Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 8 Φεβρουαρίου 2017
(OR. en)

14584/1/16
REV 1 DCL 1

GENVAL 119
CYBER 132

ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ

του εγγράφου:	14584/1/16 REV 1 RESTREINT UE/EU RESTRICTED
Με ημερομηνία:	31 Ιανουαρίου 2017
νέος χαρακτηρισμός:	Έγγραφο προσβάσιμο στο κοινό
Θέμα:	Αξιολογική έκθεση για τον έβδομο γύρο αμοιβαίων αξιολογήσεων "Πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο" - Έκθεση για την Ελλάδα

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, 31 Ιανουαρίου 2017
(OR. en)

14584/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 119
CYBER 132

ΕΚΘΕΣΗ

Θέμα:	Αξιολογική έκθεση για τον έβδομο γύρο αμοιβαίων αξιολογήσεων "Πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο" - Έκθεση για την Ελλάδα

ΠΑΡΑΡΤΗΜΑ

Πίνακας περιεχομένων

1. ΕΚΤΕΛΕΣΤΙΚΗ ΣΥΝΟΨΗ

- Η επίσκεψη αξιολόγησης στην Ελλάδα πραγματοποιήθηκε μεταξύ 29ης Σεπτεμβρίου και 2ας Οκτωβρίου 2015 και ήταν διοργανωμένη εξαιρετικά από τις εθνικές αρχές.

- Το πρόγραμμα της επίσκεψης περιλάμβανε συναντήσεις με πολλούς εκπροσώπους των συμμετεχόντων οργάνων, λ.χ. αστυνομικούς, εισαγγελείς, καθώς και άλλων σχετικών οργάνων και οργανισμών, όπως η Διεύθυνση Ηλεκτρονικού Εγκλήματος, το Υπουργείο Πολιτισμού, Παιδείας και Θρησκευμάτων, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, το Υπουργείο Υποδομών, Μεταφορών και Δικτύων, η Τράπεζα της Ελλάδος, η Ελληνική Ένωση Τραπεζών, και έναν εκπρόσωπο της κοινωνίας των πολιτών.

- Σύμφωνα με την Ομάδα Αξιολόγησης, η επιλογή των εκπροσώπων ήταν η δέουσα, μολονότι μεγαλύτερη παρουσία δικαστικών θα ήταν ενδεχομένως ακόμη πιο ωφέλιμη για την επίσκεψη αξιολόγησης.

- Όλοι οι εκπρόσωποι που συνάντησε η Ομάδα Αξιολόγησης προέβησαν σε ιδιαίτερα λεπτομερείς παρουσιάσεις PowerPoint για τα σχετικά θέματα, συμβάλλοντας στην κατανόηση όλων των πτυχών του συστήματος. Μετά την επίσκεψη αξιολόγησης οι εθνικές αρχές διένειμαν στην ομάδα πρόσθετο σχετικό υλικό.

- Η Ελλάδα δεν έχει υιοθετήσει ακόμη την εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο, αλλά οι αρμόδιες αρχές ασχολούνται ήδη με τη διαμόρφωσή της.

- Όσον αφορά τη νομοθεσία, η Ελλάδα έχει υπογράψει τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, αλλά δεν την έχει επικυρώσει ακόμη. Ούτε εξάλλου η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών έχει μεταφερθεί ακόμη στο εθνικό δίκαιο. Η οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών έχει μεταφερθεί στο εθνικό δίκαιο.

- Οι εθνικές αρχές αναφέρθηκαν σε δυσχέρειες κατά τη συλλογή στατιστικών στοιχείων σχετικά με το έγκλημα στον κυβερνοχώρο. Ωστόσο, μετά την επίσκεψη αξιολόγησης διαβιβάστηκαν πρόσθετα στατιστικά στοιχεία σχετικά με αδικήματα παιδικής πορνογραφίας.

- Υπάρχουν κάποιες εξειδικευμένες μονάδες στην αστυνομία και την εισαγγελία. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος εδρεύει στην Αθήνα και διαθέτει βοηθητική δομή στη Θεσσαλονίκη.

- Η Διατραπεζική Επιτροπή, που συγκροτείται από εκπροσώπους των τραπεζών, της Τράπεζας της Ελλάδος και της ελληνικής αστυνομίας, διοργανώνει συνεδριάσεις για να συζητηθούν νέες τάσεις στην απάτη, συμβάντα και τεχνολογίες αντιμετώπισης. Η Ελληνική Ένωση Τραπεζών διατηρεί καταλόγους επαφών επαγρύπνησης όσον αφορά το έγκλημα στον κυβερνοχώρο («ξάφρισμα» («skimming»), απάτη στο ηλεκτρονικό εμπόριο, κυβερνοεπιθέσεις, απάτη μέσω του Διαδικτύου).

- Τα πιστωτικά ιδρύματα που λειτουργούν στην Ελλάδα υποχρεούνται να αναφέρουν αμελλητί τα επεισόδια κυβερνοεπιθέσεων με στόχο τα πιστωτικά ιδρύματα και/ή τους πελάτες τους.

- Υπάρχει περιθώριο βελτίωσης όσον αφορά την εξειδικευμένη εκπαίδευση των απασχολούμενων στον τομέα. Ωστόσο, η Εθνική Σχολή Δικαστικών Λειτουργών διοργανώνει εξειδικευμένη εκπαίδευση για δικαστές και εισαγγελείς, με συμμετοχή και αστυνομικών.

- Οι εθνικές αρχές διοργανώνουν, μέσω του Υπουργείου Παιδείας και των αστυνομικών υπηρεσιών, εντυπωσιακό αριθμό εκστρατειών πρόληψης και ευαισθητοποίησης για τις σχολικές κοινότητες, που απευθύνονται τόσο στο διδακτικό προσωπικό όσο και στους μαθητές.

2. ΕΙΣΑΓΩΓΗ

Μετά την έγκριση της κοινής δράσης 97/827/ΔΕΥ της 5ης Δεκεμβρίου 1997[1] έχει καθιερωθεί μηχανισμός για την αξιολόγηση της εφαρμογής και υλοποίησης των διεθνών δεσμεύσεων στον τομέα της καταπολέμησης του οργανωμένου εγκλήματος σε εθνικό επίπεδο. Σύμφωνα με το άρθρο 2 της κοινής δράσης, η ομάδα «Γενικές υποθέσεις συμπεριλαμβανομένης 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 αξιόποινων πράξεων που καλύπτονται από τον όρο «έγκλημα στον κυβερνοχώρο», συμφωνήθηκε ότι η αξιολόγηση θα επικεντρωθεί στις αξιόποινες πράξεις στις οποίες τα κράτη μέλη θεωρούν ότι πρέπει να δοθεί ιδιαίτερη προσοχή. Προς τον σκοπό αυτό η αξιολόγηση καλύπτει τρεις συγκεκριμένους τομείς: τις επιθέσεις στον κυβερνοχώρο, 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 για τις επιθέσεις κατά συστημάτων πληροφοριών[3] (ημερομηνία μεταφοράς στο εθνικό δίκαιο: 4 Σεπτεμβρίου 2015) έχουν ιδιαίτερη σημασία εν προκειμένω.

1 Κοινή δράση της 5ης Δεκεμβρίου 1997 (97/827/ΔΕΥ), ΕΕ L 344, 15.12.1997, σ. 7-9.
2 ΕΕ L 335, 17.12.2011, σ. 1.
3 ΕΕ L 218, 14.8.2013, σ. 8.

Επιπλέον, τα συμπεράσματα του Συμβουλίου σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο του Ιουνίου 2013[4] επαναλαμβάνουν τον στόχο της ταχύτερης δυνατής επικύρωσης της Σύμβασης για το έγκλημα στον κυβερνοχώρο (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 την ξενοφοβία και τον ρατσισμό που διαπράττονται μέσω ηλεκτρονικών συστημάτων[6].

Από την πείρα των παλαιότερων αξιολογήσεων προκύπτει ότι τα κράτη μέλη θα είναι σε διαφορετικές θέσεις όσον αφορά την εφαρμογή των σχετικών νομικών πράξεων και η τρέχουσα διαδικασία αξιολόγησης θα μπορούσε να διευκολύνει αρκετά και τα 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 διάφορων πράξεων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο αλλά μάλλον στις λειτουργικές πτυχές στα κράτη μέλη.

Κατά συνέπεια, 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 επιθέσεων στον κυβερνοχώρο 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 τη στήριξη που παρέχεται στα θύματα του εγκλήματος στον κυβερνοχώρο.

[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 2011, 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.

Η σειρά των επισκέψεων στα κράτη μέλη αποφασίστηκε από την ομάδα GENVAL την 1η Απριλίου 2014. Σύμφωνα με το άρθρο 3 της κοινής δράσης, η Προεδρία έχει καταρτίσει κατάλογο εμπειρογνωμόνων για τις αξιολογήσεις που θα πρέπει να διενεργηθούν. Τα κράτη μέλη έχουν διορίσει εμπειρογνώμονες με σημαντικές πρακτικές γνώσεις στον τομέα όπως ζήτησε εγγράφως από τις αντιπροσωπίες στις 28 Ιανουαρίου 2014 ο πρόεδρος της ομάδας GENVAL.

Οι ομάδες αξιολόγησης συγκροτούνται από τρεις εθνικούς εμπειρογνώμονες, με υποστήριξη 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 και η Ευρωπαϊκή Επιτροπή, η Eurojust, ο ENISA και η Ευρωπόλ/EC3.

Οι ομάδες αξιολόγησης συγκροτούνται από τρεις εθνικούς εμπειρογνώμονες, με υποστήριξη 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 και η Ευρωπαϊκή Επιτροπή, η Eurojust, ο ENISA και η Ευρωπόλ/EC3.

Οι εμπειρογνώμονες στους οποίους ανατέθηκε η αξιολόγηση της Ελλάδας ήταν η κα Eneli Laurits (Εσθονία), ο κ. Richard Szongoth (Ουγγαρία) και η κα Ulrika Sundling (Σουηδία), από κοινού με τον κ. Gilles Duval και την κα Carmen Necula 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 Ελλάδα μεταξύ 29ης Σεπτεμβρίου και 2ας Οκτωβρίου 2015 καθώς και τις λεπτομερείς απαντήσεις της Ελλάδας στο ερωτηματολόγιο αξιολόγησης και τις λεπτομερείς απαντήσεις της στις επακόλουθες ερωτήσεις.

3. ΓΕΝΙΚΑ ΘΕΜΑΤΑ ΚΑΙ ΔΟΜΕΣ

3.1. Εθνική στρατηγική κυβερνοασφάλειας

Η Ελλάδα δεν διαθέτει εθνική στρατηγική κυβερνοασφάλειας. Ωστόσο, το Γενικό Επιτελείο Εθνικής Άμυνας/Διεύθυνση Κυβερνοάμυνας (ΓΕΕΘΑ/ΔΙΚΥΒ), με τη συμμετοχή εκπροσώπων του HDPS, ήδη επεξεργάζεται σχετικό κείμενο το οποίο σύντομα θα ολοκληρωθεί και θα προωθηθεί για έγκριση στην ιεραρχία.

Ειδικότερα, ενόψει της επεξεργασίας της πρότασης οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τα μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση (COM(2013) 48 final), πραγματοποιήθηκε σύσκεψη στις 8 Νοεμβρίου 2013 στο Υπουργείο Υποδομών, Μεταφορών και Δικτύων. Κατά τη διάρκεια της σύσκεψης και κατόπιν πρότασης του ΓΕΕΘΑ/ΔΙΚΥΒ να αναλάβει σχετική πρωτοβουλία, αποφασίστηκε να συσταθεί μια άτυπη ομάδα εργασίας για την εκπόνηση εθνικής στρατηγικής κυβερνοασφάλειας. Στην ομάδα εργασίας συμμετείχαν, κατόπιν ανοικτής πρόσκλησης, εκπρόσωποι φορέων της δημόσιας διοίκησης και του ακαδημαϊκού χώρου, συμπεριλαμβανομένης της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.ΔΑΕ). Η πρόοδος των εργασιών της ομάδας εργασίας και τα ενδιάμεσα αποτελέσματα παρουσιάζονταν και συζητούνταν με ένα ευρύτερο κοινό, που επιπλέον περιλάμβανε εκπροσώπους των παρόχων ηλεκτρονικών επικοινωνιών αλλά και κρίσιμων υποδομών της χώρας.

Στα τέλη του 2014, το ΓΕΕΘΑ έδωσε σε δημοσιότητα και έθεσε σε άτυπη διαβούλευση το τελικό προσχέδιο της εθνικής στρατηγικής κυβερνοασφάλειας. Σε συσκέψεις που πραγματοποιήθηκαν εντός του 2015 στο ΓΕΕΘΑ, στο πλαίσιο της οργάνωσης της άσκησης ΠΑΝΟΠΤΗΣ 2015, οι εκπρόσωποί του ενημέρωσαν ότι το προσχέδιο βρίσκεται υπό περαιτέρω επεξεργασία, η οποία αναμένεται να ολοκληρωθεί μέχρι τα μέσα Ιουλίου 2015, οπότε ακολούθως θα προωθηθεί για έγκριση στην ηγεσία του ΓΕΕΘΑ.

Το προσχέδιο της εθνικής στρατηγικής κυβερνοασφάλειας συνοπτικά περιλαμβάνει το «εθνικό στρατηγικό όραμα για την κυβερνοασφάλεια» (γενικές αρχές και στρατηγικές κατευθύνσεις που διέπουν την εθνική στρατηγική), την οργανωτική δομή και το μοντέλο διακυβέρνησης, καθώς και το σύνολο των δράσεων που απαιτείται να υλοποιηθούν προκειμένου να επιτευχθούν οι στρατηγικοί στόχοι. Το πλαίσιο των δράσεων-ενεργειών που θα πρέπει να πραγματοποιηθούν κατά τη διάρκεια υλοποίησης της εθνικής στρατηγικής κυβερνοασφάλειας συνοψίζεται στα εξής: Καθορισμός των φορέων που συμμετέχουν στην εθνική στρατηγική, Καταγραφή των πληροφοριακών συστημάτων κρίσιμων υποδομών και αποτίμηση επικινδυνότητας σε εθνικό επίπεδο, Καταγραφή υφιστάμενου θεσμικού πλαισίου, Εθνικό σχέδιο έκτακτης ανάγκης στον κυβερνοχώρο, Καθορισμός βασικών απαιτήσεων ασφάλειας, Αντιμετώπιση περιστατικών ασφάλειας, εθνικές ασκήσεις ετοιμότητας, Ευαισθητοποίηση χρηστών-πολιτών, Μηχανισμοί αξιόπιστης ανταλλαγής πληροφοριών, Υποστήριξη ερευνητικών και αναπτυξιακών προγραμμάτων και ακαδημαϊκών προγραμμάτων εκπαίδευσης, Συνεργασίες σε διεθνές επίπεδο και, τέλος, Αξιολόγηση και αναθεώρηση της εθνικής στρατηγικής.

3.2.Εθνικές προτεραιότητες όσον αφορά το έγκλημα στον κυβερνοχώρο

Το Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης – Αρχηγείο Ελληνικής Αστυνομίας εκπόνησε Πρόγραμμα Αντεγκληματικής Πολιτικής των ετών 2015-2019, το οποίο αποτελεί κεντρικό σημείο αναφοράς για όλες τις αστυνομικές υπηρεσίες. Το εν λόγω πρόγραμμα αποτελεί συνέχεια του Προγράμματος Αντεγκληματικής Πολιτικής των ετών 2010-2014.

- ✓ Η Αντεγκληματική Πολιτική των ετών 2015-2019 χωρίζεται σε τέσσερα βασικά θέματα.
- ✓ Ειδικότερα ως στόχοι προς ενίσχυση της ασφάλειας στον κυβερνοχώρο έχουν τεθεί τα εξής:
- ✓ Εντοπισμός μεμονωμένων προσώπων ή δικτύων που δραστηριοποιούνται στη διακίνηση παιδικής πορνογραφίας
- ✓ Καταπολέμηση του εκφοβισμού μέσω του Διαδικτύου (cyber bullying)
- ✓ Καταπολέμηση της απάτης μέσω του Διαδικτύου
- ✓ Καταπολέμηση της διακίνησης πλαστών ταξιδιωτικών εγγράφων και ναρκωτικών μέσω του Διαδικτύου

- ✓ Καταπολέμηση της αλίευσης θυμάτων εμπορίας ανθρώπων μέσω του Διαδικτύου
- ✓ Καταπολέμηση εισβολών-κυβερνοεπιθέσεων
- ✓ Αποτροπή αυτοκτονιών που ανακοινώνονται στο Διαδίκτυο
- ✓ Προς επίτευξη των εν λόγω στόχων, προβλέπονται εξειδικευμένες δράσεις, ως ακολούθως:
- ✓ Διαρκής εκπαίδευση-επιμόρφωση του προσωπικού της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος τόσο στην Ελλάδα όσο και στο εξωτερικό.
- ✓ Αναβάθμιση της εκπαίδευσης και διαρκούς επιμόρφωσης των στελεχών της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος.
- ✓ Αξιοποίηση από τις περιφερειακές υπηρεσίες των κατευθυντήριων οδηγιών για την αντιμετώπιση των απατών με τη μέθοδο του «ξαφρίσματος», βάσει εκπονηθέντος εγχειριδίου, που διαβιβάστηκε από τη Διεύθυνση Δημόσιας Ασφάλειας/ΑΕΑ σε όλες τις υπηρεσίες της Ελληνικής Αστυνομίας το έτος 2009.
- ✓ Συνεργασία των περιφερειακών υπηρεσιών με την καθ' ύλη αρμόδια Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, προκειμένου, στις περιπτώσεις κατά τις οποίες επισημαίνονται αδικήματα που διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή, να μεθοδεύονται από κοινού ο ενδεδειγμένος τρόπος εξασφάλισης των αποδεικτικών στοιχείων και ο περαιτέρω χειρισμός των περιπτώσεων.
- ✓ Ενδυνάμωση της συνεργασίας με την Ελληνική Ένωση Τραπεζών, με σκοπό την πρόληψη και αποτελεσματική αντιμετώπιση των κρουσμάτων απάτης μέσω του Διαδικτύου, που προσβάλλουν το χρηματοπιστωτικό σύστημα της χώρας.
- ✓ Ενεργός συμμετοχή σε διαδικασίες ενημέρωσης του κοινού, για την ασφαλή χρήση του Διαδικτύου και τους κινδύνους που ελλοχεύουν σε αυτό.

- ✓ Πραγματοποίηση ενημερωτικών ημερίδων-διαλέξεων σε γονείς και μαθητές για την παροχή πληροφοριών και συμβουλών για την ασφαλή χρήση του Διαδικτύου και την αποφυγή θυματοποίησής τους.
- ✓ Ενδυνάμωση της συνεργασίας με αλλοδαπές αρμόδιες διωκτικές αρχές, μέσω των θεσμοθετημένων διαύλων επικοινωνίας (INTERPOL, Ευρωπόλ, EUROJUST κ.λπ.) προκειμένου να επιτρέπονται ο εντοπισμός και η εξιχνίαση εγκλημάτων με διεθνικό χαρακτήρα που τελούνται στο Διαδίκτυο ή με τη χρήση αυτού.
- ✓ Καθημερινή «περιπολία» στους χώρους του Διαδικτύου για την πρόληψη και καταστολή εγκληματικών πράξεων.
- ✓ Εφαρμογή του μνημονίου αστυνομικών ενεργειών για τη διαχείριση εκδήλωσης πρόθεσης αυτοκτονίας.

Από τα ανωτέρω καθίσταται σαφές ότι η Ελληνική Αστυνομία έχει εναρμονιστεί πλήρως με τους στρατηγικούς στόχους και τα λειτουργικά πλάνα δράσης που έχουν τεθεί για την καταπολέμηση σε επίπεδο ΕΕ του σοβαρού και οργανωμένου εγκλήματος για το χρονικό διάστημα 2014-2017, όπως αυτά αποτυπώνονται στα συμπεράσματα του Συμβουλίου που περιλαμβάνονται στο έγγραφο 12095/13. Επισημαίνεται δε ότι, σύμφωνα και με το περιεχόμενο του προαναφερόμενου εγγράφου, οι προτεραιότητες της ΕΕ για ζητήματα καταπολέμησης του ηλεκτρονικού εγκλήματος εστιάζονται στη διαδικτυακή απάτη με κάρτες πληρωμών, στα εγκλήματα στον κυβερνοχώρο που προκαλούν σοβαρές βλάβες στα θύματά τους, όπως η σεξουαλική εκμετάλλευση παιδιών μέσω του Διαδικτύου, και επιθέσεις στον κυβερνοχώρο που επηρεάζουν βασικά συστήματα υποδομών και πληροφοριών στην ΕΕ.

Εξάλλου, το ΓΕΕΘΑ/ΔΙΚΥΒ διαθέτει σχέδιο δράσης ανάπτυξης κυβερνοάμυνας στις Ένοπλες Δυνάμεις και συχνά εκδίδει οδηγίες πρόληψης και αντιμετώπισης κυβερνοπεριστατικών, ενώ μέρος του υλικού διατίθεται και στο ευρύ κοινό μέσω της ιστοσελίδας του ΓΕΕΘΑ (http://www.geetha.mil.gr).

Επιπλέον, η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής «ΕΑΠΔΠΧ»), μολονότι δεν εντάσσεται επίσημα σε καμία εθνική στρατηγική, ως αρμόδια αρχή προστασίας δεδομένων για την Ελλάδα επιδιώκει διαρκώς την ευαισθητοποίηση του κοινού σε θέματα εγκλήματος στον κυβερνοχώρο που σχετίζονται με την προστασία των δεδομένων. Στην ιστοσελίδα της, λ.χ., υπάρχουν εξειδικευμένα τμήματα για θέματα όπως η κλοπή ταυτότητας, η αποστολή ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam), καθώς και ειδικό τμήμα που απευθύνεται στους νέους και επικεντρώνεται στην προστασία της ιδιωτικής τους ζωής στο Διαδίκτυο.

Τέλος, το Ελληνικό Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων έχει ως κύρια προτεραιότητα τη μεταφορά των νομικών πράξεων διεθνούς και ευρωπαϊκού δικαίου στο εσωτερικό δίκαιο. Προς τον σκοπό αυτό, έχει συστήσει ειδική νομοθετική επιτροπή για την επικύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβασης της Βουδαπέστης), που υπεγράφη από την Ελλάδα στις 23.11.2001, αλλά δεν έχει επικυρωθεί ακόμη. Επιπλέον, το έργο της επιτροπής αυτής περιλαμβάνει τη μεταφορά στο εσωτερικό δίκαιο της οδηγίας 2013/40/ΕΕ «για τις επιθέσεις κατά συστημάτων πληροφοριών». Αναμένεται ότι το σχέδιο της επιτροπής θα υποβληθεί σύντομα.

3.3.Στατιστικά στοιχεία σχετικά με το έγκλημα στον κυβερνοχώρο

Η Ελλάδα δεν συλλέγει χωριστά στατιστικά στοιχεία σχετικά με το έγκλημα στον κυβερνοχώρο. Η τελευταία ετήσια έκθεση δημοσιεύτηκε γύρω στο 2013. Συνολικά υποβλήθηκαν 562 καταγγελίες, 214 από τις οποίες αφορούσαν ηλεκτρονικές επικοινωνίες. Ωστόσο, ο αριθμός αυτός δεν είναι ενδεικτικός. Ορισμένες μόνο από τις περιπτώσεις αυτές συνδέονταν με εγκλήματα στον κυβερνοχώρο, αλλά στην έκθεση δεν υπήρχε σχετικός χαρακτηρισμός και κατά συνέπεια δεν μπορούν να παρασχεθούν στατιστικά στοιχεία.

Ωστόσο, μετά την επίσκεψη αξιολόγησης οι εθνικές αρχές διαβίβασαν κάποια στατιστικά στοιχεία σχετικά με την παιδική πορνογραφία, που αφορούν τον αριθμό των υποθέσεων στις δικαστικές περιφέρειες (για το 2012) και τον αριθμό των υποθέσεων στο Πρωτοδικείο Αθηνών (2013-2015).

3.3.1. Κύριες τάσεις του εγκλήματος στον κυβερνοχώρο

Από τα στατιστικά στοιχεία που έχει στη διάθεσή της η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος φαίνεται ότι ο ετήσιος αριθμός των υποθέσεων που χειρίζεται έχει αυξηθεί σημαντικά, ωστόσο παρουσιάζει μια τάση σταθεροποίησης (σε υψηλό επίπεδο).

Σημαντική αύξηση παρουσιάζουν οι απάτες που τελούνται μέσω του Διαδικτύου, ενώ παρατηρείται σημαντική εξέλιξη στην πολυπλοκότητα των μεθόδων που χρησιμοποιούν οι εγκληματίες. Αύξηση παρατηρείται επίσης στα εγκλήματα σε βάρος της γενετήσιας αξιοπρέπειας των ανηλίκων και της πορνογραφίας ανηλίκων. Αναφορικά με τις κυβερνοεπιθέσεις, δεν έχουν παρατηρηθεί αξιόλογες μεταβολές, δηλαδή ο αριθμός τους παραμένει χαμηλός σε σχέση με τα δεδομένα των υπόλοιπων κρατών μελών της Ευρωπαϊκής Ένωσης.

Από την άλλη πλευρά, στην τελευταία ετήσια έκθεση που δημοσίευσε η ΕΑΠΔΠΧ το 2013, από τις 562 καταγγελίες που υποβλήθηκαν συνολικά οι 214 αφορούσαν τις ηλεκτρονικές επικοινωνίες. Ωστόσο, ο αριθμός αυτός δεν είναι ενδεικτικός. Ορισμένες μόνο από τις υποθέσεις αυτές συνδέονταν με εγκλήματα στον κυβερνοχώρο, αλλά στην έκθεσή της δεν υπάρχει σχετικός χαρακτηρισμός και κατά συνέπεια δεν μπορούν να παρασχεθούν στατιστικά στοιχεία. Η γενική αυτή κατηγορία μπορεί να περιλαμβάνει καταγγελίες για υποθέσεις που συνδέονται με παρακολουθήσεις τηλεφώνων, ανάρτηση δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο χωρίς εξουσιοδότηση (λ.χ. βίντεο ή φωτογραφιών), κοινωνική μηχανική, παραβιάσεις δεδομένων κ.λπ.

3.3.2. Αριθμός καταγεγραμμένων υποθέσεων εγκλήματος στον κυβερνοχώρο

Τα στατιστικά στοιχεία που έχει στη διάθεσή της η Ελληνική Αστυνομία αφορούν μόνο τις υποθέσεις των οποίων επιλαμβάνεται η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Τα πιστωτικά ιδρύματα («τράπεζες») που λειτουργούν στην Ελλάδα αποστέλλουν τακτικά ανά εξάμηνο στην Τράπεζα της Ελλάδος στατιστικά δεδομένα όσον αφορά τον αριθμό, την αξία και την κατανομή των οικονομικών ζημιών από απάτες με κάρτες πληρωμών. Μια από τις κύριες κατηγορίες απάτης για τις οποίες υποβάλλονται στατιστικά στοιχεία είναι εκείνη που αφορά συναλλαγές χωρίς φυσική παρουσία της κάρτας (CNP/Card-Not-Present) μέσω Διαδικτύου, ηλεκτρονικού ταχυδρομείου και/ή τηλεφώνου. Επιπλέον, στατιστικά δεδομένα σχετικά με κυβερνοεπιθέσεις (λ.χ. phishing, κακόβουλα λογισμικά, κατανεμημένη άρνηση υπηρεσίας-DDoS) υποβάλλονται σε ετήσια βάση στο Τμήμα Πληροφοριακών Συστημάτων Εποπτευόμενων Εταιρειών της Τράπεζας της Ελλάδος.

Επιπλέον, η Τράπεζα της Ελλάδος λαμβάνει ad hoc και τακτικές αναφορές σχετικά με μείζονα περιστατικά που διαταράσσουν τη λειτουργία των ιδρυμάτων, περιλαμβανομένων των κυβερνοεπιθέσεων (λ.χ. phishing, κακόβουλων λογισμικών, κατανεμημένης άρνησης υπηρεσίας-DDoS). Τα πιστωτικά ιδρύματα υποχρεούνται εξάλλου να αναφέρουν αμελλητί τα μείζονα περιστατικά ασφαλείας (λ.χ. κυβερνοεπιθέσεις, απάτες με κάρτες και ηλεκτρονικές τραπεζικές συναλλαγές, κακόβουλα λογισμικά, DDoS) στην Τράπεζα της Ελλάδος. Οι αναφορές αυτές περιλαμβάνουν τα εξής: χρονοσφραγίδα και διάρκεια του περιστατικού, περιγραφή του, αιτίες που το προκάλεσαν και τρόπο ενεργοποίησης, ληφθέντα μέτρα, σοβαρότητα και αντίκτυπο του περιστατικού.

Επίσημες πληροφορίες από την ιστοσελίδα www.hellenicpolice.gr

2013: Δραστηριότητα της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

Θετική αποτυπώνεται η συμβολή της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος για το έτος 2013 στην αντιμετώπιση του οικονομικού και του ηλεκτρονικού εγκλήματος.

Στις σημαντικές επιτυχίες της συγκαταλέγονται η οργάνωση και υλοποίηση εκτεταμένων αστυνομικών επιχειρήσεων για την καταπολέμηση της παράνομης διακίνησης φαρμακευτικών προϊόντων, η σύλληψη εμπλεκόμενων σε ηλεκτρονικές απάτες, η ταυτοποίηση και σύλληψη δραστών για εγκληματικές δραστηριότητες που έλαβαν χώρα στα μέσα κοινωνική δικτύωσης (social media), καθώς και ο εντοπισμός και η περαιτέρω διαχείριση αρκετών εγκληματικών και αντικοινωνικών συμπεριφορών που αφορούν τη φορολογική νομοθεσία.

Επισημαίνεται ότι, το έτος 2013, ο ειδικός τηλεφωνικός αριθμός καταγγελιών 11012 της Οικονομικής Αστυνομίας δέχτηκε συνολικά 4.027 καταγγελίες. Οι καταγγελίες αυτές ομαδοποιούνται, κατά γεωγραφική περιοχή και είδος παράνομης δραστηριότητας, εξετάζονται από επιτροπές αξιολόγησης και προωθούνται στα τμήματα της Οικονομικής Αστυνομίας και της Δίωξης Ηλεκτρονικού Εγκλήματος για περαιτέρω αστυνομική έρευνα. Από το σύνολο των καταγγελιών οι 1.679 έγιναν επώνυμα, ενώ οι 2.348 ανώνυμα.

ΚΑΤΑΓΓΕΛΙΕΣ ΠΟΥ ΕΛΑΒΕ Η ΟΙΚΟΝΟΜΙΚΗ ΑΣΤΥΝΟΜΙΑ – ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.157 Τηλεφωνικές (54%)

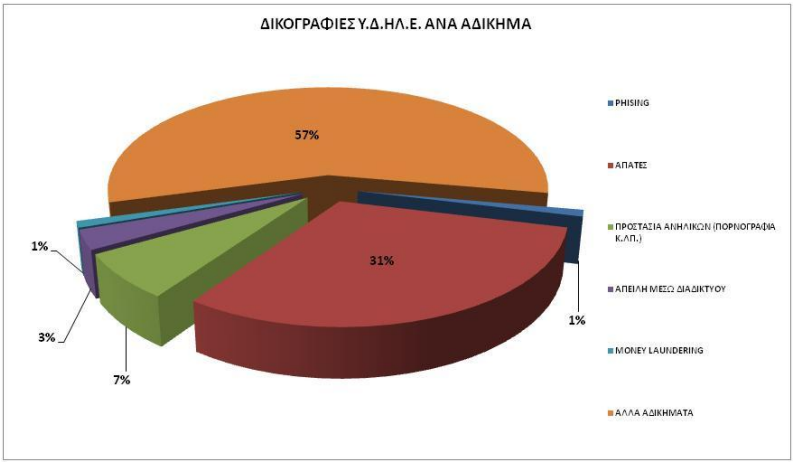
1.117 Ηλεκτρονικό ταχυδρομείο (28%)

583 Ταχυδρομείο (14%)

92 Fax (2%)

78 Αυτοπρόσωπες (2%)

Στον τομέα της ηλεκτρονικής - διαδικτυακής μορφής εγκληματικών συμπεριφορών, η Δίωξη Ηλεκτρονικού Εγκλήματος, χειρίστηκε 1.189 δικογραφίες για πληθώρα διαδικτυακών ή ηλεκτρονικών εγκλημάτων, από τις οποίες οι 292 σχηματίστηκαν αυτεπαγγέλτως, ενώ οι 897 κατόπιν εισαγγελικής παραγγελίας, ύστερα από καταγγελίες πολιτών.

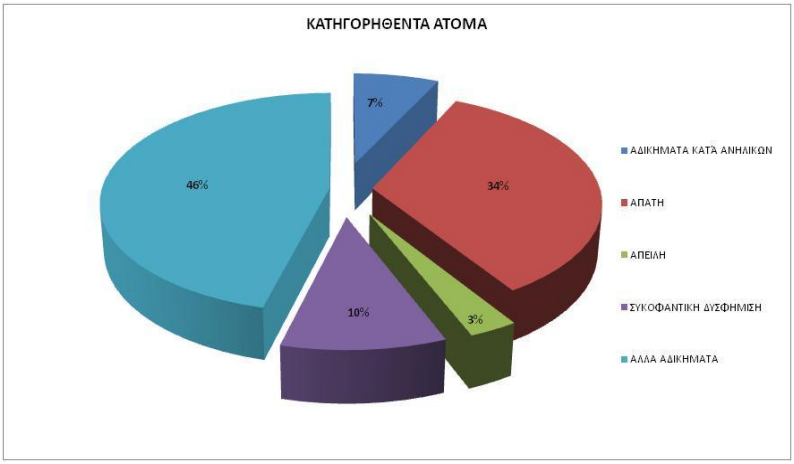


57% ΑΛΛΑ ΑΔΙΚΗΜΑΤΑ *1% PHISHING*
31% ΑΠΑΤΕΣ *1% ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΩΝ*
7% ΠΡΟΣΤΑΣΙΑ ΑΝΗΛΙΚΩΝ (Παιδική πορνογραφία κ.λπ.)
3% ΑΠΕΙΛΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Από τις παραπάνω υποθέσεις, στις 104 ακολουθήθηκε αστυνομική έρευνα και σχηματίστηκε δικογραφία από κλιμάκια της Δίωξης Ηλεκτρονικού Εγκλήματος, ύστερα από καταγγελίες πολιτών, φορέων προστασίας καταναλωτών, οργανισμών, χρηματοπιστωτικών ιδρυμάτων, εταιρειών τηλεπικοινωνιών κ.λπ.

Επιπλέον, στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol και Ευρωπόλ), η Υποδιεύθυνση Δίωξης Ηλεκτρονικού εγκλήματος διαχειρίστηκε 414 αιτήματα συνεργασίας. Τα αιτήματα αφορούσαν περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα και αφορούσαν το ηλεκτρονικό εμπόριο, τις απάτες μέσω του Διαδικτύου, τις αρπαγές στοιχείων και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοσελίδες ηλεκτρονικών οικονομικών δραστηριοτήτων.

Συνολικά έχουν αποδοθεί κατηγορίες σε 1.030 άτομα για διάφορα αδικήματα.



ΚΑΤΗΓΟΡΟΥΜΕΝΟΙ:
46% Άλλα αδικήματα
34% Απάτη
10% Συκοφαντική δυσφήμηση
7% Αδικήματα κατά ανηλίκων
3% Απειλή

2014: Δραστηριότητα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, κατά το έτος 2014, ανέπτυξε πλήθος δράσεων, αφενός στον τομέα της δίωξης των εγκλημάτων που διαπράττονται μέσω Διαδικτύου και αφετέρου στον τομέα της πρόληψης και ενημέρωσης των πολιτών για ζητήματα ασφαλούς πλοήγησης στο Διαδίκτυο.

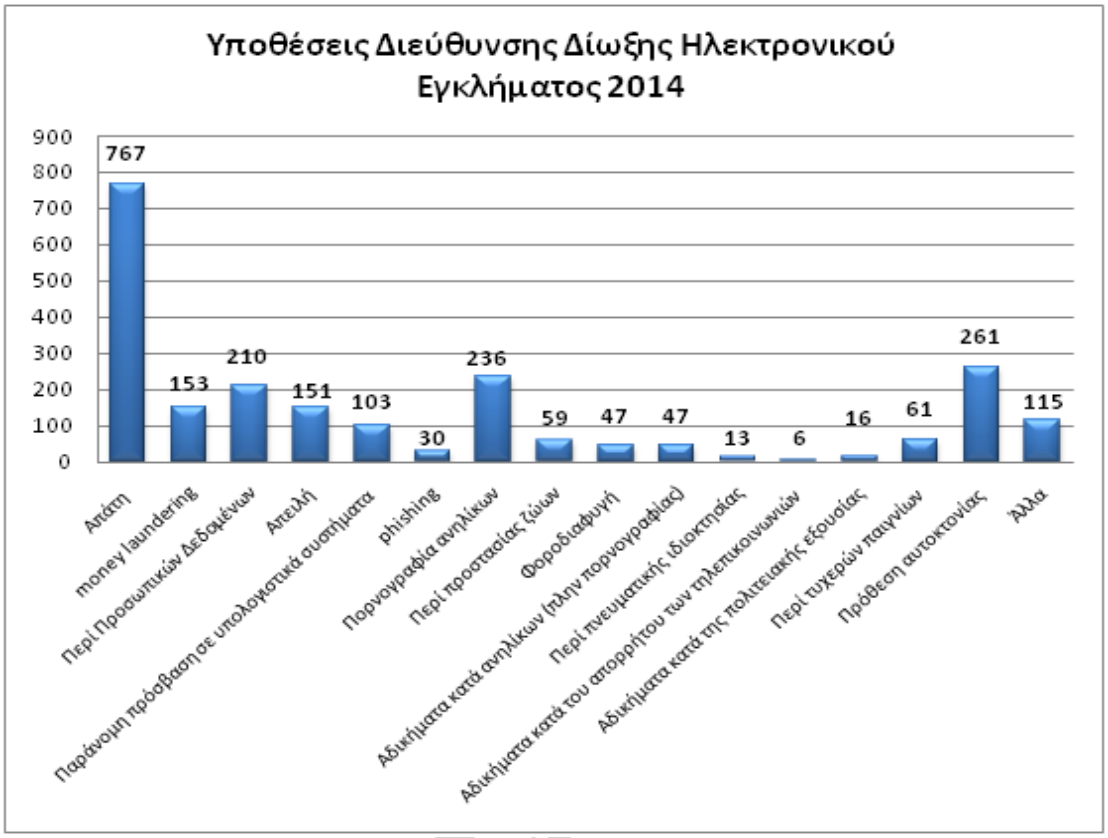
Για την εκπλήρωση της αποστολής της, συνεργάστηκε με άλλες αρμόδιες κεντρικές και περιφερειακές υπηρεσίες της Ελληνικής Αστυνομίας, ενώ μεγάλος όγκος πληροφοριών διακινήθηκε από και προς τη Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας και ειδικότερα την Εθνική Μονάδα Ευρωπόλ και το Τμήμα Διεθνών Οργανισμών – Interpol.

Παράλληλα, συνεχίστηκαν οι δράσεις για την υλοποίηση του Εθνικού Επιχειρησιακού Προγράμματος Καταπολέμησης της Φοροδιαφυγής, με τον αριθμό τους να ανέρχεται σε 150.

Σύνολο υποθέσεων

Ο συνολικός αριθμός νέων υποθέσεων που χειρίστηκε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος το έτος 2014 ανήλθε σε 2.275. Ειδικότερα, κατά περίπτωση:

Υποθέσεις της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, 2014



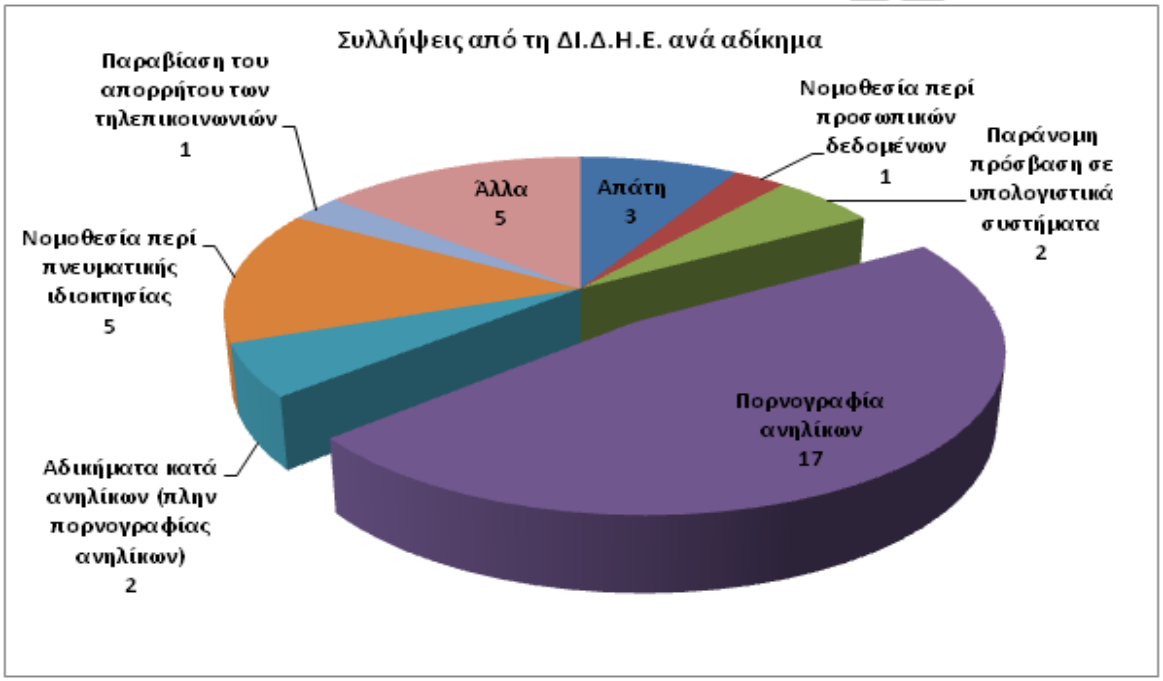
[767 Απάτη, 153 Ξέπλυμα χρημάτων, 210 Περί δεδομένων προσωπικού χαρακτήρα, 151 Απειλή, 103 Παράνομη πρόσβαση σε υπολογιστικά συστήματα, 30 Phishing, 236 Πορνογραφία ανηλίκων, 59 Περί προστασίας των ζώων, 47 Φοροδιαφυγή, 47 Αδικήματα κατά ανηλίκων (πλην πορνογραφίας ανηλίκων), 13 Περί πνευματικής ιδιοκτησίας, 6 Αδικήματα κατά του απορρήτου των τηλεπικοινωνιών, 16 Αδικήματα κατά της πολιτειακής εξουσίας, 61 Περί τυχερών παιγνίων, 261 Πρόθεση αυτοκτονίας, 115 Άλλα]

Από αυτές, οι 102 δικογραφίες σχηματίστηκαν κατόπιν καταγγελιών φορέων προστασίας καταναλωτών, οργανισμών, χρηματοπιστωτικών ιδρυμάτων, εταιρειών τηλεπικοινωνιών, καθώς και καταστημάτων ηλεκτρονικού εμπορίου (e-shops).

Επίσης, στο πλαίσιο της διεθνούς αστυνομικής συνεργασίας (Interpol και Ευρωπόλ), η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διαχειρίστηκε 573 αιτήματα συνεργασίας. Τα αιτήματα αφορούν περιπτώσεις διακρατικών αστυνομικών ερευνών, που είχαν ως αντικείμενο κακουργηματικού χαρακτήρα ηλεκτρονικά εγκλήματα και αφορούσαν σε πορνογραφία ανηλίκων, στο ηλεκτρονικό εμπόριο, στις διαδικτυακές απάτες, στις υφαρπαγές στοιχείων και κωδικών πρόσβασης σε ηλεκτρονικές βάσεις, πλατφόρμες και ιστοσελίδες ηλεκτρονικών οικονομικών δραστηριοτήτων.

<u>Συλλήψεις – Απαγγελθείσες κατηγορίες</u>

Συνελήφθησαν συνολικά 36 άτομα για τα ακόλουθα αδικήματα:



ΣΥΛΛΗΨΕΙΣ ΑΠΟ ΤΗ ΔΙ.Δ.Η.Ε *ΑΝΑ ΑΔΙΚΗΜΑ*

Παραβίαση του απορρήτου των τηλεπικοινωνιών: 1

Νομοθεσία περί προσωπικών δεδομένων: 5

Αδικήματα κατά ανηλίκων (πλην πορνογραφίας ανηλίκων): 2

Νομοθεσία περί προσωπικών δεδομένων: 1

Παράνομη πρόσβαση σε υπολογιστικά συστήματα: 2

Λοιπά: 5

Απάτη: 3

Πορνογραφία ανηλίκων: 17

Επίσης, αποδόθηκαν κατηγορίες σε 1.032 άτομα, στο πλαίσιο δικογραφιών τακτικής διαδικασίας.

Εισαγγελικές παραγγελίες

Κατά το έτος 2014, διαβιβάστηκαν προς εκτέλεση 1.244 εισαγγελικές παραγγελίες για προκαταρκτική εξέταση ή προανάκριση, από όλες τις Εισαγγελίες Πρωτοδικών της Χώρας.

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

Η πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο αποτελεί μέρος του ευρύτερου πλαισίου λειτουργίας της Ελληνικής Αστυνομίας και των συναρμόδιων φορέων. Δεν υπάρχει συγκεκριμένο ποσό στον προϋπολογισμό της Ελληνικής Αστυνομίας που να προορίζεται αποκλειστικά για την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο, πέραν της παγίας προκαταβολής της ΔΙ.Δ.Η.Ε., που αντιστοιχεί σε δαπάνες λειτουργίας της υπηρεσίας (αναλώσιμα υλικά, οδοιπορικά έξοδα σε περιπτώσεις μετακίνησης του προσωπικού κ.λπ.).

Έμμεσα, η συμμετοχή της Ελληνικής Αστυνομίας στην προτεραιότητα «Έγκλημα στον κυβερνοχώρο» του προγράμματος EMPACT του Κύκλου Πολιτικής της Ευρωπαϊκής Ένωσης και συγκεκριμένα στις υποπροτεραιότητες «Απάτες με κάρτες πληρωμών», «Σεξουαλική εκμετάλλευση παιδιών» και «Κυβερνοεπιθέσεις», αποδεικνύεται αρκετά χρήσιμη. Επίσης, σε εξέλιξη βρίσκεται το συγχρηματοδοτούμενο από πόρους του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (Ε.Σ.Π.Α.) έργο για το ηλεκτρονικό έγκλημα, προϋπολογισμού περίπου 2,5 εκατομμυρίων ευρώ. Περιλαμβάνει τη δημιουργία επιχειρησιακού μηχανογραφικού κέντρου με την προμήθεια μηχανογραφικού εξοπλισμού, κατάλληλου λογισμικού αυτοματοποιημένης αναζήτησης στο Διαδίκτυο και αποθήκευσης δεδομένων. Το έργο υλοποιείται σταδιακά, με ευθύνη της Κοινωνίας της Πληροφορίας Α.Ε. (Κ.τ.Π. Α.Ε.) και σύμφωνα με το χρονοδιάγραμμα θα είναι σε πλήρη λειτουργία πριν από το τέλος Οκτωβρίου του 2015.

Επιπλέον, η αρμόδια υπηρεσία της Ελληνικής Αστυνομίας, ήτοι η Υπηρεσία Διαχείρισης Ευρωπαϊκών και Αναπτυξιακών Προγραμμάτων, στο πλαίσιο της κατάρτισης και υποβολής του Πολυετούς Προγράμματος 2014-2020 για το Ταμείο Εσωτερικής Ασφάλειας (ISF), διαπραγματεύεται με την Ευρωπαϊκή Επιτροπή προκειμένου να εγκριθεί το τελικό σχέδιο του προαναφερόμενου προγράμματος.

