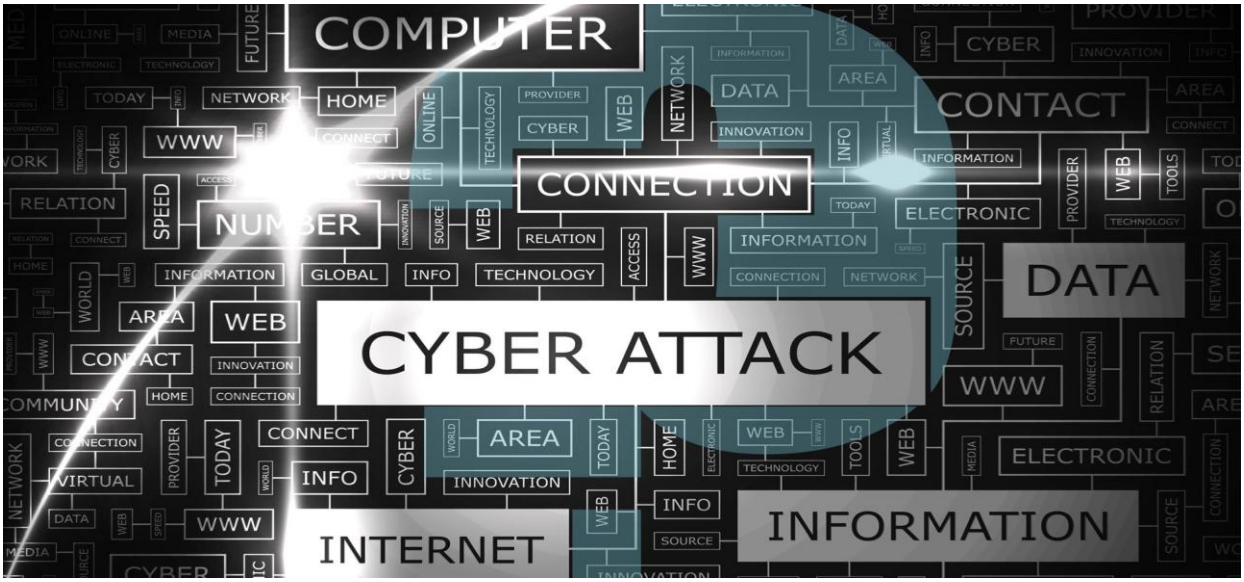
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΜΕ ΕΜΦΑΣΗ ΣΤΗ ΣΥΜΒΑΣΗ ΤΗΣ ΒΟΥΔΑΠΕΣΤΗΣ, ΤΗΝ ΟΔΗΓΙΑ 2013/40/Ε.Ε. ΚΑΙ ΤΟΝ ΝΟΜΟ 4411/2016.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Του

Κατσιαρμά Αλέξανδρου (Α.Μ. 16050)



Θεσσαλονίκη, Ιούνιος 2018

ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΜΕ ΕΜΦΑΣΗ ΣΤΗ ΣΥΜΒΑΣΗ ΤΗΣ ΒΟΥΔΑΠΕΣΤΗΣ, ΤΗΝ ΟΔΗΓΙΑ 2013/40/Ε.Ε. ΚΑΙ ΤΟΝ ΝΟΜΟ 4411/2016.

Κατσιαρμάς Αλέξανδρος

Πτυχίο Πληροφορικής και Επικοινωνιών του Τ.Ε.Ι. Σερρών

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσα Καθηγήτρια

Αλεξανδροπούλου Ευγενία

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/06/2018

Αλεξανδροπούλου Ευγενία	Χατζηγεωργίου Αλέξανδρος	Βεργίδης Κωνσταντίνος
.....	.....	.....

Περίληψη

Στα πλαίσια της παρούσας εργασίας έγινε προσπάθεια προσέγγισης του νομικού υπόβαθρου που αφορά στην αντιμετώπιση του εγκλήματος στον Κυβερνοχώρο τόσο σε επίπεδο Ε.Ε. αλλά και στην Ελλάδα. Αρχικά, εξετάζονται βασικές έννοιες και ορισμοί, όπως είναι το κυβερνοέγκλημα, το σύστημα πληροφοριών, αλλά και οι διάφορες μορφές επιθέσεων. Στη συνέχεια, αναλύεται η πρώτη προσπάθεια δημιουργίας νομικού πλαισίου με την υπογραφή της διεθνούς Σύμβασης της Βουδαπέστης το 2001, μία Σύμβαση την οποία η Ελλάδα θα υιοθετήσει αρκετά χρόνια αργότερα. Μόλις το 2005 η Ευρωπαϊκή Ένωση, μη μένοντας αδρανής στις αυξανόμενες επιθέσεις προχωρά στην έκδοση της Απόφασης-Πλαισίου 2005/222/ΔΕΥ. Μερικά χρόνια όμως αργότερα, το 2013, η διαρκώς αυξανόμενη πολυπλοκότητα των επιθέσεων, καθώς και άλλοι παράγοντες, οδήγησαν στην ψήφιση της Οδηγίας 2013/40/Ε.Ε., η οποία ήρθε να καλύψει τα κενά της προηγούμενης.

Στην Ελλάδα η εξέλιξη στην θέσπιση του κατάλληλου νόμου για το κυβερνοέγκλημα άργησε αρκετά να έρθει. Πριν το 2016 δεν υπήρχε νόμος που να αφορά ξεκάθαρα το κυβερνοέγκλημα και για το λόγο αυτό χρησιμοποιούνταν κυρίως ορισμένα άρθρα του Ποινικού Κώδικα. Ο νόμος 4411/2016 ήρθε επιτέλους να επικυρώσει τη Σύμβαση της Βουδαπέστης και να ενσωματώσει την Οδηγία 2013/40/Ε.Ε. στο ελληνικό νομικό δίκαιο, ενώ προσαρμόστηκαν και ορισμένα άρθρα του Ποινικού Κώδικα.

Είναι πλέον σαφές πως η προφύλαξη των συστημάτων των πληροφοριών, που τόσο πολύ επηρεάζουν τη ζωή μας, είναι μεγάλης σημασίας και για αυτό έχουν γίνει πολλά βήματα προς αυτή την κατεύθυνση. Σε διεθνές και ευρωπαϊκό επίπεδο τα μέτρα αυτά έχουν ληφθεί εδώ και αρκετά χρόνια, ενώ στην Ελλάδα η υιοθέτηση των μέτρων αυτών καθυστέρησε. Αναμφίβολα, τα επόμενα χρόνια θα φανεί η επάρκεια ή μη του υπάρχοντος νομικού πλαισίου δεδομένου ότι η τεχνολογία εξελίσσεται διαρκώς και αντίστοιχη εξέλιξη πιθανότατα θα υπάρξει και στις μορφές κυβερνοεγκλημάτων.

Abstract

In the context of this paper, an attempt was made to analyse the legal background which is relevant to cybercrime both in E.U. and in Greece. Firstly, basic definitions are examined, such as cybercrime, system of information and some forms of attack. The first attempt to create a legal framework is made with the signing of the Budapest Convention on Cybercrime in 2001, which is going to be adopted by Greece many years later. In 2005 the European Union issued the Council Framework Decision 2005/222 after the increasing number of attacks. Some years later in 2013, European Union voted the Directive 2013/40 due to the fact that attacks had been even more complicated and some other reasons. The last Directive came to fill the gaps that the previous Framework Decision had left.

In Greece the establishment of a proper law for the treatment of Cybercrime came many years later. Before 2016 there was not any law which would clearly refer to cybercrime. Therefore, the only legal background that it was used for such cases, was some articles of Criminal Code. Finally, the law 4411/2016 was voted in order to embody the Budapest Convention and the Directive 2013/40 to Greek law. Simultaneously, some articles of Criminal Code were adapted accordingly to the new law.

It has been clear that the protection of systems of information is a very serious issue. Internationally and at European level many measures have been taken the last 20 years, in contrast to Greece, where the same measures were taken many years later. Undoubtedly, in the next years we will see if the existing legal background is adequate, given the fact that both technology and cybercrime attacks will continue to be developed and get more complicated.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Η πληροφορική αποτελεί, πλέον, αναπόσπαστο τμήμα της ανθρώπινης ζωής. Οι υπολογιστές έχουν καταστεί απαραίτητα εργαλεία σε κάθε επαγγελματική δραστηριότητα. Χάρη στην αλματώδη εξέλιξη της Πληροφορικής Τεχνολογίας και της ψηφιοποίησης, το σύνολο των ανθρωπίνων δραστηριοτήτων εκδηλώνεται μέσω των νέων τεχνολογιών και των ηλεκτρονικών συστημάτων επικοινωνίας. Το νέο αυτό τοπίο έχει ονομαστεί Κοινωνία της Πληροφορίας και έχει οδηγήσει σε άνευ προηγουμένου κοινωνικές και οικονομικές αλλαγές. Με την άνοδο της τεχνολογίας, τη διείσδυση των πληροφορικών συστημάτων τόσο έντονα στη ζωή μας και την αλματώδη επιρροή του Διαδικτύου, *έγινε αντιληπτή η ανάγκη για αυξημένα μέτρα νομικής προστασίας των πληροφορικών συστημάτων εν γένει λόγω και της ολοένα αυξανόμενης ηλεκτρονικής εγκληματικότητας*. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Στην παρούσα εργασία, θα ασχοληθούμε με την έννοια και τη στοιχειοθέτηση της ηλεκτρονικής εγκληματικότητας και κυρίως με το νομικό πλαίσιο και αντιμετώπισής της που έχει καθιερωθεί σε διεθνές και ενωσιακό επίπεδο, μετά την σύναψη της Σύμβασης της Βουδαπέστης, που προσδιόρισε ουσιαστικά για πρώτη φορά στο νομικό κόσμο, την στοιχειοθέτηση των εν λόγω ηλεκτρονικών εγκλημάτων καθώς και τη προσαρμογή τους στα ελληνικά δεδομένα, με τη ψήφιση του Ν. 4411/2016. Τέλος, θα γίνει μία συγκριτική επισκόπηση με τα ήδη στοιχειοθετημένα από τον Έλληνα νομοθέτη, ηλεκτρονικά εγκλήματα και τις αλλαγές που επέφερε ο Ν.4411/2016 στην ελληνική έννομη τάξη, καθώς και κριτική ανάλυση επί των νέων στοιχείων που εισήγαγε ο νόμος-θεμέλιο για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας στη χώρα μας.

ΚΕΦΑΛΑΙΟ 1^{ο} : Ηλεκτρονικά Εγκλήματα : Έννοια, διακρίσεις στο διεθνές νομικό σύστημα και συστήματα πληροφοριών

1.1. Έννοια και διάκριση ηλεκτρονικών εγκλημάτων

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime), με χαρακτηριστικό παράδειγμα την παράνομη αντιγραφή απόρρητων δεδομένων και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκαν μέσω του Διαδικτύου. Για την αποτελεσματικότερη καταγραφή των ηλεκτρονικών εγκλημάτων, διακρίνουμε δύο βασικές κατηγορίες : Τα εγκλήματα που δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και δικτύων, τα οποία χαρακτηρίζονται ως γνήσια και τα εγκλήματα, των οποίων η νομοτυπική μορφή προϋπήρχε των ηλεκτρονικών υπολογιστών, μπορούν όμως να τελεσθούν και με τη χρήση ή βοήθεια ηλεκτρονικού υπολογιστή[1].

1.2. Χαρακτηριστικά του Κυβερνοεγκλήματος

Με την αλματώδη αύξηση του Διαδικτύου, τα Κυβερνοεγκλήματα αποτελούν την συχνότερη μορφή ηλεκτρονικών εγκλημάτων που αντιμετωπίζουμε στην καθημερινότητα μας. Το Κυβερνοέγκλημα ως ειδικότερη έκφανση του ηλεκτρονικού εγκλήματος φέρει τα ακόλουθα χαρακτηριστικά, που καθιστούν την ποινική του δίωξη δυσχερή :

1. Ταχύτητα – Η διάπραξη των σχετικών πράξεων λαμβάνει χώρα σε ελάχιστο χρόνο και συχνά δεν γίνεται αντιληπτή από το θύμα.
2. Ευκολία – Η διάπραξη των σχετικών πράξεων είναι εύκολη και γίνεται από τον ηλεκτρονικό υπολογιστή και τον οικείο χώρο του δράστη, ενώ συχνά δεν αφήνει ίχνη.
3. Ανωνυμία – Η διάπραξη κυβερνοεγκλημάτων εκμεταλλεύεται την σχετική ανωνυμία, που προσφέρουν ορισμένες τεχνολογικές υποδομές του διαδικτύου.

[1] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2003, σελ. 38

4. Διασυνοριακός Χαρακτήρας – Οι προπαρασκευαστικές ενέργειες, οι πράξεις αλλά και τα αποτελέσματα του κυβερνοεγκλήματος συνήθως λαμβάνουν χώρα ταυτοχρόνως σε πολλές δικαιοδοσίες. Θα μπορούσε να χαρακτηριστεί ως έγκλημα «δίχως πατρίδα», παρόλο που τα αποτελέσματα του μπορούν να γίνουν ταυτόχρονα αισθητά σε πολλούς τόπους
5. Δυσχέρεια στην Διερεύνηση – Ο διασυνοριακός χαρακτήρας αλλά και τα ψηφιακά ίχνη του Κυβερνοεγκλήματος δυσχεραίνουν τη διερεύνηση και εξιχνίασή του. Κατά κανόνα, είναι εξαιρετικά δύσκολο να προσδιοριστεί ο τόπος τελέσεως του Κυβερνοεγκλήματος, πόσο μάλλον ο δράστης του.
6. Διακρατική Συνεργασία – Ο διασυνοριακός χαρακτήρας του κυβερνοεγκλήματος απαιτεί την διακρατική συνεργασία των διωκτικών αρχών. Για παράδειγμα, η εκδήλωση του μπορεί να καταγράφεται σε μία Α χώρα, όμως τα αποδεικτικά στοιχεία του εγκλήματος να βρίσκονται στην άλλη άκρη του πλανήτη ή ακόμα και σε διαφορετικές τοποθεσίες. Γι΄ αυτό κρίνεται απαραίτητη η συνεργασία διαφορετικών κρατών για την διερεύνηση αυτών των εγκλημάτων, άλλωστε είναι σπάνιες οι περιπτώσεις που περιορίζονται στα όρια ενός μόνο κράτους[2].
7. Έλλειψη Επαρκούς Καταγραφής – Το μέγεθος των τελούμενων κυβερνοεγκλημάτων είναι δυσανάλογα μεγαλύτερο των καταγεγραμμένων περιστατικών[3]. Δεν υπάρχουν επαρκή στατιστικά στοιχεία καθώς ελάχιστες περιπτώσεις Κυβερνοεγκλημάτων καταγγέλλονται. Η αστυνομική του διερεύνηση, δε, χρειάζεται άριστη εξειδίκευση και γνώσεις.

1.3. Μορφές Κυβερνοεγκλημάτων

Ορισμένα χαρακτηριστικά παραδείγματα κυβερνοεγκλημάτων, όπως έχουν καταγραφεί στο διεθνές νομικό σύστημα είναι τα ακόλουθα :

- **Κακόβουλες εισβολές σε δίκτυα (hacking)**

Η εισβολή σ' ένα δίκτυο υπολογιστών, το λεγόμενο hacking, αποτελεί βασικό στοιχείο πολλών διαδικτυακών εγκλημάτων:

[2] Αγγελής Ι., « Διαδίκτυο (Internet) και ποινικό Δίκαιο», ΝοΒ 2000, σελ. 677
[3] Steven Furnel, «Κυβερνοέγκλημα», 2006, σελ. 25-27

«Χάκερ (Hacker) *ονομάζεται το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ένας χάκερ έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα».* Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες με σκοπό να προσπορίσουν παράνομα οικονομικό όφελος, να δημιουργήσουν ζημιά σε μια ιστοσελίδα, να κλέψουν δεδομένα, να φτιάξουν ιούς με κακό σκοπό, τότε αποκαλούνται ως **Κράκερ**.

Η πρόσβαση ενός hacker στο σύστημα του υποψήφιου θύματός του προϋποθέτει δύο στάδια: ένα προπαρασκευαστικό και ένα κύριο.

Αρχικά στο προπαρασκευαστικό στάδιο ο hacker συγκεντρώνει πληροφορίες (information gathering) για το σύστημα που επιθυμεί να προσβάλλει και προσπαθεί να αποκτήσει πρόσβαση σ' αυτό αποκτώντας τους κωδικούς εισόδου (password cracking), αποκτώντας έτσι τα δικαιώματα (privileges) ενός νόμιμου χρήστη του συστήματος[4].

- **Διασπορά κακόβουλου λογισμικού**

Ένα από τα πλέον διαδεδομένα εγκλήματα ηλεκτρονικού βανδαλισμού είναι η διασπορά κακόβουλου κώδικα (malicious code), όπου η δημιουργία του κώδικα αυτού γίνεται με σκοπό να προκαλέσει ζημία σε έναν ηλεκτρονικό υπολογιστή για την υποκλοπή ή αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων[5]. Το συγκεκριμένο έγκλημα, τυποποιείται στο ελληνικό ποινικό δίκαιο με το άρθρο 381 του ΠΚ (Φθορά Ηλεκτρονικών Δεδομένων). Ο κώδικας διακρίνεται σε τέσσερις βασικές κατηγορίες, οι οποίες αναλύονται στη συνέχεια.

α. Ιός (Virus): Ένας ιός υπολογιστών είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να

[4] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2003, σελ.41

[5] Eric J. Sinrod and William P. Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", 2000, σελ. 62

υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, μπορούν να δημιουργήσουν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να μην είναι δυνατή η ανάκτηση ολόκληρου του περιεχομένου του. Επιπλέον, πολλοί ιοί είναι, από τη δημιουργία τους, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

β. Δούρειος Ίππος (Trojan): είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης. Λογισμικό αυτού του είδους παριστάνει ότι είναι χρήσιμο για τον υπολογιστή αλλά στην πραγματικότητα μέσα από αυτό κάποιοι εγκληματίες καταφέρνουν να κλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο του συστήματος. Τις περισσότερες φορές το συγκεκριμένο λογισμικό δεν έχει στόχο τη μόλυνση του υπολογιστή, δηλαδή δεν αναπαράγεται, και για αυτό τα προγράμματα αυτά δεν χαρακτηρίζονται και επίσημα ως ιοί.

γ. Σκουλήκι (Worm): είναι κακόβουλο λογισμικό, παρόμοιο με τους ιούς, το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Ωστόσο, η διαφορά του έγκειται στο να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται, έχοντας τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντάς το με άχρηστη δραστηριότητα.

δ. Rootkit: είναι λογισμικό το οποίο μπορεί να ανήκει πολύ εύκολα σε οποιαδήποτε από τις παραπάνω κατηγορίες. Αυτό το λογισμικό έχει την ιδιαιτερότητα να κρύβει κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας. Αυτά τα προγράμματα κάποιες φορές λειτουργούν προστατευτικά έναντι των χάκερ διαγράφοντας τις πληροφορίες του εισβολέα.

- **Ανεπιθύμητη Αλληλογραφία (Spamming)**

Η ανεπιθύμητη αλληλογραφία ορίζεται ως η χρήση οποιουδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες[6]. Ένα μήνυμα spam, αποστέλλεται μέσω e-mail και έχει, συνήθως, σκοπό διάδοσης και προώθησης προϊόντων μίας εταιρίας.

- **Επιθέσεις σε δικτυακούς τόπους**

Οι επιθέσεις αυτές αποτελούν μία από τις πλέον διαδεδομένες μορφές ηλεκτρονικών εγκλημάτων, ένα φαινόμενο ηλεκτρονικού βανδαλισμού, όπου οι βάνδαλοι σε ένα πληροφορικό σύστημα με σκοπό να αλλοιώσει και να επηρεάσει το περιεχόμενο ενός δικτυακού τόπου και διακρίνονται στις **Επιθέσεις αλλοίωσης περιεχομένου** και στις **Επιθέσεις άρνησης υπηρεσίας (DDOS attacks),** ένα ξεχωριστό κυβερνοέγκλημα που θα αναλυθεί, περαιτέρω σε παρακάτω κεφάλαιο[7].

- **Phising και Pharming**

Οι εν λόγω επιθέσεις χρησιμοποιούνται από τους hackers, με σκοπό την απόσπαση προσωπικών πληροφοριών, ώστε να χρησιμοποιηθούν σε παράνομες δραστηριότητες, μέσω της εξαπάτησης του θύματος με ένα παραπλανητικό e-mail, θυμίζοντας μία μέθοδο «ηλεκτρονικού ψαρέματος».

- **Πειρατεία λογισμικού**

«Ο όρος πειρατεία λογισμικού, αναφέρεται στην αναπαραγωγή ή στη διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί

[6] Ε. Μεταξάκης, "Η ποινική αντιμετώπιση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας", ΝοΒ, 2014, σελ. 59
[7] Γρ. Λάζος, "Πληροφορική και έγκλημα", 2001, σελ.109

πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους». Η ψηφιακή μορφή των εν λόγω εφαρμογών, καθιστά εύκολη την αναπαραγωγή τους σε διάφορα αντίγραφα[8]. Παρά τα διάφορα τεχνολογικά μέτρα προστασίας που εφαρμόζουν οι εταιρίες παραγωγής λογισμικού στα προϊόντα τους, οι hackers (crackers) πάντα βρίσκουν τρόπους παράκαμψης, απενεργοποιώντας κωδικούς, κλειδιά και ότι άλλο χρησιμοποιείται για την εν λόγω προστασία.

