ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ

Διπλωματική Εργασία

του

Τελόπουλου Αντώνιου

Θεσσαλονίκη, 1/3/2024

ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ

Τελόπουλος Αντώνιος

Πτυχίο Πολιτικών Επιστημών Α.Π.Θ. ,2010

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Ι. Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 1/03/2024

Θεοχάρης Ι. Δαλακούρας	Δανιήλ Γεώργιος	Σαββίδης Νικόλαος
.....	.....	.....

Περιεχόμενα

Περίληψη

Η κυβερνοτρομοκρατία, ως έννοια, εμφανίστηκε στα τέλη του 20ού αιώνα με την ευρεία υιοθέτηση του διαδικτύου και των δικτύων υπολογιστών. Οι πρώτες επιθέσεις ήταν σχετικά απλές, όπως η αλλοίωση ιστοτόπων ή η παρεμπόδιση παροχής υπηρεσιών. Με την πάροδο του χρόνου, τα εργαλεία και οι τεχνικές που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου έγιναν πιο προηγμένα και τα κίνητρά τους πιο μοχθηρά, συμπεριλαμβανομένων πράξεων κυβερνοπολέμου, κλοπής ευαίσθητων δεδομένων και κυβερνοεπιθέσεων σε κρίσιμες υποδομές. Δεδομένης της ευρύτατης χρήσης του διαδικτύου σε κάθε έκφανση της καθημερινότητας και της διαρκώς αυξανόμενης εξάρτησης της κοινωνίας από την τεχνολογία, η απειλή της κυβερνοτρομοκρατίας καθίσταται όλο και πιο έντονη και θεωρείται πλέον μείζον ζήτημα ασφάλειας για τις κυβερνήσεις, τους οργανισμούς και τα άτομα. Στην παρούσα εργασία θίγονται λεπτομερώς όλοι οι παράγοντες που σχετίζονται με το θέμα καθώς και τα κίνητρα πίσω από αυτό το φαινόμενο. Με μια επικαιροποιημένη ματιά εξετάζονται και όλα τα σύγχρονα χαρακτηριστικά του φαινομένου.

Λέξεις κλειδιά: Κυβερνοτρομοκρατία, κυβερνοασφάλεια, διαδίκτυο, απειλή, μέτρα αντιμετώπισης

Abstract

Cyberterrorism as a concept emerged at the end of the 20th century with the widespread adoption of the internet and computer networks. The first attacks were relatively simple, such as website tampering or the obstruction of service provision. Over time, the tools and techniques used by cybercriminals have become more advanced and their motives more sinister, including acts of cyberwarfare, theft of sensitive data and cyberattacks on critical infrastructure. Given the widespread use of the internet in every aspect of everyday life and society's ever-increasing dependence on technology, the threat of cyberterrorism continues becomes more and more intense and is now considered a major security issue for governments, organisations and individuals. This paper touches in detail on all factors related to this issue as well as the motivations behind this phenomenon. With an updated look, all the contemporary features of the phenomenon are also examined.

Keywords: Cyber terrorism, cyber security, internet, threat, countermeasures

Ευχαριστίες,

1.0 Εισαγωγή

1.1 Ορισμός της κυβερνοτρομοκρατίας

Η παγκόσμια χρήση του Διαδικτύου διευκολύνθηκε από τον εκσυγχρονισμό της κοινωνίας και την πρόοδο της τεχνολογίας των πληροφοριών. Μια από τις σοβαρότερες μορφές ηλεκτρονικού εγκλήματος - η κυβερνοτρομοκρατία - εμφανίστηκε με την ανάπτυξη του παγκόσμιου δικτύου. Σε αντίθεση με την παραδοσιακή τρομοκρατία, η κυβερνοτρομοκρατία χρησιμοποιεί τις πιο πρόσφατες επιστημονικές και τεχνολογικές εξελίξεις για την πραγματοποίηση τρομοκρατικών επιθέσεων. Το 1980, ο Barry Collin, ανώτερος συνεργάτης του Ινστιτούτου Ασφάλειας και Πληροφοριών της Καλιφόρνια, επινόησε τη φράση "κυβερνοτρομοκρατία". Εκείνη την εποχή, το δίκτυο ARPANET της αμερικανικής Υπηρεσίας Προηγμένων Αμυντικών Ερευνητικών Προγραμμάτων (DARPA) συνέδεε μόνο έναν μικρό αριθμό υπολογιστών στο έδαφος μιας μόνο πολιτείας. Ο ερευνητής ήταν βέβαιος ότι τελικά οι τρομοκράτες θα χρησιμοποιήσουν κυβερνοδίκτυα, αλλά πίστευε ότι αυτό δεν θα συνέβαινε πριν από την πρώτη δεκαετία του εικοστού πρώτου αιώνα (Collin, 2008).

Η κυβερνοτρομοκρατία μπορεί να λάβει πολλές διαφορετικές μορφές, όπως η διάδοση επικίνδυνου λογισμικού (κακόβουλου λογισμικού), η παραβίαση ζωτικής σημασίας υποδομών και η διαδικτυακή διάδοση παραπλανητικών πληροφοριών. Ο κύριος στόχος των κυβερνοτρομοκρατών είναι να προκαλέσουν φόβο, πανικό και αναταραχή στην κοινωνία, διαταράσσοντας τις συνήθεις δραστηριότητες και καλλιεργώντας ένα αίσθημα ανησυχίας. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Για παράδειγμα, μπορεί να αφορά την παραβίαση επίσημων δικτυακών τόπων, τη διάδοσης ψευδών πληροφοριών και τής παρεμβολής σε δίκτυα επικοινωνίας (Kshetri, Diffusion and Effects of Cyber-Crime in Developing Economies, 2010).

Λόγω των πολιτικών ή ιδεολογικών στόχων της, η κυβερνοτρομοκρατία συχνά διακρίνεται από άλλους τύπους εγκλημάτων στον κυβερνοχώρο, όπως η πειρατεία και η κλοπή δεδομένων. Οι κυβερνοτρομοκράτες εργάζονται συχνά για την προώθηση ενός συγκεκριμένου πολιτικού στόχου ή αιτήματος και οι πράξεις τους αποσκοπούν στο να δημιουργήσουν φόβο και ανασφάλεια σε πολίτες και φορείς. Ως αποτέλεσμα, η κυβερνοτρομοκρατία αποτελεί μια ιδιαίτερα ύπουλη

απειλή, καθώς έχει τη δυνατότητα να διαβρώσει την εμπιστοσύνη του κοινού σε κρίσιμους θεσμούς και διαδικασίες που είναι απαραίτητες για τη λειτουργία της κοινωνίας (Emery, 2005).

Η κυβερνοτρομοκρατία έχει σημαντικό δυνητικό αντίκτυπο που μπορεί να γίνει αισθητός σε διάφορους κλάδους, όπως η κυβέρνηση, ο στρατός, ο χρηματοπιστωτικός τομέας, η υγειονομική περίθαλψη και οι μεταφορές. Για παράδειγμα, ένα κυβερνο-τρομοκρατικό χτύπημα σε ένα νοσοκομείο θα μπορούσε να εμποδίσει τους ασθενείς να λάβουν ιατρική περίθαλψη και να θέσει σε κίνδυνο τη ζωή τους. Ενώ μια κυβερνοεπίθεση σε ζωτικά συστήματα υποδομής, όπως τα δίκτυα ηλεκτρικής ενέργειας ή η παροχή νερού, θα μπορούσε να έχει καταστροφικές συνέπειες για τη δημόσια ασφάλεια και το περιβάλλον, μια κυβερνοεπίθεση στον χρηματοπιστωτικό τομέα θα μπορούσε να προκαλέσει σημαντικές οικονομικές αναταράξεις (Kshetri, 2003).

Οι οργανισμοί είθισται να εφαρμόζουν ισχυρά μέτρα κυβερνοασφάλειας , θέτοντας σε εφαρμογή αποτελεσματικές στρατηγικές πρόληψης και αντιμετώπισης επιθέσεων, με απώτερο σκοπό την ουσιαστική εξάλειψη της κυβερνοτρομοκρατίας. Η εφαρμογή τειχών προστασίας και συστημάτων ανίχνευσης εισβολών, η τακτική αναβάθμιση του λογισμικού, η εκπαίδευση του προσωπικού, ώστε να είναι προσεκτικό απέναντι στις απειλές στον κυβερνοχώρο. και η επιδιόρθωση του λογισμικού αποτελούν χαρακτηριστικά παραδείγματα. Οι κυβερνήσεις και οι διεθνείς οργανισμοί συμβάλλουν, επίσης, σημαντικά στην καταπολέμηση της κυβερνοτρομοκρατίας προσπαθώντας να δημιουργήσουν ένα ασφαλές και σταθερό διαδικτυακό περιβάλλον και προσφέροντας υποστήριξη και τεχνική βοήθεια σε ομάδες που το χρειάζονται (Council of Europe, 2004).

Συμπερασματικά, η κυβερνοτρομοκρατία αποτελεί μια σοβαρή και αυξανόμενη απειλή για την κοινωνία, η οποία απαιτεί τις συλλογικές προσπάθειες κυβερνήσεων, οργανισμών και ατόμων για την αποτελεσματική αντιμετώπισή της. Με την κατανόηση της φύσης και του αντίκτυπου της κυβερνοτρομοκρατίας και με την εφαρμογή αποτελεσματικών μέτρων κυβερνοασφάλειας, μπορεί να υπάρξει μείωση του κινδύνου κυβερνοεπιθέσεων και να διασφαλιστεί ότι τα κρίσιμα συστήματα και τα θεσμικά ενός κράτους όργανα παραμένουν ασφαλή και ανθεκτικά απέναντι σε αυτή την εξελισσόμενη απειλή.

1.2 Σημασία της μελέτης της κυβερνοτρομοκρατίας στο σημερινό κόσμο.

Καθώς όλο και περισσότερες από τις καθημερινές δραστηριότητες και ευαίσθητες πληροφορίες διατηρούνται και κοινοποιούνται στο διαδίκτυο, η κυβερνοτρομοκρατία βρίσκει πρόσφορο πεδίο ταχέως κλιμακούμενης ανάπτυξης στη σημερινή κοινωνία. Ο τρόπος με τον οποίο ζούμε και δραστηριοποιούμαστε επηρεάζεται άμεσα και διαρκώς από τη χρήση του διαδικτύου και τις άλλες σύγχρονες τεχνολογικές εφαρμογές, καθιστώντας απλούστερο για τα άτομα και τους ποικίλους φορείς να επιδίδονται σε συμπεριφορές που μπορούν να οδηγήσουν στην πρόκληση βλάβης στους ίδιους ή σε τρίτα άτομα.

Η κυβερνοτρομοκρατία μπορεί να λάβει πολλές διαφορετικές μορφές, όπως η φυσική επίθεση, η διάδοση ψευδών πληροφοριών, η κλοπή ιδιωτικών πληροφοριών και η βλάβη ζωτικής σημασίας υποδομών. Οι ενέργειες αυτές έχουν τη δυνατότητα να πλήξουν σοβαρά άτομα, ομάδες, ακόμη και ολόκληρες χώρες, επηρεάζοντας τη δημόσια ασφάλεια, την οικονομική σταθερότητα και την εθνική ασφάλεια (Anderson, 2012).

Στο παρελθόν, οι τρομοκράτες χρησιμοποιούσαν κυρίως συμβατικές τεχνικές, όπως βομβιστικές επιθέσεις και αεροπειρατείες, για να επιτύχουν τους στόχους τους. Καθώς όμως οι άνθρωποι βασίζονται όλο και περισσότερο στην τεχνολογία, συνειδητοποιούν τη δυνατότητα των κυβερνοεπιθέσεων να προκαλέσουν πολύ μεγαλύτερη ζημιά. Η, σε βάθος, κατανόηση του τρόπου λειτουργίας και εφαρμογής αυτού του τρόπου επίθεσης είναι σημαντική γιατί επιτρέπει στους ανθρώπους, τις ομάδες και τις κυβερνήσεις να κατανοήσουν τη φύση αυτών των κινδύνων και να δημιουργήσουν αντίμετρα (Belkasim, 2017).

Οι οργανισμοί, για παράδειγμα, μπορούν να αμυνθούν καλύτερα από επιθέσεις ερευνώντας τις στρατηγικές, τις τακτικές και τις διαδικασίες που χρησιμοποιούν οι κυβερνοτρομοκράτες. Με σκοπό την αποτροπή της παράνομης πρόσβασης στα δίκτυα και τα συστήματά τους, μπορούν να θέσουν σε εφαρμογή μέτρα ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και κρυπτογράφηση. Οι οργανισμοί τα τελευταία χρόνια είναι σε θέση να εκπαιδεύουν τα μέλη του προσωπικού τους σχετικά με ασφαλείς συνήθειες στο διαδίκτυο, όπως η αποφυγή συνδέσμων και μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνονται ύποπτα, ώστε να μειωθεί η πιθανότητα επιτυχών επιθέσεων (Bukhres, 2019).

Σε δημοσιονομικό επίπεδο, έχει καταστεί σαφής η ανάγκη επίλυσης του φαινομένου της κυβερνοτρομοκρατίας ή τουλάχιστον η ανάσχεση του. Είναι γνωστό πως στο πλαίσιο της

καταπολέμησης του φαινομένου, παρατηρείται ισχυρή σύμπραξη κυβερνήσεων και επιχειρηματικού τομέα για τον σχεδιασμό κανόνων και πολιτικών κυβερνοασφάλειας, με επιμέρους επενδύσεις στη μελέτη και τη δημιουργία νέων τεχνολογιών που παρέχουν υποστήριξη στις οργανώσεις επιβολής του νόμου και στις υπηρεσίες πληροφοριών με τη μορφή εκπαίδευσης και εξοπλισμού. Προκειμένου να διασφαλίσουν μια συντονισμένη και επιτυχημένη αντιμετώπιση των κυβερνοεπιθέσεων, έχουν επιτευχθεί διακρατικές συνεργασίες με άλλες χώρες για τη δημιουργία διεθνών συμφωνιών και βέλτιστων πρακτικών για την ασφάλεια στον κυβερνοχώρο (Clarke, 2002).

Η μελέτη της κυβερνοτρομοκρατίας είναι ζωτικής σημασίας από πολιτιστική και κοινωνική άποψη, εκτός από την ενίσχυση της ασφάλειας. Ο σύγχρονος τρόπος ζωής εξαρτάται όλο και περισσότερο από το διαδίκτυο, το οποίο έχει, παράλληλα, δημιουργήσει νέες προκλήσεις και ευκαιρίες για επικοινωνία και συνεργασία. Μελετώντας την κυβερνοτρομοκρατία καθίσταται ευχερέστερη η κατανόηση της πολυπλοκότητας και της διασύνδεσης του διαδικτυακού κόσμου, καθώς και τις επιπτώσεις που μπορούν να έχουν οι κυβερνοεπιθέσεις στη ζωή και την κοινωνία των πολιτών (Weimann G. , 2004).

Συνοψίζοντας, η μελέτη της κυβερνοτρομοκρατίας είναι κρίσιμης σημασίας στον σημερινό κόσμο, καθώς βοηθά τα άτομα, τους οργανισμούς και τις κυβερνήσεις να κατανοήσουν τη φύση και το εύρος αυτών των απειλών και να αναπτύξουν αποτελεσματικές στρατηγικές για τον μετριασμό τους. Με την αυξανόμενη εξάρτηση από την τεχνολογία, είναι πιο σημαντικό από ποτέ να υπάρχει διαρκής ενημέρωση και προετοιμασία, ώστε να εξασφαλιστεί ένα ασφαλέστερο μέλλον για όλους.

2.0 Ιστορική επισκόπηση της κυβερνοτρομοκρατίας.

Η Κυβερνοτρομοκρατία είναι όρος που περιγράφει τρομοκρατικές πράξεις που διαπράττονται με τη χρήση ψηφιακών τεχνολογιών με σκοπό να βλάψουν πολίτες και οργανισμούς. Η ιστορία της κυβερνοτρομοκρατίας ξεκίνησε με την ανάπτυξη του διαδικτύου ως μέσου επικοινωνίας και ανταλλαγής πληροφοριών. Καθώς η χρήση του διαδικτύου αυξανόταν, προσέλκυε όλο και περισσότερο παραγόντων της παρανομίας που είδαν ένα νέο πεδίο ανάπτυξης των δραστηριοτήτων τους πρόσφορο για την εκπλήρωση των επιδιώξεων τους συμπεριλαμβανομένης της τρομοκρατίας.

Η πρώτη γνωστή περίπτωση κυβερνοτρομοκρατίας σημειώθηκε στα τέλη της δεκαετίας του 1980, όταν χάκερς που συνδέονταν με τη Legion of Doom εισήλθαν παράνομα σε κυβερνητικά δίκτυα υπολογιστών και έκλεψαν ιδιωτικά δεδομένα. Η χρήση του διαδικτύου και των ψηφιακών τεχνολογιών για τη διάπραξη τρομοκρατικών και βίαιων πράξεων σηματοδότησε την έναρξη μιας νέας εποχής της τρομοκρατίας (Dowdall, 2017).

Μια από τις πιο διαβόητες περιπτώσεις κυβερνοτρομοκρατίας έλαβε χώρα στα τέλη της δεκαετίας του 1990, όταν η "Σέχτα της Νεκρής Αγελάδας" των χάκερς εγκαινίασε ένα πρόγραμμα με την ονομασία "Back Orifice" που επέτρεπε στους επιτιθέμενους να διαχειρίζονται και να τροποποιούν εξ αποστάσεως τους υπολογιστές των στόχων τους. Με τη χρήση αυτής της τεχνολογίας πραγματοποιήθηκαν αρκετές κυβερνοεπιθέσεις υψηλού προφίλ, συμπεριλαμβανομένης της διακοπής λειτουργίας παρόχων υπηρεσιών διαδικτύου και της κλοπής ιδιωτικών πληροφοριών από κυβερνητικούς οργανισμούς (Dowdall, 2017).

Τα γεγονότα της 11ης Σεπτεμβρίου 2001 αποτέλεσαν τομή στην ανάπτυξη της κυβερνοτρομοκρατίας. Η κυβέρνηση των ΗΠΑ ενέτεινε την προσοχή της στην ασφάλεια στον κυβερνοχώρο στον απόηχο των επιθέσεων, διαθέτοντας χρήματα σε καινοτόμα εργαλεία και άμυνες κατά των κυβερνοεπιθέσεων. Ως αποτέλεσμα, δημιουργήθηκε το Υπουργείο Εσωτερικής Ασφάλειας, στο οποίο ανατέθηκε η ευθύνη της υπεράσπισης των ΗΠΑ από την τρομοκρατία και άλλα είδη εγκλημάτων (Siedersberger & Plattner, 2015).

Καθώς οι τρομοκράτες γίνονται όλο και πιο επιδέξιοι στη χρήση της ψηφιακής τεχνολογίας, η απειλή της κυβερνοτρομοκρατίας έχει κλιμακωθεί σημαντικά τα τελευταία χρόνια. Για παράδειγμα, μια συμμορία χάκερς που συνδέεται με το "Ρωσικό Επιχειρηματικό Δίκτυο"

εξαπέλυσε μια σημαντική κυβερνοεπίθεση εναντίον κυβερνητικών και στρατιωτικών συστημάτων υπολογιστών το 2007, η οποία είχε ως αποτέλεσμα σημαντικές διαταραχές και βλάβες. Το 2010 ανακαλύφθηκε το σκουλήκι Stuxnet, το οποίο αποτελεί άλλη μια αξιοσημείωτη περίπτωση κυβερνοτρομοκρατίας. Το σκουλήκι χρησιμοποιήθηκε για να υπονομεύσει το πυρηνικό πρόγραμμα του Ιράν και δημιουργήθηκε για να στοχεύσει βιομηχανικά συστήματα ελέγχου. Αυτή ήταν η πρώτη γνωστή περίπτωση κυβερνοεπίθεσης με κρατική χορηγία και έδειξε πόσο αποτελεσματικά μπορεί να είναι τα ψηφιακά όπλα σε συγκρούσεις (Siedersberger & Plattner, 2015).

Το Ισλαμικό Κράτος (ISIS) αναπτύχθηκε πρόσφατα και μαζί με την ανάπτυξη αυτή αυξήθηκε και η χρήση ψηφιακών τεχνολογιών από την οργάνωση για στρατολόγηση και προπαγάνδα. Το ISIS έχει επίσης συνδεθεί με διάφορες κυβερνοεπιθέσεις, συμπεριλαμβανομένης της παραβίασης των συστημάτων ηλεκτρονικού ταχυδρομείου της Εθνικής Επιτροπής των Δημοκρατικών το 2016. Η επιδημία λύτρων WannaCry τον Μάιο του 2017 αποτελεί μια ακόμη περίπτωση κυβερνοτρομοκρατίας. Σε 150 χώρες, το hack επηρέασε εκατοντάδες χιλιάδες υπολογιστές, προκαλώντας σημαντική αναστάτωση και βλάβες, Ένα στέλεχος κακόβουλου λογισμικού που χρησιμοποιήθηκε στην επίθεση ήταν αυτό που απέκτησαν οι Shadow Brokers, μια συμμορία χάκερ, από την Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ (Kshetri, 2017).

Αυτές είναι μόνο μερικές από τις πολυάριθμες περιπτώσεις κυβερνοτρομοκρατίας που έχουν σημειωθεί τα τελευταία χρόνια. Παρά τις εξελίξεις αυτές, σε σύγκριση με άλλα είδη τρομοκρατίας, η τρομοκρατία στον κυβερνοχώρο είχε πολύ μικρό αντίκτυπο. Η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο, η οποία καθιστά δύσκολη την υλοποίηση των στόχων των τρομοκρατών, καθώς και οι αυξημένες προσπάθειες των κυβερνήσεων, των οργανισμών και των ατόμων να υπερασπιστούν τα δίκτυα και τα συστήματά τους, συμβάλλουν σε αυτό.

Σε κάθε περίπτωση, η ιστορία της τρομοκρατίας στον κυβερνοχώρο εξελίσσεται με ταχείς ρυθμούς και υπογραμμίζει την ανάγκη για συνεχή επαγρύπνηση και συνεργασία μεταξύ κυβερνήσεων, οργανισμών και ατόμων, ώστε να διασφαλιστεί ότι το διαδίκτυο παραμένει ένας ασφαλής και προστατευμένος χώρος επικοινωνίας, εμπορίου και καινοτομίας.

2.1Προέλευση της κυβερνοτρομοκρατίας και η εξέλιξή της με την πάροδο του χρόνου.

Η κυβερνοτρομοκρατία αναφέρεται στη χρήση ψηφιακών τεχνολογιών για την επίτευξη πολιτικών ή κοινωνικών στόχων μέσω του φόβου, της βλάβης ή της καταστροφής. Ο όρος κυβερνοτρομοκρατία έγινε γνωστός τη δεκαετία του 1990, καθώς η εξάπλωση των υπολογιστών και του διαδικτύου επιταχύνθηκε. Οι απαρχές της κυβερνοτρομοκρατίας μπορούν να εντοπιστούν στις δεκαετίες του 1970 και 1980, όταν οι πολιτικοί ακτιβιστές άρχισαν να χρησιμοποιούν ηλεκτρονικά συστήματα για τους δικούς τους σκοπούς. Εκείνη την εποχή, οι επιθέσεις στρέφονταν κυρίως κατά κυβερνητικών υπηρεσιών και μεγάλων εταιρειών, οι οποίες θεωρούνταν σύμβολα πολιτικής και οικονομικής ισχύος (Weimann G. , 2004).

Με την ταχεία εξάπλωση του διαδικτύου τη δεκαετία του 1990 και την επακόλουθη πρόσβαση σε μεγαλύτερο αριθμό στόχων, η απειλή της κυβερνοτρομοκρατίας αυξήθηκε. Οι τρομοκρατικές ομάδες αναγνώρισαν την ευκαιρία να χρησιμοποιήσουν τα ηλεκτρονικά συστήματα για τη διάδοση πολιτικών μηνυμάτων, τη διάδοση του φόβου και την επίθεση σε κρίσιμες υποδομές, όπως ο ενεργειακός εφοδιασμός και τα χρηματοπιστωτικά συστήματα.

Στη δεκαετία του 2000, η κυβερνοτρομοκρατία συνέχισε να εξελίσσεται και έφτασε σε ένα νέο επίπεδο όταν αρκετές κυβερνήσεις και στρατιωτικές οντότητες άρχισαν να δραστηριοποιούνται επιθετικά στον κυβερνοχώρο. Το έγκλημα στον κυβερνοχώρο, συμπεριλαμβανομένου του ακτιβισμού και της κυβερνοτρομοκρατίας, αυξήθηκε ραγδαία, οδηγώντας σε έντονη συζήτηση για την ανάγκη αποτελεσματικότερης ρύθμισης και άμυνας στον κυβερνοχώρο (Dowdall, 2017).

Με την πάροδο του χρόνου, οι κυβερνήσεις και οι επιχειρήσεις έχουν βελτιώσει τις ικανότητές τους και τις στρατηγικές άμυνας κατά των κυβερνοεπιθέσεων, αλλά η απειλή της κυβερνοτρομοκρατίας παραμένει. Τα τελευταία χρόνια έχουν αυξηθεί οι επιθέσεις σε υποδομές ζωτικής σημασίας, όπως ο ενεργειακός εφοδιασμός και τα νοσοκομεία, καθώς και σε κυβερνητικές υπηρεσίες και πολιτικές οργανώσεις (Kshetri, 2017).

Τα επόμενα χρόνια, η απειλή της κυβερνοτρομοκρατίας αναμένεται να αυξηθεί, καθώς η εξάρτηση από τις ψηφιακές τεχνολογίες συνεχίζει να αυξάνεται και οι τρομοκράτες βελτιώνουν τις δυνατότητές τους στον κυβερνοχώρο. Υπό αυτό το πρίσμα, οι κυβερνήσεις και οι επιχειρήσεις καταβάλλουν προσπάθειες για να ενισχύσουν την άμυνά τους.

2.2 Σημαντικά περιστατικά κυβερνοτρομοκρατίας στην ιστορία.

Η κυβερνοτρομοκρατία είναι μια απειλή που έχει αυξηθεί τις τελευταίες δεκαετίες. Πρόκειται για τη χρήση ψηφιακών τεχνολογιών για την πραγματοποίηση τρομοκρατικών δραστηριοτήτων, όπως επιθέσεις σε κυβερνητικούς υπολογιστές, χρηματοπιστωτικά ιδρύματα και υποδομές ζωτικής σημασίας. Οι ρίζες της κυβερνοτρομοκρατίας μπορούν να εντοπιστούν στο 2000, όταν μια ομάδα χάκερ πραγματοποίησε επίθεση άρνησης παροχής υπηρεσιών στον ιστότοπο της CIA.

Όπως προαναφέρθηκε, ένα γεγονός που σχετίζεται με την κυβερνοτρομοκρατία ήταν οι τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, οι οποίες προκάλεσαν ένα κύμα κυβερνοεπιθέσεων σε κυβερνητικές υπηρεσίες και επιχειρήσεις των ΗΠΑ. Οι επιθέσεις χρησιμοποιήθηκαν για να διαδώσουν πολιτικά μηνύματα και να τροφοδοτήσουν το φόβο και την ανασφάλεια. Συγκεκριμένα, οι επιθέσεις στον κυβερνοχώρο δεν προκαλούν, κατά κύριο λόγο, υλικές ζημίες. Οι πρώτες αντιληπτές βλάβες είναι συνήθως οικονομικές, όπως έδειξαν οι επιθέσεις DDoS26 στην Εσθονία και τη Γεωργία. Είναι σημαντικό να αναφερθεί πως, η επίθεση κατά της εσθονικής κυβέρνησης το 2007 έθεσε εκτός λειτουργίας κυβερνητικούς υπολογιστές και ιστότοπους (Droogan & Waldek, 2018).

Και στις δύο επιθέσεις, κυβερνητικοί διακομιστές, υπουργεία, τράπεζες και μέσα μαζικής ενημέρωσης αποτέλεσαν στόχο και παρέλυσαν. Αν και δεν σημειώθηκε καμία φυσική ζημία, και οι δύο περιπτώσεις είναι σίγουρα σημαντικές για την κοινότητα του διεθνούς δικαίου. Η Εσθονία απέφυγε να επικαλεστεί την περίπτωση συμμαχίας βάσει του άρθρου 5 της Βορειοατλαντικής Συνθήκης και ενήργησε αποκλειστικά σε εθνικό επίπεδο, με αποτέλεσμα να επιφέρει ως συνέπεια αλλαγή και αυστηροποίηση του εθνικού ποινικού δικαίου και εντατικοποίηση της διακυβερνητικής συνεργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο. Στα πλαίσια του ΝΑΤΟ υπήρξε επιφύλαξη να χαρακτηριστεί μια επίθεση στον κυβερνοχώρο ως μια ένοπλη επίθεση που θα ενεργοποιούσε το δικαίωμα αυτοάμυνας. Ωστόσο, εκπρόσωπος του ΝΑΤΟ δήλωσε ότι πρόκειται για ένα ζήτημα ασφάλειας που είναι σημαντικό για το ΝΑΤΟ. Στη συνέχεια, εμπειρογνώμονες του ΝΑΤΟ στάλθηκαν στην Εσθονία για να αξιολογήσουν την κατάσταση και να εξετάσουν πιθανά μέτρα υποστήριξης. Το περιστατικό στην Εσθονία οδήγησε, επίσης, στη

δημιουργία του Συνεργατικού Κέντρου Αριστείας του ΝΑΤΟ για την κυβερνοάμυνα (Calafato & Caruana, 2015).