Αναφορικά με την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο από την προαναφερόμενη υπηρεσία, με πρωτοβουλία της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, έχει ενταχθεί προς χρηματοδότηση δράση με τίτλο: «Δημιουργία Ελληνικού Κέντρου για το Ηλεκτρονικό Έγκλημα», με προϋπολογισμό έργου ύψους 900.000,00 €, η οποία σχεδιάζεται να έχει τις ακόλουθες αρμοδιότητες, επιγραμματικά:

- Σχεδιασμός και υλοποίηση εθνικής στρατηγικής για την πρόληψη του εγκλήματος στον κυβερνοχώρο.
- Αναγνώριση και καταγραφή των πληροφοριακών υποδομών της χώρας και υλοποίηση σχεδίου επιχειρηματικής συνέχειας των υποδομών αυτών.
- Εκπαίδευση αστυνομικού προσωπικού.
- Δημιουργία διαδικτυακής πύλης (Portal) ενημέρωσης του κοινού.
- Αύξηση της ευαισθητοποίησης των πολιτών.
- Υποστήριξη της ενεργής συμμετοχής των ελληνικών αρχών σε προγράμματα και δράσεις του ΕC/Ευρωπόλ.
- Εξασφάλιση της βέλτιστης συνεργασίας και συντονισμού όλων των συμμετεχόντων φορέων, σε εθνικό επίπεδο, συμπεριλαμβανομένου του ακαδημαϊκού και ιδιωτικού τομέα.
- Δημιουργία σημείου επαφής με τα διεθνή κέντρα αριστείας για το έγκλημα στον κυβερνοχώρο.

3.5.Συμπεράσματα

- Οι αρμόδιες ελληνικές αρχές θεωρούν το έγκλημα στον κυβερνοχώρο ως σοβαρή απειλή για το κράτος και την κοινωνία και, κατά συνέπεια, ευρύ φάσμα αρχών είναι επιφορτισμένο με την καταπολέμηση του εγκλήματος αυτού. Η οργάνωση της επιβολής του νόμου και η συνεργασία με τον ιδιωτικό τομέα κατά τις δραστηριότητες πρόληψης φαίνονται αποτελεσματικές και προδραστικές.
- Δεν υφίσταται στην Ελλάδα συνολική εθνική στρατηγική κυβερνοασφάλειας. Ωστόσο, οι εθνικές αρχές έχουν συστήσει ομάδα εργασίας για την εκπόνηση εθνικής στρατηγικής κυβερνοασφάλειας. Κατά την επίσκεψη αξιολόγησης δεν είχε ολοκληρωθεί ακόμη η επεξεργασία του προσχεδίου. Κατά τη γνώμη της Ομάδας Αξιολόγησης, η στρατηγική, από κοινού με τις προτεραιότητες που θα καθοριστούν και σχέδιο δράσης, θα αποτελέσει στέρεη βάση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

- Η Ελλάδα έχει καθορίσει σαφώς τις εθνικές της προτεραιότητες όσον αφορά τον χειρισμό του εγκλήματος στον κυβερνοχώρο. Το Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης – Αρχηγείο Ελληνικής Αστυνομίας εκπόνησε Πρόγραμμα Αντεγκληματικής Πολιτικής των ετών 2015-2019, το οποίο αποτελεί κεντρικό σημείο αναφοράς για όλες τις αστυνομικές υπηρεσίες. Το εν λόγω πρόγραμμα αποτελεί συνέχεια του Προγράμματος Αντεγκληματικής Πολιτικής των ετών 2010-2014, το οποίο θέτει στόχους για τα επόμενα έτη. Ειδικότερα ως στόχοι προς ενίσχυση της ασφάλειας στον κυβερνοχώρο έχουν τεθεί ο εντοπισμός μεμονωμένων προσώπων ή δικτύων που δραστηριοποιούνται στη διακίνηση παιδικής πορνογραφίας, η καταπολέμηση του εκφοβισμού μέσω Διαδικτύου (cyber bullying), η καταπολέμηση της διαδικτυακής απάτης, η καταπολέμηση της διακίνησης πλαστών ταξιδιωτικών εγγράφων και ναρκωτικών μέσω Διαδικτύου, η καταπολέμηση της αλίευσης θυμάτων εμπορίας ανθρώπων μέσω Διαδικτύου, η καταπολέμηση εισβολών-κυβερνοεπιθέσεων και η αποτροπή αυτοκτονιών που ανακοινώνονται στο Διαδίκτυο.
- Η στενή συνεργασία μεταξύ ιδιωτικού τομέα και δημόσιων οργανισμών δημιουργεί μοναδική ευκαιρία για τη συμμετοχή ευρέος φάσματος συνεργαζόμενων οντοτήτων. Αυτό θα μπορούσε να θεωρηθεί ως βέλτιστη πρακτική.
- Η Ομάδα Αξιολόγησης διαπίστωσε ότι δεν υφίστανται λεπτομερή, τυποποιημένα και συνολικά στατιστικά στοιχεία σε εθνικό επίπεδο, από τα οποία να προκύπτουν οι απειλές και τα συμβάντα όσον αφορά κυβερνοεπιθέσεις σε ετήσια βάση. Επιπλέον δεν υπάρχουν αριθμητικά στοιχεία για το έγκλημα στον κυβερνοχώρο ως ποσοστό της συνολικής εγκληματικότητας. Ωστόσο, μετά την επίσκεψη αξιολόγησης οι εθνικές αρχές διαβίβασαν κάποια στατιστικά στοιχεία σχετικά με την παιδική πορνογραφία, αλλά υπάρχει ακόμη περιθώριο για τη βελτίωση της συστηματικής συλλογής δεδομένων όσον αφορά το έγκλημα στον κυβερνοχώρο.
- Κατά τη γνώμη των αξιολογητών, τα ελλιπή στατιστικά στοιχεία δυσχεραίνουν τη σαφή αντίληψη της πορείας του εγκλήματος στον κυβερνοχώρο, αφενός, και της αποτελεσματικής καταπολέμησής του, αφετέρου. Ορισμένα από τα καταγραφέντα συμβάντα φαίνονται ίσως ασήμαντα εκ πρώτης όψεως, αποκτούν όμως μεγαλύτερη σημασία έπειτα από διεξοδική αξιολόγηση. Κατά συνέπεια, η Ομάδα Αξιολόγησης κρίνει ότι η συλλογή πλήρων στατιστικών στοιχείων θα μπορούσε να επιτρέψει τη λεπτομερή ανάλυση και να συμβάλει κατά τον τρόπο αυτό στη δημιουργία σαφέστερης εικόνας όσον αφορά την αποτελεσματική προστασία των ιδιωτικών συμφερόντων των πολιτών που έχουν πέσει θύματα εγκλημάτων στον κυβερνοχώρο.

- Δεν υφίσταται ειδικός εθνικός προϋπολογισμός για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, αλλά εκπονούνται ορισμένα προγράμματα προς χρηματοδότηση στο πλαίσιο του προγράμματος EMPACT του Κύκλου Πολιτικής της Ευρωπαϊκής Ένωσης και οι εθνικές αρχές υπέβαλαν αιτήματα χρηματοδότησης από την Ευρωπαϊκή Επιτροπή.

4. ΕΘΝΙΚΕΣ ΔΟΜΕΣ

4.1. Δικαστικός κλάδος (εισαγγελία και δικαστήρια)

4.1.1. Εσωτερική δομή

Το ελληνικό δίκαιο δεν προβλέπει ειδικό δικαστήριο αρμόδιο για την εκδίκαση του εγκλήματος στον κυβερνοχώρο. Παρά ταύτα, στην Εισαγγελία Πρωτοδικών Αθηνών υπάρχουν δύο εξειδικευμένοι εισαγγελείς που έχουν επιφορτιστεί με την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.

4.1.2. Ικανότητα και εμπόδια για την επιτυχή δίωξη

Ένα σοβαρό εμπόδιο για την επιτυχή δίωξη του εγκλήματος στον κυβερνοχώρο είναι το γεγονός ότι αυτό απαιτεί συνήθως την υποβολή και αποδοχή αιτήματος δικαστικής συνδρομής από άλλη χώρα. Η διαδικασία παροχής δικαστικής συνδρομής απαιτεί χρόνο για τη μετάφραση και αποστολή των αιτημάτων δικαστικής συνδρομής, ενώ η επιτυχής ή μη έκβασή της εξαρτάται από την έννομη τάξη της χώρας εκτέλεσης.

Πιο συγκεκριμένα, εάν στην χώρα εκτέλεσης η διερευνώμενη πράξη δεν εκπληρώνει την προϋπόθεση του διττού αξιοποίνου, επειδή, π.χ., δεν συνιστά αξιόποινη πράξη για τη χώρα αυτή ή έχει υποκύψει σε παραγραφή, τότε η δίωξη δεν μπορεί να προχωρήσει.

Ενδεικτικό παράδειγμα αποτελεί η αποστολή τέτοιων αιτημάτων δικαστικής συνδρομής προς τις Η.Π.Α.. Η Ελλάδα έχει αποστείλει και εξακολουθεί να αποστέλλει πληθώρα αιτημάτων δικαστικής συνδρομής στις Η.Π.Α βάσει της διμερούς Συμφωνίας αμοιβαίας δικαστικής συνδρομής, που υπογράφηκε στην Ουάσιγκτον στις 26-5-1999 και κυρώθηκε από την Ελλάδα με τον Ν. 2804/49 (ΦΕΚ 49/3-3-2000, τεύχ. Α΄), σε συνδυασμό με το Πρωτόκολλο στη Σύμβαση αμοιβαίας

δικαστικής συνδρομής σε ποινικές υποθέσεις μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής, που υπογράφηκε στις 26-5-1999, όπως προβλέπεται στο Άρθρο 3(2) της Συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την αμοιβαία δικαστική συνδρομή, που υπογράφηκε στις 25-6-2003, και τις Ρηματικές Διακοινώσεις με αριθμούς ΑΣ 199 του Υπουργείου Εξωτερικών της Ελληνικής Δημοκρατίας και 116/POL/09 της Πρεσβείας των Ηνωμένων Πολιτειών της Αμερικής, που κυρώθηκαν από την Ελλάδα με τον Ν. 3771/2009 (ΦΕΚ 111/ 9-7-2009, τεύχ. Α΄). Το πρόβλημα που ανέκυψε ήταν η έλλειψη διττού αξιοποίνου και η επακόλουθη μη ικανοποίηση των αιτημάτων δικαστικής συνδρομής των ελληνικών δικαστικών αρχών για αδικήματα όπως η εξύβριση ή η συκοφαντική δυσφήμιση που στην έννομη τάξη των Η.Π.Α. εμπίπτουν στην προστασία της ελευθερίας του λόγου.

Ένα άλλο ζήτημα που αντιμετωπίζει περιστασιακά η Ελλάδα αφορά το πεπερασμένο χρονικό διάστημα τήρησης των ηλεκτρονικών ιχνών το οποίο μπορεί να είναι βραχύ και έτσι το αίτημα των ελληνικών δικαστικών αρχών να μην μπορεί να ικανοποιηθεί λόγω παρέλευσης του χρόνου τήρησης των ιχνών αυτών.

4.2.Αρχές επιβολής του νόμου

Α) <u>Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος</u>

Με το Π.Δ. 178/2014 προβλέφθηκαν η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και η ίδρυση και διάρθρωση Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη. Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική υπηρεσία και υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από τα εξής:

(α) Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,
(β) Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,
(γ) Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,
(δ) Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και
(ε) Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών

Οι αρμοδιότητες του Τμήματος Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών είναι οι ακόλουθες:

(α) ο χειρισμός θεμάτων προσωπικού, η διαχείριση του χρηματικού και υλικού, η γραμματειακή, διοικητική και τεχνική υποστήριξη και γενικά η εξυπηρέτηση των λειτουργικών αναγκών της υπηρεσίας,
(β) η συλλογή, μελέτη, ανάλυση, αξιολόγηση, τυχόν συσχέτιση και επεξεργασία πληροφοριών, πειστηρίων και δεδομένων σχετικών με την αποστολή της υπηρεσίας και την προώθηση των επεξεργασμένων στοιχείων στα αρμόδια τμήματα της διεύθυνσης για επιχειρησιακή αξιοποίηση, κατά λόγο αρμοδιότητας,
(γ) η μέριμνα για τη διαρκή εξειδικευμένη εκπαίδευση και μετεκπαίδευση του προσωπικού της διεύθυνσης σε θέματα καταπολέμησης του ηλεκτρονικού εγκλήματος, μέσω της κατάρτισης και υλοποίησης εκπαιδευτικών προγραμμάτων, σύμφωνα με τις σχετικές ανάγκες των επιχειρησιακών τμημάτων και σε συνεργασία με τη Διεύθυνση Εκπαίδευσης και Ανάπτυξης Ανθρωπίνων Πόρων του Αρχηγείου, καθώς και με άλλες αρμόδιες υπηρεσίες ή φορείς της Ελλάδας και άλλων χωρών μέσω της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου.

(δ) Στο Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών λειτουργεί Κέντρο Επιχειρήσεων, το οποίο εξασφαλίζει τον συντονισμό και την επικοινωνία του προσωπικού της υπηρεσίας κατά τη διάρκεια της επιχειρησιακής του δράσης. Στο Κέντρο Επιχειρήσεων λειτουργούν, σε 24ωρη βάση, τηλεφωνικό κέντρο με ειδική γραμμή καταγγελιών, καθώς και ηλεκτρονική διεύθυνση για την επικοινωνία των πολιτών με την υπηρεσία.

Τμήμα Καινοτόμων Δράσεων και Στρατηγικής

Οι αρμοδιότητες του Τμήματος Καινοτόμων Δράσεων και Στρατηγικής είναι οι ακόλουθες:

(α) η κατάρτιση προγραμμάτων ενημέρωσης πολιτών και φορέων επί θεμάτων Διαδικτύου και ηλεκτρονικών εγκλημάτων μέσω της υλοποίησης διαφόρων δράσεων, λ.χ. συνεδρίων, ημερίδων και τηλεδιασκέψεων, καθώς και η οργάνωση άλλων καινοτόμων δράσεων στον τομέα καταπολέμησης του ηλεκτρονικού εγκλήματος,

(β) η χάραξη θεμάτων στρατηγικού σχεδιασμού, αναφορικά με έγκλημα στον κυβερνοχώρο,

(γ) η προβολή και δημοσιοποίηση του κοινωνικού έργου της υπηρεσίας μέσω της δημιουργίας και διαχείρισης προφίλ σε ιστοσελίδες κοινωνικής δικτύωσης (Twitter, Facebook κ.λπ.) προς τον σκοπό, αποκλειστικά, της επικοινωνίας, ενημέρωσης και ευαισθητοποίησης των πολιτών σε θέματα ηλεκτρονικών απειλών και κινδύνων,

(δ) η παρακολούθηση των εξελίξεων σε θέματα ηλεκτρονικού εγκλήματος, τόσο σε εσωτερικό όσο και σε διεθνές επίπεδο, η εκπόνηση σχετικής ετήσιας μελέτης με συναγωγή συμπερασμάτων για την εγκληματικότητα επί των αδικημάτων αυτών στη χώρα και η υποβολή συγκεκριμένων αιτιολογημένων προτάσεων για την αντιμετώπισή τους και

(ε) η καταγραφή δράσεων και στατιστικών στοιχείων αναφορικά με το ηλεκτρονικό έγκλημα και η τήρηση αυτών.

Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων.

Το Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων λειτουργεί σύμφωνα με τις διατάξεις της υπ' αριθ. 7001/2/1261-(21) από 28−8−2009 κοινής Υπουργικής Απόφασης των Υπουργών Εσωτερικών, Οικονομίας και Οικονομικών και Δικαιοσύνης (Β΄1879). Επίσης, το τμήμα αυτό είναι αρμόδιο για:

(α) τον χειρισμό υποθέσεων παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων που τελούνται σε ολόκληρη τη χώρα,

(β) την παροχή συνδρομής σε άλλες αρμόδιες υπηρεσίες που διερευνούν τις υποθέσεις αυτές, κατά την ισχύουσα νομοθεσία και

(γ) την παροχή αναγκαίας τεχνικής συνδρομής στα άλλα τμήματα της υπηρεσίας, τη διενέργεια ψηφιακής και διαδικτυακής έρευνας με τη χρήση σύγχρονου τεχνολογικού εξοπλισμού και την ψηφιακή και διαδικτυακή ανάλυση ψηφιακών δεδομένων, αρχείων και άλλων μέσων και ευρημάτων σε περιπτώσεις διερεύνησης σοβαρών υποθέσεων αρμοδιότητάς τους.

Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης

Οι αρμοδιότητες του Τμήματος Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης είναι οι ακόλουθες:

(α) Η εξιχνίαση και δίωξη των εγκλημάτων που διαπράττονται κατά των ανηλίκων με τη χρήση του Διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης,

(β) η διερεύνηση υποθέσεων διαδικτυακής ή ηλεκτρονικής παρενόχλησης (cyber bullying) και ρατσισμού ή ξενοφοβικού περιεχομένου στο Διαδίκτυο, καθώς και υποθέσεων συμμετοχής σε αυτοκτονία και περιπτώσεων εκδήλωσης πρόθεσης αυτοκτονίας ή εξαφάνισης μέσω Διαδικτύου και

(γ) η παροχή συνδρομής στις αρμόδιες κρατικές υπηρεσίες για την αποτροπή αυτοκτονιών που αναγγέλλονται μέσω Διαδικτύου, καθώς και στις υπηρεσίες που διερευνούν υποθέσεις για εγκλήματα που τελούνται στο Διαδίκτυο σύμφωνα με την ισχύουσα νομοθεσία.

Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

Οι αρμοδιότητες του Τμήματος Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων είναι οι ακόλουθες:

(α) Η καταπολέμηση, σε συνεργασία με τη Διεύθυνση Οικονομικής Αστυνομίας και τις άλλες αρμόδιες εθνικές, ευρωπαϊκές και αλλοδαπές υπηρεσίες και αρχές, οικονομικών εγκλημάτων και ιδίως εγκλημάτων που τελέστηκαν σε διαδικτυακό περιβάλλον, με τη χρήση ηλεκτρονικών μέσων και νέων τεχνολογιών, σε βάρος των οικονομικών συμφερόντων του δημοσίου και της εθνικής οικονομίας γενικότερα, ή εμφανίζουν τα χαρακτηριστικά του οργανωμένου οικονομικού εγκλήματος και η διερεύνησή τους απαιτεί εξειδικευμένη τεχνογνωσία.

(β) Η συνεχής έρευνα του Διαδικτύου και των άλλων μέσων ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης, για την ανακάλυψη, εξιχνίαση και δίωξη των εγκληματικών πράξεων αρμοδιότητάς του που διαπράττονται σ' αυτά ή μέσω αυτών σε ολόκληρη τη χώρα, εφόσον για τη διερεύνησή τους απαιτείται εξειδικευμένη τεχνική ή ψηφιακή έρευνα.

Αντίστοιχη διάρθρωση και αρμοδιότητες προβλέπονται και για την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Β. Εθνικό CERT – Εθνική Υπηρεσία Πληροφοριών

Ηλεκτρονικές επιθέσεις σε υποδομές του κράτους – Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.)

Η αντιμετώπιση των αδικημάτων που τελούνται μέσω του Διαδικτύου και αφορούν τη διενέργεια ηλεκτρονικών επιθέσεων σε υπουργεία και υπηρεσίες του δημοσίου, είτε εντός είτε εκτός Ελλάδας, υπάγεται στην αρμοδιότητα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), ενώ η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος παρέχει συνδρομή όπου παρίσταται ανάγκη. Πιο συγκεκριμένα:

- ✓ Με το άρθρο 2 του Π.Δ. 360/92, ορίστηκε ότι η ΕΥΠ/Διεύθυνση Ε είναι αρμόδια για τη συλλογή πληροφοριών από και με ηλεκτρονικά μέσα για την ασφάλεια των Εθνικών Επικοινωνιών.

- ✓ Με το άρθρο 2 του Π.Δ. 325/2003, η ΕΥΠ ορίστηκε ως Εθνικός Οργανισμός Ασφάλειας, η δε Διεύθυνση Ε ως Αρχή Ασφάλειας Πληροφοριών (INFOSEC) η οποία, εκτός των άλλων, προβαίνει και στην αξιολόγηση και πιστοποίηση των συσκευών και συστημάτων Ασφάλειας Επικοινωνιών και Πληροφορικής.
- ✓ Με την Υπουργική Απόφαση Φ. 120/6/200994/Σ.1691/8-6-2004 του Υπουργού Εθνικής Άμυνας η ΕΥΠ/Διεύθυνση Ε ορίζεται ως Εθνική Αρχή Ασφάλειας Επικοινωνιών-Πληροφορικής (INFOSEC).
- ✓ Με το άρθρο 4 του Ν. 3649/2008, η ΕΥΠ ορίστηκε ως Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων.

Γ. Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών

Όσον αφορά το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών (βλ. ερώτηση 1.3), του οποίου οι γενικές αρμοδιότητες προβλέπονται στην εν λόγω ερώτηση, σημειώνονται ιδίως τα εξής:

α. Εργαστήριο Εξέτασης Πειστηρίων Υπολογιστικών Συστημάτων, το οποίο:

αα. ενεργεί ανάγνωση, ανάκτηση-επαναφορά, εξέταση, αποκρυπτογράφηση, ανάλυση, σύγκριση, επεξεργασία, καταγραφή δεδομένων, ευρισκομένων σε αποθηκευτικούς ψηφιακούς χώρους τοπικών δικτύων ηλεκτρονικών υπολογιστών και περιφερειακών ή άλλων ειδικών σταθερών ή φορητών μέσων ψηφιακής αποθήκευσης δεδομένων,

ββ. αποφαίνεται για τον τρόπο λειτουργίας λογισμικού ή ψηφιακού υλικού, διαπιστώνει την αλληλουχία των ενεργειών χρήσης λογισμικού ή υλικού και ενεργεί εξετάσεις για την εξακρίβωση του δημιουργού ή του χρήστη εφαρμογών ή δεδομένων επί ψηφιακών πειστηρίων, που είναι πρόσφορα προς ανάγνωση,

γγ. ενεργεί εξετάσεις επί ηλεκτρονικών συσκευών ή άλλων ειδικών ηλεκτρονικών διατάξεων, οι οποίες είναι δυνατόν να αποθηκεύουν ψηφιακά δεδομένα,

δδ. ενεργεί εξετάσεις επί κινητών τηλεφώνων και συσκευών εντοπισμού θέσης,

εε. ενεργεί εξειδικευμένες εξετάσεις, αναγνώσεις, ανακτήσεις και αναλύσεις ψηφιακών δεδομένων επί τραπεζικών ή άλλων καρτών, καθώς και εξετάσεις επί συναφών ειδικών ηλεκτρονικών μέσων (ηλεκτρονικών διαβατηρίων), εφόσον οι εξετάσεις αυτές δεν είναι δυνατόν να διενεργηθούν στο Εργαστήριο Διερεύνησης Παραχάραξης – Κιβδηλείας και Πλαστότητας Εντύπων και Αξιών του Τμήματος Εργαστηρίων Δικαστικής Γραφολογίας και Πλαστότητας Εντύπων και Αξιών της Διεύθυνσης Εγκληματολογικών Ερευνών,

στστ. ενεργεί εξετάσεις σε συστήματα τηλεπικοινωνιών, σε συσκευές λήψης δορυφορικού τηλεοπτικού ή άλλου σήματος τα οποία περιέχουν ψηφιακά δεδομένα πρόσφορα προς ανάγνωση,

ζζ. συνεργάζεται με τις επιληφθείσες υπηρεσίες για τη διασφάλιση της κατάσχεσης, ορθής διαχείρισης και ταχύτερης αποστολής των προς εξέταση πειστηρίων, παρέχοντας σε αυτές οδηγίες ασφαλούς μεταφοράς και φύλαξης, ενώ σε εξαιρετικά κρίσιμες περιπτώσεις παρέχει τεχνική συνδρομή στην κατάσχεση, δια της αποστολής εξειδικευμένου κλιμακίου.

β. Γραφείο Γραμματειακής Υποστήριξης, το οποίο είναι αρμόδιο για:

αα. την παραλαβή, διακίνηση, παράδοση, χρέωση-αποχρέωση και γενικά διαχείριση των πειστηρίων, των εγγράφων, των εκθέσεων και της εν γένει αλληλογραφίας του τμήματος, σύμφωνα με τις ισχύουσες διατάξεις,

ββ. την τεχνική υποστήριξη της λειτουργικότητας των εργαστηρίων του τμήματος και ιδίως για την υποστήριξη των δικτύων και τη δημιουργία αντιγράφων ασφάλειας των δίσκων των υπηρεσιακών ηλεκτρονικών υπολογιστών,

γγ. την προμήθεια εξοπλισμού, υλικών και μέσων προς υποβοήθηση των αιτούμενων εργαστηριακών εξετάσεων, ύστερα από αίτημα των προϊσταμένων των εργαστηρίων,

δδ. την οργάνωση εσωτερικών εκπαιδευτικών προγραμμάτων, για την εξειδίκευση – μετεκπαίδευση του προσωπικού που υπηρετεί σε κάποιο τομέα ή πρόκειται να μετατεθεί σ’ αυτόν ύστερα από σχετικό αίτημα των προϊσταμένων των εργαστηρίων,

εε. την εύρεση, οργάνωση και ταξινόμηση της σχετικής βιβλιογραφίας, που αφορά στο αντικείμενο του τμήματος, ύστερα από σχετικό αίτημα των προϊσταμένων των εργαστηρίων,

στστ. την καταγραφή, συντήρηση, αναβάθμιση και χρέωση του κατεχόμενου ειδικού υπηρεσιακού λογισμικού, υλικού και του εν γένει εξοπλισμού του τμήματος,

ζζ. κάθε άλλη ειδική εργασία, συναφή με την αρμοδιότητά του, που του ανατίθεται σύμφωνα με τις κάθε φορά ισχύουσες διατάξεις και διαταγές,
ηη. την τήρηση των ηλεκτρονικών ή φυσικών αρχείων και υπηρεσιακών βιβλίων, όπου ενεργούνται οι σχετικές εγγραφές, για την αποτελεσματικότερη οργάνωση των αρμοδιοτήτων του κάθε εργαστηρίου και
θθ. την παραλαβή, γενική σήμανση και ασφαλή κυκλοφορία των πειστηρίων που αποστέλλονται προς εξέταση.
Επισημαίνεται επίσης ότι ανάλογες αρμοδιότητες ασκούνται από το Τμήμα Εργαστηρίων της Υποδιεύθυνσης Εγκληματολογικών Ερευνών Βορείου Ελλάδας, στο οποίο υπάγονται, όπως αναφέρεται επίσης στην ερώτηση 1.3, και οι αρμοδιότητες του Τμήματος Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών.

Στη Διεύθυνση Εγκληματολογικών Ερευνών υπάγονται επίσης, όσον αφορά την ειδική αποστολή τους, την εκπαίδευση και τον υλικοτεχνικό εξοπλισμό, τα εξής:

(α) Τα Τμήματα Εγκληματολογικών Ερευνών (εφεξής Τ.Ε.Ε), τα οποία λειτουργούν στα Επιτελεία των Γενικών Περιφερειακών Αστυνομικών Διευθύνσεων, με εξαίρεση τη Γενική Περιφερειακή Αστυνομική Διεύθυνση Κεντρικής Μακεδονίας (συνολικά 11 ανά την επικράτεια) και

(β) τα Γραφεία Εγκληματολογικών Ερευνών (εφεξής Γ.Ε.Ε.) τα οποία λειτουργούν στα Επιτελεία των Διευθύνσεων Αστυνομίας των διάφορων νομών, καθώς και σε υπηρεσίες εκτός της έδρας των Διευθύνσεων Αστυνομίας εφόσον εκεί υπάρχει έδρα Πρωτοδικείου (συνολικά 53 ανά την επικράτεια).

Επιπλέον, όσον αφορά τις ειδικές θέσεις για ιατροδικαστές στον τομέα των Τεχνολογιών των Πληροφοριών (ΤΠ), επισημαίνεται ότι στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος καθώς και στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών υπηρετούν αστυνομικοί γενικών και ειδικών καθηκόντων, οι οποίοι διαθέτουν τίτλους σπουδών προπτυχιακού, μεταπτυχιακού και ορισμένοι εξ αυτών και διδακτορικού επιπέδου σε αντικείμενα σχετικά με την πληροφορική.

4.3.Άλλες αρχές/όργανα/εταιρικές σχέσεις δημόσιου-ιδιωτικού τομέα

Η Διεύθυνση Επιθεώρησης Εποπτευόμενων Εταιρειών της Τράπεζας της Ελλάδος και ιδίως το Τμήμα Πληροφοριακών Συστημάτων Εποπτευόμενων Εταιρειών διαδραματίζουν ενεργό ρόλο, μεταξύ άλλων στην πρόληψη του εγκλήματος στον κυβερνοχώρο.

Επιπλέον, ιδιαίτερη σημασία για τον μετριασμό του κινδύνου στον κυβερνοχώρο έχει ο ρόλος της Ευρωπαϊκής Κεντρικής Τράπεζας όσον αφορά τις τέσσερις συστημικές ελληνικές τράπεζες που βρίσκονται από τον Νοέμβριο του 2014 υπό τη μικροπροληπτική εποπτεία του Ενιαίου Εποπτικού Μηχανισμού (SSM). Πολύ πρόσφατα οι ελληνικές τράπεζας έλαβαν και απάντησαν σε εκτενές ερωτηματολόγιο του SSM σχετικά με τον μετριασμό του κινδύνου από το έγκλημα στον κυβερνοχώρο.

Επιπλέον, σε προδραστικό επίπεδο, υπάρχει συνεχής συνεργασία και ανταλλαγή πληροφοριών μεταξύ των ενδιαφερομένων (τραπεζών – Ελληνικής Αστυνομίας και Τράπεζας της Ελλάδος) στο πλαίσιο τακτικών συνεδριάσεων της διατραπεζικής επιτροπής της Ελληνικής Ένωσης Τραπεζών (ΕΕΤ) όσον αφορά την πρόληψη και την αντιμετώπιση της απάτης στα συστήματα πληρωμών και τα μέσα πληρωμών. Στο πλαίσιο της επιτροπής αυτής εξετάζονται συχνά σε βάθος διεθνείς, ευρωπαϊκές και εθνικές σχετικές πρωτοβουλίες.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT είναι η Εθνική Αρχή, αρμόδια για την αντιμετώπιση-προστασία από ηλεκτρονικές απειλές-επιθέσεις σύμφωνα με τον Ν. 3649/2008 και το Π.Δ. 126/2009. Ειδικότερα:

Είναι η αρμόδια Εθνική Αρχή αντιμετώπισης-προστασίας από ηλεκτρονικές απειλές-επιθέσεις προς τον δημόσιο φορέα και τις κρίσιμες υποδομές της χώρας.
Συλλέγει στοιχεία ηλεκτρονικών επιθέσεων-απειλών από δημόσιους και ιδιωτικούς φορείς.
Αναλύει τα στοιχεία, καταγράφει-κατηγοριοποιεί το είδος των επιθέσεων-απειλών (επικίνδυνος κώδικας, εισβολή, αδυναμίες λογισμικού κ.λπ) και χειρίζεται τις επιθέσεις–απειλές ανάλογα με το είδος τους.

Παρέχει πληροφορίες και συμβουλές για την προστασία των συστημάτων Η/Υ (του δημόσιου και ιδιωτικού φορέα) από πλευράς ασφάλειας από τις παραπάνω επιθέσεις-απειλές.
Προβαίνει σε ανακοινώσεις σχετικά με επικείμενες απειλές ή γενόμενες ηλεκτρονικές επιθέσεις και προτείνει προληπτικά ή κατασταλτικά μέτρα προστασίας.
Διακινεί πληροφορίες και προτάσεις σχετικά με προστασία , αποτελέσματα, επιπτώσεις και συμπεράσματα από απειλές-επιθέσεις.
Ενημερώνεται για την εξέλιξη της τεχνολογίας πληροφοριών, συμμετέχει σε συνέδρια, σεμινάρια και σχετικές εκπαιδεύσεις.
Συνεργάζεται με άλλα εθνικά και μη CERT καθώς και υπηρεσίες του δημόσιου φορέα για σχετικά θέματα.
Παρέχει συμβουλές και βοήθεια στις εγκαταστάσεις του φορέα που δέχθηκε επίθεση για την αποκατάσταση-περιορισμό των επιπτώσεων από τις επιθέσεις, εφόσον αυτό ζητηθεί από τον φορέα.
Συντονίζει τις ενέργειες απόκρισης μεταξύ των εμπλεκομένων σε επιθέσεις.

Διαθέτει τον απαιτούμενο εξοπλισμό για τον χειρισμό, την ανάπτυξη στρατηγικής και την αντιμετώπιση απειλών-επιθέσεων καθώς και την συλλογή, επεξεργασία και διακίνηση των σχετικών πληροφοριών

Η ΕΑΠΔΠΧ είναι μια ανεξάρτητη διοικητική αρχή, συντάσσει αναφορές μόνο προς τη Βουλή και δεν υπόκειται σε διοικητικό έλεγχο, αλλά οι αποφάσεις της μπορούν προσβληθούν ενώπιον του Συμβουλίου της Επικρατείας. Την ανεξαρτησία της προβλέπουν και εγγυώνται το Σύνταγμα της Ελλάδας (άρθρο 9Α) και ο Νόμος 2472/1997. Συγκροτείται από ένα δικαστικό λειτουργό ενός από τα τρία ανώτατα εθνικά δικαστήρια ως Πρόεδρο και από έξι μέλη, δηλ. έναν καθηγητή πανεπιστημίου σε γνωστικό αντικείμενο του δικαίου, έναν καθηγητή πανεπιστημίου σε γνωστικό αντικείμενο της τεχνολογίας των πληροφοριών, έναν καθηγητή πανεπιστημίου οποιουδήποτε κλάδου και τρία πρόσωπα κύρους και εμπειρίας στον τομέα της προστασίας των δεδομένων προσωπικού χαρακτήρα. Ο Πρόεδρος, τα μέλη του Διοικητικού Συμβουλίου και οι αναπληρωτές εκλέγονται από τη Βουλή, κατόπιν προτάσεως του Προέδρου της Βουλής. Η διάρκεια της θητείας τους είναι τετραετής, με μία μόνο δυνατότητα ανανέωσης, και απολαύουν πλήρους προσωπικής και λειτουργικής ανεξαρτησίας κατά την άσκηση των καθηκόντων τους.

Όπως επεξηγείται εν συντομία σε ορισμένες προηγούμενες απαντήσεις, η ΕΑΠΔΠΧ έχει την αρμοδιότητα να διατάξει τη διόρθωση και/ή τη διαγραφή οποιωνδήποτε εσφαλμένων δεδομένων, να διενεργήσει ελέγχους της χρησιμοποιούμενης υποδομής ΤΠ από την άποψη της τήρησης της αρχής της ασφάλειας, να απευθύνει συστάσεις/γνώμες όσον αφορά την καταλληλότητα της επεξεργασίας δεδομένων (σύμφωνα με το άρθρο 19 του Νόμου 2472/1997) και έχει επίσης την αρμοδιότητα να επιβάλει διοικητικές κυρώσεις, λ.χ. πρόστιμα ή προειδοποιήσεις (σύμφωνα με το άρθρο 21 του Νόμου 2472/1997).

Η Ελληνική Αρχή Διασφάλισης του Απορρήτου των Τηλεπικοινωνιών (ΑΔΑΕ) συγκροτήθηκε το 2003 σύμφωνα με το άρθρο 19 παράγραφος 2 του Συντάγματος της Ελλάδας, που προβλέπει τη συγκρότηση ανεξάρτητης αρχής που διασφαλίζει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση ή επικοινωνία με οποιονδήποτε άλλο τρόπο. Η ΑΔΑΕ παρακολουθεί την εφαρμογή της νομοθεσίας για την άρση του απορρήτου των επικοινωνιών και, προς τον σκοπό αυτό, εξουσιοδοτείται να λαμβάνει όλες τις εντολές για την άρση του απορρήτου που εκδίδουν οι δικαστικές αρχές. Επιπλέον, ο Νόμος 3115/2003 χορηγεί στην ΑΔΑΕ, μεταξύ άλλων, την αρμοδιότητα α) να εκδίδει κανονιστικές πράξεις για τη διασφάλιση του απορρήτου των επικοινωνιών, β) να διενεργεί ελέγχους σε παρόχους δικτύων επικοινωνιών και σχετικών υπηρεσιών, δημόσιες υπηρεσίες καθώς και την Εθνική Υπηρεσία Πληροφοριών, γ) να καλεί σε ακρόαση τις προαναφερόμενες οντότητες, δ) να εξετάζει σχετικές καταγγελίες των πολιτών και ε) να συλλέγει σχετικές πληροφορίες με χρήση ειδικών ερευνητικών εξουσιών.

Η ΑΔΑΕ, που εργάζεται στον τομέα της ασφάλειας των επικοινωνιών πάνω από μία δεκαετία, έχει αποκτήσει επαρκή πείρα στη διαχείριση των κινδύνων και των ευάλωτων σημείων όσον αφορά την ασφάλεια των δικτύων και των υπηρεσιών των παρόχων επικοινωνιών. Στην πράξη, η ΑΔΑΕ διερευνά και ελέγχει τα συστήματα και τις υπηρεσίες των παρόχων επικοινωνιών, εντοπίζει και συζητεί λεπτομερώς με τους διαχειριστές τους τις ελλείψεις και παραβιάσεις από άποψη ασφάλειας και προτείνει τεχνικά και διαδικαστικά μέτρα προς διασφάλιση του απορρήτου και της ακεραιότητας των επικοινωνιακών δεδομένων των χρηστών.

Όπως ορίζεται στον Νόμο με τον οποίο συγκροτείται, η ΑΔΑΕ διενεργεί επιτόπιους ελέγχους, τόσο προγραμματισμένους (τακτικούς) όσο και ad hoc. Ένα πολύτιμο εργαλείο κατά τους ελέγχους είναι η πολιτική ασφαλείας του παρόχου, που πρέπει να προεγκρίνεται από την ΑΔΑΕ και να πληροί τους όρους του κανονισμού εσωτερικής λειτουργίας της. Στους προγραμματισμένους ελέγχους κατά κανόνα ελέγχονται όλα τα συστήματα και οι πληροφορίες του παρόχου, ενώ στους ad hoc ελέγχους ελέγχονται ειδικές λειτουργίες, συστήματα και υπηρεσίες του παρόχου. Οι ad hoc έλεγχοι κινούνται κυρίως από καταγγελίες χρηστών ή όταν γνωστοποιείται περιστατικό/παραβίαση στον τομέα της ασφάλειας. Μετά τον έλεγχο η ΑΔΑΕ υποβάλλει έκθεση ελέγχου στους παρόχους. Η έκθεση αυτή περιλαμβάνει συνήθως τις εντοπισθείσες ελλείψεις ασφαλείας και ενδεχόμενα τεχνικά, διαδικαστικά ή νομικά πορίσματα και παρεκκλίσεις από την εγκεκριμένη πολιτική ασφαλείας του παρόχου. Η έκθεση προτείνει στον πάροχο κατάλληλα τεχνικά και οργανωτικά μέτρα. Η ΑΔΑΕ μπορεί επίσης να επιβάλει διοικητικές κυρώσεις στους παρόχους, λαμβάνοντας υπόψη της τη σοβαρότητα των παρεκκλίσεων και ελλείψεων ασφαλείας που εντοπίστηκαν καθώς και την αρχή της αναλογικότητας.

Σε κεντρικό επιτελικό επίπεδο λειτουργεί στο Αρχηγείο της Ελληνικής Αστυνομίας η Διεύθυνση Δημόσιας Ασφάλειας, στη δομή της οποίας υφίσταται και λειτουργεί το Τμήμα Οργανωμένου Οικονομικού και Ηλεκτρονικού Εγκλήματος (Π.Δ. 178/2014), στην αρμοδιότητα του οποίου εντάσσεται, μεταξύ άλλων, η μελέτη μέτρων αντιμετώπισης των εγκλημάτων με τη χρήση ηλεκτρονικών υπολογιστών, καθώς και η καθοδήγηση των περιφερειακών υπηρεσιών στη δίωξη των εγκλημάτων αυτών.

Επιπροσθέτως, σύμφωνα με τις διατάξεις της παρ. 7 άρθρου 178 Π.Δ. 178/2014, για την εκπλήρωση της αποστολής της η ΔΙ.ΔΙ.Η.Ε. συνεργάζεται με άλλες καθ' ύλην και κατά τόπο αρμόδιες κεντρικές και περιφερειακές υπηρεσίες της Ελληνικής Αστυνομίας και ιδίως με τη Διεύθυνση Πληροφορικής του Αρχηγείου, τη Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών, τη Διεύθυνση Οικονομικής Αστυνομίας και τις Διευθύνσεις Ασφάλειας Αττικής και Θεσσαλονίκης. Επίσης, στο πλαίσιο αυτό, συνεργάζεται και με άλλες αρμόδιες υπηρεσίες, αρχές και φορείς της χώρας, καθώς και με αντίστοιχες υπηρεσίες, οργανισμούς και φορείς ευρωπαϊκών και άλλων χωρών, σύμφωνα με τις ισχύουσες διατάξεις και τις σχετικές διεθνείς συμφωνίες και συμβάσεις.

Τέλος, στην παράγραφο 3 του άρθρου 65 του Π.Δ. 178/2014 μνημονεύεται ότι, οι Διευθύνσεις των Κλάδων και οι περιφερειακές υπηρεσίες της Ελληνικής Αστυνομίας συνεργάζονται υπεύθυνα και αποτελεσματικά με τις αυτοτελείς κεντρικές υπηρεσίες, στο πλαίσιο των αρμοδιοτήτων τους, παρέχοντας σ' αυτές κάθε αναγκαία συνδρομή στην εκπλήρωση της αποστολής τους. Προς τούτο, όλες οι υπηρεσίες της Ελληνικής Αστυνομίας διαβιβάζουν ή κοινοποιούν στη Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών το πληροφοριακό υλικό που συλλέγουν στο πλαίσιο της υπηρεσιακής τους δραστηριότητας και ενημερώνουν τις Διευθύνσεις Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, καθώς και τη Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας για κάθε υπόθεση κοινής αρμοδιότητας της οποίας επιλαμβάνονται.

Περαιτέρω, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών συνεργάζεται με τις επιληφθείσες υπηρεσίες για τη διασφάλιση της κατάσχεσης, ορθής διαχείρισης και ταχύτερης αποστολής των προς εξέταση πειστηρίων, παρέχοντας σε αυτές οδηγίες ασφαλούς μεταφοράς και φύλαξης, ενώ σε εξαιρετικά κρίσιμες περιπτώσεις παρέχει τεχνική συνδρομή στην κατάσχεση, δια της αποστολής εξειδικευμένου κλιμακίου.

Το Εθνικό CERT ενημερώνει σε τακτική βάση τους δημόσιους φορείς για τις νεοεμφανιζόμενες κυβερνοαπειλές και τους διανέμει IoC (Indicators of Compromise) για πρόληψη ή/και αντιμετώπιση κυβερνοεπιθέσεων. Σε περίπτωση που πραγματοποιηθεί κυβερνοεπίθεση σε δημόσιο φορέα, τότε ο υπό επίθεση φορέας υποχρεούται να αναφέρει το περιστατικό στο Εθνικό CERT και να του παράσχει όλα τα απαραίτητα στοιχεία για ανάλυση της επίθεσης. Το Εθνικό CERT προβαίνει σε ανάλυση της επιθετικής δραστηριότητας και στη συνέχεια κοινοποιεί τα συμπεράσματα στον δημόσιο φορέα, στον οποίο προτείνει συμβουλευτικά μέτρα ηλεκτρονικής ασφάλειας που σκόπιμο είναι να εφαρμοστούν ώστε να αποφευχθούν παρόμοια μελλοντικά περιστατικά. Έπειτα, είναι στην ευχέρεια του φορέα αν επιθυμεί να προχωρήσει στη νομική δίωξη των επιτιθεμένων. Σε αυτή την περίπτωση, τα συμπεράσματα της ανάλυσης του Εθνικού CERT προωθούνται στην αρμόδια υπηρεσία επιβολής νόμου, που συνήθως είναι η Δίωξη Ηλεκτρονικού Εγκλήματος.

Στο πλαίσιο των εθνικών ασκήσεων κυβερνοπολέμου «Πανόπτης» υπάρχει ευρεία συμμετοχή από ακαδημαϊκά ιδρύματα, φορείς του δημοσίου και του ιδιωτικού τομέα. Η συνεργασία μεταξύ όλων των συμμετεχόντων φορέων απαιτεί περισσότερο συντονισμό..

4.4.Συνεργασία και συντονισμός σε εθνικό επίπεδο

4.4.1. Νομικές απαιτήσεις ή απαιτήσεις πολιτικής

Ο ιδιωτικός τομέας μπορεί να γνωστοποιεί, χωρίς όμως να είναι υποχρεωμένος, περιστατικά ηλεκτρονικών επιθέσεων στον κυβερνοχώρο στην Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και να λαμβάνει συμβουλές αντιμετώπισης αλλά και επιχειρησιακή-τεχνική βοήθεια από αυτήν για την αντιμετώπιση των περιστατικών εφόσον ζητηθεί.

Τα πιστωτικά ιδρύματα που λειτουργούν στην Ελλάδα υποχρεούνται να αναφέρουν αμελλητί τα επεισόδια κυβερνοεπιθέσεων με στόχο τα πιστωτικά ιδρύματα και/ή τους πελάτες τους. Η αναφορά απευθύνεται στο Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, την Τράπεζα της Ελλάδος καθώς και τον SSM της ΕΚΤ. Η ΕΕΤ έχει καταρτίσει και διατηρεί δύο καταλόγους επαφών επαγρύπνησης με τα στοιχεία επαφής των αρμόδιων εκπροσώπων των πιστωτικών ιδρυμάτων, του Τμήματος Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και της Τράπεζας της Ελλάδος.

Ο πρώτος κατάλογος επαφών επαγρύπνησης αφορά κάθε είδους συμβάν σχετικό με απάτη με κάρτες πληρωμών (λ.χ. skimming/«ξάφρισμα» ATM και σημείων πώλησης, απάτη στο ηλεκτρονικό εμπόριο κ.λπ.), ενώ ο δεύτερος κατάλογος επαφών επαγρύπνησης αφορά κάθε είδους απάτη μέσω Διαδικτύου (λ.χ. εξελιγμένες τεχνικές phishing, κλοπή ταυτότητας, γνωστοποίηση των μυστικών διαπιστευτηρίων των πελατών σε τρίτους και επιθέσεις σε «man-in-the-middle»/φυλλομετρητή με στόχο την υποκλοπή/τροποποίηση/εκτροπή δεδομένων των πελατών, κακόβουλα λογισμικά, κοινωνική μηχανική, κατανεμημένη άρνηση υπηρεσίας-DDoS και παραβίαση της περιμετρικής ζώνης κ.λπ.).

Ο Νόμος 3471/2006 (ΦΕΚ Α' 133), με τον οποίο μεταφέρεται στην εθνική έννομη τάξη η οδηγία 2002/58/ΕΚ, ορίζει την ΑΔΑΕ, από κοινού με την εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ως αρμόδια εθνική αρχή για την παραλαβή κοινοποιήσεων σχετικά με παραβιάσεις δεδομένων. Επιπλέον, η ΑΔΑΕ έχει εκδώσει τον κανονισμό 165/2011 «για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 2715). Τόσο ο κανονισμός 165/2011 της ΑΔΑΕ όσο και το άρθρο 8 του Νόμου 3674/2008 (ΦΕΚ Α' 136) περιλαμβάνουν διατάξεις για την άμεση κοινοποίηση των παραβιάσεων του απορρήτου των επικοινωνιών ή του κινδύνου σχετικών παραβιάσεων στην ΑΔΑΕ και στους αντίστοιχους συνδρομητές.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων αποτελεί την αρμόδια κυβερνητική αρχή που συντονίζει την αντιμετώπιση των κυβερνοεπιθέσεων μεταξύ των ενδιαφερομένων, εφόσον αυτό αφορά τον δημόσιο τομέα ή κρίσιμες υποδομές. Ακόμη, σε περίπτωση μεγάλης έκτασης κυβερνοεπίθεσης θα ενημερώνει τις υπηρεσίες ασφαλείας.

Ναι, υπάρχει επαρκής/αποτελεσματική συνεργασία μεταξύ τραπεζών και αρχών επιβολής του νόμου για την πρόληψη και την καταπολέμηση της διαδικτυακής απάτης με κάρτες.

