ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

"ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑ ΚΑΙ ΨΗΦΙΑΚΉ ΕΠΟΧΉ ΣΤΗ ΔΗΜΌΣΙΑ ΔΙΟΊΚΗΣΗ ΚΑΙ ΥΓΕΙΑ"

Επιβλέπων Καθηγητής

Δρ. Μάριος Π. Ευθυμιόπουλος

Ιούλιος 2022

ΑΡΓΥΡΗ ΒΛΑΣΣΟΠΟΥΛΟΥ

“ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΣΤΡΑΤΗΓΙΚΗ

ΚΑΙ ΑΣΦΑΛΕΙΑ”

“ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑ ΚΑΙ ΨΗΦΙΑΚΉ ΕΠΟΧΉ ΣΤΗ ΔΗΜΌΣΙΑ ΔΙΟΊΚΗΣΗ”

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στις “Διεθνείς Σχέσεις, Στρατηγική και Ασφάλεια”

Επιβλέπων Καθηγητής

Δρ. Μάριος Π. Ευθυμιόπουλος

Ιούλιος 2022

ΑΡΓΥΡΗ ΒΛΑΣΣΟΠΟΥΛΟΥ

Πνευματικά δικαιώματα

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΕΛΙΔΑ ΕΓΚΥΡΟΤΗΤΑΣ

Ονοματεπώνυμο: Αργυρή Βλασσοπούλου

Τίτλος Μεταπτυχιακής Διατριβής: "Κυβερνοασφάλεια και ψηφιακή εποχή στη δημόσια υγεία"

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις 9 Ιουνίου 2022 από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή: Δρ. Μάριος Π. Ευθυμιόπουλος

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)

Μέλος Εξεταστικής Επιτροπής: Δρ. Μερσίλια Αναστασιάδου

Μέλος Εξεταστικής Επιτροπής: Δρ. Σάββας Α. Χατζηχριστοφής

Ή ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Εγώ η Αργυρή Βλασσοπούλου γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «. », αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Η Δηλούσα

Αργυρή Βλασσοπούλου

ΕΥΧΑΡΙΣΤΙΕΣ

Ο πρόλογος, αντίθετα με την εισαγωγή που ακολουθεί παρακάτω, δεν αποτελεί συστατικό στοιχείο της κυρίως μελέτης, δεν έχει δηλαδή σχέση με τα θέματα και προβλήματα που ερευνώνται.

Η ολοκλήρωση της Μεταπτυχιακής αυτής εργασίας θα ήταν αδύνατη χωρίς την πολύτιμη βοήθεια του Υπεύθυνου Καθηγητή μου Μάριου-Παναγιώτη Ευθυμιόπουλου του Νεάπολις Πανεπιστημίου Πάφου. Του εκφράζω ένα μεγάλο ευχαριστώ για όλη την βοήθεια που μου προσέφερε. Επίσης ένα μεγάλο ευχαριστώ χρωστάω στην οικογένεια μου η οποία υπήρξε ένα ανεκτίμητο στήριγμα για εμένα και στην οποία οφείλω όλη τη διαδρομή των σπουδών μου μέχρι σήμερα. Τέλος ένα μεγάλο ευχαριστώ στο φιλικό μου περιβάλλον για την έμπρακτη υποστήριξη σε ένα τόσο απαιτητικό εγχείρημα.

ΠΕΡΙΛΗΨΗ

Στην παρούσα διατριβή θα πραγματευτούμε έννοιες όπως δημόσια διοίκηση, κυβερνοασφάλεια, κυβερνοεπίθεση, κυβερνοπολιτική και κυβερνοάμυνα. Η διαχείριση της συνεχούς και ραγδαίας αύξησης των επιθέσεων στον κυβερνοχώρο αποτελεί μια μεγάλη πρόκληση για όλα τα κράτη. Αδιαμφισβήτητα ο κυβερνοχώρος έχει εξελιχθεί σε πεδίο μάχης αυξανόμενων και συνεχών απειλών. Κάποιες συχνές μορφές απειλών αποτελούν τα κακόβουλα λογισμικά, υποκλοπή κωδικών, ηλεκτρονικό ψάρεμα και αποστολή ανεπιθύμητων μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου αλλά και πολλές άλλες μορφές που θα συναντήσουμε και θα αναλύσουμε κατά την ανάλυση. Βασικό μέλημα αποτελεί πλέον το γεγονός πως κάθε κράτος προσδοκά να περιορίσει με την χρήση εξελιγμένης τεχνολογίας τις επιθέσεις στον κυβερνοχώρο, καταβάλλοντας προσπάθεια για την θέσπιση αμυντικής συμπεριφοράς απέναντι στο σύστημα με την χρήση νέων τεχνολογιών. Ωστόσο οι δράστες καταφέρνουν σε σημαντικό βαθμό να διεισδύσουν τόσο σε δίκτυα όσο και σε συστήματα. Στην παρούσα διατριβή το σύστημα το οποίο θα μας απασχολήσει ερευνητικά αναφέρεται στην ηλεκτρονική πλατφόρμα gov.g και πιο συγκεκριμένα ο κλάδος της δημόσιας υγείας και η μετεξέλιξη του στην ψηφιακή μορφή.

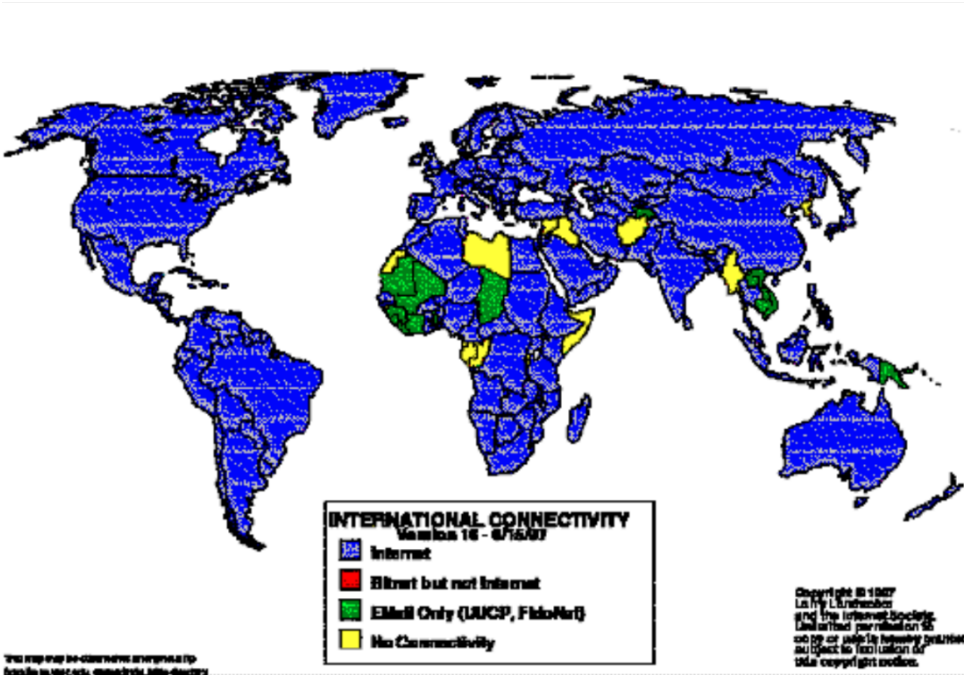
Στην συγκεκριμένη διατριβή θα χρησιμοποιηθούν στατιστικά στοιχεία από επικυρωμένες πηγές εγκυρότητας όπως εθνικές στατιστικές υπηρεσίες και ακαδημαϊκά ιδρύματα. Σημαντικός παράγοντας γνώσεων και άξιο αναφοράς στην προκειμένη διατριβή θεωρείται η ιστορική αναδρομή του Ίντερνετ με άμεσο στόχο και σκοπό την κατανόηση της εξέλιξης της πολιτικής του κυβερνοχώρου σε κρατικό επίπεδο.

Το σημερινό Ίντερνετ αποτελεί αδιαπραγμάτευτα μια μετεξέλιξη του arpanet ενός δικτύου που ξεκίνησε να εφαρμόζεται αρχικά σε πειραματικό στάδιο για πολεμική χρήση στις ΗΠΑ ην δεκαετία 1960. Οι ερευνητές στα πανεπιστήμια των ΗΠΑ ξεκινούν να πειραματίζονται με την διασύνδεση των απομακρυσμένων υπολογιστών μεταξύ τους με απώτερο σκοπό χρήση όπλων σε διαδικτυακό φάσμα εφαρμογής. Εν ολίγοις το δίκτυο arpanet όπου βασική του πηγή θεωρείται το πρόγραμμα ARPA (Advanced Research Project Agency) κατασκευής του 1969 από το Υπουργείο Εθνικής Αμύνης των ΗΠΑ. Βασικός σκοπός της δημιουργίας αυτού του προγράμματος θεωρήθηκε η σύνδεση πληροφοριών του Υπουργείου Εθνικής Αμύνης σε συνεργασία με στρατιωτικούς ερευνητικούς οργανισμούς όπου θα αποτελούσε πείραμα και μέρος ερευνητικής μελέτης για την αποτελεσματικότητα και την αξιοπιστία των λειτουργιών του στον τομέα των δικτύων. Εν συνεχεία άμεσος στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνθεσή του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης. Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

Στις αρχές της νέας δεκαετίας και πιο συγκεκριμένα το 1973 ξεκινά διεξαγωγή ενός νέου πειράματος που ονομάζεται Internetting Project (Πρόγραμμα Δικτύωσης) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Αποτέλεσμα ενός τέτοιου πειράματος αποτελεί η σύσταση του προγράμματος Internetting Project όπου έχει βασικό σκοπό να επιλύσει τους διάφορους τρόπους που χρησιμοποιεί το κάθε δίκτυο για να διακινεί τα δεδομένα του. Η λύση του προβλήματος έρχεται με την επαναστατική ανακάλυψη του IP (Internet Protocol) όπου πλέον διαφορετικά δίκτυα χρησιμοποιούν κοινό πρωτόκολλο με σκοπό την σύνδεση σε ένα ενιαίο δίκτυο.

Καθώς λοιπόν διανύσαμε μια σημαντική δεκαετία για την εξέλιξη του ίντερνετ, το 1980 φέρνει στο προσκήνιο την χρήση του ίντερνετ για ακαδημαικού λόγους. Εκατοντάδες Πανεπιστημιακά Ιδρύματα συνδέονται στο arpanet με απότελεσμα το φορτίο να γίνει αβάστακτο και το δίκτυο να χωριστεί σε δυο μέρη στο milnet (δίκτυο για στρατιωτικές επιχειρήσεις) και στο arpanet (δίκτυο αποκλειστικά για την ακαδημαϊκή κοινότητα) όπως χαρακτηριστικά αναφέρει στο έργο του *Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet* ο Michael Hauben, η ακαδημαική χρήση του arpanet γίνεται με στόχο την έρευνα και την εξέλιξη των δικτύων αφουγγραζόμενοι την αναγκη της παγκόσμιας και εμπορικής χρήσης του ιντερνετ παγοσμίως. Όπως πολύ σωστά είχε προβλέψει ο Raphael Cohen-Almagor (University of Hull, UK), η χρήση του arpanet θα εξαφανιστεί και την θέση του θα πάρει ένα ισχυρότερο και πιο εξελιγμένο δίκτυο αφότου θα έχει την δυνατότητα να συνδέει πολλά κέντρα δικτύων ταυτόχρονα. Επομένως το arpanet κατά την περίοδο 1990 καταργείται και την θέση του αντικαθιστά το Internet στο οποίο πλέον συνδέονται ταυτόχρονα πανεπιστημιακά ιδρύματα από την Γαλλία, Ιταλία, Καναδά, Σουηδία, Γερμανία κ.α.).

Η Ελλάδα εντάσσεται στο δίκτυο NSFNET δηλαδή ενός δικτύου που χρησιμοποιεί το συνδυασμό πρωτοκόλλων TCP/IP προκειμένου να συνδέει επιτυχώς και με γρήγορες ταχύτητες πολλά δίκτυα μαζί. Παράλληλα με αυτή την καινοτομία στο εργοστάσιο της Ελβετίας CERN πραγματοποιείται η εφεύρεση του World Wide Web (WWW) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Γίνεται αναφορά σε ένα σύνολο πληροφορίων που είναι αποθηκευμένες σε χιλιάδες υπολογιστές σε μορφή πολυμέσων παρουσιασμένες σε ιστοσελίδες. Σύμφωνα πάντα με αυτή την εξέλιξη το Ίντερνετ είναι σε θέση να εξυπηρετήσει εταιρικά δίκτυα και η μορφή του πλέον να είναι παγκόσμια και προσβάσιμη σε όλους. Επομένως οποιασδήποτε διαθέτει υπολογιστή και μόντεμ έχει πρόσβαση στο Ίντερνετ. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα. Επιπροσθέτως στον χάρτη που επισυνάπτεται παρακάτω μπορούμε να διαπιστώσουμε σε παγκόσμια κλίμακα την εξάπλωση του Ίντερνετ μέχρι τις 15/6/1997 όπου το Ίντερνετ είναι διαδεδομένο και για εμπορική χρήση.



Βλ. Φωτογραφία Cambridge Press 1998.

(Η κατάσταση σύνδεσης ανά χώρα, όπως είχε στις 15/6/1997. Με μωβ εμφανίζονται οι χώρες με πλήρη σύνδεση στο Internet, με πράσινο οι χώρες που διαθέτουν πρόσβαση μόνον στην υπηρεσία E-mail και με κίτρινο οι χώρες που δεν διαθέτουν κανένα είδος σύνδεσης.)

Με την πάροδο των χρόνων το Ίντερνετ γίνεται προσβάσιμο σε όλες τις περιοχές του κόσμου μετατρέποντας μάλιστα αναγκαιότητα και τρόπο ζωής ένα εγχείρημα που έμοιαζε απρόσιτο προς εμπορική και δημόσια χρήση.

Λέξεις κλειδιά : δημόσια διοίκηση, κυβερνοασφάλεια, κυβερνοεπίθεση, δημόσια υγεία

ΕΙΣΑΓΩΓΙΚΟ ΜΕΡΟΣ

1. Ορισμός Δημόσιας Διοίκησης

Η δημόσια διοίκηση αποτελεί ένα από τα πιο βασικά και σημαντικά μέρη της διαδικασίας διακυβέρνησης ενός λαού. Η δημόσια διοίκηση συμβάλει σε ένα κρατικό σύνολο υποθέσεων που συντείνει στην κοινή κρατική προσπάθεια για την επίτευξη της προετοιμασίας, της κατάρτισης, εφαρμογής και αξιολόγησης των σχεδίων δράσης και δημόσιας πολιτικής, συνυπολογιζόμενου και του σχετικού νομοθετικού πλαισίου. Ο όρος Διοίκηση αναφέρεται ουσιαστικά στην συνολική διενέργεια τόσο των νομικών πράξεων όσο και των υλικών ενεργειών με σκοπό την επιδίωξη και την μεταγενέστερα της τέλεση του τελικού στόχου. Εμβαθύνοντας στην έννοια της Δημόσιας Διοίκησης κατανοούμε πως συνδέεται αυτόματα με την διοίκηση του κράτους, των νομικών προσώπων δημοσίου δικαίου και λοιπών δημόσιων οργανισμών. Άξιο λόγου θεωρείται το γεγονός πως η δημόσια διοίκηση είναι μια οργανική έννοια, όπου σε αυτή εμπεριέχονται Δημόσιες Υπηρεσίες εκτός από το Κοινοβούλιο, τις Υπηρεσίες της Βουλής και τέλος τα Δικαστήρια. Η Δημόσια Διοίκηση εν γένει λογίζεται το σύνολο των νομικών προσώπων όπου τα οργανωμένα διοικητικά όργανα ασκούν εξουσία. Είναι σαφές πως κατά το Σύνταγμα ορίζεται η δημόσια διοίκηση ασκώντας κατά νόμο την εκτελεστική λειτουργία του κρατικού μηχανισμού. Λαμβάνοντας υπόψιν την λειτουργική έννοια της Δημόσιας Διοίκησης κατανοούμε πως ο βασικός της ρόλος είναι η διεξαγωγή υποθέσεων του κοινωνικού συνόλου, λαμβάνοντας ουσιαστικά το ρόλο της διοικητικής λειτουργείας κατ' εφαρμογή των κανόνων δικαίου. Επιπροσθέτως η Δημόσια Διοίκηση συνδέεται άρρηκτα με την εξυπηρέτηση, φροντίδα και προώθηση δημόσιων υποθέσεων. Για την τέλεση και την επίτευξη αυτών των στόχων βασίζεται στους κανόνες Δημόσιου Δικαίου.

