Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 12 Αυγούστου 2016
(OR. en)

9892/1/16
REV 1 DCL 1

GENVAL 67
CYBER 63

ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ

του εγγράφου:	9892/1/16 REV 1
Με ημερομηνία:	15 Ιουλίου 2016
νέος χαρακτηρισμός:	Έγγραφο προσβάσιμο στο κοινό
Θέμα:	Έκθεση αξιολόγησης σχετικά με τον έβδομο γύρο αμοιβαίων αξιολογήσεων «Η πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο» - Έκθεση για την Κύπρο

Διαβιβάζεται συνημμένως στις αντιπροσωπίες η αποχαρακτηρισμένη έκδοση του προαναφερόμενου εγγράφου.

Το κείμενο του παρόντος εγγράφου είναι ίδιο με αυτό της προηγούμενης έκδοσης.

Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 15 Ιουλίου 2016
(OR. en)

9892/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 67
CYBER 63

ΕΚΘΕΣΗ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Αντιπροσωπίες
Θέμα:	Έκθεση αξιολόγησης σχετικά με τον έβδομο γύρο αμοιβαίων αξιολογήσεων «Η πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο» - Έκθεση για την Κύπρο

Πίνακας περιεχομένων

1. ΠΕΡΙΛΗΨΗ 5

2. ΕΙΣΑΓΩΓΗ 10

3. ΓΕΝΙΚΑ ΘΕΜΑΤΑ ΚΑΙ ΔΟΜΕΣ 13

3.1. Εθνική στρατηγική κυβερνοασφάλειας 13

3.2. Εθνικές προτεραιότητες όσον αφορά το έγκλημα στον κυβερνοχώρο 14

3.3. Στατιστικά στοιχεία για το έγκλημα στον κυβερνοχώρο 19

3.3.1. Κύριες τάσεις του εγκλήματος στον κυβερνοχώρο 19

3.3.2. Αριθμός καταγεγραμμένων υποθέσεων εγκλήματος στον κυβερνοχώρο 20

3.4. Εθνικός προϋπολογισμός που διατίθεται για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και στήριξη από τον προϋπολογισμό της ΕΕ 21

3.5. Συμπεράσματα 22

4. ΕΘΝΙΚΕΣ ΔΟΜΕΣ 24

4.1. Δικαιοσύνη (διώξεις και δικαστήρια) 24

4.1.1. Εσωτερική δομή 24

4.1.2. Ικανότητες και εμπόδια σχετικά με την επιτυχή έρευνα 24

4.2. Αρχές επιβολής του νόμου 25

4.3. Άλλες αρχές/όργανα/συμπράξεις δημόσιου-ιδιωτικού τομέα 27

4.4. Συνεργασία και συντονισμός σε εθνικό επίπεδο 27

4.4.1. Νομικές απαιτήσεις ή απαιτήσεις πολιτικής 27

4.4.2. Πόροι που διατίθενται για τη βελτίωση της συνεργασίας 29

4.5. Συμπεράσματα 29

5. ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ 32

5.1. Ουσιαστικό ποινικό δίκαιο σχετικά με το κυβερνοέγκλημα 32

5.1.1. Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο 32

5.1.2. Περιγραφή εθνικής νομοθεσίας 32

Α/ Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών 32

Β/ Οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας 34

Γ/ Διαδικτυακή απάτη με κάρτες 37

5.2. Διαδικαστικά ζητήματα 38

5.2.1. Τεχνικές έρευνας 38

5.2.2. Εγκληματολογική εξέταση και κρυπτογράφηση 39

5.2.3. Ηλεκτρονικά αποδεικτικά στοιχεία 39

5.3. Προστασία ανθρωπίνων δικαιωμάτων/θεμελιωδών ελευθεριών 40

5.4. Δικαιοδοσία 41

5.4.1. Αρχές που διέπουν τη διερεύνηση των εγκλημάτων στον κυβερνοχώρο 41

5.4.2. Κανόνες που διέπουν τις περιπτώσεις σύγκρουσης δικαιοδοσίας και παραπομπή στην Eurojust 41

5.4.3. Δικαιοδοσία για πράξεις κυβερνοεγκλήματος που διαπράττονται στο «υπολογιστικό νέφος» 41

5.4.4. Εικόνα της Κύπρου όσον αφορά το νομικό πλαίσιο για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο 41

5.5. Συμπεράσματα 42

6. ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΠΤΥΧΕΣ 44

6.1. Κυβερνοεπιθέσεις 44

6.1.1. Φύση των κυβερνοεπιθέσεων 44

6.1.2. Μηχανισμός αντιμετώπισης κυβερνοεπιθέσεων 44

6.2. Ενέργειες κατά της παιδικής πορνογραφίας και της σεξουαλικής κακοποίησης στο Διαδίκτυο 46

6.2.1. Βάσεις δεδομένων για την ταυτοποίηση των θυμάτων και μέτρα για την αποφυγή νέας θυματοποίησης 46

6.2.2. Μέτρα για την αντιμετώπιση της σεξουαλικής εκμετάλλευσης/κακοποίησης μέσω του Διαδικτύου, της ανταλλαγής SMS σεξουαλικού περιεχομένου (sexting) και του κυβερνοεκφοβισμού 46

6.2.3. Προληπτικές ενέργειες κατά του σεξουαλικού τουρισμού, των πορνογραφικών παραστάσεων με συμμετοχή παιδιών κ.λπ. 47

6.2.4. Φορείς και μέτρα κατά ιστοτόπων που περιέχουν ή διαδίδουν παιδική πορνογραφία .. 48

6.3. Διαδικτυακή απάτη με κάρτες 50

6.3.1. Υποβολή καταγγελιών μέσω Διαδικτύου 50

6.3.2. Ρόλος του ιδιωτικού τομέα 50

6.4. Συμπεράσματα 51

7. ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ 54

7.1. Συνεργασία με οργανισμούς της ΕΕ 54

7.1.1. Επίσημες απαιτήσεις όσον αφορά τη συνεργασία με την Ευρωπόλ/EC3, την Eurojust, τον ENISA 54

7.1.2. Αξιολόγηση της συνεργασίας με την Ευρωπόλ/EC3, την Eurojust και τον ENISA 54

7.1.3. Επιχειρησιακή συμμετοχή σε κοινές ομάδες ερευνών και κυβερνοπεριπόλους 56

7.2. Συνεργασία μεταξύ των κυπριακών αρχών και της Ιντερπόλ 56

7.3. Συνεργασία με τρίτα κράτη 56

7.4. Συνεργασία με τον ιδιωτικό τομέα 57

7.5. Μέσα διεθνούς συνεργασίας 57

7.5.1. Αμοιβαία δικαστική συνδρομή 57

7.5.2. Πράξεις αμοιβαίας αναγνώρισης 59

7.5.3. Παράδοση/Έκδοση 60

7.6. Συμπεράσματα 61

8. ΚΑΤΑΡΤΙΣΗ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΠΡΟΛΗΨΗ 63

8.1. Εξειδικευμένη κατάρτιση 63

8.2. Ευαισθητοποίηση 64

8.3. Πρόληψη 68

8.3.1. Εθνική νομοθεσία/πολιτική και άλλα μέτρα 68

8.3.2. Συμπράξεις δημοσίου και ιδιωτικού τομέα (ΣΔΙΤ) 71

8.4. Συμπεράσματα 72

9. ΤΕΛΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΚΑΙ ΣΥΣΤΑΣΕΙΣ 75

9.1. Προτάσεις της Κύπρου 75

9.2. Συστάσεις 76

9.2.1. Συστάσεις προς την Κύπρο 76

9.2.2. Συστάσεις προς την Ευρωπαϊκή Ένωση, τα θεσμικά της όργανα και τα άλλα κράτη μέλη 78

Παράρτημα Α: Programme for the on-site visit 79

Παράρτημα Β: Persons interviewed/met 82

Παράρτημα Γ: List of abbreviations/glossary of terms 84

1. ΠΕΡΙΛΗΨΗ

Η επίσκεψη αξιολόγησης στην Κύπρο πραγματοποιήθηκε μεταξύ της 18ης και της 20ής Νοεμβρίου 2015. Οι κυπριακές αρχές κατέβαλαν σημαντικές προσπάθειες για τη διοργάνωση της επίσκεψης, η οποία ήταν γενικά εποικοδομητική και ενδιαφέρουσα.

Η ομάδα αξιολόγησης είχε την ευκαιρία να συνομιλήσει με αντιπροσώπους των διαφόρων αρχών που συμμετέχουν στην πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, μεταξύ των οποίων υπάλληλοι του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως, του Γραφείου του επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων, του Παιδαγωγικού Ινστιτούτου Κύπρου, της Αστυνομίας Κύπρου κ.λπ. Όλες οι αρχές με τις οποίες πραγματοποιήθηκαν συνομιλίες ήταν πρόθυμες να ανταλλάξουν απόψεις με την ομάδα αξιολόγησης με ανεπίσημο τρόπο. Όλες αυτές οι αρχές επέδειξαν υψηλό βαθμό προσήλωσης στην πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Οι Κύπριοι αντιπρόσωποι με τους οποίους πραγματοποιήθηκαν συναντήσεις ήταν καλά προετοιμασμένοι και η αποστολή ήταν καλά οργανωμένη, συμπεριλαμβανομένης της υλικοτεχνικής υποστήριξης.

Ωστόσο, μειονέκτημα της επίσκεψης αξιολόγησης ήταν ότι δεν κατέστη δυνατή η συνάντηση με τον εμπειρογνώμονα του Γραφείου του Γενικού Εισαγγελέα.

Η κυπριακή προσέγγιση όσον αφορά το έγκλημα στον κυβερνοχώρο είναι σχεδιασμένη κατά τρόπο που να επιτρέπει την ορθή λειτουργία της. Το μέγεθος της χώρας (σε επίπεδο επικράτειας και πληθυσμού) καθορίζει επίσης το μέγεθος των διαθέσιμων οικονομικών και ανθρωπίνων πόρων για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και της κυβερνοασφάλειας γενικότερα. Οι κύριοι φορείς φαίνεται να έχουν καθιερώσει μια υγιή εργασιακή ηθική και ατμόσφαιρα. Γνωρίζονται μεταξύ τους προσωπικά (γεγονός που διευκολύνει την επικοινωνία) και συνεργάζονται με ανεπίσημο τρόπο, τηρώντας ταυτόχρονα όλες τις αναγκαίες τυπικές διαδικασίες. Η προσέγγιση αυτή φαίνεται να βασίζεται αρκετά στα αποτελέσματα. Κατά τη διάρκεια της επίσκεψης αξιολόγησης δεν αναφέρθηκαν ούτε παρατηρήθηκαν συγκεκριμένα γραφειοκρατικά εμπόδια.

Η εθνική στρατηγική κυβερνοασφάλειας εγκρίθηκε από το υπουργικό συμβούλιο. Το Γραφείο του επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων είναι αρμόδιο για την παρακολούθηση και την εφαρμογή της. Η εθνική στρατηγική κυβερνοασφάλειας είναι το μέσο καθοδήγησης των προσπαθειών που καταβάλλει η Κύπρος για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η εν λόγω στρατηγική εξασφάλισε τις δομές για τη συνεργασία μεταξύ όλων των αρμόδιων αρχών, μεταξύ των οποίων δημόσιοι, ιδιωτικοί και μη κυβερνητικοί οργανισμοί ιδίως στον τομέα της ευαισθητοποίησης, στον οποίο η Κύπρος καταβάλλει σημαντικές προσπάθειες προκειμένου
να καταπολεμήσει αυτήν τη μορφή εγκλήματος. Ωστόσο, υπάρχει περιθώριο βελτίωσης όσον αφορά την ουσιαστική εφαρμογή της στρατηγικής, κυρίως σε επίπεδο ανθρωπίνων πόρων και χρηματοδότησης.

Η Κύπρος εφάρμοσε τα περισσότερα από τα ευρωπαϊκά μέσα για το έγκλημα στον κυβερνοχώρο και τα συνακόλουθα μέτρα.
Ο κύριος φορέας για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι το Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος (ΓΚΗΕ) της Αστυνομίας της Κύπρου, το οποίο είναι αρμόδιο για τη διερεύνηση υποθέσεων κυβερνοεγκλήματος, ιδίως της ηλεκτρονικής πειρατείας και της παιδικής πορνογραφίας, όπως ορίζονται στον περί της Σύμβασης κατά του εγκλήματος μέσω Διαδικτύου νόμο, Ν.22(ΙΙΙ)/2004. Το έργο του υποστηρίζεται από το δικανικό εργαστήριο ηλεκτρονικών δεδομένων (ΔΕΗΔ) της Αστυνομίας της Κύπρου, το οποίο είναι αρμόδιο για την αποτελεσματική εξέταση ηλεκτρονικών πειστηρίων. Το ΔΕΗΔ είναι επανδρωμένο με εξειδικευμένους υπαλλήλους για τη συλλογή και την δικανική ανάλυση ηλεκτρονικών συσκευών.

Η ορθή χρήση των διαθέσιμων ενωσιακών κονδυλίων για την εξασφάλιση σύγχρονου δικανικού εξοπλισμού λογισμικού και υλισμικού, τεχνικών συσκευών που χρησιμοποιούνται για την έρευνα και σύγχρονου εξοπλισμού για τους σκοπούς του ΔΕΗΔ θα πρέπει να αναφερθεί. Σύμφωνα με τους αξιολογητές, η διάθεση κατάλληλων εργαλείων πληροφορικής είναι καθοριστική για την επιτυχή διερεύνηση εγκλημάτων στον κυβερνοχώρο. Συνεπώς, κατά τους αξιολογητές η χρήση των ενωσιακών κονδυλίων έχει καθοριστική σημασία προκειμένου να μπορούν οι σχετικές αρχές να εργάζονται με τον πλέον αποτελεσματικό τρόπο και να αξιοποιούν πλήρως τις δυνατότητές τους. Ταυτόχρονα, οι κυπριακές αρχές θα πρέπει επίσης να συμβάλλουν στην παροχή επαρκούς χρηματοδότησης στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

Αναφέρθηκε η στενή συνεργασία και ο άμεσος διάλογος μεταξύ της αστυνομίας και της Εισαγγελίας. Ωστόσο, η ομάδα δεν είχε την ευκαιρία να συναντηθεί με εμπειρογνώμονα του Γραφείου του Γενικού Εισαγγελέα, γεγονός που εκλήφθηκε ως μειονέκτημα της επίσκεψης.

Η προσέγγιση της Κύπρου όσον αφορά το έγκλημα στον κυβερνοχώρο είναι πολυτομεακή. Ωστόσο, δεν έχει δημιουργηθεί ακόμη ένας συνεκτικός μηχανισμός ανταπόκρισης σε κυβερνοεπιθέσεις. Το τμήμα υπηρεσιών πληροφορικής (ΤΥΠ) ορίστηκε από την κυβέρνηση και συγκροτήθηκε υπό την εποπτεία του Γραφείου επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων (ΓΕΡΗΕΤ) ως η κυβερνητική ομάδα άμεσης ανταπόκρισης για συμβάντα που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών της Κύπρου (Cyprus GOVCIRT) (Π.Κ.Δ.358/2010). Η ανάπτυξη μιας εθνικής ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) είναι σε εξέλιξη στο πλαίσιο της εφαρμογής της εθνικής στρατηγικής κυβερνοασφάλειας. Σύμφωνα με τις κυπριακές αρχές, αναμένεται να έχει ολοκληρωθεί έως το 2017.

Η αστυνομία συνεργάζεται με ιδιωτικές εταιρίες που καταγγέλλουν κυβερνοεπιθέσεις με σκοπό τη συμβολή στην επίλυση του προβλήματος και στη διερεύνηση του αδικήματος. Οι φορείς εκμετάλλευσης κρίσιμων υποδομών στον τομέα των ηλεκτρονικών επικοινωνιών έχουν συγκεκριμένες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών, η οποία καλύπτει τη διαθεσιμότητα, τις κυβερνοεπιθέσεις, τα μέτρα πρόληψης και μετριασμού. Οι φορείς εκμετάλλευσης υπόκεινται επίσης σε υποχρεώσεις υποβολής εκθέσεων σχετικά με συμβάντα που επηρεάζουν τη διαθεσιμότητα των δικτύων και των υπηρεσιών, καθώς και παραβιάσεις δεδομένων. Η πολύπλευρη συνεργασία μεταξύ των δημόσιων αρχών και του χρηματοπιστωτικού τομέα θα μπορούσε να λειτουργήσει προς όφελος και των δύο πλευρών, αυξάνοντας σημαντικά το επίπεδο της κυβερνοασφάλειας στην Κύπρο. Επί του παρόντος, οι δημόσιες αρχές δεν συνεργάζονται απευθείας με τις τράπεζες και άλλα χρηματοπιστωτικά ιδρύματα, αλλά εξετάζεται το ενδεχόμενο δημιουργίας πλαισίου συνεργασίας.

Σύμφωνα με τα στατιστικά στοιχεία για τον αριθμό των εγκλημάτων στον κυβερνοχώρο για τα οποία έχει γίνει καταγγελία στην αστυνομία ή από την αστυνομία, η πλειονότητα των περιπτώσεων αφορά την κακοποίηση παιδιών στο Διαδίκτυο. Οι περιπτώσεις κυβερνοεπιθέσεων και απάτης με κάρτες πληρωμών για τις οποίες έχει γίνει καταγγελία είναι πολύ λιγότερες. Λαμβάνοντας αυτό υπόψη, δηλαδή τον αριθμό και το είδος των καταγγελιών σχετικά με το έγκλημα στον κυβερνοχώρο, οι αξιολογητές εκτιμούν ότι η κατάσταση στην Κύπρο δεν αντικατοπτρίζει πλήρως τις υπάρχουσες απειλές σχετικά με το έγκλημα στον κυβερνοχώρο. Επιπλέον, σύμφωνα με τους αξιολογητές, τα στατιστικά στοιχεία που είναι διαθέσιμα για το έγκλημα στον κυβερνοχώρο δεν είναι επαρκή για την εξασφάλιση συνολικής αντίληψης του φαινομένου στην Κύπρο.

Ιδιαίτερη έμφαση δίνεται στην πρόληψη και την ευαισθητοποίηση. Η Κύπρος έχει καταβάλει σημαντικές προσπάθειες και έχει επιδείξει ιδιαίτερο ενθουσιασμό σε προγράμματα διδασκαλίας και πρόληψης, τα οποία μπορούν να εκληφθούν ως παραδείγματα βέλτιστης πρακτικής. Το εγχείρημα αυτό βασίζεται στη στενή συνεργασία του δημοσίου τομέα (Υπουργείο Παιδείας και Πολιτισμού μέσω του Παιδαγωγικού Ινστιτούτου της Κύπρου) και του ιδιωτικού τομέα μέσω του οικείου κλάδου (π.χ. πάροχοι υπηρεσιών Διαδικτύου), μη κερδοσκοπικών οργανώσεων (π.χ. Ελπίδα για τα Παιδιά, CNTI), οργανωμένων ομάδων (Σχολείο για Γονείς) που συμβάλλουν με ενθουσιασμό σε προγράμματα ευαισθητοποίησης και πρόληψης.

Το 2006, το συγχρηματοδοτούμενο έργο *CyberEthics*, στο οποίο συμμετέχουν εταίροι του ιδιωτικού και του δημοσίου τομέα, εγκαινιάστηκε ως ένας κόμβος ενημέρωσης, υπεύθυνος για την ενημέρωση παιδιών, γονέων, εκπαιδευτικών και λοιπών ενδιαφερόμενων φορέων σχετικά με θέματα ασφάλειας του Διαδικτύου και για την εκπαίδευσή τους σχετικά με την ασφαλή χρήση του Διαδικτύου. Δημιουργήθηκε επίσης ένα χωριστό έργο, η γραμμή καταγγελιών για την καταγγελία παράνομου περιεχομένου στο Διαδίκτυο. Στόχος της γραμμής καταγγελιών ήταν να παρέχει τη δυνατότητα καταγγελίας παράνομου περιεχομένου στο Διαδίκτυο που αφορά εικόνες σεξουαλικής κακοποίησης παιδιών και θέματα ρατσισμού και ξενοφοβίας. Σκοπός της ήταν να μπορούν το κοινό και ιδίως οι έφηβοι και οι νέοι να διευκολύνουν τη διαδικασία δημιουργίας ασφαλέστερου διαδικτυακού περιβάλλοντος μέσω της καταγγελίας παράνομου περιεχομένου.

Το 2008 ο κόμβος ενημέρωσης και η γραμμή καταγγελιών συγχωνεύθηκαν και το 2009 το *CyberEthics* εξελίχθηκε σε Κέντρο Ασφαλούς Διαδικτύου με την ενσωμάτωση γραμμής βοήθειας. Στόχος της γραμμής βοήθειας ήταν να παρέχει στους πολίτες τα μέσα προκειμένου να λαμβάνουν υποστήριξη σε περιπτώσεις επιβλαβούς συμπεριφοράς, επικίνδυνων επαφών και βλαβερού περιεχομένου, καθώς και σε περιπτώσεις δυσάρεστων ή τρομακτικών εμπειριών στο Διαδίκτυο. Το Κέντρο προώθησε τη γραμμή βοήθειας στο κοινό προκειμένου να ενθαρρύνει τους πολίτες να χρησιμοποιούν το εργαλείο αυτό.

Το Παιδαγωγικό Ινστιτούτο της Κύπρου εισήγαγε προγράμματα για την υποστήριξη σχολείων, εκπαιδευτικών, μαθητών και γονέων με σκοπό την υλοποίηση ετήσιων σχεδίων δράσης για την ασφαλή χρήση του Διαδικτύου.
Στο πλαίσιο του προγράμματος «Ασφαλές Σχολείο για το Διαδίκτυο», εισάγονται μαθησιακά πρότυπα στις αίθουσες διδασκαλίας, καταρτίζεται εκπαιδευτικό περιεχόμενο, παρέχεται επαγγελματική εξέλιξη στους εκπαιδευτικούς και πραγματοποιούνται εργαστήρια στο πλαίσιο του σχολείου για μαθητές, γονείς και εκπαιδευτικούς όσον αφορά θέματα ασφάλειας και προστασίας στο Διαδίκτυο.

Ένα από τα πλέον ενδιαφέροντα και χρήσιμα προγράμματα που έχουν εισαχθεί στα σχολεία είναι το πρόγραμμα «Μικροί εκπαιδευτές για το Διαδίκτυο». Η βασική ιδέα είναι ότι τα παιδιά μαθαίνουν για την ασφάλεια στο Διαδίκτυο από άλλα παιδιά και όχι από ενήλικες και, με τον τρόπο αυτό, αναλαμβάνουν την ευθύνη για τη μάθησή τους, καταρτίζουν τα δικά τους σχέδια δράσης για τα σχολεία τους, συμμετέχουν σε δραστηριότητες μάθησης από συνομηλίκους και εκπαιδεύουν άλλους, συμπεριλαμβανομένων των εκπαιδευτικών και των γονέων τους. Μεταξύ των λοιπών προγραμμάτων και δραστηριοτήτων που προσφέρει το Παιδαγωγικό Ινστιτούτο της Κύπρου συγκαταλέγονται η διοργάνωση ετήσιου διαγωνισμού για την παραγωγή σύντομων βίντεο από μαθητές για θέματα ασφαλούς Διαδικτύου, η συμμετοχή στο πρόγραμμα «esafetylabel» και η διαχείριση κεντρικού φίλτρου για ασφαλές Διαδίκτυο σε όλα τα σχολεία. Ταυτόχρονα, παρέχονται στα σχολεία και άλλα προγράμματα για την καινοτόμο χρήση του Διαδικτύου στο πλαίσιο της μάθησης και της ανάπτυξης εγκάρσιων δεξιοτήτων που απαιτεί η ψηφιακή κοινωνία.

Μολονότι η Κύπρος υπογραμμίζει τη σημασία της πρόληψης και της εκπαίδευσης των παιδιών, η κατάρτιση των επαγγελματιών στον τομέα του κυβερνοεγκλήματος φαίνεται να είναι ανεπαρκής. Δεν υπάρχουν τακτικά ή εξειδικευμένα εκπαιδευτικά σεμινάρια για το έγκλημα στον κυβερνοχώρο που να απευθύνονται σε δικαστές και εισαγγελείς. Σύμφωνα με τους αξιολογητές, η κατάρτιση και η επίτευξη αριστείας έχουν καθοριστική σημασία για την αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Πιο συγκεκριμένα, τα κοινά εκπαιδευτικά σεμινάρια προσφέρουν αμοιβαία κατανόηση της ειδικής γνώσης, των νομικών απαιτήσεων και των διαφορετικών εμπειριών των κύριων φορέων που συμμετέχουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Το έγκλημα στον κυβερνοχώρο είναι ένα εξαιρετικά σύνθετο και διαρκώς εξελισσόμενο πεδίο εγκληματικότητας, το οποίο χωρίς κατάλληλη εξειδικευμένη κατάρτιση δεν είναι εύκολα κατανοητό. Επομένως, τα κοινά εκπαιδευτικά σεμινάρια για δικαστές, εισαγγελείς και αστυνομικούς θα μπορούσαν να έχουν προστιθέμενη αξία.

Η κατάσταση αυτή μπορεί να αλλάξει στο μέλλον, καθώς η Κύπρος έχει δρομολογήσει ένα έργο με τίτλο «3CE» που αποσκοπεί στη δημιουργία κέντρου αριστείας κυβερνοεγκλήματος σε εθνικό επίπεδο, στο οποίο συμμετέχουν αστυνομικοί, εισαγγελείς και δικαστές

Η Ευρωπόλ/EC3 και η Eurojust είναι γνωστές στους επαγγελματίες του χώρου και ενίοτε ζητείται η συνδρομή τους. Ωστόσο, η Ευρωπόλ χρησιμοποιείται συχνότερα.

Λαμβανομένης υπόψη της φιλόδοξης προσέγγισης όσον αφορά την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο σε σχέση με τους περιορισμένους πόρους που διατίθενται για την καταπολέμησή του, η γνώμη των αξιολογητών για την κατάσταση στην Κύπρο είναι θετική και αισιόδοξη.

2. ΕΙΣΑΓΩΓΗ

Μετά την έγκριση της κοινής δράσης 97/827/ΔΕΥ της 5ης Δεκεμβρίου 1997[1] δημιουργήθηκε μηχανισμός για την αξιολόγηση της εφαρμογής και υλοποίησης σε εθνικό επίπεδο των διεθνών επιχειρήσεων στον τομέα της καταπολέμησης του οργανωμένου εγκλήματος. Σύμφωνα με το άρθρο 2 της κοινής δράσης, η ομάδα «Γενικές υποθέσεις περιλαμβανομένης της αξιολόγησης» (GENVAL) αποφάσισε στις 3 Οκτωβρίου 2013 ότι ο έβδομος γύρος αμοιβαίων αξιολογήσεων θα πρέπει να επικεντρωθεί στην πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Η επιλογή του εγκλήματος στον κυβερνοχώρο ως αντικειμένου του έβδομου γύρου αμοιβαίων αξιολογήσεων επιδοκιμάστηκε από τα κράτη μέλη. Ωστόσο, λόγω του μεγάλου εύρους των αδικημάτων που καλύπτονται από τον όρο «έγκλημα στον κυβερνοχώρο», συμφωνήθηκε ότι η αξιολόγηση θα επικεντρωθεί στα αδικήματα στα οποία τα κράτη μέλη έκριναν ότι πρέπει να δοθεί ιδιαίτερη προσοχή.

Προς τον σκοπό αυτό, η αξιολόγηση καλύπτει τρεις συγκεκριμένους τομείς, τις κυβερνοεπιθέσεις, τη σεξουαλική κακοποίηση παιδιών/παιδική πορνογραφία στο Διαδίκτυο και τη διαδικτυακή απάτη με κάρτες, θα πρέπει δε να περιλαμβάνει συνολική εξέταση των νομικών και επιχειρησιακών πτυχών της αντιμετώπισης του εγκλήματος στον κυβερνοχώρο, της διασυνοριακής συνεργασίας και της συνεργασίας με τους αρμόδιους οργανισμούς της ΕΕ. Η οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[2] (ημερομηνία μεταφοράς στο εθνικό δίκαιο: 18 Δεκεμβρίου 2013) και η οδηγία 2013/40/ΕΕ[3] για τις επιθέσεις κατά συστημάτων πληροφοριών (ημερομηνία μεταφοράς στο εθνικό δίκαιο: 4 Σεπτεμβρίου 2015) έχουν ιδιαίτερη σημασία σε αυτό το πλαίσιο.

1 Κοινή δράση της 5ης Δεκεμβρίου 1997 (97/827/ΔΕΥ), ΕΕ L 344 της 15.12.1997, σ. 7.
2 ΕΕ L 335 της 17.12.2011, σ. 1.
3 ΕΕ L 218 της 14.8.2013, σ. 8.

Επιπλέον, τα συμπεράσματα του Συμβουλίου σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο του Ιουνίου του 2013[4] επαναλαμβάνουν τον στόχο της ταχύτερης δυνατής επικύρωσης της Σύμβασης του Συμβουλίου της Ευρώπης κατά του εγκλήματος μέσω του Διαδικτύου (Σύμβασης της Βουδαπέστης)[5] της 23ης Νοεμβρίου 2001 και υπογραμμίζουν στο προοίμιό τους ότι η «ΕΕ δεν ζητεί την κατάρτιση νέων διεθνών νομικών μέσων για θέματα που άπτονται του κυβερνοχώρου». Η εν λόγω Σύμβαση συμπληρώνεται από πρωτόκολλο για τις πράξεις ξενοφοβικού και ρατσιστικού χαρακτήρα που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών[6].