Στην ΕΕΤ έχει συσταθεί ειδική διατραπεζική επιτροπή για την αντιμετώπιση της απάτης στα συστήματα πληρωμών. Τα μέλη αυτής της επιτροπής είναι εκπρόσωποι των τραπεζών, της Τράπεζας της Ελλάδος και της Ελληνικής Αστυνομίας. Στο πλαίσιο της επιτροπής εξετάζονται οι νέες τάσεις στις απάτες, συμβάντα και μέτρα/τεχνολογίες αντιμετώπισης προκειμένου να ληφθούν κατάλληλα μέτρα. Η επιτροπή χρησιμοποιεί κατάλογο επαφών επαγρύπνησης με τα στοιχεία επαφής των αρμόδιων εκπροσώπων. Οι επαφές του καταλόγου ενημερώνονται για κάθε είδους συμβάν που αφορά απάτη με κάρτες πληρωμών (ATM & POS skimming/«ξάφρισμα», απάτη στο ηλεκτρονικό εμπόριο κ.λπ.)

• **Ειδοποιούν την αστυνομία/αρχές επιβολής του νόμου εάν αντιληφθούν κατάχρηση των νέων εργαλείων πληρωμής που αναπτύσσονται από την αντίστοιχη βιομηχανία;**

Οι αρχές επιβολής του νόμου βρίσκονται σε συνεργασία με τον ιδιωτικό τομέα της χώρας. Ειδικότερα, όσον αφορά τα πιστωτικά ιδρύματα της χώρας, στα πλαίσια της διατραπεζικής επιτροπής για την πρόληψη και την αντιμετώπιση της απάτης στα μέσα και τα συστήματα πληρωμών καθώς και της ad hoc διατραπεζικής ομάδας έργου που παραλαμβάνει εμπιστευτικού περιεχομένου ενημέρωση που διαβιβάζει η Ευρωπόλ, πραγματοποιείται ανταλλαγή εμπιστευτικής πληροφορίας μέσω της Ευρωπαϊκής Κεντρικής Τράπεζας και του EC3 που αφορούν νέες μεθόδους ή νέα εργαλεία πληρωμής. Αντίστοιχα, ανταλλαγή εμπιστευτικής πληροφορίας σε εθνικό επίπεδο μεταξύ των πιστωτικών ιδρυμάτων και των αρχών επιβολής του νόμου, πραγματοποιείται μέσω της ομάδας εργασίας για την καταπολέμηση των απατών μέσω διαδικτύου (internet fraud).

• **Αυξάνουν την ασφάλεια στις πληρωμές που δεν γίνονται με μετρητά και ελαχιστοποιούν την ευπάθεια των μαγνητικών ταινιών;**

Για την αποτελεσματική συνεργασία μεταξύ ιδιωτικού τομέα και αρχών επιβολής του νόμου, η ΔΙ.Δ.Η.Ε, στα πλαίσια των αρμοδιοτήτων της, πραγματοποιεί ενημερώσεις ευαισθητοποίησης στον ιδιωτικό τομέα αναφορικά με νέες τάσεις στο θέμα των διαδικτυακών απατών καθώς και παροχή συμβουλών για λήψη κατάλληλων μέτρων πρόληψης.

Η υιοθέτηση της νέας τεχνολογίας EMV στο σύνολο των καρτών του χαρτοφυλακίου από τα πιστωτικά ιδρύματα της χώρας έχει πλέον ως αποτέλεσμα την ενίσχυση στον μέγιστο βαθμό της ασφάλειας στις πληρωμές με παρουσία κάρτας, ελαχιστοποιώντας την ευπάθεια των μαγνητικών ταινιών.

Στις ελληνικές κάρτες πληρωμών χρησιμοποιείται κυρίως η τεχνολογία EMV/chip και PIN. Όλες οι εκδότριες τράπεζες χρησιμοποιούν συστήματα παρακολούθησης κατά της απάτης για τις συναλλαγές με κάρτες πληρωμών. Όποτε χρησιμοποιείται μια ελληνική κάρτα πληρωμής στο εξωτερικό, ιδίως σε χώρα που δεν χρησιμοποιεί τεχνολογία EMV (π.χ. ΗΠΑ), εκτελείται μια σειρά ειδικών ελέγχων ασφάλειας.

• **Ενισχύουν τη διαδικασία έγκρισης των διαδικτυακών συναλλαγών και την εξακρίβωση της ταυτότητας του πελάτη;**

Για την καταπολέμηση των απατών μέσω διαδικτύου, κάθε εταιρεία έχει υιοθετήσει το δικό της σύστημα προστασίας από απάτες. Τα συστήματα προστασίας από απάτες, πραγματοποιούν διεξαγωγή ελέγχων, σε πραγματικό χρόνο, για τον εντοπισμό περιπτώσεων απάτης στις διαδικτυακές συναλλαγές με χρήση καρτών πληρωμής.

Όσον αφορά τα πιστωτικά ιδρύματα της χώρας, υπάρχει δίαυλος επικοινωνίας και άμεσης συνεργασίας μεταξύ αυτών για την ενίσχυση της διαδικασίας εξακρίβωσης των στοιχείων των πελατών με σκοπό τον έγκαιρο περιορισμό των απατηλών συναλλαγών.

Οι ελληνικές τράπεζες διαθέτουν υπερσύγχρονη υποδομή διαδικτυακών πληρωμών καθώς επίσης εξελιγμένα και αποτελεσματικά μέτρα ασφαλείας όπως για παράδειγμα:

- Εξειδικευμένους μηχανισμούς ασφαλείας με πολλαπλά επίπεδα άμυνας.
- Παρακολούθηση και εντοπισμό δόλιων συναλλαγών με κάρτα.
- Υπηρεσίες όπως MasterCard® SecureCode™ ή Verified by VISA ως υπηρεσίες επαλήθευσης της ταυτότητας του κατόχου της κάρτας κατά την πραγματοποίηση αγορών μέσω Διαδικτύου.

Επιπλέον των ανωτέρω, τα τελευταία χρόνια οι τράπεζες εκπαιδεύουν συστηματικά τους πελάτες τους να μην αποκαλύπτουν τα στοιχεία των καρτών τους (αριθμό κάρτας, PIN, CCV2) και τα προσωπικά τους στοιχεία (αριθμό ταυτότητας, ημερομηνία γέννησης) και να τα προστατεύουν αποτελεσματικά.

Ο ρόλος του ιδιωτικού τομέα στην πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο έχει θεμελιώδη σημασία. Με τη διεξαγωγή εκτιμήσεων του κινδύνου, τη λήψη των κατάλληλων μέτρων ασφαλείας και την εφαρμογή διαρθρωμένης πολιτικής ασφαλείας, οι πάροχοι δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών όχι μόνο μπορούν να εμποδίσουν την εμφάνιση ορισμένων τύπων εγκλήματος στον κυβερνοχώρο, αλλά μπορούν επίσης να επικουρούν τις αρχές επιβολής του νόμου παρέχοντάς τους σημαντικά πειστήρια, με την προϋπόθεση ότι αυτά έχουν αποκτηθεί μέσω διαδικασιών που προβλέπονται από τον νόμο.

Μέχρι σήμερα δεν υφίσταται νομικό πλαίσιο το οποίο να παρέχει τη δυνατότητα συνεργασίας με τον ιδιωτικό τομέα σε ότι αφορά τις εργαστηριακές εξετάσεις επί πειστηρίων ηλεκτρονικού εγκλήματος.

Η συμβολή των τραπεζών στο έργο των δικαστικών και αστυνομικών αρχών είναι διαρκής και αδιάκοπη. Σε επίπεδο καταστολής, αυτή περιλαμβάνει την παροχή

- οπτικοακουστικού υλικού, ιδίως σε περιπτώσεις απάτης σε ΑΤΜ,
- δεδομένων δόλιων συναλλαγών με κάρτες πληρωμών,
- των στοιχείων λογαριασμών που έχουν χρησιμοποιηθεί για μεταφορές χρημάτων στο πλαίσιο επιθέσεων phishing (λογαριασμών λαθρομεταφορέων),
- των διευθύνσεων IP που χρησιμοποιούνται από απατεώνες του Διαδικτύου, κ.λπ.

Επιπλέον, σε προδραστικό επίπεδο, υπάρχει συνεχής συνεργασία και ανταλλαγή πληροφοριών μεταξύ των ενδιαφερομένων (τραπεζών – Ελληνικής Αστυνομίας και Τράπεζας της Ελλάδος) στο πλαίσιο τακτικών συνεδριάσεων της διατραπεζικής επιτροπής της Ελληνικής Ένωσης Τραπεζών (ΕΕΤ) όσον αφορά την πρόληψη και την αντιμετώπιση της απάτης στα συστήματα πληρωμών και τα μέσα πληρωμών. Στο πλαίσιο της επιτροπής αυτής εξετάζονται συχνά σε βάθος διεθνείς, ευρωπαϊκές και εθνικές σχετικές πρωτοβουλίες.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνεργάζεται με εταιρείες του ιδιωτικού τομέα, για τη λήψη πληροφόρησης σχετικά με τρόπους ανίχνευσης και αντιμετώπισης κυβερνοεπιθέσεων, λήψη στοιχείων καθώς επίσης και για θύματα-στόχους επιθέσεων.

Επίσης συνεργάζεται με εταιρείες του ιδιωτικού τομέα παρέχοντας οδηγίες ηλεκτρονικής ασφάλειας, ώστε να απενεργοποιηθούν πληροφοριακά συστήματα και λειτουργίες τους, στα οποία έχουν γίνει παρεμβάσεις και χρησιμοποιούνται για παράνομους σκοπούς.

Η παραπάνω συνεργασία της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικού CERT με τον ιδιωτικό τομέα δεν βασίζεται σε νομικές ή κανονιστικές υποχρεώσεις που καθορίζονται από τη νομοθεσία, αλλά πραγματοποιείται στο πλαίσιο καλής συνεργασίας για ένα κοινό σκοπό που είναι η διατήρηση ενός υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο.

Στην εθνική νομοθεσία, με την ενσωμάτωση του άρθρου 25 της οδηγίας 2011/-93/ΕΕ υπάρχουν συγκεκριμένες προβλέψεις στο άρθρο 18 του Ν. 4267/2014 για λήψη μέτρων σε βάρος ιστοσελίδων που περιέχουν ή διαδίδουν υλικό παιδικής πορνογραφίας. Με διάταξη του αρμοδίου εισαγγελέα διατάσσεται η κατάργηση ιστοσελίδας που φιλοξενείται στην Ελλάδα και περιέχει ή διαδίδει υλικό παιδικής πορνογραφίας. Αυτή η διάταξη κοινοποιείται στον πάροχο των υπηρεσιών φιλοξενίας της εν λόγω ιστοσελίδας και εκτελείται αμέσως (άρθρο 18 παράγραφος 1). Αντίστοιχες προβλέψεις υπάρχουν σε περίπτωση ιστοσελίδας που περιέχει ή διαδίδει υλικό παιδικής πορνογραφίας, όταν δεν μπορεί να διαπιστωθεί αν αυτή η ιστοσελίδα φιλοξενείται στην Ελλάδα ή εκτός Ελλάδας και βρίσκεται σε χώρο ή υποχώρο ονομάτων χώρου που έχει χορηγηθεί στην Ελλάδα. Στην περίπτωση αυτή, η σχετική διάταξη του εισαγγελέα που διατάσσει την προσωρινή απενεργοποίηση του ονόματος χώρου κοινοποιείται στον κάτοχο του ονόματος χώρου και την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (εφεξής Ε.Ε.Τ.Τ.) και εκτελείται αμέσως.

Αν πρόκειται για ιστοσελίδα που περιέχει ή διαδίδει υλικό παιδικής πορνογραφίας, δεν φιλοξενείται στην Ελλάδα και δεν ανήκει σε χώρο ή υποχώρο που έχει χορηγηθεί στην Ελλάδα, με διάταξη του Εισαγγελέα διατάσσεται η φραγή της πρόσβασης στην ιστοσελίδα αυτή. Αν εντοπιστεί ο κάτοχος, η διάταξη του εισαγγελέα κοινοποιείται σε αυτόν, κοινοποιείται όμως και στην Ε.Ε.Τ.Τ. η οποία ακολούθως την κοινοποιεί στους παρόχους υπηρεσιών πρόσβασης στο Διαδίκτυο και ζητά την άμεση εφαρμογή της και την ενημέρωση των χρηστών. Συνεπώς, στην εφαρμογή των μέτρων των οποίων την εφαρμογή αποφάσισαν οι δικαστικές αρχές σε βάρος ιστοσελίδων που περιέχουν ή διαδίδουν υλικό παιδικής πορνογραφίας συμβάλλουν και οι πάροχοι υπηρεσιών πρόσβασης στο Διαδίκτυο. Θα πρέπει ακόμη να επισημανθεί ότι, με την ενσωμάτωση της οδηγίας 2006/24/ΕΚ (η οποία κηρύχθηκε ανίσχυρη με τις αποφάσεις του Δ.Ε.Ε. επί των υποθέσεων C-293/12 και C-594/12) στην εθνική μας έννομη τάξη, η υποχρέωση των παρόχων για διατήρηση συγκεκριμένων δεδομένων, προκειμένου αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, ρυθμίζεται στα άρθρα 1-13 του Ν. 3917/2011.

Όσον αφορά τη συμμετοχή του ιδιωτικού τομέα στην πρόληψη και καταπολέμηση των σχετικών με το Διαδίκτυο εγκλημάτων και ειδικά εγκλημάτων σχετιζόμενων με το περιεχόμενο (content related), θα μπορούσε να αναφερθεί η λειτουργία ανοικτής γραμμής καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο από ενώσεις και μη κερδοσκοπικά σωματεία, όπως η γραμμή Safeline η οποία αποτελεί από τις 18/10/2005 μέλος του Διεθνούς Συνδέσμου Ανοικτών Γραμμών Διαδικτύου (INHOPE). Η συγκεκριμένη γραμμή ιδρύθηκε το 2003 από ιδιωτική εταιρεία παροχής υπηρεσιών πρόσβασης στο Διαδίκτυο, το Ελληνικό Όργανο Αυτορρύθμισης για το Περιεχόμενο του Internet (SAFENET) και δυο ιδρύματα, ενώ λειτουργεί με την υποστήριξη του Safer Internet Programme της Ευρωπαϊκής Επιτροπής (www.safeline.gr).

4.4.2. Πόροι που διατίθενται για τη βελτίωση της συνεργασίας

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει στη διάθεσή της τον απαραίτητο εξοπλισμό (μηχανήματα) για την καταπολέμηση των διαδικτυακών απατών. Επιπρόσθετα, για την παρακολούθηση των νέων τεχνολογιών που χρησιμοποιούνται στον χώρο των καρτών πληρωμής, η υπηρεσία συμμετέχει σε συνέδρια ανά την υφήλιο ενώ παράλληλα συνεργάζεται με εγχώρια πανεπιστημιακά ιδρύματα. Η υπηρεσία δεν διαθέτει ειδικό λογισμικό για τις διαδικτυακές απάτες. Ωστόσο, επιδιώκεται συνεχής αναζήτηση τεχνολογίας για τη δίωξη και καταπολέμηση των διαδικτυακών απατών.

Κάθε χρόνο η ΔΙΚΥΒ/ΓΕΕΘΑ διοργανώνει και διεξάγει την εθνική άσκηση κυβερνοάμυνας «ΠΑΝΟΠΤΗΣ», στην οποία καλούνται να συμμετάσχουν τα σώματα ασφαλείας, ο ευρύτερος δημόσιος τομέας, η ακαδημαϊκή κοινότητα, καθώς και ο ιδιωτικός τομέας. Μέσω των σεναρίων της άσκησης επιδιώκονται η εξάσκηση των ασκουμένων στην αντιμετώπιση σύγχρονων κυβερνοαπειλών, καθώς και η ενίσχυση της μεταξύ τους συνεργασίας και ανταλλαγής πληροφοριών. Επιπρόσθετα, η διεύθυνση λαμβάνει μέρος σε ευρωπαϊκές ασκήσεις στις οποίες επιδιώκει τη συμμετοχή και του ιδιωτικού τομέα, ως ασκουμένου, όπου αυτό είναι εφικτό.

4.5.Συμπεράσματα

- Σε δικαστικό επίπεδο δεν υφίστανται ειδικά δικαστήρια ή δικαστές επιφορτισμένοι με θέματα εγκλήματος στον κυβερνοχώρο. Δεν υπάρχουν εξάλλου ειδικοί εισαγγελείς, εκτός από δύο εισαγγελείς στην Εισαγγελία Πρωτοδικών Αθηνών. Συνεπώς, κατά τη γνώμη της Ομάδας Αξιολόγησης η ευαισθητοποίηση και η απόκτηση ειδικών γνώσεων για τα εγκλήματα του είδους αυτού μεταξύ δικαστών και εισαγγελέων απαιτούν τακτική και εξειδικευμένη εκπαίδευση.
- Η κεντρική αρχή επιβολής του νόμου όσον αφορά την καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι η Ελληνική Αστυνομική Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, η οποία εδρεύει στην Αθήνα και περιλαμβάνει πέντε τμήματα, καθώς και η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, που εδρεύει στη Θεσσαλονίκη. Η αποστολή της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Σύμφωνα με τις προσωπικές εμπειρίες της Ομάδας Αξιολόγησης, η οργανωτική δομή καλύπτει όλα τα πεδία της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.
- Σύμφωνα με τις παρουσιάσεις και τις προσωπικές συζητήσεις κατά την επίσκεψη αξιολόγησης, η εμπειρία της αστυνομίας φαίνεται ιδιαίτερα θετική, οι εργασίες επιβολής του νόμου είναι προδραστικές σε όλους τους τομείς, περιλαμβανομένων των κυβερνοεπιθέσεων, της απάτης με κάρτες πληρωμών και της σεξουαλικής εκμετάλλευσης παιδιών μέσω του Διαδικτύου.
- Η κεντρική ομάδα που είναι αρμόδια για τις εργαστηριακές εξετάσεις είναι το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών, που υπάγεται στην Ελληνική Αστυνομία. Σύμφωνα με την Ομάδα Αξιολόγησης οι εγκληματολογικές γνώσεις και πείρα του τμήματος φαίνεται να είναι υψηλού επιπέδου, αλλά από τη σύγκριση του αριθμού των υποθέσεων με τον αριθμό του προσωπικού προκύπτει επείγουσα ανάγκη αύξησης του προσωπικού ώστε να μειωθεί ο χρόνος που απαιτείται για τις διαδικασίες εργαστηριακής εξέτασης. Η διάρκεια της εργαστηριακής εξέτασης συχνά επηρεάζει τη διάρκεια της ποινικής διαδικασίας.
- Τα περισσότερα ψηφιακά πειστήρια πρέπει να εξετάζονται εργαστηριακά. Για το μέλλον θα πρέπει να εξεταστεί η βέλτιστη πρακτική για την αποτελεσματική διεκπεραίωση των εργαστηριακών εργασιών, ώστε να αποφεύγεται το πρόβλημα της συμφόρησης.

- Ως παράδειγμα βέλτιστης πρακτικής πρέπει να επισημανθεί ότι στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει συσταθεί ειδική υπηρεσία έκτακτης ανάγκης συνεχούς λειτουργίας (24/7), το λεγόμενο «Κέντρο Επιχειρήσεων Cyber Alert», όπου εξειδικευμένοι αστυνομικοί εξετάζουν κάθε συμβάν, μεταξύ των οποίων και εκείνα που απαιτούν άμεση αντιμετώπιση (λ.χ. εκδήλωση προθέσεων αυτοκτονίας). Επιπρόσθετα και για κινητά τηλέφωνα και tablets έχει δημιουργηθεί δωρεάν εφαρμογή με χρήσιμες συμβουλές σχετικά με την πλοήγηση στο Διαδίκτυο και με το πάτημα ενός κουμπιού πραγματοποιείται αυτόματα τηλεφωνική κλήση στο τηλεφωνικό κέντρο.
- Το τμήμα για το έγκλημα στον κυβερνοχώρο αντιμετωπίζει με επιτυχία τη διαδικτυακή απάτη με κάρτες σε συνεργασία με αεροπορικές εταιρείες και ταξιδιωτικούς πράκτορες. Η Ελλάδα είναι η πρώτη χώρα που εργάζεται στον τομέα αυτό σε καθημερινή βάση (η πρακτική ξεκίνησε ως σχέδιο της Ευρωπόλ/EC3). Είναι επίσης στις πρώτες θέσεις στις εργασίες του προγράμματος EMPACT.
- Θα άξιζε να διαμορφωθεί ειδικό τμήμα για το έγκλημα στον κυβερνοχώρο αποτελούμενο από εισαγγελείς εξειδικευμένους στον χειρισμό των σχετικών υποθέσεων, πράγμα που κατά τους αξιολογητές αποτελεί χρήσιμη μέθοδο για την ανταλλαγή πληροφοριών και πείρας. Η πείρα σε αστυνομικό επίπεδο φαίνεται ιδιαίτερα ικανοποιητική. Κατά συνέπεια η ύπαρξη τοπικών εισαγγελέων εξειδικευμένων στο έγκλημα στον κυβερνοχώρο θα μπορούσε να οδηγήσει στη δημιουργία ανάλογων δομών στο πλαίσιο των αρχών επιβολής του νόμου, δεδομένου ότι υφίσταται στενή σχέση μεταξύ εισαγγελίας και αστυνομίας από νομική και επιχειρησιακή άποψη.

5. ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ

5.1. Ουσιαστικό ποινικό δίκαιο σχετικά με το έγκλημα στον κυβερνοχώρο

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

- Η Ελλάδα έχει υπογράψει (23-1-2001) αλλά δεν έχει κυρώσει τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης, CETS 185). Προς το σκοπό αυτό έχει συγκροτηθεί ειδική νομοπαρασκευαστική επιτροπή (υπ' αριθμ. 84280 από 22-10-2013 Απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων). Αντικείμενο εργασιών της ιδίας επιτροπής αποτελούσε και η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών.

- Περαιτέρω, ως προς το πρόσθετο στην προαναφερθείσα Σύμβαση πρωτόκολλο, το οποίο επίσης υπογράφηκε την 28-1-2003 και δεν έχει κυρωθεί, πρέπει να επισημανθεί ότι πρόσφατα η Ελλάδα, με τον Ν. 4285/2014 (Α΄ 191), τροποποίησε την εθνική της νομοθεσία (Ν. 927/1979) για τα εγκλήματα που σχετίζονται με εκδηλώσεις ρατσισμού και ξενοφοβίας, προκειμένου να εναρμονιστεί με την απόφαση-πλαίσιο 2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008. Τα άρθρα 3 και 6 του Πρωτοκόλλου θεσπίζουν την υποχρέωση των κρατών μελών να ποινικοποιήσουν συγκεκριμένες συμπεριφορές, οι οποίες, αν ανατρέξουμε, αντίστοιχα, στα άρθρα 1 και 2 του Ν. 4285/2014, θα διαπιστώσουμε ότι καλύπτονται από τις προβλέψεις τους. Συγκεκριμένα, η διανομή ρατσιστικού υλικού (άρθρα 1 παρ. 1 και 3 του Πρωτοκόλλου) θα μπορούσε να ενταχθεί στο έγκλημα της δημόσιας υποκίνησης βίας ή μίσους του άρθρου 1 Ν. 927/1979, όπως τροποποιήθηκε με τον Ν. 4285/2014, υπό τον τρόπο τέλεσης της υποκίνησης, πρόκλησης ή διέγερσης. Άλλωστε, η «μέσω Διαδικτύου» τέλεση αυτών των πράξεων προβλέπεται ρητά ως έγκλημα του άρθρου αυτού όπως και έγκλημα του άρθρου 2.

Αντίστοιχα, οι προβλέψεις του άρθρου 6 του Πρωτοκόλλου για την άρνηση, την υποβάθμιση της σημασίας και την έγκριση ή τη δικαιολόγηση γενοκτονίας ή εγκλημάτων κατά της ανθρωπότητας τυποποιούνται στο άρθρο 2 Ν. 927/1979, όπως τροποποιήθηκε με το άρθρο 2 Ν. 4285/2014. Στο άρθρο αυτό τυποποιούνται ως αξιόποινες και συμπεριφορές όπως η επιδοκιμασία τέτοιων ενεργειών, κάτι που από το γράμμα του Πρωτοκόλλου δεν προκύπτει ρητά, ενώ αναφέρονται ρητά και άλλα εγκλήματα των οποίων η άρνηση καθίσταται αξιόποινη, όπως εγκλήματα πολέμου, το Ολοκαύτωμα και εγκλήματα του ναζισμού.

Στον Ν. 927/1979 προστέθηκε με το άρθρο 3 του Ν. 4285/2014, ειδική πρόβλεψη, ως άρθρο 3, για την εφαρμογή των ελληνικών ποινικών νόμων και συνεπώς την επέκταση της δικαιοδοσίας του ελληνικού κράτους. Ειδικότερα, προβλέπεται ότι σε περιπτώσεις που τα εγκλήματα των άρθρων 1 και 2 του Ν. 927/1979 τελούνται μέσω Διαδικτύου ή άλλου μέσου επικοινωνίας, εφόσον παρέχεται πρόσβαση στα μέσα αυτά από την ελληνική επικράτεια και ανεξάρτητα από τον τρόπο εγκατάστασής τους, τόπος τέλεσης θεωρείται και η Ελλάδα. Επισημαίνεται, όμως, ότι οι υπόλοιπες συμπεριφορές που προβλέπουν τα άρθρα 4 και 5 του Πρωτοκόλλου (απειλή και προσβολή αντίστοιχα λόγω ρατσιστικών ή ξενοφοβικών κινήτρων) μπορεί να μην περιλαμβάνονται στον Ν. 927/1979, όπως τροποποιήθηκε με τον Ν. 4285/2015, όμως τυποποιούνται σε αντίστοιχα εγκλήματα του ΠΚ ή σε άλλα νομοθετήματα. Η απειλή συνιστά έγκλημα κατ' άρθρο 333 ΠΚ, όταν όμως ο δράστης ορμάται από συγκεκριμένα κίνητρα, ο συνδυασμός του άρθρου αυτού με το άρθρο 81 Α ΠΚ (που προστέθηκε με το άρθρο 10 Ν. 4285/2014) επαυξάνει το κατώτερο προβλεπόμενο όριο ποινής. Μάλιστα αν συντρέχει περίπτωση εφαρμογής του άρθρου 81 Α ΠΚ προβλέφθηκε η επιβολή της παρεπόμενης ποινής της στέρησης των πολιτικών δικαιωμάτων (άρθρο 61 περ. β ΠΚ). Η δημόσια προσβολή μπορεί να μην αποτελεί έγκλημα κατά τον ελληνικό ΠΚ, έγκλημα αποτελεί, όμως, η εξύβριση κατ' άρθρο 361 ΠΚ και μπορεί και σε αυτό να ισχύσουν τα προηγούμενα, σύμφωνα με το άρθρο 81 Α ΠΚ.

Μετά την επίσκεψη αξιολόγησης το άρθρο 81 Α του Ποινικού Κώδικα τροποποιήθηκε, μέσω του άρθρου 21 του Ν. 4356/2015. Πριν από την τροποποίηση το άρθρο 81 Α είχε εφαρμογή μόνο εφόσον είχε αποδειχθεί το μίσος του δράστη. Κατά συνέπεια το άρθρο 81 Α εφαρμοζόταν σπανίως, δεδομένου ότι η απόδειξη μιας εσώτερης διάθεσης όπως το "μίσος" παρουσιάζει σοβαρές δυσκολίες. Ο νέος τίτλος του άρθρου 81 Α είναι "Έγκλημα με ρατσιστικά χαρακτηριστικά". Σύμφωνα με τη νέα διατύπωση, το άρθρο 81 Α εφαρμόζεται οσάκις ο δράστης τέλεσε έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των ιδιαίτερων χαρακτηριστικών του προσώπου αυτού, όπως η φυλή, το χρώμα, η εθνική ή εθνοτική καταγωγή, οι γενεαλογικές καταβολές, η θρησκεία, η σωματική ή ψυχική αναπηρία, ο σεξουαλικός προσανατολισμός ή τα χαρακτηριστικά φύλου. Με τη νέα τροποποιημένη διατύπωση όχι μόνο διευρύνεται το πεδίο εφαρμογής της διάταξης, αλλά επίσης διευκολύνεται η απόδειξη: αντί να απαιτείται η δυσχερής απόδειξη μιας εσώτερης διάθεσης όπως το μίσος, αρκεί να αποδειχθεί ένα αντικειμενικό γεγονός, δηλ. η επιλογή του θύματος λόγω των ιδιαίτερων χαρακτηριστικών του.

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 συστημάτων πληροφοριών

Γενικά, στην ελληνική νομοθεσία δεν προβλέπεται η ποινική ευθύνη νομικών προσώπων. Ωστόσο, σε περιπτώσεις εγκλημάτων που διαπράττονται από νομικό πρόσωπο, η ελληνική εθνική νομοθεσία προβλέπει ευθύνη των φυσικών προσώπων που έχουν το δικαίωμα εκπροσώπησης της νομικής οντότητας (π.χ. διευθύνοντες σύμβουλοι, μέλη διοικητικού συμβουλίου).

Όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, ο νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα προβλέπει κυρώσεις για οποιαδήποτε παραβίαση των διατάξεών του από υπεύθυνο επεξεργασίας. Πιο συγκεκριμένα, η ΕΑΠΔΠΧ μπορεί να επιβάλλει διοικητικές κυρώσεις έως το ποσό των 150.000 ευρώ. Στο νόμο περί προστασίας δεδομένων (2472/1997) δεν προβλέπονται σχετικά ρητά κριτήρια. Ωστόσο, το άρθρο 10 σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας ορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων που να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Ο καθορισμός του «ανάλογου» επιπέδου ασφάλειας βασίζεται σε κριτήρια όπως αριθμός υποκειμένων των δεδομένων, όγκος δεδομένων προσωπικού χαρακτήρα κ.λπ.

Όσον αφορά ελάσσονες υποθέσεις, βάσει του άρθρου 19 του νόμου περί προστασίας των δεδομένων (υπ' αριθμ. 2472/1997), η ΕΑΠΔΠΧ εξετάζει όλα τα παράπονα των υποκειμένων των δεδομένων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους, όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν. Ωστόσο, η ΕΑΠΔΠΧ μπορεί να θέτει στο αρχείο αιτήσεις ή παράπονα που κρίνονται προδήλως αόριστα, αβάσιμα ή υποβάλλονται καταχρηστικώς ή ανωνύμως. Ταυτόχρονα, μπορεί να εξετάζει κατά προτεραιότητα αιτήσεις, παράπονα και ερωτήματα με κριτήριο τη σπουδαιότητα και το γενικότερο ενδιαφέρον του θέματος.

Επιπρόσθετα σε όσα αναφέρονται στην απάντηση 1.9, σκοπεύουμε να κυρώσουμε σύντομα τη Σύμβαση για το έγκλημα στον κυβερνοχώρο και να μεταφέρουμε στο εθνικό δίκαιο την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών, καθώς και πρόσθετο στην προαναφερθείσα Σύμβαση πρωτόκολλο, το οποίο υπογράφηκε την 28-1-2003 και δεν έχει κυρωθεί.

Στόχος είναι όλα τα αναγκαία βήματα για την εν λόγω μεταφορά στο εθνικό δίκαιο να ολοκληρωθούν το συντομότερο δυνατό. Η ειδική νομοπαρασκευαστική επιτροπή που εργάζεται προς αυτόν τον σκοπό έχει σχεδόν ολοκληρώσει τις εργασίες της και το σχετικό νομοσχέδιο θα διαβιβαστεί αμέσως στη Βουλή.

Η καθυστέρηση που σημειώθηκε σε αυτή τη διαδικασία οφείλεται στον φόρτο εργασίας τόσο του Υπουργείου όσο και της Βουλής, λόγω της εντατικής προσπάθειας που καταβάλλει η Ελλάδα ώστε να ληφθούν όλα τα αναγκαία μέτρα (νομοθετικά και διαρθρωτικά) για την εκπλήρωση των υποχρεώσεών της έναντι της ΕΕ και του ΔΝΤ σύμφωνα με τη συμφωνία διευκόλυνσης οικονομικής ενίσχυσης.

Τρεις, έως σήμερα, γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου αναφέρονται στο απόρρητο της επικοινωνίας.

Αναφέρεται χαρακτηριστικά ότι τα αιτήματα εισαγγελικών, ανακριτικών και προανακριτικών αρχών προς τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών (σταθερής- κινητής τηλεφωνίας, Διαδικτύου κ.λπ.) για παροχή στοιχείων εντοπισμού της ταυτότητας προσώπων είναι συνταγματικώς ανεκτά.

Δεν έχει γίνει ακόμη ενσωμάτωση στην εθνική νομοθεσία της οδηγίας 2013/40/ΕΕ.

Ωστόσο, έχει συσταθεί ειδική νομοπαρασκευαστική επιτροπή αφενός για την ενσωμάτωση στο ελληνικό δίκαιο της οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου και αφετέρου για την επανεξέταση, την επικαιροποίηση και την αναδιατύπωση του νομοσχεδίου που συντάχθηκε για τη μεταφορά στο εθνικό δίκαιο της Σύμβασης για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης (πρέπει να σημειωθεί ότι η επικαιροποίηση του εν λόγω νομοσχεδίου είναι αναγκαία διότι με αυτό μεταφέρονται στην εθνική νομοθεσία οι διατάξεις της απόφασης-πλαισίου 2005/222/ΔΕΥ).

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

Η οδηγία έχει μεταφερθεί στο εθνικό δίκαιο με τον Ν. 4267/2014.

Η μεταφορά της οδηγίας έχει επιφέρει αλλαγές στα έως τώρα προβλεπόμενα εγκλήματα βάσει των άρθρων 348Α, 348Β, 339 παρ. 4 του Ποινικού Κώδικα, εισάγοντας το έγκλημα των πορνογραφικών παραστάσεων ανηλίκων βάσει του άρθρου 348Γ. Όσον αφορά τη θέσπιση εκτελεστικών μέτρων για τις διατάξεις της οδηγίας, σημειώνεται ότι έχουν εντοπιστεί δυσκολίες στο άρθρο 10 της οδηγίας σχετικά με την πρόσβαση τρίτων στο ποινικό μητρώο προσώπων που έχουν τακτικές επαφές με παιδιά καθώς η εν λόγω πρόσβαση, σύμφωνα με την οδηγία, ζητείται σύμφωνα με το εθνικό δίκαιο (παρ. 2) το οποίο, μέσω του Κώδικα Ποινικής Δικονομίας και του Ν. 2472/1997, έχει ορίσει επακριβώς ποιος δύναται να έχει πρόσβαση σε πληροφορίες σχετικά με ποινικές καταδίκες ή διώξεις. Επίσης, η οδηγία προβλέπει την ανταλλαγή τέτοιων πληροφοριών μέσω των διατάξεων της απόφασης-πλαισίου 2009/315/ΔΕΥ, η οποία δεν έχει ακόμη μεταφερθεί στην εθνική έννομη τάξη. Στο άρθρο 10 παράγραφος 2 της οδηγίας θεσπίζεται η υποχρέωση των κρατών μελών να λαμβάνουν τα απαραίτητα μέτρα για να διασφαλίζουν ότι οι εργοδότες δικαιούνται να ζητούν πληροφορίες, σύμφωνα με το εθνικό δίκαιο και με κάθε πρόσφορο τρόπο, όπως η πρόσβαση κατόπιν αιτήματος (στο ποινικό μητρώο προσώπων) ενώ παράλληλα στην αιτιολογική σκέψη 41 τονίζεται ότι λαμβάνονται δεόντως υπόψη οι διαφορετικές νομικές παραδόσεις των κρατών μελών και ότι δεν προβλέπεται, από την εν λόγω οδηγία, η υποχρέωση τροποποίησης των εθνικών συστημάτων που διέπουν τα ποινικά μητρώα ή τους τρόπους πρόσβασης σε αυτά. Περαιτέρω, στην παρ. 3 του άρθρου 10 της οδηγίας για την ανταλλαγή τέτοιους είδους πληροφοριών, γίνεται παραπομπή στις διατάξεις της απόφασης-πλαισίου 2009/315/ΔΕΥ.

Ένα άλλο θέμα είναι αυτό των προγραμμάτων ή των μέτρων παρέμβασης για την ελαχιστοποίηση των κινδύνων επανάληψης αδικημάτων σεξουαλικού χαρακτήρα σε βάρος παιδιών (άρθρο 24 της οδηγίας) και ιδίως η αξιολόγηση της επικινδυνότητας των προσώπων αυτών με σκοπό τον προσδιορισμό κατάλληλων προγραμμάτων ή μέτρων παρέμβασης.

Ως προς τις συμπεριφορές που πρέπει να τυποποιηθούν ως εγκλήματα, σύμφωνα με το άρθρο 5 της οδηγίας, στην παρ.3 προβλέπεται ότι η εν γνώσει απόκτηση πρόσβασης σε παιδική πορνογραφία μέσω της τεχνολογίας των πληροφοριών και των επικοινωνιών τιμωρείται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον ένα έτος. Δεν προσδιορίζεται όμως στο κείμενο η έννοια του όρου «εν γνώσει» και μόνο στο προοίμιο, στο σημείο 18, διευκρινίζεται ότι για να υφίσταται ευθύνη θα πρέπει να επιδιώξει το πρόσωπο την πρόσβαση σε ιστότοπο όπου διατίθεται τέτοιο υλικό και να γνωρίζει ότι εκεί υπάρχουν τέτοιες εικόνες. Ο εκούσιος χαρακτήρας θα πρέπει, σύμφωνα με το προοίμιο, να συναχθεί από το γεγονός ότι έχει διαπραχθεί μέσω υπηρεσίας έναντι πληρωμής ή κατ' επανάληψη. Αντιθέτως εναποτίθεται στη διακριτική ευχέρεια του κράτους μέλους να εκτιμήσει κατά πόσο η απόκτηση ή κατοχή υλικού παιδικής πορνογραφίας ή η παραγωγή του αφορά απεικονίσεις προς ιδία χρήση και η πράξη δεν συνεπάγεται κίνδυνο διάδοσης, και να κρίνει αν το εν λόγω πρόσωπο θα τιμωρηθεί ή όχι (άρθρο 5 παρ. 8). Η εν γνώσει παράβαση, όμως, πρέπει υποχρεωτικά να τυποποιηθεί ως αξιόποινη.

Γ/ Διαδικτυακή απάτη με κάρτες

Τόσο πολίτες (μηνυτής ή πληρεξούσιος δικηγόρος) όσο και οι ιδιωτικές εταιρείες έχουν τη δυνατότητα υποβολής έκθεσης ένορκης εξέτασης-καταγγελίας που αφορούν απάτη μέσω Διαδικτύου, στις αρχές επιβολής του νόμου και στις Εισαγγελικές Αρχές. Η υποβολή μηνυτήριας αναφοράς στις αρχές επιβολής του νόμου μπορεί να πραγματοποιηθεί είτε στο κατά τόπους αρμόδιο αστυνομικό τμήμα της περιοχής που διαμένει ο πολίτης ή εδρεύει η εταιρεία, είτε απ' ευθείας στη ΔΙ.Δ.Η.Ε., με φυσική παρουσία.

Η υποβολή μηνυτήριας αναφοράς, εκτός από τις αρχές επιβολής του νόμου, μπορεί να υποβληθεί σύμφωνα με την παράγραφο 2 του άρθρου 42 του Κώδικα Ποινικής Δικονομίας απ' ευθείας στον εισαγγελέα πλημμελειοδικών.

Επιπρόσθετα, οι πολίτες και οι ιδιωτικές εταιρείες έχουν τη δυνατότητα της καταγγελίας αδικημάτων που σχετίζονται με διαδικτυακή απάτη με χρήση κάρτας πληρωμής στη ΔΙ.Δ.Η.Ε., μέσω μηνύματος ηλεκτρονικού ταχυδρομείου, καθώς πρόκειται για αδίκημα διωκόμενο αυτεπαγγέλτως.

Υπάρχει συνεργασία και αλληλοενημέρωση της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων με τον τραπεζικό τομέα για περιστατικά ηλεκτρονικών επιθέσεων καθώς και εργαλεία-τεχνικές που χρησιμοποιούνται από τους επιτιθέμενους.

Υπάρχει αποτελεσματική συνεργασία μεταξύ τραπεζών και αρχών επιβολής του νόμου για την πρόληψη και την καταπολέμηση της διαδικτυακής απάτης με κάρτες.
Στην ΕΕΤ έχει συσταθεί ειδική διατραπεζική επιτροπή για την αντιμετώπιση της απάτης στα συστήματα πληρωμών. Τα μέλη αυτής της επιτροπής είναι εκπρόσωποι των τραπεζών, της Τράπεζας της Ελλάδος και της Ελληνικής Αστυνομίας. Στο πλαίσιο της επιτροπής εξετάζονται οι νέες τάσεις στις απάτες, συμβάντα και μέτρα/τεχνολογίες αντιμετώπισης προκειμένου να ληφθούν κατάλληλα μέτρα. Η επιτροπή χρησιμοποιεί κατάλογο επαφών επαγρύπνησης με τα στοιχεία επαφής των αρμόδιων εκπροσώπων. Οι επαφές του καταλόγου ενημερώνονται για κάθε είδους συμβάν που αφορά απάτη με κάρτες πληρωμών (ATM & POS skimming/«ξάφρισμα», απάτη στο ηλεκτρονικό εμπόριο κ.λπ.)

- **Ειδοποιούν την αστυνομία/αρχές επιβολής του νόμου εάν αντιληφθούν κατάχρηση των νέων εργαλείων πληρωμής που αναπτύσσονται από την αντίστοιχη βιομηχανία;**

Οι αρχές επιβολής του νόμου βρίσκονται σε συνεργασία με τον ιδιωτικό τομέα της χώρας. Ειδικότερα, όσον αφορά τα πιστωτικά ιδρύματα της χώρας, στα πλαίσια της διατραπεζικής επιτροπής για την πρόληψη και την αντιμετώπιση της απάτης στα μέσα και τα συστήματα πληρωμών καθώς και της ad hoc διατραπεζικής ομάδας έργου που παραλαμβάνει εμπιστευτικού περιεχομένου ενημέρωση που διαβιβάζει η Ευρωπόλ, πραγματοποιείται ανταλλαγή εμπιστευτικής πληροφορίας μέσω της Ευρωπαϊκής Κεντρικής Τράπεζας και του EC3 που αφορούν νέες μεθόδους ή νέα εργαλεία πληρωμής. Αντίστοιχα, ανταλλαγή εμπιστευτικής πληροφορίας σε εθνικό επίπεδο μεταξύ των πιστωτικών ιδρυμάτων και των αρχών επιβολής του νόμου, πραγματοποιείται μέσω της ομάδας εργασίας για την καταπολέμηση των απατών μέσω Διαδικτύου (internet fraud).

- **Αυξάνουν την ασφάλεια στις πληρωμές που δεν γίνονται με μετρητά και ελαχιστοποιούν την ευπάθεια των μαγνητικών ταινιών;**

Για την αποτελεσματική συνεργασία μεταξύ ιδιωτικού τομέα και αρχών επιβολής του νόμου, η ΔΙ.Δ.Η.Ε, στα πλαίσια των αρμοδιοτήτων της, πραγματοποιεί ενημερώσεις ευαισθητοποίησης στον ιδιωτικό τομέα αναφορικά με νέες τάσεις στο θέμα των διαδικτυακών απατών καθώς και παροχή συμβουλών για λήψη κατάλληλων μέτρων πρόληψης.

Η υιοθέτηση της νέας τεχνολογίας EMV στο σύνολο των καρτών του χαρτοφυλακίου από τα πιστωτικά ιδρύματα της χώρας έχει πλέον ως αποτέλεσμα την ενίσχυση στον μέγιστο βαθμό της ασφάλειας στις πληρωμές με παρουσία κάρτας, ελαχιστοποιώντας την ευπάθεια των μαγνητικών ταινιών.
Στις ελληνικές κάρτες πληρωμών χρησιμοποιείται κυρίως η τεχνολογία EMV/chip και PIN. Όλες οι εκδότριες τράπεζες χρησιμοποιούν συστήματα παρακολούθησης κατά της απάτης για τις συναλλαγές με κάρτες πληρωμών. Όποτε χρησιμοποιείται μια ελληνική κάρτα πληρωμής στο εξωτερικό, και ιδίως σε χώρα που δεν χρησιμοποιεί τεχνολογία EMV (π.χ. ΗΠΑ), εκτελείται μια σειρά ειδικών ελέγχων ασφάλειας.

- **Ενισχύουν τη διαδικασία έγκρισης των διαδικτυακών συναλλαγών και την εξακρίβωση της ταυτότητας του πελάτη;**

Για την καταπολέμηση των απατών μέσω Διαδικτύου, κάθε εταιρεία έχει υιοθετήσει το δικό της σύστημα προστασίας από απάτες. Τα συστήματα προστασίας από απάτες πραγματοποιούν διεξαγωγή ελέγχων, σε πραγματικό χρόνο, για τον εντοπισμό περιπτώσεων απάτης στις διαδικτυακές συναλλαγές με χρήση καρτών πληρωμής.
Όσον αφορά τα πιστωτικά ιδρύματα της χώρας, υπάρχει δίαυλος επικοινωνίας και άμεσης συνεργασίας μεταξύ αυτών για την ενίσχυση της διαδικασίας εξακρίβωσης των στοιχείων των πελατών με σκοπό τον έγκαιρο περιορισμό των δόλιων συναλλαγών.

Οι ελληνικές τράπεζες διαθέτουν υπερσύγχρονη υποδομή διαδικτυακών πληρωμών καθώς επίσης εξελιγμένα και αποτελεσματικά μέτρα ασφαλείας όπως για παράδειγμα:

- Εξειδικευμένους μηχανισμούς ασφαλείας με πολλαπλά επίπεδα άμυνας.
- Παρακολούθηση και εντοπισμό δόλιων συναλλαγών με κάρτα.
- Υπηρεσίες όπως MasterCard® SecureCode™ ή Verified by VISA ως υπηρεσίες επαλήθευσης της ταυτότητας του κατόχου της κάρτας κατά την πραγματοποίηση αγορών μέσω Διαδικτύου.

Επιπλέον των ανωτέρω, τα τελευταία χρόνια οι τράπεζες εκπαιδεύουν συστηματικά τους πελάτες τους να μην αποκαλύπτουν τα στοιχεία των καρτών τους (αριθμό κάρτας, PIN, CCV2) και τα προσωπικά τους στοιχεία (αριθμό ταυτότητας, ημερομηνία γέννησης) και να τα προστατεύουν αποτελεσματικά.

5.2. Διαδικαστικά ζητήματα

5.2.1. Τεχνικές έρευνας

Η εθνική νομοθεσία επιτρέπει όλες τις ειδικές τεχνικές έρευνας που **αναφέρονται στο ερωτηματολόγιο**. Το 7ο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών, βάσει του άρθρου 30 παρ. 22 του Π.Δ. 178/2014, σε συνδυασμό με τα άρθρα 183-208, 243, 251, 333, 362 και 458 του Κώδικα Ποινικής Δικονομίας, πραγματοποιεί εργαστηριακές εξετάσεις επί των ψηφιακών πειστηρίων που αποστέλλονται από τις προανακριτικές/ανακριτικές Αρχές. Ως εκ τούτου, οι ως άνω αρχές είναι υπεύθυνες για την προανακριτική διαδικασία (όπως έρευνα, κατάσχεση, παγίδευση σε πραγματικό χρόνο/συλλογή δεδομένων διακίνησης/ περιεχομένου, κ.α.). Μετά την κατάσχεση τα εν λόγω πειστήρια αποστέλλονται για περαιτέρω εργαστηριακή εξέταση, συνοδευόμενα από σαφή ερωτήματα στοιχεία/πληροφορίες σχετικά με την υπό εξέταση υπόθεση.

