κέντρου (EC3) σε ορισμένους τύπους εγκλημάτων στον κυβερνοχώρο.

Με την εγκατάσταση του εν λόγω Κέντρου (EC3) στην Europol, ήταν σημαντικό να διασφαλιστεί η συμμετοχή άλλων σημαντικών ενδιαφερόμενων φορέων στη στρατηγική διεύθυνση του κέντρου. Ως εκ τούτου, συστήθηκε επιτροπή διεύθυνσης του Κέντρου (EC3) εντός της δομής διακυβέρνησης της Europol, της οποίας προΐσταται ο διευθυντής του Κέντρου (EC3). Το όργανο αυτό παρέχει σε άλλους ενδιαφερόμενους φορείς, όπως η Eurojust, η CEPOL, τα κράτη μέλη εκπροσωπούμενα από την ομάδα δράσης της ΕΕ για εγκλήματα στον κυβερνοχώρο, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών - ENISA και η Επιτροπή, τη δυνατότητα να συνεισφέρει ο καθένας την τεχνογνωσία του, χωρίς να δημιουργούνται πρόσθετες περιττές διοικητικές επιβαρύνσεις. Η επιτροπή αυτή συμβάλλει στην ενίσχυση της λογοδοσίας κατά την άσκηση των δραστηριοτήτων του Κέντρου (EC3) για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο και με τον τρόπο αυτό διασφαλίζει την υλοποίησή τους σε πνεύμα συνεργασίας, αναγνωρίζοντας την προστιθέμενη εμπειρογνωμοσύνη και λαμβάνοντας υπόψη τις εντολές όλων των ενδιαφερομένων φορέων.

Το εν λόγω Κέντρο (EC3) διασφαλίζει μια συντονισμένη απάντηση στα εγκλήματα στον κυβερνοχώρο, όχι μόνο καθιστώντας δυνατή τη συνεργασία μεταξύ οργανισμών της ΕΕ, αλλά και λειτουργώντας ως ενιαίο ευρωπαϊκό σημείο επαφής στον εν λόγω τομέα.

Σε επίπεδο κρατών – μελών ο κύριος στόχος είναι να βοηθηθούν τα κράτη μέλη στην καταπολέμηση των εγκλημάτων στον κυβερνοχώρο. Το γραφείο συνδρομής και οι παρεχόμενες από το Κέντρο (EC3) υπηρεσίες, όπως η πιο εστιασμένη ανάλυση των απειλών και η καλύτερα ενημερωμένη επιχειρησιακή στήριξη, αποβαίνουν επωφελή για όλους όσοι διεξάγουν στην Ευρώπη έρευνες για εγκλήματα στον κυβερνοχώρο. Η ομάδα δράσης της ΕΕ για εγκλήματα στον κυβερνοχώρο διασφαλίζει ότι οι ανησυχίες των κρατών μελών λαμβάνονται υπόψη από την ομάδα διεύθυνσης του Κέντρου (EC3). Επιπλέον, τα κράτη μέλη καλούνται να συνεχίσουν να υλοποιούν τις αναγκαίες επενδύσεις στις εθνικές τους δομές καταπολέμησης των εγκλημάτων στον κυβερνοχώρο, ούτως ώστε να διαθέτουν κατάλληλες διεπαφές για διάδραση με το Κέντρο (EC3)[82].

Σε επίπεδο ευρωπαϊκών οργανισμών, σχετικοί οργανισμοί, όπως η Eurojust, η CEPOL και ο ENISA, καθώς και η CERT-EU, συμμετέχουν άμεσα στις δραστηριότητες του EC3, όχι μόνο συμμετέχοντας στην επιτροπή διεύθυνσης, αλλά και μέσω επιχειρησιακής συνεργασίας, κατά περίπτωση, και λαμβάνοντας υπόψη τις αντίστοιχες εντολές τους.

[82] Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https:// register. consilium.europa.eu/doc/srv?l=EL&f=ST%208543% 202012%20INIT (πρόσβαση στις 14-11-2019).

Σε διεθνές επίπεδο, το εν λόγω Κέντρο (EC3), στο πλαίσιο της προσπάθειάς του να εξελιχθεί σε ευρωπαϊκό εστιακό σημείο πληροφοριών για εγκλήματα στον κυβερνοχώρο, καθίσταται πολύτιμος συνομιλητής των διεθνών εταίρων στα θέματα καταπολέμησης των εγκλημάτων στον κυβερνοχώρο. Το Κέντρο (EC3), σε συνεργασία με την Interpol και τους στρατηγικούς μας εταίρους σε όλο τον κόσμο, να επιδιώκει να βελτιώσει τις συντονισμένες απαντήσεις στην καταπολέμηση των εγκλημάτων στον κυβερνοχώρο και διασφαλίζει ότι στην περαιτέρω ανάπτυξη του κυβερνοχώρου θα λαμβάνονται υπόψη οι ανάγκες εφαρμογής του νόμου.

Στο επίπεδο του ιδιωτικού τομέα και των οργανώσεων της κοινωνίας των πολιτών, η οικοδόμηση κλίματος εμπιστοσύνης μεταξύ του ιδιωτικού τομέα και των αρχών επιβολής του νόμου έχει πρωταρχική σημασία στον αγώνα για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Εδραιώνοντας το έργο της Europol με τους υφιστάμενους και τους νέους εταίρους, το Κέντρο (EC3) αναπτύσσει δίκτυα εμπιστοσύνης και πλατφόρμες ανταλλαγής πληροφοριών με τη βιομηχανία και άλλους συντελεστές όπως η κοινότητα ερευνών και οι οργανώσεις της κοινωνίας των πολιτών. Τα εν λόγω δίκτυα και πλατφόρμες διευκολύνουν την διακοινοτική ανταλλαγή πληροφοριών σε μια σειρά θεμάτων, συμπεριλαμβανομένης της έγκαιρης προειδοποίησης για απειλές στον κυβερνοχώρο, καθώς και τις συλλογικές απαντήσεις τύπου «ομάδας δράσης» στις επιθέσεις στον κυβερνοχώρο και στις άλλες μορφές εγκλημάτων στον κυβερνοχώρο. Το Κέντρο (EC3) επίσης συμβάλλει στις ευρύτερες προσπάθειες των επιχειρήσεων του ιδιωτικού τομέα που διαθέτουν σημαντικά ψηφιακά στοιχεία, όπως οι τράπεζες και οι διαδικτυακές εταιρείες λιανικής πώλησης, να καταπολεμήσουν και να προστατευθούν καλύτερα από τα εγκλήματα στον κυβερνοχώρο, και να ελαχιστοποιήσουν τις αδυναμίες στην ανάπτυξη τεχνολογιών. Οι αρχές επιβολής του νόμου και ο ιδιωτικός τομέας έχουν κοινό συμφέρον να καταλήξουν σε μια σαφέστερη εικόνα των εγκλημάτων στον κυβερνοχώρο, σε πραγματικό χρόνο, καθώς και να επιδιώξουν την αποτελεσματικότερη εξάρθρωση των δικτύων εγκλημάτων στον κυβερνοχώρο μέσω της εντατικότερης ανίχνευσης των νέων modi operandi και της ταχείας σύλληψης των δραστών εγκλημάτων στον κυβερνοχώρο[83].

4.2.2 Europol

Η Απόφαση 2009/371/ΔΕΥ του Συμβουλίου ίδρυσε την Ευρωπαϊκή Αστυνομική Υπηρεσία (Europol) ως οργανισμό της ΕΕ με έδρα τη Χάγη της Ολλανδίας. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία μέσω κανονισμών, δύνανται να καθορίζουν τη δομή, τη λειτουργία, το πεδίο δράσης και τα καθήκοντα της Europol. Τα καθήκοντα αυτά μπορούν να περιλαμβάνουν τη συλλογή, αποθήκευση, επεξεργασία, ανάλυση και ανταλλαγή πληροφοριών που διαβιβάζονται ιδίως από τις αρχές των κρατών – μελών ή τρίτων χωρών, ή οργανισμών και τον συντονισμό, τη διοργάνωση και τη διεξαγωγή ερευνών και επιχειρησιακών δράσεων, από κοινού με τις αρμόδιες αρχές των κρατών – μελών ή στο πλαίσιο κοινών ομάδων ερευνών, ενδεχομένως σε σύνδεση με την Eurojust. Κάθε επιχειρησιακή δράση της της Europol πρέπει να διεξάγεται σε συνεργασία και σε συμφωνία με τις αρχές του κράτους – μέλους ή των κρατών – μελών στο έδαφος του

[83] Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https:// register. consilium.europa.eu/doc/srv?l=EL&f=ST%208543% 202012%20INIT (πρόσβαση στις 14-11-2019).

οποίου ή των οποίων διεξάγονται (άρθρο 88 ΣΛΕΕ). Οι αρμοδιότητες της Europol εκτείνονται στην πάταξη της τρομοκρατίας, του οργανωμένου εγκλήματος, του εγκλήματος στον κυβερνοχώρο, καθώς και στην αντιμετώπιση των σοβαρών μορφών διεθνούς εγκληματικότητας. Στα καθήκοντα της Europol επιπλέον περιλαμβάνονται η ανταλλαγή και ανάλυση των στοιχείων σχετικά με το λαθρεμπόριο ναρκωτικών και πυρηνικών υλικών, τα κυκλώματα λαθρομετανάστευσης, η εμπορία ανθρώπων και το λαθρεμπόριο οχημάτων[84].

Τα μεγάλης κλίμακας εγκληματικά και τρομοκρατικά δίκτυα αποτελούν σημαντική απειλή για την εσωτερική ασφάλεια της Ε.Ε και για την ασφάλεια και τον βιοπορισμό των λαών της. Οι μεγαλύτερες απειλές στην ασφάλεια προέρχονται από την τρομοκρατία, τη διεθνή διακίνηση ναρκωτικών και το ξέπλυμα βρώμικου χρήματος, τις οργανωμένες απάτες, την πλαστογράφηση του ευρώ και το λαθρεμπόριο ανθρώπων. Ωστόσο, νέοι κίνδυνοι συσσωρεύονται με το κυβερνοέγκλημα, το εμπόριο ανθρώπων και άλλες σύγχρονες απειλές. Αυτή είναι μία επιχείρηση πολλών δισεκατομμυρίων ευρώ, εύκολα προσαρμοζόμενη σε νέες ευκαιρίες και ανθεκτική στα παραδοσιακά μέτρα επιβολής του νόμου. Η Europol προσφέρει τακτικά συνδρομή σε διεθνείς αστυνομικές επιχειρήσεις. Το 2011, η επιχείρηση Rescue, στην οποία η Europol διαδραμάτισε καθοριστικό ρόλο, κατέληξε στην ταυτοποίηση 779 υπόπτων σε πολλές χώρες (από τους οποίους συνελήφθησαν 250) και στη διάσωση 252 παιδιών. Χάρη στο έργο των αναλυτών της Europol, οι οποίοι έσπασαν τους κωδικούς ασφαλείας ενός βασικού εξυπηρετητή υπολογιστή στο κέντρο του δικτύου, αποκαλύφθηκε η ταυτότητα και οι δραστηριότητες των ύποπτων για τη διάπραξη των αξιόποινων πράξεων. Η Europol εργάζεται στενά με τις υπηρεσίες επιβολής του νόμου των 28 κρατών - μελών της Ε.Ε. και με άλλα εκτός Ε.Ε. κράτη, όπως η Αυστραλία, ο Καναδάς, οι ΗΠΑ και η Νορβηγία. Η υπηρεσία χρησιμοποιεί τις μοναδικές ικανότητες πληροφόρησης και την ειδίκευση του προσωπικού της για να ταυτοποιήσει και να εντοπίσει τα πλέον επικίνδυνα εγκληματικά και τρομοκρατικά δίκτυα στην Ευρώπη.

Οι αρχές επιβολής του νόμου στην Ε.Ε. βασίζονται σε αυτή την εργασία και στις υπηρεσίες επιχειρησιακού κέντρου συντονισμού και ασφάλειας δικτύων και πληροφοριών της Europol για να διεξάγουν 18.000 διασυνοριακές έρευνες κάθε χρόνο. Κατ' αυτό τον τρόπο έχουν διασπαστεί πολλά εγκληματικά και τρομοκρατικά δίκτυα, έχουν συλληφθεί χιλιάδες επικίνδυνοι εγκληματίες, στην ανάκτηση χιλιάδων ευρώ σε εγκληματικές ενέργειες και στην ανάκτηση από βλάβη εκατοντάδων θυμάτων, συμπεριλαμβανομένων διακινούμενων παιδιών για σεξουαλική εκμετάλλευση.

Η Europol ενεργεί σαν μείζον κέντρο ειδίκευσης σε τομείς - κλειδιά των δραστηριοτήτων επιβολής του νόμου και σαν ένα Ευρωπαϊκό κέντρο στρατηγικής κατασκοπείας του οργανωμένου εγκλήματος[85].

4.2.3 Οργανισμός της Ευρωπαϊκής Ένωσης για την κατάρτιση στον τομέα της επιβολής του νόμου (European Police College- Cepol)

Η Ευρωπαϊκή Αστυνομική Ακαδημία (ΕΑΑ) ιδρύθηκε με την Απόφαση 2005/681/ΔΕΥ του Συμβουλίου ως όργανο της Ένωσης για την κατάρτιση των υψηλό-

[84] Μούσης Ν., Ευρωπαϊκή Ένωση, Δίκαιο, Οικονομία, Πολιτική, Εκδόσεις Παπαζήση, (2015) σελ. 160.
[85] Επίσημος Διαδικτυακός ιστότοπος της Europol - www.europol.europa.eu/content/page/about-us (πρόσβαση στις 20-11-2019).

βαθμων αστυνομικών στελεχών των κρατών μελών και τη διευκόλυνση της συνεργασίας μεταξύ των εθνικών αστυνομικών αρχών, μέσω της διοργάνωσης και του συντονισμού δραστηριοτήτων κατάρτισης σχετικών με την ευρωπαϊκής εμβέλειας αστυνόμευση και έχει την έδρα της στη Βουδαπέστη της Ουγγαρίας.

Από την 1η Ιουλίου 2016, δυνάμει του Κανονισμού (ΕΕ) 2015/2219 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2015, η επίσημη ονομασία της CEPOL είναι «Οργανισμός της Ευρωπαϊκής Ένωσης για την κατάρτιση στον τομέα της επιβολής του νόμου».

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κατάρτιση στον τομέα της επιβολής του νόμου (CEPOL) είναι μία υπηρεσία της Ε.Ε. προορισμένη να παρέχει εκπαίδευση και μαθησιακές ευκαιρίες σε ανώτερους αξιωματικούς της αστυνομίας σε ζωτικά θέματα ασφαλείας της Ευρωπαϊκής Ένωσης και των πολιτών της. Η εκπαίδευση καλύπτει θέματα σχετιζόμενα με την ηγεσία στις τεχνικές επιβολής του νόμου και τη συνεργασία της Ε.Ε. για τα οικονομικά εγκλήματα. Οι δραστηριότητες είναι σχεδιασμένες να διευκολύνουν το διαμοιρασμό της γνώσης και την καλύτερη πρακτική και να συνεισφέρουν στην ανάπτυξη μίας κοινής Ευρωπαϊκής κουλτούρας επιβολής του νόμου.

Αποστολή της CEPOL ως Υπηρεσίας της Ευρωπαϊκής Ένωσης αποτελεί η συνεισφορά στην ευρωπαϊκή αστυνομική συνεργασία μέσω της μάθησης επ' ωφελεία των Ευρωπαίων πολιτών, όραμα της να αναγνωρίζεται από τις υπηρεσίες και τις αρχές στον αστυνομικό και εκπαιδευτικό κόσμο ως η πρωταρχική πηγή μάθησης και ανάπτυξης στον τομέα της εκπαίδευσης για ενισχυμένη συνεργασία και αστυνόμευση στην Ευρώπη, ενώ οι αξίες που την χαρακτηρίζουν συνίστανται στην πρωταρχική πηγή γνώσης, τον σεβασμό της διαφορετικότητας και την πίστη στην αστυνομία και την αστυνόμευση.

4.2.4 Eurojust

Η Eurojust είναι ένας οργανισμός της Ευρωπαϊκής Ένωσης για τη δικαστική συνεργασία στον τομέα της ποινικής δικαιοσύνης μεταξύ των κρατών μελών της ΕΕ. Ιδρύθηκε το 2002 με την Απόφαση 2002/187/ΔΕΥ του Συμβουλίου και έχει την έδρα της στη Χάγη της Ολλανδίας. Ιδρύθηκε ως αποτέλεσμα της απόφασης του Ευρωπαϊκού Συμβουλίου του Τάμπερε στις15-16 Οκτωβρίου 1999 να συσταθεί μια μόνιμη μονάδα δικαστικής συνεργασίας προκειμένου να βελτιωθεί η καταπολέμηση των σοβαρών μορφών εγκλήματος.