1.1 Ίδρυση, σκοπός και στο στόχοι του Υπουργείου Ψηφιακής Διακυβέρνησης

Αναγκαιότητα για την σύσταση του Υπουργείου Ψηφιακής διακυβέρνησης στάθηκαν οι εξελίξεις της πανδημίας Covid-19 κατά την διάρκεια του έτους 2019. Πρόκειται για ένα εμβληματικό έργο και συγχρόνως μιας αντιπροσω-πευτικής φιλοσοφίας του δημόσιου ελληνικού κράτους που ανήκει στον 21ο αιώνα. Σε διάστημα δύο χρόνων το ελληνικό κράτος κατάφερε να ψηφιοποιήσει την γραφειοκρατία του και να διευκολύνει τον Έλληνα πολίτη με μια απλή επίσκεψη στην ιστοσελίδα του gov.gr να εξυπηρετηθεί εξ αποστάσεως, εξαλείφοντας την φυσική του παρουσία από τις δημόσιες δομές. Άξιο λόγου θεωρείται το γεγονός πως με την έναρξη της πλατφόρμας υπήρχαν διαθέσιμες 501 υπηρεσίες και έπειτα από δύο χρόνια λειτουργείας της οι διαθέσιμες υπηρεσίες ανήκουν στις 1368 όπου προστίθενται όλο και πιο συχνά νέες υπηρεσίες. Το Υπουργείο Ψηφιακής Διακυβέρνησης μέχρι στιγμής έχει καταφέρει να συγκεντρώσει σε μία πλατφόρμα σχεδόν όλες τις κρίσιμες δομές πληροφορικής και τηλεπικοινωνίων, που σχετίζονται με την άμεση παροχή πληροφοριών μέσω των ηλεκτρονικών υπηρεσιών προς τους πολίτες και προς τον ευρύτερο ψηφιακό μετασχηματισμό της χώρας. Αρχικός στόχος ήταν η δημιουργία μιας ενιαίας δομής σε επιχειρησιακό επίπεδο που θα έβαζε φρένο στον κατακερματισμό μονάδων και συστημάτων που επηρέαζε τόσο την ποιότητα και το κόστος των δημόσιων υπηρεσιών. Επόμενος στόχος του Υπουργείου Ψηφιακής Διακυβέρνησης φαίνεται να είναι το τέλος της εποχής της απλής ψηφιοποίησης της γραφειοκρατίας αλλά η μετατροπή οποιασδήποτε διεργασίας σε ψηφιακή μορφή.

1.2 Αρχές καλής διοίκησης στην ψηφιακή διακυβέρνηση

Η ίδρυση του Υπουργείου Ψηφιακής Διακυβέρνησης που συστάθηκε κατά την χρονική περίοδο του 2019 θεωρείται κοιτίδα του ελληνικού κρατικού μηχανισμού αφότου στόχευε αρχικά στο να μετατρέψει την έγχαρτη μορφή γραφειοκρατικής υποστήριξης σε ψηφιακή. Με την χρήση ενός laptop ή ενός smartphone

και την σύνδεση στο ίντερνετ γίνεται άμεση η επίσκεψη σε διάφορες υπηρεσίες του ελληνικού κράτους, φέρνοντας σε υψηλά ποσοστά επισκεψιμότητας την ιστοσελίδα gov.gr. Το Υπουργείο Ψηφιακής Διακυβέρνησης το οποίο δημιουργήθηκε με σκοπό της προώθηση του ψηφιακού κόσμου για τις ανάγκες της πανδημίας με στόχο την προστασία των πολιτών από τον επικείμενο ιό έθεσε νέα θεμέλια και αρχές για την άμεση και αποτελεσματική διοίκηση του. Η καινοτομία αναφορικά με την ψηφιοποιηση των κρατικών υπηρεσιών έφερε μεγάλη αναστάτωση στον ελληνικό λαό, ο οποίος αναγκάστηκε σε μικρό χρονικό διάστημα με αφορμή τις δυσκολίες της πανδημίας να προσαρμοστεί στα νέα δεδομένα της ψηφιακής εποχής.

Σε συνέντευξή του ο Υπουργός Ψηφιακής Διακυβέρνησης Κυριάκος Πιερακάκης ανέλυσε το πρόγραμμα του Υπουργείου αλλά και τις αλλαγές που έχουν λάβει χώρα στις πλατφόρμα gov.gr. Πρώτο βήμα του Υπουργείου φαίνεται να απασχολούσε την ψηφιοποιήση των κρατικών δημόσιων δομών και των εγγράφων όπου θα ήταν ενσωματωμένα σε ένα σύστημα πληροφοριών. Άξιο λόγου θεωρείται το γεγονός πως η γραφειοκρατία έμεινε στάσιμη και το ίδιο απαιτητική με πριν, μόνο που από τον Μάρτιο του 2019 ήταν προσβάσιμη και σε ψηφιακή μορφή. Άξιο λόγου θεωρείται το γεγονός πως για την σωστή λειτουργεία και την εξέλιξη του Υπουργείου Ψηφιακής Διακυβέρνησης τέθηκαν επί τάπιτος κάποιες αρχές με απόλυτο σκοπό την καλή διοίκηση στον τομέα. Όπως μπορούμε να δούμε παρακάτω στο Βήμα της Ελληνικής Βουλής ο Υπουργός Κυριάκος Πιερακκάκης απαρίθμησε τις εξής αρχές :

- Η εξυπηρέτηση του συμφέροντος των πολιτών και όχι των ιδίων συμφερόντων των προσώπων, αλλά και η ανιδιοτελής άσκηση της δημόσιας υπηρεσίας .
- Η τήρηση των προϋποθέσεων της χρηστής και έντιμης διοίκησης, αλλά και η εναρμόνιση με το αίσθημα δικαίου που επικρατεί στην κοινωνία, αποτελεί όρο αξιοπιστίας και εμπιστοσύνης των πολιτών προς αυτήν. Επίσης, η αποφυγή της διαφθοράς, του χρηματισμού και της ιδιοτέλειας μπορεί να ικανοποιήσει το «δικαίωμα χρηστής διοίκησης» των πολιτών, τόσο σε εθνικό, όσο και σε ευρωπαϊκό επίπεδο.
- Η ταχύτητα, η συνέπεια, η συνοχή της διοίκησης αποτελούν καλές πρακτικές για την εξυπηρέτηση του πολίτη.
- Ο σεβασμός στα δικαιώματα και η εμπιστοσύνη του πολίτη προς το Κράτος και τις δημόσιες αρχές, που δεν πρέπει να διαψεύδουν τις προσδοκίες που οι ίδιες προξένησαν.
- Η αποτελεσματικότητα, η αποδοτικότητα της ποιότητας και ενότητας στη δράση της Διοίκησης, ώστε να δρα με ταχύτητα, οικονομία και τρόπο συνεπή προς την ενότητα και τη συνοχή του κράτους.
- Η αρχή της συνέχειας και σταθερότητας της διαρκούς λειτουργίας στη δράση της δημόσιας διοίκησης.
- Η ίση μεταχείριση των πολιτών και η αμερόληπτη δράση της διοίκησης που πρέπει να τους αντιμετωπίζει με ουδετερότητα και ισότητα.
- Η διαφανής, φανερή, ήπια δράση της διοίκησης, που πρέπει να μην είναι υπέρμετρα αυστηρή απέναντι στον πολίτη, τον οποίον πρέπει να σέβεται, να προστατεύει και να διευκολύνει την εξυπηρέτηση του (Ράικος, 2006).

Για εκατοντάδες πολίτες, οι αρχές που θέτει το Υπουργείο Ψηφιακής Διακυβέρνησης θεωρούνται απαραίτητες και αδιαμφισβήτητες ως προς την ομαλή λειτουργεία του με σκοπό την άμεση και γρήγορη εξυπηρέτηση των πολιτών. Απαραίτητο συστατικό για την ομαλή λειτουργία της ψηφιακής εποχής στο σύστημα υπηρεσιών είναι τόσο η εξοικείωση των πολίτων με την εφαρμοσμένη χρήση του όσο όμως και η ειδίκευση από τους δημόσιους υπαλλήλους σχετικά με τον χειρισμό του συστήματος αλλά και την στοχευμένη καθοδήγηση του κοινού για την κατανόηση και την άμεση εξυπηρέτηση του από την ψηφιακή πλατφόρμα.

1.3 Σημασιολογία Ψηφιακής Διακυβέρνησης και Κυβερνοασφάλειας σήμερα

Με βάσει την θεωριτική προσέγγιση του ερευνητή Charles Leslie Stevenson (1908–1979) δεν υπάρχει η δυνατότητα ύπαρξης ενός συγκεκριμένου ορισμού αναφορικά με την κυβερνοασφάλεια. Σχετικά με τον όρο φαίνεται πως υπάρχει μία ευρεία χρήση του αλλά συγχρονως λόγω της έλλειψης βιβλιογραφικών αναφορών φέρει μεγάλη σύγχυση στον ακαδημαϊκό χώρο αφότου τις περισσότερες φορές οι ορισμοί που προκύπτουν αποτελούν συνονθύλευμα υποκειμενικών και μη ενημερωτικών στοιχείων σε συνδυασμό με την έλλειψη βιβλιογραφίας. Οι *Craigen, D. , Diakun-Thibault, N. Purse,* αναφέρουν στο έργο τους *(R. 2014. Defining Cybersecurity . Ανασκόπηση Διαχείρισης Τεχνολογικής Καινοτομίας , 4(10): 13-21.)* πως «Μια επιστήμη της κυβερνοασφάλειας προσφέρει πολλές ευκαιρίες για πρόοδο που βασίζεται σε μια διεπιστημονική προσέγγιση, επειδή, σε τελική ανάλυση, η κυβερνοασφάλεια αφορά ουσιαστικά μια αντίπαλη δέσμευση. Οι άνθρωποι πρέπει να υπερασπιστούν μηχανές που δέχονται επίθεση από άλλους ανθρώπους που χρησιμοποιούν μηχανές. Έτσι, εκτός από τα κρίσιμα παραδοσιακά πεδία της επιστήμης των υπολογιστών, της ηλεκτρολογικής μηχανικής και των μαθηματικών, χρειάζονται προοπτικές από άλλους τομείς». Αναφέρει επίσης χαρακτηριστικά πως ο ορισμός με τον οποίο θα μπορούσε να υπάρχει σχετική συσχέτιση είναι η ασφάλεια με την μόνη ειδοποιό διαφορά πως το συνθετικό πρόθεμα "κυβερνό" σχετίζεται με την προστασία των δικτύων επικοινωνιών και με την εικονική πραγματικότητα *(Oxford, 2014)*. Παρακάτω έχουμε την δυνατότητα να μελετήσουμε έναν πίνακα από το Πανεπιστήμιο της Οξφόρδης που μας διαθέτει όλους τους ακαδημαϊκούς ορισμούς σχετικά με την κυβερνοασφάλεια.

A	**Ορισμοί Κυβερνοασφάλειας Ερευνητικής Φύσεως**
1	"Η κυβερνοασφάλεια είναι η προστασία πληροφοριών/δεδομένων, περιουσιακών στοιχείων, υπηρεσιών και συστημάτων αξίας για τη μείωση της πιθανότητας απώλειας, ζημίας/διαφθοράς, συμβιβασμού ή κακής χρήσης σε επίπεδο ανάλογο με την αξία που έχει εκχωρηθεί."
2	"Η κυβερνοασφάλεια είναι μια συλλογή διαδικασιών αλληλεπίδρασης που αποσκοπούν στην προστασία του κυβερνοχώρου και των συστημάτων που υποστηρίζονται από τον κυβερνοχώρο (συλλογικά πόροι) από σκόπιμες ενέργειες που έχουν σχεδιαστεί για να μη ευθυγραμμίσουν τα πραγματικά δικαιώματα ιδιοκτησίας πόρων από τα αντιληπτά δικαιώματα ιδιοκτησίας του ιδιοκτήτη του πόρου."
3	«Η κυβερνοασφάλεια είναι μια συλλογή διαδικασιών αλληλεπίδρασης που αποσκοπούν να κάνουν τον κυβερνοχώρο ασφαλή και ασφαλή».
4	«Η κυβερνοασφάλεια είναι ένας τομέας αφιερωμένος στη μελέτη και πρακτική της προστασίας συστημάτων ή ψηφιακών περιουσιακών στοιχείων από κάθε ενέργεια που λαμβάνεται για την επιβολή εξουσιοδότησης σε αυτά τα συστήματα ή ψηφιακά στοιχεία που δεν ευθυγραμμίζονται με τα δικαιώματα ιδιοκτησίας της εγκατάστασης πόρων όπως κατανοεί ο ιδιοκτήτης της. "
5	"Η κυβερνοασφάλεια είναι η κατάσταση κατά την οποία η ισχύς για την εκτέλεση υπολογιστών (sensu lato) και επί των πληροφοριών στον έλεγχο των υπολογιστών είναι εκεί που θα έπρεπε."

Στην συνέχεια με βάσει τους ορισμούς που έχουμε στην διάθεσή μας, ο αναλυτής Διεθνών Σχέσεων Cooper το 2013 πραγματοποιεί μια κριτική η οποία συνοψίζει τα τρωτα σημεία καθενός από αυτούς.

A	**Κριτική σε κάθε ορισμό ξεχωριστά**

1	« Κυρίως, η ανατροφοδότηση πρότεινε ότι η συμπερίληψη της αξίας εισήγαγε τις ανθρώπινες έννοιες που σχετίζονται με την ασφάλεια, αλλά ότι ο ορισμός ήταν πολύ δεσμευτικός και αντιμετώπιζε το πρόβλημα της περιοριστικής "καταγραφής" του τι προστατεύεται.”
2	“Αυτός ο ορισμός εισήγαγε το αναδυόμενο κυβερνοφυσικό περιβάλλον και συμπεριέλαβε τη σημαντική έννοια του ελέγχου των δικαιωμάτων ιδιοκτησίας. Ωστόσο, η εστίαση του ορισμού στις «ανθρώπινες σκόπιμες ενέργειες» θεωρήθηκε υπερβολικά περιοριστική.”
3	“Συγκεκριμένα, με σκοπό να είναι ευρύτερος από τον ορισμό των σπόρων, αυτός ο ορισμός εισήγαγε περισσότερα προβλήματα από όσα έλυνε, επειδή ήταν αδικαιολόγητα ευρύς και εισήγαγε την αμφισβητούμενη έννοια της ασφάλειας με την ασφάλεια.”
4	“Σε αυτόν τον ορισμό εισήχθησαν οι έννοιες των δικαιωμάτων ιδιοκτησίας και του ελέγχου. Ωστόσο, υπήρξαν ανησυχίες σχετικά με τις πιθανές συνέπειες της "μέτρας που ελήφθησαν" που σημαίνει περιορισμό της κυβερνοασφάλειας στους ανθρώπινους παράγοντες. Επίσης, υπήρξαν ανησυχίες σχετικά με τους όρους, οι οποίοι επέβαλαν περιορισμούς στο πεδίο εφαρμογής του ορισμού, όπως «μελέτη» και «πρακτική», τοποθετώντας έτσι τα ζητήματα σε μεγάλο βαθμό στον ακαδημαϊκό τομέα.”
5	“Αυτός ο ορισμός ενίσχυσε τις έννοιες του ελέγχου των πληροφοριών και των συστημάτων. Η κύρια κριτική ήταν ο ορισμός της κυβερνοασφάλειας ως κράτος.”