Με το πέρας των εξετάσεων συντάσσεται Έκθεση Εργαστηριακής Πραγματογνωμοσύνης, η οποία, συνοδευόμενη από τα ψηφιακά πειστήρια, αποστέλλεται στην αιτούσα υπηρεσία. Αξίζει να σημειωθεί ότι το προαναφερόμενο Τμήμα παρέχει συνδρομή στις προανακριτικές/ανακριτικές αρχές με τεχνικές πληροφορίες σε οποιοδήποτε στάδιο της προανακριτικής διαδικασίας και ειδικότερα στο στάδιο της κατάσχεσης των ψηφιακών πειστηρίων. Τέλος, το σύνολο των ενεργειών που ακολουθούνται από τη στιγμή της παραλαβής των πειστηρίων έως την σύνταξη της Έκθεσης Εργαστηριακής Πραγματογνωμοσύνης και αποστολής αυτών, πραγματοποιούνται με συγκεκριμένες διαδικασίες που περιγράφονται στα πρότυπα I.S.O. (ELOT EN ISO 9001:2008, ELOT EN ISO/IEC 17020) και είναι σύμφωνες με τις αρχές και τις κατευθυντήριες οδηγίες του Ευρωπαϊκού Δικτύου Εγκληματολογικών Ινστιτούτων (ENFSI).

Σύμφωνα με το άρθρο 19 παρ. 1 στοιχείο η) του Ν. 2472/1997, η ΕΑΠΔΠΧ έχει την αρμοδιότητα να διενεργεί ελέγχους κατόπιν καταγγελίας. Κατά τη διεξαγωγή αυτών των ελέγχων, η ΕΑΠΔΠΧ έχει δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και συλλογής κάθε πληροφορίας για τους σκοπούς του ελέγχου, χωρίς να μπορεί να της αντιταχθεί κανενός είδους απόρρητο.

Η διαδικασία για την άρση του απορρήτου των επικοινωνιών περιγράφεται στο προεδρικό διάταγμα 47/2005 με τίτλο «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου επικοινωνιών και για τη διασφάλισή του» (ΦΕΚ Α'64/10.3.2005).

Οι κυριότερες ειδικές τεχνικές διερεύνησης που χρησιμοποιούνται για την καταπολέμηση της πορνογραφίας ανηλίκων είναι η χρήση εξειδικευμένου λογισμικού για την εύρεση διαδικτυακής διακίνησης τέτοιου υλικού ή τεχνικές ανακριτικής διείσδυσης, δηλαδή κατόπιν σχετικού βουλεύματος μάς επιτρέπεται η χρήση-διαχείριση προφίλ που παριστάνουν ανήλικους ή διακινητές υλικού πορνογραφίας ανηλίκων. Επιπρόσθετα, υπάρχει στενή συνεργασία με Ευρωπόλ και Interpol, ενώ προσφάτως ενταχθήκαμε στη βάση της Interpol για την αναγνώριση ανήλικων θυμάτων σεξουαλικής παρενόχλησης.

Επιπροσθέτως, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών, κατά την εξέταση των ψηφιακών πειστηρίων επί υποθέσεων ηλεκτρονικού εγκλήματος, ακολουθεί κατάλληλες και διεθνώς αναγνωρισμένες εγκληματολογικές διαδικασίες.

Η ΕΑΠΔΠΧ χρησιμοποιεί διάφορες τεχνικές η πλέον συνήθης εκ των οποίων είναι η προσομοίωση του modus operandi του δράστη όσον αφορά τα προγράμματα που χρησιμοποιούνται για την παράνομη δραστηριότητα. Αυτό γίνεται με 2 τρόπους: α) Εικονικοποίηση σε λειτουργία μόνο για ανάγνωση του εγκληματολογικού αντιγράφου του σκληρού δίσκου του υπολογιστή του δράστη. β) Εκτέλεση του προγράμματος του δράστη (π.χ. πρόγραμμα αποστολής μαζικής αλληλογραφίας) σε απομονωμένο περιβάλλον δοκιμών με φόρτωση στο πρόγραμμα όλων των στοιχείων που αφορούν τη χρήση του προγράμματος από τον δράστη (π.χ. αρχείων ρυθμίσεων, δεδομένων μαζικής αποστολής μηνυμάτων e-mail κ.λπ.)

Με τη χρήση της ανακριτικής διείσδυσης, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος κατάφερε να εντοπίσει συνολικά εβδομήντα οχτώ (78) άτομα που διακινούσαν υλικό πορνογραφίας ανηλίκων μέσω συγκεκριμένου ιστοτόπου, τα ηλεκτρονικά ίχνη των οποίων προέκυπταν σε τριάντα δύο (32) διαφορετικές χώρες του κόσμου. Σε ό,τι αφορά την Ελλάδα, προέκυψαν τρεις (3) χρήστες.

Όσον αφορά την εξέταση των ψηφιακών πειστηρίων, μια καλή πρακτική που σχετίζεται με την δημιουργία εικονικού αντιγράφου, σε περιπτώσεις που οι προς εξέταση σκληροί δίσκοι παρουσιάζουν πολλά σφάλματα ανάγνωσης, είναι η δημιουργία αυτού από το τέλος προς την αρχή (Copy sectors in reverse order) και όχι η συνήθης διαδικασία που ακολουθείται.

Το δίδαγμα που αποκομίζει κανείς από τη χρήση τεχνικών έρευνας για το έγκλημα στον κυβερνοχώρο είναι ότι κάθε υπόθεση είναι μοναδική και τα εργαλεία που χρησιμοποιούνται σε μία υπόθεση δεν είναι βέβαιο ότι θα φέρουν αποτέλεσμα και στις υπόλοιπες. Οπότε, όπως εξάλλου ορίζουν και οι βέλτιστες πρακτικές, πρέπει κανείς να γνωρίζει τα εργαλεία του έτσι ώστε να γνωρίζει τις δυνατότητές τους, αν μεταβάλλουν τα δεδομένα (όσον αφορά τα εργαλεία συλλογής ευμετάβλητων δεδομένων) και ποιες είναι οι ροές δεδομένων τους. Αυτό πρέπει να γίνεται προκειμένου α) να συντάσσονται εκθέσεις οι οποίες να πληρούν τις προδιαγραφές της εγκληματολογικής επιστήμης και β) να είμαστε σε θέση να βελτιώνουμε διαρκώς τη μεθοδολογία μας ενσωματώνοντας στη διαδικασία τα διδάγματα που αποκομίζουμε από κάθε μας έρευνα.

5.2.2. Εγκληματολογική εξέταση και κρυπτογράφηση

Το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών πραγματοποιεί μόνο ηλεκτρονική εργαστηριακή εξέταση επί των υποβληθέντων πειστηρίων και όχι εξ αποστάσεως εξέταση. Η εγκληματολογική εξέταση των ψηφιακών πειστηρίων διέπεται από συγκεκριμένες αρχές, που πρέπει να τηρούνται απαρέγκλιτα, για να θεμελιώνεται και να αποδεικνύεται η βασιμότητα και η αξιοπιστία των εργαστηριακών εξετάσεων και ευρημάτων. Οι αρχές αυτές προβλέπονται και περιγράφονται αναλυτικότερα στις διαδικασίες ISO της ως άνω υπηρεσίας.

Η ΕΑΠΔΠΧ δεν έχει διενεργήσει εργαστηριακές εξετάσεις εξ αποστάσεως αλλά διενεργεί εργαστηριακές εξετάσεις και αναλύσεις των συλλεγόμενων πειστηρίων στο εργαστήριο που διαθέτει στις εγκαταστάσεις της. Αυτή η εξέταση αφορά ευμετάβλητα και μη ευμετάβλητα δεδομένα που μπορεί να περιλαμβάνουν από αρχεία καταγραφής διακομιστών (web server log files) έως είδωλα μνημών και εργαστηριακά αντίγραφα σκληρών δίσκων. Κατά τη διάρκεια της εξέτασης χρησιμοποιούνται τόσο ελεύθερα (open source) εργαλεία (π.χ. Volatility Memory Forensics Framework) όσο και εμπορικά εργαλεία (π.χ. Encase) προκειμένου να ανευρεθεί το modus operandi των δραστών, τα ίχνη της δραστηριότητάς τους και να συσχετισθούν όλα τα υπάρχοντα στοιχεία με άλλες πιθανές παράνομες δραστηριότητες τρίτων που δεν έχουν ακόμη περιέλθει σε γνώση μας (πελάτες δραστών, οι προμηθευτές τους κ.λπ.)

Η κρυπτογράφηση αποτελεί ίσως το μεγαλύτερό πρόβλημα της εργαστηριακής εξέτασης των ψηφιακών πειστηρίων καθώς σε περίπτωση μη επιτυχούς αποκρυπτογράφησης δεν υφίσταται η δυνατότητα εξέτασης και επομένως δεν παρέχονται καθόλου πληροφορίες στις αιτούσες αρχές. Για την αποκρυπτογράφηση των δεδομένων, η Ελληνική Αστυνομία χρησιμοποιεί ειδικό εγκληματολογικό λογισμικό καθώς και υπολογιστές με μεγάλη επεξεργαστική ισχύ.

Σε περίπτωση που τα δεδομένα έχουν κρυπτογραφηθεί, είτε με μεγάλο αριθμό χαρακτήρων, είτε με συνδυασμό αρχείων αντί για κωδικό, το ως άνω Τμήμα δεν δύναται να αποκρυπτογραφήσει τα ψηφιακά δεδομένα. Σε σοβαρές περιπτώσεις (όπως υποθέσεις τρομοκρατίας και οργανωμένου εγκλήματος) όπου δεν δύναται το προαναφερόμενο Τμήμα να αποκρυπτογραφήσει τα δεδομένα, ζητείται η συνδρομή από το Τμήμα EC3 της Ευρωπόλ.

Επιπρόσθετα, μέχρι σήμερα δεν υφίσταται νομικό πλαίσιο στο οποίο να μας δίνεται η δυνατότητα συνεργασίας με ιδιωτικές εταιρείες.

Η ΕΑΠΔΠΧ έχει συναντήσει υποθέσεις στις οποίες έπρεπε να γίνει αποκρυπτογράφηση συμπιεσμένων και κρυπτογραφημένων αρχείων καθώς και κρυπτογραφημένων αρχείων Excel και Word. Αυτά τα αρχεία αποκρυπτογραφήθηκαν με εργαλεία που είτε εκμεταλλεύονται γνωστές ευπάθειες είτε ανακαλύπτουν τους κωδικούς πρόσβασης των αρχείων δοκιμάζοντας όλους τους πιθανούς συνδυασμούς (εργαλεία «brute force»).

Η ΕΑΠΔΠΧ ασχολήθηκε επίσης με μια υπόθεση στην οποία στάθηκε αδύνατη η αποκρυπτογράφηση των αρχείων/κωδικών πρόσβασης καθώς ο ύποπτος είχε χρησιμοποιήσει συγκεκριμένο λογισμικό διαχείρισης κωδικών πρόσβασης που δεν μπορούσε να παραβιαστεί με τον διαθέσιμο εξοπλισμό.

5.2.3. Ηλεκτρονικά πειστήρια

Έννοιες όπως δεδομένα υπολογιστή, δεδομένα περιεχομένου, δεδομένα κίνησης, εντολή για αναζήτηση/κατάσχεση συστήματος πληροφοριών, δίκτυα υπαγόμενα στη διαχείριση και τον έλεγχο υπόπτων για εγκλήματα στον κυβερνοχώρο δεν ορίζονται στην εθνική νομοθεσία αλλά μόνον στη Σύμβαση της Βουδαπέστης, η οποία όμως δεν έχει μέχρι στιγμής ενσωματωθεί στο εθνικό δίκαιο. Συνεπώς, μόνο ως πρακτική ακολουθούμε τις έννοιες/όρους που περιγράφονται στην προαναφερόμενη Σύμβαση.

Τα δεδομένα κίνησης ορίζονται στο άρθρο 2 του Ν. 3471/2006 με τον οποίο μεταφέρεται στην εθνική έννομη τάξη η οδηγία 2002/58/ΕΚ και στον οποίο συμπεριλαμβάνεται ο ορισμός των «δεδομένων κίνησης».

Δεν υπάρχει νομοθεσία ειδικά για τα ηλεκτρονικά πειστήρια. Όσον αφορά τη συλλογή, αποθήκευση και μεταφορά των ηλεκτρονικών πειστηρίων, η ΕΑΠΔΠΧ τηρεί «αλυσίδα φύλαξης» και ακολουθεί διεθνώς αποδεκτές κατευθυντήριες γραμμές όπως οι κατευθυντήριες γραμμές της ACPO (Ένωση Ανώτερων Αξιωματικών της Αστυνομίας).

Σύμφωνα με το άρθρο 19 παράγραφος 3 του Συντάγματος της Ελλάδας, απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α.

Κατά τη διαδικασία κατάσχεσης και εν συνεχεία υποβολής των ηλεκτρονικών πειστηρίων, θα πρέπει να τηρούνται συγκεκριμένοι κανόνες από τις αρχές που προβαίνουν στην κατάσχεση:

1ος ΚΑΝΟΝΑΣ

Καμία ενέργεια που γίνεται από το άτομο που προβαίνει στην κατάσχεση δεν θα πρέπει να μεταβάλει τα δεδομένα που βρίσκονται αποθηκευμένα σε ένα υπολογιστικό σύστημα ή αποθηκευτικό μέσο, το οποίο στη συνέχεια θα κατασχεθεί και θα αποσταλεί ως πειστήριο.

2ος ΚΑΝΟΝΑΣ

Στην περίπτωση που το άτομο που προβαίνει στην κατάσχεση κρίνει αναγκαία την προσπέλαση των ψηφιακών δεδομένων που βρίσκονται αποθηκευμένα σε ένα υπολογιστικό σύστημα ή αποθηκευτικό μέσο, το άτομο αυτό θα πρέπει να είναι εκπαιδευμένο να το πράξει και να είναι σε θέση να τεκμηριώσει τις ενέργειες του αυτές, καθώς και τις αλλαγές που επέφερε στα ψηφιακά δεδομένα και στο υπολογιστικό σύστημα εν γένει.

3ος ΚΑΝΟΝΑΣ

Το άτομο που προβαίνει στην κατάσχεση, θα πρέπει να καταγράφει εγγράφως οποιεσδήποτε ενέργειές του επί των υπολογιστικών συστημάτων και των αποθηκευμένων δεδομένων αυτών, οι οποίες θα πρέπει να συνοδεύουν την έκθεση κατάσχεσης και το διαβιβαστικό προς τον Εισαγγελέα και την παρούσα υπηρεσία. Με την χρήση των ανωτέρω σημειώσεων ένα τρίτο άτομο θα πρέπει να μπορεί να καταλήξει στο ίδιο αποτέλεσμα, εάν προβεί στις ίδιες ενέργειες.

4ος ΚΑΝΟΝΑΣ

Ο προϊστάμενος της κατάσχεσης στην σκηνή του εγκλήματος έχει τη συνολική ευθύνη να διασφαλίζει ότι τηρούνται οι ανωτέρω αρχές.

Ακολούθως, οι αρχές που έχουν κατασχέσει τα ψηφιακά πειστήρια, θα πρέπει να συντάσσουν έγγραφο, το οποίο να συνοδεύεται από την έκθεση κατάσχεσης και το διαβιβαστικό της αιτούσας υπηρεσίας προς τον Εισαγγελέα, το οποίο να περιέχει τα εξής:

- ✓ να περιέχει πληροφορίες ως προς αδίκημα που φέρεται να τελέστηκε με τα εν λόγω πειστήρια,
- ✓ να περιέχει πληροφορίες για τους κατόχους των πειστηρίων και τους δράστες,
- ✓ να διατυπώνει με σαφήνεια στοχευμένα ερωτήματα που χρήζουν εργαστηριακής απαντήσεως και μπορούν να βοηθήσουν στην ανακριτική διερεύνηση του εγκλήματος (όχι αόριστα και ασαφή ερωτήματα ούτε μόνο το γενικό ερώτημα «Οτιδήποτε προκύπτει από την επιστήμη σας.»). Σε περίπτωση που τα ερωτήματα δεν είναι σαφή και συγκεκριμένα, ο εξεταστής δεν θα είναι σε θέση να γνωρίζει ποια είναι εκείνα τα ευρήματα τα οποία θα βοηθούσαν στην εξιχνίαση του εγκλήματος, με αποτέλεσμα να αναλωθεί στην εξέταση του συνόλου των δεδομένων των υπολογιστικών συστημάτων, καταναλώνοντας έτσι χρόνο και πόρους που θα μπορούσε να διαθέσει στην εξέταση μιας άλλης υπόθεσης.

- Η περιγραφή του πειστηρίου θα πρέπει να είναι πλήρης, συμπεριλαμβάνοντας τη μάρκα, το μοντέλο, τον σειριακό αριθμό, τυχόν φθορές ή οποιοδήποτε άλλο στοιχείο το εξατομικεύει.

Αξίζει να σημειωθεί ότι το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών δεν παραλαμβάνει προς εξέταση πειστήρια για τα οποία δεν έχει ακολουθηθεί η ορθή διαδικασία κατάσχεσης, συσκευασίας, μεταφοράς και φύλαξης και εκείνα τα οποία δεν παρουσιάζουν εγκληματολογικό ενδιαφέρον ή δεν περιέχουν ψηφιακά δεδομένα (οθόνες, πληκτρολόγια, «ποντίκια» κ.λπ.).

Τελειώνοντας, θα αναφέραμε ότι η διαδικασία παραμένει ως έχει και στην περίπτωση που τα ηλεκτρονικά πειστήρια έχουν ληφθεί από άλλο κράτος μέλος της Ε.Ε.

5.3. Προστασία ανθρωπίνων δικαιωμάτων/θεμελιωδών ελευθεριών

Υπάρχουν αρμόδιες ανεξάρτητες αρχές όπως η ΑΔΑΕ, η ΕΕΤΤ και η ΑΠΔΠΧ, οι οποίες φροντίζουν για την ιδιωτικότητα της επικοινωνίας καθώς και για την προστασία των προσωπικών δεδομένων.

Η ΑΠΔΠΧ είναι αρμόδια για τη διερεύνηση ηλεκτρονικών εγκλημάτων που συνεπάγονται την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η Ελληνική Αρχή Διασφάλισης του Απορρήτου των Τηλεπικοινωνιών (ΑΔΑΕ) συγκροτήθηκε το 2003 σύμφωνα με το άρθρο 19 παράγραφος 2 του Συντάγματος της Ελλάδας, που προβλέπει τη συγκρότηση ανεξάρτητης αρχής που διασφαλίζει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση ή επικοινωνία με οποιονδήποτε άλλο τρόπο.

Περισσότερες λεπτομέρειες σχετικά με τις εξουσίες και τα καθήκοντα της ΑΔΑΕ παρέχονται στην απάντηση της ερώτησης 3.C.1 παρακάτω. Ο Ν. 3471/2006 με τον οποίο μεταφέρεται στην εθνική έννομη τάξη η οδηγία 2002/58/ΕΚ ορίζει την ΑΔΑΕ ως αρμόδια αρχή για την εφαρμογή του άρθρου 5 της οδηγίας («Απόρρητο των επικοινωνιών») καθώς και για την εφαρμογή των άρθρων της οδηγίας που αφορούν την ένδειξη της ταυτότητας καλούσας γραμμής για τον εντοπισμό κακόβουλων ή ενοχλητικών κλήσεων και για κλήσεις άμεσης επέμβασης. Με τον ίδιο νόμο ορίζεται η ΑΔΑΕ, από κοινού με την Εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ως εθνική αρχή αρμόδια για τη λήψη κοινοποιήσεων παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Επιπλέον, η ΑΔΑΕ έχει εκδώσει τον κανονισμό 165/2011 «για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 2715). Τόσο ο κανονισμός 165/2011 της ΑΔΑΕ όσο και το άρθρο 8 του Ν. 3674/2008 (ΦΕΚ Α' 136) περιλαμβάνουν διατάξεις για την άμεση κοινοποίηση των παραβιάσεων του απορρήτου των επικοινωνιών ή του κινδύνου σχετικών παραβιάσεων στην ΑΔΑΕ και στους αντίστοιχους συνδρομητές.

Η ΕΕΤΤ είναι η εθνική ρυθμιστική αρχή που εποπτεύει και ρυθμίζει την αγορά των τηλεπικοινωνιών καθώς και την ταχυδρομική αγορά. Η θεσμική της αποστολή περιλαμβάνει την προαγωγή της ανάπτυξης των δύο αυτών τομέων, τη διασφάλιση της εύρυθμης λειτουργίας της αντίστοιχης αγοράς σε περιβάλλον υγιούς ανταγωνισμού και τη μέριμνα για την προστασία των συμφερόντων των τελικών χρηστών. Η ΕΕΤΤ είναι ανεξάρτητος, αυτοχρηματοδοτούμενος φορέας λήψης αποφάσεων.

Το άρθρο 19 παράγραφος 1 του Συντάγματος της Ελλάδας ορίζει ότι «το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται για το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.» Ο Ν. 2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» (ΦΕΚ 121/20.07.1994) ορίζει τα συγκεκριμένα σοβαρά εγκλήματα για τη διακρίβωση των οποίων επιτρέπεται η άρση του απορρήτου και εκθέτει τις σχετικές νομικές απαιτήσεις.

Σύμφωνα με το άρθρο 12 του νόμου περί προστασίας δεδομένων (2472/1997), η υποχρέωση πληροφόρησης και το δικαίωμα πρόσβασης στα δεδομένα από το υποκείμενο των δεδομένων μπορούν να αρθούν εν όλω ή εν μέρει, εφ' όσον η επεξεργασία δεδομένων προσωπικού χαρακτήρα γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Ομοίως, σύμφωνα με το άρθρο 3 του ίδιου νόμου οι διατάξεις του νόμου περί προστασίας δεδομένων δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται από τις δικαστικές- εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων. Αυτή η περίπτωση μπορεί να συντρέχει και όταν η διακρίβωση αφορά κυβερνοέγκλημα που εμπίπτει επίσης στις ανωτέρω κατηγορίες εγκλημάτων.

5.4. Διεθνής δικαιοδοσία

5.4.1. Αρχές που διέπουν τη διερεύνηση των εγκλημάτων στον κυβερνοχώρο

Αναφορικά με την επέκταση της δικαιοδοσίας της ελληνικής έννομης τάξης για εγκλήματα που χρησιμοποιούν το Διαδίκτυο ως μέσο τέλεσης πρέπει να επισημανθεί ότι προστέθηκε παρ. 3 στο άρθρο 5 ΠΚ και για τα εγκλήματα που σχετίζονται με την γενετήσια εκμετάλλευση ή κακοποίηση ανηλίκων τροποποιήθηκε το άρθρο 8 περ. η΄ ΠΚ. Οι αλλαγές αυτές έγιναν με τα άρθρα 2 και 3 του Ν. 4267/2014 με τον οποίο ενσωματώθηκε στην εθνική μας έννομη τάξη η οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας.

Η προσθήκη της εν λόγω ρύθμισης αποτελεί υποχρέωση η οποία προκύπτει από διάφορα νομικά κείμενα της Ευρωπαϊκής Ένωσης, μεταξύ των οποίων η οδηγία που ενσωματώνεται με το παρόν σχέδιο νόμου, καθώς και η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών, για την οποία υφίσταται επίσης υποχρέωση συμμόρφωσης.

Η προσθήκη των εγκλημάτων στο άρθρο 8 περ. η΄ ΠΚ γίνεται προκειμένου οι ανωτέρω διατάξεις να εναρμονιστούν με τις παραγράφους 1, 2 και 4 του άρθρου 17 της οδηγίας 2011/93/ΕΕ. Τα ανωτέρω εγκλήματα προστίθενται διότι, στρεφόμενα κατά της γενετήσιας ελευθερίας του ανηλίκου, συνιστούν, για την ευρωπαϊκή έννομη τάξη, σοβαρές παραβιάσεις θεμελιωδών δικαιωμάτων και ειδικότερα των δικαιωμάτων των παιδιών (αιτιολογική σκέψη 1 της οδηγίας). Για τον λόγο αυτόν και προκειμένου να καταστεί δυνατή η δίωξή τους εντάσσονται στην αρχή της παγκόσμιας δικαιοσύνης (Βλ. Αιτιολογική Έκθεση Ν.4267/2014).

Σύμφωνα με την διάταξη του άρθρου 16 του ΠΚ, τόπος τέλεσης της πράξης θεωρείται ο τόπος όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη, καθώς και ο τόπος όπου επήλθε ή, σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει το αξιόποινο αποτέλεσμα. Στα εγκλήματα αποστάσεως, όπως είναι εκείνα που τελούνται μέσω του Διαδικτύου, τόπος τελέσεως του όλου εγκλήματος, είναι τόσο ο τόπος όπου εκδηλώθηκε η εγκληματική συμπεριφορά, ήτοι ο τόπος αποστολής του ηλεκτρονικού μηνύματος, όσο και ο τόπος παραλαβής του μηνύματος, έστω και αν αυτός βρίσκεται στην αλλοδαπή. Ήδη στο άρθρο 5 του ΠΚ «Εγκλήματα που τελέστηκαν στην ημεδαπή» με την διάταξη του άρθρου 2 του Ν. 4267/2014 εναρμονίσθηκε η εθνική νομοθεσία με την οδηγία 2011/93/ΕΕ και προστέθηκε παράγραφος 3 στην οποία αναφέρεται ότι: *«Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφός της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους».*

Σύμφωνα με το άρθρο 3 παράγραφος 3 του Ν. 2472/1997 η ΑΠΔΠΧ είναι αρμόδια για την επεξεργασία και άρα για τα εγκλήματα στον κυβερνοχώρο που διαπράττονται α) από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην ελληνική επικράτεια ή σε τόπο όπου βάσει του δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο, και β) από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια Κράτους-Μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού Χώρου, αλλά τρίτης χώρας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στην ελληνική επικράτεια, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από αυτήν. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωσή του προς την Αρχή εκπρόσωπο εγκατεστημένο στην ελληνική επικράτεια, ο οποίος υποκαθίσταται στα δικαιώματα και υποχρεώσεις του υπεύθυνου, χωρίς ο τελευταίος αυτός να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του.

5.4.2. Κανόνες που διέπουν τις συγκρούσεις διεθνούς δικαιοδοσίας και παραπομπή στην Eurojust

Η συνδρομή της EUROJUST είναι πολύ σημαντική, αφού με την διοργάνωση συντονιστικών ομάδων μεταξύ των δικαστικών ή/και αστυνομικών αρχών των εμπλεκομένων κρατών σε περιπτώσεις υποθέσεων που απασχολούν περισσότερα του ενός κράτη μέλη, επιτυγχάνεται η επίλυση του προβλήματος των τυχόν παράλληλων δικαιοδοσιών και η αποφυγή της άσκησης πολλαπλών ποινικών διώξεων κατά του ίδιου δράστη για τις ίδιες εγκληματικές πράξεις στον κυβερνοχώρο.

Η ΑΠΔΠΧ δεν ερευνά πράξεις που διαπράχθηκαν εκτός της εθνικής επικράτειας. Εάν κάποια τέτοια πράξη περιέλθει σε γνώση της ΑΠΔΠΧ στο πλαίσιο άλλης έρευνας, η ΑΠΔΠΧ προωθεί στην αρμόδια εθνική αρχή προστασίας δεδομένων (όταν η πράξη διαπράττεται σε κράτος μέλος της ΕΕ) όλα τα σχετικά στοιχεία και πειστήρια.

Ως προς τις διατάξεις της απόφασης-πλαισίου 2009/948/ΔΕΥ για την πρόληψη και τον διακανονισμό συγκρούσεων δικαιοδοσίας σε ποινικές υποθέσεις στο πλαίσιο της Ευρωπαϊκής Ένωσης, επισημαίνεται ότι δεν έχουν ενσωματωθεί στην εθνική έννομη τάξη, αλλά έχει συγκροτηθεί ειδική νομοπαρασκευαστική επιτροπή (υπ' αριθμ. 84295 από 4-11-2013 Απόφαση Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων) η οποία έχει ολοκληρώσει το έργο της και έχει καταθέσει στο αρμόδιο Υπουργείο τα σχετικά κείμενα.

5.4.3. Δικαιοδοσία για κυβερνοεγκλήματα που διαπράττονται στο «υπολογιστικό νέφος»

Η Ελλάδα δεν διαθέτει τέτοιου είδους εμπειρία. Ωστόσο σε περίπτωση που κάποιο τέτοιο ζήτημα ήθελε προκύψει στο πλαίσιο ποινικής διαδικασίας, θα μπορούσε να αξιοποιηθεί ο δίαυλος της EUROJUST και της Ευρωπόλ.

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

Το νομικό πλαίσιο στην Ελλάδα δεν έχει ενσωματώσει πλήρως τις περιπτώσεις των εγκλημάτων που διαπράττονται με την χρήση του Διαδικτύου στο σύνολο του. Γίνεται προσπάθεια εκσυγχρονισμού των νομικών διατάξεων αλλά ακόμα εκκρεμούν αρκετές αναγκαίες αλλαγές, ιδίως μέσω της κύρωσης της Σύμβασης της Βουδαπέστης.

Όσον αφορά το υπάρχον νομικό πλαίσιο, σχετικά με τη διερεύνηση των ηλεκτρονικών πειστηρίων, κατά κύριο λόγο είναι επαρκές.

5.5. Συμπεράσματα

- Η Ελλάδα έχει υπογράψει (23-1-2001) αλλά δεν έχει κυρώσει τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης). Το πρόσθετο στην προαναφερθείσα Σύμβαση πρωτόκολλο δεν έχει κυρωθεί επίσης.
- Η οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας ενσωματώθηκε στην εθνική νομοθεσία με τον Ν. 4267/2014.
- Όσον αφορά τις τεχνικές έρευνας, υπάρχουν διάφορα μέτρα για την κατάσχεση και την διατήρηση δεδομένων στο πλαίσιο της συλλογής πειστηρίων.
- Τα κυβερνοεγκλήματα που διαπράττονται μέσω του «υπολογιστικού νέφους» συγκέντρωσαν το ενδιαφέρον κατά την επίσκεψη αξιολόγησης ως τομέας που εγείρει ζητήματα για την έρευνα και τη δίωξη, ιδίως όσον αφορά τον προσδιορισμό της πραγματικής φυσικής θέσης των δεδομένων. Η μέθοδος του υπολογιστικού νέφους δημιουργεί πρόβλημα όχι μόνο ως προς το εθνικό δίκαιο αλλά και ως προς το διεθνές δίκαιο που βασίζεται στην αναγνώριση της ανεξαρτησίας των κρατών.

- Η Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της σεξουαλικής εκμετάλλευσης και της σεξουαλικής κακοποίησης έχει κυρωθεί. Το άρθρο 348 Α του Ποινικού Κώδικα τροποποιήθηκε και προβλέπεται πλέον η δυνατότητα απαγόρευσης, προσωρινής ή μόνιμης, σε πρόσωπα που έχουν καταδικαστεί για οποιαδήποτε αξιόποινη πράξη αυτού του είδους να ασκούν επαγγελματική δραστηριότητα που περιλαμβάνει άμεση και τακτική επαφή με ανηλίκους. Η κύρωση αυτή προβλέπεται επίσης από την οδηγία 2011/93/ΕΕ σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας. Η προσέλκυση παιδιών για γενετήσιους λόγους (grooming) είναι αξιόποινη πράξη στην Ελλάδα.
- Στον ελληνικό ποινικό κώδικα ο ορισμός του υλικού παιδικής πορνογραφίας είναι ευρύτερος από τον ορισμό που παρέχεται στην οδηγία. Σύμφωνα με τον εν λόγω ορισμό (άρθρο 348Α παρ. 3 ΠΚ) η αποτύπωση ή η αναπαράσταση μπορεί να περιλαμβάνει εκτός από τα γεννητικά όργανα και το σύνολο του σώματος ενός παιδιού. Θεωρείται επίσης αξιόποινη πράξη όταν παιδί γίνεται μάρτυρας σεξουαλικών πράξεων είτε έχει φθάσει σε ηλικία σεξουαλικής συναίνεσης είτε όχι.
- Υπάρχει επίσης ένα ειδικό μέτρο που προβλέπεται από το άρθρο 73 παρ. 3 ΠΚ σύμφωνα με το οποίο, σε περίπτωση δεύτερης καταδίκης, ο καταδικασμένος υποχρεούται να δηλώσει στην αστυνομική αρχή τη διεύθυνση της κατοικίας του και, επί μία τριετία, να γνωστοποιεί κάθε μεταβολή της στην ίδια αρχή.

6. ΕΠΙΧΕΙΡΗΣΙΑΚΕΣ ΠΤΥΧΕΣ

6.1. Κυβερνοεπιθέσεις

6.1.1. Φύση των κυβερνοεπιθέσεων

Σύμφωνα με το ΓΕΕΘΑ, τα περιστατικά αφορούν κυρίως σε σαρώσεις δικτύων, σε λήψη κακόβουλης ηλεκτρονικής αλληλογραφίας και σε έλεγχο δικτύων και υπολογιστών με την χρήση ιομορφικού λογισμικού.

Με βάση πληροφορίες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικού CERT, οι βασικές κατηγορίες κυβερνοεπιθέσεων που σημειώθηκαν στην Ελλάδα είναι οι εξής:

1) Defacements σε ιστοτόπους,
2) Επιθέσεις άρνησης υπηρεσιών (DOS)
3) Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφοριακά συστήματα
4) Απόκτηση πρόσβασης σε βάσεις δεδομένων - SQL Injections
5) Ανάρτηση κακόβουλων αρχείων που σκοπό έχουν είτε το phishing (username, passwords) είτε τη διανομή κακόβουλου λογισμικού που θα μετατρέψουν το χρήστη που το κατεβάζει σε μέλος ενός botnet.
6) Spear phishing mail attacks.
7) Ransomware

6.1.2. Μηχανισμός αντιμετώπισης κυβερνοεπιθέσεων

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων αποτελεί την αρμόδια κυβερνητική αρχή που συντονίζει την αντιμετώπιση των κυβερνοεπιθέσεων μεταξύ των ενδιαφερομένων, εφόσον αυτό αφορά τον δημόσιο τομέα ή κρίσιμες υποδομές. Ακόμη, σε περίπτωση μεγάλης έκτασης κυβερνοεπίθεσης, ενημερώνει τις υπηρεσίες ασφαλείας.

Η Ελλάδα έχει υπογράψει και ενσωματώσει στην ελληνική έννομη τάξη πληθώρα διμερών και πολυμερών συμβάσεων για τη δικαστική συνεργασία σε ποινικές υποθέσεις. Συμβάσεις οι οποίες αποτελούν επαρκή βάση για την ικανοποίηση αιτημάτων δικαστικής συνδρομής με αντικείμενο το έγκλημα στον κυβερνοχώρο. Επίσης, όταν δεν υπάρχει διμερής ή πολυμερής σύμβαση, εφαρμόζεται η αρχή της αμοιβαιότητας σύμφωνα με τα ειδικότερα οριζόμενα στο άρθρο 457 κ.επ. του Κώδικα Ποινικής Δικονομίας.

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

Το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών συνεισφέρει στη βάση δεδομένων της Ιντερπόλ «International Child Sexual Exploitation Database» που σχετίζεται με την ταυτοποίηση παιδιών θυμάτων σεξουαλικής κακοποίησης.

Οι αρμόδιες αρχές προβαίνουν σε κατάσχεση των σκληρών δίσκων με το παράνομο περιεχόμενο. Οι παράνομες εικόνες και τα παράνομα βίντεο ενσωματώνονται στις οικείες εθνικές και διεθνείς (ιδίως της Ευρωπόλ) βάσεις δεδομένων, ώστε να διωχθεί ενδεχομένη νέα προμήθεια ή διακίνηση.

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

Πραγματοποιούνται από στελέχη της ΔΙ.Δ.Η.Ε. συνεχείς εκδηλώσεις-ημερίδες σε όλη την ελληνική επικράτεια σχετικά με την αντιμετώπιση των ανωτέρω ζητημάτων. Επιπλέον, σε συνεργασία με το Υπουργείο Παιδείας και Θρησκευμάτων πραγματοποιούνται δύο (2) φορές κάθε εβδομάδα κατά τη διάρκεια του σχολικού έτους ενημερώσεις μέσω ειδικής σουίτας, σε όλα τα σχολεία της χώρας. Με αυτό τον τρόπο επιτυγχάνεται να γνωρίσουν όλοι οι μαθητές τις παγίδες του Διαδικτύου και τρόπους αντιμετώπισής τους.

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

Με το άρθρο 2 παρ. 5 του Ν. 3625/2007, «Κύρωση, εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του παιδιού, σχετικά με την εμπορία παιδιών, την παιδική πορνεία, την παιδική πορνογραφία και άλλες διατάξεις» προστέθηκε το άρθρο 323Β του Ποινικού Κώδικα με τίτλο «Διενέργεια ταξιδιών με σκοπό από τους μετέχοντες σε αυτά την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου (σεξουαλικός τουρισμός)». Σύμφωνα με το περιεχόμενο του άρθρου 323Β του Π.Κ., όποιος οργανώνει, χρηματοδοτεί, κατευθύνει, εποπτεύει, διαφημίζει ή μεσολαβεί με οποιονδήποτε τρόπο ή μέσο σε διενέργεια ταξιδιών με σκοπό από τους μετέχοντες σε αυτά την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου, τιμωρείται σε βαθμό κακουργήματος. Όποιος με τον παραπάνω σκοπό μετέχει σε ταξίδια του προηγούμενου εδαφίου τιμωρείται σε βαθμό πλημμελήματος, ανεξάρτητα από την ευθύνη του για την τέλεση άλλων αξιόποινων πράξεων.

Επιπροσθέτως, με το άρθρο 2 παρ 1 του Ν. 3625/2007, ως αντικαταστάθηκε με το άρθρο 3 του Ν. 4267/2014, προβλέφθηκε στο άρθρο 8 του ΠΚ «Εγκλήματα στην αλλοδαπή που τιμωρούνται πάντοτε κατά τους ελληνικούς νόμους» ότι οι ελληνικοί ποινικοί νόμοι εφαρμόζονται σε ημεδαπούς και αλλοδαπούς, ανεξάρτητα από τους νόμους του τόπου τέλεσης, για την πράξη, μεταξύ άλλων, «της διενέργειας ταξιδιών με σκοπό την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου».

Η προστασία των ανηλίκων βρίσκεται μεταξύ των βασικών προτεραιοτήτων του Αρχηγείου της Ελληνικής Αστυνομίας, όπως αυτές απορρέουν από το Πρόγραμμα Αντεγκληματικής Πολιτικής ετών 2015-2019 (Ερώτημα 1.1) και εντάσσεται στον κεντρικό πυρήνα του ενδιαφέροντός της. Στο πλαίσιο αυτό, έχουν τεθεί ειδικότεροι στόχοι, που αφορούν ιδίως την προστασία της μαθητικής κοινότητας και τη συνεργασία με αρμόδιους φορείς προστασίας ανηλίκων, μέσω της ανάπτυξης ειδικότερων δράσεων, στις οποίες περιλαμβάνονται, μεταξύ άλλων:

- ✓ Εξειδικευμένες δράσεις για τους ανηλίκους με στόχο κυρίως την προστασία τους από τα ναρκωτικά, την αποτροπή συμμετοχής τους σε εγκληματικές ομάδες και την προστασία τους από το ενδεχόμενο θυματοποίησής τους.
- ✓ Επιτήρηση χώρων που συχνάζουν ή παραμένουν ανήλικοι, όπως χώροι σχολείων, φροντιστήρια, χώροι άθλησης, πάρκα, παιδικές χαρές κ.λπ.
  Συνέχιση συνεργασίας με τα συναρμόδια Υπουργεία και τους λοιπούς φορείς (σχολικές κοινότητες, συλλόγους κ.λπ.) για τη λήψη των αναγκαίων μέτρων, με στόχο την ασφάλεια και προστασία των μαθητών και των σχολείων.
- ✓ Ανάπτυξη επαφών και συνεργασία με συναρμόδιους για θέματα ανηλίκων δημόσιους και ιδιωτικούς φορείς και οργανισμούς.
- ✓ Ενημέρωση του προσωπικού για ενεργοποίηση του συστήματος AMBER ALERT, που αφορά στην έγκαιρη προειδοποίηση στις περιπτώσεις εξαφάνισης ανηλίκων, με την ανάπτυξη της απαιτούμενης συνεργασίας.
- ✓ Ευαισθητοποίηση και εκπαίδευση του προσωπικού που χειρίζεται υποθέσεις ανηλίκων (αρωγή θυμάτων-μεταχείριση δραστών).

Επιπροσθέτως, για την προστασία των ανηλίκων έχουν συσταθεί και λειτουργούν εξειδικευμένες υπηρεσίες της Ελληνικής Αστυνομίας.

Σε κεντρικό επίπεδο, στη δομή της Διεύθυνσης Δημόσιας Ασφάλειας του Αρχηγείου της Ελληνικής Αστυνομίας λειτουργεί το Τμήμα Καταπολέμησης Ναρκωτικών & Παραβατικότητας Ανηλίκων, το οποίο αποτελεί επιτελική Υπηρεσία, στρατηγικού χαρακτήρα, στην οποία έχει ανατεθεί, η παρακολούθηση της παραβατικότητας και της θυματοποίησης ανηλίκων.

Σε περιφερειακό-επιχειρησιακό επίπεδο λειτουργούν:

- ✓ Η Υποδιεύθυνση Προστασίας Ανηλίκων της Διεύθυνσης Ασφάλειας Αττικής, η οποία διαρθρώνεται σε δύο (2) Τμήματα, ήτοι το Τμήμα Εποπτείας Ανηλίκων και το Τμήμα Ειδικής Μεταχείρισης Ανηλίκων.
- ✓ Το Τμήμα Ανηλίκων της Διεύθυνσης Ασφάλειας Θεσσαλονίκης.
- ✓ Τα Γραφεία Ανηλίκων των Υποδιευθύνσεων Ασφάλειας Ηρακλείου Κρήτης και Πατρών.

Επισημαίνεται δε ότι, μέχρι και σήμερα τόσο από τις ως άνω υπηρεσίες, όσο και από τις λοιπές αρμόδιες υπηρεσίες της Ελληνικής Αστυνομίας (Υποδιευθύνσεις και Τμήματα Ασφάλειας ανά την επικράτεια), δεν έχει διαπιστωθεί η παραβίαση του άρθρου του 323 Β ΠΚ. Σε ανάλογη δε περίπτωση, θα εφαρμοσθεί από αυτές η σχετική ως άνω νομοθεσία σε βάρος των παραβατών αυτής.

Έχουν αναπτυχθεί ειδικά μέτρα για την αντιμετώπιση των πορνογραφικών παραστάσεων με συμμετοχή παιδιών που πραγματοποιούνται μέσω του Διαδικτύου σε πραγματικό χρόνο μέσω χρήσης ειδικού λογισμικού (Child Protection System), το οποίο επιτρέπει τον έλεγχο της επιγραμμικής διακίνησης υλικού πορνογραφίας ανηλίκων μέσω δικτύων P2P.

Μια ΜΚΟ, το «Χαμόγελο του Παιδιού» διαχειρίζεται τη γραμμή βοήθειας SOS 1056 από το 1997. Το 2007 αναγνωρίστηκε από το Υπουργείο Υγείας και Κοινωνικής Αλληλεγγύης ως Εθνική Τηλεφωνική Γραμμή για τα Παιδιά. Η γραμμή SOS 156 στελεχώνεται από κοινωνικούς λειτουργούς και ψυχολόγους και λειτουργεί σε 24ωρη βάση, 7 ημέρες την εβδομάδα. Η κλήση είναι δωρεάν και όλες οι τηλεφωνικές συνομιλίες είναι απόρρητες και ΔΕΝ καταγράφονται. Μέσω της γραμμής αυτής λαμβάνονται επίσημες καταγγελίες για παιδιά-θύματα εγκλημάτων στον κυβερνοχώρο οι οποίες προωθούνται στις αρμόδιες αρχές (εισαγγελικές και αστυνομικές) προς διερεύνηση.

Η γραμμή SOS 156 διασυνδέθηκε με τον Ευρωπαϊκό Αριθμό Έκτακτης Ανάγκης 112 της Γενικής Γραμματείας Πολιτικής Προστασίας και αναγνωρίστηκε ως Γραμμή Έκτακτης Ανάγκης. Επίσης, το «Χαμόγελο του Παιδιού» έχει συνάψει Μνημόνιο Συνεργασίας με το Υπουργείο Προστασίας του Πολίτη βάσει του οποίου το «Χαμόγελο του Παιδιού» δέχεται επίσημες καταγγελίες για παιδιά θύματα εγκλημάτων στον κυβερνοχώρο. Κατά τη διάρκεια του 2014 η εθνική γραμμή SOS 1056 δέχθηκε 283.369 κλήσεις.

Το «Χαμόγελο του Παιδιού» διαχειρίζεται την ευρωπαϊκή γραμμή για τα εξαφανισμένα παιδιά 116000 από το 2008. Στελεχώνεται από κοινωνικούς λειτουργούς και ψυχολόγους, λειτουργεί σε 24ωρη βάση, 7 ημέρες την εβδομάδα και οι κλήσεις είναι ανώνυμες και δωρεάν. Η γραμμή 116000 διασυνδέθηκε με τον Ευρωπαϊκό Αριθμό Έκτακτης Ανάγκης 112 της Γενικής Γραμματείας Πολιτικής Προστασίας και αναγνωρίστηκε ως Γραμμή Έκτακτης Ανάγκης. Μέσω αυτής της γραμμής, η οποία λειτουργεί σε 29 χώρες (27 κράτη μέλη της ΕΕ, Αλβανία και Σερβία), το «Χαμόγελο του Παιδιού» δέχεται κλήσεις για εξαφανισμένα και υπό εκμετάλλευση παιδιά. Το 2014 ο αριθμός 116 000 δέχθηκε 7.151 κλήσεις.

• **ανάπτυξη ενημερωτικών εργαλείων για την ασφαλή χρήση του Διαδικτύου από τα παιδιά·**

Ψηφιακές υπηρεσίες

Η Εθνική Τηλεφωνική Γραμμή για τα Παιδιά SOS 1056 προσφέρει δωρεάν ψηφιακή υπηρεσία έκτακτης ανάγκης και συμβουλευτικής, διαθέσιμη 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, για παιδιά και εφήβους (έως 18 ετών) στην Ελλάδα που χρησιμοποιούν μέσα κοινωνικής δικτύωσης και ηλεκτρονικό ταχυδρομείο, καθώς και για ενήλικες που ανησυχούν για κάποιο παιδί.
Η υπηρεσία αυτή είναι αυστηρά εμπιστευτική και προσφέρεται ατομικά. Η ψηφιακή υπηρεσία της γραμμής SOS 1056 παρέχει:

- Ψυχολογική υποστήριξη για παιδιά και εφήβους, καθώς και συμβουλευτική για γονείς και εκπαιδευτικούς, που χρησιμοποιούν μέσα κοινωνικής δικτύωσης (Facebook, Twitter, Instagram, Youtube), ηλεκτρονικό ταχυδρομείο και instant chat (υπό εφαρμογή)
- Παραπομπή στην τηλεφωνική γραμμή βοήθειας για την λήψη ανώνυμων και επώνυμων καταγγελιών σχετικά με παιδιά θύματα κακοποίησης ή παραμέλησης
- Παραπομπή στην τηλεφωνική γραμμή βοήθειας σε περίπτωση αιτημάτων από αρχές, φορείς, υπηρεσίες ή το ευρύ κοινό
- Διάδοση πληροφοριών σχετικά με το έγκλημα στον κυβερνοχώρο με χρήση μέσων κοινωνικής δικτύωσης και ηλεκτρονικής αλληλογραφίας και μέσω του ιστοτόπου (πρωτοβάθμια πρόληψη-ευαισθητοποίηση)
- Παρακολούθηση και αξιολόγηση πληροφοριών και παραπομπή στις αρχές (δευτεροβάθμια πρόληψη)

- Σε περιπτώσεις εκφοβισμού στον κυβερνοχώρο, το «Χαμόγελο του Παιδιού», κατόπιν αιτήματος των αρχών, παρέχει ψυχολογική υποστήριξη στο παιδί και στην οικογένειά του
- Ευαισθητοποίηση για θέματα που σχετίζονται με τα δικαιώματα και την προστασία των παιδιών με τη χρήση μέσων κοινωνικής δικτύωσης και μέσω του ιστοτόπου
- Προγράμματα επιμόρφωσης με χρήση podcast (Webinars και Video Web Casts) για γονείς, επιστήμονες και το ευρύ κοινό, σχετικά με την προστασία των παιδιών και τις ανάγκες τους (πρωτοβάθμια πρόληψη)

• **ανάπτυξη ενημερωτικών εργαλείων για την επιβλαβή/παράνομη συμπεριφορά στο Διαδίκτυο;**

Το «Χαμόγελο του Παιδιού» έχει δρομολογήσει τη χρήση νέων ψηφιακών εργαλείων, σε συνεργασία με διεθνείς αρχές και εταίρους, για τους σκοπούς της καταπολέμησης της παιδικής πορνογραφίας και άλλων εγκλημάτων στον κυβερνοχώρο, θέτοντας τα εν λόγω εργαλεία στη διάθεση των αρχών επιβολής του νόμου.