Η περίπτωση της Γεωργίας ήταν η πρώτη επίθεση στην οποία χρησιμοποιήθηκαν από κοινού κυβερνοεπιθέσεις και συμβατικά όπλα. Οι επιθέσεις σε δίκτυα υπολογιστών που εξαπολύθηκαν κατά της Γεωργίας κατέδειξαν, επίσης, τη χρησιμότητα των επιθέσεων που εξαπολύονται προς υποστήριξη συμβατικών χτυπημάτων. Στις επιθέσεις αυτές παρατηρήθηκε υψηλός βαθμός συντονισμού μεταξύ των επιθέσεων μέσω δικτύων υπολογιστών κατά στόχων σε συγκεκριμένες τοποθεσίες και του συμβατικού βομβαρδισμού τους. Αυτό καταδεικνύει ακόμη περισσότερο τον δυνητικό κίνδυνο που κρύβει αυτή η μορφή όπλων. Για παράδειγμα, οι στόχοι που πρόκειται να βομβαρδιστούν με συμβατικά όπλα μπορούν να παραλύσουν εκ των προτέρων με κυβερνοεπιθέσεις, ώστε να μειωθεί η αντίδραση του εχθρού (Pool, 2013).

Σε ένα πειραματικό εργαστήριο δοκιμών, οι ερευνητές του Εθνικού Εργαστηρίου του Idaho αναπαρέστησαν μια κυβερνοεπίθεση σε ένα μοντέλο του συστήματος ελέγχου ενός σταθμού παραγωγής ηλεκτρικής ενέργειας που περιλαμβάνει μια γεννήτρια ντίζελ. Οι ερευνητές κατάφεραν να χειραγωγήσουν τους διακόπτες κυκλώματος της γεννήτριας ντίζελ. Η συνέπεια ήταν η αυτοκαταστροφή του σταθμού παραγωγής ενέργειας.

Η περίπτωση του ιού Stuxnet το 2011, που παρουσιάστηκε στα μέσα ενημέρωσης, καταδεικνύει ότι οι κυβερνοεπιθέσεις μπορούν να οδηγήσουν σε φυσική ζημία. Ένας ιός υπολογιστή χρησιμοποιήθηκε για να στοχεύσει το σύστημα ελέγχου ενός ιρανικού πυρηνικού σταθμού παραγωγής ηλεκτρικής ενέργειας, με αποτέλεσμα τη φυσική καταστροφή μέρους του εξοπλισμού του σταθμού. Το κακόβουλο λογισμικό χειριζόταν την ταχύτητα περιστροφής των φυγοκεντρικών μηχανών που χρησιμοποιούνται για τον εμπλουτισμό ουρανίου. Μόλις η συχνότητα των κινητήρων της φυγόκεντρου έφτανε σε μια ορισμένη τιμή, ο ιός άρχιζε να ελέγχει την ταχύτητα των περιστροφών προς τα πάνω ή προς τα κάτω κατά βούληση, χωρίς οι αλλαγές να είναι εμφανείς στο σύστημα ελέγχου (Zampati, 2011).

Το ακόλουθο περιστατικό παρουσιάζει ιδιαίτερο ενδιαφέρον, Ο ιός που εξαπολύθηκε παρότι εξαπλώθηκε σε πολυάριθμους υπολογιστές σε όλο τον κόσμο, έδειξε την καταστροφική του επίδραση μόνο στο σύστημα SCAD39 που αναπτύχθηκε από τη Siemens "S-7". Δεδομένου ότι ο ιρανικός πυρηνικός σταθμός παραγωγής ενέργειας είναι ένα κλειστό σύστημα και δεν έχει σύνδεση με το διαδίκτυο, ο ιός εισήχθη πιθανώς μέσω ενός USB. Ως εκ τούτου, υπάρχει η υποψία

ότι αυτός ακριβός ο σταθμός παραγωγής ενέργειας ήταν επίσης ο στόχος της επίθεσης. Λόγω της πολυπλοκότητας του Stuxnet, οι ειδικοί υποθέτουν ότι οι δημιουργοί του έλαβαν κρατική βοήθεια (Zampati, 2011).

Ο "Φάκελος Αποχαιρετισμού" (Farewell Dossier) είναι ένα από τα πρώτα αναφερόμενα περιστατικά αυτού του τύπου κυβερνοτρομοκρατίας, το οποίο σημειώθηκε ήδη από το 1982 κατά τη διάρκεια του Ψυχρού Πολέμου. Μετά την κλοπή τεχνολογίας από τη σοβιετική KGB από τις δυτικές δυνάμεις, η αμερικανική CIA, με τη βοήθεια ενός καναδικού κατασκευαστή λογισμικού, εισήγαγε κακόβουλο κώδικα στο σύστημα ελέγχου ενός αγωγού φυσικού αερίου ενός σταθμού παραγωγής ηλεκτρικής ενέργειας. Αυτό οδήγησε σε μια τεράστια έκρηξη του σταθμού παραγωγής ενέργειας. Το λογισμικό του αγωγού που θα λειτουργούσε τις αντλίες, τις τουρμπίνες και τις βαλβίδες προγραμματίστηκε να ενεργοποιήσει τις δικλείδες ασφάλειας ατυχήματος να παθαίνει ατύχημα, μετά από ένα χρονικό διάστημα αρκετά μεγάλο ώστε να επαναφέρει τις ταχύτητες των αντλιών και τις ρυθμίσεις των βαλβίδων και να παραχθούν πιέσεις πολύ μεγαλύτερες από αυτές που ήταν αποδεκτές από τις ενώσεις και τις συγκολλήσεις του αγωγού. Το αποτέλεσμα ήταν η πιο μνημειώδης μη πυρηνική έκρηξη και πυρκαγιά που έχει παρατηρηθεί ποτέ από το διάστημα (Carr, 2013).

Συνολικά, μπορούμε να πούμε ότι η κυβερνοτρομοκρατία αποτελεί σοβαρή απειλή για την εθνική ασφάλεια και την οικονομία. Είναι σημαντικό οι κυβερνήσεις και οι επιχειρήσεις να λαμβάνουν μέτρα για την προστασία των συστημάτων και των δικτύων τους, διατηρώντας παράλληλα τις πολιτικές ελευθερίες και την προστασία των δεδομένων.

3.0 Χαρακτηριστικά της κυβερνοτρομοκρατίας.

Σύμφωνα με τον Αμερικανό ερευνητή Dan Werton, πολλές τρομοκρατικές ομάδες έχουν δημιουργήσει διαδικτυακές βάσεις δεδομένων πληροφοριών που χρησιμοποιούνται για τον σχεδιασμό επιθέσεων. Το συμπέρασμα αυτό έχει υποστηριχθεί από τις έρευνες ορισμένων τρομοκρατικών περιστατικών. Για παράδειγμα, έχει διαπιστωθεί ότι η τρομοκρατική οργάνωση Aum Shinrikyo, η οποία ήταν υπεύθυνη για την επίθεση με αέριο στο μετρό του Τόκιο το 1995, είχε προηγουμένως αναπτύξει ένα πρόγραμμα υπολογιστή που μπορούσε να υποκλέπτει τις ραδιοεπικοινωνίες της αστυνομίας και να εντοπίζει την τοποθεσία των περιπολικών της αστυνομίας (Gable, 2010).

Ως εμπειρογνώμονας του Κέντρου Μελέτης της Τρομοκρατίας των ΗΠΑ και επικεφαλής του Ινστιτούτου Ασφάλειας Πληροφοριών του Πανεπιστημίου Georgetown, η Dorothy Denning υποστηρίζει ότι υπάρχουν τρεις κατηγορίες τρομοκρατικής συμπεριφοράς στο διαδίκτυο: η δραστηριότητα, το χάκινγκ και η κυβερνοτρομοκρατία. Προτείνει τη χρήση μιας δραστηριότητας για την κατανόηση των βασικών αρχών της τεχνολογίας των υπολογιστών με σκοπό την προώθηση ιδεών, την προσέλκυση χρημάτων και νέων οπαδών. Ο κυβερνοχώρος χρησιμοποιείται σε αυτή την περίπτωση για να φέρει σε επαφή τους τρομοκράτες και να στρατολογήσει νέα μέλη στις τρομοκρατικές οργανώσεις. Υπάρχουν, επίσης, διαδικτυακοί τρόποι για τη συγκέντρωση χρημάτων για φιλανθρωπικούς σκοπούς, από την απλή δωρεά χρημάτων μέσω των προτεινόμενων μεθόδων του ιστότοπου μέχρι τη λειτουργία ολοκληρωμένων διαδικτυακών καταστημάτων. Χαρακτηριστική περίπτωση είναι η Χεζμπολάχ πωλεί βιβλία, αφίσες και μπλουζάκια με τα διακριτικά της μέσω του ιστότοπού της (Conway, 2003).

Hacking είναι η εγκληματική επίθεση σε ιστότοπους, βάσεις δεδομένων και δίκτυα υπολογιστών με στόχο την απόκτηση δεδομένων ή την κλοπή χρημάτων. Αν και η κυβερνοτρομοκρατία διεξάγεται με τρόπο παρόμοιο με το χάκινγκ, η Denning (1999) υποστηρίζει ότι πρόκειται για μια ξεχωριστή κατηγορία επιθέσεων σε υπολογιστές που σχεδιάζονται με διαφορετικούς στόχους, όπως είναι η πρόκληση μεγάλης ζημίας σε ζωτικής σημασίας υποδομές μέσω της χρήσης της τεχνολογίας της πληροφορίας. Θα πρέπει να αναγνωριστεί ότι και οι τρεις προαναφερθείσες κατηγορίες δραστηριοτήτων εξακολουθούν να είναι σημαντικές. Σύμφωνα με την ορολογία της Denning (1999), η πιο διαδεδομένη από αυτές είναι η απλή διαδικτυακή τρομοκρατία.

Το θέμα της πρόληψης της κυβερνοτρομοκρατίας αποτελεί μια από τις κορυφαίες προτεραιότητες της κυβέρνησης, επειδή χώρες του προηγμένου κόσμου έχουν ενσωματώσει ενεργά την αυτοματοποίηση και την τεχνολογία της πληροφορικής σε διάφορους κλάδους. Ανησυχίες για πιθανές κυβερνοεπιθέσεις τρομοκρατών κατά ηλεκτρονικών δικτύων κρατικών φορέων που ελέγχουν εγκαταστάσεις "υποδομών κρίσης" έχουν επίσης εκφραστεί από εκπροσώπους της Υπηρεσιών Ασφαλείας ανά το κόσμο. Στις κρίσιμες υποδομές ανήκουν οι πυρηνικοί σταθμοί παραγωγής ενέργειας, οι πυρηνικοί αντιδραστήρες, οι στρατιωτικές εγκαταστάσεις, οι αγωγοί πετρελαίου και φυσικού αερίου, κορυφαίες επιχειρήσεις του αμυντικοβιομηχανικού συμπλέγματος) (Denning, 1999).

Σε πολλά κράτη, το νομοθετικό πλαίσιο δεν έχει παράξει γνωμοδότηση σχετικά με τον ορισμό του όρου "κυβερνοτρομοκρατία". Σύμφωνα με ορισμένους συγγραφείς, η κυβερνοτρομοκρατία αποτελείται από ένα φάσμα παράνομων δραστηριοτήτων, συμπεριλαμβανομένων των απόπειρων κατά της ανθρώπινης ζωής, της καταστροφής περιουσίας, της παραποίησης γεγονότων και άλλων δραστηριοτήτων που υποδαυλίζουν το φόβο και την ένταση στην κοινωνία σε μια προσπάθεια να προωθηθούν πολιτικοί, οικονομικοί ή κοινωνικοί στόχοι. Εάν οι πράξεις αυτές έγιναν με σκοπό να θέσουν σε κίνδυνο τη δημόσια ασφάλεια, να τρομάξουν τον πληθυσμό ή να υποκινήσουν ένοπλη σύρραξη, μπορεί να θεωρηθεί σκόπιμη επίθεση σε πληροφορίες που επεξεργάζεται ένας υπολογιστής, ένα υπολογιστικό σύστημα ή ένα δίκτυο, θέτοντας σε κίνδυνο την ανθρώπινη ζωή και υγεία (Brill, 2010).

Παρόμοια άποψη έχει, παρεμπιπτόντως, και ο Ronald Dick (2002), διευθυντής του Εθνικού Κέντρου Προστασίας Υποδομών του FBI των ΗΠΑ, ο οποίος σε έκθεσή του το 2002, που δημοσιεύτηκε, στον ιστότοπο του κυβερνητικού οργανισμού χαρακτήρισε την εξάρτηση από την τεχνολογία των υπολογιστών "*την αχίλλειο πτέρνα του σύγχρονου κόσμου*" και επισήμανε ότι η κυβερνοτρομοκρατία είναι ένας νέος τύπος τρομοκρατίας που χρησιμοποιεί υπολογιστές και δίκτυα για να στοχεύσει τις δημόσιες υποδομές και να επιτύχει τους στόχους της. Από την άποψη αυτή, είναι σημαντικό να θυμόμαστε ότι η κυβερνοτρομοκρατία είναι μια σύγχρονη μορφή τρομοκρατίας που στοχεύει σε δημόσιες υποδομές και χρησιμοποιεί υπολογιστές και δίκτυα για την επίτευξη των στόχων της.

Ενδιαφέρον παρουσιάζει η εκτίμηση των συγγραφέων που συνδέει την κυβερνοτρομοκρατία με την παράνομη επίδραση στα συστήματα πληροφοριών με σκοπό τη δημιουργία κινδύνου βλάβης για τη ζωή, την υγεία και την περιουσία ενός ευρέος φάσματος ανθρώπων, δημιουργώντας τις προϋποθέσεις για ατυχήματα και καταστροφές ανθρωπογενούς φύσης ή πραγματική απειλή τέτοιου κινδύνου. Η κυβερνοτρομοκρατία είναι ικανή να καταστρέψει συστήματα διαχείρισης πληροφοριών και υποδομών (μεταφορές, ενέργεια κ.λπ.) και να οδηγήσει σε σοβαρές συνέπειες, όπως εκρήξεις σε πυρηνικούς σταθμούς παραγωγής ενέργειας παρόμοιες με το ατύχημα του Τσερνομπίλ, δυστυχήματα στα οποία εμπλέκονται τρένα και αεροπλάνα, απελευθέρωση τοξικών και ρυπογόνων ουσιών στο περιβάλλον κ.λπ .

Θα πρέπει να σημειώσουμε, συγκεκριμένα, τις περιπτώσεις όπου ο εκφοβισμός του κοινού επιτυγχάνεται με τη δημοσίευση ειδήσεων που μπορούν να προκαλέσουν πανικό και αίσθημα αδυναμίας στο γενικό πληθυσμό σε ιστότοπους που ελέγχονται από τρομοκράτες, ή απλά σε δημόσιο χώρο, όπως στο κανάλι βίντεο στο YouTube. Τέτοιοι ιστότοποι μπορεί, για παράδειγμα, να διαθέτουν τρομακτικές εικόνες και βίντεο. Μια από τις πρώτες ομάδες που χρησιμοποίησαν το δίκτυο για τον λόγο αυτό ήταν η περουβιανή ομάδα Tupac Amaru, η οποία το 1996 απήγαγε μερικές δεκάδες άτομα κατά τη διάρκεια μιας δεξίωσης στην ιαπωνική πρεσβεία. Οι ηγέτες του Tupac Amaru ενθαρρύνονταν σωματικά να σχολιάσουν τα γεγονότα από δημοσιογράφους σε προπαγανδιστικούς ιστότοπους που είχαν φτιάξει οι υποστηρικτές του (Denning, 1999).

Η Αλ Κάιντα ήταν η πρώτη ομάδα που χρησιμοποίησε το Διαδίκτυο για να δημοσιεύει απειλές και ειδοποιήσεις σχετικά με επικείμενες τρομοκρατικές ενέργειες. Τελικά και άλλα ριζοσπαστικά κινήματα υιοθέτησαν την ιδέα αυτή. Τα βίντεο με τις δολοφονίες Αμερικανών και Βρετανών δημοσιογράφων από μέλη του αυτοαποκαλούμενου Ισλαμικού Κράτους που τους είχαν απαγάγει μεταξύ Αυγούστου και Δεκεμβρίου 2014 όχι μόνο δημοσιεύτηκαν από τους τρομοκράτες, αλλά και διαμοιράστηκαν ευρέως στο διαδίκτυο μέσω διαφόρων ειδησεογραφικών πηγών και των προσπαθειών των ίδιων των χρηστών του διαδικτύου. Οι άνθρωποι σε όλο το κόσμο επηρεάστηκαν βαθιά από το βίντεο των δημοσιογράφων που αρχικά κατηγόρησαν τις κυβερνήσεις των Ηνωμένων Πολιτειών, του Ηνωμένου Βασιλείου και της Ιαπωνίας ότι σκότωσαν αμάχους στις αεροπορικές επιδρομές στη Συρία, πριν τους κόψουν τα κεφάλια (Asongu, Orim , & Nting , 2019).

Τέτοιες συμπεριφορές έχουν αναμφισβήτητα αποδειχθεί ότι είναι από τις πιο αποτελεσματικές στρατηγικές ψυχολογικού πολέμου. Επιπλέον, είναι εφικτό να ισχυριστεί κανείς ότι οι επιχειρήσεις αυτές υποκινούνται από τρομοκρατικούς στόχους για να επηρεάσουν τα όργανα λήψης αποφάσεων εντός των κυβερνήσεων ή των διεθνών οργανισμών με βάση τα αιτήματα των εγκληματιών. Επομένως, εφόσον στην προκειμένη περίπτωση έχουμε να κάνουμε με πραγματική τρομοκρατία, ο ορισμός της κυβερνοτρομοκρατίας πρέπει να διευρυνθεί. Συνεπώς, η κυβερνοτρομοκρατία κρίνεται ως η σκόπιμη εγκληματική εισβολή σε έναν πληροφοριακό πόρο ή η χρήση αυτού του πόρου, εκφοβίζοντας τον πληθυσμό και αυξάνοντας τον κίνδυνο ανθρώπινου θανάτου, προκαλώντας σημαντικές υλικές ζημιές ή άλλες σοβαρές συνέπειες σε μια προσπάθεια να επηρεαστούν οι αρχές λήψης αποφάσεων (United Nations, 2018).

Σύμφωνα με αυτή την εννοιολόγηση, θα πρέπει να υπάρξει διαχωρισμός σε δύο ομάδες ανεξάρτητων τρόπων διάπραξης της κυβερνοτρομοκρατίας. Οι επιθέσεις σε δίκτυα υπολογιστών και υποδομές θα πρέπει να περιλαμβάνονται στην πρώτη ομάδα. Η οργάνωση καταστροφικών επιθέσεων, όπως είναι η καταστροφή πληροφοριακών πόρων και γραμμών επικοινωνίας ή φυσική καταστροφή δομών που ενσωματώνουν πληροφοριακά συστήματα ή η απενεργοποίηση πληροφοριακών συστημάτων. Η τελευταία θα είχε ως αποτέλεσμα την ανεξέλεγκτη λειτουργία της πληγείσας εγκατάστασης, η οποία είναι ιδιαίτερα επικίνδυνη σε εγκαταστάσεις πυρηνικής και χημικής παραγωγής καθώς και στον στρατό για συστήματα άμυνας και επίθεσης είναι παραδείγματα που χρησιμοποιούνται από ειδικούς. Η νόμιμη χρήση της τεχνολογίας των υπολογιστών για την ανάρτηση πληροφοριών στο δίκτυο που μπορούν να εκφοβίσουν τους ανθρώπους και περιλαμβάνουν ενδείξεις μιας διαπραχθείσας τρομοκρατικής πράξης θα πρέπει να συμπεριληφθεί στη δεύτερη ομάδα τρόπων διάπραξης κυβερνοεπίθεσης. Χαρακτηριστική περίπτωση είναι η δημοσίευση του βίντεο της εκτέλεσης των δημοσιογράφων (United Nations, 2018).

Ταυτόχρονα, είναι σημαντικό να μην υπεραπλουστεύονται οι πιθανές δυνατότητες τρομοκράτησης πολιτών και κυβερνητικών αξιωματούχων μέσω ενός δικτύου. Είναι σημαντικό , επίσης, να λαμβάνονται υπόψη οι σοβαρές πιθανές επιπτώσεις της κυβερνοτρομοκρατία όπως είναι ο σοβαρός κίνδυνος ανθρώπινου θανάτου, οι σημαντικές υλικές ζημιές ή άλλες σοβαρές επιπτώσεις.

Ωστόσο, παρά το φόβο που δημιουργείται δεν μπορούν να κατηγοριοποιηθούν όλες οι περιπτώσεις επιβλαβών ενεργειών στο διαδίκτυο ως κυβερνοτρομοκρατία ή να συνιστούν αντικείμενα εκμετάλλευσης για άλλους σκοπούς. Χαρακτηριστική περίπτωση το γεγονός ότι ορισμένοι χρησιμοποιούν το περιστατικό των WikiLeaks ως παράδειγμα κυβερνοτρομοκρατικής δραστηριότητας. Σύμφωνα με διάφορες πηγές, ο Τζούλιαν Ασάνζ, ο ιδρυτής του WikiLeaks, δεν έχει ακόμη κατηγορηθεί για τρομοκρατικά αδικήματα από τον Μάρτιο του 2015. Αν και πολλές πηγές πιστοποιούν την πιθανή επιθυμία των αμερικανικών αρχών να εμπλέξουν τον εν λόγω πολίτη για την αποκάλυψη κρατικών μυστικών, ακόμη και αυτός ο χαρακτηρισμός διαφέρει σημαντικά από τον γενικά αποδεκτό ορισμό της τρομοκρατίας (Walker, 2006).

Η καταπολέμηση της κυβερνοτρομοκρατίας θα πρέπει να χωριστεί σε δύο ξεχωριστές προσεγγίσεις, στη βάση της αναγνώρισης δύο διακριτών τύπων πράξεων. Για την αντιμετώπιση των επιθέσεων που πραγματοποιούνται μέσω της τεχνολογίας των υπολογιστών, οι πιο επιτυχημένες μέθοδοι περιλαμβάνουν οργανωτικά και νομικά μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε πληροφοριακούς πόρους, συμπεριλαμβανομένων των μεθόδων προστασίας των πληροφοριών από υλικό και λογισμικό. Για τη χρήση του Διαδικτύου και την αποτροπή τρομοκρατικών δραστηριοτήτων, η εστίαση πρέπει να δοθεί στον αποκλεισμό εξτρεμιστικών ιστότοπων και πόρων (Denning, 1999).

Τα Ηνωμένα Έθνη ασχολήθηκαν για πρώτη φορά με το θέμα αυτό το 1998 με ψήφισμα που εγκρίθηκε από τη Γενική Συνέλευση. Ο Γενικός Γραμματέας έχει υποβάλει ετήσιες εκθέσεις στη Γενική Συνέλευση του ΟΗΕ, όπου τα κράτη μέλη συζήτησαν τις απόψεις τους για το θέμα και τόνισαν την ανάγκη συλλογικής δράσης. Πιο συγκεκριμένα, δημιουργήθηκαν δύο ομάδες κυβερνητικών εμπειρογνωμόνων, με την πρώτη ομάδα να συνεδριάζει το 2004 και το 2005, αλλά να μην μπορεί να καταλήξει σε συναίνεση λόγω του νεοαναφυόμενου και πολύ καινούργιων ζητημάτων που αφορούν την προστασία του κυβερνοχώρου. Η δεύτερη ομάδα ξεκίνησε τις εργασίες της το 2009 και μέχρι το 2010 μπόρεσε να συμφωνήσει σε μια έκθεση σχετικά με τις τρέχουσες και δυνητικές απειλές του κυβερνοχώρου και να διερευνήσει συλλογικά μέτρα για την αντιμετώπισή τους. Στη συνέχεια. αποφασίστηκε να συνεχιστούν οι εργασίες αυτές προκειμένου να βελτιωθεί η διεθνής συνεργασία και ενδεχομένως να μετατραπεί από μια συζήτηση σε έναν ρυθμισμένο τομέα (United Nations, 2018).

Σε διεθνές επίπεδο, υπάρχει η Σύμβαση για Το Έγκλημα στο Κυβερνοχώρο, η οποία υπογράφηκε από τα κράτη μέλη του Συμβουλίου της Ευρώπης στις 23 Νοεμβρίου 2001. Το έγγραφο αυτό περιγράφει τη διαδικασία συνεργασίας μεταξύ των χωρών για την αντιμετώπιση των εγκλημάτων κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών, καθώς και των αδικημάτων που σχετίζονται με τις εγκαταστάσεις ηλεκτρονικών υπολογιστών, το περιεχόμενο των δεδομένων και τις παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας. Πολλά από τα μέτρα που περιγράφονται στη Σύμβαση για την αποτροπή μη εξουσιοδοτημένων παρεμβάσεων σε συστήματα υπολογιστών μπορούν να χρησιμεύσουν ως εμπόδιο κατά των τρομοκρατικών εγκλημάτων (Csonka, 2006).

Το 2001 υπογράφηκε στο Μινσκ συμφωνία για τη συνεργασία στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Τα μέρη καθόρισαν τις έννοιες "εγκλήματα κατά της πληροφορικής", "κακόβουλο λογισμικό" και "παράνομη πρόσβαση", καθόρισαν κατάλογο τιμωρητέων πράξεων και μορφές συνεργασίας για την πρόληψη και την καταστολή τους. Ωστόσο, η έννοια της τρομοκρατίας στον κυβερνοχώρο, καθώς και τυχόν δεσμοί μεταξύ των εν λόγω αδικημάτων και των τρομοκρατικών αδικημάτων, δεν καθορίζονται από τη συμφωνία. Αντίθετα, ο κανονισμός αυτός αποσκοπεί στην καταπολέμηση του hacking, το οποίο, σύμφωνα με την ορολογία της Dorothy Denning, αποτελεί έναν από τους πιθανούς τρόπους διάπραξης της κυβερνοτρομοκρατίας, αλλά δεν εξαντλεί το φαινόμενο (Denning, 1999).

Συνοψίζοντας την εξέταση του φαινομένου της κυβερνοτρομοκρατίας, πρέπει να σημειωθεί ότι η διάπραξη τρομοκρατικών ενεργειών υψηλής τεχνολογίας στον 21ο αιώνα είναι ικανή να προκαλέσει παγκόσμια κρίση πληροφοριών και να θέσει σε κίνδυνο την ύπαρξη ορισμένων περιοχών του κόσμου. Η κατάσταση επιδεινώνεται από το γεγονός ότι η αντίδραση του ποινικού δικαίου στη διαδικτυακή τρομοκρατία δεν έχει ακόμη αντιμετωπίσει επαρκώς τη σοβαρότητα της απειλής. Στο πλαίσιο αυτό, το ενδιαφέρον του ποινικού δικαίου στον τομέα της αντιμετώπισης των επιθέσεων στον κυβερνοχώρο από τρομοκράτες θα πρέπει να αποτελέσει έναν από τους τομείς προτεραιότητάς της.

3.1 Διάκριση μεταξύ κυβερνοεγκλήματος και κυβερνοτρομοκρατίας.

Το έγκλημα στον κυβερνοχώρο και η κυβερνοτρομοκρατία είναι δύο μορφές κακόβουλης δραστηριότητας που λαμβάνουν χώρα στο ψηφιακό πεδίο. Ενώ υπάρχουν ομοιότητες μεταξύ των δύο, υπάρχουν επίσης αρκετές βασικές διαφορές που καθιστούν σημαντική την κατανόηση της διάκρισης. Το έγκλημα στον κυβερνοχώρο αναφέρεται σε παράνομες δραστηριότητες που διαπράττονται χρησιμοποιώντας το διαδίκτυο ή άλλες μορφές ψηφιακής τεχνολογίας. Παραδείγματα εγκλημάτων στον κυβερνοχώρο είναι η πειρατεία, η κλοπή ταυτότητας, η απάτη, η διαδικτυακή παρακολούθηση και η διανομή παράνομου υλικού ή υλικού που προστατεύεται από πνευματικά δικαιώματα. Το έγκλημα στον κυβερνοχώρο έχει συχνά ως κίνητρο το οικονομικό κέρδος ή την προσωπική εκδίκηση (Taylor, Fritsch, Liederbach, Saylor, & Tafoya, 2019).

Η κυβερνοτρομοκρατία, από την άλλη πλευρά, αναφέρεται στη χρήση της ψηφιακής τεχνολογίας για τη διάπραξη πράξεων βίας ή καταστροφής με σκοπό την πρόκληση εκτεταμένου φόβου, πανικού ή αναστάτωσης. Παραδείγματα κυβερνοτρομοκρατίας περιλαμβάνουν την ανάπτυξη κακόβουλου λογισμικού ή ιών για τη βλάβη συστημάτων υποδομής ζωτικής σημασίας, όπως σταθμοί παραγωγής ενέργειας, χρηματοπιστωτικά ιδρύματα ή στρατιωτικά δίκτυα, και τη χρήση ψηφιακής προπαγάνδας για τη διάδοση ψευδών πληροφοριών και τη δημιουργία μαζικού πανικού. Η κυβερνοτρομοκρατία έχει ως κίνητρο την επιθυμία να δημιουργήσει φόβο, τρόμο και πανικό, με απώτερο στόχο την υπονόμευση της εμπιστοσύνης στις κυβερνήσεις και τους θεσμούς (Holt, Burruss, & Bossler, 2015).