Ο *Craigen* επανέρχεται στο προσκήνιο των Διεθνών Σχέσων και το έργο του ***Craigen, D. , Diakun-Thibault, N. , & Purse, R. 2014. Defining Cybersecurity .*** *Ανασκόπηση Διαχείρισης Τεχνολογικής* ***Καινοτομίας*** δίνοντας έναν νέο ορισμό περί κυβερνοασφάλειας τον οποίο στηρίζει σε θεμελιώδης κανόνες των διεθνών σχέσεων και του διεθνούς δικαίου. Ο νέος ορισμός είναι ο εξής:

“Η κυβερνοασφάλεια είναι η οργάνωση και η συλλογή πόρων, διαδικασιών και δομών που χρησιμοποιούνται για την προστασία του κυβερνοχώρου και των συστημάτων που υποστηρίζουν τον κυβερνοχώρο από περιστατικά που δεν ευθυγραμμίζονται **de jure** ***με τα*** **de facto** ***δικαιώματα ιδιοκτησίας.”***

Ο ορισμός αυτός βασίζεται:

- Στην οργάνωση και συλλογή πόρων δηλαδή στην θεμελιώδη πτυχή η οποία καταγράφει την πολυπλοκότητα της ασφάλειας στον κυβερνοχώρο. Μάλιστα σε αυτό το σημείο δεν παραλείπονται οι αλληλεπιδράσεις μεταξύ ανθρώπων, συστημάτων-ανθρώπων και τέλος μεταξύ συστημάτων.
- Στην προστασία των συστημάτων και του κυβερνοχώρου μιας και τυχαίνει οι απειλές να είναι υπαρκτές και αδιαμφισβήτητες, είτε πρόκειται για σκόπιμες ή τυχαίες απειλές ή ακόμη και για φυσικούς κινδύνους. Αυτή η πτυχή ενσωματώνει επίσης την παραδοσιακή άποψη του κυβερνοχώρου, αλλά περιλαμβάνει εκείνα τα συστήματα που παραδοσιακά δεν θεωρούνται μέρος του κυβερνοχώρου, όπως τα συστήματα ελέγχου υπολογιστών και τα κυβερνοφυσικά συστήματα. Επομένως κατ’επέκταση η προστασία αποτελεί βασικό και παραδοσιακό στοιχείο για να συμπεριληφθεί στον ορισμό ως λειτουργικό στοιχείο.
- Γίνεται αναφορά στην έννοια των περιστατικών όπου πιο ελεύθερα θα μπορούσαμε να κάνουμε μια αξιόλογη αναφορά σε περιπτώσεις στον κυβερνοχώρο. Επιπροσθέτως πολλά από τα περιστατικά είναι τυχαία, σκόπιμα και απρόβλεπτα άρα η προστασία λειτουργεί ως λύση στην εμφάνιση κάθε πιθανού προβλήματος.

- Αναφορικά με την έννοια “δεν ευθυγραμμίζονται de jure με τα de facto δικαιώματα ιδιοκτησίας” γίνεται αναφορά σε δύο ξεχωριστές δομές στην πραγματική ιδιοκτησία και στα στοιχεία ψηφιακής περιουσίας που συμπεριλαμβάνονται στην ιδιοκτησία του κυβερνοχώρου. Για αυτόν τον λόγο οφείλουμε να ακολουθούμε και να παρατηρούμε τον πίνακα και πλαίσιο δικαιωμάτων ιδιοκτησίας των Ostrom and Hess (2007). Οποιοδήποτε συμβάν ή δραστηριότητα που παρακάμπτει τα πραγματικά (de facto) δικαιώματα ιδιοκτησίας από τα αντιληπτά (de jure) δικαιώματα ιδιοκτησίας, είτε από πρόθεση είτε από ατύχημα, είτε είναι γνωστό είτε άγνωστο, αποτελεί περιστατικό ασφάλειας στον κυβερνοχώρο.

Το υπουργείο το οποίο ασχολείται με θέματα κυβερνοασφάλειας είναι το Υπουργείο Ψηφιακής Διακυβέρνησης το οποίο όπως εχουμε ήδη αναφερθεί πρόκειται για ένα νεοσύστατο υπουργείο το οποίο έχει φέρει την ψηφιοποίηση σχεδόν όλων των υπηρεσιών και την αποφυγή της έγχαρτης μορφής στον ελλαδικό κρατικό μηχανισμό. Η βασική αιτία για την σύσταση αυτού του υπουργείου στάθηκε η τεχνολογική εξέλιξη αλλά και οι επιρροές από άλλες κρατικές ψηφιοποιήσεις που άνηκαν στην Ευρωπαική Ένωση και απέδειξαν ακράδαντα την αποτελεσματικότητα του κρατικού μηχανισμού (Αθανάσιος Κοσμόπουλος, 2022). Η εμφάνιση της πανδημίας ανάγκασε το ελληνικό κράτος να επισπεύσει τις διαδικασίες της εξέλιξης αυτού του υπουργείου. Για να υπάρξει μια μορφή επιτυχής διακυβέρνησης από το συγκεκριμένο υπουργείο οφείλει η βασική δομή και λειτουργεία του να θέσει τα θεμέλια του στις παραπάνω πτυχές που προαναφέραμε.

Η έννοια της Ηλεκτρονικής Διακυβέρνησης περιγράφεται στα αγγλικά με τους όρους “Electronic Government”, “Electronic Governance”, “Digital Government”, “Online Government” και υφίσταται μια πληθώρα ορισμών για αυτήν από διεθνείς οργανισμούς και την ερευνητική κοινότητα. Ενδεικτικά, ως ηλεκτρονική διακυβέρνηση (e-Government) ορίζεται από τον Οργανισμό Ηνωμένων Εθνών «η αξιοποίηση του διαδικτύου και του παγκόσμιου ιστού για την παροχή κυβερνητικής πληροφορίας και υπηρεσιών στους πολίτες». Εναλλακτικά, ο όρος αυτός αναφέρεται στην «αξιοποίηση των τεχνολογιών πληροφορικής και άλλων web-based τηλεπικοινωνιακών τεχνολογιών με στόχο τη βελτίωση της αποδοτικότητας και αποτελεσματικότητας της παροχής υπηρεσιών από τον δημόσιο τομέα». Ένας άλλος ορισμός που δίνεται από την Παγκόσμια Τράπεζα είναι ο εξής: «Η ηλεκτρονική διακυβέρνηση αφορά τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) από κυβερνητικούς φορείς, οι οποίες έχουν τη δυνατότητα να μεταμορφώσουν τις σχέσεις των φορέων αυτών με τους πολίτες, τις επιχειρήσεις και άλλους τομείς του κράτους».

Βασικό προαπαιτούμενο για τον ψηφιακό μετασχηματισμό της ελληνικής κοινωνίας και οικονομίας συνιστά η διαφύλαξη ενός υψηλού επιπέδου ασφάλειας των ψηφιακών συστημάτων και υπηρεσιών. Η προαγωγή της κυβερνοασφάλειας των συστημάτων δικτύων και υπηρεσιών αποτελεί μία από τις βασικότερες προϋποθέσεις για την εμπέδωση εμπιστοσύνης στους χρήστες των ψηφιακών υπηρεσιών και εφαρμογών στις νέες τεχνολογίες, με σημαντικό όφελος για το συνολικό επίπεδο της «ψηφιακής» ανάπτυξης και της συνολικής κοινωνικής και οικονομικής ευημερίας. Παράλληλα, νέες τεχνολογίες (5G, Artificial Intelligence, IoT, Cloud Computing, Big Data κλπ.) που μπορούν να μεταβάλουν ριζικά τον τρόπο εξυπηρέτησης των πολιτών και των επιχειρήσεων -σε όρους ταχύτητας, εύρους και ποιότητας ψηφιακών υπηρεσιών- αυξάνουν τη συνολική επιφάνεια για ενδεχόμενες κυβερνοεπιθέσεις. Βασικό προαπαιτούμενο για τον ψηφιακό μετασχηματισμό της ελληνικής κοινωνίας και οικονομίας συνιστά η διαφύλαξη ενός υψηλού επιπέδου ασφάλειας των ψηφιακών συστημάτων και υπηρεσιών. Η προαγωγή της κυβερνοασφάλειας των συστημάτων δικτύων και υπηρεσιών αποτελεί μία από τις βασικότερες προϋποθέσεις για την εμπέδωση εμπιστοσύνης στους χρήστες των ψηφιακών υπηρεσιών και εφαρμογών στις νέες τεχνολογίες, με σημαντικό όφελος για το συνολικό επίπεδο της «ψηφιακής» ανάπτυξης και της συνολικής κοινωνικής και οικονομικής ευημερίας. Παράλληλα, νέες τεχνολογίες (5G, Artificial Intelligence, IoT, Cloud Computing, Big Data κλπ.)

που μπορούν να μεταβάλουν ριζικά τον τρόπο εξυπηρέτησης των πολιτών και των επιχειρήσεων -σε όρους ταχύτητας, εύρους και ποιότητας ψηφιακών υπηρεσιών- αυξάνουν τη συνολική επιφάνεια για ενδεχόμενες κυβερνοεπιθέσεις. Αναφορικά με την σημασιολογία της ψηφιακής διακυβέρνησης Οι αποτελεσματικές ψηφιακές δημόσιες υπηρεσίες, ή η ηλεκτρονική διακυβέρνηση, μπορούν να προσφέρουν μεγάλη ποικιλία πλεονεκτημάτων. Αυτά περιλαμβάνουν περισσότερη αποτελεσματικότητα και εξοικονόμηση πόρων για τις κυβερνήσεις και τις επιχειρήσεις, αυξημένη διαφάνεια και μεγαλύτερη συμμετοχή των πολιτών στην πολιτική ζωή. Οι ΤΠΕ χρησιμοποιούνται ήδη ευρέως από κυβερνητικούς φορείς, αλλά η ηλεκτρονική διακυβέρνηση περιλαμβάνει περισσότερα από απλά εργαλεία: περιλαμβάνει επανεξέταση οργανισμών και διαδικασιών και αλλαγή συμπεριφοράς, έτσι ώστε οι δημόσιες υπηρεσίες να παρέχονται πιο αποτελεσματικά στους ανθρώπους. Εάν εφαρμοστεί σωστά, η ηλεκτρονική διακυβέρνηση δίνει τη δυνατότητα στους πολίτες, τις επιχειρήσεις και τους οργανισμούς να πραγματοποιούν τις αλληλεπιδράσεις τους με την κυβέρνηση πιο εύκολα, πιο γρήγορα και με χαμηλότερο κόστος.Η πιθανή εξοικονόμηση κόστους είναι τεράστια. Στη Δανία, η ηλεκτρονική τιμολόγηση εξοικονομεί 150 εκατ. ευρώ στους φορολογούμενους ετησίως και στις επιχειρήσεις 50 εκατ. ευρώ ετησίως. Εάν εισαχθεί σε ολόκληρη την ΕΕ, η ετήσια εξοικονόμηση θα μπορούσε να ξεπεράσει τα 50 δισεκατομμύρια ευρώ. Εν τω μεταξύ, στην Ιταλία τα συστήματα ηλεκτρονικών προμηθειών μείωσαν το κόστος άνω των 3 δισεκατομμυρίων ευρώ.Οι διασυνοριακές ψηφιακές δημόσιες υπηρεσίες επιτρέπουν στους ανθρώπους να μετακινούνται ελεύθερα στην ΕΕ. Είτε μετακομίζετε για δουλειά είτε για οικογένεια, μπορείτε εύκολα να ασχοληθείτε με δημόσιες υπηρεσίες εκτός της χώρας σας.Στο πλαίσιο της στρατηγικής της, η Ευρωπαϊκή Επιτροπή αναλαμβάνει συγκεκριμένες ενέργειες για την ανάπτυξη διασυνοριακών ψηφιακών δημόσιων υπηρεσιών. Αυτά περιλαμβάνουν, αλλά δεν περιορίζονται σε, τη δημιουργία ευρωπαϊκών διαλειτουργικών πλατφορμών όπως ένα κοινό πλαίσιο για τη διαχείριση ηλεκτρονικής ταυτότητας των πολιτών και την προώθηση της καινοτομίας μέσω της χρηματοδότησης πιλοτικών πιλοτικών μεγάλης κλίμακας. Διατίθενται κατευθυντήριες γραμμές σχετικά με τον τρόπο καλύτερης χρήσης των ανοιχτών προτύπων για συστήματα ΤΠΕ των δημόσιων αρχών, προκειμένου να αποφευχθούν εξαρτήσεις από ορισμένους προμηθευτές συστημάτων ΤΠΕ (lock in).

1.4 Ψηφιακή διακυβέρνηση και τομέας Υγείας

Η ψηφιακή διακυβέρνηση φθάνει στον ελληνικό δημόσιο τομέα για να αντικαταστήσει την εγχαρτη μορφή δικαιολογητικών αλλά και συγχρόνως να διευκολύνει στην εξυπηρέτηση των πολιτών μέσω της χρήσης του διαδικτύου και όχι με την έμπρακτη παρουσία στον χώρο της δημόσιας υπηρεσίας. Η απλούστευση των υπηρεσιών και των διαδικασιών αποτελούσε κινητηρια δύναμη για την ίδρυση του συγκεκριμένου Υπουργείου. Παράλληλα με την εξέλιξη της τεχνολογίας και των δυνατοτήτων της τόσο στα κρατικά πλαίσια όσο και στα πλαίσια της Ε.Ε. είναι η εξέλιξη και η βελτίωση της ποιότητας των δημόσιων υπηρεσιών. Εν συνεχεία του δεδομένου πλάνου εκσυχρόνισης των κρατών η ηλεκτρονική διακυβέρνηση έχει θέσει ως στόχο την συνεχή βελτίωση των δυνατοτήτων πρόσβασης σε αυτές, καθώς όμως τόσο το ελληνικό όσο και το κυπριακό κράτος βασίζει τα θεμέλια του στην δημοκρατία μέσω της ηλεκτρονικής διακυβέρνησης πραγματοποιείται η ενίσχυση των δημοκρατικών διαδικασιών και η παράλληλη στήριξη των δημόσιων πολιτικών αρχών. Με σκοπό την δήλωση της διευκρινιστικής γραμμής του ορισμού της ηλεκτρονικής διακυβέρνησης πρόκειται για την σύγχρονη μέθοδο μέσω χρήσης της τεχνολογίας με απόλυτο και μοναδικό σκοπό την βελτίωση ποιότητας των παρεχόμενων υπηρεσιών. Όπως προαναφέραμε σκοπός της ηλεκτρονικής διακυβέρνησης είναι η κατάργηση δικαιολογητικών και αναδιοργάνωση διαδικασιών που έχρηζαν αναγκαιότητας συνδυασμός δημόσιων υπηρεσιών και περίπλοκη γραφειοκρατική διάταξη.

Η συνεχής εξέλιξη της τεχνολογίας και η σύσταση του Υπουργείου Ψηφιακής Διακυβέρνησης έφερε στο προσκήνιο την αναγκαιότητα για ηλεκτρονική υγεία μιας και στο μεσοδιάστημα της δημιουργίας του έλαβε

χώρα παγκοσμίως η πανδημία του θανατηφόρου ιού SARS-COVID-19. Το κυβερνητικό σχέδιο με ονομασία e-health πραγματοποιείται επιτυχώς από το υφιστάμενο υπουργείο. Πρόκειται λοιπόν για συνδυασμένη χρήση πληροφοριών η οποία μπορεί να πραγματοποιηθεί σε τοπικό επίπεδο ή και από απόσταση. Βασικός λειτουργικός σκοπός του συστήματος Υγείας e-health είναι η βελτίωση πρόληψης, διάγνωσης, θεραπείας, παρακολούθησης και διαχείρισης δεδομένων υγείας. Εν συνεχεία η ανταλλαγή δεδομένων

1.6 Σημαντικότητα της συγκεκριμένης μελέτης στο πλαίσιο διεθνών σχέσεων και στρατηγικής

Η ραγδαία εξάπλωση της χρήσης του Διαδικτύου συνέβαλε στη δημιουργία μιας παγκόσμιας κοινωνίας όπου οι άνθρωποι, οι οργανώσεις και οι κυβερνήσεις σε όλη την υφήλιο έρχονται σε επαφή άμεσα και σε πραγματικό χρόνο. Με την ανάπτυξη του δικτύου και των διάφορων λειτουργειών του όπως ΔΙΚΤΥΑ 5G, ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, BIGDATA, CLOUD COMPUTING, IOT παρατηρείται μια αξιοσημείωτη αύξηση στα πολιτικά και οικονομικά κίνητρα για εκμετάλλευση του Διαδικτύου. Τις τελευταίες δεκαετίες, οι εθνικές κυβερνήσεις έχουν προβεί στην ανάπτυξη στρατηγικών για την αντιμετώπιση των ζητημάτων ασφάλειας που ανακύπτουν και συνδέονται με την ταχεία εξάπλωση της χρήσης πληροφοριών και της τεχνολογίας επικοινωνιών. Αυτά τα ζητήματα κυβερνοασφάλειας έχουν εξελιχθεί σε σημαντικά εθνικά προβλήματα, όπου περιλαμβάνονται η προστασία των περιουσιακών στοιχείων, των συστημάτων και των δικτύων με ζωτική σημασία για την λειτουργία και τη σταθερότητα ενός κράτους και χρήζουν μέριμνας από την πλευρά των κυβερνήσεων.[6] Οι προσπάθειες των κρατών για ανάπτυξη κανόνων στον κυβερνοχώρο εστιάζουν στην εφαρμογή του υφιστάμενου διεθνούς δικαίου, στην κάλυψη πιθανών κενών, στην ανάπτυξη προτύπων, καθώς και στην οικοδόμηση μέτρων εμπιστοσύνης. Κατά συνέπεια, έχει αναπτυχθεί ένα περίπλοκο καθεστώς κυβερνοασφάλειας, ώστε να συμπεριλαμβάνει πληθώρα περιφερειακών και διεθνών θεσμών που διαδραματίζουν καταλυτικό ρόλο στη διαμόρφωση ενεργητικών πολιτικών και κατ΄ επέκταση στη διαμόρφωση των σχέσεων μεταξύ των κρατών στη διεθνή σκηνή. Στο πλαίσιο, λοιπόν των διεθνών σχέσεων και της διεθνούς συνεργασίας, η Ευρωπαϊκή Ένωση έχει να επιδείξει μια πληθώρα σημαντικών πολιτικών στον τομέα της κυβερνοασφάλειας, καθώς υπάρχει μια πληθώρα οργανισμών όπως ο ENISA (European Union Agency for Network and Information Security), Europol (Police agency of the European Union), EDA (European Defence Agency), κ.λ.π που είναι επιφορτισμένοι με την διαχείριση των ζητημάτων κυβερνοασφάλειας.