Στα πλαίσια της Ελληνικής Αστυνομίας, έχει αναπτυχθεί ειδικό 24ωρο τηλεφωνικό κέντρο καταγγελιών (11188) εντός της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, όπου εξειδικευμένα στελέχη αντιμετωπίζουν όλα τα περιστατικά, συμπεριλαμβανομένων εκείνων που απαιτούν άμεσο χειρισμό (π.χ. εκδήλωση πρόθεσης αυτοκτονίας). Επιπρόσθετα έχει δημιουργηθεί από προσωπικό της ως άνω υπηρεσίας ένας ασφαλής ιστότοπος www.cyberkid.gr όπου τόσο τα ανήλικα άτομα όσο και οι γονείς μπορούν, μέσω διαδραστικών δραστηριοτήτων και συνεχούς ενημέρωσης, να πληροφορηθούν για τους τρόπους ασφαλέστερης πλοήγησης. Επιπρόσθετα και για κινητά τηλέφωνα και tablets έχει δημιουργηθεί δωρεάν εφαρμογή με χρήσιμες συμβουλές σχετικά με την πλοήγηση στο Διαδίκτυο και με το πάτημα ενός κουμπιού πραγματοποιείται αυτόματα τηλεφωνική κλήση στο τηλεφωνικό κέντρο της υπηρεσίας.

Πραγματοποιούνται από στελέχη της ΔΙ.Δ.Η.Ε. συνεχείς εκδηλώσεις-ημερίδες σε όλη την ελληνική επικράτεια σχετικά με την αντιμετώπιση των ανωτέρω ζητημάτων. Επιπλέον, σε συνεργασία με το Υπουργείο Παιδείας και Θρησκευμάτων πραγματοποιούνται δύο (2) φορές κάθε εβδομάδα κατά τη διάρκεια του σχολικού έτους ενημερώσεις μέσω ειδικής σουίτας, σε όλα τα σχολεία της χώρας. Με αυτό τον τρόπο επιτυγχάνεται όλοι οι μαθητές να γνωρίσουν τις παγίδες του Διαδικτύου και τρόπους αντιμετώπισής τους.

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

Εφαρμόζεται φιλτράρισμα, μπλοκάρισμα πρόσβασης και κατάργηση ιστοτόπου.

Οι εθνικές αρχές χρησιμοποιούν ειδικό λογισμικό (Child Protection System) το οποίο επιτρέπει τον έλεγχο της επιγραμμικής διακίνησης υλικού πορνογραφίας ανηλίκων μέσω δικτύων P2P.

Κατόπιν σχετικού αιτήματος στις εισαγγελικές αρχές και έκδοση διάταξης, υποχρεώνονται είτε η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είτε οι πάροχοι υπηρεσιών πρόσβασης στο Διαδίκτυο να κατεβάσουν την ιστοσελίδα που περιέχει υλικό πορνογραφίας ανηλίκων.

Η διαδικασία έχει ως εξής:

(α) Αν η ιστοσελίδα φιλοξενείται εντός της επικράτειας και ο πάροχος υπηρεσιών φιλοξενίας (HISP) είναι γνωστός, η αρμόδια αρχή τον διατάσσει να απενεργοποιήσει ή να κατεβάσει την ιστοσελίδα.

(β) Αν ο HISP δεν είναι γνωστός και το όνομα τομέα της ιστοσελίδας λήγει σε .gr, η αρμόδια αρχή διατάσσει την ΕΕΤΤ να απενεργοποιήσει προσωρινά το όνομα τομέα για διάστημα δύο μηνών. Εντός του διαστήματος αυτού, ο ιδιοκτήτης του ονόματος τομέα μπορεί να προσφύγει στην εισαγγελική αρχή. Εντός χρονικού διαστήματος δύο μηνών ο Εισαγγελέας εκδίδει οριστική απόφαση είτε για την κατάργηση είτε για την εκ νέου ενεργοποίηση του ονόματος τομέα. Απουσία αντίδρασης από την πλευρά του ιδιοκτήτη, το όνομα τομέα καταργείται οριστικά.

Στις περιπτώσεις που ο διακομιστής βρίσκεται στο εξωτερικό, υπάρχει στενή συνεργασία μέσω της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας (Δ.Δ.Α.Σ.) με τις μονάδες Ευρωπόλ και Ιντερπόλ για την ενημέρωσή τους και τις δικές τους περαιτέρω ενέργειες, λόγω καθ' ύλη και κατά τόπο αρμοδιότητας.

(γ) Αν μια ιστοσελίδα δεν φιλοξενείται στην επικράτεια της χώρας και το όνομα τομέα της δεν λήγει σε .gr, τότε η αρμόδια αρχή αποφασίζει το μπλοκάρισμα της πρόσβασης στην ιστοσελίδα. Η σχετική απόφαση κοινοποιείται στην ΕΕΤΤ. Η ΕΕΤΤ ενημερώνει τους παρόχους υπηρεσιών Διαδικτύου (ISP) και τους καλεί να μπλοκάρουν αμέσως την πρόσβαση στην ιστοσελίδα και να ενημερώσουν σχετικά τους πελάτες τους. Η σχετική απόφαση κοινοποιείται στον ιδιοκτήτη της ιστοσελίδας ο οποίος μπορεί να προσφύγει στην εισαγγελική αρχή. Εντός χρονικού διαστήματος δύο μηνών ο Εισαγγελέας εκδίδει οριστική απόφαση σχετικά με το μπλοκάρισμα της πρόσβασης στην ιστοσελίδα.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας χρησιμοποιεί ως διαύλους επικοινωνίας με άλλες χώρες τα τμήματα INTERPOL, Ευρωπόλ και SIRENE της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας.

6.3. Διαδικτυακή απάτη με κάρτες

6.3.1. Υποβολή αναφορών μέσω Διαδικτύου

Τόσο πολίτες (μηνυτής ή πληρεξούσιος δικηγόρος) όσο και οι ιδιωτικές εταιρείες έχουν τη δυνατότητα υποβολής έκθεσης ένορκης εξέτασης-καταγγελίας που αφορούν απάτη μέσω Διαδικτύου, στις αρχές επιβολής του νόμου και στις Εισαγγελικές Αρχές. Η υποβολή μηνυτήριας αναφοράς στις αρχές επιβολής του νόμου μπορεί να πραγματοποιηθεί είτε στο κατά τόπους αρμόδιο αστυνομικό τμήμα της περιοχής που διαμένει ο πολίτης ή εδρεύει η εταιρεία, είτε απ' ευθείας στη ΔΙ.Δ.Η.Ε., με φυσική παρουσία.

Η υποβολή μηνυτήριας αναφοράς, εκτός από τις αρχές επιβολής του νόμου, μπορεί να υποβληθεί σύμφωνα με τη παράγραφο 2 του άρθρου 42 του Κώδικα Ποινικής Δικονομίας απ' ευθείας στον εισαγγελέα πλημμελειοδικών.

Επιπρόσθετα, οι πολίτες και οι ιδιωτικές εταιρείες έχουν τη δυνατότητα της καταγγελίας αδικημάτων που σχετίζονται με διαδικτυακή απάτη με χρήση κάρτας πληρωμής στη ΔΙ.Δ.Η.Ε., μέσω μηνύματος ηλεκτρονικού ταχυδρομείου καθώς πρόκειται για αδίκημα που διώκεται αυτεπαγγέλτως.

Υπάρχει συνεργασία και αλληλοενημέρωση της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων με τον τραπεζικό τομέα για περιστατικά κυβερνοεπιθέσεων καθώς και εργαλεία-τεχνικές που χρησιμοποιούνται από τους επιτιθέμενους.

6.3.2. Ρόλος του ιδιωτικού τομέα

Ο ιδιωτικός τομέας μπορεί να γνωστοποιεί, χωρίς όμως να είναι υποχρεωμένος, περιστατικά ηλεκτρονικών επιθέσεων στον κυβερνοχώρο στην Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και να λαμβάνει συμβουλές αντιμετώπισης αλλά και επιχειρησιακή-τεχνική βοήθεια από αυτήν για την αντιμετώπιση των περιστατικών εφόσον ζητηθεί.

Τα πιστωτικά ιδρύματα που λειτουργούν στην Ελλάδα υποχρεούνται να αναφέρουν αμελλητί τα επεισόδια κυβερνοεπιθέσεων με στόχο τα πιστωτικά ιδρύματα και/ή τους πελάτες τους. Η αναφορά απευθύνεται στην Τράπεζα της Ελλάδος καθώς και στον Ενιαίο Εποπτικό Μηχανισμό (SSM) της ΕΚΤ. Λόγω στενής συνεργασίας η αναφορά απευθύνεται επίσης στο Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, μολονότι τα πιστωτικά ιδρύματα δεν υπέχουν σχετική υποχρέωση.

Η ΕΕΤ έχει καταρτίσει και διατηρεί δύο καταλόγους επαφών επαγρύπνησης με τα στοιχεία επαφής των αρμόδιων εκπροσώπων των πιστωτικών ιδρυμάτων, του Τμήματος Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και της Τράπεζας της Ελλάδος. Ο πρώτος κατάλογος επαφών επαγρύπνησης αφορά κάθε είδους συμβάν σχετικό με απάτη με κάρτες πληρωμών (λ.χ. skimming/«ξάφρισμα» ΑΤΜ και σημείων πώλησης, απάτη στο ηλεκτρονικό εμπόριο κ.λπ.), ενώ ο δεύτερος κατάλογος επαφών επαγρύπνησης αφορά κάθε είδους απάτη μέσω Διαδικτύου (λ.χ. εξελιγμένες τεχνικές phishing, κλοπή ταυτότητας, γνωστοποίηση των μυστικών διαπιστευτηρίων των πελατών σε τρίτους και επιθέσεις σε «man-in-the-middle»/φυλλομετρητή με στόχο την υποκλοπή/τροποποίηση/εκτροπή δεδομένων των πελατών, κακόβουλα λογισμικά, κοινωνική μηχανική, κατανεμημένη άρνηση υπηρεσίας-DDoS και παραβίαση της περιμετρικής ζώνης κ.λπ.).

Ο Ν. 3471/2006 (ΦΕΚ Α' 133), με τον οποίο μεταφέρεται στην εθνική έννομη τάξη η οδηγία 2002/58/ΕΚ, ορίζει την ΑΔΑΕ, από κοινού με την εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ως αρμόδια εθνική αρχή για την παραλαβή κοινοποιήσεων σχετικά με παραβιάσεις δεδομένων. Επιπλέον, η ΑΔΑΕ έχει εκδώσει τον κανονισμό 165/2011 «για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 2715). Τόσο ο κανονισμός 165/2011 της ΑΔΑΕ όσο και το άρθρο 8 του Ν. 3674/2008 (ΦΕΚ Α' 136) περιλαμβάνουν διατάξεις για την άμεση κοινοποίηση των παραβιάσεων του απορρήτου των επικοινωνιών ή του κινδύνου σχετικών παραβιάσεων στην ΑΔΑΕ και στους αντίστοιχους συνδρομητές.

6.4.Άλλα φαινόμενα της εγκληματικότητας στον κυβερνοχώρο

Σύμφωνα με την υπ' αριθ. 15/2011 (ΦΕΚ Β'419/16.03.2011) απόφαση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), τα Πιστωτικά Ιδρύματα μεριμνούν για την άμεση προστασία των χρηστών κατά τη χρήση των Αυτόματων Ταμειολογιστικών Μηχανών (ΑΤΜ), όπως επίσης και για τη σωστή και έγκυρη ενημέρωση αυτών αναφορικά με τους κινδύνους που είναι δυνατόν να απειλήσουν το απόρρητο της επικοινωνίας κατά τη χρήση των ΑΤΜ. Επιπρόσθετα, τα πιστωτικά ιδρύματα μεριμνούν για τη φυσική προστασία των ΑΤΜ καθώς και για το υλικό που χρησιμοποιείται για την παροχή των υπηρεσιών από αυτά.

Από τα παραπάνω προκύπτει ότι η βασική αρμοδιότητα για τον περιορισμό πρόσβασης των ομάδων του οργανωμένου εγκλήματος σε οικονομικά δεδομένα και διαπιστεύσεις ανήκει στα ίδια τα πιστωτικά ιδρύματα διά της υποχρέωσης διασφάλισης του πληροφοριακού τους συστήματος.

Όσον αφορά στον περιορισμό πρόσβασης των ομάδων οργανωμένου εγκλήματος σε συσκευές skimming και το σχετικό λογισμικό και τεχνογνωσία, τονίζεται ότι στις περισσότερες περιπτώσεις το λογισμικό δεν προερχόταν από ημεδαπούς προμηθευτές ενώ οι συλληφθέντες εμπλεκόμενοι σε περιστατικά skimming ήταν σχεδόν στο σύνολό τους υπήκοοι της αλλοδαπής.

Τα πιστωτικά ιδρύματα διαθέτουν οργανογράμματα για τη διακυβέρνηση της ασφάλειας των πληροφοριών (Διευθυντής Ασφάλειας Πληροφοριών - CISO, Μονάδες Ασφάλειας Πληροφοριών), καθώς και ισχυρά πλαίσια για την ασφάλεια των πληροφοριών τα οποία περιλαμβάνουν πολιτικές, διαδικασίες και πρότυπα ασφάλειας.

Όσον αφορά την υποδομή ασφάλειας, διαθέτουν εξειδικευμένα μέτρα ασφάλειας, τόσο περιμετρικά όσο και εσωτερικά, βάσει πολλαπλών επιπέδων άμυνας και σε διακριτές ζώνες. Ανάλογα με την εσωτερική πολιτική κάθε τράπεζας, τα μέτρα ασφαλείας περιλαμβάνουν, μεταξύ άλλων, τα εξής:

Firewalls δικτύου,
Firewalls για εφαρμογές web και βάσεις δεδομένων,
Συστήματα αποτροπής εισβολών (IPS),
Συστήματα ανίχνευσης εισβολών (IDS),

- Συστήματα ασφαλείας για DDos (κατανεμημένες επιθέσεις άρνησης υπηρεσιών),
- Πρόληψη διαρροής δεδομένων,
- Προστασία από κακόβουλο λογισμικό (malware),
- Φιλτράρισμα περιεχομένου,
- Ισχυρούς μηχανισμούς ελέγχου της πρόσβασης,
- Συστήματα SIEM (Security Information and Event Management) για έγκαιρο εντοπισμό (24X7X365) και πρόληψη δυνητικών εισβολών.

Επιπλέον, τα πιστωτικά ιδρύματα διενεργούν ελέγχους ασφαλείας (δοκιμές διείσδυσης, αξιολογήσεις τρωτότητας) περιοδικά, τόσο εσωτερικά όσο και σε συνεργασία με εξωτερικούς εταίρους, σύμφωνα με την πράξη υπ' αριθμ. 2577/2006 του Διοικητή της Τράπεζας της Ελλάδας. Πιστοποιούν επίσης ότι το λειτουργικό σύστημα των εφαρμογών τους είναι ανά πάσα στιγμή πλήρως επικαιροποιημένο, με όλες τις τελευταίες ενημερώσεις κώδικα (patches).

Τα ATM είναι προστατευμένα (σε επίπεδο συστήματος και δικτύου), εξοπλισμένα με συσκευές κατά του «ξαφρίσματος» και της απάτης και με προγράμματα προστασίας από κακόβουλο λογισμικό.

Υφίσταται στενή συνεργασία μεταξύ των CISO των ελληνικών τραπεζών, της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και της Τράπεζας της Ελλάδας μέσω της διατραπεζικής επιτροπής της Ελληνικής Ένωσης Τραπεζών (ΕΕΤ) και/ή μεμονωμένα για την ανταλλαγή πληροφοριών και την υιοθέτηση κοινών μέτρων και πρακτικών ασφαλείας. Επιπλέον, βρίσκονται σε διαρκή επικοινωνία με εκπροσώπους των κατασκευαστών ATM (π.χ. NCR, Wincor Nixdorf, Diebold, κ.λπ.) στην Ελλάδα για ενημέρωση και ανταλλαγή απόψεων.

Τέλος, αξίζει να σημειωθεί ότι τα πιστωτικά ιδρύματα έχουν πιστοποιηθεί ή διανύουν την τελική φάση της πιστοποίησής τους κατά το πρότυπο PCI DSS το οποίο παρέχει τη βάση για την ανάπτυξη διαδικασιών ασφαλείας για τη χρήση καρτών πληρωμής, συμπεριλαμβανομένης της πρόληψης, του εντοπισμού και της κατάλληλης αντίδρασης σε παραβιάσεις της ασφάλειας.

6.5.Συμπεράσματα

- Ο Ποινικός Κώδικας ποινικοποιεί τον σεξουαλικό τουρισμό («Διενέργεια ταξιδιών με σκοπό από τους μετέχοντες σε αυτά την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου») και άρα υπερβαίνει τις ελάχιστες απαιτήσεις που θέτει η οδηγία για την καταπολέμηση της παιδικής πορνογραφίας.
- Μία άλλη ορθή πρακτική είναι η δυνατότητα που παρέχεται από την εθνική νομοθεσία για φιλτράρισμα, μπλοκάρισμα της πρόσβασης και αφαίρεση των ιστοσελίδων που σχετίζονται με την παιδική πορνογραφία.
- Πρέπει να τονιστεί ότι το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών έχει πρόσβαση στη διεθνή βάση δεδομένων της Ιντερπόλ για την σεξουαλική εκμετάλλευση παιδιών (International Child Sexual Exploitation Database).
- Η Ομάδα Αξιολόγησης κρίνει ότι συνιστά ορθή πρακτική το γεγονός ότι τα πιστωτικά ιδρύματα που λειτουργούν στην Ελλάδα υποχρεούνται να αναφέρουν αμελλητί τα επεισόδια κυβερνοεπιθέσεων με στόχο τα πιστωτικά ιδρύματα και/ή τους πελάτες τους. Η σχετική αναφορά πρέπει να αποστέλλεται στην Τράπεζα της Ελλάδος. Λόγω στενής συνεργασίας η αναφορά απευθύνεται επίσης στο Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, μολονότι τα πιστωτικά ιδρύματα δεν υπέχουν σχετική υποχρέωση.
- Ένα άλλο παράδειγμα ορθής πρακτικής είναι η σύσταση στους κόλπους της ΕΕΤ μιας διατραπεζικής επιτροπής μέλη της οποίας είναι εκπρόσωποι των τραπεζών, της Τράπεζας της Ελλάδος και της Ελληνικής Αστυνομίας. Στο πλαίσιο της επιτροπής εξετάζονται οι νέες τάσεις στις απάτες, συμβάντα και μέτρα/τεχνολογίες αντιμετώπισης προκειμένου να ληφθούν κατάλληλα μέτρα. Για γρήγορη ανταπόκριση, η Ελληνική Ένωση Τραπεζών διατηρεί καταλόγους επαφών επαγρύπνησης όσον αφορά το έγκλημα στον κυβερνοχώρο («ξάφρισμα» («skimming»), απάτη στο ηλεκτρονικό εμπόριο, κυβερνοεπιθέσεις, απάτη μέσω του Διαδικτύου κ.λπ.).

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

Δεν προβλέπονται από την εθνική νομοθεσία ειδικές προϋποθέσεις ή ειδικότερες διατάξεις για την συνεργασία των εθνικών αρχών με την Eurojust, Ευρωπόλ EC3 και τον ENISA στα εγκλήματα στον κυβερνοχώρο, καθώς ισχύει το κοινό πλαίσιο που ισχύει και για τα λοιπά εγκλήματα.

Ο ελληνικός τραπεζικός κλάδος συνεργάζεται με το Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και συμμετέχει στο πρόγραμμα της Ευρωπόλ/EC3 με θέμα «Intelligence Requirement on Banking Malware».

Τον Σεπτέμβριο του 2014 η Ομοσπονδία Ευρωπαϊκών Τραπεζών (EBF) και το Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο (EC3) της Ευρωπόλ υπέγραψαν μνημόνιο συναντίληψης με το οποίο τίθενται οι βάσεις για την ενίσχυση της συνεργασίας μεταξύ των αρχών επιβολής του νόμου και του χρηματοοικονομικού κλάδου στην ΕΕ.

Το μνημόνιο συναντίληψης επιτρέπει την ανταλλαγή εμπειρογνωμοσύνης, στατιστικών στοιχείων και άλλων στρατηγικών πληροφοριών μεταξύ των δύο μερών. Θα διευκολύνει την ανταλλαγή δεδομένων σχετικά με απειλές επιτρέποντας στα χρηματοπιστωτικά ιδρύματα να αυτοπροστατεύονται πιο αποτελεσματικά, ενώ παράλληλα η άμεση αναφορά νέων μορφών κακόβουλου λογισμικού και απάτης στις πληρωμές θα επιτρέπουν στις αρχές επιβολής του νόμου να ερευνούν και να συλλαμβάνουν τους δράστες. Η ΕΕΤ ως μέλος της EBF συμμετέχει ενεργά σε αυτή την πρωτοβουλία των EBF/Ευρωπόλ-EC3.

Όσον αφορά τη συνεργασία με τον ENISA, η ΕΕΤ συμμετέχει επίσης ενεργά στην ομάδα εμπειρογνωμόνων του ENISA για τις ΤΠΕ στον χρηματοοικονομικό κλάδο (EG-FI).

Η ΕΕΤ συμμετέχει ακόμη στις ομάδες EBF/Cyber Security Group και EPC/Payment Security Support Group και συνεπικουρεί επίσης το Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας το οποίο συντονίζει το ευρωπαϊκό πρόγραμμα EMPACT με αντικείμενο την ενημέρωση των πελατών σχετικά με θέματα ασφάλειας.

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

Η Ελλάδα διαθέτει εμπειρία συνεργασίας με τους ανωτέρω οργανισμούς. Ειδικότερα στην Eurojust έχουν εισαχθεί δύο υποθέσεις το 2014 (μία για παιδική πορνογραφία και μία για απάτη μέσω Διαδικτύου) και τρεις υποθέσεις το 2015 (συκοφαντικές δυσφημήσεις μέσω Διαδικτύου).

Η ΔΙ.Δ.Η.Ε. συνεργάζεται σε καθημερινό επίπεδο μέσω της Ευρωπόλ με αρμόδιες αλλοδαπές αρχές, καθώς και με την Eurojust μέσω αιτήματος δικαστικής συνδρομής, ώστε να διευκολύνεται η εξιχνίαση υποθέσεων και η σύλληψη δραστών καθώς και η αποκόμιση πληροφορίας (intelligence).

Ειδικότερα, η ΔΙ.Δ.Η.Ε. έχει χειριστεί υπόθεση σχετική με απάτες και παράνομο στοιχηματισμό μέσω Διαδικτύου, στην οποία ήταν απαραίτητη η συνεργασία μέσω της Ευρωπόλ με χώρες της αλλοδαπής, για την ανταλλαγή πληροφορίας και την παροχή στοιχείων.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνεργάζεται απευθείας με τον ENISA και κυρίως όσον αφορά τα εξής:

1) Έχει συμμετάσχει στο σχεδιασμό και τη διεξαγωγή και των τριών πανευρωπαϊκών κυβερνοασκήσεων που διοργάνωσε ο ENISA. Επίσης, υπάρχει συνεργασία με τον ENISA προκειμένου να διαμορφωθεί Εθνική Στρατηγική Κυβερνοασφάλειας. Τέλος, συμμετέχει σε τακτική βάση σε workshops και προγράμματα εκπαίδευσης του ENISA.

2) Επίσης, η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συμβάλλει στις συντονισμένες προσπάθειες που γίνονται στην Ευρωπόλ/EC3 με στόχο την αντιμετώπιση κυβερνοαπειλών, όπως π.χ. Ramnit botnet takedown.

Η συμβολή των Ευρωπόλ/EC3, Eurojust και ENISA στη διεθνή συνεργασία είναι πολύτιμη, καθώς υποβοηθούν την επιτάχυνση των διαδικασιών και την εξέταση των αιτημάτων. Η εμπειρία συνεργασίας της Eurojust με το EC3 είναι θετική, καθώς το EC3, ως ικανό να λαμβάνει γνώση των νεότερων modus operandi στα εγκλήματα στον κυβερνοχώρο, μπορεί να προβαίνει και σε επιτυχή στρατηγική ανάλυση.
Η συνεργασία με την Ευρωπόλ/EC3 έχει ως στόχο τη πρόληψη και καταπολέμηση σοβαρών διεθνών εγκληματικών δραστηριοτήτων μέσω Διαδικτύου. Ο ENISA συμβάλλει στη διαμόρφωση πολιτικών και δημοσίευση βέλτιστων πρακτικών για την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Η Ελλάδα συμμετέχει στην στρατηγική ομάδα των επικεφαλής των εθνικών μονάδων εγκληματικότητας υψηλής τεχνολογίας στην Ευρωπόλ, εκπροσωπούμενη από τον επικεφαλής της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος.

7.1.3. Επιχειρησιακή συμμετοχή σε κοινές ομάδες ερευνών και κυβερνοπεριπόλους

Η Ελλάδα δεν έχει συμμετάσχει μέχρι στιγμής σε κοινές ομάδες ερευνών και σε κυβερνοπεριπόλους και δεν έχουν προς το παρόν χρησιμοποιηθεί σχετικά κονδύλια της ΕΕ.

Επισημαίνεται όμως ότι εξειδικευμένο προσωπικό της διενεργεί καθημερινούς διαδικτυακούς ελέγχους, με απώτερο στόχο την πρόληψη και καταστολή των διαδικτυακών εγκλημάτων που διαπράττονται στον παγκόσμιο ιστό.

7.2. Συνεργασία μεταξύ των ελληνικών αρχών και της Interpol

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διασυνδέθηκε λίαν προσφάτως στην εν λόγω βάση δεδομένων, και η ποιότητα της σύνδεσης κρίθηκε ικανοποιητική. Η χρήση της εν λόγω βάσης αναμένεται να επεκτείνει την επιχειρησιακή δυνατότητα της εν λόγω υπηρεσίας στην καταπολέμηση του φαινομένου της παιδικής πορνογραφίας, με παράλληλη αναβάθμιση του ρόλου της Ελλάδας στην παγκόσμια συμμαχία για την αντιμετώπιση της παιδικής σεξουαλικής εκμετάλλευσης.

Επισημαίνεται δε ότι, κατά το χρονικό διάστημα από 27 έως και 29 Μαΐου 2015, προσωπικό της εν λόγω υπηρεσίας και ειδικότερα του Τμήματος Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης εκπαιδεύτηκε στις εγκαταστάσεις της από δύο εκπαιδευτές της Interpol.

Επίσης, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών έχει πρόσβαση στη διεθνή βάση δεδομένων της Interpol για τη σεξουαλική εκμετάλλευση παιδιών (International Child Sexual Exploitation Database).

Η Ελλάδα είναι από τα ιδρυτικά μέλη της Interpol. Το αρμόδιο Εθνικό Γραφείο Interpol στη Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου της Ελληνικής Αστυνομίας αποτελεί το σημείο επαφής με τη Γενική Γραμματεία της Interpol. Μέσω του Εθνικού Κεντρικού Γραφείο Interpol, η Ελλάδα ανταλλάσσει πληροφορίες σχετικά με εγκλήματα στον κυβερνοχώρο και συμμετέχει σε όλες τις πρωτοβουλίες που λαμβάνει η Γενική Γραμματεία της Interpol.

7.3. Συνεργασία με τρίτα κράτη

Η εθνική πολιτική εφαρμόζει τις διατάξεις και τις διμερείς συμφωνίες σχετικά με την αστυνομική και δικαστική συνεργασία.

Η Ευρωπόλ προσέφερε βοήθεια μέσω του ΑΦΕ twins και του προγράμματος ανταλλαγής αρχείων της Ευρωπόλ.

Η Eurojust συμβάλλει αποφασιστικά στην συνεργασία με τα τρίτα κράτη, μέσω της συνεργασίας των Εθνικών Γραφείων με τους συνδέσμους επαφής που υπάρχουν στα τρίτα κράτη.

7.4.Συνεργασία με τον ιδιωτικό τομέα

Η ΔΙ.Δ.Η.Ε έχει αναπτύξει συνεργασία με τις εγχώριες αεροπορικές εταιρείες και ταξιδιωτικά γραφεία. Ειδικότερα, όταν οι εταιρείες εντοπίζουν ύποπτες για απάτη συναλλαγές (κρατήσεις αεροπορικών εισιτηρίων) με τη χρήση κάρτας πληρωμής, αποστέλλουν την πληροφορία στην ΔΙ.Δ.Η.Ε. και στη συνέχεια η πληροφορία αυτή διαβιβάζεται στις αρμόδιες αστυνομικές αρχές του αντίστοιχου αερολιμένα αναχώρησης του επιβάτη. Απώτερος στόχος της διαδικασίας αυτής είναι η συμμετοχή όλων των δραστηριοποιούμενων αεροπορικών εταιρειών και η αναφορά ύποπτων για απάτη συναλλαγών που αφορούν πτήσεις επιβατών που αναχωρούν από τα αεροδρόμια της χώρας.

Τα πιστωτικά ιδρύματα που δραστηριοποιούνται στην Ελλάδα προσπαθούν να αντιμετωπίζουν τυχόν προβλήματα μέσω της πάγιας συνεργασίας με:

- Διεθνή συστήματα πληρωμών (VISA/ MasterCard / AmEx / Diners / China Unionpay)
- το Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας το οποίο στη συνέχεια ενημερώνει την Ευρωπόλ
- τα αρμόδια πρόσωπα επικοινωνίας χρηματοπιστωτικών ιδρυμάτων του εξωτερικού που πραγματοποιούν ή δέχονται συναλλαγές με κάρτες πληρωμής.

Επίσης, στο πλαίσιο μιας πανευρωπαϊκής πρωτοβουλίας του τραπεζικού κλάδου (εκ μέρους της Ομάδας για την υποστήριξη της ασφάλειας των πληρωμών του Ευρωπαϊκού Συμβουλίου Πληρωμών - EPC), οι ελληνικές τράπεζες συμμετέχουν διά των εκπροσώπων τους στον κατάλογο επαφών έκτακτης ανάγκης για την ιεράρχηση των αιτημάτων μπλοκαρίσματος πληρωμών λόγω απάτης.

Οι πάροχοι υπηρεσιών Διαδικτύου, σύμφωνα με τον Ν. 3917/2011 περί διατήρησης δεδομένων, είναι υποχρεωμένοι να διατηρούν τα δεδομένα για ένα έτος.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνεργάζεται απευθείας με όλους τους τηλεπικοινωνιακούς παρόχους, για τους οποίους δεν έχουν οριστεί επιπλέον υποχρεώσεις, για την πρόληψη και αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.
Οι πάροχοι υπηρεσιών πρόσβασης στο Διαδίκτυο πρέπει ακόμη να τηρούν τις διατάξεις των Κωδίκων Δεοντολογίας για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών. Επίσης οι πάροχοι πρέπει να είναι εγγεγραμμένοι στο Μητρώο Παρόχων Δικτύων και Ηλεκτρονικών Επικοινωνιών που τηρεί η Ε.Ε.Τ.Τ. (βλ. άρθρο 18 παρ. 3 του Ν. 4267/2014, άρθρο 12 του Ν. 4070/2012 και άρθρο 7 της απόφασης υπ' αριθμ. 676/41 με ημερομηνία 20.12.2012 της Ε.Ε.Τ.Τ.-Κανονισμός Γενικών Αδειών).

Ειδικά για παίγνια, η Επιτροπή Εποπτείας και Ελέγχου Παιγνίων (Ε.Ε.Ε.Π.) μπορεί να εκδίδει κανονιστικές αποφάσεις, με σκοπό την προστασία ανηλίκων και γενικά ευάλωτων ομάδων του πληθυσμού και την εφαρμογή συγκεκριμένων μέτρων πρόληψης και καταστολής, την απαγόρευση παιγνίων με περιεχόμενο ρατσιστικό, ξενοφοβικό, πορνογραφικό ή αντίθετο σε κανόνες δημόσιας τάξης (άρθρο 28 παρ.3 περ. ε΄ του Ν. 4002/2011), με τις οποίες μπορούν να θεσπίζονται περαιτέρω υποχρεώσεις και για τους παρόχους παιγνίων. Ως προς τη διατήρηση των δεδομένων, ποινικές και διοικητικές κυρώσεις για τους παρόχους προβλέπονται στα άρθρα 11 και 12 του Ν. 3917/2011 αντίστοιχα.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, ως αρμόδια υπηρεσία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, στα πλαίσια της ποινικής έρευνας κατά την διάρκεια της προανάκρισης επικοινωνεί απευθείας με σχεδόν όλες τις μεγάλες εταιρείες που διαχειρίζονται πληροφορίες στα μέσα κοινωνικής δικτύωσης. Η επικοινωνία ποικίλλει ανάλογα με τον τρόπο που έχει προτείνει κάθε εταιρεία. Στις περισσότερες περιπτώσεις υπάρχει πρόσβαση μέσα από συγκεκριμένη πλατφόρμα. Ωστόσο, τη θετική ανταπόκρισή τους στα αιτήματα εμποδίζει συχνά το διαφορετικό ισχύον νομικό καθεστώς του κράτους όπου εδρεύει η ιδιωτική εταιρεία.

7.5.Μέσα διεθνούς συνεργασίας

7.5.1. Αμοιβαία δικαστική συνδρομή

Η Ελλάδα εφαρμόζει τις διατάξεις της Ευρωπαϊκής Σύμβασης περί αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις του Συμβουλίου της Ευρώπης του 1959 (η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με το ΝΔ 4218/1961), τα άρθρα 48 κ.επ. της Συμφωνίας του Σένγκεν (η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 2514/1997) και τα άρθρα 457 κ.επ. του Κώδικα Ποινικής Δικονομίας σχετικά με την αμοιβαία δικαστική συνδρομή.

Περαιτέρω πρέπει να σημειωθεί ότι, στα πεδία της δικαστικής συνδρομής, η Ελλάδα έχει υπογράψει διμερείς και πολυμερείς συμφωνίες με πληθώρα χωρών.

Τα αιτήματα αμοιβαίας δικαστικής συνδρομής μπορούν να διαβιβάζονται απευθείας, μέσω των κατά τόπο αρμοδίων Εισαγγελέων Εφετών. Οι δεκαεννέα (19) Εισαγγελίες Εφετών διαθέτουν τμήματα Εκδόσεων και Δικαστικών Συνδρομών.

Όσον αφορά την Εισαγγελία Εφετών Αθηνών, με πρόσφατη Απόφαση του Τριμελούς Συμβουλίου Διεύθυνσης του Πρωτοδικείου Αθηνών, ανατέθηκε η εκτέλεση των αιτημάτων δικαστικής συνδρομής της Εφετειακής Περιφέρειας Αθηνών αποκλειστικά στο 7ο Ειδικό Ανακριτικό Τμήμα του Πρωτοδικείου Αθηνών. Στο Τμήμα αυτό υπηρετεί ανώτερος δικαστικός λειτουργός (Πρόεδρος Πρωτοδικών) ο οποίος διαθέτει εξαιρετική εμπειρία στον χειρισμό των αιτημάτων δικαστικής συνδρομής.

Τα αιτήματα αμοιβαίας δικαστικής συνδρομής τρίτων χωρών διαβιβάζονται μέσω της διπλωματικής οδού ήτοι μέσω του Υπουργείου Εξωτερικών ή του Υπουργείου Δικαιοσύνης (ανάλογα με τα προβλεπόμενα στην εκάστοτε ισχύουσα διμερή ή πολυμερή Σύμβαση), στον κατά τόπο αρμόδιο Εισαγγελέα Εφετών και κατόπιν στον εκάστοτε αρμόδιο Ανακριτή (άρ. 458 ΚΠΔ).

Εάν το αίτημα δικαστικής συνδρομής έχει κατεπείγοντα χαρακτήρα μπορεί να ενεργοποιηθεί και ο δίαυλος της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας (ΔΔΑΣ-Ευρωπόλ, SIRENE, Ιντερπόλ) του Αρχηγείου της Ελληνικής Αστυνομίας.

Σε περίπτωση που το αίτημα δικαστικής συνδρομής αφορά το ενδεχόμενο άσκησης ποινικής δίωξης, τότε οπωσδήποτε αυτό διαβιβάζεται στο Υπουργείο Δικαιοσύνης, κατόπιν στον κατά τόπο αρμόδιο Εισαγγελέα Εφετών και τέλος στον κατά τόπο αρμόδιο Εισαγγελέα Πλημμελειοδικών.

Σε περίπτωση που απαιτείται η αποστολή/λήψη διευκρινίσεων ή συμπληρωματικών στοιχείων, ακολουθείται η ως άνω περιγραφείσα διαδικασία ενώ μπορεί να ενεργοποιηθούν και δίαυλοι όπως τα σημεία επαφής του Ευρωπαϊκού Δικαστικού Δικτύου (EJN Contact Points) και ο δίαυλος της EUROJUST.

Είναι δύσκολο να παρασχεθούν πλήρη στατιστικά στοιχεία για τα αιτήματα αμοιβαίας δικαστικής συνδρομής που αφορούν τα εγκλήματα στον κυβερνοχώρο καθώς αυτά διαβιβάζονται απευθείας μέσω των αρμοδίων Δικαστικών Αρχών, χωρίς να λάβουν γνώση αυτών οι υπηρεσίες του Υπουργείου Δικαιοσύνης.

Στο πλαίσιο της εκτέλεσης αιτημάτων αμοιβαίας δικαστικής συνδρομής σχετικά με το έγκλημα στον κυβερνοχώρο, συνήθως ζητείται η ανάληψη ανακριτικών πράξεων όπως η άρση του ηλεκτρονικού απορρήτου και η άρση του τραπεζικού απορρήτου.

Ο πιο συχνός λόγος για αιτήματα δικαστικής συνδρομής είναι η απάτη μέσω υπολογιστή (άρθρο 386Α του Ελληνικού Ποινικού Κώδικα).

Όσον αφορά τον πιο συχνό λόγο αποστολής αιτημάτων δικαστικής συνδρομής προς το εξωτερικό είναι η εξύβριση και η συκοφαντική δυσφήμιση μέσω των μέσων κοινωνικής δικτύωσης (Facebook κ.λπ.) και η απάτη μέσω υπολογιστή (άρθρο 386 Α του Ελληνικού Ποινικού Κώδικα).

Η Ελλάδα δεν έχει συναντήσει μέχρι σήμερα συγκεκριμένα προβλήματα στην αποστολή αιτημάτων αμοιβαίας δικαστικής συνδρομής για αδικήματα που διαπράττονται στο «υπολογιστικό νέφος».

Η Ελλάδα έχει αποστείλει και εξακολουθεί να αποστέλλει πληθώρα αιτημάτων δικαστικής συνδρομής στις Η.Π.Α βάσει της διμερούς συμφωνίας περί αμοιβαίας δικαστικής συνδρομής που υπεγράφη στην Ουάσιγκτον την 26-5-1999 και κυρώθηκε από τη χώρα μας με τον Ν. 2804/2000 (ΦΕΚ 49/3-3-2000, τεύχ. Α΄), σε συνδυασμό με το Πρωτόκολλο στη Σύμβαση αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής, που υπογράφηκε στις 26-5-1999, όπως προβλέπεται στο Άρθρο 3 παράγραφος 2 της Συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την αμοιβαία δικαστική συνδρομή, που υπογράφηκε στις 25-6-2003, και τις Ρηματικές Διακοινώσεις με αριθμούς ΑΣ 199 του Υπουργείου Εξωτερικών της Ελληνικής Δημοκρατίας και 116/POL/09 της Πρεσβείας των Ηνωμένων Πολιτειών της Αμερικής, που κυρώθηκαν από την Ελλάδα με τον Ν. 3771/2009 (ΦΕΚ 111/ 9-7-2009, τεύχ. Α΄).

Ιδίως έναντι των ΗΠΑ, το πρόβλημα που ανέκυψε ήταν η έλλειψη διττού αξιοποίνου και η επακόλουθη μη ικανοποίηση των αιτημάτων δικαστικής συνδρομής των ελληνικών δικαστικών αρχών για αδικήματα όπως η εξύβριση ή η συκοφαντική δυσφήμιση που στην έννομη τάξη των Η.Π.Α. εμπίπτουν στην προστασία της ελευθερίας του λόγου.

Ένα άλλο ζήτημα που αφορά περισσότερες περιπτώσεις είναι η βραχύτητα του χρονικού διαστήματος τήρησης των ηλεκτρονικών ιχνών, με αποτέλεσμα το αίτημα των ελληνικών Δικαστικών Αρχών να μην μπορεί να ικανοποιηθεί λόγω παρέλευσης του χρόνου τήρησης αυτών.

7.5.2. Πράξεις αμοιβαίας αναγνώρισης

Με τον Ν. 4307/2014 ενσωματώθηκαν στην ελληνική έννομη τάξη τα εξής: α) η απόφαση-πλαίσιο 2008/909/ΔΕΥ σχετικά με την εφαρμογή της αρχής της αμοιβαίας αναγνώρισης σε ποινικές αποφάσεις οι οποίες επιβάλλουν ποινές στερητικές της ελευθερίας ή μέτρα στερητικά της ελευθερίας, β) η απόφαση-πλαίσιο 2008/947/ΔΕΥ σχετικά με την εφαρμογή της αναγνώρισης δικαστικών αποφάσεων και αποφάσεων αναστολής εκτέλεσης της ποινής ή απόλυσης υπό όρους και γ) η απόφαση-πλαίσιο 2009/829/ΔΕΥ σχετικά με την εφαρμογή, μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης, της αρχής της αμοιβαίας αναγνώρισης στις αποφάσεις περί μέτρων επιτήρησης εναλλακτικά προς την προσωρινή κράτηση.

7.5.3. Παράδοση/Έκδοση

Με τον Ν. 3251/2004, η απόφαση-πλαίσιο 2002/584/ΔΕΥ για το ευρωπαϊκό ένταλμα σύλληψης και τις διαδικασίες παράδοσης μεταξύ των κρατών μελών μεταφέρθηκε στο εθνικό δίκαιο.

Οι εγκληματικές πράξεις στον κυβερνοχώρο που εμπίπτουν στα εγκλήματα για τα οποία μπορεί να εκδοθεί ή να εκτελεσθεί ευρωπαϊκό ένταλμα σύλληψης είναι όλες οι πράξεις που τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας είναι τουλάχιστον δώδεκα μηνών ή για τις οποίες έχει επιβληθεί ποινή διάρκειας τουλάχιστον τεσσάρων μηνών, σύμφωνα με τις διατάξεις των άρθρων 5 και 10 του Ν. 3251/2004, εκ των οποίων άλλες αντιστοιχούν άμεσα στην κατηγορία των εγκλημάτων στον κυβερνοχώρο (άρθρο 10 παρ. 2 περ. ια΄ εγκλήματα σχετικά με ηλεκτρονικούς υπολογιστές) και άλλες που κατά περίπτωση μπορούν να υπαχθούν σε αυτήν (π.χ. απάτη με υπολογιστή, πορνογραφία ανηλίκων μέσω Διαδικτύου κ.λπ.).

Ευρωπαϊκό ένταλμα σύλληψης (Ν. 3251/2004):

Για τα εγκλήματα στον κυβερνοχώρο, όπως και για όλες τις αξιόποινες πράξεις, σύμφωνα με τις διατάξεις των άρθρων 3 και 4 του Ν. 3251/2004, το Υπουργείο Δικαιοσύνης ορίζεται ως Κεντρική Αρχή για να επικουρεί τις αρμόδιες δικαστικές αρχές για τη διοικητική διαβίβαση και παραλαβή του ευρωπαϊκού εντάλματος σύλληψης, καθώς και της επίσημης αλληλογραφίας, ενώ αρμόδια δικαστική αρχή έκδοσης ευρωπαϊκού εντάλματος σύλληψης είναι ο εισαγγελέας εφετών στην περιφέρεια του οποίου υπάγεται η κατά τόπον αρμοδιότητα: α) για την εκδίκαση της αξιόποινης πράξης για την οποία ζητείται η σύλληψη και η προσαγωγή του εκζητουμένου ή β) για την εκτέλεση της ποινής ή του μέτρου ασφαλείας τα οποία στερούν την ελευθερία.

Όσον αφορά την εκτέλεση ευρωπαϊκών ενταλμάτων σύλληψης, αρμόδια αρχή για την παραλαβή τους είναι ο Εισαγγελέας Εφετών στην περιφέρεια του οποίου συνελήφθη ή κατοικεί ο εκάστοτε εκζητούμενος. Αν ο τόπος διαμονής του εκζητουμένου είναι άγνωστος, αρμόδιος Εισαγγελέας για την λήψη του Ε.Ε.Σ. είναι ο Εισαγγελέας Εφετών Αθηνών.

Διαδικασία έκδοσης (βάσει διμερούς, πολυμερούς συμβάσεως ή με βάση την αρχή της αμοιβαιότητας)

Η διαδικασία έκδοσης εγκληματιών στην ελληνική έννομη τάξη, έχει **δύο (2) στάδια, το δικαστικό και το διοικητικό**. **Μόνο** στην περίπτωση εκτέλεσης ευρωπαϊκού εντάλματος σύλληψης η διαδικασία παράδοσης έχει αποκλειστικά δικαστικό στάδιο.

Για την έκδοση εγκληματιών, η Ελλάδα έχει υπογράψει και ενσωματώσει στην ελληνική έννομη τάξη πληθώρα διμερών και πολυμερών συμβάσεων ενώ ακόμα και όταν δεν υφίσταται τέτοια σύμβαση, τυγχάνουν εφαρμογής οι διατάξεις των άρθρων 436 – 454 του Ελληνικού Κώδικα Ποινικής Δικονομίας, οι οποίες ρυθμίζουν την διαδικασία που πρέπει να ακολουθηθεί σε υπόθεση εκδόσεως.