Από την πείρα των παλαιότερων αξιολογήσεων προκύπτει ότι τα κράτη μέλη θα είναι σε διαφορετικά στάδια όσον αφορά την εφαρμογή των σχετικών νομικών πράξεων, η δε τρέχουσα διαδικασία αξιολόγησης θα μπορούσε επίσης να προσφέρει χρήσιμες πληροφορίες στα κράτη μέλη που δεν έχουν ενδεχομένως εφαρμόσει όλες τις πτυχές των διάφορων πράξεων. Ωστόσο, στόχος της αξιολόγησης είναι να είναι ευρεία και διακλαδική και να μην επικεντρώνεται αποκλειστικά στην εφαρμογή των διαφόρων πράξεων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, αλλά μάλλον στις συναφείς επιχειρησιακές πτυχές στα κράτη μέλη.

Συνεπώς, πέρα από τη συνεργασία με τις εισαγγελικές υπηρεσίες, θα εκτιμηθεί επίσης πώς συνεργάζονται οι αστυνομικές αρχές με την Eurojust, τον ENISA και την Ευρωπόλ/EC3 και πώς διοχετεύεται ανατροφοδότηση από τους συγκεκριμένους φορείς στις κατάλληλες αστυνομικές και κοινωνικές υπηρεσίες. Η αξιολόγηση επικεντρώνεται στην εφαρμογή των εθνικών πολιτικών όσον αφορά την καταστολή των κυβερνοεπιθέσεων και της απάτης καθώς και της παιδικής πορνογραφίας. Η αξιολόγηση καλύπτει επίσης τις επιχειρησιακές πρακτικές των κρατών μελών σε σχέση με τη διεθνή συνεργασία και την υποστήριξη που παρέχεται στα θύματα του εγκλήματος στον κυβερνοχώρο.

Η σειρά των επισκέψεων στα κράτη μέλη αποφασίστηκε από την ομάδα GENVAL την 1η Απριλίου 2014. Η Κύπρος ήταν το δέκατο έκτο κράτος μέλος προς αξιολόγηση κατά τη διάρκεια αυτού του γύρου αξιολογήσεων. Σύμφωνα με το άρθρο 3 της κοινής δράσης, η Προεδρία κατάρτισε κατάλογο εμπειρογνωμόνων για τις αξιολογήσεις που θα πρέπει να διενεργηθούν. Τα κράτη μέλη διόρισαν εμπειρογνώμονες με σημαντικές πρακτικές γνώσεις στον τομέα, όπως ζήτησε εγγράφως από τις αντιπροσωπίες στις 28 Ιανουαρίου 2014 ο πρόεδρος της ομάδας GENVAL.

---

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS αριθ. 185, άνοιξε για υπογραφή στις 23 Νοεμβρίου 2001, τέθηκε σε ισχύ την 1η Ιουλίου 2004.

6 CETS αριθ. 189, άνοιξε για υπογραφή στις 28 Ιανουαρίου 2003, τέθηκε σε ισχύ την 1η Μαρτίου 2006.

Οι ομάδες αξιολόγησης συγκροτούνται από τρεις εθνικούς εμπειρογνώμονες, επικουρούμενους από δύο μέλη του προσωπικού της Γενικής Γραμματείας του Συμβουλίου και παρατηρητές. Για τον έβδομο γύρο των αμοιβαίων αξιολογήσεων, η ομάδα GENVAL συμφώνησε με την πρόταση της Προεδρίας να προσκληθούν ως παρατηρητές η Ευρωπαϊκή Επιτροπή, η Eurojust, ο ENISA και η Ευρωπόλ/EC3.

Οι εμπειρογνώμονες στους οποίους ανατέθηκε η διενέργεια της αξιολόγησης της Κύπρου ήταν η κα Veronika Podlahová (Τσεχική Δημοκρατία), ο κ. Renato Grgurić (Κροατία) και ο κ. Rafał Kierzynka (Πολωνία). Συμμετείχαν επίσης δύο παρατηρητές: ο κ. Dimitar Hadzhiyski (Eurojust) μαζί με τον κ. Sławomir Buczma από τη Γενική Γραμματεία του Συμβουλίου.

Η παρούσα έκθεση καταρτίστηκε από την ομάδα εμπειρογνωμόνων με τη συνδρομή της Γενικής Γραμματείας του Συμβουλίου, με βάση τα πορίσματα της επίσκεψης αξιολόγησης που πραγματοποιήθηκε στην Κύπρο μεταξύ της 18ης και της 20ής Νοεμβρίου 2015, καθώς και τις λεπτομερείς απαντήσεις της Κύπρου στο ερωτηματολόγιο αξιολόγησης και τις λεπτομερείς απαντήσεις της στις επακόλουθες ερωτήσεις.

3. ΓΕΝΙΚΑ ΘΕΜΑΤΑ ΚΑΙ ΔΟΜΕΣ

3.1. Εθνική στρατηγική κυβερνοασφάλειας

Η εθνική στρατηγική κυβερνοασφάλειας της Κυπριακής Δημοκρατίας τέθηκε σε ισχύ τον Μάρτιο του 2013. Το Γραφείο του επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων (ΓΕΡΗΕΤ) είναι αρμόδιο για την παρακολούθηση και την εφαρμογή της εν λόγω στρατηγικής.

Η εθνική στρατηγική κυβερνοασφάλειας («Στρατηγική») βασίζεται στο πρότυπο της στρατηγικής της ΕΕ. Η Στρατηγική αφορά οριζόντιες δράσεις σχετικά με τους ακόλουθους τέσσερις πυλώνες: ασφάλεια δικτύων και πληροφοριών, κυβερνοάμυνα, διπλωματία στον κυβερνοχώρο και έγκλημα στον κυβερνοχώρο. Περιλαμβάνει 17 δράσεις (τομείς εργασιών) που θα πρέπει να εφαρμοστούν από όλους τους εμπλεκόμενους φορείς, μεταξύ των οποίων η προστασία κρίσιμων υποδομών, η εκτίμηση απειλών, η ευαισθητοποίηση, η διεθνής συνεργασία και η συνεργασία με τη βιομηχανία και την πανεπιστημιακή κοινότητα. Η Στρατηγική περιγράφει τον ρόλο κάθε βασικού παράγοντα στον τομέα της κυβερνοασφάλειας.

Το Υπουργείο Μεταφορών, Επικοινωνιών και Έργων είναι επικεφαλής στον τομέα της ασφάλειας δικτύων και πληροφοριών, το Υπουργείο Άμυνας είναι επικεφαλής στα θέματα κυβερνοάμυνας και το Υπουργείο Εξωτερικών είναι αρμόδιο για θέματα που αφορούν τη διπλωματία στον κυβερνοχώρο. Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως, μαζί με την Αστυνομία Κύπρου, είναι οι αρμόδιες αρχές για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Το ΓΕΡΗΕΤ, το οποίο έχει την ευθύνη για τον συνολικό συντονισμό της εφαρμογής της Στρατηγικής, δημιούργησε μια ομάδα καθοδήγησης στο πλαίσιο της Δράσης 17 της εθνικής στρατηγικής κυβερνοασφάλειας, σύμφωνα με απόφαση του υπουργικού συμβουλίου, με συμμετέχοντες από όλα τα προαναφερόμενα υπουργεία, προκειμένου να εντοπιστούν και να γίνουν αποδεκτές αλληλεξαρτήσεις και συνέργειες κατά τη διάρκεια της εφαρμογής της εθνικής στρατηγικής κυβερνοασφάλειας.

Η Αστυνομία Κύπρου συμβάλλει επίσης στις εργασίες που εκτελούνται, μεταξύ άλλων, στο πλαίσιο της Δράσης 14 περί ευαισθητοποίησης της εθνικής στρατηγικής κυβερνοασφάλειας. Η Αστυνομία Κύπρου δημιούργησε ένα εξειδικευμένο γραφείο καταπολέμησης ηλεκτρονικού εγκλήματος (ΓΚΗΕ), εξασφαλίζοντας με αυτόν τον τρόπο την αναγκαία εμπειρογνωμοσύνη για τον χειρισμό των ιδιαιτεροτήτων των εν λόγω αδικημάτων. Η Αστυνομία Κύπρου συμμετέχει επίσης σε άλλες Δράσεις στο πλαίσιο της εθνικής στρατηγικής.

3.2. Εθνικές προτεραιότητες όσον αφορά το έγκλημα στον κυβερνοχώρο

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως και η Αστυνομία Κύπρου αναλαμβάνουν δράση σε τομείς όπως η καταγγελία εγκλημάτων και η συλλογή πληροφοριών, οι τεχνικοί πόροι, η συνεργασία με άλλες αρμόδιες αρχές (μεταξύ των οποίων ιδιωτικοί οργανισμοί), η ευαισθητοποίηση, η κατάρτιση, η νομοθεσία, η αποτελεσματική διεθνής συνεργασία και η ασφάλεια των δικτύων.

Εθνικές προτεραιότητες έχουν καταρτιστεί στους ακόλουθους τομείς:

Πρόληψη

Το ΓΚΗΕ είναι αρμόδιο για την ευαισθητοποίηση στον τομέα του εγκλήματος στον κυβερνοχώρο. Επιπλέον, ένα μέλος του ΓΚΗΕ συμμετέχει στη συμβουλευτική επιτροπή του κέντρου ασφαλούς Διαδικτύου *«Cyberethics»*, συγχρηματοδοτούμενου έργου, τον συντονισμό του οποίου έχει αναλάβει το Ινστιτούτο Νευροεπιστήμης & Τεχνολογίας Κύπρου (CNTI), ένας μη κυβερνητικός οργανισμός. Το έργο «*Cyberethics*» υλοποιείται στην Κύπρο στο πλαίσιο των προγραμμάτων Insafe και Inhope για την πρόληψη του εγκλήματος στον κυβερνοχώρο. Επιπλέον, διαθέτοντας προσωπικό με υψηλό επίπεδο κατάρτισης και εκπαίδευσης, το ΓΚΗΕ πραγματοποιεί 100 ενημερωτικές διαλέξεις ετησίως για μαθητές, εκπαιδευτικούς, γονείς και άλλες οργανωμένες ομάδες. Ταυτόχρονα, το ΓΚΗΕ διοργανώνει δημόσιες εκδηλώσεις σε κεντρικά σημεία και διανέμει φυλλάδια στα ελληνικά και τα αγγλικά με ενημερωτικό υλικό για το έγκλημα στον κυβερνοχώρο.

Το ΓΚΗΕ συνέταξε εγχειρίδιο το οποίο περιγράφει το έργο που έχει πραγματοποιηθεί στον τομέα αυτό.
Επιπλέον, το ΓΚΗΕ δημιούργησε τον Ιανουάριο του 2014 τη φόρμα καταχώρισης καταγγελιών/πληροφοριών για θέματα ηλεκτρονικού εγκλήματος[7] και την εφαρμογή της Αστυνομίας Κύπρου για φορητές συσκευές[8] που παρέχουν στο κοινό τη δυνατότητα να καταγγέλλει διαδικτυακά το έγκλημα στον κυβερνοχώρο.
Λοιποί κυβερνητικοί και μη κυβερνητικοί οργανισμοί συμμετέχουν επίσης στην πρόληψη του εγκλήματος στον κυβερνοχώρο (περισσότερες πληροφορίες στο κεφάλαιο 8.2).

Νομοθεσία

Στην Κύπρο οι κύριοι νόμοι στον τομέα του εγκλήματος στον κυβερνοχώρο είναι οι ακόλουθοι:
1. Ο νόμος που κυρώνει τη Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου (Σύμβαση της Βουδαπέστης), Ν.22(ΙΙΙ)/2004. Ο νόμος αυτός καλύπτει την ηλεκτρονική πειρατεία, την παιδική πορνογραφία και την απάτη που διαπράττεται μέσω ηλεκτρονικών επικοινωνιών και του Διαδικτύου.
2. Ο νόμος που αναθεωρεί το νομικό πλαίσιο που διέπει την πρόληψη και καταπολέμηση της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας, Ν.91(Ι)/2014. Ο νόμος αυτός κυρώνει την οδηγία της ΕΕ 2011/93/ΕΕ και καλύπτει την παιδική πορνογραφία και την άγρα παιδιών μέσω Διαδικτύου, καθώς και την ειδοποίηση και αφαίρεση περιεχομένου.
3. Ο περί του πρόσθετου πρωτοκόλλου στη Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου, αναφορικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών κυρωτικός νόμος, Ν.26(ΙΙΙ)/2004. Ο νόμος αυτός καλύπτει πράξεις ρατσιστικού και ξενοφοβικού χαρακτήρα που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών και του Διαδικτύου.
4. Ο περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα νόμος, Ν.138(Ι)/2001.
5. Ο περί διατήρησης τηλεπικοινωνιακών δεδομένων με σκοπό τη διερεύνηση σοβαρών ποινικών αδικημάτων νόμος, Ν.183(Ι)/2007. Ο νόμος αυτός μετέφερε την οδηγία 2006/24/ΕΥ στο εθνικό δίκαιο. Μολονότι η οδηγία ακυρώθηκε από το Δικαστήριο της ΕΕ, ο εθνικός νόμος παραμένει σε ισχύ. Ο εθνικός νόμος βασίζεται σε συνταγματική διάταξη και περιλαμβάνει ειδικές διασφαλίσεις για την προστασία της ιδιωτικής ζωής. Για παράδειγμα, τα δεδομένα επικοινωνίας κοινοποιούνται μόνον κατόπιν διατάγματος δικαστηρίου. Πρόσφατα υποβλήθηκε υπόθεση στο Ανώτατο Δικαστήριο σχετικά με τον αντίκτυπο της ακύρωσης της οδηγίας της ΕΕ στον Νόμο 183(Ι)/2007 και το Ανώτατο Δικαστήριο αποφάνθηκε ότι ο εν λόγω νόμος ήταν σύμφωνος με την Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων.
6. Ο περί ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομικών υπηρεσιών νόμος, Ν.112(Ι)/2004.
7. Ο νόμος που εφαρμόζει την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών, Ν.147(Ι)/2015.

[7] https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm
[8] http://mobile.cypruspolicenews.com/landing/Desktop#.VbclTfmm2jw

Ανάπτυξη ικανοτήτων

Το ΓΚΗΕ και το δικανικό εργαστήριο ηλεκτρονικών δεδομένων (ΔΕΗΔ) βρίσκονται στο Αρχηγείο της Αστυνομίας Κύπρου στη Λευκωσία και απαρτίζονται από 5 και 10 εξειδικευμένους και καταρτισμένους αστυνομικούς αντιστοίχως. Ο αρχηγός και οι βοηθοί του είναι υπεύθυνοι και για τις δύο υπηρεσίες. Τρία μέλη του ΔΕΗΔ έχουν μεταπτυχιακό τίτλο σπουδών στη δικανική πληροφορική και είναι εκπαιδευτές στη δικανική εξέταση ψηφιακών πειστηρίων. Στο πλαίσιο χρηματοδοτικών προγραμμάτων, όπως το Hercule II και το Ταμείο Εσωτερικής Ασφάλειας 2014-2020, το ΓΚΗΕ και το ΔΕΗΔ έλαβαν χρηματοδότηση με σκοπό την ανανέωση κάθε απαραίτητου υλισμικού και λογισμικού που χρησιμοποιείται για τη δικανική έρευνα. Επιπλέον, μέσω δευτερεύουσας χρηματοδότησης, θα δημιουργηθεί εξειδικευμένη αίθουσα εκπαίδευσης το 2016. Το έργο Hercules II ολοκληρώθηκε στις 30/6/2015, ενώ το δεύτερο έργο στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας θα ολοκληρωθεί σε διαφορετικές φάσεις έως το 2020. Συνολικά, όσον αφορά την ανάπτυξη ικανοτήτων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, οι δύο υπηρεσίες έχουν πολύ καλό επίπεδο.

Κατάρτιση

Το προσωπικό του ΓΚΗΕ και του ΔΕΗΔ συμμετέχει σε ειδικά εκπαιδευτικά προγράμματα σε ετήσια βάση. Τα περισσότερα από τα προγράμματα αυτά παρέχονται από την Ευρωπαϊκή Αστυνομική Ακαδημία (ΕΑΑ), την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF), την Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος (ECTEG), το FBI και άλλους οργανισμούς. Ταυτόχρονα, τα μέλη του ΓΚΗΕ διοργάνωσαν προγράμματα κατάρτισης για αστυνομικούς που διενεργούν επιτόπιες έρευνες στην Κύπρο, σε συνεργασία με την Αστυνομική Ακαδημία Κύπρου.

Το 2014 το ΓΚΗΕ παρείχε εκπαιδευτικά σεμινάρια σε αστυνομικούς της Παλαιστινιακής Αρχής, καθώς και σε άλλες κυβερνητικές υπηρεσίες της Κύπρου.

Επιπλέον, στο πλαίσιο του προγράμματος «Πρόληψη και καταπολέμηση του εγκλήματος» της Ευρωπαϊκής Ένωσης (ISEC), η Κύπρος έλαβε χρηματοδότηση για τη σύσταση του Κυπριακού Κέντρου Αριστείας Κυβερνοεγκλήματος (3CE). Η δράση αυτή συντονίζεται από το Ινστιτούτο Νευροεπιστήμης & Τεχνολογίας Κύπρου, έναν μη κυβερνητικό οργανισμό, με εταίρους το Γραφείο του επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων, το Ευρωπαϊκό Πανεπιστήμιο Κύπρου, την εταιρεία Aditess LTD και το ΓΚΗΕ.

Στο πλαίσιο του έργου 3CE θα αναπτυχθούν βραχυπρόθεσμα, ιδιαίτερα στοχευμένα και εξειδικευμένα εκπαιδευτικά σεμινάρια σχετικά με θέματα που αφορούν το έγκλημα στον κυβερνοχώρο για συμμετέχοντες από τον δημόσιο και ιδιωτικό τομέα. Τα μαθήματα θα διευκολύνουν την ανταλλαγή και διάδοση σιωπηρής γνώσης και εμπειρογνωμοσύνης, θα συμβάλουν στην εξοικείωση των συμμετεχόντων με νέες τεχνολογίες και εργαλεία και θα βελτιώσουν τις καθημερινές δραστηριότητές τους σχετικά με την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Τα μαθήματα θα προσφέρονται σε εισαγγελείς και δικαστές, αστυνομικούς, φοιτητές και δημόσιους υπαλλήλους.

Ευαισθητοποίηση του κοινού

Το ΓΚΗΕ συνεργάζεται στενά με άλλες κυβερνητικές υπηρεσίες, ΜΚΟ και τον ιδιωτικό τομέα όσον αφορά την πρόληψη του εγκλήματος στον κυβερνοχώρο. Ένα μέλος του ΓΚΗΕ και ένας εκπρόσωπος του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως συμμετέχουν επίσης στη Συμβουλευτική Επιτροπή του έργου *CyberEthics*. Επιπλέον, τα μέλη του ΓΚΗΕ δίνουν διαλέξεις σε ετήσια βάση σε μαθητές και εκπαιδευτικούς, καθώς και σε άλλες οργανωμένες ομάδες, σχετικά με την ασφαλή χρήση του Διαδικτύου. Για παράδειγμα, κάθε χρόνο το ΓΚΗΕ συμμετέχει στις εκδηλώσεις που διοργανώνονται για την ημέρα ασφαλούς Διαδικτύου. Επιπρόσθετα, σε συνεργασία με τους λοιπούς εταίρους του έργου *CyberEthics*, το ΓΚΗΕ διοργάνωσε εκδηλώσεις για το κοινό με στόχο την ευαισθητοποίηση όσον αφορά την ασφάλεια στο Διαδίκτυο. Το ΓΚΗΕ συνεργάζεται στενά με παρόχους υπηρεσιών διαδικτύου, το Παιδαγωγικό Ινστιτούτο (Υπουργείο Παιδείας και Πολιτισμού) και το Γραφείο του επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων (ΓΕΡΗΕΤ).

Στο πλαίσιο της πολιτικής πρόληψης, το ΓΚΗΕ εκδίδει και διανέμει φυλλάδια για την ασφάλεια στο Διαδίκτυο, στα ελληνικά και τα αγγλικά, σε όλους τους μαθητές της πέμπτης δημοτικού της Κύπρου (5.000 φυλλάδια). Άλλοι οργανισμοί που ασχολούνται με την ασφάλεια στο Διαδίκτυο, όπως το Παιδαγωγικό Ινστιτούτο, το ΓΕΡΗΕΤ, το CNTI, το *CyberEthics* και διάφοροι πάροχοι υπηρεσιών Διαδικτύου, έχουν εκδώσει το δικό τους εκπαιδευτικό υλικό. Επιπλέον, σε συνεργασία με το Γραφείο Τύπου της Αστυνομίας Κύπρου, το ΓΚΗΕ ετοίμασε ένα σύντομο βίντεο σχετικά με τον κυβερνοεκφοβισμό, το οποίο είναι προσβάσιμο μέσω του Διαδικτύου και παρουσιάζεται συχνά στην τηλεόραση.

Επιπρόσθετα, σε συνεργασία με το Γραφείο Τύπου της Αστυνομίας Κύπρου και το τμήμα μελετών και ανάπτυξης της Αστυνομίας Κύπρου, το ΓΚΗΕ εγκαινίασε τον Ιανουάριο του 2015 τη φόρμα καταχώρισης καταγγελιών/πληροφοριών για θέματα ηλεκτρονικού εγκλήματος, η οποία είναι προσβάσιμη μέσω του ιστοτόπου *www.police.gov.cy*. Την ίδια περίοδο, το Γραφείο Τύπου της Αστυνομίας Κύπρου εγκαινίασε την εφαρμογή της Αστυνομίας Κύπρου για φορητές συσκευές, η οποία προσφέρει χρήσιμες πληροφορίες και σύνδεση με τη φόρμα καταχώρισης καταγγελιών/πληροφοριών για θέματα ηλεκτρονικού εγκλήματος.

Ευαισθητοποίηση

Από την έγκριση της εθνικής στρατηγικής κυβερνοασφάλειας και έπειτα, η ευαισθητοποίηση αποτελεί οριζόντιο θέμα υπό τον συντονισμό του ΓΕΡΗΕΤ. Στο πλαίσιο της Δράσης 14, διάφορες υποομάδες εργασίας εστιάζουν τις προσπάθειές τους σε συγκεκριμένες ομάδες. Εν προκειμένω, το Υπουργείο Παιδείας και Πολιτισμού έχει ηγετικό ρόλο στη χάραξη και υλοποίηση της εθνικής στρατηγικής για την ασφάλεια παιδιών/ μαθητών, εκπαιδευτικών και γονέων στο Διαδίκτυο.

Διεθνής συνεργασία

Η Κύπρος συνεργάζεται με τα κράτη μέλη της ΕΕ και τρίτες χώρες βάσει διμερών και πολυμερών συμφωνιών στον εν λόγω τομέα και με άλλους διαύλους ανταλλαγής πληροφοριών. Το ΓΚΗΕ συνεργάζεται στενά με τους ακόλουθους οργανισμούς:

- Ευρωπόλ/EC3/AWF/ EMPACTS
- EUCTF (Ομάδα δράσης της Ευρωπαϊκής Ένωσης για εγκλήματα στον κυβερνοχώρο)
- CIRCAMP (Σχέδιο συνολικού επιχειρησιακού στρατηγικού σχεδιασμού της αστυνομίας «COSPOL» κατά της κυκλοφορίας μέσω του Διαδικτύου υλικού κακοποίησης παιδιών)
- ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών)
- ECTEG (Ευρωπαϊκή ομάδα για την εκπαίδευση και κατάρτιση στον τομέα του κυβερνοεγκλήματος)
- EAA (Ευρωπαϊκή Αστυνομική Ακαδημία)
- EUROJUST (Ευρωπαϊκή Μονάδα Δικαστικής Συνεργασίας)

- CERT-EU (Ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική της ΕΕ)
- INTERPOL (Διεθνής Οργανισμός Εγκληματολογικής Αστυνομίας)
- Ευρωπαϊκή Επιτροπή
- ΕΥΕΔ (Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης)
- Ομοσπονδιακό Γραφείο Ερευνών (FBI) ΗΠΑ
- VCACITF (Διεθνής Ομάδα για την καταπολέμηση βίαιων εγκλημάτων σε βάρος παιδιών) του FBI ΗΠΑ.
- Συμβούλιο της Ευρώπης (Αξιολόγηση της επιτροπής για το έγκλημα στον κυβερνοχώρο)

3.3. Στατιστικά στοιχεία για το έγκλημα στον κυβερνοχώρο

3.3.1. Κύριες τάσεις του εγκλήματος στον κυβερνοχώρο

Δεν υπάρχει ενιαία στατιστική έκθεση σχετικά με το έγκλημα στον κυβερνοχώρο και αυτό οφείλεται στο γεγονός ότι διάφορες υπηρεσίες της αστυνομίας ασχολούνται με το έγκλημα στον κυβερνοχώρο ή άλλα αδικήματα μέσω Διαδικτύου. Σύμφωνα με την αστυνομική διάταξη 3/45, το ΓΚΗΕ ασχολείται με περιπτώσεις ηλεκτρονικής πειρατείας, ρατσιστικής συμπεριφοράς και παιδικής πορνογραφίας μέσω του Διαδικτύου. Υποθέσεις απάτης και άλλα συναφή οικονομικά εγκλήματα που διαπράττονται μέσω του Διαδικτύου διερευνώνται από τα επαρχιακά τμήματα ανίχνευσης εγκλημάτων, το γραφείο διερεύνησης οικονομικού εγκλήματος και τους αστυνομικούς σταθμούς επαρχιών ανάλογα με τις οικονομικές απώλειες των θυμάτων.

Το ΓΚΗΕ διατηρεί αριθμητικά στατιστικά στοιχεία σχετικά με περιπτώσεις ηλεκτρονικής πειρατείας και πλήρη στατιστικά στοιχεία σχετικά με περιπτώσεις παιδικής πορνογραφίας. Σύμφωνα με τα στατιστικά στοιχεία που διατηρεί το ΓΚΗΕ, οι κύριες τάσεις του εγκλήματος στον κυβερνοχώρο στην Κύπρο είναι οι ακόλουθες:

- Παιδική πορνογραφία – κατοχή και πρόσκληση παιδιών προκειμένου να συμμετέχουν σε παιδική πορνογραφία
- Λογισμικό «Ransomware» (κρυπτοϊός) της αστυνομίας
- Επιθέσεις κατανεμημένης άρνησης υπηρεσίας
- Επιθέσεις «Man in the Middle» – μορφές απάτης μέσω ηλεκτρονικού ταχυδρομείου
- Ιστότοποι «ηλεκτρονικού ψαρέματος».

3.3.2. Αριθμός καταγεγραμμένων υποθέσεων εγκλήματος στον κυβερνοχώρο

Το ΓΚΗΕ είναι ο μοναδικός οργανισμός που είναι υπεύθυνος για τη διερεύνηση υποθέσεων που αφορούν ηλεκτρονική πειρατεία και παιδική πορνογραφία μέσω Διαδικτύου. Το «*CyberEthics*», το οποίο λειτουργεί στο πλαίσιο των προγραμμάτων «Insafe» και «Inhope», χειρίζεται τη φόρμα καταχώρισης καταγγελιών/πληροφοριών για διαδικτυακά αδικήματα (*www.cyberethics.info*). Με τον τρόπο αυτόν, οι εταίροι του «*CyberEthics*» (κρατικοί και μη κρατικοί φορείς) τηρούν τα δικά τους στατιστικά στοιχεία σχετικά με τα καταγγελλόμενα περιστατικά και, συγχρόνως, τα εν λόγω στοιχεία διαβιβάζονται στο ΓΚΗΕ. Το ΓΚΗΕ τηρεί αριθμητικά στατιστικά στοιχεία για όλα τα αδικήματα που έχουν ερευνηθεί και πλήρη στατιστικά στοιχεία για τα αδικήματα σχετικά με την παιδική πορνογραφία.

Στατιστικά στοιχεία για τα αδικήματα σχετικά με την παιδική πορνογραφία

Κατηγορία	2014	2015
Πρόσκληση για συμμετοχή σε παιδική πορνογραφία	19	13
Έρευνες σχετικά με την κατοχή υλικού παιδικής πορνογραφίας	87	103
Συνολικός αριθμός ερευνών	106	116
Έχουν διαβιβαστεί στις αρμόδιες αρχές	14	1
Ενδείξεις που οδήγησαν σε ποινική έρευνα	20	3
Υποθέσεις που παραπέμφθηκαν στα δικαστήρια	19	1
Έχουν ανασταλεί/αποσυρθεί	18	68
Εκκρεμούν ενώπιον των δικαστηρίων	18	1
Καταδίκες	1	1
Αθωώσεις		
Υπό έρευνα	38	44

Στατιστικά στοιχεία σχετικά με υποθέσεις ηλεκτρονικής πειρατείας/παράνομης πρόσβασης/παράνομης παρέμβασης

Αδίκημα	2014	2015
Παράνομη πρόσβαση/παρέμβαση	14	22
Πλαστογραφία σχετιζόμενη με ηλεκτρονικό υπολογιστή	81	22

3.4. Εθνικός προϋπολογισμός που διατίθεται για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και στήριξη από τον προϋπολογισμό της ΕΕ

Ο εθνικός προϋπολογισμός προβλέπει ειδικά κονδύλια για την ευαισθητοποίηση του κοινού σχετικά με το κυβερνοέγκλημα.
Συγχρόνως, το ΓΚΗΕ έχει λάβει ευρωπαϊκή χρηματοδότηση (Ταμείο Εσωτερικής Ασφάλειας) για την αγορά ειδικού εξοπλισμού, ώστε να ενισχύσει τις επιχειρησιακές του δυνατότητες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και να βελτιώσει τη διαδικασία ανταλλαγής πληροφοριών μεταξύ όλων των σχετικών υπεύθυνων αρχών. Περαιτέρω, μέσω ευρωπαϊκής χρηματοδότησης, θα αναπτυχθούν προγράμματα κατάρτισης, ώστε να ενισχυθούν οι επιχειρησιακές ικανότητες για όλους τους υπαλλήλους που είναι υπεύθυνοι για την έρευνα και τη δίωξη των δραστών εγκλημάτων στον κυβερνοχώρο.