Μελετώντας όλες τις παραπάνω πληροφορίες κατανοούμε πως πρωτεύον ρόλο στη διαφύλαξη και στην προστασία ενός τέτοιου εγχειρήματος κατέχει η κυβερνοασφάλεια. Σε αυτή την διατριβή θα εμβαθύνουμε στον όρο αλλά και στην εφαρμογή της κυβερνοασφάλειας που προσφέρει τόσο το ελληνικό κράτος όσο και το κυπριακό στον τομέα της Δημόσιας Υγείας, περιστατικά παραβίασης του συστηματος, μεθόδους και πλάνα ενδυνάμωσης της κυβερνοασφάλειας στον κυβερνοχώρο αλλά και το νομοθετικό κάδρο από το οποίο πλαισιώνεται. Επιπροσθέτως να τονιστεί το γεγονός πως η πανδημία του ιού Covid-19 έπαιξε σημαντικό ρόλο στην σύσταση του Υπουργείου Ψηφιακής Διακυβέρνησης και στην αναγκαιότητα της ένταξης στην ψηφιακή εποχή με σκοπό την εξελικτική λειτουργικότητα του κρατικού μηχανισμού. Επιπροσθέτως μια τέτοια ερευνητική εργασία έχει σκοπό την ανέρευση πληροφοριών κρατικών πηγών και ακαδημαϊκών βιβλιογραφιών σχετικά με ένα νέο φαινόμενο που θέτει δυναμικές βάσεις για ένα εξυγχρονισμένο ψηφιακό κράτος.

2. Ορισμός Κυβερνοασφάλειας

Με το πρόθεμα «κυβερνό-» αναλύονται οι όροι που έχουν σχέση με το διαδίκτυο αλλά και τους ηλεκτρονικούς υπολογιστές. Στην ακαδημαϊκή κοινότητα δεν μπορεί να επιτευχθεί πλήρης συμφωνία σε σχέση με την έννοια των όρων, με αποτέλεσμα την πραγματοποίηση εναλλακτικών προσεγγίσεων. Ο όρος

«κυβερνοχώρος» περιλαμβάνει τον ψηφιακό χώρο, που δημιουργεί η χρήση του διαδικτύου και των ηλεκτρονικών υπολογιστών. Ωστόσο, ο συγκεκριμένος ορισμός δεν μπορεί να εκφράσει την απεριόριστη φύση του διαδικτύου, οπότε και καθιστά απαραίτητη την επιπλέον διεύρυνσή του. Έτσι, ανάλογα με την προσέγγιση, χρησιμοποιούνται άλλοι περισσότερο περιγραφικοί όροι. Η άποψη πως ο κυβερνοχώρος αποτελεί το εικονικό περιβάλλον εντός του οποίου δραστηριοποιείται ο χρήστης του διαδικτύου, θεωρείται περισσότερο ακριβής και οικείος. Η δραστηριότητα αυτή περιλαμβάνει συναλλαγές και αγοραπωλησίες, επικοινωνίες, έρευνες, μελέτες και άλλα.

- Το διαδίκτυο αποτελεί έναν περίπλοκο εικονικό κόσμο. Ο κυβερνοχώρος δεν μπορεί να οριοθετηθεί και δεν μπορεί να περιοριστεί, παρουσιάζοντας ένα εξαιρετικά μεγάλο μέγεθος το μεγαλύτερο τμήμα του οποίου εξακολουθεί να είναι άγνωστο στο ευρύ κοινό. Έτσι, η πρόσβαση ενός χρήστη σε όλο τον κυβερνοχώρο που δεν διαθέτει ειδικές γνώσεις πάνω στο αντικείμενο και ένα εξειδικευμένο μηχάνημα είναι αδύνατη. Το τμήμα αυτό ονομάζεται «σκοτεινό δίκτυο» ή «dark web».
- Στον κυβερνοχώρο, οι παράνομες δράσεις που πραγματοποιούνται έχουν αφετηρία το ψηφιακό περιβάλλον του διαδικτύου, αλλά είναι στενά συνδεδεμένες και με το πραγματικό περιβάλλον. Οι εγκληματικές οργανώσεις οι οποίες απειλούν τόσο την εθνική όσο και την διεθνή ασφάλεια, μέσα από τις δραστηριότητές τους στον κυβερνοχώρο είναι πιθανό να ασχολούνται με το «χακάρισμα», εν ολίγοις την παραβίαση στα συστήματα ασφαλείας είτε φορέων, είτε ιδιωτών, την διάδοση πληροφοριών χωρίς τις απαραίτητες άδειες ή την παράνομη πρόσβαση σε τραπεζικά συστήματα με την χρήση του διαδικτύου. Στην καθημερινότητα, στο διαδίκτυο πραγματοποιούνται ύποπτες δραστηριότητες και απειλές που αφορούν την παράνομη εκτέλεση συναλλαγών και αγοραπωλησιών σε εικονικό χώρο, το παρεμπόριο, τις απειλές και άλλα.
- Παράνομες δράσεις, που παρουσιάζουν τα προαναφερθέντα στοιχεία, που πραγματοποιούνται στο ψηφιακό περιβάλλον ταξινομούνται στην κατηγορία των κυβερνοεπιθέσεων. Οι επιθέσεις παρουσιάζουν μια ιδιαιτερότητα η οποία είναι η δυσκολία τόσο να εντοπιστούν, όσο και να αντιμετωπιστούν, αφού τις περισσότερες φορές, πραγματοποιούνται την ίδια στιγμή από διαφορετικά σημεία σε όλο τον κόσμο, καθιστώντας δύσκολο την εύρεση τόσο του αρχικού, όσο και του τελικού αποδέκτη.
- Το μεγαλύτερο ποσοστό των επιθέσεων του κυβερνοχώρου στοχεύει στην επίτευξη οικονομικού κέρδους ή στην πρόκληση χάους. Στην προκειμένη περίπτωση οι εγκληματικές δραστηριότητες μπορεί να προκαλέσουν μια γενικότερη κρίση. Οι πιθανότητες δημιουργίας κρίσεων οι οποίες είναι ικανές να πλήξουν μια χώρα είτε σε πολιτικό, είτε σε οικονομικό επίπεδο, αυξάνονται σημαντικά σε περιπτώσεις που παραβιάζονται συστήματα ασφαλείας με σκοπό την υποκλοπή και στη συνέχεια πώληση των πληροφοριών ή ακόμα και τον χαρακτηρισμό των φορέων αλλά και των εταιρειών ως αναξιόπιστες να προστατέψουν τόσο τους πελάτες τους όσο και τα προσωπικά τους δεδομένα και τις βάσεις δεδομένων τους.
- Είναι γεγονός πως πολλά ισχυρά κράτη αλλά και ομάδες που εμπλέκονται στο οργανωμένο έγκλημα, πολύ συχνά κρύβονται πίσω από επιθέσεις στον κυβερνοχώρο. Κάποιοι χάκερς, διαθέτουν εξαιρετικά εξελιγμένη τεχνογνωσία, την οποία και χρησιμοποιούν για να διαταράξουν την ισορροπία σε παγκόσμιο επίπεδο, διεισδύοντας σε επίπεδο που ένας απλός χρήστης του διαδικτύου αδυνατεί.
- Τέλος, η ισχύς του κυβερνοχώρου είναι ακόμα ένας ορισμός με πολύ ενδιαφέρον. Η οδηγία NIS αναλύει ένα «νομοθετικό ορισμό», ο οποίος αναφέρει πως η κυβερνοασφάλεια είναι η δυνατότητα των συστημάτων δικτύου και πληροφοριών να αμύνονται σε συγκεκριμένο βαθμό αξιοπιστίας, σε δράσεις που πλήττουν τη διαθεσιμότητα, την ανθεκτικότητα, την ακεραιότητα ή το απόρρητο των στοιχείων που αποθηκεύονται, μεταφέρονται ή επεξεργάζονται ή των συναφών υπηρεσιών που παρέχονται ή είναι προσιτές μέσω αυτών των συστημάτων δικτύου και πληροφοριών (Μήτρου, 2020).

2.1 Μέθοδοι και πλάνα για την ενδυνάμωση της κυβερνοασφάλειας στον κυβερνοχώρο σε Ελλάδα και Κύπρο από το 2020 έως το 2025.

Η Εθνική ελληνική στρατηγική κυβερνοσφάλειας για την μεγαλύτερη διάδοση και εξέλιξη των δυνατοτήτων του υπουργείου ψηφιακής διακυβέρνησης έχει προγραμματίσει μέχρι το 2025 να εφαρμόσει διάφορες μεθόδους με σκοπό την τόσο την προστασία των δεδομένων που καθιστούν απαραίτητη την πρόσβαση στις υπηρεσίες αλλά και πλάνα για τυχόν απρόβλεπτες ενέργειες.Το Μάρτιο του 2018, κατόπιν εισήγησης της Εθνικής Αρχής Κυβερνοασφάλειας, εκδόθηκε η 3η Αναθεώρηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας . Στην εν λόγω στρατηγική προσδιορίσθηκαν ως γενικές αρχές:

- Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου.
- Η συνεχής βελτίωση των δυνατοτήτων μας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και η διασφάλιση της επιχειρησιακής συνέχειας. Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.
- Η ανάπτυξη ισχυρής κουλτούρας ασφάλειας των πολιτών, του δημόσιου και ιδιωτικού τομέα, αξιοποιώντας τις σχετικές δυνατότητες της ακαδημαϊκής κοινότητας και εν γένει των φορέων του δημόσιου και ιδιωτικού τομέα. Επιπλέον, τέθηκαν συνολικά δεκατρείς στόχοι, πάνω στους οποίους δομήθηκε το στρατηγικό πλάνο της Εθνικής Αρχής:

3.1 Είδη Κυβερνοεπιθέσεων, είδη κυβερνοάμυνας με αναφορά ορισμένων περιστατικών

Μελετώντας σχετικά με τις κυβερνοεπιθέσεις κατανοούμε πως απειλούν την ικανότητά μας να χρησιμοποιούμε το Διαδίκτυο με ασφάλεια, παραγωγικότητα και δημιουργικότητα παγκοσμίως και αποτελούν τον πυρήνα πολλών ανησυχιών για την ασφάλεια τόσο στη δημόσια ζωή όσο και στην ιδιωτική. Η έννοια των κυβερνο-επιθέσεων, ωστόσο, παραμένει υπανάπτυκτη στην ακαδημαϊκή βιβλιογραφία. Σύμφωνα με τον ορισμό που δίνει το Ινστιτούτο IBM πρόκειται για επιθέσεις στον κυβερνοχώρο οι οποίες είναι ανεπιθύμητες προσπάθειες κλοπής, έκθεσης, αλλαγής, απενεργοποίησης ή καταστροφής πληροφοριών μέσω μη εξουσιοδοτημένης πρόσβασης σε συστήματα υπολογιστών. Αν και η λέξη «*κυβερνοεπίθεση*» χρησιμοποιείται συχνά, η σημασία της παραμένει ασαφής (Hathaway et al., 2012, Roscini, 2014). Σε αυτό το σημείο η προσέγγιση για την αποσαφήνιση του ορισμού της επίθεση στον κυβερνοχώρο είναι παρόμοια με την προσέγγιση που ακολούθησαν οι ερευνητές για να διευκρινίσουν τι εννοούσε «ασφάλεια» στα τέλη της δεκαετίας του 1990 (π.χ. Baldwin, 1997· Buzan, 1998· Huysmans, 1998) . Οι ερευνητές ασφαλείας εντόπισαν βασικά χαρακτηριστικά για να καταστήσουν σαφές τι σημαίνει ασφάλεια. Εξάλειψαν τις ασάφειες και τις ασυνέπειες στις διαφορετικές χρήσεις της έννοιας της ασφάλειας. Ο στόχος τους δεν ήταν να παράγουν άλλον έναν ορισμό της ασφάλειας. ξεκίνησαν να προσδιορίσουν τα βασικά χαρακτηριστικά της ασφάλειας *(State of the Union 2017 – Cybesecurity: Commission scales up EU's response to cyber-attacks , 19 Sept. 2017).* Μέχρι στιγμής από τα στοιχεία και τις στατιστικές που έχουμε συλλέξει από επίσημους φορείς όπως η ΕΛΣΤΑΤ και η Statista το σύστημα υγείας έχει δεχθεί παραβιάσεις σε βαθμό που αντιμετωπίστηκαν έγκυρα και με μεγάλη επιτυχία. Δυστυχώς ακόμη δεν έχει κυκλοφορήσει δημοσίως κάποια στατιστική από τις δύο αυτές αναλυτικές υπηρεσίες

3.2 Είδη Κυβερνοεπιθέσεων

Σύμφωνα με έρευνα της Hiscox το φαινόμενο των κυβερνοεπιθέσεων έχει εντατικοποιηθεί ως μέθοδος υποκλοπής δεδομένων και πληροφοριών σε κρατικούς φορείς τόσο στο Ηνωμένο Βασίλειο, στην Γαλλία,

στην Γερμανία, όσο στην Κύπρο. Το 2019 σύμφωνα με την έρευνα συμμετοχή έλαβαν 5.300 χώρες από τις οποίες παρατηρήθηκε αύξηση των κυβερνοεπιθέσεων στο 45% κατά την διάρκεια του 2019 σε αντίθεση με το 2020 όπου το ποσοστό εκτοξεύθηκε στο 61% .

Οι κυβερνοεπιθέσεις υπάγονται στις παρακάτω πληροφορίες

- Κυβερνοκατασκοπεία /Cyber Espionage: Η κυβερνοκατασκοπεία αποτελεί ένα μέσο κυβερνοεπίθεσης και αφορά την συλλογή διάφορων σημαντικών πληροφοριών με την χρήση των ψηφιακών μέσων τεχνολογίας. Ο βασικός στόχος της κυβερνοκατασκοπείας είναι η κλοπή και η συλλογή κρατικών, πολιτικών και πολιτειακών στοιχείων που παίζουν ρόλο υποβιβάζοντας την ανώτερη κρατική λειτουργία. Επιπροσθέτως στόχοι της κυβερνοκατασκοπειας στις κυβερνητικές υπηρεσίες είναι τη κλοπή προσωπικών δεδομένων των πολιτών του κράτους όπως τα προσωπικά στοιχεία των πολιτών.
- Κυβερνοτρομοκρατία /Cyber Terrorism: Σύμφωνα με το Ομοσπονδιακό Γραφείο Διερεύνησης των ΗΠΑ, η κυβερνοτρομοκρατία είναι οποιαδήποτε «προμελετημένη, πολιτικά παρακινούμενη επίθεση κατά των πληροφοριών, των υπολογιστικών συστημάτων, των προγραμμάτων ηλεκτρονικών υπολογιστών και των δεδομένων, που οδηγεί σε επίθεση κατά μη-μαχητικών στόχων από υποεθνικές ομάδες ή παράνομους πράκτορες». Μια κυβερνοεπίθεση υπάγεται στο καθεστώς της κυβερνοτρομοκρατίας όταν ασκεί βία κατά ατόμων ή περιουσιών, ή όταν προκαλεί τέτοια ζημιά που επιφέρει τον τρόμο. Η κυβερνοτρομοκρατία περιλαμβάνει προμελετημένες και πολιτικά υποκινούμενες κυβερνοεπιθέσεις, ενώ πιθανοί της στόχοι είναι τα κυβερνητικά δίκτυα Η/Υ, τα οικονομικά δίκτυα, τα εργοστάσια παραγωγής ενέργειας και τα πληροφοριακά δίκτυα ελέγχου της εναέριας κυκλοφορίας.

