



ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ

Βρυξέλλες, 22.5.2007
COM(2007) 267 τελικό

**ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ
ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ
ΚΑΙ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ**

**Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος
στον κυβερνοχώρο**

{SEC(2007) 641}

{SEC(2007) 642}

**ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ
ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ
ΚΑΙ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ**

**Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος
στον κυβερνοχώρο**

1. ΕΙΣΑΓΩΓΗ

1.1. Τι είναι το έγκλημα στον κυβερνοχώρο;

Τι είναι το έγκλημα στον κυβερνοχώρο;

Η ασφάλεια των συστημάτων πληροφοριών, τα οποία προσλαμβάνουν στις κοινωνίες μας όλο και μεγαλύτερη σημασία, καλύπτει πολλές πτυχές, μεταξύ των οποίων κεντρική θέση έχει η καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Δεδομένου ότι ο ορισμός του εγκλήματος στον κυβερνοχώρο δεν έχει αποτελέσει αντικείμενο συμφωνίας, οι όροι «έγκλημα στον κυβερνοχώρο», «ηλεκτρονικό έγκλημα», «έγκλημα πληροφορικής» ή «έγκλημα υψηλής τεχνολογίας» χρησιμοποιούνται συχνά αδιακρίτως. Για τους σκοπούς της παρούσας ανακοίνωσης, ο όρος «έγκλημα στον κυβερνοχώρο» νοείται ως «αξιόποινες πράξεις που διαπράττονται με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων».

Στην πράξη, ο όρος έγκλημα στον κυβερνοχώρο εφαρμόζεται σε τρεις κατηγορίες αξιόποινων δραστηριοτήτων. Η πρώτη καλύπτει τις **παραδοσιακές μορφές αδικημάτων** όπως την απάτη ή την πλαστογραφία, παρόλο που, στα πλαίσια του εγκλήματος στον κυβερνοχώρο, αφορά ειδικά αξιόποινες πράξεις οι οποίες διαπράττονται μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών (εφεξής: ηλεκτρονικά δίκτυα). Η δεύτερη μορφή αφορά τη δημοσίευση **παράνομου περιεχομένου** με χρήση ηλεκτρονικών μέσων (π.χ., υλικό σεξουαλικής κακοποίησης παιδιών ή προτροπή σε φυλετικό μίσος). Η τρίτη κατηγορία περιλαμβάνει **αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων**, π.χ. επιθέσεις κατά συστημάτων πληροφοριών, άρνηση παροχής υπηρεσιών και παράνομη επέμβαση στο σύστημα πληροφοριών. Αυτά τα είδη επίθεσης μπορεί επίσης να στρέφονται κατά των θεμελιωδών υποδομών κρίσιμης σημασίας στην Ευρώπη και να έχουν επιπτώσεις στα υφιστάμενα συστήματα έγκαιρης προειδοποίησης σε πολλούς τομείς, με ενδεχόμενες καταστροφικές συνέπειες για το κοινωνικό σύνολο. Το κοινό στοιχείο μεταξύ αυτών των κατηγοριών αξιόποινων πράξεων είναι ότι μπορούν να διαπραχθούν σε μαζική κλίμακα και με μεγάλη γεωγραφική απόσταση μεταξύ του τόπου της διάπραξης της αξιόποινης πράξης και των συνεπειών της. Ως εκ τούτου, οι τεχνικές πτυχές των εφαρμοζόμενων ανακριτικών μεθόδων είναι συχνά οι ίδιες. Η παρούσα ανακοίνωση εστιάζεται σ'αυτά τα κοινά στοιχεία.

1.2. Οι τελευταίες εξελίξεις όσον αφορά το έγκλημα στον κυβερνοχώρο

1.2.1. Γενικότητες

Ο συνδυασμός της συνεχούς εξέλιξης των αξιόποινων δραστηριοτήτων και της έλλειψης αξιόπιστης πληροφόρησης καθιστά δυσχερή τη διαμόρφωση επακριβούς εικόνας της σημερινής κατάστασης. Εντούτοις, μπορούμε να διακρίνουμε ορισμένες γενικές τάσεις:

- Ο αριθμός των αξιόποινων πράξεων στον κυβερνοχώρο αυξάνεται, ενώ οι αξιόποινες δραστηριότητες όλο και περισσότερο εκσυγχρονίζονται και προσλαμβάνουν διεθνή χαρακτήρα¹
- Υπάρχουν σαφείς ενδείξεις σχετικά με την αυξανόμενη συμμετοχή ομάδων οργανωμένου εγκλήματος σε αξιόποινες πράξεις στον κυβερνοχώρο
- Εντούτοις, δεν σημειώνεται αύξηση του αριθμού των ποινικών δώξεων που ασκούνται στην Ευρώπη στο πλαίσιο της διασυνοριακής συνεργασίας μεταξύ των αρχών επιβολής του νόμου

1.2.2. Αξιόποινες πράξεις παραδοσιακής μορφής σε ηλεκτρονικά δίκτυα

Οι περισσότερες αξιόποινες πράξεις μπορεί να διαπράττονται με χρήση ηλεκτρονικών δικτύων, και διάφορες κατηγορίες απάτης και απόπειρας απάτης είναι ιδιαίτερος συνηθισμένες και αποτελούν μορφή εγκληματικότητας η οποία εμφανίζεται όλο και πιο συχνά στα ηλεκτρονικά δίκτυα. Αξιόποινες τεχνικές όπως η κλοπή ταυτότητας, το «ψάρεμα»², ανεπίκλητα ηλεκτρονικά μηνύματα και κακόβουλοι κώδικες μπορεί να χρησιμοποιούνται για τη διάπραξη απάτης μεγάλης κλίμακας. Το παράνομο εμπόριο μέσω του Διαδικτύου σε εθνικό και διεθνές επίπεδο συνιστά επίσης πρόβλημα του οποίου η σοβαρότητα αυξάνεται συνεχώς. Στις δραστηριότητες αυτές περιλαμβάνεται η λαθρεμπορία ναρκωτικών, ειδών απειλούμενων με εξαφάνιση και όπλων.