Σε γενικές γραμμές η διαδικασία έκδοσης στην Ελλάδα έχει ως εξής:

Α΄ Περίπτωση: Τα δικαιολογητικά έχουν περιέλθει μέσω της διπλωματικής οδού στο ελληνικό Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων:

Α. Σύμφωνα λοιπόν με την παρ. 2 του **άρθρου 443 του Κ. Ποιν. Δικ.**:

«2. Η αίτηση για την έκδοση, μαζί με τα έγγραφα που απαιτούνται κατά την παρ. 1 και με την επικυρωμένη μετάφρασή τους, διαβιβάζονται από τον Υπουργό Εξωτερικών στον Υπουργό Δικαιοσύνης· ο τελευταίος αφού ελέγξει τη νομιμότητα της αίτησης, τη στέλνει μαζί με τα έγγραφα, και με τη φροντίδα του εισαγγελέα εφετών, στον πρόεδρο εφετών στην περιφέρεια του οποίου διαμένει εκείνος για τον οποίο ζητείται η έκδοση». Αμέσως μετά και κατά τα διαλαμβανόμενα στο άρθρο **445 παρ. 1**: *«Ο πρόεδρος εφετών έχει υποχρέωση, μόλις παραλάβει τα έγγραφα να διατάξει χωρίς αναβολή, με ένταλμα τη σύλληψη του προσώπου του οποίου ζητείται η έκδοση και την κατάσχεση όλων των πειστηρίων...». Αμέσως μετά ο κατά τόπο αρμόδιος Εισαγγελέας Εφετών μεριμνά για την εκτέλεση του εντάλματος σύλληψης και την προσαγωγή του συλληφθέντος – εκζητουμένου και λαμβάνει χώρα η διαδικασία που προβλέπεται από το άρθρο 446 του Κ. Ποιν. Δικ. Πιο συγκεκριμένα: «Εκείνος που έχει συλληφθεί οδηγείται χωρίς αναβολή μαζί με τις εκθέσεις σύλληψης και κατάσχεσης στον εισαγγελέα εφετών, ο οποίος τον εξετάζει για να βεβαιώσει την ταυτότητά του, λαμβάνοντας υπόψη και τις πληροφορίες της αρχής που πραγματοποίησε τη σύλληψη. Όταν η ταυτότητα βεβαιωθεί, ο εισαγγελέας εφετών διατάσσει την κράτησή του στις φυλακές υποδίκων και στέλνει όλες τις εκθέσεις για τη σύλληψη, την κατάσχεση και τη βεβαίωση της ταυτότητας στον Πρόεδρο Εφετών».*

Αμέσως μετά και εντός είκοσι τεσσάρων (24) ωρών ο κατά τόπο αρμόδιος Πρόεδρος Εφετών συγκαλεί το Συμβούλιο Εφετών σε τριμελή σύνθεση στο συμβούλιο προκειμένου αυτό να γνωμοδοτήσει υπέρ ή κατά της εκδόσεως κατά τα οριζόμενα στο **άρθρο 448 παρ. 1** του Κ. Ποιν. Δικ. Ενώπιον του Συμβουλίου καλείται και προσάγεται, αν συναινεί, εκείνος που έχει συλληφθεί, ο οποίος και δικαιούται να παραστεί με συνήγορο και διερμηνέα της εκλογής του ή, αν δεν έχει, να ζητήσει να διοριστούν συνήγοροι από τον πρόεδρο εφετών. Το Συμβούλιο Εφετών συνεδριάζει δημόσια, εκτός αν εκείνος που έχει συλληφθεί ζητήσει να γίνει η συνεδρίαση κεκλεισμένων των θυρών ή δεν παραστεί καθόλου στο συμβούλιο. Το συμβούλιο μπορεί και αυτεπαγγέλτως να διατάξει να γίνει η συνεδρίαση κεκλεισμένων των θυρών. Το Συμβούλιο Εφετών, μετά την εξέταση εκείνου που έχει συλληφθεί, αν εμφανίστηκε, και μετά τις αγορεύσεις του Εισαγγελέα και εκείνου για τον οποίο ζητείται η έκδοση ή του συνηγόρου του, **γνωμοδοτεί αιτιολογημένα για την αίτηση της έκδοσης και αποφαίνεται: α) για το αν εκείνος που έχει συλληφθεί είναι το ίδιο πρόσωπο με εκείνον για τον οποίον ζητείται η έκδοση, β) για την ύπαρξη των δικαιολογητικών εγγράφων που απαιτούνται από τον Κώδικα ή από τη συνθήκη για την έκδοση, γ) για το αν εκείνος που έχει συλληφθεί και το έγκλημα που αποδίδεται σ' αυτόν ή (προκειμένου για αίτηση έκδοσης ύστερα από καταδικαστική απόφαση) το έγκλημα για το οποίο καταδικάστηκε είναι από εκείνα για τα οποία επιτρέπεται η έκδοση, δ) για το αν συντρέχουν οι όροι του άρ. 438 στοιχ. δ ήτοι κάποιος από τους λόγους για τους οποίους απαγορεύεται η έκδοση (άρθρο 450 παρ. 1 του Κ. Ποιν. Δικ.).**

2. Το Συμβούλιο Εφετών εξετάζει ακόμη, αν δεν κωλύεται από τη σύμβαση, αν υπάρχουν ενδείξεις για τη βασιμότητα της κατηγορίας που αποδίδεται στον εκζητούμενο που έχει συλληφθεί, με βάση τα προσαγόμενα επίσημα αποδεικτικά στοιχεία από το κράτος που ζητεί την έκδοση, και αποφαίνεται αν αυτά θα επέτρεπαν τη σύλληψη και την παραπομπή του σε δίκη στην Ελλάδα, αν το έγκλημα είχε τελεστεί σε ελληνικό έδαφος. Το Συμβούλιο μπορεί, για να σχηματίσει γνώμη στην ουσία της περίπτωσης, να προβεί με ένα από τα μέλη του στη συλλογή κάθε χρήσιμου αποδεικτικού υλικού, **αναβάλλοντας την οριστική απόφαση το πολύ για δεκαπέντε ημέρες.**

Αν το Συμβούλιο Εφετών γνωμοδοτήσει υπέρ της εκδόσεως του εκζητουμένου, ο εκζητούμενος έχει το δικαίωμα να ασκήσει το **ένδικο μέσο της έφεσης** κατά τα προβλεπόμενα στο άρθρο 451 του Κ.Ποιν.Δικ. Πιο συγκεκριμένα: «1. *Κατά της οριστικής απόφασης του Συμβουλίου Εφετών επιτρέπεται σ' αυτόν για τον οποίο ζητείται η έκδοση και στον εισαγγελέα να ασκήσουν έφεση στο β΄ τμήμα του Αρείου Πάγου* ***μέσα σε είκοσι τέσσερις (24) ώρες από τη δημοσίευση της απόφασης****. Για την έφεση συντάσσεται έκθεση από το γραμματέα εφετών.*

2. Ο Άρειος Πάγος σε Συμβούλιο αποφαίνεται μέσα σε οκτώ ημέρες με ανάλογη εφαρμογή των άρθρων 448 και 450. Αυτός για τον οποίο ζητείται η έκδοση κλητεύεται αυτοπροσώπως ή μέσω του αντικλήτου του είκοσι τέσσερις τουλάχιστον ώρες πριν από τη συζήτηση με τη φροντίδα του εισαγγελέα του Αρείου Πάγου.».

Αν η Απόφαση του Αρείου Πάγου κάνει δεκτή κατ' ουσία την έφεση του εκζητουμένου κατά της Απόφασης του Συμβουλίου Εφετών που είχε γνωμοδοτήσει υπέρ της έκδοσης, τότε **ο εκζητούμενος απολύεται και η διαδικασία της έκδοσης τερματίζεται εδώ χωρίς να ακολουθηθεί το διοικητικό στάδιο (άρθρο 452 παρ. 2 του Κ. Ποιν. Δικ.)**.

Το ίδιο συμβαίνει επίσης εάν το Συμβούλιο Εφετών αποφασίσει αμετάκλητα ότι δεν πρέπει να γίνει έκδοση. Στην προκειμένη περίπτωση θεωρείται ότι η απόφαση του Συμβουλίου Εφετών είναι αμετάκλητη εάν δεν ασκηθεί το ένδικο μέσο της έφεσης από τον κατά τόπο αρμόδιο Εισαγγελέα Εφετών.

Κατά της απόφασης του Υπουργού Δικαιοσύνης υπέρ της έκδοσης, ο εκζητούμενος μπορεί να ασκήσει το ένδικο βοήθημα της Αίτησης Ακύρωσης Διαδικασίας ενώπιον του κατά τόπο αρμοδίου Διοικητικού Εφετείου η οποία όμως δεν έχει ανασταλτικό αποτέλεσμα. Ωστόσο ο εν λόγω εκζητούμενος μπορεί μαζί με την Αίτηση Ακυρώσεως να ασκήσει και Αίτηση Αναστολής ζητώντας την αναστολή της εκτέλεσης της προσβαλλόμενης Απόφασης Υπουργού η οποία αν τελεσφορήσει αναστέλλει την έκδοση του εκζητουμένου μέχρι εκδόσεως Απόφασης επί της Αιτήσεως Ακυρώσεως.

Β΄ Περίπτωση: Τα δικαιολογητικά δεν έχουν περιέλθει μέσω της διπλωματικής οδού στο ελληνικό υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, ωστόσο συντρέχει περίπτωση επείγοντος και γίνεται προσωρινή σύλληψη του εκζητουμένου και ακολουθείται κατόπιν η διαδικασία που περιγράφεται από το **άρθρο 445 παρ. 2 του Κ. Ποιν. Δικ.** και έχει ως εξής:

«Άρθρο 445

2. Και χωρίς ένταλμα μπορεί, σε περίπτωση επείγουσας ανάγκης και ιδιαίτερα όταν υπάρχει βάσιμη υπόνοια φυγής του προσώπου που ζητείται η έκδοσή του, να γίνει σύλληψη, πριν ακόμα υποβληθεί η αίτηση για έκδοση, με εντολή του εισαγγελέα εφετών· για τη σύλληψη δεν χρειάζεται διπλωματική μεσολάβηση· απαιτείται όμως αγγελία που διαβιβάζεται ταχυδρομικώς ή τηλεγραφικώς από τη δικαστική ή άλλη αρμόδια αρχή του κράτους που ζητεί την έκδοση. Η αγγελία πρέπει να μνημονεύει το ένταλμα σύλληψης ή την απόφαση και το έγκλημα. Ο Εισαγγελέας Εφετών ανακοινώνει αμέσως τη σύλληψη στον Υπουργό Δικαιοσύνης, ο οποίος μπορεί να διατάξει την απόλυση εκείνου που έχει συλληφθεί.

3. Αν μέσα σε ένα μήνα το πολύ από τη σύλληψη δεν υποβληθεί η αίτηση για έκδοση κατά το άρθρο 443, ο κρατούμενος προσωρινά απολύεται με διαταγή του Εισαγγελέα των Εφετών. Αν υποβληθούν εμπροθέσμως τα έγγραφα, εφαρμόζονται οι διατάξεις της παρ. 1 και των άρθρων 448 επ..

4. Αν ύστερα από την απόλυση του προσώπου που ζητείται η έκδοσή του σύμφωνα με τα παραπάνω περιέλθει στο Υπουργείο Εξωτερικών η αίτηση για έκδοση κατά το άρθρο 443, ακολουθεί η διαδικασία της έκδοσης.

5. Εκείνος που έχει συλληφθεί προσωρινά μπορεί, αμφισβητώντας την ταυτότητά του, να προσφύγει στο συμβούλιο εφετών, μέσα σε είκοσι τέσσερις (24) ώρες από την προσαγωγή του στον Εισαγγελέα των Εφετών· το Συμβούλιο αποφασίζει αμετάκλητα, αφού ακούσει εκείνον που ασκεί την προσφυγή και το συνήγορό του. Η προσφυγή μπορεί να γίνει και προφορικά στον Εισαγγελέα Εφετών.»

Η προθεσμία της προσωρινής κράτησης ποικίλλει ανάλογα με την εκάστοτε διμερή ή πολυμερή σύμβαση που εφαρμόζεται.
Κατά τα λοιπά η διαδικασία έχει όπως περιγράφηκε αμέσως παραπάνω στην περίπτωση Α΄.

Πρέπει να σημειωθεί ότι το Τμήμα SIRENE της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου της Ελληνικής Αστυνομίας, σύμφωνα με το άρθρο 8 παράγραφος 4η του Π.Δ. 178/2014 περί Οργάνωσης των Υπηρεσιών της Ελληνικής Αστυνομίας, μεταξύ άλλων, μεριμνά σε συνεργασία με τις δικαστικές αρχές, για την εισαγωγή, τροποποίηση και διαγραφή των μέτρων των ευρωπαϊκών ενταλμάτων σύλληψης, που εκδίδονται βάσει του Ν. 3251/2004 και του άρθρου 26 της απόφασης 2007/533, στο Σύστημα Πληροφοριών Σένγκεν 2ης Γενιάς.

Είναι δύσκολο να παρασχεθούν πλήρη στατιστικά στοιχεία για τα αιτήματα που αφορούν τα εγκλήματα στον κυβερνοχώρο, μεταξύ των κρατών μελών της Ε.Ε., με δεδομένο ότι αυτά διαβιβάζονται απευθείας μέσω των αρμοδίων δικαστικών αρχών, χωρίς να λάβουν γνώση αυτών οι υπηρεσίες του Υπουργείου Δικαιοσύνης.

Δεν υπάρχουν συγκεκριμένες ειδικές διαδικασίες σχετικά με αιτήματα που αφορούν εγκληματικές πράξεις στον κυβερνοχώρο, ούτε υπάρχει κάποια καθορισμένη ειδική διαδικασία για επείγοντα αιτήματα, τα οποία σε κάθε περίπτωση προωθούνται και διεκπεραιώνονται από τις αρμόδιες δικαστικές αρχές κατά προτεραιότητα, χωρίς καθυστερήσεις και μέσα στα όρια που τάσσει η σύμβαση που τυγχάνει εφαρμογής ή ο Κώδικας Ποινικής Δικονομίας.

Σε κάθε περίπτωση, απαιτείται ευρωπαϊκό ένταλμα σύλληψης για τη σύλληψη και παράδοση σε άλλο κράτος μέλος διωκομένου για εγκλήματα στον κυβερνοχώρο.

Τα εγκλήματα αυτά αντιμετωπίζονται με άμεση ενημέρωση είτε της αρμόδιας ελληνικής αρχής είτε της ξένης, μέσω των αντίστοιχων διαύλων επικοινωνίας.

Υπάρχει η δυνατότητα προσωρινής σύλληψης, κατόπιν έκδοσης σχετικής εντολής του αρμόδιου εισαγγελέα.

Ο χρόνος ανταπόκρισης εξαρτάται από την κάθε περίπτωση, τα δεδομένα, τις συνθήκες τα υπάρχοντα στοιχεία κ.λπ.. Αναφορικά με αιτήματα τα οποία δεν αφορούν σύλληψη προσώπου, αλλά ανταλλάσσονται στο πλαίσιο αστυνομικής συνεργασίας για την πρόληψη και διερεύνηση αξιόποινων πράξεων, αυτά διαβιβάζονται στην αρμόδια Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και, εφόσον είναι σύμφωνα με την εθνική μας νομοθεσία, ικανοποιούνται το συντομότερο, ει δυνατόν εντός της ιδίας ημέρας.
Κατά τα έτη 2011-2015, έχουν συλληφθεί δύο διωκόμενοι βάσει Ε.Ε.Σ. για αδικήματα σχετικά με τον κυβερνοχώρο (ηλεκτρονικές απάτες, κ.α.). Ο ένας εξ αυτών παραδόθηκε στη χώρα έκδοσης του εντάλματος, ενώ ο δεύτερος εξέτισε την επιβληθείσα ποινή.

Αυτή την περίοδο εκκρεμεί προς εξέταση ενώπιον των Ιταλικών Αρχών, ευρωπαϊκό ένταλμα σύλληψης της Εισαγγελίας Εφετών Αθηνών κατά ρουμάνου υπηκόου που αφορά απάτες με πιστωτικές κάρτες και πιο συγκεκριμένα τις αξιόποινες πράξεις: i) της απάτης με υπολογιστή κατ' εξακολούθηση, από υπαίτιους που διαπράττουν απάτες κατ' επάγγελμα και κατά συνήθεια και όπου το συνολικό όφελος και η αντίστοιχη συνολική ζημία υπερβαίνουν το ποσό των 15.000 ευρώ και ii) της παράβασης του άρθρου 22 παράγραφος 6 του Ν. 2472/97 (παραβίασης δεδομένων προσωπικού χαρακτήρα) κατ' εξακολούθηση.

Το έτος 2013 η Ελλάδα είχε δεχθεί και εκτελέσει αίτημα έκδοσης από τις Η.Π.Α. για εκζητούμενο-κατηγορούμενο για αξιόποινη πράξη που συνιστά έγκλημα στον κυβερνοχώρο και ο οποίος πιο συγκεκριμένα εκζητείτο προκειμένου να δικαστεί για τις αξιόποινες πράξεις: 1) της απόσπασης πληροφοριών από προστατευόμενο Η/Υ, 2) της κατοχής μη εξουσιοδοτημένων μέσων (συσκευών) πρόσβασης, 3) διακεκριμένης κλοπής προσωπικών δεδομένων (ταυτότητας), ήτοι για παράβαση του τίτλου 18 του Ποινικού Κώδικα των Η.Π.Α., τμήμα 1030 (α) (2) , του τίτλου 18 του Ποινικού Κώδικα των Η.Π.Α., τμήμα 1029 (α) (3) , του τίτλου 18 του Ποινικού Κώδικα των ΗΠΑ , τμήμα 1028 (α) (1). Η όλη διαδικασία βασίσθηκε από νομική άποψη στη διμερή σύμβαση μεταξύ της Ελλάδας και των ΗΠΑ «περί αμοιβαίας εκδόσεως εγκληματιών», που κυρώθηκε από ελληνικής πλευράς με τον Νόμο 5554/1932, σε συνδυασμό με τις διατάξεις του Πρωτοκόλλου στη Συνθήκη περί αμοιβαίας εκδόσεως εγκληματιών μεταξύ Ελλάδος και Ηνωμένων Πολιτειών της Αμερικής, που υπογράφηκε στις 6.5.1931, και στο Ερμηνευτικό Πρωτόκολλο αυτής, που υπογράφηκε στις 2.9.1937, όπως προβλέπεται στο άρθρο 3 (2) της Συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την έκδοση, που υπογράφηκε στις 25.6.2003, και τις Ρηματικές Διακοινώσεις με αριθμούς ΑΣ 200 του Υπουργείου Εξωτερικών της Ελληνικής Δημοκρατίας και 117/POL/09 της Πρεσβείας των Ηνωμένων Πολιτειών της Αμερικής, όπως ενσωματώθηκαν στην Ελληνική έννομη τάξη με τον Ν. 3770/2009.

Επίσης, υπάρχει ανταλλαγή αιτημάτων στο πλαίσιο της διεθνούς αστυνομικής και δικαστικής συνεργασίας μέσω του διαύλου της INTERPOL. Σε περιπτώσεις έρευνας/σύλληψης/έκδοσης εφαρμόζονται οι διατάξεις περί δικαστικής συνδρομής του Κώδικα Ποινικής Δικονομίας, ενώ δυνάμει διεθνούς εντάλματος σύλληψης εκδίδεται «κόκκινο σήμα» διεθνών ερευνών της INTERPOL. Σε περιπτώσεις ανταλλαγής πληροφοριών και αιτημάτων για ανακριτικές πράξεις, εφαρμόζονται οι ισχύουσες διατάξεις για την αμοιβαία αστυνομική και δικαστική συνεργασία.

7.6. Συμπεράσματα

- Η εφαρμογή της «Σύμβασης της Βουδαπέστης» θα διευκόλυνε και θα επιτάχυνε τη διαφύλαξη των ψηφιακών πειστηρίων πριν από την αποστολή αιτήματος αμοιβαίας δικαστικής συνδρομής. Μετά την εφαρμογή της Σύμβασης οι ελληνικές υπηρεσίες επιβολής του νόμου θα ήταν σε θέση να αποστέλλουν ταχέως αιτήματα διαφύλαξης μέσω του καταλόγου σημείων επαφής συνεχούς λειτουργίας (24/7) του Συμβουλίου της Ευρώπης, που θα αποτελούσε χρήσιμο εργαλείο για τη χώρα στο πεδίο της καταπολέμησης του διεθνούς εγκλήματος στον κυβερνοχώρο.
- Πρέπει να υπογραμμισθεί ότι η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας συμμετέχει - για ορισμένες δραστηριότητες του επιχειρησιακού σχεδίου δράσης ως επικεφαλής ή μεταξύ των επικεφαλής - στις εργασίες όλων των υποπροτεραιοτήτων του προγράμματος Empact που σχετίζονται με το έγκλημα στον κυβερνοχώρο, λ.χ. των Cyberattacks, Payment Card Fraud και Child Sexual Exploitation Online.
- Οι εθνικές αρχές κρίνουν ότι υπάρχει καλή συνεργασία με την Ευρωπόλ, την Eurojust και τον ENISA. Ωστόσο, έως την πραγματοποίηση της επίσκεψης αξιολόγησης η Ελλάδα δεν διαθέτει πείρα όσον αφορά τις κοινές ομάδες ερευνών και τις κυβερνοπεριπόλους.
- Τα αιτήματα αμοιβαίας δικαστικής συνδρομής μπορούν να απευθύνονται απευθείας στις δικαστικές αρχές, μέσω των τοπικών εισαγγελικών υπηρεσιών. Για τον λόγο αυτό δεν ήταν δυνατόν να παρασχεθούν σε κεντρικό επίπεδο στατιστικά στοιχεία σχετικά με τα αιτήματα αυτά.
- Η Ελλάδα υπέβαλε πληροφορίες που είχε ζητήσει από χώρες όπως η Κίνα και η Ρωσία σε υποθέσεις σχετικές με Σεξουαλική Εκμετάλλευση Παιδιών. Το Υπουργείο Δικαιοσύνης και η Eurojust διαδραματίζουν σημαντικό ρόλο εν προκειμένω.
- Σύμφωνα με τις εθνικές αρχές, η Ελλάδα έχει υποβάλει αιτήματα αμοιβαίας δικαστικής συνδρομής στις ΗΠΑ. Οι κύριες δυσκολίες στην πράξη οφείλονται στην έλλειψη διττού αξιοποίνου, με αποτέλεσμα τη μη ικανοποίηση των αιτημάτων αυτών για το λόγο ότι ορισμένες πράξεις, όπως η συκοφαντική δυσφήμηση, στην έννομη τάξη των ΗΠΑ εμπίπτουν στην προστασία της ελευθερίας του λόγου.

8. ΚΑΤΑΡΤΙΣΗ, ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΠΡΟΛΗΨΗ

8.1. Εξειδικευμένη κατάρτιση

Α) ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

Παρέχεται εκπαίδευση σχετική με το έγκλημα στο κυβερνοχώρο στους σπουδαστές της Αστυνομικής Ακαδημίας, τόσο σε βασικό όσο και σε μετεκπαιδευτικό επίπεδο. Επίσης, παρέχεται τέτοιου είδους εκπαίδευση μέσω των διαδικτυακών σεμιναρίων (webinars), καθώς και με τη συμμετοχή στελεχών της Ελληνικής Αστυνομίας σε σεμινάρια που διοργανώνουν η CEPOL και άλλοι διεθνείς και ευρωπαϊκοί φορείς.

Πιο συγκεκριμένα:

Α. ΒΑΣΙΚΟ ΕΠΙΠΕΔΟ:

Σχολή Αξιωματικών Ελληνικής Αστυνομίας

Μάθημα: Αστυνομία Δημόσιας Ασφάλειας

(α) Θεματική ενότητα: «Ηλεκτρονικό Έγκλημα»

(β) Στόχος (του μαθήματος Δημόσιας Ασφάλειας - δεν υφίσταται ξεχωριστός στόχος της θεματικής ενότητας: Ηλεκτρονικό Έγκλημα): Επιδιώκεται να αποκτήσουν οι εκπαιδευόμενοι Δόκιμοι Υπαστυνόμοι: (1) τις εξειδικευμένες γνώσεις Αστυνομικής Μεθοδολογίας για αποτελεσματική δίωξη, καταπολέμηση του εγκλήματος και επιτυχή εκτέλεση των ανακριτικών καθηκόντων, (2) τη ικανότητα προσέγγισης των αναπαραστάσεων, τάσεων και των μέτρων αντιμετώπισης της εγχώριας εγκληματικότητας καθώς και των διαύλων της διεθνούς αστυνομικής συνεργασίας.

(γ) Διάρκεια εκπαίδευσης: δύο (2) διδακτικές ώρες.

(δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος στο 2ο εκπαιδευτικό τμήμα.

(ε) Επίσης το ανωτέρω θέμα αποτελεί και αντικείμενο πτυχιακής εργασίας από τους σπουδαστές της Σχολής.

Μάθημα: Ουσιαστικό Ποινικό Δίκαιο

(α) Θεματική ενότητα: «Απάτη με ηλεκτρονικό υπολογιστή» Άρθρο 386Α Ποινικού Κώδικα

(β) Στόχος (του μαθήματος Ουσιαστικού Ποινικού Δικαίου - δεν υφίσταται ξεχωριστός στόχος της εν λόγω θεματικής ενότητας): Κατανόηση των διατάξεων του ειδικού μέρους του Ποινικού Κώδικα, με έμφαση στα εγκλήματα που παρουσιάζονται συχνότερα κατά την αστυνομική δράση και τα οποία θα αντιμετωπίσουν οι Δόκιμοι Υπαστυνόμοι μετά την αποφοίτησή τους, κατά την άσκηση των καθηκόντων τους.

(γ) Διάρκεια εκπαίδευσης: δύο (2) διδακτικές ώρες

(δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος στο 3ο εκπαιδευτικό τμήμα.

(ε) Μάθημα: Επιστημονική Αστυνομία-Ανακριτική

(στ) α) Θεματική Ενότητα της Επιστημονικής Αστυνομίας: Θέματα εξέτασης ψηφιακών και ηχητικών πειστηρίων και διδακτέα ύλη: Εξέταση ψηφιακών πειστηρίων (τρόπος κατάσχεσης, διακίνησης, φύλαξης, εξέτασης κ.λπ.)- εξέταση θεμάτων διακίνησης στοιχείων μέσω Διαδικτύου (ψηφιακές απάτες).

β) Στόχος (του μαθήματος Επιστημονική Αστυνομία-Ανακριτική - δεν υφίσταται ξεχωριστός στόχος της θεματικής ενότητας: Θέματα εξέτασης ψηφιακών και ηχητικών πειστηρίων): Να κατανοήσουν και εμπεδώσουν οι εκπαιδευόμενοι Δόκιμοι Υπαστυνόμοι την αναγκαιότητα των τεκμηριωμένων υλικών αποδείξεων που προκύπτουν από την επιστημονική διερεύνηση του τόπου του εγκλήματος και από τις εργαστηριακές εξετάσεις.

γ) Διάρκεια εκπαίδευσης: Τρεις (3) διδακτικές ώρες.

δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος στο 3ο εκπαιδευτικό τμήμα.

Σχολή Αστυφυλάκων

Μάθημα: Θέματα Δημόσιας Ασφάλειας

(α) Θεματική ενότητα: «Ηλεκτρονικό Έγκλημα»

(β) Στόχος (του μαθήματος Δημόσιας Ασφάλειας - δεν υφίσταται ξεχωριστός στόχος της θεματικής ενότητας: Ηλεκτρονικό Έγκλημα): Να καταστούν οι εκπαιδευόμενοι ικανοί να κατανοούν τρόπους διάπραξης εγκλημάτων που αφορούν τη Δημόσια Ασφάλεια και να εφαρμόζουν κατάλληλους τρόπους πρόληψης και καταστολής τους. Να φέρει τους Δόκιμους Αστυφύλακες σε επαφή με το πρόβλημα αντιμετώπισης της εγκληματικότητας και ειδικότερα να τους καταστήσει γνώστες των αιτιών εγκληματικής συμπεριφοράς ατόμων και κοινωνικών ομάδων, της προσωπικότητάς τους, των ιδιαιτεροτήτων στον τρόπο δράσης τους, καθώς και των δυνατοτήτων, επιστημονικών ή αστυνομικών που διατίθενται.

(γ) Διάρκεια εκπαίδευσης: Μία (1) διδακτική ώρα.

(δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος για τους Δόκιμους Αστυφύλακες του 1ου εκπαιδευτικού τμήματος.

Β. ΜΕΤΕΚΠΑΙΔΕΥΤΙΚΟ ΕΠΙΠΕΔΟ

✓Σχολή Μετεκπαίδευσης και Επιμόρφωσης/Τμήμα Επαγγελματικής Μετεκπαίδευσης Ανθυπαστυνόμων

Μάθημα: Θέματα Δημόσιας Ασφάλειας

(α) Υποχρεωτική διάλεξη: Ηλεκτρονικό Έγκλημα

(β) Στόχος (του μαθήματος Δημόσιας Ασφάλειας): Η συμπλήρωση της επαγγελματικής μόρφωσης των σπουδαστών, η συζήτηση και ανάλυση προβλημάτων που ανέκυψαν κατά την άσκηση των καθηκόντων τους και η ενημέρωσή τους σε σύγχρονα και γενικότερα θέματα.

(γ) Διάρκεια εκπαίδευσης: Δύο (2) διδακτικές ώρες

(δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος στους φοιτούντες του Τμήματος Επαγγελματικής Μετεκπαίδευσης Ανθυπαστυνόμων.

Σχολή Εθνικής Ασφάλειας

Γνωστικό αντικείμενο: Θέματα Δημόσιας Ασφάλειας

(α) Θέμα διάλεξης: Η επιστήμη του Διαδικτύου και το ηλεκτρονικό έγκλημα.

(β) Στόχος (του γνωστικού αντικειμένου «Θέματα Δημόσιας Ασφάλειας»): Η μετεκπαίδευση και επιμόρφωση σε μεταπτυχιακό επίπεδο των σπουδαστών της στα θέματα που αφορούν τη Δημόσια Ασφάλεια και σχετίζονται με τη Στρατηγική και Πολιτική Εθνικής Ασφάλειας, ώστε να μπορούν να ανταποκριθούν στα καθήκοντα του ανώτατου κρατικού λειτουργού.

(γ) Διάρκεια εκπαίδευσης: τρεις (3) διδακτικές ώρες

(δ) Συχνότητα εκπαίδευσης: Η εκπαίδευση πραγματοποιείται κάθε εκπαιδευτικό έτος στους σπουδαστές της Σχολής Εθνικής Ασφάλειας.

(ε) Επίσης, το ανωτέρω θέμα αποτελεί και αντικείμενο μεταπτυχιακής έρευνας και εργασίας από τους σπουδαστές της Σχολής.

Γ. Διαδικτυακά Σεμινάρια (Webinars) που έχουν διοργανωθεί από το έτος 2011 έως και σήμερα.

Ιδιαίτερα σημαντική σε μετεκπαιδευτικό επίπεδο είναι η δυνατότητα συμμετοχής προσωπικού της Ελληνικής Αστυνομίας στα διαδικτυακά σεμινάρια webinars, που διοργανώνονται με πρωτοβουλία της Ευρωπαϊκής Αστυνομικής Ακαδημίας (CEPOL).

Επισημαίνεται ότι η διάρκεια των διαδικτυακών σεμιναρίων είναι περίπου 90 λεπτά και προσωπικό της Ελληνικής Αστυνομίας συμμετείχε στα κάτωθι Σεμινάρια:

✓ **CEPOL webinar 111/2012 «Διαδικτυακή Ενότητα Μάθησης για το έγκλημα στον κυβερνοχώρο» («Cyber Crime Online Learning Module»), 21/2/2012.**

Στο εν λόγω Διαδικτυακό Σεμινάριο συμμετείχαν τριάντα δύο (32) στελέχη της Ελληνικής Αστυνομίας και είχε ως σκοπό οι συμμετέχοντες:

- Να εισαχθούν στην ηλεκτρονική ενότητα του εγκλήματος στον κυβερνοχώρο, που είναι διαθέσιμη στην ηλεκτρονική πλατφόρμα της CEPOL.
- Να προσδιορίσουν και να προτείνουν τρόπους και παραδείγματα για το πώς οι εκπαιδευτικοί, οι δάσκαλοι, οι υπεύθυνοι για την ανάπτυξη σειράς μαθημάτων/προγραμμάτων σπουδών στις σχολές της Αστυνομίας μπορούν να την ενσωματώσουν στις διδακτικές τους ενότητες.

✓ **CEPOL webinar 10/2014 «Έγκλημα στον κυβερνοχώρο: Εργαστηριακά και ψηφιακά πειστήρια» (Cybercrime: Forensic and Digital Evidence), 4/12/2014.**

Στο εν λόγω Διαδικτυακό Σεμινάριο συμμετείχαν έντεκα (11) στελέχη της Ελληνικής Αστυνομίας και στόχος του ήταν να παρουσιαστούν η παρούσα κατάσταση στις χώρες της Ε.Ε. σχετικά με τα ψηφιακά πειστήρια και τις πιο πρόσφατες τάσεις, καθώς και μελλοντικές προοπτικές.

- ✓ **CEPOL webinar 09/2014 «Έγκλημα στον κυβερνοχώρο: Γνωστοποίηση στις αρμόδιες αρχές, έρευνα και πρόληψη» (Cybercrime: Disclosure, Investigation and Prevention), 27/11/2014.**

Στο εν λόγω Διαδικτυακό Σεμινάριο συμμετείχαν δέκα (10) στελέχη της Ελληνικής Αστυνομίας και στόχος του ήταν να παρουσιαστούν οι τελευταίες τάσεις και οι μελλοντικές προοπτικές στο χώρο του εγκλήματος στον κυβερνοχώρο.

- ✓ **CEPOL webinar 8/214 «Έγκλημα στον κυβερνοχώρο: Ηλεκτρονικές απάτες» (Cybercrime: E-Frauds), 6/11/2014.**

Στο εν λόγω Διαδικτυακό Σεμινάριο συμμετείχαν δεκαπέντε (15) στελέχη της Ελληνικής Αστυνομίας και στόχος του ήταν να παρουσιαστούν οι τελευταίες τάσεις στις ηλεκτρονικές απάτες μέσω πιστωτικών καρτών και η συνεργασία μεταξύ δικαστικών αρχών και ιδιωτικού τομέα.

Δ. Σεμινάρια που έχουν διοργανωθεί από τη CEPOL από το έτος 2010 έως και σήμερα

Παράλληλα, η Ελληνική Αστυνομία επωφελείται των Σεμιναρίων που υλοποιούνται από την Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL), προσωπικό δε αυτής έχει συμμετάσχει στα κάτωθι σεμινάρια:

- ✓ «Διαδικτυακό Έγκλημα και έγκλημα με τη χρήση υψηλής τεχνολογίας», (18-21 Μαΐου 2010, Αθήνα) - τρεις (3) συμμετέχοντες
- ✓ «Διαδικτυακό Έγκλημα και έγκλημα με τη χρήση υψηλής τεχνολογίας – Γενικότερες Τάσεις» (16–19 Οκτωβρίου 2012, Avila Ισπανίας) – Συμμετοχή ενός (1) εκπροσώπου της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
- ✓ «Κακοποίηση ανηλίκων μέσω Διαδικτύου» (1-4 Οκτωβρίου 2013, Βαρκελώνη Ισπανίας) – Συμμετοχή δύο (2) εκπροσώπων της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
- ✓ «Δυνατότητα της Ε.Ε και των κρατών μελών να ανιχνεύουν, να διερευνούν και να ασκούν δίωξη κατά των εγκλημάτων στον Κυβερνοχώρο» (23-26 Απριλίου 2013, Στοκχόλμη Σουηδίας) - Συμμετοχή ενός (1) εκπροσώπου της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
- ✓ «Παιδική κακοποίηση στον κυβερνοχώρο» (8-11/04/2014, Βαρκελώνη Ισπανίας) – Συμμετοχή ενός (1) εκπροσώπου της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
- ✓ «Το έγκλημα στον κυβερνοχώρο και η ασφάλεια του κυβερνοχώρου» (27-30 Οκτωβρίου 2015, Φινλανδία) – Συμμετοχή ενός (1) εκπροσώπου της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

- ✓ Προεδρικό Συνέδριο Λετονίας στο πλαίσιο της Ευρωπαϊκής Αστυνομικής Ακαδημίας (CEPOL) με θέμα «Καταπολέμηση Διαδικτυακού εγκλήματος σε στρατηγικό επίπεδο. Μελλοντικές προκλήσεις στην αντιμετώπιση της διαδικτυακής εγκληματικότητας» (Jurmala Λετονίας, 25-27/3/2015) – Συμμετοχή δύο (2) εκπροσώπων της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και ενός (1) εκπροσώπου της Διεύθυνσης Πληροφορικής/ΑΕΑ.
- ✓ «Οι πρώτοι ανταποκριτές και οι εργαστηριακές έρευνες στον κυβερνοχώρο» (8-12 Ιουνίου 2015, Εσθονία) – Συμμετοχή ενός (1) εκπροσώπου της Υποδιεύθυνσης Εγκληματολογικών Ερευνών Βορείου Ελλάδας.

Ε. ΣΥΜΜΕΤΟΧΗ ΣΕ ΑΛΛΕΣ ΜΕΤΕΚΠΑΙΔΕΥΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

α. Αναφέρεται ενδεικτικά η συμμετοχή προσωπικού της Ελληνικής Αστυνομίας στις κάτωθι εκπαιδευτικές δραστηριότητες:

- ✓ Το έτος 2013 πραγματοποιήθηκε εκπαιδευτικό σεμινάριο στο πλαίσιο του προγράμματος αντιτρομοκρατικής βοήθειας (ΑΤΑ), του Υπουργείου Εξωτερικών των ΗΠΑ, με θέμα «Εγρήγορση σε θέματα Κυβερνοχώρου/Διαδικτύου», με συμμετοχή δεκαπέντε (15) στελεχών.
- ✓ Συμμετοχή τεσσάρων (4) αξιωματικών της Διεύθυνσης Ασφάλειας Αττικής, στο Ετήσιο Συνέδριο για την Έρευνα και την Ασφάλεια στον Κυβερνοχώρο (Abu Dhabi Ηνωμένων Αραβικών Εμιράτων, 10-11/11/2010)
- ✓ Συμμετοχή ενός (1) αξιωματικού της Διεύθυνσης Ασφάλειας Αττικής στο 2ο Διεθνές συνέδριο για την καταπολέμηση του παράνομου διαδικτυακού υλικού και της κακοποίησης ανηλίκων (2nd INHOPE Building Collaboration Conference) (Άμστερνταμ Ολλανδίας, 4-5/11/2010)
- ✓ Συμμετοχή ενός (1) αξιωματικού της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος/Α.Ε.Α. σε εκπαιδευτικό Διεθνές Συνέδριο του F.B.I. για το «Έγκλημα στον Κυβερνοχώρο» (Πράγα Τσεχίας, 17/5/2012).
- ✓ Συμμετοχή ενός (1) στελέχους της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος/Α.Ε.Α. σε εκπαιδευτικό Διεθνές Συνέδριο της EUROPOL για την αντιμετώπιση της Σεξουαλικής εκμετάλλευσης ανηλίκων μέσω Διαδικτύου (Selm Γερμανίας, 21-29/10/2013).

- ✓ Συμμετοχή ενός (1) στελέχους της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος/Α.Ε.Α. στο Εκπαιδευτικό Εργαστήριο του Κέντρου «George Marshall» σε θέματα ασφάλειας στο Διαδίκτυο (Program on Cyber Security studies) (Garmish-Partenkirchen Γερμανίας, 5-8/05/2014).
- ✓ Συμμετοχή ενός (1) στελέχους της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος/Α.Ε.Α στο Εκπαιδευτικό Πρόγραμμα της EUROPOL με θέμα την καταπολέμηση της σεξουαλικής εκμετάλλευσης ανηλίκων μέσω του Διαδικτύου (Selm Γερμανίας, 6-14/10/2014).
- ✓ Συμμετοχή ενός (1) στελέχους της Διεύθυνσης Εγκληματολογικών Ερευνών στη συνάντηση Εθνικών Εμπειρογνωμόνων του Δικτύου ECTEG (European Cybercrime Training and Education Group) (ΕΥΡΩΠΟΛ (Χάγη Ολλανδίας, 6-7/5/2015).

β. Περαιτέρω, προσωπικό της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμμετείχε στα κάτωθι εκπαιδευτικά προγράμματα, κατόπιν χορηγίας-δωρεάς.

- ✓ Σεμινάριο Computer Forensics – Online Infosec Institute: Αφορά εξ' αποστάσεως εκπαίδευση, διάρκειας 45 ωρών. Συμμετοχή ενός (1) Αξιωματικού.
- ✓ Πλατφόρμα ηλεκτρονικής μάθησης ACM (Association for Computing Machinery) και πλατφόρμα ηλεκτρονικής μάθησης-ηλεκτρονικά περιοδικά «Hakin9, eForensics και SDJ», με θεματολογία το ηλεκτρονικό έγκλημα και την ψηφιακή εγκληματολογία. Ειδικότερα οι συμμετέχοντες αποκτούν πρόσβαση σε υλικό, που είναι διαθέσιμο διαδικτυακά. Στην πρώτη πλατφόρμα απέκτησαν πρόσβαση πέντε (5) Αξιωματικοί και στη δεύτερη ένας (1) Ανθυπαστυνόμος.
- ✓ Σεμινάριο MCITP Windows Server 2012 Administrator, το οποίο διοργανώνεται από την Ελληνοαμερικανική Ένωση, με συνολική διάρκεια 200 ώρες. Συμμετοχή ενός (1) Αξιωματικού.
- ✓ Σεμινάριο Advanced Ethical Hacking, το οποίο διοργανώνεται από το Infosec Institute. Πρόκειται για εξ' αποστάσεως εκπαίδευση, που δύναται να ολοκληρωθεί σε ένα (1) έτος. Συμμετοχή ενός (1) Αξιωματικού.

- ✓ Σεμινάριο Ethical Hacking Live OnLine: Διοργανώνεται από το Infosec Institute, πρόκειται για εξ' αποστάσεως εκπαίδευση, που δύναται να ολοκληρωθεί σε ένα (1) έτος. Συμμετοχή ενός Αξιωματικού.
- ✓ Πρόγραμμα Μεταπτυχιακών Σπουδών «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων», του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Συμμετοχή δύο (2) Αξιωματικών.

γ) Περαιτέρω αξίζει να επισημανθεί ότι, όπως μνημονεύθηκε και ανωτέρω (βλ. ερώτ. 3Β2), τόσο στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, όσο και στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών, υπηρετούν αστυνομικοί γενικών και ειδικών καθηκόντων, οι οποίοι διαθέτουν τίτλους σπουδών προπτυχιακού, μεταπτυχιακού και ορισμένοι εξ αυτών και διδακτορικού επιπέδου σε αντικείμενα σχετικά με την πληροφορική.

Β) Δικαστικό σώμα

Με απόφασή του το Συμβούλιο Σπουδών της Εθνικής Σχολής Δικαστικών Λειτουργών ενέταξε στο Πρόγραμμα Σπουδών της Κατεύθυνσης των Εισαγγελέων του έτους 2015 το μάθημα:

15. ΝΟΜΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ

Ποινικά θέματα νομικής πληροφορικής

Έγκλημα·στον κυβερνοχώρο

Διδάσκων: Ιωάννης Αγγελής, Εισαγγελέας Εφετών

Ώρες διδασκαλίας: 9 δίωρα

Και στην Κατεύθυνση της Πολιτικής-Ποινικής Δικαιοσύνης του έτους 2015, διδάσκεται το μάθημα:

4. Ηλεκτρονικό Έγκλημα

Διδάσκων: Ιωάννης Αγγελής, Εισαγγελέας Εφετών

Ώρες διδασκαλίας: 6 δίωρα

Τελικές διευκρινίσεις

Η επικοινωνία – διδασκαλία με τους σπουδαστές της Σχολής γίνεται κατά τρόπο ώστε, να «κατευθύνουν» αυτοί τα θέματα (με προτάσεις, με υποβολή ερωτήσεων, κ.λπ.) σύμφωνα με τις ανάγκες τους και ανάλογα με τις γνώσεις τους σε τεχνικά και νομικά θέματα νέων τεχνολογιών. Έχει διαπιστωθεί ότι σχεδόν όλοι κατέχουν «ένα ελάχιστο ποσοστό τεχνικών και νομικών γνώσεων», που κατά κανόνα έχουν αποκτήσει με δική τους πρωτοβουλία (διευκρινίζεται ότι η νομική πληροφορική διδάσκεται στις Νομικές Σχολές ως μάθημα επιλογής).

Η διδασκαλία γίνεται με τη χρήση ηλεκτρονικών υπολογιστών. Στους σπουδαστές έχουν αποσταλεί διάφορα νομικά άρθρα και μελέτες (μεταξύ των οποίων και οι εργασίες και παρουσιάσεις του διδάσκοντος σε συνέδρια), καθώς και δικαστικές αποφάσεις προς νομική (και τεχνική) ανάλυση. Συζητούνται δε διάφορα πρακτικά θέματα όπως, ο τρόπος έρευνας σε βάσεις νομικών δεδομένων, η αναζήτηση νομικών θεμάτων στο Διαδίκτυο, ο τρόπος τηρήσεως αρχείων από τον Δικαστή και τον Εισαγγελέα.

Σε ετήσια βάση, πραγματοποιείται ειδικό εκπαιδευτικό σεμινάριο της «OLAF» σε συγκεκριμένο αριθμό ατόμων του Τμήματος Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών/ΑΕΑ, προκειμένου να εκπαιδευτούν σε θέματα εξέτασης ψηφιακών πειστηρίων από τον Διεθνή οργανισμό IACIS.

Επιπρόσθετα, αντίστοιχες εκπαιδεύσεις διοργανώνονται από τις CEPOL, ECTEG (European Cybercrime Training and Education Group) και ΕΥΡΩΠΟΛ/EC3 κατά την διάρκεια του έτους, στις οποίες η χώρα συμμετέχει κατά περίπτωση.

Τέλος, στην ημεδαπή διοργανώνεται σε ετήσια βάση διήμερο εκπαιδευτικό σεμινάριο από το Κέντρο Μελετών Ασφαλείας (ΚΕΜΕΑ).

Περαιτέρω, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων κάθε χρόνο διοργανώνει συντηρητικές εκπαιδεύσεις στο προσωπικό των Τμημάτων & Γραφείων Εγκληματολογικών Ερευνών (Τ.Ε.Ε. και Γ.Ε.Ε) της χώρας για θέματα που άπτονται της εγκληματολογικής εξέτασης υπολογιστικών συστημάτων και ψηφιακών πειστηρίων. Ειδικότερα, παρέχεται εκπαίδευση στους εξής τομείς:

- στην αναγνώριση των πειστηρίων υπολογιστικών συστημάτων,
- στη συλλογή των πειστηρίων
- και στον τρόπο αποστολής των πειστηρίων (ως προς την προστασία-διασφάλιση και τα τεθέντα ερωτήματα) για εξέταση είτε στη Διεύθυνση Εγκληματολογικών Ερευνών είτε στο αντίστοιχο Τμήμα της Υποδιεύθυνσης Εγκληματολογικών Ερευνών Βορείου Ελλάδος (ανάλογα με την εδαφική αρμοδιότητα του εκάστοτε Τ.Ε.Ε. – Γ.Ε.Ε.)

Την ευθύνη για την εκπαίδευση σχετικά με το έγκλημα στον κυβερνοχώρο έχουν περισσότερες από μία αρχές και ιδρύματα:
α) Υπεύθυνος για την παροχή της εκπαίδευσης σχετικά με το έγκλημα στον κυβερνοχώρο, σε βασικό αλλά και σε μετεκπαιδευτικό επίπεδο, είναι η κάθε Σχολή που υλοποιεί την εκπαίδευση, όπως περιγράφεται στο ερώτημα 10Β1, ως υπεύθυνη του προγράμματος εκπαίδευσής της και συγκεκριμένα η Σχολή Αξιωματικών Ελληνικής Αστυνομίας, η Σχολή Αστυφυλάκων, η Σχολή Μετεκπαίδευσης και Επιμόρφωσης και η Σχολή Εθνικής Ασφάλειας.
β) Υπεύθυνη για την παροχή της εκπαίδευσης σχετικά με το έγκλημα στον κυβερνοχώρο, μέσω των σεμιναρίων που διοργανώνει η CEPOL καθώς και μέσω των διαδικτυακών σεμιναρίων (webinars), είναι η CEPOL.
γ) Ως προς τον βαθμό συνεισφοράς των ευρωπαϊκών οργανισμών στην εκπαίδευση των αρχών επιβολής του νόμου, αυτός είναι ιδιαίτερα σημαντικός και επωφελής, όπως αναλυτικά εμφαίνεται ανωτέρω.

Η ετησία δαπάνη στον ΚΑΕ 0881 (Αμοιβές για εκπαίδευση, μετεκπαίδευση, επιμόρφωση) καθώς και στον ΚΑΕ 0517 (Αμοιβές ωρομισθίων εκπαιδευτικών και λοιπών προσώπων για την προσφορά διδακτικού έργου) για το τρέχον έτος έχει προβλεφθεί καθ' ύψος στα ποσά των 800.000,00 € και 1.600.00,00 € αντίστοιχα (συνολικό ποσό δαπάνης για όλο το φάσμα εκπαίδευσης και όχι μόνο για το ειδικότερο αντικείμενο του ηλεκτρονικού εγκλήματος).

Όσον αφορά τα διαδικτυακά σεμινάρια (webinars), επισημαίνεται ότι προκαλείται μηδενική ετήσια δαπάνη για την Ελληνική Αστυνομία, ενώ επίσης επιβαρύνεται με το 25% της εκτός έδρας αποζημίωσης του συμμετέχοντος αστυνομικού σε σεμινάριο που διοργανώνει η Cepol στο εξωτερικό ή στο εσωτερικό της χώρας.