Ειδικό προϋπολογισμό για την υλοποίηση δράσεων στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας διαθέτει και το Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ).

3.5. Συμπεράσματα

- Η Κύπρος κατήρτισε Εθνική Στρατηγική Κυβερνοασφάλειας το 2013. Το σχετικό έγγραφο εγκρίθηκε από το Υπουργικό Συμβούλιο. Το Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων συστάθηκε ως αρμόδιο όργανο για να συντονίσει την υλοποίησή της. Στο πλαίσιο της Στρατηγικής, συστάθηκε επίσης η συντονιστική επιτροπή κυβερνοασφάλειας, η οποία θεωρείται βασικός παράγων για τον συντονισμό, αν και αποστολή της είναι περισσότερο η υλοποίηση της Στρατηγικής παρά η ίδια η κυβερνοασφάλεια.
  Η Στρατηγική καλύπτει όλους τους τομείς του εγκλήματος στον κυβερνοχώρο και περιλαμβάνει 4 βασικούς πυλώνες, δηλαδή την ασφάλεια δικτύων και πληροφοριών, το κυβερνοέγκλημα, τη διπλωματία στον κυβερνοχώρο και την κυβερνοάμυνα.

- Το έγγραφο αποτελεί μία από τις βάσεις των δημόσιων και των μη κυβερνητικών δραστηριοτήτων στον τομέα αυτόν, με αποτέλεσμα τη δημιουργία ενός περίπλοκου και πολύπλευρου συστήματος αποτελούμενου από διάφορους δημόσιους και ιδιωτικούς οργανισμούς, οι οποίοι είναι υπεύθυνοι για την υλοποίηση της Στρατηγικής και για την ταχεία ανταπόκριση σε διάφορες απειλές στον κυβερνοχώρο. Ως εκ τούτου, θεωρείται ότι παρέχει την ευκαιρία δημιουργίας συνεργειών και μεγιστοποίησης της ετοιμότητας, καθώς και των ικανοτήτων αντίδρασης. Σε συνδυασμό με το νομοθετικό πλαίσιο, η υλοποίηση της Στρατηγικής αποτελεί βασικό παράγοντα για την περαιτέρω ανάπτυξη της συνεργασίας και την ανάπτυξη ικανοτήτων στην καταπολέμηση του κυβερνοεγκλήματος και την ενίσχυση της κυβερνοασφάλειας.

- Εντούτοις, θα πρέπει να σημειωθεί ότι η ορθή υλοποίηση της Στρατηγικής συνεπάγεται τη διασφάλιση επαρκών ανθρώπινων και οικονομικών πόρων, πράγμα που, κατά την εκτίμηση των αξιολογητών, δεν φαίνεται να συμβαίνει. Πέρα από το μέγεθος του προσωπικού, η ποιότητα των δημόσιων εγκαταστάσεων που επηρεάζει τις συνθήκες εργασίας και τις δαπάνες δεν δημιουργεί περιβάλλον που μπορεί να θεωρηθεί ότι συμβάλλει στην περαιτέρω ανάπτυξη της δραστηριότητας για την καταπολέμηση του κυβερνοεγκλήματος.[9]

[9] Μετά την επιτόπια επίσκεψη, η ομάδα αξιολόγησης ενημερώθηκε ότι η Κυπριακή Δημοκρατία υπέκειτο μέχρι πολύ πρόσφατα (Μάρτιος 2016) σε πρόγραμμα χρηματοδοτικής συνδρομής με την ΕΕ. Οι προσλήψεις αστυνομικών πάγωσαν μετά το 2012. Πρόσφατα, το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως της Κύπρου και η Αστυνομία Κύπρου ανέθεσαν τη διεξαγωγή μελέτης για την αναδιάρθρωση της Αστυνομίας Κύπρου και οι ανάγκες σε προσωπικό θα εκτιμηθούν εκ νέου στο συγκεκριμένο πλαίσιο.

- Από την άλλη πλευρά, θα πρέπει να υπογραμμιστεί ότι οι κυπριακές αρχές έχουν σημειώσει αξιοσημείωτη πρόοδο στη χρήση των ευρωπαϊκών κονδυλίων για τον εξοπλισμό των υπηρεσιών επιβολής του νόμου με σύγχρονες συσκευές και υλισμικό, που είναι απαραίτητα στον τομέα της καταπολέμησης του κυβερνοεγκλήματος. Θα πρέπει να δοθεί ιδιαίτερη προσοχή σε ό,τι αφορά το ΔΕΗΔ, το οποίο είναι σωστά και καλά εξοπλισμένο με εργαλεία της τεχνολογίας των πληροφοριών, παρά τις πολύ ταπεινές συνθήκες εργασίας που οφείλονται στις χαμηλής ποιότητας εγκαταστάσεις.

- Κατά τη γνώμη των αξιολογητών, θα μπορούσε να θεωρηθεί παράδειγμα καλής πρακτικής η αποτελεσματική χρήση των ευρωπαϊκών κονδυλίων για τον εξοπλισμό των αρχών επιβολής του νόμου με εργαλεία της τεχνολογίας των πληροφοριών, συμπεριλαμβανομένων υλισμικού και λογισμικού δικανικών ερευνών.

- Η ομάδα των αξιολογητών ενημερώθηκε ότι οι στατιστικές για το κυβερνοέγκλημα τηρούνται από διαφορετικά θεσμικά όργανα και τμήματα που συμμετέχουν στην πρόληψη, την ανίχνευση, την έρευνα και τη δίωξη. Εντούτοις, δεν έχει αναπτυχθεί ολοκληρωμένη στατιστική προσέγγιση, ούτε αξιόπιστες και εξαντλητικές στατιστικές όσον αφορά τους καταδικασθέντες για διαφορετικά είδη κυβερνοεγκλημάτων. Ως εκ τούτου, θα πρέπει να υπάρξει γενική ενοποίηση των στοιχείων που αφορούν το κυβερνοέγκλημα και αυτά να μετατραπούν ταχέως σε στατιστικές πληροφορίες, οι οποίες θα πρέπει να είναι διαθέσιμες σε όλους τους φορείς που συμμετέχουν στην κυβερνοασφάλεια.

- Παρότι δόθηκαν στην ομάδα των αξιολογητών ορισμένα στατιστικά στοιχεία σχετικά με το κυβερνοέγκλημα, κατά τη γνώμη των αξιολογητών τα στοιχεία αυτά δεν επαρκούν για να σχηματιστεί συνολική αντίληψη του συγκεκριμένου φαινομένου στην Κύπρο. Αν και η συλλογή και η επεξεργασία τους μπορούν να θεωρηθούν χρονοβόρες και περίπλοκες για τις δημόσιες αρχές, τα στατιστικά στοιχεία εξυπηρετούν στην κατανόηση της ανάπτυξης του κυβερνοεγκλήματος στην Κύπρο και στην αποτελεσματικότητα των ενεργειών που πραγματοποιούνται για την καταπολέμησή του. Ακόμη, οι στατιστικές θα πρέπει να καλύπτουν όλα τα πεδία που θεωρούνται σημαντικά για αυτό το είδος εγκλήματος.[10]

[10] Οι αρχές στην Κύπρο ανάφεραν ότι έχουν επίγνωση αυτού του ζητήματος και ότι το ΓΕΡΗΕΤ και το ΓΚΗΕ βρίσκονται σε επαφή με τον ιδιωτικό τομέα για τη διερεύνηση πιθανών τρόπων συλλογής περισσότερων πληροφοριών.

4. ΕΘΝΙΚΕΣ ΔΟΜΕΣ

4.1. Δικαιοσύνη (διώξεις και δικαστήρια)

4.1.1. Εσωτερική δομή

Τα κυβερνοεγκλήματα δικάζονται από τα επαρχιακά δικαστήρια ή τα κακουργιοδικεία, ανάλογα με τη σοβαρότητα της υπόθεσης. Δεν υπάρχουν ειδικά δικαστήρια ή εισαγγελικές υπηρεσίες για τα κυβερνοεγκλήματα.

Η αρχή της διάκρισης των εξουσιών εφαρμόζεται στην Κύπρο και η Δικαιοσύνη είναι ανεξάρτητη λειτουργία. Η Κατηγορούσα Αρχή τελεί υπό τη διεύθυνση της Γενικής Εισαγγελίας.

Δεν κατέστη δυνατό να δοθούν περαιτέρω λεπτομέρειες σχετικά με τη δομή της Δικαιοσύνης, επειδή απουσίαζε ο εμπειρογνώμων του γραφείου του Γενικού Εισαγγελέα, ο οποίος, σύμφωνα με το πρόγραμμα της επίσκεψης, προβλεπόταν να παρουσιάσει το θέμα και να απαντήσει στις σχετικές ερωτήσεις των ειδικών.

4.1.2. Ικανότητες και εμπόδια σχετικά με την επιτυχή έρευνα

Στο πλαίσιο του προγράμματος «Πρόληψη και καταπολέμηση της εγκληματικότητας» της Ευρωπαϊκής Ένωσης (ISEC), η Κύπρος έλαβε χρηματοδότηση για τη σύσταση του Κυπριακού Κέντρου Αριστείας Κυβερνοεγκλήματος (3CE). Το 3CE θα παρέχει βραχυπρόθεσμα, ιδιαίτερα στοχευμένα και εξειδικευμένα εκπαιδευτικά σεμινάρια σχετικά με θέματα που αφορούν το έγκλημα στον κυβερνοχώρο για συμμετέχοντες από τον δημόσιο και ιδιωτικό τομέα. Θα αναπτυχθούν ενότητες ειδικά για δικαστές, εισαγγελείς και υπαλλήλους επιβολής του νόμου.

Περαιτέρω, οι κυπριακές αρχές θεωρούν ότι, σε πολλές υποθέσεις, η διεθνής συνεργασία και η συμβολή εξειδικευμένων οργανισμών, όπως η Ευρωπόλ, είναι πολύ σημαντικές για την επιτυχή διερεύνηση.

Από την άλλη πλευρά, η κρυπτογράφηση, το περιορισμένο χρονικό διάστημα για τη διατήρηση δεδομένων (6 μήνες) και η απουσία νομικού πλαισίου για την πραγματοποίηση ηλεκτρονικής επιτήρησης ιδιωτικών επικοινωνιών, η έλλειψη συνεργασίας με ξένους εταίρους και το μεγάλο χρονικό διάστημα που απαιτείται για τη λήψη αποδεικτικών στοιχείων από ξένες δικαιοδοσίες αναφέρθηκαν ως τα κύρια εμπόδια κατά το στάδιο της έρευνας του κυβερνοεγκλήματος. Ωστόσο, προβλήματα όπως η διατήρηση και η κρυπτογράφηση δεδομένων φαίνεται ότι είναι γενικότερα και αναφέρονται και από άλλα κράτη μέλη.

Επί του παρόντος εξετάζονται ενδεχόμενες λύσεις για τα προβλήματα αυτά από το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως και την Αστυνομία, που εκπονούν επίσης το αναγκαίο νομικό πλαίσιο για την πραγματοποίηση ηλεκτρονικής επιτήρησης ιδιωτικών επικοινωνιών για περιορισμένο αριθμό σοβαρών αδικημάτων και/ή για λόγους εθνικής ασφάλειας.

Θα εξεταστεί επίσης περαιτέρω η παράταση της περιόδου διατήρησης των δεδομένων, μετά από την ανάλυση των επιπτώσεων που θα έχει η απόφαση του Ανωτάτου Δικαστηρίου σχετικά με τον νόμο Ν.183(Ι)/2007.
Επιπροσθέτως, δεδομένου ότι τα περισσότερα κυβερνοεγκλήματα είναι διακρατικά, υπάρχουν καθυστερήσεις στην υλοποίηση της αμοιβαίας δικαστικής συνδρομής με διαφορετικές χώρες σε ολόκληρο τον κόσμο. Αυτό αποτελεί επίσης εμπόδιο για την αποτελεσματική έρευνα.

4.2. Αρχές επιβολής του νόμου

Το ΓΚΗΕ και το ΔΕΗΔ αποτελούν τις κυπριακές υπηρεσίες που είναι ικανές και υπεύθυνες για την αποτελεσματική έρευνα του κυβερνοεγκλήματος. Και οι δύο υπηρεσίες βρίσκονται στο Αρχηγείο της Αστυνομίας Κύπρου και τελούν υπό την επίβλεψη του ίδιου διευθυντή.

Το Γραφείο καταπολέμησης ηλεκτρονικού εγκλήματος (ΓΚΗΕ)
Το Γραφείο καταπολέμησης ηλεκτρονικού εγκλήματος της Αστυνομίας Κύπρου είναι ο εξειδικευμένος οργανισμός για τη διερεύνηση των κυβερνοεγκλημάτων. Το Γραφείο συστάθηκε τον Σεπτέμβριο του 2007 βάσει της αστυνομικής διάταξης αριθ. 3/45, προκειμένου να εφαρμόσει τον νόμο περί της σύμβασης κατά του εγκλήματος μέσω του Διαδικτύου (κυρωτικός νόμος) Ν. 22(ΙΙΙ)/2004. Ο νόμος αυτός καλύπτει την ηλεκτρονική πειρατεία, την παιδική πορνογραφία και την απάτη που διαπράττεται μέσω ηλεκτρονικών επικοινωνιών και του Διαδικτύου. Σύμφωνα με την αστυνομική διάταξη αριθ. 3/45, το Γραφείο είναι υπεύθυνο για τη διερεύνηση εγκλημάτων που διαπράττονται μέσω Διαδικτύου ή μέσω ηλεκτρονικών υπολογιστών και, συγχρόνως, είναι υπεύθυνο για τη διερεύνηση όλων των αδικημάτων που παραβιάζουν τους κανόνες του νόμου Ν.22(ΙΙΙ)/2004.

Είναι επίσης υπεύθυνο για την ευαισθητοποίηση σχετικά με το κυβερνοέγκλημα. Ένα μέλος του ΓΚΗΕ συμμετέχει επίσης στη Συμβουλευτική Επιτροπή της κοινοπραξίας «*CyberEthics*», έργου που λειτουργεί στο πλαίσιο των προγραμμάτων «Insafe» και «Inhope» στην Κύπρο για την πρόληψη του κυβερνοεγκλήματος. Περαιτέρω, το Γραφείο έχει εκπαιδευμένο προσωπικό, τα μέλη του οποίου δίνουν 100 διαλέξεις περίπου ανά έτος σε σχολεία και άλλες οργανωμένες ομάδες. Συγχρόνως, το Γραφείο διοργανώνει δημόσιες εκδηλώσεις σε κεντρικά σημεία και διανέμει φυλλάδια στα ελληνικά και τα αγγλικά για την ευαισθητοποίηση σχετικά με το έγκλημα στον κυβερνοχώρο. Ακόμη, το ΓΚΗΕ συμμετέχει στη Δράση 14 της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, η οποία περιλαμβάνει και την ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια, συμπεριλαμβανομένου του κυβερνοεγκλήματος.

Το Δικανικό Εργαστήριο Ηλεκτρονικών Δεδομένων (ΔΕΗΔ)
Το ΔΕΗΔ συστάθηκε το 2009 και είναι υπεύθυνο για την αποτελεσματική εξέταση των ηλεκτρονικών αποδεικτικών στοιχείων. Το ΔΕΗΔ είναι επανδρωμένο με εξειδικευμένους υπαλλήλους για τη συλλογή και την δικανική ανάλυση ηλεκτρονικών συσκευών. Όλα τα στελέχη του ΔΕΗΔ είναι απόφοιτοι πανεπιστημίου σε ακαδημαϊκά πεδία σχετικά με το αντικείμενό τους. Ορισμένα στελέχη έχουν επίσης μεταπτυχιακό τίτλο σπουδών στη δικανική εξέταση ηλεκτρονικών αποδεικτικών στοιχείων, ενώ κάποιοι εξ αυτών έχουν τον τίτλο του εκπαιδευτή. Αποστολή τους είναι η συλλογή και η δικανική ανάλυση ψηφιακών συσκευών, καθώς και η παρουσίαση επιστημονικών στοιχείων υπό την ιδιότητα του εμπειρογνώμονα στα δικαστήρια.

<u>Τμήματα ανίχνευσης εγκλημάτων</u>
Η ευθύνη για τις έρευνες σχετικά με την απάτη μέσω Διαδικτύου και με άλλα οικονομικά εγκλήματα που διαπράττονται μέσω του Διαδικτύου ανήκει στο τμήμα ανίχνευσης εγκλημάτων κάθε επαρχίας. Τα οικονομικά αδικήματα που διαπράττονται μέσω του Διαδικτύου ερευνώνται επίσης από το Γραφείο διερεύνησης οικονομικού εγκλήματος στο Αρχηγείο της Αστυνομίας Κύπρου.

Στο πλαίσιο της Σύμβασης για το κυβερνοέγκλημα, το σημείο επαφής που λειτουργεί επί εικοσιτετραώρου βάσεως είναι ο επικεφαλής του ΓΚΗΕ, ο οποίος είναι επίσης υπεύθυνος για τη διεκπεραίωση των αιτήσεων ΑΔΣ. Το δεύτερο σημείο επαφής είναι το Εθνικό Κεντρικό Γραφείο (Ιντερπόλ) στη Λευκωσία, που είναι υπεύθυνο για τη διαβίβαση των πληροφοριών που ζητούνται στον επικεφαλής του τμήματος κυβερνοεγκλήματος εκτός εργάσιμων ωρών. Η Αστυνομία Κύπρου είναι επίσης το σημείο επαφής που προβλέπεται στον νόμο 147(I)/2015 για τη μεταφορά στο εσωτερικό δίκαιο της οδηγίας 2013/40/ΕΕ.

4.3. Άλλες αρχές/όργανα/συμπράξεις δημόσιου-ιδιωτικού τομέα

Η Εθνική Στρατηγική Κυβερνοασφάλειας παρέχει τη δυνατότητα χρήσης συμπράξεων δημοσίου-ιδιωτικού τομέα (ΣΔΙΤ) για την πρόληψη και την καταπολέμηση του κυβερνοεγκλήματος. Επί του παρόντος τελεί υπό εξέταση από της κυπριακές αρχές.
Εντούτοις, έχει καταρτιστεί υπόδειγμα συνεργασίας, ειδικά στον τομέα της πρόληψης και της ευαισθητοποίησης, όπου συμμετέχουν οι ακόλουθοι φορείς:

- Το Γραφείο του Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων
- Μη κυβερνητικές οργανώσεις όπως το CNTI και η οργάνωση «Ελπίδα για τα Παιδιά»
- Το Υπουργείο Παιδείας και Πολιτισμού έχει τον ηγετικό ρόλο βάσει της Δράσης 14 «Ευαισθητοποίηση» της Εθνικής Στρατηγικής Κυβερνοασφάλειας.
- Το Τμήμα Υπηρεσιών Πληροφορικής (Υπουργείο Οικονομικών) λειτουργεί ως GOV CIRT (κυβερνητική ομάδα άμεσης ανταπόκρισης για συμβάντα που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών της Κύπρου).
- Το Υπουργείο Εργασίας Πρόνοιας και Κοινωνικών Ασφαλίσεων είναι η αρμόδια αρχή για την εφαρμογή του νόμου 91(I)/2014
- Το Υπουργείο Ενέργειας, Εμπορίου, Βιομηχανίας και Τουρισμού είναι η αρμόδια αρχή για την εφαρμογή της οδηγίας για το ηλεκτρονικό εμπόριο
- Πάροχοι υπηρεσιών Διαδικτύου.

4.4. Συνεργασία και συντονισμός σε εθνικό επίπεδο

4.4.1. Νομικές απαιτήσεις ή απαιτήσεις πολιτικής

Η Αστυνομία Κύπρου είναι η μόνη αρχή στην Κύπρο που είναι υπεύθυνη για τη διερεύνηση του κυβερνοεγκλήματος.
Σε ό,τι αφορά την πρόληψη και την ευαισθητοποίηση, μετά την έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, τα εν λόγω ζητήματα αντιμετωπίζονται οριζόντια στο πλαίσιο της Δράσης 14 της Στρατηγικής. Το Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ) είναι υπεύθυνο για τον συντονισμό της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Το ΓΕΡΗΕΤ έχει επίσης επιβάλει αρκετές υποχρεώσεις στους παρόχους ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των παρόχων υπηρεσιών Διαδικτύου σχετικά με την ασφάλεια δικτύων και πληροφοριών, και σε ό,τι αφορά τη συνεργασία και την παροχή πληροφοριών για συναφή ζητήματα στις υπηρεσίες έκτακτης ανάγκης και την αστυνομία. Το ΓΕΡΗΕΤ διευκολύνει τις συνομιλίες μεταξύ των φορέων εκμετάλλευσης και της αστυνομίας για τη βελτίωση της συνεργασίας τους στο πλαίσιο της παροχής πληροφοριών, της ταυτοποίησης των παραβατών, της φραγής πρόσβασης σε ιστότοπους με παράνομο περιεχόμενο κλπ. Το ΓΕΡΗΕΤ δύναται να επιβάλει όρους και υποχρεώσεις που καθορίζουν οι αρμόδιες αρχές, συμπεριλαμβανομένης της αστυνομίας, για συναφή ζητήματα, όπως το έγκλημα στον κυβερνοχώρο.

Σύμφωνα με τις κυπριακές αρχές, η συνεργασία με τις τράπεζες είναι επαρκής σε ό,τι αφορά την κοινοποίηση νέων εργαλείων πληρωμής. Οι τράπεζες καταβάλλουν διαρκείς προσπάθειες για τη βελτίωση της ασφάλειας και την ενίσχυση της διαδικασίας έγκρισης των διαδικτυακών συναλλαγών. Το ΓΕΡΗΕΤ μαζί με την Κεντρική Τράπεζα της Κύπρου και τον Σύνδεσμο Τραπεζών Κύπρου διευκολύνουν τις συζητήσεις μεταξύ των φορέων εκμετάλλευσης, των τραπεζών και της αστυνομίας για τη βελτίωση της συνεργασίας τους όσον αφορά την ανταλλαγή πληροφοριών.

Το Υπουργείο Παιδείας και Πολιτισμού έχει τον ηγετικό ρόλο σε ορισμένα καθήκοντα της Δράσης 14 «Ευαισθητοποίηση». Η αστυνομία και άλλες κυβερνητικές αρχές και μη κυβερνητικές οργανώσεις συμμετέχουν στο έργο που επιτελείται στο πλαίσιο της Δράσης 14.

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως συμμετέχει επίσης στη Δράση 17 της Εθνικής Στρατηγικής Κυβερνοασφάλειας, όπου οι συμμετέχοντες 4 υπουργείων ενημερώνονται για όλο το έργο που επιτελείται στο πλαίσιο της υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας, συμπεριλαμβανομένων των δραστηριοτήτων ευαισθητοποίησης.

4.4.2. Πόροι που διατίθενται για τη βελτίωση της συνεργασίας

Στο πλαίσιο χρηματοδοτικών προγραμμάτων, όπως το Hercule II και το Ταμείο Εσωτερικής Ασφάλειας 2014-2020, το ΓΚΗΕ και το ΔΕΗΔ έλαβαν χρηματοδότηση, με σκοπό την ανανέωση κάθε απαραίτητου υλισμικού και λογισμικού που χρησιμοποιείται για τη δικανική έρευνα. Επιπλέον, χορηγήθηκε πρόσθετη χρηματοδότηση για τη δημιουργία ειδικής αίθουσας εκπαίδευσης στις αρχές του 2016. Το έργο Hercules II ολοκληρώθηκε στις 30/6/2015, ενώ το δεύτερο έργο στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας θα ολοκληρωθεί σε διαφορετικές φάσεις έως το 2020. Συνολικά, όσον αφορά την ανάπτυξη ικανοτήτων για την καταπολέμηση του κυβερνοεγκλήματος, τα δύο γραφεία έχουν καλό επίπεδο. Ενώ από τη μία ο εξοπλισμός ΤΠ είναι εξαιρετικός, δεν μπορεί να λεχθεί το ίδιο για την ποιότητα των εγκαταστάσεων (κτίριο) στις οποίες στεγάζεται το ΔΕΗΔ[11].

4.5. Συμπεράσματα

- Η ομάδα των αξιολογητών δεν είχε την ευκαιρία να συναντήσει στελέχη από τον χώρο της Δικαιοσύνης της Κύπρου. Εντούτοις, γνωστοποιήθηκε ότι δεν υπάρχουν ειδικοί εισαγγελείς και δικαστές για τις υποθέσεις κυβερνοεγκλήματος.

- Η Αστυνομία Κύπρου είναι υπεύθυνη για την προδικασία στον χώρο του κυβερνοεγκλήματος, καθώς και για τη συλλογή και την ανάλυση πληροφοριών και δεδομένων. Παρέχει επίσης δικανική εμπειρογνωσία και είναι υπεύθυνη για την πρόληψη και την αποτροπή, καθώς και για ορισμένες πτυχές διεθνούς συνεργασίας στον τομέα αυτόν. Το ΓΚΗΕ είναι υπεύθυνο για τη διερεύνηση του κυβερνοεγκλήματος, όπως ορίζεται στον νόμο Ν. 22(ΙΙΙ)/2004. Συγχρόνως, το ΓΚΗΕ είναι υπεύθυνο για τη διερεύνηση υποθέσεων που αφορούν ρατσισμό και ξενοφοβία μέσω του Διαδικτύου.

[11] Μετά την επιτόπια επίσκεψη, η ομάδα αξιολόγησης ενημερώθηκε σχετικά με τις βελτιώσεις που επήλθαν στις σχετικές εγκαταστάσεις. Αναμένεται ότι θα είναι διαθέσιμες νέες εγκαταστάσεις έως το 2016 οι οποίες θα περιλαμβάνουν νέα αίθουσα εκπαίδευσης και νέα γραφεία.

- Κατά τις συναντήσεις μαζί τους, οι εκπρόσωποι της Αστυνομίας Κύπρου επέδειξαν υψηλό επίπεδο επαγγελματισμού και προσήλωσης στο έργο τους. Οι εκπρόσωποι των κυπριακών αρχών, με τους οποίους συναντήθηκε η ομάδα, συμμετέχουν ατύπως στις δραστηριότητες έρευνας και δίωξης του κυβερνοεγκλήματος, και αυτό λειτουργεί ικανοποιητικά. Οι αρμόδιοι γνωρίζουν τους ομολόγους τους στις άλλες αρχές και, ως εκ τούτου, έρχονται σε επαφή μαζί τους πολύ εύκολα. Με τον τρόπο αυτόν, επιτελούν το έργο τους χωρίς περιττές γραφειοκρατικές καθυστερήσεις.

- Η συλλογή και το παραδεκτό των αποδεικτικών στοιχείων και το πρόβλημα της διατήρησης των δεδομένων στα κράτη μέλη αναφέρθηκαν ως τα κύρια εμπόδια στις επιτυχείς έρευνες. Σύμφωνα με την πρόσφατη απόφαση του Ανωτάτου Δικαστηρίου σχετικά με τις επιπτώσεις που έχει η ακύρωση της οδηγίας της ΕΕ για τη διατήρηση δεδομένων όσον αφορά τον νόμο 183(I)/2007, ο εν λόγω νόμος συνάδει με την Ευρωπαϊκή Σύμβαση για τα δικαιώματα του ανθρώπου. Εντούτοις, οι αξιολογητές αναγνωρίζουν ότι το πρόβλημα της διατήρησης δεδομένων είναι γενικό και απαιτεί την ανάληψη δράσης σε επίπεδο ΕΕ. Επιπροσθέτως, κατά τη γνώμη των αξιολογητών, θα μπορούσε να είναι χρήσιμος ο διάλογος με τον ιδιωτικό τομέα, προκειμένου να αναζητηθούν δυνατότητες για τη διατήρηση δεδομένων, καθώς και για να εξασφαλιστεί η συλλογή πληροφοριών κατά τρόπο ώστε να διασφαλίζεται το παραδεκτό τους στα δικαστήρια.

- Αναφέρθηκε ότι η συνεργασία με τον ιδιωτικό κανόνα είναι γενικώς καλή. Πραγματοποιούνται τακτικές επαφές μεταξύ των αρχών επιβολής του νόμου και του ιδιωτικού τομέα. Αναφέρθηκαν κάποιες δυσκολίες στην επικοινωνία με τον τραπεζικό τομέα.

- Ωστόσο, δεν κατέστη σαφές αν οι εισαγγελείς έχουν επαφές με τον ιδιωτικό τομέα στο πλαίσιο της υπάρχουσας δομής για την κυβερνοασφάλεια. Επομένως, κατά τη γνώμη των αξιολογητών, θα είναι χρήσιμο να εξεταστεί το ενδεχόμενο συμμετοχής των εισαγγελέων στις συσκέψεις/συζητήσεις με τον ιδιωτικό τομέα, ώστε να εξασφαλίζεται ότι τα αποδεικτικά στοιχεία συλλέγονται σύμφωνα με την ισχύουσα νομοθεσία και ότι είναι παραδεκτά στις δικαστικές διαδικασίες.