1.2.3. Παράνομο περιεχόμενο

Στην Ευρώπη, υπάρχει πρόσβαση σε έναν συνεχώς αυξανόμενο αριθμό ιστοτόπων με παράνομο περιεχόμενο. Πρόκειται για ιστοτόπους με υλικό σεξουαλικής κακοποίησης παιδιών, προτροπή σε τρομοκρατικές ενέργειες, παράνομη εξύμνηση της βίας, της τρομοκρατίας, του ρατσισμού και της ξενοφοβίας. Η δράση για την επιβολή του νόμου εναντίον αυτών των ιστοτόπων είναι εξαιρετικά δυσχερής, δεδομένου ότι οι ιδιοκτήτες και οι διαχειριστές τους βρίσκονται συχνά σε χώρες διαφορετικές από τη χώρα-στόχο, και συχνά εκτός της ΕΕ. Οι ιστότοποι αυτοί μπορούν να μετατοπίζονται με μεγάλη ταχύτητα, εντός και εκτός της εδαφικής επικράτειας της ΕΕ, ενώ ο ορισμός του παρανόμου σ' αυτόν τον τομέα παρουσιάζει μεγάλες διαφορές από το ένα κράτος στο άλλο.

¹ Οι περισσότερες από τις παρατηρήσεις που περιλαμβάνονται στην παρούσα ανακοίνωση σχετικά με τις σημερινές τάσεις βασίζονται στην μελέτη για την εκτίμηση του αντικτύπου που είχε μια ανακοίνωση για το έγκλημα στον τομέα της πληροφορικής, την οποία είχε παραγγείλει η Επιτροπή το 2006 (Σύμβαση αριθ. JLS/2006/A1/003).

² Ως "ψάρεμα" (Phishing) χαρακτηρίζονται οι απόπειρες παράνομης πρόσβασης σε ευαίσθητες πληροφορίες, όπως είναι οι κωδικοί διέλευσης και τα στοιχεία πιστωτικών καρτών· προς αυτόν τον σκοπό, ο απатеύνας συμπεριφέρεται ως αξιόπιστο πρόσωπο στο πλαίσιο μιας ηλεκτρονικής επικοινωνίας.

1.2.4. Αξιοποιινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων

Οι επιθέσεις μεγάλης κλίμακας που στρέφονται εναντίον συστημάτων πληροφοριών ή οργανισμών και ατόμων (συχνά μέσω των επονομαζόμενων «δικτύων προγραμμαμάτων ρομπότ» (botnets³)) φαίνεται ότι εμφανίζονται με συνεχώς αυξανόμενη συχνότητα. Επίσης, έχουν σημειωθεί προσφάτως περιστατικά συστηματικών, καλά συντονισμένων και ευρείας κλίμακας άμεσων επιθέσεων κατά των κρίσιμων υποδομών πληροφόρησης ενός κράτους. Το φαινόμενο αυτό έχει επιδεινωθεί εξαιτίας της συγχώνευσης των τεχνολογιών και της επιταχυνόμενης διασύνδεσης των συστημάτων πληροφοριών, στις οποίες οφείλεται το γεγονός ότι τα συστήματα αυτά έχουν γίνει πιο ευάλωτα. Οι επιθέσεις αυτές είναι συχνά καλά οργανωμένες και χρησιμοποιούνται για σκοπούς εκβιαστικής απόσπασης. Μπορούμε να υποθέσουμε ότι τα κρούσματα αυτά παρουσιάζονται έτσι ώστε να μετριάζεται η σοβαρότητά τους, πράγμα που οφείλεται εν μέρει στο ενδεχόμενο ζημιών των εμπορικών συμφερόντων των εμπλεκόμενων επιχειρήσεων σε περίπτωση που θα δινόταν δημοσιότητα σε προβλήματα ασφάλειας.

1.3. Οι στόχοι

Λαμβάνοντας υπόψη αυτές τις συνεχείς εξελίξεις, συμπεραίνουμε ότι υπάρχει επείγουσα ανάγκη να ληφθούν μέτρα – σε εθνικό και σε ευρωπαϊκό επίπεδο –κατά όλων των μορφών εγκλήματος στον κυβερνοχώρο, που συνιστούν όλο και πιο σημαντικές απειλές για την κοινωνία, τις επιχειρήσεις και τους πολίτες. Η προστασία των ατόμων κατά του εγκλήματος στον κυβερνοχώρο περιπλέκεται συχνά εξ αιτίας προβλημάτων που έχουν σχέση με τον προσδιορισμό της αρμόδιας δικαιοδοσίας, με την εφαρμοστέα νομοθεσία, με τη διασυνοριακή επιβολή του νόμου ή με την αναγνώριση και τη χρησιμοποίηση ηλεκτρονικών αποδεικτικών στοιχείων. Η κατ' ουσίαν διασυνοριακή φύση του εγκλήματος στον κυβερνοχώρο οξύνει αυτά τα προβλήματα. Για να αντιμετωπίσει αυτές τις απειλές, η Επιτροπή εγκαινιάζει πρωτοβουλία υπέρ γενικής πολιτικής η οποία αποσκοπεί στη βελτίωση του συντονισμού της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε ευρωπαϊκό και διεθνές επίπεδο.

Σκοπός είναι η ενίσχυση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Τα κράτη μέλη και η Επιτροπή εκτιμούν εδώ και πολύ καιρό ότι η περαιτέρω διαμόρφωση συγκεκριμένης πολιτικής της ΕΕ για αυτά τα ζητήματα, ιδίως, αποτελεί προτεραιότητα. Η πρωτοβουλία θα επικεντρωθεί σε δύο από τις διαστάσεις αυτής της καταπολέμησης, την επιβολή του νόμου και το ποινικό δίκαιο· η πολιτική που θα διαμορφωθεί θα συμπληρώσει άλλα μέτρα της ΕΕ τα οποία αποσκοπούν στη βελτίωση της ασφάλειας στον κυβερνοχώρο εν γένει. Μακροπρόθεσμα, η πολιτική αυτή θα περιλαμβάνει: βελτιωμένη επιχειρησιακή συνεργασία μεταξύ των αρχών επιβολής του νόμου· βελτιωμένη πολιτική συνεργασία και συντονισμό μεταξύ των κρατών μελών· πολιτική και νομική συνεργασία με τρίτες χώρες· ευαισθητοποίηση· κατάρτιση· έρευνα· ενισχυμένο διάλογο με τις επιχειρήσεις και ενδεχομένως νομοθετικά μέτρα.