Η Eurojust διεγείρει και βελτιώνει τη συνεργασία για έρευνες και διώξεις μεταξύ των αρμόδιων αρχών στα κράτη μέλη, διευκολύνοντας ιδιαιτέρως την εκτέλεση της διεθνούς αμοιβαίας νομικής βοήθειας και την έκδοση ενταλμάτων σύλληψης. Η Eurojust υποστηρίζει με κάθε δυνατό τρόπο τις αρμόδιες αρχές των κρατών μελών να καταστήσουν τις έρευνες και τις διώξεις τους περισσότερο αποτελεσματικές όταν αντιμετωπίζουν διασυνοριακό έγκλημα.

Σε αίτημα ενός κράτους μέλους, η Eurojust μπορεί να βοηθήσει έρευνες και διώξεις που αφορούν το εν λόγω κράτος μέλος και ένα κράτος μη μέλος, αν έχει συναφθεί συμφωνία συνεργασίας ή εκδηλώνεται ουσιαστικό ενδιαφέρον στην παροχή τέτοιας βοήθειας.

Η αρμοδιότητα της Eurojust καλύπτει όλους τους τύπους εγκλήματος και αδικημάτων για τα οποία έχει δικαιοδοσία και η Europol, εγκληματικά παραπτώματα που επηρεάζουν τα οικονομικά συμφέροντα της Ευρωπαϊκής Κοινότητας, περιβαλλοντικά εγκλήματα και συμμετοχή σε εγκληματική οργάνωση. Για άλλους τύπους αδικημάτων, η Eurojust μπορεί να βοηθήσει στις έρευνες και τις διώξεις, κατόπιν αιτήματος του κράτους μέλους.

Η Eurojust εξασφαλίζει ότι οι ιθύνουσες αρχές ενημερώνουν η μία την άλλη σχετικά με έρευνες και διώξεις για τις οποίες έχουν ενημερωθεί, βοηθάει τις αρμόδιες αρχές εξασφαλίζοντας την καλύτερη δυνατή συνεργασία ερευνών και διώξεων, είναι αρωγός στη βελτίωση της συνεργασίας μεταξύ των αρμόδιων εθνικών αρχών, ιδιαιτέρως βασιζόμενη στις αναλύσεις της Europol, συνεργάζεται και συμβουλεύεται το Ευρωπαϊκό Δικαστικό Δίκτυο (European Judicial Network- EJN) και χρησιμοποιεί και συνεισφέρει στην βελτίωση βάσεων δεδομένων εγγράφων, βοηθάει τη Europol, ιδιαιτέρως με γνώμες βασιζόμενες σε αναλύσεις που έχουν διεξαχθεί από τη Europol, προσπαθεί να βελτιώνει τη συνεργασία μεταξύ των αρμόδιων αρχών, σε εναρμόνιση με τους στόχους της, καθώς και να προωθεί αιτήματα δικαστικής υποστήριξης όταν αυτά πραγματοποιούνται από τις αρμόδιες αρχές ενός κράτους μέλους, όταν αφορούν μία έρευνα ή μία δίωξη από αυτή την αρχή για μία συγκεκριμένη υπόθεση και όταν απαιτείται η παρέμβασή της με σκοπό τη συντονισμένη δράση,

Προκειμένου να φέρει εις πέρας το έργο της, η Eurojust διατηρεί προνομιούχες σχέσεις με τις EJN, Europol, το Ευρωπαϊκό Γραφείο κατά της Απάτης (Anti-Fraud Office - OLAF) και τους Δικαστές- Συνδέσμους (Liaison Magistrates). Δύναται επίσης, μέσω του Συμβουλίου, να συνάψει συμφωνίες συνεργασίας με μη μέλη κράτη και διεθνείς οργανισμούς ή σώματα για την ανταλλαγή πληροφοριών ή την απόσπαση αξιωματικών[86].

Το Διαδίκτυο, εξ ορισμού, δεν έχει ούτε εθνικούς φραγμούς ούτε ενιαία παγκόσμια δομή διακυβέρνησης. Στην προσπάθεια προώθησης και προστασίας της ελευθερίας στο διαδίκτυο, πρέπει να υπάρξει μέριμνα και για την προστασία των πολιτών από συμμορίες οργανωμένου εγκλήματος που επιδιώκουν να εκμεταλλευτούν τον ανοικτό χαρακτήρα του Διαδικτύου. Το έγκλημα στον κυβερνοχώρο διαπερνά τα σύνορα περισσότερο από οιαδήποτε άλλη μορφή εγκλήματος και απαιτείται από τις αρχές επιβολής του νόμου να υιοθετήσουν μια συντονισμένη και συνεργατική προσέγγιση από κοινού με δημόσιους και ιδιωτικούς ενδιαφερόμενους φορείς, πέρα από τα εθνικά σύνορα.

4.3 Τομέας της Άμυνας

4.3.1 Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης - ΕΥΕΔ (European External Action Service - EEAS)

Η Ευρωπαϊκή Ένωση διαδραματίζει σημαντικό ρόλο στις διεθνείς εξελίξεις, αναπτύσσοντας δράση στους τομείς της διπλωματίας, του εμπορίου, της αναπτυξιακής βοήθειας και της συνεργασίας με διεθνείς οργανισμούς.

[86] Επίσημος Διαδικτυακός ιστότοπος της Eurojust - www.eurojust.europa.eu/content/page/about-us (πρόσβαση στις 20-11-2019).

Η Συνθήκη της Λισαβόνας (2009) αποτέλεσε σημαντική εξέλιξη για την εξωτερική δράση της Ένωσης, καθώς θέσπισε τη θέση του Ύπατου Εκπροσώπου της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας και την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ), δηλ. το διπλωματικό σώμα της Ένωσης.

Η ΕΥΕΔ επικουρεί την Ύπατη Εκπρόσωπο διασφαλίζοντας τη συνέπεια και τον συντονισμό της εξωτερικής δράσης της Ένωσης, καταρτίζοντας προτάσεις πολιτικής και προετοιμάζοντας την εφαρμογή τους μετά την έγκρισή τους από το Συμβούλιο. Επικουρεί επίσης τον πρόεδρο του Ευρωπαϊκού Συμβουλίου και τον Πρόεδρο και τα μέλη της Ευρωπαϊκής Επιτροπής στον τομέα των εξωτερικών σχέσεων και αναπτύσσει στενή συνεργασία με τα κράτη μέλη. Μέρος της ΕΥΕΔ είναι ένα δίκτυο αντιπροσωπειών της ΕΕ σε όλο τον κόσμο.

4.3.2 Ευρωπαϊκή Υπηρεσία Άμυνας (European Defence Agency- EDA)

Η Ευρωπαϊκή Υπηρεσία Άμυνας ιδρύθηκε από την Κοινή Δράση του Συμβουλίου των Υπουργών στις 12 Ιουλίου του 2004 «για να υποστηρίξει τα κράτη μέλη και το Συμβούλιο στην προσπάθειά του να βελτιώσει τις Ευρωπαϊκές δυνατότητες άμυνας στον τομέα της διαχείρισης κρίσεων και να διατηρήσει την Ευρωπαϊκή Ασφάλεια και την Αμυντική Πολιτική ως έχει τώρα και να αναπτυχθεί στο μέλλον». Στις 12 Ιουλίου του 2011 το Συμβούλιο υιοθέτησε μία απόφαση που όριζε το καταστατικό, την έδρα και τους κανονισμούς λειτουργίας της Ευρωπαϊκής Υπηρεσίας Άμυνας. Η απόφαση αυτή του Συμβουλίου αντικατέστησε την Κοινή Δράση του Συμβουλίου.

Η Ευρωπαϊκή Υπηρεσία Άμυνας, στο πλαίσιο της συνολικής της αποστολής που καθορίζεται στην Κοινή Δράση, έχει επιφορτισθεί με τέσσερις λειτουργίες που καλύπτουν την ανάπτυξη αμυντικών ικανοτήτων, την προώθηση Αμυντικής Έρευνας και Τεχνολογίας (Defence Research and Technology- R&T), την προώθηση εξοπλιστικής συνεργασίας, τη δημιουργία μίας ανταγωνιστικής Ευρωπαϊκής Αγοράς Αμυντικών Εξοπλισμών και την ενδυνάμωση της Ευρωπαϊκής Αμυντικής, Τεχνολογικής και Βιομηχανικής Βάσης.

Αυτοί οι τέσσερις κύριες λειτουργίες διαμορφώνουν την αλυσίδα για αναπτυξιακή ικανότητα, από τον ορισμό των απαιτούμενων μέσω της έρευνας και της εξοπλιστικής συνεργασίας μέχρι τη βιομηχανική προμήθεια. Αυτή η ολοκληρωμένη προσέγγιση συμβάλλει στη συνεκτική ανάπτυξη δυνατοτήτων, όπου η ζήτηση και η προσφορά είναι άριστα συνδεδεμένες με σκοπό την εξοικονόμηση χρόνου και κόστους για τα κράτη μέλη. Περισσότερες συνεργασίες, στη συνέχεια, παρέχουν ευκαιρίες για την ευρωπαϊκή αμυντική βιομηχανία. Ο Οργανισμός υποστηρίζει επίσης τα Υπουργεία Άμυνας στις αλληλεπιδράσεις τους με άλλα ευρωπαϊκά θεσμικά όργανα και τους κρατά ενήμερους όσον αφορά ευρύτερες πολιτικές της ΕΕ που έχουν συνέπειες για την άμυνα. Η Ευρωπαϊκή Υπηρεσία Άμυνας δρα ως καταλύτης, προωθεί συνεργασίες, εγκαινιάζει νέες πρωτοβουλίες και εισάγει λύσεις για τη βελτίωση των αμυντικών δυνατοτήτων. Είναι ο τόπος όπου τα κράτη μέλη που επιθυμούν να αναπτύξουν ικανότητες σε συνεργασία, το πράττουν. Είναι επίσης βασικός διαμεσολαβητής στην ανάπτυξη των ικανοτήτων που απαιτούνται για την υποστήριξη της Κοινής Πολιτικής Ασφάλειας και Άμυνας της Ευρωπαϊκής Ένωσης.

Τα κράτη μέλη πρέπει να συνεργαστούν στενά με τον Ευρωπαϊκό Οργανισμό Άμυνας για την ανάπτυξη των εθνικών δυνατοτήτων τους στον τομέα της κυβερνοάμυνας. Η ανάπτυξη συνεργειών σε ευρωπαϊκό επίπεδο είναι κρίσιμης σημασίας για την αποτελεσματική κυβερνοάμυνα σε ευρωπαϊκό και εθνικό επίπεδο. Ο Ευρωπαϊκός Οργανισμός Άμυνας, από την άλλη, καλείται να εμβαθύνει τη συνεργασία του με το ΝΑΤΟ, με εθνικά και διεθνή κέντρα αριστείας, με το Ευρωπαϊκό Κέντρο Κυβερνοεγκληματικότητας της Europol, που συμβάλλει στην ταχύτερη αντίδραση σε περίπτωση κυβερνοεπιθέσεων, και ειδικά το Συνεργατικό Κέντρο Αριστείας για την Κυβερνοάμυνα (CCDCOE)[87], και να επικεντρωθεί στην ανάπτυξη ικανοτήτων, την κατάρτιση καθώς και την ανταλλαγή πληροφοριών και πρακτικών[88].

4.4 Συνεργασία Αρμοδίων Αρχών, Φορέων και Οργάνων

Οι αρμόδιοι φορείς που δραστηριοποιούνται κάτω από τη σκοπιά της Ασφάλειας Δικτύων και Πληροφοριών, όπως ο ENISA, το EC3 και ο EDA, πρέπει να συνεργάζονται και να συντονίζουν το έργο τους για την επίλυση καίριων ζητημάτων, που αφορούν ιδιαίτερα στην ανάλυση των εγκληματικών τάσεων, την εκτίμηση του κινδύνου και την κατάρτιση και ανταλλαγή βέλτιστων πρακτικών. Οι οργανισμοί αυτοί, μαζί με τις ομάδες CERT, την Επιτροπή και τα κράτη μέλη της ΕΕ, θα πρέπει να συνδράμουν στην ανάπτυξη μιας έμπιστης κοινότητας εμπειρογνωμόνων πάνω σε θέματα κυβερνοασφάλειας και κυβερνοάμυνας. Θα πρέπει ο καθένας, έχοντας ως γνώμονα την επίτευξη του κοινού τους σκοπού αλλά και τις αρμοδιότητες-υποχρεώσεις που έχει, να δραστηριοποιηθεί ανάλογα.

Βασική προϋπόθεση είναι τα κράτη μέλη να τηρούν ένα επίπεδο συνεργασίας με τους αρμόδιους φορείς, που θα διαμορφώνει κοινές πολιτικές και στρατηγικές πάνω στα θέματα της κυβερνοασφάλειας. Η δράση των επιβλεπουσών κρατικών αρχών θα πρέπει να στηρίζεται σε ένα συντονισμένο πρόγραμμα δράσης, με σκοπό την αλληλοεπικάλυψη των θεμάτων ασφάλειας σε όλο τον κοινοτικό τομέα της Ευρωπαϊκής Ένωσης.

Το EC3 θα φέρει σε επαφή τα κράτη μέλη, την Επιτροπή και τη Eurojust, με σκοπό της ανταλλαγή τεχνογνωσίας και την επιβεβαίωση ότι οι ενέργειες που πραγματοποιούνται στο πλαίσιο της ευρωπαϊκής κοινοπραξίας, σέβονται τις κατευθύνσεις όλων των ενδιαφερόμενων μελών. Ακόμη, για να τεθεί σε εφαρμογή μια πλήρης λειτουργία συγχώνευσης πληροφοριών σχετικών με συμβάντα και κινδύνους κυβερνοασφάλειας και εγκλημάτων στον κυβερνοχώρο, η ομάδα υλοποίησης του EC3 θα πρέπει να αναπτύξει δεσμούς με τις ομάδες CERT-EU, καθώς και με τον ENISA.

Ο ENISA, επίσης, κατευθύνεται προς την αύξηση των δεσμών του με τηEuropol και την ενίσχυση των σχέσεων του με τους βιομηχανικού φορείς στο χώρο των πληροφοριακών και επικοινωνιακών συστημάτων.

---

[87] Cooperative Cyber Defence Centre of Excellence.

[88] Επίσημος Διαδικτυακός ιστότοπος της Ευρωπαϊκής Υπηρεσίας Άμυνας - www.eda.europa.eu / content / page/about-us (πρόσβαση στις 20-11-2019).

Για την ενίσχυση της διεθνούς συνεργασίας στον τομέα της παγκόσμιας ασφάλειας δικτύων και πληροφοριών και την καθιέρωση διεθνών στρατηγικών συνεργασιών σε διμερές και πολυμερές επίπεδο, τα κράτη μέλη και η Επιτροπή καλούνται να συντονισθούν σε στενή συνεργασία.

5. Η ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ Ε.Ε.