Όσον αφορά τις μεθόδους που χρησιμοποιούνται, το κυβερνοέγκλημα και η κυβερνοτρομοκρατία έχουν πολλές ομοιότητες. Και οι δύο βασίζονται στην ψηφιακή τεχνολογία για την επίτευξη των στόχων τους και οι δύο περιλαμβάνουν συχνά τη χρήση τεχνικών hacking για την απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες ή συστήματα. Ωστόσο, τα κίνητρα πίσω από τα εγκλήματα είναι πολύ διαφορετικά. Οι εγκληματίες στον κυβερνοχώρο συνήθως έχουν ως κίνητρο το οικονομικό κέρδος, ενώ οι κυβερνοτρομοκράτες έχουν ως στόχο να δημιουργήσουν χάος και να σπείρουν τη δυσπιστία (Li & Qinghui , 2021).

Μια άλλη βασική διαφορά μεταξύ του εγκλήματος στον κυβερνοχώρο και της κυβερνοτρομοκρατίας είναι η κλίμακα των επιπτώσεών τους. Ενώ το έγκλημα στον κυβερνοχώρο μπορεί να είναι καταστροφικό για μεμονωμένα θύματα, ο αντίκτυπός του συνήθως περιορίζεται στα θύματα και σε έναν σχετικά μικρό αριθμό ατόμων ή οργανισμών. Η κυβερνοτρομοκρατία,

από την άλλη πλευρά, έχει τη δυνατότητα να προκαλέσει εκτεταμένη ζημία και να επηρεάσει εκατομμύρια ανθρώπους, καθώς και να διαταράξει κρίσιμες υποδομές και ιδρύματα (Gross, Canetti, & Vashdi, 2017).

Ο τρόπος με τον οποίο το έγκλημα στον κυβερνοχώρο και η κυβερνοτρομοκρατία αντιμετωπίζονται από τις αρχές επιβολής του νόμου και τις κυβερνητικές υπηρεσίες διαφέρει επίσης. Το έγκλημα στον κυβερνοχώρο αντιμετωπίζεται συνήθως από εθνικές υπηρεσίες επιβολής του νόμου, όπως το Ομοσπονδιακό Γραφείο Ερευνών (FBI) στις Ηνωμένες Πολιτείες, ενώ η κυβερνοτρομοκρατία θεωρείται ζήτημα εθνικής ασφάλειας και συχνά αντιμετωπίζεται από στρατιωτικές υπηρεσίες ή υπηρεσίες πληροφοριών, όπως το Υπουργείο Εσωτερικής Ασφάλειας ή η Υπηρεσία Εθνικής Ασφάλειας (Gross, Canetti, & Vashdi, 2017).

Συμπερασματικά, το κυβερνοέγκλημα και η κυβερνοτρομοκρατία είναι δύο διαφορετικές μορφές κακόβουλης δραστηριότητας που λαμβάνουν χώρα στο ψηφιακό πεδίο. Ενώ και οι δύο βασίζονται στην ψηφιακή τεχνολογία για την επίτευξη των στόχων τους, τα κίνητρα πίσω από τα εγκλήματα και ο αντίκτυπος που έχουν είναι πολύ διαφορετικά. Η κατανόηση της διάκρισης μεταξύ εγκλήματος στον κυβερνοχώρο και κυβερνοτρομοκρατίας είναι σημαντική για την αποτελεσματική πρόληψη και αντιμετώπιση αυτών των απειλών.

3.2 Κοινές τακτικές που χρησιμοποιούν οι κυβερνοτρομοκράτες.

Η κυβερνοτρομοκρατία αναφέρεται στη χρήση της τεχνολογίας για την πρόκληση βλάβης ή διαταραχής σε άτομα, οργανισμούς ή κοινωνίες. Για να επιτύχουν τους στόχους τους, οι κυβερνοτρομοκράτες χρησιμοποιούν συχνά μια ποικιλία τακτικών που εκμεταλλεύονται τα τρωτά σημεία των τεχνολογικών συστημάτων και της ανθρώπινης συμπεριφοράς.

Οι απάτες ηλεκτρονικού "ψαρέματος" είναι μια από τις πιο συνηθισμένες τακτικές που χρησιμοποιούν οι κυβερνοτρομοκράτες. Στόχος μιας απάτης phishing είναι να εξαπατήσει τα θύματα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών. Οι απάτες ηλεκτρονικού "ψαρέματος" έχουν συχνά τη μορφή πλαστών μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από μια αξιόπιστη πηγή, όπως ένα χρηματοπιστωτικό ίδρυμα ή μια γνωστή εταιρεία. Τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να περιέχουν μια αίσθηση επείγοντος ή φόβου για να ενθαρρύνουν τον

παραλήπτη να προβεί σε άμεσες ενέργειες, όπως να κάνει κλικ σε έναν σύνδεσμο ή να παράσχει πληροφορίες. Ο σύνδεσμος μπορεί να οδηγεί σε έναν ψεύτικο ιστότοπο που μοιάζει νόμιμος αλλά στην πραγματικότητα έχει σχεδιαστεί για την κλοπή ευαίσθητων πληροφοριών (Alkhalil, Hewage, Nawaf, & Khan, 2021).

Οι απάτες ηλεκτρονικού "ψαρέματος" μπορεί επίσης να έχουν τη μορφή τηλεφωνικών κλήσεων ή μηνυμάτων κειμένου. Σε αυτές τις περιπτώσεις, ο επιτιθέμενος μπορεί να παρουσιαστεί ως εκπρόσωπος ενός αξιόπιστου οργανισμού και να χρησιμοποιήσει τεχνικές κοινωνικής μηχανικής για να πείσει το θύμα να παράσχει ευαίσθητες πληροφορίες.

Για την προστασία από απάτες phishing, είναι σημαντικό να είναι προσεκτικοί όσοι παρέχουν ευαίσθητες πληροφορίες, ιδίως μέσω ηλεκτρονικού ταχυδρομείου ή ηλεκτρονικών φορμών, επαληθεύοντας την πηγή οποιουδήποτε απροσδόκητου email ή μηνύματος και μην παρέχονται ποτέ ευαίσθητες πληροφορίες μέσω συνδέσμου σε email ή γραπτό μήνυμα. Είναι σημαντικό να διατηρείται ενημερωμένο το λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό ενώ απαραίτητη κρίνεται η ενημέρωση σχετικά με τις τακτικές που χρησιμοποιούνται στις απάτες phishing (Fette, Sadeh, & Tomasic, 2007).

Οι επιθέσεις Ransomware είναι ένας τύπος κυβερνοεπίθεσης που περιλαμβάνει την κρυπτογράφηση των αρχείων του θύματος και την απαίτηση καταβολής λύτρων για την αποκατάσταση της πρόσβασης. Αυτός ο τύπος επίθεσης είναι ιδιαίτερα αποτελεσματικός εναντίον οργανισμών, καθώς μπορεί να διαταράξει τις επιχειρηματικές λειτουργίες και να οδηγήσει σε σημαντικές οικονομικές απώλειες. Σε μια επίθεση ransomware, τα αρχεία ενός θύματος κρυπτογραφούνται με τη χρήση ενός ισχυρού αλγορίθμου κρυπτογράφησης, καθιστώντας τα μη προσβάσιμα από τον χρήστη. Στη συνέχεια, ο επιτιθέμενος απαιτεί την καταβολή λύτρων, συνήθως με τη μορφή κρυπτονομισμάτων, για την παροχή του κλειδιού αποκρυπτογράφησης (Ghulam, Irfan, & Hassan, 2022).

Οι επιθέσεις Ransomware μπορούν να μεταδοθούν με διάφορα μέσα, όπως απάτες phishing, κακόβουλες ιστοσελίδες και drive-by λήψεις. Μόλις μολυνθεί μια συσκευή, το ransomware μπορεί να εξαπλωθεί σε άλλες συσκευές στο δίκτυο, καθιστώντας την επίθεση ακόμη πιο επιζήμια. Για την προστασία από επιθέσεις ransomware, είναι σημαντικό να διατηρείται το λογισμικό και τα συστήματα ασφαλείας ενημερωμένα, να δημιουργούνται τακτικά αντίγραφα ασφαλείας σημαντικών δεδομένων και να εκπαιδεύετε τους υπαλλήλους σχετικά με τις ασφαλείς

πρακτικές υπολογισμού. Επιπλέον, οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο εφαρμογής μέτρων ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και φιλτράρισμα ηλεκτρονικού ταχυδρομείου, για να μειώσουν τον κίνδυνο μιας επιτυχημένης επίθεσης. Εάν συμβεί μια επίθεση ransomware, είναι σημαντικό να μην καταβληθούν τα λύτρα, καθώς αυτό μπορεί να ενθαρρύνει περαιτέρω επιθέσεις και δεν εγγυάται την αποκατάσταση των κρυπτογραφημένων αρχείων. Αντ' αυτού, οι οργανισμοί θα πρέπει να ζητήσουν βοήθεια από έναν επαγγελματία στον τομέα της ασφάλειας στον κυβερνοχώρο για να ελαχιστοποιήσουν τις επιπτώσεις της επίθεσης (Zafri, 2022).

Η επίθεση κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS) είναι ένας τύπος επίθεσης στον κυβερνοχώρο που αποσκοπεί στη διακοπή της διαθεσιμότητας ενός ιστότοπου ή ενός δικτύου με την υπερφόρτωσή του με κίνηση. Στόχος μιας επίθεσης DDoS είναι να καταστήσει έναν ιστότοπο ή ένα δίκτυο μη διαθέσιμο στους χρήστες, συχνά για πολιτικούς ή οικονομικούς λόγους. Μια επίθεση DDoS πραγματοποιείται από ένα δίκτυο μολυσμένων υπολογιστών, που ονομάζεται botnet, οι οποίοι συνεργάζονται για να στείλουν μεγάλο όγκο κίνησης στον ιστότοπο ή το δίκτυο-στόχο. Αυτή η κίνηση υπερφορτώνει το σύστημα, με αποτέλεσμα να γίνεται αργό ή να μην είναι διαθέσιμο στους χρήστες (He, et al., 2022).

Οι επιθέσεις DDoS μπορεί να έχουν σημαντικές συνέπειες για τους οργανισμούς, όπως απώλεια εσόδων, βλάβη της φήμης και διακοπή κρίσιμων υπηρεσιών. Σε ορισμένες περιπτώσεις, οι επιθέσεις DDoS μπορούν επίσης να χρησιμοποιηθούν ως προπέτασμα καπνού για άλλους τύπους επιθέσεων στον κυβερνοχώρο, όπως κλοπή δεδομένων ή μολύνσεις από κακόβουλο λογισμικό.

Για την προστασία από τις επιθέσεις DDoS, οι οργανισμοί μπορούν να εφαρμόσουν μέτρα ασφαλείας, όπως ο περιορισμός του ρυθμού, το φιλτράρισμα της κίνησης και τα δίκτυα διανομής περιεχομένου. Επιπλέον, οι οργανισμοί μπορούν να συνεργαστούν με παρόχους υπηρεσιών διαδικτύου και επαγγελματίες κυβερνοασφάλειας για την ανάπτυξη ενός ολοκληρωμένου σχεδίου αντιμετώπισης σε περίπτωση επίθεσης. Αυτό μπορεί να περιλαμβάνει την εφαρμογή πρόσθετης χωρητικότητας δικτύου για την απορρόφηση της κίνησης της επίθεσης, την αναδρομολόγηση της κίνησης και τον αποκλεισμό της κακόβουλης κίνησης στην άκρη του δικτύου. Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις DDoS εξελίσσονται συνεχώς και αναπτύσσονται νέες τεχνικές για την παράκαμψη των παραδοσιακών μέτρων ασφαλείας. Ως αποτέλεσμα, οι οργανισμοί πρέπει να

επαγρυπνούν και να ενημερώνονται για τις τελευταίες τάσεις στις επιθέσεις DDoS, ώστε να προστατεύουν αποτελεσματικά τα δίκτυα και τους ιστότοπούς τους (Cvitić, Peraković, Gupta, & Choo, 2021).

Το κακόβουλο λογισμικό είναι ένας τύπος κακόβουλου λογισμικού που έχει σχεδιαστεί για να βλάπτει τα συστήματα υπολογιστών και να υποκλέπτει ευαίσθητες πληροφορίες. Οι μολύνσεις από κακόβουλο λογισμικό μπορούν να λάβουν πολλές μορφές, όπως ιούς, σκουλήκια, trojans, spyware και adware. Οι μολύνσεις από κακόβουλο λογισμικό συνήθως εξαπλώνονται μέσω συνημμένων email, κακόβουλων ιστότοπων, μολυσμένων λήψεων λογισμικού και drive-by λήψεων. Μόλις μολυνθεί μια συσκευή, το κακόβουλο λογισμικό μπορεί να υποκλέψει ευαίσθητες πληροφορίες, να διαταράξει την απόδοση του συστήματος και να εξαπλωθεί σε άλλες συσκευές στο δίκτυο (Chernikova, et al., 2022).

Οι μολύνσεις από κακόβουλο λογισμικό μπορεί να έχουν σοβαρές συνέπειες για άτομα και οργανισμούς, συμπεριλαμβανομένης της απώλειας ευαίσθητων πληροφοριών, οικονομικών απωλειών και της διακοπής των επιχειρηματικών λειτουργιών. Σε ορισμένες περιπτώσεις, οι μολύνσεις από κακόβουλο λογισμικό μπορούν επίσης να χρησιμοποιηθούν ως εφαλτήριο για πιο προηγμένες επιθέσεις στον κυβερνοχώρο, όπως ransomware ή κλοπή δεδομένων.

Για την προστασία από μολύνσεις από κακόβουλο λογισμικό, είναι σημαντικό να διατηρείται το λογισμικό και τα συστήματα ασφαλείας ενημερωμένα, να δημιουργούνται τακτικά αντίγραφα ασφαλείας σημαντικών δεδομένων και να εκπαιδεύονται οι υπάλληλοι σχετικά με τις ασφαλείς πρακτικές πληροφορικής. Επιπλέον, οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο εφαρμογής μέτρων ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και λογισμικό προστασίας από ιούς, για να μειώσουν τον κίνδυνο μιας επιτυχημένης επίθεσης. Εάν συμβεί μια μόλυνση από κακόβουλο λογισμικό, είναι σημαντικό να παρέχετε βοήθεια από έναν επαγγελματία στον τομέα της ασφάλειας στον κυβερνοχώρο για να ελαχιστοποιηθούν οι επιπτώσεις της επίθεσης και να αποκατασταθούν οι κανονικές λειτουργίες (Chernikova, et al., 2022).

Η κοινωνική μηχανική (social engineering) είναι ένας τύπος επίθεσης στον κυβερνοχώρο που περιλαμβάνει τη χειραγώγηση ανθρώπων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ενέργειες που είναι επιζήμιες για τον οργανισμό. Ο στόχος της κοινωνικής μηχανικής είναι να εξαπατήσει τα θύματα ώστε να παραβιάσουν τις συνήθεις διαδικασίες

ασφαλείας, συχνά εκμεταλλευόμενοι τα ανθρώπινα συναισθήματα όπως η εμπιστοσύνη, ο φόβος, το επείγον ή η περιέργεια (Minchev, 2015).

Οι επιθέσεις κοινωνικής μηχανικής μπορούν να λάβουν πολλές μορφές, όπως απάτες phishing, δολώματα, προσχηματικές ενέργειες, ανταλλάγματα και αναζητήσεις σε κάδους απορριμμάτων. Σε μια απάτη phishing, για παράδειγμα, ο επιτιθέμενος μπορεί να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα που φαίνεται να προέρχεται από μια αξιόπιστη πηγή, όπως ένα χρηματοπιστωτικό ίδρυμα ή μια γνωστή εταιρεία. Το μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να περιέχει μια αίσθηση επείγοντος ή φόβου για να ενθαρρύνει τον παραλήπτη να προβεί σε άμεσες ενέργειες, όπως να κάνει κλικ σε έναν σύνδεσμο ή να παράσχει πληροφορίες.

Για την προστασία από επιθέσεις κοινωνικής μηχανικής, είναι σημαντικό να μην παρέχονται ευαίσθητες πληροφορίες, ιδίως μέσω ηλεκτρονικού ταχυδρομείου ή ηλεκτρονικών φορμών, με απαραίτητη την επαλήθευση της πηγής οποιουδήποτε απροσδόκητου email ή μηνύματος και μην παρέχονται ποτέ ευαίσθητες πληροφορίες μέσω συνδέσμου σε email ή γραπτό μήνυμα. Είναι σημαντική η διατήρηση ενός καλά ενημερωμένου λογισμικού προστασίας από ιούς και κακόβουλο λογισμικό με ανάλογη εκπαίδευση σχετικά με τις τακτικές που χρησιμοποιούνται στις επιθέσεις κοινωνικής μηχανικής. Επιπλέον, οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο εφαρμογής προγραμμάτων εκπαίδευσης ευαισθητοποίησης σε θέματα ασφάλειας για την εκπαίδευση των εργαζομένων σχετικά με τις ασφαλείς πρακτικές πληροφορικής και τους κινδύνους των επιθέσεων κοινωνικής μηχανικής (Joshi, 2000).

Μια προηγμένη επίμονη απειλή (Advanced Persistent Threat - APT) είναι ένας τύπος επίθεσης στον κυβερνοχώρο που είναι ιδιαίτερα εξελιγμένη, επίμονη και στοχευμένη. Οι επιθέσεις APT πραγματοποιούνται συνήθως από έθνη-κράτη, ομάδες οργανωμένου εγκλήματος ή άλλες οργανώσεις με υψηλά κίνητρα και καλή χρηματοδότηση. Στόχος μιας επίθεσης APT είναι η κλοπή ευαίσθητων πληροφοριών ή η διατάραξη κρίσιμων συστημάτων για μεγάλο χρονικό διάστημα, συχνά για στρατηγικό ή οικονομικό όφελος (Chen, Chen, & Hong, 2022).

Οι επιθέσεις APT είναι σχεδιασμένες ώστε να είναι αθόρυβες και δύσκολα ανιχνεύσιμες. Συνήθως περιλαμβάνουν πολλαπλά στάδια, συμπεριλαμβανομένης της αρχικής παραβίασης, της διοίκησης και του ελέγχου και της διαρροής δεδομένων. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει

έναν συνδυασμό τεχνικών, όπως εκμεταλλεύσεις μηδενικής ημέρας, spear phishing και μολύνσεις κακόβουλου λογισμικού, για να αποκτήσει πρόσβαση στο δίκτυο του στόχου.

Μόλις ο επιτιθέμενος αποκτήσει πρόσβαση στο δίκτυο του στόχου, συχνά χρησιμοποιεί τεχνικές όπως η πλευρική μετακίνηση και η συλλογή δεδομένων για να επεκτείνει τον έλεγχό του και να συλλέξει ευαίσθητες πληροφορίες. Οι επιθέσεις APT μπορούν να επιμείνουν για μήνες ή και χρόνια, γεγονός που τις καθιστά ιδιαίτερα επικίνδυνες για τους οργανισμούς.

Για την προστασία από τις επιθέσεις APT, οι οργανισμοί πρέπει να εφαρμόζουν μια ολοκληρωμένη στρατηγική ασφάλειας που περιλαμβάνει ισχυρά μέτρα ασφάλειας δικτύου, ανίχνευση και αντιμετώπιση απειλών και εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας. Αυτό μπορεί να περιλαμβάνει την εφαρμογή τειχών προστασίας, συστημάτων ανίχνευσης εισβολών και λογισμικού προστασίας από ιούς, καθώς και τακτικές επιθεωρήσεις ασφαλείας, δοκιμές διείσδυσης και σχεδιασμό αντιμετώπισης περιστατικών. Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις APT εξελίσσονται συνεχώς και αναπτύσσονται νέες τεχνικές για την παράκαμψη των παραδοσιακών μέτρων ασφαλείας. Ως αποτέλεσμα, οι οργανισμοί πρέπει να επαγρυπνούν και να ενημερώνονται για τις τελευταίες τάσεις στις επιθέσεις APT, ώστε να προστατεύουν αποτελεσματικά τα δίκτυα και τις ευαίσθητες πληροφορίες τους (Alsanad & Altuwaijri, 2022).

Οι επιθέσεις IoT (Internet of Things) αφορούν κυβερνοεπιθέσεις σε συνδεδεμένες συσκευές, όπως έξυπνα σπίτια, έξυπνα αυτοκίνητα και βιομηχανικά συστήματα ελέγχου. Αυτές οι συσκευές είναι συνήθως σχεδιασμένες να συλλέγουν και να μεταδίδουν δεδομένα μέσω του διαδικτύου, καθιστώντας τις ευάλωτες σε κυβερνοαπειλές. Οι επιθέσεις IoT μπορούν να λάβουν πολλές μορφές, όπως επιθέσεις άρνησης παροχής υπηρεσιών (DoS), επιθέσεις man-in-the-middle (MitM) και μολύνσεις κακόβουλου λογισμικού. Σε μια επίθεση DoS, ο επιτιθέμενος μπορεί να κατακλύσει μια συσκευή με κίνηση, προκαλώντας την υπερφόρτωσή της και την αδυναμία της να λειτουργήσει σωστά. Σε μια επίθεση MitM, ο επιτιθέμενος υποκλέπτει και χειρίζεται την επικοινωνία μεταξύ μιας συσκευής και ενός διακομιστή, κλέβοντας ενδεχομένως ευαίσθητες πληροφορίες ή τροποποιώντας τη συμπεριφορά της συσκευής (Henschke, 2021).

Οι συσκευές IoT είναι συχνά ευάλωτες σε επιθέσεις επειδή μπορεί να έχουν αδύναμα μέτρα ασφαλείας, να μην έχουν ενημερώσεις λογισμικού ή να είναι κακώς ρυθμισμένες. Αυτό μπορεί να διευκολύνει τους επιτιθέμενους να αποκτήσουν πρόσβαση στη συσκευή και τα σχετικά δεδομένα της.

Για την προστασία από επιθέσεις IoT, είναι σημαντικό να ακολουθούνται οι βέλτιστες πρακτικές για την ασφάλεια των συνδεδεμένων συσκευών, όπως η αλλαγή του προεπιλεγμένου κωδικού πρόσβασης, η ενεργοποίηση ενημερώσεων λογισμικού και η χρήση ασφαλών πρωτοκόλλων όπως το SSL/TLS. Επιπλέον, οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο εφαρμογής μέτρων ασφαλείας σε επίπεδο δικτύου, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και τμηματοποίηση δικτύου, για να μειώσουν τον κίνδυνο μιας επιτυχημένης επίθεσης (Sullivan & Montasari, 2022).

Συμπερασματικά, η κυβερνοτρομοκρατία αποτελεί μια αυξανόμενη απειλή που απαιτεί μια ολοκληρωμένη προσέγγιση της ασφάλειας, η οποία περιλαμβάνει ισχυρά τεχνολογικά συστήματα και ευαισθητοποίηση σχετικά με τις τακτικές που χρησιμοποιούν οι κυβερνοτρομοκράτες.

3.3 Βασικά κίνητρα πίσω από την κυβερνοτρομοκρατία.

Τα πολιτικά κίνητρα είναι ένας από τους βασικούς μοχλούς πίσω από την κυβερνοτρομοκρατία. Σε αυτές τις περιπτώσεις, οι κυβερνοεπιθέσεις χρησιμοποιούνται ως εργαλείο για πολιτικό ακτιβισμό ή για την προώθηση μιας συγκεκριμένης ιδεολογίας ή αιτίας. Ο στόχος είναι συχνά να διαταράξουν ή να δυσφημίσουν πολιτικούς αντιπάλους ή κυβερνήσεις ή να τραβήξουν την προσοχή σε ένα συγκεκριμένο θέμα ή αιτία.

Οι κυβερνοεπιθέσεις με πολιτικά κίνητρα μπορούν να λάβουν πολλές μορφές, όπως επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS), αλλοιώσεις ιστότοπων και παραβιάσεις δεδομένων. Σε μια επίθεση DDoS, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει ένα δίκτυο μολυσμένων υπολογιστών για να κατακλύσει τον ιστότοπο ενός στόχου με κίνηση, προκαλώντας την μη διαθεσιμότητά του. Σε μια αλλοίωση ιστότοπου, ο επιτιθέμενος μπορεί να αλλάξει το περιεχόμενο ενός ιστότοπου για να διαδώσει ένα πολιτικό μήνυμα ή να δυσφημίσει τον στόχο. Σε μια παραβίαση δεδομένων, ο επιτιθέμενος μπορεί να κλέψει ευαίσθητες πληροφορίες, όπως εμπιστευτικά έγγραφα ή μηνύματα ηλεκτρονικού ταχυδρομείου, και να τις χρησιμοποιήσει για να υπονομεύσει τη φήμη του στόχου ή να βλάψει τις δραστηριότητές του (Gandhi, et al., 2011).

Οι επιθέσεις στον κυβερνοχώρο με πολιτικά κίνητρα μπορεί να έχουν εκτεταμένες συνέπειες, συμπεριλαμβανομένης της ζημίας στη φήμη του στόχου, της απώλειας εσόδων και της βλάβης κρίσιμων υποδομών.

Σε ορισμένες περιπτώσεις, οι κυβερνοεπιθέσεις μπορεί επίσης να οδηγήσουν σε φυσική ζημία, όπως είναι η διακοπή υπηρεσιών έκτακτης ανάγκης ή κρίσιμων υποδομών, όπως τα δίκτυα ηλεκτρικής ενέργειας ή τα χρηματοπιστωτικά συστήματα (Nazario, 2009).

Τα οικονομικά κίνητρα αποτελούν κοινή κινητήρια δύναμη πίσω από την κυβερνοτρομοκρατία και το κυβερνοέγκλημα. Σε αυτές τις περιπτώσεις, οι κυβερνοεπιθέσεις χρησιμοποιούνται για την κλοπή ευαίσθητων πληροφοριών, όπως αριθμούς πιστωτικών καρτών, πληροφορίες τραπεζικών λογαριασμών και άλλα προσωπικά δεδομένα, ή για την απαίτηση πληρωμής με αντάλλαγμα την αποδέσμευση ευαίσθητων πληροφοριών ή την πρόσβαση σε κλειδωμένα συστήματα (Gandhi, et al., 2011).

Μια από τις πιο συνηθισμένες μορφές οικονομικών κυβερνοεπιθέσεων είναι το ransomware. Σε μια επίθεση ransomware, ο επιτιθέμενος μολύνει το σύστημα υπολογιστή του στόχου με κακόβουλο λογισμικό και κρυπτογραφεί τα αρχεία του, καθιστώντας τα μη προσβάσιμα. Στη συνέχεια, ο επιτιθέμενος απαιτεί πληρωμή, συνήθως με τη μορφή κρυπτονομίσματος, σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης. Μια άλλη κοινή μορφή οικονομικής κυβερνοεπίθεσης είναι το phishing. Σε μια επίθεση phishing, ο επιτιθέμενος στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα που φαίνεται να προέρχεται από μια αξιόπιστη πηγή, όπως μια τράπεζα ή έναν ηλεκτρονικό έμπορο λιανικής πώλησης, προκειμένου να εξαπατήσει τον παραλήπτη να παράσχει ευαίσθητες πληροφορίες, όπως στοιχεία σύνδεσης ή οικονομικές πληροφορίες (Goldman & McCoy, 2016).

Οι οικονομικές επιθέσεις στον κυβερνοχώρο μπορεί να έχουν σημαντικές συνέπειες για άτομα και οργανισμούς, όπως οικονομικές απώλειες, απώλεια φήμης και νομικές ευθύνες. Σε ορισμένες περιπτώσεις, οι οικονομικές απώλειες μπορεί να είναι σημαντικές, ιδίως για τις μικρές επιχειρήσεις και τους ιδιώτες που μπορεί να μην έχουν τους πόρους για να ανακάμψουν από μια μεγάλη κυβερνοεπίθεση (Gandhi, et al., 2011).

Τα ιδεολογικά κίνητρα αποτελούν βασική κινητήρια δύναμη πίσω από την κυβερνοτρομοκρατία. Σε αυτές τις περιπτώσεις, οι κυβερνοεπιθέσεις χρησιμοποιούνται ως

εργαλείο για την προώθηση μιας συγκεκριμένης ιδεολογίας ή αιτίας ή για την επίθεση σε όσους έχουν αντίθετες απόψεις.