- Οι κυπριακές αρχές ωφελούνται τα μάλα από τη χρήση της χρηματοδότησης που παρέχεται από την ΕΕ για τα προγράμματά τους, για παράδειγμα στο πλαίσιο του προγράμματος «Πρόληψη και καταπολέμηση της εγκληματικότητας» της Ευρωπαϊκής Ένωσης (ISEC). Συστάθηκε έτσι το Κυπριακό Κέντρο Αριστείας Κυβερνοεγκλήματος (3CE). Στο πλαίσιο χρηματοδοτικών προγραμμάτων, όπως το Hercule II και το Ταμείο Εσωτερικής Ασφάλειας 2014-2020, το ΓΚΗΕ και το ΔΕΗΔ έλαβαν χρηματοδοτική ενίσχυση, με σκοπό την ανανέωση κάθε απαραίτητου υλισμικού και λογισμικού που χρησιμοποιείται για τις έρευνες. Χωρίς αυτή τη χρηματοδότηση, δεν θα ήταν ικανά να λειτουργήσουν εξίσου αποτελεσματικά στους οικείους τομείς. Ορισμένες αρχές, για παράδειγμα το ΔΕΗΔ, ενδέχεται επίσης να επωφεληθούν από αύξηση του προσωπικού στα γραφεία τους. Συνεπώς, κατά τους αξιολογητές, η χρήση των ενωσιακών κονδυλίων έχει καθοριστική σημασία προκειμένου να μπορέσουν οι σχετικές αρχές να εργαστούν με τον πλέον αποτελεσματικό τρόπο και να αξιοποιήσουν πλήρως τις δυνατότητές τους. Ταυτόχρονα, οι κυπριακές αρχές θα πρέπει επίσης να συμβάλουν στην παροχή επαρκούς χρηματοδότησης στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

5. ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ

5.1. Ουσιαστικό ποινικό δίκαιο σχετικά με το κυβερνοέγκλημα

5.1.1. Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο

Η Κυπριακή Δημοκρατία είναι συμβαλλόμενο μέρος στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης). Ο σχετικός κυρωτικός νόμος είναι ο Ν.22(ΙΙΙ)/2004.

5.1.2. Περιγραφή εθνικής νομοθεσίας

Α/ Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών

Κατά τον χρόνο της επίσκεψης αξιολόγησης, γνωστοποιήθηκε στην ομάδα των αξιολογητών ότι ο νόμος 147(Ι)/2015, σχετικά με τη μεταφορά στο εσωτερικό δίκαιο της οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών, έχει ψηφιστεί από τη Βουλή των Αντιπροσώπων.

Εντούτοις, πριν από την έναρξη ισχύος του εν λόγω νόμου, ο νόμος L22(III) 2004 που κυρώνει τη Σύμβαση κατά του εγκλήματος μέσω Διαδικτύου είχε ποινικοποιήσει τις ακόλουθες πράξεις:

<u>Παράνομη πρόσβαση σε σύστημα ηλεκτρονικών υπολογιστών</u> (Άρθρο 4)
Όποιος με πρόθεση και χωρίς δικαίωμα εισέρχεται στο σύνολο ή μέρος συστήματος ηλεκτρονικών υπολογιστών παραβιάζοντας τα μέτρα ασφαλείας διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές.

Παράνομη επέμβαση σε σύστημα (Άρθρο 7)
Πρόσωπο το οποίο με πρόθεση και χωρίς δικαίωμα προκαλεί 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, είναι ένοχος αδικήματος που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές.

Παράνομη επέμβαση σε δεδομένα (Άρθρο 6)
Όποιος εκ προθέσεως και χωρίς δικαίωμα καταστρέφει, διαγράφει, μεταβάλλει ή αποκρύπτει δεδομένα ηλεκτρονικού υπολογιστή διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές.

Παράνομη υποκλοπή ηλεκτρονικών δεδομένων (Άρθρο 5)
Όποιος με πρόθεση και χωρίς δικαίωμα παρεμβαίνει με τεχνικά μέσα σε δεδομένα ηλεκτρονικού υπολογιστή τα οποία δεν εκπέμπονται δημόσια από, προς ή μέσα σ' ένα σύστημα ηλεκτρονικού υπολογιστή, διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές.

Κατάχρηση επινοήσεων (Άρθρο 8)
Το άρθρο απαγορεύει τη με πρόθεση και χωρίς δικαίωμα παραγωγή, πώληση, προμήθευση προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση εργαλείων κατάχρησης ηλεκτρονικών συστημάτων και καθιστά την πράξη αυτή αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές.

Κατά την επιβολή της ποινής, τα δικαστήρια λαμβάνουν υπόψη επιβαρυντικές ή ελαφρυντικές περιστάσεις που αφορούν είτε το αδίκημα (περιστάσεις υπό τις οποίες τελέστηκε) ή τον δράστη (προσωπικές περιστάσεις).

Β/ Οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας

Η Κύπρος μετέφερε την οδηγία 2011/93/ΕΕ της 13ης Δεκεμβρίου 2011 σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας στο εσωτερικό δίκαιο τον Ιούλιο του 2014 με τον νόμο 91(Ι)/2014.
Η εφαρμογή άρχισε πολύ πρόσφατα και δεν έχει ακόμη αξιολογηθεί. Οι κυπριακές αρχές δεν ανέφεραν ιδιαίτερες δυσκολίες κατά τη βραχεία περίοδο που διέρρευσε μετά την έκδοση του νόμου.
Ο νόμος 91(Ι)/2014 ορίζει ότι συναινετικές σεξουαλικές δραστηριότητες μεταξύ δύο παιδιών που δεν έχουν φτάσει στην ηλικία συναίνεσης και τα οποία έχουν παρόμοια ηλικία και παρόμοιο βαθμό ψυχολογικής και σωματικής ωριμότητας δεν συνιστούν ποινικό αδίκημα, υπό την προϋπόθεση ότι οι εν λόγω δραστηριότητες δεν περιλαμβάνουν βία ή εκμετάλλευση [η ηλικία συναίνεσης είναι τα δεκαεπτά έτη (17)]. Περιλαμβάνονται παρόμοιες διατάξεις που διέπουν τις σχέσεις ενηλίκων και παιδιών, μεταξύ των οποίων η διαφορά ηλικίας δεν υπερβαίνει τα 3 έτη.

Η νομοθεσία περιέχει διατάξεις για επιβαρυντικές περιστάσεις, όπως ο νόμος 91(Ι)/2014, ο οποίος ορίζει ότι όταν το θύμα πορνογραφικής παράστασης είναι παιδί ηλικίας κάτω των δεκατριών (13) ετών, ο δράστης υπόκειται σε ποινή ισόβιας φυλάκισης.
Επιπλέον, θεσπίστηκαν οι ακόλουθοι κανόνες για την ποινικοποίηση της κακοποίησης παιδιών και της παιδικής πορνογραφίας.

Παραγωγή παιδικής πορνογραφίας
Όποιος με πρόθεση και χωρίς δικαίωμα παράγει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα δέκα έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 42.175 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 11(1)(α)]

Προσφορά ή διάθεση υλικού παιδικής πορνογραφίας
Όποιος με πρόθεση και χωρίς δικαίωμα προσφέρει ή καθιστά διαθέσιμη παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα δέκα έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 42.175 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 11(1)(β)]

Διανομή ή διαβίβαση παιδικής πορνογραφίας μέσω συστήματος ηλεκτρονικού υπολογιστή

Όποιος με πρόθεση και χωρίς δικαίωμα διανέμει ή διαβιβάζει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα δέκα έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 42.175 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 11(1)(γ)]

Προαγωγή παιδικής πορνογραφίας μέσω ηλεκτρονικού υπολογιστή για το ίδιο ή άλλο πρόσωπο

Όποιος με πρόθεση και χωρίς δικαίωμα προάγει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή για τον ίδιο ή για άλλον διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα δέκα έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 42.175 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 11(1)(δ)]

Κατοχή παιδικής πορνογραφίας σε σύστημα ηλεκτρονικού υπολογιστή ή σε μέσον αποθήκευσης δεδομένων ηλεκτρονικού υπολογιστή

Όποιος με πρόθεση και χωρίς δικαίωμα κατέχει παιδική πορνογραφία σε σύστημα ηλεκτρονικού υπολογιστή ή σε μέσον αποθήκευσης δεδομένων ηλεκτρονικού υπολογιστή διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα δέκα έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 42.175 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 11(1)(ε)]

Κατοχή παιδικής πορνογραφίας σε σύστημα ηλεκτρονικού υπολογιστή ή σε μέσον αποθήκευσης δεδομένων ηλεκτρονικού υπολογιστή

Με την επιφύλαξη των διατάξεων του άρθρου 12, όποιος αποκτά ή έχει στην κατοχή του υλικό παιδικής πορνογραφίας είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα (10) έτη.
Νόμος 91(Ι)/2014, άρθρο 8(1)

Πρόσβαση σε υλικό παιδικής πορνογραφίας

Όποιος εν γνώσει του αποκτά πρόσβαση σε παιδική πορνογραφία μέσω της τεχνολογίας της πληροφορικής και των επικοινωνιών είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα (10) έτη [Νόμος 91(Ι)/2014 άρθρο 8(2)]
Νόμος 91(Ι)/2014, άρθρο 8(3)
Όποιος διανέμει, διαδίδει ή μεταδίδει υλικό παιδικής πορνογραφίας είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα πέντε (15) έτη.

Νόμος 91(I)/2014, άρθρο 8(4)

Προσφορά ή διάθεση υλικού παιδικής πορνογραφίας

Νόμος 91(I)/2014, άρθρο 8(5)

Με την επιφύλαξη των διατάξεων του άρθρου 12, όποιος παράγει υλικό παιδικής πορνογραφίας είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα είκοσι (20) έτη.

Ηλεκτρονική προσέγγιση ή άγρα παιδιών

Όποιος προκαλεί τη συμμετοχή παιδιού σε πορνογραφικές παραστάσεις ή στρατολογεί παιδί προκειμένου αυτό να συμμετάσχει σε αυτές ή αποκομίζει κέρδη από τη συμμετοχή παιδιού σε πορνογραφικές παραστάσεις ή εκμεταλλεύεται παιδί με άλλους τρόπους προς τον σκοπό αυτό είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα είκοσι (20) έτη.

(2) Ο εξαναγκασμός παιδιού να πράξει όπως αναφέρεται στην παράγραφο (1), 25 έτη

(3) Η παρακολούθηση πορνογραφικών παραστάσεων, 15 έτη

(4) Όποιος διά ζώσης ή μέσω της τεχνολογίας της πληροφορικής και των επικοινωνιών, προκαλεί ή προτείνει σε παιδί το οποίο δεν έχει φτάσει στην ηλικία συναίνεσης, όπως το παιδί αυτό συμμετέχει σε πορνογραφική παράσταση, με σκοπό ο προκαλών ή ο προτείνων ή το τρίτο πρόσωπο να παρακολουθήσει την παράσταση αυτή, είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα (10) έτη.

(5) Όποιος προκαλεί τη συμμετοχή παιδιού σε παιδική πορνεία ή στρατολογεί παιδί προκειμένου να συμμετάσχει σε παιδική πορνεία για να αποκομίσει κέρδη από το παιδί είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα είκοσι πέντε (25) έτη.

(6) Ο εξαναγκασμός παιδιού να συμμετάσχει σε παιδική πορνεία, 25 έτη

Νόμος 91(I)/2014 άρθρο 7(1)

Νόμος 91(I)/2014 άρθρο 9(1)

Με την επιφύλαξη των διατάξεων του άρθρου 12, όποιος προτείνει σε παιδί το οποίο δεν έχει φτάσει στην ηλικία συναίνεσης, μέσω της τεχνολογίας της πληροφορικής και των επικοινωνιών, να το συναντήσει, με σκοπό την τέλεση σεξουαλικής πράξης μαζί του ή την παραγωγή υλικού παιδικής πορνογραφίας ή τη σεξουαλική εκμετάλλευση του παιδιού το οποίο δεν έχει φτάσει στην ηλικία συναίνεσης, και η εν λόγω πρόταση ακολουθείται από την τέλεση πράξεων οι οποίες οδηγούν σε συνάντηση, είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα (10) έτη.

Νόμος 91(I)/2014 άρθρο 9(2)

Με την επιφύλαξη των διατάξεων του άρθρου 12, όποιος μέσω της τεχνολογίας της πληροφορικής και των επικοινωνιών, προσκαλεί ή προσεγγίζει παιδί το οποίο δεν έχει φτάσει στην ηλικία συναίνεσης και αποπειράται να αποκτήσει ή αποπειράται να έχει πρόσβαση ή αποκτά ή επιτυγχάνει πρόσβαση σε υλικό παιδικής πορνογραφίας που απεικονίζει το παιδί αυτό, είναι ένοχος κακουργήματος και, σε περίπτωση καταδίκης του, υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δέκα (10) έτη.

Γ/ Διαδικτυακή απάτη με κάρτες

Ο νόμος 22(ΙΙΙ)/2004 που κυρώνει τη Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου ορίζει κανόνες για την ποινικοποίηση της απάτης και της πλαστογραφίας που σχετίζονται με ηλεκτρονικό υπολογιστή.

Απάτη σχετιζόμενη με ηλεκτρονικό υπολογιστή

Όποιος με πρόθεση και χωρίς δικαίωμα και με σκοπό την καταδολίευση προκαλεί απώλεια στην περιουσία άλλου προσώπου με:

(α) εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικού υπολογιστή,

(β) επέμβαση στη λειτουργία ενός συστήματος υπολογιστή με σκοπό να επιφέρει χωρίς δικαίωμα οικονομικό όφελος στον εαυτό του ή σε άλλο πρόσωπο, διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 10(α)(β)]

Πλαστογραφία σχετιζόμενη με ηλεκτρονικό υπολογιστή

Όποιος με πρόθεση και χωρίς δικαίωμα και με σκοπό την καταδολίευση εισάγει, μεταβάλλει, διαγράφει ή αποκρύπτει δεδομένα ηλεκτρονικού υπολογιστή με τρόπον ώστε μη αυθεντικά δεδομένα που δημιουργούνται ως αποτέλεσμα των πιο πάνω παρεμβάσεων να παρουσιάζονται ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά, ανεξάρτητα από το αν τα δεδομένα είναι άμεσα αναγνώσιμα και κατανοητά, διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 34.172 ευρώ ή και με τις δύο ποινές [Ν. 22(ΙΙΙ)/2004, άρθρο 9)]

Αποστολή ή έλεγχος της αποστολής ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam)

Οποιοσδήποτε παραβιάζει τις διατάξεις του άρθρου 10 περί μη ζητηθείσας εμπορικής επικοινωνίας υπόκειται, σε περίπτωση καταδίκης του, σε χρηματική ποινή που δεν υπερβαίνει τα 8.250 ευρώ. Σε περίπτωση δεύτερης ή μετέπειτα καταδίκης, η χρηματική ποινή μπορεί να διπλασιασθεί. Είναι επίσης διοικητικό αδίκημα. [Νόμος 156 (Ι)/ 2004, άρθρο 23].

5.2. Διαδικαστικά ζητήματα

5.2.1. Τεχνικές έρευνας

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως εγκαινίασε διάλογο με άλλες αρμόδιες αρχές για την κατάρτιση νέας νομοθεσίας που θα επιτρέπει την παρακολούθηση ιδιωτικών επικοινωνιών για σκοπούς πρόληψης και διερεύνησης σοβαρών αδικημάτων ή για λόγους εθνικής ασφάλειας.
Η παρακολούθηση αυτή θα συνάδει πλήρως με το άρθρο 17 του Συντάγματος που προστατεύει το δικαίωμα στην ιδιωτική ζωή.

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως δήλωσε ότι παρακολουθεί στενά όλες τις εξελίξεις σχετικά με την ακύρωση της οδηγίας περί διατήρησης δεδομένων και βρίσκεται σε στενή επαφή με την αστυνομία και τη Νομική Υπηρεσία Κύπρου για την πιθανή έγκριση ενδεχόμενων μελλοντικών μέτρων.
Μετά την επιτόπια επίσκεψη, η ομάδα αξιολόγησης ενημερώθηκε ότι ο νόμος για την πρόσβαση σε καταγεγραμμένα δεδομένα που περιέχουν ιδιωτικές επικοινωνίες εγκρίθηκε από τη Βουλή των Αντιπροσώπων και έχει πλέον τεθεί σε ισχύ.

Οι ακόλουθες τεχνικές έρευνας είναι επιτρεπτές δυνάμει της εθνικής νομοθεσίας:
• αναζήτηση και κατάσχεση συστημάτων πληροφοριών/δεδομένων υπολογιστή· (κώδικας ποινικής δικονομίας)
• διαφύλαξη δεδομένων υπολογιστή (νόμος 22(III)/2004)
• διάταγμα για αποθηκευμένα δεδομένα κίνησης/περιεχομένου - ωστόσο, μόνο για αποθηκευμένα δεδομένα κίνησης (νόμος 183(I)/2007)
• διάταγμα για στοιχεία χρήστη [νόμος 183(I)/2007].
Η εθνική νομοθεσία δεν επιτρέπει την υποκλοπή/συλλογή δεδομένων κίνησης/περιεχομένου σε πραγματικό χρόνο. Ωστόσο, ο νόμος 183(I)/2007 υποχρεώνει τους παρόχους υπηρεσιών Διαδικτύου να αποθηκεύουν δεδομένα τηλεπικοινωνιών και κίνησης για σκοπούς έρευνας για περίοδο έξι μηνών. Η χρήση εξειδικευμένου λογισμικού, όπως το «Child Protection System» (CPS) και το «NetClean», διευκολύνει τις έρευνες σχετικά με το έγκλημα στον κυβερνοχώρο.

5.2.2. Εγκληματολογική εξέταση και κρυπτογράφηση

Οι εκπρόσωποι της αστυνομίας υπογράμμισαν το γεγονός ότι η κρυπτογράφηση δημιουργεί επί του παρόντος σημαντικά προβλήματα για τους ιατροδικαστές σε ολόκληρο τον κόσμο. Τα προβλήματα κρυπτογράφησης ανακύπτουν κυρίως κατά τη διάρκεια ερευνών σε περιπτώσεις ηλεκτρονικής πειρατείας και παράνομων ηλεκτρονικών παιχνιδιών. Μολαταύτα, το δικανικό εργαστήριο ηλεκτρονικών δεδομένων διαθέτει εργαλεία που επιτρέπουν την αποκρυπτογράφηση ορισμένων μορφών κρυπτογράφησης, όπως το PRTK μέσω της πλατφόρμας FTK. Ωστόσο, οι λύσεις αυτές δεν είναι πάντα αποτελεσματικές.

Εάν υπάρχει ανάγκη προώθησης αποδεικτικών στοιχείων σε άλλες αρχές για αποκρυπτογράφηση, αυτό γίνεται πάντα μέσω της Ευρωπόλ και της Interpol. Η αποκρυπτογράφηση δεν διενεργείται σε συνεργασία με ιδιωτικές εταιρίες. Δεν υπάρχουν εξειδικευμένα κέντρα αποκρυπτογράφησης στην Κύπρο. Το ΓΚΗΕ έχει προτείνει, ως εκ τούτου, τη θέσπιση ειδικής νομοθεσίας που θα επιβάλλει σε χρήστες και διαχειριστές ηλεκτρονικών υπολογιστών να παρέχουν τους κωδικούς κρυπτογράφησής τους κατά τη διάρκεια έρευνας. Η άρνηση θα θεωρείται αδίκημα. Η πρόταση εξετάζεται υπό το πρίσμα του πιθανού αντίκτυπου που μπορεί να έχει στο δικαίωμα σιωπής του κατηγορουμένου.

5.2.3. Ηλεκτρονικά αποδεικτικά στοιχεία

Δεν υπάρχουν ειδικοί κανόνες παραδεκτού σχετικά με τα ηλεκτρονικά αποδεικτικά στοιχεία. Τα ηλεκτρονικά αποδεικτικά στοιχεία υπόκεινται στους ίδιους κανόνες περί αποδεικτικών στοιχείων με τα έντυπα έγγραφα και είναι παραδεκτά δυνάμει του δικαίου της απόδειξης, κεφ. 9. Ωστόσο, η φύση των ηλεκτρονικών αποδεικτικών στοιχείων και η ευκολία με την οποία μπορούν να αποτελέσουν αντικείμενο χειρισμού ή παραποίησης, μπορούν να δημιουργήσουν προβλήματα ως προς το παραδεκτό που δεν προκύπτουν με άλλα είδη αποδεικτικών στοιχείων, για παράδειγμα ίσως χρειάζεται περισσότερο αποδεικτικό υλικό όπως η ανάλυση δικανικών εργαλείων ή η μαρτυρία εμπειρογνώμονα από δικανικό ερευνητή.

Τα ηλεκτρονικά αποδεικτικά στοιχεία συλλέγονται από τον τόπο του εγκλήματος με βάση διεθνή πρότυπα. Αφού συλλέξει και σφραγίσει τα αποδεικτικά στοιχεία, ο ερευνητής τα παραδίδει στο ΔΕΗΔ για εξέταση. Η διαδικασία συλλογής, μεταφοράς και εξέτασης των ηλεκτρονικών αποδεικτικών στοιχείων ακολουθεί τους κανόνες περί αποδεικτικών στοιχείων και η αλυσίδα

φύλαξης είναι πάντα πλήρως τεκμηριωμένη, με βάση την αστυνομική διάταξη 3/17 και το εγχειρίδιο του δικανικού εργαστηρίου. Για κάθε είδος ηλεκτρονικού αποδεικτικού στοιχείου, οι ιατροδικαστές δημιουργούν μια εικόνα και στη συνέχεια προβαίνουν σε ανάλυση με τη χρήση εγκεκριμένων δικανικών εργαλείων, όπως τα FTK και IEF. Το εξαγόμενο αποδεικτικό στοιχείο αποθηκεύεται σε εξωτερικούς δίσκους ή σε CD/DVD από τον ιατροδικαστή πριν δοθεί για εξέταση από τον ερευνητή. Σε περιπτώσεις παιδικής πορνογραφίας, διενεργείται περαιτέρω ανάλυση από τους ερευνητές μέσω του λογισμικού NetClean και όλες οι εικόνες ελέγχονται έναντι της βάσης δεδομένων ICSE. Τα εξαγόμενα αποδεικτικά στοιχεία, μαζί με την έκθεση του ερευνητή και την έκθεση του ιατροδικαστή, υποβάλλονται στο δικαστήριο και μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της δίκης.

5.3. Προστασία ανθρωπίνων δικαιωμάτων/θεμελιωδών ελευθεριών

Το δικαίωμα στην ιδιωτική ζωή και η ελευθερία της επικοινωνίας προστατεύονται δυνάμει των άρθρων 15 και 17 του Συντάγματος της Κύπρου. Ειδικές διατάξεις για την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών περιλαμβάνονται επίσης στη σχετική νομοθεσία (αναφέρονται στο κεφάλαιο 3.2).
Επιπλέον, ο περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα νόμος 138(I)/2001 ρυθμίζει τη διασφάλιση των δεδομένων προσωπικού χαρακτήρα.

Σε ορισμένες περιπτώσεις, αλλά υπό πολύ αυστηρές προϋποθέσεις, για παράδειγμα δυνάμει του νόμου 183(I)/2007 (νόμος περί της διατήρησης δεδομένων), τα δικαιώματα που αφορούν την ιδιωτική ζωή μπορούν να περιορίζονται, αλλά σε κάθε περίπτωση απαιτείται διάταγμα δικαστηρίου. Επιπλέον, ο νόμος εφαρμόζεται μόνο σε πολύ σοβαρά αδικήματα που τιμωρούνται με ελάχιστη ποινή φυλάκισης 5 ετών.

5.4. Δικαιοδοσία

5.4.1. Αρχές που διέπουν τη διερεύνηση των εγκλημάτων στον κυβερνοχώρο

Δυνάμει του νόμου 22(III)/2004, το άρθρο 22 της Σύμβασης της Βουδαπέστης αφορά τη δικαιοδοσία σχετικά με πράξεις ηλεκτρονικού εγκλήματος που διαπράττονται εκτός του εδάφους της Κύπρου. Επιπρόσθετες διατάξεις σχετικά με τη δικαιοδοσία περιλαμβάνονται επίσης στον νόμο 147(I)/2015 που μεταφέρει στο εθνικό δίκαιο την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών, και είναι ταυτόσημες με εκείνες που περιλαμβάνονται στην εν λόγω οδηγία.

5.4.2. Κανόνες που διέπουν τις περιπτώσεις σύγκρουσης δικαιοδοσίας και παραπομπή στην Eurojust

Η απόφαση-πλαίσιο 2009/948/ΔΕΥ του Συμβουλίου, της 30ής Νοεμβρίου 2009, για την πρόληψη και τον διακανονισμό συγκρούσεων δικαιοδοσίας σε ποινικές υποθέσεις μεταφέρθηκε στο εθνικό δίκαιο. Ωστόσο, δεν έχει αναφερθεί καμία εμπειρία σε επίπεδο σύγκρουσης δικαιοδοσίας.

5.4.3. Δικαιοδοσία για πράξεις κυβερνοεγκλήματος που διαπράττονται στο «υπολογιστικό νέφος»

Οι κυπριακές αρχές ανέφεραν ότι πρέπει να χρησιμοποιούνται μέσα ΑΔΣ, εάν το υπολογιστικό νέφος φιλοξενείται σε άλλες χώρες. Αυτό μπορεί να προκαλέσει καθυστερήσεις.

5.4.4. Εικόνα της Κύπρου όσον αφορά το νομικό πλαίσιο για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Σύμφωνα με την κυπριακή αξιολόγηση, ο νόμος 147(I)/2015 που μεταφέρει στο εθνικό δίκαιο την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών αναμένεται να βελτιώσει περαιτέρω τη διερεύνηση των εγκλημάτων στον κυβερνοχώρο που διαπράττονται εκτός του εθνικού εδάφους, καθώς προβλέπει ευρύτερες εξουσίες όσον αφορά τη δικαιοδοσία. Διευρύνει επίσης το φάσμα των αδικημάτων που διαπράττονται σε βάρος συστημάτων πληροφοριών αντί συστημάτων ηλεκτρονικών υπολογιστών, όπως ορίζεται επί του παρόντος στη Σύμβαση της Βουδαπέστης.

5.5. Συμπεράσματα

- Η Κύπρος επικύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης κατά του εγκλήματος μέσω του Διαδικτύου το 2004 [Νόμος 22(III)/2004], αλλά δεν μετέφερε στο εθνικό δίκαιο δικονομικά μέτρα που θα εξουσιοδοτούσαν τις αρμόδιες εθνικές αρχές να καταγράφουν δεδομένα περιεχομένου σε πραγματικό χρόνο σε περιπτώσεις κυβερνοεγκλήματος για ποινικά αδικήματα που ορίζονται στο Μέρος 1 της εν λόγω Σύμβασης. Θα πρέπει, επομένως, να εξεταστούν τρόποι για την έγκριση νομοθετικών ή άλλων μέτρων προκειμένου να συνάδουν πλήρως με το άρθρο 21 της Σύμβασης της Βουδαπέστης. [12]

- Ο Νόμος 91(I)/2014 μεταφέρει στο εθνικό δίκαιο την οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και περιέχει διατάξεις για την καλύτερη εφαρμογή της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας εκμετάλλευσης και κακοποίησης (Σύμβαση του Lanzarote).

- Μέτρα για την καταπολέμηση της απάτης και της πλαστογραφίας που σχετίζονται με ηλεκτρονικούς υπολογιστές προβλέπονται στον νόμο Ν.22(III)2004. Επιπλέον, η αποστολή ή ο έλεγχος της αποστολής ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam) τιμωρείται από τον Νόμο 156(I)/2004.

- Τα ηλεκτρονικά αποδεικτικά στοιχεία δεν ορίζονται από την εθνική νομοθεσία και δεν υπάρχουν ειδικοί κανόνες παραδεκτού σχετικά με αυτά. Τα ηλεκτρονικά αποδεικτικά στοιχεία υπόκεινται στους ίδιους κανόνες περί αποδεικτικών στοιχείων με τα έντυπα έγγραφα και είναι παραδεκτά δυνάμει του δικαίου της απόδειξης.

[12] Μετά την επιτόπια επίσκεψη, η ομάδα αξιολόγησης πληροφορήθηκε ότι το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως εξετάζει τροποποιήσεις για τον νόμο 92(I)/1996 περί προστασίας του απορρήτου της ιδιωτικής επικοινωνίας. Αναμένεται ότι οι τροποποιήσεις αυτές θα δώσουν στις αρμόδιες αρχές τη δυνατότητα να προβαίνουν σε παρακολούθηση ιδιωτικών επικοινωνιών σε πραγματικό χρόνο στο πλαίσιο των περιορισμών που αναφέρονται στο άρθρο 17 του Συντάγματος της Κύπρου.

- Η κρυπτογράφηση θεωρείται ότι αποτελεί πρόκληση. Ωστόσο, το ΓΚΗΕ έχει προτείνει τη θέσπιση ειδικής νομοθεσίας που θα επιβάλλει σε χρήστες και διαχειριστές ηλεκτρονικών υπολογιστών να παρέχουν τους κωδικούς κρυπτογράφησής τους κατά τη διάρκεια έρευνας. Η άρνηση θα θεωρείται αδίκημα. Η πρόταση εξετάζεται υπό το πρίσμα του αντικτύπου που μπορεί να έχει στο δικαίωμα σιωπής του κατηγορουμένου.

- Δεν υπάρχουν ειδικές διατάξεις για τη δικαιοδοσία της Κύπρου όσον αφορά το έγκλημα στον κυβερνοχώρο. Ο προσφάτως εγκριθείς Νόμος 147(Ι)/2015 που μεταφέρει στο εθνικό δίκαιο την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών αναμένεται να βελτιώσει περαιτέρω τη διερεύνηση των εγκλημάτων στον κυβερνοχώρο που διαπράττονται εκτός του εθνικού εδάφους, καθώς προβλέπει ευρύτερες εξουσίες όσον αφορά τη δικαιοδοσία.