Σε μία πιο εξειδικευμένη και τεχνική ανάλυση οι κυβερνοεπιθέσεις μπορούν να διαχωριστούν ως εξής:

- Κυβερνοεπιθέσεις που έχουν σκοπό την απόλυτη συλλογή των δεδομένων και των πληροφοριών. Απτό παράδειγμα υποκλοπής πληροφοριών όπως οι κωδικοί των χρηστών του ηλεκτρονικού ταχυδρομείου της εταιρείας Google τον Ιούνιο του 2011. Να σημειωθεί πως στην συγκεκριμένη περίπτωση η παραβίαση δεν πραγματοποιήθηκε σε απλούς χρήστες αλλά σε υψηλόβαθμα στελέχη των ΗΠΑ, της Κίνα και της Ρωσίας. Υπεύθυνη θεωρήθηκε η Κίνα, όπως και τον Ιανουάριο του 2010 όταν και σημειώθηκαν ανάλογες παραβιάσεις.
- Οι κατανεμημένες επιθέσεις άρνησης υπηρεσιών (Distributed Denial of service Attacks - DDoS) που αποτελούν την βασικότερη και σημαντικότερη πηγή παραβίασης. Στόχος αυτών των επιθέσεων είναι η μη πρόσβαση στο σύστημα λόγω της υψηλής εισροής δεδομένων και του υπολογιστικού φόρτου που προκαλείται από την συστηματική επίθεση.
- Κυβερνοέγκλημα σε καμία περίπτωση δεν μπορεί να υπάρξει ταύτιση με την κυβερνοεπιθεση μιας και όταν γίνεται αναφορά στο κυβερνοέγκλημα θεωρείται η χρήση διάφορων ηλεκτρονικών μεθόδων που βασίζονται σε ηλεκτρονικούς υπολογιστές και σχετικά δίκτυα, προκειμένου να διαπραχθεί μια παράνομη πράξη. Βασικά χαρακτηριστικά του είναι ότι η παραβίαση πραγματοποιείται συνήθως από ιδιώτες και όχι από κράτη ή κρατικές υπηρεσίες. Ως επί το πλείστον οι δράστες του δεν έχουν πολιτικούς σκοπούς και δεν επιδιώκουν να πλήξουν την εθνική ασφάλεια ενός κράτους και ότι η διαπραχθείσα ενέργεια ποινικοποιείται με βάση το εκάστοτε εθνικό ή το διεθνές δίκαιο.
- Επιθέσεις από το διαδίκτυο(webbasedattacks). Πρόκειται για απειλές που έχουν ως βασικό στόχο την κατάρρευση των γνωστών browsers, καθώς και την ολοκληρωτική κατάρρευσης στα συστήματα διαχείρισης περιεχομένου.

- Κάνοντας αναφορά στο Phishing μιλάμε για κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.
- Επιθέσεις σε διαδικτυακές εφαρμογές (webapplicationattacks). Πρόκειται λοιπόν για επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications).
- Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου είτε αλλιώς γνωστές ως επιθέσεις SPAM, πρόκειται για ηλεκτρονικά μηνύματα υπό την μορφή ανεπιθύμητης αλληλογραφίας. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.
- Επιθέσεις άρνησης υπηρεσίας(Denial of Service –DoS attacks)Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών(απώλεια διαθεσιμότητας).
- Κλοπή ταυτότητας χρήστη (identitytheft)Ο επιτιθέμενοςαποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ιδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.Παραβιάσεις προσωπικών δεδομένωνΕπιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις.

3.3 Νομοθετικό πλαίσιο Ευρωπαϊκής Ένωσης στον τομέα Υγειας Ελλάδας και Κύπρου

Η ψηφιακή υγεία και περίθαλψη αφορά εργαλεία και υπηρεσίες που χρησιμοποιούν τεχνολογίες των πληροφοριών και των επικοινωνιών (ΤΠΕ) για τη βελτίωση της πρόληψης, της διάγνωσης, της θεραπείας, της παρακολούθησης και της διαχείρισης θεμάτων υγείας, καθώς και για την παρακολούθηση και τη διαχείριση των συνηθειών του τρόπου ζωής που επηρεάζουν την υγεία. Η ψηφιακή υγεία και περίθαλψη είναι καινοτόμος και μπορεί να βελτιώσει την πρόσβαση στην περίθαλψη και την ποιότητα αυτής της περίθαλψης, καθώς και να αυξήσει τη συνολική αποδοτικότητα του τομέα της υγείας. Η Ευρωπαϊκή Ένωση Υγείας θα εστιάσει τόσο σε επείγουσες όσο και σε μακροπρόθεσμες προτεραιότητες στον τομέα της υγείας, από την αντιμετώπιση της κρίσης της COVID-19 και την ανθεκτικότητα απέναντι σε διασυνοριακές απειλές κατά της υγείας, έως το ευρωπαϊκό σχέδιο για την καταπολέμηση του καρκίνου, τη φαρμακευτική στρατηγική για την Ευρώπη και την ψηφιακή υγεία. Η ΕΕ θα συνεχίσει να επιδιώκει τη διεθνή συνεργασία όσον αφορά τις παγκόσμιες απειλές και προκλήσεις για την υγεία, όπως είναι οι ανθεκτικές στα αντιμικροβιακά λοιμώξεις και ο εμβολιασμός.

3.4 Ο ρόλος και η πολιτική της Ε.Ε. στην κυβερνοάμυνα

Ακρογωνιαίος λίθος της πολιτικής της ΕΕ είναι η στρατηγική για την κυβερνοασφάλεια του 201363 . Άμεση προτεραιότητα της στρατηγικής είναι το ψηφιακό περιβάλλον της ΕΕ να καταστεί το ασφαλέστερο παγκοσμίως, με παράλληλη προάσπιση των θεμελιωδών ανθρώπινων αξιών και ελευθεριών. Έχει πέντε βασικούς στόχους:

- την ενίσχυση της κυβερνοανθεκτικότητας
- τη μείωση της κυβερνοεγκληματικότητας·
- την ανάπτυξη πολιτικών και ικανοτήτων κυβερνοάμυνας
- την ανάπτυξη βιομηχανικών και τεχνολογικών πόρων κυβερνοασφάλειας
- τη θέσπιση διεθνούς πολιτικής για τον κυβερνοχώρο, σύμφωνη με τις θεμελιώδεις αξίες της ΕΕ.

Η στρατηγική για την κυβερνοασφάλεια είναι άρρηκτα συνδεδεμένη με τρεις στρατηγικές που ακολούθησαν και εγκρίθηκαν μεταγενέστερα: α. Το Ευρωπαϊκό Θεματολόγιο για την ασφάλεια (2015), όπου η Ευρωπαϊκή Επιτροπή καθορίζει τη στρατηγική της Ένωσης για την αντιμετώπιση απειλών στον τομέα της ασφάλειας κατά την περίοδο 2015-2020. Κύριος στόχος του είναι η βελτίωση της επιβολής του νόμου και της δικαστικής αντιμετώπισης της κυβερνοεγκληματικότητας. Επιδίωξή του είναι επίσης ο προσδιορισμός των εμποδίων που παρακωλύουν τις ποινικές έρευνες στον τομέα του κυβερνοεγκλήματος και η ανάπτυξη των σχετικών ικανοτήτων για την δραστική καταπολέμησή του.

1. Η στρατηγική για την Ψηφιακή Ενιαία Αγορά (2015) έχει ως στόχο τη βελτίωση της πρόσβασης σε ψηφιακά προϊόντα και υπηρεσίες. Η επίτευξη της ψηφιακής ενιαίας αγοράς θα επιτρέψει στην Ευρώπη να διατηρήσει τη θέση της ως παγκόσμιου ηγέτη στην ψηφιακή οικονομία, καθώς θα βοηθήσει τις ευρωπαϊκές επιχειρήσεις να αναπτύξουν τις δραστηριότητές τους σε παγκόσμιο επίπεδο.
2. Η Συνολική Στρατηγική (2016) επιδιώκει την ενίσχυση του ρόλου της ΕΕ στην παγκόσμια ασφάλεια μέσω της δέσμευσης για ενίσχυση των προσπαθειών σε θέματα κυβερνοχώρου, της συνεργασίας με βασικούς εταίρους και της αποφασιστικότητας για την αντιμετώπιση των απειλών του κυβερνοχώρου σε όλους τους τομείς πολιτικής, συμπεριλαμβανομένης της αντιμετώπισης της παραπληροφόρησης μέσω στρατηγικής επικοινωνίας. Το 2014 εγκρίθηκε το ευρωπαϊκό Πλαίσιο Πολιτικής για την Κυβερνοάμυνα (EU Cyber Defence Policy Framework) το οποίο τονίζει ότι ο κυβερνοχώρος είναι το πέμπτο πεδίο στρατιωτικής δραστηριότητας μαζί με την ξηρά, τη θάλασσα, τον αέρα και το διάστημα, και συμπληρώνει ότι η επιτυχής εφαρμογή της ΚΠΑΑ εξαρτάται από έναν ασφαλή κυβερνοχώρο. Το πλαίσιο αυτό, το οποίο επικαιροποιήθηκε τον Νοέμβριο του 2018 από το Ευρωπαϊκό Συμβούλιο, δίνει ιδιαίτερη έμφαση στη προστασία των δικτύων επικοινωνιών και πληροφοριών της ΚΠΑΑ και στόχος του είναι να αναπτυχθεί περαιτέρω η πολιτική της ΕΕ για την κυβερνοάμυνα λαμβάνοντας υπόψη σχετικές εξελίξεις σε άλλα φόρουμ και τομείς πολιτικής που έλαβαν χώρα από το 2014 μέχρι το 2018. Το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα στηρίζει την ανάπτυξη ικανοτήτων κυβερνοάμυνας των κρατών μελών της ΕΕ καθώς και την ενίσχυση της κυβερνοπροστασίας των υποδομών της ΕΕ για την ασφάλεια και την άμυνα, με την επιφύλαξη της εθνικής νομοθεσίας των κρατών μελών και της νομοθεσίας της ΕΕ, συμπεριλαμβανομένου του πεδίου εφαρμογής της κυβερνοάμυνας, όπου αυτό ορίζεται. Προσδιορίζονται ως τομείς προτεραιότητας για την κυβερνοάμυνα η κατάρτιση και οι ασκήσεις, η έρευνα, η τεχνολογία, η συνεργασία με πολιτικούς φορείς και διεθνείς οργανισμούς ώστε να βελτιωθεί η ικανότητα αντίδρασης της ΕΕ στις κυβερνοκρίσεις και στις υβριδικές επιχειρήσεις μέσω της βελτίωσης των διαδικασιών λήψης αποφάσεων και της διαθεσιμότητας των πληροφοριών. Παράλληλα βέβαια, διευκρινίζονται οι ρόλοι των διαφόρων ευρωπαϊκών φορέων με πλήρη σεβασμό των αρμοδιοτήτων και ευθυνών των φορέων της Ένωσης και των κρατών μελών καθώς και του θεσμικού πλαισίου της ΕΕ και της αυτονομίας της κατά τη λήψη αποφάσεων. Στο πλαίσιο της αποτελεσματικής αντιμετώπισης των κυβερνοαπειλών κατά των ψηφιακών υποδομών ζωτικής σημασίας της ΕΕ αλλά και των ιδιωτών χρηστών εγκρίνεται το 2016 το Κοινό Πλαίσιο για την Αντιμετώπιση Υβριδικών Απειλών. Το κείμενο αυτό υπογραμμίζει ότι οι κυβερνοεπιθέσεις μπορούν να εκδηλωθούν με τη μορφή εκστρατειών παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης με στόχο την κοινωνική αναταραχή και τη διατάραξη της κοινωνικής συνοχής. Επιπλέον, επισημαίνει την ανάγκη καλύτερης ενημέρωσης και ευαισθητοποίησης των ευρωπαίων πολιτών για τις αναδυόμενες απειλές στον κυβερνοχώρο αλλά και της ενίσχυσης της συνεργασίας μεταξύ της ΕΕ και του NATO69 . Μια νέα δέσμη μέτρων παρουσιάστηκε για την κυβερνοασφάλεια το 201770 , στην οποία γινόταν σαφής αναφορά στην αναγκαιότητα επικαιροποίησης της στρατηγικής για την κυβερνοασφάλεια του 2013 ώστε αυτή να ανταποκρίνεται αποτελεσματικά στις νέες μορφές

κυβερνοαπειλών που αναδύονται ραγδαία. Η δέσμη μέτρων αφορούσε επίσης σε μια σειρά νομοθετικών προτάσεων καθώς και σ' ένα προσχέδιο για ταχεία και συντονισμένη αντίδραση σε περίπτωση μεγάλης κλίμακας κυβερνοεπίθεσης κατά των ψηφιακών και επικοινωνιακών συστημάτων της ΕΕ. Στο πλαίσιο αυτό προτάθηκε και η αναβάθμιση του οργανισμού της ΕΕ για την Κυβερνοασφάλεια ENISA. Σύμφωνα με την πρόταση, ο «νέος» οργανισμός θα είχε ως μόνιμη εντολή να συνδράμει τα κράτη μέλη στην αποτελεσματική αποτροπή και αντιμετώπιση κυβερνοεπιθέσεων ενώ θα ενίσχυε την ετοιμότητα αντίδρασης της ΕΕ μέσω της διοργάνωσης ετήσιων πανευρωπαϊκών ασκήσεων με αντικείμενο την κυβερνοασφάλεια, καθώς και μέσω της διασφάλισης της καλύτερης ανταλλαγής πληροφοριών και γνώσεων σχετικά με απειλές.

Είναι αναμφισβήτητο γεγονός ότι κατά την δεύτερη δεκαετία του 21ου αιώνα έχουν πραγματοποιηθεί σημαντικά βήματα προόδου στο χώρο της κυβερνοασφάλειας με τη θέσπιση νομοθετικών ρυθμίσεων και δημιουργία φορέων με στόχο τη συμπαγή θωράκιση της ευρωπαϊκής ανθεκτικότητας ως μια δυναμική απάντηση στις ολοένα και αυξανόμενες απειλές των κυβερνοεπιθέσεων. Το 2013, η ΕΕ παρουσίασε μια στρατηγική για την ασφάλεια στον κυβερνοχώρο δρομολογώντας μια σειρά βασικών αξόνων εργασίας για τη βελτίωση της ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο. Οι κύριοι στόχοι και οι βασικές αρχές της, όσον αφορά την προώθηση ενός αξιόπιστου, ασφαλούς και ανοικτού οικοσυστήματος του κυβερνοχώρου, εξακολουθούν να ισχύουν. Ωστόσο, η απουσία ουσιαστικών κριτηρίων αξιολόγησης και μέτρησης του αντικτύπου των εφαρμοζόμενων πολιτικών και νομοθετικών αλλαγών επιδρούν αρνητικά στην εξαγωγή ασφαλών συμπερασμάτων ως προς την αποτελεσματικότητα τους. Το γεγονός βέβαια αυτό, ως ένα βαθμό, έχει κάποια λογική εξήγηση αν αναλογιστούμε ότι ένα πλήθος πολιτικών και νομοθετικών μέτρων που έχουν υιοθετηθεί και αφορούν στην ευρωπαϊκή κυβερνοασφάλεια άρχισαν πρόσφατα να εφαρμόζονται, γεγονός που εμποδίζει την πλήρη και εμπεριστατωμένη αξιολόγηση των συνεπειών τους. Επίσης, δεν πρέπει να μας διαφεύγει το γεγονός ότι, σημαντικό ρόλο στη διαδικασία της αξιολόγησης διαδραματίζουν τα στατιστικά στοιχεία και χρήσιμα δεδομένα για ζητήματα που σχετίζονται με τον κυβερνοχώρο. Μέχρι στιγμής, ελάχιστα κράτη μέλη έχουν την πρόβλεψη να συγκεντρώνουν συστηματικά επίσημα δεδομένα. Πολλά κράτη δεν είναι πρόθυμα να μοιραστούν με άλλα κράτη πληροφορίες τις οποίες τα ίδια θεωρούν ευαίσθητες για την εθνική τους ασφάλεια. Οι παραπάνω διαπιστώσεις έχουν ως αποτέλεσμα να μην υπάρχει η δυνατότητα της σύγκρισης, με προγενέστερα στατιστικά στοιχεία, που θα αποτύπωνε ως ένα μετρήσιμο μέγεθος το βαθμό προόδου και την αποτελεσματικότητα συγκεκριμένων πολιτικών δράσεων και νομοθεσιών στο χώρο της κυβερνοασφάλειας. Οι ταχύτητες με τις οποίες αναδύονται οι νέες ψηφιακές τεχνολογίες και αναβαθμίζονται οι δυνατότητες των κυβερνοαπειλών υπερβαίνουν σε μεγάλο βαθμό τις αντίστοιχες ταχύτητες σχεδιασμού και εφαρμογής της νομοθεσίας της ΕΕ. Το γεγονός αυτό έχει ως αποτέλεσμα προβλέψεις και διατάξεις του νομοθετικού πλαισίου να εμφανίζονται ως παρωχημένες στην αντιμετώπιση και καταστολή κυβερνοεπιθέσεων και κυβερνοεγκλημάτων που βασίζονται και εξαπλώνονται χρησιμοποιώντας νέες τεχνολογικές μεθόδους.