Οι κυβερνοεπιθέσεις με ιδεολογικά κίνητρα μπορούν να λάβουν πολλές μορφές, συμπεριλαμβανομένων των αλλοιώσεων ιστότοπων, των παραβιάσεων δεδομένων και των επιθέσεων κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS). Σε μια αλλοίωση ιστότοπου, ο επιτιθέμενος μπορεί να αλλάξει το περιεχόμενο ενός ιστότοπου για να διαδώσει ένα πολιτικό ή ιδεολογικό μήνυμα ή να δυσφημίσει τον στόχο. Σε μια παραβίαση δεδομένων, ο επιτιθέμενος μπορεί να κλέψει ευαίσθητες πληροφορίες, όπως εμπιστευτικά έγγραφα ή μηνύματα ηλεκτρονικού ταχυδρομείου, και να τις χρησιμοποιήσει για να υπονομεύσει τη φήμη του στόχου ή να βλάψει τις δραστηριότητές του. Σε μια επίθεση DDoS, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα δίκτυο μολυσμένων υπολογιστών για να κατακλύσει τον ιστότοπο ενός στόχου με κίνηση, προκαλώντας την μη διαθεσιμότητά του (Yunos & Sulaman, 2017).

Οι ιδεολογικές επιθέσεις στον κυβερνοχώρο μπορεί να έχουν εκτεταμένες συνέπειες, συμπεριλαμβανομένης της ζημίας στη φήμη του στόχου, της απώλειας εσόδων και της βλάβης κρίσιμων υποδομών. Σε ορισμένες περιπτώσεις, οι κυβερνοεπιθέσεις μπορεί επίσης να οδηγήσουν σε σωματική βλάβη, όπως η διακοπή υπηρεσιών έκτακτης ανάγκης ή κρίσιμων υποδομών, όπως τα δίκτυα ηλεκτρικής ενέργειας ή τα χρηματοπιστωτικά συστήματα (Dogrul, Aslan, & Celik, 2011).

Τα στρατιωτικά κίνητρα αποτελούν σημαντική κινητήρια δύναμη πίσω από την κυβερνοτρομοκρατία και τον κυβερνοπόλεμο. Σε αυτές τις περιπτώσεις, οι κυβερνοεπιθέσεις χρησιμοποιούνται ως εργαλείο για τη συλλογή πληροφοριών, τη δολιοφθορά στρατιωτικών επιχειρήσεων ή τη διατάραξη κρίσιμων υποδομών.

Οι κυβερνοεπιθέσεις με στρατιωτικά κίνητρα μπορούν να λάβουν πολλές μορφές, όπως η διείσδυση σε ασφαλή δίκτυα για την κλοπή ευαίσθητων πληροφοριών, η τοποθέτηση κακόβουλου λογισμικού για τη διακοπή επιχειρήσεων ή η χρήση επιθέσεων DDoS για την κατάρριψη κρίσιμων συστημάτων. Σε ορισμένες περιπτώσεις, αυτές οι κυβερνοεπιθέσεις μπορεί να πραγματοποιούνται από ομάδες που χρηματοδοτούνται από το κράτος, στρατιωτικές οργανώσεις ή ανεξάρτητους χάκερ με στρατιωτικούς ή στρατηγικούς στόχους (Weimann G. , 2004).

Οι συνέπειες των επιθέσεων στον κυβερνοχώρο με στρατιωτικά κίνητρα μπορεί να είναι σοβαρές, συμπεριλαμβανομένης της απώλειας ανθρώπινων ζωών, σημαντικών οικονομικών

ζημιών και βλάβης της εθνικής ασφάλειας. Σε ορισμένες περιπτώσεις, αυτές οι κυβερνοεπιθέσεις μπορεί επίσης να κλιμακωθούν σε παραδοσιακές στρατιωτικές συγκρούσεις, περιπλέκοντας περαιτέρω την κατάσταση.

Για να προστατευθούν από κυβερνοεπιθέσεις με στρατιωτικά κίνητρα, οι κυβερνήσεις και οι στρατιωτικοί οργανισμοί εφαρμόζουν ισχυρά μέτρα κυβερνοασφάλειας, όπως ασφαλή δίκτυα, κρυπτογράφηση και έλεγχο ταυτότητας πολλαπλών παραγόντων. Επίσης επαγρυπνούν για την παρακολούθηση των ενδείξεων κυβερνοεπιθέσεων και είναι προετοιμασμένοι να αντιδράσουν γρήγορα και αποτελεσματικά σε περίπτωση επίθεσης. Επιπλέον, οι κυβερνήσεις και οι στρατιωτικοί οργανισμοί συνεργάζονται για τη θέσπιση σαφών κανόνων συμπεριφοράς στον κυβερνοχώρο και για την απόδοση ευθυνών σε όσους εμπλέκονται σε κυβερνοεπιθέσεις. Καθώς οι επιθέσεις στον κυβερνοχώρο με στρατιωτικά κίνητρα μπορούν να αποτελέσουν σημαντικές απειλές για την εθνική ασφάλεια, οι κυβερνήσεις και οι στρατιωτικοί οργανισμοί λαμβάνουν προληπτικά μέτρα για την άμυνα κατά των επιθέσεων αυτών και παραμένουν σε εγρήγορση στις προσπάθειές τους για τον εντοπισμό τους και την αντιμετώπισή τους (Lewis, 2002).

Τα προσωπικά κίνητρα αναφέρονται σε κυβερνοεπιθέσεις που πραγματοποιούνται από άτομα που έχουν προσωπικούς λόγους ή κίνητρα για τις ενέργειές τους. Τα κίνητρα αυτά μπορεί να κυμαίνονται από εκδίκηση ή προσωπική μνησικακία έως απλή περιέργεια ή επιθυμία να προκαλέσουν αναστάτωση.

Οι επιθέσεις στον κυβερνοχώρο με προσωπικά κίνητρα μπορούν να λάβουν πολλές μορφές, όπως η παραβίαση προσωπικών λογαριασμών, η εξαπόλυση επιθέσεων DDoS ή η εξάπλωση κακόβουλου λογισμικού. Σε ορισμένες περιπτώσεις, αυτές οι κυβερνοεπιθέσεις μπορεί να πραγματοποιούνται από εξειδικευμένους χάκερ με συγκεκριμένο στόχο στο μυαλό τους, ενώ σε άλλες περιπτώσεις μπορεί να πραγματοποιούνται από άτομα με μικρή τεχνική εμπειρία που χρησιμοποιούν εύκολα διαθέσιμα εργαλεία και τεχνικές για να πραγματοποιήσουν τις επιθέσεις τους (Vernacchia, 2018).

Οι συνέπειες των επιθέσεων στον κυβερνοχώρο με προσωπικά κίνητρα μπορεί να ποικίλλουν σε μεγάλο βαθμό, από μικρή ενόχληση ή αμηχανία έως σοβαρές οικονομικές απώλειες ή βλάβη σε υποδομές ζωτικής σημασίας. Σε ορισμένες περιπτώσεις, οι εν λόγω κυβερνοεπιθέσεις μπορεί επίσης να οδηγήσουν σε σωματική βλάβη, όπως με τη διακοπή υπηρεσιών έκτακτης ανάγκης ή κρίσιμων υποδομών.

Ανεξάρτητα από το κίνητρο, η κυβερνοτρομοκρατία μπορεί να έχει σημαντικές συνέπειες για τα άτομα, τους οργανισμούς και την κοινωνία στο σύνολό της. Ως εκ τούτου, είναι κρίσιμο να κατανοηθεί η απειλή και να ληφθούν τα κατάλληλα μέτρα για την προστασία από τις κυβερνοεπιθέσεις.

4.0 Απειλές από την κυβερνοτρομοκρατία.

Η κυβερνοτρομοκρατία αναφέρεται στη χρήση ψηφιακών τεχνολογιών για τη διενέργεια βίαιων πράξεων που έχουν ως αποτέλεσμα ή απειλούν με απώλεια ζωής ή σημαντική σωματική βλάβη, καθώς και με ζημία ή καταστροφή κρίσιμων υποδομών ή/και μαζική διατάραξη της οικονομίας. Η ανάπτυξη του διαδικτύου και η αυξανόμενη διασύνδεση της κοινωνίας έχουν δημιουργήσει νέες ευκαιρίες για κακόβουλους φορείς να προκαλέσουν ζημιά και η κυβερνοτρομοκρατία έχει γίνει μια αυξανόμενη ανησυχία για τις κυβερνήσεις, τους οργανισμούς και τα άτομα σε όλο τον κόσμο.

Μια από τις σημαντικότερες απειλές της κυβερνοτρομοκρατίας είναι η πιθανότητα κυβερνοεπιθέσεων σε κρίσιμες υποδομές. Οι κυβερνοεπιθέσεις σε υποδομές ζωτικής σημασίας αφορούν κακόβουλες κυβερνοδραστηριότητες που στοχεύουν σε συστήματα και περιουσιακά στοιχεία που είναι απαραίτητα για τη λειτουργία μιας κοινωνίας, όπως τα δίκτυα ηλεκτρικής ενέργειας, τα χρηματοπιστωτικά συστήματα, τα δίκτυα μεταφορών, τα συστήματα υγειονομικής περίθαλψης και τα συστήματα αντιμετώπισης εκτάκτων αναγκών. Οι επιθέσεις αυτές μπορούν να προκαλέσουν εκτεταμένες διαταραχές, οικονομικές απώλειες, ακόμη και απώλειες ανθρώπινων ζωών (Geers, 2009).

Μια από τις κύριες ανησυχίες για τις κυβερνοεπιθέσεις σε κρίσιμες υποδομές είναι το ενδεχόμενο εκτεταμένων διακοπών ρεύματος. Μια κυβερνοεπίθεση σε ένα σύστημα ηλεκτρικού δικτύου μπορεί να οδηγήσει σε διακοπές ρεύματος που επηρεάζουν μεγάλες γεωγραφικές περιοχές, προκαλώντας σημαντική αναστάτωση στην καθημερινή ζωή, τις επιχειρήσεις και τις δημόσιες υπηρεσίες. Μια άλλη ανησυχία είναι το ενδεχόμενο παραβίασης δεδομένων. Οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές μπορεί να έχουν ως αποτέλεσμα την κλοπή ευαίσθητων πληροφοριών, όπως οικονομικές πληροφορίες, προσωπικές ταυτότητες ή πνευματική ιδιοκτησία. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως κλοπή ταυτότητας ή οικονομική απάτη (Li & Qinghui , 2021).

Οι κυβερνοεπιθέσεις σε συστήματα υγειονομικής περίθαλψης μπορεί να έχουν ιδιαίτερα σοβαρές συνέπειες. Για παράδειγμα, μια κυβερνοεπίθεση στα συστήματα πληροφορικής ενός νοσοκομείου θα μπορούσε να θέσει σε κίνδυνο ευαίσθητες πληροφορίες ασθενών και να

διαταράξει τις ιατρικές υπηρεσίες. Σε ορισμένες περιπτώσεις, οι κυβερνοεπιθέσεις σε ιατρικές συσκευές και εξοπλισμό μπορούν να θέσουν σε κίνδυνο ακόμη και τη ζωή των ασθενών (Ahmed, Sindi , & Nour, 2022).

Τα δίκτυα μεταφορών αποτελούν. Επίσης, στόχο για τους εγκληματίες του κυβερνοχώρου. Για παράδειγμα, μια κυβερνοεπίθεση στα συστήματα ελέγχου ενός συστήματος μεταφορών θα μπορούσε να έχει ως αποτέλεσμα τη διακοπή των δρομολογίων των τρένων ή των αεροπλάνων, προκαλώντας εκτεταμένη ταλαιπωρία και οικονομικές απώλειες. Τα συστήματα αντιμετώπισης εκτάκτων αναγκών αποτελούν επίσης πηγή ανησυχίας, καθώς μια κυβερνοεπίθεση σε αυτά τα συστήματα θα μπορούσε να θέσει σε κίνδυνο την ικανότητα των πρώτων ανταποκριτών να ανταποκριθούν σε καταστάσεις έκτακτης ανάγκης (Hathaway, et al., 2012).

Μια άλλη απειλή της κυβερνοτρομοκρατίας είναι οι επιθέσεις ransomware, οι οποίες εντάσσονται στο πλαίσιο της κυβερνοτρομοκρατίας που περιλαμβάνει τη χρήση κακόβουλου λογισμικού για την κρυπτογράφηση των δεδομένων στον υπολογιστή ή το δίκτυο του θύματος. Ο επιτιθέμενος απαιτεί πληρωμή (συνήθως με τη μορφή κρυπτονομίσματος) σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης, το οποίο είναι απαραίτητο για την αποκατάσταση της πρόσβασης στα δεδομένα (Peters, 2022).

Οι επιθέσεις Ransomware μπορεί να έχουν καταστροφικές συνέπειες για άτομα, οργανισμούς, ακόμη και για συστήματα κρίσιμων υποδομών. Για τα άτομα, μια επίθεση ransomware μπορεί να οδηγήσει στην απώλεια σημαντικών προσωπικών δεδομένων, όπως οικογενειακές φωτογραφίες ή οικονομικές πληροφορίες. Για τους οργανισμούς, μια επίθεση ransomware μπορεί να έχει ως αποτέλεσμα τη διακοπή των επιχειρηματικών λειτουργιών και την απώλεια ευαίσθητων δεδομένων, γεγονός που μπορεί να έχει σοβαρές οικονομικές συνέπειες και συνέπειες για τη φήμη τους (Lella, Tsekmezoglou, Naydenov, & Malatras, 2022).

Τα συστήματα κρίσιμων υποδομών, όπως τα δίκτυα ηλεκτρικής ενέργειας, τα χρηματοπιστωτικά συστήματα, τα δίκτυα μεταφορών και τα συστήματα υγειονομικής περίθαλψης, κινδυνεύουν επίσης από επιθέσεις ransomware. Μια επίθεση ransomware σε αυτά τα συστήματα θα μπορούσε να οδηγήσει σε εκτεταμένες διαταραχές, οικονομικές απώλειες, ακόμη και σε απώλεια ζωής. Για παράδειγμα, μια επίθεση ransomware στα υπολογιστικά συστήματα ενός νοσοκομείου θα μπορούσε να θέσει σε κίνδυνο ευαίσθητες πληροφορίες ασθενών και να διακόψει τις ιατρικές υπηρεσίες, θέτοντας σε κίνδυνο τη ζωή των ασθενών (Watney, 2022).

Οι παραβιάσεις δεδομένων αποτελούν μια άλλη απειλή της κυβερνοτρομοκρατίας. Η παραβίαση δεδομένων είναι ένα περιστατικό ασφαλείας κατά το οποίο ευαίσθητες, εμπιστευτικές ή προστατευόμενες πληροφορίες δημοσιοποιούνται, κλέβονται ή αποκτούν πρόσβαση με άλλο τρόπο από μη εξουσιοδοτημένα μέρη. Οι παραβιάσεις δεδομένων μπορεί να προκύψουν ως αποτέλεσμα διαφόρων παραγόντων, όπως hacking, κακόβουλο λογισμικό, ανθρώπινο λάθος ή φυσική κλοπή συσκευών που περιέχουν ευαίσθητες πληροφορίες (Seh, et al., 2020).

Οι παραβιάσεις δεδομένων μπορεί να έχουν σημαντικές συνέπειες για άτομα, οργανισμούς, ακόμη και για ολόκληρες κοινωνίες. Για τα άτομα, μια παραβίαση δεδομένων μπορεί να έχει ως αποτέλεσμα την κλοπή προσωπικών πληροφοριών, όπως ονόματα, διευθύνσεις, αριθμούς κοινωνικής ασφάλισης ή οικονομικές πληροφορίες. Οι πληροφορίες αυτές μπορούν στη συνέχεια να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως κλοπή ταυτότητας ή οικονομική απάτη (Seh, et al., 2020).

Για τους οργανισμούς, μια παραβίαση δεδομένων μπορεί να οδηγήσει στην απώλεια ευαίσθητων επιχειρηματικών πληροφοριών, όπως εμπορικά μυστικά, οικονομικές πληροφορίες ή δεδομένα πελατών. Αυτό μπορεί να έχει σοβαρές οικονομικές συνέπειες και συνέπειες για τη φήμη του οργανισμού, όπως απώλεια εσόδων, νομικές κυρώσεις και ζημία στο εμπορικό σήμα του. Τα συστήματα κρίσιμων υποδομών, όπως τα δίκτυα ηλεκτρικής ενέργειας, τα χρηματοπιστωτικά συστήματα, τα δίκτυα μεταφορών και τα συστήματα υγειονομικής περίθαλψης, κινδυνεύουν επίσης από παραβιάσεις δεδομένων. Μια παραβίαση δεδομένων σε αυτά τα συστήματα θα μπορούσε να οδηγήσει σε εκτεταμένη διαταραχή, οικονομικές απώλειες, ακόμη και απώλεια ζωής. Για παράδειγμα, μια παραβίαση δεδομένων σε ένα σύστημα ηλεκτρικού δικτύου θα μπορούσε να οδηγήσει σε κλοπή ευαίσθητων πληροφοριών, όπως κωδικοί πρόσβασης σε συστήματα ελέγχου, οι οποίες θα μπορούσαν στη συνέχεια να χρησιμοποιηθούν από επιτιθέμενους για τη διακοπή της παροχής ηλεκτρικής ενέργειας (Dhillon, 2015).

Η παρέμβαση στις εκλογές είναι ένας άλλος τομέας ανησυχίας όσον αφορά την τρομοκρατία στον κυβερνοχώρο. Η παρέμβαση στις εκλογές μέσω της κυβερνοτρομοκρατίας αναφέρεται στη χρήση της τεχνολογίας και του διαδικτύου για τη χειραγώγηση, τη διατάραξη ή την επιρροή του αποτελέσματος των εκλογών. Αυτό μπορεί να περιλαμβάνει την παραβίαση βάσεων δεδομένων και ιστότοπων για τις εκλογές, τη διάδοση ψευδών πληροφοριών και προπαγάνδας και την εξαπόλυση κυβερνοεπιθέσεων κατά πολιτικών εκστρατειών και υποψηφίων.

Η παρέμβαση στις εκλογές αποτελεί αυξανόμενη απειλή, καθώς όλο και περισσότερες εκλογές διεξάγονται με τη χρήση ηλεκτρονικών συστημάτων ψηφοφορίας και όλο και περισσότερες ευαίσθητες πληροφορίες αποθηκεύονται και μεταδίδονται στο διαδίκτυο. Οι συνέπειες των εκλογικών παρεμβάσεων μπορεί να κυμαίνονται από την αλλοίωση των εκλογικών αποτελεσμάτων έως την υπονόμευση της εμπιστοσύνης του κοινού στη δημοκρατική διαδικασία. Είναι σημαντικό για τις κυβερνήσεις και τους εκλογικούς οργανισμούς να εφαρμόσουν ισχυρά μέτρα κυβερνοασφάλειας για την προστασία από εκλογικές παρεμβάσεις και για την προώθηση της διαφάνειας και της εμπιστοσύνης του κοινού στην εκλογική διαδικασία (Garnett & James, 2020).

Τέλος, οι εκστρατείες παραπληροφόρησης αποτελούν αυξανόμενη ανησυχία στο πλαίσιο της τρομοκρατίας στον κυβερνοχώρο, καθώς μπορούν να χρησιμοποιηθούν για τη διάδοση ψευδών ή παραπλανητικών πληροφοριών με σκοπό τη χειραγώγηση της κοινής γνώμης, τη δημιουργία κοινωνικής αναταραχής και την παρέμβαση στις πολιτικές διαδικασίες. Οι εκστρατείες αυτές χρησιμοποιούν συχνά τα μέσα κοινωνικής δικτύωσης και άλλες διαδικτυακές πλατφόρμες για να προσεγγίσουν ένα μεγάλο κοινό και μπορούν να επωφεληθούν από αλγόριθμους που προωθούν εντυπωσιακό ή αμφιλεγόμενο περιεχόμενο. Οι εκστρατείες παραπληροφόρησης μπορούν επίσης να συντονίζονται και να ενισχύονται από κρατικά υποστηριζόμενους φορείς και οργανωμένες εγκληματικές ομάδες που επιδιώκουν να επιτύχουν συγκεκριμένους πολιτικούς, οικονομικούς ή στρατιωτικούς στόχους (Dhillon, 2015).

Ο αντίκτυπος των εκστρατειών παραπληροφόρησης μπορεί να είναι σημαντικός, καθώς μπορούν να διαβρώσουν την εμπιστοσύνη στην κυβέρνηση και τους θεσμούς, να σπείρουν τη διαίρεση και την κοινωνική αναταραχή και να χειραγωγήσουν την κοινή γνώμη για σημαντικά ζητήματα. Οι εκστρατείες παραπληροφόρησης μπορούν επίσης να παρεμβαίνουν στις εκλογές και να θέτουν σε κίνδυνο την εθνική ασφάλεια, διαδίδοντας ψευδείς πληροφορίες σχετικά με τους πολιτικούς υποψηφίους, τις διαδικασίες καταμέτρησης των ψήφων και άλλα βασικά στοιχεία της εκλογικής διαδικασίας.

Συνοψίζοντας, η τρομοκρατία στον κυβερνοχώρο αποτελεί αυξανόμενη ανησυχία στον σημερινό ολοένα και πιο διασυνδεδεμένο κόσμο. Το ενδεχόμενο κυβερνοεπιθέσεων σε υποδομές ζωτικής σημασίας, επιθέσεων ransomware, παραβιάσεων δεδομένων, παρεμβολών στις εκλογές και εκστρατειών παραπληροφόρησης υπογραμμίζει την ανάγκη για άτομα, οργανισμούς και

κυβερνήσεις να λάβουν προληπτικά μέτρα για την προστασία από αυτές τις απειλές. Παραμένοντας ενημερωμένοι, επαγρυπνώντας και λαμβάνοντας μέτρα για την ενίσχυση της ασφάλειας στον κυβερνοχώρο, μπορούμε να μειώσουμε τους κινδύνους της κυβερνοτρομοκρατίας και να συμβάλουμε στην εξασφάλιση ενός ασφαλέστερου ψηφιακού περιβάλλοντος.

4.1 Οικονομικές συνέπειες της κυβερνοτρομοκρατίας.

Οι οικονομικές συνέπειες της τρομοκρατίας στον κυβερνοχώρο μπορεί να είναι εκτεταμένες και καταστροφικές. Οι επιθέσεις στον κυβερνοχώρο μπορούν να διαταράξουν τις επιχειρηματικές λειτουργίες, να προκαλέσουν σημαντικές οικονομικές απώλειες και να βλάψουν τη συνολική οικονομία.

Μία από τις άμεσες συνέπειες της τρομοκρατίας στον κυβερνοχώρο είναι η άμεση οικονομική απώλεια για τους στοχοποιημένους οργανισμούς. Για παράδειγμα, μια επιτυχημένη επίθεση στον κυβερνοχώρο σε ένα χρηματοπιστωτικό ίδρυμα θα μπορούσε να οδηγήσει στην κλοπή μεγάλων χρηματικών ποσών, ενώ μια επίθεση στον κυβερνοχώρο σε μια κατασκευαστική εταιρεία θα μπορούσε να προκαλέσει τη διακοπή της παραγωγής και να οδηγήσει σε απώλεια πωλήσεων και κερδών.

Μια άλλη έμμεση οικονομική συνέπεια της τρομοκρατίας στον κυβερνοχώρο είναι η ζημία στη φήμη και την εικόνα του εμπορικού σήματος μιας εταιρείας. Όταν μια εταιρεία πέφτει θύμα κυβερνοεπίθεσης, οι πελάτες μπορεί να χάσουν την εμπιστοσύνη τους στην εταιρεία και στην ικανότητά της να προστατεύει τις προσωπικές και οικονομικές τους πληροφορίες. Αυτό μπορεί να οδηγήσει σε μείωση της πελατείας και απώλεια εργασιών για την εταιρεία (Hower & Uradnik, 2011).

Επιπλέον, οι επιθέσεις στον κυβερνοχώρο μπορούν να διαταράξουν τη λειτουργία ολόκληρων βιομηχανιών, οδηγώντας σε εκτεταμένη οικονομική διαταραχή. Για παράδειγμα, μια επιτυχής επίθεση σε μια κρίσιμη υποδομή, όπως το δίκτυο ηλεκτρικής ενέργειας ή το σύστημα μεταφορών, μπορεί να προκαλέσει εκτεταμένες διακοπές ρεύματος ή καθυστερήσεις στις μεταφορές, οδηγώντας σε απώλεια παραγωγικότητας και αύξηση του κόστους για τις επιχειρήσεις και τους καταναλωτές (Krause, Ernst, Klaer, Hacker, & Henze, 2021).

Οι έμμεσες οικονομικές συνέπειες της τρομοκρατίας στον κυβερνοχώρο μπορούν επίσης να επεκταθούν πέρα από τα άμεσα θύματα της επίθεσης. Για παράδειγμα, μια επίθεση στον

κυβερνοχώρο σε έναν σημαντικό προμηθευτή μπορεί να διαταράξει ολόκληρη την αλυσίδα εφοδιασμού, επηρεάζοντας πολλές επιχειρήσεις και κλάδους. Τέλος, το κόστος της αντιμετώπισης και της ανάκαμψης από τις επιθέσεις στον κυβερνοχώρο μπορεί να είναι σημαντικό, τόσο για τους στοχοθετημένους οργανισμούς όσο και για την κυβέρνηση. Αυτό περιλαμβάνει το κόστος της αποκατάστασης των συστημάτων, της διερεύνησης της επίθεσης και της εφαρμογής νέων μέτρων ασφαλείας (Anderson, 2012).

Συμπερασματικά, η κυβερνοτρομοκρατία έχει τη δυνατότητα να προκαλέσει σημαντική οικονομική ζημία, τόσο σε μεμονωμένους οργανισμούς όσο και στη συνολική οικονομία. Είναι σημαντικό για τις επιχειρήσεις και τις κυβερνήσεις να επενδύσουν σε μέτρα ασφάλειας στον κυβερνοχώρο για να ελαχιστοποιήσουν τον κίνδυνο επιθέσεων στον κυβερνοχώρο και τις πιθανές συνέπειές τους.

5.0 Προστασία από την κυβερνοτρομοκρατία.

Η αντιμετώπιση της κυβερνοτρομοκρατίας είναι εφικτή μέσω ενός συνόλου νομοθετικών, ιδεολογικών και πληροφοριακών, οργανωτικών, διοικητικών και νομικών, εκπαιδευτικών, συμπεριλαμβανομένων των προπαγανδιστικών μέτρων που αποσκοπούν στην πρόληψη της εμφάνισης υποκειμένων της κυβερνοτρομοκρατίας (ιδίως ομάδων και οργανώσεων), στην αποτροπή τους, στη μη μετάβασή τους σε ενεργό δράση, στην υλοποίηση εγκληματικών προθέσεων. Η εμπειρία πολλών ξένων χωρών στον αγώνα κατά της τρομοκρατίας θα πρέπει οπωσδήποτε να μελετηθεί και, αφού μελετηθεί, να χρησιμοποιηθεί προς όφελος της κοινωνίας. Οι πολιτικοί ηγέτες των μεγάλων χωρών της Δύσης και των Ηνωμένων Πολιτειών θεωρούν την καταπολέμηση της τρομοκρατίας ως ένα από τα σημαντικότερα εθνικά καθήκοντα (Yamamoto, 2015).

Έτσι, η αντιμετώπιση είναι ένα σύνολο μέτρων μέσω των οποίων δεν αναλαμβάνεται ενεργός δράση για την υλοποίηση των τρομοκρατικών προθέσεων. Υπάρχουν στόχοι και καθήκοντα, κατευθύνσεις και αρχές αντιμετώπισης της τρομοκρατίας. Οι κύριες κατευθύνσεις των αντιτρομοκρατικών δραστηριοτήτων είναι: βελτίωση του νομικού πλαισίου- ενίσχυση της αλληλεπίδρασης μεταξύ των αρμόδιων ομοσπονδιακών φορέων- δημιουργία ειδικών μονάδων και αύξηση του αριθμού των υπαλλήλων των ομοσπονδιακών δομών που ασχολούνται με το πρόβλημα της τρομοκρατίας, βελτίωση του τεχνικού τους εξοπλισμού. Το οπλοστάσιο των τρομοκρατών υπολογιστών περιλαμβάνει διάφορους ιούς, λογικές βόμβες - εντολές που έχουν ενσωματωθεί στο πρόγραμμα εκ των προτέρων και ενεργοποιούνται την κατάλληλη στιγμή. Οι σύγχρονοι τρομοκράτες χρησιμοποιούν το διαδίκτυο κυρίως ως μέσο προπαγάνδας και μεταφοράς πληροφοριών και όχι ως νέο όπλο (Clarke, 2002).

Ωστόσο, μπορεί να υποτεθεί ότι η τρομοκρατία μέσω υπολογιστών αποτελεί σήμερα ήδη μια πραγματική απειλή για την κοινωνία. Σήμερα υπάρχουν πολύ λίγα συστήματα που μπορούν να θεωρηθούν ασφαλή. Κατά κανόνα, διαδίδουν πολιτικές ιδέες και διεξάγουν δραστηριότητες προπαγάνδας και στρατολόγησης με στόχο την αύξηση του αριθμού των υποστηρικτών τους. Η αντιμετώπιση της τρομοκρατίας μέσω υπολογιστών, η οποία είναι συμπληρωματική της συμβατικής τρομοκρατίας, είναι σήμερα σχεδόν αδύνατη. Αυτό οφείλεται στο γεγονός ότι απουσιάζουν οι κρατικές ρυθμίσεις, η λογοκρισία και άλλες μορφές ελέγχου των πληροφοριών που διαδίδονται στο διαδίκτυο (Weimann G. , 2004).