Δεδομένου ότι στις αρμοδιότητες του προσωπικού της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας δεν ανάγεται η διερεύνηση υποθέσεων δίωξης ηλεκτρονικού εγκλήματος, αλλά η ανταλλαγή πληροφοριών, εμπειριών και γνώσεων μεταξύ της Ελληνικής Αστυνομίας και των ξένων αστυνομιών (αποτελεί δηλαδή δίαυλο επικοινωνίας μέσω των Τμημάτων INTERPOL, ΕΥΡΩΠΟΛ, SIRENE), στο πλαίσιο των τακτικών προγραμμάτων της Σχολής Μετεκπαίδευσης, δεν προβλέπεται εκπαίδευση σε σχέση με το έγκλημα στον κυβερνοχώρο στα άτομα που συμμετέχουν στη διαδικασία διεθνούς συνεργασίας.

Κάθε χρόνο διοργανώνεται διήμερο Σεμινάριο από το Ελληνικό Κέντρο για το κυβερνοέγκλημα του Κέντρου Μελετών Ασφαλείας (ΚΕΜΕΑ), στο οποίο συμμετέχουν τόσο εμπειρογνώμονες από την ημεδαπή όσο και από την αλλοδαπή.

Το ForthCERT στο Ηράκλειο της Κρήτης είναι το μόνο πιθανό σχετικό κέντρο αριστείας σε θέματα κυβερνοασφάλειας, όπως επίσης και η ομάδα του ΙΤΥΕ «ΔΙΟΦΑΝΤΟΣ» και το ΚΕΜΕΑ.

Α) ΠΡΩΤΟΒΑΘΜΙΑ ΚΑΙ ΔΕΥΤΕΡΟΒΑΘΜΙΑ ΕΚΠΑΙΔΕΥΣΗ

Ιδρύματα και δράσεις για την πρόληψη του εκφοβισμού

Α. Το Υπουργείο Παιδείας και η Γενική Γραμματεία Νεολαίας συμμετείχαν στην ίδρυση του Δικτύου κατά της Βίας στο Σχολείο, που πραγματοποιήθηκε το 2011 με πρωτοβουλία της Εταιρείας Ψυχοκοινωνικής Υγείας του Παιδιού και του Εφήβου (ΕΨΥΠΕ) στην Ελλάδα.

Β. Στα σχολεία έχουν εισαχθεί πολλά προγράμματα υγειονομικής εκπαίδευσης με θέματα σχετικά με: την πρόληψη της βίας, τη διαχείριση των συγκρούσεων, τον ρατσισμό, τις διαπροσωπικές σχέσεις (με το διδακτικό προσωπικό, τους γονείς, τις ομάδες συνομηλίκων), την ισότητα των φύλων, τις σχέσεις μεταξύ των φύλων, τη σεξουαλική κακοποίηση, τη βία στο Διαδίκτυο, την εκμετάλλευση παιδιών και την οικογενειακή βία.

Γ. Το Υπουργείο Παιδείας έχει ιδρύσει το Κέντρο Πρόληψης για την Ενδοσχολική Βία και τον Εκφοβισμό. Σκοπός του Κέντρου είναι ο σχεδιασμός και η εφαρμογή μέτρων για την πρόληψη της ενδοσχολικής βίας και του εκφοβισμού μέσω του εντοπισμού και της μελέτης συμβάντων ενδοσχολικής βίας και εκφοβισμού και της διοχέτευσής τους προς διαχείριση σε πιστοποιημένους οργανισμούς.

Ειδικές δράσεις και προγράμματα για την ασφάλεια στο Διαδίκτυο

Ειδικά για την ασφάλεια στο Διαδίκτυο έχουν υλοποιηθεί οι ακόλουθες δράσεις:

Το Υπουργείο Παιδείας, σε συνεργασία με το Υπουργείο Δημόσιας Τάξης και Προστασίας του Πολίτη/Διεύθυνση Ηλεκτρονικού Εγκλήματος, διεξήγαγε συνεδριάσεις μέσω τηλεδιασκέψεων με σχολικές μονάδες πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, με τίτλο «Ασφαλής πλοήγηση στο Διαδίκτυο».

Στο πλαίσιο του eTwinning

l. Webinar με θέμα την ασφάλεια στο Διαδίκτυο και το eTwinning (www.youtubexom/watch?v=bMirHUp8NEQ&feature=voutu.be)

2. Πλήρης παρουσίαση της διάσκεψης «e2 (twinning + safety): Μια υπεύθυνη και ασφαλής συνεργασία» (http://conf2014.etwinning.gr/index.php/2014-06-02-15-21-07)

3. Μάθημα στην πλατφόρμα eTwinning με θέμα «Τα πνευματικά δικαιώματα και η σημασία αναφοράς των πηγών που χρησιμοποιούμε στο Διαδίκτυο», που προορίζεται για διδακτικό προσωπικό πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης (2014) και περιλαμβάνεται στα ηλεκτρονικά μαθήματα της Ελληνικής Υπηρεσίας Υποστήριξης (ΕΥΥ) του eTwinning, με σκοπό τη διερεύνηση των τρόπων αξιοποίησης του διαδικτυακού υλικού, το οποίο υπόκειται στους ίδιους κανόνες που αφορούν τα πνευματικά δικαιώματα γενικότερα, χωρίς να παραβιάζονται τα δικαιώματα αυτά σε e-Twinning projects.

4. Πολλά ελληνικά σχολεία έχουν εταιρικές σχέσεις με σχολεία της αλλοδαπής για θέματα εκφοβισμού και γενικά θέματα ασφάλειας στο Διαδίκτυο.

Στο πλαίσιο του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (Ε.Σ.Π.Α.)

l. Πράξη «Ολοκληρωμένες υπηρεσίες ενίσχυσης ψηφιακής εμπιστοσύνης»

Η πράξη «Ολοκληρωμένες υπηρεσίες ενίσχυσης ψηφιακής εμπιστοσύνης», στο πλαίσιο του Επιχειρησιακού Προγράμματος Ψηφιακής Σύγκλισης (Έναρξη: 1/10/2009 - Τέλος: 10/31/2015). Με την πράξη επιδιώκεται να καλυφθούν θέματα ασφάλειας και εμπιστοσύνης όσον αφορά τις Τεχνολογίες Πληροφοριών και Επικοινωνιών στην Εκπαίδευση, με έμφαση στην παραγωγή πληροφοριών και εκπαιδευτικών υπηρεσιών/περιεχομένου, καθώς και στην παραγωγή υπηρεσιών ψηφιακής ασφάλειας και εμπιστοσύνης. Η πράξη αποτελείται από δύο υποέργα:

Υποέργο 1: Πύλη Ψηφιακής Ασφάλειας και Ψηφιακή Ασφάλεια στην Πρώτη Γυμνασίου, που περιλαμβάνουν τα εξής:

Δραστηριότητα 1: Πύλη Ψηφιακής Ασφάλειας

Η πύλη αυτή, που απευθύνεται κυρίως σε μαθητές, γονείς και εκπαιδευτικούς (την εκπαιδευτική κοινότητα), επιδιώκει να αποτελέσει σημείο μεταφοράς και σημείο συνάντησης για τους χρήστες που ενδιαφέρονται για την ψηφιακή ασφάλεια και την αξιοπιστία στην εκπαίδευση.

Δραστηριότητα 2: Ψηφιακή Ασφάλεια στην Πρώτη Γυμνασίου

Στο πλαίσιο της δραστηριότητας 2 αναπτύσσονται α) μαθήματα εξ αποστάσεως (e-Learning) για την ψηφιακή ασφάλεια (με το κατάλληλο υλικό όσον αφορά την ασφάλεια του Διαδικτύου και τους κινδύνους χρήσης του Διαδικτύου και των υπολογιστών εν γένει) και β) ένα διαδραστικό εκπαιδευτικό παιχνίδι που περιλαμβάνει στο περιβάλλον του δραστηριότητες με στόχο την εξοικείωση των μαθητών με δυνητικούς κινδύνους από τη χρήση των υπολογιστών και του Διαδικτύου.

Υποέργο 2: Υπηρεσίες Ψηφιακής Ασφάλειας, που περιλαμβάνει τα εξής:

Δραστηριότητα Α: «Σύστημα Έγκαιρης Προειδοποίησης για κινδύνους στο Διαδίκτυο» (PROTOS) [protos.cti.gr]

Αυτό το σύστημα έγκαιρης προειδοποίησης για κυβερνοεπιθέσεις (Σύστημα Ανίχνευσης Εισβολών) είναι διαθέσιμο για MS Windows και Linux (Ubuntu) και αναμένεται να αποκτήσει πάνω από 100.000 χρήστες.

Δραστηριότητα Β: «Έλεγχος Ασφάλειας Υπολογιστών» (Διανομή Ασφάλειας) [secure-distro.cti.gr]

Αφορά την παρακολούθηση των εφαρμογών που εγκαθίστανται σε υπολογιστές με λειτουργικό Ubuntu (14.04), με στόχο τη δημιουργία ασφαλούς περιβάλλοντος για τους μαθητές της δευτεροβάθμιας εκπαίδευσης.

2. Δράση «Καλέστε έναν Ειδικό για το Ασφαλές Διαδίκτυο»

Προκειμένου να παρασχεθεί στα σχολεία ένα μοντέλο ασφαλούς πλοήγησης στο Διαδίκτυο και να αποκτήσουν οι μαθητές τις απαιτούμενες δεξιότητες ώστε να χρησιμοποιούν με ασφάλεια και υπευθυνότητα το Διαδίκτυο, το Υπουργείο Πολιτισμού, Παιδείας και Θρησκευμάτων (ΥΠΟΠΑΙΘ), μέσω του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ), λειτουργεί τον ενημερωτικό κόμβο «Ασφάλεια στο Διαδίκτυο» http://internet-safetv.sch.gr, ο οποίος παρέχει αξιόπιστες στοχευμένες πληροφορίες και στήριξη καθώς και ποιοτικό εκπαιδευτικό υλικό σε μαθητές, εκπαιδευτικούς και γονείς.

Επιπλέον, το ΠΣΔ, ως εθνικός συντονιστής της δράσης eSafety Label http://www.esafetylabel.eu/) του Ευρωπαϊκού Σχολικού Δικτύου (EUN), παρέχει στα ελληνικά σχολεία μια ειδική πιστοποίηση, με στόχο τη στήριξή τους κατά τη διαμόρφωση μιας πολιτικής Ασφαλέστερου Διαδικτύου και την παροχή ασφαλέστερου διαδικτυακού περιβάλλοντος σε εκπαιδευτικούς και μαθητές. Μέσω ειδικά σχεδιασμένης διαδικασίας πιστοποίησης εξετάζονται οι παράγοντες εκείνοι που είναι δυνατόν να επηρεάσουν το επίπεδο της διαδικτυακής ασφάλειας. Βάσει συγκεκριμένων αποτελεσμάτων διαμορφώνεται για κάθε σχολείο ειδικό σχέδιο δράσης για την ασφάλεια στο Διαδίκτυο. Πέραν των ανωτέρω, το ΠΣΔ δημιούργησε τη νέα δράση «Καλέστε έναν Ειδικό για το Ασφαλές Διαδίκτυο»

http://internet-safety.sch.gr/call-an-expert, που προσφέρει στα σχολεία τη δυνατότητα να προσκαλούν έναν ειδικό καταρτισμένο σε θέματα ασφαλούς Διαδικτύου, προκειμένου να υλοποιηθεί μια διά ζώσης ενημέρωση και εκπαίδευση στη σχολική κοινότητα. Το σώμα των ειδικών αποτελείται από ειδικά εκπαιδευμένους και πιστοποιημένους εκπαιδευτικούς και στελέχη της εκπαίδευσης.
Τα σχολεία που συμμετείχαν στη δράση «Καλέστε έναν Ειδικό για το Ασφαλές Διαδίκτυο» έκριναν ότι αυτή ήταν απλή και φιλική προς τον χρήστη. Τα ενδιαφερόμενα σχολεία μπορούν να υποβάλουν το αίτημα συμμετοχής τους μέσω του http://internet-safety.sch.gr/call-an-expert.

Μετά την ολοκλήρωση της εκπαίδευσης θα συμπληρώσουν ερωτηματολόγιο με σχετικές παρατηρήσεις και υποδείξεις για τη γενική βελτίωση στης δράσης. Ο ειδικός θα υποβάλει επίσης σύντομη ενημερωτική έκθεση με απλά στατιστικά στοιχεία, όπως η ημερομηνία κατά την οποία πραγματοποιήθηκε η εκπαίδευση, ο αριθμός των μαθητών που εκπαιδεύτηκαν κ.λπ.

Η δράση αυτή θα πραγματοποιείται χωρίς κόστος για τα σχολεία ή το ΥΠΟΠΑΙΘ, καθώς όλοι οι συντελεστές της συμμετέχουν εθελοντικά.

Β) ΠΑΝΕΠΙΣΤΗΜΙΑ

Τα ακόλουθα μαθήματα και δράσεις στα προγράμματα σπουδών της ανώτατης εκπαίδευσης παρατίθενται ενδεικτικά:

- Στο πρόγραμμα σπουδών του **Τμήματος Τεχνών Ήχου και Εικόνας του Ιονίου Πανεπιστημίου** περιλαμβάνεται το μάθημα επιλογής «Διαδικτυακή Επικοινωνία». Στο μάθημα αυτό διδάσκονται και συζητούνται, υπό την ευρεία έννοια και από θεωρητική και τεχνική άποψη, θέματα σχετικά με την ασφάλεια του Διαδικτύου και το έγκλημα στον κυβερνοχώρο.

- Στην **Παιδαγωγική Σχολή του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης,** προσφέρονται τα ακόλουθα μαθήματα:

α) Στο Παιδαγωγικό Τμήμα Δημοτικής Εκπαίδευσης το μάθημα επιλογής του 5ου εξαμήνου των προπτυχιακών σπουδών με τίτλο: «Ψηφιακός Γραμματισμός» (Κωδικός μαθήματος: Ε44). Το 1/3 περίπου του μαθήματος ασχολείται με την καλλιέργεια στάσεων και αντιλήψεων απέναντι στα ψηφιακά και ηλεκτρονικά ΜΜΕ και την ευαισθητοποίηση σε σχέση με τα κοινωνικά, ηθικά, νομικά και ανθρώπινα ζητήματα της αξιοποίησης των ΤΠΕ στην καθημερινή ζωή. Στο πλαίσιο αυτό υπάρχουν σαφείς και αδιαμφισβήτητες αναφορές στο φαινόμενο του ηλεκτρονικού εκφοβισμού ή εκφοβισμού μέσω του Διαδικτύου και εξετάζονται διάφορα θέματα σχετικά με το έγκλημα και την ασφάλεια στο Διαδίκτυο.

β) Στο Τμήμα Επιστημών Προσχολικής Αγωγής και Εκπαίδευσης προσφέρονται οι «Τεχνολογίες της Πληροφορίας και της Επικοινωνίας στη Διδασκαλία και τη Μάθηση» ως μάθημα βάσης, που θα περιλαμβάνει ενότητες σχετικά με την ασφάλεια και το έγκλημα στο Διαδίκτυο, τον ηλεκτρονικό εκφοβισμό και γενικά την προστασία της ιδιωτικής ζωής.

- Στο Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου της Κρήτης διδάσκονται τα ακόλουθα δύο μαθήματα (ένα προπτυχιακό και ένα μεταπτυχιακό) όσον αφορά την ασφάλεια στο Διαδίκτυο: - Εισαγωγή στα Συστήματα Ασφάλειας Υπολογιστών (προπτυχιακό μάθημα του 4ου έτους). Προσφέρεται κάθε ακαδημαϊκό έτος κατά το χειμερινό εξάμηνο

- Ασφαλή Συστήματα (μεταπτυχιακό μάθημα που προσφέρεται κάθε ακαδημαϊκό έτος κατά το εαρινό εξάμηνο)

Το Τμήμα Επιστήμης Υπολογιστών συμμετέχει επίσης στη διοργάνωση διαλέξεων, σεμιναρίων και θερινών σχολείων σε συνεργασία με το Ίδρυμα Τεχνολογίας και Έρευνας (FORTH) και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) όσον αφορά την ασφάλεια στο Διαδίκτυο και την πρόληψη της εγκληματικής δραστηριότητας στον κυβερνοχώρο. Στις δράσεις αυτές μπορούν να συμμετέχουν οι μεταπτυχιακοί και προπτυχιακοί φοιτητές του τμήματος.

- Στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών προσφέρονται μαθήματα σχετικά με το έγκλημα στον κυβερνοχώρο και την ασφάλεια στο Διαδίκτυο, όπως: η «Ασφάλεια Πληροφοριακών Συστημάτων» με διδάσκοντα τον καθηγητή Δ. Γκρίτζαλη.
Ο καθηγητής του τμήματος Δ. Γκρίτζαλης διοργανώνει τακτικά 2-3 φορές το χρόνο προγράμματα ενημέρωσης και ευαισθητοποίησης σχετικά με τις απειλές και την πρόληψη της εγκληματικής δραστηριότητας στον κυβερνοχώρο, τα οποία μπορεί να παρακολουθήσει το ευρύτερο κοινό, υπό την αιγίδα του Οικονομικού Πανεπιστημίου Αθηνών.

- Σχολή Οικονομίας, Διοίκησης και Νομικών Επιστημών (ΣΟΔΝΕ) του Διεθνούς Πανεπιστημίου της Ελλάδος (ΔιΠαΕ)

α) Το έγκλημα στον κυβερνοχώρο και η ασφάλεια στο Διαδίκτυο περιλαμβάνονται στο πρόγραμμα σπουδών στο πλαίσιο του μαθήματος επιλογής «Δίκαιο του Διαδικτύου και Ηλεκτρονικό Επιχειρείν» του Προγράμματος Μεταπτυχιακών Σπουδών (ΠΜΣ) «LLM in in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law» («LLM στο Διεθνικό και Ευρωπαϊκό Οικονομικό Δίκαιο, Διαμεσολάβηση, Διαιτησία και Δίκαιο Ενέργειας» της Σχολής Οικονομίας, Διοίκησης και Νομικών Επιστημών του ΔιΠαΕ.

β) Στο πλαίσιο του εν λόγω ΠΜΣ, στις 22/11/2013 έλαβε χώρα στο ΔιΠαΕ Διεθνές Συνέδριο με αντικείμενο την «Ασφάλεια του Διαδικτύου και Ασφάλεια στο Διαδίκτυο».

- Σχολή Επιστημών και Τεχνολογίας (ΣΕΤ) του Διεθνούς Πανεπιστημίου της Ελλάδος.

α) Η Σχολή Επιστημών και Τεχνολογίας προσφέρει τα πέντε τελευταία ακαδημαϊκά έτη το ΠΜΣ «Συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών», υποχρεωτικό μάθημα σχετικά με την Ασφάλεια των Πληροφορικών Συστημάτων, που περιγράφει τα διάφορα είδη κυβερνοαπειλών και τις πρακτικές αντιμετώπισής τους. Το πρόγραμμα σπουδών περιλαμβάνει ευρύ φάσμα αντικειμένων, τεχνικές (ασφάλεια του Διαδικτύου, βάσεις δεδομένων, κρυπτογραφία κ.λπ.), διαχείριση (διαχείριση της ασφάλειας, σχεδιασμός συνέχειας της επιχειρηματικής δραστηριότητας, ασφάλεια λογισμικού, ανάλυση και διαχείριση κινδύνων κ.λπ.), καθώς και νομικά και δεοντολογικά θέματα.

β) Η ΣΕΤ, αναγνωρίζοντας την ανάγκη της αγοράς και της κοινωνίας για κυβερνοασφάλεια, από το 2015-16 έχει προγραμματίσει να προσφέρει κατά το επόμενο ακαδημαϊκό έτος το ΠΜΣ «Τηλεπικοινωνίες και Κυβερνοασφάλεια», που θα περιλαμβάνει μαθήματα όπως το Έγκλημα στον Κυβερνοχώρο και η Ηλεκτρονική Εγκληματολογία (Computer Forensics), καθώς και οι Νομικές και Δεοντολογικές Βάσεις της Προστασίας της Ιδιωτικής Ζωής και της Ασφάλειας.
Η ΣΕΤ σχεδιάζει σχετικές εκδηλώσεις, διαλέξεις και εκπαιδευτικά σεμινάρια, ώστε να ευαισθητοποιηθούν η κοινωνία και οι επιχειρήσεις σε θέματα κυβερνοασφάλειας.

- Ελληνικό Ανοικτό Πανεπιστήμιο. Σχολή Θετικών Επιστημών και Τεχνολογίας
Κατά τις προπτυχιακές σπουδές διδάσκονται το Έγκλημα στον Κυβερνοχώρο και η Ασφάλεια στο Διαδίκτυο. Τα δύο αντικείμενα περιλαμβάνονται στο μάθημα «Πληροφορική», στο πλαίσιο της «Προστασίας και Ασφάλειας Συστημάτων Υπολογιστών». Οι φοιτητές προσκαλούνται επίσης να συμμετέχουν σε σχετικές εκδηλώσεις.

- Πανεπιστήμιο Δυτικής Μακεδονίας
α) Στο Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών της Πολυτεχνικής Σχολής, διδάσκεται το μάθημα «Ασφάλεια Υπολογιστών και Δικτύων». Στο σχετικό πρόγραμμα σπουδών περιλαμβάνονται το έγκλημα στον κυβερνοχώρο και η ασφάλεια του Διαδικτύου,
β) Στο Παιδαγωγικό Τμήμα Νηπιαγωγών, τα προπτυχιακά μαθήματα «Πληροφορική και ΤΠΕ στην Εκπαίδευση», «Νέες Τεχνολογίες και Καλλιτεχνική Δημιουργία», «Ανάπτυξη Εκπαιδευτικού Λογισμικού», «Λογοτεχνία» και «Εκπαιδευτική Πολιτική», καθώς και τα μεταπτυχιακά μαθήματα «ΤΠΕ στη Διδασκαλία και τη Μάθηση» και «Ψηφιακή Αφήγηση» περιέχουν αναφορές στο έγκλημα στον κυβερνοχώρο και την ασφάλεια του Διαδικτύου.

Επίσης ενδιαφέρουσα είναι η προσπάθεια που καταβάλλεται στο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Θεσσαλίας από τον Δρα Βασίλη Βλάχο στο πλαίσιο του έργου OWASP Hackademic Challenges, όπου οι φοιτητές καλούνται να σκεφτούν σαν επιτιθέμενοι προκειμένου να κατανοήσουν την τρωτότητα των υπαρχόντων πληροφοριακών συστημάτων όταν αυτά δεν έχουν ασφαλιστεί επαρκώς.

8.2. Ευαισθητοποίηση

Α) ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

Το Διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο, το οποίο επιτρέπει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ οποιωνδήποτε σημείων στον πλανήτη. Έχει χαρακτηριστεί ως η μεγαλύτερη εφεύρεση όλων των εποχών, κατακτώντας ολόκληρη την υφήλιο μέσα σε μόλις μερικές δεκαετίες ζωής, αποτελώντας πλέον τη μεγαλύτερη οργανωμένη κοινωνία παγκοσμίως. Αποτελεί μια παράλληλη, «εικονική» παγκόσμια κοινότητα, η οποία καταλύει όλες τις κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν.

Σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης και επικοινωνίας, καθιστά δυνατή τη ζωντανή αμφίδρομη επικοινωνία και δίνει τη δυνατότητα της άμεσης συμμετοχής σε όλους τους χρήστες με την ελεύθερη επιλογή λήψης, παροχής και διάχυσης της πληροφορίας. Καταργώντας τα σύνορα και μηδενίζοντας τις αποστάσεις, το Διαδίκτυο φαίνεται πλέον σαφώς να «γέρνει τη ζυγαριά» προς τη μεριά των επικοινωνιών στην αιώνια διαμάχη μεταξύ μεταφορών και επικοινωνιών.

Με βάση τις προηγούμενες εξελίξεις και την τάση για ανάπτυξη, αναμένουμε ότι το μέλλον θα μας παρουσιάσει νέες καινοτόμες λύσεις και υπηρεσίες. Στο πλαίσιο των μελλοντικών εξελίξεων, το Αρχηγείο της Ελληνικής Αστυνομίας έχει αναπτύξει διάφορες καινοτόμες δράσεις με στόχο την ενημέρωση των πολιτών για τους κινδύνους που ελλοχεύουν κατά την πλοήγησή τους στο Διαδίκτυο και για τους τρόπους αποφυγής τους. Όλες οι καινοτόμες δράσεις που περιγράφονται αναλυτικά κατωτέρω εφαρμόζονται από το εξειδικευμένο προσωπικό της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, ενώ οι δαπάνες εφαρμογής καλύπτονται από χορηγίες εταιρειών του τομέα της πληροφορικής και των επικοινωνιών που ενδιαφέρονται ιδιαίτερα για θέματα όπως η Ασφαλής Πλοήγηση, χωρίς επιβάρυνση του κρατικού προϋπολογισμού.

<u>Ημερίδες Ασφαλούς Πλοήγησης</u>

Το Αρχηγείο της Ελληνικής Αστυνομίας, μέσω της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, διοργανώνει ημερίδες σε όλη την Ελληνική Επικράτεια, έχοντας ως στόχο την ενημέρωση μαθητών, γονέων και εκπαιδευτικών για τα φαινόμενα διαδικτυακής βίας, τους κινδύνους που ελλοχεύουν στις ιστοσελίδες κοινωνικής δικτύωσης και γενικά την πρόληψη και την αντιμετώπιση των κινδύνων που σχετίζονται με τις νέες τεχνολογίες.

Αναφέρεται χαρακτηριστικά ότι έχουν διοργανωθεί 132 ενημερωτικές ημερίδες σε διάφορες ελληνικές πόλεις (Αθήνα, Θεσσαλονίκη, Πρέβεζα, Ηγουμενίτσα, Τρίπολη, Ρόδο, Ηράκλειο Κρήτης, Χανιά) από το έτος 2011 έως σήμερα, ενώ κατά την περίοδο αυτή έχουν υποβληθεί 515 αιτήματα για διεξαγωγή ημερίδων από διάφορους φορείς (τοπική αυτοδιοίκηση, συλλόγους γονέων και κηδεμόνων, σχολεία κ.λπ.), πράγμα που αποδεικνύει το έντονο ενδιαφέρον των πολιτών για ενημέρωση όσον αφορά θέματα κινδύνου στο Διαδίκτυο.

Διοργάνωση συνεδρίων σε πανευρωπαϊκό επίπεδο

Κατά τα έτη 2012 έως και 2015, με αφορμή τον εορτασμό της Παγκόσμιας Ημέρας Ασφαλούς Πλοήγησης στο Διαδίκτυο, πραγματοποιήθηκαν από τη ΔΙ.Δ.Η.Ε. τέσσερα (4) συνέδρια σχετικά με Ασφαλή Πλοήγηση στο Διαδίκτυο, τα οποία περιλάμβαναν παρουσιάσεις από διακεκριμένους και εξειδικευμένους, σε θέματα που αφορούν στην Ασφαλή Πλοήγηση στο Διαδίκτυο, επιστήμονες της Ελλάδας και του εξωτερικού. Στα συνέδρια αυτά, τα θέματα που εξετάστηκαν αφορούσαν τις μελλοντικές εξελίξεις σε θέματα Διαδικτύου, καθώς και σχετικά με τη νομοθεσία που διέπει το έγκλημα στον κυβερνοχώρο. Τα συνέδρια ήταν ανοιχτής δομής και επικοινωνίας, δεδομένου ότι μεταδίδονταν μέσω Διαδικτύου, με εφαρμογές live-streaming, από τον ιστότοπο της Ελληνικής Αστυνομίας.

Αναλυτικότερα:

- *1ο Συνέδριο Ασφαλούς Πλοήγησης, την Τετάρτη 8 Φεβρουαρίου 2012 στο Divani Caravel*

Η διοργάνωση περιελάμβανε τρεις (3) ενότητες, οι οποίες διεξήχθησαν παράλληλα σε διαφορετικές αίθουσες, και παρουσιάστηκαν τα ακόλουθα θέματα:

- Τα θετικά του Διαδικτύου, που περιλάμβανε ανάλυση και συζήτηση σχετικά με τα πλεονεκτήματα που έφεραν το Διαδίκτυο και οι νέες τεχνολογίες στην καθημερινότητα των ανθρώπων. Επιπλέον, παρουσιάστηκαν νέα πληροφοριακά συστήματα που συμβάλλουν στη δημιουργία και ενίσχυση της καινοτομικής επιχειρηματικότητας.
- Εθισμός στο Διαδίκτυο, που περιλάμβανε την ανάλυση και την προβολή κινδύνων που ενέχει η αλόγιστη χρήση του Διαδικτύου, σε ψυχολογικό και σωματικό επίπεδο.
- Νομική Προσέγγιση και Ασφαλής Πλοήγηση, που περιλάμβανε την ενημέρωση των εκπροσώπων των Εισαγγελικών και Δικαστικών Αρχών, καθώς και των νομικών γύρω από τις νέες τεχνολογίες και το ηλεκτρονικό έγκλημα καθόσον το παραδοσιακό έγκλημα έχει μεταλλαχθεί σε ηλεκτρονικό και μάλιστα σε ποσοστό πάνω από 82%.

2ο Συνέδριο Ασφαλούς Πλοήγησης, την Πέμπτη 7 Φεβρουαρίου 2013 στο Athenaum Intercontinental

Η διοργάνωση περιελάμβανε τρεις (3) ενότητες, οι οποίες διεξήχθησαν παράλληλα σε διαφορετικές αίθουσες, και παρουσιάστηκαν τα ακόλουθα θέματα:

- **Ασφάλεια Ηλεκτρονικών Πληροφοριών** – Βιομηχανική Κατασκοπεία. Σκοπός της ενότητας αυτής ήταν η παρουσίαση του προβλήματος της ασφάλειας των ηλεκτρονικών πληροφοριών και συγκεκριμένα του φαινομένου της ηλεκτρονικής Βιομηχανικής Κατασκοπείας. Το ακροατήριο αποτελείτο από εκπροσώπους επιχειρήσεων, επιχειρηματίες καθώς και διευθύνοντες σύμβουλους εταιρειών. Οι ομιλητές που ανέπτυξαν τη θεματολογία αυτή ήταν καθηγητές πανεπιστημίου και διακεκριμένες προσωπικότητες του χώρου.
- **Έγκλημα στον κυβερνοχώρο και νομοθεσία** – Κραυγές απόγνωσης-πρόληψη αυτοκτονιών. Στόχος της ενότητας αυτής ήταν να ενημερωθούν οι εισαγγελικές αρχές και κατ' επέκταση οι νομικοί σχετικά με την ορολογία του Διαδικτύου, τη μετάλλαξη του παραδοσιακού-συμβατικού εγκλήματος σε ηλεκτρονικό και το ανησυχητικό πλέον φαινόμενο που συνδέεται με τις απόπειρες αυτοκτονίας. Το ακροατήριο αποτελείτο από δικαστές, εισαγγελείς, καθηγητές συναφών επιστημών, δικηγόρους, φοιτητές Νομικής και δόκιμους αξιωματικούς των Παραγωγικών Σχολών των Ε.Δ. και Σωμάτων Ασφαλείας. Οι ομιλητές που ανέπτυξαν τη θεματολογία αυτή ήταν καθηγητές πανεπιστημίου συναφών επιστημών και εκπρόσωποι των δικαστικών αρχών και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
- **Ηλεκτρονικός εκφοβισμός (cyber bullying).** Σκοπός της ενότητας αυτής ήταν να προβληματίσει και να ενεργοποιήσει προς την κατεύθυνση άμβλυνσης των συνεπειών από τη ψυχοσωματική βία και τον εκφοβισμό που ασκείται στα παιδιά μέσω του Διαδικτύου. Το ακροατήριο αποτελείτο από τριακόσια πενήντα (350) παιδιά – μαθητές 3ης τάξης δημοτικού μέχρι 3ης τάξης γυμνασίου, από δημόσια και ιδιωτικά σχολεία της Αττικής. Οι ομιλητές που ανέπτυξαν το θέμα αυτό, λόγω της ιδιαιτερότητας του, ήταν καθηγητές πανεπιστημίου ειδικευμένοι σε θέματα εφηβικής υγείας, κλινικοί ψυχολόγοι, παιδαγωγοί και εκπαιδευτικοί.

Κατά την έναρξη των εργασιών του Συνεδρίου προβλήθηκε οπτικοακουστικό υλικό που εστάλη για τις ανάγκες του συνεδρίου από την ευρωπαία Επίτροπο, υπεύθυνη για την Ψηφιακή Ατζέντα της Ευρωπαϊκής Ένωσης, κα Neelie Kroes, ειδικά για το Αρχηγείο της Ελληνικής Αστυνομίας και τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

3ο Συνέδριο Ασφαλούς Πλοήγησης, την Πέμπτη 6 Φεβρουαρίου 2014 στο Athenaum Intercontinental

Συγκεκριμένα, οι δύο θεματικές ενότητες που αναπτύχθηκαν ήταν οι ακόλουθες:

- **«Οι δράσεις της Ελληνικής Αστυνομίας σχετικά με το Διαδίκτυο»**, κατά την οποία παρουσιάσθηκε το πρόγραμμα των δράσεων στο πεδίο ενημέρωσης μαθητών, γονέων και άλλων ενδιαφερόμενων φορέων, για τα θετικά και αρνητικά του Διαδικτύου και συνακόλουθα τους κινδύνους που ελλοχεύουν κατά την πλοήγησή τους σε αυτό. Κατά τη διάρκεια της ενότητας αυτής, παρουσιάστηκε το έργο της Ελληνικής Αστυνομίας στον τομέα αυτό μέχρι και σήμερα, καθώς επίσης και το πρόγραμμα των μελλοντικών δράσεων για το 2014. Επιπλέον, προβλήθηκε το τηλεοπτικό «σποτ» της νέας εκστρατείας ενημέρωσης για το 2014.
- «**Το Διαδίκτυο στη ζωή μας»:** τι μέλλει γενέσθαι, στο πλαίσιο της οποίας αναπτύχθηκαν οι δυνατότητες που παρέχονται μέσω του Διαδικτύου, αποτελώντας πηγή γνώσης, μάθησης, επικοινωνίας, διασκέδασης, ενημέρωσης, ενώ σκοπός της ενότητας αυτής ήταν να αναδειχθεί η σημαντικότητα του Διαδικτύου στην καθημερινότητα του σύγχρονου ανθρώπου.

4ο Συνέδριο Ασφαλούς Πλοήγησης, την Παρασκευή 13 Φεβρουαρίου 2015 στο Μέγαρο Μουσικής Αθηνών

Η εκδήλωση περιλάμβανε δύο (2) θεματικές ενότητες και συγκεκριμένα τις εξής:

- **«Το λόγο έχουν τα παιδιά μας!»** Στο συνέδριο αυτό το λόγο είχαν τα παιδιά, που ενημέρωσαν τους συμμαθητές τους για το Διαδίκτυο και τους κινδύνους του, προκειμένου αυτοί με τη σειρά τους να μεταφέρουν τις χρήσιμες πληροφορίες και τη γνώση που απέκτησαν στους φίλους τους, αλλά και στους γονείς τους. Τονίστηκε ότι το Διαδίκτυο είναι «ΦΩΣ», καθώς έχει μόνο 2% αρνητικά και 98% θετικά. Για τα αρνητικά, τα παιδιά μπορούν να απευθύνονται στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, μέσω του τηλεφωνικού αριθμού 11188 ή του CyberAlert.

- Το Διαδίκτυο στη ζωή μας, στο πλαίσιο της οποίας αναπτύχθηκαν οι δυνατότητες που παρέχονται μέσω του διαδικτύου, αποτελώντας πηγή γνώσης, μάθησης, επικοινωνίας, διασκέδασης, ενημέρωσης. Σκοπός της ενότητας ήταν να αναδειχθεί η σημαντικότητα του Διαδικτύου στην καθημερινότητα του σύγχρονου ανθρώπου.

Συνέδριο στο Μέγαρο Μουσικής Αθηνών για μαθητές του Ειδικού Γυμνασίου-Λυκείου Αθηνών και του Ειδικού Γυμνασίου-Λυκείου Ιλίου: Το συνέδριο πραγματοποιήθηκε την Τετάρτη 17 Δεκεμβρίου στο Μέγαρο Μουσικής Αθηνών και το ακροατήριο αποτελείτο από περίπου εκατό (100) μαθητές του Ειδικού Γυμνασίου -Λυκείου Αθηνών και του Ειδικού Γυμνασίου-Λυκείου Ιλίου, με τους συνοδούς εκπαιδευτικούς. Στόχος του ήταν η ενημέρωση της ευαίσθητης ομάδας των παιδιών, για τους κινδύνους που κρύβει το διαδίκτυο και για τους τρόπους αντιμετώπισης των προκλήσεων του ψηφιακού κόσμου, καθώς είναι ύψιστης σημασίας η ισότιμη συμμετοχή των μαθητών αυτών στην κοινωνία της γνώσης και των σύγχρονων τεχνολογιών.

-Ημερίδα για την παρουσίαση του ιστοτόπου www.cyberkid.gr: Η ημερίδα πραγματοποιήθηκε την Τετάρτη 7 Μαΐου 2014 στο ξενοδοχείο Intercontinental. Το ακροατήριο αποτελείτο από περίπου 1.000 μαθητές, από όλες τις σχολικές βαθμίδες, με τους συνοδούς εκπαιδευτικούς. Στην ημερίδα παρουσιάστηκε η νέα ενότητα του ιστοτόπου www.cyberkid.gr, η οποία ονομάζεται «Ψηφιακή Αλάνα» και περιλαμβάνει την ψηφιοποίηση δεκαέξι παραδοσιακών παιχνιδιών (γκρινιάρης, σκάκι, ντάμα κ.α.), τα οποία είναι προσβάσιμα σε όλους τους επισκέπτες ανάλογα με την ηλικία τους.

-**Έκδοση πρακτικών συνεδρίων:** Μετά την ολοκλήρωση τεσσάρων συνεδρίων η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προχώρησε στην έκδοση των πρακτικών των συνεδρίων σε έντυπη και ηλεκτρονική μορφή, μέσα από τα οποία δίνεται η δυνατότητα στους πολίτες να ενημερωθούν αναλυτικά για τις εισηγήσεις που πραγματοποιήθηκαν στα συνέδρια.

Τηλεδιασκέψεις με σχολικές μονάδες

Πραγματοποιούνται, κάθε εβδομάδα (Τρίτη και Πέμπτη), με ιδιαίτερη επιτυχία ενημερώσεις σε σχολεία ανά την επικράτεια, μέσω της υιοθέτησης της τεχνολογίας των τηλεδιασκέψεων με παράλληλη σύνδεση σε πολλαπλά σημεία. Η τηλεδιάσκεψη γίνεται σε πραγματικό χρόνο και επιτρέπει να πραγματοποιηθούν παρουσίαση, συνομιλία, ερωτήσεις και απαντήσεις μεταξύ ομιλητών και ακροατών που βρίσκονται σε απόσταση.

Τα σχολεία που συμμετέχουν στην τηλεδιάσκεψη δέχονται πρόσκληση μέσω του συστήματος «meetings.sch.gr», του Πανελλήνιου Σχολικού Δικτύου. Με τον τρόπο αυτό, εντάσσονται στην τηλεδιάσκεψη.

Από την αρχή της σχολικής χρονιάς έως σήμερα η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συνδέθηκε μέσω πολλαπλών τηλεδιασκέψεων με 5.225 σχολεία σε όλη τη χώρα, ενώ ο στόχος είναι, μέχρι το τέλος της σχολικής χρονιάς, οι μαθητές όλων των σχολείων της επικράτειας να έχουν ενημερωθεί για την ασφαλή πλοήγηση στο Διαδίκτυο και για τους τρόπους με τους οποίους μπορούν να αντιμετωπίσουν τους κινδύνους του.

- Τηλεοπτικά «σποτ»: Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προχώρησε στην παραγωγή και προβολή μέσω ραδιοφωνικών και τηλεοπτικών σταθμών πανελλαδικής εμβέλειας, τριών τηλεοπτικών «σποτ» στο πλαίσιο της εκστρατείας πληροφόρησης ευαίσθητων κοινωνικών ομάδων για την προστασία τους από τις παγίδες του Διαδικτύου. Μπορεί το Διαδίκτυο να έχει γίνει μέρος της καθημερινότητάς μας ωστόσο αυτό εγκυμονεί αρκετούς και σοβαρούς κινδύνους τόσο για εμάς όσο και για τα παιδιά. Πλέον οι μικροί μας φίλοι, μιμούμενοι τους γονείς, έχουν από μικρή ηλικία tablet, που έχει αντικαταστήσει δυστυχώς το παιχνίδι.

- Το πρώτο «σποτ» αφορά τους αόρατους κινδύνους του Διαδικτύου και παρουσιάσθηκε το 2010. Σκοπός είναι η αφύπνιση τόσο των παιδιών όσο και των γονιών, καθώς οι τελευταίοι αποτελούν το μοναδικό «τείχος» προστασίας των παιδιών απέναντι στα αρπακτικά. Οι γονείς πρέπει να βρίσκονται κοντά στα παιδιά τους και να συζητούν μαζί τους. Μόνο τότε το παιδί θα μπορέσει να μιλήσει για απειλές που το προσεγγίζουν.
- Το δεύτερο αφορά τον ηλεκτρονικό εκφοβισμό (cyberbullying) και παρουσιάσθηκε το 2014. Υπενθυμίζεται ότι, σύμφωνα με πρόσφατες έρευνες, 1 στους 20 μαθητές γυμνασίου έχει πέσει θύμα ηλεκτρονικού εκφοβισμού, ενώ το συγκεκριμένο ποσοστό διπλασιάζεται σχεδόν σε μαθητές που φοιτούν στις τάξεις του Λυκείου.

- Το τρίτο αφορά τους κινδύνους που κρύβουν οι επαφές με αγνώστους και παρουσιάσθηκε το 2014. Στόχος είναι να προστατευτούν τα παιδιά από τα λεγόμενα «αρπακτικά», που παραμονεύουν στο Διαδίκτυο με το μανδύα του «φίλου» ή του «συνομήλικου» και τους πιάνουν την κουβέντα για θέματα που τα αφορούν, ώστε να κερδίσουν την εμπιστοσύνη τους και στη συνέχεια να τα αποπλανήσουν.

- Συγγραφή και διαμοιρασμός ενημερωτικών φυλλαδίων:
Η ΔΙ.Δ.Η.Ε. έχει προβεί στην έκδοση ενημερωτικών φυλλαδίων με δέκα (10) διαφορετικές θεματικές ενότητες για την παροχή συμβουλών για ασφαλέστερη πλοήγηση στο Διαδίκτυο.

- Εκπαιδευτικές Επισκέψεις: Καθημερινά η ΔΙ.Δ.Η.Ε. γίνεται αποδέκτης πολλών αιτημάτων σχολείων και διάφορων φορέων που θέλουν να επισκεφτούν τις εγκαταστάσεις μας και να ενημερωθούν σε θέματα που αφορούν την ασφάλεια στο Διαδίκτυο. Μέχρι σήμερα, έχει δεχτεί 12 ενημερωτικές επισκέψεις (1ο ΓΕΛ Ελληνικού, 1ο Γυμνάσιο Ζωγράφου, Ερευνητικός Όμιλος Φοιτητών Νομικής, Εκπαιδευτήρια Δούκα, Κολέγιο Ψυχικού κ.λπ.).

- Συμμετοχή στο Πληροφοριακό Κέντρο της ΕΛ.ΑΣ. στη 79η ΔΕΘ: Περισσότεροι από 37.000 πολίτες επισκέφθηκαν το περίπτερο της Ελληνικής Αστυνομίας και ενημερώθηκαν σχετικά με την «Ασφαλή Διαδικτυακή Πλοήγηση», με αποτέλεσμα το περίπτερο να αποτελέσει σημαντικό πόλο έλξης. Τα διοικητικά στελέχη της Δ.Ε.Θ.– HELEXPO απένειμαν Αναμνηστικό Συμμετοχής στο Πληροφοριακό Κέντρο της Ελληνικής Αστυνομίας.

- Ιστότοπος «cyberkid.gr»: Στο www.cyberkid.gr παρέχονται χρήσιμες πληροφορίες και συμβουλές σχετικά με το πως μπορεί να εκμεταλλευτεί όλη η οικογένεια τα θετικά των σύγχρονων τεχνολογιών που μας περιβάλλουν και φυσικά του Διαδικτύου.
Στο πλαίσιο της συνεχούς ενημέρωσης και ανάπτυξης του ιστοτόπου www.cyberkid.gr, δημιουργήθηκε πρόσφατα η ενότητα «Ψηφιακή Αλάνα», όπου τα παιδιά μπορούν να παίζουν τα αγαπημένα τους ηλεκτρονικά παιχνίδια με απόλυτη προστασία από τους κινδύνους που παραμονεύουν στο Διαδίκτυο. Τα παιχνίδια, 31 στο σύνολό τους, έχουν σύγχρονα γραφικά και γρήγορη εξέλιξη ώστε να διατηρούν το ενδιαφέρον των παιδιών αμείωτο μέσα στην «Ψηφιακή Αλάνα».

Ακόμη, η ιστοσελίδα εμπλουτίστηκε με δυο καινούριες ενότητες. Την ενότητα «CyberAlert», όπου το κοινό μπορεί να ενημερωθεί για τους πιο συχνά εμφανιζόμενους κινδύνους που κυκλοφορούν στο Διαδίκτυο, και την ενότητα «Νέα», όπου αναρτώνται οι ανακοινώσεις που αφορούν τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

- Εφαρμογές Cyberkid για φορητές συσκευές (Apps): Η εφαρμογή Cyberkid για κινητά δημιουργήθηκε με σκοπό να ενημερώνει καθημερινά τους γονείς και τα παιδιά κάθε οικογένειας για την ασφαλή πλοήγηση στο Διαδίκτυο και τους κινδύνους που ελλοχεύουν σε αυτό. Παράλληλα, είναι μια διαδραστική εφαρμογή, η οποία δίνει τη δυνατότητα άμεσης επικοινωνίας με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος μέσω της γραμμής CYBER ALERT αλλά και μέσω αποστολής άμεσου μηνύματος e-mail, με τη χρήση ενός κουμπιού, ενώ υπάρχει η δυνατότητα ψυχαγωγίας μέσω των διάφορων παιχνιδιών.

- Σελίδα Cyberkid στο Facebook: Η Σελίδα του Cyberkid στο Facebook δημιουργήθηκε τον Μάιο του 2014 με σκοπό να ενισχύσει την προβολή του ιστοτόπου www.cyberkid.gr στα μέσα κοινωνικής δικτύωσης. Παρουσιάζει ιδιαίτερη απήχηση, καθώς 2.450 χρήστες του Facebook έχουν ήδη δηλώσει ότι τους «αρέσει» (like) και «ακολουθούν» τη δραστηριότητα της Σελίδας. Ακόμη πολλές φορές προβαίνουν σε κοινοποιήσεις των αναρτήσεών της, μέσω της πλατφόρμας του Facebook. Συνολικά έχουν πραγματοποιηθεί 108 αναρτήσεις στην ανωτέρω Σελίδα από την υπηρεσία.

- Λογαριασμός «@CyberAlertGR» στο Twitter: Τον Απρίλιο του 2015 ξεκίνησε η λειτουργία του λογαριασμού Twitter «@CyberAlertGR», που έχει ως στόχο την άμεση και σε πραγματικό χρόνο (real time) ενημέρωση των πολιτών για τους κινδύνους που ανακύπτουν καθημερινά στο Διαδίκτυο, ενώ ταυτόχρονα και οι ίδιοι θα μπορούν να ενημερώσουν τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος σε περίπτωση κινδύνου ή απειλής στο Διαδίκτυο.

Β) Ελληνική Ένωση Τραπεζών

Η Ελληνική Ένωση Τραπεζών, συμπληρωματικά προς τις ίδιες πρωτοβουλίες των τραπεζών που την απαρτίζουν, συμμετέχει στην ευαισθητοποίηση των πελατών των τραπεζών μέσω δημοσιεύσεων (ενημερωτικών δελτίων, δελτίων τύπου κ.λπ.) και της συμμετοχής της σε συγκεκριμένες θεματικές εκδηλώσεις και διαλέξεις.

Επιπλέον, σύμφωνα με τον καταστατικό της ρόλο, η ΕΕΤ ενημερώνει τα μέλη της για τις αντίστοιχες πρωτοβουλίες σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης, συντονίζει ειδικές παρουσιάσεις όσον αφορά θέματα ασφάλειας και προωθεί τις βέλτιστες διεθνείς και ευρωπαϊκές πρακτικές για την αντιμετώπιση του χρηματοπιστωτικού εγκλήματος στον κυβερνοχώρο.