4. Τεχνολογία, το 5G και το μελλοντικό πλαίσιο τεχνολογικής ανάπτυξης και μέσα κυβερνοάμυνας στο Δημόσιο Σύστημα Υγείας Ελλάδας και Κύπρου

Οι τεχνολογικές εξελίξεις παρουσιάζουν ταχύτατους ρυθμούς σε παγκόσμιο επίπεδο, περνώντας σε μια νέα τροχιά εφαρμογών και δικτύωσης. Στο πλαίσιο της νέας τεχνολογίας δικτύων 5ης γενιάς, όπου οι ταχύτητες συνδεσιμότητας εκτιμάται να φτάσουν έως και 20 Gigabits ανά δευτερόλεπτο4 , επιτρέπεται η βελτιστοποίηση της αξιοποίησης νέων τεχνολογιών από τη μονάδα του νοικοκυριού (smart home) και της επιχείρησης (smart business) μέχρι το επίπεδο των πόλεων, τις λεγόμενες έξυπνες πόλεις (smart cities), αλλά και ολόκληρους τομείς υπηρεσιών. Οι νέες τεχνολογίες, όπως η τεχνητή νοημοσύνη (artificial intelligence), η δυνατότητα περαιτέρω ανάπτυξης έξυπνων μηχανών (έξυπνα κινητά τηλέφωνα, έξυπνα αυτοκίνητα, έξυπνες συσκευές), σε συνδυασμό με τεχνολογίες νέφους (cloud computing) και τις νέες

δυνατότητες δικτύωσης των δικτύων 5ης γενιάς, έχουν τεράστιο εύρος εφαρμογών στους τομείς της υγείας (Internet of Medical Things - IoMT, ψηφιακό σύστημα υγείας, διασύνδεση υπηρεσιών παροχής υγείας και υγειονομικών πόρων), των μεταφορών (σε επίπεδο οχήματος, οδηγού, αλλά και υποδομής, με αποτέλεσμα καινοτόμες υπηρεσίες στους τομείς της οδικής ασφάλειας, του ταξιδιού, των logistics κ.λπ.), τον κατασκευαστικό τομέα (Industry 4.0), τον αγροδιατροφικό τομέα, αλλά και άλλους τομείς όπως την εθνική άμυνα (Internet of Military Things). Με το δεδομένο αυτό δεν είναι τυχαίο ότι ήδη γίνεται λόγος για Internet of Everything (IoE), ή άλλως η διαδικτύωση των πάντων. Παράλληλα με τις εξελίξεις αυτές, η πανδημία COVID-19 έθεσε νέα δεδομένα και νέες απαιτήσεις σε όλο το φάσμα της οικονομικής και κοινωνικής ζωής. Οι προκλήσεις και οι αδυναμίες λειτουργίας της φυσικής επαφής των ανθρώπων υπό το φως των αυξημένων κινδύνων μετάδοσης της ασθένειας, τα μέτρα περιορισμού που λαμβάνονται σε παγκόσμια κλίμακα, η παύση λειτουργίας καταστημάτων και χώρων συνάθροισης κοινού, αναζητούν εναλλακτικές μέσα στον ψηφιακό κόσμο: την τηλεδιάσκεψη (teleconference, telco), τη βιντεο-κλήση (video call), την απομακρυσμένη πρόσβαση (remote access), το ηλεκτρονικό κατάστημα (e-shop), το ψηφιακό κράτος (digital state). Όλες οι ανωτέρω ταχύτατες εξελίξεις, σε συνδυασμό με την αυξανόμενη ζήτηση για ψηφιακές εφαρμογές και υπηρεσίες, ενέχουν σημαντικές προκλήσεις. Όσο ταχύτερα εξαπλώνεται ο ψηφιακός κόσμος σε κάθε έκφανση της καθημερινής οικονομικής και κοινωνικής ζωής, τόσο εξαπλώνεται και η επιφάνεια (surface) για κακόβουλες και παράνομες ενέργειες. Όσο οι νέες υπηρεσίες μας επιτρέπουν μεγαλύτερη προσωποποίηση και εστίαση στις δικές μας ανάγκες, τόσο αυξάνονται οι κίνδυνοι για την εκμετάλλευση ή παραβίαση των προσωπικών μας δεδομένων. Όσο ευχερέστερη καθίσταται η επικοινωνία μας με φίλους και συνεργάτες σε όλο τον πλανήτη, τόσο εξίσου εύκολη μπορεί να καταστεί η αξιοποίηση της έκθεσής μας σε ιστοτόπους κοινωνικής δικτύωσης (social networking) για την πραγματοποίηση έκνομων ενεργειών. Πρόκειται για ελάχιστα παραδείγματα, που καταδεικνύουν ότι όχι μόνο η ίδια η τεχνολογία, αλλά κυρίως ο τρόπος που τη χρησιμοποιούμε, κρύβουν κινδύνους. Για τους λόγους αυτούς, ο σχεδιασμός και η εφαρμογή μιας ολιστικής Στρατηγικής Κυβερνοασφάλειας, οφείλουν να εστιάζουν στη διαρκή εισροή γνώσης και κατανόησης των σύγχρονων τεχνολογικών εξελίξεων, την πρόβλεψη ειδικών δικλείδων ασφαλείας, αλλά και τη διαρκή ενημέρωση και ευαισθητοποίηση των χρηστών στο πλαίσιο της προαγωγής της κυβερνο-υγιεινής (cyber-hygiene).

4.1 Η τεχνολογία σήμερα

Εν έτη 2021 έχουμε φτάσει σε ένα σημείο που οι νέες τεχνολογίες κατέχουν έναν από τους πιο σημαντικούς παράγοντες της καθημερινής μας ζωής. Πλέον, όλοι οι κοινωνικοί τομείς, οι παραγωγικοί κλάδοι και οι κρατικοί φορείς βασίζονται στην πληροφορική και στις νέες τεχνολογίες για τη λειτουργία τους. Η δημόσια υγεία δεν αποτελεί εξαίρεση καθώς σημείωσε ραγδαία εξέλιξη κυρίως μέσω της τεχνολογίας και ιδιαιτέρως η ψηφιοποίηση των απαραίτητων υπηρεσιών στο δημόσιο σύστημα υγείας. Η είσοδος της τεχνολογίας σε όλους τους τομείς της υγείας, από απλές συνταγογραφήσεις μέχρι η εφαρμογή της τηλεϊατρικής. Η Ελλάδα έχει κάνει σημαντικά βήματα προόδου σε όλους τους τομείς που αφορούν πληροφοριακά συστήματα τηλεπικοινωνιών και δικτύων, αλλά είναι απαραίτητο να κάνει και άλλα προκειμένου να είναι σε ανταγωνιστικό επίπεδο σε σχέση με άλλες χώρες που ανήκουν στην Ε.Ε. Η διείσδυση της τεχνολογίας στις δημόσιες επιχειρήσεις είναι σε πολύ καλό, αλλά όχι ακόμα σε αρκετά ικανοποιητικό επίπεδο ώστε ο κρατικός μηχανισμός να εξαρτάται κάθε αυτού από την τεχνολογική εξέλιξη.

4.2 Σημαντικότητα του δικτύου 5G στο Δημόσιο Σύστημα Υγείας

Το 5G δεν είναι απλώς μια εξέλιξη της τεχνολογίας στις τηλεπικοινωνίες. Είναι η θεμελιώδης πλατφόρμα για την τέταρτη βιομηχανική επανάσταση και θα γίνει αναπόσπαστο μέρος των κοινωνιών και των πολιτικών υποδομών, όπως ακριβώς οι δρόμοι, η ενέργεια και οι μεταφορές. Αποτελεί την πύλη για τον εικονικό κόσμο, ο οποίος θα αρχίσει να προσαρμόζεται οργανικά στις ποικίλες ανάγκες των χρηστών με εφαρμογές σε πραγματικό χρόνο και κατ' απαίτηση. Για τους διαχειριστές δικτύων, το 5G θα γίνει η απόλυτη πλατφόρμα για πραγματική επιχειρηματική καινοτομία και νέες ροές εσόδων. Η πιο ριζοσπαστική του ικανότητα είναι η μεταφορά τεράστιου όγκου δεδομένων σε πραγματικό χρόνο. Το 5G, η νέα γενιά κινητών επικοινωνιών, κυκλοφόρησε το 2019 και από τον Μάιο του 2020 125 χώρες σε όλο τον κόσμο έχουν αρχίσει να επενδύουν στη συγκεκριμένη τεχνολογία.

Ωστόσο, μόνο το ένα τέταρτο του παγκόσμιου πληθυσμού είναι πιθανό να αποκτήσει κάλυψη 5G υψηλής ταχύτητας έως το 2030.σύμφωνα με επίσημα στοιχεία της Deloitte. Παράλληλα σημαντικές θα είναι οι διαφορές μεταξύ των χωρών που θα μπουν στον κόσμο του 5G. Σε αυτό το πλαίσιο οι αναλυτές της McKinsey χωρίζουν τον κόσμο σε Πρωτοπόρες χώρες-Pioneers countries (Ηνωμένες Πολιτείες, Ιαπωνία και Νότια Κορέα) και η Κίνα, σε Ηγέτιδες αγορές Leader Markets όπως η Γαλλία, ο Καναδάς, στις Χώρες που Ακολουθούν-Followers και συγκεκριμένα η Βραζιλία και η Πολωνία και σε χώρες που είναι πολύ πιο πίσω - Trailing Countries όπως το Πακιστάν και η Βολιβία. Μέχρι το 2030 θα πραγματοποιηθεί ένα σύμπλεγμα συνδυασμού τάσεων, συμπεριλαμβανομένης όχι μόνο της ευρύτερης κάλυψης δικτύου, αλλά και του αυξανόμενου αριθμού συσκευών σε προσιτή τιμή, στην ανάπτυξη ευρύτερου διαδικτυακού περιεχομένου δημογραφικά και κοινωνικά προσαρμοσμένο. Στην Ευρώπη το 5G μπορεί να προσφέρει οφέλη 210 δια. ευρώ, σύμφωνα με τη μελέτη Analysys Mason. Τα έξυπνα εργοστάσια, η γεωργία και οι προαστιακές και αγροτικές περιοχές έχουν μεγαλύτερο αντίκτυπο στο ΑΕΠ. Πάνω από 50 δισεκατομμύρια ευρώ πρόσθετου οφέλους 5G μπορούν να παραδοθούν για λιγότερο από 20 δισεκατομμύρια ευρώ δημόσιας χρηματοδότησης. Η Statista, η διεθνής εταιρεία μετρήσεων, περιμένει έκρηξη συνδρομητών 5G παγκοσμίως από 80 εκατομμύρια το 2020 στα 2,7 δισεκατομμύρια το 2025, με τις περισσότερες συνδρομές 5G στη Βορειοανατολική Ασία, τη Βόρεια Αμερική και τη Δυτική Ευρώπη μέλος της οποίας είναι και το ελληνικό κράτος. Για την ιστορία χρειάστηκαν 12 χρόνια το 3G, που εισήχθη στις αρχές της δεκαετίας του 2000, για να προσεγγίσει ένα δισεκατομμύριο χρήστες παγκοσμίως. Συγκριτικά, το 4G εξαπλώθηκε τρεις φορές πιο γρήγορα, φτάνοντας το σήμα ενός δισεκατομμυρίου χρηστών τέσσερα χρόνια μετά την εισαγωγή του το 2010.

Όπως τονίζεται, τα επόμενα χρόνια, η διασύνδεση των μηχανών θα επιτυγχάνεται με υψηλότερες ταχύτητες δεδομένων, εξαιρετικά χαμηλό λανθάνοντα χρόνο και αυξημένη διαθεσιμότητα, και με πολλαπλά οφέλη για τους χρήστες. Μέχρι το 2023 τα συνδεδεμένα αυτοκίνητα πρόκειται να σχηματίσουν τη μεγαλύτερη εγκατεστημένη βάση των τελικών σημείων 5G IoT παγκοσμίως με περισσότερα από 19 εκατομμύρια εγκατεστημένα τελικά σημεία. Οι εξωτερικές κάμερες παρακολούθησης και οι συσκευές τηλεματικής

στόλου αποτελούν επίσης μεγάλα μέρη της εγκατεστημένης βάσης 5G IoT. Σύμφωνα με τη McKinsey, μέχρι το 2030, η διασύνδεση μηχανών θα μπορούσε να αντιπροσωπεύει περισσότερο από το 70% όλων των συνδεδεμένων συσκευών, αλλά μόνο το 12% της κίνησης δεδομένων. Όπως τονίζουν οι τηλεπικοινωνιακοί πάροχοι, παρόλο που το όφελος από την εισαγωγή των νέων δικτύων θα γίνει άμεσα αισθητός από τη ραγδαία βελτίωση της εμπειρίας διαδικτύου στα κινητά τηλέφωνα και τους φορητούς υπολογιστές, η πραγματική μεταμόρφωση της ζωής των χρηστών θα προκύψει από την ψηφιοποίηση των καθημερινών υπηρεσιών που προσφέρονται και κυρίως, μέσω των νέων τεχνολογιών που θα αναδείξει. Η ικανότητά του να υποστηρίζει την τεχνητή νοημοσύνη, τη ρομποτική, το διαδίκτυο των πραγμάτων, τον εξ αποστάσεως έλεγχο και την εικονική πραγματικότητα, θα επιτρέψει τη δημιουργία καινοτομιών που θα προσφέρουν ανυπολόγιστη αξία στην καθημερινότητά μας, επηρεάζοντας ένα μεγάλο φάσμα βιομηχανικών και οικονομικών κλάδων. Σε σχέση με τις προηγούμενες τεχνολογίες, η ευελιξία του 5G του επιτρέπει να προσαρμόζεται στις διαφορετικές ανάγκες που έχει ο κάθε ξεχωριστός κλάδος, γεγονός που αυξάνει τις ευκαιρίες για συνδυαστική καινοτομία μεταξύ των κλάδων.