Από τις αρχές της δεκαετίας του 2000, η Ευρωπαϊκή ένωση συμμετέχει ενεργά στην ανάπτυξη διεθνών κανόνων που κατοχυρώνουν μέτρα για την καταπολέμηση της κυβερνοτρομοκρατίας. Ωστόσο, τα μέτρα κατά της κυβερνοτρομοκρατίας είναι περισσότερο τυπικής φύσης και συχνά αποδεικνύονται αναποτελεσματικά στην πράξη. Αυτό αποδεικνύεται από τις επανειλημμένες επιθέσεις στον κυβερνοχώρο εναντίον μεγάλων εταιρειών και κυβερνητικών οργανισμών, κάθε χρόνο.

Είναι σημαντικό να επισημανθούν οι κύριοι τομείς εργασίας του αντίστοιχου αρμόδιου φορέα για την καταπολέμηση της τρομοκρατίας στον κυβερνοχώρο. Παράλληλα, η καταπολέμηση της τρομοκρατίας στον κυβερνοχώρο είναι μια σύνθετη και συνεχής διαδικασία που απαιτεί συντονισμένες προσπάθειες από πολλές κυβερνητικές υπηρεσίες, οργανισμούς του ιδιωτικού τομέα και διεθνείς εταίρους. Επιπλέον, είναι σημαντικό να υπάρχει μια προληπτική προσέγγιση για την πρόληψη των επιθέσεων στον κυβερνοχώρο και την προώθηση της ασφάλειας στον κυβερνοχώρο, αντί απλώς να ανταποκρίνεται σε αυτές μετά την εκδήλωσή τους. Αυτό περιλαμβάνει την προώθηση της ευαισθητοποίησης και της εκπαίδευσης, καθώς και την επένδυση στην έρευνα και την ανάπτυξη νέων τεχνολογιών και στρατηγικών για την άμυνα κατά των επιθέσεων στον κυβερνοχώρο (Kertysova, Frinking, van den Dool, Maričić, & Bhattacharyya, 2018).

Πρωτίστως, η ανίχνευση και η καταστολή της μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες υπολογιστών αποτελεί σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο, καθώς η μη εξουσιοδοτημένη πρόσβαση μπορεί να οδηγήσει σε παραβίαση ευαίσθητων πληροφοριών, βλάβη των συστημάτων ή διακοπή της λειτουργίας των δικτύων. Ο στόχος της ανίχνευσης και της καταστολής της μη εξουσιοδοτημένης πρόσβασης είναι να αποτραπεί η πρόσβαση μη εξουσιοδοτημένων ατόμων σε ένα υπολογιστικό σύστημα, δίκτυο ή βάση δεδομένων και να αποτραπεί η πρόκληση βλάβης στις πληροφορίες που περιέχονται σε αυτά. Αυτό επιτυγχάνεται συνήθως μέσω ενός συνδυασμού τεχνικών μέτρων, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και κρυπτογράφηση, καθώς και διαδικαστικών μέτρων, όπως η πιστοποίηση ταυτότητας των χρηστών και ο έλεγχος πρόσβασης (IAEA, 2011).

Συγχρόνως, η καταπολέμηση της κατασκευής, της διανομής και της χρήσης κακόβουλου λογισμικού (malware) είναι μια άλλη σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο. Το

κακόβουλο λογισμικό είναι ένας τύπος λογισμικού που έχει σχεδιαστεί για να βλάπτει ή να εκμεταλλεύεται συστήματα και δίκτυα υπολογιστών. Μπορεί να λάβει πολλές μορφές, όπως ιούς, σκουλήκια, δούρειους ίππους, λογισμικό λύτρων και λογισμικό κατασκοπείας, και μπορεί να προκαλέσει μια σειρά από δυσμενείς επιπτώσεις, όπως κλοπή δεδομένων, διακοπή του συστήματος και εξάπλωση του κακόβουλου λογισμικού σε άλλα συστήματα (Colarik, 2006).

Στόχος της καταπολέμησης του κακόβουλου λογισμικού είναι η πρόληψη της δημιουργίας, της διανομής και της χρήσης του και η μείωση της βλάβης που προκαλεί στα συστήματα και τα δίκτυα υπολογιστών. Αυτό επιτυγχάνεται συνήθως μέσω ενός συνδυασμού τεχνικών μέτρων, όπως το λογισμικό προστασίας από ιούς και τα συστήματα ανίχνευσης εισβολών, και διαδικαστικών μέτρων, όπως η εκπαίδευση των χρηστών και οι βέλτιστες πρακτικές για την ασφάλεια του λογισμικού (Colarik, 2006).

Η πρόληψη της δόλιας χρήσης των συστημάτων ηλεκτρονικών πληρωμών αποτελεί μείζον ζήτημα για τους ιδιώτες, τις επιχειρήσεις και τις κυβερνήσεις, καθώς τα ηλεκτρονικά συστήματα πληρωμών γίνονται όλο και περισσότερο η προτιμώμενη μέθοδος πληρωμής για πολλές συναλλαγές. Η δόλια χρήση των συστημάτων ηλεκτρονικών πληρωμών μπορεί να οδηγήσει σε οικονομικές απώλειες, ζημία στη φήμη και μείωση της εμπιστοσύνης των καταναλωτών στις ηλεκτρονικές πληρωμές (IAEA, 2011).

Στόχος της πρόληψης της δόλιας χρήσης των συστημάτων ηλεκτρονικών πληρωμών είναι να διασφαλιστεί ότι οι συναλλαγές ηλεκτρονικών πληρωμών είναι ασφαλείς, νόμιμες και εγκεκριμένες. Αυτό συνήθως επιτυγχάνεται με συνδυασμό τεχνικών μέτρων, όπως η κρυπτογράφηση και η πιστοποίηση ταυτότητας, και διαδικαστικών μέτρων, όπως η αξιολόγηση και η παρακολούθηση του κινδύνου. Για παράδειγμα, πολλά συστήματα ηλεκτρονικών πληρωμών χρησιμοποιούν κρυπτογράφηση για την προστασία της εμπιστευτικότητας ευαίσθητων πληροφοριών, όπως οι αριθμοί πιστωτικών καρτών και τα υπόλοιπα λογαριασμών. Μπορεί επίσης να χρησιμοποιούν έλεγχο ταυτότητας πολλαπλών παραγόντων για να διασφαλίσουν ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση και να πραγματοποιούν συναλλαγές χρησιμοποιώντας το σύστημα (Colarik, 2006).

Η καταστολή των παράνομων δραστηριοτήτων στα δίκτυα πληροφοριών και τηλεπικοινωνιών, συμπεριλαμβανομένου του Διαδικτύου, είναι μια κρίσιμη πτυχή της ασφάλειας στον κυβερνοχώρο, καθώς το Διαδίκτυο έχει καταστεί κόμβος για διάφορες μορφές εγκληματικής

δραστηριότητας, όπως η πειρατεία, η απάτη στον κυβερνοχώρο, η κυβερνοτρομοκρατία και η πώληση παράνομων αγαθών και υπηρεσιών (IAEA, 2011).

Ο στόχος της καταστολής των παράνομων δραστηριοτήτων στα δίκτυα πληροφοριών και τηλεπικοινωνιών είναι να αποτραπούν αυτές οι δραστηριότητες και να προσαχθούν οι υπεύθυνοι στη δικαιοσύνη. Αυτό συνήθως επιτυγχάνεται με συνδυασμό τεχνικών μέτρων, όπως συστήματα ανίχνευσης εισβολών και παρακολούθησης δικτύων, και διαδικαστικών μέτρων, όπως η δημιουργία μονάδων για το έγκλημα στον κυβερνοχώρο στο πλαίσιο των υπηρεσιών επιβολής του νόμου. Οι υπηρεσίες επιβολής του νόμου διαδραματίζουν βασικό ρόλο στην καταστολή παράνομων δραστηριοτήτων σε δίκτυα πληροφοριών και τηλεπικοινωνιών, συμπεριλαμβανομένου του διαδικτύου. Διερευνούν και διώκουν άτομα και οργανώσεις που συμμετέχουν σε παράνομες δραστηριότητες και συνεργάζονται με διεθνείς εταίρους για την παραπομπή των υπευθύνων στη δικαιοσύνη (Colarik, 2006).

Η ανίχνευση και η καταστολή των εγκλημάτων που σχετίζονται με την παράνομη χρήση των πόρων των κυψελοειδών και ενσύρματων δικτύων επικοινωνιών αποτελεί σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο, καθώς τα δίκτυα αυτά γίνονται όλο και περισσότερο το κύριο μέσο επικοινωνίας για άτομα και οργανισμούς. Τα εγκλήματα που σχετίζονται με την παράνομη χρήση πόρων κυψελοειδών και ενσύρματων δικτύων επικοινωνίας μπορεί να περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση σε αυτά τα δίκτυα, κλοπή ευαίσθητων πληροφοριών που μεταδίδονται μέσω αυτών των δικτύων και χρήση αυτών των δικτύων για τη συμμετοχή σε παράνομες δραστηριότητες, όπως η κυβερνοαπάτη και η κυβερνοτρομοκρατία (IAEA, 2011).

Ο στόχος της ανίχνευσης και καταστολής εγκλημάτων που σχετίζονται με την παράνομη χρήση πόρων κυψελοειδών και ενσύρματων δικτύων επικοινωνιών είναι να αποτραπούν αυτά τα εγκλήματα και να προσαχθούν οι υπεύθυνοι στη δικαιοσύνη. Αυτό συνήθως επιτυγχάνεται με συνδυασμό τεχνικών μέτρων, όπως η παρακολούθηση δικτύων και τα συστήματα ανίχνευσης εισβολών, και διαδικαστικών μέτρων, όπως η δημιουργία μονάδων για το έγκλημα στον κυβερνοχώρο στο πλαίσιο των υπηρεσιών επιβολής του νόμου. Οι υπηρεσίες επιβολής του νόμου διαδραματίζουν κρίσιμο ρόλο στον εντοπισμό και την καταστολή των εγκλημάτων που σχετίζονται με την παράνομη χρήση των πόρων των κυψελοειδών και ενσύρματων δικτύων επικοινωνιών και συνεργάζονται με διεθνείς εταίρους για την προσαγωγή των υπευθύνων στη δικαιοσύνη (Colarik, 2006).

Η καταπολέμηση των δόλιων πράξεων που διαπράττονται με τη χρήση δικτύων πληροφοριών και τηλεπικοινωνιών, συμπεριλαμβανομένου του διαδικτύου, αποτελεί σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο, καθώς τα δίκτυα αυτά καθίστανται όλο και περισσότερο το κύριο μέσο επικοινωνίας και εμπορίου για άτομα και οργανισμούς. Οι δόλιες πράξεις που διαπράττονται με τη χρήση δικτύων πληροφοριών και τηλεπικοινωνιών μπορεί να περιλαμβάνουν διαδικτυακές απάτες, επιθέσεις phishing, κλοπή ταυτότητας και πώληση πλαστών ή κλεμμένων αγαθών και υπηρεσιών. Αυτοί οι τύποι απάτης μπορεί να οδηγήσουν σε σημαντικές οικονομικές απώλειες για άτομα και οργανισμούς, καθώς και σε ζημία της φήμης τους (IAEA, 2011).

Στόχος της καταπολέμησης των δόλιων πράξεων που διαπράττονται με τη χρήση δικτύων πληροφοριών και τηλεπικοινωνιών είναι να αποτραπούν οι πράξεις αυτές και να προσαχθούν οι υπεύθυνοι στη δικαιοσύνη. Αυτό συνήθως επιτυγχάνεται με συνδυασμό τεχνικών μέτρων, όπως η παρακολούθηση δικτύων και τα συστήματα ανίχνευσης εισβολών, και διαδικαστικών μέτρων, όπως η δημιουργία μονάδων ηλεκτρονικού εγκλήματος στο πλαίσιο των υπηρεσιών επιβολής του νόμου.

Ένα ουσιαστικό στοιχείο της ασφάλειας στον κυβερνοχώρο είναι η πρόληψη και η αποτροπή προσπαθειών μη εξουσιοδοτημένης πρόσβασης σε εμπορικά δορυφορικά και καλωδιακά τηλεοπτικά κανάλια, καθώς αποτελούν πολύτιμη πηγή πληροφόρησης και ευχαρίστησης για εκατομμύρια ανθρώπους σε όλο τον κόσμο. Η παραβίαση αυτών των συστημάτων για τη λήψη προγραμμάτων χωρίς να πληρώσετε γι' αυτά ή η μη εξουσιοδοτημένη πρόσβαση σε αυτά τα συστήματα για την επεξεργασία ή τη χειραγώγηση του προγράμματος αποτελούν και τα δύο παραδείγματα παράνομης πρόσβασης σε εμπορικά δορυφορικά και καλωδιακά τηλεοπτικά κανάλια. Οι εταιρείες που προσφέρουν αυτές τις υπηρεσίες ενδέχεται να υποστούν μεγάλες οικονομικές απώλειες ως αποτέλεσμα τέτοιου είδους πράξεων, οι οποίες ενδέχεται επίσης να παρεμποδίσουν τη δυνατότητα των νόμιμων καταναλωτών να λαμβάνουν περιεχόμενο (Li & Qinghui , 2021).

Για να σταματήσουν αυτές οι ενέργειες και να λογοδοτήσουν τα άτομα, καταπολεμούνται και καταστέλλονται οι προσπάθειες παράνομης πρόσβασης σε εμπορικά δορυφορικά και καλωδιακά τηλεοπτικά κανάλια. Αυτό επιτυγχάνεται συχνά με το συνδυασμό τεχνικών μέτρων, όπως συστήματα ανίχνευσης εισβολών και παρακολούθησης δικτύων, με διαδικαστικά μέτρα, συμπεριλαμβανομένης της δημιουργίας μονάδων ηλεκτρονικού εγκλήματος εντός των

οργανισμών επιβολής του νόμου. Προκειμένου να αποτραπούν και να σταματήσουν οι απόπειρες μη εξουσιοδοτημένης πρόσβασης σε εμπορικά δορυφορικά και καλωδιακά τηλεοπτικά κανάλια, οι αρχές επιβολής του νόμου διαδραματίζουν καθοριστικό ρόλο. Συνεργάζονται επίσης με διεθνείς εταίρους για τη δίωξη των παραβατών (Gable, 2010).

Κρίσιμα στοιχεία της ασφάλειας στον κυβερνοχώρο περιλαμβάνουν τον εντοπισμό και την καταστολή των παραβιάσεων των δικαιωμάτων πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων στον τομέα της τεχνολογίας των πληροφοριών, καθώς και την καταπολέμηση του διεθνούς εγκλήματος στον τομέα αυτό. Εκτός του ότι καθιστά απλούστερη την πρόσβαση και την ανταλλαγή πληροφοριών για τους ανθρώπους και τους οργανισμούς, η αυξανόμενη χρήση των τεχνολογιών της πληροφορίας έχει επίσης ανοίξει νέες ευκαιρίες για παραβιάσεις της πνευματικής ιδιοκτησίας, συμπεριλαμβανομένης της μη εξουσιοδοτημένης διανομής περιεχομένου που προστατεύεται από πνευματικά δικαιώματα, της παραβίασης εμπορικών σημάτων και των παραβιάσεων διπλωμάτων ευρεσιτεχνίας (Csonka, 2006).

Η κατασκοπεία στον κυβερνοχώρο, η διαδικτυακή πώληση πλαστών ή κλεμμένων αγαθών και υπηρεσιών και η παράνομη διακίνηση ευαίσθητων δεδομένων είναι μερικά μόνο παραδείγματα του διεθνούς εγκλήματος στο πεδίο των τεχνολογιών της πληροφορίας. Για να σταματήσουν αυτές οι πράξεις και να λογοδοτήσουν οι υπεύθυνοι, η ανίχνευση και η καταστολή των παραβιάσεων των δικαιωμάτων διανοητικής ιδιοκτησίας και των συγγενικών δικαιωμάτων, καθώς και η καταπολέμηση του διεθνούς εγκλήματος στον τομέα της πληροφορικής αποτελούν στόχους. Αυτό επιτυγχάνεται συχνά με τον συνδυασμό τεχνικών μέτρων, όπως συστήματα ανίχνευσης εισβολών και παρακολούθησης δικτύων, με διαδικαστικά μέτρα, συμπεριλαμβανομένης της δημιουργίας μονάδων ηλεκτρονικού εγκλήματος εντός των οργανισμών επιβολής του νόμου. προκειμένου να διώκονται τα ένοχα άτομα, οι υπηρεσίες επιβολής του νόμου συνεργάζονται με ξένους εταίρους και διαδραματίζουν καθοριστικό ρόλο στην καταπολέμηση του διεθνικού εγκλήματος στον τομέα των τεχνολογιών της πληροφορίας (Colarik, 2006).

Συνολικά, η προστασία από την τρομοκρατία στον κυβερνοχώρο απαιτεί δέσμευση για την εφαρμογή ισχυρών τεχνικών, διαδικαστικών και ευαισθητοποιητικών μέτρων, καθώς και μια κουλτούρα ασφάλειας που περιλαμβάνει όλους τους εργαζόμενους και τους ενδιαφερόμενους φορείς.

5.1 Το Ελληνικό νομοθετικό πλαίσιο γύρω από την κυβερνοτρομοκρατία.

Ο ποινικός κώδικας δεν αναφέρει ρητά την κυβερνοτρομοκρατία ως τέτοια. Το πρόσθετο αποτέλεσμα αυτού είναι ότι δεν θεωρείται πλέον έγκλημα βάσει του νόμου. Ολόκληρη η δομή του Ποινικού Κώδικα βασίζεται, επίσης, στην ιδέα του εγκλήματος, η οποία ορίζεται νομικά με απλό τρόπο από το άρθρο 14 του κώδικα. Το τελευταίο, ορίζει ότι έγκλημα είναι κάθε παράνομη συμπεριφορά που καταλογίζεται στον δράστη της και υπόκειται σε νομικές κυρώσεις. Το γεγονός ότι το έγκλημα είναι πράξη υποδηλώνει ότι, ενώ η πράξη δεν τιμωρείται και δεν αποτελεί αντικείμενο ποινικής έρευνας, κωδικοποιείται στις ποινικές διατάξεις και, ως εκ τούτου, αποκτά τα χαρακτηριστικά του (νομικού) εγκλήματος. η πράξη χαρακτηρίζεται περαιτέρω από τον τόπο, τον χρόνο, το μέσο και το πλαίσιο στο οποίο πραγματοποιείται και στο οποίο παράγει τα αποτελέσματά της. Περιλαμβάνει επίσης συγκεκριμένη πράξη ή παράλειψη και έχει συγκεκριμένο υποκείμενο (Βαγιάτη, 2014).

Δεδομένου ότι δεν υπάρχει ανεξάρτητη τυποποίηση της κυβερνοτρομοκρατίας, είναι επομένως αδύνατο να μιλήσουμε για αντικειμενικό και υποκειμενικό περιεχόμενο και η προσέγγιση της κυβερνοτρομοκρατίας μπορεί να είναι μόνο εννοιολογική. Ωστόσο, θα χρησιμοποιήσουμε ιδέες από το διαδίκτυο και το ποινικό δίκαιο για να ορίσουμε τα όριά της. Όπως είδαμε παραπάνω, το πρώτο συστατικό του όρου παραπέμπει σε εγκληματική δραστηριότητα που λαμβάνει χώρα στον "ψηφιακό κόσμο", μια νέα ηλεκτρονική πραγματικότητα που κατέστη δυνατή χάρη στην ανάπτυξη των ψηφιακών τεχνολογιών, η οποία συνυπάρχει και επηρεάζει τον φυσικό κόσμο. Η παραδοσιακή θεωρία του ποινικού δικαίου υποστηρίζει ότι, ακόμη και αν το έννομο αγαθό που παραβιάζεται είναι άυλο ή αφηρημένο, η πράξη της παραβίασης του άρθρου 14 ΠΚ, όπως τυποποιείται στην αντικειμενική υπόσταση κάθε επιμέρους διάταξης του σχετικού μέρους του Ποινικού Κώδικα, αποτελεί βίαιη πράξη, διότι λαμβάνει χώρα στον φυσικό, ορατό και απτό κόσμο γύρω μας (Βαγιάτη, 2014).

Οι ευκαιρίες που παρέχει ο κυβερνοχώρος, ή το ψηφιακό περιβάλλον, στους χρήστες του, λειτούργησαν για πρώτη φορά είτε ως "μέσο" είτε ως "εργαλείο" για τη διάπραξη εγκλημάτων. Ο ψηφιακός κόσμος και οι δομές του δεν ήταν ο στόχος ή ο επιδιωκόμενος στόχος της επίθεσης. Όπως είδαμε, ο νόμος 4411/2016 θέσπισε για πρώτη φορά στο ελληνικό ποινικό δίκαιο μια νέα κατηγορία εγκλημάτων. Τα εγκλήματα αυτά αναφέρονται ως "εγκλήματα στον κυβερνοχώρο" (με

τη στενή έννοια του όρου) και δεν διαπράττονται μόνο στον κυβερνοχώρο ή πραγματοποιούνται με τη βοήθεια των πόρων του κυβερνοχώρου, αλλά στοχεύουν και στα ίδια τα δομικά στοιχεία του κυβερνοχώρου, όπως τα δεδομένα και τα πληροφοριακά συστήματα. Τα εγκλήματα αυτά στοχεύουν συγκεκριμένα στη διαθεσιμότητα, την ακεραιότητα ή τα συστήματα πληροφορικής, καθώς και σε αδικήματα που περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση, υποκλοπές, αλλοίωση δεδομένων και παρεμβολές στο σύστημα (Βαγιάτη, 2014).

Ο όρος "έγκλημα στον κυβερνοχώρο" εισήχθη για να αντικατοπτρίζει τα μοναδικά χαρακτηριστικά των εγκλημάτων που διαπράττονται στον ψηφιακό κόσμο. Η Σύμβαση της Βουδαπέστης, η οποία εισήχθη στο ελληνικό δίκαιο με τον ν. 4411/2016, παρέχει ένα πλαίσιο για τον ορισμό και την τιμωρία των εγκλημάτων στον κυβερνοχώρο. Η εν λόγω σύμβαση αναγνωρίζει ότι τα εγκλήματα στον κυβερνοχώρο διαφέρουν από τα παραδοσιακά εγκλήματα και απαιτούν διαφορετικό νομικό πλαίσιο για την αντιμετώπισή τους. Τα εγκλήματα στον κυβερνοχώρο, όπως ορίζονται από τη Σύμβαση της Βουδαπέστης, περιλαμβάνουν ένα ευρύ φάσμα αδικημάτων, όπως η μη εξουσιοδοτημένη πρόσβαση σε συστήματα υπολογιστών, η πειρατεία, οι κυβερνοεπιθέσεις, η διανομή κακόβουλου λογισμικού και η κλοπή προσωπικών δεδομένων. Τα εγκλήματα αυτά διαπράττονται στον ψηφιακό κόσμο και συχνά έχουν διασυνοριακές επιπτώσεις, γεγονός που καθιστά δύσκολη την αποτελεσματική αντιμετώπισή τους από μία μόνο χώρα (Eurojust, 2016).

Η εισαγωγή της Σύμβασης της Βουδαπέστης και η υιοθέτηση του όρου "έγκλημα στον κυβερνοχώρο" συνέβαλαν στην αποσαφήνιση του νομικού ορισμού αυτών των τύπων εγκλημάτων και στη δημιουργία ενός πλαισίου για τη διερεύνηση και τη δίωξη των εγκληματιών στον κυβερνοχώρο. Αναγνωρίζοντας τη μοναδική φύση του εγκλήματος στον κυβερνοχώρο, η Σύμβαση άνοιξε το δρόμο για την αποτελεσματική αντιμετώπιση αυτής της αυξανόμενης απειλής, τόσο στην Ελλάδα όσο και διεθνώς (Eurojust, 2016).

Ως εκ τούτου, είναι σημαντικό να κατανοήσουμε αυτούς τους δύο διαφορετικούς τρόπους με τους οποίους το έγκλημα στον κυβερνοχώρο μπορεί να επηρεάσει τόσο τον φυσικό όσο και τον ψηφιακό κόσμο, καθώς βοηθά στην ανάπτυξη αποτελεσματικών στρατηγικών για την καταπολέμηση και την πρόληψη αυτών των εγκλημάτων. Στο πρώτο σενάριο, το ψηφιακό περιβάλλον χρησιμεύει ως εργαλείο ή μέσο για τη διάπραξη ενός εγκλήματος που έχει επιπτώσεις τόσο στον φυσικό όσο και στον ψηφιακό κόσμο. Για παράδειγμα, η αλλοίωση ενός προγράμματος πυρασφάλειας, ώστε οι αισθητήρες ανίχνευσης πυρκαγιάς να μην λειτουργούν, είναι ένα

παράδειγμα του πώς το έγκλημα στον κυβερνοχώρο μπορεί να επηρεάσει τον φυσικό κόσμο. Στο δεύτερο σενάριο, οι επιπτώσεις του εγκλήματος εμφανίζονται εξ ολοκλήρου και αποκλειστικά στο ψηφιακό περιβάλλον. Για παράδειγμα, η διαγραφή ενός λογαριασμού bitcoin είναι ένα παράδειγμα εγκλήματος που έχει τις επιπτώσεις του αποκλειστικά στον ψηφιακό κόσμο. Στην περίπτωση αυτή, το ψηφιακό περιβάλλον δεν είναι απλώς το μέσο για τη διάπραξη του εγκλήματος, αλλά το ίδιο το αντικείμενο του αδικήματος (Ma, 2020).

Τα κριτήρια κατηγοριοποίησης του ηλεκτρονικού εγκλήματος μπορούν να αναλυθούν στο αντικείμενο που δέχεται την άμεση επίθεση, στο περιβάλλον στο οποίο διαπράττεται η πράξη, στο αποτέλεσμα της πράξης και στο κίνητρο της πράξης. Όταν πρόκειται για το έγκλημα στον κυβερνοχώρο με τη στενή έννοια, απαιτείται το περιβάλλον να είναι εξ ολοκλήρου ψηφιακό, το αποτέλεσμα της πράξης να έχει συγκεκριμένο και αναγνωρίσιμο αποτέλεσμα στον ψηφιακό κόσμο και το κίνητρο της πράξης να μην σχετίζεται με την τρομοκρατία. Αυτά τα κριτήρια μπορούν να βοηθήσουν στη διάκριση μεταξύ των διαφόρων τύπων εγκληματικών δραστηριοτήτων και των επιπτώσεών τους, τόσο στον φυσικό όσο και στον ψηφιακό κόσμο.

Όπως διαφαίνεται από τα ανωτέρω στο ελληνικό νομικό πλαίσιο δεν υπάρχουν συγκεκριμένες διατάξεις για την κυβερνοτρομοκρατία. Τα εγκλήματα του κυβερνοχώρου τιμωρούνται με βάση ποικίλες διατάξεις για ηλεκτρονικά αδικήματα όπως αναλύεται ακολούθως.

Η πειρατεία (μη εξουσιοδοτημένη πρόσβαση), σύμφωνα με τον Ελληνικό Ποινικό Κώδικα είναι ποινικό αδίκημα σύμφωνα με το άρθρο. 370Β παρ. 1, που ισχύει για μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικά δεδομένα, και το άρθρο. 370Δ παρ. 2 του ΓΚΚ, που εφαρμόζεται σε μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα ή σε πληροφορίες που μεταδίδονται μέσω τηλεπικοινωνιακών συστημάτων. Σύμφωνα με το άρθρο. 370Β παρ. 1, η πειρατεία επισύρει ποινή φυλάκισης έως δύο ετών, ενώ σύμφωνα με το άρθ. 370Δ παρ. 2 ΠΚ, το hacking επισύρει ποινή φυλάκισης από 10 ημέρες έως πέντε χρόνια. Εάν η παραβίαση προκαλεί σοβαρό εμπόδιο στη λειτουργία ενός πληροφοριακού συστήματος ή όταν τα δεδομένα τροποποιούνται ή αποσιωπούνται ως αποτέλεσμα πειρατείας, το άρθρο. Μπορεί επίσης να ισχύει το 292Β, σύμφωνα με το οποίο η ποινή κυμαίνεται από 10 ημέρες έως πέντε χρόνια φυλάκισης ανάλογα με τη σοβαρότητα του αποτελέσματος περιλαμβάνει και την επιβολή προστίμου.

Οι επιθέσεις άρνησης παροχής υπηρεσιών συνιστούν ποινικό αδίκημα σύμφωνα με το άρθρο 292Β του ΠΚ. Ειδικότερα, όποιος αδικαιολόγητα παρακωλύει ή διαταράσσει σοβαρά τη

λειτουργία πληροφοριακού συστήματος εισάγοντας, μεταδίδοντας, διαγράφοντας, καταστρέφοντας, τροποποιώντας ή εμποδίζοντας την πρόσβαση σε ψηφιακά δεδομένα, τιμωρείται με φυλάκιση από δέκα ημέρες έως πέντε έτη και την επιβολή πρόστιμο. Εάν ένα συγκεκριμένο εργαλείο (π.χ. botnet) χρησιμοποιήθηκε για τις επιθέσεις, η ποινή θα είναι τουλάχιστον ένα έτος φυλάκισης και πρόστιμο. Ωστόσο, εάν η επίθεση προκάλεσε σοβαρές ζημιές ή στόχευσε υποδομές ζωτικής σημασίας, επιβάλλεται σε κάθε περίπτωση ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματική ποινή ή φυλάκιση τριών ετών και χρηματική ποινή (άρθρο 292Β του πκ παρ. 2 δευτ. α, και δευτ. β και γ, αντίστοιχα).

