Νομικές και Κοινωνικές Πτυχές του Εγκλήματος στον Κυβερνοχώρο

Ιωάννης Δ. Ιγγλεζάκης
Αν. Καθηγητής
Νομική Σχολή ΑΠΘ

Η Εξέλιξη του Κυβερνοεγκλήματος

- Η ανάπτυξη της ψηφιακής τεχνολογίας και η σύγκληση η/υ και τηλεπικοινωνιών επέφερε βαθύ μετασχηματισμό στην κοινωνικοποίηση του ατόμου και στη διενέργεια οικονομικών συναλλαγών και στο ηλεκτρονικό επιχειρείν.
- Δίπλα σε αυτές τις εξελίξεις, η αρνητική όψη της κοινωνίας της πληροφορίας υπήρξε η κατάχρηση της πληροφορικής και του διαδικτύου για τη διενέργεια εγκληματικών πράξεων.

Η Εξέλιξη του Κυβερνοεγκλήματος

- Η σύλληψη του «ηλεκτρονικού εγκλήματος» ως μιας ξεχωριστής κατηγορίας προέκυψε στην πράξη από τις αναφορές για σαμποτάζ στους η/υ, κατασκοπεία και παράνομη χρήση η/υ.

- Στη δεκαετία του ’70 ο περιορισμένος ρόλος του η/υ στην καθημερινή ζωή είχε ως συνέπεια ότι μόνο περιορισμένος αριθμός εγκλημάτων διαπράττονταν με τη χρήση η/υ. Τις επόμενες δεκαετίες, ωστόσο, η διάδοση της χρήσης υπολογιστών και η δικτύωση επέφεραν δομικές αλλαγές και την ένταση των εγκλημάτων που διαπράττονταν ηλεκτρονικά.

Η Εξέλιξη του Κυβερνοεγκλήματος

- Αρχικά, το πρόβλημα εντοπίζονταν στην παράνομη πρόσβαση σε ιδιωτικές πληροφορίες, ωστόσο, αργότερα, έγινε αντιληπτό ότι οι η/υ μπορούσαν να χρησιμοποιηθούν για τη διάπραξη οικονομικών εγκλημάτων.

- Τα προβλήματα αυτά αντιμετωπίσθηκαν, αρχικώς, με την εισαγωγή ειδικής νομοθεσίας και πιο συγκεκριμένα, με το ν. 1805/1988, ο οποίος προσέθεσε τέσσερα εμβόλιμα άρθρα στον ΠΚ (εδ. β΄ στο άρθρ. 13 περ. γ΄, 370Β, 370Γ και 386Α). Με τις διατάξεις αυτές επιχειρήθηκε η αντιμετώπιση ορισμένων μορφών εγκληματικότητας που συνδέονται με την πληροφορική και τους η/υ, οι οποίες ήταν καινοφανείς για την εποχή τους.

Η εξέλιξη του Κυβερνοεγκλήματος

- Με την ανάδειξη του Διαδικτύου ως ενός νέου μέσου επικοινωνίας με παγκόσμια εμβέλεια ανέκυψαν νέες προκλήσεις για την επιστήμη του ποινικού δικαίου, καθώς εμφανίσθηκαν νέες μορφές αδικημάτων που συσχετίζονται με αυτό, όπως είναι η παιδική πορνογραφία και η απάτη μέσω υπολογιστή. Η νομοθεσία στον Ευρωπαϊκό χώρο και στην Χώρα μας σταδιακά προσαρμόσθηκε στη νέα αυτή πραγματικότητα και νέες διατάξεις θεσπίσθηκαν για την κύρωση των αδικημάτων που τελούνται στο Διαδίκτυο.

Η εξέλιξη του Κυβερνοεγκλήματος

- Το διαδικτυακό έγκλημα εξελίχθηκε και αναπτύχθηκαν νέες, σύγχρονες μορφές διαδικτυακού εγκλήματος, όπως είναι η διαδικτυακή τρομοκρατία, η διαδικτυακή παρενόχληση, η κλοπή ταυτότητας, οι επιθέσεις άρνησης εξυπηρέτησης σε συστήματα υπολογιστών κ.λπ., οι οποίες δεν αντιμετωπίζονται, αφού νέες προκλήσεις εξακολουθούν να παρουσιάζονται, συνεχώς.