Τέλος, καταγράφονται πολλά από τα ήδη υπάρχοντα εγκλήματα του κοινού ποινικού δικαίου, ως ηλεκτρονικά, επειδή το μέσο τέλεσης τους είναι ο ηλεκτρονικός υπολογιστής. Συνοπτικά, ορισμένα από αυτά είναι : Η απάτη μέσω υπολογιστή είτε με e-mail είτε μέσω πιστωτικών καρτών (Αρ.386^{A} ΠΚ), η κλοπή ταυτότητας (Identity Theft), το ξέπλυμα χρήματος, η διακίνηση πορνογραφικού υλικού και το ολοένα αυξανόμενο έγκλημα του cyberbullying γνωστό ως εκφοβισμός μέσω διαδικτύου.

1.4. Συστήματα πληροφοριών : Ορισμός και μορφές επιθέσεων

Όπως, προαναφέρθηκε, μία από τις πιο ενδιαφέρουσες μορφές ηλεκτρονικής εγκληματικότητας με ολοένα και συχνότερο ρυθμό εμφάνισης, είναι οι επιθέσεις σε συστήματα πληροφοριών, όπου διακρίνουμε δύο κατηγορίες: τις **Επιθέσεις αλλοίωσης περιεχομένου** και τις **Επιθέσεις άρνησης υπηρεσίας (DDOS attacks).** Για να κατανοήσουμε περαιτέρω, όμως, την ανάλυση των τρόπων επίθεσης στα συστήματα πληροφοριών, θα πρέπει πρωτίστως να δούμε τι ορίζεται ως σύστημα πληροφοριών. Στην έννοια του συστήματος πληροφοριών συμπεριλαμβάνονται πέντε στοιχεία, τα οποία σε πλήρη συνεργασία εξυπηρετούν τους εκάστοτε σκοπούς δημιουργίας του συστήματος πληροφοριών. Τα πέντε αυτά στοιχεία είναι τα δεδομένα (Data) , ο ανθρώπινος παράγοντας, το υλικό των ηλεκτρονικών υπολογιστών (Hardware), το λογισμικό (Software) και οι διαδικασίες (Procedures) που ορίζονται από τον χρήστη.

Η πλέον πρόσφατη οδηγία 2013/40 της Ε.Ε. ορίζει το σύστημα πληροφοριών ως «τη συσκευή ή την ομάδα διασυνδεδεμένων συσκευών ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που

[8] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», σελ.61,2003

αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και την συντήρηση τους»[9].

Όσον αφορά την πρώτη κατηγορία επιθέσεων, τις Επιθέσεις αλλοίωσης περιεχομένου, αυτές αφορούν τις πληροφορίες που διακινούνται στα συστήματα και έχουν ως αποτέλεσμα είτε την παράνομη προσθήκη νέων πληροφοριών, είτε την διαγραφή των υπαρχουσών είτε την παράνομη επεξεργασία τους.

Η δεύτερη και συχνότερη κατηγορία επιθέσεων, οι Επιθέσεις άρνησης υπηρεσίας (DDOS attacks), αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή, ώστε να μη μπορεί να εξυπηρετήσει άλλους υπολογιστές. Επιτίθεται, δηλαδή, ενάντια στα ίδια τα συστήματα πληροφοριών[10].

Οι επιθέσεις που στρέφονται ενάντια στα ίδια τα συστήματα μπορούν να προσβάλλουν δύο γενικές αρχές:

- Την εμπιστευτικότητα, με την παράνομη πρόσβαση
- Την ακεραιότητα, με την καταστροφή ή αδρανοποίηση ενός συστήματος

Αυτή η κατηγορία επιθέσεων ανήκει σε αυτές που επηρεάζουν όλο το πληροφοριακό σύστημα, καθώς δεν επιτρέπουν την εξυπηρέτηση του νόμιμου χρήστη. Λαμβάνοντας ως δεδομένο πως ο κάθε εξυπηρετητής - server μπορεί να εξυπηρετήσει συγκεκριμένο αριθμό ερωτημάτων από τους χρήστες, η συμφόρηση του εξυπηρετητή σημαίνει αδυναμία εξυπηρέτησης. Μερικοί από τους πιο διαδεδομένους τρόπους τέτοιας μορφής επίθεσης είναι να μειωθούν στο ελάχιστο οι διαθέσιμοι πόροι και να μπλοκάρει το σύστημα ή ακόμα και να αποσυνδεθούν συσκευές από το υλικό (hardware) του συστήματος.

Σε αυτή τη μορφή επιθέσεων ανήκουν οι εξής ακόλουθες κατηγορίες:

Η επίθεση "Smurf", η επίθεση Fraggle, η Ping Flood, η Ping of Death, η Land, SYN Flood, η Teardrop και η επίθεση Slow HTTP DoS.

Η επίθεση **Smurf,** η οποία ονομάστηκε έτσι από το πρώτο πρόγραμμα που την έκανε πράξη, μπλοκάρει το θύμα-σύστημα στέλνοντας διαρκώς πακέτα ping ICMP Echo Reply σε

[9] Βλέπε Οδηγία 2013/40/Ε.Ε., https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33193
[10] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2003, σελ.42

διευθύνσεις IP Broadcast που ανήκουν σε διάφορα δίκτυα. Οι διευθύνσεις αυτές έπειτα στέλνουν τα πακέτα στους υπολογιστές του δικτύου τους και με τον τρόπο αυτό ενισχύουν την επίθεση (Smurf Amplifiers). Ακολουθεί η απάντηση από την πλευρά των υπολογιστών στο ping που δημιούργησε ο θύτης με πακέτα Echo Request. Η σημαντική λεπτομέρεια που κάνει τη διαφορά είναι πως κατά την δημιουργία του ping ο θύτης δεν βάζει τη δική του διεύθυνση, αλλά του θύματος. Έτσι, το σύστημα-θύμα δέχεται πολλαπλές απαντήσεις σε ένα ping που υποτίθεται πως δημιούργησε το ίδιο σε τέτοιο σημείο που εξαντλούνται οι πόροι του και αρνείται την εξυπηρέτηση στους νόμιμους χρήστες του.

Μια επίθεση **Fraggle** δρα ακριβώς σαν την προηγούμενη της επίθεση Smurf με την μόνη διαφορά το ότι η επίθεση Fraggle χρησιμοποιεί το σπανιότερο πρωτόκολλο User Datagram Protocol {UDP} από το πιο συνηθισμένο Transmission Control Protocol {TCP} Η επίθεση Fraggle θεωρείται ξεπερασμένη διότι τα πιο πολλά προγράμματα antivirus την αποτρέπουν.

Με την επίθεση **Teardrop,** ο επιτιθέμενος μπορεί και χρησιμοποιεί ένα πρόγραμμα με όνομα Teardrop με το οποίο χωρίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στα πεδία των πακέτων. Όταν ο στόχος του επιτιθέμενου προσπαθήσει να συναρμολογήσει αυτά τα τμήματα, θα κολλήσει ή θα προχωρήσει σε επανεκκίνηση.

Η επίθεση **SYN Flood** έχει ως εξής : Ο επιτιθέμενος αποστέλλει στον διακομιστή-θύμα πολλαπλά πακέτα SYN. Ο διακομιστής θεωρεί ότι τα πακέτα αυτά προέρχονται από κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει. Επειδή για κάθε ημιτελή σύνδεση TCP ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όριά του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρήστες. Αποτέλεσμα είναι η δέσμευση των πόρων του διακομιστή, που μπορεί να οδηγήσει στη πλήρη κατάρρευση του.

Η επίθεση **LAND** περιλαμβάνει την αποστολή ενός ειδικού μολυσμένου πακέτου σε έναν υπολογιστή με σκοπό να τον κάνει να "κολλήσει". Ο επιτιθέμενος στέλνει στο θύμα ένα ειδικά κατασκευασμένο πακέτο TCP SYN (έναρξη σύνδεσης TCP/IP). Στα πεδία αποστολέας και παραλήπτης της κεφαλίδας αυτού του ειδικά κατασκευασμένου TCP πακέτου βρίσκεται η διεύθυνση IP του θύματος. Η παραλαβή ενός τέτοιου πακέτου οδηγεί

τον υπολογιστή του θύματος να απαντά στον εαυτό του συνέχεια και κατά συνέπεια να καθίσταται μη λειτουργικός. Συνεπώς, το χαρακτηριστικό της επίθεσης LAND που την διαχωρίζει από άλλες επιθέσεις είναι ότι το πακέτο που στέλνεται έχει ως αποστολέα και παραλήπτη την διεύθυνση IP του θύματος[11].

Κατά την επίθεση **Ping of Death,** ο επιτιθέμενος υπολογιστής αποστέλλει σε έναν άλλο υπολογιστή κακοσχηματισμένα μηνύματα ping με σκοπό να τον θέσει εκτός λειτουργίας.

Η επίθεση **Ping Flood** είναι μία διαδικτυακή εφαρμογή, μέσω της οποίας ο επιτιθέμενος αποστέλλει μαζικά μηνύματα ping σε μία διεύθυνση IP. Σ' αυτά τα μηνύματα, ο server είναι αναγκασμένος να απαντήσει, δαπανώντας μέρος της υπολογιστικής του ισχύος, έχοντας ως επακόλουθο να μην διαθέτει άλλους πόρους και να μην μπορεί να προσφέρει σε άλλες υπηρεσίες.

Τέλος, η επίθεση **Slow HTTP Dos** αφορά στην αποστολή αιτήματος σύνδεσης http σε έναν υπολογιστή, αλλά όταν ο τελευταίος απαντήσει, τότε ο επιτιθέμενος υπολογιστής σκόπιμα καθυστερεί στην λήψη της απάντησης του. Την τακτική αυτή ακολουθούν αρκετοί υπολογιστές μαζικά με αποτέλεσμα ο επιτιθέμενος υπολογιστής τελικά να μην μπορεί να προσφέρει την οποιαδήποτε υπηρεσία.

ΚΕΦΑΛΑΙΟ 2^{ο} : Το νομικό πλαίσιο των ηλεκτρονικών εγκλημάτων στο διεθνές νομικό σύστημα και στην Ευρωπαϊκή Ένωση

2.1. Σύμβαση της Βουδαπέστης

Το ηλεκτρονικό έγκλημα, όπως προαναφέρθηκε παραπάνω, είναι ένα ιδιαίτερο έγκλημα, που διαφέρει και ουσιαστικά αλλά και τεχνικά από το συμβατικό έγκλημα. Για να μπορέσει να αντιμετωπιστεί αρκούντως η τέλεση τους, χρειάζονται ρυθμίσεις τόσο σε επίπεδο ουσιαστικού δικαίου όσο και δικονομικού δικαίου. Λαμβάνοντας ως δεδομένο, πως η τεχνολογία «καλπάζει σε γοργούς ρυθμούς» τις τελευταίες δεκαετίες, συνακόλουθα η ηλεκτρονική εγκληματικότητα αλλάζει και εξελίσσεται, οι νομοθετικές ρυθμίσεις που θα καθορίσουν το δίκαιο κατά των ηλεκτρονικών εγκλημάτων και ιδιαιτέρως, κατά των

[11] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2003, σελ. 45

κυβερνοεγκλημάτων, θα τίθενται πολύ γρήγορα σε αμφισβήτηση. Υπό αυτό το πρίσμα, κρίθηκε απαραίτητη η θέσπιση ενός ενιαίου νομοθετικού πλαισίου που θα ορίσει αφ' ενός και θα αποτυπώσει την ηλεκτρονική εγκληματικότητα, η οποία μέχρι τότε δε μπορούσε να οριστεί νομοτεχνικά με ακρίβεια, αφετέρου να ρυθμίσει δικονομικά και ουσιαστικά το σύνολο αυτών των αδικημάτων.

Η διεθνής κοινότητα δεν έμεινε αδιάφορη μπροστά στην ολοένα και αυξανόμενη ηλεκτρονική εγκληματικότητα, διαπιστώνοντας την ανάγκη για την ύπαρξη ενός κατάλληλου νομοθετικού πλαισίου για την καταπολέμηση του εγκλήματος στο κυβερνοχώρο[12]. Το Διαδίκτυο και η χρήση των Η/Υ εξαπλωνόταν ραγδαία και ήταν φυσικό επακόλουθο να εξαπλώνονται και τα προβλήματα που το αφορούσαν.

Τον Νοέμβριο του 1996 η Ευρωπαϊκή Επιτροπή για τα ποινικά θέματα (European Comitte on Crime Problems- CDPC) με την απόφασή της CDPC/103/211196, εισηγήθηκε την δημιουργία μίας ξεχωριστής επιτροπής εμπειρογνωμόνων που θα αντιμετώπιζε βάσει ενός νέου νομοθετικού πλαισίου, το έγκλημα στον Κυβερνοχώρο[13]. Για την ακρίβεια, η Ευρωπαϊκή Επιτροπή εξήγησε πως «με τη σύνδεση τους σε υπηρεσίες επικοινωνιών και πληροφορίας, οι χρήστες δημιουργούν ένα είδος κοινού χώρου, που καλείται κυβερνοχώρος και ο οποίος χρησιμοποιείται για θεμιτούς σκοπούς, αλλά μπορεί να γίνει και αντικείμενο κακοπροαίρετης χρήσης. Αυτά τα αδικήματα του κυβερνοχώρου είτε διαπράττονται ενάντια στην ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριακών συστημάτων και των τηλεπικοινωνιακών δικτύων είτε προκύπτουν από την χρήση των υπηρεσιών τέτοιων δικτύων για να διαπραχθούν παραδοσιακά εγκλήματα». Μεταξύ των υπόλοιπων Συστάσεων επί του θέματος, η Επιτροπή έλαβε υπόψη της και την έκθεση που συνέταξε κατ' απαίτηση της ο καθηγητής H.W.K. Kaspersen ο οποίος κατέληξε στο ότι «θα πρέπει να στραφεί σε ένα άλλο νομικό όργανο μεγαλύτερης δεσμευτικότητας από ότι έχει μία Σύσταση, όπως μία Σύμβαση. Αυτή η σύμβαση δεν θα πρέπει να ασχολείται μόνο με θέματα ουσιαστικού ποινικού δικαίου, αλλά και με ερωτήματα ποινικού περιεχομένου καθώς και διεθνείς ποινικές διαδικασίες και συμφωνίες.»

[12] Αγγελής Ι. « Διαδίκτυο και ποινικό δίκαιο», ΝοΒ, 2000, σελ.680

[13] Βλέπε Αιτιολογική Έκθεση της Σύμβασης για την καταπολέμηση του Κυβερνοεγκλήματος—χExplanatory Report to the Convention on Cybercrime, CETS (Council of Europe Treaty Series) 185, https://rm.coe.int/16800cce5b

Βάσει της πρότασης της Ευρωπαϊκής Επιτροπής, το Συμβούλιο των Υπουργών προχώρησε στην δημιουργία της Επιτροπής των Εμπειρογνωμόνων για το Έγκλημα στον Κυβερνοχώρο (Committee of Experts on Crime in Cyber-space (PC-CY)). Η εν λόγω Επιτροπή ξεκίνησε τις εργασίες της τον Απρίλη του 1997 με στόχο να τις έχει ολοκληρώσει έως τον Δεκέμβριο του 1999. Έως τον Δεκέμβριο του 2000 η Επιτροπή είχε συνεδριάσει 10 φορές ως ολομέλεια και άλλες 15 φορές είχαν γίνει ανοιχτού τύπου συναντήσεις με την προπαρασκευαστική ομάδα. Έπειτα από πολλές συνεδριάσεις και προσχέδια η Ευρωπαϊκή Επιτροπή CDPC στην 50η συνεδρίαση της τον Ιούνιο του 2001 είχε έτοιμο το προσχέδιο το οποίο κατατέθηκε στο Συμβούλιο των Υπουργών για ψήφιση.

Στις 23 Νοεμβρίου 2001 στη Βουδαπέστη υπογράφηκε μεταξύ 30 χωρών, εκ των οποίων οι 26 ήταν μέλη του Ευρωπαϊκού Συμβουλίου και 4 παρατηρητές-μη μέλη (Καναδάς, Ιαπωνία, Νότια Αφρική και Η.Π.Α) η πρώτη διεθνής σύμβαση για την καταπολέμηση του κυβερνοεγκλήματος (Convention on Cybercrime). Δύο χρόνια αργότερα, τον Ιανουάριο του 2003 η σύμβαση συμπληρώθηκε από το Πρόσθετο Πρωτόκολλο, το οποίο αφορούσε την ποινικοποίηση της εξάπλωσης του ρατσισμού και της ξενοφοβίας μέσω του Διαδικτύου. Θα πρέπει να σημειωθεί πως σύμφωνα με το άρθρο 36 παρ. 3 της Συμβάσεως για να τεθεί σε ισχύ θα έπρεπε να υπογραφεί από πέντε μέλη εκ των οποίων τα τρία έπρεπε να είναι μέλη του Συμβουλίου της Ευρώπης. Η σύμβασή ως ένα πρωτότυπο νομοθετικό κείμενο, το πρώτο που ασχολείται επιστάμενα με τα εγκλήματα στον κυβερνοχώρο, θέτει τους σκοπούς της συμβάσεως, διακηρύσσοντας πως ο σεβασμός των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, όπως αποτυπώνονται στη Σύμβαση του 1950 του Συμβουλίου της Ευρώπης, κατά την κατάρτιση της Συμβάσεως, είναι υψίστης σημασίας.

Οι στόχοι της Σύμβασης ήταν να εναρμονίσει το ουσιαστικό ποινικό δίκαιο, το δικονομικό ποινικό δίκαιο και να θεσπίσει ένα αποτελεσματικό και ταχύτατο σύστημα συνεργασίας σε διεθνές επίπεδο. Σύμφωνα με την αιτιολογική έκθεση της Σύμβασης για το Κυβερνοέγκλημα, σκοπός της Συμβάσεως είναι η εναρμόνιση των εθνικών νομοθεσιών σε ό,τι αφορά την ποινικοποίηση συγκεκριμένων συμπεριφορών και η καθιέρωση μιας κοινής αντεγκληματικής πολιτικής που στοχεύει στην προστασία της Κοινωνίας των Πληροφοριών από τους εγκληματίες του διαδικτύου. Επιπροσθέτως, στοχεύει στην θέσπιση εσωτερικών δικονομικών ποινικών διατάξεων για την δίωξη και εκδίκαση των ηλεκτρονικών εγκλημάτων

στο σύνολο τους[14]. Γενικότερα, η Σύμβαση προσφέρει ένα πρώτο δικαιικό πλαίσιο που θα διέπει τον χώρο του Διαδικτύου, όμως, σύμφωνα και με τους επικριτές της, δεν πρόσφερε κάτι καινούριο στο θέμα της δικαιοδοσίας, ένα ζήτημα με έντονο δικονομικό ενδιαφέρον[15].

Αναλυτικότερα :

Πρώτο μέρος- Άρθρο 1

Στο πρώτο μέρος της Σύμβασης αναφέρονται ορισμένοι ορισμοί όρων που θα βοηθήσουν στην θέσπιση των μετέπειτα κανόνων. Ο πρώτος ορισμός αφορά το σύστημα υπολογιστή, το οποίο περιγράφεται ως μία συσκευή ή των σύνολο των συσχετιζόμενων συσκευών το οποίο συνοδεύεται από ένα πρόγραμμα και επεξεργάζεται αυτόματα δεδομένα με τη βοήθεια του. Μάλιστα, ως πρόγραμμα ορίζεται το σύνολο των οδηγιών που εκτελούνται από τον υπολογιστή για να επιτευχθεί το επιθυμητό αποτέλεσμα. Συμπληρώνοντας τον ορισμό, η αιτιολογική έκθεση αναφέρει πως με τον όρο «αυτόματα» εννοείται η επεξεργασία χωρίς ανθρώπινη παρέμβαση και η «επεξεργασία δεδομένων» σημαίνει την διαχείριση τους μέσω ενός προγράμματος στον υπολογιστή. Ένα σύστημα υπολογιστή αποτελείται συνήθως από τον επεξεργαστή ή αλλιώς την κεντρική μονάδα επεξεργασίας και τις περιφερειακές συσκευές. Η περιφερειακή συσκευή είναι μία συσκευή η οποία εκτελεί συγκεκριμένες λειτουργίες σε συνεργασία με την κεντρική μονάδα επεξεργασίας. Παραδείγματα περιφερειακών συσκευών είναι ένας εκτυπωτής, μία οθόνη κ.τ.λ.