³ Δίκτυο προγραμμαμάτων ρομπότ ονομάζεται μια ομάδα προσβεβλημένων υπολογιστών που εκτελούν προγράμματα υπό κεντρικό έλεγχο.

Η πολιτική σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και με τις συναφείς δικαστικές προσφυγές θα καθοριστεί και θα υλοποιηθεί με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων, ιδίως του δικαιώματος έκφρασης της γνώμης, του σεβασμού της ιδιωτικής και οικογενειακής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Κάθε νομοθετικό μέτρο που θα λαμβάνεται στο πλαίσιο αυτής της πολιτικής θα εξετάζεται προηγουμένως για να αξιολογηθεί η συμβατότητά του με τα δικαιώματα αυτά, ιδίως υπό το πρίσμα του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Σημειωτέον επίσης ότι όλες αυτές οι πολιτικές πρωτοβουλίες θα υλοποιηθούν λαμβάνοντας πλήρως υπόψη τα άρθρα 12 έως 15 της επονομαζόμενης οδηγίας για το ηλεκτρονικό εμπόριο⁴, στις περιπτώσεις που αυτό το νομικό μέσο είναι εφαρμοστέο.

Ο στόχος της παρούσας ανακοίνωσης μπορεί να υποδιαιρεθεί σε τρεις κύριες λειτουργικές πτυχές, οι οποίες μπορούν να συνοψιστούν ως εξής:

- Βελτίωση και διευκόλυνση του συντονισμού και της συνεργασίας μεταξύ των μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο, άλλων αρμόδιων αρχών και άλλων εμπειρογνομόνων στην Ευρωπαϊκή Ένωση
- Διαμόρφωση, σε συνεργασία με τα κράτη μέλη, με τους αρμόδιους ευρωπαϊκούς και διεθνείς οργανισμούς και με άλλα ενδιαφερόμενα μέρη, ενός συνεκτικού πλαισίου πολιτικών της ΕΕ για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο
- Ευαισθητοποίηση σχετικά με το κόστος και τους κινδύνους που συνεπάγεται το έγκλημα στον κυβερνοχώρο.

2. ΥΦΙΣΤΑΜΕΝΑ ΝΟΜΙΚΑ ΜΕΣΑ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

2.1. Υφιστάμενα μέσα και μέτρα στο επίπεδο της ΕΕ

Η παρούσα ανακοίνωση σχετικά με την πολιτική για το έγκλημα στον κυβερνοχώρο παγιώνει και αναπτύσσει την ανακοίνωση του 2001 για μια ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής⁵ (εφεξής: η ανακοίνωση του 2001). Η ανακοίνωση του 2001 πρότεινε κατάλληλες ουσιαστικές και διαδικαστικές νομοθετικές διατάξεις για την αντιμετώπιση τόσο των εγχώριων όσο και των διεθνικών αξιόποινων ενεργειών. Η ανακοίνωση αυτή είχε ως επακόλουθο πολλές σημαντικές προτάσεις, μεταξύ των οποίων, ιδίως, αυτές οι οποίες περιλάμβαναν την πρόταση που οδήγησε στην οδηγία πλαίσιο 2005/222/ΔΕΥ για τις επιθέσεις κατά των συστημάτων πληροφοριών⁶. Σημειωτέον σχετικά με τα προαναφερόμενα ότι έχουν επίσης ληφθεί και άλλα, γενικότερα νομοθετικά μέτρα τα οποία καλύπτουν επίσης πτυχές της καταπολέμησης του εγκλήματος στον κυβερνοχώρο,

⁴ Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8^{ης} Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά (ΕΕ L 178, 17.7.2000, σ. 1).

⁵ COM(2000) 890, 26.1.2001.

⁶ ΕΕ L 69, 16.3.2005, σ. 67.

όπως η απόφαση πλαίσιο 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών⁷.

Η απόφαση Πλαίσιο 2004/68/ΔΕΥ για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών⁸ είναι ένα καλό παράδειγμα της ιδιαίτερης έμφασης που δίνει η Επιτροπή στην **προστασία των παιδιών**, ιδίως σε σχέση με την καταπολέμηση κάθε μορφής υλικού σεξουαλικής κακοποίησης παιδιών το οποίο δημοσιεύεται παράνομα με χρήση συστημάτων πληροφοριών· πρόκειται για οριζόντια προτεραιότητα που θα εξακολουθήσει να ισχύει και μελλοντικά.

Για να απαντήσει στις προκλήσεις που αφορούν την κοινωνία της πληροφορίας, η Ευρωπαϊκή Κοινότητα έχει διαμορφώσει τρίπτυχη προσέγγιση σχετικά με την ασφάλεια των δικτύων και της πληροφόρησης: ειδικά μέτρα για την ασφάλεια των δικτύων και της πληροφόρησης, το κανονιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Παρόλο που οι τρεις αυτές πτυχές μπορούν, ως έναν ορισμένο βαθμό, να αναπτυχθούν ξεχωριστά, οι πολυάριθμες αλληλεξαρτήσεις μεταξύ τους συνιστούν επιχείρημα υπέρ της στενής συνεργασίας. Στον συναφή τομέα της ασφάλειας των δικτύων και των πληροφοριών έχει εκδοθεί, εκ παραλλήλου με την ανακοίνωση του 2001 για το έγκλημα στον κυβερνοχώρο, πρόταση ευρωπαϊκής πολιτικής⁹. Η οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ορίζει υποχρέωση για τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό να κατοχυρώνουν την ασφάλεια των υπηρεσιών τους. Σ' αυτή την οδηγία προβλέπονται επίσης διατάξεις για την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων και των κατασκοπευτικών λογισμικών. Η ασφάλεια των δικτύων και των πληροφοριών έχει έκτοτε αναπτυχθεί μέσω ενός αριθμού δράσεων, πιο πρόσφατα με τις ανακοινώσεις σχετικά με μια στρατηγική για ασφαλή κοινωνία της πληροφορίας¹⁰ στην οποία παρουσιάζεται η αναζωογονημένη στρατηγική και ορίζεται το πλαίσιο που επιτρέπει την εμβάθυνση και τη διευκρίνιση συνεκτικής προσέγγισης όσον αφορά την ασφάλεια των δικτύων και των πληροφοριών, καθώς επίσης και στην ανακοίνωση σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού¹¹, και με τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών το 2004¹². Ο κύριος στόχος του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών είναι να αποκτήσει την εμπειρογνομosύνη που χρειάζεται για την προώθηση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα και για να παρέχει αρωγή στην Επιτροπή και τα κράτη μέλη. Τα **πορίσματα των ερευνών** στον τομέα των τεχνολογιών για την εξασφάλιση της ασφάλειας των συστημάτων πληροφοριών θα διαδραματίσουν επίσης σημαντικό ρόλο κατά την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Συνεπώς, οι τεχνολογίες πληροφοριών και επικοινωνιών καθώς επίσης και η ασφάλεια περιλαμβάνονται μεταξύ των στόχων του Έβδομου Ερευνητικού Προγράμματος Πλαισίου της ΕΕ (7^ο ΠΠ), που θα ισχύει για την περίοδο 2007-