Επιπλέον, σύμφωνα με το άρθ. 292Ε οποιοσδήποτε (i) παρεμποδίζει ή διακόπτει, (ii) σε μεγάλο βαθμό ή για μεγάλο χρονικό διάστημα, (iii) τη λειτουργία μιας δημόσιας εγκατάστασης υπηρεσιών τηλεφωνίας ή ηλεκτρονικών επικοινωνιών (ιδίως του Διαδικτύου), (iv) με η παράνομη επέμβαση σε πράγμα, πληροφοριακό σύστημα ή ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της εγκατάστασης, τιμωρείται με χρηματική ποινή και φυλάκιση τουλάχιστον ενός έτους. Όταν το ηλεκτρονικό ψάρεμα έχει την έννοια της απόπειρας δόλιας απόκτησης μέσω εξαπάτησης ευαίσθητων προσωπικών πληροφοριών (όπως κωδικοί πρόσβασης), εμπίπτει στο άρθρο. 386 παρ. 1 του ΚΠΔ και επισύρει ποινή φυλάκισης από 10 ημέρες έως πέντε χρόνια. Αντίθετα, εάν το phishing ορίζεται ως ένας τύπος απάτης που περιλαμβάνει τη χρήση υπολογιστή, με τη δημιουργία ψευδών ψηφιακών πόρων που προορίζονται να μοιάζουν με εκείνες νόμιμων οντοτήτων, να παρακινήσουν τα άτομα να αποκαλύψουν ή να αποκαλύψουν ευαίσθητες προσωπικές πληροφορίες, τότε εμπίπτει στο άρθρο . 386Α παρ. 1 του ΚΠΔ και επισύρει ποινή φυλάκισης από 10 ημέρες έως πέντε χρόνια. Και στις δύο περιπτώσεις, εάν η ζημιά που προκλήθηκε ως αποτέλεσμα του phishing είναι εξαιρετικά σοβαρή, η ποινή είναι φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή. Και στις δύο περιπτώσεις, όταν η ζημιά που προκλήθηκε από phishing υπερβαίνει το ποσό των 120.000 €, η ποινή είναι φυλάκιση από πέντε έως 10 χρόνια και χρηματική ποινή.

Η μόλυνση συστημάτων πληροφορικής με κακόβουλο λογισμικό είναι ποινικό αδίκημα και μπορεί να επιβληθεί κυρώσεις σύμφωνα με τα Άρθρα 292Β, 292δ, 370Α, 370Β, 370Δ παρ. 2, 370Ε και 386ΑΒ ΠΚ, ανάλογα με τον τύπο μόλυνσης του συστήματος πληροφορικής.

Η διανομή, πώληση ή προσφορά προς πώληση υλικού, λογισμικού ή άλλων εργαλείων που χρησιμοποιούνται για τη διάπραξη εγκλήματος στον κυβερνοχώρο. Βάσει του 292Γ τιμωρείται με

χρηματική ποινή ή φυλάκιση μέχρι δύο ετών όποιος, χωρίς δικαίωμα και με σκοπό τη διάπραξη του εγκλήματος της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων (άρθρ. 292Β), παράγει, πουλά, προμηθεύεται για χρήση, εισάγει, κατέχει, διανέμει ή διακινεί με άλλον τρόπο συσκευές ή προγράμματα υπολογιστών, κωδικούς πρόσβασης ή κωδικούς πρόσβασης ή άλλα παρόμοια δεδομένα μέσω των οποίων είναι δυνατή η πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος. Επιπλέον, το άρθ. 370 τιμωρεί με φυλάκιση τουλάχιστον δύο ετών οποιονδήποτε παράγει, πουλά, προμηθεύει για χρήση, εισάγει, εξάγει ή διανέμει με άλλο τρόπο λογισμικό ή συσκευές παρακολούθησης ικανές για υποκλοπή, καταγραφή και κάθε είδους εξαγωγή περιεχομένου ή/και δεδομένων επικοινωνίας (κίνηση και τοποθεσία), με την οποία μπορούν να διαπραχθούν οι πράξεις παραβίασης του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας.

Σε ότι αφορά την κατοχή ή χρήση υλικού, λογισμικού ή άλλων εργαλείων που χρησιμοποιούνται για τη διάπραξη εγκλήματος στον κυβερνοχώρο επισύρεται βάσει του 292 Γ ΠΚ με ποινή φυλάκισης έως δύο ετών ή χρηματική ποινή υπό την προϋπόθεση ότι χρησιμοποιήθηκαν το υλικό, το λογισμικό ή άλλα εργαλεία για τη διάπραξη των εγκλημάτων στον κυβερνοχώρο που περιγράφονται στο άρθρο. 292Β ΠΚ.

Στη συνέχεια σύμφωνα με το άρθ. 386Α του ΠΚ, όποιος, με σκοπό την απόκτηση παράνομου κέρδους, βλάπτει ξένη περιουσία επηρεάζοντας με οποιοδήποτε μέσο επεξεργασίας δεδομένων, αντιμετωπίζει ποινή φυλάκισης έως πέντε ετών. Εκτός από την προαναφερθείσα περίπτωση, η κλοπή ταυτότητας μπορεί να συνιστά διάφορα ποινικά αδικήματα βάσει του ΠΚ, ανάλογα με τον τρόπο και τον λόγο για τον οποίο ο δράστης αποκτά πρόσβαση στα δεδομένα ταυτότητας.

Δεδομένου ότι η ηλεκτρονική κλοπή δεν αποτελεί συγκεκριμένο ποινικό αδίκημα βάσει του ΠΚ, τα ελληνικά δικαστήρια έκριναν ότι: (α) βάσει του άρθρου. 370Γ παρ. 1 του ΠΚ (παραβίαση κρατικών και μη μυστικών), με ποινή φυλάκισης από τρεις μήνες έως πέντε χρόνια. και (β) σύμφωνα με το άρθρο. 370Δ του ΠΚ, εάν ο δράστης προσφέρει τις υπηρεσίες του στον ιδιοκτήτη του πληροφοριακού συστήματος (π.χ. νυν υπάλληλο), το αδίκημα τιμωρείται μόνο εάν αναφέρεται ρητά στο καταστατικό ή σε γραπτή απόφαση του ιδιοκτήτη.

Ν. 2121/1993 περί πνευματικής ιδιοκτησίας, στο άρθ. 66, προβλέπει ποινικές κυρώσεις φυλάκισης τουλάχιστον ενός έτους και πρόστιμο από 2.900 έως 15.000 ευρώ για παράνομη μη εξουσιοδοτημένη αντιγραφή, αναπαραγωγή και πώληση υλικού που προστατεύεται από τις διατάξεις του. Τέχνη. 65 του ίδιου νόμου προβλέπει αστική ευθύνη σε περίπτωση προσβολής πνευματικών δικαιωμάτων και το άρθ. 65Α για διοικητικές κυρώσεις έως 1.000 ευρώ ανά αντίτυπο εάν κάποιος αναπαράγει ή πουλήσει παράνομα αντίγραφα.

Τα περισσότερα από τα εγκλήματα που περιγράφονται παραπάνω περιέχουν την προϋπόθεση του σκοπού για την εφαρμογή των κυρώσεων τους. Για παράδειγμα, στο υποκειμενικό στοιχείο της κλοπής ταυτότητας ή της απάτης ταυτότητας, ο δράστης μιας πράξης τιμωρείται όταν υπάρχει πρόθεση προσωπικού (ή υπέρ τρίτου) οικονομικού κέρδους. Ως παρόμοια προϋπόθεση, η πειρατεία τιμωρείται όταν ο δράστης ενεργεί άδικα, πράγμα που σημαίνει χωρίς την άδεια του ιδιοκτήτη του. Όπως αναφέρθηκε παραπάνω, κάθε είδους πρόσβαση σε ένα πληροφοριακό σύστημα χωρίς την άδεια του κατόχου του, όπως η πειρατεία, θα θεωρείται έγκλημα, ανεξάρτητα από τον σκοπό του δράστη και ανεξάρτητα από το εάν προκαλείται ή όχι ζημιά, συμπεριλαμβανομένης της ηθικής εισβολής.

Οι ακόλουθοι νόμοι είναι τα πιο σημαντικά μέσα όσον αφορά την ασφάλεια στον κυβερνοχώρο:

- ✓ Νόμος 4961/2022 για τις «Αναδυόμενες Τεχνολογίες Πληροφορικής και Επικοινωνιών, Ενίσχυση της Ψηφιακής Διακυβέρνησης και άλλες διατάξεις».
- ✓ Ο Νόμος 5002/2022 για την «άρση του απορρήτου της διαδικασίας επικοινωνίας, θέματα κυβερνοασφάλειας και προστασία προσωπικών δεδομένων πολιτών».
- ✓ Νόμος 4727/2020 για την «Ψηφιακή Διακυβέρνηση (Μεταφορά στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Μεταφορά στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 1 και άλλες διατάξεις 2. "
- ✓ Ο Νόμος 4577/2018, με τον οποίο ενσωματώθηκε η Οδηγία NIS 2016/1148/ΕΕ στο ελληνικό δίκαιο, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύων και πληροφοριών.

- ✓ 1027/2019 Υπουργική Απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης, η οποία καθορίζει την εφαρμογή και τις διαδικασίες που προβλέπονται στο Ν. 4577/2018.
- ✓ Ο GDPR και ο σχετικός Ελληνικός Νόμος 4624/2019.
- ✓ Ο Νόμος 4411/2016 με τον οποίο ενσωματώθηκε η Οδηγία 2013/40/ΕΕ στο ελληνικό δίκαιο για τις επιθέσεις κατά των πληροφοριακών συστημάτων.
- ✓ Ν. 4070/2012, σε σχέση με τη λειτουργία δικτύων ηλεκτρονικών επικοινωνιών και την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών.
- ✓ Κανονισμός υπ' αριθμ. 205/2013 της Ελληνικής Αρχής για την Ασφάλεια και το Απόρρητο των Επικοινωνιών (ΑΔΑΕ), ο οποίος είναι Κανονισμός για την Ασφάλεια και Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.
- ✓ Κανονισμός υπ' αριθμ. 165/2011 της ΑΔΑΕ, ο οποίος είναι Κανονισμός Διασφάλισης Απορρήτου στις ηλεκτρονικές επικοινωνίες.
- ✓ Άρθρο του Ν. 3471/2006, σχετικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών τηλεπικοινωνιών και την υποχρέωση των φορέων εκμετάλλευσης να λαμβάνουν τα απαραίτητα μέτρα ασφαλείας.
- ✓ Άρθρο 386Α του Ελληνικού Ποινικού Κώδικα, σχετικά με απάτη που διαπράχθηκε μέσω υπολογιστή.
- ✓ Ν. 2121/1993, δηλαδή τον Ελληνικό Νόμο περί Πνευματικής Ιδιοκτησίας.
- ✓ Ν. 3674/2008, που αφορά τη διασφάλιση του απορρήτου της τηλεφωνικής επικοινωνίας.

Παρόλο που τα ακόλουθα δεν αποτελούν νομοθεσία αυτού, περιλαμβάνονται για λόγους πληρότητας:

Η Ελληνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης εξέδωσε την Εθνική Στρατηγική Κυβερνοασφάλειας για την περίοδο 2020–2025.

Η ΕΑΚ έχει εκδώσει ένα Εγχειρίδιο Κυβερνοασφάλειας σχετικά με τις βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων.

Η ΕΑΚ εξέδωσε ένα εργαλείο αυτοαξιολόγησης της κυβερνοασφάλειας για εταιρείες, με βάση το Εγχειρίδιο Κυβερνοασφάλειας. Αυτό είναι ένα εργαλείο μέσω του οποίου οι οργανισμοί

μπορούν να πραγματοποιήσουν μια αυτοαξιολόγηση του επιπέδου ασφάλειας των συστημάτων και των υπολογιστών τους.

Όσον αφορά τις τρέχουσες νομοθετικές εξελίξεις, θα πρέπει επίσης να συμπεριληφθούν τα ακόλουθα (παρόλο που δεν έχουν ακόμη οριστικοποιηθεί):

Στις 12.12.2022, η ΑΔΑΕ ξεκίνησε δημόσια διαβούλευση για την γνωστοποίηση Συμβάντων ασφαλείας με σημαντική επίπτωση στη λειτουργία δικτύων και υπηρεσιών από παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

Στις 19.06.2023, η ΑΔΑΕ ξεκίνησε δημόσια διαβούλευση για το σχέδιο Κανονισμού για την Ασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών. Ο παρών Κανονισμός θα αντικαταστήσει τους υφιστάμενους Κανονισμούς της ΑΔΑΕ, δηλαδή τον Κανονισμό για τη Διασφάλιση του Απορρήτου στις ηλεκτρονικές επικοινωνίες (Απόφαση ΑΔΑΕ Αρ. 165/2011) και τον Κανονισμό για την ασφάλεια και την ακεραιότητα δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (Απόφαση ΑΔΑΕ Αρ. 205/2013).

Στη συνέχεια, υπάρχουν απαιτήσεις κυβερνοασφάλειας σύμφωνα με την ισχύουσα νομοθεσία (επιπλέον αυτών που περιγράφονται παραπάνω) που ισχύουν ειδικά για κρίσιμης σημασίας υποδομές, φορείς εκμετάλλευσης βασικών υπηρεσιών ή παρόμοια.

Αναλυτικότερα, ο 4577/2018 και η υπουργική απόφαση αριθ. 1027/08.10.2019 σκιαγραφούν τις αρμοδιότητες των φορέων εκμετάλλευσης βασικών υπηρεσιών, δηλαδή των φορέων εκμετάλλευσης υποδομών ζωτικής σημασίας στους τομείς της ενέργειας, των μεταφορών, των τραπεζών και των οικονομικών, της υγείας, του πόσιμου νερού και των υποδομών πληροφορικής, οι οποίες είναι οι ακόλουθες :

- ✓ υιοθέτηση αποτελεσματικών, κατάλληλων, αναλογικών και ειδικών τεχνικών και οργανωτικών μέτρων για τον εντοπισμό πιθανών κινδύνων για την ασφάλεια και την πρόληψη και ελαχιστοποίηση των επιπτώσεων των συμβάντων στον κυβερνοχώρο·
- ✓ ειδοποίηση για όλα τα Συμβάντα που ενδέχεται να επηρεάσουν σοβαρά τη λειτουργική συνέχεια των βασικών υπηρεσιών που παρέχουν στην ΕΑΚ και την Ελληνική Ομάδα Αντιμετώπισης Συμβάντων Ασφάλειας Υπολογιστών (CSIRT) χωρίς αδικαιολόγητη καθυστέρηση·

- ✓ συνεργασία με τις αρμόδιες αρχές·
- ✓ κατάρτιση, εφαρμογή και ενημέρωση γραπτής Πολιτικής Ασφαλείας σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που υποστηρίζουν την παροχή υπηρεσιών για λογαριασμό του φορέα εκμετάλλευσης·
- ✓ διασφάλιση ότι η Πολιτική Ασφαλείας του χειριστή είναι σύμφωνη με την Περιεκτική Πολιτική Ασφαλείας που εκδίδεται από την HCA και ότι τηρούνται οι «Βασικές Απαιτήσεις Ασφαλείας», όπως περιγράφονται από την HCA· και

Ο πολύ πρόσφατος νόμος 4961/2022 εισάγει μέτρα για τη διαφανή και ασφαλή λειτουργία των συσκευών Διαδικτύου των Πραγμάτων (IoT) που χρησιμοποιούνται από φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών που ενεργούν ως φορείς εκμετάλλευσης IoT. Αυτοί οι φορείς εκμετάλλευσης IoT υποχρεούνται να χρησιμοποιούν τεχνολογίες IoT σύμφωνα με τις τεχνικές προδιαγραφές ασφάλειας, συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας, που θα καθοριστούν σε μελλοντική απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης. Οι βασικοί φορείς εκμετάλλευσης υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών που ενεργούν ως φορείς εκμετάλλευσης IoT έχουν ορισμένες υποχρεώσεις βάσει αυτής της νέας νομοθεσίας:

- Απαιτείται να ορίσουν έναν Υπεύθυνο Ασφάλειας IoT που είναι υπεύθυνος για την παρακολούθηση της ορθής εφαρμογής των τεχνικών και οργανωτικών μέτρων και τη διασφάλιση ότι το αρχείο καταγραφής που δημιουργείται από τη συσκευή τηρείται για εύλογο χρονικό διάστημα.
- Εάν μετά τη διενέργεια αξιολόγησης ή ελέγχου, η ΕΑΑ διαπιστώσει ότι μια συσκευή IoT, παρά τη συμμόρφωση με τις απαραίτητες τεχνικές προδιαγραφές ασφαλείας, παρουσιάζει κίνδυνο ασφάλειας στη λειτουργία της ή στην ασφάλεια του δικτύου και των συστημάτων πληροφοριών του σχετικού χειριστή, η ΕΑΑ ενημερώνει ο χειριστής IoT του οποίου η συσκευή παρουσιάζει κίνδυνο, ο οποίος στη συνέχεια πρέπει να αναστείλει τη χρήση της συσκευής χωρίς καθυστέρηση.
- Οφείλουν να τηρούν μητρώο των συσκευών τεχνολογίας IoT που χρησιμοποιούν, το οποίο πρέπει να ενημερώνεται σε ετήσια βάση και, σε κάθε περίπτωση, όταν ο χειριστής IoT αρχίσει να χρησιμοποιεί μια νέα συσκευή IoT. Ο χειριστής IoT καθιστά

αυτό το μητρώο διαθέσιμο στην HCA ή στην αρμόδια ομάδα απόκρισης όταν του ζητηθεί.

Σύμφωνα με τον Κώδικα Ποινικής Δικονομίας (ΚΠΔ), οι ποινικές έρευνες διενεργούνται από ανακριτές, μετά από έγγραφη εντολή του εισαγγελέα. Οι εξουσίες διερεύνησης που παρέχονται στις αρχές που διεξάγουν ποινικές έρευνες περιγράφονται επίσης στον ΚΠΔ. Σε ό,τι αφορά τα ηλεκτρονικά εγκλήματα, η Διεύθυνση Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας αναζητά ψηφιακά στοιχεία και ίχνη εγκλημάτων που διαπράχθηκαν αποκλειστικά με χρήση τεχνολογιών πληροφορικής και επικοινωνιών και στο διαδίκτυο, η επιβεβαίωση και η ταυτοποίηση του δράστη των οποίων απαιτεί εξειδικευμένη ψηφιακή και τεχνική έρευνα, συμπεριλαμβανομένης της χρήσης ειδικού λογισμικού και εργαλείων, κατασχέσεων και εξετάσεων ψηφιακών αποδεικτικών στοιχείων, διασυνοριακής συνεργασίας και ροής δεδομένων.

Το 2019 εισήχθη στον νέο ΚΠΔ ειδική νομοθετική διάταξη σχετικά με την κατάσχεση ψηφιακών αποδεικτικών στοιχείων. Το άρθρο 265 ΚΠΔ παρέχει πλέον ρητώς στις ανακριτικές αρχές την εξουσία να κατάσχουν συστήματα υπολογιστών και τα δεδομένα που είναι αποθηκευμένα σε αυτά, καθώς και μέσα αποθήκευσης που περιέχουν δεδομένα ηλεκτρονικών υπολογιστών, όπου τα πρόσωπα που διεξάγουν την έρευνα έχουν πρόσβαση σε τέτοια συστήματα υπολογιστών και μέσα αποθήκευσης. Είναι, επίσης, δυνατή η κατάσχεση απομακρυσμένων συστημάτων υπολογιστών ή μέσων αποθήκευσης και των δεδομένων που είναι αποθηκευμένα σε αυτά, όταν τέτοια συστήματα ή μέσα αποθήκευσης συνδέονται με το σύστημα υπολογιστή στο οποίο έχουν πρόσβαση οι ανακριτικές αρχές. Ωστόσο, τα ψηφιακά δεδομένα που αποθηκεύονται και έχουν πρόσβαση μέσω υπηρεσιών cloud δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή μέσο αποθήκευσης συνδεδεμένο με το σύστημα υπολογιστή στο οποίο οι αρχές έχουν φυσική πρόσβαση.

Ειδικές Ανακριτικές Πράξεις

Μετά την υπογραφή της Διεθνούς σύμβασης του Οργανισμού των Ηνωμένων Εθνών για το οργανωμένο έγκλημα στο Παλέρμο της Ιταλίας το Δεκέμβριο του 2000.Στη συνέχεια η Ελλάδα έπρεπε να εισαγάγει στον ΚΠΔ μία σειρά από ειδικές ανακριτικές τεχνικές (special investigative Techniques) για την καταπολέμηση του οργανωμένου εγκλήματος. Οι ειδικές ανακριτικές πράξεις εφαρμόζονται σε πολύ περιορισμένο εύρος εγκληματικών ενεργειών.

Έννοια και ιδιαίτερα χαρακτηριστικά των επίμαχων ανακριτικών πράξεων

Το άρθ. 254 ΚΠΔ ορίζει ότι έξι ειδικές ανακριτικές πράξεις μπορούν να διεξαχθούν εάν υπάρχουν σοβαρές ενδείξεις ότι κάποιο από τα αδικήματα που αναφέρονται στο ανωτέρω άρθρο πρόκειται να διαπραχθεί ή έχει διαπραχθεί, όπως η συγκρότηση, η συμμετοχή ή η διεύθυνση εγκληματικής ή τρομοκρατικής οργάνωσης και διάπραξη τρομοκρατικών ενεργειών, όπου δεν είναι δυνατό ή εξαιρετικά δύσκολο να επαληθευτεί με οποιονδήποτε άλλο τρόπο ότι έχει διαπραχθεί το αδίκημα. Από τις ανακριτικές πράξεις που αναφέρονται σε αυτό το άρθρο, οι πιο σχετικές με το έγκλημα στον κυβερνοχώρο είναι η άρση του απορρήτου του περιεχομένου των επικοινωνιών ή των δεδομένων τοποθεσίας και κυκλοφορίας τους, η συσχέτιση ή ο συνδυασμός προσωπικών δεδομένων και η διεξαγωγή «κρυφής έρευνας», στην οποία ο ανακριτής ή ένα άτομο που ενεργεί υπό τις διαταγές τους, προσφέρεται να διευκολύνει ένα ποινικό αδίκημα που ο δράστης έχει ήδη αποφασίσει να διαπράξει.

Προϋποθέσεις διενέργειας των Ειδικών Ανακριτικών Πράξεων

Υπάρχουν τρείς προϋποθέσεις διενέργειας των ειδικών ανακριτικών πράξεων:

1. *Η προϋπόθεση συνδρομής σοβαρών ενδείξεων*
2. *Η προϋπόθεση κατάφασης της αναγκαιότητας των ανακριτικών πράξεων*
3. *Η προϋπόθεση έκδοσης ειδικά αιτιολογημένου βουλεύματος του αρμοδίου συμβουλίου*

Με τον ΚΠΔ του 2019, βελτιώθηκε το κανονιστικό πλαίσιο των ειδικών ανακριτικών πράξεων με την υιοθέτηση θεμελιωδών παραδοχών του ΕΔΔΑ .

Αναλυτικότερα:

α) Εισήχθη αυτοτελώς η ειδική ανακριτική πράξη της συγκαλυμμένης έρευνας, η οποία υπήρχε 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).

Ανακριτική Διείσδυση

Με τον όρο ανακριτική διείσδυση θεωρείται η χρησιμοποίηση, είτε των ίδιων των ανακριτικών υπαλλήλων, είτε άλλων συνεργαζόμενων με τις ανακριτικές αρχές ιδιωτών-έμπιστων προσώπων. Η σύλληψη του δράστη τη στιγμή της διάπραξης εγκληματικής ενέργειας , όσο και τη συλλογή αποδεικτικών στοιχείων αναφορικά με την αντιμετώπιση της οργανωμένης εγκληματικής δραστηριότητας.

Με τον ΚΠΔ του 2019 υιοθετήθηκαν θεμελιακές παραδοχές του ΕΔΔΑ και η εποπτεία από τον Εισαγγελέα πλημμελειοδικών αποτελεί εγγυητικό ρόλο νομιμοποίησης της ανωτέρω ανακριτικής πράξης. Αναντίρρητα, μόνο με χρήση εξειδικευμένης ψηφιακής διερεύνησης και συνακόλουθα την χρήση εργαλείων και ειδικών λογισμικών μπορεί ενδεχομένως να αποκαλυφθούν οι δράστες σχετικών εγκλημάτων. Επιπροσθέτως, η εμπλοκή της Δίωξης ηλεκτρονικού εγκλήματος και συνακόλουθα άλλων αντίστοιχων υπηρεσιών επιβολής του νόμου εκτός των συνόρων της Ελλάδας με ανάλογες συνεργασίες, αποτελεί επιτακτική ανάγκη.Συμπερασματικά η ψηφιακή έρευνα αποτελεί εξειδικευμένη τεχνική μορφή έρευνας που συντελείται τόσο με την διασυνοριακή συνεργασία όσο και την χρήση ειδικών εργαλείων και λογισμικών και συνακόλουθα διατάσσεται μόνο για εγκλήματα που αφορούν τον κυβερνοχώρο.

Οι ελεγχόμενες μεταφορές

Η ρυθμιζόμενη στο άρθρο 38 του ν. 2145/1993 ανακριτική αυτή πράξη, αποτελεί μια ειδική περίπτωση παρακολούθησης, που σχετίζεται με την μεταφορά παράνομων αγαθών από την είσοδό τους στη χώρα μέχρι την έξοδό τους από την επικράτεια, ή μέχρι τον τελικό τόπο παραλαβής τους χωρίς να υπάρχει παρέμβαση των αρμοδίων αρχών επιβολής του νόμου η με ελάχιστη παρεμβολή, έτσι ώστε να συλληφθούν όλα τα εμπλεκόμενα στην υπόθεση πρόσωπα.

Η άρση του απορρήτου των τηλεπικοινωνιών

Οι ρυθμίσεις των άρθρων 4 και 5 του ν. 2225/1994 θεωρούνται ως οι πληρέστερες από δικαιοκρατική σκοπιά προβλέψεις αναφορικά με την παρακολούθηση εμπλεκόμενων προσώπων σε περιπτώσεις διερεύνησης συγκεκριμένων εγκλημάτων. Αυτό αποδεικνύεται από το ότι, με εξαίρεση την ελλείπουσα προϋπόθεση της παρ. 2 στοιχ. αΔ του άρθρου 253Α ΚΠΔ περί σοβαρών

ενδείξεων, οι λοιπές γενικές προϋποθέσεις των παρ. 2, 3 και 4 του ιδίου άρθρου υπήρχαν ήδη στο κείμενο του ν. 2225/1994.

Ηχητική και οπτική παρακολούθηση άρθρου 6 παρ. 4 ν. 2713/1999

Το ζήτημα της χρήσης ειδικών τεχνικών μέσων δημιουργεί σοβαρά προβλήματα διάκρισης του ιδιωτικού από το δημόσιο χώρο. Πως καθορίζονται δηλαδή τα όρια επέμβασης στο δικαίωμα της ελεύθερης ανάπτυξης ενός προσώπου και της ιδιωτικής ζωής καθώς και στις ειδικότερες εκφάνσεις τους, ήτοι στο δικαίωμα επί της ιδίας εικόνας και στο δικαίωμα επί του μη δημόσια εκφερόμενου προφορικού λόγου (άρθρα 5, 9 και 9Α Συντ.).

Η χρήση της ανωτέρω αναφερόμενης ανακριτικής πράξης και ειδικότερα η παρ. 4 του άρθρου 6 ν. 2713/1999, που θεωρείται η νομιμοποιητική της βάση, δεν είναι ξεκάθαρη.

Διασταύρωση δεδομένων προσωπικού χαρακτήρα

Ο συνδυασμός δεδομένων προσωπικού χαρακτήρα (ευαίσθητα η μη), που ενυπάρχουν σε αρχεία διαφόρων φυσικών ή νομικών προσώπων, με στόχο τη δημιουργία του ηλεκτρονικού προφίλ ενός υπόπτου, θεωρείται και η τελευταία ανακριτική πράξη αυτού του είδους.

Η συσχέτιση ευαίσθητων προσωπικών δεδομένων είναι απαγορευμένη, όταν αυτά δεν έχουν συλλεχθεί και καταχωρηθεί με νόμιμο τρόπο, αλλά και όταν αυτά δεν εισφέρουν σχετικά με την υπό εξέταση ποινική υπόθεση.