Είναι δεδομένο ότι ο αντίκτυπος του κυβερνοχώρου στις κοινωνικές μας αλληλεπιδράσεις, στην εξέλιξή μας σε κάθε τομέα, στην ανταλλαγή ιδεών και πληροφορίας, στη θεμελίωση των δικαιωμάτων μας μέσα στο διαδικτυακό περιβάλλον και γενικότερα σε κάθε πτυχή της ζωής μας είναι τεράστιος. Και όλα αυτά εξαρτώνται από την τεχνολογία της πληροφορίας και βασίζονται σε έναν κυβερνοχώρο ανοιχτό και ελεύθερο, ο οποίος έχει σπάσει σύνορα και φραγμούς μεταξύ κοινοτήτων και πολιτών. Μέσα στον κυβερνοχώρο προωθείται η ελευθερία της έκφρασης, η άσκηση των θεμελιωδών δικαιωμάτων και η ενδυνάμωση των ανθρώπων στην προσπάθειά τους να ζουν σε δημοκρατικές και δίκαιες κοινωνίες. Για να παραμείνει, όμως, ο κυβερνοχώρος ανοιχτός στην ελεύθερη κυκλοφορία ιδεών και πληροφοριών και στην ελεύθερη έκφραση, η διασφάλιση του οποίου είναι κομβικής σημασίας, θα πρέπει να εφαρμόζονται και να προστατεύονται και στο περιβάλλον του κυβερνοχώρου οι ίδιοι κανόνες, οι ίδιες αρχές και αξίες και τα ίδια δικαιώματα που ισχύουν και εκτός αυτού[89]. Η ελευθερία όμως και η ευημερία μας εξαρτώνται από ένα διαδίκτυο, το οποίο εξελίσσεται συνεχώς και γίνεται όλο και πιο ισχυρό. Η ελευθερία, λοιπόν, στο διαδίκτυο απαιτεί ασφάλεια. Ο κυβερνοχώρος θα πρέπει να προστατεύεται από τις κακόβουλες δραστηριότητες και οι κυβερνήσεις διαδραματίζουν σημαντικό ρόλο στη διασφάλιση ενός ασφαλούς και ελεύθερου κυβερνοχώρου. Είναι υπεύθυνες για τη διασφάλιση της πρόσβασης και της διαφάνειας, της προστασίας των θεμελιωδών δικαιωμάτων και τη διατήρηση της αξιοπιστίας και της διαλειτουργικότητας του διαδικτύου. Οι κυβερνοεπιθέσεις γίνονται όλο και πιο συχνές και οι κυβερνοεγκληματίες χρησιμοποιούν πλέον πιο εξελιγμένες μεθόδους για να εισέλθουν στα πληροφοριακά συστήματα και στα δίκτυα στόχους. Όλα αυτά λοιπόν εξηγούν γιατί οι κυβερνήσεις σε όλο τον κόσμο εξετάζουν τον κυβερνοχώρο ως ένα θέμα ύψιστης σημασίας και διεθνούς κλίμακας και αναπτύσσουν στρατηγικές κυβερνοασφάλειας.

Κατωτέρω παρατίθενται οι τρόποι αντιμετώπισης του εγκλήματος στον κυβερνοχώρο από την Ευρωπαϊκή Ένωση, οι τρόποι με τους οποίους η Επιτροπή επιδιώκει να πετύχει τους τιθέμενους στόχους, καθώς και η πρόοδος που έχει σημειωθεί μέχρι σήμερα[90].

5.1 Επίτευξη ανθεκτικότητας αναφορικά με την ασφάλεια στον Κυβερνοχώρο

[89] JOIN(2013) 1 – Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (7.2.2013)

[90] Οι τιθέμενοι στόχοι από : (JOIN(2013) 1 – Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace (7.2.2013). Η πρόοδος από : Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"(JOIN(2013) 1), 28 February 2014.

Αναφορικά με τον πρώτο στόχο της επίτευξης ανθεκτικότητας στον τομέα της ασφάλειας στον κυβερνοχώρο, η Επιτροπή συνεχίζει τις δραστηριότητές της, μέσω του Κοινού Κέντρου Ερευνών, σε στενή συνεργασία με τις αρχές των κρατών μελών και με τους ιδιοκτήτες υποδομών ζωτικής σημασίας και τους οργανισμούς εκμετάλλευσης, για τον εντοπισμό των ευάλωτων σημείων της Ασφάλειας Δικτύων και Πληροφοριών των ευρωπαϊκών υποδομών ζωτικής σημασίας και θα ενθαρρύνει την ανάπτυξη ανθεκτικών συστημάτων.

Στο πλαίσιο του στόχου αυτού, το ενωμένο ερευνητικό κέντρο της Ευρωπαϊκής Επιτροπής (JRC)[91] ασχολείται με ερευνητικές δραστηριότητες πάνω στην αναγνώριση της αλληλεξάρτησης μεταξύ των ICT[92] συστημάτων και των ενεργειακών τομέων. Το JRC επίσης εργάζεται προς την αύξηση της ευαισθητοποίησης στην κυβερνοασφάλεια εντός των θεματικών δικτύων της προστασίας κρίσιμων ενεργειακών υποδομών και έχει δρομολογήσει δραστηριότητες για να παρέχει πληροφορίες στους ενεργειακούς παράγοντες σχετικά με απειλές και περιστατικά, διαμέσου του ευρωπαϊκού κέντρου διαμοιρασμού πληροφοριών. Υπό την αιγίδα της Smart Grid Task Force, που ιδρύθηκε από την Επιτροπή στα τέλη του 2009, μία ομάδα ειδικών, που θα συγκεντρώνει τα ενδιαφερόμενα μέλη από τους ενεργειακούς και ICT τομείς, τις ενώσεις καταναλωτών και τις ρυθμιστικές αρχές, το Μάρτιο του 2014 προέβη στην παράδοση ενός προτύπου εκτίμησης απειλών απέναντι στην προστασία δεδομένων και ενός συνόλου καλύτερων διαθέσιμων τεχνικών που καταδεικνύουν πιθανούς κινδύνους για την κυβερνοασφάλεια, σχετικούς με τις ελάχιστες λειτουργικές απαιτήσεις των έξυπνων συστημάτων μετρήσεων, όπως στη σύσταση 2012/148. Η ειδική ομάδα θα παρέχει επίσης συστάσεις στα κράτη μέλη για τις ελάχιστες απαιτήσεις κυβερνοασφάλειας των έξυπνων δικτύων.

Αναφορικά με τον δεύτερο στόχο για την επίτευξη ανθεκτικότητας στο πεδίο της ασφάλειας στον κυβερνοχώρο, η Επιτροπή έχει δρομολογήσει πιλοτικό έργο με ενωσιακή χρηματοδότηση για την καταπολέμηση δικτύων-ρομπότ (botnets) και κακόβουλου λογισμικού, με στόχο να παρασχεθεί πλαίσιο για τον συντονισμό και τη συνεργασία μεταξύ των κρατών μελών της ΕΕ, οργανισμών του ιδιωτικού τομέα όπως οι πάροχοι υπηρεσιών διαδικτύου, και διεθνών εταίρων.

Στο πλαίσιο του στόχου αυτού, η Επιτροπή έχει διεξαγάγει μια συνδιάσκεψη για ένα ευρωπαϊκό πιλοτικό πρόγραμμα που χρηματοδοτείται στο πλαίσιο του προγράμματος CIP-PSP (Policy Support Programme of Critical Infrastructure Protection), το ACDC (Advanced Cyber Defence Centre), για να αντιμετωπίσει botnets και κακόβουλα λογισμικά διαμέσου της συνεργασίας ενός ευρωπαϊκού συνασπισμού αποτελούμενου από δημόσιους και ιδιωτικούς φορείς.

Αναφορικά με τον τρίτο στόχο για την επίτευξη ανθεκτικότητας στο πεδίο της ασφάλειας στον κυβερνοχώρο, η Επιτροπή καλεί τον ENISA να βοηθήσει τα κράτη μέλη να αναπτύξουν ισχυρές εθνικές ικανότητες ανθεκτικότητας όσον αφορά την ασφάλεια του κυβερνοχώρου, ιδίως με την ανάπτυξη εμπειρογνωμοσύνης στην ασφάλεια και την ανθεκτικότητα βιομηχανικών συστημάτων ελέγχου, και υποδομών μεταφορών και ενέργειας.

[91] Joint Research Centre
[92] Information and Communication Technology

Στο πλαίσιο του στόχου αυτού, ο ENISA έχει υιοθετήσει την αναφορά «Smart Grid Threat Landscape and Good Practice Guide».

Αναφορικά με τον τέταρτο στόχο για την επίτευξη ανθεκτικότητας στον τομέα της ασφάλειας στον κυβερνοχώρο, η Επιτροπή κάλεσε τον ENISA να εξετάσει την σκοπιμότητα δημιουργίας ομάδας αντιμετώπισης περιστατικών ασφάλειας πληροφορικής για τα βιομηχανικά συστήματα ελέγχου (ICS-CSIRTs) για την ΕΕ.

Στο πλαίσιο του στόχου αυτού, ο ENISA έχει εκδώσει έναν οδηγό ορθής πρακτικής για τις ομάδες CERT για τα βιομηχανική συστήματα ελέγχου, που βασίστηκε στις παρούσες βέλτιστες πρακτικές των CERT που ήταν υπεύθυνες για τα ICT δίκτυα και στο έργο που διεξήχθη από τον ENISA πάνω στις βασικές ικανότητες των εθνικών/κυβερνητικών CERTS. Ο οδηγός είναι δομημένος πάνω σε 4 κατηγορίες βασικών ικανοτήτων, ήτοι εντολή, υπηρεσία, portfolio, λειτουργίες, ενώ εξετάζει παράλληλα τη συνεργασία με τους σχετικούς ICS ενδιαφερόμενους.

Αναφορικά με τον πέμπτο στόχο για την επίτευξη ανθεκτικότητας στο πεδίο της ασφάλειας στον κυβερνοχώρο, η Επιτροπή καλεί τον ENISA να συνεχίσει να υποστηρίζει τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ στην διεξαγωγή τακτικών πανευρωπαϊκών ασκήσεων αντιμετώπισης συμβάντων ασφάλειας στην κυβερνοχώρο που θα αποτελέσουν επίσης την επιχειρησιακή βάση για την συμμετοχή της ΕΕ σε διεθνείς ασκήσεις αντιμετώπισης συμβάντων ασφάλειας στην κυβερνοχώρο.

Στο πλαίσιο του στόχου αυτού, ο ENISA έχει πραγματοποιήσει με τα κράτη μέλη και τις χώρες της Ευρωπαϊκής Ζώνης Ελευθέρων Συναλλαγών (ΕΖΕΣ) (ή European Free Trade Association - EFTA) ευρωπαϊκές ασκήσεις "CyberEurope", όπου συμμετείχαν 29 Ευρωπαϊκές χώρες (ΕΕ και ΕΖΕΣ) μαζί με τα ευρωπαϊκά ιδρύματα με στόχο να δοκιμάσουν την ευρωπαϊκή ετοιμότητα, να συνεργαστούν και να ανταλλάξουν πληροφορίες μέσω διαδικασιών μεταξύ των εθνικών αρμόδιων αρχών, να παρέχουν μία ευκαιρία στα κράτη μέλη να δοκιμάσουν στο εσωτερικό τους τα ενδεχόμενα εθνικά σχέδια της Ασφάλειας Δικτύων και Πληροφοριών, να ερευνήσουν το αποτέλεσμα της πολλαπλής και παράλληλης ανταλλαγής πληροφοριών μεταξύ ιδιωτικού και δημόσιου τομέα, να ερευνήσουν την κλιμάκωση και αποκλιμάκωση διαδικασιών για τις αντιδράσεις σε περιστατικά και να ερευνήσουν τον χειρισμό των μεγάλης κλίμακας περιστατικών[93].

Αναφορικά με τον έκτο στόχο για την επίτευξη ανθεκτικότητας στον τομέα της ασφάλειας στον κυβερνοχώρο, η Επιτροπή καλεί το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο να εγκρίνουν χωρίς καθυστέρηση την πρόταση οδηγίας για κοινό υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών ανά την Ένωση, που καλύπτει τις εθνικές ικανότητες και ετοιμότητα, την συνεργασία σε ενωσιακό επίπεδο, την υιοθέτηση πρακτικών διαχείρισης κινδύνου και την ανταλλαγή πληροφοριών σχετικά με την Ασφάλεια Δικτύων και Πληροφοριών.

[93]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 22-11-2019).

Στο πλαίσιο του στόχου αυτού, έχει εκδοθεί με τη συνήθη νομοθετική διαδικασία από το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο η Οδηγία 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

Αναφορικά με τον έβδομο στόχο για την επίτευξη ανθεκτικότητας στο πεδίο της ασφάλειας στον κυβερνοχώρο, η Επιτροπή καλεί τον κλάδο να αναλάβει ηγετικό ρόλο στις επενδύσεις σε ασφάλεια κυβερνοχώρου υψηλής ποιότητας και να αναπτύξει βέλτιστες πρακτικές και ανταλλαγή πληροφοριών σε επίπεδο κλάδου και με τις δημόσιες αρχές με στόχο να εξασφαλιστεί ισχυρή και αποτελεσματική προστασία των στοιχείων ενεργητικού και των προσώπων, ιδίως μέσω συμπράξεων δημόσιου -ιδιωτικού τομέα, όπως η Ευρωπαϊκή Κοινοπραξία Δημοσίου – Ιδιωτικού Τομέα για την Ανθεκτικότητα - EP3R και η σύμπραξη «Trust in Digital Life» (TDL).

Στο πλαίσιο του στόχου αυτού, η ομάδα σύμπραξης ιδιωτικού και δημόσιου τομέα «Trust in Digital life» με την υποστήριξη του DG CNECT[94], διοργανώνει ετησίως το «Trust in Digital life» για να θέσουν τις βέλτιστες πρακτικές στις αποδιοργανωτικές τεχνολογίες κυβερνοασφάλειας.

5.2 Δραστική μείωση του Ηλεκτρονικού Εγκλήματος

Αναφορικά με τη δραστική μείωση του ηλεκτρονικού εγκλήματος, η Επιτροπή θέτει σαν στόχους αφενός να εξασφαλίσει την ταχεία στο εθνικό δίκαιο ενσωμάτωση και εφαρμογή των οδηγιών που σχετίζονται με το ηλεκτρονικό έγκλημα, αφετέρου τα κράτη μέλη που δεν έχουν ακόμη κυρώσει την σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, να την κυρώσουν και να εφαρμόσουν τις διατάξεις της το ταχύτερο δυνατόν.

Ειδικότερα, οι συννομοθέτες της ΕΕ έχουν υιοθετήσει δύο οδηγίες που σχετίζονται με το έγκλημα στον κυβερνοχώρο μέχρι σήμερα. Αφενός την Οδηγία 2011/92/EU της 13ης Δεκεμβρίου 2011 σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο του Συμβουλίου 2004/68/ JHA και αφετέρου την Οδηγία 2013/40/EU της 12ης Αυγούστου 2013 σχετικά με επιθέσεις κατά των συστημάτων πληροφοριών, η οποία ενσωματώθηκε στο εθνικό δίκαιο με τον Νόμο 4411/2016 και αντικατέστησε την απόφαση-πλαίσιο 2005/222 /JHA του Συμβουλίου.

Αναφορικά με την ενισχυμένη επιχειρησιακή ικανότητα καταπολέμησης του ηλεκτρονικού εγκλήματος, η Επιτροπή υποστηρίζει, μέσω των χρηματοδοτικών της προγραμμάτων, τα κράτη μέλη να εντοπίσουν κενά και να ενισχύσουν τις ικανότητές τους όσον αφορά στη διερεύνηση και την καταπολέμηση του ηλεκτρονικού εγκλήματος. Περαιτέρω υποστηρίζει τους φορείς που συνδέουν την έρευνα, τα πανεπιστήμια, τους υπεύθυνους επιβολής του νόμου και τον ιδιωτικό τομέα, με τρόπο παρόμοιο με τις εν εξελίξει εργασίες στα χρηματοδοτούμενα από την Επιτροπή κέντρα αριστείας για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο που έχουν ήδη δημιουργηθεί σε ορισμένα κράτη μέλη.

[94] DG for Communication, Network, Content and Technology.

Επιπλέον, η Επιτροπή σε συνεργασία με τα κράτη μέλη και με την υποστήριξη του Κοινού Κέντρου Ερευνών, συντονίζει τις προσπάθειες εντοπισμού βέλτιστων πρακτικών και βέλτιστων διαθέσιμων τεχνικών για την καταπολέμηση του ηλεκτρονικού εγκλήματος, όπως την ανάπτυξη εργαλείων για εγκληματολογικές έρευνες ή για την ανάλυση απειλών.

Στο πλαίσιο των ανωτέρω στόχων, η Ευρωπαϊκή Επιτροπή υποστηρίζει τις προσπάθειες των κρατών μελών στο να ανταλλάξουν γνώσεις και ειδικότητες και μαζί να αναπτύξουν ενιαίο υλικό εκπαίδευσης.

Σκοπός αυτού είναι επιπλέον η στήριξη της Ευρωπαϊκής Ομάδας Μελέτης του Κυβερνοεγκλήματος, η οποία εντάσσει συμμετέχοντες από το χώρο της επιβολής του νόμου, της ακαδημαϊκής κοινότητας και του ιδιωτικού τομέα από όλες τα κράτη μέλη για να εντοπίσουν τις ανάγκες στην εκπαίδευση και να αναπτύξουν υλικό για μελέτη, το οποίο θα εγκριθεί από την ΕΕ. Την τελευταία δεκαετία πάνω από 5 εκ. ευρώ έχουν διατεθεί για την ενίσχυση των Ευρωπαϊκών Αρχών Επιβολής του Νόμου στην καταπολέμηση του Κυβερνοεγκλήματος. Αυτό έχει ως αποτέλεσμα την δημιουργία ενός ολοκληρωμένου πακέτου που έχει χρησιμοποιηθεί στην εκπαίδευση άνω των 1500 ερευνητών του Κυβερνοεγκλήματος στον τομέα της ανάλυσης και συλλογής αποδεικτικών. Μάλιστα έχει πραγματοποιηθεί και σύμπραξη μεταξύ του Ευρωπαϊκού Κέντρου Κυβερνοεγκλήματος, της Ευρωπαϊκής Αστυνομικής Ακαδημίας και της Ομάδας Μελέτης του Κυβερνοεγκλήματος.