Νέες Απειλές

- Στην επιχειρηματική κοινότητα οι συναλλαγές πλέον διενεργούνται μέσω η/υ και ως εκ τούτου υπάρχει η ανάγκη για ασφαλή υποδομή επικοινωνιών.
- Επιπλέον, πολλές επιχειρήσεις αποθηκεύουν τα απόρρητά τους σε ηλεκτρονικά συστήματα στο εταιρικό δίκτυο που μπορεί να προσπελαστεί εξωτερικά.
- Με την εφαρμογή συστημάτων η/υ στη βιομηχανική παραγωγή, ολόκληρη η παραγωγή στηρίζεται στα υπολογιστικά συστήματα.
- Τα διεθνοποιημένα δίκτυα υπολογιστών είναι σήμερα απαραίτητα όχι μόνο για την οικονομία, αλλά και για τον δημόσιο τομέα και την κοινωνία, εν γένει
- Επιπλέον, οι υπολογιστές και του διαδίκτυο παίζουν ένα αυξημένο ρόλο στην εκπαίδευση και την ψυχαγωγία νέων και έτσι προκύπτουν αυξημένοι κίνδυνο για τα παιδιά.

Οι προκλήσεις του κυβερνοεγκλήματος

- Το ψηφιακό περιβάλλον προσφέρει εύφορο έδαφος για τη διάπραξη εγκλημάτων. Τα βασικά χαρακτηριστικά της ψηφιακής τεχνολογίας είναι τα εξής:
  - Κλίμακα
  - Προσβασιμότητα
  - Ανωνυμία
  - φορητότητα
  - Παγκόσμια εμβέλεια
  - Απουσία φυλάκων

Οι προκλήσεις του κυβερνοεγκλήματος

- *Α. Κλίμακα*
- Τα 4 δις χρηστών του διαδικτύου παρέχουν μια δεξαμενή για πιθανούς θύτες και θύματα. Αυτό δρα ως πολλαπλασιαστής που επιτρέπει να διαπράττονται αδικήματα σε μια κλίμακα που δεν μπορούσε να επιτευχθεί στην προψηφιακή εποχή. Η δυνατότητα αυτοματοποίησης, έχει περαιτέρω πολλαπλασιαστικά αποτελέσματα.

Οι προκλήσεις του κυβερνοεγκλήματος

- *Β. Προσβασιμότητα*

- Παλαιότερα, οι υπολογιστές ήταν μεγάλου μεγέθους συστήματα (‘*mainframes*’) που τα χρησιμοποιούσαν οι κυβερνήσεις και τα πιστωτικά ιδρύματα. Κατά συνέπεια, τα ηλεκτρονικά εγκλήματα περιορίζονταν μόνο σε όσους είχαν πρόσβαση στους υπολογιστές αυτές και τις κατάλληλες γνώσεις. Σήμερα οι υπολογιστές είναι τμήμα της καθημερινής ζωής και η χρήση τους είναι εύκολη, με αποτέλεσμα να χρησιμοποιούνται από τους θύτες και τα θύματα.

- Μέσω του Διαδικτύου οι πιθανοί δράστες αποκτούν εύκολη πρόσβαση στο έγκλημα και μπορούν να βρουν άλλους συμμετόχους και να δημιουργηθούν εικονικές κοινότητες εγκληματιών.

Οι προκλήσεις του κυβερνοεγκλήματος

- C. *Ανωνυμία*

- Οι χρήστες του διαδικτύου έχουν ανώνυμη πρόσβαση σε αυτό, πράγμα που τους δίνει πλεονέκτημα στη διάπραξη εγκληματικών πράξεων.

- Οι δράστες μπορούν να αποκρύψουν την πραγματική τους ταυτότητα και η ψηφιακή τεχνολογία παρέχει τα μέσα για το σκοπό αυτό, είτε με τη χρήση proxy servers, spoofed email or IP addresses or ανωνυμοποιημένες υπηρεσίες emailers. Ακόμα και να δημιουργήσει κάποιος λογαριασμό εμαιλ μπορεί εύκολα. Με την κρυπτογράφηση προστατεύεται η εμπιστευτικότητα ενώ τα ψηφιακά ίχνη μπορούν να αποκρυβούν με μεγάλη ευκολία.

Οι προκλήσεις του κυβερνοεγκλήματος

- Η δικτύωση σημαίνει ότι τα δεδομένα μεταφέρονται μέσω πολλών δικαιοδοσιών πριν φτάσουν στον προορισμό τους και αυτό έχει ως συνέπεια να μην μπορούν να εντοπιστούν εύκολα τα ψηφιακά ίχνη των επικοινωνιών. Η πρόσβαση μέσω ασύρματων δικτύων χωρίς εξουσιοδότηση μπορεί επίσης να βοηθήσει στην κάλυψη της ταυτότητας του χρήση. Ενίοτε τα δεδομένα εσκεμμένα αποθηκεύονται σε δικαιοδοσίες όπου υπάρχει ευνοϊκή νομοθεσία.