Το δίκτυο είναι μία διασύνδεση ανάμεσα σε δύο ή περισσότερα συστήματα υπολογιστών. Η διασύνδεση μπορεί να είναι ενσύρματη (καλώδιο ή σύρμα) ή ασύρματη (ραδιοκύματα, υπέρυθρες ή δορυφορικές) ή και τα δύο. Ένα δίκτυο μπορεί να είναι περιορισμένο σε μία μικρή γεωγραφική περιοχή (Local Area Networks) ή να καλύπτει μία ευρύτερη γεωγραφική περιοχή (Wide Area Networks) ή μπορεί ακόμα και τέτοιου είδους διαφορετικά δίκτυα να είναι συνδεδεμένα μεταξύ τους. Χαρακτηριστικό παράδειγμα αποτελεί το Διαδίκτυο (Internet) το οποίο δεν είναι άλλο από ένα παγκόσμιο δίκτυο αποτελούμενο από πολλά διασυνδεδεμένα μεταξύ τους δίκτυα, τα οποία χρησιμοποιούν

[14] Αγγελής Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)», ΠοινΔικ 2001, σελ. 1219

[15] Κριθαράς Θ., «Ποινικό Δίκαιο και Διαδίκτυο», Νομική Βιβλιοθήκη, 2009, σελ 36

κοινό πρωτόκολλο. Η λειτουργία ενός συστήματος υπολογιστή σε ένα δίκτυο μπορεί να είναι ως τερματικό (endpoint) ή ως ένα μέσο διευκόλυνσης της επικοινωνίας.

Ο επόμενος ορισμός αφορά στα δεδομένα υπολογιστών (computer data), τα οποία τα ορίζει ως τις πληροφορίες ή τα γεγονότα τα οποία αναπαρίστανται και τίθενται σε μορφή κατάλληλη για άμεση επεξεργασία από ένα σύστημα υπολογιστών. Τα δεδομένα υπολογιστών είναι αφενός ο στόχος των επιθέσεων που θα αναφερθούν παρακάτω, αλλά και το αντικείμενο για την εφαρμογή των μέτρων που θα πρέπει να υιοθετήσουν τα κράτη μέλη.

Ως πάροχος υπηρεσιών περιγράφεται μία μεγάλη κατηγορία φορέων που διαδραματίζουν σημαντικό ρόλο στις τηλεπικοινωνίες και στη διάδοση των δεδομένων. Οι φορείς αυτοί μπορεί να είναι είτε δημόσιοι είτε ιδιωτικοί, εφόσον παρέχουν την δυνατότητα επικοινωνίας στους χρήστες. Οι χρήστες μπορεί να είναι μία κλειστή ομάδα αλλά και το ευρύ κοινό, ενώ η δυνατότητα επικοινωνίας να είναι είτε δωρεάν είτε με χρέωση.

Στην κατηγορία αυτή ανήκουν και οι φορείς που αποθηκεύουν ή επεξεργάζονται δεδομένα είτε για λογαριασμό της υπηρεσίας είτε για λογαριασμό των χρηστών. Ακόμη, στους παρόχους υπηρεσιών εντάσσονται και αυτοί που προσφέρουν υπηρεσίες φιλοξενίας και επικοινωνίας σε ένα δίκτυο. Ωστόσο, ένας μερικός πάροχος υπηρεσιών δεν ανήκει σε αυτή την κατηγορία των παρόχων υπηρεσιών που ορίζεται στη σύμβαση. Παράδειγμα τέτοιου παρόχου είναι η περίπτωση που ένα φυσικό πρόσωπο συνεργάζεται με μία εταιρία φιλοξενίας ιστοσελίδων για την φιλοξενία της ιστοσελίδας της επιχείρησης του. Στην τελευταία περίπτωση ο πάροχος δεν προσφέρει ούτε επεξεργασία δεδομένων αλλά ούτε και την δυνατότητα επικοινωνίας μεταξύ των χρηστών. Στην ουσία, η Σύμβαση προσφέρει διατάξεις που προσδιορίζουν με έμμεσο τρόπο τα όρια ευθύνης των παρόχων. Ρητώς, επισημαίνεται ένα ζήτημα που είχε απασχολήσει έντονα τη νομική κοινότητα, ότι δηλαδή πάροχος υπηρεσιών που ενεργεί ως «αναμεταδότης- αγωγός» («condult») κακόβουλου λογισμικού, εφόσον δε τεκμαίρεται εγκληματική πρόθεση, δεν θα υπέχει ποινική ευθύνη[16].

Μάλιστα, στην ερμηνευτική διάταξη της αιτιολογικής έκθεσης, επαναλαμβάνεται ότι ο πάροχος δεν υπέχει ποινική ευθύνη απλά και μόνο γιατί κάποιος τρίτος «χρησιμοποίησε» το σύστημα του για να διαπράξει εγκληματική ενέργεια. Το εν λόγω ζήτημα ρυθμίζεται με άψογα ρητό και σαφή τρόπο, δείχνοντας με εμφανή τρόπο ότι η επιρροή της Οδηγίας για το

[16] Κριθαράς Θ., «Ποινικό Δίκαιο και Διαδίκτυο», Νομική Βιβλιοθήκη, 2009, σελ. 67

Ηλεκτρονικό Εμπόριο, που είχε ψηφιστεί νωρίτερα, επηρέασε τον τρόπο που προσεγγίστηκε από το κείμενο της Σύμβασης, η ευθύνη του παρόχου.

Τέλος, στο τμήμα των ορισμών περιγράφονται τα δεδομένα κίνησης, τα οποία ορίζονται ως κατηγορία των δεδομένων υπολογιστών που ανήκουν σε διαφορετικό νομικό καθεστώς. Αυτού του είδους τα δεδομένα παράγονται από τους υπολογιστές κατά τη διάρκεια της επικοινωνίας των χρηστών έτσι ώστε να καθορίζονται η πηγή της επικοινωνίας, ο προορισμός, η πορεία των δεδομένων, η διάρκεια της, η ημερομηνία, το μέγεθος, η ώρα καθώς και ο τύπος της επικοινωνίας. Τα δεδομένα αυτού του είδους αποτελούν το σημείο εκκίνησης για την έρευνα σε περίπτωση αδικήματος. Θα πρέπει να σημειωθεί ωστόσο πως πολλά από αυτά τα δεδομένα διατηρούνται για μικρό χρονικό διάστημα αποθηκευμένα κατά τη συνήθη διεξαγωγή της επικοινωνίας. Συνεπώς, εάν υπάρχει ανάγκη διατήρησης των δεδομένων για περαιτέρω επεξεργασία θα πρέπει αυτό να ζητηθεί εγκαίρως.

Ως «πηγή της επικοινωνίας» εννοείται ένας αριθμός τηλεφώνου, μία διεύθυνση διαδικτυακού πρωτοκόλλου είτε μία εγκατάσταση παρόμοιων χαρακτηριστικών από όπου ένας πάροχος προσφέρει τις υπηρεσίες του. Παρομοίως, ως «προορισμός» εννοείται μία εγκατάσταση από όπου οι επικοινωνίες διαβιβάζονται. Τέλος, ως «τύπος της επικοινωνίας» εννοείται ο τύπος των υπηρεσιών που χρησιμοποιείται στο δίκτυο, όπως για παράδειγμα η μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο ή η αποστολή μηνυμάτων.

Θα πρέπει να τονίσουμε πως ο ορισμός των δεδομένων κίνησης επιτρέπει στους νομοθέτες του κάθε κράτους μέλους να χειριστούν διαφορετικά τα δεδομένα κίνησης ως προς την νομική τους προστασία ανάλογα με την ευαισθησία τους. Το άρθρο 15 της αιτιολογικής έκθεσης υποχρεώνει τα μέλη να ορίσουν όρους και δικλείδες ασφαλείας για την προστασία των ανθρώπινων δικαιωμάτων και ελευθεριών. Αυτό σημαίνει πως πρέπει να υπάρχουν σαφή κριτήρια και προκαθορισμένη διαδικασία, που να είναι σύμφωνη με τον ευαίσθητο χαρακτήρα των δεδομένων αυτών, για τη διεξαγωγή έρευνας σε περίπτωση αδικήματος.

Σύμφωνα με την αιτιολογική έκθεση της Σύμβασης, τα συμβαλλόμενα μέρη δεν θα είναι υποχρεωμένα να υιοθετήσουν αυτολεξεί τους παραπάνω ορισμούς, αλλά τους δίνεται η διακριτική ευχέρεια να καλύψουν τις ανωτέρω έννοιες κατά τρόπο σύμφωνο με τις αρχές της Σύμβασης. Έτσι το κάθε κράτος μέλος θα πρέπει να διατυπώσει κατά το δοκούν τους

ορισμούς που απαιτούνται αλλά με τέτοιο τρόπο που να συμφωνούν με το περιεχόμενο και το πλαίσιο της Σύμβασης.

Το δεύτερο κεφάλαιο της Σύμβασης ορίζει τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο. Αρχικά περιλαμβάνονται οι οδηγίες που αφορούν το ουσιαστικό ποινικό δίκαιο. Για την ακρίβεια, το κεφάλαιο αυτό περιέχει μέτρα που αφορούν αδικήματα ενάντια στην εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) των δεδομένων που επεξεργάζονται οι υπολογιστές. Στα άρθρα 2-6 περιγράφονται και τιμωρούνται τα αδικήματα που ανήκουν στην κατηγορία, των εγκλημάτων κατά των συστημάτων πληροφοριών όπως η παράνομη πρόσβαση, η υποκλοπή, οι παρεμβολές στα δεδομένα, οι παρεμβολές στους υπολογιστές και η κακή χρήση των υπολογιστών.

Ουσιαστικού ποινικού δικαίου αδικήματα που σχετίζονται με υπολογιστές (Computer related offences) όπως η πλαστογραφία και η διακίνηση παράνομου υλικού (πορνογραφία) περιγράφονται στα επόμενα άρθρα (7-9), ενώ τα αδικήματα που αφορούν το περιεχόμενο, δηλαδή για παραβιάσεις πνευματικής ιδιοκτησίας και λοιπών δικαιωμάτων αναφέρονται στο άρθρο 10.

Ο κατάλογος των αδικημάτων που ορίζονται από τη Σύμβαση αποτελεί μια αποδεκτή από όλα τα μέλη αλλά ελάχιστη ποινικοποίηση (consensus) των συμπεριφορών που αποτελούν ποινικά αδικήματα , χωρίς αυτό να σημαίνει ότι αποκλείεται η επέκταση του εύρους τους στο εσωτερικό δίκαιο του κάθε κράτους μέλους. Η λίστα των αδικημάτων προέκυψε κυρίως από τις οδηγίες που δόθηκαν από τη Σύσταση 89 (9) του Συμβουλίου της Ευρώπης, όσον αφορά τα εγκλήματα που σχετίζονται με τους ηλεκτρονικούς υπολογιστές, καθώς και από τις μελέτες άλλων δημόσιων και ιδιωτικών διεθνών οργανισμών (Ο.Ο.Σ.Α., Ηνωμένα Έθνη, AIDP), έχοντας λάβει υπόψη τις σύγχρονες εμπειρίες από τις καταχρήσεις που έγιναν λόγω της επέκτασης των τηλεπικοινωνιακών δικτύων.

Ιδιαιτέρως σημαντική διαπίστωση είναι το ότι οι διατάξεις του ουσιαστικού δικαίου αφορούν αδικήματα, που για την πραγματοποίηση τους απαιτείται η χρήση της τεχνολογίας των πληροφοριών, αλλά η Σύμβαση χρησιμοποιεί γλώσσα που είναι τεχνολογικά ουδέτερη για την περιγραφή των προαναφερόμενων εγκλημάτων. Αυτό έχει ως αποτέλεσμα τα αδικήματα που αναφέρονται στις διατάξεις του ουσιαστικού δικαίου να έχουν ευρύτερο

πεδίο εφαρμογής, τόσο με την χρήση της τρέχουσας τεχνολογίας όσο και με την μελλοντική που θα αναπτυχθεί. Επιπρόσθετα, οι συντάκτες της Σύμβασης κατανόησαν και έδωσαν το περιθώρια στα κράτη μέλη να μπορούν να εξαιρούν από την ποινικοποίηση τα ασήμαντα αδικήματα και να μην τα εντάσσουν στις κατηγορίες αδικημάτων που περιγράφονται στα άρθρα 2 ως 10 της Σύμβασης.

Μια ιδιαιτερότητα που συναντά κανείς στις περιγραφές των αδικημάτων που προβλέπονται στη Σύμβαση, είναι η προϋπόθεση ότι αυτά πρέπει να πραγματοποιούνται χωρίς την ύπαρξη σχετικού δικαιώματος («without right»). Η προϋπόθεση αυτή φανερώνει την θέση του Συμβουλίου να μην τιμωρείται κάθε φορά ένα αδίκημα, αλλά να εξετάζεται και η περίπτωση αυτό να είναι νόμιμο ή δικαιολογημένο, όχι μόνο στις περιπτώσεις οπού συντρέχουν κλασσικοί λόγοι για την νόμιμη υποστήριξη του, όπως η συγκατάθεση , η αυτοάμυνα είτε μία κατάσταση ανάγκης, αλλά και σε περιπτώσεις που άλλες αρχές ή συμφέροντα αποποινικοποιούν το αδίκημα. Η φράση «without right» που εμφανίζεται στους διάφορους ορισμούς της Σύμβασης ερμηνεύεται αφού λάβουμε υπόψη μας το γενικότερο νόημα του κειμένου στο οποίο χρησιμοποιείται. Επομένως, επιτρέπεται και πάλι στα κράτη μέλη να αναπτύξουν το εσωτερικό τους δίκαιο με ευελιξία. Έτσι, λοιπόν, το κάθε κράτος μέλος μπορεί να καθορίσει ότι το «χωρίς δικαίωμα» αφορά πράξη που τελέστηκε χωρίς εξουσιοδότηση (νομοθετική, εκτελεστική, διοικητική, δικαστική, στα πλαίσια συμβολαίου ή συναίνεσης) ή πράξη που δεν καλύπτεται με άλλον τρόπο από τις καθιερωμένες μορφές νομικής άμυνας, υποστήριξης ή δικαιολόγησης κατά το εθνικό δίκαιο του κράτους μέλους.

Η Σύμβαση, λοιπόν, αφήνει ανεπηρέαστη την πράξη που πραγματοποιείται στα πλαίσια της νόμιμης άσκησης εξουσίας από την Κυβέρνηση[17]. Επιπλέον, η Σύμβαση προβλέπει και τις νόμιμες και συνήθεις ενέργειες που έχουν σχέση με τον σχεδιασμό των δικτύων, ή τις νόμιμες και συνήθεις λειτουργικές ή εμπορικές πρακτικές ως περιπτώσεις που δεν είναι ποινικές. Όλες οι προαναφερόμενες εξαιρέσεις τέθηκαν στην διακριτική ευχέρεια των εθνικών νομοθετών να καθοριστούν με ακρίβεια ανάλογα με το εθνικό τους δίκαιο.

[17] Παραδείγματα τέτοιων περιπτώσεων αποτελούν η διατήρηση της δημοσίας τάξης, η προστασία της εθνικής ασφάλειας και η διερεύνηση εγκληματικών ενεργειών.
Βλέπε Αιτιολογική Έκθεση European Treaty Series – ETS 185, Σύμβαση Βουδαπέστης, παρ. 39, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Άρθρο 2-Παράνομη πρόσβαση

Στο άρθρο 2 η Σύμβαση *ορίζει «πως κάθε συμβαλλόμενο μέρος θα πρέπει να λάβει νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η πρόσβαση στο σύνολο ή σε οποιοδήποτε μέρος ενός υπολογιστικού συστήματος, όταν αυτή διαπράττεται από πρόθεση και δεν υπάρχει η σχετική άδεια. Ένα μέρος μπορεί να θέσει ως προϋπόθεση διάπραξης του εγκλήματος την παραβίαση μέτρων ασφαλείας, με την πρόθεση απόκτησης δεδομένων υπολογιστή ή με άλλη αθέμιτη πρόθεση, ή σε σχέση με ένα σύστημα υπολογιστή που συνδέεται με ένα άλλο σύστημα υπολογιστή».*

Η αιτιολογική έκθεση αναλύει ακόμη περισσότερο την περίπτωση της παράνομης πρόσβασης.[18] Για την ακρίβεια αναφέρει πως η ανάγκη για προστασία αντικατοπτρίζει το ενδιαφέρον των οργανισμών και ιδιωτών να διαχειρίζονται, λειτουργούν και ελέγχουν τα συστήματά τους με ανενόχλητο και χωρίς περιορισμούς τρόπο. Η αμιγής εισβολή χωρίς εξουσία, δηλ. το «χάκινγκ», το «κράκινγκ» ή η «παραβίαση υπολογιστή» θα έπρεπε κατ' αρχήν να είναι παράνομη από μόνη της. Μπορεί να οδηγήσει σε κωλύματα για νόμιμους χρήστες συστημάτων και δεδομένων και να προκαλέσει μεταβολή ή καταστροφή με υψηλά κόστη για επανακατασκευή. Τέτοιες εισβολές μπορεί να χορηγήσουν πρόσβαση σε εμπιστευτικά δεδομένα (συμπεριλαμβανομένων των κωδικών πρόσβασης σε πληροφορίες για το στοχευόμενο σύστημα) και μυστικά, για την χρήση του συστήματος χωρίς πληρωμή ή ακόμη να ενθαρρύνει τους «χάκερς» να διαπράξουν πιο επικίνδυνες μορφές προσβολών που σχετίζονται με υπολογιστές, όπως απάτη με υπολογιστή ή πλαστογραφία». Η έκθεση αναφέρει ακόμη ότι «η πρόσβαση αφορά την είσοδο στο σύνολο ή σε οποιοδήποτε μέρος ενός συστήματος υπολογιστή (συνιστώντα μέρη, αποθηκευμένα δεδομένα του εγκατεστημένου συστήματος, αρχεία αρχειοθέτησης, δεδομένα κίνησης και περιεχομένου). Παρόλα αυτά, δεν περιλαμβάνει την απλή αποστολή ενός μηνύματος e-mail ή αρχείου σε αυτό το σύστημα. Η πρόσβαση περιλαμβάνει την διείσδυση σε άλλο σύστημα υπολογιστή, όπου είναι συνδεδεμένο με δημόσια δίκτυα τηλεπικοινωνιών, ή σε ένα σύστημα υπολογιστή που βρίσκεται στο ίδιο δίκτυο, όπως το Τοπικό Δίκτυο (LAN) ή εσωτερικά δίκτυα εντός ενός

[18] Βλέπε Αιτιολογική Έκθεση European Treaty Series- ETS X185, Σύμβαση Βουδαπέστης, παρ. 44, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

οργανισμού. Η μέθοδος επικοινωνίας (π.χ. από απόσταση, περιλαμβάνοντας συνδέσεις μέσω ασύρματου δικτύου ή από κοντινή εμβέλεια) είναι αδιάφορη».

Όσον αφορά τον όρο που τίθεται και σε αυτόν τον ορισμό περί μη ύπαρξης σχετικού δικαιώματος, στην αιτιολογική έκθεση[19] διευκρινίζεται πως η φράση αυτή σημαίνει ότι δεν υπάρχει ποινικοποίηση της πρόσβασης που εγκρίνεται από τον ιδιοκτήτη ή άλλον κάτοχο δικαιώματος του συστήματος ή μέρους αυτού, για παράδειγμα η περίπτωση της εγκεκριμένης δοκιμής ή της προστασίας του συστήματος υπολογιστή που αφορά. Επιπλέον, δεν υπάρχει ποινικοποίηση για πρόσβαση σε ένα σύστημα υπολογιστή που επιτρέπει την ελεύθερη και ανοιχτή πρόσβαση στο κοινό, καθώς για τέτοια πρόσβαση θεωρείται ότι υπάρχει το σχετικό δικαίωμα. Η εφαρμογή συγκεκριμένων τεχνικών εργαλείων μπορεί να οδηγήσει σε πρόσβαση σύμφωνα με την έννοια του Άρθρου 2, όπως είναι η πρόσβαση σε μια ιστοσελίδα, άμεσα ή μέσω υπερσυνδέσμων, περιλαμβάνοντας «βαθείς συνδέσμους» ή την εφαρμογή εφαρμογών "cookies" ή "bots" για να εντοπίσει και να λάβει πληροφορίες που εξυπηρετούν την επικοινωνία. Η εφαρμογή τέτοιων εργαλείων δεν είναι αυτή καθεαυτή «χωρίς δικαίωμα». Το να διατηρεί κανείς μια δημόσια ιστοσελίδα προϋποθέτει συγκατάθεση από τον ιδιοκτήτη της ιστοσελίδας ότι μπορεί να την προσπελάσει οποιοσδήποτε χρήστης του Διαδικτύου. Η εφαρμογή συνηθισμένων εργαλείων που χρησιμοποιούνται για διαδεδομένα στην πράξη πρωτόκολλα επικοινωνίας και προγράμματα, δεν είναι από μόνη της «χωρίς δικαίωμα», ειδικότερα όπου ο δικαιούχος του συστήματος που έχει επισκεφτεί ο χρήστης μπορεί να θεωρηθεί ότι έχει αποδεχθεί την εφαρμογή τους, π.χ. στην περίπτωση των «cookies» με την μη απόρριψη της αρχικής εγκατάστασης ή με την μη διαγραφή τους».

Άρθρο 3- Υποκλοπή

Ακολούθως, στο 3^{ο} άρθρο της Σύμβασης διατυπώνεται ο ορισμός της υποκλοπής. Συγκεκριμένα, ορίζεται πως κάθε συμβαλλόμενο μέρος θα πρέπει να λάβει νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η υποκλοπή, όταν διαπράττεται από πρόθεση, η υποκλοπή στο σύνολο ή σε ένα μέρος ενός υπολογιστικού συστήματος χωρίς να υπάρχει σχετικό δικαίωμα, που πραγματοποιείται με τεχνικά μέσα, σε περιπτώσεις μη δημόσιας μεταφοράς τους από, προς ή μέσα σε ένα σύστημα υπολογιστών,

[19] Βλέπε Αιτιολογική Έκθεση European Treaty Series- ETS 185, Σύμβαση Βουδαπέστης, παρ. 47-48, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών που μεταφέρει τέτοια δεδομένα. Το συμβαλλόμενο μέρος μπορεί να θεωρήσει πως η υποκλοπή γίνεται για αθέμιτους λόγους σε ένα σύστημα υπολογιστών που συνδέεται με ένα άλλο σύστημα υπολογιστών.

Συμπληρώνοντας τον παραπάνω ορισμό, στην αιτιολογική έκθεση[20] αναφέρεται ότι η διάταξη έχει σκοπό να προστατέψει το δικαίωμα της ιδιωτικότητας των δεδομένων επικοινωνίας. Η προσβολή θεωρείται ίδια με την παραβίαση στην ιδιωτικότητα των επικοινωνιών όπως η παραδοσιακή παρακολούθηση και ηχογράφηση φωνητικών τηλεφωνικών συνομιλιών μεταξύ ατόμων. Το δικαίωμα στην ιδιωτικότητα των επικοινωνιών κατοχυρώνεται με το άρθρο 8 της Ευρωπαϊκής Σύμβασης Ανθρώπινων Δικαιωμάτων. Η προσβολή που καθιερώνεται με το άρθρο 3 εφαρμόζει αυτή την αρχή σε όλες τις μορφές ηλεκτρονικής μεταφοράς δεδομένων, είτε αφορά τηλέφωνο, φαξ, e-mail, είτε μεταφορά αρχείων. Στην παρούσα σύμβαση έγινε σαφές ότι οι σχετικές διατάξεις αφορούν την "διακίνηση δεδομένων υπολογιστών" καθώς και η ηλεκτρομαγνητική ακτινοβολία, υπό τις προϋποθέσεις που εξηγούνται παρακάτω.

Στη συνέχεια η Αιτιολογική έκθεση επεξηγεί πως με τον όρο υποκλοπή εννοείται η υποκλοπή με τεχνικά μέσα που σχετίζεται με την ακρόαση, παρακολούθηση ή επιτήρηση του περιεχομένου των επικοινωνιών, για την απόκτηση του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης του συστήματος υπολογιστή, είτε έμμεσα, μέσω της χρήσης ηλεκτρονικών συσκευών ωτακουστικής ή παρακολούθησης. Η υποκλοπή μπορεί να περιλαμβάνει και την καταγραφή. Στα τεχνικά μέσα ανήκουν οι τεχνικές συσκευές που τοποθετούνται στα καλώδια μεταφοράς δεδομένων αλλά και οι συσκευές για συλλογή και καταγραφή των δεδομένων που διακινούνται ασύρματα. Επιπλέον, μπορεί να περιλαμβάνει την χρήση λογισμικού ή κωδικών πρόσβασης. Η προϋπόθεση για την χρήση τεχνικών μέσων αποτελεί έναν περιοριστικό όρο για την αποφυγή της υπερβολικής ποινικοποίησης».

Ένα ακόμα θέμα που θίγεται στην έκθεση είναι ο όρος μη δημόσια. Συγκεκριμένα διευκρινίζεται ότι ο όρος «μη-δημόσια» προσδιορίζει την φύση της διαδικασίας μετάδοσης (επικοινωνίας) και όχι την φύση των δεδομένων που μεταδίδονται. Τα δεδομένα που

[20] Βλέπε Αιτιολογική Έκθεση European Treaty Series- ETS 185, Σύμβαση Βουδαπέστης, παρ. 51, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

διακινούνται μπορεί να είναι πληροφορίες διαθέσιμες για το κοινό, τις οποίες όμως τα μέρη επιθυμούν να διακινήσουν εμπιστευτικά. Ακόμη, μπορεί τα δεδομένα να διατηρούνται κρυφά για εμπορικούς λόγους μέχρι την πληρωμή της υπηρεσίας , όπως στην περίπτωση της τηλεόρασης επί πληρωμή (Pay-TV). Προκύπτει πως με τον όρο «μη δημόσια» δεν αποκλείεται η επικοινωνία μέσω δημόσιων δικτύων. Η επικοινωνία μεταξύ εργαζομένων, είτε αφορά επαγγελματικούς σκοπούς ή όχι, η οποία αποτελεί «μη δημόσια μετάδοση δεδομένων υπολογιστή» προστατεύεται επίσης από την υποκλοπή χωρίς δικαίωμα με τους όρους του άρθρου 3.

Στην επόμενη παράγραφο της αιτιολογικής έκθεσης[21] αναφέρεται πως η επικοινωνία με την μορφή της μεταφοράς δεδομένων υπολογιστή μπορεί να πραγματοποιηθεί είτε σε ένα μεμονωμένο σύστημα υπολογιστή, όπως για παράδειγμα η μεταφορά δεδομένων από την κεντρική μονάδα επεξεργασίας CPU στην οθόνη ή τον εκτυπωτή, είτε μεταξύ δύο συστημάτων υπολογιστή που ανήκουν στην κατοχή του ίδιου προσώπου, είτε μεταξύ δύο υπολογιστών που επικοινωνούν μεταξύ τους, ή ακόμα ανάμεσα σε έναν υπολογιστή και ένα πρόσωπο (λ.χ. μέσω της χρήσης του πληκτρολογίου). Παρά ταύτα, τα κράτη μέλη μπορούν να απαιτήσουν ως πρόσθετη προϋπόθεση η επικοινωνία να πραγματοποιείται μεταξύ δύο συστημάτων υπολογιστή με απομακρυσμένη σύνδεση. Η έκθεση συνεχίζει σημειώνοντας πως δεν είναι δεσμευτικό για τα κράτη μέλη να εντάξουν στις υποκλοπές τις ραδιοφωνικές μεταδόσεις, ακόμα και αν είναι μη δημόσιες, καθώς αυτές μεταδίδονται με τέτοιο τρόπο που τις καθιστά ευάλωτες σε υποκλοπή ακόμα και από ερασιτέχνες.

Αποσαφηνίζεται ακολούθως μία ακόμη περίπτωση κατά την οποία οι ηλεκτρομαγνητικές εκπομπές μπορεί να εκπέμπονται από έναν υπολογιστή κατά την διάρκεια της λειτουργίας του. Αυτού του είδους οι εκπομπές δεν θεωρούνται δεδομένα σύμφωνα με τον ορισμό που δόθηκε στο άρθρο 1 της Σύμβασης. Ωστόσο, από τέτοιες εκπομπές μπορούν να ανασχηματιστούν δεδομένα. Επομένως, υπό αυτή τη σκοπιά, η υποκλοπή δεδομένων από ηλεκτρομαγνητικές εκπομπές ενός συστήματος υπολογιστή εντάσσεται στον ορισμό της υποκλοπή που δόθηκε παραπάνω.

[21] Βλέπε Αιτιολογική Έκθεση European Treaty Series- ETS 185, Σύμβαση Βουδαπέστης, παρ. 55, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Κλείνοντας την αιτιολόγηση του άρθρου 3, η έκθεση αναφέρει πως η πράξη είναι θεμιτή όταν, για παράδειγμα, το πρόσωπο που διενεργεί την υποκλοπή έχει το δικαίωμα να πράξει τοιουτοτρόπως, ή πράττει υπό οδηγίες ή πράττει λόγω δικαιώματος που του δόθηκε από τους συμμετέχοντες στην επικοινωνία (παράδειγμα αποτελεί ο δοκιμαστικός έλεγχος ή δραστηριότητες προστασίας που συμφωνήθηκαν από τους συμμετέχοντες), ή η επιτήρηση επιτρέπεται νομίμως για λόγους εθνικής ασφαλείας ή τον εντοπισμό προσβολών από τις αρχές. Ακόμη έγινε κατανοητό πως η χρησιμοποίηση κοινών εμπορικών πρακτικών, όπως η εφαρμογή «cookies», δεν δύναται να ποινικοποιηθεί, καθώς δεν είναι υποκλοπή χωρίς δικαίωμα. Τέλος, τα κράτη μέλη μπορούν να θέσουν και άλλες προϋποθέσεις για την ποινικοποίηση των υποκλοπών αλλά αυτές να ερμηνεύονται και να λειτουργούν πάντα σε συνδυασμό με τους όρους «από πρόθεση» και «χωρίς δικαίωμα» που τέθηκαν από την Σύμβαση.

Άρθρο 4- Παρεμβολή σε δεδομένα (Data interference)

Στο άρθρο 4 παρ. 1 της Σύμβασης ορίζεται ότι κάθε συμβαλλόμενο μέρος θα πρέπει να υιοθετήσει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστών, όταν αυτή διαπράττεται από πρόθεση. Το κάθε συμβαλλόμενο μέρος μπορεί να διατηρήσει το δικαίωμα να θέσει ως προϋπόθεση ύπαρξης εγκλήματος για την συμπεριφορά που περιγράφεται στην παρ . 1 την πρόκληση σοβαρής ζημίας.

Άρθρο 5 - Παρεμβολές σε συστήματα

Παρακάτω το άρ. 5 αναφέρει ότι κάθε συμβαλλόμενο μέρος θα πρέπει να υιοθετήσει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η σοβαρή παρεμπόδιση της λειτουργίας ενός συστήματος υπολογιστή χωρίς την ύπαρξη του σχετικού δικαιώματος μέσω της εισαγωγής, διαβίβασης, βλάβης, διαγραφής, φθοράς, αλλοίωσης ή καταστολής δεδομένων υπολογιστή, όταν αυτή διαπράττεται από πρόθεση.

Άρθρο 6 - Κακή χρήση συσκευών

Στη συνέχεια, στο άρθρο 6 παρ. 1 αναφέρεται ότι κάθε συμβαλλόμενο μέρος θα πρέπει να λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο

εσωτερικό του δίκαιο, η άνευ δικαιώματος και από πρόθεση διάπραξη των παρακάτω πράξεων:

α. Η παραγωγή, η πώληση, η προμήθεια προς χρήση, η εισαγωγή, η διανομή ή η με οποιονδήποτε τρόπο διάθεση:

- μιας συσκευής, περιλαμβανομένου και ενός προγράμματος υπολογιστή, σχεδιασμένης ή προσαρμοσμένης πρωτίστως με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5,

- ενός συνθηματικού ή κωδικού πρόσβασης, ή άλλου παρεμφερούς δεδομένου, με την χρήση του οποίου είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός συστήματος υπολογιστή, με πρόθεση να χρησιμοποιηθούν για τον σκοπό της διάπραξης κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5, και

β. Η κατοχή ενός αντικειμένου από τα αναφερόμενα στις παραγράφους ανωτέρω, με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5. Το κάθε συμβαλλόμενο μέρος μπορεί να θέσει ως προϋπόθεση να υπάρχει κατοχή ενός συγκεκριμένου αριθμού τέτοιων αντικειμένων πριν θεμελιωθεί ποινική ευθύνη.

Στην παρ. 2 του ίδιου άρθρου αναφέρεται ότι το παρόν άρθρο δεν πρέπει να ερμηνευθεί ότι δημιουργεί ποινική ευθύνη σε περίπτωση που η παραγωγή, η πώληση, η προμήθεια προς χρήση, η εισαγωγή, η διανομή ή η με οποιονδήποτε τρόπο διάθεση ή κατοχή όπως περιγράφεται στην παράγραφο 1 του παρόντος άρθρου δεν γίνεται με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα Άρθρα 2 έως 5 της παρούσας Σύμβασης, όπως π.χ. για την πραγματοποίηση επιτρεπτών δοκιμών ή για την προστασία ενός συστήματος υπολογιστή. Έπειτα, στην παρ. 3 ορίζεται πως το κάθε συμβαλλόμενο μέρος μπορεί να διατηρήσει το δικαίωμα να μην εφαρμόσει την παράγραφο 1 του παρόντος άρθρου, υπό τον όρο ότι η επιφύλαξη αυτή δεν θα αφορά στην πώληση, στην διανομή ή στην με οποιονδήποτε τρόπο διάθεση των αντικειμένων που περιγράφονται στην παράγραφο 1 α. του παρόντος άρθρου, δηλαδή τα συνθηματικά ή τους κωδικούς πρόσβασης σε ένα σύστημα υπολογιστή.

Με τα άρθρα 7 (Πλαστογραφία σχετικά με υπολογιστές) και 8 (Απάτη σχετική με υπολογιστές), ως ηλεκτρονικά εγκλήματα που σχετίζονται με Η/Υ, προβλέπεται η υποχρέωση των Συμβαλλομένων Μερών να καταστήσουν αξιόποινες την πλαστογραφία και την απάτη μέσω υπολογιστή, αντιστοίχως. Με το άρθρο 9 (Εγκλήματα σχετικά με την παιδική πορνογραφία) επιβάλλεται στα Συμβαλλόμενά Μέρη η υποχρέωση να καταστήσουν αξιόποινες συμπεριφορές που σχετίζονται με την παιδική πορνογραφία. Το πεδίο εφαρμογής της τελευταίας αυτής διάταξης είναι ιδιαιτέρως ευρύ, δεδομένου ότι με αυτή καλύπτεται η απαγόρευση της παραγωγής, διάδοσης [ιδίως μέσω Συνδέσμων Υπερκειμένων («liens hypertextes»)], η τηλεφόρτωση ή η απλή κατοχή υλικού παιδικής πορνογραφίας περιλαμβανόμενης και της οπτικής αναπαραγωγής προσώπων ηλικίας κάτω των 18 ετών (ή κάτω των 16 ετών για τα Συμβαλλόμενά Μέρη που έχουν θεσπίσει το όριο αυτό), ενηλίκων που εμφανίζονται ως ανήλικοι καθώς και κάθε εικονικής, αναπαράστασης ανηλίκων που επιδίδονται σε σεξουαλικές πράξεις. Η δυνατότητα διατύπωσης, από τα Συμβαλλόμενά Μέρη, επιφυλάξεων, *«παρέχεται σε ό,τι αφορά στην απλή κατοχή ή στην τηλεφόρτωση («telechargement») εικονικού υλικού παιδικής πορνογραφίας («materiel pornographique virtuel»)*[22]**.** Σημειωτέον ότι το θέμα της παιδικής πορνογραφίας έχει ρυθμιστεί προσφάτως (Ιούνιος 2014) με το άρθρο 8 του ν. 4267/2014, το οποίο τροποποίησε το άρθρο 348Α του Ποινικού Κώδικα, οι δε ουσιαστικές του διατάξεις εφαρμόζονται mutatis mutandis και σε εγκλήματα του Κυβερνοχώρου. Με τη διάταξη του άρθρου 10 (Εγκλήματα σχετικά με παραβιάσεις πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων), αντιμετωπίζονται εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας, εφ όσον αυτά διαπράττονται για εμπορικούς σκοπούς, αποβλέπουν δηλαδή στην επίτευξη κέρδους και μόνο.

Άρθρο 11 - Απόπειρα και συμμετοχή

Σύμφωνα με το άρθρο 11 κάθε συμβαλλόμενο μέρος θα πρέπει να λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η συνδρομή ή εξώθηση στη διάπραξη οποιουδήποτε εκ των εγκλημάτων που ποινικοποιούνται σύμφωνα με τα άρθρα 2 έως 10 της παρούσης Συμβάσεως, όταν αυτά διαπράττονται από πρόθεση.

[22] Βλέπε Αιτιολογική Έκθεση της Σύμβασης του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα,ETS 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Στην παρ. 2 του ίδιου άρθρου ορίζεται ακόμη ότι κάθε συμβαλλόμενο μέρος θα πρέπει να υιοθετήσει τα κατάλληλα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο του η απόπειρα διάπραξης οποιουδήποτε εγκλήματος από αυτά που ποινικοποιούνται σύμφωνα με τα άρθρα 3 έως 5, 7, 8 και 9.1α και γ της παρούσης Συμβάσεως, όταν η απόπειρα αυτή γίνεται από πρόθεση. Τέλος, στην παρ.3 αναφέρεται πως κάθε συμβαλλόμενο μέρος μπορεί να διατηρήσει το δικαίωμα να μην εφαρμόσει ολικά ή εν μέρει την παράγραφο 2 του παρόντος άρθρου.

Άρθρο 13 - Ποινές και Μέτρα

«Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που απαιτούνται για να εξασφαλίσει ότι τα ποινικά αδικήματα που καθιερώνονται σύμφωνα με τα Άρθρα 2 έως 11 θα τιμωρούνται με αποτελεσματικές, αναλογικές, αποτρεπτικές ποινικές ή μη κυρώσεις ή μέτρα, περιλαμβανομένων των χρηματικών κυρώσεων». Στο άρθρο 13 της Σύμβασης προβλέπονται οι «ποινές και τα μέτρα» που τα συμβαλλόμενα μέρη καλούνται να επιβάλλουν για την τέλεση των αδικημάτων της Σύμβασης. Με το παρόν άρθρο δεν θεσπίζονται συγκεκριμένες ποινικές κυρώσεις για τα αδικήματα της Σύμβασης, παρά μόνο προτείνεται ως γενική επιταγή, προς τα συμβαλλόμενα μέρη να εξαρτήσουν τις ποινές από τη σοβαρότητα των αδικημάτων, 59 προβλέποντας ποινικές κυρώσεις που είναι «αποτελεσματικές, αναλογικές και αποτρεπτικές». Στην περίπτωση των φυσικών προσώπων, περιλαμβάνεται η δυνατότητα επιβολής ποινών φυλάκισης. Τα νομικά πρόσωπα, των οποίων η ευθύνη πρέπει να καθοριστεί σύμφωνα με το άρθρο 12 πρέπει επίσης να υπόκεινται σε κυρώσεις που είναι «αποτελεσματικές, αναλογικές και αποτρεπτικές», οι οποίες μπορεί να είναι ποινικής, διοικητικής ή αστικής φύσεως. Τα συμβαλλόμενα μέρη είναι υποχρεωμένα, σύμφωνα με την παρ. 2, να προβλέπουν και τη δυνατότητα επιβολής χρηματικών κυρώσεων σε νομικά πρόσωπα.

Άρθρο 22 – Δικαιοδοσία

«1.Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να θεμελιωθεί η δικαιοδοσία επί κάθε εγκλήματος που ποινικοποιείται σύμφωνα με τα Άρθρα 2 έως 11 της παρούσας Σύμβασης, όταν τα εγκλήματα αυτά διαπράττονται:

α. εντός της επικράτειάς του ή

β. επί ενός πλοίου που φέρει την σημαία του εν λόγω Συμβαλλόμενου Μέρους, ή

γ. επί ενός αεροσκάφους που είναι καταχωρημένο σύμφωνα με τους νόμους του εν λόγω Συμβαλλόμενου Μέρους, ή

δ. από ένα πολίτη του, εάν το έγκλημα τιμωρείται από το ποινικό δίκαιο στον τόπο που διαπράχθηκε ή εάν το έγκλημα διαπράχθηκε εκτός της εδαφικής δικαιοδοσίας ενός κράτους.

2. Κάθε Συμβαλλόμενο Μέρος μπορεί να επιφυλαχθεί να εφαρμόσει μόνο σε συγκεκριμένες περιπτώσεις υπό συγκεκριμένες συνθήκες τους κανόνες περί δικαιοδοσίας που αναφέρονται στις παραγράφους 1.β έως 1.δ του παρόντος Άρθρου ή μέρους αυτού.

3. Κάθε Συμβαλλόμενο Μέρος θα λάβει τα μέτρα που είναι αναγκαία για να θεμελιωθεί δικαιοδοσία επί των εγκλημάτων που αναφέρονται στο Άρθρο 24 παράγραφος 1, της παρούσας Σύμβασης, σε περιπτώσεις όπου ο φερόμενος ως εγκληματίας είναι παρών μέσα στην επικράτειά του και δεν τον εκδίδει σε άλλο Συμβαλλόμενο Μέρος αποκλειστικώς και μόνον με βάση την εθνικότητά του, κατόπιν αίτησης έκδοσης.

4. Η παρούσα Σύμβαση δεν αποκλείει την άσκηση ποινικής δικαιοδοσίας από ένα Συμβαλλόμενο Μέρος σύμφωνα με το εγχώριο δίκαιό του.

5. Όταν περισσότερα από ένα Συμβαλλόμενα Μέρη διεκδικούν δικαιοδοσία επί ενός εγκλήματος που ποινικοποιείται σύμφωνα με την παρούσα Σύμβαση, τα εμπλεκόμενα μέρη θα διαβουλευθούν, όπου αυτό απαιτείται, με σκοπό να προσδιορισθεί η καταλληλότερη δικαιοδοσία για να ασκηθεί δίωξη».

Η παράγραφος 1α βασίζεται στην αρχή της εδαφικότητας, αρχή που διέπει σύννομα, όπως ισχύει διεθνώς, τη Σύμβαση[23]. Κάθε μέρος έχει την υποχρέωση να τιμωρήσει τη διάπραξη εγκλημάτων που προβλέπονται στην παρούσα Σύμβαση τα οποία διαπράττονται στο έδαφός του. Οι περιπτώσεις β και γ της παρ. 1 είναι βασισμένες σε μια παραλλαγή της αρχής της εδαφικότητας. Η παράγραφος 1δ βασίζεται στην αρχή της εθνικότητας. Στη παράγραφο 2 του παρόντος, ορίζονται τα εξαιρετικά όρια σε ορισμένες περιπτώσεις των παραγράφων 1β-1δ, ενώ στις παραγράφους 3-4, καθορίζονται τα μέτρα συνεργασίας μεταξύ των κρατών που συμμετέχουν στη σύμβαση καθώς και το πεδίο ποινικής δράσης τους. Τέλος, με την παρ. 5 του παρόντος προβλέπονται διαδικασίες διαβούλευσης μεταξύ των συμβαλλομένων μερών, στις περιπτώσεις που περισσότερα κράτη διεκδικούν τη θεμελίωση δικαιοδοσίας. Αυτό είναι συνηθισμένο φαινόμενο στα εγκλήματα που διαπράττονται με τη

[23] Κριθαράς Θ., «Ποινικό Δίκαιο και Διαδίκτυο», Νομική Βιβλιοθήκη, 2009, σελ 38

χρήση συστημάτων πληροφοριών, όπου σε αρκετές περιπτώσεις περισσότερα από ένα συμβαλλόμενα μέρη θα έχουν δικαιοδοσία επί μερικών ή όλων των συμμετεχόντων στο έγκλημα, με επακόλουθο τη δυσχερέστερη καταγραφή αυτών των εγκλημάτων[24].

Όσο αφορά, μία συνολική αποτίμηση και αξιολόγηση της Σύμβασης, έχει ορθώς χαρακτηριστεί στο σύνολο της, ως το σημαντικότερο κείμενο για την αντιμετώπιση της ηλεκτρονικής εγκληματικότητας[25]. Παρά τη γενική ομολογία και τη κοινή παραδοχή του πόσο σημαντική ήταν η Σύμβαση ως το πρώτο ουσιαστικά κείμενο που κατέγραφε και ποινικοποιούσε συμπεριφορές ενός εννόμου αγαθού, σχετικά άγνωστου μέχρι τότε, υπήρξαν επικρίσεις για το κατά πόσο δεν θα είναι ένα ακόμα θεωρητικό κείμενο και πως θα μπορούσε να συμβάλει πρακτικά στην αντιμετώπιση της ηλεκτρονικής εγκληματικότητάς. Η Σύμβαση της Βουδαπέστης, παρά τις αρχικές προβλέψεις ότι θα επικεντρώνεται στην ποινικοποίηση συμπεριφορών που στοχεύουν πληροφοριακά συστήματα, δηλαδή στα γνήσια πληροφορικά εγκλήματα, προχώρησε ένα βήμα παρακάτω, ποινικοποιώντας δράσεις που στρέφονται κατά άλλων εννόμων αγαθών, απλά τελούνται μέσω Η/Υ (π.χ. απάτη με υπολογιστή). Βέβαια, υπήρξε από μία μερίδα επιστημόνων αρνητική κριτική καθώς θα έπρεπε η Σύμβαση να περιορίζεται μόνο στα γνήσια εγκλήματα κατά του Κυβερνοχώρου. Άλλο σημείο κριτικής, αποτέλεσε το γεγονός πως είναι δύσκολη και χρονοβόρα η διαδικασία για κράτη μη μέλη του Συμβουλίου της Ευρώπης να προσχωρήσουν στη Σύμβαση, με αποτέλεσμα στη πράξη να μην εφαρμόζεται παγκοσμίως. Τη τελευταία δεκαετία, μάλιστα, αυξήθηκε η κριτική, διότι υπήρξε ελλειμματική προσέγγιση στο τομέα των προσωπικών δεδομένων καθώς και στη προστασία θεμελιωδών δικαιωμάτων που απορρέουν από το εν λόγω πεδίο[26]. Επιπροσθέτως, υποστηρίζεται πως ο κατάλογος με τα εγκλήματα, όπως αποτυπώνονται στο δεύτερο κεφάλαιο, θα έπρεπε να είναι πιο περιεκτικός κυρίως για να μην υπάρξουν διαφοροποιήσεις από χώρα σε χώρα, δημιουργώντας τη πεποίθηση πως χρειάζεται επιπρόσθετη νομοθέτηση επί τούτου. Τέλος, ίσως το μεγαλύτερο «ψεγάδι» θα μπορούσαμε να πούμε πως είναι η έλλειψη διαδικασιών για την έρευνα και δίωξη του ηλεκτρονικού εγκλήματος, στοιχείο απαραίτητο για την πρακτική εκδίωξη της ηλεκτρονικής εγκληματικότητας. Το ηλεκτρονικό έγκλημα απαιτεί ιδιαίτερο τρόπο προσέγγισης καθώς ο παραδοσιακός τρόπος έρευνας και

[24] Αγγελής Ι. « Διαδίκτυο (Internet) και ποινικό Δίκαιο», ΝοΒ 2000, σελ.679

[25] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ. 5.

[26] Wennerstorm E. , "EU-legislation and Cybercrime", 2011, σελ. 465.

δίωξης μιας πράξης, δεν ισχύει στον κυβερνοχώρο[27]. Χρειάζεται ιδιαίτερα τεχνικά τρόπος έρευνας και καταγραφής μιας ποινικής πράξης στον κυβερνοχώρο, με έναν συνδυασμό τεχνικών και νομικών γνώσεων να κρίνεται απαραίτητος για την ουσιαστική αντιμετώπιση ενός κράτους κατά του ηλεκτρονικού εγκλήματος, κατάσταση που προκάλεσε και προκαλεί ακόμα και σήμερα, προβλήματα και στην ελληνική έννομη τάξη, κυρίως ως προς την αντίληψη των πραγμάτων που συμβαίνουν στο διαδίκτυο και συνολικά στον τομέα των ηλεκτρονικών υπολογιστών. Πέρα από τις διάφορες επικρίσεις, που αν μη τι άλλο στόχευαν καθαρά στη βελτίωση του κορυφαίου μέχρι τότε νομοθετικού κειμένου για το ηλεκτρονικό έγκλημα και στην καθολική ενδυνάμωση του, ώστε όλα τα κράτη παγκοσμίως να μπορούν να αντιμετωπίζουν αποτελεσματικά ένα άγνωστο πεδίο με ακόμα περισσότερο άγνωστο μέλλον ως προς την τεχνολογική εξέλιξης, η Σύμβαση της Βουδαπέστης αποτέλεσε το πρώτο βήμα για τη διακρατική συνεργασία των κρατών στον εν λόγω τομέα, με όλα τα άλλα νομοθετήματα που ακολούθησαν « να χρωστάνε τη γένεση τους» σε αυτό το νομοθετικό κείμενο.

2.2. Απόφαση-Πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών.

Η Ευρωπαϊκή Ένωση δε θα μπορούσε να μείνει αμέτοχη και αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα και στον κυβερνοχώρο ειδικότερα, με την ολοένα και αυξανόμενη συχνότητα των ηλεκτρονικών επιθέσεων στα τέλη της δεκαετίας του 90. Σε πρώτο στάδιο, το Συμβούλιο της Ένωσης εξέδωσε ψήφισμα, το No 97/C 70/01, το οποίο αναγνώριζε τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος και κυρίως, διαχώριζε τα δεδομένα που διακινούνται στο διαδίκτυο, σε παράνομα και επιβλαβή. Με το εν λόγω ψήφισμα τέθηκε μία πρώτη ενασχόληση της Ένωσης με τον Κυβερνοχώρο αναδεικνύοντας, όπως είπαμε τα οφέλη του διαδικτύου και μία πρώτη στοιχειοθέτηση των δεδομένων που κυκλοφορούν στο διαδίκτυο[28].

Ως επακόλουθο της Σύμβασης της Βουδαπέστης, ήταν δεδομένη η αναζήτηση σε ενωσιακό επίπεδο ενός νομικού εργαλείου με τεχνικές προεκτάσεις, για τις επιθέσεις κατά

[27] Αγγελής Ι. «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», *ΠοινΔικ 12/2001,* σελ. 1298

[28] Αγγελής Ι. «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», *ΠοινΔικ 12/2001,* σελ. 1293

των πληροφοριακών συστημάτων. Η Απόφαση-Πλαίσιο 2005/222/ΔΕΥ, εκδόθηκε στις 24 Φεβρουαρίου του 2005 από το Συμβούλιο της Ευρωπαϊκής Ένωσης και τέθηκε σε ισχύ από τη δημοσίευση της, δηλαδή στις 16 Μαρτίου 2005. Κύριος στόχος της Απόφασης ήταν η βελτίωση της συνεργασίας μεταξύ των δικαστικών και λοιπών αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, μέσω της προσέγγισης των κανόνων του ποινικού δικαίου των κρατών μελών που αφορούν επιθέσεις κατά των συστημάτων πληροφοριών. Στόχευε, λοιπόν στην αντιμετώπιση των επιθέσεων κατά των πληροφοριακών συστημάτων.

Το Συμβούλιο της Ένωσης έκρινε ως απαραίτητη την ύπαρξη ενός εξειδικευμένου νομοθετικού κειμένου που θα ορίσει ακριβώς τα πληροφοριακά συστήματα και θα στοιχειοθετήσει νομικά τις επιθέσεις κατά αυτών, ενώ υπήρχε έντονη ανησυχία και για τις τρομοκρατικές επιθέσεις. Ο έντονα υπερεθνικός και χωρίς σύνορα χαρακτήρας των σύγχρονων συστημάτων πληροφοριών συνεπάγεται ότι οι επιθέσεις κατά των συστημάτων έχουν συχνά διασυνοριακή διάσταση, τονίζοντας την ανάγκη για αυξημένη συνεργασία μεταξύ των κρατών μελών ώστε να υπάρχει ορθή εναρμόνιση του ποινικού δικαίου στο εσωτερικό των κρατών. Ο μεγάλος κίνδυνος για την αντιμετώπιση αυτή ήταν η διαφοροποίηση στις νομοθεσίες των κρατών μελών στο συγκεκριμένο τομέα καθώς και τα όποια νομικά κενά που θα μπορούσαν να παρεμποδίσουν την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας και να κάνουν περίπλοκη και δυσλειτουργική τη συνεργασία των αστυνομικών και δικαστικών υπηρεσιών σε περίπτωση επιθέσεων κατά των συστημάτων πληροφοριών[29].

Τα σημαντικότερα σημεία στο κείμενο της απόφασης ήταν τα εξής :

Στο άρθρο 1 αποτυπώνονταν όπως και στο πρώτο μέρος της Σύμβασης κάποιοι χρήσιμοι ορισμοί για τη περαιτέρω διευκρίνιση των επιθέσεων και του νομοθετικού πλαισίου για τη προστασία της, ενώ δόθηκε για πρώτη φορά σε νομοθετικό κείμενο ο όρος του συστήματος πληροφοριών. Συγκεκριμένα :

Ως «Σύστημα πληροφοριών» ορίζεται οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με

[29] Βλέπε την Πρόταση για την Απόφαση-Πλαίσιο του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών (υποβληθείσα από την Επιτροπή), Επιτροπή των Ευρωπαϊκών Κοινοτήτων, Βρυξέλλες, 19.04.2002, COM(2002) 173 τελικό 2002/0086(CNS).

ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τους υπολογιστές με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους.

Ως «Ηλεκτρονικά δεδομένα» ορίζονται οποιαδήποτε παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου ενός προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία.

Ως «Νομικό πρόσωπο» ορίζεται κάθε οντότητα που έχει αυτό το καθεστώς βάσει του ισχύοντος δικαίου, εκτός των κρατών ή άλλχων δημόσιων οργάνων κατά την άσκηση κρατικής εξουσίας και των δημόσιων διεθνών οργανισμών.

Ως «Χωρίς δικαίωμα»: πρόσβαση ή παρεμβολή μη εξουσιοδοτημένη από τον ιδιοκτήτη ή άλλο δικαιούχο του συστήματος ή μέρους του, ή μη επιτρεπόμενη δυνάμει της εθνικής νομοθεσίας.

Στο άρθρο 2 ορίζεται η Παράνομη πρόσβαση σε συστήματα πληροφοριών, με παραπλήσιο τρόπο όπως στη Σύμβαση της Βουδαπέστης, *« Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως πρόσβαση, χωρίς δικαίωμα, στο σύνολο ή σε μέρος συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις»*, ενώ στην παράγραφο 2 του ιδίου άρθρου *«Κάθε κράτος μέλος μπορεί να αποφασίσει ότι η αναφερόμενη στην παράγραφο 1 πράξη ποινικοποιείται μόνον όταν το αδίκημα διαπράττεται κατά παράβαση μέτρου ασφαλείας»*.

Στο άρθρο 3 ορίζεται ρητά πέρα από την παράνομη παρεμβολή σε δεδομένα και η Παράνομη παρεμβολή σε σύστημα, ήτοι, *«Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή, μετάδοση, ζημία, διαγραφή, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις»*.

Ενώ στο άρθρο 4 η Παράνομη παρεμβολή σε δεδομένα ορίζεται ακριβώς όπως στο κείμενο της Συμβάσεως **«** *Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως διαγραφή, ζημία, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις»*.

Το άρθρο 5 Ορίζει τις συμμετοχικές προϋποθέσεις (Ηθική αυτουργία, υποβοήθηση και συνέργεια) για τις επιθέσεις στα πληροφοριακά συστήματα καθώς και την απόπειρα επίθεσης ως ποινικό αδίκημα και απόπειρα ενώ αφήνει στη διακριτική ευχέρεια των κρατών τη μη τιμώρηση της απόπειρας στο αδίκημα της Παράνομης πρόσβασης σε συστήματα πληροφοριών.

Στα άρθρα 6 και 7 αναφέρονται οι κυρώσεις και οι επιβαρυντικές περιστάσεις των αδικημάτων, τονίζοντας ότι κάθε κράτος πρέπει να λαμβάνει τα αναγκαία μέτρα για την αποτελεσματική αντιμετώπιση των εν λόγω εγκλημάτων. Στο άρθρο 7, πιο συγκεκριμένα, ορίζεται η αύξηση του αξιοποίνου στις περιπτώσεις των άρθρων 2 παρ.2, 3 και 4, όταν διαπράττονται στα πλαίσια εγκληματικής οργάνωσης.

Στο άρθρο 10 θεμελιώνονται οι προϋποθέσεις για τη δικαιοδοσία, ζήτημα φλέγον και πολύ ιδιαίτερα προσεγγίσιμο στις περιπτώσεις των πληροφοριακών συστημάτων, όπως έχει τονιστεί σε παραπάνω κεφάλαιο. Η παράγραφος 1 ορίζει ότι *«Κάθε κράτος μέλος θεμελιώνει τη δικαιοδοσία του για τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, όταν το αδίκημα διαπράττεται α) εν όλω ή β) εν μέρει στην επικράτειά του από υπήκοό του, ή γ) προς όφελος νομικού προσώπου που εδρεύει στην επικράτειά του εν λόγω κράτους μέλους»,* παράγραφο η οποία διέπεται από τις αρχές τις εδαφικότητας και της υπηκοότητας. Στη παράγραφο 2 διατυπώνεται ότι *«Για να θεμελιώσει τη δικαιοδοσία του σύμφωνα με την παράγραφο 1 στοιχείο α), κάθε κράτος μέλος εξασφαλίζει ότι στη δικαιοδοσία αυτή εμπίπτουν περιπτώσεις κατά τις οποίες, ο δράστης διέπραξε το αδίκημα ευρισκόμενος στην επικράτειά του, ανεξάρτητα από το αν το αδίκημα στρέφεται κατά συστήματος πληροφοριών στην επικράτειά του, ή το αδίκημα στρέφεται κατά συστήματος πληροφοριών στην επικράτειά του, ανεξάρτητα από το αν ο δράστης διαπράττει το αδίκημα ευρισκόμενος στην επικράτειά του»* . Στη παράγραφο 2 διευρύνεται η δικαιοδοτική αρμοδιότητα καθώς ένα κράτος-μέλος έχει διττή ευθύνη να διώξει ποινικά τη πράξη είτε βρίσκεται στην επικράτεια του το σύστημα

πληροφοριών που δέχεται επίθεση είτε αν ο δράστης της επίθεσης βρίσκεται στην επικράτεια του ιδίου κράτους.

Στη παράγραφο 3 ορίζεται ότι *«Κράτος μέλος το οποίο, δυνάμει του εθνικού του δικαίου, δεν εκδίδει ή δεν παραδίδει μέχρι στιγμής τους υπηκόους του, λαμβάνει τα αναγκαία μέτρα προκειμένου να θεμελιώσει τη δικαιοδοσία του και, όταν απαιτείται, προκειμένου να ασκήσει δίωξη όσον αφορά τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, εφόσον διαπράττονται από υπήκοο του εκτός της επικράτειάς του»*, ενώ στη παράγραφο 4 ορίζεται *ότι « Όταν αδίκημα υπάγεται στη δικαιοδοσία περισσοτέρων του ενός κρατών μελών και οποιοδήποτε εκ των συγκεκριμένων κρατών μπορεί εγκύρως να ασκήσει δίωξη βάσει των ίδιων πραγματικών περιστατικών, τα συγκεκριμένα κράτη μέλη συνεργάζονται προκειμένου να αποφασίσουν ποιο εξ αυτών θα προβεί στη δίωξη των δραστών με σκοπό, εφόσον είναι δυνατό, να συγκεντρωθεί η διαδικασία σε ένα μόνο κράτος μέλος. Προς το σκοπό αυτό, τα κράτη μέλη μπορούν να προσφεύγουν σε οποιοδήποτε όργανο ή μηχανισμό εγκαθιδρυμένο στο εσωτερικό της Ευρωπαϊκής Ένωσης για να διευκολύνουν τη συνεργασία μεταξύ των δικαστικών τους αρχών καθώς και το συντονισμό των ενεργειών τους. Λαμβάνονται υπόψη διαδοχικά τα ακόλουθα στοιχεία**: κράτος μέλος είναι εκείνο στην επικράτεια του οποίου ετελέσθησαν τα αδικήματα σύμφωνα με την παράγραφο 1 στοιχείο α) και την παράγραφο 2, κράτος μέλος είναι εκείνο του οποίου είναι υπήκοος ο δράστης, κράτος μέλος είναι εκείνο στο οποίο ανακαλύφθηκε ο δράστης»***

Στην παράγραφο 5 του άρθρου 10 αναφέρεται η δυνατότητα μη εφαρμογής ή εφαρμογής μόνο σε ειδικές περιστάσεις τις περιπτώσεις β και γ της παραγράφου 1, καθορίζοντας ουσιαστικά ως κύρια δικαιοδοσία τη περίπτωση α, δηλαδή τη περίπτωση όπου το αδίκημα τελέσθηκε εξ ολοκλήρου στην επικράτειά του, ενώ στην παράγραφο 6 ορίζεται ότι για περαιτέρω διευκρινήσεις σχετικά με τις ειδικές περιστάσεις της παραγράφου 5, τα κράτη-μέλη οφείλουν να ενημερώνουν την Επιτροπή και τη γραμματεία του Συμβουλίου.

Τέλος το άρθρο 11 καθιερώνει την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, καινοτομία απαραίτητη για την ευχερέστερη έρευνα και δίωξη των αδικημάτων. Συγκεκριμένα, «*1. Με σκοπό την ανταλλαγή πληροφοριών σχετικά με τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5 και σύμφωνα με τους κανόνες προστασίας δεδομένων, τα κράτη μέλη διασφαλίζουν τη χρήση του υφιστάμενου δικτύου λειτουργικών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας.*

2. Κάθε κράτος μέλος ενημερώνει τη γενική γραμματεία του Συμβουλίου και την Επιτροπή για το σημείο επαφής που έχει ορίσει με σκοπό την ανταλλαγή πληροφοριών για τα αδικήματα που αφορούν επιθέσεις κατά των συστημάτων πληροφοριών. Η γενική γραμματεία διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη».

Βασική διαφορά από τη Σύμβαση τα Βουδαπέστης , κείμενο επάνω στο οποίο βασίστηκε η οριοθέτηση ορισμένων αδικημάτων από την Απόφαση, υπήρξε η εξειδίκευση στα εγκλήματα του Κυβερνοχώρου και δη στις επιθέσεις των συστημάτων πληροφοριών, πεδίο στο οποίο το κείμενο της Σύμβασης υπήρξαν κάποια νομικά κενά, σύμφωνα με ορισμένη μερίδα επικριτών της.