⁷ EE L 149, 2.6.2001, σ. 1.

⁸ EE L 13, 20.1.2004, σ. 44.

⁹ COM(2001) 298.

¹⁰ COM(2006) 251.

¹¹ COM(2006) 688.

¹² Κανονισμός αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών, (EE L 77, 13.3.2004, σ. 1).

2013¹³. Η αναθεώρηση του κανονιστικού πλαισίου το οποίο διέπει τις ηλεκτρονικές επικοινωνίες θα μπορούσε να συνεπάγεται τροποποιήσεις έτσι ώστε να ενισχυθεί η αποτελεσματικότητα των σχετικών με την ασφάλεια διατάξεων της οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία¹⁴.

2.2. Τα υφιστάμενα διεθνή μέσα

Λόγω της παγκόσμιας φύσης των δικτύων πληροφοριών, καμία πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο δεν μπορεί να είναι αποτελεσματική αν οι προσπάθειες περιορίζονται εντός της ΕΕ. Οι κακοποιοί μπορούν όχι μόνο να επιτίθενται σε συστήματα πληροφοριών ή να διαπράττουν αξιόπινες πράξεις από το ένα κράτος μέλος στο άλλο, αλλά μπορούν να τις διαπράττουν επίσης με ευκολία όταν βρίσκονται εκτός της δικαιοδοσίας της ΕΕ. Συνεπώς, η Επιτροπή έχει συμμετάσχει ενεργά σε διεθνείς συζητήσεις και δομές συνεργασίας, όπως στην ομάδα Λυών-Ρώμη του G 8 για το έγκλημα υψηλής τεχνολογίας και σε έργα που διαχειρίζεται η Ιντερπόλ. Η Επιτροπή παρακολουθεί στενά, ιδίως, τις εργασίες του δικτύου 24ωρων επαφών σχετικά με το διεθνές έγκλημα υψηλής τεχνολογίας (το δίκτυο 24/7)¹⁵, μέλη του οποίου είναι ένας σημαντικός αριθμός κρατών παγκοσμίως, συμπεριλαμβανομένων των περισσότερων κρατών μελών της ΕΕ. Το δίκτυο του G8 είναι μηχανισμός ο οποίος επιτρέπει την επιτάχυνση των επαφών μεταξύ των συμμετεχόντων κρατών, με σημεία επαφής που λειτουργούν 24 ώρες το 24ωρο για υποθέσεις για τις οποίες υπάρχουν ηλεκτρονικά αποδεικτικά στοιχεία, και για υποθέσεις για τις οποίες απαιτείται κατεπείγουσα αρωγή από αρχές επιβολής του νόμου άλλων χωρών.

Σ' αυτόν τον τομέα, το κυριότερο ευρωπαϊκό και διεθνές μέσο είναι αναμφισβήτητα η Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης το 2001¹⁶. Η Σύμβαση αυτή, η οποία έχει εκδοθεί και τεθεί σε ισχύ το 2004, περιλαμβάνει κοινούς ορισμούς διαφόρων ειδών εγκλήματος στον κυβερνοχώρο και θέτει τις βάσεις για επιχειρησιακή δικαστική συνεργασία μεταξύ των συμβαλλομένων κρατών. Την έχουν υπογράψει πολλά κράτη, συμπεριλαμβανομένων των ΗΠΑ και άλλων μη ευρωπαϊκών κρατών, καθώς επίσης και όλα τα κράτη μέλη. Ένας ορισμένος αριθμός κρατών μελών δεν έχουν ακόμα επικυρώσει αυτή τη σύμβαση ή το συμπληρωματικό πρωτόκολλό της που αφορά τις πράξεις ρατσιστικής και ξενοφοβικής φύσης οι οποίες διαπράττονται μέσω συστημάτων υπολογιστή. Δεδομένου ότι όλοι συμφωνούν για τη σημασία αυτής της Σύμβασης, η Επιτροπή θα ενθαρρύνει τα κράτη μέλη και τις οικείες τρίτες χώρες να επικυρώσουν τη Σύμβαση και εξετάζει τη δυνατότητα η Ευρωπαϊκή Κοινότητα να αποτελέσει συμβαλλόμενο μέρος της Σύμβασης.

¹³ Η Ευρωπαϊκή Ένωση έχει ήδη, δυνάμει του 6^{ου} προγράμματος πλαισίου για την έρευνα και την τεχνολογική ανάπτυξη, υποστηρίξει έναν ορισμένο αριθμό ενδιαφερόντων, και επιτυχημένων, ερευνητικών σχεδίων έργων.

¹⁴ COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

¹⁵ Βλέπε άρθρο 35 της Σύμβασης για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης

¹⁶ <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

3. ΠΕΡΑΙΤΕΡΩ ΔΙΑΜΟΡΦΩΣΗ ΕΙΔΙΚΩΝ ΜΕΣΩΝ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

3.1. Ενίσχυση της επιχειρησιακής συνεργασίας για την επιβολή του νόμου και των προσπαθειών κατάρτισης στο επίπεδο της ΕΕ

Η έλλειψη, ή η ανεπαρκής χρησιμοποίηση των άμεσων δομών για την **επιχειρησιακή διασυνοριακή συνεργασία** εξακολουθεί να αποτελεί αδυναμία μείζονος σημασίας στον τομέα της Δικαιοσύνης, της Ελευθερίας και της Ασφάλειας. Η παραδοσιακή αλληλοβοήθεια, όταν πρόκειται για επείγουσες υποθέσεις εγκλήματος στον κυβερνοχώρο, έχει αποδειχθεί ότι πάσχει από βραδύτητα και αναποτελεσματικότητα, ενώ δεν έχουν ακόμα αναπτυχθεί επαρκώς νέες δομές συνεργασίας. Παρόλο που οι εθνικές δικαστικές αρχές και οι αρχές επιβολής του νόμου συνεργάζονται στενά στην Ευρώπη μέσω της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Europol), της Eurojust και άλλων οργανισμών, παραμένει η προφανής ανάγκη ενίσχυσης και διευκρίνισης των αρμοδιοτήτων. Από διαβουλεύσεις που έχει αναλάβει η Επιτροπή, φαίνεται ότι αυτά τα κρίσιμης σημασίας μέσα δεν χρησιμοποιούνται κατά τον βέλτιστο δυνατό τρόπο. Μια περισσότερο συντονισμένη ευρωπαϊκή προσέγγιση πρέπει να είναι τόσο επιχειρησιακή όσο και στρατηγική και να καλύπτει επίσης την ανταλλαγή πληροφοριών και τις βέλτιστες πρακτικές.

Στο εγγύς μέλλον, η Επιτροπή θα δώσει ιδιαίτερη έμφαση στις ανάγκες **κατάρτισης**. Είναι αποδεδειγμένο ότι οι τεχνολογικές εξελίξεις δημιουργούν ανάγκη διαρκούς κατάρτισης των αρχών επιβολής του νόμου και των δικαστικών αρχών όσον αφορά ζητήματα σχετικά με το έγκλημα στον κυβερνοχώρο. Κατά συνέπεια, προβλέπεται ενισχυμένη και καλύτερα συντονισμένη χρηματική στήριξη από την ΕΕ σε πολυεθνικά προγράμματα κατάρτισης. Η Επιτροπή πρόκειται επίσης, σε στενή συνεργασία με τα κράτη μέλη και με άλλους αρμόδιους οργανισμούς όπως η Europol, η Eurojust, η Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL) και το Ευρωπαϊκό Δίκτυο Κατάρτισης Δικαστικών (EJNT), να εργαστεί για να επιτύχει συντονισμό και διασύνδεση όλων των οικείων προγραμμάτων κατάρτισης σε επίπεδο ΕΕ.

Η Επιτροπή θα διοργανώσει **συνάντηση** μεταξύ εμπειρογνομόνων στον τομέα της επιβολής του νόμου, οι οποίοι θα προέρχονται από τα κράτη μέλη αλλά επίσης και από την Europol, το CEPOL και EJTN, για να συζητήσουν πώς θα βελτιωθεί η στρατηγική και επιχειρησιακή συνεργασία καθώς επίσης και η κατάρτιση σχετικά με το έγκλημα στον κυβερνοχώρο στην Ευρώπη το 2007. Μεταξύ άλλων, θα εξεταστεί η σκοπιμότητα της δημιουργίας μόνιμου ευρωπαϊκού σημείου επαφής για ανταλλαγή πληροφοριών καθώς επίσης και ευρωπαϊκής πλατφόρμας κατάρτισης σχετικά με το έγκλημα στον κυβερνοχώρο. Αυτή η συνάντηση του 2007 θα είναι η πρώτη μιας σειράς συναντήσεων που έχουν προγραμματιστεί για το εγγύς μέλλον.

3.2. Ενίσχυση του διαλόγου με τη βιομηχανία

Τόσο ο ιδιωτικός όσο και ο δημόσιος τομέας έχουν συμφέρον να διαμορφώσουν από κοινού μεθόδους ανίχνευσης και πρόληψης των ζημιών που προξενούνται από τις αξιόποινες δραστηριότητες. Η κοινή συμμετοχή του ιδιωτικού και του δημόσιου τομέα, βασιζόμενη σε αμοιβαία εμπιστοσύνη και έχοντας κοινό στόχο τη μείωση των ζημιών, υπόσχεται να αποτελέσει αποτελεσματικό δρόμο για τη βελτίωση της ασφάλειας, όσον αφορά επίσης και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η δημόσια και η ιδιωτική πτυχή της πολιτικής της Επιτροπής όσον αφορά το έγκλημα στον κυβερνοχώρο θα αποτελέσουν εν καιρώ μέρος προγραμματισμένης σφαιρικής ευρωπαϊκής πολιτικής για τον διάλογο μεταξύ του δημόσιου και του ιδιωτικού τομέα, καλύπτοντας ολόκληρο τον τομέα της ευρωπαϊκής ασφάλειας. Η πολιτική αυτή θα σημειώσει πρόοδο, ιδίως, χάρη στο ευρωπαϊκό φόρουμ για την ασφάλεια, την έρευνα και την καινοτομία, το οποίο η Επιτροπή σχεδιάζει να δημιουργήσει στο εγγύς μέλλον και στο οποίο θα συμμετέχουν τα ενδιαφερόμενα μέρη του δημόσιου και του ιδιωτικού τομέα.

Οι εξελίξεις σχετικά με τις σύγχρονες τεχνολογίες πληροφοριών και τα συστήματα ηλεκτρονικής επικοινωνίας ελέγχονται σε μεγάλο βαθμό από ιδιωτικές επιχειρήσεις. Ιδιωτικές εταιρίες πραγματοποιούν αξιολογήσεις κινδύνων, καταρτίζουν προγράμματα καταπολέμησης των αξιόποινων πράξεων και επινοούν τεχνικές λύσεις για την πρόληψη των αξιόποινων πράξεων. Η βιομηχανία έχει φανεί πολύ πρόθυμη να βοηθήσει τις δημόσιες αρχές για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ιδίως όσον αφορά την καταπολέμηση της παιδοφιλικής πορνογραφίας¹⁷ και άλλα είδη παράνομου περιεχομένου στο Διαδίκτυο.

Ένα άλλο ζήτημα αφορά την εμφανή έλλειψη ανταλλαγής πληροφοριών, εμπειρογνομοσύνης και βέλτιστων πρακτικών μεταξύ του δημόσιου και του ιδιωτικού τομέα. Συχνά, για να προστατεύσουν τα εμπορικά τους πρότυπα και μυστικά, οι επιχειρήσεις του ιδιωτικού τομέα είναι απρόθυμες, ή δεν δεσμεύονται από τη νομοθεσία από καμία σαφή υποχρέωση ώστε να αναφέρουν ή να συμμερίζονται με τις αρχές επιβολής του νόμου χρήσιμες πληροφορίες σχετικά με αξιόποινες δραστηριότητες. Εντούτοις, οι πληροφορίες αυτές μπορεί να είναι απαραίτητες για να είναι σε θέση οι δημόσιες αρχές να διαμορφώνουν αποτελεσματική και κατάλληλη πολιτική καταπολέμησης των αξιόποινων πράξεων. Οι δυνατότητες βελτίωσης της διατομεακής ανταλλαγής πληροφοριών θα εξεταστούν επίσης υπό το πρίσμα των εν ισχύ κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η Επιτροπή διαδραματίζει ήδη σημαντικό ρόλο σε διάφορες δομές με συμμετοχή του δημοσίου και του ιδιωτικού τομέα οι οποίες καταπολεμούν το έγκλημα στον κυβερνοχώρο, όπως είναι η Ομάδα Εμπειρογνομόνων για την πρόληψη της απάτης¹⁸. Η Επιτροπή είναι πεπεισμένη για το ότι μια αποτελεσματική γενική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο πρέπει επίσης να περιλαμβάνει στρατηγική συνεργασίας μεταξύ των επιχειρήσεων του δημόσιου και του ιδιωτικού τομέα, συμπεριλαμβανομένων των οργανώσεων της κοινωνίας των πολιτών.

¹⁷ Ένα πρόσφατο παράδειγμα είναι η συνεργασία σ' αυτόν τον τομέα μεταξύ των υπηρεσιών καταστολής και των εταιριών τραπεζικών καρτών, στο πλαίσιο της οποίας οι εταιρίες τραπεζικών καρτών βοήθησαν την αστυνομία να εντοπίσει αγοραστές παιδοφιλικού πορνογραφικού υλικού σε ηλεκτρονική μορφή.

¹⁸ Βλέπε http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

Για να επιτύχει τη διεύρυνση της συνεργασίας μεταξύ του δημοσίου και του ιδιωτικού τομέα για τα ζητήματα αυτά, η Επιτροπή πρόκειται να διοργανώσει εντός του 2007 συνεδρίαση μεταξύ εμπειρογνομόνων των αρχών επιβολής του νόμου και εκπροσώπων του ιδιωτικού τομέα, ιδίως παρόχων υπηρεσιών Διαδικτύου, για να συζητήσουν το πώς θα βελτιώσουν την επιχειρησιακή συνεργασία στην Ευρώπη μεταξύ του δημόσιου και του ιδιωτικού τομέα¹⁹. Κατά τη διάρκεια αυτής της συνεδρίασης θα συζητηθούν όλα τα θέματα που θα κριθεί ότι μπορεί να προσθέσουν αξία σε αμφότερου τους τομείς, αλλά κυρίως τα ακόλουθα:

- Βελτίωση της επιχειρησιακής συνεργασίας κατά την καταπολέμηση αξιόποινων πράξεων και παράνομου περιεχομένου του Διαδικτύου, ειδικότερα στους τομείς της τρομοκρατίας, του υλικού σεξουαλικής κακοποίησης παιδιών και άλλων αξιόποινων δραστηριοτήτων ιδιαίτερα ευαίσθητων από τη σκοπιά της προστασίας των παιδιών
- Εγκαινίαση συμφωνιών μεταξύ του δημόσιου και του ιδιωτικού τομέα με σκοπό την παρεμπόδιση, σε όλα τα κράτη μέλη της ΕΕ, ιστοτόπων που περιλαμβάνουν παράνομο υλικό, ειδικότερα υλικό σεξουαλικής κακοποίησης παιδιών
- Διαμόρφωση προτύπου για την ανταλλαγή απαραίτητων και χρήσιμων πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα· ένας από τους σχετικούς προβληματισμούς θα είναι η καλλιέργεια ατμόσφαιρας αμοιβαίας εμπιστοσύνης και λήψης υπόψη των συμφερόντων όλων των μερών
- Δημιουργία δικτύου σημείων επαφής για την επιβολή του νόμου, τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα

3.3. Η νομοθεσία

Η γενική εναρμόνιση των ορισμών των αξιόποινων πράξεων και των εθνικών ποινικών νομοθεσιών στον τομέα του εγκλήματος στον κυβερνοχώρο δεν είναι ακόμα σκόπιμη, λόγω της ποικιλομορφίας των ειδών αδικημάτων που καλύπτονται από την έννοια αυτή. Δεδομένου ότι η αποτελεσματική συνεργασία μεταξύ των αρχών επιβολής του νόμου εξαρτάται συχνά από το κατά πόσον έχουν τουλάχιστον εν μέρει εναρμονιστεί οι ορισμοί των αξιόποινων πράξεων, η εξακολούθηση της εναρμόνισης των νομοθεσιών των κρατών μελών συνεχίζει να αποτελεί στόχο μακροπρόθεσμο²⁰. Όσον αφορά ορισμένους από τους ορισμούς των κυριότερων αξιόποινων πράξεων, έχει ήδη σημειωθεί ένα σημαντικό βήμα με την απόφαση πλαίσιο σχετικά με τις επιθέσεις εναντίον συστημάτων πληροφοριών. Όπως περιγράφεται ως άνω, έχουν εν τω μεταξύ εμφανιστεί νέες απειλές και η Επιτροπή παρακολουθεί προσεκτικά αυτές τις εξελίξεις, δεδομένης της σημασίας που έχει η διαρκής αξιολόγηση των αναγκών επιπρόσθετων νομοθετικών μέτρων. Η παρακολούθηση των εξελίξεων σχετικά με αυτές τις απειλές είναι στενά συντονισμένη με το Ευρωπαϊκό Πρόγραμμα Προστασίας των Υποδομών Ζωτικής Σημασίας.

¹⁹ Η συνεδρίαση αυτή θα μπορούσε να θεωρηθεί ότι αποτελεί συνέχεια του φόρουμ της ΕΕ που παρουσιάζεται στο τμήμα 6.4 της ανακοίνωσης σχετικά με το ηλεκτρονικό έγκλημα.