Η Επιτροπή έχει επιπλέον υιοθετήσει μια επικοινωνία στην εγκαθίδρυση ενός ευρωπαϊκού εκπαιδευτικού σχήματος επιβολής του νόμου για να εφοδιάσει τους υπεύθυνους της επιβολής του νόμου με γνώσεις και ικανότητες που χρειάζονται για την καταπολέμηση του διασυνοριακού εγκλήματος μέσω της επιτυχούς συνεργασίας με τις ευρωπαϊκές αρχές. Το εκπαιδευτικό σχήμα αποσκοπεί στο να βοηθήσει στην αποτελεσματικότερη αντιμετώπιση κοινών απειλών ασφάλειας στην Ευρωπαϊκή Ένωση και να βοηθήσει στη διαμόρφωση μιας κοινής κουλτούρας για την επιβολή του νόμου.

Περαιτέρω, η ευρωπαϊκή χρηματοδότηση διαχειριζόμενη από τη DG HOME, χρησιμοποιείται για την ίδρυση 10 Κέντρων Κυβερνοεγκλήματος Αναπτυγμένης Έρευνας και Εκπαίδευση στην Ελλάδα, Γαλλία, Εσθονία, Τσεχία, Βουλγαρία, Βέλγιο, Ρουμανία, ΗΒ, Ισπανία και Πολωνία. Τα Κέντρα αυτά εστιάζουν στην ανάπτυξη ερευνητικών εργαλείων, στη δημιουργία ενός εύρους από προγράμματα εκπαίδευσης Κυβερνοεγκλήματος και στην πρακτική έρευνα σε θέματα που επηρεάζουν τους ευρωπαίους πολίτες, όπως online οικονομικό έγκλημα, τηλεπικοινωνιακές απάτες και κυβερνοασφάλεια κρίσιμων εθνικών υποδομών[95].

Η ΕΕ επίσης χρηματοδοτεί την Ευρωπαϊκή Ακαδημία του Νόμου για ένα πρόγραμμα αποτελούμενο από οχτώ βασικές κατευθύνσεις σε νομικά και τεχνικά θέματα του Κυβερνοεγκλήματος που λαμβάνουν μέρος μέσα στην τριετία 2012-2015. Το πρόγραμμα θα παρέχει περίπου 500 δικαστικούς και εισαγγελείς με εξειδικευμένες ικανότητες σε παραβάσεις σχετικές με το διαδίκτυο.

[95]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 24-11-2019).

Άλλες πρωτοβουλίες των κρατών μελών στον εντοπισμό και την κάλυψη των κενών, συγκεκριμένα πάνω στην διασυνοριακή συνεργασία, έχουν επίσης αναληφθεί υπό την υποστήριξη του ISEC, πρόγραμμα του οποίου διέθεσε 5 εκ. ευρώ αναφορικά με τη σεξουαλική κακοποίηση των παιδιών και την παράνομη χρήση του διαδικτύου, με σκοπό να υποστηρίξει, μεταξύ άλλων, και τη συνεργασία ανάμεσα σε ειδικούς και τις αρχές επιβολής του νόμου στη κατανόηση και καταπολέμηση του κυβερνοεγκλήματος.

Το Ενωμένο Ερευνητικό Κέντρο της Επιτροπής έχει αναπτύξει στενές συνεργασίες με το Ευρωπαϊκό κέντρο Κυβερνοεγκλήματος από την αρχή της λειτουργίας του το 2013. Τα πρώτο θέμα που επιλέχθηκε για την από κοινού έρευνα επικεντρώθηκε σε ένα εργαλείο έρευνας σε βάσεις δεδομένων βίντεο και εικόνας για ερευνητικούς σκοπούς. Ο σκοπός είναι η ανάπτυξη και ενοποίηση έξυπνων εργαλείων για αναγνώριση των θυμάτων και των αυτουργών των online παιδικών κακοποιήσεων σε αρκετά μεγάλες βάσεις δεδομένων μέσω ενισχυμένης αυτοματοποιημένης κατηγοριοποίησης αυτών των μέσων. Το JRC (Joint Research Center) επιπλέον έχει αναπτύξει εργαλεία για έξυπνη ανάλυση από ανοιχτές πηγές για τις αρχές επιβολής του νόμου των κρατών μελών και έχουν ήδη αναπτυχθεί σε ένα αριθμό από αυτά.

Η Επιτροπή επίσης υποστηρίζει την αμοιβαία εκτίμηση των κρατών μελών για το Κυβερνοέγκλημα υπό την αιγίδα της Ομάδας Εργασίας του Συμβουλίου σε Γενικά Θέματα που αφορούν Αξιολογήσεις (GENVAL), το οποίο περιλαμβάνει δυνατότητες για τον διαμοιρασμό των καλύτερων πρακτικών και εντοπισμένων αδυναμιών.

Τέλος, η Επιτροπή συνεργάζεται στενά με Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) στο πλαίσιο της Europol και της Eurojust για να συντονίσει τις εν λόγω προσεγγίσεις πολιτικής με βέλτιστες πρακτικές από επιχειρησιακής πλευράς.

Ειδικότερα, η Επιτροπή και το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) είναι σε στενή επαφή για να διασφαλίσουν την ευθυγράμμιση των επιχειρησιακών δραστηριοτήτων με τις υπάρχουσες ευρωπαϊκές πολιτικές, από τη μία μεριά, και την αποτελεσματική υποστήριξη στις επιχειρησιακές δραστηριότητες από την πολιτική, από την άλλη μεριά. Η ευθυγράμμιση ενδυναμώνεται μέσω των κυκλικών πολιτικών διαδικασιών EMPACT[96]. Η κυκλική πολιτική έχει δημιουργηθεί από το Συμβούλιο της Ευρωπαϊκής Ένωσης για να αντιμετωπίσει τις πιο σημαντικές εγκληματικές απειλές με ένα συναφή μεθοδολογικό τρόπο μέσω της βέλτιστης συνεργασίας μεταξύ των κρατών μελών, των Ευρωπαϊκών Ινστιτούτων και Ευρωπαϊκών Αρχών, όπως επίσης και με τις σχετικές τρίτες χώρες και οργανισμούς. Για την αναγνώριση αυτών των αρκετά σημαντικών εγκληματικών απειλών, η υπηρεσία Εκτίμησης Σοβαρών και Οργανωμένων Εγκληματικών Απειλών της Europol (SOCTA) παρέχει σημαντικές πληροφορίες. Στα μέσα του 2013, εντοπίστηκαν από τις αρχές του SOCTA[97] τρείς από τις σημαντικότερες απειλές στον χώρο του κυβερνοεγκλήματος, οι οποίες σχετίζονται με την online απάτη πληρωμών και καρτών, κυβερνοεγκλήματα που προκαλούν σοβαρές κακοποιήσεις στα θύματά τους, όπως η online παιδική πορνογραφία και κυβερνοεπιθέσεις που επηρεάζουν κρίσιμες υποδομές και πληροφοριακά συστή-

[96] European Multidisciplinary Platform Against Criminal Threats
[97] Serious and Organised Crime Threat Assessment

ματα στην ΕΕ. Ειδικοί από όλες τις χώρες μέλη και το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) σε αυτήν τη δουλειά συνεργάστηκαν για να ανταποκριθούν στις προτεραιότητες αυτές και στις επιχειρησιακές δράσεις.

Για να διασφαλιστεί, η συνεχόμενη υποστήριξη και η πολιτική ευθυγράμμιση, η Επιτροπή οργανώνει κάθε χρόνο διασκέψεις για να αξιολογήσει τις δράσεις του Ευρωπαϊκού Κέντρου για εγκλήματα στον Κυβερνοχώρο (EC3), να εντοπίσει τις άμεσες απειλές και να προτείνει προτεραιότητες για τη μελλοντική εργασία, σε στενή συνεργασία με του φορείς, συμπεριλαμβανομένων των αρχών επιβολής του νόμου των κρατών μελών και του ιδιωτικού και ακαδημαϊκού τομέα.

Αναφορικά με τον βελτιωμένο συντονισμό σε επίπεδο ΕΕ, η Επιτροπή υποστηρίζει το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) ως ευρωπαϊκό σημείο αναφοράς για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Το εν λόγω Κέντρο (EC3) παρέχει ανάλυση και πληροφορίες, υποστηρίζει τις ανακρίσεις, παρέχει υψηλού επιπέδου εγκληματολογικές έρευνες, διευκολύνει τη συνεργασία, δημιουργεί διαύλους για την ανταλλαγή πληροφοριών μεταξύ των αρμόδιων αρχών στα κράτη μέλη, τον ιδιωτικό τομέα και άλλους ενδιαφερόμενους, και χρησιμεύει σταδιακά ως εκπρόσωπος της κοινότητας επιβολής του νόμου.

Ειδικότερα, η Επιτροπή υποστηρίζει τη δουλειά του Ευρωπαϊκού Κέντρου για εγκλήματα στον Κυβερνοχώρο (EC3) σε διαρκή βάση και τηρεί εβδομαδιαίες επαφές για να εξασφαλίσει το συντονισμό μεταξύ των ενεργών συμμετεχόντων στον Πίνακα Προγραμμάτων, τις συμβουλευτικές ομάδες, τις συνεδρίες και τα γεγονότα, όπου η Επιτροπή τακτικά παρουσιάζει την πολιτική του εν λόγω Κέντρου (EC3) που σχετίζεται με το θεματικό αντικείμενο για να εξασφαλίσει ότι οι πολιτικές διαμορφώνονται στα πλαίσια αντιμετώπισης του προβλήματος με τη διευκόλυνση της συνεργασίας μεταξύ των αρχών επιβολής του νόμου.

Η Επιτροπή σχεδιάζει την αποστολή χρηματοδοτήσεων από τα Εσωτερικά Κεφάλαια Ασφαλείας στην Europol για να υποστηρίξει τη δουλειά του Κύκλου Πολιτικής του EMPACT και να χρηματοδοτήσει την επιχειρησιακή συνεργασία.

Η Επιτροπή επίσης πρότεινε τον δανεισμό κεφαλαίων από τον προϋπολογισμό του Horizon 2020 στην Europol με στόχο την περαιτέρω στοχευόμενη έρευνα. Αυτά τα κεφάλαια, που θα χορηγούνται απευθείας από την Europol, θα επέτρεπαν έναν στενότερο έλεγχο μεταξύ των αρχών επιβολής του νόμου πάνω στα αποτελέσματα της έρευνας και ανάπτυξης, για να εξασφαλίσει ότι τα παραγόμενα έργα που χρηματοδοτούνται είναι χρήσιμα για τις αρχές επιβολής του νόμου μεταξύ των κρατών μελών. Δυστυχώς, αυτό απορρίφθηκε από τα κράτη μέλη στην επιτροπή του Horizon 2020 για την εργασία του τρέχοντος προγράμματος. Η Επιτροπή προτίθεται να επιλύσει κάθε πρόβλημα και να συνεχίσει περαιτέρω μια τέτοια αντιπροσωπία, η οποία θα μπορούσε να είναι επωφελής για τις αρχές επιβολής του νόμου στα κράτη μέλη[98].

Η Επιτροπή επιπλέον υποστηρίζει τις προσπάθειες αναβάθμισης της λογοδοσίας των καταχωριστών ονομάτων χώρου και να εξασφαλίσει την ακρίβεια των πληροφοριών σχετικά με την ιδιοκτησία ιστοτόπων βάσει των συστάσεων περί επιβολής

[98]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 27-11-2019).

του νόμου του Οργανισμού του διαδικτύου για την εκχώρηση ονομάτων και αριθμών (ICANN)[99], τηρουμένου του ενωσιακού δικαίου, συμπεριλαμβανομένων των κανόνων για την προστασία των δεδομένων.

Η Επιτροπή επίσης αξιοποιεί την πρόσφατη νομοθεσία για περαιτέρω ενίσχυση των προσπαθειών της ΕΕ όσον αφορά στην αντιμετώπιση της διαδικτυακής σεξουαλικής κακοποίησης παιδιών. Η Επιτροπή έχει εκδώσει ευρωπαϊκή στρατηγική για ένα διαδίκτυο καλύτερα προσαρμοσμένο στα παιδιά, και σε συνεργασία με κράτρη εντός και εκτός της ΕΕ, ενώ παράλληλα έχει δρομολογήσει μια Παγκόσμια συμμαχία κατά της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο. Η Συμμαχία αποτελεί φορέα για περαιτέρω δράσεις από τα κράτη μέλη με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου για εγκλήματα στον Κυβερνοχώρο (EC3).

Ειδικότερα, η Παγκόσμια Ένωση Εναντίον της Παιδικής Σεξουαλικής Κακοποίησης στο Διαδίκτυο, που έχει ιδρυθεί από το 2012, έφερε σε συνεργασία 48 χώρες με σκοπό την βελτίωση της διαδικασίας αναγνώρισης των θυμάτων, την αποτελεσματικότερη προσαγωγή των αυτουργών, την ενίσχυση της ενημέρωσης και την μείωση του υλικού παιδικής πορνογραφίας στο διαδίκτυο. Η Ένωση κατάφερε την επέκτασή της σε 52 χώρες ανά τον κόσμο και δρα διαρκώς αναζητώντας αποτελεσματικούς τρόπους για την προώθηση της παγκόσμιας συνεργασίας πάνω στην καταπολέμηση αυτών των εγκλημάτων. Οι συμμετέχουσες χώρες έχουν δεσμευτεί για την επίτευξη των υψηλών επιπέδου πολιτικής στόχων της Συμμαχίας και η Επιτροπή έχει δημοσιεύσει μια αναφορά επισυνάπτοντας τις δεσμεύσεις αυτές.

Οι αμοιβαίες εκτιμήσεις των κρατών μελών υπό την αιγίδα του Συμβουλίου της Ομάδας Εργασίας σε Γενικά Θέματα που αφορούν Αξιολογήσεις (GENVAL) περιλαμβάνουν επίσης ερωτήματα σχετικά με την καταπολέμηση της σεξουαλικής παιδικής κακοποίησης που θα δημιουργήσουν επιπλέον δυνατότητες για προώθηση των προσπαθειών για την εξάλειψη αυτού του φαινόμενου.

Το JRC υποστηρίζει την πολιτική κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης πάνω στην καταπολέμηση της διαδικτυακής σεξουαλικής παιδικής κακοποίησης με νέες και εξελιγμένες τεχνικές που αφορούν βιομετρικά συστήματα και υπολογιστική όραση για την αναγνώριση των θυμάτων και των αυτουργών. Οι εργασίες αυτές πραγματοποιούνται σε στενή συνεργασίας με το Ευρωπαϊκό Κέντρο Κυβερνοεγκλήματος και τις κρατικές αρχές επιβολής του νόμου.

Μάλιστα, η Επιτροπή καλεί το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3), που ανήκει στην Europol να εστιάσει αρχικά την αναλυτική και επιχειρησιακή υποστήριξή της στις έρευνες των κρατών μελών στον τομέα του ηλεκτρονικού εγκλήματος, να συμβάλλει στην εξάρθρωση και αποσταθεροποίηση των δικτύων ηλεκτρονικού εγκλήματος κυρίως στους τομείς της σεξουαλικής κακοποίησης παιδιών, της απάτης στις πληρωμές, των δικτύων-ρομπότ και της παρείσδυσης[100].

[99] Internet Corporation for Assigned Names and Numbers

[100]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean. gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y» (πρόσβαση στις 28-11-2019).

Επιπρόσθετα, η Επιτροπή καλεί το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) της Europol να καταρτίζει σε τακτική βάση στρατηγικές και επιχειρησιακές εκθέσεις επί των τάσεων και των αναδυόμενων απειλών για τον προσδιορισμό προτεραιοτήτων και την επικέντρωση των διερευνητικών δράσεων των ομάδων καταπολέμησης του ηλεκτρονικού εγκλήματος στα κράτη μέλη.