Οι προκλήσεις του κυβερνοεγκλήματος

- *D. Φορητότητα*
- Σημαντική είναι η δυνατότητα της ψηφιακής τεχνολογίας για την αποθήκευση τεραστίων ποσοτήτων δεδομένων σε μικρό χώρο και της αντιγραφής τους χωρίς μείωση της ποιότητας. Τα αποθηκευτικά μέσα σήμερα έχουν μικρό όγκο και κόστος, ενώ τα αντίγραφα εικόνων ή ήχου μπορούν να μεταφερθούν σε εκατομμύρια παραλήπτες.

Οι προκλήσεις του κυβερνοεγκλήματος

- *Ε. Παγκόσμια εμβέλεια*
- Το ποινικό δίκαιο διέπεται από την αρχή της εδαφικότητας. Οι σύγχρονοι υπολογιστές ωστόσο έχουν επιφέρει αλλαγή παραδείγματος, καθώς τα άτομα επικοινωνούν απευθείας σε μεγάλες αποστάσεις και ένα έγκλημα μπορεί να εκδηλωθεί σε απομακρυσμένες τοποθεσίες. Δεν χρειάζεται, έτσι, θύμα και θύτης να βρίσκονται στην ίδια δικαιοδοσία.
- Προβλήματα στην εφαρμογή του νόμου.

Οι προκλήσεις του κυβερνοεγκλήματος

- *F. Έλλειψη φυλάκων*
- Η ψηφιακή τεχνολογία δημιουργεί πολλά προβλήματα στην επιβολή του δικαίου, καθώς χρειάζονται εξειδικευμένες γνώσεις για την αξιολόγηση των ψηφιακών πειστηρίων.
- Η ανάδειξη του διαδικτύου ως ενός χώρου ελευθερίας χωρίς επίβλεψη σημαίνει απουσία ελέγχου
- Το ρόλο αυτό αναλαμβάνουν οι παροχείς υπηρεσιών διαδικτύου, οι γονείς, οι διαχειριστές συστήματος κλπ.

Ορισμός του κυβερνοεγκλήματος

- 1.Εγκλήματα στα οποία στόχος του εγκλήματος είναι ο υπολογιστής (π.χ. hacking, επιθέσεις με ιούς, επιθέσεις DoS).
- 2. Αδικήματα στα οποία ο υπολογιστής χρησιμοποιείται ως μέσο για τη διάπραξή τους (π.χ. παιδική πορνογραφία, απάτη κλπ.).
- 3. Εγκλήματα στα οποία χρησιμοποιείται ο υπολογιστής παρέχει απόδειξη για την τέλεση του αδικήματος

Εναρμόνιση του νομοθετικού πλαισίου

- Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (2001).
- Η Σύμβαση έχει ως στόχο την εναρμόνιση των εθνικών διατάξεων του ουσιαστικού ποινικού δικαίου που αφορούν τα αδικήματα που διαπράττονται στον κυβερνοχώρο, παράλληλα, δε, προβλέπει διατάξεις δικονομικού ποινικού δικαίου οι οποίες είναι απαραίτητες για τη διερεύνηση και δίωξη τέτοιων αδικημάτων και αδικημάτων που διαπράττονται με η/υ, ενώ, ακόμα, θέτει τις βάσεις για άμεση και αποτελεσματική διεθνή συνεργασία.

Κυβερνοέγκλημα

- Η Σύμβαση αυτή κυρώθηκε με το ν. 4411/2016, με τον οποίο μεταφέρθηκαν στο ελληνικό δίκαιο και οι διατάξεις της οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών.

- Η οδηγία, η οποία είναι μέτρο ελάχιστης εναρμόνισης, προβλέπει την υποχρέωση των κρατών μελών να θεσπίσουν κανόνες για τον ορισμό ποινικών αδικημάτων και κυρώσεων στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών.

- α) παράνομη πρόσβαση σε συστήματα πληροφοριών, β) παράνομη παρεμβολή σε σύστημα, γ) παράνομη παρεμβολή σε δεδομένα, δ) παράνομη υποκλοπή και ε) εργαλεία για τη διάπραξη των ως άνω αδικημάτων

Κυβερνοέγκλημα και ασφάλεια πληροφοριών

- Ζητούμενο για την αποτροπή ηλεκτρονικών εγκλημάτων είναι η δημιουργία πλαισίου ασφάλειας δεδομένων και δικτύων η/υ.
- Οδηγία (ΕΕ) 2016/1148 «σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση»