ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ
ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΑΓΚΟΣΜΙΟ ΚΑΙ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ
- ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΤΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ -

Διπλωματική Εργασία

της

Θάλειας Δερμεντζή

Φεβρουάριος 2022
Θεσσαλονίκη

ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΑΓΚΟΣΜΙΟ ΚΑΙ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ
- ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΤΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ -

Θάλεια Δερμεντζή

Πτυχιούχος Νομικής ΑΠΘ, 2010

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 26/02/2022

Θεοχάρης Δαλακούρας	Εμμανουήλ Στειακάκης	Αποστολίδης Νικόλαος
.....	.....	.....

Θάλεια Δερμεντζή

Περίληψη

Η ασφάλεια στον κυβερνοχώρο αποτελεί στις μέρες μας ένα από τα σημαντικότερα αντικείμενα μελέτης διεθνώς. Ειδικά, στην εποχή covid19 που διανύουμε τα κράτη έχουν να διαχειριστούν αμέτρητες προκλήσεις σε επίπεδο κυβερνοασφάλειας, αφού η πανδημία έχει περιορίσει κατά πολύ τις συναλλαγές πέρα από το διαδίκτυο.

Η παρούσα μελέτη έχει ως σκοπό να αναλύσει τα χαρακτηριστικά, τις μεθόδους και τους δράστες της κυβερνοτρομοκρατίας, αλλά και το νομικό πλαίσιο αυτής στην Ευρωπαϊκή Ένωση, αλλά και στην Ελλάδα. Επιπρόσθετα, θα γίνει αναφορά στην κυβερνοασφάλεια και πώς αυτή επιτυγχάνεται. Ιδιαίτερη αναφορά θα γίνει στην κυβερνοασφάλεια εν μέσω πανδημίας και στους τρόπους αντιμετώπισης και διαχείρισης των κινδύνων της ψηφιακής εποχής.

Λέξεις κλειδιά: κυβερνοτρομοκρατία, κυβερνοασφάλεια, κυβερνοχώρος

Abstract

Cybersecurity is nowadays one of the most important subjects of study internationally. Especially in this time of covid19, states have countless cybersecurity challenges to manage, since the pandemic has greatly limited transactions beyond the internet.

The present study aims to analyze the characteristics of the methods and perpetrators of cyberterrorism and the legal framework in the European Union and in Greece. In addition, reference will be made to cybersecurity and how it is achieved. Particular reference will be made to post-coronavirus cybersecurity and ways to address and manage the risks of the digital age.

Keywords: cyber terrorism, cyber security, cyberspace

Πρόλογος – Ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε κατά την χειμερινή περίοδο του Ακαδημαϊκού Έτους 2021 - 2022, στα πλαίσια του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) “Δίκαιο και Πληροφορική” του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας και του Τμήματος Νομικής του Δημοκριτείου Πανεπιστημίου Θράκης.

Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Θεοχάρη Δαλακούρα, Καθηγητή Ποινικού Δικονομικού Δικαίου στη Νομική Σχολή ΔΠΘ, στον οποίο οφείλω να εκφράσω τις θερμές μου ευχαριστίες για την καθοδήγησή του, κατά την εκπόνηση της Διπλωματικής μου Εργασίας.

Τέλος, ευχαριστώ θερμά την οικογένειά μου, τον σύζυγο και τους δυο γιους μου για την συμπαράσταση που μου έδειξαν ολόκληρη την περίοδο εκπόνησης της εργασίας αυτής.

Περιεχόμενα

Πίνακας αρκτικόλεξων και βραχυγραφιών

CSIRT	**Computer Security Incident Response Team** - Ομάδα απόκρισης για περιστατικά που αφορούν την ασφάλεια των υπολογιστών και τον κίνδυνο εθνικών προκλήσεων στα συστήματα δικτύου και πληροφορικής
ENISA	**European Union Agency for Cybersecurity** - Οργανισμός Ευρωπαϊκής Ένωσης. Πρόκειται για το κέντρο πληροφοριών και εμπειρογνωμοσύνης σε ό, τι αφορά τα θέματα της κυβερνοασφάλειας.
EMP	**Electromagnetic Pulse** - Ηλεκτρομαγνητικός Παλμός. Πρόκειται για ένα ισχυρότατο κύμα μέσω του οποίου μεταφέρεται ηλεκτρομαγνητική ενέργεια ικανή να καταστρέψει πληροφορικά συστήματα και συστήματα τηλεπικοινωνίας.
ΡΑΕ	**Ρυθμιστική Αρχή Ενέργειας**
ISIS	**Islamic State of Iraq and Syria:** Πρόκειται για τρομοκρατική ομάδα
PESCO	**PErmanent Structured COoperation on security and defence:** Στρατιωτική συνεργασία μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης που θέλουν να συμμετάσχουν ιδιαίτερα στην Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)
EUGS	**European Union Global Strategy:** Επικαιροποιημένο δόγμα - έγγραφο της Ευρωπαϊκής Ένωσης για τη βελτίωση της αποτελεσματικότητας της άμυνας και της ασφάλειας της Ένωσης και των κρατών μελών της
CARD	**Coordinated Annual Review on Defence** -Ετήσια Αναθεώρηση Άμυνας
ΕΤΑ	Ευρωπαϊκό Ταμείο Άμυνας
DDoS	**Distributed Denial of Service** - Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας: Είναι μια προσπάθεια για να καταστεί μια online υπηρεσία μη διαθέσιμη από υπέρογκη κυκλοφορία με κλήσεις για εμφάνιση από πολλαπλές πηγές. Οι επιθέσεις αυτές στοχεύουν μια μεγάλη ποικιλία από σημαντικούς πόρους, από τις τράπεζες έως τις ιστοσελίδες ειδήσεων και αποτελούν σημαντική πρόκληση στο να διασφαλιστεί ότι οι άνθρωποι απρόσκοπτα θα μπορούν να δημοσιεύουν και να έχουν πρόσβαση σε σημαντικές πληροφορίες
NIS	**Network and Information Security**: Πρόκειται για Ευρωπαϊκή Οδηγία, που στην ουσία αποτελεί το πρώτο νομοσχέδιο σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο και ο ειδικός του στόχος ήταν να επιτευχθεί υψηλό κοινό επίπεδο ασφάλειας στον κυβερνοχώρο στα κράτη μέλη.
ΝΑΚ	**Νέα Ανεξάρτητα Κράτη (πρώην ΕΣΣΔ)**
Φ.Ε.Β.Υ.	Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών
RAT	**Remote Access Trojan:** Είναι ένας τύπος κακόβουλου λογισμικού (malware) που επιτρέπει στους hackers να παρακολουθούν και να ελέγχουν τον υπολογιστή ή το δίκτυο.
Μ.Δ.Σ.	**Μόνιμη Διαρθρωμένη Συνεργασία (PESCO)**
ΣΛΕΕ	**Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης**
ΑΔΑΕ	**Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών**

1 Εισαγωγή

1.1 Από την εποχή της πληροφορίας στην ψηφιακή εποχή

Η μελέτη της ανθρώπινης ιστορίας είναι αλληλένδετη με την πρόοδο της τεχνολογίας. Η τεχνολογία άσκησε τεράστια επίδραση στην ανθρώπινη σκέψη και δράση, άλλαξε τα πολιτικά και οικονομικά συστήματα και την αντίληψη για τη γνώση.

Η σημερινή περίοδος χαρακτηρίζεται ως «μεταμοντέρνα» και ως αφετηρία της θεωρείται η ίδρυση του Οργανισμού των Ηνωμένων Εθνών. Αυτή είναι ουσιαστικά και η πρώτη προσπάθεια για παγκοσμιοποίηση. Πιο συγκεκριμένα, το γεγονός που συνετέλεσε ώστε να εισέλθει η ανθρωπότητα στην εποχή της πληροφορίας ήταν η εφεύρεση του τρανζίστορ το 1947. Μετέπειτα, οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο ήταν ο δίαυλος για την έναρξη της ψηφιακής εποχής.

Η ψηφιακή εποχή δημιούργησε έναν καινούργιο και παράλληλα άυλο κόσμο που κινείται ταυτόχρονα με τον υλικό. Έναν κόσμο, όμως, χωρίς προκαθορισμένο περιεχόμενο, αλλά που υπόκειται στην εκπαίδευση, την κοινωνικοποίηση, την ύπαρξη ή απουσία κανόνων και τις συνέπειες της παραβίασης τους.

Η ραγδαία εξέλιξη αυτού του ψηφιακού κόσμου, χωρίς καμία διαδικασία προετοιμασίας και προσαρμογής, δημιούργησε δυσκολίες στην «ψηφιακή κοινωνικοποίηση», αφού απουσιάζουν σημαντικοί θεσμοί που συμβάλλουν στην ομαλή ένταξη σε μια ομάδα, όπως η οικογένεια και το σχολείο. Επομένως, το άτομο λειτουργεί αυτόνομα, χωρίς περιορισμούς και με τη συγκάλυψη της ανωνυμίας που του προσφέρεται δρα με απεριόριστο το αίσθημα της ελευθερίας, φτάνοντας στα όρια της αναρχίας. Η κατάσταση αυτή φέρει ως αποτέλεσμα τη δημιουργία απειλών τόσο για την εθνική όσο και για την εσωτερική ασφάλεια των κρατών.

Σε καθημερινή βάση οι πιο ισχυρές χώρες της γης προσπαθούν να θωρακιστούν στον κυβερνοχώρο και να αποτρέψουν κυβερνοεπιθέσεις από άλλα κράτη, μη κυβερνητικές οργανώσεις και hackers. Στον κυβερνοχώρο, εξαιτίας των απροσδιόριστων παρακρατικών και τρομοκρατικών οργανώσεων, του πλήθους των πληροφοριών που διατίθενται και κυρίως της ανωνυμίας των χρηστών, οι κυβερνοεπιθέσεις είναι δύσκολο να εντοπιστούν και εύκολο να οργανωθούν. Ο κυβερνοχώρος δε διαθέτει συγκεκριμένα

γεωγραφικά όρια, γεγονός που ενισχύει τη δυνατότητα πραγματοποίησης μεγάλου βαθμού εγκληματικής δραστηριότητας σε περισσότερα του ενός κράτη.

Ειδικότερα, το δεύτερο τρίμηνο του 2017 οι κυβερνοεπιθέσεις παρουσίασαν σημαντική αύξηση και ο στόχος τους είναι ολοένα και περισσότερο οι Οργανισμοί και οι πολυεθνικές οργανώσεις. Με τη χρήση εξελιγμένων και πιο περίπλοκων μεθόδων, όπως η μόλυνση με κακόβουλο λογισμικό που ελέγχεται από απόσταση, επιτίθενται στα πληροφορικά συστήματα. Επιπρόσθετα, το τελευταίο διάστημα έχει εμφανιστεί ένα νέο είδος επίθεσης που δεν απαιτεί την εγκατάσταση κακόβουλου λογισμικού. Αντιθέτως, με την αποστολή ενός απλού ηλεκτρονικού μηνύματος οι δράστες, ζητούν από τους θύτες χρηματικά ποσά και απειλούν με επίθεση, αν δεν τους καταβληθούν σε προκαθορισμένο χρονικό διάστημα.

Συμπερασματικά, σύμφωνα με τις προαναφερθείσες εξελίξεις, επιβάλλεται η νομική ρύθμιση της κατάστασης, ώστε να αντιμετωπιστεί και να αποφευχθεί οποιαδήποτε μορφή κυβερνοεπίθεσης, όπως αυτή της κυβερνοτρομοκρατίας.

Επομένως, γίνεται κατανοητό ότι είναι επιτακτική η ανάγκη της παρουσίας κυβερνοασφάλειας, ώστε να υπάρχει ομαλή λειτουργία των θεσμών και προστασία της οικονομίας και του πολιτισμού των κρατών, μέσω μίας πιο ενισχυμένης και οργανωμένης διακρατικής προσπάθειας και διατομεακής συνεργασίας για την πρόληψη, αλλά και την στοχευμένη αντιμετώπιση της κυβερνοεγκληματικότητας. Οι λόγοι που την καθιστούν προτεραιότητα είναι αρκετοί. Πιο συγκεκριμένα, στη σημερινή εποχή το διαδίκτυο χρησιμοποιείται όλο και περισσότερο για καθημερινές οικονομικές συναλλαγές και επικοινωνίες των ιδιωτών, αλλά και των κρατικών φορέων για τις ημερήσιες λειτουργίες τους. Οι παραπάνω λόγοι επεξηγούν γιατί τα κράτη ασχολούνται συστηματικά με την αντιμετώπιση οποιουδήποτε προβλήματος και οποιασδήποτε απειλής επιτελείται στον κυβερνοχώρο.

Η Ευρωπαϊκή Ένωση συχνά εφαρμόζει στρατηγικές για να αντιμετωπίζει και να προβλέπει περιπτώσεις κυβερνοτρομοκρατίας με κύριο γνώμονα την εξασφάλιση της λειτουργίας της κοινής αγοράς, την προστασία της ίδιας της Ένωσης, τη διασφάλιση ενός καλού επιπέδου ασφάλειας και ευημερίας και την προάσπιση των δικαιωμάτων των πολιτών.

1.2 Ορισμοί και βασικές έννοιες

Οι βασικοί όροι που θα χρησιμοποιηθούν στην παρούσα εργασία έχουν ως πρώτο συνθετικό το πρόθεμα «κυβερνο-» (cyber-). Με αυτό το πρόθεμα ξεκινούν όσες λέξεις σχετίζονται με το διαδίκτυο και τους ηλεκτρονικούς υπολογιστές και χρησιμοποιείται για να περιγράψει ένα πρόσωπο, ένα πράγμα ή μια ιδέα, ως μέρος της εποχής του υπολογιστή και της πληροφορίας.

Αρχικά, ο όρος «κυβερνοχώρος» οριοθετεί εννοιολογικά τον νοητό χώρο που δημιουργείται από τη χρήση του διαδικτύου και των ηλεκτρονικών υπολογιστών.

Ο όρος αποδίδεται στον συγγραφέα επιστημονικής φαντασίας William Gibson και συγκεκριμένα πρωτοεμφανίστηκε στο έργο του Neuromancer (Νευρομάντης) το 1984:

> *"Μία ομόφωνη παραίσθηση που βιώνεται καθημερινά από δισεκατομμύρια νόμιμους χρήστες, σε κάθε χώρα, από παιδιά που μαθαίνουν μαθηματικές αρχές... Μία γραφική απεικόνιση δεδομένων απομονωμένων από κάθε υπολογιστή στο ανθρώπινο σύστημα. Αδιανόητη περιπλοκότητα. Γραμμές φωτός εκτείνονται στο μή-χώρο της διανόησης, ομάδες και αστερισμοί πληροφοριών. Όπως τα φώτα μιας πόλης υποχωρούν…".*

Στην πραγματικότητα, ο κυβερνοχώρος μπορεί να θεωρηθεί ως η διασύνδεση των ανθρώπων μέσω υπολογιστών και τηλεπικοινωνιών, ανεξάρτητα από τη φυσική γεωγραφία.

Δημιουργήθηκε σταδιακά και οφείλεται στην ανάπτυξη της επιστήμης και της τεχνολογίας. Αποτελείται από έναν ιστό διασυνδεδεμένων δικτύων, όπου αποθηκεύονται παντός είδους πληροφορίες και όπου συνδέονται και οι υποδομές των χωρών, αφού πλέον όλο και περισσότερο διεξάγονται σε αυτόν οι ανθρώπινες δραστηριότητες.

Οι ρυθμοί ανάπτυξης του Κυβερνοχώρου και η έλλειψη παρουσίας κάποιας ρυθμιστικής Αρχής επιτρέπουν να λαμβάνουν μέρος παράνομες ενέργειες από μεμονωμένα άτομα, πολιτικές ομάδες ή ομάδες κρατών.

Ουσιαστικά, το διαδίκτυο και κατ’ επέκταση ο κυβερνοχώρος είναι ένα περίπλοκο περιβάλλον, όπου το μέγεθος του είναι πρακτικά άπειρο και κατά συνέπεια η δυνατότητα πρόσβασης στο σύνολό του καθίσταται αδύνατη. Γι’ αυτό και ο έλεγχος και η προστασία του για αποφυγή παράνομων και εγκληματικών ενεργειών είναι αρκετά πολύπλοκη υπόθεση.

Στις εγκληματικές ενέργειες εντάσσεται η κυβερνοτρομοκρατία και οι κυβερνοεπιθέσεις.

Ο όρος κυβερνοτρομοκρατία είναι σύλληψη του Μπάρυ Κόλλιν, ανώτερου στελέχους του Ινστιτούτου Πληροφοριών των Η.Π.Α. και αναφέρεται στη συνάντηση του κυβερνοχώρου με την τρομοκρατία. Ξεκίνησε στα μέσα της δεκαετίας του 1990 αναφορικά με τις απειλές της επερχόμενης ψηφιακής εποχής. Περιλαμβάνει δύο από τις μεγαλύτερες φοβίες της εποχής μας: τον φόβο μιας ξαφνικής και συνάμα καταστροφικής τρομοκρατικής επίθεσης και τον φόβο της απρόβλεπτης και πολύπλοκης ηλεκτρονικής τεχνολογίας. Ως όρος η κυβερνοτρομοκρατία δεν συναντάται ούτε στα διεθνή ούτε στα εθνικά νομοθετικά κείμενα.

Το 2000 η ερευνήτρια και Καθηγήτρια της επιστήμης της Πληροφορικής, Dorothy Denning, συμπλήρωσε τον ορισμό, συσχετίζοντάς τον με παράνομες επιθέσεις εναντίον του υπολογιστή, του δικτύου ή πληροφοριών δικτύου, με σκοπό τον εκφοβισμό ή εξαναγκασμό μιας κυβέρνησης, ώστε να επιτευχθούν πολιτικοί ή κοινωνικοί στόχοι. Προϋπόθεση όμως είναι, η επίθεση να καταλήγει σε βία απέναντι στα πρόσωπα που απευθύνεται ή έστω να δημιουργεί έντονο το συναίσθημα του φόβου ή να έχει ως αποτέλεσμα θάνατο, τραυματισμό ή οικονομική απώλεια.

Κατά έναν άλλον ορισμό, ως κυβερνοτρομοκρατία ορίζεται η εκτέλεση μιας ξαφνικής επίθεσης από εθνική ή τρομοκρατική οργάνωση με τη χρήση της τεχνολογίας, των υπολογιστών και του ίντερνετ, με στόχο να απενεργοποιηθούν οι εθνικές ηλεκτρονικές και φυσικές υποδομές και να δημιουργηθεί απώλεια σε βασικές υπηρεσίες.

Γενικότερα υπάρχει μία διχογνωμία σχετικά με τον ορισμό του φαινομένου της κυβερνοτρομοκρατίας. Η μία άποψη ερευνά το φαινόμενο με βάση την μέθοδο της αιτίας-αποτελέσματος και η άλλη είναι εκείνη που την ερευνά στηριζόμενη στην διαδικτυακή της δράση. Σε ό, τι αφορά την πρώτη άποψη, εκείνη της αιτίας - αποτελέσματος, η τρομοκρατία του κυβερνοχώρου υπάρχει όταν επιθέσεις μέσω των ηλεκτρονικών υπολογιστών καταλήγουν σε μία κατάσταση όπου ο φόβος παράγεται, όπως και σε μία παραδοσιακή τρομοκρατική πράξη.

Με μία πιο σαφή και απλουστευμένη ερμηνεία, ως κυβερνοτρομοκρατία ορίζεται μια «Εγκληματική πράξη που διαπράττεται μέσω υπολογιστών και έχει ως αποτέλεσμα τη βία, θανάτους ή καταστροφές, δημιουργώντας ένα αίσθημα τρόμου, το οποίο έχει στόχο να επηρεάσει την πολιτική μίας κυβέρνησης».

Επιπλέον, για να χαρακτηριστεί κάποιος ως τρομοκράτης και η ενέργειά του ως τρομοκρατική, θα πρέπει να πληροί τα ακόλουθα κριτήρια:

1. Η πράξη του πρέπει να είναι προμελετημένη και να υποκινείται από ιδεολογικά συμφέροντα
2. Να πραγματοποιείται ενάντια σε αμάχους, από συγκεκριμένες ομάδες.
3. Να είναι ικανή να διασπείρει τον τρόμο με σκοπό να επηρεαστούν οι κυβερνόντες.

Η χρήση του διαδικτύου, καθώς και άλλων συσκευών τηλεπικοινωνίας είναι συνεχώς αυξανόμενη. Η ασφάλεια των συνόρων και των ατόμων οδηγεί τους τρομοκράτες και τους εξτρεμιστές να χρησιμοποιούν το Ιντερνέτ για να πλήξουν ισχυρά κράτη του διεθνούς συστήματος, κυρίως τις Ηνωμένες Πολιτείες. Εξαιτίας των αδυναμιών σε ότι έχει να κάνει με την ασφάλεια στην χρήση του Διαδικτύου και των υπολογιστών, αυτό θα μπορούσε να δώσει την ευκαιρία στους τρομοκράτες να ενισχύσουν τις γνώσεις τους στα υπολογιστικά συστήματα, καθώς και να συμπράξουν με εγκληματικές οργανώσεις.

Επομένως, γίνεται εύκολα κατανοητό ότι η παρουσία κυβερνοασφάλειας είναι ζωτικής σημασίας, ώστε να προληφθούν και να αποφευχθούν οποιασδήποτε μορφής εγκληματικές ενέργειες εναντίον των συστημάτων πληροφορικής και επικοινωνιών.

Ως κυβερνοσφάλεια, ορίζεται η προστασία των δικτύων, των συστημάτων η/υ και των δεδομένων από κυβερνοεπιθέσεις. Για τον σκοπό αυτό αναπτύχθηκαν στρατηγικές με στόχο την διασφάλιση οικονομικής και κοινωνικής ευημερίας και την προστασία απέναντι στις απειλές ασφάλειας. Οι στρατηγικές αυτές ενισχύουν την κυβερνητική συνεργασία και δίνουν έμφαση στον προσδιορισμό των ρόλων και των αρμοδιοτήτων σε ό, τι σχετίζεται με τη δίωξη του ηλεκτρονικού εγκλήματος. Επίσης, ενισχύουν τη συνεργασία μεταξύ δημοσίων και ιδιωτικών φορέων (ειδικά σε ό, τι αφορά παρόχους υπηρεσιών διαδικτύου), αλλά και τη διεθνή συνεργασία.

Οι υπηρεσίες που ηγούνται της κυβερνοασφάλειας είναι:

1. Η Εθνική Αρχή Κυβερνοασφάλειας: Είναι η εθνική αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.
2. Η Ομάδα CSIRT: Είναι ομάδα απόκρισης για περιστατικά που αφορούν την ασφάλεια των υπολογιστών και τον κίνδυνο εθνικών προκλήσεων στα συστήματα δικτύου και πληροφορικής.
3. Ο Οργανισμός Ευρωπαϊκής Ένωσης (ENISA): Πρόκειται για το κέντρο πληροφοριών και εμπειρογνωμοσύνης σε ό, τι αφορά θέματα

κυβερνοασφάλειας. Έχει ως σκοπό την ανταλλαγή βέλτιστων πρακτικών και την υποβολή προτάσεων ανάμεσα στα κράτη- μέλη της Ευρωπαϊκής Ένωσης, αλλά και την ενθάρρυνση συνεργασίας ανάμεσά τους, για την προστασία από κυβερνοεπιθέσεις.

4. Το Ευρωπαϊκό Κέντρο Ικανοτήτων, το οποίο δημιουργήθηκε για να συμβάλλει στην υλοποίηση του προγράμματος για την Ψηφιακή Ευρώπη σε θέματα που σχετίζονται με την κυβερνοασφάλεια. Επιπλέον, θα βοηθάει και θα συντονίζει το έργο των Εθνικών Κέντρων Συντονισμού και θα βρίσκεται στον τομέα της βιομηχανίας, του δημοσίου τομέα και των ερευνητικών κοινοτήτων. Τέλος, θα προβαίνει σε χρηματοδοτήσεις σε ό, τι αφορά τα παραπάνω, με τη μορφή επιχορήγησης ή βραβείων.

2 Κυβερνοτρομοκρατία

Η πρώτη εμφάνιση των τρομοκρατών στο διαδίκτυο παρουσιάστηκε στο τέλος της δεκαετίας του 1990 με την ψηφιακή υποδομή να γίνεται σταδιακά ολοένα και περισσότερο επικίνδυνη στα χέρια των τρομοκρατών αφενός με τη χρήση των μέσων ενημέρωσης και αφετέρου με την χρήση των κοινωνικών δικτύων. Το διαδίκτυο ενέπνευσε τους τρομοκράτες να δημιουργήσουν μια διαδικτυακή αίθουσα για εκπαιδευτική προετοιμασία με σκοπό τη διεξαγωγή τρομοκρατικών επιθέσεων. Μετά τα γεγονότα της 11ης Σεπτεμβρίου, η απειλή της διεθνούς ασφάλειας βρέθηκε στο επίκεντρο της προσοχής των κυβερνήσεων, με το έργο της διατήρησης της ασφάλειας να καθίστανται ιδιαίτερα δύσκολο, καθώς οι νέες τεχνολογίες δεν είναι ικανές να αντιμετωπίσουν πλήρως τις τακτικές και μεθόδους των σύγχρονων τρομοκρατών.

Το 2001 θεωρείται ως το τελευταίο στάδιο της κλασσικής τρομοκρατίας, με το τρομοκρατικό χτύπημα των Δίδυμων Πύργων και με την Al-Qaeda να αναλαμβάνει την ευθύνη της επίθεσης. Επίσης το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden και κατ’ επέκταση στην κορυφή του καταλόγου των καταζητούμενων του FBI.

Το 1998 οι Tamil Guerrillas πλημμύρισαν τις βάσεις της SriLanka με ηλεκτρονικά μηνύματα στέλνοντας περίπου 800 την ημέρα για μια περίοδο δύο εβδομάδων. Στόχος τους ήταν να διακόψουν την ικανότητα επικοινωνίας και το περιστατικό αυτό είναι το πρώτο γνωστό περιστατικό τρομοκρατικής επίθεσης εναντίον των ηλεκτρονικών συστημάτων μιας χώρας.

2.1 Δράστες και μέθοδοι

2.1.1 Χαρακτηριστικά κυβερνοτρομοκρατίας

Η κυβερνοτρομοκρατία θεωρείται μία αόρατη απειλή, η οποία προκαλεί φόβο και ανασφάλεια, αφού δεν προσδιορίζεται από κάποιον συγκεκριμένο χώρο ή τόπο.

Τα χαρακτηριστικά τα οποία την καθιστούν άκρως επικίνδυνη, σύμφωνα με τον Καθηγητή του Πανεπιστημίου της Χάιφα, G. Weimann, είναι τα ακόλουθα:

- Είναι μία 'οικονομική λύση', εφόσον οι κυβερνοτρομοκράτες δε χρειάζεται να αγοράσουν όπλα ή εκρηκτικές ύλες. Το μόνο απαραίτητο είναι ένας υπολογιστής, μία σύνδεση στο διαδίκτυο και η δημιουργία ιών.
- ο κυβερνοχώρος προσφέρει ανωνυμία. Είναι αποκεντρωμένος, δεν μπορεί να υποβληθεί σε έλεγχο ή περιορισμούς, δεν μπορεί να λογοκριθεί και επιτρέπει ελεύθερη πρόσβαση σε όποιον το επιθυμεί. Οι τρομοκράτες έχουν πρόσβαση μέσω του διαδικτύου σε πληροφοριακά συστήματα προκειμένου να καλύψουν την ταυτότητά τους ή να "μεταμφιεστούν".
- Το δυνητικό κοινό, η γρήγορη ροή πληροφοριών, οι ουσιώδεις υποδομές μιας χώρας όπως η παροχή ηλεκτρικού ρεύματος κάνουν ευκολότερη την ύπαρξη της κυβερνοτρομοκρατίας, καθώς τα συστήματα των υπολογιστών είναι εξαιρετικά περίπλοκα.
- Οι επιθέσεις πραγματοποιούνται από απόσταση, χωρίς τη φυσική παρουσία των εμπλεκόμενων.
- Οι πιο σημαντικές υποδομές είναι συνδεδεμένες σε δίκτυα υπολογιστών (συστήματα ελέγχου εναέριας κυκλοφορίας και εθνικής άμυνας), με αποτέλεσμα μια κοινωνία να είναι περισσότερο εκτεθειμένη και ευάλωτη σε επιθέσεις τρομοκρατίας.

2.1.2 Κατηγορίες δραστών

Οι εγκληματίες του κυβερνοχώρου προέρχονται από διάφορες κοινωνικές κατηγορίες.

Οι πιο γνωστές κατηγορίες δραστών είναι οι ακόλουθες:

- Οργανωμένοι Χάκερ (Cyber Criminals/Hackers), ακόμα και σε επαγγελματικό επίπεδο
- Εκπαιδευμένα νεαρά παιδιά, καθοδηγούμενα από εχθρικές κυβερνήσεις να διαπράττουν ηλεκτρονικά εγκλήματα (Online Wizz kids)
- Τρομοκρατικές οργανώσεις

- Κατάσκοποι με στόχο τις υποκλοπές δεδομένων με ανταγωνιστικά κίνητρα και οικονομικά συμφέροντα.

2.1.3 Συχνές μέθοδοι κακόβουλων ενεργειών

Το διαδίκτυο αποτελεί ένα σύγχρονο εργαλείο που χρησιμοποιούν οι τρομοκράτες προς όφελός τους. Οι τρομοκρατικές οργανώσεις για να ολοκληρώσουν με επιτυχία έναν διαδικτυακό σχεδιασμό επιθέσεων θα πρέπει να έχουν μια προσεκτικά προετοιμασμένη στρατηγική επικοινωνίας με τα σωστά κανάλια και εργαλεία που να επιτρέπουν τη διεξαγωγή αυτής της επίθεσης. Μια επιτυχημένη στρατηγική επικοινωνίας περιλαμβάνει χαρισματικούς αρχηγούς και ενεργούς δέκτες. Στόχος των επιθέσεων διαδικτυακών και μη, είναι η στρατηγική προσέγγισης πιθανών θυμάτων που είναι πρόθυμα να στηρίξουν την οργάνωση, χρησιμοποιώντας διάφορες μεθόδους.

Οι πιο συχνές μέθοδοι που διευκολύνουν τις κακόβουλες ενέργειές τους είναι:

- Κακόβουλο λογισμικό που επιτρέπει στον χάκερ την πρόσβαση στον υπολογιστή εξ αποστάσεως ή τον αποκλεισμό του συστήματος μέχρι να δοθούν «λύτρα» [Malware/Ransomware/Remote Access Trojan (RAT)]
- Μόλυνση Εφαρμογών που βρίσκονται στον υπολογιστή – στόχο (Web Based/Web Application attacks)
- Δίκτυα μολυσμένων υπολογιστών, τα οποία χρησιμοποιούνται για δραστηριότητες κυβερνοεγκλήματος (Botnets)
- Επιθέσεις με στόχο το «ρίξιμο» ιστοσελίδων μέσω μεγάλου όγκου traffic) [Denial of Service (DoS) attacks]
- Αποστολή παραπλανητικών email τα οποία παραπέμπουν τον παραλήπτη σε ιστοσελίδες με κακόβουλο λογισμικό (Phishing Email)
- Αποστολή μεγάλων όγκων ανεπιθύμητων email (spam)
- Παραβιάσεις/υποκλοπές προσωπικών δεδομένων που βρίσκονται online (Data fraud – data breaches)
- Διαδικτυακή προπαγάνδα μέσω ψεύτικων ειδήσεων (Fake media news)
- Online πλαστοπροσωπία (Identity theft/loss)
- Διαρροή εμπιστευτικών δεδομένων (Information leakage)
- Κακόβουλες ή λανθασμένες ενέργειες που οφείλονται στον ανθρώπινο παράγοντα, ο οποίος μέχρι σήμερα αποτελεί τη μεγαλύτερη απειλή για την ασφάλεια ενός οργανισμού ή ενός συστήματος (Insider threats)

2.2 Μορφές κυβερνοεπιθέσεων

Τα όπλα δραστηριότητας των κυβερνοτρομοκρατών δεν είναι σχεδιασμένα να σκοτώνουν άτομα ή να προξενούν ζημιές σε υλικά αντικείμενα. Απεναντίας, υπάρχουν αποκλειστικά για να παραποιήσουν ή να καταστρέψουν ηλεκτρονικά αρχεία.

Οι κυβερνοτρομοκρατικές επιθέσεις μπορούν να εκδηλωθούν με διαφορετικούς τρόπους, οι οποίοι θα περιγραφούν παρακάτω.

Με Φυσική Επίθεση, η οποία ενέχει συμβατικά όπλα κατευθυνόμενα ενάντια σε εγκαταστάσεις υψηλής τεχνολογίας (εγκαταστάσεις πληροφορικών συστημάτων ή τηλεπικοινωνιών).

Οι φυσικές επιθέσεις που πραγματοποιούνται σε σημαντικές εγκαταστάσεις και υποδομές, δεν είναι κάτι το πρωτόγνωρο. Η πλειοψηφία των τρομοκρατικών χτυπημάτων λαμβάνει χώρα ενάντια σε εγκαταστάσεις που θεωρούνται σημαντικές για την ομαλή λειτουργία του κράτους.

Για παράδειγμα, οι επιθέσεις εναντίον του Παγκόσμιου Κέντρου Εμπορίου και του Υπουργείου Εθνικής Άμυνας των Η.Π.Α. την 11η Σεπτεμβρίου 2001, ήταν φυσικές επιθέσεις εναντίον εγκαταστάσεων και προκάλεσαν σοβαρά προβλήματα στην ομαλή λειτουργία του κρατικού μηχανισμού των Η.Π.Α. Επομένως, γίνεται κατανοητό πως οι φυσικές επιθέσεις, όχι μόνο δεν αποτελούν κάτι νέο, αλλά μέχρι και τη σημερινή εποχή αποτελούν τον βασικό τρόπο με τον οποίο οι τρομοκρατικές οργανώσεις δρουν.

Συνοψίζοντας, είναι ολοφάνερο ότι η χρήση της πληροφορικής τεχνολογίας έχει γίνει τόσο εκτενής και οι κοινωνίες είναι εξαρτώμενες από αυτήν, ώστε εγκαταστάσεις που την υποστηρίζουν θεωρούνται υψίστης σημασίας και χαρακτηρίζονται ως πιθανοί στόχοι τρομοκρατικών επιθέσεων. Επίσης, με αυτόν τον τρόπο εμπεδώνουμε πλέον την εξάρτησή μας από την πληροφορική τεχνολογία και τις εφαρμογές της. Για παράδειγμα, μία φυσική επίθεση που θα προβεί σε καταστροφή των σκληρών δίσκων ενός χρηματιστηρίου, θα μπορούσε να έχει σοβαρές συνέπειες στην ομαλή λειτουργία της οικονομίας ενός κράτους. Οι εγκαταστάσεις επομένως, που υποστηρίζουν ή λειτουργούν με πληροφορική τεχνολογία, αυξάνουν σε σημαντικότητα και πιθανολογείται ότι όσο πιο πολύ οι κοινωνίες εξαρτώνται από την τεχνολογία, τόσο πιο σημαντικές θα θεωρούνται οι εγκαταστάσεις τέτοιου τύπου.

Με Ηλεκτρομαγνητική Επίθεση, η οποία ενέχει τη χρήση της ηλεκτρομαγνητικής ενέργειας ως όπλο, με την μορφή ηλεκτρομαγνητικού παλμού με σκοπό την υπερφόρτωση των κυκλωμάτων των υπολογιστών και την ολική καταστροφή των αποθηκευμένων αρχείων για να προκληθούν σοβαρές βλάβες και δυσλειτουργίες στα ηλεκτρονικά συστήματα και στους ηλεκτρονικούς υπολογιστές αντίστοιχα.

Σε μια λιγότερο βίαιη μορφή, συνίσταται στην εισαγωγή μιας αλληλουχίας αλφαριθμητικών κωδικών στις ηλεκτρομαγνητικές επικοινωνίες.

Ο ηλεκτρομαγνητικός παλμός ή αλλιώς EMP, είναι ουσιαστικά ένα ισχυρότατο κύμα μέσω του οποίου μεταφέρεται ηλεκτρομαγνητική ενέργεια ικανή να καταστρέψει πληροφορικά συστήματα και συστήματα τηλεπικοινωνίας.

Αν για παράδειγμα, ένας ηλεκτρονικός υπολογιστής εκτεθεί σε ισχυρή ηλεκτρομαγνητική ακτινοβολία, τότε καταστρέφεται ολοσχερώς (όπως αν τοποθετήσουμε έναν ισχυρό μαγνήτη δίπλα από ένα σκληρό δίσκο, τότε αυτόματα ο σκληρός δίσκος καταστρέφεται).

Σύμφωνα με τις αμερικανικές αρχές, ο EMP χαρακτηρίζεται ως ένα ενεργό όπλο, το οποίο αποτελεί απειλή για την εθνική ασφάλεια και μπορεί να προκαλέσει σοβαρή ζημιά στους ηλεκτρονικούς υπολογιστές (συνήθως τους καταστρέφει ολοσχερώς).

Η εμβέλεια ενός EMP, ο οποίος παράγεται είτε από μπαταρίες είτε από μία χημική έκρηξη, είναι περιορισμένη μεν, αλλά υπέρ αρκετή για πρόκληση σοβαρών ζημιών στα ηλεκτρονικά οποιουδήποτε κρατικού κτιρίου.

Ένα όπλο EMP αποτελείται από μία πηγή ενέργειας (η οποία μπορεί να είναι είτε χημικές εκρηκτικές ύλες είτε ισχυρές μπαταρίες), μία γεννήτρια μετατροπής ροής (η οποία κατασκευάζεται ιδιαίτερα εύκολα και υπάρχουν αναλυτικές οδηγίες για την κατασκευή της στο διαδίκτυο) και τέλος, μία κεραία προκειμένου να κατευθυνθεί ο παλμός.

Επομένως, εφόσον δεν απαιτούνται εξειδικευμένες γνώσεις, ο καθένας μπορεί να κατασκευάσει ένα τέτοιο όπλο, γεγονός που το καθιστά άκρως ανησυχητικό για τις κρίσιμες υποδομές των κρατών, αφού μπορεί η χρήση του να προκαλέσει ολοκληρωτική παράλυση στα ηλεκτρονικά συστήματα.

Άλλη μορφή επίθεσης είναι η **Δικτυακή Επίθεση**, η οποία ενέχει γενικά τη χρήση του κακόβουλου λογισμικού (malware) σαν όπλο με σκοπό να μολύνει τους υπολογιστές

εκμεταλλευόμενο τα λογισμικά χάσματα (π.χ. μία μαζική επίθεση από χιλιάδες ιούς, είναι ικανή να προκαλέσει κατάρρευση σε ένα δικτυακό σύστημα). Μια άλλη μορφή επίθεσης αυτού του είδους είναι η χρήση κλεμμένων πληροφοριών με σκοπό την παραβίαση ενός συστήματος περιορισμένης πρόσβασης.

Οι δικτυακές επιθέσεις είναι οι επιθέσεις του μέλλοντος ενάντια στα πληροφορικά συστήματα. Αυξάνουν με σταθερό ρυθμό και σε συνάρτηση με την εξάρτηση των κοινωνιών από τα πληροφορικά συστήματα και τη δικτύωση αυτών, τόσο πιο πολλές και επικίνδυνες θα είναι οι δικτυακές επιθέσεις. Η δικτυακή επίθεση μπορεί να καταστρέψει την ακεραιότητα δεδομένων, συνήθως με χρησιμοποίηση κακόβουλων λογισμικών (ιών), οι οποίοι παραποιούν τα προγράμματα που ελέγχουν τα δεδομένα, οδηγώντας σε κρίσιμα λάθη. Οι hackers μέσω προγραμμάτων του διαδικτύου προβαίνουν σε τροποποίηση της ομαλής διάταξης των λογισμικών.

Από τη στιγμή που ένας ιός προσβάλλει έναν ηλεκτρονικό υπολογιστή, τότε ο υπολογιστής μπορεί να ελέγχεται από τον Hacker, ο οποίος έχει τη δυνατότητα μέσω του διαδικτύου να τον κατασκοπεύει ή ακόμα και να τον καταστρέψει.

Αξίζει να σημειωθεί πως η πλειοψηφία των σημαντικών υποδομών των δυτικών κρατών λειτουργούν με υπολογιστές, οι οποίοι επικοινωνούν μεταξύ τους δικτυακά. Στηριζόμενοι σε αυτό το γεγονός κατανοούμε πως τέτοιες δικτυακές επιθέσεις μπορεί να είναι πολύ επιζήμιες, προξενώντας τεράστια προβλήματα στον κρατικό μηχανισμό ή ακόμα και θέτοντας ολόκληρες χώρες σε καταστάσεις έκτακτης ανάγκης.

Στις Η.Π.Α., θεωρείται σίγουρο πως οι τρομοκρατικές επιθέσεις στο άμεσο μέλλον θα πραγματοποιούνται είτε αποκλειστικά με δικτυακές επιθέσεις είτε σε συνδυασμό με δικτυακές και φυσικές επιθέσεις.

Οι δικτυακές επιθέσεις, είναι ένα βασικό στοιχείο της κυβερνοτρομοκρατίας, και αναμένεται στο μέλλον ότι θα οικειοποιούνται από όλο και μεγαλύτερο αριθμό τρομοκρατικών οργανώσεων διεθνών ή μη, ενώ η προστασία των κρατικών υποδομών ενάντια σε αυτές, προβληματίζει ιδιαίτερα τις κυβερνήσεις, καθώς πιστεύεται σήμερα ότι υπάρχουν αρκετά τρωτά σημεία σε αυτές.

2.3 Κυβερνοτρομοκρατία ως ειδικότερη μορφή κυβερνοεπίθεσης

Είναι πολύ σημαντικό να κατανοήσουμε αν οι δύο έννοιες, ήτοι αυτή της κυβερνοτρομοκρατίας και εκείνη της κυβερνοεπίθεσης είναι ταυτόσημες.

Κατά πολλούς, η κυβερνοτρομοκρατία είναι ένα είδος κυβερνοεπίθεσης.

Τα κυριότερα χαρακτηριστικά που προσδίδουν σε μία κυβερνοεπίθεση την χροιά της τρομοκρατικής ενέργειας είναι το είδος των αποτελεσμάτων που η επίθεση επιφέρει, αλλά και η ίδια η πρόθεση των εγκληματιών.

Ειδικότερα, η κυβερνοτρομοκρατία, υπάρχει όταν επιθέσεις μέσω υπολογιστών καταλήγουν σε αποτελέσματα τα οποία προξενούν διαταραχές και είναι δυνατό να γεννήσουν φόβο ανάλογο με εκείνο που μπορεί να προκαλέσει μία παραδοσιακή τρομοκρατική επίθεση, ακόμη κι αν οι δράστες είναι κατά βάση, εγκληματίες, ενώ η πρόθεση των κυβερνοτρομοκρατών να προχωρήσουν σε επιθέσεις εναντίον ηλεκτρονικών δικτύων γίνονται με σκοπό να εξαναγκάσουν και να τρομοκρατήσουν τον κυβερνητικό μηχανισμό ενός κράτους, με πολιτικά κίνητρα για την πρόκληση ζημίας ή οικονομικής καταστροφής.

2.4 Οι κρίσιμες υποδομές ως στόχοι των κυβερνοτρομοκρατών

Οι προαναφερόμενοι τρόποι επιθέσεων έχουν ως κύριο στόχο τις κρίσιμες υποδομές ενός κράτους. Οι κακόβουλοι χρήστες του διαδικτύου, αποτελούν την μεγαλύτερη απειλή σε κρατικές υποδομές ζωτικής σημασίας για τη σταθερότητα και την ανάπτυξη ενός κράτους. Διαθέτουν επίσης καταρτισμένη γνώση σε συστήματα και αυξημένη πρόσβαση, η οποία μπορεί να είναι αρκετά επιζήμια. Η τραγωδία της 11ης Σεπτεμβρίου, έδειξε ότι οι τρομοκράτες είναι πιθανό να βρίσκονται στον εσωτερικό πυρήνα του αμερικανικού κράτους, αποκτώντας εξειδικευμένες γνώσεις με φονικές τάσεις.

Ως κρίσιμες υποδομές ορίζουμε τις φυσικές πηγές, τις υπηρεσίες, τις τεχνολογικές και επικοινωνιακές εγκαταστάσεις, τα δίκτυα και τις υποδομές, οι οποίες, αν διακοπούν ή καταστραφούν, θα έχουν ισχυρό αντίκτυπο στην υγεία, την ασφάλεια την οικονομία και την ευημερία ενός κράτους. Επομένως, οι κρίσιμες υποδομές είναι σημαντικές για την εύρυθμη και ομαλή λειτουργία του κρατικού μηχανισμού και θα πρέπει να θεωρείται ως πρώτη προτεραιότητα η διασφάλισή τους και η μη διακοπή της λειτουργίας τους.

Οι κρίσιμες υποδομές μας περιβάλλουν και είναι απαραίτητες για τη διασφάλιση των υπηρεσιών κοινής ωφέλειας και την ομαλή διαβίωση του ανθρώπου στον σύγχρονο «πραγματικό» κόσμο. Παρέχουν τις βασικές υπηρεσίες και τα συστήματα που είναι ζωτικής σημασίας για τη διασφάλιση της εύρυθμης λειτουργίας της οικονομίας μιας

χώρας, της κυβέρνησης και ολόκληρης της κοινωνίας. Στην Ελλάδα οι υποδομές ζωτικής σημασίας ορίζονται ως εκείνες οι υποδομές των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο στη χώρα, αλλά και σε άλλα κράτη μέλη της Ε.Ε.

2.5 Τρόπος χρήσης τεχνολογίας

Η εξέλιξη των αμυντικών συστημάτων με τη χρήση ηλεκτρονικών υπολογιστών, δορυφορικών συστημάτων κ.λ.π, πολλαπλασίασε εν τέλει την τρωτότητά τους. Ειδικότερα, πολλά από τα μηχανήματα και μέρος του εξοπλισμού που περιλαμβάνονται στις στρατιωτικές επιχειρήσεις επιβλέπονται εξ αποστάσεως. Συνεπώς, μία ενδεχόμενη κυβερνοεπίθεση θα μπορούσε να αλλάξει την έκβαση μίας επίθεσης σε πραγματικό χρόνο. Πέραν τούτου, η τεχνητή νοημοσύνη εξελίσσεται διαρκώς, με τα ρομποτικά συστήματα να χρησιμοποιούνται όλο και περισσότερο και στο πεδίο των μαχών. Την ίδια την εξέλιξη των εξοπλισμών, όσο και γενικότερα, της τεχνολογίας, εκμεταλλεύονται οι διάφορες εγκληματικές και τρομοκρατικές ομάδες που δραστηριοποιούνται στον κυβερνοχώρο, γεγονός που καθιστά αναγκαία την προσαρμογή των αρχών επιβολής του νόμου στη διαρκώς μεταβαλλόμενη πραγματικότητα.

Στο σημείο αυτό θα αναλυθεί ο τρόπος χρήσης της τεχνολογίας των υπολογιστών με σκοπό την επίτευξη κυβερνοτρομοκρατίας που κατηγοριοποιείται σε τρεις περιπτώσεις:

2.5.1 Όπλα μαζικής καταστροφής (Weapons of Mass Destruction)

Επισημαίνεται εξαρχής ότι η αυτή η χρήση της τεχνολογίας είναι θεωρητικής μορφής, αφού οι υπολογιστές δεν είναι δυνατόν να επιφέρουν φυσική βλάβη σε άτομα ή περιουσίες. Μπορούν όμως να κινητοποιήσουν δυνάμεις, ώστε να προκληθεί φυσική καταστροφή. Ένα αξιοσημείωτο παράδειγμα είναι η περίπτωση κατά την οποία οι κυβερνοτρομοκράτες έχουν την ικανότητα να απενεργοποιήσουν τα συστήματα προστασίας και ελέγχου του πυρηνικού αντιδραστήρα σε κάποιο εργοστάσιο που παράγει ηλεκτρική ενέργεια, όπως αυτό του Τσέρνομπιλ, το 1986.

Μετέπειτα, αναλαμβάνοντας την ευθύνη και εκμεταλλευόμενοι τους θανάτους και τις καταστροφικές συνέπειες της ραδιενεργούς μόλυνσης υπονομεύουν την ικανότητα της εκάστοτε κυβέρνησης, παρουσιάζοντάς την ως ανίκανη να διατηρήσει την εσωτερική τάξη.

Παρόλα αυτά όμως, και ενώ το σενάριο της κυβερνοτρομοκρατίας στην συγκεκριμένη περίπτωση φαίνεται λογικό, εφόσον χρησιμοποιήθηκαν υπολογιστές για να δρομολογηθεί η καταστροφή, οι πολίτες κατονομάζουν το περιστατικό αυτό ως πυρηνική καταστροφή και όχι κυβερνοκαταστροφή.

Επομένως, συμπεραίνεται ότι η χρήση της τεχνολογίας ήταν συμπτωματική σε ό, τι αφορά την τρομοκρατική πράξη, χωρίς η ίδια να θεωρείται τέτοιου είδους πράξη.

2.5.2 Όπλα μαζικού περισπασμού (Weapons of Mass Distraction)

Αυτή η χρήση της τεχνολογίας είναι εξίσου θεωρητική όσο και πραγματική. Στην συγκεκριμένη περίπτωση η χρήση της τεχνολογίας αποσκοπεί ξεκάθαρα στον χειρισμό της ψυχολογίας των ανθρώπων. Και εδώ σκοπός είναι η υπονόμευση της ικανότητας της κυβέρνησης στη διατήρηση της έννομης τάξης. Επίσης, ανάλογα με την κάθε εγκληματική πράξη που διαπράττεται το αποτέλεσμα που μπορεί να προκληθεί είναι θάνατος ή τραυματισμός ανθρώπων ή καταστροφή περιουσίας.

2.5.3 Όπλα Μαζικής Κοινωνικής Αναστάτωσης (Weapon of Mass Disruption)

Τα όπλα κοινωνικής αναστάτωσης έχουν ως στόχο να προκαλέσουν την έλλειψη εμπιστοσύνης του πληθυσμού απέναντι στην αξιοπιστία των απαραίτητων υποδομών, όπως είναι τα μέσα μετακίνησης, τα δίκτυα και οι υπηρεσίες τροφοδοσίας, οι επικοινωνίες, τα χρηματοπιστωτικά ιδρύματα και οι υπηρεσίες παροχής υγείας. Στόχος τους σε αυτήν την περίπτωση είναι να επιτύχουν ζημιά σε ένα οι περισσότερα συστήματα και να υπονομεύσουν την εμπιστοσύνη των πολιτών σε ότι αφορά τις κοινωνικές υπηρεσίες και δομές. Συχνά ο τύπος κάνει αναφορές για τρομοκράτες που κλείνουν τα δίκτυα ηλεκτρικής ενέργειας ή πετρελαίου ή παροχής φυσικού αερίου.

Η χρήση αυτής της τεχνολογίας είναι και εδώ τόσο ρεαλιστική όσο και θεωρητική. Σκοπός της είναι να εξαχρειώσει τους πολίτες ενάντια στην κυβέρνηση για να την αποδομήσουν, αφού είναι ανίκανη να παρέχει την εγγύηση ασφάλειας για τις υπηρεσίες που είναι απόλυτα απαραίτητες στους πολίτες της.

2.6 Επίπεδα Κυβερνοτρομοκρατίας

Τον Αύγουστο του 1999, το Κέντρο Μελέτης της Τρομοκρατίας και του Παράτυπου Πολέμου στη Ναυτική Μεταπτυχιακή Σχολή στο Μοντερέι της Καλιφόρνια, εξέδωσε μια έκθεση με τίτλο "Cyberterror: Προοπτικές και Επιπτώσεις". Στόχος τους

ήταν να εκφράσουν την πλευρά της ζήτησης της τρομοκρατίας. Συγκεκριμένα, αξιολόγησαν τις προοπτικές τρομοκρατικών οργανώσεων που επιδιώκουν την κυβερνοτρομοκρατία. Κατέληξαν στο συμπέρασμα ότι το εμπόδιο εισόδου για οτιδήποτε πέρα από ενοχλητικές παραβιάσεις είναι αρκετά υψηλό και ότι οι τρομοκράτες γενικά δε διαθέτουν τα μέσα και το ανθρώπινο κεφάλαιο που απαιτούνται για να οργανώσουν μια ουσιαστική επιχείρηση. Η κυβερνοτρομοκρατία, υποστήριξαν, ήταν ένα πράγμα του μέλλοντος, αν και θα μπορούσε να επιδιωχθεί ως βοηθητικό εργαλείο.

Η ομάδα του Monterey καθόρισε τρία επίπεδα ικανότητας της κυβερνοτρομοκρατίας:

- **Την απλή-μη δομημένη:** Ως απλή νοείται η δυνατότητα διεξαγωγής βασικών hacks κατά μεμονωμένων συστημάτων χρησιμοποιώντας εργαλεία που δημιουργήθηκαν από κάποιον άλλο. Ο οργανισμός διαθέτει μικρή ανάλυση στόχων, διοίκηση και έλεγχο ή ικανότητα μάθησης.
- **Την προηγμένη δομή:** Πρόκειται για την δυνατότητα διεξαγωγής πιο εξελιγμένων επιθέσεων εναντίον πολλαπλών συστημάτων ή δικτύων και ενδεχομένως, τροποποίησης ή δημιουργίας βασικών εργαλείων hacking. Ο οργανισμός διαθέτει στοιχειώδη ανάλυση στόχων, διοίκηση και έλεγχο και ικανότητα μάθησης.
- **Πολύπλοκη-συντονισμένη:** Είναι η ικανότητα για μια συντονισμένη επίθεση ικανή να προκαλέσει τη μαζική διακοπή ενάντια στις ενσωματωμένες, ετερογενείς άμυνες (συμπεριλαμβανομένης της κρυπτογραφίας). Δυνατότητα δημιουργίας εξελιγμένων εργαλείων hacking. Εξαιρετικά ικανή ανάλυση στόχων, ικανότητα διοίκησης και ελέγχου και ικανότητα εκμάθησης οργανισμού.

Οι υπολογισμοί που έκαναν έδειξαν πως μία ομάδα ξεκινώντας από το μηδέν χρειάζεται περίπου 2-4 χρόνια για να οδηγηθεί στο προηγμένο δομημένο επίπεδο και αντίστοιχα 6-10 χρόνια για να φτάσει στο πολύπλοκο συντονισμένο επίπεδο. Παρατήρησαν και κάποιες εξαιρέσεις όπου κάποιες ομάδες μπορεί να φτάσουν σε αυτό το τελευταίο επίπεδο μέσα σε λίγα μόλις χρόνια ή να αναζητήσουν χορηγία για να επεκτείνουν την ικανότητα τους.

Η συγκεκριμένη μελέτη εξέτασε πέντε τύπους τρομοκρατικών ομάδων:

- θρησκευτικούς,
- νέα εποχή,
- εθνο-εθνικιστές αυτονομιστές,

- επαναστάτες και
- ακροδεξιούς εξτρεμιστές.

Διαπιστώθηκε πως μόνο η πρώτη ομάδα είναι σε θέση να επιδιώξει το επιζήμιο επίπεδο ικανοτήτων, εφόσον συμφωνεί με την αδιάκριτη εφαρμογή βίας. Την πιο άμεση απειλή ωστόσο, αποτελούν οι τρομοκράτες νέας εποχής, αφού δέχονται την απειλή ως υποκατάστατο της καταστροφής. Αντίθετα οι επαναστατικοί και οι εθνο-εθνικιστές αυτονομιστές έχουν ως σκοπό την αναζήτηση μιας προηγμένης δομημένης ικανότητας. Τέλος, οι ακροδεξιοί εξτρεμιστές συμβιβάζονται με μια απλή-δομημένη ικανότητα. Θεωρούν πως ο κυβερνοτρομοϊος δεν τους παρέχει τα βασικά στοιχεία που απαρτίζουν την ψυχολογία τους, όπως οικειότητα και καθαρτικά αποτελέσματα.

Επιπρόσθετα, μέσα από την συγκεκριμένη μελέτη έγινε φανερό πως οι ομάδες χάκερ είναι ψυχολογικά και οργανωτικά ακατάλληλες για κυβερνοτρομοκρατία και πως θα ήταν ενάντια στα συμφέροντά τους να προκαλέσουν μαζική διακοπή της υποδομής πληροφοριών.

2.7 Περιπτώσεις – Υποθέσεις Κυβερνοτρομοκρατίας

Οι σημαντικότερες και πιο γνωστές περιπτώσεις – υποθέσεις κυβερνοτρομοκρατίας σε παγκόσμιο επίπεδο είναι οι ακόλουθες:

2.7.1 Υπόθεση Ferizi

Η υπόθεση Ferizi είναι η πρώτη υπόθεση στην οποία η κυβέρνηση των ΗΠΑ κατηγόρησε ένα άτομο για κυβερνοτρομοκρατία. Ο Ferizi με καταγωγή από τη Γκιάκοβα του Κοσσυφοπεδίου, συνελήφθη τον Σεπτέμβριο του 2015 στην Μαλαισία με την κατηγορία ότι υπέκλεψε δεδομένα και πληροφορίες που ανήκαν σε στρατιωτικούς και τα μετέφερε σε μέλη του ISIS ώστε να ενισχύσει τις επιθέσεις τους κατά της Δύσης.

Πιο συγκεκριμένα, υπέκλεψε ονόματα και διευθύνσεις ηλεκτρονικού ταχυδρομείου, κωδικούς πρόσβασης, τοποθεσίες και αριθμούς τηλεφώνου 1.351 στρατιωτικών και άλλων κυβερνητικών εκπροσώπων, για να βοηθήσει μέλη του ISIS να χτυπήσουν αμερικανούς στρατιώτες. Τα δεδομένα τα παρείχε στον δημοφιλή μαχητή Junaid Hussain, ο οποίος τα αποκάλυψε στο διαδίκτυο, δημοσιεύοντας τα στο Twitter. Ο Ferizi δεν ήταν μόνος. Λειτουργούσε ως μέλος του πληρώματος πειρατείας γνωστό ως Ασφάλεια Χάκερ του Κοσσυφοπεδίου (KHS). Η ομάδα της KHS διεξήγαγε πολυάριθμες κυβερνοεπιθέσεις εναντίον οργανισμών σε όλο τον κόσμο. Η οργάνωση πραγματοποίησε

έφοδο σε περισσότερους από 20.000 ιστότοπους και υπολογιστές σε Σερβία, Ελλάδα, Ουκρανία και άλλες χώρες.

2.7.2 Η περίπτωση της Εσθονίας

Τον Μάιο του 2007, η Εσθονία δέχθηκε μία μαζική ηλεκτρονική επίθεση που έπληξε κυβερνητικές υπηρεσίες, κομματικές οργανώσεις, τα ΜΜΕ και το τραπεζικό σύστημα της χώρας. Η περίπτωση αυτή αποτελεί την πρώτη κυβερνοεπίθεση εναντίον ενός κράτους, που συνεχίστηκε, μάλιστα, επί τρεις εβδομάδες. Βασική αιτία θεωρήθηκε η απομάκρυνση του "Χάλκινου Στρατιώτη", μνημείου υπέρ των πεσόντων σοβιετικών του Β' Παγκοσμίου πολέμου, από το κέντρο της εσθονικής πρωτεύουσας. Κατ' επέκταση, ευθύνες για την επίθεση αποδόθηκαν στο ρωσικό κράτος αλλά σχετική ανάμειξη δεν αποδείχτηκε ποτέ.

Εν τέλει, τον Ιανουάριο του 2008, ένας νεαρός φοιτητής ρωσικής καταγωγής καταδικάστηκε με χρηματική ποινή 1100 Ευρώ από εσθονικό δικαστήριο ως υπεύθυνος της υπόθεσης. Στο μεταξύ, όμως, η έντονη αντίδραση της εσθονικής κυβέρνησης που κάλεσε τόσο την Ευρωπαϊκή Ένωση όσο και το ΝΑΤΟ να προχωρήσουν άμεσα σε λήψη μέτρων κατά του υπαρκτού κινδύνου της κυβερνοτρομοκρατίας, κινητοποίησε τα διεθνή αντανακλαστικά. Μέχρι σήμερα,η περίπτωση της Εσθονίας είναι η μόνη που άγγιξε τα όρια της κυβερνοτρομοκρατίας.

2.8 Νομικό Πλαίσιο και Πολιτικές Προστασίας

Οι τρομοκρατικές πράξεις αποτελούν μία από τις σοβαρότερες παραβιάσεις των παγκόσμιων αξιών της ανθρώπινης αξιοπρέπειας, της ελευθερίας, της ισότητας και της αλληλεγγύης, και του σεβασμού των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, στις οποίες έχει θεμελιωθεί η Ένωση. Πρόκειται, εξάλλου, για μία από τις σοβαρότερες προσβολές της δημοκρατίας και του κράτους δικαίου, που είναι κοινές στα κράτη μέλη και στις οποίες βασίζεται η Ένωση.

Στην προσπάθεια να οργανωθούν συστήματα ασφαλείας ενάντια σε επιθέσεις μέσω του Κυβερνοχώρου, τίθεται ως βασική προτεραιότητα η ύπαρξη δύο σταδίων δράσεως, της προορατικής και της αντιδραστικής. Η πρώτη δράση επιτυγχάνεται κυρίως με την εγκατάσταση εμποδίων ενάντια σε προσπάθειες τρομοκρατών για εκπλήρωση επιθέσεων ενάντια σε συστήματα υποδομών της πληροφόρησης. Η εφαρμογή ενός μοντέλου πολύπλευρης προστασίας, το οποίο περιλαμβάνει την φυσική προστασία (=άρνηση της

φυσικής πρόσβασης), την τεχνική προστασία (π.χ. συστήματα εντοπισμού για πρόληψη επιθέσεων), τους ανθρώπινους πόρους (ορθός καταμερισμός εργασίας, ορθή επιλογή εκπαιδευμένου προσωπικού), την οργανωτική σφαίρα (αξιοποίηση ικανοτήτων και πόρων, κατανομή δραστηριοτήτων) και την νομική σφαίρα (Νόμοι, Οδηγίες, Κανονισμοί) θα διευκόλυνε την αποτελεσματικότερη αντιμετώπιση του φαινομένου.

Η δεύτερη δράση επιτυγχάνεται με την εφαρμογή μέτρων που θα επιτρέψουν στα συστήματα επικοινωνιών και πληροφόρησης να επαναφέρουν τις βασικές λειτουργίες τους μετά από μία επίθεση (εντοπισμός της καταστροφής, εκτίμηση του μεγέθους της ζημίας, εύρεση των αιτιών, διόρθωση σφαλμάτων, ανανέωση της πολιτικής προστασίας). Επιπλέον, η υιοθέτηση εθνικών πολιτικών προστασίας για την ασφάλεια του κυβερνοχώρου θα εξαλείψει ή θα μειώσει σημαντικά την ευπάθεια σε επιθέσεις μέσω του κυβερνοχώρου και θα ελαχιστοποιήσει την ζημιά δίνοντας χρόνο για γρήγορη επαναφορά με την παροχή κατευθυντήριων γραμμών για την ασφάλεια του κυβερνοχώρου.

Ένα μέτρο που λαμβάνεται σε διεθνές επίπεδο για την καταπολέμηση της κυβερνητικής τρομοκρατίας είναι η μορφοποίηση κοινών ομάδων εργασίας. Οι κοινές ομάδες εργασίας είναι πλέον σε θέση να αυξήσουν την ανταλλαγή πληροφοριών μεταξύ χωρών, να ενισχύσουν την συνεργασία στις έρευνες, να διευκολύνουν την υπογραφή συνθηκών αμοιβαίας νομικής αρωγής και έχουν κατορθώσει να υπογράψουν αρκετές άλλες σημαντικές συνθήκες κατά της τρομοκρατίας.

2.8.1 Συλλογική Προσέγγιση για την αντιμετώπιση του φαινομένου

Ο διασυνοριακός χαρακτήρας της τρομοκρατίας απαιτεί ισχυρή και συντονισμένη αντίδραση και συνεργασία εντός και μεταξύ των κρατών μελών, καθώς και μεταξύ των αρμόδιων υπηρεσιών και οργανισμών της Ένωσης για την καταπολέμηση της τρομοκρατίας, συμπεριλαμβανομένων της Eurojust και της Ευρωπόλ. Για τον σκοπό αυτό, επιβάλλεται η αποτελεσματική χρήση των διαθέσιμων μέσων και πόρων για τη συνεργασία, για παράδειγμα των κοινών ομάδων έρευνας και των συνεδριάσεων συντονισμού που υποστηρίζονται από την Eurojust. Η δημιουργία μίας ενιαίας πολιτικής προστασίας ενάντια σε επιθέσεις που μπορεί να πλήξουν κρατικές υποδομές και κεφάλαια, εκτιμώντας παράλληλα τις κυβερνοαπειλές, αλλά και ο συλλογικός συντονισμός με κοινές υπερεθνικές πλατφόρμες εργασίας, είναι πρωτίστης σημασίας για την αντιμετώπιση των κυβερνοεπιθέσεων. Η παγκόσμια διάσταση της τρομοκρατίας απαιτεί διεθνή απάντηση, στο πλαίσιο της οποίας θα κληθούν η Ένωση και τα κράτη μέλη

της να ενισχύσουν τη συνεργασία με τις ενδιαφερόμενες τρίτες χώρες. Η ισχυρή και συντονισμένη αντίδραση και συνεργασία είναι επίσης απαραίτητες προκειμένου να επιτευχθούν η διασφάλιση και απόκτηση ηλεκτρονικών αποδείξεων.

Τα εγκλήματα που σχετίζονται με τρομοκρατικές δραστηριότητες είναι πολύ σοβαρά, καθώς είναι δυνατόν να οδηγήσουν στην τέλεση τρομοκρατικών εγκλημάτων και να παράσχουν σε τρομοκράτες και τρομοκρατικές ομάδες τη δυνατότητα να διατηρήσουν και να αναπτύξουν περαιτέρω τις εγκληματικές τους δραστηριότητες, πράγμα που δικαιολογεί την ποινικοποίηση τέτοιων συμπεριφορών.

Για να διασφαλιστεί η επιτυχία των ερευνών και η δίωξη των τρομοκρατικών εγκλημάτων, των εγκλημάτων που σχετίζονται με τρομοκρατική ομάδα ή των εγκλημάτων που σχετίζονται με τρομοκρατικές δραστηριότητες, οι αρμόδιοι για τη διερεύνηση ή τη δίωξη τέτοιων εγκλημάτων θα πρέπει να μπορούν να χρησιμοποιούν αποτελεσματικά ερευνητικά μέσα, όπως αυτά που χρησιμοποιούνται για την καταπολέμηση του οργανωμένου εγκλήματος ή άλλων σοβαρών εγκλημάτων. Η χρήση των μέσων αυτών, σύμφωνα με το εθνικό δίκαιο, θα πρέπει να επικεντρώνεται και να λαμβάνει υπόψη την αρχή της αναλογικότητας, καθώς και τη φύση και τη σοβαρότητα των υπό διερεύνηση αδικημάτων και θα πρέπει να σέβεται το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Σε αυτά τα μέσα θα μπορούσαν, κατά περίπτωση, να περιλαμβάνονται, μεταξύ άλλων, η έρευνα οποιασδήποτε προσωπικής περιουσίας, η παρακολούθηση των επικοινωνιών, η διακριτική παρακολούθηση, συμπεριλαμβανομένης της ηλεκτρονικής παρακολούθησης, η λήψη, ανάκτηση και καταγραφή ήχου και φωνής σε ιδιωτικά ή δημόσια οχήματα και χώρους και οπτικής εικόνας προσώπων σε δημόσια οχήματα και χώρους και έρευνες οικονομικού χαρακτήρα.

Περαιτέρω, είναι απαραίτητο να επενδυθεί μεγαλύτερη ποσότητα οικονομικών πόρων για την ανάπτυξη λογισμικού προστασίας, λειτουργικών συστημάτων και απόκρυψη αλγορίθμων σε διεθνές επίπεδο. Σε εθνικό επίπεδο ακόμη, είναι σημαντικό, οι δημόσιοι λειτουργοί να λαμβάνουν επαρκή μέτρα προστασίας απορρήτων πληροφοριών, καθώς και να φροντίζουν για τη δημιουργία εφεδρικών εγγράφων στα οποία καταγράφονται σημαντικές πληροφορίες, καθώς και την εφαρμογή λύσεων για προβλήματα προστασίας με την ομαδοποίηση αντιγράφων ασφαλείας για λογισμικό και μη.

Ένα αποτελεσματικό μέσο για την καταπολέμηση της τρομοκρατίας στο διαδίκτυο είναι η αφαίρεση διαδικτυακού περιεχομένου που αποτελεί δημόσια υποκίνηση σε τέλεση τρομοκρατικού εγκλήματος στην πηγή του. Τα κράτη μέλη οφείλουν να επιδιώκουν με κάθε τρόπο τη συνεργασία με τρίτες χώρες προκειμένου να διασφαλίζεται η αφαίρεση αυτού του διαδικτυακού περιεχομένου που αποτελεί δημόσια υποκίνηση σε τέλεση τρομοκρατικού εγκλήματος από τους διακομιστές στην επικράτειά τους. Ωστόσο, στις περιπτώσεις όπου η αφαίρεση περιεχομένου στην πηγή δεν είναι εφικτή, θα πρέπει να δημιουργηθούν επίσης μηχανισμοί για τη φραγή της πρόσβασης από το έδαφος της Ένωσης σε αυτό το περιεχόμενο.

Συνοψίζοντας, ένα κατάλληλο σύστημα προστασίας ενάντια σε κυβερνοεπιθέσεις, σε εθνικό επίπεδο, θα βοηθήσει τις ανακριτικές και άλλες Αρχές επιβολής του δικαίου να βρουν την οποιαδήποτε σύνδεση μεταξύ συγκεκριμένων ατόμων και συμβάντων, με τον συνδυασμό πολιτικών προστασίας με διαθέσιμες πληροφορίες, στο σωστό χρόνο.

Για την αποτελεσματικότητα της στρατηγικής αυτής, είναι αναγκαία η ενεργός συμμετοχή όλων των χρηστών του διαδικτύου, ακόμη και μέσω των κυβερνητικών υπηρεσιών. Εξαιτίας της πολύπλοκης φύσης και δραστηριότητας αυτών των επιθέσεων, απαιτείται μια συνδυασμένη προσπάθεια των διεθνών, ομοσπονδιακών και τοπικών δυνάμεων απονομής δικαιοσύνης, για να συγκροτηθεί ένας αποτελεσματικός παράγοντας ασφάλειας ενάντια στην κυβερνοτρομοκρατία.

2.8.2 Αντιμετώπιση σε Ευρωπαϊκό Επίπεδο

Οι προσπάθειες καταπολέμησης της διεθνούς τρομοκρατικής δραστηριότητας από την Ευρωπαϊκή Ένωση, ξεκίνησαν κατά τα τέλη του έτους 2003 και στις αρχές του 2004. Η αφορμή για την κίνηση αυτή ήταν η τρομοκρατική επίθεση στην Μαδρίτη, το Μάρτιο του 2004, η οποία έθεσε τις βάσεις για ευρύτερη εφαρμογή της πολιτικής ασφαλείας στην Ευρωπαϊκή Ένωση κατά τη διάρκεια του πολέμου ενάντια στην τρομοκρατία[1].

Το όραμα της ΕΕ για την αντιμετώπιση της τρομοκρατίας είναι να δημιουργήσει μία τάξη ασφάλειας, ώστε να διασφαλίσει την ομαλή βιωσιμότητα μέσα σε ένα κλίμα ειρήνης και ευνομίας. Για την πραγματοποίηση αυτού του οράματος επιβάλλεται το επίπεδο ασφάλειας μέσα στην ευρωπαϊκή κοινότητα να λειτουργεί, συγχρόνως με την προώθηση σταθερότητας και ευημερίας με άλλες χώρες.

1 Muslims in Europe: Promoting Integration and Countering Extremism. Congressional Research Service

Υπό το πρίσμα αυτό, αλλά και βάσει των συμπερασμάτων του Ευρωπαϊκού Συμβουλίου του Τάμπερε του 1999, στα οποία η τρομοκρατία χαρακτηρίζεται μία από τις σοβαρότερες παραβιάσεις των θεμελιωδών ελευθεριών και των δικαιωμάτων του ανθρώπου και μετά την έγκριση του σχετικού προγράμματος δράσης του έκτακτου Ευρωπαϊκού Συμβουλίου της 21ης Σεπτεμβρίου 2001, εγκρίθηκε η απόφαση-πλαίσιο 2002/475/ΔΕΥ για την πιο αποτελεσματική καταπολέμηση της τρομοκρατίας.

Η απόφαση-πλαίσιο 2002/475/ΔΕΥ του Συμβουλίου είναι ο ακρογωνιαίος λίθος της απάντησης της ποινικής δικαιοσύνης των κρατών μελών ενάντια στην τρομοκρατία.

Η ως άνω απόφαση-πλαίσιο (2002/475/ΔΕΥ) και η τροποποιητική απόφαση (2008/919/ΔΕΥ)[2] υποχρεώνουν τις χώρες της ΕΕ να εναρμονίσουν τη νομοθεσία τους και να θεσπίσουν ελάχιστες κυρώσεις σχετικά με τα εγκλήματα τρομοκρατίας. Οι δύο αυτές αποφάσεις ορίζουν τα εγκλήματα τρομοκρατίας, καθώς και τα εγκλήματα σχετικά με τρομοκρατικές ομάδες ή τα εγκλήματα που συνδέονται με τρομοκρατικές δραστηριότητες, και θεσπίζουν τους κανόνες για τη μεταφορά τους στο δίκαιο των χωρών της ΕΕ.

Στην έκθεση που εξέδωσε τον Σεπτέμβριο του 2014 σχετικά με την εφαρμογή της απόφασης-πλαίσιο του 2008[3], η Ευρωπαϊκή Επιτροπή επισημαίνει ότι οι περισσότερες χώρες της ΕΕ (εκτός από την Ιρλανδία και την Ελλάδα) έχουν θεσπίσει μέτρα για την ποινικοποίηση των νέων εγκλημάτων της δημόσιας πρόκλησης, της στρατολόγησης και της εκπαίδευσης τρομοκρατών, ενώ επισημαίνεται και η ανάγκη μιας πιο ολοκληρωμένης προσέγγισης ως προς την επιβολή του νόμου με στόχο την εστίαση στην έγκαιρη πρόληψη της ριζοσπαστικοποίησης και της στρατολόγησης τρομοκρατών.

Στις 28 Νοεμβρίου 2008 υιοθετήθηκε μία νέα απόφαση – πλαίσιο, η 2008/919 ΔΕΥ, για την καταπολέμηση της τρομοκρατίας, με την οποία αντιμετωπίζεται το φαινόμενο της «βίαιης ριζοσπαστικοποίησης», τροποποιώντας προς το σκοπό αυτό την απόφαση πλαίσιο 2002/475 ΔΕΥ. Η έννοια της «βίαιης ριζοσπαστικοποίησης» - όρος που αργότερα εγκαταλείφθηκε - προσδιορίζεται σε Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, το 2005, ως «το φαινόμενο όπου άτομα

2 βλ. Έγγραφο εργασίας των υπηρεσιών της Επιτροπής που συνοδεύει το έγγραφο «Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την εφαρμογή της απόφασης-πλαίσιο 2008/919/ΔΕΥ του Συμβουλίου, της 28ης Νοεμβρίου 2008, σχετικά με την τροποποίηση της απόφασης-πλαίσιο 2002/475/ΔΕΥ για την καταπολέμηση της τρομοκρατίας» [SWD(2014) 270 final της 5 Σεπτεμβρίου 2014].

3 [COM(2007) 681 τελικό της 6.11.2007], [COM(2004) 409 τελικό της 8.6.2004], [COM(2014) 554 final της 5 Σεπτεμβρίου 2014]

ασπάζονται ορισμένες απόψεις, γνώμες και ιδέες που μπορεί να οδηγήσουν σε τρομοκρατικές ενέργειες[4]».

Στην Αιτιολογική Έκθεση της Πρότασης απόφασης – πλαισίου σημειώνεται ότι «το διαδίκτυο αποτελεί μία από τις από τις βασικές δυνάμεις πυροδότησης διαδικασιών ριζοσπαστικοποίησης και στρατολόγησης, καθώς επίσης χρησιμεύει ως πηγή πληροφοριών σχετικά με τα τρομοκρατικά μέσα και μεθόδους, λειτουργώντας κατ' αυτό τον τρόπο ως ένα «εικονικό στρατόπεδο εκπαίδευσης». Η διάδοση της προπαγάνδας και της τεχνογνωσίας των τρομοκρατών μέσω του διαδικτύου συμπληρώνει και ενισχύει την παραδοσιακή ιδεολογική χειραγώγηση και εκπαίδευση και συμβάλλει στην ανάπτυξη ενός ισχυροτέρου και ευρύτερου δικτύου ενεργών τρομοκρατών και υποστηριχτών. Η πρόληψη μιας τέτοιας αυξανόμενης απειλής αποτελεί πολιτική προτεραιότητα».

Στο δε Προοίμιο της απόφασης – πλαισίου ορίζεται ότι στόχος της είναι «η πρόληψη της τρομοκρατίας μέσω της μείωσης της διάδοσης εγγράφων ή μηνυμάτων που δύνανται να υποκινήσουν ή να βοηθήσουν άτομα σε τέλεση τρομοκρατικών επιθέσεων. Δίνεται εξάλλου ιδιαίτερη έμφαση στην αντιμετώπιση αυτών των συμπεριφορών μέσω διαδικτύου, αφού αυτό χρησιμοποιείται ως για να εμπνεύσει και να κινητοποιήσει τοπικά τρομοκρατικά δίκτυα και άλλα άτομα. Η απόφαση – πλαίσιο αποτυπώνει το αίτημα της ΕΕ απέναντι στα κράτη – μέλη να καταστήσουν αξιόποινες, ως εγκλήματα που συνδέονται με τρομοκρατικές δραστηριότητες τη δημόσια πρόκληση για τέλεση τρομοκρατικού εγκλήματος, τη στρατολόγηση και την εκπαίδευση τρομοκρατών.

Στις 31 Μαρτίου 2017, δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης η Οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της Απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της Απόφασης 2005/671/ΔΕΥ του Συμβουλίου.

Με την εν λόγω Οδηγία θεσπίζονται ελάχιστοι κανόνες αναφορικά με τον ορισμό των ποινικών αδικημάτων και των ποινών στον τομέα των τρομοκρατικών εγκλημάτων, τα εγκλήματα που απορρέουν από δραστηριότητες τρομοκρατικών ομάδων, και τα μέτρα προστασίας, στήριξης και αρωγής των θυμάτων της τρομοκρατίας.

4 Ε. Συμεωνίδου – Καστανίδου, Η «βίαιη ριζοσπαστικοποίηση» στο στόχαστρο της Ευρωπαϊκής Ένωσης», ΠοινΧρον 2009, σελ. 583

Η Οδηγία απαριθμεί κατά τρόπο εξαντλητικό μια σειρά σοβαρών εγκλημάτων, όπως η προσβολή της ζωής ενός προσώπου, ως εκ προθέσεως πράξεις που μπορούν να χαρακτηριστούν ως τρομοκρατικά εγκλήματα όταν και στον βαθμό που τελούνται με συγκεκριμένο τρομοκρατικό σκοπό, ήτοι για να εκφοβίσουν σοβαρά έναν πληθυσμό, να εξαναγκάσουν αθέμιτα κυβέρνηση ή διεθνή οργανισμό να εκτελέσουν οποιαδήποτε πράξη ή να απόσχουν από την εκτέλεσή της, ή να αποσταθεροποιήσουν σοβαρά ή να καταστρέψουν τις θεμελιώδεις πολιτικές, συνταγματικές, οικονομικές ή κοινωνικές δομές μιας χώρας ή ενός διεθνούς οργανισμού. Η απειλή τέλεσης αυτών των εκ προθέσεως πράξεων θα πρέπει επίσης να θεωρείται ότι είναι τρομοκρατικό έγκλημα, όταν αποδεικνύεται, βάσει αντικειμενικών στοιχείων, ότι η απειλή αυτή πραγματοποιήθηκε με οποιονδήποτε από αυτούς τους τρομοκρατικούς σκοπούς. Αντιθέτως, πράξεις που αποσκοπούν, για παράδειγμα, να εξαναγκάσουν μια κυβέρνηση να προβεί ή να απέχει από οποιαδήποτε πράξη, χωρίς, ωστόσο, να περιλαμβάνονται στον εξαντλητικό κατάλογο σοβαρών εγκλημάτων, δεν θεωρούνται ως τρομοκρατικά εγκλήματα σύμφωνα με την ως άνω Οδηγία.

Τα μέτρα που λαμβάνουν τα κράτη μέλη σύμφωνα με την παρούσα οδηγία για την αφαίρεση διαδικτυακού περιεχομένου που αποτελεί δημόσια υποκίνηση σε τέλεση τρομοκρατικού εγκλήματος ή, όταν αυτή δεν είναι εφικτή, το κλείδωμα της πρόσβασης στο εν λόγω περιεχόμενο θα μπορούσαν να βασίζονται σε δημόσιες δράσεις, για παράδειγμα νομοθετικές, μη νομοθετικές ή δικαστικές δράσεις. Σε αυτό το πλαίσιο, η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη της εθελοντικής δράσης που αναλαμβάνει ο κλάδος του διαδικτύου για την πρόληψη της αθέμιτης χρήσης των υπηρεσιών του ή οποιασδήποτε στήριξης της δράσης αυτής από κράτη μέλη, όπως είναι ο εντοπισμός και η επισήμανση τρομοκρατικού περιεχομένου. Ανεξάρτητα από τη βάση ή μέθοδο δράσης που θα επιλεγεί, τα κράτη μέλη θα πρέπει να μεριμνούν ώστε να παρέχεται επαρκές επίπεδο ασφάλειας δικαίου και προβλεψιμότητας για τους χρήστες και τους παρόχους υπηρεσιών, καθώς και η δυνατότητα άσκησης δικαστικής προσφυγής σύμφωνα με το εθνικό δίκαιο. Οποιαδήποτε τέτοια μέτρα θα πρέπει να λαμβάνουν υπόψη τα δικαιώματα των τελικών χρηστών και να συμμορφώνονται με τις ισχύουσες νομικές και δικαστικές διαδικασίες, καθώς και με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («ο Χάρτης»).

Για την πραγματική καταπολέμηση της τρομοκρατίας, έχει ζωτική σημασία η αποτελεσματική ανταλλαγή πληροφοριών που θεωρούνται ότι είναι συναφείς από τις

αρμόδιες Αρχές για τους σκοπούς της πρόληψης, ανίχνευσης, διερεύνησης και δίωξης τρομοκρατικών εγκλημάτων μεταξύ αρμόδιων Αρχών και Οργανισμών της Ένωσης. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι πληροφορίες ανταλλάσσονται με αποτελεσματικό και έγκαιρο τρόπο, σύμφωνα με το εθνικό δίκαιο και το υφιστάμενο νομικό πλαίσιο της Ένωσης, όπως η απόφαση 2005/671/ΔΕΥ, η απόφαση 2007/533/ΔΕΥ του Συμβουλίου και η οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Οι αρμόδιες εθνικές αρχές, όταν εξετάζουν το ενδεχόμενο ανταλλαγής συναφών πληροφοριών, θα πρέπει να λαμβάνουν υπόψη τους τη σοβαρή απειλή που συνιστούν τα τρομοκρατικά αδικήματα.

2.8.3 Νομοθετικό Πλαίσιο για την αντιμετώπιση της τρομοκρατίας στην Ελλάδα

Το πρώτο νομοθέτημα, που θεσπίστηκε για να αντιμετωπίσει το φαινόμενο της τρομοκρατίας, ήταν ο νόμος 774/1978 «περί καταστολής της τρομοκρατίας και προστασίας του δημοκρατικού πολιτεύματος», στον οποίο δεν υπήρχε ορισμός της τρομοκρατίας, αλλά μόνον μια γενική αναφορά στον όρο «ομάδα».

Δεύτερο νομοθέτημα ήταν αυτό του Ν. 1916/1990 με τίτλο «για την προστασία της κοινωνίας από το οργανωμένο έγκλημα», όπου δε γινόταν λόγος ούτε για οργανωμένο έγκλημα, παρά τον οξύμωρο τίτλο του, ενώ έλειπαν από τις αξιόποινες πράξεις του εντελώς τα οικονομικά εγκλήματα, που χαρακτηρίζουν κατ' εξοχήν την οργανωμένη εγκληματικότητα και που αργότερα καταργήθηκε με τον ν. 2172/1993. Ακολούθησαν ο Ν. 2928/2001 και 3251/2004, ενώ με τον τελευταίο δημιουργείται αυτοτελές τρομοκρατικό αδίκημα, χωρίς την προϋπόθεση ύπαρξης οργάνωσης ή ομάδας.

Η βασική καινοτομία του Ν. 3251/2004 συνίσταται στην εισαγωγή για πρώτη φορά στο ελληνικό δίκαιο του ευρωπαϊκού εντάλματος σύλληψης, ενώ δια του νόμου αυτού η ελληνική έννομη τάξη επιχειρεί να συμμορφωθεί στην ουσία με την απόφαση – πλαίσιο της Ευρωπαϊκής Ένωσης 2002/584/ΔΕΥ, όπως ίσχυε μετά την τροποποίηση από την απόφαση – πλαίσιο 2009/299/ΔΕΥ και να ενσωματώσει, περαιτέρω, τις Οδηγίες 2012/13/ΕΕ και 2013/48/ΕΕ για την αντιμετώπιση της τρομοκρατίας. Τυποποιούνται πλέον ως τρομοκρατικές πράξεις μια σειρά από κοινά εγκλήματα (πράξεις ποινικά κολάσιμες κατά τις διατάξεις του Ειδικού Μέρους του ΠΚ), εφόσον αυτά χαρακτηρίζονται από ένα αντικειμενικό στοιχείο, ότι δηλαδή τελούνται με τρόπο, σε έκταση ή υπό συνθήκες που είναι δυνατόν να βλάψουν σοβαρά μία χώρα ή έναν διεθνή οργανισμό και από ένα υποκειμενικό στοιχείο, ότι δηλαδή τελούνται με σκοπό να εκφοβίσουν σοβαρά

έναν πληθυσμό, να εξαναγκάσουν μία δημόσια αρχή ή έναν διεθνή οργανισμό να εκτελέσει οποιαδήποτε πράξη ή να απόσχει από αυτήν ή να βλάψουν σοβαρά ή να καταστρέψουν τις θεμελιώδεις συνταγματικές, πολιτικές, οικονομικές δομές μιας χώρας ή ενός διεθνούς οργανισμού.

2.8.4 Τα εγκλήματα των άρθρων 187 Α και 187 Β ΠΚ

Σε συμμόρφωση με την Οδηγία (ΕΕ) 2017/541 του ΕΚ και του Συμβουλίου της Ευρώπης, η οποία ενσωματώθηκε στην ελληνική νομοθεσία με τον Ν. 4689/2020, ποινικοποιήθηκαν νέα εγκλήματα που σχετίζονται με τρομοκρατικές δραστηριότητες.

Στον ελληνικό Ποινικό Κώδικα σήμερα οι τρομοκρατικές ενέργειες και δη το έγκλημα της τρομοκρατικής οργάνωσης τυποποιούνται στο άρθρο 187 Α και 187 Β αυτού.

- **<u>Άρθρο 187 Α ΠΚ</u>**

Στο άρθρο αυτό προβλέπεται ότι τρομοκρατικό έγκλημα μπορεί να είναι οποιοδήποτε κακούργημα ή οποιοδήποτε κοινώς επικίνδυνο έγκλημα, εφόσον τελείται υπό συνθήκες ή με τέτοιο τρόπο ή σε τέτοια έκταση που να προκαλεί σοβαρό κίνδυνο για τη χώρα ή για διεθνή οργανισμό και με τους σκοπούς που περιγράφονται στο συγκεκριμένο άρθρο.

Επέρχεται κατ' αυτό τον τρόπο μία ουσιώδης αλλαγή, η οποία συνίσταται στην κατάργηση του καταλόγου των αξιόποινων πράξεων που μπορούν να χαρακτηριστούν ως τρομοκρατικές. Σημαντική είναι και η αλλαγή που υιοθετείται για την σύσταση τρομοκρατικής οργάνωσης ή τη συμμετοχή σε αυτή. Ενώ η σύσταση της οργάνωσης ή συμμετοχή σε αυτή για την τέλεση τρομοκρατικού εγκλήματος που έχει τη μορφή κακουργήματος διατηρεί τον κακουργηματικό της χαρακτήρα και απειλείται με ποινή κάθειρξης ως δέκα έτη, η σύσταση τρομοκρατικής οργάνωσης ή η συμμετοχή σε αυτή προκειμένου να τελεστεί τρομοκρατικό έγκλημα που έχει τη μορφή πλημμελήματος αντιμετωπίζεται ως πλημμέλημα και τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους, σε αντίθεση με όσα προέβλεπε η προϊσχύσασα διάταξη, στο πλαίσιο της οποίας απειλείτο η ποινή του κακουργήματος μειωμένη στο μέτρο του άρθρου 83 ΠΚ[5].

Επιπλέον, προστίθενται πλέον στο άρθρο αυτό οι παράγραφοι 4 έως 6 σε συμμόρφωση της χώρας μας προς την Απόφαση - Πλαίσιο 2008/919/ΔΕΥ του Συμβουλίου της 28ης Νοεμβρίου 2008. Στην παρ. 4 τυποποιείται, ειδικότερα, η πράξη της

5 Α. Χαραλαμπάκης, Ο Νέος Ποινικός Κώδικας – Συνοπτική Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Νομική Βιβλιοθήκη, 2η έκδοση, σελ. 175

στρατολόγησης άλλου σε τρομοκρατική οργάνωση ή σε τέλεση τρομοκρατικών πράξεων, ενώ στην παράγραφο 5 τυποποιείται η εκπαίδευση άλλου για την τέλεση συγκεκριμένης τρομοκρατικής πράξης. Τέλος, στην παράγραφο 6 έχει μεταφερθεί η διάταξη της παρ. 3 του προϊσχύσαντος άρθρου με αρκετές αλλαγές, που ήταν αναγκαίες προκειμένου να προσδιοριστούν με μεγαλύτερη σαφήνεια τα στοιχεία της αξιόποινης συμπεριφοράς.

Πιο συγκεκριμένα, στην παράγραφο αυτή τιμωρείται όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου απειλεί με τέλεση τρομοκρατικών πράξεων ή προκαλεί ή διεγείρει σε διάπραξή τους και έτσι εκθέτει σε κίνδυνο τη δημόσια τάξη.

Τέλος, με τη διάταξη του άρθρου 3 παρ. 14 Ν 4637/2019, προστέθηκε στο άρθρο 187Α ΠΚ έβδομη παράγραφος, η οποία έχει ως εξής: «Με την ποινή της προηγούμενης παραγράφου τιμωρείται και όποιος με σκοπό να τελέσει ή να συμβάλει στην τέλεση τρομοκρατικού εγκλήματος, να συμμετάσχει στις δραστηριότητες τρομοκρατικής ομάδας, με επίγνωση του γεγονότος ότι η εν λόγω συμμετοχή θα συμβάλει στις εγκληματικές δραστηριότητες αυτής της ομάδας ή με σκοπό να προσφέρει ή να παρακολουθήσει εκπαίδευση για τέλεση τρομοκρατικών πράξεων, πραγματοποιεί ταξίδι το οποίο διευκολύνει την πραγμάτωση του σκοπού του».

- **<u>Άρθρο 187 Β ΠΚ</u>**

Στο άρθρο αυτό τυποποιείται ως αυτοτελές έγκλημα η αξιόποινη υποστήριξη, μια πράξη που τυποποιείται σήμερα εν μέρει στο άρθρο 187 παρ. 2 και 4 και εν μέρει στο άρθρο 187Α παρ. 6-8 ΠΚ. Στην προτεινόμενη διάταξη, ως πρώτη μορφή αξιόποινης υποστήριξης, προβλέπεται η παροχή ουσιωδών πληροφοριών ή υλικών μέσων με σκοπό να διευκολυνθεί ή να υποβοηθηθεί εγκληματική ή τρομοκρατική οργάνωση για τη διάπραξη των επιδιωκόμενων από αυτήν κακουργημάτων. Στην παρ. 2 επαναλαμβάνεται κατά βάση αυτούσια η διάταξη του άρθρου 187Α παρ. 6 ΠΚ, ενώ στην παρ. 3 επαναλαμβάνεται η διάταξη του άρθρου 187 παρ. 4 ΠΚ, η οποία, με βάση το άρθρο 187Α παρ. 8 ΠΚ ισχύει τόσο για το τρομοκρατικό έγκλημα όσο και για τις τρομοκρατικές οργανώσεις. Αντίθετα, δεν κρίθηκε αναγκαία η αυτοτελής τυποποίηση των πράξεων που περιγράφονται στο άρθρο 187Α παρ. 7 ΠΚ (διακεκριμένη κλοπή, ληστεία, πλαστογραφία και εκβίαση). Αν από τα προϊόντα που θα προκύψουν από τις συγκεκριμένες πράξεις ενισχυθεί πράγματι η δράση των εγκληματικών ή τρομοκρατικών οργανώσεων, οι πράξεις υπάγονται ούτως ή άλλως στις προβλεπόμενες στο άρθρο 187Β του νέου ΠΚ πράξεις.

Με τη διάταξη του άρθρου 3 παρ. 16 Ν 4637/2019, προστέθηκε στο άρθρο 187Β νέα παρ. 4, η οποία έχει ως εξής: «Κατά την επιμέτρηση της ποινής των εγκλημάτων της παραγράφου 1 λαμβάνονται υπόψη ως επιβαρυντικές περιστάσεις οι αμετάκλητες καταδικαστικές αποφάσεις που εκδίδουν δικαστήρια άλλων κρατών - μερών της Σύμβασης της Βαρσοβίας της 16ης Μαΐου 2005 του Συμβουλίου της Ευρώπης για τη νομιμοποίηση, ανίχνευση, κατάσχεση και δήμευση εσόδων από εγκληματικές δραστηριότητες και για τη χρηματοδότηση της τρομοκρατίας».

2.9 Συμπερασματικές Παρατηρήσεις

Συνοψίζοντας, είναι γεγονός πως ηλεκτρονική τρομοκρατία δεν υφίσταται με την αυστηρή έννοια του όρου στις μέρες μας. Οι απόψεις των ειδικών ποικίλουν, αφού είναι αμφιλεγόμενο το αν μια επίθεση μέσω κυβερνοχώρου δεν θα μπορούσε να προκαλέσει ανθρώπινες απώλειες. Λαμβανομένων υπόψη της εξέλιξης των τρομοκρατικών απειλών και των νομικών υποχρεώσεων για την Ένωση και τα κράτη μέλη στο πλαίσιο του διεθνούς δικαίου, θα πρέπει να υπάρξει μεγαλύτερη σύγκλιση σε όλα τα κράτη μέλη όσον αφορά τον ορισμό των τρομοκρατικών εγκλημάτων, των εγκλημάτων που σχετίζονται με τρομοκρατική ομάδα και αυτών που σχετίζονται με τρομοκρατικές δραστηριότητες, ώστε να καλύπτει πληρέστερα συμπεριφορές συνδεόμενες ιδίως με τους αλλοδαπούς τρομοκράτες μαχητές και τη χρηματοδότηση της τρομοκρατίας. Αυτές οι μορφές συμπεριφοράς θα πρέπει επίσης να τιμωρούνται όταν τελούνται μέσω του διαδικτύου, αλλά και μέσω των μέσων κοινωνικής δικτύωσης.

Η κυβερνοτρομοκρατία διακρίνεται από την τρομοκρατία από τον «τόπο» στον οποίο διαπράττεται ή από το «μέσο» μέσω του οποίου διαπράττεται, δηλαδή τον κυβερνοχώρο. Από αυτή την άποψη, η κυβερνοτρομοκρατία δεν είναι ένα αυτόνομο έγκλημα και μάλιστα ως έγκλημα δεν τυποποιείται αυτοτελώς ούτε στον Ποινικό μας Κώδικα ούτε σε διεθνή νομοθετικά κείμενα και συνεπώς δεν τιμωρείται, αλλά υπονοεί ένα είδος τρομοκρατίας που χαρακτηρίζεται από μια μοναδική μέθοδο εκτέλεσης.

Η κυβερνοτρομοκρατία πρέπει να συμμορφώνεται με τη δομή, την αρχή της βλάβης και τα στοιχεία που ορίζουν την τρομοκρατία. Συνεπώς, εάν αυτά δεν επαληθευτούν, μπορεί να βρισκόμαστε υπό την παρουσία κυβερνοεγκλήματος και όχι κυβερνοτρομοκρατίας (για παράδειγμα, δολιοφθοράς υπολογιστή). Όσον αφορά στη δομή της, η κυβερνοτρομοκρατία απαιτεί την ύπαρξη μιας οργάνωσης που προορίζεται να διαπράξει (κυβερνο)τρομοκρατικές επιθέσεις. Όσον αφορά στην αρχή της βλάβης, η

κυβερνοτρομοκρατία πρέπει να παραβιάζει άμεσα ένα συλλογικό συμφέρον που ταυτίζεται με τη δημοκρατική συνταγματική τάξη, ενώ ως προς τα στοιχεία της, η κυβερνοτρομοκρατία πρέπει να εκτελείται με συγκεκριμένο σκοπό την αλλαγή της συνταγματικής τάξης ή την ανατροπή της νόμιμα εκλεγμένης κυβέρνησης και με τρόπο κατάλληλο, ώστε να ενσταλάξει τον τρόμο στον ανθρώπινο νου, καθιερώνοντας την πεποίθηση ότι οποιοσδήποτε, οπουδήποτε, μπορεί να πέσει θύμα επίθεσης.

Τέλος, η κυβερνοτρομοκρατία δημιουργεί πολλές προκλήσεις σε έναν παγκόσμιο και τεχνολογικά διασυνδεδεμένο κόσμο. Η διάπραξη κυβερνοτρομοκρατίας περιλαμβάνει τη χρήση του διαδικτύου, το οποίο προσφέρει μια σειρά πλεονεκτημάτων για όσους συμμετέχουν στην πράξη. Επιπλέον, επειδή οι πραγματικές διαστάσεις και οι δυνατότητες της κυβερνοτρομοκρατίας δεν είναι ακόμη σαφείς, παραμένει δυσχερής η πρόληψη και η αντιμετώπισή της.

Πάντως, είναι γενικά αποδεκτό ότι στο μέλλον ο κόσμος θα κληθεί να αντιμετωπίσει τέτοιου είδους κυβερνοεπιθέσεις από τη στιγμή που οι επιθέσεις μέσω διαδικτύου απαιτούν σχετικά μικρούς προϋπολογισμούς και ταυτόχρονα επιφέρουν καταστροφικές συνέπειες. Παράλληλα, το διαδίκτυο είναι ένα αχανές βασίλειο ατιμωρησίας και τα μέσα που προσφέρονται στις Αρχές, καθώς και η έλλειψη διεθνούς συνεργασίας και στιβαρού παγκοσμίου νομοθετικού πλαισίου καθιστούν δύσκολες τις συλλήψεις.

Παρόλο όμως, που το διαδίκτυο είναι αρκετά ελκυστικό για τους τρομοκράτες από πλευράς προπαγάνδας, επιφέρει συνέπειες λιγότερο θεαματικές από μια φυσική επίθεση.

Όμως η τρομοκρατία συνεχώς εξελίσσεται, και έτσι οι πιο ριζοσπαστικοί είναι συχνά οι νέοι προσηλυτισμένοι, οι οποίοι αν και δεν μιλούν καν αραβικά είναι ικανοί να αφομοιωθούν μέσα στον πληθυσμό, χωρίς να τραβήξουν την προσοχή των αρχών, αφού έχουν λάβει υψηλή εκπαίδευση. Αυτή η καινούργια γενιά τρομοκρατών θα μπορούσε σε μερικά χρόνια να αποτελέσει μια επικίνδυνη απειλή για τα κράτη.

Τα συστήματα εκμετάλλευσης γίνονται όλο και περισσότερο περίπλοκα, γι’ αυτό περιλαμβάνουν έναν αυξημένο αριθμό λαθών προγραμματισμού, επιτρέποντας τον εξ αποστάσεως έλεγχο. Παράλληλα, οι χρήστες δεν έχουν την κατάλληλη παιδεία να αντιληφθούν τον κίνδυνο και μη δείχνοντας ιδιαίτερη σύνεση προμηθεύουν άθελά τους με όπλα τους κυβερνοτρομοκράτες.

Από όλα τα παραπάνω, γίνεται ευχερώς αντιληπτό ότι η κυβερνοτρομοκρατία, αν και διαγράφεται στον ορίζοντα, δεν είναι ακόμη καθαρά ορατή. Εντούτοις, εάν και η πιθανότητα μιας επίθεσης είναι μικρή, ο κίνδυνος εκδήλωσής της λαμβάνεται υπόψη από πολλά πολιτισμένα κράτη και προκαλεί τις συζητήσεις των ειδικών.

Επομένως, δε μπορούμε να εφησυχάζουμε για το μέλλον. Η κυβερνοτρομοκρατία μπορεί να γίνει πολύ πιο ελκυστική για τους επερχόμενους τρομοκράτες όσο ο πραγματικός και ο εικονικός κόσμος συνδέονται στενότερα.

Τέλος, από τη στιγμή που οι σύγχρονες κοινωνίες και οικονομίες στηρίζονται όλο και περισσότερο στην ηλεκτρονική πληροφορία και το διαδίκτυο και ταυτόχρονα η επόμενη γενιά τρομοκρατών μεγαλώνει σε έναν ψηφιακό κόσμο, όπου τα εργαλεία hacking γίνονται μέρα με την μέρα απλούστερα στην χρήση τους, ισχυρότερα και πιο διαδεδομένα, η εκάστοτε κυβέρνηση πρέπει να προετοιμαστεί, ώστε να είναι ικανή να αντεπεξέλθει σε οποιαδήποτε επίθεση τους.

3 Κυβερνοασφάλεια

3.1 Κυβερνοασφάλεια και Ευρωπαϊκή Ένωση (Ε.Ε.)

Στην εποχή μας υπάρχουν περισσότερες ηλεκτρονικές συσκευές από ανθρώπους. Επομένως οι εγκληματίες γίνονται συνεχώς πιο εφευρετικοί. Καθημερινά βρισκόμαστε αντιμέτωποι με νέες ψηφιακές απειλές ή κυβερνοαπειλές όπως αποκαλούνται, (ιοί των υπολογιστών, Ransomware, Malware, παραβιάσεις ηλεκτρονικών συστημάτων από κακόβουλους χρήστες (Hackers), παραβίαση ηλεκτρονικής ταυτότητας κλπ).

Οι κυβερνοαπειλές (Cyber Threats), είναι ενέργειες που γίνονται από τρίτους με σκοπό να αποκτήσουν πρόσβαση σε πόρους που δεν έχουν τα κατάλληλα δικαιώματα, να καταστρέψουν ευαίσθητες και σημαντικές πληροφορίες, να αποσπάσουν χρήματα από χρήστες ή να διακόψουν τη ροή εργασιών μιας επιχείρησης.

Η κυβερνοασφάλεια αποτελεί προτεραιότητα για πολλές χώρες που έχουν αντιληφθεί τη σημασία της. Αναφέρεται στην πρακτική της διασφάλισης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Η κυβερνοασφάλεια αποτελείται από ένα εξελισσόμενο σύνολο εργαλείων, προσεγγίσεων διαχείρισης κινδύνου, τεχνολογιών, εκπαίδευσης και βέλτιστων πρακτικών που έχουν σχεδιαστεί για την προστασία δικτύων, συσκευών, προγραμμάτων και δεδομένων από

επιθέσεις ή μη εξουσιοδοτημένη πρόσβαση. Οι βασικοί και πιο σημαντικοί παράγοντες που σχετίζονται με την κυβερνοασφάλεια είναι οι χρήστες (άνθρωποι), οι διαδικασίες που θέτει ένας Οργανισμός ή κάποιος ατομικά και η τεχνολογία και το software ή το hardware που απαιτείται για την προστασία από τις κυβερνοαπειλές. Για τον λόγο αυτό αναπτύχθηκαν και στρατηγικές κυβερνοασφάλειας. Σκοπός τους είναι η προστασία απέναντι σε απειλές ασφάλειας και η διασφάλιση της οικονομικής και κοινωνικής ευημερίας. Ως στόχο έχουν την ενίσχυση της κυβερνητικής συνεργασίας και τον προσδιορισμό ρόλων και αρμοδιοτήτων σε ό,τι αφορά τη δίωξη των διαδικτυακών εγκλημάτων, αλλά και τη διεθνή συνεργασία.

3.1.1 Το υφιστάμενο περιβάλλον της Κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση

Οι βασικοί παράγοντες που επηρεάζουν την κυβερνοασφάλεια είναι η τεχνολογική πρόοδος, οι απαιτήσεις των κανονισμών σχετικά με την κυβερνοασφάλεια και οι συνεχείς αλλαγές στο τύπο και το είδος των απειλών. Οι ταχύτατες εξελίξεις δημιουργούν σοβαρές προκλήσεις στη διασφάλιση της δημόσιας ασφάλειας και στο συντονισμό μίας διεθνούς συνεργασίας σε επίπεδο κρατών. Επομένως, όλες αυτές οι προκλήσεις πρέπει να λαμβάνονται υπόψη κατά τα στάδια της ανάπτυξης, της εφαρμογής και της αξιολόγησης των εθνικών στρατηγικών της κυβερνοασφάλειας[6].

Οι κυβερνοαπειλές αποτελούν μία από τις σημαντικότερες απειλές σε εθνικό επίπεδο, ενώ θεωρούνται εφάμιλλες με την τρομοκρατία και το οργανωμένο έγκλημα. Σε ένα μεγάλο ποσοστό, τα κράτη έχουν αναγνωρίσει την απειλή που προκύπτει από την ανάπτυξη του κυβερνοχώρου και γι' αυτό το λόγο τα περισσότερα κράτη της Ευρωπαϊκής Ένωσης (ΕΕ) έχουν σχεδιάσει και αναπτύξει μια εθνική στρατηγική κυβερνοασφάλειας. Πολλές από αυτές τις στρατηγικές έχουν σχεδιαστεί πριν από μερικά χρόνια, χωρίς να έχουν ενημερωθεί προσφάτως. Παράλληλα, έχει διαπιστωθεί ότι πολλά από τα συμβάντα κυβερνοασφάλειας που έλαβαν χώρα σε παγκόσμιο επίπεδο δεν οδήγησαν σε αναδιαμόρφωση των στρατηγικών.

Ορισμένα ευρωπαϊκά κράτη έχουν θέσει ένα συγκεκριμένο χρονικό όριο επανεξέτασης των στρατηγικών τους, με σκοπό την ενημέρωση και την επικαιροποίησή τους, ώστε να ανταποκρίνονται στις νέες εξελίξεις στον κυβερνοχώρο. Ωστόσο, παρότι υπάρχει ο σχετικός σχεδιασμός, ελάχιστα κράτη τον εφαρμόζουν στην πράξη.

6 https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/risk/gr_SEV_Deloitte_Cybersecurity_noexp.pdf

Ένα ακόμη τρωτό σημείο είναι ότι ο διαχωρισμός των καθηκόντων, που συμπεριλαμβάνεται στις περισσότερες εθνικές στρατηγικές, δεν είναι ξεκάθαρος, ενώ ελάχιστες στρατηγικές αναφέρουν και εφαρμόζουν μία ολιστική προσέγγιση συνεργασίας (networked approach). Η συγκεκριμένη προσέγγιση περιλαμβάνει τη συνεργασία κρατικών φορέων και ιδιωτικών Οργανισμών με σκοπό την αποτελεσματική διαχείριση και αντιμετώπιση σοβαρών περιστατικών κυβερνοασφάλειας, όπως είναι οι υβριδικές απειλές.

Τέλος, παρόλο που η Ευρωπαϊκή Ένωση και το ΝΑΤΟ έχουν κάνει σημαντικά βήματα στη θέσπιση μίας γενικά αποδεκτής ορολογίας στον τομέα της κυβερνοασφάλειας, πολλές ευρωπαϊκές χώρες χρησιμοποιούν διαφορετικές ορολογίες και ορισμούς στις στρατηγικές τους, ενώ τις περισσότερες φορές επικρατεί σύγχυση σχετικά με τους ορισμούς και τους θεσμοθετημένους κανόνες στο χώρο της κυβερνοασφάλειας, καθώς τα διάφορα κράτη ερμηνεύουν με διαφορετικό τρόπο την υφιστάμενη ορολογία.

3.1.2 Κανονιστικές Αποφάσεις σε Ευρωπαϊκό Επίπεδο - Νομική Θεμελίωση των Οδηγιών 2013/40 και 2016/1148

Σε καθημερινή βάση οι κακόβουλες επιθέσεις αυξάνονται εκθετικά, δεδομένης και της ευρείας χρήσης του διαδικτύου στην εποχή μας. Ιδίως οι επιθέσεις κατά των συστημάτων πληροφοριών και ιδίως εκείνες που συνδέονται με το οργανωμένο έγκλημα αποτελούν αυξανόμενη απειλή τόσο στην ΕΕ όσο και παγκόσμια, αλλά και για την επίτευξη ασφαλέστερης κοινωνίας της πληροφορίας. Το περιβάλλον στο οποίο διεξάγονται οι εν λόγω επιθέσεις είναι, ασφαλώς, ιδιαίτερα περίπλοκο, καθ' ότι η υποδομή του Διαδικτύου ανήκει στην ιδιοκτησία ιδιωτικών επιχειρήσεων που βρίσκονται σε πολλές χώρες του κόσμου και το ίδιο το δίκτυο διαθέτει ανοικτή αρχιτεκτονική. Το γεγονός δε ότι το Διαδίκτυο είναι ένα παγκοσμιοποιημένο δίκτυο δικτύων η/υ σημαίνει ότι μια επίθεση σε έναν τομέα έχει επίδραση και σε άλλους τομείς, διεθνώς και όχι μόνο σε μία χώρα[7].

Η ποινική αντιμετώπιση του φαινομένου αυτού στο πλαίσιο ενός υπερεθνικού Οργανισμού, όπως είναι η ΕΕ, αποκτά, συνεπώς, εξαιρετική σημασία. Τα τελευταία χρόνια έχουν εισαχθεί στο ευρωπαϊκό, αλλά και στο εθνικό δίκαιο μία σειρά από νομοθετήματα που ορίζουν τις έννοιες, αλλά και τις απαιτήσεις σχετικά με την κυβερνοασφάλεια για τα κράτη μέλη, αλλά και για τις επιχειρήσεις που δραστηριοποιούνται εντός της Ε.Ε.

7 Ι. Ιγγλεζάκης, Δίκαιο και Νέες Τεχνολογίες, Συνήγορος, τεύχος 98, 2013, "Επιθέσεις κατά συστημάτων πληροφοριών"

Στο πλαίσιο της ΕΕ εκδόθηκε η απόφαση-πλαίσιο 2005/222/ΔΕΥ, η οποία είχε ως στόχο την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο και την προώθηση της ασφάλειας πληροφοριών σε ό,τι αφορά τη νέα μορφή διεθνικής εγκληματικότητας που συνιστούν οι επιθέσεις κατά συστημάτων πληροφοριών.

Η απόφαση - πλαίσιο προέβλεπε, μεταξύ άλλων, την ποινικοποίηση της παράνομης πρόσβασης σε σύστημα πληροφοριών, της παράνομης παρεμβολής σε σύστημα και της παράνομης παρεμβολής σε δεδομένα. Ακόμα, η απόφαση - πλαίσιο προέβλεπε ρυθμίσεις για την ηθική αυτουργία, υποβοήθηση, συνέργεια και απόπειρα, σε σχέση με τα παραπάνω αδικήματα, καθώς και επιβαρυντικές περιστάσεις, όπως είναι ιδίως η διάπραξη των εν λόγω πράξεων στα πλαίσια εγκληματικής οργάνωσης. Επιπλέον, ρύθμιζε την ευθύνη νομικών προσώπων, όταν τα αδικήματα αυτά τελούνταν από εκπροσώπους τους.

Η άνω πράξη δε μεταφέρθηκε πλήρως στα κράτη μέλη, σύμφωνα με την από 14.7.2008 Έκθεση της Επιτροπής, στην οποία διαπιστώθηκε ότι σημειώθηκε αξιοσημείωτη πρόοδος στην πλειοψηφία των κρατών μελών, με εξαίρεση επτά κράτη μέλη, μεταξύ των οποίων και η Ελλάδα, τα οποία δεν κοινοποίησαν στην Επιτροπή τα μέτρα εφαρμογής της απόφασης – πλαισίου.

Η ανάγκη για περαιτέρω δράση στην αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, στο πλαίσιο της ΕΕ οδήγησε στην ψήφιση μιας νέας οδηγίας, η οποία θα ρύθμιζε επιπλέον θέματα, υποβοηθώντας το επίπεδο της κυβερνοασφάλειας.

Τον Αύγουστο του 2013, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, εξέδωσαν την Οδηγία 2013/40[8] για τις επιθέσεις κατά των συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Η Οδηγία αυτή στόχευε στο να προσεγγίσει το ποινικό δίκαιο των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων και αποσκοπούσε στη βελτίωση της συνεργασίας μεταξύ δικαστικών και άλλων αρμοδίων Αρχών.

Ένας σημαντικός νεωτερισμός της οδηγίας σε σχέση με την απόφαση - πλαίσιο 2005/222/ΔΕΥ είναι ότι λαμβάνει υπόψη και ποινικοποιεί τη χρήση νέων μεθόδων για τη διάπραξη κυβερνοεγκλημάτων, όπως είναι η χρήση δικτύων προγραμμάτων ρομπότ (botnets). Με τον όρο αυτό δηλώνεται ένα δίκτυο η/υ που έχουν μολυνθεί με κακόβουλο

8 EEL 218/8 13.8.2013, Οδηγία 2013/40/ΕΕ

λογισμικό και ελέγχονται από έναν άλλο η/υ, συχνά δίχως να το γνωρίζει ο κάτοχός τους (υπολογιστές «ζόμπι»). Τα δίκτυα αυτά μπορεί να ενεργοποιηθούν προκειμένου να εκτελέσουν συγκεκριμένες ενέργειες, όπως π.χ. να επιτεθούν σε συστήματα πληροφοριών. Ένα δίκτυο προγραμμάτων ρομπότ μπορεί να χρησιμοποιηθεί για την αποστολή ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, για την αλίευση προσωπικών δεδομένων (phishing) ή την κλοπή τέτοιων στοιχείων από τους η/υ των χρηστών, την αποστολή και καταφόρτωση κακόβουλου λογισμικού κ.λπ.

Περαιτέρω, η οδηγία περιέχει διατάξεις για αδικήματα που θίγουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων συστημάτων η/υ.

Ιδιαίτερο ενδιαφέρον παρουσιάζει το άρθρο 13 της εν λόγω Οδηγίας που αφορά στην ανταλλαγή πληροφοριών μέσω εθνικών δικτύων επαφής (CSIRT) τα οποία οφείλουν να είναι λειτουργικά σε 24ωρη βάση και επτά ημέρες την εβδομάδα, να ανταποκρίνονται σε επείγοντα αιτήματα για βοήθεια εντός 8 ωρών προκειμένου να δηλώσουν αν και πότε θα μπορέσουν να απαντήσουν και να συλλέγουν στατιστικά δεδομένα σχετικά με το έγκλημα στον κυβερνοχώρο.

Ωστόσο, πέραν των όσων ανωτέρω αναλύθηκαν, σε επίπεδο ΕΕ, αναγνωρίστηκε η επιτακτικότατη ανάγκη για την ενίσχυση της κυβερνοασφάλειας, με την θέσπιση ενός αποτελεσματικότερου και καθοριστικότερης σημασίας νομικού πλαισίου προστασίας των δεδομένων για την οικοδόμηση εμπιστοσύνης και την ανάπτυξη αισθήματος ασφάλειας στον κόσμο του διαδικτύου, το οποίο θα επιτρέπει στους καταναλωτές και τις επιχειρήσεις να αξιοποιήσουν πλήρως τα οφέλη της ψηφιακής ενιαίας αγοράς και να αντιμετωπίσουν την κυβερνοεγκληματικότητα. Το γεγονός αυτό οδήγησε στην ψήφιση της οδηγίας 2016/1148 (“Οδηγία NIS”), με την οποία θεσπίζονται μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και ειδικότερα:

- Προβλέπονται οι υποχρεώσεις να θεσπιστεί εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κράτη μέλη
- Δημιουργούνται ομάδες συνεργασίας, ώστε να υποστηριχθεί και να διευκολυνθεί η στρατηγική συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, αλλά και να προωθηθεί η εμπιστοσύνη και η αξιοπιστία μεταξύ τους
- Δημιουργείται δίκτυο ομάδων απόκρισης για συμβάντα που σχετίζονται με την ασφάλεια των υπολογιστών (δίκτυο CSIRT), ώστε να αναπτυχθεί αίσθημα

αξιοπιστίας και εμπιστοσύνης μεταξύ των κρατών μελών και να υπάρξει γρήγορη και αποτελεσματική επιχειρησιακή συνεργασία

- Θεσπίζονται απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών
- Προβλέπονται οι υποχρεώσεις των κρατών μελών να ορίζουν εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και CSIRT με καθήκοντα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Πρόκειται για το πρώτο ενιαίο πανευρωπαϊκό νομοθετικό πλαίσιο σχετικά με την ασφάλεια στον κυβερνοχώρο. Η Οδηγία NIS αποτελεί μέρος μιας στρατηγικής της Ευρωπαϊκής Ένωσης για την συλλογική και σφαιρική προσέγγιση της ασφάλειας στον κυβερνοχώρο με απώτερο σκοπό την αποτελεσματική αντιμετώπιση των περιστατικών και των κινδύνων ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση.

Επιπρόσθετα, η συγκεκριμένη οδηγία ενθαρρύνει τη συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών («ENISA»), ώστε να υπάρχει και ενιαία στρατηγική αντιμετώπισης των κινδύνων και προωθεί τη συνεργασία μεταξύ των Εθνικών Αρχών Επιβολής του Νόμου (Δικαστικές και Αστυνομικές Αρχές) των Κρατών Μελών μέσω κριτηρίων και διαδικασιών που θεσπίζονται στο εθνικό δίκαιο και με σεβασμό των υφιστάμενων διαύλων ανταλλαγής πληροφοριών. Οι Εθνικές Αρχές επιβολής του Νόμου και οι αποκλειστικές περιφερειακές πλατφόρμες της Europol και του Ευρωπαϊκού Κέντρου για τα Εγκλήματα στον Κυβερνοχώρο (EC3), μέσω διαφόρων περιφερειακών μέσων, έλαβαν εντολές και δομές για να συνεργαστούν για τη διασυνοριακή εγκληματικότητα στον κυβερνοχώρο. Ωστόσο, νομικά και διαρθρωτικά το επίπεδο της περιφερειακής επισημοποίησης παραμένει πολύ χαμηλότερο για την ανταλλαγή μεταξύ των NIS και των κοινοτήτων LEA (Law Enforcement Agencies – Αρχές επιβολής του νόμου).

Πιο συγκεκριμένα, η Οδηγία NIS αποτελεί το πρώτο νομοθετικό κείμενο που επισημοποιεί τις δομές και τις διαδικασίες ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, ώστε να επιτευχθεί η διασυνοριακή ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης μέσω της ανταλλαγής πληροφοριών και βέλτιστων πρακτικών και της αξιολόγησης των εθνικών στρατηγικών, της αποτελεσματικότητας των ομάδων απόκρισης – CSIRT κ.λ.π.

Η ομάδα συνεργασίας και το δίκτυο των ομάδων CSIRT αποτελούν δύο δομές που θεσπίζονται από την Οδηγία, προκειμένου να ενθαρρύνουν και να βελτιώσουν την ανταλλαγή πληροφοριών. Η ομάδα συνεργασίας απαρτίζεται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA και διαδραματίζει ηγετικό ρόλο στην υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας, εστιάζοντας στην ανταλλαγή πληροφοριών, όπως για παράδειγμα την ανταλλαγή πληροφοριών με την κοινοποίηση συμβάντων ασφαλείας. Το δίκτυο των ομάδων CSIRT αποτελείται από εκπροσώπους των CSIRT των κρατών μελών και της CERT-EU.

Βάσει της Οδηγίας και ειδικότερα του άρθρου 8 αυτής, απαιτείται από τα κράτη μέλη να ορίσουν μια εθνική αρμόδια Αρχή ή πολλαπλές Αρχές και ένα ενιαίο σημείο επαφής, ενώ, κατά το άρθρο 14 αυτής, απαιτείται μεταγενέστερα από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών να ενημερώνουν, «χωρίς αδικαιολόγητη καθυστέρηση», την αρμόδια Αρχή ή την ομάδα CSIRT για «συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν». Για τον προσδιορισμό της σοβαρότητας ενός συμβάντος ασφαλείας λαμβάνονται υπόψη α) ο αριθμός των χρηστών που επηρεάστηκε (ποσοτικό κριτήριο) β) η διάρκεια του συμβάντος ασφαλείας (χρονικό κριτήριο), αλλά και γ) το γεωγραφικό εύρος της περιοχής που επηρεάστηκε από το συμβάν.

3.1.3 ENISA

Ο Οργανισμός της ΕΕ για την Κυβερνοασφάλεια (ENISA) διέπεται από τον Κανονισμό 2019/881[9], με τον οποίο ιδρύεται από τις 27.6.2019, σε αντικατάσταση του Οργανισμού που είχε συσταθεί με τον Κανονισμό 526/2013 και είχε θητεία 7 ετών.

Ο ENISA ιδρύθηκε το 2004 με τον Κανονισμό 460/2004 με περιορισμένο αρχικά αντικείμενο για 5 έτη, θητεία η οποία στην συνέχεια ανανεώθηκε διαδοχικά με τους Κανονισμούς 1007/2008/ΕΚ και 580/2011/ΕΚ και ακολούθως με τον 526/2013, ενώ μεταξύ των στόχων του συγκαταλέγονται:

- Η επίτευξη ενός κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση.
- Η ενίσχυση και προστασία συστημάτων δικτύου και πληροφοριών,
- Η προαγωγή και συνεργασία ανάμεσα στα κράτη μέλη,
- Η συμβολή στην αύξηση των ικανοτήτων κυβερνοασφάλειας σε επίπεδο ΕΕ.

9 ΕΕ L 151/15, 7.6.2019

- Η βοήθεια στις προσπάθειες των κρατών να βελτιώσουν την ικανότητα πρόληψης, εντοπισμού και ανάλυσης κυβερνοαπειλών
- Η παροχή γραμματειακής υποστήριξης στο δίκτυο CSIRT
- Η στήριξη στην επιχειρησιακή συνεργασία μέσα στο δίκτυο
- Η διοργάνωση ασκήσεων κυβερνοασφάλειας
- Η εκπόνηση τακτικών τεχνικών εκθέσεων
- Η παρακολούθηση των εξελίξεων σε ότι αφορά την προτυποποίηση
- Η επεξεργασία υποψήφιων συστημάτων πιστοποίησης
- Η αξιολόγηση των εγκριθέντων συστημάτων
- Η συμμετοχή σε αξιολογήσεις
- Η σύνταξη και δημοσιοποίηση κατευθυντήριων γραμμών
- Η δράση ευαισθητοποίησης του κοινού σχετικά με τους κινδύνους
- Η παροχή συμβουλευτικών υπηρεσιών στα όργανα της ΕΕ και
- Η ανάπτυξη διεθνών συνεργασιών.

Οι στόχοι τους οποίους υπηρετεί αναλύονται στο άρθρο 4 του Κανονισμού, ενώ ιδιαίτερα ουσιώδες, κατά την παρ. 1 του άρθρου αυτού, είναι ότι αποτελεί κέντρο εμπειρογνωσίας σε θέματα κυβερνοασφάλειας, χάρη στην ανεξαρτησία του, την επιστημονική ποιότητα των συμβουλών του και της επικουρίας που παρέχει, τη διαφάνεια των επιχειρησιακών διαδικασιών του και την επιμέλεια με την οποία εκτελεί τα καθήκοντά του, ενώ μεταξύ άλλων επικουρεί τα Όργανα και τους Οργανισμούς της Ένωσης, αλλά και τα κράτη μέλη στην ανάπτυξη και εφαρμογή πολιτικών για την κυβερνοασφάλεια.

Η δομή διοίκησης του ENISA απαρτίζεται από:

- Το διοικητικό συμβούλιο
- Το εκτελεστικό συμβούλιο
- Τον εκτελεστικό διευθυντή
- Τη συμβουλευτική ομάδα του ENISA
- Την ομάδα συμφεροντούχων για την πιστοποίηση της κυβερνοασφάλειας
- Το δίκτυο εθνικών υπαλλήλων- συνδέσμων

Ο ENISA λειτουργεί σύμφωνα με το ενιαίο έγγραφο προγραμματισμού που περιέχει το ετήσιο και πολυτελές πρόγραμμα του και περιλαμβάνει όλες τις προγραμματισμένες δραστηριότητες του.

Επιπλέον, προβλέπεται ότι τα μέλη του διοικητικού συμβουλίου, ο εκτελεστικός διευθυντής, και οι υπάλληλοι που αποσπώνται προσωρινά από τα κράτη μέλη υποβάλλουν ο καθένας δήλωση δεσμεύσεων και γραπτή δήλωση συμφερόντων.

Επιπρόσθετα, ο Οργανισμός διέπεται από την αρχή της διαφάνειας και εφαρμόζεται από τον Κανονισμό 1049/2001 για τα έγγραφα που τηρεί.

Τέλος, ο ENISA δεν αποκαλύπτει σε τρίτους πληροφορίες που επεξεργάζεται ή λαμβάνει. Υποχρέωση της τήρησης του απορρήτου έχουν εξίσου και τα μέλη του Διοικητικού Συμβουλίου, ο εκτελεστικός Διευθυντής, τα μέλη της συμβουλευτικής ομάδας, εξωτερικοί πραγματογνώμονες και μέλη προσωπικού του ENISA.

3.1.4 PESCO

Κομβικής σημασίας για την ενίσχυση του περιβάλλοντος ασφάλειας της Ένωσης είναι η επιτυχής πρωτοβουλία για την αντιμετώπιση των προβλημάτων στην κυβερνοασφάλεια υπό τον τίτλο Μόνιμη Δομημένη Συνεργασία ή Permanent Structured Cooperation (PESCO). Η PESCO αποτελεί τμήμα της Παγκόσμιας Στρατηγικής της ΕΕ για την πολιτική ασφαλείας της και εμπίπτει, συνεπώς, στον τομέα της εξωτερικής πολιτικής της.

Αναλυτικότερα, στις 13 Νοεμβρίου 2017, Υπουργοί Εξωτερικών και Άμυνας από 23 κράτη μέλη υπέγραψαν κοινή ανακοίνωση για τη Μόνιμη Δομημένη Συνεργασία (Μ.Δ.Σ.-PESCO) και την απέστειλαν στην Ύπατο Εκπρόσωπο και στο Συμβούλιο. Την κοινή αυτή ανακοίνωση προσυπέγραψαν δύο επιπλέον χώρες στις 7 Δεκεμβρίου 2017.

Τα 25 κράτη – μέλη είναι: Αυστρία, Βέλγιο, Βουλγαρία, Τσεχική Δημοκρατία, Κροατία, Κύπρος, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Ολλανδία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβενία, Σλοβακία, Ισπανία, Ιρλανδία και Σουηδία.

Η δυνατότητα της Μόνιμης Διαρθρωμένης Συνεργασίας στον τομέα της ασφάλειας και αμυντικής πολιτικής εισήχθη με τη Συνθήκη της Λισαβόνας και προβλέπει τη δυνατότητα περισσότερων κρατών μελών της ΕΕ να συνεργάζονται στενότερα στον τομέα της ασφάλειας και της άμυνας.

Υπό το πρίσμα ενός μεταβαλλόμενου περιβάλλοντος ασφαλείας, η ΕΕ στο πλαίσιο της παγκόσμιας στρατηγικής για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (EUGS), ξεκίνησε μια διαδικασία ενισχυμένης συνεργασίας για την ασφάλεια και την άμυνα. Τα κράτη μέλη συμφώνησαν η Ευρωπαϊκή Ένωση να εντείνει τις εργασίες της στον τομέα αυτό και αναγνώρισαν ότι ο ενισχυμένος συντονισμός, οι αυξημένες επενδύσεις στην άμυνα και η συνεργασία στην ανάπτυξη των αμυντικών δυνατοτήτων, είναι οι βασικές απαιτήσεις για την επίτευξή του. Μέσω PESCO, τα κράτη μέλη αυξάνουν την αποτελεσματικότητά τους στην αντιμετώπιση των προκλήσεων ασφαλείας, προχωρώντας προς την περαιτέρω ενσωμάτωση και ενίσχυση της αμυντικής τους συνεργασίας, εντός του πλαισίου της ΕΕ.

- Η Μ.Δ.Σ - PESCO είναι ένα μόνιμο πλαίσιο για στενότερη λειτουργία και μια δομημένη διαδικασία για σταδιακή εμβάθυνση της αμυντικής συνεργασίας στο πλαίσιο της Ένωσης. Θα είναι ένας οδηγός για ολοκλήρωση στον τομέα της άμυνας.
- Κάθε συμμετέχον κράτος μέλος παρέχει ένα σχέδιο για τις εθνικές συνεισφορές και τις προσπάθειες, που έχει συμφωνήσει να κάνει. Αυτά τα εθνικά σχέδια εφαρμογής υπόκεινται σε τακτική αξιολόγηση. Αυτό που είναι διαφορετικό από την εθελοντική προσέγγιση είναι, ο κανόνας εντός της Ευρωπαϊκής Ένωσης κοινής ασφάλειας και αμυντικής πολιτικής.
- Η Μ.Δ.Σ - PESCO σχεδιάζεται για να καταστεί αποτελεσματικότερη η ευρωπαϊκή άμυνα και να παρέχει μεγαλύτερη απόδοση, παρέχοντας ενισχυμένο συντονισμό και συνεργασία στους τομείς των επενδύσεων, την ανάπτυξη δυνατοτήτων και την επιχειρησιακή ετοιμότητα. Η ενισχυμένη συνεργασία σε αυτόν τον τομέα θα επιτρέψει, μειώνοντας τον αριθμό των διαφορετικών οπλικών συστημάτων στην Ευρώπη και ως εκ τούτου, ενισχύοντας την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών, να αυξάνουν τη διαλειτουργικότητα και τη βιομηχανική ανταγωνιστικότητα.
- Η Μ.Δ.Σ - PESCO θα βοηθήσει να ενισχυθεί η στρατηγική αυτονομία της ΕΕ να δράσει μόνη της, όταν είναι απαραίτητο και με συνεργάτες οσάκις είναι δυνατόν. Ενισχύεται από την ιδέα ότι η κυριαρχία μπορεί να ασκείται καλύτερα όταν εργάζονται από κοινού, ενώ η εθνική κυριαρχία παραμένει ουσιαστικά άθικτη.
- Πρόκειται για παροχή μιας ομπρέλας τέτοιων παραδειγμάτων περιφερειακής αμυντικής ολοκλήρωσης όπως το Ναυτικό Βελγίου – Ολλανδίας ή της Διοίκησης Ευρωπαϊκής Αερομεταφοράς.
- Στρατιωτικές ικανότητες, που αναπτύχθηκαν εντός PESCO παραμένουν στα χέρια των κρατών μελών, οι οποίες μπορούν επίσης να γίνουν διαθέσιμες σε άλλα πλαίσια, όπως τα Ηνωμένα Έθνη ή το ΝΑΤΟ.

Η Μ.Δ.Σ. - PESCO συνδέεται στενά με τη νέα συντονισμένη ετήσια αναθεώρηση άμυνας (CARD - Coordinated Annual Review on Defence) και το Ευρωπαϊκό Ταμείο Άμυνας (ΕΤΑ), το οποίο αναπτύσσεται επί του παρόντος στο πλαίσιο του προγράμματος της Ευρωπαϊκής Αμυντικής Βιομηχανικής ανάπτυξης. Είναι συμπληρωματικά και αμοιβαία ενισχυόμενα εργαλεία, που συμβάλλουν στον ίδιο πολιτικό στόχο :

- Coordinated Annual Review on Defence (CARD) πρέπει να εκτελεστούν από τον Ευρωπαϊκό Οργανισμό Άμυνας, μέσα από συστηματική παρακολούθηση των σχεδίων των εθνικών αμυντικών δαπανών και βοηθούν στον εντοπισμό ευκαιριών για νέες πρωτοβουλίες συνεργασίας.
- Το ΕΤΑ θα παρέχει οικονομικά κίνητρα για την προώθηση της αμυντικής συνεργασίας από την έρευνα στη φάση της ανάπτυξης των ικανοτήτων, περιλαμβανομένων των πρωτοτύπων.
- Η Μ.Δ.Σ - PESCO θα αναπτύξει ικανότητα έργων, ταυτοποιημένων ιδίως μέσω της διαδικασίας της CARD σε τομείς προτεραιότητας. Επιλέξιμα έργα θα μπορούσαν επίσης να επωφεληθούν από χρηματοδότηση από το ΕΤΑ, το οποίο θα προβλέπει ένα πρόσθετο 10% χρηματοδότηση για τη φάση της βιομηχανικής ανάπτυξης άμυνας των έργων, που αναπτύχθηκαν στο πλαίσιο της Μ.Δ.Σ. - PESCO.

3.2 Κυβερνοασφάλεια στην Ελλάδα

Στη χώρα μας, αρμόδια υπηρεσία για τον εθνικό στρατηγικό σχεδιασμό κυβερνοασφάλειας είναι η Γενική Διεύθυνση Κυβερνοασφάλειας, η οποία υπάγεται στη Γενική Γραμματεία Τηλεπικοινωνιών & Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης. Η εν λόγω Υπηρεσία έχει οριστεί ως Εθνική Αρχή Κυβερνοασφάλειας (National Cyber Security Authority – NCSA), εποπτεύει την εφαρμογή του νόμου 4577/2018 (Α’ 199) και λειτουργεί ως το εθνικό ενιαίο σημείο επαφής για την ασφάλεια δικτύου και πληροφοριών, ενεργώντας επίσης ως σύνδεσμος διασφάλισης της διασυνοριακής συνεργασίας εντός της Ε.Ε. Με την Εθνική Στρατηγική Κυβερνοασφάλειας (η οποία δημοσιεύεται με την απόφαση από 7/3/2018 υπ’ αριθ. πρωτ. 3218/2018 του Υπουργού Ψηφιακής Διακυβέρνησης), ξεκίνησε μια σημαντική προσπάθεια αναβάθμισης του επιπέδου Κυβερνοασφάλειας των δικτύων και υπηρεσιών, καλύπτοντας συνολικά δεκατρείς (13) στόχους, σε ευθυγράμμιση με τις ευρωπαϊκές και διεθνείς πρακτικές. Επιπλέον, με τις διατάξεις του ν. 4577/2018 (Α’ 199) και της Υ.Α. υπ’ αριθμ. 1027/2019 (Β’ 3739), η νομοθεσία της χώρας μας εναρμονίσθηκε με τις διατάξεις της Οδηγίας NIS. Τα εν λόγω θεσμικά κείμενα περιλαμβάνουν, μεταξύ άλλων, τις

υποχρεώσεις των φορέων, τις βασικές απαιτήσεις ασφάλειας συστημάτων δικτύου και πληροφοριών, και προσδιορίζουν τις διαδικασίες διαμοιρασμού πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές.

Στην Ελλάδα, η εναρμόνιση του εθνικού Δικαίου με την οδηγία έγινε με τον Ν. 4577/2018 και τις διατάξεις της Υπουργικής Απόφασης υπ' αριθ. 1027/ΦΕΚΒ/3739/8.10.2019. Σκοπός του νόμου είναι η ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148, με την οποία θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφαλείας των συστημάτων δικτύου και πληροφοριών.

Οι απαιτήσεις ασφαλείας και κοινοποίησης που προβλέπονται στον νόμο αφορούν:

- Τους φορείς εκμετάλλευσης βασικών υπηρεσιών
- Τους παρόχους ψηφιακών υπηρεσιών σε κρίσιμους τομείς

Οι συγκεκριμένες απαιτήσεις έχουν αποκλειστικά δικαιώματα παροχής υπηρεσιών σε άλλες αγορές πλην των αγορών δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, στην Ελλάδα ή σε άλλο κράτος μέλος της Ε.Ε.

Ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών, σύμφωνα το Παράρτημα ΙΙ της Ευρωπαϊκής Οδηγίας (2016/1148/ΕΕ), ορίζονται οι Οργανισμοί που δραστηριοποιούνται σε 7 τομείς δραστηριότητας: την ενέργεια (ηλεκτρική ενέργεια, πετρέλαιο, φυσικό αέριο), την υγεία, το πόσιμο νερό, το τραπεζικό και χρηματοοικονομικό σύστημα, τις τηλεπικοινωνίες, τις μεταφορές (οδικές, σιδηροδρομικές, αεροπορικές, εσωτερικές πλωτές – θαλάσσιες), τους λιμένες και τις ψηφιακές υποδομές, δηλαδή cloud computing, search engines, online marketplaces.

Η Εθνική Αρχή Κυβερνοασφάλειας έχει τις εξής αρμοδιότητες:

- Παρακολουθεί την εφαρμογή του ν. 4577/2018
- Ορίζεται ως το εθνικό ενιαίο κέντρο επαφής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και παράλληλα ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών κρατών μελών
- Υποβάλλει ετησίως στην ομάδα συνεργασίας συνοπτική έκθεση αναφορικά με τις κοινοποιήσεις που έχει παραλάβει
- Συνεργάζεται με την αρμόδια CSIRT, ώστε να τηρούνται από κοινού οι υποχρεώσεις της χώρας

- Συνεργάζεται με τις Αρμόδιες Εθνικές Αρχές επιβολής του νόμου, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς και τις λοιπές αρχές και φορείς για θέματα σχετικά με την εφαρμογή του νόμου
- Συνεργάζεται με τις Αρμόδιες Αρχές των υπολοίπων κρατών μελών
- Ορίζει τους εθνικούς αντιπροσώπους της χώρας και ενημερώνει τους εμπλεκόμενος φορείς αναφορικά με τις εργασίες που λαμβάνονται
- Συνεργάζεται με διεθνείς Οργανισμούς για θέματα Κυβερνοασφάλειας και προστασίας κρίσιμων υποδομών
- Συμμετέχει σε συναντήσεις με επιτροπές και ομάδες εργασίας.

Στις αρμοδιότητες της Εθνικής Αρχής Κυβερνοασφάλειας περικλείεται η επικαιροποίηση της «Εθνικής Στρατηγικής», η οποία περιλαμβάνει:

- Τους στόχους και τις προτεραιότητες της εθνικής στρατηγικής, ώστε να παραμένουν ασφαλή τα συστήματα δικτύων και πληροφοριών
- Το πλαίσιο διακυβέρνησης ώστε να επιτυγχάνονται οι στόχοι της εθνικής στρατηγικής
- Τον προσδιορισμό των μέτρων ετοιμότητας, απόκρισης και αποκατάστασης
- Τα προγράμματα εκπαίδευσης και κατάρτισης αναφορικά με την εθνική στρατηγική ασφαλείας
- Τα σχέδια έρευνας, ανάπτυξης, αλλά και εκτίμησης κινδύνου
- Κατάλογο των διάφορων φορέων που σχετίζονται με την υλοποίηση της εθνικής στρατηγικής.

Μία άλλη ομάδα που διαδραματίζει σημαντικό ρόλο και αφορά συμβάντα σχετικά με την ασφάλεια των υπολογιστών είναι η ομάδα απόκρισης (CSIRT). Οι αρμοδιότητές της είναι:

- Η παρακολούθηση συμβάντων σε εθνικό επίπεδο
- Η παροχή προειδοποιήσεων και ανακοινώσεων
- Η παρέμβαση σε περίπτωση συμβάντος
- Η παροχή δυναμικής ανάλυσης κινδύνων και
- Η συνεργασία με τις αρχές άλλων κρατών μελών

3.2.1 Ασφάλεια δικτύου και υπηρεσιών σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών

Ειδικοί κανόνες ισχύουν για την ασφάλεια δικτύου και πληροφοριών σε ό, τι αφορά την εκμετάλλευση βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών.

Οι συγκεκριμένοι φορείς είναι υποχρεωμένοι να λάβουν μέτρα αναφορικά με την ασφάλεια των συστημάτων δικτύου, ώστε να ελαχιστοποιηθεί ο αντίκτυπος των οποιονδήποτε συμβάντων, με σκοπό να διασφαλιστεί η επιχειρησιακή συνέχεια τους.

Για τον λόγο αυτό, η Εθνική Αρχή Κυβερνοασφάλειας συνεργάζεται με την ομάδα CSIRT και άλλους εμπλεκόμενους φορείς ώστε να αξιολογήσει την καταλληλότητά τους.

Επιπλέον, καθορίζουν τη διαδικασία κοινοποίησης των φορέων για συμβάντα με σοβαρές επιπτώσεις.

Για την εφαρμογή των παραπάνω μέτρων η Εθνική Αρχή Κυβερνοασφάλειας:

- Αξιολογεί κατά πόσο συμμορφώνονται οι φορείς ως προς τις υποχρεώσεις τους και τι επιπτώσεις έχουν στην ασφάλεια των συστημάτων δικτύου και υπηρεσιών
- Απαιτεί από τους φορείς να παρέχουν τις απαραίτητες πληροφορίες για να εκτιμηθεί αν ανταποκρίνεται η ασφάλεια και παρέχει στοιχεία για την απόδειξη της εφαρμογής πολιτικών ασφαλείας.

Ωστόσο, έρευνες δείχνουν ότι η Ελλάδα έχει στοχοποιηθεί σε μικρό βαθμό. Αυτό ίσως οφείλεται στη μικρή οικονομία της, στο γεγονός ότι ακόμα δεν έχει ψηφιοποιηθεί τόσο πολύ η ζωή των Ελλήνων, αλλά και στο ότι η γλώσσα δεν είναι διαδεδομένη: Οι επιτιθέμενοι προτιμούν να κάνουν επιθέσεις/ηλεκτρονικές απάτες στα αγγλικά, ισπανικά, γαλλικά κτλ)».

Επομένως, δεν έχουν σημειωθεί αξιοσημείωτα περιστατικά στην Ελλάδα. Έχουν καταγραφεί μόνο επιθέσεις σε ιστοσελίδες μεγάλων τραπεζών και υπουργείων και συγκεκριμένα όχι στα συστήματά τους, αλλά μόνο στις ιστοσελίδες τους.

Ειδικότερα, επρόκειτο για επιθέσεις με τη μέθοδο DDoS (distributed denial of service): Πρόκειται για μια μέθοδο επιθέσεων μέσω διαφόρων προγραμμάτων, με στόχο να προκληθεί η «κατάρρευση» μιας διαδικτυακής υπηρεσίας ή ενός εξυπηρετητή (server). Μια τέτοια κατάρρευση σημαίνει πως ο στόχος αδυνατεί να εξυπηρετήσει τις απαιτήσεις ενός χρήστη. Σε μία DDoS επίθεση, ο υπολογιστής (attacker) αποστέλλει μεγάλο πλήθος δεδομένων (πακέτων) στο επιτιθέμενο δίκτυο (server ή website) με αποτέλεσμα να το υπερφορτώσει ή να το αναγκάσει να επανεκκινήσει τη λειτουργία του, με συνέπεια την απώλεια δεδομένων).

Οι Hackers χτυπούν τη σελίδα μίας τράπεζας, προσπαθώντας να δημιουργήσουν δυσπιστία. Δε μπορούν όμως να χτυπήσουν τα συστήματά τους. Στόχος είναι ο εντυπωσιασμός ή τα λύτρα.

Η Ελλάδα όμως, δεν έχει απειληθεί από κυβερνοτρομοκράτες, ούτε έχει παρατηρηθεί κάποια αξιοσημείωτη/συντεταγμένη δραστηριότητα σε επίπεδο προπαγάνδας μέσω κυβερνοχώρου με στόχο την Ελλάδα. Γενικότερα, δεν υπάρχουν ενδείξεις πως η χώρα μας διατρέχει κάποιον σημαντικό κίνδυνο από κυβερνοαπειλές.

Ωστόσο, η παραβίαση προσωπικών δεδομένων, η διαρροή απόρρητων πληροφοριών και διαβαθμισμένων εγγράφων, οι τηλεφωνικές υποκλοπές, η παράνομη πρόσβαση σε σημαντικές και αξιοποιήσιμες πληροφορίες σχετικά με τα προσωπικά δεδομένα πολιτών είναι μερικά από τα περιστατικά που αντιμετωπίζει συχνά η χώρα μας. Κύριοι στόχοι των επιθέσεων είναι κυρίως οι κυβερνητικοί φορείς, οι τράπεζες, ακόμα και οι απλοί πολίτες. Η σκοπιμότητα ποικίλει και σχετίζεται με την εναντίωση σε πολιτικά μέτρα, την απόπειρα υποκλοπής δεδομένων, τον εκβιασμό και άλλες κακόβουλες ενέργειες.

3.3 Η Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα – Κανονιστικό Πλαίσιο

Μία πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος είχε λάβει χώρα το 1976 από το Συμβούλιο της Ευρώπης στο Στρασβούργο στο πλαίσιο των εργασιών του Συνεδρίου για τις εγκληματολογικές πλευρές του Οικονομικού Εγκλήματος.

Στην Ελλάδα η εξέλιξη στη 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 εν τέλει 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. Η προφύλαξη των συστημάτων των πληροφοριών, που καθημερινά και σε μέγιστο βαθμό ασκούν επιρροή στην ζωή μας, είναι πρωτίστης σημασίας και εξ αυτού του λόγου έχουν γίνει αξιοσημείωτες ενέργειες προς αυτή την κατεύθυνση. Σε διεθνές και ευρωπαϊκό επίπεδο οι ενέργειες αυτές έχουν λάβει χώρα με την θέσπιση σχετικών νομοθετημάτων πριν από αρκετά χρόνια, ενώ στην Ελλάδα η αντίστοιχη θεσμοθέτηση καθυστέρησε.

Το πιο σημαντικό συνεπώς βήμα για την καταπολέμηση της εγκληματικότητας στο διαδίκτυο είναι η Σύμβαση της Βουδαπέστης. Υπογράφηκε στις 23/11/2001, όχι μόνο από τις χώρες που είναι μέλη του Συμβουλίου της Ευρώπης, αλλά και από τρίτες χώρες και αποτελεί μια δεσμευτική διεθνή νομική πράξη που αφορά τα εγκλήματα που διαπράττονται κατά ή μέσω ηλεκτρονικών δικτύων.

Η Σύμβαση περιλαμβάνει 4 κατηγορίες αδικημάτων, για τα οποία τα συμβαλλόμενα κράτη μέλη πρέπει να θεσπίσουν τα κατάλληλα μέτρα.

Η πρώτη κατηγορία εμπεριέχει τα εξής αδικήματα:

- Παράνομη πρόσβαση στο σύνολο ή μέρος ενός ηλεκτρονικού υπολογιστή
- Παράνομη υποκλοπή δεδομένων
- Καταστροφή ή αλλοίωση δεδομένων
- Καταστροφή ή αλλοίωση του συστήματος
- Παράνομη παραγωγή και πώληση συσκευής ή κωδικών πρόσβασης

Η δεύτερη κατηγορία περιλαμβάνει τα εξής αδικήματα:

- Πλαστογραφία αναφορικά με τους ηλεκτρονικούς υπολογιστές
- Απάτη με ηλεκτρονικούς υπολογιστές εις βάρος τρίτων για αποκόμιση οικονομικού οφέλους

Η τρίτη κατηγορία σχετίζεται με το περιεχόμενο και αφορά το αδίκημα της παιδικής πορνογραφίας.

Η τέταρτη κατηγορία αφορά αδικήματα σχετικά με την παραβίαση της πνευματικής ιδιοκτησίας.

Επιπρόσθετα, η Σύμβαση περιλαμβάνει και δικονομικές διατάξεις. Σε αυτές συμπεριλαμβάνεται:

- Η διατήρηση δεδομένων που είναι αποθηκευμένα σε έναν ηλεκτρονικό υπολογιστή, έως και 90 μέρες και το δικαίωμα ταχείας πρόσβασης σε αυτά
- Η έκδοση διάταξης που υποχρεώνει ένα πρόσωπο να προσκομίσει στις αρχές δεδομένα που είναι αποθηκευμένα σε έναν ηλεκτρονικό υπολογιστή
- Η εξουσία των αρχών για αναζήτηση δεδομένων που είναι αποθηκευμένα σε ένα σύστημα ηλεκτρονικού υπολογιστή ή σε ένα φορητό μέσο.

Οι υπόλοιπες διατάξεις της Σύμβασης αναφέρονται σε ζητήματα δικαιοδοσίας και στη διεθνή συνεργασία μεταξύ των διωκτικών αρχών.

4 Η κυβερνοασφάλεια εν μέσω πανδημίας (Covid-19)

Η πανδημία του κορωνοϊού επιτάχυνε τον ψηφιακό μετασχηματισμό της οικονομίας και της κοινωνίας, καθώς έφερε νέες ευκαιρίες και προκλήσεις στο προσκήνιο, οι οποίες απαιτούν προσαρμοσμένες και καινοτόμες απαντήσεις. 125 δισεκατομμύρια συσκευές θα έχουν συνδεθεί στο διαδίκτυο μέχρι το 2030, από 27 δισεκατομμύρια το 2021, και το 90% των ανθρώπων άνω των 6 ετών εκτιμάται ότι θα έχει διαδικτυακή παρουσία. Ο κυβερνοχώρος από την φύση του βασίζεται στη διασύνδεση των κοινοτήτων κάθε μορφής και καθώς ο ψηφιακός και φυσικός κόσμος είναι όλο και πιο αλληλένδετοι, προκύπτουν νέοι κίνδυνοι.

Όλο και περισσότερος κόσμος χρησιμοποιεί ψηφιακά εργαλεία στην καθημερινότητά του. Η τηλεργασία, οι διαδικτυακές αγορές και η επικοινωνία μέσω διαδικτύου αύξησαν τη ζήτησή τους κατακόρυφα κατά την περίοδο του εγκλεισμού. Οι ψηφιακές αυτές λύσεις μπορούν να είναι ωφέλιμες για τους καταναλωτές και να συμβάλουν στην ανάκαμψη της οικονομίας από τον κορωνοϊό. Στον αντίποδα βρίσκεται, ωστόσο, η αύξηση των κακόβουλων διαδικτυακών δραστηριοτήτων. Ο αριθμός των κυβερνοεπιθέσεων εξακολουθεί να αυξάνεται, καθώς εξαπολύονται ολοένα και πιο εξελιγμένες επιθέσεις από ένα ευρύ φάσμα πηγών εντός και εκτός της Ευρωπαϊκής Ένωσης.

Από την έναρξη ισχύος της Οδηγίας (ΕΕ) 2016/1148, παρατηρήθηκε σημαντική πρόοδος όσον αφορά την αύξηση του επιπέδου ανθεκτικότητας της κυβερνοασφάλειας στην ΕΕ. Διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων με τον καθορισμό εθνικών στρατηγικών Κυβερνοασφάλειας, τη θέσπιση εθνικών ικανοτήτων και την εφαρμογή ρυθμιστικών μέτρων που καλύπτουν βασικές υποδομές και φορείς που προσδιορίζονται από κάθε κράτος μέλος.

Η νομική βάση της Οδηγίας 1148/2014/ΕΕ ήταν το άρθρο 114 της Συνθήκης για τη λειτουργία της ΕΕ (ΣΛΕΕ), στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για την προσέγγιση των εθνικών κανόνων.

Ωστόσο, τα δικτυακά και πληροφοριακά συστήματα έχουν εξελιχθεί σε κεντρικό σημείο της καθημερινότητάς μας με τον ταχύ ψηφιακό μετασχηματισμό και τη διασύνδεση της κοινωνίας, μεταξύ άλλων, στις διασυνοριακές συναλλαγές. Η εξέλιξη αυτή έχει οδηγήσει σε επέκταση του τοπίου των απειλών για την Κυβερνοασφάλεια,

γεγονός που απαιτεί ετοιμότητα και αποτελεσματικότητα, ώστε να διασφαλιστεί η εύρυθμη και ασφαλής λειτουργία της εσωτερικής αγοράς.

4.1 Κυβερνοασφάλεια της Ε.Ε.

Στις 16/12/2020 δημοσιεύθηκε η νέα στρατηγική της Ε.Ε. για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων. Ο στόχος της νέας στρατηγικής είναι να ενισχύσει τη συλλογική ανθεκτικότητα της Ευρώπης απέναντι στις κυβερνοαπειλές και να προβεί στη διασφάλιση πως όλοι οι πολίτες και οι επιχειρήσεις θα έχουν τη δυνατότητα να επωφεληθούν ολοκληρωτικά από αξιόπιστες υπηρεσίες και αξιόπιστα ψηφιακά εργαλεία.

Η νέα στρατηγική για την κυβερνοασφάλεια δίνει επίσης στην ΕΕ τη δυνατότητα να ενισχύσει τον ηγετικό της ρόλο όσον αφορά τους διεθνείς κανόνες και τα διεθνή πρότυπα στον κυβερνοχώρο και να εντείνει τη συνεργασία με εταίρους σε ολόκληρο τον κόσμο για την προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου, βασισμένου στο κράτος δικαίου, τα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες και τις δημοκρατικές αξίες.

Η νέα στρατηγική βασιζόμενη στα επιτεύγματα των τελευταίων μηνών και ετών περιέχει συγκεκριμένες προτάσεις αναφορικά με επενδυτικές, κανονιστικές και πρωτοβουλίες πολιτικής, σε 3 τομείς δράσης της Ε.Ε:

1. Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγετική θέση

Η Ευρωπαϊκή Επιτροπή προτείνει τη μεταρρύθμιση των κανόνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, βάσει οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, ώστε να αυξηθεί το επίπεδο κυβερνοανθεκτικότητας των κρίσιμων ιδιωτικών και δημόσιων τομέων.

Η Επιτροπή προτείνει επίσης τη δημιουργία ενός δικτύου κέντρων επιχειρήσεων ασφάλειας σε ολόκληρη την ΕΕ, που θα τροφοδοτείται από την τεχνητή νοημοσύνη (ΤΝ), και το οποίο θα αποτελεί πραγματική «ασπίδα κυβερνοασφάλειας» για την ΕΕ, ικανή να εντοπίζει εγκαίρως ενδείξεις κυβερνοεπίθεσης και να καθιστά δυνατή την ανάληψη προορατικής δράσης πριν από την πρόκληση βλάβης.

2. Ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντιμετώπισης

Η Επιτροπή προετοιμάζει μια νέα Κοινή Μονάδα Κυβερνοχώρου, με σκοπό να ενισχύσει την συνεργασία μεταξύ των οργάνων της ΕΕ και των αρχών των κρατών μελών που έχουν την αρμοδιότητα πρόληψης, αποτροπής και αντιμετώπισης κυβερνοεπιθέσεων, συμπεριλαμβανομένων των μη στρατιωτικών και διπλωματικών κοινοτήτων, καθώς και των κοινοτήτων επιβολής του νόμου και κυβερνοάμυνας. Ο ύπατος εκπρόσωπος υποβάλλει προτάσεις για την ενίσχυση της εργαλειοθήκης της ΕΕ και για τη διπλωματία στον κυβερνοχώρο με σκοπό την αποτελεσματική πρόληψη, αποθάρρυνση, αποτροπή και αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, ιδίως εκείνων που επηρεάζουν τις υποδομές ζωτικής σημασίας, τις αλυσίδες εφοδιασμού, τους δημοκρατικούς θεσμούς και τις δημοκρατικές διαδικασίες μας.

3. Προώθηση ενός παγκόσμιου και ανοιχτού κυβερνοχώρου μέσω αυξημένης συνεργασίας

Η ΕΕ θα εντείνει τη συνεργασία της με τους διεθνείς εταίρους για την ενίσχυση της παγκόσμιας τάξης που βασίζεται σε κανόνες, θα προωθήσει τη διεθνή ασφάλεια και σταθερότητα στον κυβερνοχώρο, και θα προστατεύσει τα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες στο διαδίκτυο.

Θα προωθήσει διεθνείς κανόνες και πρότυπα που αντικατοπτρίζουν αυτές τις βασικές αξίες της ΕΕ, συνεργαζόμενη με τους διεθνείς εταίρους της στα Ηνωμένα Έθνη και σε άλλα σχετικά φόρουμ. Επιπλέον, θα ενισχύσει περαιτέρω την εργαλειοθήκη της για τη διπλωματία στον κυβερνοχώρο και θα εντείνει τις προσπάθειες ανάπτυξης ικανοτήτων σε τρίτες χώρες με την εκπόνηση ενός θεματολογίου σχετικού με την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ.

Τέλος, η ΕΕ θα δημιουργήσει δίκτυο για τη διπλωματία στον κυβερνοχώρο σε ολόκληρο τον κόσμο με σκοπό να προωθήσει το όραμά της γι’ αυτόν.

Τα μέτρα που λαμβάνει η Ε.Ε. αποσκοπούν στην προστασία των βασικών υπηρεσιών και υποδομών για την αποφυγή κυβερνοεπιθέσεων.

Η οδηγία (NIS2) που έχει ληφθεί σχετικά με την ανθεκτικότητα των κρίσιμων υποδομών καλύπτει πλέον 10 τομείς:

- ενέργεια
- μεταφορές
- τράπεζες

- υποδομές χρηματοπιστωτικών αγορών
- υγεία
- πόσιμο νερό
- λύματα
- ψηφιακή υποδομή
- δημόσια διοίκηση και διάστημα.

Βάσει της προτεινόμενης ως άνω Οδηγίας, κάθε κράτος μέλος θα εγκρίνει εθνική στρατηγική για να διασφαλιστεί η ανθεκτικότητα των κρίσιμων οντοτήτων και θα διενεργεί τακτικές εκτιμήσεις κινδύνου.

4.1.1 Κυβερνοασφάλεια των δικτύων 5ης γενιάς (5G)

Η Ευρωπαϊκή Επιτροπή ενέκρινε την κοινή εργαλειοθήκη μέτρων μετριασμού που συμφωνήθηκε από τα κράτη μέλη της ΕΕ για την αντιμετώπιση των κινδύνων για την ασφάλεια που σχετίζονται με την ανάπτυξη των δικτύων 5G, της πέμπτης γενιάς δικτύων κινητών επικοινωνιών.

Μέσω της εργαλειοθήκης, τα κράτη μέλη δεσμεύονται να κάνουν μαζί τα επόμενα βήματα βάσει αντικειμενικής αξιολόγησης των προσδιορισθέντων κινδύνων και αναλογικών μέτρων μετριασμού.

Κατά την άποψη της Μαργκρέιτε Βέστεϊγιερ, Εκτελεστικής Αντιπροέδρου για μια Ευρώπη Έτοιμη για την Ψηφιακή Εποχή, η συγκεκριμένη τεχνολογία υποστηρίζει την εξατομικευμένη ιατρική, τη γεωργία ακριβείας, καθώς και ενεργειακά δίκτυα που μπορούν να ενσωματώσουν ενέργεια από όλες τις ανανεώσιμες πηγές. Οι επιπτώσεις της εν λόγω τεχνολογίας θα είναι θετικές, υπό την προϋπόθεση όμως ότι οι χρήστες μπορούν να εγγυηθούν την ασφάλεια των δικτύων τους, έτσι ώστε να επωφεληθούν όλοι από τις ψηφιακές αλλαγές, χωρίς να υπονομεύσουν την ασφάλεια της εσωτερικής αγοράς.

Το 5G αποτελεί μια ρηξικέλευθη τεχνολογία, με έσοδα που εκτιμάται ότι θα ανέρχονται σε 225 δισ. ευρώ το 2025 παγκοσμίως, αποτελεί βασικό πλεονέκτημα για την ανταγωνιστικότητα της Ευρώπης στην παγκόσμια αγορά και η κυβερνοασφάλεια στον τομέα αυτό είναι καίριας σημασίας, ώστε να διασφαλιστεί η στρατηγική αυτονομία της Ένωσης. Αφορά δισεκατομμύρια συνδεδεμένα αντικείμενα και συστήματα, μεταξύ των οποίων συγκαταλέγονται και κρίσιμοι τομείς όπως:

- η ενέργεια

- οι μεταφορές
- οι τραπεζικές συναλλαγές
- η υγεία
- συστήματα βιομηχανικού ελέγχου που μεταφέρουν ευαίσθητες πληροφορίες και υποστηρίζουν συστήματα ασφαλούς λειτουργίας.

Ταυτόχρονα, τα δίκτυα 5G προσφέρουν περισσότερα δυνητικά σημεία εισόδου για όσους θέλουν να επιτεθούν λόγω της πιο αποκεντρωμένης αρχιτεκτονικής τους, της έξυπνης υπολογιστικής ισχύος στις παρυφές του δικτύου, της ανάγκης για περισσότερες κεραίες και της αυξημένης εξάρτησής τους από λογισμικό. Οι απειλές για την κυβερνοασφάλεια αυξάνονται και γίνονται όλο και περισσότερο πολύπλοκες. Δεδομένου ότι πολλές κρίσιμες υπηρεσίες θα εξαρτώνται από το 5G, η εγγύηση της ασφάλειας των δικτύων είναι ύψιστης στρατηγικής σημασίας για ολόκληρη την ΕΕ.

Η Επιτροπή θα παραμείνει ενωμένη όσον αφορά την κυβερνοασφάλεια των δικτύων 5G και θα αναλάβει δράση, όπως ζητήθηκε από τα κράτη μέλη, χρησιμοποιώντας, ανάλογα με την περίπτωση, όλα τα μέσα που έχει στη διάθεσή της για να εγγυηθεί την ασφάλεια των υποδομών και της αλυσίδας εφοδιασμού 5G, όπως:

- κανόνες για τις τηλεπικοινωνίες και την κυβερνοασφάλεια·
- συντονισμό στους τομείς της τυποποίησης και της πιστοποίησης σε επίπεδο ΕΕ·
- πλαίσιο ελέγχου των άμεσων ξένων επενδύσεων για την προστασία της ευρωπαϊκής αλυσίδας εφοδιασμού 5G·
- μέσα εμπορικής άμυνας·
- κανόνες ανταγωνισμού·
- δημόσιες συμβάσεις, εξασφαλίζοντας ότι λαμβάνονται δεόντως υπόψη οι πτυχές που αφορούν την ασφάλεια
- προγράμματα χρηματοδότησης της ΕΕ, εξασφαλίζοντας ότι οι δικαιούχοι συμμορφώνονται με τις σχετικές απαιτήσεις ασφάλειας.

4.1.2 Η οδηγία NIS και NIS2

Η οδηγία υπ' αρ. 2016/1148 για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (γνωστή και ως NIS – Network and Information Systems) παρέχει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην ΕΕ, αλλά και αναφορικά με τα ΝΑΚ [Νέα Ανεξάρτητα Κράτη (πρώην ΕΣΣΔ)], διασφαλίζοντας:

- την ετοιμότητα των κρατών μελών, απαιτώντας τον κατάλληλο εξοπλισμό τους.
- την συνεργασία μεταξύ όλων των κρατών μελών, με τη σύσταση ομάδας συνεργασίας για τη στήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών.
- μια κουλτούρα ασφάλειας σε όλους τους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία μας, όπως η ενέργεια, οι μεταφορές, το νερό, οι τράπεζες, οι υποδομές των χρηματοπιστωτικών αγορών, η υγειονομική περίθαλψη και οι ψηφιακές υποδομές.

Οι επιχειρήσεις που προσδιορίζονται από τα κράτη μέλη ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) στους ανωτέρω τομείς θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας και να ενημερώνουν τις αρμόδιες εθνικές αρχές για σοβαρά συμβάντα.

Καθώς το τοπίο της απειλής για την κυβερνοασφάλεια εξελίσσεται με ταχείς ρυθμούς, ήταν αναγκαίο να εφαρμοστεί γρήγορα η οδηγία για τα ΝΑΚ.

Το άρθρο 23 της Οδηγίας απαιτεί από την Ευρωπαϊκή Επιτροπή να επανεξετάζει περιοδικά τη λειτουργία της. Στο πλαίσιο του βασικού στόχου πολιτικής της να καταστήσει την Ευρώπη κατάλληλη για την ψηφιακή εποχή, καθώς και σύμφωνα με τους στόχους της Ένωσης Ασφάλειας, η Επιτροπή ανακοίνωσε στο πρόγραμμα εργασίας της για το 2020 ότι θα διενεργήσει την επανεξέταση έως το τέλος του 2020.

Ως αποτέλεσμα της διαδικασίας επανεξέτασης, η νέα νομοθετική πρόταση κατατέθηκε από την Επιτροπή της ΕΕ στις 16 Δεκεμβρίου 2020[10].

Από την αξιολόγηση της λειτουργίας της Οδηγίας NIS (2016/1148), εντοπίστηκαν τα ακόλουθα ζητήματα:

1) Χαμηλό επίπεδο κυβερνοανθεκτικότητας των επιχειρήσεων που δραστηριοποιούνται στην ΕΕ, 2) διαφορές όσον αφορά την ανθεκτικότητα μεταξύ κρατών μελών και τομέων, 3) χαμηλό επίπεδο κοινής επίγνωσης της κατάστασης και έλλειψη κοινής αντιμετώπισης των κρίσεων. Ένα τρανό παράδειγμα είναι ότι ορισμένα μεγάλα νοσοκομεία σε ένα κράτος μέλος δεν εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας NIS και ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν τα ανάλογα μέτρα ασφάλειας, ενώ σε ένα άλλο κράτος μέλος σχεδόν όλοι οι πάροχοι υγειονομικής περίθαλψης στη χώρα καλύπτονται από τις απαιτήσεις ασφάλειας της οδηγίας NIS.

10 COM(2020) 823 final

Η Επιτροπή προέβη σε αξιολόγηση της λειτουργίας της οδηγίας NIS[11]. Ανέλυσε τη συνάφεια, την ενωσιακή προστιθέμενη αξία, τη συνοχή, την αποτελεσματικότητα και την αποδοτικότητά της. Τα κυριότερα συμπεράσματα της ανάλυσης έχουν ως εξής:

- Το πεδίο εφαρμογής της οδηγίας NIS είναι υπερβολικά περιορισμένο όσον αφορά τους τομείς που καλύπτει, κυρίως λόγω i) της αυξημένης ψηφιοποίησης κατά τα τελευταία έτη και του υψηλότερου βαθμού διασύνδεσης, και ii) του πεδίου εφαρμογής της οδηγίας NIS, το οποίο δεν καλύπτει πλέον όλους τους ψηφιοποιημένους τομείς που παρέχουν βασικές υπηρεσίες στην οικονομία και την κοινωνία στο σύνολό της.
- Η οδηγία NIS δεν είναι επαρκώς σαφής όσον αφορά το πεδίο εφαρμογής για τους φορείς εκμετάλλευσης βασικών υπηρεσιών, αλλά και την εθνική αρμοδιότητα επί των παρόχων ψηφιακών υπηρεσιών. Αυτό οδήγησε σε μια κατάσταση στην οποία ορισμένα είδη οντοτήτων δεν έχουν προσδιοριστεί σε όλα τα κράτη μέλη και, ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν μέτρα ασφάλειας και να αναφέρουν περιστατικά.
- Η οδηγία NIS παρείχε ευρεία διακριτική ευχέρεια στα κράτη μέλη κατά τον καθορισμό απαιτήσεων όσον αφορά την ασφάλεια και την αναφορά περιστατικών για τους φορείς εκμετάλλευσης βασικών υπηρεσιών. Από την αξιολόγηση προκύπτει ότι, σε ορισμένες περιπτώσεις, τα κράτη μέλη έχουν εφαρμόσει τις απαιτήσεις αυτές με πολύ διαφορετικούς τρόπους, γεγονός που δημιουργεί πρόσθετη επιβάρυνση για τις εταιρείες που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη.
- Το καθεστώς εποπτείας και επιβολής της οδηγίας NIS είναι αναποτελεσματικό. Για παράδειγμα, τα κράτη μέλη ήταν πολύ απρόθυμα να επιβάλουν κυρώσεις σε οντότητες που δεν έχουν θεσπίσει απαιτήσεις ασφάλειας ή δεν αναφέρουν περιστατικά. Αυτό μπορεί να έχει αρνητικές συνέπειες για την κυβερνοανθεκτικότητα μεμονωμένων οντοτήτων.
- Οι οικονομικοί και ανθρώπινοι πόροι που διαθέτουν τα κράτη μέλη για την εκπλήρωση των καθηκόντων τους (όπως ο προσδιορισμός ή η εποπτεία των φορέων εκμετάλλευσης βασικών υπηρεσιών) και, κατά συνέπεια, τα διαφορετικά επίπεδα ωριμότητας όσον αφορά την αντιμετώπιση των κινδύνων κυβερνοασφάλειας, ποικίλλουν σε μεγάλο βαθμό. Αυτό εντείνει περαιτέρω τις διαφορές όσον αφορά την κυβερνοανθεκτικότητα μεταξύ των κρατών μελών.
- Τα κράτη μέλη δεν ανταλλάσσουν συστηματικά πληροφορίες μεταξύ τους, γεγονός που έχει αρνητικές συνέπειες ιδίως για την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας και για το επίπεδο κοινής επίγνωσης της κατάστασης στο σύνολο της ΕΕ. Το ίδιο ισχύει και για την ανταλλαγή πληροφοριών μεταξύ ιδιωτικών οντοτήτων, αλλά και για τη συνεργασία μεταξύ των δομών συνεργασίας σε επίπεδο ΕΕ και των ιδιωτικών οντοτήτων.

11 Παράρτημα 5 της εκτίμησης επιπτώσεων

Στον τομέα της υλικής ασφάλειας, η πρόταση συμπληρώνει την πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων, η οποία αναθεωρεί την οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (οδηγία ECI), η οποία θεσπίζει ενωσιακή διαδικασία για τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και καθορίζει προσέγγιση για τη βελτίωση της προστασίας τους.

Τον Ιούλιο του 2020, η Επιτροπή ενέκρινε τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας[12], με την οποία αναγνωρίζεται η αυξανόμενη διασύνδεση και αλληλεξάρτηση μεταξύ υλικών και ψηφιακών υποδομών. Η στρατηγική υπογράμμισε την ανάγκη για μια πιο συνεκτική και συνεπή προσέγγιση μεταξύ της οδηγίας ECI και της οδηγίας (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων σε ολόκληρη την Ένωση.

Ως εκ τούτου, η πρόταση ευθυγραμμίζεται άμεσα με την πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων, η οποία αποσκοπεί στην ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων έναντι υλικών απειλών σε μεγάλο αριθμό τομέων.

Η πρόταση έχει ως στόχο να διασφαλίσει ότι, δυνάμει αμφότερων των νομικών πράξεων, οι αρμόδιες αρχές λαμβάνουν συμπληρωματικά μέτρα και ανταλλάσσουν πληροφορίες, ανάλογα με τις ανάγκες, όσον αφορά την ανθεκτικότητα εντός και εκτός κυβερνοχώρου, και ότι οι ιδιαίτερα κρίσιμοι φορείς εκμετάλλευσης στους τομείς που θεωρούνται «βασικοί», κατά την παρούσα πρόταση, υπέχουν επίσης γενικότερες υποχρεώσεις ενίσχυσης της ανθεκτικότητας, με έμφαση στους κινδύνους που δε σχετίζονται με τον κυβερνοχώρο.

Η πρόταση αποτελεί μέρος δέσμης μέτρων για να βελτιωθούν περισσότερο οι ικανότητες ανθεκτικότητας και να αντιμετωπιστούν αποτελεσματικά τα περιστατικά δημόσιων και ιδιωτικών φορέων, αρμόδιων αρχών και της ΕΕ στο σύνολό της.

Επιπρόσθετα, η πρόταση καλύπτει τον τομέα της κυβερνοασφάλειας και της προστασίας των υποδομών ζωτικής σημασίας, αφού συμφωνεί με τις προτεραιότητες της

12 COM(2020) 605 final

Επιτροπής να καταστήσει την Ευρώπη κατάλληλη για την ψηφιακή εποχή και να οικοδομήσει μια οικονομία έτοιμη για ένα μέλλον που θα λειτουργεί για τους ανθρώπους.

Η πρόταση βασίζεται και καταργεί την ισχύουσα οδηγία για τα ΝΑΚ. Εκσυγχρονίζει το υφιστάμενο νομικό πλαίσιο λαμβάνοντας υπόψη την αυξημένη ψηφιοποίηση της εσωτερικής αγοράς τα τελευταία χρόνια και ένα εξελισσόμενο τοπίο απειλών για την κυβερνοασφάλεια.

Κατά συνέπεια, θα εξορθολογίσει περαιτέρω τις υποχρεώσεις που επιβάλλονται στις επιχειρήσεις και θα αυξήσει το επίπεδο εναρμόνισής τους. Ταυτοχρόνως, η πρόταση έχει ως στόχο να παράσχει στα κράτη μέλη την απαιτούμενη ευελιξία, ώστε να λαμβάνουν υπόψη τις εθνικές ιδιαιτερότητες (όπως η δυνατότητα εντοπισμού πρόσθετων βασικών ή σημαντικών οντοτήτων που υπερβαίνουν το βασικό σενάριο που καθορίζεται στη νομική πράξη). Ως εκ τούτου, το μελλοντικό νομικό μέσο θα πρέπει να είναι Οδηγία, δεδομένου ότι αυτός ο νομικός τύπος επιτρέπει τη στοχευμένη βελτίωση της εναρμόνισης, αλλά και έναν ορισμένο βαθμό ευελιξίας για τις αρμόδιες Αρχές.

4.1.3 Το Ευρωπαϊκό Κέντρο Ικανοτήτων Κυβερνοασφάλειας

Στις 9 Δεκεμβρίου 2021 εγκρίθηκε και συστάθηκε το Ευρωπαϊκό Κέντρο Ικανοτήτων Κυβερνοασφάλειας και το Δίκτυο Εθνικών Κέντρων Συντονισμού. Επιλέχθηκε ως έδρα του το Βουκουρέστι της Ρουμανίας. Ως στόχο έχει να βελτιωθεί ο συντονισμός της έρευνας και της καινοτομίας στον τομέα της κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης και να προωθηθούν επενδύσεις με σκοπό την ερευνητική, τεχνολογική και βιομηχανική ανάπτυξη στον εν λόγω τομέα.

Επιπρόσθετα, το Κέντρο Ικανοτήτων συμβάλλει στην υλοποίηση του προγράμματος για την Ψηφιακή Ευρώπη που σχετίζεται με την κυβερνοασφάλεια και παράλληλα θα προσφέρει βοήθεια και θα συντονίζει το έργο των Εθνικών Κέντρων Συντονισμού.

Επίσης, ενισχύει τη γνώση και τις υποδομές στον τομέα της κυβερνοασφάλειας και βρίσκεται στην υπηρεσία της βιομηχανίας, του δημοσίου τομέα και των ερευνητικών κοινοτήτων.

Τέλος, προβαίνει σε χρηματοδοτήσεις που σχετίζονται με τα παραπάνω, υπό μορφή επιχορήγησης ή βραβείων.

4.1.4 Ψηφιακή Ευρώπη

Το πρόγραμμα «Ψηφιακή Ευρώπη» (DIGITAL) είναι ένα νέο πρόγραμμα χρηματοδότησης της ΕΕ που επικεντρώνεται στην εισαγωγή της ψηφιακής τεχνολογίας στις επιχειρήσεις, τους πολίτες και τις δημόσιες διοικήσεις. Έχει σχεδιαστεί για να γεφυρώσει το χάσμα μεταξύ της έρευνας στον τομέα της ψηφιακής τεχνολογίας και της διείσδυσης στην αγορά.

Η Ευρωπαϊκή Επιτροπή έχει ξεκινήσει συζητήσεις σε ότι αφορά τη μετάβαση σε έναν πιο ψηφιακό κόσμο, την ψηφιακή μετάβαση. Τόσο η ψηφιακή τεχνολογία όσο και οι υποδομές κατέχουν πολύ σημαντικό ρόλο στην ιδιωτική ζωή, αλλά και στο επιχειρησιακό περιβάλλον των ανθρώπων.

Ταυτόχρονα, η πανδημία Covid-19 υπερθεμάτισε το πόσο βασίζονται οι άνθρωποι στην τεχνολογία, αλλά και πόσο σημαντικό είναι για την Ευρώπη να μην εξαρτάται από συστήματα προερχόμενα από άλλες περιοχές του κόσμου, αλλά να βρίσκει λύσεις στηριζόμενη στις δυνάμεις της. Έτσι, το πρόγραμμα "Ψηφιακή Ευρώπη" (DIGITAL), ανοίγει τον δρόμο για την επίτευξη αυτού του στόχου.

Το πρόγραμμα θα παρέχει στρατηγική χρηματοδότηση για την αντιμετώπιση των προκλήσεων και θα υποστηρίζει έργα σε 5 βασικούς τομείς δυναμικότητας:

- στον υπερυπολογισμό
- την τεχνητή νοημοσύνη
- την κυβερνοασφάλεια
- τις προηγμένες ψηφιακές δεξιότητες.

Με αυτόν τον τρόπο θα διασφαλίζει την ευρεία χρήση των ψηφιακών τεχνολογιών σε ολόκληρη οικονομία και την κοινωνία, μέσω των Κόμβων Ψηφιακής Καινοτομίας.

Με προγραμματισμένο συνολικό προϋπολογισμό 7,5 δισεκατομμυρίων ευρώ, αποσκοπεί στην επιτάχυνση της οικονομικής ανάκαμψης και στη διαμόρφωση του ψηφιακού μετασχηματισμού της κοινωνίας και της οικονομίας της Ευρώπης, αποφέροντας οφέλη σε όλους, αλλά ιδίως στις μικρές και μεσαίες επιχειρήσεις.

Στο ψήφισμά[13] του σχετικά με την ψηφιοποίηση της ευρωπαϊκής βιομηχανίας, το Ευρωπαϊκό Κοινοβούλιο υπογράμμισε τη σημασία μιας κοινής ευρωπαϊκής προσέγγισης για την κυβερνοασφάλεια και αναγνώρισε την ανάγκη ευαισθητοποίησης. Χαρακτήρισε

13 ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2021/694/29.04.2021

την κυβερνοανθεκτικότητα ως βασική ευθύνη των ηγετικών στελεχών των επιχειρήσεων και των ευρωπαίων και εθνικών υπευθύνων χάραξης πολιτικής για τη βιομηχανική ασφάλεια, όπως και την εφαρμογή της ασφάλειας και της ιδιωτικότητας εκ σχεδιασμού και εξ ορισμού.

Η κυβερνοασφάλεια αποτελεί πρόκληση για ολόκληρη την Ένωση, η οποία δε μπορεί να αντιμετωπιστεί μόνο με εθνικές πρωτοβουλίες. Οι δυνατότητες της Ευρώπης όσον αφορά την κυβερνοασφάλεια θα πρέπει να ενισχυθούν, ώστε να εφοδιαστεί η Ευρώπη με τις απαραίτητες δυνατότητες για την προστασία των πολιτών, των δημόσιων διοικήσεων και των επιχειρήσεων από τις κυβερνοαπειλές. Επιπλέον, οι καταναλωτές θα πρέπει να προστατεύονται όταν χρησιμοποιούν συνδεδεμένα προϊόντα που μπορούν να παραβιαστούν και να θέσουν σε κίνδυνο την ασφάλειά τους. Η προστασία αυτή θα πρέπει να επιτευχθεί από κοινού με τα κράτη μέλη και τον ιδιωτικό τομέα με την ανάπτυξη έργων που ενισχύουν τις δυνατότητες της Ευρώπης στον τομέα της κυβερνοασφάλειας, με την εξασφάλιση του συντονισμού μεταξύ των εν λόγω έργων και με την εξασφάλιση της ευρείας εκδίπλωσης των πλέον σύγχρονων λύσεων στον τομέα της κυβερνοασφάλειας σε ολόκληρη την οικονομία συμπεριλαμβανομένων έργων, υπηρεσιών, δεξιοτήτων και εφαρμογών διπλής χρήσεως, καθώς και με τη συγκέντρωση δεξιοτήτων στο πεδίο αυτό, για να εξασφαλιστεί κρίσιμη μάζα και αριστεία.

Τον Σεπτέμβριο του 2017 η Επιτροπή υπέβαλε δέσμη πρωτοβουλιών με την οποία παρουσίασε μια ολοκληρωμένη ενωσιακή προσέγγιση στον τομέα της κυβερνοασφάλειας, με στόχο να ενισχυθούν οι δυνατότητες της Ευρώπης για την αντιμετώπιση κυβερνοεπιθέσεων και κυβερνοαπειλών και για την ενίσχυση των τεχνολογικών και βιομηχανικών δυνατοτήτων στο συγκεκριμένο πεδίο. Η εν λόγω δέσμη περιλαμβάνει τον Κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Η εμπιστοσύνη αποτελεί προαπαιτούμενο για τη λειτουργία της ψηφιακής ενιαίας αγοράς. Οι τεχνολογίες για την κυβερνοασφάλεια, όπως οι ψηφιακές ταυτότητες, η κρυπτογραφία και η ανίχνευση εισβολών και η εφαρμογή τους σε τομείς, όπως τα χρηματοοικονομικά, η βιομηχανία, η ενέργεια, οι μεταφορές, η υγειονομική περίθαλψη και η ηλεκτρονική διακυβέρνηση, είναι απαραίτητες για να διαφυλαχθεί η ασφάλεια των ηλεκτρονικών δραστηριοτήτων και των διαδικτυακών συναλλαγών και η εμπιστοσύνη των πολιτών, των δημόσιων διοικήσεων και των επιχειρήσεων σε αυτές.

Στα συμπεράσματά του της 19ης Οκτωβρίου 2017, το Ευρωπαϊκό Συμβούλιο τόνισε ότι, για να οικοδομηθεί επιτυχώς μια Ψηφιακή Ευρώπη, η Ένωση χρειάζεται αγορές εργασίας, εκπαιδευτικά συστήματα και συστήματα κατάρτισης κατάλληλα για την ψηφιακή εποχή και ότι υπάρχει ανάγκη για επενδύσεις σε ψηφιακές δεξιότητες, ώστε να δοθούν σε όλους τους Ευρωπαίους οι σχετικές δυνατότητες και τα μέσα.

4.2 Κυβερνοασφάλεια στην Ελλάδα

Οι σύγχρονες τεχνολογίες έχουν συμβάλει στην ανάπτυξη ενός έντονα διασυνδεδεμένου περιβάλλοντος που δεν οριοθετείται από σύνορα. Με στόχο να διαφυλαχτούν τα κοινά συμφέροντα, έχει αναπτυχθεί ο κλάδος της κυβερνοδιπλωματίας που προωθεί την υπεύθυνη συμπεριφορά στον κυβερνοχώρο σε επίπεδο κρατών.

Παράλληλα, οι διασυνοριακές εξαρτήσεις επιβάλλουν τη διεθνή συνεργασία με σκοπό να επιτευχθεί ένα κοινό υψηλό επίπεδο ασφάλειας.

Σε αυτό το πλαίσιο, η χώρα μας οφείλει να συντηρήσει και να ενισχύσει την παρουσία της και τη συμμετοχή της σε όλο το φάσμα της διεθνούς συνεργασίας στοχεύοντας:

- στη διασφάλιση συνεργασιών για την από κοινού ανάπτυξη μέσων αντιμετώπισης απειλών και προκλήσεων,
- στη δημιουργία και ενίσχυση συμμαχιών για την από κοινού αντιμετώπιση κυβερνοεπιθέσεων,
- στην εξασφάλιση πρόσβασης σε πληροφορίες και τεχνογνωσία
- στην από κοινού διαμόρφωση νομοθετικών προτάσεων σε ευρωπαϊκό επίπεδο και
- στην από κοινού υλοποίηση αποφάσεων που έχουν υιοθετηθεί στο πλαίσιο διεθνών Οργανισμών στους οποίους συμμετέχει η Ελλάδα

Ειδικότερα, στις δραστηριότητες του εν λόγω ειδικού στόχου συγκαταλέγονται:

- Η Ενίσχυση της Ελληνικής παρουσίας και συμμετοχής σε διεθνείς συμμαχίες για θέματα κυβερνοασφάλειας
- Η Υποστήριξη των συνεργασιών με τρίτες χώρες για μεταφορά τεχνογνωσίας από και προς αυτές με στόχο την ενίσχυση του κοινά υψηλού επιπέδου ασφάλειας και την αποδοτικότερη αντιμετώπιση των διασυνοριακών απειλών.

- Η Δημιουργία μεθόδου καθορισμού των προσδοκώμενων συνεργασιών για θέματα κυβερνοασφάλειας και σύναψη συμφώνων συνεργασίας με τρίτες χώρες.
- Η Δημιουργία μοντέλου διαχείρισής τους ώστε μέσω της συνεργασίας να επιτυγχάνεται πρόοδος στην περαιτέρω ανάπτυξη του εθνικού επιπέδου ασφάλειας, ικανοτήτων και ευαισθητοποίησης. (Εθνική Στρατηγική Κυβερνοασφάλειας)

4.2.1 Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων και Ηλεκτρονικών Επικοινωνιών - Ν. 4070/2012

Με το άρθρο 37 του Ν. 4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις» ρυθμίζονται οι υποχρεώσεις που έχουν οι πάροχοι δικτύων/υπηρεσιών ηλεκτρονικών επικοινωνιών, για την ασφάλεια και ακεραιότητα των υπηρεσιών αυτών.

Συγκεκριμένα, ο νόμος αναφέρει ρητά στο ως άνω άρθρο ότι οι πάροχοι οφείλουν να λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και των υπηρεσιών, εξασφαλίζοντας ένα επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο, διασφαλίζοντας την ακώλυτη και αδιάλειπτη παροχή των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών, ενώ οφείλουν και να κοινοποιούν στην ΕΕΤΤ κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που είχαν σημαντικό αντίκτυπο στη λειτουργία των ως άνω δικτύων ή υπηρεσιών.

Αρμόδια για την εποπτεία της προστασίας του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας, καθώς και της ασφάλειας των δικτύων και πληροφοριών είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών («ΑΔΑΕ»), που συστάθηκε ως ανεξάρτητη συνταγματική Αρχή με το άρθρο 1 του Ν. 3115/2003 σε εκτέλεση του άρθρου 19 § 2 του Συντάγματος.

Με την υπ' αρ. 205/2013 απόφασή της με τίτλο «Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών», όπως δημοσιεύθηκε και στο ΦΕΚ 1742/Β΄/15-7-2013, η ΑΔΑΕ εξειδίκευσε/ερμήνευσε τις διατάξεις του άρθρου 37 του Ν. 4070/2012, αναφορικά με την ασφάλεια και την ακεραιότητα των δικτύων/υπηρεσιών ηλεκτρονικών επικοινωνιών, προβλέποντας ενδεικτικά τις ακόλουθες υποχρεώσεις για τους παρόχους:

- Κατάρτιση/Σχεδιασμός και τήρηση πολιτικής ασφάλειας δικτύων και υπηρεσιών.
- Διορισμός υπευθύνου ασφάλειας δικτύων και υπηρεσιών.
- Κατάρτιση/Δημιουργία και τήρηση σχεδίου έκτακτων αναγκών.
- Συμμόρφωση με πρότυπα ασφαλείας, τεχνικές διεπαφές και στοιχεία λειτουργίας δικτύων που συμφωνούνται σε Ενωσιακό επίπεδο.
- ανάλυση επιχειρησιακών επιπτώσεων και αξιολόγησης επικινδυνότητας αναφορικά με την ασφάλεια και την ακεραιότητα των δικτύων.
- Κατάρτιση/Δημιουργία/Οργάνωση και τήρηση σχεδίου επιχειρησιακής συνέχειας/αδιάλειπτης λειτουργίας.
- Διεξαγωγή ελέγχων αποτελεσματικότητας και κατάρτιση σχετικών σχεδίων και διαδικασιών (δοκιμών, penetration tests, vulnerability assessments).
- Τήρηση κατάλληλων μέτρων φυσικής και λογικής/πληροφοριακής ασφάλειας.
- Σχεδιασμός/Επιλογή και τήρηση διαδικασίας διαχείρισης περιστατικών ασφαλείας.
- Σχεδιασμός/Επιλογή και τήρηση διαδικασίας εσωτερικού ελέγχου για την ασφάλεια και την ακεραιότητα των δικτύων / υπηρεσιών.
- Τήρηση σχετικών αρχείων.

4.2.2 Ν. 4577/2018 – Πεδίο και Μέτρα Εφαρμογής

Επιπλέον, ο Ν. 4577/2018 θεσπίζει σημαντικές υποχρεώσεις κυβερνοασφάλειας για παρόχους ψηφιακών υπηρεσιών, καθώς και φορείς εκμετάλλευσης βασικών υπηρεσιών, μεταξύ άλλων και του τομέα των ψηφιακών υποδομών. Όπως έχει ήδη ανωτέρω διαληφθεί, η εναρμόνιση του εθνικού δικαίου στη χώρα μας με την Οδηγία 1148/2016 έγινε με τον Ν. 4577/2018 και τις διατάξεις της ΥΑ υπ' αριθ.1027/ΦΕΚΒ/3739/8.10.2019. Σύμφωνα με το άρθρο 1 της ΥΑ, σκοπός της είναι η έκδοση των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών, της διαδικασίας παροχής πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές, η μεθοδολογία προσδιορισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.), καθώς και η μεθοδολογία αξιολόγησης και ελέγχου, σύμφωνα με τις προβλέψεις της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής της 30ης Ιανουαρίου 2018 και του ν. 4577/2018 (Α΄199), ο

οποίος κατ' εφαρμογή της ως άνω Οδηγίας θεσπίζει μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων αυτών.

Αντικείμενο του Ν. 4577/2018 αποτελεί η ασφάλεια των συστημάτων δικτύου και πληροφοριών και συγκεκριμένα η ικανότητά τους να ανθίστανται με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών.

Οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στον νόμο αφορούν αποκλειστικά: α) τους φορείς εκμετάλλευσης βασικών υπηρεσιών και β) τους παρόχους ψηφιακών υπηρεσιών σε κρίσιμους τομείς, ενώ ταυτόχρονα ισχύει και το Π.Δ. 39/2011 με το οποίο θεσπίζεται η διαδικασία προσδιορισμού των ευρωπαϊκών υποδομών ζωτικής σημασίας και αξιολόγησης της ανάγκης προστασίας των υποδομών αυτών, καθώς και οι διατάξεις που αφορούν την παιδική πορνογραφία και του ν. 4360/2016 περί ευρωπαϊκής εντολής προστασίας.

Στο άρθρο 3 της ως άνω απόφασης θεσπίζεται ο καθορισμός της ενιαίας πολιτικής ασφαλείας από την Εθνική Αρχή Κυβερνοασφάλειας, δηλαδή η τήρηση ενός ενιαίου ελάχιστου βασικού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών, στο οποίο πρέπει να προσαρμόζεται η εθνική πολιτική κάθε κράτους μέλους. Βασικοί στόχοι της πολιτικής ασφάλειας είναι:

- Η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων, συστημάτων και υπηρεσιών έναντι εκούσιων ή ακούσιων απειλών
- Η ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικών με την ασφάλεια και προστασία των δεδομένων
- Η επιχειρησιακή συνέχεια των βασικών υπηρεσιών του Οργανισμού έναντι των κυβερνοεπιθέσεων
- Η ενημέρωση και εκπαίδευση όλων των εμπλεκομένων σχετικά με την παροχή των βασικών υπηρεσιών του Οργανισμού
- Η άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

Στο άρθρο 4 περιγράφονται οι βασικές απαιτήσεις ασφάλειας, οι οποίες χωρίζονται σε τρεις κατηγορίες, ήτοι την Αναγνώριση, την Προστασία και την Αντιμετώπιση των αδυναμιών ασφάλειας.