Είναι ξεκάθαρο ότι η ανακριτική αυτή πράξη προσβάλλει, το δικαίωμα πληροφορικής αυτοδιάθεσης του άρθρου 9Α Σ, και προφανώς η μη ύπαρξη των προϋποθέσεων απόκτησης του σχετικού αποδεικτικού υλικού σίγουρα θα επισύρει απαγόρευση χρήσης του κατά τα οριζόμενα στο άρθρο 19 παρ. 3 .

Επιπλέον, ο νόμος 5002/2022 για τη «Διαδικασία άρσης του απορρήτου των επικοινωνιών, την κυβερνοασφάλεια και την προστασία των προσωπικών δεδομένων των πολιτών» θεσπίζει κανόνες για την άρση του απορρήτου των επικοινωνιών, πάντα κατόπιν εντολής της αρμόδιας δικαστικής αρχής. για δύο λόγους: για λόγους εθνικής ασφάλειας, που περιλαμβάνουν λόγους που σχετίζονται με την εθνική άμυνα, την εξωτερική πολιτική, την ενεργειακή ασφάλεια και την

ασφάλεια στον κυβερνοχώρο· και για τον εντοπισμό ιδιαίτερα σοβαρών αδικημάτων. Ο Νόμος 5002/2022 ορίζει τις αρμόδιες αρχές για την υποβολή τέτοιων αιτημάτων, τον τρόπο χειρισμού του υλικού και τη διαδικασία άρσης του απορρήτου των επικοινωνιών.

Εάν το Συμβάν αφορά τη συμμόρφωση των φορέων εκμετάλλευσης βασικών υπηρεσιών με τις υποχρεώσεις τους, η HCA θα είναι η αρμόδια αρχή και μπορεί να απαιτεί από τους φορείς εκμετάλλευσης να παρέχουν τις απαραίτητες πληροφορίες για την αξιολόγηση της ασφάλειας των συστημάτων και πληροφοριών δικτύου τους, συμπεριλαμβανομένων επαληθευμένων πολιτικών ασφαλείας και αποδεικτικών στοιχείων αποτελεσματική εφαρμογή των πολιτικών ασφαλείας, όπως τα αποτελέσματα μιας επιθεώρησης ασφαλείας που διενεργείται είτε από την HCA είτε από φορέα που έχει εξουσιοδοτηθεί από αυτήν. Μετά την αξιολόγηση αυτών των πληροφοριών, η HCA μπορεί να εκδώσει δεσμευτικές οδηγίες προς τους φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποκατάσταση των διαπιστωθέντων ελλείψεων.

Όταν το Συμβάν αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το HDPA έχει τις εξουσίες διερεύνησης που του παραχωρούνται σύμφωνα με το άρθρο. Ο ΓΚΠΔ ως η αρμόδια εποπτική αρχή στην Ελλάδα, καθώς και αυτές που περιγράφονται στο άρθρο. 15 του Ν. 4624/2019, δυνάμει του οποίου η ΥΔΔΑ μπορεί να διενεργεί έρευνες και ελέγχους σχετικά με τη συμμόρφωση με τον παρόντα νόμο, στο πλαίσιο των οποίων ελέγχεται η τεχνολογική υποδομή και άλλα αυτοματοποιημένα ή μη μέσα που υποστηρίζουν την επεξεργασία προσωπικών δεδομένων. Κατά τη διεξαγωγή τέτοιων ερευνών και επιθεωρήσεων, το HDPA έχει την εξουσία να αποκτά, από τους υπευθύνους επεξεργασίας και τους υπεύθυνους επεξεργασίας, πρόσβαση σε όλα τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία και σε όλες τις πληροφορίες που είναι απαραίτητες για τους σκοπούς τέτοιων ελέγχων και την εκτέλεση των καθηκόντων του, και κανένα είδος εμπιστευτικότητας μπορεί να επικαλεστεί εναντίον του. Το HDPA, κατ' εξαίρεση, δεν θα έχει πρόσβαση σε δεδομένα ταυτοποίησης συνεργατών ή προσωπικού που απασχολείται σε οντότητες που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων.

Η πιο πρόσφατη εξέλιξη στην ελληνική έννομη τάξη είναι η θέση προς διαβούλευση από το Υπουργείο Ψηφιακής Διακυβέρνησης του σχεδίου νόμου «Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις». Το τελευταίο προβλέπει τη δημιουργία ενός Νομικού Προσώπου Δημοσίου Δικαίου με την επωνυμία «Εθνική Αρχή Κυβερνοασφάλειας». Η τελευταία θα έχει ως κύριο στόχο

της το συντονισμό και την πραγμάτωση της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια. Ταυτόχρονα, θα λειτουργεί έτσι ώστε να επιτυγχάνει την αποτελεσματική πρόληψη και την αποτελεσματική διαχείριση των κυβερνοεπιθέσων στην Ελλάδα. Ακόμη, στις αρμοδιότητες της συγκαταλέγεται η επίτευξη ενός υψηλού επιπέδου ασφαλείας των συστημάτων δικτύου και πληροφοριών στον δημόσιο και στον ιδιωτικό τομέα.

Σε δομικό επίπεδο Εθνική Αρχή Κυβερνοασφάλειας θα συνιστά μια αναβαθμισμένη μετεξέλιξη της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης. Θα βρίσκεται υπό την εποπτεία του Υπουργού Ψηφιακής Διακυβέρνησης και θα διοικείται από Διοικητή και Υποδιοικητές προκειμένου να υπάρχει ταχύτητα στη λήψης αποφάσεων. Σε ότι αφορά τη διάρθρωση της αυτή θα συμπεριλαμβάνει δύο Γενικές Διευθύνσεις εκ των οποίων η μια θα είναι επιχειρησιακή και η άλλη επιτελικού σχεδιασμού. Θα της αποδοθούν 155 οργανικές θέσεις σαφώς περισσότερες από τις 50 που έχει σήμερα, Παράλληλα θα λαμβάνεται ειδική μέριμνα προκειμένου να υπάρχει η βέλτιστη διαχείριση του ανθρώπινου δυναμικού και να ενισχυθεί η Αρχή με προσωπικό που θα έχει υψηλή εξειδίκευση. Παράλληλα, η Αρχή θα λειτουργεί Εθνικό Κέντρο Συντονισμού και Εθνική Αρχή Πιστοποίησης για την Κυβερνοασφάλεια.

Βάσει των προτεινόμενων ρυθμίσεων η Αρχή θα δρα σε μια σειρά κρίσιμων πυλώνων. Πρώτον αναμένεται να καλύπτει το σύνολο του «κύκλου της ζωής» της εθνικής στρατηγικής κυβερνοασφάλειας μέσω της στρατηγικής διοίκησης και διακυβέρνησης, ενισχύοντας στον πυρήνα του το μοντέλο διακυβέρνησης και διασφαλίζοντας τον αναγκαίο συντονισμό για την αναγνώριση και τον μετριασμό των κινδύνων στον κυβερνοχώρο σε εθνικό επίπεδο. Ταυτόχρονα, αναμένεται να υπάρξει ενίσχυση της διαφάνειας και της λογοδοσίας στη δημόσια πολιτική κυβερνοασφάλειας μέσω της παροχής ενός σαφούς ρυθμιστικού πλαισίου στα πλαίσια του οποίου γίνεται, επίσης, η καθιέρωση ρόλων, διαδικασιών και απόδοση αντίστοιχων ευθυνών στις αρμόδιες εθνικές αρχές. Δεύτερον, θα δημιουργηθούν επιχειρησιακές λειτουργίες οι οποίες θα στοχεύουν στη διασφάλιση της ενίσχυσης του επιπέδου κυβερνοασφάλειας στο σύνολο των τομέων της κοινωνικής και οικονομικής ζωής. Τρίτον, κρίσιμη είναι η ενίσχυση των τεχνικών λειτουργιών έτσι ώστε να συμπεριληφθούν νέες τεχνολογίες και εργαλεία. Τέλος, θα δημιουργηθεί ένας πυλώνας εποπτικών λειτουργιών και καθηκόντων, που θα μπορεί να διασφαλίζει την κανονιστική συμμόρφωση των οργανισμών και ειδικότερα των κρίσιμων υποδομών της χώρας.

Γενικότερα, με τη θέσπιση της ανωτέρω Αρχής, το Υπουργείο Ψηφιακής Διακυβέρνησης στοχεύει στην ενίσχυση της τεχνολογική και θεσμικής ενίσχυσης της Ελλάδας απέναντι στις κυβερνοαπειλές (ΣΝ_κυβερνοασφάλειας, 2024).

5.2 Σημασία της ανάπτυξης μιας ισχυρής κουλτούρας κυβερνοασφάλειας.

Η ενσωμάτωση της ασφάλειας στον κυβερνοχώρο στην κουλτούρα του οργανισμού είναι μία από τις καλύτερες μεθόδους για τη μείωση του κινδύνου στον κυβερνοχώρο. Αυτό προϋποθέτει την εμπέδωση στους εργαζομένους της πεποίθησης ότι ο κίνδυνος είναι υπαρκτός και ότι επηρεάζεται από την καθημερινή τους συμπεριφορά. Η κουλτούρα της κυβερνοασφάλειας είναι ζωτικής σημασίας επειδή συμβάλλει στη διασφάλιση των εταιρικών περιουσιακών στοιχείων, συμπεριλαμβανομένης της τεχνολογίας και των δεδομένων. Πρέπει να αποτελεί συστατικό στοιχείο μιας ευρύτερης επιχειρηματικής κουλτούρας καθημερινών δραστηριοτήτων που παρακινεί τους εργαζόμενους να κάνουν συνειδητές επιλογές που συμμορφώνονται με τα πρότυπα ασφαλείας (ENISA, 2017).

Η ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας είναι μόνο μία πτυχή της κουλτούρας ασφάλειας. Το προσωπικό πρέπει να γνωρίζει τον κίνδυνο ασφάλειας και τη διαδικασία αποφυγής του. Η επιχείρηση διατηρείται ασφαλής με την ανάπτυξη και την επιβολή μιας μεθόδου λειτουργίας των καθηκόντων. Η πλειονότητα των επιχειρήσεων έχει επενδύσει χρόνια και πολυάριθμους πόρους για την απόκτηση και τη δημιουργία του περιουσιακού στοιχείου των δεδομένων τους, οπότε αν αυτό χαθεί, κλαπεί ή καταστραφεί, θα μπορούσε να έχει μακροπρόθεσμα αρνητική επίδραση στην οικονομική τους κατάσταση (ENISA, 2017).

Οι εταιρείες των οποίων η ασφάλεια είναι χαλαρή βρίσκονται συχνά στο στόχαστρο των πρωτοσέλιδων εφημερίδων. Οι περισσότερες από αυτές θα μπορούσαν να είχαν αποφευχθεί εάν το προσωπικό είχε τηρήσει τις βασικές κατευθυντήριες γραμμές ασφαλείας. Το 90% των επιθέσεων στον κυβερνοχώρο οφείλονται σε ανθρώπινο λάθος ή συμπεριφορά. Τα λάθη των εργαζομένων, όπως η πτώση του φορητού υπολογιστή ή του τηλεφώνου τους, η σύνδεση ενός

flash drive ή το άνοιγμα ενός email, είναι πιο πιθανό να βλάψουν μια εταιρεία από ό,τι ένας εξωτερικός χάκερ με κακόβουλες προθέσεις (Colarik, 2006).

Οι επιχειρήσεις επενδύουν εκατομμύρια δολάρια σε εξοπλισμό και λογισμικό, αλλά παραβλέπουν το κρίσιμο βήμα της σωστής εκπαίδευσης του προσωπικού τους σε θέματα ασφάλειας. Η υψηλότερη απόδοση της επένδυσης μπορεί να προκύψει από την εκπαίδευση του προσωπικού για τον εντοπισμό κινδύνων, τον έλεγχο της ανεπιθύμητης συμπεριφοράς και την τήρηση των θεμελιωδών πρακτικών ασφαλείας. Ωστόσο, μπορεί να είναι δύσκολο να ποσοτικοποιηθεί και συνεπώς να δικαιολογηθεί το κόστος. Συχνά είναι δύσκολο να πειστεί η ανώτερη διοίκηση για την αξία της επένδυσης στην εκπαίδευση των εργαζομένων και τη δημιουργία μιας κουλτούρας με συνείδηση της ασφάλειας. Σε πολλές περιπτώσεις, η διοίκηση δεν πιστεύει ότι η απλή παροχή εκπαίδευσης στο προσωπικό μπορεί να το βοηθήσει να γίνει λιγότερο ευάλωτο σε απώλειες στον κυβερνοχώρο (ENISA, 2017).

Ένα παράδειγμα είναι το phishing email. Οι επιθέσεις στον κυβερνοχώρο ξεκινούν με μηνύματα ηλεκτρονικού "ψαρέματος" στο 90% των περιπτώσεων. Ωστόσο, η πλειονότητα των εργαζομένων πιστεύει ότι θα ήταν σε θέση να εντοπίσει ένα ηλεκτρονικό μήνυμα ηλεκτρονικού "ψαρέματος" και δεν θα συμμορφωνόταν με το αίτημα σε αυτό. Ωστόσο, η έκθεση Verizon 2019 Data Breach Investigations Report αναφέρει ότι το 12% όλων των μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing emails) επιλέγεται, ενώ το 30% όλων των μηνυμάτων ηλεκτρονικού "ψαρέματος" ανοίγει. Δεδομένου ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing προκαλούν εννέα στις δέκα μολύνσεις ransomware, η επένδυση στην εκπαίδευση των εργαζομένων σχετικά με τα μηνύματα ηλεκτρονικού ταχυδρομείου phishing μπορεί να μειώσει σημαντικά τον κίνδυνο. Το Ransomware αποτελεί μια ταχέως αναπτυσσόμενη απειλή στον κυβερνοχώρο για τις επιχειρήσεις το 2020, ιδίως στο περιβάλλον COVID-19. Η επένδυση στην εκπαίδευση του προσωπικού είναι πλέον πολύ πιο κρίσιμη. Επειδή οι απάτες phishing είναι η κύρια πηγή ransomware, αν ένας οργανισμός μπορεί να σταματήσει τα μέλη της ομάδας από το να ανταποκρίνονται σε αυτές, θα αποφύγει πολλά μελλοντικά προβλήματα. Μια επιχειρησιακή κουλτούρα κυβερνοασφάλειας μπορεί να μειώσει τα προβλήματα για χρόνια, να εξοικονομήσει εκατομμύρια δολάρια και να ενισχύσει τη φήμη μιας επιχείρησης (Verizon, 2019).

5.3 Η αντιμετώπιση της κυβερνοτρομοκρατίας στην ΕΕ

Η ΕΕ άρχισε να αναπτύσσει για πρώτη φορά μια συλλογική αντιτρομοκρατική πολιτική το 2001, αμέσως μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου στις Ηνωμένες Πολιτείες. Εστιάζοντας αρχικά στην εξωτερική απειλή που συνιστά η τρομοκρατία (European Commission, 2001), το πρώτο σχέδιο δράσης της ΕΕ για την καταπολέμηση της τρομοκρατίας εγκρίθηκε τον Νοέμβριο του 2001 και ακολουθήθηκε αργότερα, μετά τις τρομοκρατικές επιθέσεις στη Μαδρίτη το 2004 και στο Λονδίνο το 2005, από την Αντιτρομοκρατική Στρατηγική της ΕΕ (Council of the European Union, 2005). Από τότε, η αντιτρομοκρατική πολιτική της ΕΕ έχει εξελιχθεί για να επικεντρωθεί, ολιστικά, σε θέματα εσωτερικής και εξωτερικής ασφάλειας, όπως η αντιριζοσπαστικοποίηση, οι απαντήσεις σε ξένους μαχητές, η ασφάλεια των συνόρων ως αντιτρομοκρατικό μέτρο και η τρομοκρατική χρήση του Διαδικτύου. Κατά τη διάρκεια αυτής της ανάπτυξης της αντιτρομοκρατικής πολιτικής της ΕΕ, η απειλή από την «κυβερνοτρομοκρατία» επικαλέστηκε κατά διαστήματα ως πιθανή μελλοντική ανησυχία για την ΕΕ σε αυτόν τον τομέα, αν και με πολύ μεγαλύτερη συχνότητα από το 2010. Επί του παρόντος, υπάρχει μικρή έρευνα για την Ε.Ε. απάντηση στο συγκεκριμένο ζήτημα της κυβερνοτρομοκρατίας (Argomaniz, 2015). Αυτό το άρθρο, επομένως, συμβάλλει σε ένα μικρό αλλά αναπτυσσόμενο πεδίο βιβλιογραφίας που αναλύει τον ρόλο της ΕΕ ως περιφερειακού παράγοντα κυβερνοασφάλειας, προσφέροντας μια ανάλυση λόγου για το πώς η ΕΕ αντιλαμβάνεται την απειλή από την κυβερνοτρομοκρατία.

Η πρώτη καταγεγραμμένη περίπτωση χρήσης του όρου κυβερνοτρομοκρατία από θεσμικό όργανο της ΕΕ ήταν στη δράση του Συμβουλίου της Ευρωπαϊκής Ένωσης (2002) σχέδιο για την προώθηση της συνεργασίας ΕΕ-Ιαπωνίας από τον Ιανουάριο του 2002. Η κυβερνοτρομοκρατία αναφέρθηκε ως μια μορφή «εγκλήματος στον κυβερνοχώρο» και μια από μια ομάδα πιθανών απειλών για την ασφάλεια, που θα απαιτούσε αυξημένη διμερή συνεργασία μεταξύ της Europol και των ιαπωνικών αστυνομικών τμημάτων για την καταπολέμηση του διεθνικού εγκλήματος. Η απόφαση-πλαίσιο για τις επιθέσεις κατά των συστημάτων πληροφοριών υπογράφηκε σε νόμο το 2005. Ωστόσο, ενώ περιέγραφε ξεκάθαρα «το ενδεχόμενο τρομοκρατικών επιθέσεων κατά συστημάτων πληροφοριών που αποτελούν μέρος της ζωτικής σημασίας υποδομής των κρατών μελών» ως πρωταρχικό μέλημα που καθιστά αναγκαία την προσέγγιση του σχετικού ποινικού δικαίου (Council of the European Union, 2005). Ομοίως, η έννοια της κυβερνοτρομοκρατίας απουσίαζε επίσης από την πρώτη Αντιτρομοκρατική Στρατηγική της ΕΕ, που κυκλοφόρησε τον Δεκέμβριο του 2005. Σε αυτό το σημείο, η ΕΕ εστίασε στην παρεμπόδιση της πιθανής χρήσης του Διαδικτύου από τρομοκράτες είτε για να χρηματοδοτήσουν επιθέσεις, να στρατολογήσουν είτε

«για να επικοινωνήσουν και να διαδώσουν τεχνική εμπειρογνωμοσύνη σχετικά με την τρομοκρατία» (Council of the European Union, 2005).

Αν και αγνοήθηκε στην αρχική αντιτρομοκρατική στρατηγική, το θέμα της κυβερνοτρομοκρατίας προσδιορίστηκε ως μία από τις τρεις κύριες προτεραιότητες μήνες αργότερα, τον Μάιο του 2006, ως μέρος του αναθεωρημένου σχεδίου δράσης της ΕΕ για την καταπολέμηση της τρομοκρατίας. Για την ΕΕ, η κυβερνοτρομοκρατία θεωρείται μία από τις πολλές υβριδικές απειλές για την ασφάλεια που προκαλούν τα κράτη μέλη της. Όπως σημείωσε η Ευρωπαϊκή Ατζέντα για την Ασφάλεια, «οι απειλές όπως αυτές που θέτει η κυβερνοτρομοκρατία και οι υβριδικές απειλές θα μπορούσαν να αυξηθούν τα επόμενα χρόνια» (European Commission, 2015). Η ανησυχία για τις υβριδικές απειλές έχει επίσης επικληθεί σε πολλές από τις συζητήσεις για θέματα ασφάλειας στο Ευρωπαϊκό Κοινοβούλιο. Για παράδειγμα, σε μια συζήτηση για την 71η Σύνοδο της Γενικής Συνέλευσης των Ηνωμένων Εθνών το 2016, ο Kovatchev ισχυρίστηκε ότι η ευκαιρία να εκφράσει τη γνώμη του ΕΚ ήταν μεγάλης σημασίας σε περιόδους προκλήσεων, ειδικά όταν τίθεται ενάντια στη «σύγκρουση στην ΕΕ Το κατώφλι του 39, η αυξανόμενη έκθεση της Ευρώπης στον υβριδικό πόλεμο, την κυβερνοτρομοκρατία, τους ξένους μαχητές, τα πρωτοφανή κύματα μεταναστών και τη ασάφεια της διάκρισης μεταξύ εξωτερικών και εσωτερικών απειλών» (Kovatchev, 2016).

Ομοίως, η Europol έχει προειδοποιήσει για τους κινδύνους της σύγκλισης «κυβερνο-τρομοκρατίας», σημειώνοντας ότι «μια κυβερνοεπίθεση μπορεί να ενισχύσει τον αντίκτυπο μιας πραγματικής επίθεσης, εάν πραγματοποιηθεί σε συνδυασμό με την τελευταία, σε αυτό που μπορεί να ονομαστεί υβριδική επίθεση, για παράδειγμα, με διακοπή έκτακτης ανάγκης ή άλλες βασικές δημόσιες υπηρεσίες» (Europol, 2018). Ο διάλογος της ΕΕ για την κυβερνοτρομοκρατία τη βλέπει ως μια νέα και αυξανόμενη απειλή, μια απειλή που είναι ταυτόχρονα χωρίς σύνορα και πολύ πραγματική απειλή για τη δημοκρατία. Η Ευρωπόλ υπήρξε βασικός θεσμός στην άρθρωση αυτής της πτυχής της αντιληπτής απειλής από την κυβερνοτρομοκρατία, τονίζοντας ότι τα κράτη μέλη πρέπει να γνωρίζουν ότι η κυβερνοτρομοκρατία χρησιμοποιεί έναν «νέο τρόπο λειτουργίας» όπου «οι τρομοκράτες είναι σε θέση να επιχειρούν από απομακρυσμένες τοποθεσίες, ελαχιστοποιώντας τον κίνδυνο εντοπισμού». Europol, 2016).

Στις 28 Οκτωβρίου 2021, το Κοινοβούλιο της Ευρωπαϊκής Ένωσης (ΕΕ) ενέκρινε την αναθεωρημένη Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS), κοινώς αναφερόμενη

ως NIS-2, η οποία βασίζεται και καταργεί την Οδηγία (ΕΕ) 2016/1148 για την Ασφάλεια Δικτύων και Πληροφοριακά Συστήματα (Οδηγία NIS) (1). Η Οδηγία NIS που εφαρμόστηκε αρχικά το 2016 είναι η πρώτη νομοθεσία σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο που στοχεύει στην παροχή νομικών μέτρων για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην ΕΕ και ο ειδικός της στόχος ήταν να επιτύχει ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας στα κράτη μέλη .

Αν και η Οδηγία NIS αύξησε τις δυνατότητες κυβερνοασφάλειας των κρατών μελών, η εφαρμογή της έχει αποδειχθεί δύσκολη, με αποτέλεσμα τον κατακερματισμό σε διαφορετικά επίπεδα στην εσωτερική αγορά. Ως εκ τούτου, η νέα Οδηγία NIS-2 έχει σχεδιαστεί για να ενημερώσει την προηγούμενη έκδοση που εκδόθηκε το 2016 εκσυγχρονίζοντας το υφιστάμενο νομικό πλαίσιο ασφάλειας στον κυβερνοχώρο ώστε να αντικατοπτρίζει τον συνεχιζόμενο ψηφιακό μετασχηματισμό της κοινωνίας. Αυτός ο μετασχηματισμός έχει ενταθεί από την πανδημία COVID-19, η οποία έχει διευρύνει το τοπίο απειλών φέρνοντας νέες προκλήσεις με πιθανές κλιμακωτές επιπτώσεις που μπορούν να επηρεάσουν αρνητικά την παροχή κρίσιμων υπηρεσιών σε ολόκληρη την εσωτερική αγορά . Ο αριθμός των κυβερνοεπιθέσεων συνεχίζει να αυξάνεται, με ολοένα και πιο εξελιγμένες επιθέσεις να προέρχονται από ευρύ φάσμα πηγών τόσο εντός όσο και εκτός της ΕΕ.

Η αναθεωρημένη οδηγία NIS-2 έχει ανατεθεί στην Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας (ITRE), εντός του Ευρωπαϊκού Κοινοβουλίου, και προορίζεται να αποτελέσει μία από τις βασικές γραμμές για το ευρωπαϊκό πλαίσιο ασφάλειας στον κυβερνοχώρο, καθώς και να λειτουργήσει ως κεντρικό εργαλείο για την προώθηση της στρατηγικής αυτονομίας της Ευρώπης και του προγράμματος Ψηφιακή Ευρώπη.

6.0 Τρέχουσα κατάσταση της κυβερνοτρομοκρατίας

6.1 Τρέχουσες εξελίξεις στον τομέα της κυβερνοτρομοκρατίας.

Η πανδημία COVID-19 δημιούργησε νέες προκλήσεις για τους οργανισμούς και τα άτομα όσον αφορά την ασφάλεια στον κυβερνοχώρο, καθώς όλο και περισσότεροι άνθρωποι εργάζονται από το σπίτι και βασίζονται σε ψηφιακά συστήματα για να παραμείνουν συνδεδεμένοι. Αυτή η αλλαγή έχει δημιουργήσει νέες ευκαιρίες για τους εγκληματίες του κυβερνοχώρου να

πραγματοποιήσουν επιθέσεις, καθώς οι απομακρυσμένοι εργαζόμενοι μπορεί να είναι πιο ευάλωτοι σε απάτες phishing και άλλες μορφές εγκλήματος στον κυβερνοχώρο.

Μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζουν οι οργανισμοί κατά τη διάρκεια της πανδημίας είναι η διασφάλιση των απομακρυσμένων εργαζομένων, οι οποίοι ενδέχεται να μην έχουν το ίδιο επίπεδο ασφάλειας με αυτό που θα είχαν σε ένα παραδοσιακό περιβάλλον γραφείου. Αυτό περιλαμβάνει ζητήματα όπως η χρήση μη ασφαλών δικτύων Wi-Fi, η χρήση προσωπικών συσκευών για εργασιακούς σκοπούς και η μεγαλύτερη ευαισθησία σε απάτες phishing και άλλες μορφές κοινωνικής μηχανικής. Επιπλέον, η ξαφνική στροφή στην απομακρυσμένη εργασία έχει διαταράξει τις λειτουργίες κυβερνοασφάλειας πολλών οργανισμών, καθώς οι ομάδες πληροφορικής έπρεπε να λειτουργήσουν με ταχύτητα για να υποστηρίξουν την απομακρυσμένη εργασία και να διασφαλίσουν νέα συστήματα και συσκευές. Αυτό δημιούργησε νέες προκλήσεις στον τομέα της ασφάλειας και πολλοί οργανισμοί δυσκολεύτηκαν να ακολουθήσουν τον ρυθμό των αλλαγών (Nugroho & Chandrawulan , 2022).

Η πανδημία COVID-19 έχει, επίσης, οδηγήσει σε αύξηση των ηλεκτρονικών απατών, καθώς οι άνθρωποι είναι πιο ευάλωτοι σε απάτες phishing και άλλες μορφές ψηφιακής εξαπάτησης σε μια περίοδο αβεβαιότητας και οικονομικής δυσχέρειας. Αυτό υπογραμμίζει τη σημασία της επαγρύπνησης και της λήψης μέτρων για την προστασία από τέτοιου είδους επιθέσεις.

Ως εκ τούτου, Η πανδημία COVID-19 ανέδειξε τον κρίσιμο ρόλο που διαδραματίζουν η τεχνολογία και τα ψηφιακά συστήματα στην υγειονομική περίθαλψη και είναι πιθανό ότι η τάση αυτή θα συνεχιστεί ακόμη και μετά την υποχώρηση της πανδημίας. Ως αποτέλεσμα, η απειλή της κυβερνοτρομοκρατίας στον τομέα της υγείας είναι πιθανό να παραμείνει υψηλή στον κόσμο μετά την COVID-19 (Nugroho & Chandrawulan , 2022).

Μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει ο τομέας της υγειονομικής περίθαλψης μετά το COVID-19 είναι η διασφάλιση του αυξημένου όγκου δεδομένων ασθενών που παράγονται και αποθηκεύονται ηλεκτρονικά. Αυτά περιλαμβάνουν ευαίσθητες πληροφορίες, όπως ιατρικά αρχεία, οικονομικά δεδομένα και πληροφορίες προσωπικής ταυτοποίησης, οι οποίες μπορεί να είναι πολύτιμες για τους εγκληματίες του κυβερνοχώρου για διάφορους λόγους.

Επιπλέον, η συνεχής ενσωμάτωση της τεχνολογίας στην υγειονομική περίθαλψη θα δημιουργήσει νέες ευκαιρίες για τους εγκληματίες του κυβερνοχώρου να πραγματοποιήσουν

επιθέσεις, όπως η διακοπή της αλυσίδας εφοδιασμού ιατρικού εξοπλισμού, η παραβίαση της ασφάλειας των ιατρικών συσκευών και η κλοπή ευαίσθητων πληροφοριών από παρόχους υγειονομικής περίθαλψης και ασθενείς.