Στο πλαίσιο της αναγκαιότητας της αναπτυξης του δικτύου 5G εντάσσεται και το δημόσιο σύστημα υγείας. Τα συνολικά οφέλη της ψηφιοποίησης της υγειονομικής περίθαλψης (πέρα από τα οφέλη που σχετίζονται με τη συνδεσιμότητα) είναι τεράστια. Σύμφωνα με τη McKinsey τα απομακρυσμένα συστήματα παρακολούθησης ασθενών που θα λειτουργούν σε προηγμένα δίκτυα θα μπορούσαν να αποδώσουν περίπου 70 δισ. δολ. έως 120 δισ. δολ. σε ετήσια αξία παγκοσμίως, μαζί με χαμηλότερη νοσηρότητα και μεγαλύτερη ικανοποίηση του ασθενούς, ευκολία και ανεξαρτησία. Η συνδεσιμότητα σε 5G μπορεί να δώσει σε αυτά τα συστήματα πιο εξελιγμένες δυνατότητες. Ακριβής και συνεχής μετάδοση δεδομένων, μπορεί να εντοπίσει προειδοποιητικά σημάδια ασθένειας νωρίτερα και να τα επιλύσει γρηγορότερα με ελάχιστες παρεμβάσεις. Οι νέες εφαρμογές υγείας πάνω στο 5G θα μπορούσαν να ενεργοποιήσουν περίπου από 1,5 τρισ. δολ. έως 3,0 τρισ. δολ. ετησίως έως το 2030, με όφελος από το 11% έως το 20% των σχεδόν 15 τρισ. δολ. σε παγκόσμια έργα υγειονομικής περίθαλψης. Πέρα από αυτά τα άμεσα οικονομικά οφέλη, θα μπορούσε επίσης ένα περαιτέρω ψηφιοποιημένο σύστημα υγειονομικής περίθαλψης να έχει σημαντικές έμμεσες επιπτώσεις στην οικονομία που προκύπτουν από καλύτερα αποτελέσματα για την υγεία και υγιέστεροι πληθυσμοί. Επίσης μπορεί να επιτευχθεί πιο αποτελεσματική απομακρυσμένη παρακολούθηση ασθενούς, μέσω αισθητήρων και τα δεδομένα που θα προκύπτουν μπορούν να μεταδοθούν αμέσως σε προηγμένη κινητή σύνδεση για αξιολόγηση. Αυτά τα συστήματα μπορούν να βοηθήσουν τους ασθενείς αλλά και τους παρόχους φροντίδας σε πραγματικό χρόνο, εάν απαιτούνται προληπτικά μέτρα. Αυτό μπορεί να οδηγήσει στην αποφυγή ή τη συντόμευση της διαμονής στο νοσοκομείο καθώς και σε χαμηλότερα ποσοστά

νοσοκομειακής νοσηλείας. Η απομακρυσμένη παρακολούθηση μπορεί να βοηθήσει τους ασθενείς να διατηρήσουν χρόνιες ασθένειες όπως ο διαβήτης, χρόνια αποφρακτική αναπνευστική νόσος, καρδιακή ανεπάρκεια και υπόταση υπό έλεγχο, απαλλάσσοντάς τους από συνεχή ιατρικά ραντεβού. Αυτό έχει ως αποτέλεσμα ένα τεράστιο μερίδιο των δαπανών υγειονομικής περίθαλψης, να περιορίζεται.

4.3 Ο ρόλος των ταχυτήτων και της οπτικής ίνας καθώς και ο ρόλος τους στην κυβερνοασφάλεια

Στη νέα ψηφιακή εποχή, η συνδεσιμότητα αποτελεί πλέον βασικό προαπαιτούμενο για τον ψηφιακό μετασχηματισμό των κρατών, καθώς τα αναμενόμενα οικονομικά και κοινωνικά οφέλη θα επιτευχθούν μόνο εάν τα κράτη διασφαλίσουν την ευρεία εγκατάσταση δικτύων και παροχή υπηρεσιών πολύ υψηλής χωρητικότητας σε όλη την επικράτειά τους. Ειδικότερα, η ευρυζωνικότητα θεωρείται ένα δημόσιο αγαθό το οποίο, ως ψηφιακό ανάλογο των δημόσιων συγκοινωνιακών υποδομών, συμβάλλει τα μέγιστα στην οικονομική ανάπτυξη και ευημερία. Η Ευρωπαϊκή Ένωση, αναγνωρίζοντας τον καταλυτικό ρόλο της συνδεσιμότητας για την ανάπτυξη της ενιαίας ψηφιακής αγοράς και τη διασφάλιση του ψηφιακού της μέλλοντος, συνέταξε το 2010 το Ψηφιακό Θεματολόγιο για την Ευρώπη 2020 (Digital Agenda for Europe 2020), το οποίο προδιέγραφε σαφείς στόχους για την εξασφάλιση της παροχής πολύ ταχύτερης πρόσβασης στο διαδίκτυο. Στη συνέχεια, το 2016 η Ε.Ε. αναβάθμισε τους στόχους αυτούς, μέσω της ευρωπαϊκής κοινωνίας των Gigabit, σύμφωνα με την οποία η Ε.Ε. ως το 2025 επιδιώκει:

- Να εξασφαλίσει εξαιρετικά υψηλή συνδεσιμότητα της τάξης των Gigabits σε όλους τους κύριους κοινωνικο-οικονομικούς μοχλούς όπως εκπαιδευτικά ιδρύματα, ερευνητικά κέντρα, κόμβοι μεταφορών, φορείς δημοσίων υπηρεσιών όπως νοσοκομεία και διοίκηση καθώς και επιχειρήσεις που βασίζονται στις ψηφιακές τεχνολογίες,
- Να παρέχει αδιάλειπτη κάλυψη 5G σε όλες τις αστικές περιοχές και όλες τις κύριες επίγειες διαδρομές μεταφορών,
- Να παρέχει πρόσβαση σε συνδεσιμότητα στο διαδίκτυο για όλα τα ευρωπαϊκά νοικοκυριά, σε αστικές και αγροτικές περιοχές, με ελάχιστη ταχύτητα 100 Mbps, η οποία θα δύναται να αναβαθμιστεί σε ταχύτητες της τάξης των Gbps.

Περαιτέρω, η Ε.Ε. προσδιόρισε τις ζώνες συχνοτήτων που θα χρησιμοποιηθούν για την εισαγωγή και ανάπτυξη των δικτύων 5G στην Ευρωπαϊκή Ένωση (700 MHz, 3400-3800 MHz και 26 GHz).Επιπλέον, στις 16 Σεπτεμβρίου 2020, η ΕΕ ανακοίνωσε την πρόθεσή της για επιτάχυνση και συγκεκριμενοποίηση των στόχων του σχεδίου για την ψηφιακή Ευρώπη μέχρι το 2030, δίνοντας έμφαση στην ψηφιακή της κυριαρχία. Για το σκοπό αυτό, θα θέσει συγκεκριμένους στόχους σε τομείς όπως η συνδεσιμότητα, οι δεξιότητες και οι ψηφιακές δημόσιες υπηρεσίες. Στο πλαίσιο αυτό δημοσιεύτηκε η Σύσταση της Επιτροπής (C(2020) 6270)[3]σχετικά με την κοινή εργαλειοθήκη της Ένωσης για τη μείωση του κόστους εγκατάστασης δικτύων πολύ υψηλής χωρητικότητας και τη διασφάλιση έγκαιρης και ευνοϊκής για τις επενδύσεις πρόσβασης στο ραδιοφάσμα 5G, με σκοπό την προώθηση της συνδεσιμότητας για τη στήριξη της οικονομικής ανάκαμψης από την κρίση λόγω COVID-19 στην Ένωση.Η Ελλάδα παραμένει προσηλωμένη στους στόχους του European Gigabit Society έχοντας καταρτίσει σχέδιο για την προώθηση της

ευρυζωνικότητας, που επικαιροποιείται διαρκώς, σχεδιάζοντας και αξιολογώντας τις απαιτούμενες δράσεις με βάση τα δεδομένα και τις ιδιαιτερότητες της ελληνικής αγοράς. Αναφορικά με την υφιστάμενη κατάσταση, η χώρα παρουσιάζει υψηλή διαθεσιμότητα σταθερών ευρυζωνικών δικτύων σε νοικοκυριά (99,3% για πρώτη φορά στο τέλος του 2019). Σχετικά με την κάλυψη ευρυζωνικών δικτύων υψηλής ταχύτητας (Next Generation Access – NGA) ανά νοικοκυριό, καταγράφεται σημαντική επιτάχυνση στη σύγκλιση με τον ευρωπαϊκό μέσο όρο. Αναφορικά με την κάλυψη σε δίκτυα υπερυψηλών ταχυτήτων, στην Ελλάδα, η χρήση τεχνολογίας Vectoring παρέχει, στην πλειονότητα των περιπτώσεων, πραγματικές υπερυψηλές ταχύτητες (>100Mbps έως 200Mbps). Όσον αφορά την κάλυψη της τεχνολογίας 4G (LTE), αυτή προσεγγίζει το μέσο όρο της Ε.Ε (98-99% περίπου).Στην κατηγορία κάλυψης με ταχύτητες >100 Mbps, σύμφωνα με τα τελευταία διαθέσιμα στοιχεία, καταγράφεται σημαντική υστέρηση κατά περίπου 25 ποσοστιαίες μονάδες σε σχέση με τον ευρωπαϊκό μέσο όρο, γεγονός που συνδέεται κυρίως με τις διαδικασίες ηλεκτροδότησης των καμπινών (τεχνολογία Vectoring). Το αμέσως επόμενο διάστημα, στο στόχο αυτό θα συμβάλει και η επιτάχυνση της ανάπτυξης των δικτύων FTTH στη χώρα.Σχετικά με τη διείσδυση των σύγχρονων σταθερών ευρυζωνικών επικοινωνιών, αυτή κινείται με αργούς ρυθμούς, σε σύγκριση με το μέσο όρο της Ε.Ε. Το ζήτημα της διείσδυσης, είναι ιδιαίτερα σύνθετο, με παραμέτρους που συνδέονται, μεταξύ άλλων, με την οικονομική κατάσταση των νοικοκυριών και την τεχνολογική τους ωριμότητα.

4.4 Πανδημία COVID-19 και Ψηφιοποίηση των Δημόσιων Υπηρεσιών Υγείας

Σύμφωνα με την άποψη των συγγραφέων Γ. Μαρή και Π. Σκλιά <<Η ελληνική δημόσια διοίκηση παρουσιάζει ομοιότητες με διοικήσεις άλλων ευρωπαϊκών χωρών, αλλά και δικές της ιδιομορφίες. Αυτές είναι γνωστές σε πολλούς Έλληνες λόγω προσωπικών εμπειριών κατά τις συναλλαγές τους με δημόσιες υπηρεσίες πολύ άνισης ποιότητας. Υπάρχουν θετικά και αρνητικά στοιχεία (Gao & Yu, 2020). Αφενός, ιδίως κατά τις τελευταίες δύο δεκαετίες, έχουν συμβεί μεγάλες πρόοδοι ως προς την εξυπηρέτηση πολιτών και επιχειρήσεων από τη διοίκηση, την ψηφιοποίηση των παρεχόμενων υπηρεσιών και της ενδο-διοικητικής επικοινωνίας. Αφετέρου, όμως, στη χώρα μας η διοίκηση συνεχίζει να πάσχει, μεταξύ άλλων, από πελατειακές τάσεις στις προσλήψεις μη μόνιμων, δηλαδή έκτακτων, εποχικών και άλλων υπαλλήλων, υπερσυγκεντρωτισμό όσον αφορά τη λήψη αποφάσεων, πολύ παραδοσιακές, αργές και συχνά αναποτελεσματικές μεθόδους οργάνωσης της εργασίας, βαθύ χάσμα ανάμεσα αφενός στις ρυθμίσεις που θεσπίζονται και αφετέρου τις πρακτικές που ακολουθούνται σε πλήθος τομέων της δημόσιας πολιτικής. Μία ακόμα παθογένεια είναι η ’’εκμετάλευση’’ (ΕΛΣΤΑΤ, 2020) του ανθρώπινου δυναμικού όπως και η χρησιμοποίηση ακατάλληλων υπαλλήλων σε θέσεις που δεν υπάγονται στις αρμοδιότητες τους. Το σύστημα εμφάνισε δυσλειτουργίες στην τοπική / περιφερειακή κυβέρνηση. Υπήρξε περιορισμένος και προβληματικός λειτουργικός τομέας (κυρίως ευθύνη για γραφειοκρατικές διαδικασίες, διαδικασίες επεξεργασίας, καθαριότητα, ορισμένα θέματα υποδομής). Ωστόσο η χώρα μας προσπάθησε να μετατρέψει την κρίση αυτή σε ευκαιρία, μία ευκαιρία που όλοι οι Έλληνες περιμένουν εδώ και χρόνια να δουν να

υλοποιείται αλλάζοντας την καθημερινότητά τους *(Makrydimitris & Michalopoulos, 2000; Hlepas, 2003; OECD, 2011; Spanou & Sotiropoulos, 2011; Spanou, 2018, 2020b; Sotiropoulos, 2021)*. Είναι γεγονός ότι πάντοτε για τη λήψη πολιτικών αποφάσεων συμβάλλουν σημαντικά και τα στελέχη της Δημόσιας Διοίκησης. Σήμερα η Ελλάδα διαθέτει προσωπικό στις Δημόσιες Υπηρεσίες υψηλού επιπέδου που βοηθούν καθημερινά προς την κατεύθυνση αυτή *(Weible et al. 2020)*. Η έκρηξη της κρίσης προκάλεσε την ξαφνική αναστολή των περισσότερων δημοσίων δραστηριοτήτων λόγω του κινδύνου μόλυνσης, της έλλειψης προστατευτικού εξοπλισμού και της αβεβαιότητας των ιατρικών στοιχείων. Τα ταχεία βήματα ψηφιακού μετασχηματισμού που άρχισαν στα μέσα Μαρτίου 2020, λόγω Covid-19, δεν έχουν ακόμη αποτυπωθεί ούτε στις δομές, ούτε στις στατιστικές. Αυτές, αντιθέτως, δείχνουν το μέγεθος των προκλήσεων ψηφιακού μετασχηματισμού, ο οποίος προϋποθέτει ανθρώπινο δυναμικό με ψηφιακές γνώσεις και δεξιότητες. Οι ψηφιακές γνώσεις, δεξιότητες και ικανότητες, είναι πλέον, στις αρχές του 21ου αιώνα, προϋπόθεση ατομικής και συλλογικής ευημερίας. Η ελληνική κυβέρνηση έδωσε ιδιαίτερη έμφαση στον ψηφιακό μετασχηματισμό και τη διακυβέρνηση δεδομένων στο δημόσιο τομέα. Πολυάριθμες διοικητικές διαδικασίες και συνθήκες λειτουργίας ψηφιοποιήθηκαν και συνδέθηκαν με νέες εφαρμογές και συστήματα ηλεκτρονικής διακυβέρνησης. Ξεκίνησε μια σειρά σημαντικών πρωτοβουλιών για τη βελτίωση της διαλειτουργικότητας και την ανάπτυξη διεπαφών που χρησιμοποιούνται για διασύνδεση μητρώων και βάσεων δεδομένων. Συγκεκριμένα επιταχύνθηκε η ψηφιοποίηση του δημοσίου με τη προσθήκη τριών υπηρεσιών που αφορούν μεγάλο όγκο συναλλαγών (εξουσιοδότηση, υπεύθυνη δήλωση, άυλη και εξ αποστάσεως συνταγογράφηση). Παράλληλα η Κυβέρνηση με την εποπτεία και σχεδιασμό από το Υπουργείο Ψηφιακής Διακυβέρνησης προχώρησε το σχέδιο της νέας εποχής ψηφιακής διακυβέρνησης στη δημόσια διοίκηση της χώρας μας μέσα από συγκεκριμένα μέτρα που θα διευκόλυναν την καθημερινότητα των πολιτών, πόσο μάλλον εν μέσω κρίσης της πανδημίας όπου όλοι οι κάτοικοι έμεναν κλεισμένοι μέσα στα σπίτια τους και οι συναλλαγές με φυσική παρουσία με το δημόσιο έχριζε τεράστιας δυσκολίας και ειδικά σε άτομα που ανήκουν στις ευπαθείς ομάδες *(Maris,G., Sklias, P., & Maravegias, N.(2020))*. The political economy of the Greek economic crisis in 2020. (European Politics and Society). Η ενσωμάτωση νέων εργαλείων και πλατφορμών πληροφορικής συνοδεύτηκε από την ανάπτυξη και την επέκταση υπαρχόντων προγραμμάτων και πρακτικών. Η χρήση e-mail για την κυκλοφορία εγγράφων, ψηφιακών υπογραφών, κέντρων διαλειτουργικότητας, εφαρμογών και πλατφορμών για την ηλεκτρονική δημοσίευση και διαχείριση διοικητικών εγγράφων είναι μερικές ενδεικτικές ενέργειες ηλεκτρονικής διακυβέρνησης που έχουν ενισχυθεί κατά τη διάρκεια της πανδημίας. Επιπλέον, πραγματοποιήθηκαν πολλές συναντήσεις και διαβουλεύσεις μέσω τηλεφωνίας ή διαδικτυακών πλατφορμών, όπως η ηλεκτρονική παρουσία της πλατφόρμας τηλεδιάσκεψης. Η Κυβέρνηση θεσμοθέτησε νέες μεθόδους και μέτρα λειτουργίας για την