Γ) ΓΕΕΘΑ/ΔΙΚΥΒ

Η ΔΙΚΥΒ συμβάλλει στην πρόληψη των κυβερνοεπιθέσεων, συντάσσοντας και διαθέτοντας στο ευρύ κοινό οδηγίες για ασφαλή παραμετροποίηση των πληροφοριακών συστημάτων. Παράλληλα, οργανώνει και διεξάγει εκπαιδευτικά προγράμματα τα οποία απευθύνονται στο προσωπικό των Ενόπλων Δυνάμεων και των δημόσιων φορέων. Η ΔΙΚΥΒ διοργανώνει σχολείο κυβερνοάμυνας (τεσσάρων εβδομάδων), όπου οι εκπαιδευόμενοι αποκτούν την δυνατότητα να κατανοήσουν τον τρόπο εντοπισμού και αντιμετώπισης των κυβερνοεπιθέσεων.

Δ) ΕΑΠΔΠΧ

Η ΕΑΠΔΠΧ, όπως έχει αναφερθεί ήδη, ασχολείται με την ευαισθητοποίηση, τόσο των υπευθύνων επεξεργασίας των δεδομένων όσο και των υποκειμένων των δεδομένων, σε θέματα σχετικά με την προστασία των δεδομένων και την προστασία της ιδιωτικής ζωής μέσω του ιστοτόπου της, της ετήσιας έκθεσης δραστηριοτήτων της η οποία δημοσιεύεται επίσης στον ιστότοπο αυτό, καθώς και των ομιλιών των ελεγκτών της.

Ε) «Το Χαμόγελο του Παιδιού»

Α. Οδυσσέας – 1ο Κινητό Εργαστήριο Ενημέρωσης, Εκπαίδευσης και Τεχνολογίας

Το «Χαμόγελο του Παιδιού», χρησιμοποιώντας την τεχνολογία, δημιούργησε ως κύριο εκπαιδευτικό «εργαλείο» τον «ΟΔΥΣΣΕΑ», το 1ο Κινητό Εργαστήριο Ενημέρωσης, Εκπαίδευσης και Τεχνολογίας. Ο «ΟΔΥΣΣΕΑΣ» αποτελεί ένα μοναδικό για τα ελληνικά δεδομένα «εργαλείο», με απόλυτη αυτονομία και εξοπλισμένο με: Τηλεφωνικό κέντρο, φωτοβολταϊκό σύστημα εναλλακτικής ενέργειας, δορυφορική κεραία για μεταφορά δεδομένων, 10 κάμερες εσωτερικά και εξωτερικά του οχήματος (εκ των οποίων 1 ρομποτική), 35 θέσεις εργασίας με πρόσβαση στο Διαδίκτυο, smart TVs, ηχεία εσωτερικά και εξωτερικά του οχήματος, φορητούς υπολογιστές (Laptops), Tablets και Smart phones.

Η μονάδα λειτουργεί υπό την αιγίδα του Υπουργείου Παιδείας και Θρησκευμάτων. Στο πλαίσιο της παροχής πληροφοριών σε μαθητές, γονείς και εκπαιδευτικούς στον «ΟΔΥΣΣΕΑ», η κύρια θεματική ενότητα είναι η Ασφαλής Χρήση του Διαδικτύου. Με τη χρήση διαδραστικών εργαλείων και ειδικευμένο επιστημονικό προσωπικό, ο «ΟΔΥΣΣΕΑΣ» προσφέρει γνώσεις σχετικά με την ασφαλή χρήση του Διαδικτύου, το έγκλημα στον κυβερνοχώρο και τους κινδύνους που πηγάζουν από την ανεύθυνη χρήση των μέσων κοινωνικής δικτύωσης. Ο «ΟΔΥΣΣΕΑΣ» έγινε πραγματικότητα χάρη στην ανεκτίμητη και πολύτιμη συνδρομή μερικών από τις μεγαλύτερες ελληνικές επιχειρήσεις, ιδίως από τον κλάδο των τηλεπικοινωνιών και των ΤΠΕ, όπως η Cisco, η Microsoft, η Hewlett Packard, η Dell, ο όμιλος OTE (Deutsche Telekom), η Dixons, η Vodafone, η Cyta, η Wind και άλλες.

Από τον Νοέμβριο του 2014 έως τον Μάρτιο του 2015 ο «ΟΔΥΣΣΕΑΣ» διοργάνωσε 160 παρεμβάσεις για 3.287 μαθητές σε όλη την Ελλάδα. Οι δραστηριότητες ευαισθητοποίησης του «ΟΔΥΣΣΕΑ» εμπίπτουν στην κατηγορία της πρόληψης του εγκλήματος στον κυβερνοχώρο μεταξύ μαθητών, γονέων και σχολικών κοινοτήτων (10. Α. Πρόληψη).

Β. YouSmile

Το YouSmile είναι ένα ασφαλές διαδραστικό διαδικτυακό περιβάλλον για εφήβους, που ενισχύει τις δεξιότητες και τις μαθησιακές δυνατότητες των μαθητών με τη χρήση νέων τεχνολογιών. Προωθεί επίσης την εθνική τηλεφωνική γραμμή για παιδιά SOS 1056 και την ευρωπαϊκή γραμμή για τα εξαφανισμένα παιδιά 116 000 και ενθαρρύνει τους νέους να τηλεφωνούν ή να επικοινωνούν μέσω του ηλεκτρονικού ταχυδρομείου με την εθνική τηλεφωνική γραμμή σε περίπτωση που αντιμετωπίζουν προβλήματα, επιθυμούν να καταγγείλουν κάποια πράξη ή ζητούν βοήθεια και συνδρομή ή χρειάζονται απλώς να μιλήσουν με κάποιον που θα τους ακούσει.

Το εργαλείο YouSmile περιλαμβάνει διαδραστικό ιστότοπο, διαδικτυακό ραδιόφωνο και διαδικτυακή τηλεόραση και αποτελεί μια διαδικτυακή πλατφόρμα διδασκαλίας που επιτρέπει την επιγραμμική ζωντανή επικοινωνία και δίνει στα παιδιά την ευκαιρία ενίσχυσης των μαθησιακών δεξιοτήτων τους και διάχυσης της γνώσης, ένα χώρο όπου τα παιδιά μπορούν να μοιραστούν τις ιδέες και τη δημιουργικότητά τους. Από την έναρξη λειτουργίας του YouSmile το 2012, 300 έλληνες έφηβοι από 27 σχολεία έχουν πάρει μέρος στις δραστηριότητές του. Το YouSmile επιδιώκει μεταξύ άλλων τη χειραφέτηση των μαθητών, την προαγωγή της διαδραστικής επικοινωνίας, την ευαισθητοποίηση σε διάφορα θέματα όπως η υπεύθυνη χρήση της τεχνολογίας και η παροχή ασφαλούς διαδικτυακού περιβάλλοντος στους εφήβους.

Το YouSmile αναγνωρίζεται επίσημα από το ελληνικό Υπουργείο Παιδείας και Θρησκευμάτων ως πλατφόρμα διδασκαλίας και ευαισθητοποίησης και φιλοδοξεί να επεκτείνει τις δραστηριότητές του σε όλη την Ευρώπη με τη μορφή Ευρωπαϊκού Εθελοντικού Δικτύου για τους Μαθητές. Περισσότερες πληροφορίες για το YouSmile μπορείτε να βρείτε στον ιστότοπο www.yousmile.gr.

Γ. «Ημέρα Ασφαλούς Διαδικτύου» από τη Microsoft Hellas και το «Χαμόγελο του Παιδιού»
Κάθε χρόνο, με την ευκαιρία της Ημέρας Ασφαλούς Διαδικτύου, μιας πρωτοβουλίας της Ευρωπαϊκής Ένωσης που δίνει έμφαση στην υπεύθυνη χρήση των επιγραμμικών τεχνολογιών, η Microsoft Hellas, σε συνεργασία με το «Χαμόγελο του Παιδιού», διοργανώνει μια ειδική εκδήλωση για την ευαισθητοποίηση των νέων σε θέματα ασφάλειας και ορθής χρήσης του Διαδικτύου.

Ο κύριος σκοπός αυτής της συνεργασίας είναι να εκπαιδευτούν τα παιδιά σχετικά με τους κινδύνους και να ενημερωθούν για την υπεύθυνη χρήση της τεχνολογίας. Η εκδήλωση αυτή αποτελεί ένα από τα καλύτερα παραδείγματα αποτελεσματικής συνεργασίας μεταξύ του ιδιωτικού τεχνολογικού κλάδου και μιας οργάνωσης για τα δικαιώματα του παιδιού στον τομέα της πρόληψης και ευαισθητοποίησης για ένα ασφαλές Διαδίκτυο.

Δ. Εκστρατεία ευαισθητοποίησης - Παγκόσμια Ημέρα ενάντια στην Παιδική Κακοποίηση
Με αφορμή τη 19η Νοεμβρίου, Παγκόσμια Ημέρα ενάντια στην Παιδική Κακοποίηση, και στο πλαίσιο των 19 Ημερών Ακτιβισμού κατά της Παιδικής Κακοποίησης (1-19 Νοεμβρίου) (Women's World Summit Foundation – WWSF), το «Χαμόγελο του Παιδιού» παρουσιάζει κάθε χρόνο στατιστικά στοιχεία και ευαισθητοποιεί το κοινό σχετικά με το φαινόμενο αυτό και τους κινδύνους για τα παιδιά. Πέρυσι (2014) η εκδήλωση αυτή έλαβε χώρα στη Θεσσαλονίκη, όπου ο «ΟΔΥΣΣΕΑΣ», η κινητή μονάδα Ενημέρωσης, Εκπαίδευσης και Τεχνολογίας, ευαισθητοποίησε τους μαθητές του κέντρου της πόλης σχετικά με την υπεύθυνη χρήση της τεχνολογίας. Ανάλογη εκδήλωση θα πραγματοποιηθεί όπως κάθε χρόνο τον ερχόμενο Νοέμβριο (2015).

Ε. Το Ευρωπαϊκό Δίκτυο κατά του Σχολικού Εκφοβισμού (EAN)

Το «Χαμόγελο του Παιδιού» συντονίζει το Ευρωπαϊκό Δίκτυο κατά του Σχολικού Εκφοβισμού (European Anti-bullying Network (EAN)), στο οποίο εκπροσωπούνται 19 οργανώσεις από 14 κράτη μέλη της ΕΕ. Ένας από τους κύριους στόχους του Δικτύου είναι ο καλύτερος συντονισμός των δράσεων των ευρωπαϊκών οργανώσεων κατά του εκφοβισμού στο σχολικό και το διαδικτυακό περιβάλλον και η ευαισθητοποίηση σχετικά με το φαινόμενο αυτό και τους κινδύνους του μεταξύ ευρύτερου κοινού, παιδιών, γονέων και εκπαιδευτικών. Η ανταλλαγή καλών πρακτικών και εργαλείων στον τομέα της πρόληψης, καθώς και η ευαισθητοποίηση και η ανάπτυξη της συνεργασίας σε θέματα ασφάλειας του Διαδικτύου όσον αφορά τα παιδιά περιλαμβάνονται στο έργο του Δικτύου. Τον Ιούνιο του 2014 πραγματοποιήθηκε στην Αθήνα το 1ο Επιστημονικό Συνέδριο κατά του εκφοβισμού στο σχολικό και διαδικτυακό περιβάλλον, υπό την αιγίδα της Ελληνικής Προεδρίας του Συμβουλίου της ΕΕ, καλύπτοντας μεταξύ άλλων το θεματικό χώρο του εκφοβισμού μέσω του Διαδικτύου και θέματα ασφάλειας του Διαδικτύου.

ΣΤ. Ευρωπαϊκή Επιτροπή Οικονομικού Συνασπισμού

Το «Χαμόγελο του Παιδιού», ως μέλος του Missing Children Europe (MCE) και του Διεθνούς Κέντρου για τα Εξαφανισμένα και Θύματα Εκμετάλλευσης Παιδιά (International Centre for Missing and Exploited Children (ICMEC)), συμμετέχει στην Ευρωπαϊκή Επιτροπή Οικονομικού Συνασπισμού για την καταπολέμηση της εμπορικής σεξουαλικής εκμετάλλευσης παιδιών μέσω του Διαδικτύου (EFC). Στην πρωτοβουλία αυτή συμμετέχουν φορείς ζωτικής σημασίας από τις υπηρεσίες υποβολής του νόμου, τον ιδιωτικό τομέα και την κοινωνία των πολιτών στην Ευρώπη, με στόχο την καταπολέμηση της εμπορικής σεξουαλικής εκμετάλλευσης παιδιών μέσω του Διαδικτύου. Τα μέλη της EFC λαμβάνουν από κοινού δράσεις σχετικά με τα συστήματα πληρωμών και ΤΠΕ που χρησιμοποιούνται για τη λειτουργία αυτών των παράνομων επιχειρήσεων. Περισσότερες πληροφορίες θα βρείτε στον ιστότοπο:
http://www.europeanfinancialcoalition.eu/index.php

Οι περισσότερες δράσεις ενημερωτικού χαρακτήρα εφαρμόζονται από τη Δι.Δ.Η.Ε, αλλά και από διάφορες Μη Κυβερνητικές Οργανώσεις που ασχολούνται με την ασφαλέστερη χρήση του Διαδικτύου.

Το Αρχηγείο της Ελληνικής Αστυνομίας και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, πέραν της καταστολής του Ηλεκτρονικού Εγκλήματος, δίνουν ιδιαίτερη έμφαση και στην πρόληψη μέσω της ενημέρωσης και της ευαισθητοποίησης των πολιτών. Στο πλαίσιο αυτό έχει σχεδιαστεί μία ολοκληρωμένη εκστρατεία ενημέρωσης και ευαισθητοποίησης, η οποία περιλαμβάνει πληθώρα καινοτόμων δράσεων, έχοντας ως στόχο να ενημερώνει τους πολίτες, με έμφαση στην ενημέρωση της μαθητικής κοινότητας, για τους κινδύνους που ελλοχεύουν κατά την πλοήγησή τους στο Διαδίκτυο και για τους τρόπους με τους οποίους οι κίνδυνοι αυτοί μπορούν να αποφευχθούν. Οι εν λόγω δράσεις είναι οι παρακάτω:

- Εφαρμογές Cyberkid για φορητές συσκευές (APPS): Η εφαρμογή Cyberkid για κινητά δημιουργήθηκε με σκοπό να ενημερώνει καθημερινά τους γονείς και τα παιδιά κάθε οικογένειας για την ασφαλή πλοήγηση στο Διαδίκτυο και τους κινδύνους που ελλοχεύουν σε αυτό. Παράλληλα, είναι μία διαδραστική εφαρμογή, η οποία δίνει την δυνατότητα άμεσης επικοινωνίας με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος μέσω της γραμμής CYBER ALERT αλλά και μέσω αποστολής άμεσου μηνύματος e-mail, με τη χρήση ενός κουμπιού, ενώ υπάρχει η δυνατότητα ψυχαγωγίας μέσω των διαφόρων παιχνιδιών.

- Ιστότοπος της Ελληνικής Αστυνομίας www.hellenicpolice.gr: Στον εν λόγω ιστότοπο και ειδικότερα στην Ενότητα «Οδηγός του Πολίτη» έχουν συμπεριληφθεί με μέριμνα της ΔΙ.Δ.Η.Ε. χρήσιμες συμβουλές, όσον αφορά την ασφαλή πλοήγηση στο Διαδίκτυο. Περαιτέρω, η ΔΙ.Δ.Η.Ε. εκδίδει σε καθημερινή βάση δελτία τύπου, τα οποία δημοσιεύονται στον προαναφερόμενο ιστότοπο και με τα οποία ενημερώνει τους πολίτες αναφορικά με την δραστηριότητά της, καθώς και για νέες εμφανιζόμενες μεθόδους διάπραξης ηλεκτρονικού εγκλήματος. Ενδεικτικά μνημονεύεται ότι, στις 3-3-2015, δημοσίευσε για ενημέρωση και ευαισθητοποίηση των γονέων, τον «Κώδικα Επικοινωνίας» των παιδοφίλων στο Διαδίκτυο, ο οποίος παρουσιάστηκε σε περίληψη, μαζί με τα σύμβολα που χρησιμοποιούν οι παιδόφιλοι για να αναγνωρίζουν τις μεταξύ τους σεξουαλικές προτιμήσεις και ο οποίος προέκυψε από σχετικό εγχειρίδιο που εντοπίστηκε στο σκοτεινό Διαδίκτυο (darknet), ύστερα από πολύμηνες και στοχευμένες έρευνες εξειδικευμένων Αξιωματικών της εν λόγω υπηρεσίας.

Ο Εθνικός CERT συμβάλλει στην πρόληψη του εγκλήματος στον κυβερνοχώρο διοργανώνοντας εκπαιδεύσεις (ημερίδες σεμινάρια), που απευθύνονται κυρίως σε προσωπικό του δημόσιου τομέα και κρίσιμων υποδομών.
Η πρόληψη δεν ρυθμίζεται ούτε αναφέρεται ρητά στον εθνικό Ν. 2472/1997. Ωστόσο, σύμφωνα με τις αρμοδιότητές της, όπως περιγράφονται στο άρθρο 19, η ΑΠΔΠΧ:

- εκδίδει οδηγίες προς τον σκοπό ενιαίας εφαρμογής των ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- καλεί και επικουρεί τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα στην κατάρτιση κωδίκων δεοντολογίας για την αποτελεσματικότερη προστασία της ιδιωτικής ζωής και των εν γένει δικαιωμάτων και θεμελιωδών ελευθεριών των φυσικών προσώπων στον τομέα της δραστηριότητάς τους,

- γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα,
- εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο νόμος περί προστασίας δεδομένων.
- Ασκώντας τις προαναφερόμενες αρμοδιότητες, συμβάλλει στην ευαισθητοποίηση τόσο των υπευθύνων επεξεργασίας των δεδομένων όσο και των υποκειμένων των δεδομένων, πράγμα που αποτελεί αυτό καθεαυτό ένα είδος πρόληψης.

8.3. Πρόληψη

8.3.1. Εθνική νομοθεσία/πολιτική και άλλα μέτρα

Το Αρχηγείο της Ελληνικής Αστυνομίας και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, πέραν της καταστολής του ηλεκτρονικού εγκλήματος, δίνουν ιδιαίτερη έμφαση στην πρόληψη μέσω της ενημέρωσης και της ευαισθητοποίησης των πολιτών. Στο πλαίσιο αυτό έχει σχεδιαστεί μία ολοκληρωμένη εκστρατεία ενημέρωσης και ευαισθητοποίησης, η οποία περιλαμβάνει πληθώρα καινοτόμων δράσεων, έχοντας ως στόχο να ενημερώνει τους πολίτες, με έμφαση στην ενημέρωση της μαθητικής κοινότητας, για τους κινδύνους που ελλοχεύουν κατά την πλοήγησή τους στο Διαδίκτυο και για τους τρόπους με τους οποίους μπορούν να αποφευχθούν οι κίνδυνοι αυτοί.
Πρωτόκολλο Συνεργασίας με την Εθνική Συνομοσπονδία Ελληνικού Εμπορίου (ΕΣΕΕ)

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και η Εθνική Συνομοσπονδία Ελληνικού Εμπορίου (ΕΣΕΕ) υπέγραψαν Πρωτόκολλο Συνεργασίας για την προώθηση και το συντονισμό δράσεων προς όφελος του υγιούς οργανωμένου εμπορίου και των καταναλωτών. Στόχος της εν λόγω συνεργασίας είναι η από κοινού συστηματική και επιστημονική μελέτη των θεμάτων και προβλημάτων που προκύπτουν για το εμπόριο και τους καταναλωτές από τις ηλεκτρονικές συναλλαγές, καθώς και ο σχεδιασμός και υλοποίηση στοχευμένων ενημερωτικών δράσεων, με σκοπό την ενημέρωση εμπόρων και καταναλωτών για τους διαδικτυακούς κινδύνους και την ασφαλή χρήση του Διαδικτύου στις εμπορικές συναλλαγές και τις διαδικτυακές αγορές.

Με την αυξανόμενη χρήση του Διαδικτύου στις διαδικτυακές αγορές και τις εμπορικές συναλλαγές, κρίθηκε επιβεβλημένη η διεύρυνση της ενημέρωσης ασφαλούς χρήσης του Διαδικτύου και η περαιτέρω ενημέρωση, μεταξύ άλλων, και του εμπορικού κόσμου. Στο πλαίσιο αυτό, η ΔΙ.Δ.Η.Ε. θα προχωρήσει στην ενημέρωση και κατάρτιση του εμπορικού κόσμου σε όλο το εύρος χρήσης των ηλεκτρονικών υπολογιστών και σε όλα τα προβλήματα που προκύπτουν από τις συναλλαγές μέσω αυτών με στόχο την ασφαλή πραγματοποίηση συναλλαγών μέσω Διαδικτύου και την προστασία τόσο των εμπορικών εταιριών όσο και των καταναλωτών από κάθε μορφής ηλεκτρονική απάτη.

Επισημαίνεται ότι η Εθνική Συνομοσπονδία Ελληνικού Εμπορίου (ΕΣΕΕ), με τη δράση αυτή, στοχεύει στη διαρκή ενημέρωση μέσω καινοτόμων δράσεων και διαδικτυακών εφαρμογών των 630.000 εμπορικών επιχειρήσεων σε θέματα ασφαλούς χρήσης του Διαδικτύου και ασφαλούς διαχείρισης των διαδικασιών ηλεκτρονικού εμπορίου, διαδικασία η οποία θα αποτελέσει εργαλείο ανάπτυξης και αύξησης της παραγωγικότητας και του ηλεκτρονικού εμπορίου μέσω της ταχύτερης διάθεσης των προϊόντων στην «ψηφιακή» αγορά.

Ιστότοπος cyberkid.gr

Με σκοπό την καλύτερη ενημέρωση του κοινού και λόγω της ευρείας αποδοχής της δράσης αυτής αλλά και της υψηλής επισκεψιμότητας του ιστοτόπου από μαθητές και πολίτες, θα υπάρχει συστηματική παρακολούθηση του ιστοτόπου cyberkid.gr και συνεχής επικαιροποίηση των παρεχόμενων πληροφοριών σχετικά με τα θέματα που εμπίπτουν στο πεδίο αρμοδιότητας της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, καθόσον αυτό επιτάσσει η αποδοχή του ως βασικού κόμβου ενημέρωσης αλλά και εκπαίδευσης μέσω των καινοτόμων εφαρμογών που λειτουργούν εντός του εν λόγω ιστοτόπου. Ήδη πολλά σχολεία πλοηγούνται στην ιστοσελίδα μας καθημερινά και μέσα εκεί πραγματοποιούν τη διαδικτυακή εκπαίδευση των μαθητών τους μέσω διαφόρων καινοτόμων εφαρμογών που υπάρχουν για αυτόν το σκοπό.

Η ΑΠΔΠΧ δεν διοργανώνει πραγματικές δραστηριότητες πρόληψης. Ωστόσο, επιδιώκουμε την ευαισθητοποίηση όσον αφορά την προστασία των δεδομένων και της ιδιωτικής ζωής. Λ.χ., η ΑΠΔΠΧ διοργανώνει συχνά ομιλίες σε σχολεία, όπου οι ακροατές επισημαίνουν θέματα προστασίας της ιδιωτικής ζωής και των δεδομένων που προκύπτουν από τη χρήση του Διαδικτύου. Πρόσφατα πραγματοποιήθηκαν επίσης ομιλίες για φοιτητές από σχετικά πεδία σπουδών (λ.χ. δίκαιο, δημοσιογραφία). Κάθε χρόνο πραγματοποιείται επίσης σειρά ομιλιών στο πλαίσιο της Ευρωπαϊκής Ημέρας Προστασίας Δεδομένων στις 28 Ιανουαρίου. Τέλος, η ΑΠΔΠΧ δημοσιεύει στον ιστότοπό της τριμηνιαίο ενημερωτικό δελτίο με τις πρόσφατες αποφάσεις της, τις τρέχουσες εξελίξεις στον τομέα των δεδομένων προσωπικού χαρακτήρα σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, καθώς και πληροφορίες σχετικά με άλλες δραστηριότητες της ΑΠΔΠΧ.

Το «Χαμόγελο του Παιδιού» έχει αναπτύξει ευρύ φάσμα δράσεων στήριξης και κοινωνικών δράσεων για τα παιδιά που κινδυνεύουν και τα παιδιά που υπήρξαν θύματα σεξουαλικής κακοποίησης. Μία από τις κύριες δράσεις είναι η Εθνική Τηλεφωνική Γραμμή για τα Παιδιά SOS 1056. Με βάση τη σχετική πείρα η οργάνωση έχει αναπτύξει πρόγραμμα πρωτοβάθμιας και δευτεροβάθμιας πρόληψης σε θεματικά πεδία όπως η ασφάλεια στο Διαδίκτυο. Το πρόγραμμα αυτό αφορά την εκπαιδευτική κοινότητα και περιλαμβάνει σχετικές πρωτοβουλίες ενημέρωσης και ευαισθητοποίησης για μαθητές, γονείς και εκπαιδευτικούς.

Το πρόγραμμα εφαρμόζεται ιδίως σε σχολικές τάξεις στο πλαίσιο μνημονίου συνεργασίας που έχει υπογραφεί ανάμεσα στο «Χαμόγελο του Παιδιού» και το Υπουργείο Παιδείας και Θρησκευμάτων. Οι προληπτικές συνεδρίες λαμβάνουν χώρα έπειτα από πρόσκληση είτε του Σχολικού Συμβούλου, του Υπευθύνου Υγειονομικής Εκπαίδευσης, του Διευθυντή ή του Συλλόγου Διδασκόντων είτε του Συλλόγου Γονέων και Κηδεμόνων. Ωστόσο, το πρόγραμμα εφαρμόζεται επίσης σε ιδιωτικά σχολεία, αθλητικούς συλλόγους, κατασκηνώσεις κ.λπ., όπου οι ψυχολόγοι προβαίνουν επίσης σε προληπτικές παρεμβάσεις.

Ένα από τα κύρια εργαλεία εν προκειμένω είναι η διαδραστική πλατφόρμα εκπαίδευσης και ενημέρωσης YouLearn, που μας επιτρέπει να προσεγγίσουμε περισσότερους μαθητές, γονείς και εκπαιδευτικούς και να αναλάβουμε δραστηριότητες πρόληψης σε σχολεία που βρίσκονται σε γεωγραφικά απομακρυσμένες περιοχές της Ελλάδας και ελληνικά σχολεία του εξωτερικού.
Το 2014 το «Χαμόγελο του Παιδιού» πραγματοποίησε παρεμβάσεις σε 35.279 παιδιά, 5.636 γονείς και 1.415 εκπαιδευτικούς. 614 παρεμβάσεις πραγματοποιήθηκαν σε 13 περιοχές της Ελλάδας.
Το 2014 η ομάδα διοργάνωσε 23 παρεμβάσεις για θέματα ασφάλειας στο Διαδίκτυο για γονείς και κηδεμόνες και 95 παρεμβάσεις για μαθητές. Η πλατφόρμα YouSmile είναι επίσης ένα από τα κύρια εργαλεία εν προκειμένω σε επίπεδο πρόληψης και ευαισθητοποίησης.

8.3.2. Public Private Partnership (PPP)

Οι δικαστικές και αστυνομικές αρχές συνεργάζονται με τις τράπεζες και την Ελληνική Ένωση Τραπεζών, όπως έχει εκτεθεί ήδη ανωτέρω.

8.4. Συμπεράσματα

- Η Ελλάδα είναι δραστήρια στον τομέα αυτό και συμμετέχει σε διάφορες ασκήσεις. Στο πλαίσιο των εθνικών ασκήσεων κυβερνοπολέμου «Πανόπτης» υπάρχει ευρεία συμμετοχή από ακαδημαϊκά ιδρύματα, φορείς του δημοσίου και του ιδιωτικού τομέα.
- Η εκπαίδευση σχετικά με το έγκλημα στον κυβερνοχώρο δεν είναι υποχρεωτική για όλους τους εισαγγελείς και δικαστές, αλλά στο μέλλον θα πρέπει να συμπληρώνουν κάποιον αριθμό ωρών σε αυτό το πεδίο εκπαίδευσης.
- Γενικά, οι ελληνικές αρχές ασχολούνται ιδιαίτερα με την πρόληψη και την ευαισθητοποίηση, καθώς και με την εκπαίδευση στους διάφορους τομείς του εγκλήματος στον κυβερνοχώρο. Έχουν καλή συνεργασία με τον ιδιωτικό τομέα και με άλλες υπηρεσίες.
- Οι δαπάνες για εκστρατείες ευαισθητοποίησης μπορούν να καλύπτονται με χορηγίες εταιρειών του τομέα της πληροφορικής και των επικοινωνιών, πράγμα που συνιστά καλή πρακτική.

- Καλό παράδειγμα πρόληψης και ευαισθητοποίησης είναι το έργο της μη κυβερνητικής οργάνωσης «Το Χαμόγελο του Παιδιού». Αυτή η μη κερδοσκοπική οργάνωση εθελοντών προσφέρει υπηρεσίες στα παιδιά 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, 365 ημέρες το χρόνο, επιδιώκοντας τη σωματική, πνευματική και ψυχολογική σταθερότητά τους. Το «Χαμόγελο του Παιδιού» έχει δρομολογήσει τη χρήση νέων ψηφιακών εργαλείων, σε συνεργασία με διεθνείς αρχές και εταίρους, για τους σκοπούς της καταπολέμησης της παιδικής πορνογραφίας και άλλων εγκλημάτων στον κυβερνοχώρο, θέτοντας τα εν λόγω εργαλεία στη διάθεση των αρχών επιβολής του νόμου.
- Άλλο ένα καλό παράδειγμα που συνδέεται επίσης με την πρόληψη και την ευαισθητοποίηση είναι το έργο του *Cyberkid*. Αυτός ο ασφαλής ιστότοπος (www.cyberkid.gr) έχει δημιουργηθεί από το προσωπικό της Ελληνικής Αστυνομίας και συγκεκριμένα τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Στον ιστότοπο τα παιδιά αλλά και οι γονείς μπορούν, μέσω διαδραστικών δραστηριοτήτων και συνεχούς ενημέρωσης, να καταρτίζονται σχετικά με τους τρόπους ασφαλούς πλοήγησης. Επιπρόσθετα και για κινητά τηλέφωνα και tablets έχει δημιουργηθεί δωρεάν εφαρμογή με χρήσιμες συμβουλές σχετικά με την πλοήγηση στο Διαδίκτυο και με το πάτημα ενός κουμπιού πραγματοποιείται αυτόματα τηλεφωνική κλήση στο τηλεφωνικό κέντρο της υπηρεσίας. Εξειδικευμένα στελέχη αντιμετωπίζουν όλα τα περιστατικά, μεταξύ των οποίων και εκείνα που απαιτούν άμεσο χειρισμό (λ.χ. εκδήλωση πρόθεσης αυτοκτονίας). Η υπηρεσία μπορεί να χρησιμοποιηθεί μέσα από διάφορες πλατφόρμες και μέσα κοινωνικής δικτύωσης (Facebook, Twitter).
- Το Τμήμα Καινοτόμων Δράσεων και Στρατηγικής παρήγαγε διάφορα ενημερωτικά φυλλάδια και τηλεοπτικά και ραδιοφωνικά «σποτ» με στόχο την προσέγγιση των πολιτών σε θέματα ενημέρωσης για το Διαδίκτυο και το ηλεκτρονικό έγκλημα.
- Αξίζει επίσης να αναφερθεί το γεγονός ότι η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας θα ολοκληρώσει την ενημέρωση μέσω τηλεδιασκέψεων των μαθητών όλων των σχολείων της επικράτειας, δηλ. περίπου 10.000 σχολικών μονάδων, για την ασφαλή πλοήγησή τους στο Διαδίκτυο, τους κινδύνους που ελλοχεύουν σε αυτό και τους τρόπους αντιμετώπισής τους.

9. ΤΕΛΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΚΑΙ ΣΥΣΤΑΣΕΙΣ

9.1. Προτάσεις προς την Ελλάδα

9.2. Συστάσεις

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

Η Ελλάδα 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 συμπεριλαμβανομένης της αξιολόγησης» (GENVAL).

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

9.2.1. Συστάσεις προς την Ελλάδα[7]

1. Η Ελλάδα θα πρέπει να υιοθετήσει το συντομότερο δυνατόν την εθνική στρατηγική κυβερνοασφάλειας, σε συνδυασμό με πρόγραμμα δράσης για την εφαρμογή της[8].

2. Η Ελλάδα θα πρέπει να θέσει σε λειτουργία μηχανισμό για την παροχή συνεπών και τυποποιημένων στατιστικών όσον αφορά τις έρευνες, διώξεις και καταδίκες για εγκλήματα στον κυβερνοχώρο, που θα ήταν ιδιαίτερα χρήσιμες ώστε να δημιουργηθεί σφαιρική εικόνα ως προς το φαινόμενο αυτό[9].

[7] Με τον Ν. 4411/2016, η Ελλάδα α) κύρωσε τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης, CETS 185) και β) μετέφερε στην εθνική έννομη τάξη της τις διατάξεις της οδηγίας 2013/40/ΕΚ για τις επιθέσεις κατά συστημάτων πληροφοριών.

[8] Από τον Νοέμβριο του 2016, έχει συσταθεί (νέο) Υπουργείο Ψηφιακής Πολιτικής βάσει του άρθρου 4 του Π.Δ. 123/2016. Επιπλέον, με τον Ν. 4386/2016, στο πλαίσιο του νέου Υπουργείου συγκροτήθηκε Γενική Γραμματεία Ψηφιακής Πολιτικής. Με τις εξελίξεις αυτές ενισχύεται ο συντονισμός μεταξύ των υπουργείων για την κατάρτιση Εθνικού Στρατηγικού Σχεδίου Ψηφιακής Πολιτικής και υλοποιείται η δέσμευση της χώρας μας να αποκτήσει κεντρική δομή, στο πλέον υψηλό επίπεδο, για τον σχεδιασμό και τον συντονισμό των έργων ψηφιακής πολιτικής, που παρακολουθούνται από την Ευρωπαϊκή Επιτροπή ως θεματικός στόχος του ΕΣΠΑ (Εταιρικό Σύμφωνο για το Πλαίσιο Ανάπτυξης) για την περίοδο 2014-2020.

[9] Επί του παρόντος, αναπτύσσεται στο πλαίσιο του συστήματος δικαιοσύνης το «Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων Πολιτικής και Ποινικής Δικαιοσύνης» (μετά από την επίσκεψη αξιολόγησης) με στόχο, μεταξύ άλλων, την παροχή όλων των απαιτούμενων δεδομένων και στατιστικών σχετικά με το κυβερνοέγκλημα (κυρίως διώξεις και καταδικαστικές αποφάσεις).

3. Οι εθνικές αρχές θα πρέπει να καταβάλουν προσπάθειες ώστε να αυξηθεί το προσωπικό του Τμήματος Εξέτασης Ψηφιακών Πειστηρίων της Ελληνικής Αστυνομίας. Αυτό θα ήταν ιδιαίτερα χρήσιμο προκειμένου να μειωθεί η διάρκεια των εργαστηριακών εξετάσεων και συνεπώς θα επηρέαζε ευνοϊκά τη διάρκεια των δικών[10].

4. Η Ελλάδα θα πρέπει να εξετάσει τη δυνατότητα αύξησης του αριθμού των εισαγγελέων με εξειδίκευση στο έγκλημα στον κυβερνοχώρο, πράγμα που θα αποτελούσε ενδεχομένως χρήσιμη μέθοδο για την ανταλλαγή πληροφοριών και πείρας[11].

5. Στον τομέα της καταπολέμησης της σεξουαλικής εκμετάλλευσης παιδιών μέσω του Διαδικτύου, θα ήταν ενδεδειγμένη η δημιουργία οργανωμένης εθνικής βάσης δεδομένων, ώστε να βελτιωθεί η ορθή χρήση της ICSE της Interpol και να αναπτυχθεί η αναγνώριση των θυμάτων.

6. Η Ελλάδα θα πρέπει να χρησιμοποιεί περισσότερο τα μέσα δικαστικής και αστυνομικής συνεργασίας, όπως οι κοινές ομάδες ερευνών και οι κυβερνοπερίπολοι.

7. Η Ελλάδα θα πρέπει να συνεχίσει να αναπτύσσει τα εξαίρετα εκπαιδευτικά προγράμματα σχετικά με το έγκλημα στον κυβερνοχώρο, μεταξύ άλλων με την αξιοποίηση των γνώσεων και άλλων σχετικών φορέων που συμμετέχουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο, όπως οι εισαγγελείς και δικαστές.

[10] Η παράγραφος 2 του άρθρου 41 του Ν. 4249/2014 προβλέπει την πρόσληψη τριακοσίων αστυνομικών ειδικών καθηκόντων. Το προσωπικό αυτό θα κατανεμηθεί (τοποθετηθεί) με προεδρικό διάταγμα που πρόκειται να εκδοθεί σε διάφορες αστυνομικές υπηρεσίες, μεταξύ των οποίων και το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Ελληνικής Αστυνομίας.

[11] Μετά την ίδρυση της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος στη Θεσσαλονίκη, διορίστηκε Ειδικός Εισαγγελέας στην Εισαγγελία Πρωτοδικών Θεσσαλονίκης.

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

1. Τα κράτη μέλη θα πρέπει να εξετάσουν την ανάπτυξη χρήσιμων εργαλείων και σωμάτων, όπως η ελληνική ειδική υπηρεσία έκτακτης ανάγκης συνεχούς λειτουργίας (24/7), το λεγόμενο «Κέντρο Επιχειρήσεων Cyber Alert», όπου εξειδικευμένα στελέχη αντιμετωπίζουν όλα τα περιστατικά, μεταξύ των οποίων και εκείνα που απαιτούν άμεσο χειρισμό (λ.χ. εκδήλωση πρόθεσης αυτοκτονίας).

2. Τα κράτη μέλη θα πρέπει να λάβουν υπόψη τους την ελληνική καλή πρακτική που συνίσταται στο μπλοκάρισμα, το φιλτράρισμα της πρόσβασης και την κατάργηση των ιστοτόπων με παράνομο περιεχόμενο.

3. Τα κράτη μέλη ενθαρρύνονται να εξετάσουν τη δυνατότητα εισαγωγής στο εθνικό τους δίκαιο της υποχρέωσης των πιστωτικών ιδρυμάτων να αναφέρουν αμελλητί τα επεισόδια κυβερνοεπιθέσεων με στόχο τα πιστωτικά ιδρύματα και/ή τους πελάτες τους.

4. Μετά την ακύρωση της οδηγίας 2006/24/ΕΚ της 15ης Μαρτίου 2006, η Ευρωπαϊκή Ένωση και τα κράτη μέλη της ενθαρρύνονται να εξετάσουν τον καταλληλότερο τρόπο για να αντιμετωπιστεί η έλλειψη εναρμόνισης των εθνικών δικαίων όσον αφορά τη φύλαξη των ηλεκτρονικών δεδομένων κίνησης, λαμβάνοντας ταυτόχρονα υπόψη τις επιχειρησιακές ανάγκες και την προστασία των θεμελιωδών δικαιωμάτων.

5. Τα ευρωπαϊκά θεσμικά όργανα θα πρέπει να αυξήσουν τη χρηματοδότηση της ΕΕ, ώστε να στηριχθούν τα κράτη μέλη στη διοργάνωση περαιτέρω εκπαίδευσης για όσους ασχολούνται επαγγελματικά στην επικράτειά τους με το φαινόμενο του εγκλήματος στον κυβερνοχώρο.

6. Η Ευρωπαϊκή Ένωση και τα κράτη μέλη της θα πρέπει να εξετάσουν πώς θα βελτιωθεί η συνεργασία με τις μεγαλύτερες διεθνείς εταιρείες τηλεπικοινωνιών.

9.2.3. Συστάσεις προς την Eurojust/την Ευρωπόλ/τον ENISA

1. Η Eurojust/η Ευρωπόλ/ο ENISA θα πρέπει να εξετάσουν την ευαισθητοποίηση των υπηρεσιών τους και την αύξηση των δυνατοτήτων συνεργασίας και ειδικής εκπαίδευσης που προσφέρουν στον τομέα του εγκλήματος στον κυβερνοχώρο.

2. Η Eurojust, η Ευρωπόλ και ο ENISA θα πρέπει να εξετάσουν το ενδεχόμενο της ενεργής στήριξης εκδηλώσεων που ενισχύουν τη διεθνή συνεργασία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, όπως η Παγκόσμια Διάσκεψη για τον Κυβερνοχώρο.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

7th Round of Mutual Evaluations - Greece 29 September - 2 OCTOBER 2015

Tuesday 29 September 2015

Venue: Ministry of Justice, Transparency and Human Right

9.30-10.00 Welcome speech and opening remarks

10.00-10.30 "Implementation of the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography"

10.30-11.00 "Provisions of substantive criminal law, statistics on the number of registered cases, investigations, prosecutions and final convictions regarding Mutual Legal Assistance with third countries"

11.00-11.30 "The fight against cybercrime under the Hellenic National Defence General Staff"

11.30-12.00 Coffee break

12.00-12.30 "The competences of the National Authority against Electronic Attacks / handling cybersecurity incidents"

12.30-13.00 Education and training

13.00-13.30 "The contribution of the Greek Desk at Eurojust in cybercrime cases"

13.30-14.00 "Blocking of access to web pages containing or disseminating child pornography"

14.00-15.00 Lunch at the Ministry's premises

15.00-15.30 "Assurance of Infrastructures, Privacy of Services and Internet applications"

15.30-16.30 Presentation of the NGO "The smile of the child"

16.00-16.30 "National Cybersecurity Strategy"

Wednesday 30 September 2015

Venue: the Division of Cybercrime Hellenic Police - Ministry of Interior and Administrative Reconstruction

9.30-11.30 "Cybercrime and online payment card fraud"
"Child sexual exploitation"

11.30-12.00 Coffee Break

12.00-14.00 "Cybercrime: current and future status"

"Innovative actions and strategy of Cyber Crime Division"

14.00-15.00 Lunch in the restaurant of general Police Directorate of Attica

Venue: Public Prosecutor's Office to the Court of Appeals - Athens

15.30-16.00 "International cooperation tools, surrender and extradition"

16.00-16.30 "Case law in relation to the provisions of substantive criminal law on cybercrime"

Thursday 1 October 2015

Venue: Forensic Division - Hellenic Police - Ministry of Interior and Administrative Reconstruction

10.00-10.05 Welcome Speech by the Deputy Director of the Forensic Division

10.05-10.20 "General presentation of the Digital Evidence Examination Laboratory"

10.20-10.45 "Forensic examination of cases regarding child sexual abuse"

10.45-1.05 "Fraud and financial forensics"

11.05-11.30 "Digital forensics in cyber attacks"

11.30-12.00 Coffee break

12.00-12.20 "Digital forensics: research challenges and open problems"

12.20-12.40 "Presentation of the activities of the Division, including trainings initiative"

12.40-13.00 "Education, further education regarding cybercrime"

13.00-13.30 Discussion with representatives of the Division. Presentation of facilities and the Labs

Venue: Hellenic Bank Association

14.00-15.00 Lunch at the Hellenic Bank Association premises

15.00-15.10 "Banking supervision framework for cyber risk"

15.10-15.20 "Supervisory assessment of cyber risk in the Greek banking sector"

15.20-15.25 "Payment systems oversight approach to cyber resilience"

15.25-15.30 "Cybercrime prevention: the HBA's role"

15.30-15.40 "Cyber security dealing in the Greek banking sector"

15.40-15.50 "Web banking and credit card fraud"

15.50-16.00 "Cyber-threats: before and after Capital-Controls"

16.00-16.10 "Distributed denial of Service (DDoS) Attack - a case study anaysis"

16.10-17.00 Questions and answers

Friday 2 October 2014

Venue: Ministry of Justice, Transparency and Human Rights

09.30-11.00 Wrap-up meeting

ANNEX B: PERSONS INTERVIEWED/MET

Meetings

Venue: Ministry of Justice, Transparency and Human rights

Person interviewed/met	**Organisation represented**
Sotiropoulou Sophia	Judge to the Court of Appeal, Athens
Skouvaris Kostas	Judge to the Court of First Instance
Preventis Sergios	Police Lieutenant, Directorate of Organization and Legal Support of the Greek Police Headquarters
Gizis Dimitrios	Prosecutor, had of criminal Prosecution Division, responsible for cybercrime issues
Eleftheriadou Argyro	Head of the Directorate of Legislative Work, International Relations and International Judicial Cooperation
Anastopoulos Vasileios	Captain, Hellenic national Defence General Staff - Cyberdefence Directorate
Trandalidi Magda	Ministry of Culture, Education and Religious Affairs
Angelis Ioannis	Prosecutor to the Court of Appeal, Athens, head of MLA Division, National School of Judges
Paschalis Nikolaos	Deputy national member of the Greek Desk of Eurojust
Giannopoulou Mina	National Telecommunications and Post Commission
Kanakaris Panagiotis	Expert, Hellenic Authority for Communication Security and Privacy
Pardalis Panos	Communications Officer, The Smile of the Child
Athanasiou Irini	Ministry of Infrastructure, Transport and Networks

Venue: Division of cybercrime - Hellenic Police - Ministry of Interior and Administrative reconstruction

Person interviewed/met	**Organisation represented**
Fragkiadaki Despina	Police captain
Germanos Georgios	Police captain
Chatzipanagiotis Panagiotis	Police captain
Kioulafas Christos	Police captain
Doukeli Aimilia	Police captain
Groutzidou Maria	Police lieutenant

Venue: Forensic Division - Hellenic Police - Ministry of Interior and Administrative Reconstruction

Person interviewed/met	**Organisation represented**
Deltsidis Apostolos	Police major
Antonopoulos Panagiotis	Police captain
Antoniou Dimitrios	Police captain
Georgakis Efthimios	Police lieutenant
Antonatos Ioannis	Police lieutenant
Krieris Dimitrios	Police lieutenant

Venue: Hellenic Bank Association

Person interviewed/met	**Organisation represented**
Gallis Dimosthenis	Deputy Head of IT Supervision and Audit Section, Bank of Greece
Kanellopoulos Ioannis	Head of IT Supervision and Audit Section, Bank of Greece
Kaliontzoglou Alexandros	Payment Systems Oversight Section, Bank of Greece
Panagiotidis Vasilis	Director, Hellenic Bank Association
Moschonas Gerasimos	Group Information Security Officer, Alpha Bank
Topakas Christakis	Group IT Security and Control Office, Piraeus Bank
Mavroforakis Michael	Group IT Governance Director, CISO, National Bank of Greece
Tzanos Ioannis	Group Corporate Security Officer, Eurobank

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
ADAE			Hellenic Authority for Communication, Security and Privacy
BoG			Bank of Greece
CCPA			Communication Privacy Protection Authority
CERT			National Information Agency
CIO			Criminal Investigation Offices
CIS			Criminal Investigation Stations
CSS			Center for Security Studies
Di.E.C.P.			Directorate of Electronic Crime Prosecution
DCD			Directorate of Cyber Defence
DCI			Directorate of Criminal Investigations
EBF			European Banking Federation
EC3			Europol's European Cybercrime Center

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
EETT			Hellenic Telecommunications and Post Commission
EFC			European Financial Coalition against Commercial Sexual Exploitation of Children Online
EMPACT			European Multidisciplinary Platform against Crime Threats
ENISA			European Union Agency for Network and Information Security
GENVAL			Working Party on General Matters including Evaluations
HBA			Hellenic Bank Association
HDPA			Hellenic Data Protection Authority
HISP			Hosting Internet Service Provider
ICMEC			International Centre for Missing and Exploited Children
INHOPE			International Association of InternetHotlines
IP			Internet Protocol
MCE			Missing Children Europe
MLA			Mutual Legal Assistance

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
MCCC			Military Center for the Confrontation of Cyber incidents
MoU			Memorandum of Understanding
National CERT			National Authority for the Confrontation of cyber Attacks
NCPC			National Communication and Post Commitee
NDGH			National Defence General Headquarters
NIA			National Information Agency
NSRF			National Strategic Reference Framework
SAFENET			Hellenic Organ of Self-Regulation for the Internet Content
SSM			Single Supervisory Mechanism