²⁰ Αυτός ο πιο μακροπρόθεσμος στόχος έχει ήδη αναφερθεί στη σελίδα 3 της Ανακοίνωσης 2001.

Ωστόσο, θα πρέπει επίσης να προβλεφθεί η λήψη στοχοθετημένων νομοθετικών μέτρων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Ένα ιδιαίτερο ζήτημα για το οποίο ενδέχεται να απαιτηθεί λήψη νομοθετικών μέτρων αφορά τις καταστάσεις στις οποίες το έγκλημα στον κυβερνοχώρο διαπράττεται σε συνδυασμό με **κλοπή ταυτότητας**. Κατά γενικό κανόνα, «κλοπή ταυτότητας» νοείται η χρησιμοποίηση προσωπικών στοιχείων ταυτοποίησης, π.χ. ενός αριθμού πιστωτικής κάρτας, ως μέσο για διάπραξη άλλων αξιόποινων πράξεων. Στα περισσότερα κράτη μέλη, ο κακοποιός που διαπράττει κλοπή ταυτότητας θα διωχθεί κατά πάσαν πιθανότητα για την απάτη, ή ενδεχομένως για κάποιο άλλο αδίκημα, μάλλον αντί για την κλοπή ταυτότητας, δεδομένου ότι η απάτη θεωρείται ότι αποτελεί σοβαρότερο αδίκημα. Η κλοπή ταυτότητας αυτή καθεαυτή δεν συνιστά αξιόποινη πράξη σε όλα τα κράτη μέλη. Είναι συχνά ευκολότερο να αποδειχτεί το αδίκημα της κλοπής ταυτότητας από το αδίκημα της απάτης, έτσι ώστε η ευρωπαϊκή συνεργασία στον τομέα της επιβολής του νόμου θα επωφεληθεί αν η κλοπή ταυτότητας θεωρείται αξιόποινη πράξη σε όλα τα κράτη μέλη. Η Επιτροπή πρόκειται εντός του 2007 να εγκαινιάσει διαβουλεύσεις για να καθοριστεί κατά πόσον είναι σκόπιμη η λήψη νομοθετικών μέτρων.

3.4. Η κατάρτιση στατιστικών

Αποτελεί αντικείμενο γενικής συμφωνίας ότι είναι σε μεγάλο βαθμό ακατάλληλη η παρούσα κατάσταση της πληροφόρησης σχετικά με την επικράτηση της εγκληματικότητας, και ιδίως ότι χρειάζεται να βελτιωθεί σε μεγάλο βαθμό για να καταστεί εφικτή η σύγκριση δεδομένων μεταξύ κρατών μελών. Ένα φιλόδοξο πενταετές πρόγραμμα για την αντιμετώπιση αυτού του προβλήματος εκτίθεται στην ανακοίνωση της Επιτροπής για *χάραξη ολοκληρωμένης και συνεκτικής στρατηγικής της ΕΕ για την κατάρτιση στατιστικών σχετικά με την εγκληματικότητα και την ποινική δικαιοσύνη: Σχέδιο Δράσης της ΕΕ 2006 – 2010* της²¹. Η Ομάδα Εμπειρογνομόνων που συγκροτήθηκε δυνάμει αυτού του σχεδίου δράσης αναμένεται ότι θα αποτελέσει κατάλληλο πλαίσιο για τη διαμόρφωση των απαιτούμενων δεικτών για τη μέτρηση της έκτασης του εγκλήματος στον κυβερνοχώρο.

4. Η ΑΚΟΛΟΥΘΗΤΕΑ ΟΔΟΣ

Η Επιτροπή σκοπεύει εφεξής να προχωρήσει όσον αφορά τη γενική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο. Λόγω των περιορισμένων εξουσιών της Επιτροπής στον τομέα του ποινικού δικαίου, η πολιτική αυτή μπορεί μόνο να αποτελέσει συμπλήρωμα των μέτρων που λαμβάνονται από τα κράτη μέλη και από άλλους φορείς. Τα σημαντικότερα μέτρα – έκαστο εκ των οποίων θα συνεπάγεται τη χρησιμοποίηση ενός, πολλών ή όλων των μέσων που παρουσιάζονται στο κεφάλαιο 3 – θα στηριχθούν επίσης μέσω του χρηματοδοτικού προγράμματος «Πρόληψη και Καταπολέμηση του Εγκλήματος».

4.1. Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο εν γένει

- Εξασφάλιση ενισχυμένης επιχειρησιακής συνεργασίας μεταξύ των αρχών επιβολής του νόμου και των δικαστικών αρχών των κρατών μελών, δράση η οποία θα αρχίσει με τη διοργάνωση ειδικής συνεδρίασης μεταξύ εμπειρογνομόνων το 2007 και η οποία ενδέχεται να περιλαμβάνει τη δημιουργία ενός κεντρικού σημείου επαφής της ΕΕ όσον αφορά το έγκλημα στον κυβερνοχώρο

²¹ COM(2006) 437, 7.8.2006.