Στο άρθρο 5 γίνεται αναφορά στα χαρακτηριστικά που πρέπει να έχουν τα μέτρα ασφαλείας που επιλέγονται, ώστε να ενισχύουν ενεργά το επίπεδο ασφάλειας.

Στο άρθρο 6 ορίζεται η υποχρέωση του κάθε Οργανισμού που εμπίπτει στην κατηγορία των Φ.Ε.Β.Υ. να ορίσει συγκεκριμένο εργαζόμενό του ως Υπεύθυνο Ασφάλειας πληροφοριών και δικτύων του, που πρέπει να διαθέτει ανεξαρτησία και να μην έρχεται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

Τέλος στη τμήμα Β της Υ.Α. και συγκεκριμένα στα άρθρα 7 έως 11, αναλύεται η διαδικασία ελέγχου από την Εθνική Αρχή Κυβερνοασφάλειας (άρθρο 12) και στο τμήμα Δ η διαδικασία επιβολής κυρώσεων (άρθρα 13 έως 15), ενώ στο άρθρο 16 αναφέρεται η μεθοδολογία προσδιορισμού Φ.Ε.Β.Υ. και στο Παράρτημα 1προσαρτάται ο κατάλογος των βασικών υπηρεσιών.

4.2.3 Αξιολόγηση κινδύνων και κατάρτιση Εθνικού Σχεδίου Αποτίμησης Επικινδυνότητας

Η αξιολόγηση των κινδύνων κυβερνοασφάλειας και η αποτελεσματική διαχείρισή τους αποτελούν έναν από τους βασικούς πυλώνες της κυβερνοασφάλειας και της ψηφιακής διακυβέρνησης. Για το σκοπό αυτό απαιτείται:

- Ο καθορισμός συγκεκριμένου πλαισίου βάσει του οποίου οι Φορείς θα αναγνωρίζουν τις κρίσιμες επιχειρησιακές δραστηριότητες και πληροφοριακούς πόρους που τις υποστηρίζουν,
- Ο καθορισμός συγκεκριμένου πλαισίου βάσει του οποίου οι Φορείς θα αναγνωρίζουν τους εξωτερικούς και εσωτερικούς παράγοντες οι οποίοι δύναται να επηρεάσουν την ασφάλεια των πληροφοριακών πόρων,
- Η κατάρτιση προφίλ απειλών και αξιολόγηση των αδυναμιών που οι απειλές ενδέχεται να εκμεταλλευτούν,
- Η κατάρτιση σχεδίου αντιμετώπισης κινδύνων κυβερνοασφάλειας.

Επίσης, καθοριστική δράση διαδραματίζει η εκπόνηση μελέτης αποτίμησης επικινδυνότητας σε εθνικό επίπεδο, ακολουθώντας μια επιστημονική διαδικασία που συνοπτικά στηρίζεται στην αναγνώριση, ανάλυση και αποτίμηση των επιπτώσεων των κινδύνων και οδηγεί στον καθορισμό ενός σχεδίου προστασίας των κρίσιμων υποδομών ανά τομέα ή/και ανά φορέα.

Η μελέτη, η οποία θα αναθεωρείται το αργότερο κάθε τριετία, λαμβάνει υπόψη της όλες τις πιθανές απειλές, ιδιαίτερα αυτές που σχετίζονται με κακόβουλες ενέργειες (πχ

κυβερνοέγκλημα, κυβερνοεπιθέσεις), αλλά και τους κινδύνους που σχετίζονται με φυσικά φαινόμενα, τεχνικές αστοχίες ή δυσλειτουργίες και ανθρώπινα λάθη.

Επίσης, θα ληφθούν υπόψη οι απειλές που προκύπτουν από την αλληλεξάρτηση των συστημάτων επικοινωνιών και πληροφοριών των φορέων που συμμετέχουν στην Εθνική Στρατηγική και ιδιαίτερα των κρίσιμων υποδομών, ενώ περαιτέρω θα αξιολογείται η έκταση και η κρισιμότητα των επιπτώσεων σε εθνικό επίπεδο.

4.2.4 Εθνικό Σχέδιο Έκτακτης Ανάγκης

Το εθνικό σχέδιο έκτακτης ανάγκης αποτελεί τον οδηγό ώστε να αντιμετωπιστούν συμβάντα που υπάγονται στη σφαίρα της διαχείρισης κρίσεων. Περιλαμβάνει κριτήρια που κατηγοριοποιούν ένα συμβάν, τους ρόλους σχετικά με τη διαχείριση κρίσεων και τις ενέργειες που θα υλοποιηθούν ώστε να αντιμετωπιστεί το συμβάν. Ενεργοποιείται για να ανταποκριθεί σε συμβάντα που προκαλούν σοβαρή διατάραξη στην παροχή υπηρεσιών από τους φορείς ή θέτουν σε κίνδυνο παροχές υπηρεσιών προς τους πολίτες. Τέτοιου είδους συμβάντα αναφέρονται ως κρίσεις, με το Σχέδιο να αποτελεί το εγχειρίδιο διαχείρισης κρίσεων.

Το εθνικό σχέδιο έκτακτης ανάγκης περιλαμβάνει τα κάτωθι:

- Ορισμούς (διαχείρισης κρίσεων, επιχειρησιακής συνέχειας). Περιλαμβάνονται ορισμοί ώστε να υπάρχει συγκεκριμένη ορολογία και να αναπτυχθεί μια κοινή γλώσσα επικοινωνίας.
- Κριτήρια. Ορίζουν πότε ένα συμβάν θεωρείται ως κρίση ώστε να ενεργοποιηθεί το Εθνικό Σχέδιο Έκτακτης Ανάγκης.
- Σενάρια, ρόλους και αρμοδιότητες. Περιγραφή σεναρίων και ενεργειών που υπάγονται στον ορισμό της κρίσης, καταγραφή ρόλων και αρμοδιοτήτων ώστε να βρίσκονται σε ετοιμότητα σε περίπτωση ενεργοποίησης του εθνικού σχεδίου έκτακτης ανάγκης.
- Συσχετισμούς με σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές. Καταγραφή καταστροφών, ώστε να διευκολύνεται η επίλυση μιας κρίσης και να εκτελούνται οι απαιτούμενες ενέργειες για ανάκαμψη και επιστροφή στην κανονικότητα.
- Εκτίμηση, ανάλυση και αναγνώριση κινδύνων. Καταγραφή αποτελεσμάτων αξιολόγησης κινδύνων κυβερνοασφάλειας που ενδέχεται να οδηγήσουν σε κρίση.

- Αναγνώριση επικείμενης κρίσης (Identify Crisis Signals). Μεθοδολογία έγκαιρης αναγνώρισης επικείμενης κρίσης, με στόχο την άμεση ενεργοποίηση του Σχεδίου.
- Επικοινωνία για τη διαχείριση κρίσης (επικοινωνία μεταξύ Φορέων, διαχείριση σχέσεων, επικοινωνία με τα Μ.Μ.Ε., επικοινωνία με αρμόδια υπουργεία, κ.λπ.) Στοιχεία επικοινωνίας, έτοιμα μηνύματα, απόδοση ρόλων.
- Επιλογές ασκήσεων. Περιλαμβάνεται ανάλυση ασκήσεων, ενδεικτικά σενάρια και σχέδιο διενέργειας ασκήσεων. (Εθνική Στρατηγική Κυβερνοασφάλειας)

4.3 Μελλοντική Δράση

Στην εποχή που διανύουμε η κυβερνοασφάλεια είναι μεγίστης σημασίας και αποτελεί το κεντρικό θέμα στις συζητήσεις της Ευρωπαϊκής Ένωσης.

Για τον λόγο αυτό, η Ευρωπαϊκή Επιτροπή και ο ύπατος εκπρόσωπος δεσμεύονται να εφαρμόσουν τη νέα στρατηγική για την κυβερνοασφάλεια κατά τους προσεχείς μήνες. Θα υποβάλλουν τακτικά εκθέσεις σχετικά με την πρόοδο που σημειώνεται και θα ενημερώνουν πλήρως το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ευρωπαϊκής Ένωσης και τα ενδιαφερόμενα μέρη για όλες τις σχετικές δράσεις, ενώ θα ενθαρρύνεται η συμμετοχή τους σε αυτές.

Επιπλέον, σε ό, τι αφορά την οδηγία NIS2, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα την εξετάσουν και θα την εγκρίνουν. Μόλις επιτευχθεί συμφωνία και εγκριθούν οι προτάσεις, τα κράτη μέλη θα πρέπει να τις μεταφέρουν στο εθνικό τους δίκαιο εντός 18 μηνών από την έναρξη ισχύος τους.

Τέλος, η Επιτροπή θα επανεξετάζει περιοδικά την οδηγία NIS2 και θα υποβάλλει εκθέσεις σχετικά με τη λειτουργία τους.

Και στην Ελλάδα αντίστοιχα, η υλοποίηση των στρατηγικών στόχων της Εθνικής Στρατηγικής Κυβερνοασφάλειας παρακολουθείται από την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αξιολόγηση και την ανατροφοδότηση της Στρατηγικής.

Λαμβάνοντας δε υπόψη την ανάγκη διαμόρφωσης ενός πιο μακροπρόθεσμου ορίζοντα στην υλοποίηση των περιγραφόμενων πρωτοβουλιών και δράσεων, προτείνεται η παρούσα στρατηγική να επικαιροποιείται ανά πέντε έτη.

5 Η εγκληματοπροληπτική λειτουργία των Ειδικών Ανακριτικών Πράξεων του άρ. 6 του Ν. 2928/2001

Το άρθρο 254 ΚΠοινΔ προβλέπει τη διενέργεια ειδικών ανακριτικών πράξεων σε ορισμένα εγκλήματα που απαριθμούνται περιοριστικά στην παρ. 1 αυτού και διενεργούνται κατ' απόλυτη μυστικότητα επί συγκεκριμένων μόνο εγκλημάτων προς υλοποίηση δικονομικών και κυρίως εγκληματοπροληπτικών σκοπών.

Οι ειδικές ανακριτικές πράξεις εισήχθησαν στην ποινική διαδικασία για να καλύψουν ανάγκες πρόληψης και καταστολής συγκεκριμένων εγκλημάτων, ώστε να αρθεί το πρόβλημα ανασφάλειας που προκαλείται από την εγκληματική συμπεριφορά. Ωστόσο, λόγω του επαχθούς χαρακτήρα τους παράγουν σημαντικές συνέπειες για τα ατομικά δικαιώματα καταδεικνύοντας την έλλειψη ενός άρτιου νομοθετικού πλαισίου για την ρύθμιση των αστυνομικού δικαίου ζητημάτων, έλλειψη η οποία συνιστά πρόβλημα για το κράτος δικαίου και πρέπει σύντομα να αντιμετωπιστεί, ώστε οι πράξεις αυτές να είναι αποτελεσματικές και να επιτελούν το έργο για το οποίο είναι προορισμένες.

Ως ειδικές ανακριτικές πράξεις αναφέρονται στον νόμο η ανακριτική διείσδυση, οι ελεγχόμενες μεταφορές, η παρακολούθηση της αλληλογραφίας και των τηλεφωνικών συνδιαλέξεων, η ηχητική και οπτική παρακολούθηση και η συσχέτιση δεδομένων προσωπικού χαρακτήρα.[14]

Τα ιδιαίτερα χαρακτηριστικά των πράξεων αυτών που τις διαφοροποιούν από τις κλασσικές ανακριτικές πράξεις, είναι η απόλυτη erga omnes μυστικότητα της διενέργειάς τους και η εγκληματοπροληπτική λειτουργία τους. Τα χαρακτηριστικά τους αυτά, σε συνδυασμό και με την αποτελεσματικότητά τους για την καταπολέμηση του οργανωμένου εγκλήματος, καθιστούν το ρυθμιστικό πεδίο τους έναν χώρο έντασης ανάμεσα στην πρόληψη και την καταστολή των εγκλημάτων και την προστασία των ατομικών δικαιωμάτων[15].

Το 2001 η Ελλάδα, με το άρθρο 6 του ν. 2928/2001, εισάγει στον Κώδικα Ποινικής Δικονομίας το άρθρο 253 Α ως όφειλε, ως συμβαλλόμενο κράτος, μετά την υπογραφή της στη Διεθνή Σύμβαση του ΟΗΕ του 2000 στο Παλέρμο της Ιταλίας. Αποστολή του άρθρου 253 Α ΚΠΔ δεν ήταν η θέσπιση νέων ανακριτικών πράξεων, αλλά η συστηματοποίησή τους εντός του πλαισίου του ΚΠΔ, η θέσπιση δικαστικών εγγυήσεων και η σύνδεσή τους

14 Θ. Δαλακούρας, Ειδικές ανακριτικές πράξεις κατ' άρθρο 253Α ΚΠΔ και ηλεκτρονικό έγκλημα, σε Δαλακούρα (επιμ.), "Ηλεκτρονικό Έγκλημα", Νομική Βιβλιοθήκη, 2019, σελ. 248

15 Χρ. Νάϊντος, Ειδικές ανακριτικές πράξεις : *Επίκαιρα ζητήματα, Ποινικά Χρονικά 2017, 491

με το κακούργημα της εγκληματικής οργάνωσης του άρθρου 187 παρ. 1 ΠΚ. Επρόκειτο για εκπλήρωση διεθνούς υποχρέωσης της Ελλάδας, που απέρρεε από το άρθρο 20 παρ. 1 της Σύμβασης του ΟΗΕ για το οργανωμένο έγκλημα.

Με το άρθρο 20 της άνω Σύμβασης η ελληνική πολιτεία ανταποκρίνεται στο κέλευσμα για την ενσωμάτωση ειδικών ανακριτικών πράξεων για την καταπολέμηση του οργανωμένου εγκλήματος. Πρόκειται για διάταξη που συνιστά συμμόρφωση της νομοθεσίας μας, στις διεθνείς συμβατικές δεσμεύσεις της χώρας μας και εναρμόνιση με τις δικαιικές επιταγές της ΕΣΔΑ.

Με την εν λόγω διάταξη καθιερώνονται πλέον επίσημα οι λεγόμενες ειδικές ανακριτικές πράξεις, όχι απλώς ως μέθοδοι για την αποκάλυψη των επί μέρους αξιόποινων πράξεων των εγκληματικών οργανώσεων, αλλά και ως όπλα για την εξάρθρωση μιας εγκληματικής οργανωτικής υποδομής.

5.1 Οι τροποποιήσεις των ειδικών ανακριτικών πράξεων με το νέο ΚΠοιν.Δ.

Ο νέος ΚΠΔ, βελτίωσε το κανονιστικό πλαίσιο των ειδικών ανακριτικών πράξεων υιοθετώντας θεμελιακές παραδοχές του ΕΔΔΑ και αναγνωρίζοντας ένα είδος αυξημένης εισαγγελικής εποπτείας στη διενέργειά τους. Ειδικότερα:

α) Προβλέφθηκε αυτοτελώς η ειδική ανακριτική πράξη της συγκαλυμμένης έρευνας, η οποία είχε τυποποιηθεί παλαιότερα μόνο στο άρθρο 253Β ΚΠΔ για τις ανακριτικές πράξεις εγκλημάτων διαφθοράς.

β) Θεσμοθετείται η ουσιαστική αιτιολόγηση των προϋποθέσεων για τη διενέργεια των ειδικών ανακριτικών πράξεων με την αναλυτική καταγραφή των κρίσιμων παραμέτρων της αξιούμενης αιτιολογίας του σχετικού βουλεύματος (άρ. 254 § 3 ΚΠΔ),

γ) Τίθεται υπό έλεγχο η δράση των προσώπων που δρουν συγκαλυμμένα, καθώς προβλέπεται εποπτεία του εισαγγελέα πλημμελειοδικών ενώ συντάσσεται για την δράση των ανακριτικών υπαλλήλων ή του τρίτου αναλυτική έκθεση κατά τα άρθρα 148 έως 153 (άρ. 254 § 1 α΄ και β΄ ΚΠΔ).

δ) Τέλος, οριακής αποδοχής ρύθμιση συνιστά η θεσπιζόμενη επέμβαση για έλεγχο μεταφορών, άρση του απορρήτου και την καταγραφή της δραστηριότητας εκτός κατοικίας (άρ. 254 § 2 γ΄, δ΄, ε΄ ΚΠΔ) και κατά τρίτου αμέτοχου στο έγκλημα προσώπου,

προκειμένου να αποκαλυφθεί η ταυτότητα του κατηγορουμένου ή ο τόπος διαμονής ή κατοικίας του και εφόσον είναι τεχνικά αδύνατη η εξακρίβωση αυτών των στοιχείων με άλλο τρόπο.

Οι εξελίξεις στον τεχνολογικό τομέα διεύρυναν τόσο τα πεδία εγκληματικής δράσης και τους τρόπους τέλεσης των παραδοσιακών εγκλημάτων, όσο και τις δυνατότητες της έννομης τάξης να αντιμετωπίσει ή και να προλάβει την τέλεσή τους. Οι τελευταίες δυνατότητες ωστόσο, πέρα από το ότι έχουν επεκταθεί σε έναν τόσο σημαντικό τομέα της ιδιωτικής σφαίρας, αφορούν έναν ολοένα πιο διευρυμένο κύκλο θιγόμενων προσώπων. Τα πρόσωπα αυτά ενδέχεται να μην έχουν καμία ανάμειξη σε εγκληματικές πράξεις.

Η διερεύνηση του εγκλήματος στον χώρο των πληροφοριακών συστημάτων, όπου δραστηριοποιείται ένα, για τους σκοπούς της ποινικής δίκης, πρωτοφανές σε μέγεθος ποσοστό ατόμων (εντός/εκτός διαδικτύου), μπορεί λοιπόν να οδηγήσει σε απρόβλεπτα ανασφαλείς δρόμους για πολλούς απλούς πολίτες, με αποτέλεσμα να τίθενται σε κίνδυνο, μεταξύ άλλων, τα προσωπικά δεδομένα, το απόρρητο της επικοινωνίας, ο ιδιωτικός βίος και τελικά η ελεύθερη ανάπτυξη της προσωπικότητας. Οι νέες επομένως εξουσίες των ανακριτικών αρχών διαφέρουν σε σχέση με τις παραδοσιακές μεθόδους πρόληψης και καταστολής του εγκλήματος στο πεδίο των ερευνών, τόσο ποιοτικά (καταγραφή σχεδόν κάθε πτυχής της σύγχρονης ζωής) όσο και ποσοτικά (αριθμός προσώπων που θίγονται[16]).

Από την άλλη πλευρά βέβαια, η επιλογή του νομοθέτη εν προκειμένω να ορίσει ΚΠΔ ειδικώς τις νέες ανακριτικές πράξεις που ενέχουν τόσο σοβαρές επεμβάσεις σε ατομικά δικαιώματα, αντί να επαναπαυτεί σε αμφιβόλου συνταγματικότητας αναλογικές ή διασταλτικές εφαρμογές των ήδη προβλεπόμενων ερευνών, αποτελεί θετικό δικαιοκρατικό βήμα.

Η διενέργεια των ειδικών ανακριτικών πράξεων συνεπάγεται, την προσβολή εννόμων αγαθών, ιδίως της προσωπικής ελευθερίας, της ιδιωτικής ζωής και της προσωπικότητας των υποκειμένων σε αυτές. Δε θα πρέπει να παραβλεφθεί όμως και το γεγονός ότι από τις ειδικές ανακριτικές πράξεις δεν πλήττονται μόνο τα δικαιώματα των υποκειμένων σε αυτές, αλλά και τρίτα πρόσωπα, με τα οποία τα υποκείμενα έρχονται σε επαφή και που πιθανόν να μην έχουν καμία σχέση με παράνομες δραστηριότητες.

16 https://theartofcrime.gr

Ο μυστικός χαρακτήρας τους αποτελεί απόκλιση από την αρχή της εσωτερικής δημοσιότητας και την αρχή της έγγραφης διαδικασίας, δύο βασικές αρχές της προδικασίας. Επιπλέον, ο προληπτικός τους χαρακτήρας είναι συνυφασμένος με τη διεύρυνση του κύκλου των θιγόμενων προσώπων, πέραν αυτών στους οποίους θα απαγγελθούν αργότερα καταγγελίες, γεγονός που αποτελεί κάμψη της αρχής του τεκμηρίου αθωότητας αυτών.

Στην παράγραφο 2 του άρθρου 254 ΚΠΔ αναφέρονται οι προϋποθέσεις διεξαγωγής των ανακριτικών πράξεων που περιγράφονται στην παράγραφο 1. Συγκεκριμένα, αναφέρεται ότι οι ανακριτικές αυτές πράξεις διενεργούνται μόνο α) αν προκύπτουν σοβαρές ενδείξεις ότι έχει τελεσθεί αξιόποινη πράξη των παραγράφων 1 και 2 του άρθρου 187, των άρθρων 187Α, 207 εδάφιο α΄, 208 παρ. 1, εδάφιο α΄, 208Α, εκτός από τις ιδιαίτερα ελαφρές περιπτώσεις, 323Α, 336 σε βάρος ανηλίκου, της παρ. 1 του άρθρου 338 σε βάρος ανηλίκου, των παραγράφων 1 και 4 του άρθρου 339, των παραγράφων 1 και 2 του άρθρου 342, των άρθρων 348Α, 348Β, 348Γ, 351 και 351Α του Ποινικού Κώδικα, και β) αν η εξάρθρωση της εγκληματικής οργάνωσης ή η εξιχνίαση των τρομοκρατικών πράξεων του άρθρου 187Α ή των πράξεων των άρθρων 207 εδάφιο α΄, 208 παρ. 1, εδάφιο α΄, 208Α, εκτός από τις ιδιαίτερα ελαφρές περιπτώσεις, 323Α, 336 σε βάρος ανηλίκου, της παρ. 1 του άρθρου 338 σε βάρος ανηλίκου, των παραγράφων 1 και 4 του άρθρου 339, των παραγράφων 1 και 2 του άρθρου 342, των άρθρων 348Α, 348Β, 348Γ, 351 και 351Α του Ποινικού Κώδικα είναι διαφορετικά αδύνατη ή ιδιαιτέρως δυσχερής.

Επίσης, τίθεται ως προϋπόθεση και η έκδοση ειδικά αιτιολογημένου βουλεύματος από το αρμόδιο δικαστικό συμβούλιο μετά από πρόταση του εισαγγελέα. Σε εξαιρετικά επείγουσες περιπτώσεις την έρευνα μπορεί να διατάξει ο εισαγγελέας ή ο ανακριτής.

5.1.1 Οι ειδικές ανακριτικές πράξεις ως μέσο πρόληψης της τρομοκρατικής οργάνωσης

- Ανακριτική Διείσδυση

Η ορθή εφαρμογή της ανακριτικής διείσδυσης, ως ειδικής ανακριτικής πράξης του σημερινού άρθρου 254 Κ.Π.Δ. αποτελεί, χωρίς αμφιβολία, βασικό εχέγγυο κατ' αρχήν για την πρόληψη, αλλά και για την αντιμετώπιση σοβαρότατων ποινικών εγκλημάτων, όπως αυτό της τρομοκρατικής οργάνωσης του άρθρου 187 Α και ειδικότερα της παρ. 6 του ιδίου άρθρου που αφορά την τέλεση της τρομοκρατικών πράξεων μέσω διαδικτύου.

Με τον όρο ανακριτική διείσδυση στον Κώδικα Ποινικής Δικονομίας νοείται η «χρησιμοποίηση», είτε των ίδιων των ανακριτικών υπαλλήλων, είτε άλλων εμπίστων σε αυτούς προσώπων (ιδιωτών)[17], που συνεργάζονται με τις ανακριτικές αρχές, με στόχο τη συλλογή ουσιαστικών για την πορεία της υπόθεσης αποδεικτικών στοιχείων και τελικώς την κατάληψη του δράστη ή των δραστών τη στιγμή που διαπράττεται η αξιόποινη πράξη. Σχετικά με την αντιμετώπιση της οργανωμένης εγκληματικής δραστηριότητας, ένα βασικό πλεονέκτημα της ανακριτικής διείσδυσης, είναι ότι διασπά τη στεγανότητα των κλειστών μαφιόζικων και τρομοκρατικών οργανώσεων με την υιοθέτηση ανάλογων, προς τους δικούς τους, συνωμοτικών κανόνων δράσης. Το πρόσωπο που αναλαμβάνει τον ρόλο αυτό εντάσσεται ή αλλιώς διεισδύει στην εκάστοτε εγκληματική οργάνωση, και δρα ως agent provocateur (προκαλών πράκτορας) όπως αυτός νοείται στο άρθρο 46 παρ.2 του Π.Κ., αποσπώντας πληροφορίες, εντοπίζοντας κρίσιμα για την υπόθεση στοιχεία, και καθ' αυτόν τον τρόπο δρα προλαμβάνοντας το έγκλημα και συνάμα καταστέλλοντάς το αποτελεσματικά. Πρόκειται έτσι, σύμφωνα με τη θεωρία, για ειδική ανακριτική πράξη, αλλά ταυτοχρόνως και για έρευνα με μυστικό χαρακτήρα, χωρίς γνώση του καθ' ού, ο οποίος ενδέχεται να μην πληροφορηθεί ποτέ τον τρόπο με τον οποίο δημιουργήθηκε η σε βάρος του κατηγορία.

Εκτός όμως από την αποτελεσματικότητά της, η εν λόγω ειδική ανακριτική πράξη, γεννά ορισμένους προβληματισμούς, κυρίως λόγω της διττής νομικής της φύσης, εφόσον το κράτος φαίνεται να «εξαπατά» κατά μία έννοια τους πολίτες, έχοντας ως στόχο την καταστολή σοβαρών ποινικών φαινομένων, περιορίζοντας όμως, με τον τρόπο αυτό, τα δικαιώματα του κατηγορουμένου. Η προβληματική που γεννήθηκε γύρω από την χρήση της ανακριτικής διείσδυσης είναι ιδιαίτερα σοβαρή, καθώς για τη σύμφωνη με το Νόμο διενέργειά της, πρέπει να ελέγχεται in concreto, αν η αστυνομία ή οι ανακριτικοί υπάλληλοι έδρασαν σύννομα, χωρίς να παγιδεύουν, με οποιοδήποτε κόστος, τον δράστη ή τους δράστες των εγκλημάτων.

Συνεπώς, με την παρούσα ειδική πράξη διείσδυσης, η οποία χαρακτηρίζεται μάλιστα, ως ιδιαίτερα επαχθής, «δοκιμάζεται» θα λέγαμε, το συνταγματικά κατοχυρωμένο στο άρθ. 20 Σ, αλλά και στο αυξημένης τυπικής ισχύος αρ. 6 παρ. 1 της ΕΣΔΑ δικαίωμα του κατηγορουμένου σε μια δίκαιη δίκη, το δικαίωμα σιωπής και μη αυτοενοχοποίησης του, όπως αυτοτελώς προβλέπεται πλέον στο αρ. 104 Κ.Π.Δ., καθώς και το τεκμήριο αθωότητας του κατηγορουμένου. Σε κάθε περίπτωση, είναι ιδιαίτερα σημαντικό εκ

17 Α. Παπαδαμάκης, Ανακριτική διείσδυση: όρια και υπερβάσεις, ΠοινΔικ Νοέμβριος-Δεκέμβριος 2010

μέρους των Αρχών, να μην παραβιάζονται, στο όνομα της καταστολής του οργανωμένου εγκλήματος, τα ως άνω δικαιώματα, σεβόμενοι ταυτόχρονα τη σημασία της ανθρώπινης αξίας (άρθ. 2 παρ. 1 του Συντ.) και το κατά πόσο αυτή καταπατάται με την εφαρμογή αυτών των «ακραίων» τεχνικών.

- **Άρση απορρήτου των τηλεπικοινωνιών**

Ένα άλλο είδος ειδικής ανακριτικής πράξης που δύναται να χρησιμοποιηθεί για την πρόληψη της Κυβερνοτρομοκρατίας είναι η άρση του απορρήτου των τηλεπικοινωνιών.

Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία, απόρρητα θεωρούνται:

- Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων).
- Η ταυτότητα του καλούντος και του καλουμένου.
- Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
- Τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός).

Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας προστατεύεται από το Σύνταγμα στο άρθρο 19 παρ. 1. Η ειδική ανακριτική πράξη της άρσης του απορρήτου των τηλεπικοινωνιών υλοποιεί την εξαίρεση της παρ. 1 περ. β΄ του άρθρου 19 του Συντάγματος, σύμφωνα με την οποία ειδικός νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δε δεσμεύεται από το απόρρητο, για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Στην άρση του απορρήτου περιλαμβάνονται η συνακρόαση συνδιαλέξεων, η εγγραφή και η αποτύπωση των τηλεφωνικών ή με άλλη μορφή επικοινωνίας συνομιλιών, η παρεμβολή σε συσκευή για την πληροφόρηση των καταγεγραμμένων μηνυμάτων.

Η άρση του απορρήτου των επικοινωνιών είναι μια κατ' εξαίρεση επιτρεπόμενη διαδικασία, βάσει της οποίας τα στοιχεία της επικοινωνίας, τα οποία είναι καταρχήν απόρρητα, καθίστανται γνωστά σε συγκεκριμένες Αρχές και για συγκεκριμένους λόγους[18].

18 https://eclass.ekdd.gr/esdda/modules/document/file.php/KZ_AEID_APP111/%CE%92%CE%91%CE%A3%CE%99%CE%9A%CE%9F%20%CE%A5%CE%9B%CE%99%CE%9A%CE%9F/%CE%95%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CF%8C%20%CF%85%CE%BB%CE%B9%CE%BA%CF%8C%20%CE%95%CE%A3%CE%94%CE%94%CE%91%20%20CYBERSECURITY.pdf

Οι προαναφερθέντες λόγοι εξειδικεύονται με τις διατάξεις του ν. 2225/1994, όπως ισχύει, ο οποίος περιλαμβάνει και κατάλογο των εγκλημάτων για τη διακρίβωση των οποίων μπορεί να διαταχθεί με διάταξη του αρμόδιου δικαστικού συμβουλίου η άρση του απορρήτου.

Τις διαδικασίες, τις τεχνικές και τις οργανωτικές ρυθμίσεις για την άρση του απορρήτου των επικοινωνιών προβλέπουν, εξειδικεύοντας τη διάταξη του άρθρου 19 του Συντάγματος, οι διατάξεις του ν. 2225/1994 και του ΠΔ 47/2005, όπως ισχύουν.

Ειδικότερα ο ν. 2225/1994, όπως ισχύει, προβλέπει τους λόγους για τους οποίους η άρση του απορρήτου επιτρέπεται, τα όργανα που μπορούν να τη διατάξουν, τα χρονικά όρια εντός των οποίων μπορεί η άρση να πραγματώνεται, καθώς και τη διαδικασία που πρέπει να ακολουθείται σε κάθε περίπτωση.

Το ΠΔ 47/2005, όπως ισχύει, προβλέπει τα είδη αλλά και τα επιμέρους στοιχεία της επικοινωνίας, τα οποία μπορεί να αφορά η άρση του απορρήτου. Προβλέπει επίσης τα μέσα και τις μεθόδους πραγμάτωσης της άρσης, καθώς και τις σχετικές υποχρεώσεις των παρόχων υπηρεσιών και δικτύων επικοινωνίας.

Μεταγενέστερα με το άρθρο 6 παρ. 1 ν. 2713/1999 «Υπηρεσία εσωτερικών υποθέσεων της ελληνικής αστυνομίας και άλλες διατάξεις» προβλέφθηκε η αποδέσμευση από το απόρρητο των επιστολών και της τηλεφωνικής ή κάθε άλλης μορφής ανταπόκρισης για τις ανάγκες της έρευνας εγκλημάτων που παραθέτονται στα εδ. ά και ΄β παρ. 2 άρθρ. 1 του ν. 2713/1999. Ήδη, με το εδ. δ παρ. 1 άρθρο 254 του ΚΠΔ το ίδιο μέτρο επεκτείνεται και στις περιπτώσεις τέλεσης εγκλημάτων του άρθρου 187Α ΠΚ, ήτοι της τέλεσης τρομοκρατικών πράξεων.