- Η απόφαση-πλαίσιο 2009/948/ΔΕΥ του Συμβουλίου, της 30ής Νοεμβρίου 2009, για την πρόληψη και τον διακανονισμό συγκρούσεων δικαιοδοσίας σε ποινικές υποθέσεις μεταφέρθηκε στο εθνικό δίκαιο. Μέχρι σήμερα δεν έχουν καταγραφεί περιπτώσεις σύγκρουσης δικαιοδοσίας.

6. ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΠΤΥΧΕΣ

6.1. Κυβερνοεπιθέσεις

6.1.1. Φύση των κυβερνοεπιθέσεων

Στο πλαίσιο των καθηκόντων του, το τμήμα υπηρεσιών πληροφορικής (ΤΥΠ) ασκεί τον ρόλο του παρόχου υπηρεσιών Διαδικτύου για τον δημόσιο τομέα της Κύπρου. Όσον αφορά τη φύση των πρόσφατων επιθέσεων, δεν αναφέρθηκαν μείζονα/σοβαρά περιστατικά.

Οι κατηγορίες επιθέσεων ήταν οι ακόλουθες:

- Άκυρα πακέτα

- Φιλτράρισμα παραμορφωμένων HTTP

- Πρόληψη δικτύων προγραμμάτων ρομπότ («botnet»)

- Ανίχνευση πλημμύρας TCP SYN

- Ανίχνευση πλημμύρας ICMP

Όλες αυτές οι επιθέσεις εξουδετερώθηκαν αυτόματα χωρίς παρέμβαση χρήστη από το σύστημα DDOS.

6.1.2. Μηχανισμός αντιμετώπισης κυβερνοεπιθέσεων

Το τμήμα υπηρεσιών πληροφορικής (ΤΥΠ) σχεδιάστηκε από την κυβέρνηση ως η κυβερνητική ομάδα άμεσης ανταπόκρισης για συμβάντα που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών της Κύπρου (Cyprus GOVCIRT). Με τη συνδρομή της ΔΕΤ – IMPACT και του Γραφείου επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων (ΓΕΡΗΕΤ), το ΤΥΠ δημιούργησε την αναγκαία τεχνική υποδομή και την πύλη της CIRT (http://www.cirt.gov.cy). Επιπλέον, η ΔΕΤ – IMPACT παρείχε εκτενή εκπαίδευση όσον αφορά τη CIRT. Επί του παρόντος, το ΤΥΠ επεξεργάζεται τον ορισμό των εσωτερικών πολιτικών σχετικά με τη διακυβέρνηση της GOVCIRT Κύπρου.

Η ανάπτυξη μιας εθνικής ομάδας άμεσης ανταπόκρισης (CERT) είναι υπό εξέταση στο πλαίσιο της εφαρμογής της εθνικής στρατηγικής κυβερνοασφάλειας. Η δημιουργία μιας εθνικής CERT θα συνάδει με τη Δράση 38 του πυλώνα ΙΙΙ της Στρατηγικής Ευρώπη 2020 που παρέχει κίνητρα στα κράτη μέλη να δημιουργήσουν έως το 2012 ένα λειτουργικό δίκτυο CERT σε εθνικό επίπεδο που θα καλύπτει ολόκληρη την Ευρώπη, καθώς και με την οδηγία για την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ). Η Ευρωπαϊκή Επιτροπή κάλεσε τα κράτη μέλη να ενισχύσουν τη συνεργασία μεταξύ των υφιστάμενων εθνικών CERT και να διευρύνουν τους υπάρχοντες μηχανισμούς συνεργασίας, όπως η ευρωπαϊκή ομάδα κυβερνητικών CERT.

Η αστυνομία συνεργάζεται με ιδιωτικές εταιρείες που καταγγέλλουν κυβερνοεπιθέσεις με σκοπό τη συμβολή στην επίλυση των προβλημάτων και τη διερεύνηση των αδικημάτων.

Το ΤΥΠ, μολονότι δεν είναι υπηρεσία επιβολής του νόμου, λαμβάνει όλα τα απαραίτητα μέτρα για την πρόληψη των κυβερνοεπιθέσεων και διενεργεί επίσης αναλύσεις δεδομένων ανάλογα με την περίπτωση. Ωστόσο, η ανάλυση δεδομένων μεγάλου όγκου μπορεί να μην είναι πάντα εφικτή. Το ΤΥΠ βρίσκεται σε στενή επαφή με το ΓΚΗΕ.

Επιπλέον, οι φορείς εκμετάλλευσης κρίσιμων υποδομών στον τομέα των ηλεκτρονικών επικοινωνιών έχουν συγκεκριμένες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών που καλύπτουν τη διαθεσιμότητα, τις κυβερνοεπιθέσεις, τα μέτρα πρόληψης και μετριασμού. Οι φορείς εκμετάλλευσης υπόκεινται επίσης σε υποχρεώσεις υποβολής εκθέσεων σχετικά με συμβάντα που επηρεάζουν τη διαθεσιμότητα των δικτύων και των υπηρεσιών, καθώς και παραβιάσεις δεδομένων.

Σύμφωνα με τις κυπριακές αρχές, απαιτούνται περαιτέρω προσπάθειες για να διασφαλιστεί ότι οι φορείς εκμετάλλευσης παρέχουν στην αστυνομία όλα τα απαραίτητα στοιχεία, όπως διευθύνσεις IP και εργαλεία φιλτραρίσματος, και περιορίζουν την πρόσβαση σε παράνομο περιεχόμενο και την πρόσβαση σε άλλα στοιχεία κατά τη διάρκεια ερευνών, κ.λπ.
Οι προσπάθειες επικεντρώνονται επίσης στις προφυλάξεις του δημόσιου και ιδιωτικού απορρήτου των τραπεζών. Ωστόσο, οι τράπεζες και ο χρηματοπιστωτικός τομέας δεν υπόκεινται σε καμία γενική υποχρέωση να καταγγέλλουν αδικήματα απάτης με κάρτες ή πλαστογραφίας. Αυτό μπορεί να οφείλεται στον χαμηλό αριθμό περιπτώσεων που έχουν εντοπιστεί. Σύμφωνα με τα στατιστικά στοιχεία που έχει δώσει το ΓΚΗΕ για σοβαρές περιπτώσεις που αφορούν διαδικτυακή απάτη, 36 περιπτώσεις καταγράφηκαν το 2013, 52 το 2014 και 64 το 2015 (έως τον Νοέμβριο του 2015). Η απάτη με πιστωτικές κάρτες βρίσκεται σε πολύ χαμηλό επίπεδο, με μόνον 3 περιπτώσεις για το 2015 (έως τον Νοέμβριο του 2015). Ωστόσο, το ΓΚΗΕ έχει παρατηρήσει έναν αυξανόμενο αριθμό τέτοιων περιπτώσεων από χρόνο σε χρόνο.

Σύμφωνα με την τελευταία ποσοτική έκθεση της Ευρωπόλ για το έγκλημα στον κυβερνοχώρο για το τρίτο τρίμηνο του 2015, οι 5 δημοφιλέστερες απειλές κακόβουλου λογισμικού ήταν οι ακόλουθες: Conficker, Brontok, Ammyy, Gamarue και Scar. Η τελευταία είναι ένας ιός Trojan που ανακατευθύνει την πλοήγηση του φυλλομετρητή από ορισμένους διαδικτυακούς χρηματοπιστωτικούς ιστοτόπους σε άλλη διεύθυνση IP και ο εξυπηρετητής και η σελίδα προορισμού μπορούν να φιλοξενούν σελίδα εισόδου απομίμησης με σκοπό την απόσπαση των στοιχείων που εισάγει ο χρήστης.

6.2. Ενέργειες κατά της παιδικής πορνογραφίας και της σεξουαλικής κακοποίησης στο Διαδίκτυο

6.2.1. Βάσεις δεδομένων για την ταυτοποίηση των θυμάτων και μέτρα για την αποφυγή νέας θυματοποίησης

Η Κύπρος χρησιμοποιεί το λογισμικό «NetClean» για να ταυτοποιήσει θύματα παιδικής πορνογραφίας.
Εάν εικόνες/βίντεο δεν έχουν διαγραφεί, μια οντότητα διαπράττει αδίκημα όπως ορίζεται στο άρθρο 30 του νόμου 91(I)/2014. Το άρθρο αυτό ορίζει ότι οποιοσδήποτε παραλείπει να καταγγείλει περίπτωση παιδικής πορνογραφίας που περιέρχεται σε γνώση του διαπράττει αδίκημα και υπόκειται σε ποινή φυλάκισης που δεν υπερβαίνει τα δεκαπέντε (15) έτη.
Δυνάμει των διατάξεων του άρθρου 11(3) (α) του ίδιου νόμου, πάροχοι Διαδικτύου οι οποίοι προσφέρουν υπηρεσίες ή πρόσβαση στο Διαδίκτυο εντός του εδάφους της Δημοκρατίας υπέχουν υποχρέωση όπως, όταν αποκτήσουν γνώση, λάβουν άμεσα τα κατάλληλα μέτρα για τη διακοπή της πρόσβασης από τους χρήστες του Διαδικτύου στο εν λόγω υλικό. Εάν ο πάροχος Διαδικτύου δεν διαγράψει το εν λόγω υλικό ή δεν διακόψει την πρόσβαση σε αυτό, διαπράττει αδίκημα και τιμωρείται με ποινή φυλάκισης που δεν υπερβαίνει τα τρία (3) έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 170.000 ευρώ ή και με τις δύο ποινές.

6.2.2. Μέτρα για την αντιμετώπιση της σεξουαλικής εκμετάλλευσης/κακοποίησης μέσω του Διαδικτύου, της ανταλλαγής SMS σεξουαλικού περιεχομένου (sexting) και του κυβερνοεκφοβισμού

Η σεξουαλική εκμετάλλευση/κακοποίηση μέσω του Διαδικτύου, η ανταλλαγή SMS σεξουαλικού περιεχομένου (sexting) και ο κυβερνοεκφοβισμός αντιμετωπίζονται με δραστηριότητες γενικού περιεχομένου και εκπαιδευτικές δραστηριότητες.

Όσον αφορά τον κυβερνοεκφοβισμό, η Κύπρος υπέβαλε δύο προτάσεις για ευρωπαϊκή χρηματοδότηση στο πλαίσιο της πρόσκλησης υποβολής προτάσεων του προγράμματος Daphne με στόχο τη διεξοδικότερη αντιμετώπιση του θέματος.

6.2.3. Προληπτικές ενέργειες κατά του σεξουαλικού τουρισμού, των πορνογραφικών παραστάσεων με συμμετοχή παιδιών κ.λπ.

Σύμφωνα με το άρθρο 10(2) του νόμου του 2014 για την πρόληψη και καταπολέμηση της σεξουαλικής κακοποίησης και σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας, όποιος διοργανώνει ταξίδια με σκοπό τη διάπραξη οποιασδήποτε μορφής σεξουαλικής εκμετάλλευσης ή/και σεξουαλικής κακοποίησης παιδιών είναι ένοχος κακουργήματος. Το εν λόγω άρθρο προβλέπει επίσης ποινές φυλάκισης που δεν υπερβαίνουν τα 10 έτη.

Επιπλέον, στις 15/04/2014 η Κύπρος θέσπισε ένα αναθεωρημένο νομικό πλαίσιο που διέπει την πρόληψη, την καταπολέμηση της εμπορίας και της εκμετάλλευσης προσώπων και την προστασία των θυμάτων (νόμος 60(Ι)/2014).

Κανένα ειδικό μέτρο δεν έχει αναπτυχθεί για την αντιμετώπιση των πορνογραφικών παραστάσεων με συμμετοχή παιδιών που πραγματοποιούνται μέσω του Διαδικτύου σε πραγματικό χρόνο.

Μέσω του προγράμματος ασφαλούς Διαδικτύου που αποτελεί μέρος της διευκόλυνσης «Συνδέοντας την Ευρώπη» και ειδικότερα του έργου *CyberEthics* που χρηματοδοτείται από τον Εκτελεστικό Οργανισμό Καινοτομίας και Δικτύων (ΙΝΕΑ) της Ευρωπαϊκής Επιτροπής, παρέχονται μια γραμμή βοήθειας και μια γραμμή καταγγελιών. Η γραμμή βοήθειας και η γραμμή καταγγελιών εξυπηρετούνται από την Παγκύπρια συντονιστική επιτροπή για την προστασία και την ευημερία των παιδιών (ΠΣΕΠΕΠ) που είναι εταίρος του έργου *CyberEthics*, μολονότι από τον Ιανουάριο του 2015 στην τελευταία σύμβαση του έργου, το Ινστιτούτο Νευροεπιστήμης και Τεχνολογίας Κύπρου, ένας μη κυβερνητικός οργανισμός, εξυπηρετεί τις δύο γραμμές. Με τη λήξη της τρέχουσας σύμβασης τον Ιούνιο του 2016, εκτιμάται ότι το Υπουργείο Παιδείας και Πολιτισμού (αξιοποιώντας τις υπηρεσίες εκπαιδευτικής ψυχολογίας που διαθέτει) μπορεί να υποστηρίξει τη γραμμή βοήθειας και τη γραμμή καταγγελιών.

Περιεχόμενο και εργαλεία έχουν αναπτυχθεί και διαρκώς επικαιροποιούνται και εμπλουτίζονται όσον αφορά την ασφαλή χρήση του Διαδικτύου, μαζί με εκπαιδευτικά προγράμματα για μαθητές, εκπαιδευτικούς και γονείς. Όλο το περιεχόμενο διατίθεται με άδεια Creative Commons στην πύλη του Παιδαγωγικού Ινστιτούτου Κύπρου στη διεύθυνση www.pi.ac.cy/internetsafety, και ένα εκπαιδευτικό πακέτο έχει διανεμηθεί σε όλα τα σχολεία (διατίθεται επίσης σε ηλεκτρονική μορφή στη διεύθυνση www.pi.ac.cy/InternetSafety/eSafeSchool.html). Ταυτόχρονα, περιεχόμενο που παράγεται από μαθητές και εκπαιδευτικούς μέσω των διαφόρων προγραμμάτων ασφαλούς Διαδικτύου ανταλλάσσεται διαδικτυακά, όπως τα σύντομα βίντεο που παράγουν μαθητές για τον ετήσιο σχολικό διαγωνισμό και το υλικό και τα εργαλεία που παράγουν οι Μικροί εκπαιδευτές για το Διαδίκτυο[13].

Το Υπουργείο Παιδείας και Πολιτισμού συνεργάζεται στενά με άλλους οργανισμούς και προωθεί υλικό και εργαλεία που παράγουν εταίροι, όπως η Microsoft, το Γραφείο επιτρόπου ρυθμίσεως ηλεκτρονικών επικοινωνιών και ταχυδρομείων (ΓΕΡΗΕΤ), ο μη κερδοσκοπικός οργανισμός CNTI, η Αρχή Τηλεπικοινωνιών Κύπρου, ο τηλεπικοινωνιακός πάροχος MTN, κ.λπ.
Το περιεχόμενο και τα εργαλεία τονίζουν την κριτική και υπεύθυνη χρήση του Διαδικτύου με σκοπό την ασφάλεια στο Διαδίκτυο, ενώ ταυτόχρονα στοχεύουν σε κάθε διαδικτυακή συμπεριφορά των μαθητών που θα μπορούσε να είναι παράνομη και επιζήμια. Προχωρώντας ένα βήμα περαιτέρω και προσεγγίζοντας τους μαθητές ως θύματα ή πρωταγωνιστές, το περιεχόμενο και τα εργαλεία στοχεύουν στον ρόλο των μαθητών ως μαρτύρων με σκοπό την πρόληψη ή/και την καταγγελία εγκλημάτων στον κυβερνοχώρο.

6.2.4. Φορείς και μέτρα κατά ιστοτόπων που περιέχουν ή διαδίδουν παιδική πορνογραφία

Το ΓΚΗΕ ασχολείται με την παιδική πορνογραφία. Είναι αρμόδιο για τη διερεύνηση σοβαρών εγκλημάτων που διαπράττονται μέσω του Διαδικτύου και αδικημάτων που σχετίζονται με ηλεκτρονικούς υπολογιστές, καθώς και για τη διενέργεια αναζητήσεων μέσω του Διαδικτύου σε σχέση με τη διανομή υλικού παιδικής πορνογραφίας κατά παράβαση των νόμων 22(ΙΙΙ)/2004 και 91(Ι)/2014.

[13] www.pi.ac.cy/InternetSafety/drastiriotites_diagonismoi.html and www.pi.ac.cy/InternetSafety/YoungCoaches.html

Κύρια αρμοδιότητα του ΓΚΗΕ είναι η διερεύνηση περιπτώσεων παιδικής πορνογραφίας και ηλεκτρονικής πειρατείας, καθώς και

- η παρακολούθηση των υποθέσεων που μπορεί να είναι υπό διερεύνηση από άλλα τμήματα και συνδέονται με εγκλήματα σχετιζόμενα με το Διαδίκτυο,
- η συνεργασία με ερευνητές από άλλα τμήματα,
- η συνεργασία με αρμόδιους υπαλλήλους από άλλους οργανισμούς,
- η διοργάνωση εκπαιδευτικών σεμιναρίων,
- η κατάρτιση στατιστικών εκθέσεων,
- η συμμετοχή σε εκδηλώσεις και διαλέξεις,
- η ενημέρωση σχετικά με τις τελευταίες τεχνολογικές εξελίξεις στον εν λόγω τομέα.

Το ΓΚΗΕ διαθέτει 5 ερευνητές που εργάζονται με βάρδιες (0700-1900) και δύο μέλη διοικητικού προσωπικού.

Σύμφωνα με τις διατάξεις του άρθρου 11 του νόμου 91(I)/2014, η αστυνομία και τα δικαστήρια εξουσιοδοτούνται να παρεμποδίσουν την πρόσβαση/να αφαιρέσουν περιεχόμενο ή/και να αποσύρουν ιστοσελίδες. Στην πράξη, αφού ενημερωθεί σχετικά με την ύπαρξη υλικού που αφορά τη σεξουαλική κακοποίηση παιδιού, το ΓΚΗΕ προβαίνει σε εξέταση του υλικού. Κατόπιν επιβεβαίωσης ότι το υλικό αφορά τη σεξουαλική εκμετάλλευση παιδιού, το ΓΚΗΕ αποστέλλει αμέσως την πληροφορία μέσω ηλεκτρονικού ταχυδρομείου σε όλους τους παρόχους υπηρεσιών Διαδικτύου της Κύπρου, προκειμένου να διακοπεί η πρόσβαση και ταυτόχρονα τους παρέχει αρχεία καταγραφής και άλλες πληροφορίες. Δεν υπάρχει αυτοματοποιημένη διαδικασία που ακολουθείται για την επικοινωνία μεταξύ της αστυνομίας και των παρόχων υπηρεσιών Διαδικτύου.

Ωστόσο, δυνάμει των διατάξεων του άρθρου 11(3) (α) του νόμου 91(I)/2014, πάροχοι Διαδικτύου οι οποίοι προσφέρουν υπηρεσίες ή πρόσβαση στο Διαδίκτυο εντός του εδάφους της Δημοκρατίας υπέχουν υποχρέωση όπως, όταν αποκτήσουν γνώση, λάβουν άμεσα τα κατάλληλα μέτρα για τη διακοπή της πρόσβασης από τους χρήστες του Διαδικτύου στο εν λόγω υλικό (υλικό παιδικής πορνογραφίας). Εάν ο πάροχος Διαδικτύου δεν διαγράψει το εν λόγω υλικό ή δεν διακόψει την πρόσβαση σε αυτό, διαπράττει αδίκημα για το οποίο τιμωρείται με ποινή φυλάκισης που δεν υπερβαίνει τα τρία (3) έτη ή με χρηματική ποινή που δεν υπερβαίνει τα 170.000 ευρώ ή και με τις δύο ποινές.
Ορισμένοι πάροχοι υπηρεσιών Διαδικτύου της Κύπρου χρησιμοποιούν εξειδικευμένα φίλτρα, όπως το Clean Field, προκειμένου να φιλτράρουν ιστοτόπους για υλικό παιδικής πορνογραφίας.

Εάν το υλικό φιλοξενείται σε χώρα εκτός Κύπρου, οι αρχές επιβολής του νόμου ενημερώνονται μέσω της Ευρωπόλ ή/και της Interpol για να μπορέσουν να ενεργήσουν ανάλογα. Ταυτόχρονα, οι πάροχοι υπηρεσιών Διαδικτύου της Κύπρου ενημερώνονται μέσω ηλεκτρονικού ταχυδρομείου προκειμένου να μπορέσει να διακοπεί η πρόσβαση στο εν λόγω υλικό από τους χρήστες της Κύπρου.

6.3. Διαδικτυακή απάτη με κάρτες

6.3.1. Υποβολή καταγγελιών μέσω Διαδικτύου

Οι πολίτες και οι εταιρείες καταγγέλλουν αδικήματα διαδικτυακής απάτης με κάρτες στην αστυνομία, εκτός των περιπτώσεων που αφορούν πολύ μικρά χρηματικά ποσά. Στις περιπτώσεις αυτές προτιμούν να συνεργάζονται με τις τράπεζες για να επιλύσουν το πρόβλημα.

Βάσει του Ν. 112(Ι)/2004 όλοι οι πάροχοι υπηρεσιών Διαδικτύου υπόκεινται στην εποπτεία του ΓΕΡΗΕΤ. Επιπλέον, ο Ν. 187(Ι)/2007 υποχρεώνει τους παρόχους υπηρεσιών Διαδικτύου να τηρούν δεδομένα κίνησης και ταυτοποίησης χρηστών για περίοδο έξι μηνών. Τέλος, σύμφωνα με το άρθρο 11 του Ν. 91(Ι)/2014, η αστυνομία και τα δικαστήρια μπορούν να διατάσσουν τους παρόχους υπηρεσιών Διαδικτύου να καταργούν την πρόσβαση σε / αφαιρούν περιεχόμενο / αποσύρουν ιστοσελίδες.

6.3.2. Ρόλος του ιδιωτικού τομέα

Η συνεργασία με τις τράπεζες και τον ιδιωτικό τομέα είναι επαρκής, ιδιαίτερα σε ό,τι αφορά την κοινοποίηση νέων εργαλείων πληρωμής. Οι τράπεζες καταβάλλουν διαρκείς προσπάθειες για τη βελτίωση της ασφάλειας και την ενίσχυση της διαδικασίας έγκρισης των διαδικτυακών συναλλαγών.

Το ΓΕΡΗΕΤ έχει επιβάλει αρκετές υποχρεώσεις στους παρόχους ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των παρόχων υπηρεσιών Διαδικτύου στον τομέα της ασφάλειας δικτύων και πληροφοριών, και σε ό,τι αφορά τη συνεργασία και την παροχή πληροφοριών για συναφή ζητήματα στις υπηρεσίες έκτακτης ανάγκης και την αστυνομία. Το ΓΕΡΗΕΤ διευκολύνει τις συνομιλίες μεταξύ των φορέων εκμετάλλευσης και της αστυνομίας για τη βελτίωση της συνεργασίας τους στο πλαίσιο της παροχής πληροφοριών, της ταυτοποίησης των παραβατών, της φραγής πρόσβασης σε ιστοτόπους με παράνομο περιεχόμενο κ.λπ. Το ΓΕΡΗΕΤ δύναται να επιβάλει όρους και προϋποθέσεις που καθορίζουν οι αρμόδιες αρχές, συμπεριλαμβανομένης της αστυνομίας, για συναφή ζητήματα, όπως το έγκλημα στον κυβερνοχώρο.

Ο ρόλος του χρηματοοικονομικού κλάδου είναι καθοριστικής σημασίας για την κυπριακή οικονομία. Σύμφωνα με ευρέως διαθέσιμες πηγές, ο κλάδος αυτός παράγει περίπου το 45% του ΑΕγχΠ της χώρας. Στο πλαίσιο αυτού του κλάδου αιτιολογούνται περίπλοκες σχέσεις μεταξύ των δημόσιων αρχών και των χρηματοπιστωτικών ιδρυμάτων, καθώς και η μάλλον συναινετική και όχι τόσο επιβλητική προσέγγιση της κυβέρνησης ως προς τον κλάδο αυτό. Επομένως, κατά την άποψη των αξιολογητών, θα πρέπει να επιτευχθεί στενή συνεργασία μεταξύ των φορέων αυτών, προκειμένου να βελτιωθεί η αποτελεσματικότητα της πολιτικής για την καταπολέμηση του κυβερνοεγκλήματος, ιδίως σε ό,τι αφορά τις απάτες και τις επιθέσεις στον κυβερνοχώρο.

6.4. Συμπεράσματα

- Η αστυνομία συνεργάζεται με ιδιωτικές εταιρείες που καταγγέλλουν κυβερνοεπιθέσεις με σκοπό τη συμβολή στην επίλυση των προβλημάτων και τη διερεύνηση των αδικημάτων. Επιπλέον, διατηρεί στενές επαφές με το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) για την πρόληψη των κυβερνοεπιθέσεων, καθώς και για να λαμβάνει αναλύσεις δεδομένων ανάλογα με την υπόθεση.

- Η Κύπρος συγκρότησε κρατική ομάδα ανταπόκρισης σε συμβάντα που σχετίζονται με την πληροφορική (CIRT), η οποία ήδη λειτουργεί. Το ΤΥΠ δημιούργησε την τεχνική υποδομή και τη διαδικτυακή πύλη της CIRT. Ωστόσο, δεν λειτουργεί ως εθνική CERT (ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική) για την προστασία ιδιωτικών εταιριών και πολιτών, με την παροχή υπηρεσιών άμεσης ανταπόκρισης σε θύματα κυβερνοεπιθέσεων, τη δημοσίευση ειδοποιήσεων για διαδικτυακές απειλές ή την παροχή άλλων πληροφοριών για τη βελτίωση της ασφάλειας των υπολογιστών και των δικτύων. Ως εκ τούτου, θα πρέπει να εξεταστεί το ενδεχόμενο σύστασης εθνικής CERT, ως κεντρικού φορέα πρόληψης των απειλών για την ασφάλεια των δημόσιων συστημάτων πληροφοριών, και ενίσχυσης της ανθεκτικότητας του συστήματος κυβερνοασφάλειας της Κύπρου.

- Οι φορείς εκμετάλλευσης κρίσιμων υποδομών στον τομέα των ηλεκτρονικών επικοινωνιών έχουν συγκεκριμένες νομικές και κανονιστικές υποχρεώσεις σχετικά με την ασφάλεια δικτύων και πληροφοριών. Οι υποχρεώσεις αυτές αφορούν τις κυβερνοεπιθέσεις και τα μέτρα πρόληψης και μετριασμού. Οι φορείς εκμετάλλευσης υποχρεούνται επίσης να αναφέρουν συμβάντα που επηρεάζουν τη διαθεσιμότητα των δικτύων και των υπηρεσιών, καθώς και παραβιάσεις δεδομένων. Εντούτοις, σύμφωνα με τις κυπριακές αρχές, απαιτούνται επιπλέον προσπάθειες για να διασφαλιστεί ότι οι φορείς εκμετάλλευσης παρέχουν στην αστυνομία όλα τα απαραίτητα στοιχεία, όπως διευθύνσεις IP, εργαλεία φιλτραρίσματος, περιορισμός πρόσβασης σε παράνομο περιεχόμενο και πρόσβαση σε άλλα στοιχεία κατά τη διάρκεια ερευνών κ.λπ.

- Οι αρχές που μπορούν να συντονίσουν τη φραγή πρόσβασης/αφαίρεση περιεχομένου/απόσυρση ιστοσελίδων είναι τα δικαστήρια και η αστυνομία. Ωστόσο, δεν υπάρχει νομική διάταξη που επιβάλλει στους παρόχους υπηρεσιών Διαδικτύου να χρησιμοποιούν φίλτρα για την παιδική πορνογραφία στο Διαδίκτυο [άρθρο 11 του Ν.91(Ι)/2014].

- Η Κύπρος διαθέτει εξαιρετικό σύστημα για την εκπαίδευση των παιδιών σε θέματα κυβερνοεγκλήματος, με επαγγελματίες εξαιρετικά αφοσιωμένους στο έργο τους, που χρησιμοποιούν σύγχρονες τεχνικές, όπως τη διδασκαλία παιδιών από άλλα παιδιά (Μικροί εκπαιδευτές). Κατά την άποψη των αξιολογητών, το σύστημα αυτό θα πρέπει να θεωρηθεί παράδειγμα βέλτιστης πρακτικής.

- Σύμφωνα με τα στατιστικά στοιχεία για το πλήθος εγκλημάτων στον κυβερνοχώρο που έχουν αναφερθεί στην αστυνομία ή από την αστυνομία, η πλειονότητα των υποθέσεων αφορούν την κακοποίηση παιδιών στο Διαδίκτυο. Οι περιπτώσεις κυβερνοεπιθέσεων και απάτης με κάρτες πληρωμών που έχουν αναφερθεί είναι πολύ λιγότερες. Λαμβάνοντας υπόψη αυτό το γεγονός, οι αξιολογητές κρίνουν ότι η κατάσταση στην Κύπρο δεν αντικατοπτρίζει πλήρως τις τρέχουσες απειλές που συνδέονται με το έγκλημα στον κυβερνοχώρο.