Ειδικότερα, το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) έχει εστιάσει στην βοήθεια των αρχών επιβολής του νόμου των κρατών μελών για την αποδιοργάνωση και εξάλειψη των δικτύων του κυβερνοεγκλήματος στα πεδία της σεξουαλικής παιδικής κακοποίησης, των οικονομικών απατών, των botnets και των παραβιάσεων. Η πρώτη χρονιά λειτουργίας των διαδικασιών υπήρξε αρκετά αποτελεσματική.

Στον τομέα της καταπολέμησης των botnets, των παραβιάσεων και άλλων κυβερνοεπιθέσεων για παράδειγμα μπορεί να αναφερθεί η καταπολέμηση του κακόβουλου λογισμικού που κλείδωνε τις λειτουργίες του υπολογιστή και τον απελευθέρωνε μόνο όταν καταβαλλόταν ένα συγκεκριμένο χρηματικό ποσό (ο λεγόμενος «ιός της δίωξης ηλεκτρονικού εγκλήματος» για την Ελλάδα). Οι εγκληματίες είχαν μολύνει δεκάδες χιλιάδες υπολογιστές ανά τον κόσμο και αποσπούσαν πάνω από ένα εκατομμύριο ευρώ ετησίως προτού αποκλειστούν. Το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) επίσης υποστήριξε ορισμένες διεθνείς πρωτοβουλίες στον τομέα της καταπολέμησης των botnets, της διάσπασης και έρευνας των εγκληματικών forums και των επιθέσεων με κακόβουλα λογισμικά κατά των οικονομικών ιδρυμάτων.

Σημαντικές προσπάθειες, που έγιναν σε συνεργασία με πολλά κράτη μέλη και μη ευρωπαϊκούς φορείς, αφιερώθηκαν στην καταπολέμηση της διαδικτυακής παιδικής σεξουαλικής κακοποίησης. Το αποτέλεσμα ήταν η διάσπαση μιας καλυμμένης διαδικτυακής συνομιλίας άνω των 25.000 παιδόφιλων που εμπλέκονταν στη διάδοση περίπου 2 εκατομμυρίων εικόνων παιδικής σεξουαλικής κακοποίησης, με επακόλουθο την σύλληψη εκατοντάδων υπόπτων εντός και εκτός της Ευρωπαϊκής Ένωσης.

Τέλος, στον τομέα των οικονομικών απατών, το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) υποστήριξε έρευνες που κατέληξαν σε τρία διαφορετικά διεθνή δίκτυα με απάτες πιστωτικών καρτών και είχαν ως αποτέλεσμα δεκάδες υπόπτους να συλλαμβάνονται και να ανακαλύπτονται παράνομα καταστήματα που παρήγαγαν και παρείχαν υλικό και λογισμικό για να παρακολουθούν τερματικά σημεία πωλήσεων. Πέρα από τον κεντρικό ρόλο της βοήθειας και συνεργασίας στις διασυνοριακές έρευνες, το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) έχει δημοσιεύσει στρατηγικές ανάλυσης και έχει παραδώσει ειδικευμένες αναφορές πάνω σε νέες τάσεις και απειλές[101].

Το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) καταρτίζει και δημοσιεύει μια αναφορά ετησίως πάνω στις επίκαιρες τάσεις και απειλές και τις πιθανές μελλοντικές προτεραιότητες για την καταπολέμηση του κυβερνοεγκλήματος.

[101]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y (πρόσβαση στις 30-11-2019).

Επιπρόσθετα, η Επιτροπή καλεί την Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL) σε συνεργασία με την Europol να συντονίσει τον σχεδιασμό και τον προγραμματισμό εκπαιδευτικών προγραμμάτων προκειμένου οι υπηρεσίες επιβολής του νόμου να αποκτήσουν τις γνώσεις και την εμπειρογνωμοσύνη για την αποτελεσματική αντιμετώπιση του ηλεκτρονικού εγκλήματος.

Ειδικότερα, η CEPOL σε στενή συνεργασία με την Europol και την Ευρωπαϊκή Ομάδα Εκπαίδευσης και Επιμόρφωσης Κυβερνοεγκλήματος διεξάγει επί του παρόντος μια εκτίμηση για τις ανάγκες εκπαίδευσης σε δύο από τις τρείς περιοχές προτεραιότητας που αναγνωρίστηκαν από τον Πολιτικό Κύκλο του EMPACT, οι οποίες είναι οι κυβερνοεπιθέσεις και οι οικονομικές απάτες. Με αυτό, θα οργανωθούν επιπλέον κατευθύνσεις που να επικαλύπτουν αυτόν τον τομέα. Η CEPOL διοργανώνει πολιτικές εκπαιδεύσεις σχετικά με τα θέματα της κακοποίησης των παιδιών στον κυβερνοχώρο, καθώς και της ικανότητας των κρατών μελών και της Ένωσης για την ανίχνευση, έρευνα και δίωξη του κυβερνοεγκλήματος.

Η CEPOL συνεχίζει την προαγωγή της συνεργασίας στον τομέα της δίωξης του κυβερνοεγκλήματος, ακολουθώντας τις προτεραιότητες του EMPACT και σε ευθυγράμμιση με την Ανακοίνωση της Ευρωπαϊκής Επιτροπής για το Σχήμα Εκπαιδεύσεως για την Επιβολή του Νόμου. Επιπλέον, συντάσσει μια εκτίμηση σε ανάγκες εκπαιδεύσεως πάνω στην αντιμετώπιση της κακοποίησης παιδιών στον κυβερνοχώρο, των κυβερνοεπιθέσεων και των οικονομικών απατών σε συνεργασία με την Europol. Πέραν αυτού οργάνωσε τέσσερις πολιτικές κατευθύνσεις με θεματικές ενότητες «Κακοποίηση Παιδιών στον Κυβερνοχώρο», «Ικανότητες των κρατών μελών και της Ένωσης για την ανίχνευση, έρευνα και δίωξη του κυβερνοεγκλήματος», «Κυβερνοέγκλημα και Κυβερνοασφάλεια» και Κυβερνοέρευνα και Ψηφιακές Αποδείξεις». Τέλος, δημιούργησε 5 διαδικτυακά συνέδρια πάνω στις κατευθύνσεις «Διαδικτυακές Απάτες», «Ανίχνευση, Έρευνα και Δίωξη του Κυβερνοεγκλήματος», «Έρευνα και Διαδικτυακές Αποδείξεις», «Σεξουαλική Εκμετάλλευση των Παιδιών στο Διαδίκτυο», «Συνεργασία μεταξύ Αστυνομικών και Δικαστικών Αρχών για το θέμα της Παιδικής Σεξουαλικής Εκμετάλλευσης».

Περαιτέρω, η Επιτροπή καλεί την Eurojust να εντοπίσει τα κύρια εμπόδια που παρεμβάλλονται στην δικαστική συνεργασία στον τομέα των διερευνήσεων ηλεκτρονικών εγκλημάτων και στον συντονισμό μεταξύ κρατών μελών και τρίτων χωρών και να υποστηρίξει την διερεύνηση και τη δίωξη του ηλεκτρονικού εγκλήματος σε επιχειρησιακό και στρατηγικό επίπεδο καθώς και τις εκπαιδευτικές δραστηριότητες στον τομέα.

Τέλος, η Επιτροπή καλεί την Eurojust και το Ευρωπαϊκό Κέντρο για εγκλήματα στον Κυβερνοχώρο (EC3) της Europol να συνεργαστούν στενά, μεταξύ άλλων μέσω ανταλλαγής πληροφοριών, προκειμένου να ενισχύσουν την αποτελεσματικότητά τους στην καταπολέμηση του ηλεκτρονικού εγκλήματος, με βάση τις αντίστοιχες εντολές και τις αρμοδιότητές τους[102].

Ως εκ τούτου, η Eurojust και η Europol έχουν στενή συνεργασία στα τρία σημεία εστίασης που αφορούν το κυβερνοέγκλημα, δηλαδή τις κυνερνοεπιθέσεις, την

[102]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean. gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y» (πρόσβαση στις 1-12-2019).

παιδική κακοποίηση και τις οικονομικές απάτες. Η Eurojust ασχολείται με τα παραπάνω σημεία την τελευταία δεκαετία και επιπλέον είχε συμμετάσχει στον Πολιτικό Κύκλο του EMPACT 2014-2017 ενώ συμμετέχει στον τρέχοντα Πολιτικό Κύκλο του EMPACT 2018-2021 για όλες τις τρεις προτεραιότητες που σχετίζονται με τον κυβερνοχώρο. Για να διασφαλίσουν ότι τα κράτη μέλη επωφελούνται περισσότερο από τις δύο υπηρεσίες, η Europol και η Eurojust εκτελούν τις διαδικασίες τους με τέτοιο τρόπο έτσι ώστε να αποφευχθεί η επικάλυψη των εργασιών τους και να εξασφαλιστεί το καλύτερο δυνατόν επίπεδο συνεργασίας τους.

5.3 Επεξεργασία πολιτικής και ανάπτυξη ικανοτήτων για την άμυνα στον Κυβερνοχώρο σε σχέση με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)

Η Ύπατη Εκπρόσωπος έχει αιτηθεί από τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας να συνεργαστούν για την εκτίμηση των επιχειρησιακών απαιτήσεων της ΕΕ για άμυνα στον κυβερνοχώρο και προώθηση της ανάπτυξης ενωσιακών ικανοτήτων και τεχνολογιών άμυνας στον κυβερνοχώρο για την αντιμετώπιση όλων των πτυχών της ανάπτυξης ικανοτήτων – συμπεριλαμβανομένων του δόγματος, της ηγεσίας, της οργάνωσης, του προσωπικού, της εκπαίδευσης, της τεχνολογίας, της υποδομής, της εφοδιαστικής και της διαλειτουργικότητας.

Επιπλέον, η Ύπατη Εκπρόσωπος έχει αιτηθεί από τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας να συνεργαστούν για τη διαμόρφωση του ενωσιακού πλαισίου πολιτικής της άμυνας στον κυβερνοχώρο για την προστασία δικτύων στο πλαίσιο των αποστολών της ΚΠΑΑ, συμπεριλαμβανόμενης της δυναμικής διαχείρισης κινδύνων, της βελτιωμένης ανάλυσης απειλών και της ανταλλαγής πληροφοριών, καθώς και για τη βελτίωση των ευκαιριών για εκπαίδευση και ασκήσεις άμυνας στον κυβερνοχώρο για τους στρατιωτικούς σε ευρωπαϊκό και πολυεθνικό πλαίσιο, συμπεριλαμβανομένης της ενσωμάτωσης στοιχείων άμυνας στον κυβερνοχώρο σε υφιστάμενους καταλόγους ασκήσεων.

Σε αυτό το πλαίσιο, το θέμα της Κυβερνοασφάλειας συζητήθηκε στο Ευρωπαϊκό Συμβούλιο το Δεκέμβριο του 2013, το οποίο απεφάνθη ανάπτυξη δράσης στους εξής πέντε τομείς: Πρώτον, στην προαγωγή της ανάπτυξης κυβερνοαμυντικών ικανοτήτων, έρευνας και τεχνολογιών στο πλαίσιο του Χάρτη Κυβερνοασφάλειας της EDA. Δεύτερον, στην προστασία των δικτύων που υποστηρίζουν τα ιδρύματα του CSDP[103], τις αποστολές και τις διεργασίες τους. Τρίτον, στη βελτίωση της εκπαίδευσης, επιμόρφωσης και της εξάσκησης των χωρών μελών στην Κυβερνοάμυνα, σε ευρωπαϊκό και διεθνικό επίπεδο. Τέταρτον, στην ενδυνάμωση της συνεργασίας με το ΝΑΤΟ και άλλους διεθνείς οργανισμούς, τον ιδιωτικό τομέα και την ακαδημαϊκή κοινότητα για την εξασφάλιση αποτελεσματικών μηχανισμών άμυνας και πέμπτον, στην ανάπτυξη μηχανισμών έγκαιρων προειδοποιήσεων και αντίδρασης και στην υλοποίηση συνεργειών μεταξύ διαφορετικών φορέων στην αντιμετώπιση των κυβερνοαπειλών[104].

Περαιτέρω, η Ύπατη Εκπρόσωπος έχει αιτηθεί από τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας να συνεργαστούν για την προώθηση του διαλόγου και του συντονισμού μεταξύ πολιτικών και στρατιωτικών φορέων στην ΕΕ – με ιδιαίτερη

[103] Common Security and Defense Policy

[104]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean. gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y (πρόσβαση στις 2-12-2019).

έμφαση στην ανταλλαγή καλών πρακτικών, πληροφοριών και έγκαιρης προειδοποίησης, την αντιμετώπιση συμβάντων, την εκτίμηση κινδύνου και την ευαισθητοποίηση και απόδοση προτεραιότητας στην ασφάλεια στον κυβερνοχώρο.

Τέλος, η Ύπατη Εκπρόσωπος έχει αιτηθεί από τα κράτη μέλη και τον Ευρωπαϊκό Οργανισμό Άμυνας να συνεργαστούν για τον διάλογο με διεθνείς εταίρους, συμπεριλαμβανομένου του ΝΑΤΟ, άλλους διεθνείς οργανισμούς και διεθνή κέντρα αριστείας για να εξασφαλιστούν αποτελεσματικές αμυντικές δυνατότητες, να προσδιοριστούν τομείς συνεργασίας και να αποφευχθεί αλληλοεπικάλυψη προσπαθειών.

Σε αυτό το πλαίσιο, οι ανεπίσημες συναντήσεις εκπροσώπων της ΕΕ και του ΝΑΤΟ σε θέματα κυβερνοασφάλειας διεξάγονται τακτικά την τελευταία δεκαετία, ενώ κοινοί τομείς για περαιτέρω συνεργασία έχουν ήδη εντοπιστεί, όπως η ανάγκη για την ανάπτυξη της γνώσης στα θέματα κυβερνοασφάλειας, για την εκπαίδευση και την ανάπτυξη ικανοτήτων στα πλαίσια της κυβερνοάμυνας.

5.4 Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων με στόχο την ασφάλεια στον Κυβερνοχώρο

Αναφορικά με την προώθηση της ενιαίας αγοράς για προϊόντα ασφάλειας στον κυβερνοχώρο, η Επιτροπή έχει εγκαινιάσει μια πλατφόρμα σχετικά με λύσεις Ασφαλείας Δικτύων και Πληροφοριών δημόσιου - ιδιωτικού τομέα αναπτύσσει κίνητρα για τη θέσπιση ασφαλών λύσεων της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) και την αφομοίωση καλών επιδόσεων ασφάλειας κυβερνοχώρου που θα εφαρμοστεί σε προϊόντα της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) που χρησιμοποιούνται στην Ευρώπη.

Στο πλαίσιο αυτό, η Πλατφόρμα Ασφαλείας, Δικτύων και Πληροφοριών ακολουθεί μια προσέγγιση από κάτω προς τα πάνω, αντλώντας από τις πρακτικές εργασίας των δημόσιων και ιδιωτικών συμμετεχόντων. Έχουν πραγματοποιηθεί συνεδριάσεις της πλατφόρμας Ασφαλείας, Δικτύων και Πληροφοριών από τα μέσα του 2013, μετά από πρόσκληση εκδήλωσης ενδιαφέροντος, όπου περίπου 230 δημόσιοι και ιδιωτικοί οργανισμοί συμμετείχαν στην πλατφόρμα, ήτοι οργανισμοί από τη Νορβηγία, συμπεριλαμβανομένων εκπροσώπων από τα υπουργεία, τους οργανισμούς Ασφαλείας, Δικτύων και Πληροφοριών, NRAs[105] και εθνικών CERT, καθώς και την ερευνητική και την ακαδημαϊκή κοινότητα, από διάφορους τομείς της βιομηχανίας, όπως της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας (ΤΠΕ), ταχυδρομεία, μεταφορές, υγειονομική περίθαλψη, άμυνα, ενέργεια, νερό καθώς και συνάδελφοι από DG ENER, MOVE, HOME, MARKT, ENTR, JRC ή εκπρόσωποι του Ευρωπαϊκού Κοινοβουλίου που συμμετείχαν ή ακολουθούσαν τις εργασίες της πλατφόρμας[106].

Μετά την πρώτη συνεδρίαση της ολομέλειας, η Πλατφόρμα Ασφαλείας, Δικτύων και Πληροφοριών χωρίστηκε σε 3 Ομάδες Εργασίας (ΟΕ): Η πρώτη (ΟΕ1) για τη διαχείριση των κινδύνων ασφάλειας στον κυβερνοχώρο, η δεύτερη (ΟΕ2) σχετικά με την ανταλλαγή πληροφοριών και την κοινοποίηση περιστατικών και η τρίτη (ΟΕ3) στην έρευνα για την ασφάλεια ICT και στην καινοτομία.