Οι ρυθμίσεις των άρθρων 4 και 5 του Ν 2225/1994 εγγράφονται ως οι επαρκέστερες από δικαιοκρατική άποψη προβλέψεις, σχετικά με την παρακολούθηση των θιγόμενων προσώπων στο πλαίσιο της ποινικής διαδικασίας. Του λόγου το αληθές αποδεικνύει το γεγονός ότι, με εξαίρεση την ελλείπουσα προϋπόθεση περί σοβαρών ενδείξεων, οι λοιπές γενικές προϋποθέσεις των παρ. 2, 3 και 4 του ιδίου άρθρου ήταν ήδη ενσωματωμένες στο κείμενο του Ν 2225/1994[19].

Τούτο δε σημαίνει, ωστόσο, ότι το σχετικό νομικό πλαίσιο στερείται ασαφειών και κενών. Έτσι εύστοχα επισημαίνεται ότι από την ανάγνωση των σχετικών διατάξεων δεν

19 Θ. Δαλακούρας, Ποινικά Χρονικά, ΝΑ/2001, "Οι Ειδικές Ανακριτικές πράξεις του άρ. 6 του Ν. 2928/2001", σελ. 1028

συνάγεται σαφώς, αν στο απόρρητο των τηλεπικοινωνιών εμπίπτουν και τα λεγόμενα συνδετικά δεδομένα, ενώ μόνον εμμέσως προκύπτει ότι με τον όρο «άρση του απορρήτου» νοούνται παράλληλα με τις παρεμβολές και συνακροάσεις συνδιαλέξεων και οι εγγραφές και αποτυπώσεις των τηλεπικοινωνιών σε υλικό φορέα.

Προβληματική υπό το φως της αρχής της αναλογικότητας οφείλει να θεωρηθεί περαιτέρω και η προβλεπόμενη στην παρ. 6 του άρθρου 5 Ν 2225/1994 χρονική διάρκεια της άρσης του απορρήτου, η οποία δύναται άνευ ειδικών λόγων να ανέλθει στους δέκα μήνες.

5.2 Οι προϋποθέσεις διενέργειας των ειδικών ανακριτικών πράξεων

Ως προς την πρώτη προϋπόθεση, ο νομοθέτης γνωρίζοντας ότι οι ειδικές ανακριτικές πράξεις είναι ιδιαίτερα επαχθείς, όρισε τον υψηλότερο βαθμό ενδείξεων ενοχής, ήτοι των σοβαρών ενδείξεων, γεγονός που συνιστά μια πρώτη εγγύηση προστασίας του ατόμου, περιορίζοντας πιθανότατα έτσι τον κίνδυνο αυθαιρεσιών κατά το στάδιο λήψης της σχετικής απόφασης. Περαιτέρω, η επιλογή του νομοθέτη να αναγάγει τις σοβαρές ενδείξεις σε προϋπόθεση διενέργειας των εν λόγω ανακριτικών πράξεων, προωθεί την αυξημένη απαίτηση προστασίας του ατομικού συμφέροντος, αλλά και την διαφοροποίηση αυτού του υψηλότερου βαθμού πιθανότητας της ενοχής από τις επαρκείς ή αποχρώσες ενδείξεις που αξιώνονται για την παραπομπή του κατηγορουμένου.

Η προϋπόθεση της συνδρομής «σοβαρών ενδείξεων» δρα προς όφελος του προσώπου εναντίον του οποίου πρόκειται να διενεργηθούν οι ειδικές ανακριτικές πράξεις, διότι η μη συνδρομή τους απαγορεύει τη διενέργεια αυτών, ακόμα και αν συντρέχουν οι υπόλοιπες προϋποθέσεις που θέτει ο νόμος. Η θεσμοθέτηση της προϋπόθεσης της ύπαρξης των σοβαρών ενδείξεων για τη διενέργεια των ειδικών ανακριτικών πράξεων είναι απόλυτα συμβατή με την Συνταγματική επιταγή της αρχής της αναλογικότητας, δεδομένου μάλιστα ότι σταθμίζονται δύο μεγέθη. Από τη μία το δημόσιο έννομο συμφέρον και από την άλλη το ατομικό έννομο συμφέρον.

Η δεύτερη γενική προϋπόθεση διενέργειας των ειδικών ανακριτικών πράξεων είναι αυτή της αναγκαιότητας διενέργειας αυτών. Η σύμφωνη με την αρχή της αναγκαιότητας ερμηνεία και εφαρμογή της ως άνω διάταξης απαιτεί να διατάσσεται η διενέργεια ειδικών ανακριτικών πράξεων μόνον εφόσον η συγκεκριμένη επέμβαση με κάποια από αυτές είναι

είτε το μοναδικό πρόσφορο και άρα αναγκαίο μέσο, είτε το λιγότερο επαχθές για την υλοποίηση του επιδιωκόμενου σκοπού της εξάρθρωσης της εγκληματικής οργάνωσης.

Συνεπώς, για να επιτραπεί η διενέργεια των ειδικών ανακριτικών πράξεων, προϋποτίθεται ότι θα πρέπει να έχει αποτύχει ή να έχει κριθεί απρόσφορος οποιοσδήποτε άλλος τρόπος, ήτοι κάθε άλλη γενική ανακριτική πράξη, από αυτές που αναφέρονται στο άρθρο 251 Κ.Π.Δ. (π.χ. η συγκέντρωση πληροφοριών για το έγκλημα, η εξέταση μαρτύρων και κατηγορουμένων, η διενέργεια αυτοψίας κ.λ.π.). Ωστόσο, η θεσμοθέτηση των ειδικών ανακριτικών πράξεων αποσκοπούσε στην κάλυψη των αναγκών πρόληψης και καταστολής συγκεκριμένων εγκλημάτων, οι οποίες δε θα μπορούσαν να καλυφθούν με τις ήδη υπάρχουσες γενικές ανακριτικές πράξεις του άρθρου 251 Κ.Π.Δ. Δεδομένου ότι η εξάρθρωση των εγκληματικών οργανώσεων είναι λόγω της υποδομής τους αντικειμενικά δυσχερής, καθίσταται αυτονόητος και ο κίνδυνος αυτόματης επιβεβαίωσης της ως άνω ανάγκης επέμβασης με ειδικές ανακριτικές πράξεις.

Η έκδοση ειδικά αιτιολογημένου βουλεύματος ως τρίτη προϋπόθεση διενέργειας των ειδικών ανακριτικών πράξεων, θεωρείται εύλογα κομβική εγγύηση για την αποτροπή των αυθαιρεσιών κατά τη λήψη της απόφασης διενέργειάς τους.

Ωστόσο, σε κάθε περίπτωση, η εγγυητική λειτουργία της προϋπόθεσης αυτής, αποκτά ουσιαστικό περιεχόμενο μόνον εφόσον το ειδικά αιτιολογημένο βούλευμα πληροί τις απαιτήσεις ελεγξιμότητας των άρθρων 93 παρ. 3Σ και 139 ΚΠΔ αντίστοιχα. Ειδικότερα, το βούλευμα θα πρέπει να περιλαμβάνει μνεία: α) της αξιόποινης πράξη για την εξιχνίαση της οποίας διατάσσεται η επέμβαση, β) των σοβαρών ενδείξεων τέλεσης της πράξης, γ) του σκοπού της επέμβασης, της αδυναμίας ή ιδιαίτερης δυσχέρειας εξάρθρωσης της οργάνωσης, ε) της απολύτως αναγκαίας χρονικής διάρκειας του μέτρου και στ) του/των προσώπου/ων εναντίον των οποίων στρέφεται το μέτρο και για τα οποία υφίστανται σοβαρές ενδείξεις συμμετοχής τους στη δράση της εγκληματικής οργάνωσης.

5.3 Οι ελλείπουσες εγγυήσεις και τα κενά του σχετικού νομικού πλαισίου

Εξέχουσα θέση καταλαμβάνει το συνδεόμενο με τον μυστικό χαρακτήρα των επίμαχων ανακριτικών πράξεων έλλειμμα ενημέρωσης του θιγόμενου προσώπου, σχετικά με το είδος του αποδεικτικού υλικού, τον τρόπο συλλογής του και τη χρήση του.

Σημαντικό και ευδιάκριτο είναι και το δεύτερο έλλειμμα των σχετικών διατάξεων, ήτοι της μη διάκρισης των προϋποθέσεων επέμβασης σε ανύποπτα πρόσωπα, έλλειμμα το οποίο παραπέμπει στο γενικότερο ζήτημα της αναπόφευκτης διεύρυνσης του κύκλου των προσώπων που θίγονται από τη διενέργεια των ειδικών ανακριτικών πράξεων. Στο πλαίσιο αυτό γεννάται η ανάγκη για τον αυστηρό διαχωρισμό των όρων διεξαγωγής των ειδικών ανακριτικών πράξεων ανάλογα με τον χαρακτήρα τους, έτσι ώστε όπου εμπλέκονται τρίτα πρόσωπα, να αυστηροποιούνται και οι προϋποθέσεις επέμβασης.

Συνοψίζοντας, το ελληνικό νομικό πλαίσιο διεξαγωγής ειδικών ανακριτικών πράξεων θα πρέπει –αν όχι να μεταρρυθμιστεί- σίγουρα να επανεξεταστεί υπό το φως της αποτελεσματικής προστασίας των προσβαλλόμενων ατομικών δικαιωμάτων, όχι μόνο λόγω των τεχνολογικών εξελίξεων, αλλά ειδικότερα των εγγυήσεων που απαιτούνται από τις σχετικές υπερνομοθετικής ισχύος διατάξεις, στον ενωσιακό χώρο και στο Συμβούλιο της Ευρώπης. Οι πρωτοφανείς πάντως για τα δεδομένα της ποινικής δίκης επεμβάσεις στα ατομικά δικαιώματα απαιτούν αντίστοιχες δικονομικές εγγυήσεις, από τη στιγμή που οι προληπτικές/κατασταλτικές κρατικές ενέργειες δεν είναι πάντα από μόνες τους θετικές/αρνητικές, αλλά κρίνονται από τις προϋποθέσεις διεξαγωγής τους.

6 Σύνοψη και Συμπεράσματα

Οι σύγχρονες τεχνολογίες, επέφεραν σημαντικές αλλαγές σε κάθε μορφή εγκληματικής συμπεριφοράς, που μέχρι σήμερα χαρακτηριζόταν συμβατική. Η αδιάκοπη εξάρτηση των ανθρώπινων δραστηριοτήτων από τις υποδομές πληροφοριών εγείρει το ζήτημα της ασφάλειας.

Σήμερα υπάρχει επιτακτική ανάγκη οι επιχειρήσεις να υλοποιούν τις δράσεις τους και να εκτελούν τον επιχειρηματικό σκοπό τους βασιζόμενες στην τεχνολογία και τα πληροφοριακά συστήματα, γεγονός που τις καθιστά πιο ευπαθείς σε εξωγενείς κινδύνους , με σημαντικότερο το κυβερνοέγκλημα.

Για την αντιμετώπιση του κινδύνου αυτού, κάθε Οργανισμός πρέπει να μεριμνήσει για την πρόληψη εκδήλωσης των κυβερνοεπιθέσεων, την ανίχνευση αυτών και την αντίδραση προς αποκατάσταση της ζημίας που προκλήθηκε από την επίθεση.

Η διαμορφωθείσα νέα πραγματικότητα καθιστά επιτακτική την ανάγκη για εξελιγμένες υπηρεσίες εντοπισμού και αποτροπής απειλών στον κυβερνοχώρο, λαμβάνοντας υπόψη ότι σημαντικός αριθμός κυβερνοεγκλημάτων παραμένουν στις μέρες

μας ακόμη αδίωκτα και ατιμώρητα, ενώ εξακολουθεί να υπάρχει σημαντική απουσία καταγγελιών.

Παράλληλα, ο μεγάλος χρόνος εντοπισμού που επιτρέπει στους κυβερνοεγκληματίες να αναπτύσσουν πολλαπλές εισόδους/εξόδους ή κερκόπορτες, η δύσκολη πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία και η προβληματική απόκτησή τους, σε συνδυασμό με την αποδοχή τους από τα δικαστήρια, η πολυπλοκότητα των δικαστικών διαδικασιών και της δικαιοδοσίας λόγω της διασυνοριακής φύσης των κυβερνοεγκλημάτων, επιβάλλουν την άμεση βελτίωση της ασφάλειας στον Κυβερνοχώρο, θέτοντας ως καθοριστικής σημασίας την ύπαρξη ενός αποτελεσματικού νομικού πλαισίου προστασίας για την οικοδόμηση εμπιστοσύνης και την ανάπτυξη αισθήματος ασφάλειας στον κόσμο του διαδικτύου.

Με την ανάπτυξη του εγκλήματος στον κυβερνοχώρο, το οποίο βρίσκεται στο υψηλότερο επίπεδο όλων των εποχών, η κυβερνοασφάλεια έχει γίνει ο ταχύτερα αναπτυσσόμενος τομέας τεχνολογίας. Η ανάγκη για την θωράκιση των επιχειρήσεων από τους κακόβουλους χρήστες είναι συνεχώς αυξανόμενη και η ραγδαία ανάπτυξη της τεχνολογίας καθιστά αναγκαία την ενσωμάτωση άρτιων διαδικασιών και ελέγχων.

Η κυβερνοασφάλεια επομένως, ήρθε για να εγκατασταθεί στις ζωές μας. Απομένει να αποδείξουμε ότι μπορούμε να αντεπεξέλθουμε στις προκλήσεις που φέρνει μαζί της.

7 Προτάσεις

Το κυβερνοέγκλημα, δεν είναι το ίδιο εύκολο στην αντιμετώπισή του με το παραδοσιακό έγκλημα. Ως εκ τούτου, προκειμένου να καταστεί εφικτή η επίτευξη σταθερότητας και η διατήρηση της τάξης στο εσωτερικό του κράτους, καθίσταται αναγκαία η πλήρης εποπτεία κάθε δραστηριότητας εντός του κυβερνοχώρου, γεγονός που σε κρατικό επίπεδο, μάλλον φαντάζει αδύνατο, λαμβανομένου υπόψη του όγκου και της ταχύτητας ανταλλαγής των πληροφοριών στο διαδικτυακό περιβάλλον. Αυτή η αβεβαιότητα λόγω της αδυναμίας πλήρους εποπτείας αποτελεί ταυτόχρονα το τρωτό σημείο που επιχειρούν να εκμεταλλευτούν οι τρομοκρατικές οργανώσεις και οι εγκληματίες, με σκοπό να πλήξουν την κυβερνοισχύ των κρατών.

Από τα ανωτέρω γίνεται αντιληπτό, ότι η πρόληψη και η καταστολή του κυβερνοεγκλήματος, λόγω του διασυνοριακού και ποικιλόμορφου χαρακτήρα του, χρήζει άμεσων και καίριων νομοθετικών καταστρώσεων στην κατεύθυνση δράσεων υπερεθνικού

ποινικού πλαισίου, καθώς και δικαστικής και αστυνομικής συνεργασίας σε εθνικό και διεθνές επίπεδο. Η συμβολή της Ευρωπαϊκής Ένωσης προς την κατεύθυνση αυτή είναι καθοριστικής σημασίας. Ωστόσο, οι προκλήσεις που αυτή έχει να αντιμετωπίσει, στο πλαίσιο ενός ψηφιακού και ιδιαιτέρως ανταγωνιστικού κόσμου που διαρκώς μεταβάλλεται και εξελίσσεται, γεννά το εύλογο ερώτημα αν και πως θα μπορέσει να αντεπεξέλθει.

Όπως έχει ήδη αναφερθεί, ο κυβερνοχώρος, δεδομένου ότι δε διαθέτει συγκεκριμένα γεωγραφικά σύνορα, παρέχει τη δυνατότητα πραγματοποίησης παράνομων δραστηριοτήτων σε περισσότερα κράτη, γεγονός που αναδεικνύει την αναγκαιότητα μιας αυξημένης, ταχείας και καλά συντονισμένης διεθνούς συνεργασίας σε θέματα ποινικού ενδιαφέροντος με την αμοιβαία ανταλλαγή τεχνογνωσίας και τεχνολογίας.

Ήδη έχουν γίνει αξιοσημείωτα βήματα προς αυτή την κατεύθυνση. Ωστόσο, μέσω της κοινής αντιμετώπισης των απειλών, γίνεται σαφές πως η νομοθεσία δεν καλύπτει πλήρως και πάντα τις ανάγκες της κοινωνίας. Το διαδίκτυο εξελίσσεται και διευρύνεται συνεχώς, καθιστώντας επιτακτική την ανάγκη διαρκούς επικαιροποίησης και αναδιαμόρφωσης των υφιστάμενων πολιτικών με στόχο την παρεμπόδιση κατάχρησης του διαδικτύου και τον περιορισμό της εγκληματικής δραστηριότητας εντός του κυβερνοχώρου.

Το υφιστάμενο νομικό πλαίσιο της ΕΕ για την αντιμετώπιση του κυβερνοεγκλήματος είναι μεν πλούσιο, αλλά ιδιαίτερα σύνθετο και με πολλές νομικές ασάφειες και ελλείψεις. Η απλούστευση της πληθώρας των Κανονισμών, Οδηγιών και Νόμων που ισχύουν σήμερα μέσω ενός ενοποιημένου και πιο εύληπτου για τον πολίτη νομικού πλαισίου, φαίνεται ως μία δελεαστική εναλλακτική λύση αντιμετώπισης του προβλήματος.

Η νομοθεσία της ΕΕ, επί του παρόντος, περιλαμβάνει κώδικες δεοντολογίας, νόμους, διατάξεις, κατευθυντήριες γραμμές, κανονισμούς και δράσεις για την πάταξη του ηλεκτρονικού εγκλήματος και την προστασία των δικαιωμάτων των πολιτών, ενώ τα κράτη μέλη εναρμονίζονται με τις ευρωπαϊκές επιταγές, ενσωματώνοντας το ευρωπαϊκό στο εθνικό τους δίκαιο. Το κάθε κράτος μέλος όμως έχοντας τις δικές του ιδιαιτερότητες και ανάγκες, θα μπορούσε να προβεί στην εφαρμογή επιπρόσθετων διατάξεων, βάσει των επιταγών της νομικής και θεσμικής του παράδοσης, όπως επίσης και των εθνικών προτεραιοτήτων του και να διευρύνει το επίπεδο κυβερνοισχύος του, θεσπίζοντας

επιπρόσθετα μέτρα και διατάξεις και εφαρμόζοντας αυστηρότερους ελέγχους, χωρίς φυσικά να έρχεται σε ρήξη και με το ευρωπαϊκό δίκαιο.

Από την πλευρά της η ΕΕ θα πρέπει να δημιουργήσει μία συνεκτική πολιτική απέναντι στο φαινόμενο της κυβερνοεγκληματικότητας, στοχεύοντας ταυτόχρονα στην ενίσχυση της διαφάνειας στα αδύναμα κράτη μέλη της και στην προστασία των πολιτών τόσο στις οικονομικά εύρωστες, όσο και στις ασθενέστερες συγκριτικά χώρες.

Με την διάχυση της τεχνογνωσίας και των πληροφοριών μεταξύ των κρατών μελών μπορεί να επιτευχθεί αμεσότερη, εγκυρότερη και εν τέλει αποδοτικότερη αντιμετώπιση των περιστατικών ασφάλειας και διαχείριση των ζητημάτων κυβερνοασφάλειας, εν γένει, έτσι ώστε να επιτύχουμε τόσο σε ευρωπαϊκό, αλλά και σε εθνικό επίπεδο την στοχευμένη και αποτελεσματικότερη αντιμετώπιση των κυβερνοαπειλών, ανοίγοντας τον δρόμο σε ένα πιο ενισχυμένο και αυξημένο επίπεδο κυβερνοασφάλειας.

Υπό το πρίσμα των βέλτιστων πρακτικών που θα μπορούσαν να αναπτύξουν οι επιχειρήσεις και οι Οργανισμοί για την καλύτερη πρόληψη και αντιμετώπιση των κυβερνοαπειλών, πρωταρχικής σημασίας είναι η υιοθέτηση ενός ολιστικού προγράμματος Κυβερνοασφάλειας για την αποτελεσματική διαχείριση των κινδύνων του Κυβερνοχώρου, επενδύοντας σε εξελισσόμενες τεχνικές προστασίας, οι οποίες θα τους καταστήσουν έτοιμους για να αντιμετωπίσουν και τις επερχόμενες απειλές. Οι πρακτικές αυτές θα πρέπει να επικεντρώνονται σε τέσσερις βασικούς πυλώνες, όπως είναι η Διακυβέρνηση, η Προστασία, η Επίγνωση και η Ανθεκτικότητα.

Η Διακυβέρνηση εστιάζει στο διαχειριστικό μέρος των τεχνικών προστασίας και πιο συγκεκριμένα σε θέματα που αφορούν τη στρατηγική του Οργανισμού γύρω από την Κυβερνοασφάλεια, τις αντίστοιχες πολιτικές που υποστηρίζουν τη στρατηγική, καθώς και τη διαχείριση κινδύνων. Η προστασία, περιλαμβάνει μία ευρεία γκάμα από τεχνικές δικλείδες ασφαλείας που σκοπό έχουν να προστατεύσουν τον Οργανισμό από κυβερνοεπιθέσεις τόσο σε ψηφιακό όσο και σε φυσικό επίπεδο. Ως Επίγνωση, νοείται η γνώση που κάθε Οργανισμός θα πρέπει να έχει ως προς τις δυνητικές απειλές που τον αφορούν, ώστε να είναι κατάλληλα προετοιμασμένος για τον περιορισμό και την αντιμετώπισή τους.

Η αποτελεσματική αντιμετώπιση των υφιστάμενων, αλλά και των μελλοντικών κυβερνοαπειλών απαιτεί τη δημιουργία ενός ολιστικού πλαισίου διακυβέρνησης για την

ασφάλεια των πληροφοριών. Η δόμηση του εν λόγω πλαισίου εξαρτάται από την κουλτούρα, το επιχειρηματικό και τεχνολογικό περιβάλλον, τον βαθμό ωριμότητας και την προσέγγιση για την επιχειρηματική βιωσιμότητα και ανθεκτικότητα σε επίπεδο ενός Οργανισμού ή/και ενός Κρατικού Θεσμού κατ' επέκταση.

Σε διακρατικό επίπεδο, οι κυβερνοεγκληματίες χρησιμοποιούν αυτοματοποιημένους μηχανισμούς για την ανίχνευση τεχνολογικών ευπαθειών και διαμοίρασης σχετικών πληροφοριών μεταξύ τους. Τα κράτη θα πρέπει να σχεδιάσουν ευέλικτες στρατηγικές για να αντιμετωπίσουν και να διαχειριστούν μελλοντικές Κυβερνοαπειλές. Η συνεχής θωράκιση των συστημάτων προλαμβάνει τις κυβερνοεπιθέσεις και περιορίζει σημαντικά τον βαθμό παρείσδυσης και τις επιπτώσεις των περιστατικών ασφάλειας. Συνεπώς, κύριο μέλημα όλων θα πρέπει να είναι η συνεργασία τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Δημόσιοι φορείς, ιδιωτικοί και παγκόσμιοι Οργανισμοί θα πρέπει να συνεργαστούν με σκοπό τον σχεδιασμό ενός δυναμικού στρατηγικού χάρτη για την κυβερνοασφάλεια. Η αντίληψη των απειλών και η ικανότητα της στρατηγικής ασφαλείας να ανταποκρίνεται στις συνθήκες, θα πρέπει να εξετάζεται και να επικαιροποιείται σε τακτά χρονικά διαστήματα.

Σε εθνικό επίπεδο, ιδιαίτερα οι Φορείς Δημόσιας Διοίκησης είναι σημαντικό να προβλέπουν στις επιμέρους πολιτικές Κυβερνοασφάλειας την εφαρμογή μέτρων «επιθετικής» άμυνας για την πρόληψη και την αντιμετώπιση μελλοντικών κινδύνων και να ορίζουν με σαφήνεια τα καθήκοντα ευθύνης και διαχείρισής τους, λειτουργώντας βάσει των κεντρικών οδηγιών της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης.

Εν κατακλείδι, όλες οι κυβερνήσεις πρέπει να εργαστούν για την επίτευξη μιας ενιαίας πολιτικής απάντησης για την πρόληψη επιθέσεων σε κάθε είδους υποδομές. Μόνο με τον συνδυασμό των δυναμικών τόσο του ιδιωτικού, όσο και του δημόσιου φορέα σε θέματα όπως η έγκαιρη προειδοποίηση, η προώθηση των καλύτερων πρακτικών και η συμφωνία σχετικά με πολιτικές προστασίας, θα καταστεί βέβαιη η αλλαγή στην τάση για την ασφάλεια των μηχανισμών του κυβερνοχώρου.

Η αποτελεσματική αντιμετώπιση των κυβερνοαπειλών, προϋποθέτει την ανάληψη δράσης σε ευρωπαϊκό και διεθνές επίπεδο και ιδίως την χρήση ενός κοινού, οικουμενικού ορισμού του κυβερνοεγκλήματος, ο οποίος θα λάβει υπόψη του ότι αυτού του είδους τα εγκλήματα δε "γνωρίζουν" τοπικούς και χρονικούς περιορισμούς, δεν προϋποθέτουν τη

φυσική υπόσταση και παρουσία των δραστών, ενώ δύνανται να αφορούν σε επιθέσεις, η ταχύτητα, η δυναμική και η μαζικότητα των οποίων μπορούν να λάβουν απροσδιόριστες και μη δυνάμενες να προβλεφθούν στο παρόν διαστάσεις στον ψηφιακό κόσμο.

Είναι αδύνατο να εξαλειφθεί το κυβερνοέγκλημα από τον κυβερνοχώρο ολοκληρωτικά. Ωστόσο αξίζει να προσπαθήσουμε, ώστε να θέσουμε τους κατάλληλους περιορισμούς που θα μετριάσουν την εξάπλωσή του.

Βιβλιογραφία – Δικτυογραφία

Βιβλία

- Κωνσταντίνος Βλαχόπουλος, Έκδοση 2007, Νομική Βιβλιοθήκη, Ηλεκτρονικό Έγκλημα -Μορφές, Πρόληψη, Αντιμετώπιση-
- Θ. Δαλακούρας (επιμ.), "Ηλεκτρονικό Έγκλημα", Νομική Βιβλιοθήκη, 2019
- Ιωάννης Δημ. Ιγγλεζάκης, Δ΄ Έκδοση 2021, εκδόσεις Σάκκουλα, Δίκαιο Πληροφορικής
- Α. Χαραλαμπάκης, Ο Νέος Ποινικός Κώδικας – Συνοπτική Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Νομική Βιβλιοθήκη, 2η έκδοση, σελ. 175

Ηλεκτρονικά Περιοδικά

- Journal of Criminal Law and Criminology,Volume 97, Issue 2 Winter Article 2, Winter 2007, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, Susan W. Brenner

  https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc

- IT SECURITY Professional, *Παναγιώτης Κικίλιας, Στέλεχος της Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος της Αστυνομίας, 1 Ιουλίου 2008,* "Κυβερνοτρομοκρατία και εφαρμογή νέων τεχνολογιών στην τρομοκρατία"

  https://www.itsecuritypro.gr/kyvernotromokratia-ke-efarmogi-neon-technologion-stin-tromokratia/

- e-πίκαιρα, 26 Σεπτεμβρίου 2008, "ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ: ΜΥΘΟΣ Ή ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ?"

  http://e-pikaira.blogspot.com/2008/09?m=1

- Ι. Ιγγλεζάκης, Δίκαιο και Νέες Τεχνολογίες, Συνήγορος, τεύχος 98, 2013, "Επιθέσεις κατά συστημάτων πληροφοριών"

Δημοσιεύσεις σε Νομικά Περιοδικά

- Θ. Δαλακούρας, "Οι ειδικές ανακριτικές πράξεις του άρ. 6 του Ν. 2928/2001, Ποινικά Χρονικά, ΝΑ/2001, σελ. 1022,
- Χρ. Νάϊντος, "Ειδικές ανακριτικές πράξεις: *Επίκαιρα ζητήματα", Ποινικά Χρονικά 2017, 491

- Ε. Συμεωνίδου – Καστανίδου, Η «βίαιη ριζοσπαστικοποίηση» στο στόχαστρο της Ευρωπαϊκής Ένωσης», ΠοινΧρον 2009, σελ. 583

Ιστοσελίδες

- Ελληνική Δημοκρατία, Υπουργείο Ψηφιακής Διακυβέρνησης, Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, Δεκέμβριος 2020,

  https://mindigital.gr/%CE%B5%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7-%CF%83%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%83-2020

- RESEARCHGATE, Gabriel Weimann, University of Haifa, 2006, “Terror on the Internet: The New Arena, The New Challenges”

  https://www.researchgate.net/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges, Gabriel Weimann)

- official website of the European Union, 2020, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient"

  https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

- http://vr.arch.uth.gr/VR-Arch/01_Cyberspace/index.html

- Μένω Ευρώπη, Βίκυ Καρυστινού, 1η Ιουνίου 2016, “Κυβερνοτρομοκρατία: Πραγματική Απειλή ή Σύγχρονη Νεύρωση;”

  http://www.menoeuropi.gr/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%84%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%AF%CE%B1-%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%B1%CF%80%CE%B5%CE%B9/

- Αδήωτος, "Κυβερνοτρομοκρατία”

  https://adiotos.wordpress.com/2010/11/29/electronic-terorism/

- INFOSEC, March 9, 2016 by Pierluigi Paganini, “The Ferizi Case: The First Man Charged with Cyber Terrorism”

  https://resources.infosecinstitute.com/topic/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/

- Αντιπτέραρχος (Μ) ε.α. Θεόδωρος Γιαννιτσόπουλος, Επίτιμος Διευθυντής Γ' Κλάδου ΓΕΑ, Αντιπρόεδρος Συνδέσμου Αποφοίτων Σχολής Ικάρων, "Η Μόνιμη Διαρθρωμένη Συνεργασία (Μ.Δ.Σ.) για την Άμυνα και την Ασφάλεια (PESCO) της Ευρωπαϊκής Ένωσης ως Μοχλός Εμβάθυνσης της Αμυντικής Συνεργασίας μεταξύ των Κρατών Μελών της ΕΕ και Πρώτιστη Ευκαιρία για το ΥΠΕΘΑ και την Αμυντική Βιομηχανία της Χώρας"

  https://www.militaire.gr/wp-content/uploads/2018/01/pesco.pdf

- SECURENET, 2017, Κυβερνοεπιθέσεις και κυβερνοασφάλεια στην Ελλάδα: Η θέση της χώρας μας στον αθόρυβο, ψηφιακό «πόλεμο»

  http://www.securnet.gr/2017/05/blog-post_8.html?m=1

- Νόμος 4411/2016 - Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο

  https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

- Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης, Δελτίο Τύπου, 16 Δεκεμβρίου 2020, Βρυξέλλες, "Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων"

  https://ec.europa.eu/commission/presscorner/detail/el/ip_20_2391

- Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης, Policy and legislation, δημοσίευση την 16 Δεκεμβρίου 2020, Shaping Europe's digital future/Proposal for directive on measures for high common level of cybersecurity across the Union

  https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

- Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης

  https://ec.europa.eu/greece/news/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%84%CE%B7%CF%82-%CE%B5%CE%B5-%CE%B7-%CE%B5%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE-%CF%80%CF%81%CE%BF%CF%84%CE%B5%CE%AF%CE%BD%CE%B5%CE%B9-%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1-%CE%BC%CE%B9%CE%B1%CF%82-%CE%BA%CE%BF%CE%B9%CE%BD%CE%AE%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%BC%CE%BF%CE%BD%CE%AC

%CE%B4%CE%B1%CF%82-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD_el

- United States Institute of peace, Gabriel Weimann, 2004, Cyberterrorism: How Real Is the Threat?

  https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat (,)

- Ηλεκτρονική αρθρογραφία (Scielo), Laura Mayer Lux, Lawer, 2018, Defining cyberterrorism (Una definición de ciberterrorismo)

  https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005

- Πανεπιστήμιο Τζορτζτάουν, Ντόροθι Ε. Ντένινγκ, 23 Μαΐου 2000

  https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

- ΒΙΚΙΠΑΙΔΕΙΑ – Ψηφιακή Επανάσταση

  https://el.m.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CE%B5%CF%80%CE%B1%CE%BD%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7