- Η πολύπλευρη συνεργασία μεταξύ των δημόσιων αρχών και του χρηματοοικονομικού κλάδου θα μπορούσε να ωφελήσει και τις δύο πλευρές, αυξάνοντας σημαντικά το επίπεδο της κυβερνοασφάλειας στην Κύπρο. Επί του παρόντος, οι δημόσιες αρχές δεν συνεργάζονται απευθείας με τις τράπεζες και άλλα χρηματοπιστωτικά ιδρύματα. Η αλληλεπίδραση μεταξύ αυτών των φορέων επαφίεται στην κεντρική τράπεζα, η οποία ενεργεί ως διαμεσολαβητής. Οι αξιολογητές πιστεύουν πως η προσέγγιση αυτή φαίνεται να υπονομεύει την αποτελεσματικότητα της συνεργασίας, ειδικά στην περίπτωση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

- Κατά συνέπεια, κατά την άποψη των αξιολογητών, η Κύπρος θα πρέπει να ενθαρρύνει τη συνεργασία μεταξύ των αρχών επιβολής του νόμου, των εισαγγελέων και του ιδιωτικού τομέα, ιδίως των τραπεζών, για να καθιερώσει βιώσιμο μηχανισμό αναφοράς των κυβερνοεπιθέσεων που πλήττουν τόσο τους πολίτες όσο και τον ιδιωτικό τομέα.

- Μία από τις προτεραιότητες της αξιολόγησης απειλών όσον αφορά το σοβαρό και οργανωμένο έγκλημα (SOCTA) του 2013 είναι το έγκλημα στον κυβερνοχώρο που καλύπτει τρεις επιμέρους προτεραιότητες: σεξουαλική κακοποίηση παιδιών, απάτη με κάρτες και κυβερνοεπιθέσεις. Η Κύπρος συμμετέχει στις εργασίες για την επιμέρους προτεραιότητα που αφορά το επιχειρησιακό σχέδιο δράσης της EMPACT για τη σεξουαλική κακοποίηση παιδιών. Εξετάζει, ωστόσο, το ενδεχόμενο να προσχωρήσει και στην επιμέρους προτεραιότητα για τις επιθέσεις στον κυβερνοχώρο. Σε ό,τι αφορά τις δράσεις που θα υλοποιηθούν το 2016, δίδεται έμφαση στη στενή συνεργασία μεταξύ των υπηρεσιών επιβολής του νόμου, των CERT, της βιομηχανίας και του ακαδημαϊκού τομέα, και υπάρχουν ορισμένες προσαρμοσμένες δραστηριότητες για την προώθηση των βέλτιστων πρακτικών στον τομέα ανταλλαγής γενικών πληροφοριών και πληροφοριών ασφαλείας μεταξύ των τραπεζών και των υπηρεσιών επιβολής του νόμου. Σύμφωνα με τις πληροφορίες που διαβιβάστηκαν στην ομάδα αξιολόγησης, το ΓΚΗΕ συμμετέχει στις δράσεις της EMPACT για τις κυβερνοεπιθέσεις από την 1η Ιανουαρίου 2016.

7. ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ

7.1. Συνεργασία με οργανισμούς της ΕΕ

7.1.1. Επίσημες απαιτήσεις όσον αφορά τη συνεργασία με την Ευρωπόλ/EC3, την Eurojust, τον ENISA

Ο Ν. 102(Ι)/2011 ρυθμίζει όλες τις επίσημες απαιτήσεις και τις ειδικές διαδικασίες όσον αφορά τη συνεργασία με την Ευρωπόλ.

Ο Ν. 112(Ι)/2004, όπως τροποποιήθηκε, δεν περιλαμβάνει ειδικές διαδικασίες σχετικά με τις υποθέσεις εγκλήματος στον κυβερνοχώρο. Περιλαμβάνει, όμως, γενικές διατάξεις για την εκπροσώπηση της Κύπρου σε διεθνείς οργανισμούς, όπως ο ENISA μέσω του ΓΕΡΗΕΤ, η ΔΕΤ, το ICANN κ.λπ. ανάλογα με τις αρμοδιότητες.

7.1.2. Αξιολόγηση της συνεργασίας με την Ευρωπόλ/EC3, την Eurojust και τον ENISA

Οι κυπριακές αρχές δίδουν μεγάλη σημασία στον ρόλο και τη συμβολή της Ευρωπόλ/EC3, της Eurojust και του ENISA σε ό,τι αφορά την αντιμετώπιση της ασφάλειας και του εγκλήματος στον κυβερνοχώρο λόγω του χαρακτήρα αυτών των παραβάσεων. Πιστεύουν επίσης ότι μπορούν να υποστηρίξουν ενεργά την Ευρωπαϊκή Επιτροπή και τα κράτη μέλη στο πλαίσιο της διεθνούς συνεργασίας με βάση την εμπειρία και την εμπειρογνωμοσύνη τους στον τομέα τους. Μπορούν να ενεργήσουν ως σύμβουλοι και να συμμετάσχουν σε συναφείς δραστηριότητες για την υποστήριξη των αρμόδιων ευρωπαϊκών αρχών.

Η συμβολή της Ευρωπόλ θεωρείται καίριας σημασίας για τη διερεύνηση του εγκλήματος στον κυβερνοχώρο. Η υπόθεση Darkode αποτελεί ένα πρόσφατο παράδειγμα της στενής συνεργασίας μεταξύ της Αστυνομίας Κύπρου και του EC3. Κατά τη διάρκεια αυτής της επιχείρησης, η Αστυνομία Κύπρου εντόπισε και ανέκρινε έναν ύποπτο στην Κύπρο, ο οποίος είχε σχέση με την υπόθεση, ενώ υπήρχε άμεση επικοινωνία με όλα τα εμπλεκόμενα μέρη, τα κράτη μέλη και τις τρίτες χώρες. Κατόπιν ανάλυσης, όλες οι δέσμες πληροφοριών κοινοποιήθηκαν μέσω του EC3, ενώ η διαδικασία ανταλλαγής πληροφοριών με το EC3 βρίσκεται ακόμη σε εξέλιξη. Η υπόθεση Darkode θεωρείται γενικά μια επιτυχής διεθνής επιχείρηση. Η επιχείρηση Daylight σχετικά με την παιδική πορνογραφία, που πραγματοποιήθηκε στο πλαίσιο της Δράσης 5.2 του έργου EMPACT CSE, συνιστά άλλο ένα παράδειγμα συνεργασίας μεταξύ της Αστυνομίας Κύπρου και της Ευρωπόλ. Η συνεργασία μεταξύ της Αστυνομίας Κύπρου και του EC3 είναι υψίστης σημασίας και η Αστυνομία Κύπρου είναι ικανοποιημένη από το επίπεδο της συνεργασίας.

Το ΓΕΡΗΕΤ εκπροσωπεί την Κύπρο στο Διοικητικό Συμβούλιο και άλλες επιτροπές του ENISA και είναι αρμόδιο για τη συνεργασία με τον Οργανισμό για θέματα που αφορούν την ασφάλεια και τον κυβερνοχώρο. Συνεργάζεται με τον ENISA και έχει ήδη λάβει γενική συνδρομή σε συναφή θέματα. Παρόλο που δεν έχει ακόμη υπάρξει συνεργασία για συγκεκριμένη υπόθεση, το ΓΕΡΗΕΤ επιδιώκει την ενίσχυση της επιχειρησιακής συνεργασίας με τον ENISA στο εγγύς μέλλον σχετικά με συγκεκριμένα ζητήματα, όπως ο χειρισμός επιθέσεων στον κυβερνοχώρο και άλλων συμβάντων που επηρεάζουν τα δίκτυα και τα δεδομένα προσωπικού χαρακτήρα.

Το ΤΥΠ και το ΓΕΡΗΕΤ είχαν συνεργαστεί με τον ENISA για τη δημιουργία της ομάδας άμεσης ανταπόκρισης για συμβάντα που σχετίζονται με την ασφάλεια δικτύων και πληροφοριών της Κύπρου (Cyprus GOVCIRT).
Επιπλέον, ο ENISA παρείχε συνδρομή στις κυπριακές αρχές για τη διενέργεια της εθνικής αξιολόγησης κινδύνων στον κυβερνοχώρο, η οποία βρίσκεται σε εξέλιξη. Το ΓΕΡΗΕΤ θεωρεί πολύ θετική τη δραστηριοποίηση του ENISA στους τομείς της ασφάλειας και της κυβερνοασφάλειας, συμπεριλαμβανομένης της συνεργασίας για το έγκλημα στον κυβερνοχώρο. Υπογράμμισε, ωστόσο, ότι ο ENISA θα πρέπει να επιδιώξει την ενεργό συνεργασία με την Ευρωπόλ/EC3 και την Eurojust, όπου αυτό είναι αναγκαίο, υποστηρίζοντας τις αντίστοιχες δραστηριότητές τους και αποφεύγοντας τις επικαλύψεις.

Ο επικεφαλής του ΓΚΗΕ συμμετέχει στην EUCTF (Ειδική ομάδα δίωξης ηλεκτρονικού εγκλήματος) της Ευρωπόλ. Επίσης, ένα μέλος του ΓΚΗΕ συμμετέχει στο EMPACT CSE.

7.1.3. Επιχειρησιακή συμμετοχή σε κοινές ομάδες ερευνών και κυβερνοπεριπόλους

Η Κύπρος δεν έχει συμμετάσχει ακόμη σε κοινές ομάδες ερευνών. Το ΓΕΡΗΕΤ έχει λάβει μέρος μόνο στις ασκήσεις στον κυβερνοχώρο για την ασφάλεια δικτύων και πληροφοριών.

7.2. Συνεργασία μεταξύ των κυπριακών αρχών και της Ιντερπόλ

Ο δίαυλος που χρησιμοποιείται για την ανταλλαγή επιχειρησιακών πληροφοριών και αιτήσεων με τρίτες χώρες είναι η Ιντερπόλ. Επιπλέον, τα τελευταία τέσσερα χρόνια το ΓΚΗΕ χρησιμοποιεί τη βάση δεδομένων ICSE για την ταυτοποίηση των θυμάτων.

7.3. Συνεργασία με τρίτα κράτη

Η συνεργασία με τρίτα κράτη για τη διερεύνηση αστυνομικών υποθέσεων βασίζεται σε διμερείς και πολυμερείς συμφωνίες. Στον τομέα του εγκλήματος στον κυβερνοχώρο και ειδικότερα σε ό,τι αφορά τις έρευνες και την ευαισθητοποίηση για την παιδική πορνογραφία, το ΓΚΗΕ έχει συμμετάσχει σε διάφορες πρωτοβουλίες, όπως οι εξής:

- Διεθνής επιχειρησιακή ομάδα «Αθώες εικόνες» (Innocent Images International Task Force - IIITF) ή Διεθνής επιχειρησιακή ομάδα για τα εγκλήματα βίας κατά των παιδιών (Violent Crimes Against Children International Task Force - VCACITF)·
- Παγκόσμια συμμαχία κατά της σεξουαλικής κακοποίησης των παιδιών στο Διαδίκτυο και
- Επιτροπή του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (TC-Y).

Επιπλέον, η Κύπρος έχει αξιοποιήσει τις επιχειρησιακές και στρατηγικές συμφωνίες που έχει υπογράψει η Europol/EC3 με τρίτες χώρες και άλλους φορείς. Στο πλαίσιο αυτών των συμφωνιών, η ανάλυση και η ανταλλαγή πληροφοριών σχετικά με το έγκλημα στον κυβερνοχώρο έχει επιταχυνθεί, με θετικά αποτελέσματα για τις σχετικές έρευνες. Υπάρχουν πολλά παραδείγματα επιτυχών επιχειρήσεων που πραγματοποιήθηκαν σε αυτό το πλαίσιο.

7.4. Συνεργασία με τον ιδιωτικό τομέα

Στην περίπτωση ιδιωτικών εταιριών με έδρα σε τρίτα κράτη, το ΓΚΗΕ υποβάλλει αίτηση απευθείας στο τοπικό παράρτημα που είναι αρμόδιο σύμφωνα με την εθνική νομοθεσία για την παροχή των ζητούμενων πληροφοριών. Εάν θεωρηθεί αναγκαίο, μπορεί να εκδοθεί ένταλμα έρευνας από το δικαστήριο για την αποτελεσματική διενέργεια της έρευνας.

Η Κύπρος καταβάλλει προσπάθειες για να ξεπεράσει τα εμπόδια στη διασυνοριακή συνεργασία στον ειδικό τομέα της διαδικτυακής απάτης με κάρτες ενισχύοντας τους διαύλους συνεργασίας της με άλλα κράτη μέλη.

7.5. Μέσα διεθνούς συνεργασίας

7.5.1. Αμοιβαία δικαστική συνδρομή

Ο Ν. 23(Ι)/2001 περί διεθνούς συνεργασίας σε ποινικά θέματα αποτελεί την εθνική νομοθεσία που εφαρμόζεται στις αιτήσεις αμοιβαίας δικαστικής συνδρομής (ΑΔΣ). Επιπλέον, η αμοιβαία δικαστική συνδρομή παρέχεται βάσει διμερών συμφωνιών και συμβάσεων, όπως η Ευρωπαϊκή Σύμβαση για την αμοιβαία αρωγή σε ποινικά θέματα (Ν.2(ΙΙΙ)/2000) και η Σύμβαση κατά του εγκλήματος μέσω του Διαδικτύου (Ν. 22(ΙΙΙ)/2004).

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως συνιστά την κεντρική αρχή για την παραλαβή και την αποστολή αιτήσεων αμοιβαίας δικαστικής συνδρομής. Για την απλούστευση και τη βελτίωση της διεθνούς συνεργασίας έχει συγκροτηθεί Μονάδα Διεθνούς Νομικής Συνεργασίας στο Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως. Η έγγραφη επιστολή της αίτησης πρέπει να αποστέλλεται με ηλεκτρονικό ταχυδρομείο, φαξ ή ταχυδρομικώς.

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως παραλαμβάνει εισερχόμενες αιτήσεις από το εξωτερικό και αποστέλλει αιτήσεις ΑΔΣ. Επίσης, αξιολογεί τις εισερχόμενες αιτήσεις και τις διαβιβάζει προς εκτέλεση στην αρμόδια δικαστική αρχή της Κύπρου. Σε ό,τι αφορά τις εξερχόμενες αιτήσεις, το Υπουργείο συγκεντρώνει τις παραληφθείσες σε εσωτερικό επίπεδο αιτήσεις και τις αποστέλλει στο εξωτερικό.

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως χρησιμοποιεί πολύ συχνά το ΕΔΔ, καθώς φαίνεται ότι είναι αρκετά αποτελεσματικό και συμβάλλει στην ταχεία και ομαλή συνεργασία μεταξύ των κρατών μελών. Χρησιμοποιεί, επίσης, την Eurojust για να λαμβάνει ταχείες απαντήσεις.

Η συνηθέστερη αιτιολογία των αιτήσεων ΑΔΣ αφορά τη συλλογή αποδεικτικών στοιχείων που οδηγούν σε έναν τελικό χρήστη. Οι επείγουσες αιτήσεις διεκπεραιώνονται κατά προτεραιότητα. Ανάλογα με τις ενέργειες που ζητούνται, ο χρόνος ανταπόκρισης ενδέχεται να ποικίλλει από αρκετούς μήνες έως περίοδο μεγαλύτερη του έτους.

Για τη διεκπεραίωση των αιτήσεων, το ΓΚΗΕ αναζητά πληροφορίες και αποδεικτικά στοιχεία σε σχέση με διευθύνσεις IP, την ημερομηνία και ώρα πρόσβασης, στοιχεία δημιουργίας, αρχεία καταγραφής (log files) ή άλλα δεδομένα σχετικά με την ταυτοποίηση των στοιχείων του τελικού χρήστη. Επιπλέον, εάν χρειαστεί, το ΓΚΗΕ ζητά έγγραφες δηλώσεις από διαχειριστές συστημάτων πληροφορικής.

Εάν παραστεί ανάγκη διατήρησης των δεδομένων πριν από την αποστολή της επίσημης αίτησης ΑΔΣ, το ΓΚΗΕ έρχεται σε επαφή με τη χώρα στην οποία απευθύνεται η αίτηση μέσω της Ιντερπόλ ή της Ευρωπόλ. Παράλληλα, βάσει της Σύμβασης της Βουδαπέστης το ΓΚΗΕ δύναται να ζητά ορισμένες πληροφορίες μέσω άμεσης επικοινωνίας ή μέσω της Ιντερπόλ. Επιπλέον, σε περιπτώσεις όπου ο διαχειριστής (hosting administrator) είναι σε θέση να συνεργαστεί, το ΓΚΗΕ μπορεί να υποβάλει απευθείας αίτηση σε εκείνον μέσω ηλεκτρονικού ταχυδρομείου ζητώντας τη διατήρηση των δεδομένων.

Το σημείο επαφής (επικεφαλής του ΓΚΗΕ) υπάγεται στον Διευθυντή του Γ΄ Τμήματος στο Αρχηγείο της Αστυνομίας και είναι υπεύθυνο για την εκτέλεση όλων των αιτήσεων που αφορούν το έγκλημα στον κυβερνοχώρο κατά τα οριζόμενα στην Αστυνομική Διάταξη 3/45. Το δεύτερο σημείο επαφής (ΚΕΓ Ιντερπόλ Λευκωσίας) ενεργεί βάσει οδηγιών της Διεύθυνσης Ευρωπαϊκής Ένωσης και Διεθνούς Αστυνομικής Συνεργασίας και δεν έχει εξουσιοδότηση για την εκτέλεση των αιτήσεων. Αντιθέτως, ο ρόλος του περιορίζεται στην αποστολή των αιτήσεων.
Στις περιπτώσεις που η αίτηση αποστέλλεται απευθείας στο σημείο επαφής (επικεφαλής του ΓΚΗΕ), αξιολογείται και στη συνέχεια εκτελείται. Η διαδικασία αυτή ακολουθείται όταν δεν απαιτείται αίτηση ΑΔΣ.

Μόλις εκτελεσθεί η αίτηση, ενημερώνεται το ΚΕΓ Λευκωσίας, απλά και μόνο για λόγους συντονισμού. Εάν απαιτείται αίτηση ΑΔΣ, ενημερώνεται το ΚΕΓ Λευκωσίας για να διαβιβάσει την επίσημη απάντηση στη χώρα από την οποία προήλθε η αίτηση. Κατά κανόνα, οι αιτήσεις που μπορούν να διεκπεραιωθούν χωρίς να απαιτείται συμφωνία αμοιβαίας δικαστικής συνδρομής είναι μόνον εκείνες για τις οποίες η αστυνομία διαθέτει το σύνολο των πληροφοριών και δεν απαιτείται υποβολή αίτησης στο δικαστήριο για την έγκριση της πρόσβασης στις ζητούμενες πληροφορίες.

Σε ό,τι αφορά τα στατιστικά στοιχεία για τον αριθμό αιτήσεων ΑΔΣ που έχουν παραληφθεί στον τομέα του εγκλήματος στον κυβερνοχώρο: Το 2014 ελήφθησαν 12 αιτήσεις και 6 το 2015.

Αναφέρθηκαν ορισμένα εμπόδια σχετικά με την ταχεία συνεργασία με τις ΗΠΑ. Οι εκπρόσωποι που συναντήθηκαν υπογράμμισαν ότι όσον αφορά τη διεθνή συνδρομή ο βασικότερος παράγοντας είναι η ομαλή και ταχεία συνεργασία με τις ΗΠΑ, καθώς πολλοί δημοφιλείς διακομιστές Διαδικτύου υπάγονται στη δικαιοδοσία τους. Εξέφρασαν παράπονα για την ποιότητα της συνεργασίας, ιδίως στον τομέα της διατήρησης δεδομένων και της κοινοποίησης διευθύνσεων IP κατόχων λογαριασμών στο Facebook και άλλα μέσα κοινωνικής δικτύωσης. Κατά την άποψη των αξιολογητών, η δυνατότητα πρόσβασης στις βάσεις δεδομένων των μέσων κοινωνικής δικτύωσης μέσω Διαδικτύου που προέρχονται από τις ΗΠΑ αποτελεί διαρκές πρόβλημα που αντιμετωπίζουν όλα τα κράτη μέλη.

7.5.2. Πράξεις αμοιβαίας αναγνώρισης

Η Κύπρος δεν έχει εφαρμόσει πράξεις αμοιβαίας αναγνώρισης για υποθέσεις εγκλημάτων στον κυβερνοχώρο.
Ωστόσο, έχει εφαρμοστεί η απόφαση-πλαίσιο 2003/577/ΔΕΥ, της 22ας Ιουλίου 2003, σχετικά με την εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων, στο πλαίσιο αιτήσεων που υπέβαλαν άλλα κράτη μέλη στις αρμόδιες αρχές της Κύπρου, ήτοι το Υπουργείο Δικαιοσύνης και Δημόσιας Τάξεως και η Μονάδα Καταπολέμησης Αδικημάτων Συγκάλυψης (ΜΟ.Κ.Α.Σ). Πράγματι, σε ορισμένες περιπτώσεις, αποφάσεις δέσμευσης που εκδόθηκαν σε άλλα κράτη μέλη καταχωρίστηκαν και εκτελέστηκαν στην Κύπρο σύμφωνα με τη διαδικασία που προβλέπει η ανωτέρω απόφαση-πλαίσιο.

7.5.3. Παράδοση/Έκδοση

Οι αξιόποινες πράξεις που αναφέρονται στην απόφαση-πλαίσιο για το ευρωπαϊκό ένταλμα σύλληψης επισύρουν ποινές και έκδοση σύμφωνα με την εθνική νομοθεσία. Στις αξιόποινες πράξεις που αφορούν το έγκλημα στον κυβερνοχώρο περιλαμβάνονται η σεξουαλική εκμετάλλευση παιδιών και η παιδική πορνογραφία, τα εγκλήματα σχετικά με ηλεκτρονικούς υπολογιστές, η παραχάραξη μέσων πληρωμής, ο ρατσισμός και η ξενοφοβία μέσω του Διαδικτύου.

Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως συνιστά την κεντρική αρχή για την παραλαβή, την αποστολή και τη λήψη αποφάσεων για αιτήσεις παράδοσης/έκδοσης. Οι επίσημες αιτήσεις έκδοσης πρέπει να αποστέλλονται είτε απευθείας είτε μέσω της διπλωματικής οδού.

Για τις αιτήσεις που αφορούν το έγκλημα στον κυβερνοχώρο, δεν χρειάζεται να τηρούνται συγκεκριμένες διαδικασίες ή προϋποθέσεις. Οι επείγουσες αιτήσεις διεκπεραιώνονται κατά προτεραιότητα.

Σε ό,τι αφορά τα στατιστικά στοιχεία, το 2014 εκδόθηκαν 12 ευρωπαϊκά εντάλματα σύλληψης για εγκλήματα στον κυβερνοχώρο. Το 2014, ελήφθη μία αίτηση έκδοσης για έγκλημα στον κυβερνοχώρο.

Επιπλέον, ελήφθη μία αίτηση έκδοσης από τις ΗΠΑ. Επιπλέον, ελήφθη μία αίτηση έκδοσης από τις ΗΠΑ, βάσει της Συμφωνίας Έκδοσης μεταξύ των Ηνωμένων Πολιτειών Αμερικής και της Κύπρου, η οποία υπεγράφη στις 17/6/1996, και της πράξης που αναφέρεται στο άρθρο 3 παράγραφος 2 της Συμφωνίας Έκδοσης μεταξύ των Ηνωμένων Πολιτειών Αμερικής και της ΕΕ, που υπεγράφη στις 15/6/2003, σχετικά με την εφαρμογή της Συμφωνίας Έκδοσης μεταξύ των ΗΠΑ και της Κύπρου με το σχετικό παράρτημα που υπεγράφη στις 20/1/2006.

7.6. Συμπεράσματα

- Οι νόμοι 102(I)/2011 και 112(I)/2004 ρυθμίζουν τις επίσημες απαιτήσεις για τη συνεργασία με την Ευρωπόλ, την Eurojust και τον ENISA. Ωστόσο, δεν περιλαμβάνουν ειδικές διαδικασίες σχετικά με τις υποθέσεις εγκλήματος στον κυβερνοχώρο.

- Η Κύπρος αναγνωρίζει την υποστήριξη που παρέχουν όλοι οι οργανισμοί της ΕΕ. Οι κυπριακές αρχές δίδουν μεγάλη σημασία στον ρόλο και τη συμβολή της Ευρωπόλ/EC3, της Eurojust και του ENISA σε ό,τι αφορά την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο λόγω του χαρακτήρα αυτών των παραβάσεων.

- Η Κύπρος δείχνει να συνεργάζεται στενά με τον ENISA και αξιοποιεί ευρέως τις υπηρεσίες που παρέχει η Ευρωπόλ σχετικά με το έγκλημα στον κυβερνοχώρο. Οι εκπρόσωποι τους οποίους συνάντησαν οι αξιολογητές, ιδίως από την αστυνομία, γνωρίζουν πολύ καλά τον ρόλο της Ευρωπόλ/EC3. Ωστόσο, η Eurojust φαίνεται να χρησιμοποιείται σε μικρότερο βαθμό.

- Η Κύπρος διαθέτει πολύ συγκεντρωτικό σύστημα δικαστικής συνεργασίας σε ποινικές υποθέσεις. Στο Υπουργείο Δικαιοσύνης και Δημοσίας Τάξης έχει ανατεθεί ο ρόλος της κεντρικής αρχής τόσο για ορισμένες πολυμερείς διεθνείς συμφωνίες στις οποίες έχει προσχωρήσει η Κύπρος όσο και για την εκτέλεση των αιτήσεων ΑΔΣ. Για την απλούστευση και τη βελτίωση της διεθνούς συνεργασίας έχει συγκροτηθεί Μονάδα Διεθνούς Νομικής Συνεργασίας στο Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως. Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως επεξεργάζεται όλες τις αιτήσεις δικαστικής συνεργασίας πριν σταλούν στις δικαστικές αρχές. Αξιολογεί όλες τις πτυχές κάθε αίτησης ή της εκτέλεσής της και, εάν χρειαστεί, διορθώνει τυχόν σφάλματα.

- Το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως χρησιμοποιεί πολύ συχνά το ΕΔΔ, το οποίο φαίνεται ότι είναι αρκετά αποτελεσματικό και συμβάλλει στην ταχεία και ομαλή συνεργασία μεταξύ των κρατών μελών. Χρησιμοποιεί, επίσης, την Eurojust για να λαμβάνει ταχείες απαντήσεις. Κατά την άποψη των αξιολογητών, η διαδικασία βάσει της οποίας το Υπουργείο Δικαιοσύνης και Δημόσιας Τάξεως χρησιμοποιεί το ΕΔΔ και η συνδρομή που μπορούν να παράσχουν τα σημεία επαφής του με στόχο τη διευκόλυνση της δικαστικής συνεργασίας σε ποινικές υποθέσεις μπορούν να χαρακτηριστούν παράδειγμα βέλτιστης πρακτικής.

- Αναφέρθηκαν ορισμένα εμπόδια σχετικά με την ποιότητα της συνεργασίας με τις ΗΠΑ, καθώς πολλοί δημοφιλείς και ευρέως χρησιμοποιούμενοι διακομιστές Διαδικτύου υπάγονται στη δικαιοδοσία τους. Οι κυπριακές αρχές δήλωσαν ότι η δικαστική συνεργασία σε ποινικές υποθέσεις με τις ΗΠΑ στον τομέα του εγκλήματος στον κυβερνοχώρο και της παιδικής πορνογραφίας είναι ιδιαίτερα περίπλοκη. Η εκτέλεση των αιτήσεων ΑΔΣ είναι συνήθως υπερβολικά χρονοβόρα και συχνά δεν παρέχονται τα δεδομένα. Καθώς ειδικότερα στις ΗΠΑ βρίσκεται συνήθως η έδρα ιστοτόπων μέσων κοινωνικής δικτύωσης, η συνεργασία με την εν λόγω χώρα είναι ζωτικής σημασίας για τη διερεύνηση του εγκλήματος στον κυβερνοχώρο.

- Κατά συνέπεια, σύμφωνα με τους αξιολογητές, τα μέσα που διατίθενται μέσω της Eurojust θα μπορούσαν να χρησιμοποιούνται συχνότερα. Ο ρόλος της Eurojust σχετικά με την παροχή συνδρομής στους επαγγελματίες του κλάδου θα μπορούσε να διερευνηθεί ειδικότερα, όπως οι δυνατότητες που παρέχει ο εισαγγελέας σύνδεσμος για τις ΗΠΑ, με στόχο την παροχή ταχύτερων απαντήσεων στις αιτήσεις ΑΔΣ που υποβάλλονται στις ΗΠΑ. Από την άλλη πλευρά, η ΕΕ θα πρέπει να εξακολουθήσει να βελτιώνει τις σχέσεις της με τις ΗΠΑ, ιδίως σε ό,τι αφορά τις αιτήσεις ΑΔΣ και την εκτέλεσή τους κατόπιν αιτήσεων των κρατών μελών.

8. ΚΑΤΑΡΤΙΣΗ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΠΡΟΛΗΨΗ

8.1. Εξειδικευμένη κατάρτιση

Δεν προβλέπεται ειδική κατάρτιση σχετικά με το έγκλημα στον κυβερνοχώρο για τους εισαγγελείς και τους δικαστές. Στο πλαίσιο του προγράμματος χρηματοδότησης «ISEC - Ετήσιο πρόγραμμα 2014», η Κύπρος έλαβε χρηματοδότηση για να αναπτύξει και να διοργανώσει μαθήματα κατάρτισης για εισαγγελείς και/ή δικαστές στο πλαίσιο του έργου 3CE[14].