[105] National Risk Assessments

[106]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean. gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 3-12-2019).

Οι Ομάδες Εργασίας οργανώνονται σε υποομάδες. Ειδικότερα, η πρώτη Ομάδας Εργασίας (ΟΕ1) αναφορικά με τη διαχείριση κινδύνων ασφάλειας στον κυβερνοχώρο περιλαμβάνει τέσσερις (4) υποομάδες, όπου η πρώτη αφορά στις υπάρχουσες μεθόδους διαχείρισης του κινδύνου και ανάλυση των ελλείψεων, η δεύτερη (ΟΕ2) στις υπάρχουσες μετρήσεις κινδύνων και στην ανάγκη για την έρευνα νέων μέτρων, η τρίτη (ΟΕ3) στις υφιστάμενες προσεγγίσεις για την εφαρμογή της ομάδας πλαισίων και στα μοντέλα αξιολόγησης ωριμότητας και η τέταρτη στην επίγνωση.

Η δεύτερη Ομάδας Εργασίας (ΟΕ2) αναφορικά με την ανταλλαγή πληροφοριών και την κοινοποίηση περιστατικών περιλαμβάνει τρεις (3) υποομάδες, όπου η πρώτη αφορά στις υπάρχουσες πλατφόρμες ανταλλαγής πληροφοριών, η δεύτερη στην ανταλλαγή πληροφοριών, συμπεριλαμβανομένης της κοινοποίησης περιστατικών και η Τρίτη στα πρωτόκολλα ανταλλαγής πληροφοριών.

Η τρίτη Ομάδα Εργασίας (ΟΕ3) αναφορικά με την έρευνα για την ασφάλεια ICT και την καινοτομία περιλαμβάνει πέντε (5) υποομάδες, όπου η πρώτη αναφέρεται στην οργανωτική επιτροπή, η δεύτερη στο ερευνητικό τοπίο ασφάλειας ICT, η τρίτη στις περιπτώσεις επιχειρήσεων και στις πορείες καινοτομίας, η τέταρτη στη στρατηγική ερευνητική ατζέντα και η έμπτη στο στιγμιότυπο της εκπαίδευσης και της κατάρτισης

Το μεγαλύτερο μέρος των εργασιών της πλατφόρμας πραγματοποιείται στις Ομάδες Εργασίας, οι οποίες συναντιούνται σε μία τακτική βάση για τη διεξαγωγή τεχνικών συζητήσεων και την παροχή των σχεδίων εγγράφων συναίνεσης, τα οποία συζητιούνται και εγκρίνονται από την Ολομέλεια. Η Ολομέλεια διοργανώνει συνεδριάσεις προκειμένου να προβεί σε απολογισμό της προόδου των τριών Ομάδων Εργασιών.

Μάλιστα, η πλατφόρμα NIS[107] εξέδωσε ως παραδοτέα οδηγίες σχετικά με τη διαχείριση των κινδύνων και την ανταλλαγή πληροφοριών της πρώτης και της δεύτερης Ομάδας Εργασίας, ερευνητικό τοπίο ασφάλειας ICT, περιπτώσεις επιχειρήσεων και καινοτομία, στρατηγική ερευνητική ατζέντα και στιγμιότυπο της εκπαίδευσης και της κατάρτισης της τρίτης Ομάδας Εργασίας (ΟΕ3).

Η Επιτροπή προτείνει συστάσεις για την ασφάλεια στον κυβερνοχώρο ολόκληρης της αξιακής αλυσίδας της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας (ΤΠΕ), αξιοποιώντας τις εργασίες της εν λόγω πλατφόρμας.

Στο πλαίσιο αυτό, η πλατφόρμα Ασφαλείας Δικτύων και Πληροφοριών έχει εκδώσει κατευθυντήριες γραμμές σχετικά με τη διαχείριση των κινδύνων, την ανταλλαγή πληροφοριών και την κοινοποίηση περιστατικών. Αυτές χρησίμευσαν ως βάση για την Επιτροπή για να αναπτύξει τις συστάσεις της για την ασφάλεια στον κυβερνοχώρο.

Η Επιτροπή είχε σκοπό να εξετάσει τρόπους με τους οποίους οι μεγάλοι πάροχοι υλισμικού και λογισμικού της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας

[107] Network and Information Systems

(ΤΠΕ) θα ήταν δυνατόν να ενημερώνουν τις αρμόδιες εθνικές αρχές περί των ευάλωτων σημείων που εντοπίζουν και τα οποία θα μπορούσαν να έχουν σημαντικές επιπτώσεις ασφάλειας.

Η Επιτροπή έχει αιτηθεί από τον ENISA να αναπτύξει, σε συνεργασία με τις συναφείς αρμόδιες εθνικές αρχές, τους ενδιαφερόμενους φορείς, τους διεθνείς και ευρωπαϊκούς οργανισμούς τυποποίησης και το Κοινό Κέντρο Ερευνών της Ευρωπαϊκής Επιτροπής, τεχνικές κατευθυντήριες γραμμές και συστάσεις για την θέσπιση προτύπων Ασφαλείας Δικτύων και Πληροφοριών και καλών πρακτικών στον δημόσιο και τον ιδιωτικό τομέα.

Στο πλαίσιο αυτό, ο ENISA υποστηρίζει τις δραστηριότητες της πλατφόρμας Ασφαλείας Δικτύων και Πληροφοριών και έχει δημοσιεύσει κατευθυντήριες γραμμές και εκθέσεις σε διάφορους τομείς. Ειδικότερα, έχει δημοσιεύσει κατευθυντήριες γραμμές για τους παρόχους υπηρεσιών εμπιστοσύνης για να μετριαστούν οι επιπτώσεις των περιστατικών ασφάλειας και να διενεργηθεί αξιολόγηση του κινδύνου, συστάσεις για τη μεθοδολογία της αξιολόγησης της σοβαρότητας των παραβιάσεων προσωπικών δεδομένων, αναλύσεις σχετικά με τις εξαρτήσεις του τομέα των ηλεκτρονικών επικοινωνιών από την παροχή ηλεκτρικού ρεύματος, οδηγό ορθής πρακτικής για τις ομάδες CERT σχετικά με την οδηγία για τις επιθέσεις κατά των πληροφοριακών συστημάτων, έκθεση σχετικά με την εθνική αγωγή για την ανθεκτικότητα, οδηγό ορθής πρακτικής για Συναγερμούς-Προειδοποιήσεις-Ανακοινώσεις για τις ομάδες CERT, αξιολόγηση του κινδύνου σε εθνικό επίπεδο, οδηγό ορθής πρακτικής για την ασφαλή ανάπτυξη κυβερνητικών cloud, σχέδια για τα μέτρα ασφαλείας του λογιστικού ελέγχου, και τεχνικές κατευθυντήριες γραμμές για την αναφορά συμβάντων στον τομέα των ηλεκτρονικών επικοινωνιών.

Η Επιτροπή καλεί τους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα να προωθήσουν την ανάπτυξη και θέσπιση, υπό την καθοδήγηση της βιομηχανίας, προτύπων ασφάλειας, τεχνικών προτύπων και αρχές για την ασφάλεια και την ιδιωτικότητα βάσει σχεδιασμού, από τους κατασκευαστές προϊόντων της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) και τους παρόχους υπηρεσιών, συμπεριλαμβανομένων και των παρόχων υπηρεσιών cloud computing. Οι νέες γενιές λογισμικού και υλισμικού πρέπει να είναι εξοπλισμένες με ισχυρότερα, ενσωματωμένα και εύχρηστα χαρακτηριστικά ασφάλειας[108].

Ως εκ τούτου, στο πρόγραμμα πλαίσιο «Ορίζοντας 2020» της ΕΕ υπήρξαν κλήσεις για την έρευνα και την καινοτομία σε αρχιτεκτονικές-εφαρμογές security-by-design και privacy-by-design, δηλαδή εφαρμογές για την ασφάλεια δια του σχεδιασμού και εφαρμογές για την προστασία των προσωπικών δεδομένων δια του σχεδιασμού.

Η Επιτροπή καλεί τους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα να αναπτύξουν, υπό την καθοδήγηση της βιομηχανίας, πρότυπα για τις επιδόσεις των επιχειρήσεων στον τομέα της ασφάλειας του κυβερνοχώρου και να βελτιώσουν τις διαθέσιμες στο κοινό πληροφορίες, αναπτύσσοντας σήματα ασφάλειας ή επίσημα σήματα που θα υποβοηθούν τους καταναλωτές στη διερεύνηση της αγοράς.

[108] Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y (πρόσβαση στις 3-12-2019).

Συνεπεία της ανωτέρω κλήσης και στα πλαίσια της στρατηγικής Cloud Computing της ΕΕ, έχει γίνει έργο για να βρεθεί η άκρη στο λαβύρινθο των υφιστάμενων προτύπων, έτσι ώστε οι χρήστες να απολαμβάνουν τη διαλειτουργικότητα, τη φορητότητα των δεδομένων και την αναστρεψιμότητα. Η Επιτροπή εργάζεται με την υποστήριξη του ENISA, καθώς και άλλων αρμόδιων φορέων, για να βοηθήσει στην ανάπτυξη των πανευρωπαϊκών εθελοντικών συστημάτων πιστοποίησης και να καθιερώσει μια λίστα των εν λόγω συστημάτων.

Αναφορικά με την προώθηση των επενδύσεων για Έρευνα και Ανάπτυξη καθώς και της καινοτομίας, η Επιτροπή χρησιμοποιεί το πρόγραμμα Ορίζοντας 2020 για την αντιμετώπιση σειράς τομέων ιδιωτικότητας και ασφάλειας της Τεχνολογίας της Πληροφορίας και της Επικοινωνίας από την Έρευνα & Ανάπτυξη μέχρι την καινοτομία και την εγκατάσταση. Με το πρόγραμμα Ορίζοντας 2020 αναπτύσσονται επίσης εργαλεία και μέσα καταπολέμησης των εγκληματικών και τρομοκρατικών δραστηριοτήτων με στόχο τον κυβερνοχώρο.

Ειδικότερα, το Ευρωπαϊκό Πρόγραμμα Πλαίσιο για την Έρευνα και την καινοτομία, «Ορίζοντας 2020», έχει τεθεί σε ισχύ την 1η Ιανουαρίου 2014. Τα προγράμματα εργασιών και οι προτάσεις για όλα τα έτη μέχρι το 2020 έχουν ήδη δημοσιευθεί και καλύπτουν τις δράσεις έρευνας στις Τεχνολογίες της Πληροφορίας και της Επικοινωνίας (ΤΠΕ), τις αναπτυξιακές και καινοτόμες δράσεις για την προστασία της ιδιωτικότητας, την ασφάλεια στον κυβερνοχώρο, την ενίσχυση της εμπιστοσύνης προς τις Τεχνολογίες της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) και το έγκλημα στον κυβερνοχώρο[109].

Η Επιτροπή δημιουργεί μηχανισμούς για τον καλύτερο συντονισμό των ερευνητικών θεματολογίων των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης και των κρατών μελών θεσπίζει κίνητρα προκειμένου τα κράτη μέλη να επενδύσουν περισσότερο στην Έρευνα και την Ανάπτυξη.

Σε αυτό το πλαίσιο, η τρίτη Ομάδα Εργασίας (ΟΕ3) της Πλατφόρμας Ασφαλείας Δικτύων και Πληροφοριών αντιμετωπίζει τα ζητήματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, την έρευνα και την καινοτομία.

Λαμβάνοντας υπόψη την πολυπλοκότητα των προκλήσεων και την ποικιλία των παραγόντων που εμπλέκονται στην ασφάλεια στον κυβερνοχώρο, στην προστασία της ιδιωτικότητας και στην έρευνα για την ενίσχυση της εμπιστοσύνης, η τρίτη Ομάδα Εργασίας (ΟΕ3) χρησιμεύει επίσης ως διαμεσολαβητής για το συντονισμό και τη συνεργασία μεταξύ ερευνητικών προγραμμάτων σε όλη την Ευρώπη, συμπεριλαμβανομένων των βιομηχανικών ερευνών και εθνικών προγραμμάτων έρευνας και καινοτομίας των κρατών μελών.

Η τρίτη Ομάδα Εργασίας (ΟΕ3) της Πλατφόρμας Ασφαλείας Δικτύων και Πληροφοριών παρουσίασε ένα χάρτη του ερευνητικού τοπίου, συμπεριλαμβανομένου του εντοπισμού-ταυτοποίησης, των εθνικών προγραμμάτων Έρευνας & Ανάπτυξης

[109] Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 3-12-2019).

στην ασφάλεια στον κυβερνοχώρο, της αξιοπιστίας των Τεχνολογιών της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) και της προστασίας της ιδιωτικότητας, ο οποίος χρησιμεύει ως βάση για τη συμμετοχή των εθνικών οργανισμών έρευνας στον καλύτερο συντονισμό ερευνητικών προγραμμάτων και πόρων.

Η Επιτροπή έχει αιτηθεί από τα κράτη μέλη να αναπτύξουν, καλές πρακτικές προκειμένου να χρησιμοποιήσουν την αγοραστική δύναμη της δημόσιας διοίκησης (πχ. μέσω των δημόσιων συμβάσεων) για να τονώσουν την ανάπτυξη και την εγκατάσταση χαρακτηριστικών ασφάλειας σε προϊόντα και υπηρεσίες Τεχνολογιών της Πληροφορίας και της Επικοινωνίας (ΤΠΕ).

Η Επιτροπή έχει αιτηθεί από τα κράτη μέλη να προωθήσουν την έγκαιρη εμπλοκή της βιομηχανίας και της πανεπιστημιακής κοινότητας στην ανάπτυξη και τον συντονισμό λύσεων. Αυτό επιτυγχάνεται μέσω της πλήρους αξιοποίησης της ευρωπαϊκής βιομηχανικής βάσης και των συναφών τεχνολογικών καινοτομιών Έρευνας & Ανάπτυξης και αποτελεί αντικείμενο συντονισμού των ερευνητικών θεματολογίων πολιτικών και στρατιωτικών οργανισμών.

Στο πλαίσιο αυτό, η τρίτη Ομάδα Εργασίας (ΟΕ3) της πλατφόρμας Ασφαλείας Δικτύων και Πληροφοριών, προάγει τη συμμετοχή της βιομηχανίας και της ακαδημαϊκής κοινότητας σε μελλοντικές έρευνες και καινοτομίες.

Η Επιτροπή έχει αιτηθεί από την Europol και τον ENISA να προσδιορίσουν τις αναδυόμενες τάσεις και ανάγκες με βάση τα εξελισσόμενα χαρακτηριστικά του ηλεκτρονικού εγκλήματος και της ασφάλειας στον κυβερνοχώρο, έτσι ώστε να αναπτυχθούν επαρκή ψηφιακά εργαλεία και τεχνολογίες για εγκληματολογικές έρευνες.

Σε αυτό το πλαίσιο, ο ENISA εγκρίνει κάθε έτος την ετήσια έκθεσή του σχετικά με το τοπίο των απειλών.

Η Επιτροπή καλεί τους ενδιαφερόμενους από τον δημόσιο και τον ιδιωτικό τομέα να αναπτύξουν, σε συνεργασία με τον κλάδο των ασφαλειών, εναρμονισμένα συστήματα μέτρησης για τον υπολογισμό των ασφαλίστρων κινδύνου, που θα επιτρέψουν στις εταιρείες οι οποίες έχουν κάνει επενδύσεις στον τομέα της ασφάλειας να επωφεληθούν από χαμηλότερα ασφάλιστρα κινδύνου[110].

Σε αυτό το πλαίσιο, η Επιτροπή εργάζεται για την ανάλυση της ευρωπαϊκής αγοράς ασφάλειας του κυβερνοχώρου και εξετάζει διάφορους τρόπους επιρροής των ασφάλιστρων του κυβερνοχώρου για την ενίσχυση της ασφάλειας και της ανθεκτικότητας του κυβερνοχώρου.

5.5 Θέσπιση συνεκτικής διεθνούς πολιτικής στον Κυβερνοχώρο για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της ΕΕ

Αναφορικά με την ενσωμάτωση των ζητημάτων που αφορούν τον κυβερνοχώρο στις εξωτερικές σχέσεις της ΕΕ και στην κοινή εξωτερική πολιτική και την πολιτική ασφάλειας, κατά πρώτον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία

[110]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 4-12-2019).

με τα κράτη μέλη, εργάζονται προς την κατεύθυνση κατάρτισης συνεκτικής διεθνούς πολιτικής της ΕΕ για τον κυβερνοχώρο ώστε να ενισχυθεί η συνεργασία με διεθνείς εταίρους και οργανισμούς ζωτικής σημασίας, να ενσωματωθούν τα ζητήματα που αφορούν τον κυβερνοχώρο στην Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (ΚΕΠΠΑ) και να βελτιωθεί ο συντονισμός σχετικά με τα ζητήματα που αφορούν στον κυβερνοχώρο σε παγκόσμιο επίπεδο.

Στο πλαίσιο αυτό, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης - ΕΥΕΔ (European External Action Service - EAAS) έχει τακτικές επαφές με τρίτες χώρες, οι οποίες έχουν καθιερώσει υψηλού επιπέδου διάλογο με την ΕΕ στον κυβερνοχώρο. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης συντονίζει αυτούς τους διαλόγους, με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Δομημένος διάλογος σχετικά με τον κυβερνοχώρο υπάρχει σήμερα με τις ΗΠΑ, με τη μορφή της ομάδας εργασίας ΕΕ-ΗΠΑ για την ασφάλεια και το έγκλημα στον κυβερνοχώρο. Η εν λόγω Ομάδα Εργασίας είναι χωρισμένη σε τέσσερις μικρότερες ομάδες που εργάζονται για τη διαχείριση των συμβάντων στον κυβερνοχώρο, τη συνεργασία δημόσιου και ιδιωτικού τομέα, την ευαισθητοποίηση και το έγκλημα στον κυβερνοχώρο[111].

Η Ομάδα Εργασίας συμβάλλει σημαντικά στη συνεργασία ΕΕ-ΗΠΑ για την ασφάλεια στον κυβερνοχώρο, ιδίως στην προώθηση των συζητήσεων σε επίπεδο εμπειρογνωμόνων σχετικά με επιχειρησιακά θέματα. Μεταξύ άλλων, αξίζει να αναφερθούν οι ασκήσεις για περιστατικά κυβενοασφάλειας της ΕΕ-ΗΠΑ, οι δημόσιες και ιδιωτικές ομάδες εργασίας πάνω σε botnets και έξυπνα δίκτυα, και η κοινή δήλωση για τη δημιουργία ασφαλούς διαδικτύου για τα παιδιά.

Η δεύτερη συνεδρίαση για το Task Force της Ευρώπης και της Κίνας, που φιλοξενήθηκε από την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) με την υποστήριξη της Επιτροπής, πραγματοποιήθηκε με τη συμμετοχή των κρατών μελών. Η συνάντηση αποτέλεσε μια καλή ευκαιρία για εμβάθυνση της συνεργασίας, αλλά τόνισε αναπόφευκτες διαφορές μεταξύ των προσεγγίσεων μας στον κυβερνοχώρο.

Δομημένος διάλογος έχει συσταθεί και με την Ινδία με την οποία τα θέματα που συζητήθηκαν περιελάμβαναν προετοιμασία των στρατηγικών ασφάλειας του κυβερνοχώρου, τυποποίηση και ρυθμιστικά ζητήματα, θέματα της εγκληματικότητας στον κυβερνοχώρο και διεθνή θέματα για τον κυβερνοχώρο. Μάλιστα, έχει συναφθεί συνεργασία σχετικά με θέματα ασφάλειας και του εγκλήματος στον κυβερνοχώρο, με την Ιαπωνία, τη Νότια Κορέα, τη Βραζιλία και την Ταϊβάν.

Κατά δεύτερον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία με τα κράτη μέλη, υποστηρίζουν την ανάπτυξη προτύπων συμπεριφοράς και μέτρων οικοδόμησης εμπιστοσύνης στον τομέα της ασφάλειας του κυβερνοχώρου, διευκολύνουν το διάλογο σχετικά με τον τρόπο εφαρμογής του ισχύοντος διεθνούς δικαίου στον κυβερνοχώρο και προωθούν τη σύμβαση της Βουδαπέστης για την αντιμετώπιση του ηλεκτρονικού εγκλήματος.

Στο πλαίσιο αυτό, τα συνεργαζόμενα κράτη εργάζονται ενεργά για την οικοδόμηση παγκόσμιας συναίνεσης πάνω στα πρότυπα για την υπεύθυνη συμπεριφορά

[111] Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 5-12-2019).

στον κυβερνοχώρο και υποστηρίζουν τη συνέχιση της εφαρμογής του τρέχοντος διεθνούς δικαίου επί της εισαγωγής των νέων κρατών μελών, η οποία θα μπορούσε να αποτρέψει τον ανεπιθύμητο έλεγχο της κυβέρνησης. Η Διαδικασία Λονδίνο αναπτύσσει μια κοινή κατανόηση μεταξύ των ενδιαφερομένων σχετικά με το πώς να διατηρήσει θετικές πτυχές του κυβερνοχώρου και εργάζεται προς την κατεύθυνση που ορίζουν τα καθολικά πρότυπα.

Περαιτέρω, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) διαδραμάτισε ενεργό ρόλο στην οργάνωση του Συνεδρίου της Σεούλ, όπου 1600 συμμετέχοντες έλαβαν μέρος, 87 χώρες με συμμετοχή από τις κυβερνήσεις, την κοινωνία των πολιτών, τον ιδιωτικό τομέα, την ακαδημαϊκή κοινότητα και τους διεθνείς οργανισμούς. Οκτώ υπουργικού επιπέδου ομιλητές ήταν παρόντες από τα κράτη μέλη της ΕΕ. Τα θέματα των συζητήσεων επικεντρώθηκαν στις οικονομικές δυνατότητες του κυβερνοχώρου, την ανάπτυξη ικανοτήτων, το έγκλημα στον κυβερνοχώρο, τη διεθνή ασφάλεια, τα θέματα εμπιστοσύνης και την ανθεκτικότητα στον κυβερνοχώρο. Η Διάσκεψη επικύρωσε δύο παράλληλες διαδικασίες στον κυβερνοχώρο, αφενός το αυξανόμενο χάσμα σε ζητήματα διακυβέρνησης του διαδικτύου και αφετέρου την αυξανόμενη συναίνεση για την ανάγκη περισσότερων επενδύσεων στην οικοδόμηση ικανοτήτων στον κυβερνοχώρο. Τα Μέτρα Οικοδόμησης Εμπιστοσύνης έχουν σχεδιαστεί για την αντιμετώπιση εσφαλμένης κατανόησης και εκτίμησης των συμβάντων του κυβερνοχώρου, για να μειωθεί ο κίνδυνος της σύγχυσης μεταξύ των κρατών. Ο OSCE (Organization for Security and Co-operation in Europe) έχει συμφωνήσει σε μια πρώτη δέσμη μέτρων οικοδόμησης εμπιστοσύνης, τα πρώτα εκ των οποίων έχουν συμφωνηθεί σε πολυμερές επίπεδο. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) και τα κράτη μέλη της ΕΕ υποστηρίζουν τις πρωτοβουλίες για την ανάπτυξη των μέτρων οικοδόμησης εμπιστοσύνης εντός του ARF (ASEAN Regional Forum, ASEAN: Association of South East Asian Nations)[112].

Κατά τρίτον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία με τα κράτη μέλη, υποστηρίζουν την προώθηση και την προστασία των θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένων της πρόσβασης στις πληροφορίες και της ελευθερίας της έκφρασης, εστιάζοντας στην ανάπτυξη νέων δημόσιων κατευθυντηρίων γραμμών σχετικά με την ελευθερία της έκφρασης ηλεκτρονικά, είτε σε διαδικτυακή σύνδεση είτε εκτός, στην παρακολούθηση της εξαγωγής προϊόντων ή υπηρεσιών που ενδέχεται να χρησιμοποιηθούν για διαδικτυακή λογοκρισία ή μαζική επιτήρηση, στην ανάπτυξη μέτρων και εργαλείων για την επέκταση της πρόσβασης στο διαδίκτυο, του ανοικτού χαρακτήρα του και της ανθεκτικότητας για την αντιμετώπιση λογοκρισίας ή μαζικής επιτήρησης από τεχνολογίες επικοινωνιών και στην ενίσχυση των ενδιαφερόμενων για να χρησιμοποιούν τεχνολογίες επικοινωνιών προκειμένου να προωθήσουν τα θεμελιώδη δικαιώματα.

Στο πλαίσιο αυτό, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) προέβη σε ανεπίσημες συζητήσεις με την Επιτροπή και τα κράτη μέλη, σύμφωνα με το σχέδιο δράσης, στο πλαίσιο της προετοιμασίας για το σχέδιο κατευθυντήριων γραμμών σχετικά με την ελευθερία της έκφρασης online και offline. Ο στόχος των κατευθυντήριων γραμμών]ήταν να αντιμετωπιστούν οι αδικαιολόγητοι περιορισμοί στην ελευθερία της έκφρασης, Επιπλέον, πραγματοποιήθηκαν διαβουλεύσεις με την κοινωνία των

[112]Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 3-12-2019).

πολιτών σχετικά με τη βελτίωση της επαφής και της προστασίας δημοσιογράφων και bloggers, ενώ παράλληλα η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) δρομολόγησε δημόσια διαβούλευση μέσω του Διαδικτύου.

Κατά τέταρτον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία με τα κράτη μέλη, συνεργάζονται με διεθνείς εταίρους και οργανισμούς, τον ιδιωτικό τομέα και την κοινωνία των πολιτών για την υποστήριξη της γενικής οικοδόμησης ικανοτήτων σε τρίτες χώρες αποβλέποντας στη βελτίωση της πρόσβασης στις πληροφορίες και στο ανοικτό διαδίκτυο, την πρόληψη και την αντιμετώπιση απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων τυχαίων συμβάντων, του ηλεκτρονικού εγκλήματος και της τρομοκρατίας στον κυβερνοχώρο, καθώς και για την ανάπτυξη συντονισμού μεταξύ των δωρητών με στόχο την καθοδήγηση των προσπαθειών οικοδόμησης ικανοτήτων.

Στο πλαίσιο αυτό, η ΕΕ επιδιώκει να διαδραματίζει ένα ρόλο στην καθοδήγηση των προσπαθειών ενίσχυσης των ικανοτήτων του κυβερνοχώρου σε παγκόσμιο επίπεδο. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) από την πλευρά της συνεργάζεται με το Ινστιτούτο Μελετών Ασφαλείας της ΕΕ για να προωθήσει αυτό το έργο. Τα συνέδρια διοργανώνονται για να συμφωνήσουν σχετικά με την περιφερειακή και λειτουργική εστίαση των προσπαθειών δημιουργίας ικανοτήτων ασφάλειας στον κυβερνοχώρο, την ανάπτυξη του διεθνούς συντονισμού στην ανάπτυξη ικανοτήτων και την ανάπτυξη κατάλληλων λειτουργικών μοντέλων.

Κατά πέμπτον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία με τα κράτη μέλη, χρησιμοποιούν διάφορα ενωσιακά μέτρα παροχής βοήθειας για την οικοδόμηση ικανοτήτων στον τομέα της ασφάλειας του κυβερνοχώρου. Σε αυτά συμπεριλαμβάνονται η στήριξη της κατάρτισης του προσωπικού των υπηρεσιών εφαρμογής του νόμου, του δικαστικού και τεχνικού προσωπικού για την αντιμετώπιση απειλών στον κυβερνοχώρο, καθώς και η υποστήριξη της κατάρτισης συναφών εθνικών πολιτικών, στρατηγικών και θεσμικών οργάνων σε τρίτες χώρες[113].

Στο πλαίσιο αυτό, η ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε τρίτες χώρες αποτελεί προτεραιότητα τόσο στη στρατηγική της ΕΕ όσο και παγκοσμίως. Απαιτεί να επικεντρωθεί στη βελτίωση της διακυβέρνησης, την προστασία των υποδομών, την έγκριση του κράτους δικαίου και την παροχή κατάρτισης. Πιλοτικά έργα για την ανάπτυξη ικανοτήτων κυβερνοασφάλειας έχουν ήδη ξεκινήσει από το 2015. Για την επίτευξη απτών αποτελεσμάτων και την προώθηση των βασικών αξιών της ΕΕ μέσα από την ανάπτυξη ικανοτήτων κυβερνοασφάλειας, το θέμα αυτό πρέπει να γίνει το κεντρικό στοιχείο της ευρωπαϊκής διεθνούς πολιτικής για την ασφάλεια στον κυβερνοχώρο.

Κατά έκτον, η Επιτροπή και η Ύπατη Εκπρόσωπος, σε συνεργασία με τα κράτη μέλη, ενισχύουν τον συντονισμό σε θέματα πολιτικής και ανταλλαγής πληροφοριών μέσω των διεθνών δικτύων προστασίας υποδομών πληροφοριών ζωτικής σημασίας, όπως το δίκτυο Meridian, τη συνεργασία μεταξύ των αρμόδιων αρχών Ασφάλειας Δικτύων και Πληροφοριών και άλλων φορέων.

[113] Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus -«hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1& is Allowed=y » (πρόσβαση στις 5-12-2019).

Στο πλαίσιο αυτό, το Ευρωπαϊκό forum για τα κράτη μέλη εξετάζει την πολιτική συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για θέματα ασφάλειας δικτύων.

Συνοπτικά, η ενίσχυση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, επιτυγχάνεται πρώτον μέσα από τη βελτίωση της επιχειρησιακής συνεργασίας μεταξύ των αρχών επιβολής του νόμου μέσω της ενίσχυσης και της διευκρίνισης των αρμοδιοτήτων της Europol, της Eurojust και άλλων δομών. Δεύτερον, μέσα από συντονισμένα και διασυνδεδεμένα προγράμματα κατάρτισης για τις αρχές επιβολής του νόμου και τις δικαστικές αρχές των χωρών της ΕΕ συμπεριλαμβανομένων της Europol, της Eurojust, της Ευρωπαϊκής Αστυνομικής Ακαδημίας και του Ευρωπαϊκού Δικτύου Κατάρτισης Δικαστικών. Τρίτον, μέσα από τη βελτιωμένη πολιτική συνεργασία και συντονισμό μεταξύ των χωρών της ΕΕ με τη δημιουργία μονίμου ευρωπαϊκού σημείου επαφής για την ανταλλαγή πληροφοριών καθώς επίσης και ευρωπαϊκής πλατφόρμας κατάρτισης σχετικά με το έγκλημα στον κυβερνοχώρο. Τέταρτον, μέσα από πολιτική και νομική συνεργασία με τρίτες χώρες μέσω της Σύμβασης για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης το 2001 (και του συμπληρωματικού της πρωτοκόλλου), της ομάδας Λυών-Ρώμη του G8 για το έγκλημα υψηλής τεχνολογίας και έργων που διαχειρίζεται η Interpol. Πέμπτον, μέσα από βελτιωμένο διάλογο μεταξύ δημόσιου και ιδιωτικού τομέα για την καλλιέργεια αμοιβαίας εμπιστοσύνης και την ανταλλαγή σχετικών πληροφοριών. Έκτον, μέσα από την τυποποίηση της νομοθεσίας και των ορισμών των χωρών της ΕΕ στον τομέα του εγκλήματος στον κυβερνοχώρο. Έβδομον, μέσα από τη διαμόρφωση μετρήσεων/δεικτών όσον αφορά την έκταση του εγκλήματος στον κυβερνοχώρο. Όγδοον, μέσα από την ευαισθητοποίηση όσον αφορά τους κινδύνους και το κόστος του εγκλήματος στον κυβερνοχώρο. Ένατον μέσα από ερευνητικά προγράμματα της ΕΕ, όπως στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας - Αστυνομία.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η αυξανόμενη εξάρτηση από τις τεχνολογίες πληροφοριών και επικοινωνιών σε όλους του τομείς της ανθρώπινης ζωής είναι δεδομένη, με το διαδίκτυο να παίζει πρωταγωνιστικό ρόλο. Η διαχείριση, όμως, των πόρων και των εργαλείων ανάπτυξης των διαδικτυακών χώρων δε ρυθμίζεται από συγκεκριμένα όργανα, αλλά αντίθετα ακολουθεί την αρχή μιας πολυμερούς διακυβέρνησης, στην οποία συμμετέχει ένα πλήθος κυβερνητικών και μη παραγόντων.

Όλοι οι εμπλεκόμενοι φορείς, δηλαδή οι κυβερνήσεις, οι δημόσιες αρχές, ο ιδιωτικός τομέας ή οι μεμονωμένοι πολίτες-χρήστες, πρέπει να αναγνωρίσουν την συνυπευθυνότητα, να αναλάβουν δράση για να αυτοπροστατευθούν και να συνεργάζονται για την εξασφάλιση συντονισμένης αντίδρασης με σκοπό την ενίσχυση της ασφάλειας του κυβερνοχώρου. Η υλοποίηση ενός ανοιχτού και ελεύθερου κυβερνοχώρου συνεπάγεται με την ανάληψη μιας κοινής ευθύνης από κάθε χρήστη σε θέματα ευαισθητοποίησης. Κάθε χρήστης θα πρέπει να δίνει τη δέουσα προσοχή και να λαμβάνει κάθε απαραίτητο μηχανισμό άμυνας για τη διαφύλαξη των προσωπικών του δεδομένων και την ατομική του συμβολή στη διαμόρφωση ενός ασφαλούς διαδικτυακού περιβάλλοντος.

Η ασφάλεια και η άμυνα εναντίον των απειλών στον κυβερνοχώρο είναι ένα δύσκολα διαχειρίσιμο πρόβλημα. Απαιτεί επισταμένη προσοχή τόσο από το δημόσιο

όσο και από τον ιδιωτικό τομέα. Για την ενίσχυση του επιπέδου της ασφάλειας του κυβερνοχώρου και τη διαφύλαξη των δικαιωμάτων των πολιτών απαιτείται ισχυρή υποστήριξη και δέσμευση από τον ιδιωτικό τομέα. Για την ανάπτυξη αμοιβαίας εμπιστοσύνης κρίσιμο ρόλο διαδραματίζει όχι μόνο η ουσιαστική και συμπληρωματική συνεργασία στον τομέα της κυβερνοασφάλειας του ιδιωτικού τομέα και των δημόσιων αρχών, τόσο σε επίπεδο ΕΕ όσο και σε εθνικό επίπεδο, αλλά και η ανταλλαγή γνώσεων και καλύτερων πρακτικών μεταξύ αυτών. Και αυτό γιατί οι προκλήσεις που έχουν να αντιμετωπίσουν τόσο ο ιδιωτικός όσο και ο δημόσιος τομέας έχουν εντυπωσιακές ομοιότητες. Μέσω της σύμπραξης του δημόσιου και ιδιωτικού τομέα είναι δυνατή η ανάπτυξη έγκυρων σεναρίων και η αξιολόγηση των επιπτώσεων στις υπηρεσίες που παρέχουν αλλά και της αποτελεσματικότητας του τρόπου αντίδρασης. Ο ιδιωτικός τομέας θα πρέπει επίσης να έχει μια ξεκάθαρη στάση στις μελλοντικές διασκέψεις, με επίκεντρο το ρόλο του στην συνεργασία για την αντιμετώπιση της κρίσης στον κυβερνοχώρο, στην αντιμετώπιση πιθανών απειλών και στην ανταπόκριση σε σενάρια ασκήσεων στον ιδιωτικό τομέα. Δεν είναι πλέον επαρκές για τις εταιρείες του ιδιωτικού τομέα να μένουν αμέτοχες και να περιμένουν για την επιβολή της νομοθεσίας κατά του εγκλήματος στον κυβερνοχώρο. Για το δικό τους αρχικά συμφέρον αλλά και για το συμφέρον όλου του δικτυωμένου περιβάλλοντος απαιτείται η επαγρύπνησή τους.

Επιπλέον, οι ασκήσεις αντιμετώπισης κρίσης στον κυβερνοχώρο παρέχουν ένα εξαιρετικό τρόπο να εξετάζονται και να διατηρούνται σε ισχύ οι διαδικασίες συνεργασίας, τα σχέδια και οι δομές για την αντιμετώπιση κρίσεων μεγάλης κλίμακας. Ιδέες και γνώσεις, πάνω σε αυτόν τον τομέα, θα πρέπει να ανταλλάσσονται όσο το δυνατόν περισσότερο και οι προσπάθειες πρέπει να είναι ευθυγραμμισμένες μεταξύ τους, τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Αυτές οι ασκήσεις θα πρέπει να συμπληρώνονται με τεχνική εκπαίδευση σε θέματα ασφάλειας στον κυβερνοχώρο που να εστιάζει κυρίως στην ανάπτυξη δεξιοτήτων. Οι τεχνικές ασκήσεις για την ασφάλεια στον κυβερνοχώρο θα βοηθήσουν, επίσης, στην μεγάλης σημασίας επαγγελματική κατάρτιση των εμπειρογνωμόνων πάνω στα θέματα αυτά. Κατά την επόμενη δεκαετία, λόγω της αυξανόμενης πολυπλοκότητα της ασφάλειας στον κυβερνοχώρο, το ειδικευμένο και ικανό προσωπικό του κυβερνοχώρου θα αποτελεί ένα σπάνιο και ακριβό πόρο, τόσο στην Ευρώπη όσο και σε όλο τον κόσμο.

Η Ευρωπαϊκή Ένωση επιδιώκει την προώθηση ενός ανοιχτού και ελεύθερου κυβερνοχώρου που να ενθαρρύνει την ανάπτυξη των βασικών προτύπων συμπεριφοράς και να τηρεί την εφαρμογή της ισχύουσας διεθνούς νομοθεσίας. Οι βασικές αξίες της ανθρώπινης αξιοπρέπειας, της ελευθερίας, της δημοκρατίας, της ισότητας, του κράτους δικαίου και του σεβασμού των θεμελιωδών ανθρωπίνων δικαιωμάτων αποτελούν δεσμεύσεις, τις οποίες η ευρωπαϊκή κοινότητα οφείλει να κατοχυρώσει με την ενεργή συμμετοχή της στις διεθνείς προσπάθειες για τη θεμελίωση των προδιαγραφών ασφαλείας στον κυβερνοχώρο και τη διεξαγωγή ουσιαστικού διαλόγου πάνω στα θέματα αυτά. Η ευθύνη για έναν ασφαλέστερο κυβερνοχώρο αντανακλά σε όλους τους εμπλεκόμενους φορείς της διεθνούς πληροφοριακής κοινωνίας.

Ένας αυξανόμενος αριθμός των χωρών της Ευρώπης έχει μια Εθνική Στρατηγική Κυβερνοαφάλειας, η οποία βοηθά στην αντιμετώπιση των κινδύνων που δύναται να υπονομεύσουν την επίτευξη οικονομικών και κοινωνικών οφελών της χώρας από τον κυβερνοχώρο.

Τα περισσότερα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν δημοσιεύσει μια Εθνική Στρατηγική Κυβερνοασφάλειας και μερικά από αυτά την εκδίδουν για δεύτερη φορά. Ο πρακτικός οδηγός του ENISA για τη δημιουργία Εθνικών Στρατηγικών Κυβερνοασφάλειας, σημείωσε τέσσερα σημαντικά βήματα: την ανάπτυξη, εφαρμογή, αξιολόγηση και προσαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Οι Εθνικές Στρατηγικές Κυβερνοασφάλειας παρουσιάζουν κάποιες προκλήσεις μέσα από την αξιολόγησή τους, όπως είναι η ανάγκη επενδύσεων για τον προϋπολογισμό και τους απαιτούμενους πόρους, η έλλειψη καλών πρακτικών και η δυσκολία μέτρησης των επιπτώσεων. Ωστόσο, η αξιολόγηση, πέραν των οικονομικών ελέγχων, μπορεί να προσφέρει σημαντική προστιθέμενη αξία για τον στρατηγικό σχεδιασμό και την υλοποίηση της πολιτικής σε μεσοπρόθεσμη και μακροπρόθεσμη βάση.

Είναι δύσκολο όμως να δημιουργηθεί μία ενιαία πολιτική για τη δημιουργία Στρατηγικών Κυβερνοασφάλειας, καθώς υπάρχει μια αποσπασματική προσέγγιση προς τους τελικούς σκοπούς που μία Εθνική Στρατηγική Κυβερνοασφάλειας αναμένεται να πετύχει. Το γεγονός αυτό είναι σε ένα βαθμό κατανοητό καθώς κάθε χώρα έχει τις δικές της ανάγκες και προτεραιότητες. Εξάλλου, κάθε χώρα πραγματοποιεί την εκτίμηση των κινδύνων που πιθανόν θα κληθεί να αντιμετωπίσει σε εθνικό επίπεδο για την ασφάλεια στον κυβερνοχώρο, ανάλογα με τις υποδομές που διαθέτει και σύμφωνα με τις ιδιαιτερότητές της. Στην εκτίμηση κινδύνου συμμετέχουν φορείς οι οποίοι δεν θα πρέπει να διστάζουν να ζητήσουν καθοδήγηση για τη λήψη ορθών πρακτικών από άλλες χώρες ή ευρωπαϊκούς οργανισμούς.

Ωστόσο, αυτή η αποσπασματική προσέγγιση και ασυνέπεια προς μία κοινή πολιτική έρχεται σε αντίθεση με την ανάγκη για εφαρμογή ενός ευρύτερου πλαισίου μέσω του οποίου οι Εθνικές Στρατηγικές Κυβερνοασφάλειας μπορούν να αξιολογηθούν. Μία αξιολόγηση τόσο της από πρακτική έννοιας αποτελεσματικότητας τους, όσο και της ευρύτερης και πιο σημαντικής αίσθησης του αν οι εκτεταμένες επενδύσεις χρόνου και προσπαθειών αξίζουν τον κόπο για την επίτευξη των τιθέμενων στόχων.

Παρόλα αυτά, είναι δεδομένο ότι η ζημία που προκαλείται από τις κυβερνοεπιθέσεις κάνει την πρόληψη πιο σημαντική από την επιβολή του νόμου και τα διορθωτικά μέτρα. Επίσης, η συνεργασία ο συντονισμός των προσπαθειών σε παγκόσμιο επίπεδο έχουν κομβική σημασία για την ασφάλεια του κυβερνοχώρου, καθώς το μόνο σίγουρο είναι ότι μία απειλή ή ένας στόχος μπορεί να καταστραφεί ταχύτερα και πιο εύκολα όταν βάλλεται συντεταγμένα από πολλούς «σκοπευτές».

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ι. ΕΛΛΗΝΟΓΛΩΣΣΗ

Α. Βιβλία – Μελέτες – Ομιλίες

- Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, Έγκλημα στον Κυβερνοχώρο (ΠοινΧρ 8/2000,675).
- Αργυρόπουλος Α.Δ., «Ηλεκτρονική εγκληματικότητα», Εκδόσεις Σάκκουλα (2001)
- Βλαχόπουλος Κων., Ηλεκτρονικό Έγκλημα: μορφές, πρόληψη, αντιμετώπιση, Νομική Βιβλιοθήκη (2007).
- Γερμανός Γ. - Παπαθανασίου Αν., Νομοθεσία για το Έγκλημα στον Κυβερνοχώρο και την Ψηφιακή Εγκληματικότητα, Εκδόσεις Σάκκουλα (2017).
- Γιαννόπουλος Γ., Η ευθύνη των παρόχων υπηρεσιών στο Internet, Νομική Βιβλιοθήκη (2003).

- Λάζος Γ., Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη (2001).
- Μούσης Ν., Ευρωπαϊκή Ένωση, Δίκαιο, Οικονομία, Πολιτική, Εκδόσεις Παπαζήση, (2015).
- Νάσκου – Περράκη Π., Θεωρήσεις, άσυλο, μετανάστευση και άλλες πολιτικές σχετικές με την ελεύθερη κυκλοφορία των προσώπων, στο Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Ερμηνεία συνθηκών για την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα, Εκδόσεις Σάκκουλα, (2017).
- Νικολακοπούλου–Στεφάνου Η., Οι πολιτικές μετανάστευσης και ασύλου της Ευρωπαϊκής Ένωσης.
- Παπαγιάννης Δον., Ο ευρωπαϊκός χώρος ελευθερίας, ασφάλειας και δικαιοσύνης, Εκδόσεις Σάκκουλα, (2001).
- Παπαγιάννης Δον., Ο χώρος ελευθερίας, ασφάλειας και δικαιοσύνης μετά τη Συνθήκη της Λισαβόνας, ΕΕΕυρΔ.
- Παπαγιάννης Δον., Ο χώρος ασφάλειας στην ΕΕ, Εκδόσεις Σάκκουλα, (2008).
- Παπακωνσταντής Μ., Η τρομοκρατία στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης της Ευρωπαϊκής Ένωσης, Νομική Βιβλιοθήκη, (2019).
- Περράκης Σ., Ο Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης στην ΕΕ Εκδόσεις Σάκκουλας, (2007).
- Στεφάνου Κ./Καταπόδης Γ., Οι ευρωπαϊκές συνθήκες μετά την αναθεώρηση της Λισαβόνας, Εκδόσεις Σάκκουλας, (2008).
- Χριστογιαννόπουλος Ν., Θεωρήσεις, άσυλο, μετανάστευση και άλλες πολιτικές σχετικές με τη ελεύθερη κυκλοφορία των προσώπων, Ερμηνεία κατ' άρθρο της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για την ίδρυση της Ευρωπαϊκής Κοινότητας.

ΙΙ. ΞΕΝΟΓΛΩΣΣΗ

Α. Βιβλία – Μελέτες – Ομιλίες

- Conseil de l' Europeenne, Vivre dans un espace de liberte, securite et justice.
- Elsen C., L' esprit et les ambitions de Tampere, une ere nouvelle pour la cooperation dans le domaine de la justice et les affaires interiures.
- Forester T. and Morisson P., « Computer ethics: Cautionary Tales and ethical dilemmas in computing », Massachusetts Institute of Technology, (1994).
- Furnell Steven , « Κυβερνοέγκλημα, καταστρέφοντας την κοινωνία της πληροφορίας », Εκδ. Παπαζήση (2006).

- Halder, D. και Jaishankar K., «Cybercrime and the Victimization of Women: Laws Rights, and Regulations», Hershey:IGI Global, (2011).

- Jougleux Philippe, Ευρωπαϊκό δίκαιο του διαδικτύου – Νομικές πτυχές του διαδικτύου στην Ευρώπη, σελ. 116, Εκδόσεις Σάκκουλα (2016).

- Miguel P., Freitas F. & Goncalves N., Illegal access to information systems.

- Muller – Graff P.Chr. (Hrsg.) Der Raum der Freiheit, der Sicherheit und des Rechts, 2005, Peers S,, EU Justice and Home Affairs 2. Aufl.(2006).

- Schiffauer P., Zum Verfassungzustand der Europaischen Union nach Unterzeichnung des Vertrages von Lissabon , EuGRZ (2008).

ΙΙΙ. ΙΣΤΟΤΟΠΟΙ

- Επίσημος Διαδικτυακός ιστότοπος του Ευρωπαϊκού Χώρου Δικαιοσύνης, Ελευθερίας και Ασφάλειας - http://www.mfa.gr/ brussels / monimi – antiprosopeia–ee/ellada-sten-ee/europaikos-khoros-dikaiosunes-eleutherias-kai-asfaleia /html ?page=3.

- Επίσημος Διαδικτυακός ιστότοπος του Ευρωπαϊκού Συμβουλίου - http://data.consilium.europa.eu/doc/document/ST-79-2014-INIT/el/pdf.

- Επίσημος Διαδικτυακός ιστότοπος βοηθητικών νομικών κειμένων / ηλεκτρονικό έγκλημα - https://www.lawspot.gr / nomikes - plirofories / voithitika - keimena/elektroniko-egklima.

- Επίσημος Διαδικτυακός ιστότοπος Ηλεκτρονικού Εγκλήματος - https://sites.google.com / site / elektronikoenklema 2012 / ti-einai-elektroniko-enklema.

- Επίσημος Διαδικτυακός ιστότοπος Ευρωπαϊκής Ένωσης https://eur-lex.europa.eu/legal–content/EL/TXT/PDF/?uri=CELEX:32013R0526&from= el.

- Επίσημος Διαδικτυακός ιστότοπος του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών - https://www.enisa.europa.eu / activities/cert.

- Επίσημος Διαδικτυακός ιστότοπος του Συμβουλίου της Ευρωπαϊκής Ένωσης - https://register.consilium.europa.eu/doc/srv?l=EL&f=ST%208543%202012%20INIT.

- Επίσημος Διαδικτυακός ιστότοπος της Europol - www.europol.europa.eu /content/page/about-us.

- Επίσημος Διαδικτυακός ιστότοπος της Eurojust - www.eurojust.europa.eu /content/page/about-us.

- Επίσημος Διαδικτυακός ιστότοπος της Ευρωπαϊκής Υπηρεσίας Άμυνας - www.eda.europa.eu / content / page/about-us

- Επίσημος Διαδικτυακός ιστότοπος του Ιδρυματικού Αποθετήριου Hellanicus - «hellanicus.lib.aegean.gr/bitstream/handle/11610/12450/file0.pdf?sequence=1 &isAllowed=y»