2.3. Οδηγία 2013/40/ΕΕ : νέο θεσμικό πλαίσιο της Ευρωπαϊκής Ένωσης για τις επιθέσεις κατά των συστημάτων πληροφοριών και οι λόγοι που οδήγησαν στην αντικατάσταση της Απόφασης-Πλαισίου 2005/222/ΔΕΥ.

Στις 30 Σεπτεμβρίου του 2010, δηλαδή ένα χρόνο μετά την ισχύ της Συνθήκης της Λισαβώνας, η Ευρωπαϊκή Επιτροπή εισήγαγε πρόταση Οδηγίας για τις επιθέσεις κατά των πληροφοριακών συστημάτων με στόχο την αντικατάσταση της Απόφασης-Πλαίσιο 2005/222/ΔΕΥ[30].

Ένα βασικός προβληματισμός που ανέκυψε μετά την πρόταση Οδηγίας ήταν για ποιο λόγο κρίθηκε αναγκαία η αντικατάσταση της Απόφασης από τη στιγμή που κοιτώντας προσεκτικά το κείμενο της Οδηγίας, παραμένει κατά βάση ίδιο. Η Οδηγία 2013/40/ΕΕ ψηφίστηκε στις 12 Αυγούστου 2013 αντικαθιστώντας την Απόφαση-Πλαίσιο 2005/222/ΔΕΥ και αποτελώντας το νέο νομικό εργαλείο της Ένωσης , το οποίο δεσμεύει τα κράτη-μέλη για τη τήρηση του περιεχομένου της. Όπως και στην περίπτωση της Απόφασης, η Σύμβαση της Βουδαπέστης αποτέλεσε τη βάση στην οποία στηρίχθηκε νομικά το πνεύμα της Οδηγίας. Άλλωστε, το γεγονός πως όλα τα κράτη μέλη της Ένωσης δεσμεύονται από το κείμενο της Σύμβασης δε σήμαινε ότι η Ένωση δε μπορεί να δημιουργήσει το δικό της πιο εξειδικευμένο θεσμικό πλαίσιο για τη προστασία των συστημάτων πληροφοριών. Αυτονόητο είναι ότι η Ένωση ως υπερκρατικός οργανισμός έχει τη δυνατότητα να δεσμεύει τα κράτη μέλη

[30] Βλέπε "Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA", http://europa.eu/rapid/press-release_MEMO-10-463_en.htm?locale=en

τουλάχιστον ως προς τη δημιουργία αξιοποίνου σύμφωνα με τις επιλογές της[31]. Όπως αναφέρθηκε παραπάνω, εύλογα ήταν τα ερωτήματα για την αντικατάσταση της Απόφασης και η θέσπιση ενός νέου θεσμικού πλαισίου με παρόμοιο περιεχόμενο. Βασική αιτία θεωρήθηκε η αύξηση των επιθέσεων στην Ευρώπη, έπειτα από την ψήφιση της Απόφασης με ολοένα και πιο οργανωμένο τρόπο, με την εγκληματική χρήση του καλούμενου δικτύου προγραμμάτων ρομπότ (botnet) και τις μαζικές Επιθέσεις άρνησης υπηρεσίας (DDOS attacks). Η χρήση των αποκαλούμενων "botnet" (δίκτυα προγραμμάτων ρομπότ) περιλαμβάνει διάφορα στάδια της αξιόποινης πράξης, καθένα από τα οποία μπορεί από μόνο του να θέσει σε σοβαρό κίνδυνο το δημόσιο συμφέρον. Η παρούσα οδηγία σκοπεύει, μεταξύ άλλων, στην εισαγωγή ποινικών κυρώσεων για τη δημιουργία των "botnet", δηλαδή την πράξη της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο. Μόλις δημιουργηθεί, τότε το προσβεβλημένο δίκτυο υπολογιστών, που συνιστά το "botnet", μπορεί να ενεργοποιείται εν αγνοία των χρηστών των εν λόγω υπολογιστών, με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία συνήθως μπορεί να προκαλέσει σοβαρές ζημίες, όπως αναφέρεται στην σχετική οδηγία[32].

Ο ευάλωτος χαρακτήρας των συστημάτων πληροφοριών ενίσχυσε την αντικατάσταση του θεσμικού πλαισίου ώστε να ανταποκρίνεται σε μεταγενέστερα δεδομένα ενώ η εξέλιξη της τεχνολογίας είχαν καταστήσει ευκολότερη τη διασπορά και παραγωγή κακόβουλου λογισμικού και δικτύων προγραμμάτων ρομπότ από το 2005 και έπειτα.

Ένα άλλο σημαντικό γεγονός που οδήγησε στην αντικατάσταση της Απόφασης ήταν και η ισχύς της Συνθήκης της Λισσαβόνας, η οποία επέφερε τεράστιες αλλαγές τόσο στο κοινοτικό όσο και στο ευρωπαϊκό ποινικό δίκαιο. Καταργήθηκαν οι μέχρι τότε τρεις πυλώνες, ενώ για την έγκριση των οδηγιών πλέον αρκεί η πλειοψηφία των κρατών μελών στο Συμβούλιο μαζί με το Κοινοβούλιο.

Η Οδηγία 2013/40/ΕΕ δεν έχει ουσιαστικές παραλλαγές στο κείμενο της από την προηγούμενη Απόφαση-Πλαίσιο, έχει όμως αλλαγές, οι οποίες θα αναλυθούν παρακάτω, επειδή θεωρήθηκε, ορθώς κατά πολλούς, ότι η μέχρι τότε ισχύουσα Απόφαση περιορίζει τον αριθμό των αδικημάτων και δεν αντιμετωπίζει πλήρως την απειλή που αντιπροσωπεύουν οι

[31] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ.491

[32] Βλέπε Οδηγία 2013/40/Ε.Ε. Σκέψη 5, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33193

επιθέσεις μεγάλης κλίμακας[33]. Στο παρακάτω κεφάλαιο θα γίνει μία συγκριτική προεπισκόπηση του ισχύοντος θεσμικού πλαισίου με το παλαιό.

2.4. Το περιεχόμενο της Οδηγίας 2013/40/ΕΕ

Οι στόχοι της παρούσας οδηγίας είναι η προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων. Τα συστήματα πληροφοριών είναι βασικό στοιχείο για την πολιτική, κοινωνική και οικονομική αλληλεπίδραση στην Ένωση. Η εξασφάλιση κατάλληλων επιπέδων προστασίας των συστημάτων πληροφοριών θα πρέπει να αποτελεί μέρος ενός αποτελεσματικού ολοκληρωμένου πλαισίου από μέτρα πρόληψης τα οποία συνοδεύουν τις απαντήσεις του ποινικού δικαίου στον κυβερνοχώρο. Αναλυτικότερα, το περιεχόμενο της Οδηγίας :

Άρθρο 1 : **Αντικείμενο**

«Η παρούσα οδηγία θεσπίζει ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των κυρώσεων στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών. Σκοπεύει επίσης να διευκολύνει την πρόληψη των αδικημάτων αυτών και να βελτιώσει τη συνεργασία μεταξύ δικαστικών και άλλων αρμόδιων αρχών».

Άρθρο 2 : **Ορισμοί**

« Για τους σκοπούς της παρούσας οδηγίας, εφαρμόζονται οι ακόλουθοι ορισμοί:
α) "σύστημα πληροφοριών" : η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους.

[33] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ.495

β) "ηλεκτρονικά δεδομένα" : η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία?

γ) "νομικό πρόσωπο" : κάθε οντότητα που έχει το καθεστώς του νομικού προσώπου βάσει του εφαρμοστέου δικαίου, αλλά δεν περιλαμβάνει κράτη, ή δημόσιους φορείς κατά την άσκηση της εξουσίας τους ή δημόσιους διεθνείς οργανισμούς?

δ) "χωρίς δικαίωμα" : η αναφερόμενη στην παρούσα οδηγία συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου». Η μόνη διαφορά στη διατύπωση των ορισμών σε σχέση με το κείμενο της Απόφασης είναι ότι στον ορισμό των συστημάτων πληροφοριών *«τα δεδομένα ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα των συσκευών»* και όχι από τους υπολογιστές όπως προβλεπόταν στα παλαιότερα κείμενα, καλύπτοντας πιο γενικά την τεχνολογική εξέλιξη ώστε αν υπάρχει κάποια αντίστοιχη συσκευή μελλοντικά, να ανήκει στο άρθρο αυτό.

Άρθρο 3 : **Παράνομη πρόσβαση σε συστήματα πληροφοριών**

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις». Το περιεχόμενο και στα δύο κείμενα είναι παρόμοιο, αν και αρχικά η Οδηγία δεν περιείχε αντίστοιχη φράση με τη *«κατά παράβαση μέτρου ασφαλείας»,* δηλαδή η Απόφαση άφηνε μεγαλύτερο πεδίο διακριτικής ευχέρειας στα κράτη να αποφασίσουν το αξιόποινο της πράξης[34]. Όμως, ύστερα από αντιδράσεις περιλήφθηκε η παραβίαση των μέτρων ασφαλείας, ακριβώς όπως και στο περιεχόμενο της Σύμβασης, περιορίζοντας έτσι το αξιόποινο σε συγκεκριμένες συμπεριφορές και περιπτώσεις.

Άρθρο 4 : **Παράνομη παρεμβολή σε σύστημα**

[34] Τσόλιας Γρ., «Η πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου», σε Πρακτικά 2ου Πανελλήνιου Συνεδρίου e-ΘΕΜΙΣ

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις».

Άρθρο 5 : **Παράνομη παρεμβολή σε δεδομένα**

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις». Στα άρθρα 4 και 5, το περιεχόμενο φαίνεται αναλλοίωτο σχετικά με τα αντίστοιχα άρθρα της Απόφασης ενώ με τις αντίστοιχες διατάξεις της Σύμβασης της Βουδαπέστης, στη περίπτωση, ιδίως, της παράνομης παρεμβολής σε δεδομένα υπάρχει δυνατότητα αποκλεισμού του αξιοποίνου για ήσσονος σημασίας περιπτώσεις[35]. Στη Σύμβαση του Συμβουλίου της Ευρώπης, ο περιορισμός του αξιοποίνου προβλέπεται μόνο για σοβαρές ζημίες. Κοινώς, δε υπάρχει απόλυτη ταύτιση αλλά μία διεύρυνση του αξιοποίνου ως προς την διάταξη της Οδηγίας, στην εν λόγω περίπτωση.

Άρθρο 6 : **Παράνομη υποκλοπή**

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις».

Άρθρο 7 : **Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων**

[35] Καϊάφα' Γκμπάντι Μ., "Criminalizing Attacks against Information Systems in the EU: The Anticipated", ΠοινΧρ, σελ.5

«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις:

Α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6·

Β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών».

Η μεγαλύτερη διαφορά που εισήγαγε η Οδηγία 2013/40/ΕΕ, σε σχέση με την Απόφαση-Πλαίσιο είναι η εισαγωγή δύο νέων ποινικών διατάξεων, που αφορούν την παράνομη υποκλοπή δεδομένων (άρθρο 6) και την παραγωγή, πώληση εργαλείων που χρησιμοποιούνται για τη διάπραξη των αδικημάτων για τα άρθρα 3 έως 6. Ως προς τη παράνομη υποκλοπή δεδομένων, διάταξη η οποία είχε στοιχειοθετηθεί στη Σύμβαση της Βουδαπέστης, υπήρχε η δυνατότητα περιορισμού του αξιοποίνου στα κράτη μόνο σε περιπτώσεις όπου η υποκλοπή έχει γίνει *με παράνομο σκοπό* ή σε σχέση με ένα σύστημα πληροφοριών που συνδέεται με ένα άλλο. Η συγκεκριμένη πρόβλεψη δε προβλέπεται στο κείμενο της Οδηγίας, δημιουργώντας κάποιες αντιδράσεις λόγω της διεύρυνσης του αξιοποίνου.

Αντίστοιχα, στο άρθρο 7 επί της ουσίας τιμωρούνται οι προπαρασκευαστικές πράξεις, διάταξη που η Ένωση πρώτη φορά ζητά να ποινικοποιήσουν τα κράτη-μέλη. Στην αντίστοιχη διάταξη της Σύμβασης, δίνεται η δυνατότητα περιορισμού του αξιοποίνου στο άρθρο 6 σε περίπτωση που έγινε και εδώ με πρόθεση παρανομίας. Δεύτερη ειδοποιός διαφορά των δύο νομικών κειμένων, ως προς τη διατύπωση των τεχνικών μέσων, είναι ότι δε γίνεται καμία προσπάθεια ορισμού της υποκλοπής στο κείμενο της Οδηγίας. Επίσης, το άρθρο 6 παρ.2 της Συμβάσεως δε μπορούμε να πούμε ότι ποινικοποιεί τις ανωτέρω προπαρασκευαστικές πράξεις όταν γίνονται για λόγους προστασίας πληροφοριακού συστήματος, διάταξη που δεν αναφέρεται στην Οδηγία. Η εν λόγω διάταξη, ενδεχομένως και να είναι ευκόλως εννοούμενη, όμως, αυτή η σαφής διατύπωση αποκλεισμού του αξιοποίνου

μόνο θετικά λειτουργεί[36]. Γενικότερα, το αξιόποινο περιορίζεται περισσότερο στο άρθρο 6 της Σύμβασης από το άρθρο 7 της Οδηγίας, δίνοντας μία πιο σταθμισμένη στάση στο κείμενο της Σύμβασης, καθώς αξιολογεί ορθότερα το εύρος που εύκολα μπορεί να λάβει το αξιόποινο στις προπαρασκευαστικές πράξεις. Επιλέγει, τη ποινικοποίηση μόνο των *αναμφισβήτητα επικίνδυνων μέσων* τέλεσης, όπως πχ. είναι οι υπολογιστές και οι συνθηματικοί κωδικοί, μέσα τέλεσης που πραγματικά μπορούν να δώσουν πρόσβαση σε πληροφοριακό σύστημα. Γι' αυτόν, ακριβώς το λόγο η ευρύτητα του αξιοποίνου, προκάλεσε αντιδράσεις για τη συγκεκριμένη διάταξη της Οδηγίας.

Άρθρο 8 : **Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα**

«1. Τα κράτη μέλη εξασφαλίζουν ότι η ηθική αυτουργία, ή η υποβοήθηση και η συνέργεια, προς διάπραξη αδικήματος που αναφέρεται στα άρθρα 3 έως 7 τιμωρείται ως ποινικό αδίκημα.

2. Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα».

Στο άρθρο 8 παρ.1, προβλέπεται η τιμώρηση ακόμα και της απλής συνέργειας σε προπαρασκευαστικές πράξεις που χρησιμοποιούνται στις επιθέσεις κατά των πληροφοριακών συστημάτων ενώ στη παράγραφο 2 η τιμώρηση της απόπειρας επιβάλλεται στα κράτη μέλη για πρώτη φορά σε σχέση με την Απόφαση-Πλαίσιο, όπου αφήνεται η μη τιμώρηση της απόπειρας στη διακριτική ευχέρεια των κρατών. Στη Σύμβαση του Συμβουλίου της Ευρώπης, αντίθετα, προβλέπεται η δυνατότητα επιφύλαξης εκ μέρους των κρατών ως προς την τιμώρηση ή μη της απόπειρας επιθέσεων κατά πληροφοριακών συστημάτων. Το θετικό στοιχείο, όμως, σε αυτήν την υποχρέωση επιβολής αξιοποίνου στις περιπτώσεις απόπειρας, είναι ότι περιορίζονται μόνο στα αδικήματα των άρθρων 4 και 5, δηλαδή στις περιπτώσεις της παράνομης παρεμβολής και της παράνομης παρεμβολής σε δεδομένα.

[36] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, *σελ.* 494

Άρθρο 9 : **Κυρώσεις**

«1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 τιμωρούνται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη, τουλάχιστον για περιπτώσεις που δεν είναι ήσσονος σημασίας.

3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, οσάκις τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται εκ προθέσεως, και εφόσον έχει πληγεί σημαντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργαλείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή προσαρμοσθεί πρωτίστως για τον σκοπό αυτό, τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη.

4. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον:

Α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης κατάχχ την έννοια της απόφασης-πλαισίου 2008/841/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή·

Β) προκαλούν σημαντικές ζημίες, ή

Γ) διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής.

5. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι εφόσον τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων, και, ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, το γεγονός αυτό μπορεί, σύμφωνα με το εθνικό δίκαιο, να εκλαμβάνεται ως επιβαρυντική περίσταση, εκτός εάν οι εν λόγω περιστάσεις καλύπτονται ήδη από άλλο αδίκημα που τιμωρείται σύμφωνα με το εθνικό δίκαιο».

Η Οδηγία 2013/40/ΕΕ προβλέπει δύο έτη, τουλάχιστον, ανώτατο όριο ποινής, ακόμα και για τις προπαρασκευαστικές πράξεις του άρθρου 7. Μετά τη Συνθήκη της Λισαβώνας , η ΕΕ απέκτησε ρητή αρμοδιότητα καθορισμού του ελάχιστου ορίου των ποινών με τις οποίες τιμωρούνται οι προβλεπόμενες συμπεριφορές. Οι διατάξεις της Οδηγίας είναι αρκετά πιο αυστηρές από τις αντίστοιχες της Σύμβασης του Συμβουλίου της Ευρώπης (άρθρο 13) και θα λέγαμε πως έρχονται σε έντονη αντίθεση με την αρχή της αναλογικότητας. Η καταργούμενη διάταξη του άρθρου 6 παρ. 2 της Απόφασης ήταν σαφώς πιο ελαστική με όριο ποινής από 1-3 χρόνια, δίνοντας την ευκαιρία στα κράτη-μέλη να υπηρετήσουν ορθότερα την αρχή της αναλογικότητας, επιτρέποντας τα να μετρήσουν την βαρύτητα του εγκλήματος ανάλογα με τη σκάλα απαξίας που ορίζονται τα αδικήματα αυτά στο εσωτερικό τους ποινικό σύστημα[37]. Η σχετικά δεσμευτική πρόβλεψη του ελάχιστου ορίου της Οδηγίας, πέρα από την ανελαστικότητα της, αυστηροποιεί τις ποινές και περιορίζει τις διαφορές μεταξύ των κρατών-μελών, μη λαμβάνοντας υπόψη τις όποιες διαφορές των εσωτερικών ποινικών συστημάτων κάθε κράτους. Τουλάχιστον, είναι ενθαρρυντική και σε αυτό το άρθρο, η πρόβλεψη της εξαιρέσεως των περιπτώσεων «ήσσονος σημασίας», δίνοντας έτσι τη δυνατότητα στα κράτη να καθορίσουν ποιες πράξεις κρίνονται ασήμαντες στο ποινικό τους σύστημα.

Ως προς τις επιβαρυντικές περιστάσεις της παραγράφου 4, υπάρχει διεύρυνση αυτών σε σχέση με την Απόφαση-Πλαίσιο, ενώ αυστηροποιείται και το ελάχιστο όριο αυτών με όριο τα 5 έτη, αντίθετα με το άρθρο 7 παρ.1 της Απόφασης, όπου ορίζονταν από 2 έως 5 έτη ανάλογα τη περίπτωση, όμως περιορίζεται στα αδικήματα των άρθρων 4 και 5, της παράνομης παρεμβολής, ευτυχώς σε αντίθεση με τη πρόβλεψη της πρότασης της οδηγίας που δε περιόριζε τα αδικήματα[38]. Στην τρίτη παράγραφο, ορίζεται ελάχιστο όριο ποινής τα τρία έτη στις περιπτώσεις των άρθρων 4 και 5 που διαπράττονται με πρόθεση και εφόσον έχει προηγηθεί *«χρήση εργαλείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή προσαρμοσθεί πρωτίστως για τον σκοπό αυτό»,* τιμωρώντας αυξημένα τον συνδυασμό των ανωτέρω αδικημάτων με τις προπαρασκευαστικές πράξεις του άρθρου 7 συνδυάζοντας την τέλεση.

[37] Adrian Christian, "Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level", Journal of law and international science, 2015, σελ. 10

[38] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ. 496

Άρθρο 12 : **Δικαιοδοσία**

1. *«Τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, εφόσον το αδίκημα έχει διαπραχθεί:*

α) εν όλω ή εν μέρει στο έδαφος τους· ή

β)από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί.

2. Κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμφωνα με την παράγραφο 1 στοιχείο α), εξασφαλίζει ότι διαθέτει δικαιοδοσία, οσάκις:

α)ο δράστης διέπραξε το αδίκημα, όταν ευρίσκετο στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του· ή

β)το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός του ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα ευρίσκετο στο έδαφός του.

3. Το κράτος μέλος ενημερώνει σχετικά την Επιτροπή οσάκις αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8, το οποίο διαπράττεται εκτός του εδάφους του, οσάκις, μεταξύ άλλων:

α) ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή

β)το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του».

Άρθρο 13 : **Ανταλλαγή πληροφοριών**

1. «*Για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, τα κράτη μέλη εξασφαλίζουν ότι διαθέτουν ένα λειτουργικό εθνικό σημείο επαφής και κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας. Τα κράτη μέλη εξασφαλίζουν επίσης ότι διαθέτουν διαδικασίες ώστε, σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής.*

2. Τα κράτη μέλη ενημερώνουν την Επιτροπή για το σημείο επαφής που έχουν ορίσει κατά τα αναφερόμενα στην παράγραφο 1. Η Επιτροπή διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη και τους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης.