Το προσωπικό του ΔΕΗΔ και του ΓΚΗΕ παρακολουθεί σε ετήσια βάση ειδικά μαθήματα κατάρτισης σχετικά με τη διερεύνηση του εγκλήματος στον κυβερνοχώρο. Τα περισσότερα από αυτά τα μαθήματα κατάρτισης διοργανώνονται από την Ευρωπαϊκή Αστυνομική Ακαδημία (EAA), το FBI, την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) και την Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος (ECTEG). Όσο για τους υπαλλήλους που διενεργούν επιτόπιες έρευνες (field officers), η Αστυνομική Ακαδημία Κύπρου διοργανώνει εξειδικευμένο σεμινάριο σχετικά με τη διερεύνηση του εγκλήματος στον κυβερνοχώρο (συλλογή ηλεκτρονικών αποδεικτικών στοιχείων, ερευνητικές μέθοδοι) και τη νομοθεσία. Επίσης, η Αστυνομική Ακαδημία παρέχει βασική κατάρτιση στη διεθνή συνεργασία και το έγκλημα στον κυβερνοχώρο σε όλους τους εκπαιδευόμενους αστυνομικούς. Επιπλέον, οι αστυνομικοί λαμβάνουν περαιτέρω επιμόρφωση για τη διεθνή αστυνομική συνεργασία από την ΕΕ και διεθνείς οργανισμούς, όπως η Ευρωπόλ και η Ευρωπαϊκή Αστυνομική Ακαδημία, ανάλογα με τα καθήκοντά τους. Η Αστυνομική Ακαδημία διοργανώνει επίσης επαναληπτικά εκπαιδευτικά σεμινάρια (refreshers).

Επιπλέον, το ΓΚΗΕ διοργανώνει σεμινάριο κατάρτισης μία φορά τον χρόνο για μια ομάδα δεκαπέντε αστυνομικών που είναι υπεύθυνοι για την κατάσχεση ηλεκτρονικών αποδεικτικών στοιχείων από τους τόπους του εγκλήματος. Το σεμινάριο αυτό αφορά τη συλλογή αποδεικτικών στοιχείων, τις προερευνητικές διαδικασίες, τη μαζική εκταμίευση μνήμης και άλλα ζητήματα. Καλύπτει τα εξής θέματα:

- νομοθεσία για το έγκλημα στον κυβερνοχώρο
- συλλογή ψηφιακών αποδεικτικών στοιχείων
- εισαγωγή στην έρευνα δικτύων
- ερευνητικά μέσα
- διαδικασίες

Η Εθνική Στρατηγική Κυβερνοασφάλειας προβλέπει στη Δράση 13 την περαιτέρω δραστηριοποίηση των πανεπιστημίων, των εκπαιδευτικών κέντρων και άλλων εμπλεκομένων φορέων για την παροχή κατάρτισης, ειδικών μαθημάτων και πανεπιστημιακών κύκλων σπουδών σχετικά με την ασφάλεια και το έγκλημα στον κυβερνοχώρο.

[14] Μετά από την επιτόπια επίσκεψη η ομάδα αξιολόγησης πληροφορήθηκε ότι το έργο 3CE του Κυπριακού Κέντρου Αριστείας Κυβερνοεγκλήματος βρίσκεται στο τελικό στάδιο υλοποίησής του. Στις 27.5.2016 πραγματοποιήθηκε εκπαιδευτικό σεμινάριο για 50 μέλη της αστυνομίας και στις 10.6.2016 διοργανώθηκε κοινό σεμινάριο κατάρτισης για δικαστές και εισαγγελείς. Στις 14.6.2016 πραγματοποιήθηκε ακόμα ένα σεμινάριο για δικηγόρους.

8.2. Ευαισθητοποίηση

Η Εθνική Στρατηγική Κυβερνοασφάλειας προσεγγίζει την ευαισθητοποίηση σε θέματα κυβερνοασφάλειας με συστημικό τρόπο· η εφαρμογή της προσέγγισης αυτής συντονίζεται από το Γραφείο του Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων.
Η ευαισθητοποίηση μνημονεύεται στη Δράση 14 της στρατηγικής και, μέσω της σύστασης επιτροπής και διαφόρων υπο-επιτροπών, επιδιώκεται να υπαχθούν όλες οι εθνικές προσπάθειες σε μία κοινή θεώρηση.

Η ευαισθητοποίηση και η εκπαίδευση σχετικά με το κυβερνοέγκλημα ξεκίνησαν από το Υπουργείο Παιδείας και Πολιτισμού με την εισαγωγή της ΤΠΕ στο εκπαιδευτικό σύστημα.

Προκειμένου να δημιουργήσει περιεχόμενο, εργαλεία και δραστηριότητες με σκοπό την ευαισθητοποίηση, η Κύπρος αξιοποιεί εθνικούς και ευρωπαϊκούς πόρους, καθώς και τη στήριξη που λαμβάνει από τον ιδιωτικό τομέα, ημικυβερνητικές οργανώσεις, άλλους δημόσιους οργανισμούς, τον ακαδημαϊκό χώρο, καθώς και από μη κερδοσκοπικές οργανώσεις και οργανωμένες κοινωνικές ομάδες. Η ευρύτερη ευαισθητοποίηση επιτυγχάνεται μέσω της συνεργασίας με τα μέσα ενημέρωσης, με την προβολή σύντομων βιντεοκλίπ, συζητήσεων και παρουσιάσεων, ιδίως στο πλαίσιο των δραστηριοτήτων της Ημέρας Ασφαλούς Διαδικτύου που λαμβάνουν χώρα τον Φεβρουάριο.

Οι πρώτοι ευρωπαϊκοί πόροι για την ευαισθητοποίηση ελήφθησαν το 2004, στο πλαίσιο του Προγράμματος Ασφαλούς Διαδικτύου· επίσης, μέσω του έργου SafeWeb, το οποίο συντονίζεται από το Πανεπιστήμιο Κύπρου, δημιουργήθηκαν γραμμή βοήθειας και γραμμή καταγγελιών· η ευρωπαϊκή χρηματοδότηση εξακολουθεί να λαμβάνεται έως και σήμερα στο πλαίσιο του ίδιου προγράμματος, καθώς και στο πλαίσιο του έργου CyberEthics.

Το έργο CyberEthics, με κοινοπραξία 5 εταίρων (δημόσιοι και ιδιωτικοί εταίροι, συμπεριλαμβανομένων του CNTI, του Παιδαγωγικού Ινστιτούτου Κύπρου και του τηλεπικοινωνιακού παρόχου Cyta που σε μεταγενέστερο στάδιο αντικαταστάθηκε από την MTN), τέθηκε σε λειτουργία το 2006 με τη συγχρηματοδότηση της ΕΕ, στο πλαίσιο του προγράμματος για την ασφαλέστερη χρήση του Διαδικτύου και του προγράμματος ΔΣΕ, και περιλαμβάνει κόμβο ενημέρωσης, γραμμή καταγγελιών και γραμμή βοήθειας. Το έργο *CyberEthics* συνιστά την εθνική εκπροσώπηση της Κύπρου στο ευρωπαϊκό δίκτυο κέντρων ευαισθητοποίησης (INSAFE), καθώς και στον διεθνή σύνδεσμο ανοικτών γραμμών επικοινωνίας για την καταγγελία παράνομου περιεχομένου στο Διαδίκτυο (INHOPE).

Συνεργάζεται με διάφορους ενδιαφερόμενους φορείς του δημοσίου και του ιδιωτικού τομέα στην Κύπρο, καθώς και με ενδιαφερόμενους από το εξωτερικό, επιδιώκοντας την εξασφάλιση ενός καλύτερου Διαδικτύου για όλους. Το έργο θα ολοκληρωθεί στα τέλη Ιουνίου του 2016. Οι δραστηριότητές του θα αποτελέσουν αντικείμενο παρόμοιου έργου που θα συντονίζει το Παιδαγωγικό Ινστιτούτο Κύπρου.

Στους στόχους του κόμβου ενημέρωσης περιλαμβάνεται η πραγματοποίηση ελκυστικών και στοχευμένων εκστρατειών ευαισθητοποίησης που θα ενημερώνουν το κοινό σχετικά με την ασφάλεια του Διαδικτύου και τους κινδύνους στο Διαδίκτυο, η εκπαίδευση των μαθητών, των δασκάλων, των γονέων, άλλων επαγγελματιών και του κοινού ώστε να χρησιμοποιούν με μεγαλύτερη ασφάλεια το Διαδίκτυο, και η δημιουργία υλικού προώθησης και άλλων εργαλείων ευαισθητοποίησης σχετικά με την ασφάλεια του Διαδικτύου το οποίο θα μπορεί να χρησιμοποιείται από παιδιά, εφήβους, δασκάλους και γονείς.

Ειδικότερα, οι δραστηριότητες του κόμβου ενημέρωσης, τις οποίες διοργανώνουν οι εταίροι του έργου *CyberEthics* και οι οποίες εστιάζουν στα παιδιά, περιλαμβάνουν παρουσιάσεις, σεμινάρια, θεατρικές παραστάσεις, παραστάσεις κουκλοθέατρου, κυνήγι θησαυρού, τη διοργάνωση διαγωνισμών, εκστρατείες πιστοποίησης και έρευνα όσον αφορά την χρήση του Διαδικτύου από ανηλίκους. Τα θέματα που καλύπτονται από τις παραπάνω δραστηριότητες και για τα οποία μπορούν να ενημερωθούν οι εκπαιδευτές, τα σχολεία, οι κοινωνικοί λειτουργοί, οι γονείς και άλλοι οργανωμένοι φορείς είναι η άγρα παιδιών (grooming), ο κυβερνοεκφοβισμός, η ηλεκτρονική πειρατεία, το υλικό σεξουαλικής κακοποίησης παιδιών (παιδική πορνογραφία), η ανταλλαγή γραπτών μηνυμάτων (SMS) σεξουαλικού περιεχομένου, η εκδικητική πορνογραφία, ο ρατσισμός/η ξενοφοβία και η κλοπή ταυτότητας.

Εκτός αυτού, παρέχεται εκπαίδευση και για άλλους κινδύνους, που αφορούν ενηλίκους, όπως το ηλεκτρονικό «ψάρεμα» και το φαινόμενο «sextortion» (εκβίαση με απειλή χρήσης σεξουαλικών δεδομένων), και προσφέρονται δύο κύριες υπηρεσίες με σκοπό να βοηθηθεί το κοινό. Πρόκειται για τη γραμμή καταγγελιών και για τη γραμμή βοήθειας.
Η γραμμή καταγγελιών επιτρέπει στο κοινό, και ιδίως στους εφήβους και τους νέους ενηλίκους να συμβάλλουν στην προσπάθεια για τη δημιουργία ενός ασφαλέστερου διαδικτυακού περιβάλλοντος μέσω της καταγγελίας του παράνομου περιεχομένου σε περιστατικά σεξουαλικής κακοποίησης παιδιών και σε περιστατικά ρατσισμού/ ξενοφοβίας. Η καταγγελία του παράνομου περιεχομένου στη γραμμή καταγγελιών μπορεί να γίνει μέσω:
1. του ηλεκτρονικού εντύπου που βρίσκεται στον ιστότοπο www.cyberethics.info
2. τηλεφωνικής κλήσης στον αριθμό: 22674747
3. αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση reports@cyberethics.info
4. της εφαρμογής για φορητές συσκευές «*CyberEthics* HotHelp»

Η γραμμή βοήθειας παρέχει απαντήσεις σε ερωτήσεις και προβληματισμούς σχετικά με θέματα επιβλαβούς συμπεριφοράς, επικίνδυνων επαφών και βλαβερού περιεχομένου. Η γραμμή βοήθειας είναι προσβάσιμη μέσω:

1. της υπηρεσίας διαδικτυακής συζήτησης (chat) στον ιστότοπο www.cyberethics.info (3 μμ - 7 μμ, από Δευτέρα έως Παρασκευή)
2. τηλεφωνικής κλήσης στον αριθμό: 70000 116 (9 πμ -7 μμ, από Δευτέρα έως Παρασκευή)
3. αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση helpline@cyberethics.info
4. αποστολής μηνύματος χωρίς σύνδεση (offline) στην υπηρεσία διαδικτυακής συζήτησης (chat) σε 24ωρη βάση
5. της εφαρμογής για φορητές συσκευές «*CyberEthics* HotHelp».

Το κέντρο πολιτικής «Ελπίδα για τα παιδιά» (Hope for Children) της Σύμβασης του ΟΗΕ για τα δικαιώματα του παιδιού (UNCRC) εφαρμόζει μια σταθερή και ελκυστική προσέγγιση που προωθεί την προστασία και προαγωγή των δικαιωμάτων του παιδιού, καθώς και την υποστήριξη της ενεργού συμμετοχής των παιδιών και των νέων στην κοινωνία. Στόχος είναι η στήριξη και η προστασία των δικαιωμάτων των παιδιών με βάση τα πρότυπα και τις αρχές της Σύμβασης του ΟΗΕ για τα δικαιώματα του παιδιού και της νομοθεσίας της ΕΕ, ανεξάρτητα από το περιβάλλον από το οποίο προέρχονται τα παιδιά. Τα προγράμματα και οι δραστηριότητες του κέντρου που σχετίζονται με την πρόληψη του κυβερνοεγκλήματος είναι τα ακόλουθα:

- η ευρωπαϊκή γραμμή στήριξης παιδιών και εφήβων 116 111, η οποία παρέχει άμεση ψυχολογική στήριξη στα παιδιά και τους εφήβους, δωρεάν και με εχεμύθεια·
- το πρόγραμμα «Beat Bullying» (καταπολέμηση του εκφοβισμού) το οποίο έχει ως στόχο να αυξήσει την ευαισθητοποίηση και να εξοπλίσει την εκπαιδευτική κοινότητα και τα παιδιά με γνώσεις μέσω της ανάπτυξης μεθόδων ταυτοποίησης, πρόληψης και διαχείρισης περιστατικών εκφοβισμού·
- η εκστρατεία ONE in Five (ΕΝΑ στα πέντε), η οποία επιδιώκει να σταματήσει τη σεξουαλική βία εις βάρος των παιδιών, καθώς και σειρά δράσεων που απευθύνονται σε παιδιά, γονείς, εκπαιδευτικούς και στο ευρύτερο κοινό·
- η ανάπτυξη της εφαρμογής φορητών συσκευών «HFCBeatBullying», ως εργαλείου για την πρόληψη και την αντιμετώπιση του εκφοβισμού, το οποίο μπορεί να χρησιμοποιηθεί σε 23 χώρες της ΕΕ και το οποίο, επιπροσθέτως των χρήσιμων συμβουλών που περιέχει, προσφέρει άμεση πρόσβαση στην Ευρωπαϊκή γραμμή στήριξης παιδιών και εφήβων 116 111.

Στο πλαίσιο αυτών των προγραμμάτων το κέντρο πολιτικής «Ελπίδα για τα παιδιά» της UNCRC πραγματοποιεί σεμινάρια για γονείς, καθώς και εργαστήρια, και διοργανώνει κύκλους μαθημάτων σε σχολεία, με σκοπό να ενημερώσει, να εκπαιδεύσει και να ενδυναμώσει τους μαθητές όσον αφορά τα θέματα του εκφοβισμού, της σεξουαλικής κακοποίησης και του κυβερνοεγκλήματος, σε συνεργασία με το Υπουργείο Παιδείας και Πολιτισμού και το παρατηρητήριο για τη βία στο σχολείο. Επιπλέον, διοργανώθηκε κύκλος μαθημάτων κατάρτισης για ξενοδοχοϋπαλλήλους με θέμα τον ασφαλή για τα παιδιά τουρισμό (περιλαμβανομένου του θέματος της παιδικής πορνογραφίας).

Το κέντρο πολιτικής «Ελπίδα για τα παιδιά» διεξήγαγε επίσης ακαδημαϊκή έρευνα σχετικά με την άγρα παιδιών στο Διαδίκτυο (grooming), η οποία ήταν η πρώτη του είδους της στην Κύπρο (http://uncrcpc.org.cy/index.php?id=47).

Το κέντρο πολιτικής «Ελπίδα για τα παιδιά» υπέβαλε, κατόπιν έκκλησης που απηύθυνε η επιτροπή για τα δικαιώματα του παιδιού στη γενική παρατήρησή της σχετικά με τα δικαιώματα των εφήβων, έκθεση, η οποία περιελάμβανε πληροφορίες σχετικά με τις βέλτιστες πρακτικές των κοινωνιολογικών μελετών του κέντρου πολιτικής «Ελπίδα για τα παιδιά» της UNCRC όσον αφορά τη συχνότητα εμφάνισης διάφορων προβλημάτων που αντιμετωπίζουν οι έφηβοι, όπως ο εκφοβισμός, η σεξουαλική κακοποίηση και η σεξουαλική εκμετάλλευση.

Το κέντρο πολιτικής «Ελπίδα για τα παιδιά» της UNCRC συμμετέχει, ως ενεργός παράγοντας του τομέα αυτού σε εθνικό επίπεδο, στη συντονιστική ομάδα της εκστρατείας «ONE in Five» και στις κοινοβουλευτικές συνεδριάσεις για την κύρωση και εφαρμογή της Σύμβασης του Lanzarote (η οποία επιβάλλει την ποινικοποίηση κάθε είδους σεξουαλικής εκμετάλλευσης εις βάρος των παιδιών και ορίζει ότι τα κράτη εντός και εκτός Ευρώπης πρέπει να εγκρίνουν ειδική νομοθεσία και να λάβουν μέτρα για την πρόληψη της σεξουαλικής βίας, την προστασία των ανήλικων θυμάτων και τη δίωξη των δραστών).

Εκτός αυτού, προβλέπεται να χρηματοδοτηθεί από την Ευρωπαϊκή Επιτροπή το προσεχές έργο «JudEx +: Towards a child-friendly justice in cases of sexual violence against children» (JudEx +: Προς μια φιλική προς τα παιδιά δικαιοσύνη σε υποθέσεις σεξουαλικής βίας εις βάρος παιδιών), για το οποίο υπεβλήθη πρόταση στο πλαίσιο της πρόσκλησης υποβολής προτάσεων της Ευρωπαϊκής Επιτροπής JUST/2014/RCHI/AG/PROF. Τον συντονισμό του έργου θα αναλάβει το κέντρο πολιτικής «Ελπίδα για τα παιδιά» της UNCRC, από κοινού με έξι ακόμη εταίρους από χώρες της ΕΕ. Οι εταίροι επελέγησαν από χώρες που έχουν κυρώσει πρόσφατα (εντός των 3-4 περασμένων ετών) τη Σύμβαση του Lanzarote, στις οποίες υπάρχει επείγουσα ανάγκη για κατάρτιση των επαγγελματιών που συμμετέχουν σε δικαστικές διαδικασίες για υποθέσεις κακοποίησης παιδιών στο πλαίσιο της Σύμβασης. Το έργο ξεκίνησε τον Ιανουάριο του 2016 και θα διαρκέσει δύο έτη.

8.3. Πρόληψη

8.3.1. Εθνική νομοθεσία/πολιτική και άλλα μέτρα

Οι προσπάθειες για την πρόληψη αντικατοπτρίζονται τόσο στη νομοθεσία όσο και στην πολιτική της Κύπρου, ενώ δίνεται ιδιαίτερη έμφαση στην πρόληψη της παιδικής πορνογραφίας. Το Υπουργείο Παιδείας και Πολιτισμού (ΥΠΠ) συμμετέχει στην πρόληψη του κυβερνοεγκλήματος εστιάζοντας στις *αξιόποινες πράξεις που σχετίζονται με το περιεχόμενο*. Τα παιδιά νεαρής ηλικίας εκπαιδεύονται ώστε να μπορούν να αναγνωρίζουν τους εν λόγω κινδύνους, να αποφεύγουν και να προλαμβάνουν την έκθεσή τους σε αυτούς και –σε περίπτωση που πέσουν θύματα ή γίνουν μάρτυρες κυβερνοεγκλήματος– να είναι σε θέση να το αντιμετωπίσουν και να το καταγγείλουν.

Το αρμόδιο τμήμα για θέματα του ασφαλούς Διαδικτύου στο ΥΠΠ είναι το Παιδαγωγικό Ινστιτούτο Κύπρου (ΠΙΚ). Το ΠΙΚ, σε συνεργασία με τις εκπαιδευτικές διευθύνσεις, χαράσσει πολιτικές και εκτελεί προγράμματα που σχετίζονται με την κριτική και υπεύθυνη χρήση του Διαδικτύου. Οι δράσεις που σχετίζονται με τον ασφαλή διαδικτυακό χώρο είναι οι ακόλουθες:
– εισαγωγή του *Ασφαλούς Διαδικτύου* στη σχολική ύλη·
– διοργάνωση εργαστηρίων στους χώρους του σχολείου για μαθητές, εκπαιδευτικούς και γονείς·
– παρουσιάσεις σε συνέδρια και άλλες εκδηλώσεις·
– εκτέλεση σχολικών προγραμμάτων που στηρίζονται από το Παιδαγωγικό Ινστιτούτο Κύπρου, όπως το σήμα *Ασφαλές σχολείο για το Διαδίκτυο*, ο διαγωνισμός για την *παραγωγή σύντομου βίντεο από μαθητές*, το πρόγραμμα *Μικροί εκπαιδευτές για το Διαδίκτυο*, *το σήμα eSafety* κ.ά., σε συνεργασία με άλλους ενδιαφερόμενους φορείς[15].
– συμμετοχή στην υλοποίηση, σε εθνικό επίπεδο, των προγραμμάτων *Ασφαλούς Διαδικτύου* που λαμβάνουν ευρωπαϊκή στήριξη, όπως το πρόγραμμα «Ασφαλέστερο Διαδίκτυο» που χρηματοδοτείται από τη διευκόλυνση «Συνδέοντας την Ευρώπη» (ΔΣΕ) και το έργο *CyberEthics* που χρηματοδοτείται από τον Εκτελεστικό Οργανισμό Καινοτομίας και Δικτύων (ΙΝΕΑ) της Ευρωπαϊκής Επιτροπής, στο πλαίσιο του οποίου λειτουργούν μια γραμμή βοήθειας και μια γραμμή καταγγελιών·
– διοργάνωση συνεδρίων και άλλων εκδηλώσεων (για παράδειγμα την Ημέρα Ασφαλούς Διαδικτύου συνδιοργανώνεται σε εθνικό επίπεδο συνέδριο από το ΥΠΠ και την Αρχή Τηλεπικοινωνιών Κύπρου (CYTA), στο οποίο συμμετέχουν περίπου 800 μαθητές, και πραγματοποιούνται εκδηλώσεις ευαισθητοποίησης σε όλο το νησί σε συνεργασία με άλλες κερδοσκοπικές και μη οργανώσεις)·

[15] www.pi.ac.cy/internetsafety

– εκστρατεία ευαισθητοποίησης με σύντομα βιντεοκλίπ, συζητήσεις και παρουσιάσεις στα μέσα ενημέρωσης·
– σχεδιασμός και παραγωγή εκπαιδευτικού υλικού, δραστηριοτήτων και εργαλείων·
– διαχείριση κεντρικού φίλτρου για ασφαλές Διαδίκτυο σε όλα τα σχολεία·
– κατάρτιση εκπαιδευτικών σε θέματα σχετικά με το κυβερνοέγκλημα και την προστασία από αυτό.

Το ΥΠΠ συνεργάζεται στενά με διάφορους ενδιαφερόμενους φορείς (του δημοσίου και του ιδιωτικού τομέα). Για παράδειγμα, πραγματοποιήθηκε σειρά παρουσιάσεων σε σχολεία από την Αρχή Τηλεπικοινωνιών Κύπρου, το Ινστιτούτο Νευροεπιστήμης και Τεχνολογίας Κύπρου και το Γραφείο του Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, καθώς και σειρά εργαστηρίων για την εξοικείωση με τα μέσα επικοινωνίας, σε συνεργασία με την Αρχή Ραδιοτηλεόρασης Κύπρου.

Το περασμένο έτος ζητήθηκε από το Υπουργείο Παιδείας και Πολιτισμού να αναλάβει τον συντονισμό της υπό-ομάδας της Δράσης 14, που στοχεύει στην ευαισθητοποίηση και την εκπαίδευση παιδιών/μαθητών, εκπαιδευτικών και γονέων στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας της Κύπρου, η οποία συντονίζεται από το Γραφείο του Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων. Η Δράση 14 στοχεύει στην ανάπτυξη ενός συνολικού εθνικού προγράμματος ευαισθητοποίησης σε θέματα κυβερνοασφάλειας, το οποίο θα καλύπτει όλους τους χρήστες ηλεκτρονικών συστημάτων, από τους κυβερνητικούς υπαλλήλους έως και τους απλούς πολίτες. Ως εκ τούτου, εστάλη ανοικτή πρόσκληση σε όλους τους ενδιαφερόμενους φορείς που ήθελαν να συμμετάσχουν και συστάθηκε, στο πλαίσιο της Δράσης 14, μια επιτροπή που στην παρούσα φάση καταρτίζει την εθνική στρατηγική ευαισθητοποίησης και εκπαίδευσης, η οποία θα περιλαμβάνει όλα τα υπάρχοντα μέτρα και θα παρέχει δυνατότητες για τη δημιουργία νέων.
Ο νόμος 91(I)/2014 περιλαμβάνει διατάξεις που υποχρεώνουν νομικά τους εκπαιδευτικούς να καταγγέλλουν ύποπτα περιστατικά. Στον ίδιο Νόμο αναφέρεται ότι συνιστά ευθύνη του υπουργείου να εξασφαλίσει την εκπαίδευση των μαθητών όσον αφορά τους κινδύνους της σεξουαλικής κακοποίησης και τους τρόπους προστασίας από αυτούς.

Στις 30 Σεπτεμβρίου 2015 συστάθηκε με απόφαση του υπουργικού συμβουλίου μια Αρχή, δυνάμει του άρθρου 47 του νόμου για την πρόληψη και καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας [N. 91(I)/2014], για την παρακολούθηση ανθρώπων που έχουν καταδικαστεί για σεξουαλικά εγκλήματα εις βάρος παιδιών. Της Αρχής αυτής προεδρεύει ο Γενικός Γραμματέας του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως. Απαρτίζεται από εκπροσώπους του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως, της Αστυνομίας, της νομικής υπηρεσίας, του Υπουργείου Υγείας, του Υπουργείου Εργασίας, Πρόνοιας και Κοινωνικών Ασφαλίσεων, του Υπουργείου Παιδείας και Πολιτισμού, του τμήματος φυλακών, του συμβουλίου αποφυλάκισης κρατουμένων επ' αδεία και του οργανισμού νεολαίας.

Επιπλέον, διορίστηκε από υπουργική επιτροπή μια ad hoc επιτροπή, καθήκον της οποίας είναι να καταρτίσει μια εθνική στρατηγική για την προστασία των παιδιών από την σεξουαλική εκμετάλλευση και την παιδική πορνογραφία.

Διοργανώνονται επίσης δραστηριότητες πρόληψης για αξιόποινες πράξεις που αφορούν μόνο πληροφοριακά συστήματα, και ιδίως για όσες σχετίζονται με κυβερνοεπιθέσεις. Οι διευθύνσεις και υπηρεσίες του ΥΠΠ δίδουν μεγάλη προσοχή στο θέμα των προσωπικών δεδομένων μαθητών και εκπαιδευτικών και συμμορφώνονται προς τους κανονισμούς της Κύπρου, όπως ορίζονται από το Γραφείο του Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Συγχρόνως, έχει αποσπαστεί μια ομάδα από το Τμήμα Υπηρεσιών Πληροφορικής (κυβερνητικό επίπεδο) στο υπουργείο προκειμένου να συνδράμει στην ασφάλεια των συστημάτων πληροφορικής. Εκτός αυτού, σχεδιάζεται να ζητηθεί από τη Μονάδα Ελέγχων ΤΠ της Υπηρεσίας Εσωτερικού Ελέγχου Κύπρου να διεξάγει δοκιμές διείσδυσης σε ορισμένα τμήματα (συγκεκριμένα στο Παιδαγωγικό Ινστιτούτο Κύπρου).

Πέραν τούτου, η συνεργασία με την Αρχή Τηλεπικοινωνιών Κύπρου εφοδίασε το Υπουργείο με κεντρικό σύστημα διαδικτυακού φίλτρου για την πρόσβαση των σχολείων στο Διαδίκτυο.

Υπάρχει στενή συνεργασία με το ΓΚΗΕ στον τομέα της ενημέρωσης και της εκπαίδευσης μαθητών, εκπαιδευτικών και γονέων όσον αφορά τη νομοθεσία σχετικά με το κυβερνοέγκλημα και τις διαδικασίες καταγγελίας.

Στην πρώιμη εκπαίδευση (πρωτοβάθμια) εισάγονται προγράμματα που αφορούν τις *αξιόποινες πράξεις που σχετίζονται με το περιεχόμενο*. Τα προγράμματα αυτά είτε έχουν τη μορφή δραστηριοτήτων και αποτελούν μέρος της σχολικής ύλης (για παράδειγμα μέσω μαθημάτων ΤΠΕ), είτε έχουν τη μορφή σχολικών παρεμβάσεων και πιστοποιήσεων (όπως το *σήμα eSafety*) ή διαγωνισμών (παραγωγή σύντομου βίντεο από μαθητές), είτε επιτρέπουν στους μαθητές να αναλάβουν ενεργό ρόλο (όπως το πρόγραμμα *Μικροί εκπαιδευτές για το διαδίκτυο*).

Στόχος της πρότασης για τη δημιουργία *Κέντρου Ασφαλούς Διαδικτύου* (την οποία κατάρτισε η επιτροπή που εργάζεται πάνω στη Δράση 14 της Εθνικής Στρατηγικής Κυβερνοασφάλειας), είναι να προσφέρονται κύκλοι μαθημάτων που να απευθύνονται σε διαφορετικές ομάδες του πληθυσμού, οι οποίοι θα μπορούν να πραγματοποιούνται στους χώρους του κέντρου, διαδικτυακά και σε συνεργασία με πανεπιστήμια και άλλα κέντρα κατάρτισης (για παράδειγμα όταν πρόκειται για μαθήματα που απευθύνονται σε δημόσιους υπαλλήλους).