- Μεγέθυνση της χρηματοδοτικής στήριξης σε πρωτοβουλίες για βελτίωση της κατάρτισης των αρχών επιβολής του νόμου και των δικαστικών αρχών σχετικά με τους χειρισμούς που αφορούν υποθέσεις εγκλήματος στον κυβερνοχώρο και λήψη μέτρων για τον συντονισμό όλων των πολυεθνικών προσπαθειών κατάρτισης σ' αυτόν τον τομέα, χάρη στη δημιουργία πλατφόρμας κατάρτισης της ΕΕ
- Παρακίνηση των κρατών μελών και όλων των δημόσιων αρχών να δώσουν μεγαλύτερη έμφαση στη λήψη αποτελεσματικών μέτρων καταπολέμησης του εγκλήματος στον κυβερνοχώρο και στη χορήγηση επαρκών πόρων για την καταπολέμησή του
- Στήριξη των ερευνητικών δραστηριοτήτων που συμβάλλουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο
- Διοργάνωση τουλάχιστον ενός συνεδρίου μείζονος σημασίας (το 2007) με συμμετοχή των αρχών επιβολής του νόμου και φορέων του ιδιωτικού τομέα, ιδίως για την εγκαινίαση συνεργασίας για την καταπολέμηση των παρανόμων δραστηριοτήτων στο Διαδίκτυο, με χρήση ηλεκτρονικών δικτύων και εναντίον τους, καθώς επίσης και για την προώθηση αποτελεσματικότερων ανταλλαγών πληροφοριών μη προσωπικού χαρακτήρα, και για τη μεταπαρακολούθηση των πορισμάτων αυτού του συνεδρίου του 2007 με συγκεκριμένα σχέδια συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα
- Ανάλυση πρωτοβουλίας και συμμετοχή σε δράσεις με από κοινού συμμετοχή του δημόσιου και του ιδιωτικού τομέα οι οποίες αποσκοπούν στην ευαισθητοποίηση, ιδίως μεταξύ των καταναλωτών, του κόστους και των κινδύνων που αντιπροσωπεύει το έγκλημα στον κυβερνοχώρο, αποφεύγοντας εκ παραλλήλου την υπονόμηση της εμπιστοσύνης των καταναλωτών και των χρηστών την οποία θα συνεπάγετο η εστίαση στις αρνητικές μόνο πτυχές της ασφάλειας
- Ενεργός συμμετοχή και προώθηση της διεθνούς συνεργασίας παγκοσμίως για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο
- Εγκαινίαση, συμβολή και παροχή στήριξης σε διεθνή σχέδια έργων που είναι σύμφωνα με την πολιτική της Επιτροπής σ' αυτόν τον τομέα, π.χ. έργα τα οποία διαχειρίζεται το G 8 και έργα συμβατά με τα έγγραφα στρατηγικής ανά χώρα και ανά περιφέρεια (όσον αφορά τη συνεργασία με τις τρίτες χώρες)
- Λήψη συγκεκριμένων μέτρων για την ενθάρρυνση όλων των κρατών μελών και των οικείων τρίτων χωρών να επικυρώσουν τη Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης και το συμπληρωματικό της πρωτόκολλο και εξέταση της δυνατότητας η Κοινότητα να καταστεί συμβαλλόμενο μέρος αυτής της Σύμβασης
- Εξέταση, μαζί με τα κράτη μέλη, του φαινομένου των συντονισμένων και ευρείας κλίμακας επιθέσεων κατά της υποδομής πληροφόρησης των κρατών μελών, αποσκοπώντας στην πρόληψη και την καταπολέμησή τους, συμπεριλαμβανομένων συντονισμένων απαντήσεων και ανταλλαγής πληροφοριών και βέλτιστων πρακτικών

4.2. Η καταπολέμηση των παραδοσιακών μορφών εγκληματικότητας στα ηλεκτρονικά δίκτυα

- Εγκαινίαση ανάλυσης εις βάθος, αποσκοπώντας στην εκπόνηση πρότασης για συγκεκριμένα νομοθετικά μέτρα της ΕΕ για την καταπολέμηση της κλοπής ταυτότητας
- Προώθηση της διαμόρφωσης τεχνικών μεθόδων και διαδικασιών για την καταπολέμηση της απάτης και του παράνομου εμπορίου στο Διαδίκτυο, συμπεριλαμβανομένων σχεδίων συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα
- Εξακολούθηση και εμβάθυνση των εργασιών που πραγματοποιούνται σε συγκεκριμένους στοχοθετημένους τομείς, όπως είναι οι εργασίες της Ομάδας Εμπειρογνομόνων για την πρόληψη της απάτης οι οποίες αφορούν την καταπολέμηση της απάτης με μέσα πληρωμής άλλα εκτός από τα μετρητά σε ηλεκτρονικά δίκτυα

4.3. Παράνομα περιεχόμενα

- Εξακολούθηση εκπόνησης μέτρων για την καταπολέμηση συγκεκριμένων παράνομων περιεχομένων, ειδικά όσον αφορά το υλικό σεξουαλικής κακοποίησης παιδιών και προτροπής στην τρομοκρατία και ιδίως μέσω της μεταπαρακολούθησης της εφαρμογής της απόφασης πλαισίου για τη σεξουαλική εκμετάλλευση παιδιών
- Να κληθούν τα κράτη μέλη να διαθέσουν επαρκείς χρηματικούς πόρους για την ενίσχυση του έργου των αρχών επιβολής του νόμου, με ειδική έμφαση στην ταυτοποίηση των θυμάτων υλικού σεξουαλικής κακοποίησης το οποίο διανέμεται ηλεκτρονικά
- Εγκαινίαση και στήριξη δράσεων κατά των παρανόμων περιεχομένων που υπάρχει κίνδυνος να προτρέπουν ανηλίκους σε βίαιες και άλλου τύπου σοβαρές παράνομες συμπεριφορές, π.χ. ορισμένες μορφές ιδιαιτέρως βίαιων ηλεκτρονικών παιχνιδιών βίντεο
- Εγκαινίαση και προώθηση του διαλόγου μεταξύ κρατών μελών και με τρίτες χώρες σχετικά με τεχνικές μεθόδους για τη δράση κατά των παράνομων περιεχομένων καθώς επίσης και σχετικά με διαδικασίες για το κλείσιμο των παράνομων ιστοτόπων, αποσκοπώντας επίσης στη σύναψη επισήμων συμφωνιών με γειτονικές και άλλες χώρες σχετικά με το ζήτημα αυτό
- Σύναψη εθελούσιων συμφωνιών και συμβάσεων σε επίπεδο ΕΕ μεταξύ δημοσίων αρχών και ιδιωτικών επιχειρήσεων, ιδίως παρόχων υπηρεσιών Διαδικτύου, σχετικά με διαδικασίες για την παρεμπόδιση και το κλείσιμο των παράνομων ιστοτόπων του Διαδικτύου

4.4. Μεταπαρακολούθηση

Στην παρούσα ανακοίνωση περιγράφεται ένας ορισμένος αριθμός δράσεων που αποσκοπούν στη βελτίωση των δομών συνεργασίας στην ΕΕ, ως επόμενα βήματα. Η Επιτροπή θα δώσει συνέχεια σ' αυτές τις δράσεις, θα αξιολογήσει την πρόοδο που θα έχει σημειωθεί κατά την υλοποίησή τους και θα απευθύνει εκθέσεις σχετικά στο Συμβούλιο και στο Κοινοβούλιο.