3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να εξασφαλίσουν ότι διατίθενται οι κατάλληλοι δίαυλοι αναφοράς προκειμένου να διευκολυνθεί η υποβολή αναφορών χωρίς αδικαιολόγητη καθυστέρηση σχετικά με αδικήματα που αναφέρονται στα άρθρα 3 έως 6 στις αρμόδιες εθνικές τους αρχές».

Όσο αναφορά τις ρυθμίσεις για τη δικαιοδοσία, αρχικά υπήρξαν έντονες αντιδράσεις με το κείμενο της προτάσεως της Οδηγίας καθώς σε αντίθεση με το άρθρο 22 της Συμβάσεως, επιβαλλόταν στα κράτη μέλη η θεμελίωση δικαιοδοσίας σε περιπτώσεις όπου το αδίκημα έχει διαπραχθεί από υπήκοο τους ή από πρόσωπο που έχει τη συνήθη διαμονή του στο έδαφος του οικείου κράτους μέλους, χωρίς όμως να εξαρτάται από την όρο του διττού αξιοποίνου[39]. Ο κανόνας του διπλού αξιοποίνου εξ αρχής, ορθώς, καθιερώθηκε από τη Σύμβαση της Βουδαπέστης με σκοπό να εξασφαλιστεί κάθε πολίτης της Ένωσης έναντι του ενδεχόμενου να διώκεται ποινικά σε κράτος, στο οποίο απευθύνεται η αίτηση, όμως, έχει αξιολογήσει ως μη αξιόποινη τη πράξη για την οποία διώκεται στο κράτος που έκανε την αίτηση. Κοινώς, το κείμενο της πρότασης ανεπίτρεπτα εξαιρούσε το διπλό αξιόποινο, παραβιάζοντας θεμελιώδη δικαιώματα καθώς και την αρχή της χρήσης του ποινικού δικαίου ως ultima ratio. Μετά τις προαναφερόμενες και απόλυτα λογικές επικρίσεις, η Επιτροπή επανάφερε το όρο του διττού αξιοποίνου, όπως ορίζεται στο άρθρο 12 παρ.1 β' «*Τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, εφόσον το αδίκημα έχει διαπραχθεί: από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί».*

Σημαντική είναι η επίσης η ύπαρξη διακριτικής ευχέρειας στα κράτη μέλη (παράγραφος 3) για τη θεμελίωση δικαιοδοσίας σε δύο περιπτώσεις, σε περιπτώσεις που ένα από τα αδικήματα της Οδηγίας διαπράττεται εκτός του εδάφους του κράτους μέλους, εφόσον «*ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του».*

[39] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, *σελ.* 497

Σύμφωνα με το άρθρο 13, παραμένει το δίκτυο επιχειρησιακών επαφών επί 24ωρου μεταξύ των κρατών περί ανταλλαγής πληροφοριών για επιθέσεις στα πληροφοριακά συστήματα, όπως και στην Απόφαση-Πλαίσιο. Παράλληλα, όμως, η διάταξη ενισχύεται περαιτέρω σε πολύ σημαντικό βαθμό, καθιερώνοντας διαδικασίες σε επείγουσες περιπτώσεις όπου *«η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής»*, η οποία αποτελεί σημαντική προσθήκη στο διευρυμένο πλαίσιο συνεργασίας ,όπου φαίνεται η πρόθεση της ΕΕ να ενισχύσει αυτό τον τομέα, ειδικά σε περιπτώσεις μαζικών επιθέσεων. Η άμεση επικοινωνία και η γρήγορη ανταλλαγή πληροφοριών, κρίνεται επιβεβλημένη στα κράτη έλη, ώστε να αντιμετωπιστούν ορθά οι επιθέσεις, ανάγκη που γιγαντώθηκε από τις μαζικές συστηματικές επιθέσεις μεγάλου εύρους που παρατηρήθηκαν στην Ευρώπη μετά το 2005.

Συμπερασματικά, η Ε.Ε προσπάθησε με την Οδηγία 2013/40/ΕΕ να ανανεώσει το θεσμικό της πλαίσιο για την ποινική προστασία από επιθέσεις κατά πληροφοριακών συστημάτων. Η Οδηγία στόχευε στην καταπολέμηση των οργανωμένων επιθέσεων, εισάγοντας σημαντικές προσθήκες όπως αυτό της πρόβλεψης της παράνομης υποκλοπής καθώς και της καθιέρωσης ενός πιο οργανωμένου συστήματος συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των χωρών. Εξάλειψε τα νομικά κενά στα εσωτερικά δίκαια των κρατών για την ακώλυτη αντιμετώπιση των οργανωμένων επιθέσεων, καθώς και εξαίρεσε το αξιόποινο στις περιπτώσεις «ήσσονος σημασίας». Προβληματισμό, όμως, προκάλεσε ο τρόπος με τον οποίο η Ένωση προσπάθησε να καλύψει τα όποια νομικά κενά υπήρχαν, διευρύνοντας σε τέτοιο σημείο το αξιόποινο, παραβιάζοντας βασικές δικαιικές αρχές, όπως της αναλογικότητας καθώς και θεμελιώδη δικαιώματα του Χάρτη της Ε.Ε. Ιδιαίτερα, η διεύρυνση του αξιοποίνου και η αύξηση του ελάχιστου ορίου, συγκριτικά με την Απόφαση – Πλαίσιο, είναι οι διατάξεις που επιδίδονται περισσότερης κριτικής. Άλλωστε, εάν είχαν καθιερωθεί πλαίσια ποινής όπως στην Απόφαση –Πλαίσιο (2χρ.με 5χρ., όπως ίσχυε) θα εξυπηρετούνταν καλύτερα η θεμελιώδης αρχή της αναλογικότητας.

Όλα αυτά τα στοιχεία έθεσαν προβλήματα στο εσωτερικό των εννόμων τάξεων των χωρών της Ένωσης για το πώς θα τα μεταφέρουν ορθά λόγω των αρκετών νομικών κενών που υπήρχαν στα περισσότερα κράτη παρά τη Σύμβαση της Βουδαπέστης, καθώς αρκετές χώρες της Ένωσης, μεταξύ άλλων και της Ελλάδας μέχρι τη ψήφιση της Οδηγίας δεν είχαν

εναρμονιστεί ούτε με το κείμενο της Συμβάσεως του Συμβουλίου της Ευρώπης. Αναμφίβολα, η Οδηγία 2013/40/ΕΕ, παρά τις όποιες επικρίσεις προκάλεσαν κάποιες διατάξεις της, αποτελεί ένα ισχυρό και εξειδικευμένο νομικό πλαίσιο-οδηγό στα κράτη-μέλη της Ένωσης για την καλύτερη αντιμετώπιση των κυβερνοεγκλημάτων και για την ασφαλέστερη προστασία των πληροφοριακών συστημάτων, συμπληρώνοντας ιδανικά σε αρκετά σημεία τη Σύμβαση της Βουδαπέστης, πάντα επηρεασμένη και καθοδηγούμενη από τις βασικές αρχές που διέπουν το δίκαιο της ΕΕ.

ΚΕΦΑΛΑΙΟ 3^{Ο} : Το ελληνικό νομικό πλαίσιο για την καταπολέμηση των επιθέσεων στα πληροφοριακά συστήματα. Οι πρώτες προσπάθειες αντιμετώπισης και οι αλλαγές που επέφερε ο νόμος 4411/2016.

3.1. ΕΙΣΑΓΩΓΗ

Ο νόμος 4411/2016 επέφερε σημαντικές αλλαγές στην ελληνική έννομη τάξη, προσαρμόζοντας το εσωτερικό δίκαιο στο κείμενο της Σύμβασης της Βουδαπέστης, έστω και αρκετά καθυστερημένα καθώς και το ευρωπαϊκό θεσμικό πλαίσιο με την Οδηγία 2013/40/ΕΕ Στο ελληνικό νομικό πλαίσιο, μέχρι πρότινος, οι επιθέσεις κατά πληροφοριακών συστημάτων αντιμετωπίζονταν συνδυαστικά τόσο από διατάξεις του Π.Κ. όσο και από διατάξεις ειδικών νόμων. Η παράνομη πρόσβαση καλύπτονταν στο ελληνικό ποινικό δίκαιο, κυρίως από το πλαίσιο προστασίας του απορρήτου των επικοινωνιών. Ο Ν.4411/2016 αποτέλεσε το πρώτο οργανωμένο θεσμικό πλαίσιο προστασίας των πληροφοριακών συστημάτων, άμεσα προσαρμοσμένο στις διεθνείς συμβάσεις. Η ελληνική έννομη τάξη, είχε επικριθεί για τη χρόνια αμέλεια της να προσαρμοστεί στη Σύμβαση της Βουδαπέστης όσο και για τη μη αναγνώριση του πληροφοριακού συστήματος ως εννόμου αγαθού. Ο νέος νόμος για το ηλεκτρονικό έγκλημα, έστω και με χρόνια καθυστέρηση, επέφερε σημαντικές αλλαγές, *«βάζοντας στον χάρτη του εσωτερικού μας ποινικού δικαίου»* τις προσβολές κατά των πληροφοριακών συστημάτων, αναγνωρίζοντας παράλληλα το πληροφοριακό σύστημα ως έννομο αγαθό, εξέλιξη που κάθε προηγμένη και προσαρμοσμένη στις νέες εξελίξεις, έννομη τάξη, όφειλε να έχει πραγματοποιήσει.

3.2. Το ελληνικό νομικό πλαίσιο πριν τη ψήφιση του Ν.4411/2016

Στην ελληνική έννομη τάξη, πριν από τη ψήφιση του Ν.4411/2016, δεν υπήρχε νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου, όπως προαναφέρθηκε, παρά μόνο σκόρπιες διατάξεις του ελληνικού ποινικού δικαίου. Ο πρώτος σχετικός νόμος, υπήρξε ο Ν.1805/88, ο οποίος αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, πρόσθεσε τα άρθρα 370 Β (Παραβίαση στοιχείων ή προγραμμάτων των υπολογιστών που θεωρούνται απόρρητα) , 370Γ (Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών και 386^{Α} (Απάτη με υπολογιστή)[40]. Τα άρθρα αυτά δεν επαρκούσαν για να καλύψουν τις ανάγκες δίωξης των σύγχρονων εγκλημάτων, λογικό και αυτονόητο επακόλουθο της αυξανόμενης τεχνολογικής εξέλιξης των υπολογιστών όσο και της χρήσης του διαδικτύου[41]. Ειδικές διατάξεις για θέματα συγγενικά με ηλεκτρονικό έγκλημα, υπήρχαν στο Π.Δ. 131/2003, το οποίο θεσπίστηκε για το ηλεκτρονικό εμπόριο και αναφερόταν στην ανεπιθύμητη ηλεκτρονική αλληλογραφία, στον νόμο 2246/1994 για την οργάνωση και λειτουργία των τηλεπικοινωνιών, τον Ν.2472/1997 περί προσωπικών δεδομένων και τον Ν.2225/2994 για την προστασία της ελευθερίας της ανταπόκρισης και της επικοινωνίας. Το συγκεκριμένο νομικό πλαίσιο δεν κάλυπτε περιπτώσεις παρακώλυσης λειτουργίας υπολογιστικών συστημάτων ούτε ρυθμίσεις για αλλοίωση ή φθορά δεδομένων. Άλλωστε, η φθορά ηλεκτρονικών δεδομένων δε μπορούσε στον μέχρι τότε Ποινικό Κώδικα να τιμωρηθούν γιατί κατά την έννοια του άρθρου 381, τα δεδομένα δε θεωρούνταν πράγμα για να μπορεί να υποστεί φθορά. Το πληροφοριακό σύστημα δε κατοχυρωνόταν ως έννομο αγαθό, ενώ ως έννομο αγαθό προστατευμένο στα ηλεκτρονικά εγκλήματα αναγνωριζόταν το ηλεκτρονικό έγγραφο ως ειδική περίπτωση του εγγράφου κατά άρθρο 13 περ.γ' ΠΚ. Όταν είχε ψηφιστεί ο Ν.1805/1988, το κυρίαρχο φαινόμενο προσβολής της περιουσίας μη χρήση υπολογιστή, ήταν η χωρίς δικαίωμα χρήση κωδικών καρτών τραπεζικής ανάληψης[42]. Ο νόμος ήταν ήδη ξεπερασμένος από το νομικό κείμενο της Σύμβασης της Βουδαπέστης, πόσο μάλλον για όλο αυτό το διάστημα, που κωλυσιεργούσαν οι διαδικασίες εσωτερικής προσαρμογής. Όταν η Οδηγία 2013/40/ΕΕ, όριζε ελάχιστο όριο της παράνομης πρόσβασης σε υπολογιστή τα τρία χρόνια, η αντίστοιχη

[40] Αγγελής Ι. «Διαδίκτυο (Internet) και ποινικό δίκαιο, ΝοΒ, 2000, σελ.679

[41] Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», 2007,σελ.144

[42] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ. 498

συμπεριφορά, κατά το ελληνικό ποινικό δίκαιο τιμωρούνταν με φυλάκιση μέχρι τριών μηνών (βλέπε αρ. 370Γ ΠΚ).

Στο νέο περιβάλλον που δημιουργήθηκε, ο εκσυγχρονισμός του θεσμικού πλαισίου καταπολέμησης του ηλεκτρονικού εγκλήματος ήταν κάτι παραπάνω από επιβεβλημένος. Πέρα από το νομοθετικό πλαίσιο προσδιορισμού ηλεκτρονικών εγκλημάτων και εννόμων αγαθών που δε μπορούσε να καλύψει η προϋπάρχουσα κατάσταση, επιβεβλημένη κρίθηκε και η βελτίωση της διερεύνησης του ηλεκτρονικού εγκλήματος. Η έρευνα και η κατάσχεση πληροφοριών είναι η πρώτη διαδικασία που αμφισβητείται σε μία ποινική δίκη. Τα αποδεικτικά στοιχεία έχουν ψηφιακή μορφή και κρίνεται επιβεβλημένο κατά τη διαδικασία της καταγραφής μίας τέτοιας συμπεριφοράς να υπάρχουν αποτελεσματικά τεχνικά μέσα για την έρευνα και καταγραφή αυτών των εγκλημάτων. Λόγω του ιδιαίτερου των κυβερνοεγκλημάτων, το αντικείμενο όπως και ο τόπος τέλεσης μπορεί να βρίσκονται ταυτόχρονα σε πολλές χώρες. Ο παραδοσιακός τρόπος εξιχνίασης αυτών των εγκλημάτων δεν αρκεί, όπως ο παραδοσιακός Εισαγγελέας και η παραδοσιακή αστυνομία δεν επαρκούν πλέον[43]. Απαιτούνται εξειδικευμένες υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, όπως έχουν τεθεί με επιτυχία στις ΗΠΑ, στην Αυστραλία και την Αγγλία. Στην Ελλάδα, ιδρύθηκε, αρκετά καθυστερημένα, το 2014 η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και αφού είχαν παρατηρηθεί αυξημένες υποθέσεις ηλεκτρονικών εγκλημάτων, όπου η δίωξη δε γινόταν με την απαιτούμενη γνώση και εξειδίκευση. Είχαν καταγραφεί, τη τελευταία δεκαετία, δεκάδες διαμαρτυρίες αστυνομικών οργάνων αλλά και εισαγγελέων που αντιδρούσαν έντονα καθώς δεν είχαν στα χέρια τους τα απαιτούμενα μέσα για την ορθή καταπολέμηση των εγκλημάτων του διαδικτύου[44]. Βήματα προόδου πραγματοποιήθηκαν, τα τελευταία τρία χρόνια, στη χώρα μας, πρέπει, όμως, να συνεχίζουν οι διωκτικές αρχές να εκσυγχρονίζουν τις υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, να αναβαθμιστούν τα εργαστήρια εξέτασης ψηφιακών τεκμηρίων σε απόλυτα υψηλές τεχνολογίες, καθότι είναι γνωστό πως οι hackers χρησιμοποιούν άριστα εξελιγμένους υπολογιστές και να εκπαιδευτεί το προσωπικό των προανακριτικών υπαλλήλων στη μεθοδολογία διερεύνησης με ψηφιακή τεχνολογία.

[43] Αγγελής Ι. «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», *ΠοινΔικ 12/2001,* σελ. 1299.

[44] Θ. Σιδηρόπουλος, «Το δίκαιο του διαδικτύου», 2009,σελ 35

3.3. Το ελληνικό πλαίσιο μετά τη ψήφιση του Ν.4411/2016

Με τον Ν. 4411/2016, στις 3-8-2016, κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο, καθώς και το Πρόσθετο Πρωτόκολλο αυτής σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως, όπως επίσης ενσωματώθηκε στην Ελληνική έννομη τάξη η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών. Επήλθαν πρωτόγνωρες αλλαγές στην ελληνική νομική τάξη, καθώς πρώτη φορά αποτυπώνονταν με ακρίβεια ηλεκτρονικά εγκλήματα, συγκεκριμένα τα εγκλήματα του διαδικτύου, θεσπίστηκε για πρώτη φορά η παράνομη παρακώληση πληροφοριακών συστημάτων, αναγκαία διάταξη λόγω των αυξανόμενων οργανωμένων επιθέσεων στην Ευρώπη[45]. Επίσης, προβλέφθηκε η φθορά και αλλοίωση των δεδομένων υπολογιστή και προσαρμόστηκαν τα αρ. 370Β και 370Γ του Ποινικού Κώδικα, στις νέες τεχνολογικές εξελίξεις, αλλάζοντας τους όρους του αρ.370Γ παρ. 2 από «στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή σε «*σύνολο ή τμήμα πληροφοριακού συστήματος*» .

Αναλυτικότερα :

Στο άρθρο 13, στην έννοια όρων του Ποινικού Κώδικα προστέθηκαν οι περιπτώσεις η΄ και θ΄, καθιερώνοντας το πληροφοριακό σύστημα και τα ψηφιακά δεδομένα ως έννομα αγαθά, αναγκαία προϋπόθεση για να στοιχειοθετηθούν ποινικά οι παράνομες επιθέσεις σε πληροφοριακά συστήματα. Συγκεκριμένα:

«η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

[45] Βλέπε Αιτιολογική έκθεση του Ν.4411/2016, βλέπε http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=z7c0XwYgEpY%3d&tabid=132

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

Μετά το άρθρο 292Α του Ποινικού Κώδικα, των εγκλημάτων κατά της ασφάλειας των τηλεπικοινωνιών, προστίθεται το άρθρο 292Β ως εξής:

« Άρθρο 292Β

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

Τα άρθρα 292Β παρ.1 και παρ.2α είναι άμεσα προσαρμοσμένα με το άρθρο 4 της Οδηγίας, αυτό της παράνομης παρεμβολής σε σύστημα σε συνδυασμό με τις κυρώσεις του άρθρου 9 της Οδηγίας με ανάλογα πλαίσια ποινής. Ουσιαστικά ποινικοποιούνται οι επιθέσεις κατά συστημάτων πληροφοριών, αποκεντρωμένες ή μη [DoS & DDoS], και επομένως και σχετικές πράξεις παράνομης πρόσβασης (hacking, cracking), οι οποίες προκαλούν προσωρινές επιπλοκές σε ένα πληροφοριακό σύστημα. Η διάταξη, επίσης, προβλέπει κυρώσεις σε περίπτωση σοβαρής παρεμπόδισης ή διακοπής της λειτουργίας ενός πληροφοριακού συστήματός[46]. Αντίθετα, όμως, δεν ορίζεται κάποιο ελάχιστο επίπεδο παρακώλυσης με τις ανάλογες συνέπειες. Βαρύτερα, τιμωρούνται οι πράξεις που τελούνται στο πλαίσιο δράσης εγκληματικής οργάνωσης, σε αντιστοιχία με τον ορισμό αυτής στο άρθρο 187 ΠΚ στην παράγραφο 3, όπως και οι πράξεις των περιπτώσεων 292Β παρ.2β' και 292Β παρ.2γ'. Οι ποινές είναι σταθμισμένες ανάλογα με την ένταση και το είδος της προσβολής, άρρηκτα συνδεδεμένες με την αρχή της αναλογικότητας. Η μόνη επιβαρυντική περίσταση του άρθρου 9 παρ.5 της Οδηγίας που δε προβλέφθηκε είναι αυτό της τέλεσης με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, πιθανότατα επειδή υπάρχει η δυνατότητα εφαρμογής του υφιστάμενου άρθρου 386 ΠΚ περί κοινής απάτης.

3. Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται άρθρο 292Γ ως εξής:

« Άρθρο 292Γ

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί:

α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β,

β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Με το άρθρο 292Γ ΠΚ, ενσωματώνεται το άρθρο 7 της Οδηγίας, το οποίο προβλέπει κυρώσεις για την τέλεση του 292Β με τις προπαρασκευαστικές ενέργειες του εγκλήματος. Όπως αναφέρθηκε σε παραπάνω κεφάλαιο, σύμφωνα με την αιτιολογική έκθεση της

[46] Ε. Βαγενά, « Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», ΔΙΜΕΕ, 2017, σελ.33

Οδηγίας, αυτά τα εργαλεία μπορεί να περιλαμβάνουν κακόβουλο λογισμικό, το οποίο χρησιμοποιείται για τις επιθέσεις κατά πληροφοριακών συστημάτων, όπου συμπεριλαμβάνονται και τα εργαλεία που δημιουργούν botnet, επιθέσεις που οδήγησαν στην ανανέωση του θεσμικού ενωσιακού νομικού πλαισίου.

Το άρθρο 370Β ΠΚ παρέμεινε ως έχει :

« 1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση».

Το 370Β ΠΚ, θεσπίστηκε για τη προστασία για την προστασία των απορρήτων που συνδέονται με χρήση ηλεκτρονικού υπολογιστή. Προστατεύει ως έννομο αγαθό τα κρατικά, επιστημονικά ή επαγγελματικά απόρρητα, όταν έχουν τη μορφή στοιχείων ή προγραμμάτων υπολογιστή. Ως απόρρητο μπορεί να θεωρηθεί κάθε τη μορφή στοιχείων υπολογιστή που είναι γνωστή μόνο σε συγκεκριμένο κύκλο προσώπων, υπόχρεων για τη τήρηση της μυστικότητας[47].

Το άρθρο 370Γ του Ποινικού Κώδικα αντικαθίσταται ως εξής:

«Άρθρο 370Γ Παράνομη πρόσβαση σε πληροφοριακό σύστημα

[47] Κωνσταντινίδης Α., « Η διακεκριμένη παραβίαση απόρρητων στοιχείων», Ποιν.Χρ, ΜΖ',1997, σελ. 876 επ.

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση».

Το άρθρο 370Γ ΠΚ, τροποποιείται και ενσωματώνει το άρθρο 3 της Οδηγίας, αποκτώντας τον τίτλο παράνομη πρόσβαση σε πληροφοριακό σύστημα. Καθιερώνει, πλέον ρητά, ως έγκλημα στο ελληνικό ποινικό σύστημα τις ενέργειες hacking/cracking κατά των πληροφοριακών συστημάτων. Στη διάταξη δε γίνεται διάκριση ανάλογα με το μέγεθος της προκαλούμενης ζημίας και προϋποθέσεις είναι οι χωρίς δικαίωμα απόκτησης πρόσβασης σε πληροφοριακό σύστημα και η παραβίαση μέτρων ασφαλείας ή απαγορεύσεων που έχει λάβει ο εγκαλών και νόμιμος κάτοχος του[48]. Ο Έλληνας νομοθέτης ποινικοποιεί και τις περιπτώσεις ήσσονος σημασίας, χωρίς να είναι επιβεβλημένο από την Οδηγία, προφανώς για να προλαμβάνει τις περιπτώσεις που κάποιος νέος επιχειρήσει να αποκτήσει πρόσβαση σε πληροφοριακό σύστημα.

Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:

«Άρθρο 370Δ

1. Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

[48] Ε. Βαγενά, « Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», ΔΙΜΕΕ, 2017, σελ.33

2. Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.

3. Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

Με το άρθρο 370Δ ΠΚ, ενσωματώνεται το άρθρο 6 της Οδηγίας σχετικά με την παράνομη υποκλοπή επικοινωνιών μέσω πληροφοριακών συστημάτων, τιμωρώντας πλέον αυτοτελώς την παραβίαση του απορρήτου των επικοινωνιών αν γίνεται μέσω πληροφοριακών συστημάτων. Η υποκλοπή περιλαμβάνει, ενδεικτικά, την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και παροχή του περιεχομένου των δεδομένων είτε άμεσα, με πρόσβαση και χρήση των συστημάτων πληροφοριών, είτε έμμεσα με τη χρήση ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα.

Μετά το άρθρο 370Δ του Ποινικού Κώδικα προστίθεται άρθρο 370Ε ως εξής:

«Άρθρο 370Ε

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Το άρθρο 370Ε ΠΚ, συμμορφώνεται πλήρως με το άρθρο 7 της Οδηγίας και προβλέπεται η τιμωρία της εκ προθέσεως διάθεσης προγραμμάτων, συσκευών ή άλλων εργαλείων, με τα οποία μπορεί να πραγματοποιηθεί πρόσβαση σε πληροφοριακό σύστημα και δυνατότητα διάπραξης των εγκλημάτων 370^{Α} έως 370Δ. Όπως και στο 292Γ , σε αυτήν την κατηγορία εντάσσονται κακόβουλο λογισμικό ή ιοί με σκοπό τη προσβολή μαζικού πλήθους υπολογιστών για την εκδήλωση επιθέσεων.

Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται άρθρο 381Α ως εξής

«Άρθρο 381Α

Φθορά ηλεκτρονικών δεδομένων

1. Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

Το άρθρο 381^{Α} ΠΚ ενσωματώνει το άρθρο 5 της Οδηγίας, αυτό της παράνομης παρεμβολής σε δεδομένα, προστατεύοντας πλέον και ρητά τα ψηφιακά δεδομένα από

πράξεις αλλοίωσης, φθοράς και καταστροφής. Καλύπτεται με αυτό το άρθρο άλλο ένα σημαντικό κενό της ελληνικής νομοθεσίας, καθώς δε μπορούσαν με κανένα τρόπο να προστατευτούν τα ηλεκτρονικά δεδομένα με το πρότερο νομοθετικό πλαίσιο και κρίθηκε επιβεβλημένη η αυτοτελής τυποποίηση του άρθρου 5 της Οδηγίας. Μέχρι πρότινος, τέτοιες πράξεις τιμωρούνταν από την Ελληνική νομοθεσία με τη διάταξη του άρθρου 381 ΠΚ περί φθοράς ξένης ιδιοκτησίας, η οποία δε μπορούσε να καλύψει ουσιαστικά την έννοια των ηλεκτρονικών δεδομένων, καθώς δε μπορούσε να λογιστεί ως πράγμα κατά την έννοια του αρ.381 ΠΚ. Σχετικά ποινικά αδικήματα, επίσης, προβλέπονται στο άρθρο 15 του Ν. 3471/2006 για πράξεις αφαίρεσης, αλλοίωσης, καταστροφή δεδομένων συνδρομητών ή χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών καθώς και στο άρθρο 22 § 4 Ν 2472/1997 αναφορικά με δεδομένα προσωπικού χαρακτήρα[49].

Μετά το άρθρο 381Α του Ποινικού Κώδικα προστίθεται άρθρο 381Β ως εξής:

«Άρθρο 381Β

Με φυλάκιση μέχρι δύο (2) ετών, τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα του άρθρου 381Α παράγραφοι 1, 2 και 3 παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Με το άρθρο 381Β ΠΚ, η ελληνική νομοθεσία εναρμονίζεται και σε αυτό το άρθρο, όπως στο αρ.292Γ με το άρθρο 7 της Οδηγίας, τυποποιώντας τη ποινική ευθύνη των προσώπων για πράξεις αγοράς, πώλησης , προμήθειας, κατοχής και λοιπών προγραμμάτων ή κωδικών που θα μπορούσαν να αποτελέσουν μέσο τέλεσης για τις πράξεις του 381Α. Συνεπώς, θα προβλέπεται ποινική δίωξη των επιθέσεων που διαπράττονται με διάδοση κακόβουλου λογισμικού ή ιών.

Το άρθρο 386Α του Ποινικού Κώδικα αντικαθίσταται ως εξής:

[49] Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011, σελ. 500

«Άρθρο 386Α

Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».

Το άρθρο 386^{Α}, τροποποιείται σύμφωνα με το άρθρο 8 της Σύμβασης της Βουδαπέστης. Στην προηγουμένη μορφή του αυτή η διάταξη είχε χρησιμοποιηθεί για την επιβολή κυρώσεων σε υποθέσεις υποκλοπής καρτών ανάληψης με παρέμβαση στα στοιχεία υπολογιστή. Σύμφωνα, με τις νέες τροποποιήσεις περιλαμβάνεται και σε περιπτώσεις απάτης με υπολογιστή, η χρήση ορθών δεδομένων που γίνεται χωρίς δικαίωμα, όπως για παράδειγμα σε περίπτωση που ο δράστης έχει αποκτήσει παράνομα και το όνομα χρήστη και τον κωδικό του δικαιούχου.

Σε συμμόρφωση με το άρθρο 11 της Οδηγίας, βρίσκεται το άρθρο 4 του Ν.4411/2016 για την ευθύνη των νομικών προσώπων, όπου ορίζονται τα παρακάτω :

«Αν κάποια από τις πράξεις των άρθρων 292Β, 370Γ, 370Δ, 370Ε, 381Α και 386Α του Ποινικού Κώδικα τελέστηκε, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, από φυσικό πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου ή της ένωσης προσώπων και έχει εξουσία εκπροσώπησής τους ή εξουσιοδότηση για τη λήψη αποφάσεων για λογαριασμό τους ή για την άσκηση ελέγχου εντός αυτών, επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων με ειδικά αιτιολογημένη απόφαση της Αρχής Διασφάλισης του Απόρρητου των Επικοινωνιών, κατά περίπτωση, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις,

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 20.000 έως 1.000.000 ευρώ,

γ) ανάκληση ή αναστολή της άδειας λειτουργίας τους για χρονικό διάστημα από ένα (1) μήνα έως δύο (2) έτη ή απαγόρευση άσκησης της επιχειρηματικής τους δραστηριότητας για το ίδιο χρονικό διάστημα,

δ) αποκλεισμός από δημόσιες παροχές, ενισχύσεις, επιδοτήσεις, αναθέσεις έργων και υπηρεσιών, προμήθειες, διαφημίσεις και διαγωνισμούς του Δημοσίου ή των νομικών προσώπων του δημόσιου τομέα για το ίδιο διάστημα.

Σε περίπτωση υποτροπής οι κυρώσεις των περιπτώσεων γ΄ και δ΄ μπορεί να έχουν οριστικό χαρακτήρα και εφόσον πρόκειται περί σωματείων ή ενώσεων προσώπων, η υποτροπή μπορεί να έχει ως συνέπεια τη διάλυσή τους, σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις.

2. Όταν η έλλειψη εποπτείας ή ελέγχου από φυσικό πρόσωπο που αναφέρεται στην παράγραφο 1, κατέστησε δυνατή την τέλεση από πρόσωπο που τελεί υπό την εξουσία του κάποιας από τις αξιόποινες πράξεις που αναφέρονται στην ίδια ως άνω παράγραφο, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, επιβάλλονται στο νομικό πρόσωπο, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις:

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 10.000 έως 1.000.000 ευρώ,

γ) οι προβλεπόμενες στις περιπτώσεις γ΄ και δ΄ της προηγούμενης παραγράφου κυρώσεις για χρονικό διάστημα από δέκα (10) ημέρες έως έξι (6) μήνες.

3. Για τη σωρευτική ή διαζευκτική επιβολή των κυρώσεων που προβλέπονται στις προηγούμενες παραγράφους και για την επιμέτρηση των κυρώσεων αυτών λαμβάνονται υπόψη ιδίως η βαρύτητα της παράβασης, ο βαθμός της υπαιτιότητας, η οικονομική επιφάνεια του νομικού προσώπου ή της ένωσης προσώπων και η τυχόν υποτροπή τους.

4. Η εφαρμογή των διατάξεων των προηγούμενων παραγράφων είναι ανεξάρτητη από την αστική, πειθαρχική ή ποινική ευθύνη των αναφερόμενων σε αυτές φυσικών προσώπων. Καμιά κύρωση δεν επιβάλλεται χωρίς προηγούμενη κλήτευση των νόμιμων εκπροσώπων του νομικού

προσώπου ή της ένωσης προσώπων προς παροχή εξηγήσεων. Η κλήση κοινοποιείται τουλάχιστον δέκα (10) ημέρες πριν από την ημέρα της ακρόασης. Κατά τα λοιπά, εφαρμόζονται οι διατάξεις των παραγράφων 1 και 2 του άρθρου 6 του Κώδικα Διοικητικής Διαδικασίας. Σε περίπτωση άσκησης ποινικής δίωξης για κάποια από τις προβλεπόμενες στην παράγραφο 1 αξιόποινες πράξεις που τελέστηκε από πρόσωπο αναφερόμενο στις παραγράφους 1 και 2 και προκειμένου να εφαρμοστεί η προβλεπόμενη στο άρθρο αυτό διαδικασία επιβολής διοικητικών κυρώσεων, οι εισαγγελικές αρχές ενημερώνουν αμέσως τον Υπουργό Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και αποστέλλουν σε αυτόν αντίγραφα της δικογραφίας.

5. Σε περίπτωση αμετάκλητης απαλλαγής του παραπεφθέντος οι κατά τα ανωτέρω αποφάσεις επιβολής διοικητικών κυρώσεων ανακαλούνται.

6. Οι διατάξεις των προηγουμένων παραγράφων δεν εφαρμόζονται στο κράτος, στους φορείς δημόσιας εξουσίας και στους διεθνείς οργανισμούς δημοσίου δικαίου, χωρίς αυτό να επηρεάζει την εφαρμογή των ισχυουσών κάθε φορά διατάξεων περί αστικής, πειθαρχικής ή ποινικής ευθύνης».

Η ανάγκη της σχετικής πρόβλεψης έγκειται στο γεγονός ότι οι σχετικές ενέργειες με την παράνομη πρόσβαση ή παρακώλυση πληροφοριακών συστημάτων στοχεύουν συχνά στην παρεμπόδιση της δραστηριότητας μίας ανταγωνιστικής επιχείρησης ή κάποιου φορέα που προωθεί διαφορετικές θέσεις από ένα άλλο νομικό πρόσωπο[50]. Ενδεχομένως, όμως, να έπρεπε στη συγκεκριμένη διάταξη να εμπίπτει και ευθύνη κρατών, φορέων δημόσιας εξουσίας ή και ακόμα διεθνών οργανισμών.

Τέλος, ένας τομέας, αρκετά ιδιαίτερος, όμως, όπως προαναφέρθηκε σε παραπάνω κεφάλαιο και δεν θίγεται καθόλου είναι αυτός της εξιχνίασης των ηλεκτρονικών εγκλημάτων κα ιδιαίτερα στην εξέταση των ψηφιακών πειστηρίων. Παρά την ύπαρξη της αρμόδιας υπηρεσίας, η οποία τα τελευταία χρόνια σημειώνει βήματα προόδου, θα έπρεπε να προβλεφθεί από τον 4411/2016 σχετική διάταξη και για αυτόν τον τομέα που θα είχε περισσότερο ρόλο οδηγού, όπως στην Αγγλία ή και στην Ευρώπη, όπου ο Enisa έχει εκδώσει σχετικό οδηγό.

[50] Ε. Βαγενά, « Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», ΔΙΜΕΕ, 2017, σελ.36

Το νέο θεσμοθετημένο νομοθετικό πλαίσιο παρά τη μακροχρόνια και περιπετειώδη νομοπαρασκευαστική διαδικασία, συμβάλλει στον εκσυγχρονισμό της καταπολέμησης του ηλεκτρονικού εγκλήματος στην Ελλάδα. Τυποποιεί αυτοτελώς νέα αδικήματα, εισάγει ως έννομα αγαθά, το πληροφοριακό σύστημα και τα ψηφιακά δεδομένα και ενσωματώνεται πλήρως στα διεθνή και ενωσιακά νομικά πλαίσια. Παρά τις όποιες ελλείψεις, δε παύσει να αποτελεί τον νόμο-θεμέλιο για την ορθή και αποτελεσματική αντιμετώπιση των εγκλημάτων του διαδικτύου στην χώρα μας.

4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η τεχνολογία, οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο, σήμερα εν έτει 2018, αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας μας πόσο μάλλον της επαγγελματικής και οικονομικής μας ευημερίας. Γι' αυτόν τον λόγο κρίνεται απαραίτητο να προασπίσουμε με κάθε τρόπο τα αγαθά που μας έχουν προσφέρει οι νέες τεχνολογίες. Τα διεθνή, ενωσιακά και εθνικά νομικά πλαίσια είναι επιβεβλημένα για να χαράξουν τον τρόπο καταπολέμησης των εγκλημάτων του διαδικτύου, αλλά από μόνο του δεν αρκεί. Πρέπει να διαδοθεί από τα κράτη και από τους αρμόδιους φορείς η ανάγκη διαφύλαξης και προστασίας των πληροφοριακών συστημάτων, τα οποία είναι ύψιστης σημασίας ζωτικό αγαθό για την ομαλή λειτουργία μιας κοινωνίας. Πρέπει η πρόληψη και η αποφυγή των ηλεκτρονικών εγκλημάτων να βρίσκονται σε πρώτη κλίμακα στην ατζέντα των κρατών και των αρμοδίων οργανισμών, χωρίς να συνεπάγεται πως το αυστηρό πλαίσιο κυρώσεων και η συστηματική τους στοιχειοθέτηση στο εσωτερικό δίκαιο των χωρών δεν είναι ένα πολύ σημαντικό βήμα στην καταπολέμηση της εγκληματικότητας του διαδικτύου.

Το διαδίκτυο έχει φτιαχτεί για να κάνει καλύτερη τη ζωή των ανθρώπων. Δεν πρέπει αυτή η «σκοτεινή πλευρά του» να παραβλέπει όλα τα σημαντικά οφέλη που παρέχει στις ζωές μας. Αντίθετα, θα πρέπει να αποτελεί κίνητρο για τη καλύτερη συνεργασία μεταξύ των κρατών και των διεθνών οργανισμών. Ο τομέας των δικαστικών και αστυνομικών αρχών επιδέχεται περισσότερης εξέλιξης, καθώς στον τομέα εξιχνίασης αυτών των ιδιαίτερων εγκλημάτων, είναι δυσχερής η καταγραφή και έρευνα των εγκλημάτων. Θα πρέπει να χρησιμοποιηθούν περισσότερο άκρως προηγμένης τεχνολογίας εργαλεία, ως αντίβαρο στις οργανωμένες και εξελιγμένες επιθέσεις κατά των πληροφοριακών συστημάτων. Υπάρχει, πλέον το απαραίτητο ανθρώπινο δυναμικό με την ανάλογη τεχνογνωσία ώστε να μπορεί να

προλαμβάνει κάθε είδους ηλεκτρονική επίθεση. Η ασφάλεια του διαδικτύου αποτελεί το ζητούμενο της σημερινής εποχής. Για να έρθει απαιτείται διαρκής συντονισμός σε διεθνές επίπεδο και τεχνολογική εγρήγορση.

ΒΙΒΛΙΟΓΡΑΦΙΑ- ΑΡΘΡΟΓΡΑΦΙΑ

- Αγγελής Ι. «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», *ΠοινΔικ 12/2001*
- Αγγελής Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime)», ΠοινΔικ 2001
- Αιτιολογική Έκθεση της Πρότασης Απόφασης-Πλαισίου του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών (υποβληθείσα από την Επιτροπή), Επιτροπή των Ευρωπαϊκών Κοινοτήτων, Βρυξέλλες, 19.04.2002, COM(2002) 173
- Ε. Βαγενά, «Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», ΔΙΜΕΕ, 2017
- Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα. Μορφές, πρόληψη, αντιμετώπιση», Νομική Βιβλιοθήκη, 2007
- Christian Adrian, «Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level», Journal of law and international science, 2015
- Καϊάφα-Γκμπάντι Μ., «Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη», ΠοινΧρ 2011
- Καϊάφα-Γκμπάντι Μ., «Εισηγήσεις Ποινικό Δίκαιο και Καταχρήσεις της Πληροφορικής», Αρμ 2007
- Καράκωστας Ι., «Δίκαιο και internet», Π.Ν. Σάκκουλας, 2009
- Κριθαράς Θ., «Ποινικό Δίκαιο και διαδίκτυο», Νομική Βιβλιοθήκη, 2009
- Κωνσταντινίδης Α., «Παρατηρήσεις στην ΑΠ 121/2003», ΠοινΧρ, 2003
- Κωνσταντινίδης Α., « Η διακεκριμένη παραβίαση απόρρητων στοιχείων», Ποιν.Χρ, ΜΖ', 1997
- Σιδηρόπουλος Θ., «Το δίκαιο του διαδικτύου», 2009
- Τσόλιας Γρ., «Η πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου», σε Πρακτικά

2ου Πανελλήνιου Συνεδρίου e-ΘΕΜΙΣ «Αντιμέτωποι με τις σύγχρονες τεχνολογικές εξελίξεις» (Προσωπικά Δεδομένα-Ηλεκτρονικό Έγκλημα-Ηλεκτρονικό Εμπόριο), Νομική Βιβλιοθήκη, 2011

- Φαραντούρης Ν., "Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο. Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του hacking και της μόλυνσης με ιούς", ΠοινΔικ 2003
- Χαραλαμπάκης Αρ., "Ποινικός Κώδικας Ερμηνεία κατ' άρθρο", Τόμος Δεύτερος (Άρθρα 207-435), Νομική Βιβλιοθήκη, 2011
- Wennerstorm E., "EU-legislation and Cybercrime", 2011