Τα πανεπιστήμια, στο πλαίσιο της συνεργασίας τους με άλλους εταίρους σε έργα χρηματοδοτούμενα από την ΕΕ, έχουν ήδη αρχίσει να προσφέρουν ειδικά μαθήματα για το κυβερνοέγκλημα και να απονέμουν διπλώματα στον τομέα του κυβερνοεγκλήματος (για παράδειγμα το Ευρωπαϊκό Πανεπιστήμιο Κύπρου, ως εταίρος στο έργο για τη δημιουργία Κυπριακού Κέντρου Αριστείας Κυβερνοεγκλήματος για την κατάρτιση, την εκπαίδευση και την έρευνα *(3CE)*, προσφέρει εκπαιδευτικό πρόγραμμα για φοιτητές Νομικής).

8.3.2. Συμπράξεις δημοσίου και ιδιωτικού τομέα (ΣΔΙΤ)

Η χρήση του μοντέλου των συμπράξεων δημοσίου και ιδιωτικού τομέα (ΣΔΙΤ) θεωρείται, στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας, ζωτικής σημασίας για την πρόληψη και καταπολέμηση του κυβερνοεγκλήματος. Επί του παρόντος τελεί υπό εξέταση από της κυπριακές αρχές.

8.4. Συμπεράσματα

- Η Κύπρος χρησιμοποιεί εσωτερική και εξωτερική χρηματοδότηση για την διοργάνωση μαθημάτων κατάρτισης. Στο πλαίσιο του προγράμματος χρηματοδότησης «ISEC - Ετήσιο πρόγραμμα 2014», η Κύπρος έλαβε χρηματοδότηση για να αναπτύξει και να διοργανώσει μαθήματα κατάρτισης για εισαγγελείς και/ή δικαστές στο πλαίσιο του έργου 3CE.

- Το προσωπικό του ΔΕΗΔ και του ΓΚΗΕ φαίνεται άρτια καταρτισμένο. Παρακολουθεί σε ετήσια βάση ειδικά μαθήματα κατάρτισης σχετικά με τη διερεύνηση του κυβερνοεγκλήματος, τα οποία στην πλειονότητά τους διοργανώνονται από την EAA, το FBI, την OLAF, την ECTEG και την Αστυνομική Ακαδημία Κύπρου. Συνεπώς, οι αστυνομικοί υπάλληλοι εκπαιδεύουν και άλλους επαγγελματίες του κλάδου.

- Ωστόσο, δεν προβλέπεται ειδική κατάρτιση για τους εισαγγελείς και τους δικαστές στον τομέα αυτό. Δεδομένου ότι οι δράστες του κυβερνοεγκλήματος θα πρέπει να καταλήγουν στο δικαστήριο, θεωρείται σκόπιμο να προσφέρονται μαθήματα κατάρτισης που να απευθύνονται ειδικά σε εισαγγελείς και δικαστές. Είναι προφανές ότι η κατάρτιση δεν θα πρέπει να είναι υποχρεωτική για το δικαστικό και εισαγγελικό σώμα. Ωστόσο, η συμμετοχή σε αυτά τα μαθήματα θα πρέπει να θεωρείται από τη διοίκηση ως πλεονέκτημα για κάθε είδους προαγωγή. Η παροχή ενός τέτοιου κινήτρου θα προτρέψει το δικαστικό σώμα και τους εισαγγελείς να συμμετάσχουν σε εξειδικευμένα μαθήματα κατάρτισης, χωρίς ωστόσο να πλήξει την ανεξαρτησία τους.

- Δεδομένου ότι το κυβερνοέγκλημα συνιστά σχετικά νέο φαινόμενο, αποκτούν ζωτική σημασία η κατάρτιση σε θέματα κυβερνοεγκλήματος και η επίτευξη αριστείας. Κατά τη γνώμη των αξιολογητών θα μπορέσουν να επιτευχθούν τα καλύτερα αποτελέσματα με τη διοργάνωση κοινών μαθημάτων κατάρτισης για δικαστές και εισαγγελείς, γραμματείς δικαστηρίου, αστυνομικούς και ειδικούς στην ΤΠ. Η ομάδα αξιολόγησης ενημερώθηκε, ωστόσο, ότι τέτοια μαθήματα δεν διοργανώθηκαν, επειδή τα μέλη του δικαστικού σώματος εμφανίζονται γενικά επιφυλακτικά όσον αφορά τέτοιες πρωτοβουλίες. Επομένως, οι κυπριακές αρχές θα πρέπει να επιδιώξουν να διοργανώσουν κοινά μαθήματα κατάρτισης για δικαστές, εισαγγελείς και αστυνομικούς υπαλλήλους, στα οποία η παρακολούθηση θα έχει περισσότερο υποχρεωτικό χαρακτήρα. Η ενσωμάτωση στα μαθήματα αυτά πληροφοριών που σχετίζονται με την υποστήριξη που παρέχεται από την Eurojust, το ΕΔΔ και την Ευρωπόλ θα συμβάλει στην καλύτερη κατανόηση των τρεχουσών εξελίξεων και των νέων τάσεων στο κυβερνοέγκλημα, των ρόλων που διαδραματίζουν οι φορείς που είναι αρμόδιοι για τον εντοπισμό, τη διερεύνηση και τη δίωξη, και των τρόπων με τους οποίους μπορεί να προαχθεί και/ή να βελτιωθεί η συνεργασία.

- Οι κυπριακές αρχές δήλωσαν ότι το θέμα των μαθημάτων κατάρτισης θα επιλυθεί μελλοντικά με τη δημιουργία του 3CE, το οποίο θα παρέχει βραχυπρόθεσμα, εξαιρετικά στοχευμένα και εξειδικευμένα σεμινάρια κατάρτισης για θέματα που αφορούν το κυβερνοέγκλημα, τα οποία θα απευθύνονται σε συμμετέχοντες από τον δημόσιο και τον ιδιωτικό τομέα. Τα μαθήματα θα διευκολύνουν την ανταλλαγή και διάδοση σιωπηρής γνώσης, θα συμβάλουν στην εξοικείωση των συμμετεχόντων με νέες τεχνολογίες και εργαλεία, και θα βελτιώσουν τις καθημερινές ικανότητές τους σε θέματα που αφορούν το κυβερνοέγκλημα. Μελλοντικά θα μπορούσαν να αναπτυχθούν ενότητες ειδικά για δικαστές, εισαγγελείς και υπαλλήλους αρμόδιους για την επιβολή του νόμου. Οι αξιολογητές θεωρούν σκόπιμη τη σύσταση κέντρου αριστείας υψηλής εξειδίκευσης για την παροχή μαθημάτων κατάρτισης, πιστεύουν, ωστόσο, ότι είναι αναγκαίο να προβλεφθούν επίσης επαρκείς ανθρώπινοι και χρηματοδοτικοί πόροι, ώστε το κέντρο να μπορεί να φέρει εις πέρας τα καθήκοντά του.

- Στην Κύπρο έχουν καταβληθεί πολλές προσπάθειες και έχουν καθιερωθεί άριστες πρακτικές σε θέματα ευαισθητοποίησης και πρόληψης, ιδίως όσον αφορά τους μαθητές και τα μικρά παιδιά. Η Κύπρος διαθέτει ένα άρτια ανεπτυγμένο σύστημα για την εκπαίδευση παιδιών σε θέματα κυβερνοεγκλήματος από επαγγελματίες που ασχολούνται ειδικά με αυτό το θέμα. Το Υπουργείο Παιδείας και Πολιτισμού (ΥΠΠ) συμμετέχει στην πρόληψη του κυβερνοεγκλήματος, εστιάζοντας στις *αξιόποινες πράξεις που σχετίζονται με το περιεχόμενο*, μέσω της παροχής της σχετικής εκπαίδευσης σε παιδιά νεαρής ηλικίας. Το ΥΠΠ συνεργάζεται στενά με διάφορους ενδιαφερόμενους φορείς (του δημοσίου και του ιδιωτικού τομέα). Για παράδειγμα, πραγματοποιήθηκε σειρά παρουσιάσεων σε σχολεία από την Αρχή Τηλεπικοινωνιών Κύπρου, το Ινστιτούτο Νευροεπιστήμης και Τεχνολογίας Κύπρου και το Γραφείο του Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων, καθώς και σειρά εργαστηρίων για την εξοικείωση με τα μέσα επικοινωνίας, σε συνεργασία με την Αρχή Ραδιοτηλεόρασης Κύπρου. Όλα τα μέσα για την εκπαίδευση των παιδιών, όπως το σύστημα των μικρών εκπαιδευτών, τα εκπαιδευτικά βίντεο και η χρήση διάφορων εργαλείων σε μέσα κοινωνικής δικτύωσης κρίνονται σκόπιμα και παραγωγικά.

- Τα προγράμματα που απευθύνονται στην κοινωνία με στόχο να αυξήσουν την ευαισθητοποίηση σχετικά με την ασφαλή χρήση του Διαδικτύου είναι πολλά. Ορισμένα από αυτά, όπως τα προγράμματα *CyberEthics*, «Ασφαλές σχολείο για το Διαδίκτυο» (eSafe School) και «Μικροί εκπαιδευτές για το Διαδίκτυο» κρίθηκαν ως ιδιαίτερα χρήσιμα από την ομάδα των αξιολογητών, καθώς ενθαρρύνουν τους μαθητές να αναλάβουν την ευθύνη για την εκπαίδευση, τόσο τη δική τους όσο και των συνομηλίκων, των γονέων και των δασκάλων τους. Σύμφωνα με τις συστάσεις των αξιολογητών, τα παραπάνω προγράμματα, καθώς και το πρόγραμμα Safe Internet, πρέπει να αποτελέσουν κανονικά μαθήματα του σχολικού προγράμματος ή να συμπεριληφθούν στην εκπαίδευση ΤΠ, ακολουθώντας το πρότυπο του συστήματος των μικρών εκπαιδευτών που εφαρμόστηκε στην Κύπρο με σκοπό να εκπαιδευθούν τα παιδιά σχετικά με τους κινδύνους που απορρέουν από τη χρήση του Διαδικτύου.

- Επιπλέον, η Κύπρος έχει προβεί στην κατάρτιση μητρώου δραστών σεξουαλικών αδικημάτων με στόχο την καλύτερη προστασία των παιδιών από τυχόν μελλοντικές βλάβες που θα μπορούσαν να υποστούν από ανθρώπους που είναι ήδη αναγνωρισμένοι δράστες σεξουαλικών αδικημάτων. Το παραπάνω θα μπορούσε να αποτελέσει έναυσμα για τη δημιουργία ενός χρήσιμου συστήματος προστασίας των παιδιών, ιδίως από δράστες σεξουαλικών αδικημάτων.

9. ΤΕΛΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΚΑΙ ΣΥΣΤΑΣΕΙΣ

9.1. Προτάσεις της Κύπρου

Η Εθνική Στρατηγική Κυβερνοασφάλειας είναι το μέσο που κατευθύνει τις προσπάθειες που καταβάλλει η Κύπρος για την πρόληψη και την καταπολέμηση του κυβερνοεγκλήματος. Στο πλαίσιό της έχουν δημιουργηθεί δομές συνεργασίας ανάμεσα σε όλες τις αρμόδιες αρχές, συμπεριλαμβανομένων των δημοσίων, ιδιωτικών και μη κυβερνητικών φορέων, ιδίως σε ό,τι αφορά τον τομέα της ευαισθητοποίησης, στον οποίο η Κύπρος έχει καταβάλει πολλές προσπάθειες προκειμένου να καταπολεμηθεί αυτή η μορφή εγκλήματος.

Η Αστυνομία Κύπρου δημιούργησε ένα ειδικό γραφείο για την καταπολέμηση του ηλεκτρονικού εγκλήματος, το ΓΚΗΕ, εξασφαλίζοντας με αυτόν τον τρόπο την αναγκαία εμπειρογνωμοσύνη για την αντιμετώπιση των ιδιαιτεροτήτων των εν λόγω αδικημάτων. Η δημιουργία ad hoc τεχνικής επιτροπής στο πλαίσιο του ΓΕΡΗΕΤ με τη συμμετοχή εμπειρογνωμόνων στον τομέα της επιβολής του νόμου και εκπροσώπων των παρόχων υπηρεσιών Διαδικτύου ενισχύει τις ικανότητες για επίλυση των τεχνικών προβλημάτων. Στο πλαίσιο του εν εξελίξει προγράμματος 3CE, θα καταρτιστεί εκπαιδευτικό υλικό για τις εισαγγελικές, αρχές, τις αρχές επιβολής του νόμου και τις δικαστικές αρχές.

Οι παρεμβάσεις στα σχολεία, στις οποίες οι μαθητές αναλαμβάνουν ενεργό ρόλο όσον αφορά την κριτική και υπεύθυνη χρήση του Διαδικτύου ως χρήστες και δημιουργοί, είναι ζωτικής σημασίας για την εκπαίδευση των παιδιών. Προγράμματα όπως το *Ασφαλές σχολείο για το Διαδίκτυο* –στο οποίο η σχολική μονάδα αναλαμβάνει να καλλιεργήσει μια νοοτροπία ασφαλούς χρήσης του Διαδικτύου ανάμεσα στους μαθητές, τους εκπαιδευτικούς, τους γονείς και την ευρύτερη κοινότητα– και οι *Μικροί εκπαιδευτές για το Διαδίκτυο* –στο οποίο οι μαθητές αναλαμβάνουν την ευθύνη τόσο για τη δική τους εκπαίδευση όσο και για εκείνη των συνομηλίκων τους, των γονέων τους, των δασκάλων τους και της ευρύτερης κοινότητας– θεωρείται ότι συνιστούν ορθές πρακτικές για την πρόληψη των απειλών στον κυβερνοχώρο.

Ένα πρακτικό μέτρο που θα μπορούσε να βοηθήσει ώστε να καλλιεργηθεί μια νοοτροπία ευαισθητοποίησης είναι η έκδοση κανονισμού που θα απαιτούσε από τους παρόχους υπηρεσιών Διαδικτύου να θέτουν στη διάθεση των πελατών τους δέσμη υπηρεσιών ευαισθητοποίησης, στην οποία θα περιλαμβανόταν η παροχή διαδικτυακών φίλτρων.

Εκτός αυτού, θα μπορούσε να διατεθεί άμεση ευρωπαϊκή χρηματοδότηση στα κράτη μέλη, ειδικά για τις προτεραιότητες που έχουν τεθεί από τις πολιτικές της ΕΕ, ούτως ώστε να επιτευχθεί ένα καλό επίπεδο κυβερνοασφάλειας.

9.2. Συστάσεις

Όσον αφορά την πρακτική εφαρμογή και λειτουργία της απόφασης-πλαισίου και των οδηγιών, η ομάδα εμπειρογνωμόνων που διενήργησε την αξιολόγηση της Κύπρου ήταν σε θέση να εκφράσει την ικανοποίησή της για το κυπριακό σύστημα.

Η Κύπρος θα πρέπει να ελέγξει τη συνέχεια που θα δοθεί στις συστάσεις της παρούσας έκθεσης 18 μήνες μετά την αξιολόγηση και να υποβάλει έκθεση προόδου στην ομάδα «Γενικές υποθέσεις περιλαμβανομένης της αξιολόγησης» (GENVAL).

Η ομάδα αξιολόγησης έκρινε σκόπιμο να διατυπώσει ορισμένες προτάσεις προς τις κυπριακές αρχές. Επιπλέον, με βάση τις υφιστάμενες ορθές πρακτικές, διατυπώνονται επίσης συστάσεις προς την ΕΕ και τα θεσμικά και άλλα όργανά της, ιδίως την Ευρωπόλ.

9.2.1. Συστάσεις προς την Κύπρο

1. Η Κύπρος προτρέπεται να συνεχίσει να εφαρμόζει την Εθνική Στρατηγική Κυβερνοασφάλειας, ιδίως μέσω της διενέργειας οργανωτικών και δομικών δραστηριοτήτων, οι οποίες θα πρέπει να συνοδευθούν από αύξηση των δαπανών και του ανθρώπινου δυναμικού ώστε να βελτιωθεί το εργασιακό περιβάλλον του ΓΚΗΕ και του ΔΕΗΔ (3.1, 3.2 και 3.5)

2. Η Κύπρος θα πρέπει να βρει μια μέθοδο ώστε να συλλέγει ολοκληρωμένα στατιστικά στοιχεία σχετικά με τις έρευνες, τις διώξεις και τις καταδίκες που σχετίζονται με το κυβερνοέγκλημα και να τα κατανέμει ανά ειδικούς τομείς κυβερνοεγκλήματος, κατά προτίμηση ανά τους τομείς που έχουν καθοριστεί σε επίπεδο ΕΕ, οι οποίοι, πιο συγκεκριμένα, είναι: η σεξουαλική κακοποίηση παιδιών στο Διαδίκτυο, η διαδικτυακή απάτη με κάρτες και οι κυβερνοεπιθέσεις· (πρβλ. 3.3 και 3.5).

3. Η Κύπρος θα πρέπει να εξετάσει τη δυνατότητα να εγκρίνει νομοθετικά ή άλλα μέτρα ώστε να καταστεί δυνατή η υποκλοπή/συλλογή σε πραγματικό χρόνο δεδομένων κίνησης/περιεχομένου, προκειμένου η αστυνομία να γίνει αποτελεσματικότερη κατά τη διερεύνηση του κυβερνοεγκλήματος· (πρβλ. 5.2.1 και 5.5)

4. Η Κύπρος θα πρέπει να λάβει υπόψη το ενδεχόμενο να παράσχει τη δυνατότητα στους εισαγγελείς να συμμετέχουν στις συσκέψεις/συζητήσεις με τον ιδιωτικό τομέα, ώστε να εξασφαλίζεται ότι τα αποδεικτικά στοιχεία συλλέγονται σύμφωνα με την τρέχουσα νομοθεσία και ότι γίνονται δεκτά σε δικαστικές διαδικασίες· (πρβλ. 4.5, 6.1.2 και 6.4)

5. Η Κύπρος προτρέπεται να συστήσει μια εθνική CERT (ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική) ως εθνικό φορέα για την πρόληψη και για την προστασία από τις απειλές του κυβερνοχώρου που θέτουν σε κίνδυνο την ασφάλεια των δημόσιων πληροφοριακών συστημάτων· (πρβλ. 6.1.2 και 6.4)

6. Η Κύπρος θα πρέπει να ενθαρρύνει τη συνεργασία μεταξύ των αρχών επιβολής του νόμου και του κλάδου, ιδίως στον χρηματοπιστωτικό τομέα, ώστε να δημιουργηθεί ένας βιώσιμος μηχανισμός υποβολής στοιχείων σχετικά με τις κυβερνοεπιθέσεις, οι οποίες πλήττουν τόσο την κοινωνία όσο και τον ιδιωτικό τομέα· (πρβλ. 6.1.2, 6.3.2 και 6.4)

7. Η Κύπρος θα πρέπει να εξετάσει την ενσωμάτωση στα εκπαιδευτικά προγράμματα πληροφοριών σχετικά με την υποστήριξη που μπορεί να παρασχεθεί από την Eurojust και το ΕΔΔ στις εθνικές αρχές, ιδίως όσον αφορά τους όρους συνεργασίας με τρίτα κράτη· (πρβλ. 7.1.2, 7.5.1 και 7.6)

8. Η Κύπρος ενθαρρύνεται να διατηρήσει τη βασική ιδέα των 3CE και *CyberEthics* παρέχοντάς τους τούς κατάλληλους χρηματοδοτικούς και ανθρώπινους πόρους (πρβλ.. 8.1, 8.3.1 και 8.4)

9. Η Κύπρος θα πρέπει να λάβει τα αναγκαία μέτρα για να διοργανώσει κατάλληλα μαθήματα κατάρτισης σχετικά με το κυβερνοέγκλημα για επαγγελματίες –στα οποία θα συμμετέχουν αστυνομικοί, εισαγγελείς και δικαστές– καθώς και για να ενθαρρύνει τους δικαστές να παρακολουθήσουν αυτά τα μαθήματα· (πρβλ. 8.1 και 8.4)

9.2.2. Συστάσεις προς την Ευρωπαϊκή Ένωση, τα θεσμικά της όργανα και τα άλλα κράτη μέλη

1. Τα κράτη μέλη ενθαρρύνονται να εξετάσουν τη δυνατότητα να υποβάλουν αίτηση για να λάβουν χρηματοδοτική βοήθεια από την ΕΕ για εξοπλισμό ΤΠ και επικαιροποιημένο λογισμικό και υλισμικό για εγκληματολογικές έρευνες· (πρβλ. 3.5 και 4.5)

2. Τα κράτη μέλη ενθαρρύνονται να καθιστούν δυνατή τη συμμετοχή εκπροσώπων της Δικαιοσύνης, και ιδίως εισαγγελέων και δικαστών, σε επισκέψεις αξιολόγησης· (πρβλ. 4.1.1 και 4.5)

3. Τα κράτη μέλη θα πρέπει να συμμετέχουν στον διάλογο με τον ιδιωτικό τομέα ώστε να αναζητηθούν δυνατότητες για να επιτευχθεί η διατήρηση δεδομένων, καθώς και για να εξασφαλιστεί η συλλογή πληροφοριών κατά τρόπο που να γίνονται δεκτές στα δικαστήρια· (πρβλ. 4.1.2 και 4.5)

4. Τα κράτη μέλη θα πρέπει να εξετάσουν τη δυνατότητα αξιοποίησης του ΕΔΔ και της αρωγής που προσφέρουν τα σημεία επαφής του, ώστε να προωθηθεί η δικαστική συνεργασία σε ποινικές υποθέσεις· (πρβλ. 7.5.1 και 7.6)

5. Τα κράτη μέλη ενθαρρύνονται να διερευνήσουν τη δυνατότητα να αξιοποιούν τακτικότερα την Eurojust και τα εργαλεία που είναι διαθέσιμα μέσω αυτής, και ιδίως τον εισαγγελέα σύνδεσμο για τις ΗΠΑ στη Eurojust, ώστε να λαμβάνονται ταχύτερα οι απαντήσεις των ΗΠΑ όσον αφορά αιτήσεις ΑΔΣ· (πρβλ. 7.5.1 και 7.6)

6. Τα κράτη μέλη θα πρέπει να προτρέπονται να ενθαρρύνουν τη συμμετοχή μεγάλου φάσματος φορέων και προγραμμάτων στην πρόληψη του κυβερνοεγκλήματος, καθώς και οργανισμών αρμόδιων για την εκπαίδευση των μαθητών πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, ακολουθώντας το παράδειγμα των δράσεων που ανέλαβαν οι κυπριακές αρχές στον τομέα της εκπαίδευσης των παιδιών· (πρβλ. 8.3.1 και 8.4)

7. Τα κράτη μέλη θα πρέπει να ενισχύσουν τις πολιτικές τους που αφορούν την προστασία των παιδιών από κάθε δυνατή βλάβη που είναι πιθανό να υποστούν από ανθρώπους που είναι ήδη αναγνωρισμένοι δράστες σεξουαλικών αδικημάτων· (πρβλ. 8.4)

8. Τα θεσμικά όργανα της ΕΕ θα πρέπει να εξετάσουν το συντομότερο δυνατόν το θέμα της διατήρησης των δεδομένων· (πρβλ. 4.1.2 και 4.5)

9. Η ΕΕ θα πρέπει να συνεχίσει να βελτιώνει τις σχέσεις της με τις ΗΠΑ στον τομέα της καταπολέμησης του κυβερνοεγκλήματος, ιδίως σε ό,τι αφορά τις αιτήσεις ΑΔΣ και τη διεκπεραίωσή τους· (πρβλ. 7.5.1 και 7.6)

ΠΑΡΑΡΤΗΜΑ A: PROGRAMME FOR THE ON-SITE VISIT

7th round of mutual evaluations GENVAL

Cybercrime Evaluation Visit

Nicosia, 18 -20 November 2015

Programme of the Evaluation Visit

17th of November 2015

Arrival of delegates at Larnaca Airport (Transport by CYPOL)

1800 - 1830 Start of meeting at the hotel in Nicosia

18th of November 2015

0830 Departure from the hotel (Transport by CYPOL)

0845Arrival at the Ministry of Justice and Public Order

0900 – 0915 Welcome speech by the Permanent Secretary of the Ministry of Justice and Public Order

0915– 0930Introductory Presentation – Key stakeholders and Structures *(***Ministry of Justice and Public Order)**

0930 – 1030 National Cybersecurity Strategy , Q &A (**Office of the Commissioner for Electronic Communication and Postal Regulation)**

1030 – 1100 Coffee break

1100 – 1130 Government CSIRT, Q &A(**Department of Information Technology**)

1130 – 1200 Law on Preventing and Combating Sexual Abuse and Sexual Exploitation of Children and Child Pornography, Q &A (**MLSI**)

1200 – 1400 Prevention and Awareness - **Cyprus Pedagogical Institute** (**MOEC**)

(Prevention and awareness presentations will cover:

-Current situation

- eSafe schools programme (material, good practices)

- Young coaches for the Internet programme (material, good practices, video)

- Short video production completion

Coffee break

- Hotline and Helpline

- Safer Internet for Children – National Strategy

- Safer Internet Centre

1430 Buffet lunch hosted by the Permanent Secretary of the Ministry of Justice and Public Order, Venue TBC (transport by CYPOL)

1600 Transfer to the hotel (transport by CYPOL)

End of Day 1

19th of November 2015

0830 Departure from hotel (transport by CYPOL)

0845 Arrival at the European Union and International Police Cooperation Directorate, Cyprus Police Headquarters

0900-0915 Welcome speech by the Assistant Chief of Police

0915 –1000 Legal Framework Q & A (**Attorney General's Office TBC**)

100– 1030 Mutual Legal Assistance Q &A (**MJPO)**

1030- 1115 Coffee break

1115 – 1145 Structure of the Cyprus Police, Structures for EU and International Police Cooperation **(EUIPCD, Cyprus Police Headquarters**)

1145– 1215 Police training in International Police Cooperation and Cybercrime, Q & A (**Cyprus Police Academy, Cyprus Police Headquarters)**

1215 – 1315 Cybercrime Unit of the Cyprus Police (**DEPT C, Cyprus Police Headquarters**)

- Mandate/ Investigations
- International Cooperation
- Training (Available exclusively for the members of the OCC)
- Statistics
- "Darkcode" case study

1315 – 1345 Q & A

1345 – 1445 Buffet lunch on premises

1515 –1615 Visit to the Cybercrime Unit of the Cyprus Police, including a presentation on forensic examination (transport by CYPOL)

1615 Transfer to hotel (transport by CYPOL)

1930 Dinner hosted by the Cyprus Police, venue TBC

20th of November 2015

10 00 -11 00Wrap up meeting with evaluators at the hotel (if needed)

Departure of delegates(transport by CYPOL)

ΠΑΡΑΡΤΗΜΑ B: PERSONS INTERVIEWED/MET

Meetings on 18 November 2015

Venue: Ministry of Justice and Public Order

Person interviewed/met	**Organisation represented**
Andreas Mylonas	Permanent Secretary Ministry of Justice and Public Order
Loizos Hadjivasiliou	Ministry of Justice and Public Order
Marios Djiapouras	Government CSIRT (Department of Information Technology Services)
Iliada Spyrou,	Helpline, Hotline and 3CE
Elena Aristodemou	Helpline, Hotline and 3CE
Antonis Antoniades	Commissioner for Electronic Communications and Postal Regulation
Costas Efthymiou	Commissioner for Electronic Communications and Postal Regulation
Anastasia Economou	Ministry of Education and Culture
Andreas Anastasiades	Head of the Office for Combating Cyber Crime and Digital Forensic Lab Police Headquarters
George Karkas	Crime and Criminology Office for Combating Cybercrime & Forensic Lab Cyprus Police Headquarters

Meetings on 19 November 2015

Venue: Cyprus Police Headquarters

Person interviewed/met	**Organisation represented**
Lambros Themistokleous	Assistant Chief of Police
Andreas Anastasiades	Head of the Office for Combating Cyber Crime and Digital Forensic Lab Police Headquarters
George Karkas	Crime and Criminology Office for Combating Cybercrime & Forensic Lab Cyprus Police Headquarters
Maria Mounti	Ministry of Justice and Public Order (MLATs)
Maria Kyrmizi	Senior Counsel, Attorney General's Office, MOKAS Financial Intelligence Unit
Kyriaki Lambrianidou	Cyprus Police Academy
Andreas Papadopoulos	International Cooperation Directorate, Cyprus Police Headquarters

ΠΑΡΑΡΤΗΜΑ Γ: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	CYPRUS OR ACRONYM IN ORIGINAL LANGUAGE	CYPRUS OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CEF	*CEF*		Connecting Europe Facility
CIRT	*CIRT*		Computer Incident Report Team
CNTI	*CNTI*		Cyprus Neuroscience and Technology Institute, NGO
CPI	*CPI*		Cyprus Pedagogical Institute
CyberEthics	*CyberEthics*		Cyprus Neuroscience & Technology Institute
DEFL	*DEFL*		Digital Evidence Forensic Laboratory, Cyprus Police
DITS	*DITS*		Department of Information Technology Services, Ministry of Finance
IAS	*IAS*		Internal Audit Service
INEA	*INEA*		European Commission Innovation and Networks Executive Agency
ISPs	*ISPs*		Internet Service Providers
PCCPWC	*PCCPWC*		Pancyprian Coordinating Committee for the Protection and Welfare for Children
O.C.C.	*O.C.C.*		Office For Combating Cybercrime, Cyprus Police
OCECPR	*OCECPR*		Office of the Commissioner of Electronic Communications and Postal Regulation
3CE	*3CE*		Cyprus Cybercrime Center of Excellence