Συμπερασματικά, η απειλή της κυβερνοτρομοκρατίας στον τομέα της υγείας θα παραμείνει υψηλή και μετά τον COVID-19 και είναι σημαντικό οι οργανισμοί να λάβουν μέτρα για να προστατεύσουν τους εαυτούς τους και τους ασθενείς τους από επιθέσεις. Επενδύοντας σε μέτρα κυβερνοασφάλειας και βελτιώνοντας τη συνολική στάση της κυβερνοασφάλειας, ο τομέας της υγειονομικής περίθαλψης μπορεί να διασφαλίσει ότι είναι προετοιμασμένος να αντιμετωπίσει τη συνεχιζόμενη απειλή της κυβερνοτρομοκρατίας (Kuhn, Bicakci, & Shaikh, 2021).

6.1.1. Ο ρόλος της κυβερνοτρομοκρατίας στο διεθνές πολιτικό γίγνεσθαι το 2022. Η περίπτωση του Ρωσο-Ουκρανικού Πολέμου.

Η τρομοκρατία στον κυβερνοχώρο έχει παίξει ρόλο στη συνεχιζόμενη σύγκρουση μεταξύ της Ρωσίας και της Ουκρανίας, η οποία ξεκίνησε το 2014 και κλιμακώθηκε το 2022 με την εισβολή του ρωσικού στρατού στην Ουκρανία. Και οι δύο πλευρές έχουν χρησιμοποιήσει τις επιθέσεις στον κυβερνοχώρο ως εργαλείο για τη συλλογή πληροφοριών, τη διατάραξη των επιχειρήσεων του αντιπάλου τους και τον επηρεασμό της κοινής γνώμης.

Για παράδειγμα, ουκρανικές κυβερνητικές υπηρεσίες και στρατιωτικοί στόχοι έχουν στοχοποιηθεί με κακόβουλο λογισμικό, επιθέσεις phishing και άλλες μορφές κυβερνοεγκλήματος. Οι ρωσικές στρατιωτικές υπηρεσίες πληροφοριών έχουν κατηγορηθεί για τη διεξαγωγή κυβερνοεπιθέσεων εναντίον ουκρανικών υποδομών, συμπεριλαμβανομένων δικτύων ηλεκτρικής ενέργειας, συστημάτων μεταφορών και κρίσιμων χρηματοπιστωτικών ιδρυμάτων.

Επιπλέον, και οι δύο πλευρές έχουν χρησιμοποιήσει εκστρατείες προπαγάνδας και παραπληροφόρησης για να επηρεάσουν την κοινή γνώμη, τόσο στο εσωτερικό όσο και διεθνώς. Αυτό περιελάμβανε τη διάδοση ψευδών πληροφοριών μέσω των μέσων κοινωνικής δικτύωσης, την παραβίαση ειδησεογραφικών ιστότοπων και τη χειραγώγηση διαδικτυακών φόρουμ συζητήσεων (Przetacznik & Tarpova, 2022).

Εν κατακλείδι, η συνεχιζόμενη σύγκρουση μεταξύ Ρωσίας και Ουκρανίας κατέδειξε τον αυξανόμενο ρόλο που διαδραματίζει η κυβερνοτρομοκρατία στον σύγχρονο πόλεμο και την ανάγκη οι κυβερνήσεις και οι στρατιωτικοί οργανισμοί να λάβουν μέτρα για την προστασία τους

από αυτού του είδους τις επιθέσεις. Επενδύοντας σε μέτρα κυβερνοασφάλειας και βελτιώνοντας τη συνολική στάση κυβερνοασφάλειας, οι οργανισμοί αυτοί μπορούν να διασφαλίσουν ότι είναι προετοιμασμένοι να αντιμετωπίσουν τη συνεχιζόμενη απειλή της κυβερνοτρομοκρατίας.

6.2 Γεωγραφική κατανομή των κυβερνοτρομοκρατών και των στόχων τους.

Η γεωγραφική κατανομή των κυβερνοτρομοκρατών και των στόχων τους είναι δύσκολο να ποσοτικοποιηθεί, καθώς το κυβερνοέγκλημα είναι μια δραστηριότητα άκρως διεθνής και χωρίς σύνορα. Ωστόσο, ορισμένες χώρες έχουν μεγαλύτερη συγκέντρωση κυβερνοτρομοκρατών και είναι πιθανότερο να αποτελέσουν στόχο από άλλες.

Όσον αφορά την προέλευση των κυβερνοτρομοκρατών, οι χώρες με μεγάλο αριθμό εξειδικευμένων τεχνικών εμπειρογνωμόνων, όπως η Ρωσία, η Κίνα και η Βόρεια Κορέα, έχουν αναγνωριστεί ως πιθανές πηγές κυβερνοτρομοκρατίας. Ωστόσο, είναι σημαντικό να σημειωθεί ότι πολλοί κυβερνοτρομοκράτες δρουν από πολλαπλές τοποθεσίες, γεγονός που καθιστά δύσκολο τον εντοπισμό της ακριβούς προέλευσής τους. Όσον αφορά τους στόχους, οι ανεπτυγμένες χώρες με ιδιαίτερα ανεπτυγμένες ψηφιακές υποδομές, όπως οι Ηνωμένες Πολιτείες, το Ηνωμένο Βασίλειο και η Γερμανία, αποτελούν συχνά στόχο των κυβερνοτρομοκρατών λόγω των πολύτιμων πληροφοριών που κατέχουν (Lella, Tsekmezoglou, Naydenov, & Malatras, 2022).

Ωστόσο, οι αναδυόμενες οικονομίες και οι αναπτυσσόμενες χώρες γίνονται, επίσης, όλο και περισσότερο στόχοι, καθώς επενδύουν σε ψηφιακές υποδομές και διαθέτουν πολύτιμες πληροφορίες και περιουσιακά στοιχεία. Για παράδειγμα, οι χώρες της Μέσης Ανατολής και της Αφρικής έχουν βιώσει αύξηση της κυβερνοτρομοκρατίας τα τελευταία χρόνια.

Συμπερασματικά, η γεωγραφική κατανομή των κυβερνοτρομοκρατών και των στόχων τους είναι δύσκολο να ποσοτικοποιηθεί και μπορεί να ποικίλλει ανάλογα με τα κίνητρα και τους στόχους των κυβερνοτρομοκρατών. Ωστόσο, οι ανεπτυγμένες χώρες με ιδιαίτερα ανεπτυγμένες ψηφιακές υποδομές και οι αναδυόμενες οικονομίες με αναπτυσσόμενες ψηφιακές υποδομές είναι πιθανό να συνεχίσουν να αποτελούν στόχο των κυβερνοτρομοκρατών.

6.3 Αντιδράσεις κυβερνήσεων και διεθνών οργανισμών.

Οι κυβερνήσεις και οι διεθνείς οργανισμοί ανταποκρίνονται στην απειλή της τρομοκρατίας στον κυβερνοχώρο με μια πολύπλευρη προσέγγιση, η οποία περιλαμβάνει τόσο νομικά όσο και

τεχνικά μέτρα. Τα νομικά μέτρα περιλαμβάνουν τη θέσπιση νέων νόμων και κανονισμών με στόχο την αύξηση της ασφάλειας των ψηφιακών συστημάτων και την προστασία από τις απειλές στον κυβερνοχώρο. Για παράδειγμα, πολλές χώρες έχουν θεσπίσει νόμους για την προστασία των δεδομένων που απαιτούν από τους οργανισμούς να εφαρμόζουν κατάλληλα μέτρα ασφαλείας για την προστασία ευαίσθητων πληροφοριών. Επιπλέον, οι κυβερνήσεις έχουν συστήσει οργανισμούς και ομάδες εργασίας για την ασφάλεια στον κυβερνοχώρο με σκοπό τον συντονισμό της αντίδρασής τους στις απειλές στον κυβερνοχώρο και την προστασία της εθνικής ασφάλειας (Abeyratne, 2011).

Διεθνείς οργανισμοί, όπως τα Ηνωμένα Έθνη, η Ευρωπαϊκή Ένωση και το ΝΑΤΟ, εργάζονται επίσης για την αντιμετώπιση της απειλής της τρομοκρατίας στον κυβερνοχώρο μέσω μιας σειράς πρωτοβουλιών. Για παράδειγμα, τα Ηνωμένα Έθνη δημιούργησαν την Ομάδα Κυβερνητικών Εμπειρογνωμόνων για τις Εξελίξεις στον τομέα των Πληροφοριών και των Τηλεπικοινωνιών στο πλαίσιο της Διεθνούς Ασφάλειας με σκοπό να συζητήσουν και να συντονίσουν τις διεθνείς απαντήσεις στις απειλές στον κυβερνοχώρο. Η Ευρωπαϊκή Ένωση έχει συστήσει το Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο (EC3) για να συντονίζει την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και της τρομοκρατίας στον κυβερνοχώρο στην Ευρώπη (Kaljurand, 2016).

Τα τεχνικά μέτρα περιλαμβάνουν επενδύσεις σε τεχνολογίες κυβερνοασφάλειας και κατάρτιση για τη βελτίωση της συνολικής στάσης των κυβερνήσεων και των οργανισμών στον κυβερνοχώρο. Αυτό περιελάμβανε την ανάπτυξη προηγμένων τεχνολογιών κυβερνοασφάλειας, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση, για την καλύτερη ανίχνευση και αντιμετώπιση των απειλών στον κυβερνοχώρο. Επιπλέον, οι κυβερνήσεις και οι οργανισμοί έχουν επενδύσει σε προγράμματα κατάρτισης και ευαισθητοποίησης σε θέματα κυβερνοασφάλειας για να εκπαιδεύσουν τους υπαλλήλους σχετικά με τους κινδύνους και τις συνέπειες των απειλών στον κυβερνοχώρο και να τους παράσχουν τις δεξιότητες και τις γνώσεις που θα τους βοηθήσουν στην προστασία από αυτές τις απειλές.

Διεθνείς οργανισμοί, όπως η ITU και ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης, εργάζονται για την ανάπτυξη παγκόσμιων προτύπων και κατευθυντήριων γραμμών για την ασφάλεια στον κυβερνοχώρο, προκειμένου να βοηθήσουν στην προστασία από τις απειλές στον κυβερνοχώρο. Αυτά τα πρότυπα και οι κατευθυντήριες γραμμές παρέχουν ένα πλαίσιο για

τις κυβερνήσεις και τους οργανισμούς ώστε να υιοθετήσουν βέλτιστες πρακτικές για την προστασία από τις απειλές στον κυβερνοχώρο και να διασφαλίσουν ότι τα μέτρα κυβερνοασφάλειας που εφαρμόζουν είναι αποτελεσματικά και επικαιροποιημένα (Lella, Tsekmezoglou, Naydenov, & Malatras, 2022).

Συνοψίζοντας, η αντίδραση των κυβερνήσεων και των διεθνών οργανισμών στην απειλή της τρομοκρατίας στον κυβερνοχώρο ήταν ολοκληρωμένη και πολύπλευρη, περιλαμβάνοντας τόσο νομικά όσο και τεχνικά μέτρα. Συνεργαζόμενοι, οι οργανισμοί αυτοί μπορούν να συμβάλουν στην προστασία από την κυβερνοτρομοκρατία και να προωθήσουν ένα ασφαλέστερο ψηφιακό περιβάλλον.

Συμπεράσματα.

Η κυβερνοτρομοκρατία έχει αναπτυχθεί έντονα και ραγδαία με την πάροδο των ετών και έχει καταστεί μείζον ζήτημα ασφάλειας σε όλο τον κόσμο. Η κυβερνοτρομοκρατία αναφέρεται στη χρήση ψηφιακών τεχνολογιών, όπως το διαδίκτυο και τα συστήματα υπολογιστών, για την πραγματοποίηση τρομοκρατικών ενεργειών. Στις πρώτες ημέρες του διαδικτύου, η κυβερνοτρομοκρατία περιοριζόταν σε μεγάλο βαθμό σε διασπαστικές επιθέσεις σε συστήματα υπολογιστών, όπως επιθέσεις άρνησης παροχής υπηρεσιών (DoS). Ωστόσο, καθώς η τεχνολογία έχει εξελιχθεί και το διαδίκτυο έχει γίνει πιο διαδεδομένο, το πεδίο εφαρμογής της κυβερνοτρομοκρατίας έχει επεκταθεί και περιλαμβάνει πιο εξελιγμένες και επιζήμιες επιθέσεις, όπως παραβιάσεις δεδομένων, κυβερνοκατασκοπεία και επιθέσεις ransomware.

Η κυβερνοτρομοκρατία έχει γίνει παγκόσμιο ζήτημα, με δράστες που δραστηριοποιούνται σε μεμονωμένες χώρες, αλλά και σε σε όλο τον κόσμο. Ορισμένοι από τους πιο εξέχοντες φορείς της κυβερνοτρομοκρατίας περιλαμβάνουν κρατικά χρηματοδοτούμενους χάκερ, ομάδες ακτιβιστών και συνδικάτα οργανωμένου εγκλήματος. Οι εν λόγω φορείς ευθύνονται για ένα ευρύ φάσμα κυβερνοεπιθέσεων, από σχετικά μικρές παραβιάσεις δεδομένων έως μεγάλες κυβερνοεπιθέσεις που έχουν προκαλέσει εκτεταμένη αναστάτωση και οικονομική ζημία. Τα τελευταία χρόνια, η πανδημία COVID-19 έχει επιδεινώσει την απειλή της κυβερνοτρομοκρατίας, καθώς πολλοί άνθρωποι και οργανισμοί έχουν αναγκαστεί να στραφούν σε απομακρυσμένη εργασία και να βασίζονται περισσότερο στις ψηφιακές τεχνολογίες. Αυτό δημιούργησε νέες ευκαιρίες για τους εγκληματίες και τους τρομοκράτες του κυβερνοχώρου να εκμεταλλευτούν τα τρωτά σημεία των ψηφιακών συστημάτων και να πραγματοποιήσουν επιθέσεις.

Το μέλλον της κυβερνοτρομοκρατίας είναι δύσκολο να προβλεφθεί, αλλά είναι πιθανό να συνεχίσει να εξελίσσεται και να αποτελεί αυξανόμενη απειλή για την κοινωνία. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται και το διαδίκτυο αφορά όλο και περισσότερες εκφάνσεις της κοινωνικής και προσωπικής ζωής, είναι πιθανό ότι το πεδίο εφαρμογής της κυβερνοτρομοκρατίας θα συνεχίσει να διευρύνεται, με τους εγκληματίες και τους τρομοκράτες του κυβερνοχώρου να χρησιμοποιούν νέες και πιο εξελιγμένες τεχνικές για την πραγματοποίηση των επιθέσεών τους.

Μια πιθανή επίπτωση της κυβερνοτρομοκρατίας στην κοινωνία είναι η αυξημένη οικονομική ζημία. Καθώς οι οργανισμοί εξαρτώνται όλο και περισσότερο από τις ψηφιακές τεχνολογίες, οι κυβερνοεπιθέσεις που διαταράσσουν ή θέτουν σε κίνδυνο κρίσιμα συστήματα και

υποδομές θα μπορούσαν να έχουν καταστροφικές συνέπειες για την παγκόσμια οικονομία. Για παράδειγμα, μια μεγάλη επίθεση με ransomware θα μπορούσε να παραλύσει μια βασική βιομηχανία, προκαλώντας εκτεταμένη αναστάτωση και οικονομικές απώλειες.

Ένας άλλος πιθανός αντίκτυπος της κυβερνοτρομοκρατίας στην κοινωνία είναι οι αυξημένες ανησυχίες για την προστασία της ιδιωτικής ζωής. Καθώς οι εγκληματίες και οι τρομοκράτες του κυβερνοχώρου γίνονται πιο εξελιγμένοι, μπορεί να είναι σε θέση να πραγματοποιούν παραβιάσεις δεδομένων που θέτουν σε κίνδυνο ευαίσθητες πληροφορίες, όπως προσωπικά δεδομένα, οικονομικές πληροφορίες και εμπιστευτικές επιχειρηματικές πληροφορίες. Αυτό θα μπορούσε να έχει σοβαρές συνέπειες για άτομα και οργανισμούς και να υπονομεύσει την εμπιστοσύνη του κοινού στις ψηφιακές τεχνολογίες. Η αυξανόμενη διασύνδεση των ψηφιακών συστημάτων και η άνοδος του Διαδικτύου των Πραγμάτων (IoT) θα μπορούσαν επίσης να αυξήσουν τον κίνδυνο κυβερνοτρομοκρατίας στο μέλλον. Καθώς όλο και περισσότερες συσκευές συνδέονται στο διαδίκτυο, θα υπάρχουν περισσότερες ευκαιρίες για εγκληματίες και τρομοκράτες του κυβερνοχώρου να πραγματοποιήσουν επιθέσεις, και οι συνέπειες αυτών των επιθέσεων θα μπορούσαν να είναι ακόμη πιο σοβαρές.

Συμπερασματικά, η απειλή της κυβερνοτρομοκρατίας αποτελεί μείζονα ανησυχία για την κοινωνία και είναι πιθανό να συνεχίσει να εξελίσσεται και να δημιουργεί νέες προκλήσεις τα επόμενα χρόνια. Η αντιμετώπιση αυτής της απειλής θα απαιτήσει συντονισμένες και συνεχείς προσπάθειες από κυβερνήσεις, οργανισμούς και άτομα, καθώς και συνεχή έρευνα και ανάπτυξη στον τομέα της κυβερνοασφάλειας.

Υπάρχουν ορισμένοι τομείς στους οποίους απαιτείται περαιτέρω έρευνα για την καλύτερη κατανόηση και αντιμετώπιση της απειλής της κυβερνοτρομοκρατίας. Για παράδειγμα, υπάρχει ανάγκη για περισσότερη έρευνα σχετικά με τα κίνητρα και τις τακτικές των εγκληματιών και τρομοκρατών του κυβερνοχώρου, καθώς και σχετικά με τους τρόπους με τους οποίους χρησιμοποιούνται οι ψηφιακές τεχνολογίες για την πραγματοποίηση επιθέσεων. Επιπλέον, υπάρχει ανάγκη για περαιτέρω έρευνα σχετικά με τους τρόπους με τους οποίους οι οργανισμοί μπορούν να προστατευθούν καλύτερα από τις απειλές στον κυβερνοχώρο, καθώς και σχετικά με τον ρόλο που μπορούν να διαδραματίσουν οι κυβερνήσεις και οι διεθνείς οργανισμοί στη βελτίωση της παγκόσμιας ασφάλειας στον κυβερνοχώρο.

Τέλος, είναι σημαντικό οι ιθύνοντες να αναλάβουν δράση για την αντιμετώπιση της απειλής της κυβερνοτρομοκρατίας. Αυτό μπορεί να περιλαμβάνει επενδύσεις σε τεχνολογίες και κατάρτιση στον κυβερνοχώρο, εφαρμογή βέλτιστων πρακτικών για την προστασία από απειλές στον κυβερνοχώρο και συνεργασία για την προώθηση ενός ασφαλέστερου ψηφιακού περιβάλλοντος. Με τη λήψη αυτών των μέτρων, μπορούμε να συμβάλουμε στη διασφάλιση ότι οι ψηφιακές τεχνολογίες χρησιμοποιούνται με ασφαλή και προστατευμένο τρόπο και ότι η απειλή της κυβερνοτρομοκρατίας μειώνεται και τελικά εξαλείφεται.

Βιβλιογραφία

Abeyratne, R. (2011). Cyber terrorism and aviation—national and international responses. *Journal of Transportation Security*, 337–349.

Ahmed, M. A., Sindi , H., & Nour, M. (2022). Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy*, 853–861.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 1-23.

Alsanad, A., & Altuwaijri, S. (2022). Advanced Persistent Threat Attack Detection using Clustering Algorithms. *International Journal of Advanced Computer Science and Applications*, 640-649.

Anderson, R. (2012). Cybercrime and cyber terrorism. . *Computer Law & Security Review*, 5-14.

Asongu, A., Orim , S.-M., & Nting , R. (2019). Terrorism and social media: global evidence. *Journal of Global Information Technology Management*, 208-228.

Belkasim, O. (2017). Understanding cyberterrorism. *Journal of Strategic Security*, 15-28.

Brill, A. E. (2010). From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems. In *Defence Against Terrorism Review* (pp. 23-36). Ankara: Center of Excellence-Defence Against Terrorism.

Bukhres, A. (2019). Cyberterrorism: A review of the literature. . *Journal of Cybersecurity*, 77-87.

Calafato, T., & Caruana, P. (2015). Terrorism in Transition: The Implications of Cyber-Terrorism. *Societies in Transition* , 207–220.

Carr, J. (2013). The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*, 32-37.

Chen, Z., Chen, G., & Hong, Y. (2022). Defense for Advanced Persistent Threat with Inadvertent or Malicious Insider Threats. *Institute of Electrical and Electronics Engineers*, 1-12.

Chernikova, A., Gozzi, N., Boboila, S., Angadi, P., Loughner, J., Wilden, M., . . . Oprea, A. (2022). Cyber Network Resilience against Self-Propagating Malware Attacks. *Computer Security – ESORICS 2022*, 1-20.

Clarke, R. (2002). Defining cyber terrorism. *The Journal of Strategic Information Systems*, 171-180.

Colarik, A. (2006). *Cyber Terrorism: Political and Economic Implications.* Pennsylvania: International Academic Publisher.

Collin, B. (2008). *Cyber terrorism: Understanding, Assessment, and Response.* . Boca Raton: Auerbach Publications.

Conway, M. (2003). Cyberterrorism: The Story So Far. *Journal of Information Warfare*, 33–42.

Council of Europe. (2004). *Convention on Cybercrime.* Budapest : Council of Europe.

Csonka, P. (2006). The council of europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit pénal*, 473-501.

Cvitić, I., Peraković, D., Gupta, B., & Choo, K. (2021). Boosting-Based DDoS Detection in Internet of Things Systems. *IEEE Internet of Things Journal*, 2109-2123.

Denning, D. E. (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", Global Problem Solving Information Technology and Tools. *Internet and International Systems: Information Technology and American Foreign Policy Decision-making Workshop* (pp. 1-31). San Francisco: Nautilus Institute.

Dhillon, G. (2015). *What to do before and after a cybersecurity breach?* Washington D.C.: Kogod Cybersecurity Governance Center.

Dick, R. (2002). *CIO Magazine, FBI, and Secret Service Announce New Cyberthreat Reporting Guidelines for Businesses.* Washington, D.C.: FBI National Press Office.

Dogrul, M., Aslan, A., & Celik, E. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. *3rd International Conference on Cyber Conflict* (pp. 29-43). Tallinn: CCD COE Publications.

Dowdall, J. (2017). Understanding cyber terrorism: A comprehensive history. *Journal of Strategic Security*, 1-22.

Droogan, J., & Waldek, L. (2018). (). Should we be afraid of cyber-terrorism? *International Journal of Electronic Security and Digital Forensics*, 242-254.

Emery, N. E. (2005). The Myth of Cyberterrorism. *Journal of Information Warfare*, 80-89.

ENISA. (2017). *Cyber Security Culture in organisations.* Heraklion: European Union Agency for Network and Information Security (ENISA) .

Eurojust. (2016). *Cybercrime Judicial Monitor.* Hague: European Union Agency for Criminal Justice Cooperation.

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. *16th international conference on world wide web* (pp. 649–656). New York: ACM Press.

Gable, K. A. (2010). Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law*, 57-118.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, 28-38.

Garnett, H. A., & James, T. (2020). Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. *Election Law Journal: Rules, Politics, and Policy*, 111-126.

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, 1-10.

Ghulam, F., Irfan, M., & Hassan, F. (2022). A study of ransomware attacks on windows platform. *i-manager's Journal on Computer Science*, 21-27.

Goldman, Z. K., & McCoy, D. (2016). Deterring Financially Motivated Cybercrime. *Journal of National security law & policy*, 595-619.

Gross, M. L., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, 49–58.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, , W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, 817–885.

He, Q., Wang, C., Cui, G., Li, B., Zhou, R., Zhou, Q., . . . Yang, Y. (2022). A Game-Theoretical Approach for Mitigating Edge DDoS Attack. *IEEE Transactions on Dependable and Secure Computing*, 2333-2348.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. . *Advanced Sciences and Technologies for Security Applications*, 71- 87.

Holt, T. J., Burruss, G., & Bossler, A. (2015). *Policing Cybercrime and Cyberterror.* Michigan: Department of Criminal Justice and Criminology Faculty Publications.

Hower, S., & Uradnik, K. (2011). *Cyberterrorism (1st έκδοση).* Santa Barbara: CA: Greenwood.

IAEA. (2011). *Computer Security at Nuclear Facilities* . Vienna: International Atomic Energy Agency.

Joshi, A. (2000). The scourge of cyber-terrorism. . *Strategic Analysis*, 827 - 831.

Kaljurand, M. (2016). *United Nations Group of Governmental Experts: The Estonian Perspective.* Tallinn : NATO CCD COE Publications.

Kertysova, K., Frinking, E., van den Dool, K., Maričić, A., & Bhattacharyya, K. (2018). *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.* Hague: European Economic and Social Committee.

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors (Basel)*, 1-19.

Kshetri, N. (2003). Cyber Terrorism: Political and Economic Implications. *Information Systems Management*, 47-56.

Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Quarterly*, 1057–1079.

Kshetri, N. (2017). Cyber terrorism and cyber warfare: An overview of their past, present and future. *International Journal of Information Management*, 121-131.

Kuhn, K., Bicakci, S., & Shaikh, S. (2021). COVID-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs volume*, 193–214.

Lella, I., Tsekmezoglou, E., Naydenov, R., & Malatras, A. (2022). *ENISA Threat Landscape for Ransomware Attacks.* Athens: European Union Agency for Cybersecurity.

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, 1-12.

Li, Y., & Qinghui , L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 8176-8186.

Ma, X. (2020). Research on the Governance of Cyber Terrorism under the Construction of National Trust. *The Modern Law Review* , 35-44.

Minchev, Z. (2015). Human Factor Dual Role in Modern Cyberspace Social Engineering. . *Terrorist Use of Cyberspace and Cyber Terrorism.*, 1-20.

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. *Cryptology and Information Security Series*, 163 - 181.

Nugroho, A., & Chandrawulan , A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. *Nature Public Health Emergency Collection*, 1-20.

Peters, G. (2022). *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns.* Washington, DC: Senate Homeland Security and Governmental Affairs Committee.

Pool, P. (2013). War of the Cyber World: The Law of Cyber Warfare. *The International Lawyer*, 299–323.

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* Brussels: European Parliamentary Research Service.

Seh, A., Zarour , M., Alenezi, M., Sarkar , A., Agrawal , A., Kumar, R., & Khan , R. (2020). *Healthcare Data Breaches: Insights and Implications.* Basel: Healthcare.

Siedersberger, C., & Plattner, M. (2015). The history of cyber terrorism. *Springer*, 19-30.

Sullivan, A., & Montasari, R. (2022). The Use of the Internet and the Internet of Things in Modern Terrorism and Violent Extremism. *Privacy, Security And Forensics in The Internet of Things (IoT)*, 151–165.

Taylor, R. W., Fritsch, E., Liederbach, J., Saylor, M., & Tafoya, W. (2019). *Cybercrime and Cyber Terrorism.* New York: Pearson Education.

United Nations. (2018). *Introduction to International terrorism* . Vienna: United Nations.

Verizon. (2019). *2019 Data Breach Investigations Report, Results & Analysis.* New York: Verizon Enterprise.

Vernacchia, S. (2018). *A practical method of identifying cyberattacks.* Middle East: Price waterhouse Coopers.

Walker, C. (2006). Cyber-Terrorism: Legal Principle and Law in the United Kingdom. *Dickinson Law Review*, 625-665.

Watney, M. (2022). Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective. *21st European Conference on Cyber Warfare and Security* (pp. 319-327). Johannesburg: University of Johannesburg.

Weimann, G. (2004). *The theatre of terror: Mass media and international terrorism.* London: Longman.

Weimann, G. (2004). Cyberterrorism How Real Is the Threat? *Institute of Peace*, 1-12.

Yamamoto, M. (2015). *Terrorism Against Democracy.* Washington D.C.: Center for International and Security Studies at Maryland .

Yunos, Z., & Sulaman, S. (2017). Understanding Cyber Terrorism from Motivational Perspectives. *Journal of Information Warfare*, 1–13.

Zafri, F. (2022). Ransomware Attacks in History of Cyber World. . *International Journal for Research in Applied Science and Engineering Technology.*, 39-43.

Zampati, M. G. (2011). *Cybersecurity and Energy. The Case Study of Stuxnet.* Piraeus: University of Piraeus.

Βαγιάτη, Ε. (2014). *Ηλεκτρονικό έγκλημα και προστασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση.* Κομοτηνή: Δημοκρίτειο Πανεπιστήμιο Θράκης. Σχολή Νομικής.

ΣΝ_κυβερνοασφάλειας (2024). *ΣΧΕΔΙΟ ΝΟΜΟΥ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ με τίτλο «Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις του*

Υπουργείου Ψηφιακής Διακυβέρνησης», http://www.opengov.gr/digitalandbrief/wp-content/uploads/downloads/2024/01/%CE%A3%CE%9D_%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82_02012024_2115.pdf

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4620 Τεύχος Α' 96/11.06.2019