εξυπηρέτηση των πολιτών. Τα εν λόγω μέτρα στοχεύουν σε μια νέα γενιά δημόσιας διοίκησης που πριν χρόνια φάνταζαν αδιανόητα. Συγκεκριμένα ο κρατικός μηχανισμός πέτυχε μια αποτελεσματική παρέμβαση ως αποτέλεσμα της ευρύτερης κινητοποίησης μέσα από πλατφόρμες ψηφιακών υπηρεσιών, νομοθετικές *(European Parliament, 2020)* και ρυθμιστικές πρωτοβουλίες, οδηγίες για τη διευκόλυνση και την ασφάλεια των πολιτών κατά την ψηφιακή διεκπεραίωση των υποθέσεών τους, αποδεικνύοντας με αυτό τον τρόπο τα έγκαιρα μέτρα που έλαβε το Υπουργείο Ψηφιακής Διακυβέρνησης τη δύσκολη περίοδο του κορονοϊού, με σκοπό την εξ αποστάσεως λειτουργία του Δημοσίου, την απομακρυσμένη εξυπηρέτηση των πολιτών, την τηλεργασία και την τηλεκπαίδευση *(Christensen & Lægreid, 2020)*. Μέσα σε όλα τα μέτρα που πήρε η Κυβέρνηση κατά την περίοδο της υγειονομικής κρίσης ήταν η λειτουργία του gov.gr, η άυλη συνταγογράφηση, έτσι ώστε οι πολίτες πλέον να έχουν εφόσον το επιθυμούν τη δυνατότητα να λαμβάνουν τις ιατρικές τους συνταγές στο κινητό τους, χωρίς να χρειάζεται να τις προσκομίζουν τυπωμένες στον φαρμακοποιό. Στη συνέχεια, όλες οι συνεδριάσεις όλων των συλλογικών οργάνων της τοπικής αυτοδιοίκησης διεξάγονταν μέσω τηλεδιάσκεψης. Οι Δήμοι στο πλαίσιο των αρμοδιοτήτων τους, παρά τις δυσκολίες που επέφερε η υγειονομική κρίση, συνέχισαν να ασκούν τον θεσμικό τους ρόλο, για να διαφυλάξουν τη δημόσια υγεία. Έκαναν σημαντικά βήματα μπροστά, όσον αφορά την καλύτερη εξυπηρέτηση και διευκόλυνση των πολιτών, μέσω της επιτάχυνσης της διαδικασίας ψηφιακής αναβάθμισης των υπηρεσιών τους, προσπάθεια που θα συνεχιστεί με ακόμη μεγαλύτερη ένταση το επόμενο διάστημα, ώστε να γίνει πράξη το όραμα για τους Ψηφιακούς Δήμους. Παράλληλα ανέδειξαν για μια ακόμη φορά το ανθρώπινο πρόσωπο της αυτοδιοίκησης, μέσα από τις κοινωνικές τους δράσεις και πρωτοβουλίες, καθώς μέσα από τις 880 δημοτικές Δομές Βοήθειας, κάλυψαν τις ανάγκες σε βασικά είδη (φάρμακα, τρόφιμα, είδη υγιεινής) 80.000 περίπου συμπολιτών τους (Greece 2.0).>>

Σύμφωνα λοιπόν με τον *Ιωάννης Μουρούτσος* <<Η κρίση Covid-19 υπήρξε ένας εξαιρετικά ισχυρός παράγοντας για την ενεργοποίηση των εκκρεμών μεταρρυθμίσεων και για την επιτάχυνση των προγραμμάτων μεταρρυθμίσεων που ήταν ήδη σε εξέλιξη. Ωστόσο, η ταχεία κλιμάκωση της κρίσης και η έλλειψη χρόνου για επαρκή προετοιμασία αποτελεσματικών πολιτικών αντιδράσεων οδήγησαν σε μια σειρά αλλαγών που συχνά πραγματοποιήθηκαν με διαχωρισμένο τρόπο, χωρίς σαφή σύνδεση με ένα συνολικό σχέδιο διοικητικής μεταρρύθμισης. Η αντίδραση της κυβέρνησης στην πανδημία, ειδικά στα αρχικά στάδια, φαίνεται να στερείται οργάνωσης που θα διασυνδέει και θα συντονίζει αυτά τα στοιχεία σε μια ευρύτερη στρατηγική κατεύθυνση. Ωστόσο η κυβέρνηση και η διοίκηση αντέδρασαν στην εκδήλωση της πανδημίας, με περιοριστικά μέτρα για τη λειτουργία δημόσιων υπηρεσιών και ιδιωτικών επιχειρήσεων, περιορισμό της κυκλοφορίας και μέτρα υποστήριξης προς επιχειρήσεις και εργαζομένους. Εκδόθηκε πλήθος Πράξεων

Νομοθετικού Περιεχομένου (ΠΝΠ) για την προστασία των δημοσίων υπαλλήλων και την κατά το δυνατό ομαλή εξακολούθηση λειτουργίας των δημοσίων υπηρεσιών. Για παράδειγμα, σχετικό με το θέμα μας, η ΠΝΠ προέβλεψε τη μετατροπή διαφόρων διαδικασιών της διοίκησης σε ψηφιακές με σκοπό τη διευκόλυνση πολιτών και επιχειρήσεων. Μετά από αναγκαίες ηλεκτρονικές ενέργειες ταυτοποίησης, πολίτες και εκπρόσωποι επιχειρήσεων μπορούν να λαμβάνουν ηλεκτρονικά διάφορα πιστοποιητικά. Παρομοίως δυνατή είναι και η υπογραφή και έκδοση υπεύθυνης δήλωσης μέσω της ηλεκτρονικής εφαρμογής «e-Dilosi», όπως και η παροχή εξουσιοδότησης προς τρίτους μέσω της ηλεκτρονικής εφαρμογής «e-Exousiodotisi». Αντί για την αυτοπρόσωπη υποβολή αιτήσεων στα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), είναι δυνατή η ηλεκτρονική υποβολή τους μέσω του ermis.gov.gr. Πολλές διαδικασίες και ειδικές ενέργειες (π.χ., στις Δ.Ο.Υ.) δεν έχουν βέβαια ψηφιοποιηθεί. Ωστόσο, η δραματική κατάσταση που δημιουργήθηκε με τη διασπορά του κορονοϊού λειτούργησε ως καταλύτης εξελίξεων στη δημόσια διοίκηση. Η απότομη ψηφιοποίηση των σχέσεων κράτους– πολιτών, με είσοδο και εγγραφή πολλών χρηστών υπολογιστών σε διαφορετικές ψηφιακές πλατφόρμες, συνεπάγεται προφανώς τη δήλωση διαφόρων προσωπικών δεδομένων τους και νέες δυνατότητες επεξεργασίας τέτοιων δεδομένων από πλήθος δημόσιων φορέων. Υπάρχουν τέτοιοι και άλλοι εύλογοι προβληματισμοί για τα όρια παρέμβασης του κράτους στις ατομικές ελευθερίες των πολιτών και για τα περιοριστικά μέτρα που επιβλήθηκαν για την προστασία της δημόσιας υγείας.

Παρολ’αυτά, αν σκεφτεί κανείς τις χαμένες εργατοώρες και το κόστος μετακινήσεων και συνεννοήσεων χιλιάδων επιχειρήσεων και πολιτών, κατά τις αυτοπρόσωπες επισκέψεις τους σε δημόσιες υπηρεσίες, κατά την περίοδο πριν από τις ανωτέρω βελτιωτικές αλλαγές, το οικονομικό και διοικητικό όφελος θα πρέπει να είναι υπολογίσιμο και μεγάλο. Ένα άλλο κρίσιμο στοιχείο που λείπει από την ατζέντα μεταρρυθμίσεων ήταν η ενσωμάτωση της διαχείρισης κρίσεων ως οριζόντιας ικανότητας του κρατικού μηχανισμού για την αντιμετώπιση των σημερινών και μελλοντικών κρίσεων. Έτσι, ένα κρίσιμο ερώτημα είναι εάν θα αναπτυχθεί ένα γενικό σχέδιο και αποτελεσματικοί προ-ενεργητικοί μηχανισμοί για να διασφαλιστεί ότι η δημόσια διοίκηση θα είναι προετοιμασμένη για μελλοντικές παγκόσμιες κρίσεις, όπως απειλές για την ασφάλεια των συστημάτων μετανάστευσης ή πληροφορικής. Το ξέσπασμα της πανδημίας έφερε στο προσκήνιο τις πολιτικές απαντήσεις το ζήτημα της ικανότητας του εσωτερικού διοικητικού συστήματος να προσαρμόζεται γρήγορα σε αβέβαια και μεταβαλλόμενα περιβάλλοντα και να αντιμετωπίζει έγκαιρα και αποτελεσματικά σοκ. Μια βασική πρόκληση παραμένει η ανθεκτικότητα του διοικητικού συστήματος σε εξωτερικούς κραδασμούς και η ικανότητά του να ανταποκρίνεται αποτελεσματικά σε καταστάσεις αυξημένης πολυπλοκότητας. Η ελληνική διοίκηση στερείται σε μεγάλο βαθμό ένα σχέδιο έκτακτης ανάγκης, καθώς και τους απαραίτητους πόρους για τη διαχείριση των πολύπλοκων κοινωνικών και

οικονομικών επιπτώσεων της κρίσης, ειδικά στην αρχική της φάση. Ως εκ τούτου, οι πολιτικές και οι θεσμικές αντιδράσεις ήταν κυρίως επανενεργοποιητικές. Ωστόσο, σε σχετικά σύντομο χρονικό διάστημα, το εγχώριο διοικητικό σύστημα κατάφερε να προσαρμοστεί σε αυτό το νέο περιβάλλον και να υποστηρίξει την καταπολέμηση της πανδημίας και την εφαρμογή των μέτρων για την αντιμετώπιση των επιπτώσεών της. Από την άποψη αυτή, η πανδημία επεσήμανε την ανάγκη ανάπτυξης ισχυρότερων προληπτικών μηχανισμών για τη διαχείριση κρίσεων. Μαζί με τις πολιτικές και τα προγράμματα που συνδέονται άμεσα με την πανδημία και την προσπάθεια ανάκαμψης, άλλες σημαντικές μεταρρυθμίσεις έχουν εισαχθεί πρόσφατα ή / και βρίσκονται σε εξέλιξη, για παράδειγμα το νέο νομοθετικό πλαίσιο για τις διαδικασίες πρόσληψης στο δημόσιο τομέα (2021) και εσωτερικός έλεγχος. Ωστόσο, στην Ελλάδα παρατηρούνται συχνά σημαντικά «κενά εφαρμογής» μεταξύ των στόχων και των αποτελεσμάτων των προγραμμάτων μεταρρύθμισης, καθώς και μεταξύ των επίσημων (νομικών) διατάξεων και της πραγματικής εφαρμογής. Επιπλέον, ο διοικητικός μηχανισμός πρέπει να μεταρρυθμιστεί «εν κινήσει», εν μέσω κρίσης υγείας, ενώ οι πόροι του παραμένουν περιορισμένοι. Επομένως, πρέπει να αποφευχθεί μια υπερφόρτωση της ατζέντας μεταρρυθμίσεων προτού εξασφαλιστεί κάποιος βαθμός σταθεροποίησης του συστήματος και ικανότητας διαχείρισης αλλαγών. Οι οντότητες του δημόσιου τομέα έχουν βιώσει σημαντικές αλλαγές και έχουν επέλθει ευεργετικές αλλαγές σε όλα τα επίπεδα διακυβέρνησης που θα μπορούσαν να οδηγήσουν σε ευρύτερες, συστημικές βελτιώσεις. Για το σκοπό αυτό, το διοικητικό σύστημα μπορεί να εκμεταλλευτεί αυτό το παράθυρο ευκαιριών και να εκμεταλλευτεί τις θετικές προοπτικές μακροπρόθεσμων και βαθύτερων μεταρρυθμίσεων. Λαμβάνοντας υπόψη τα επόμενα κύματα της πανδημίας, θα χρειαστούν ορισμένες προσαρμογές και αναθεωρήσεις στα μέτρα έκτακτης ανάγκης που είχαν προσαρμοστεί στις αρχικές φάσεις. Στις περισσότερες περιπτώσεις, οι πολιτικές απαντήσεις ήταν το αποτέλεσμα γρήγορων διαδικασιών και αποφάσεων που δεν είχαν επαρκή προετοιμασία. Επομένως, ενδέχεται να απαιτείται αναθεώρηση και επανασχεδιασμός των πρώιμων επιλογών λαμβάνοντας υπόψη την εξέλιξη της πανδημίας. Μια βασική πρόκληση θα είναι ιδιαίτερα η απόσπαση των διαρθρωτικών μέτρων από τις στοχευμένες (τεχνικές) απαντήσεις στην πανδημία και την ενσωμάτωσή τους σε ένα μακροπρόθεσμο σχέδιο διοικητικής μεταρρύθμισης στην εποχή μετά την κρίση.>>

Έτσι στο πλαίσιο αξιοποίησης των ευκαιριών που δημιουργήθηκαν λόγω της αποφυγής εξάπλωσης του covid-19, προτείνονται τα ακόλουθα

1. Η εκτεταμένη εφαρμογή της τηλεϊατρικής. Συνεργασία μεταξύ Υπουργείου Υγείας και Υπουργείου Ψηφιακής Διακυβέρνησης, για την εφαρμογή ψηφιακών προγραμμάτων τηλεϊατρικής που να επιτρέπουν στους γιατρούς την εξ αποστάσεως παροχή ιατρικών υπηρεσιών στους ασθενείς.

2. Η καθιέρωση κεντρικού συστήματος προμηθειών υγειονομικού υλικού, καθώς με την εφαρμογή του θα υφίσταται συνολική εικόνα των αναγκών για την καλύτερη προμήθεια του υγειονομικού υλικού. Παράλληλα θα εξοικονομείται χρόνος ως προς τη διαδικασία παροχής του υλικού και ανθρώπινοι πόροι.

3. Η διατήρηση του νομοθετικού πλαισίου για τηλεργασία των ευπαθών ομάδων καθώς και η επέκταση του μέτρου αυτού για όλο το προσωπικό, όπου αυτό είναι εφικτό.

4. Η επέκταση εφαρμογής νέων τεχνολογιών και η εκπαίδευση του προσωπικού της δημόσιας διοίκησης μέσω του Εθνικού Κέντρου Δημόσιας Διοίκησης - Ινστιτούτο Εκπαίδευσης Προσωπικού.

5. Η δημιουργία κόμβου Υποστήριξης Επενδυτικών και Επιχειρηματικών Δραστηριοτήτων, με αναδιοργάνωση των υπηρεσιών της τοπικής αυτοδιοίκησης, οι οποίες θα παρέχουν αξιόπιστες πληροφορίες για όλες τις παραμέτρους που συμβάλλουν στη λήψη επενδυτικών αποφάσεων και θα υποστηρίζουν ενδεχόμενους επενδυτές των σχετικών διαδικασιών και αιτημάτων τους.

6. Ψηφιοποίηση περισσότερων υπηρεσιών δημόσιας διοίκησης σε πολίτες και επιχειρήσεις.

7. Αποτελεσματικότερη ένταξη των αποφοίτων της Εθνικής Σχολής Δημόσιας Διοίκησης και Τοπικής Αυτοδιοίκησης στις υψηλού επιπέδου θέσεις της διοίκησης.

8. Επέκταση της ήδη απόπειρας ευελιξίας της δημόσιας διοίκησης και επέκταση της τηλεργασίας στο κράτος.

9. Δημιουργία δικτύων μόνιμης συνεργασίας μεταξύ δημοσίων υπαλλήλων, εκπροσώπων των κοινωνικών εταίρων και εμπειρογνωμόνων.

10. Συλλογή και ανάλυση δεδομένων αφενός για την ανταπόκριση των εργαζομένων στις προκλήσεις που δημιουργεί η πανδημία στην εργασία τους και αφετέρου για την εμπειρία, τις στάσεις και τις αντιλήψεις των ίδιων των εργαζομένων κατά τη διάρκεια της πανδημίας *(Ιωάννης Μουρούτσος (2020) E-Journals.E-Publishing, Public Administration and Local Government in coronavirus crisis)*

4.5 Το μελλοντικό σχέδιο μελλοντικής ανάπτυξης και προκλήσεις στο Δημόσιο Σύστημα Υγείας

Στην εποχή που διανύουμε η κυβερνοασφάλεια είναι μεγίστης σημασίας και αποτελεί το κεντρικό θέμα στις συζητήσεις της Ευρωπαϊκής Ένωσης. Για τον λόγο αυτό, η Ευρωπαϊκή Επιτροπή και ο ύπατος εκπρόσωπος δεσμεύονται να εφαρμόσουν τη νέα στρατηγική για την κυβερνοασφάλεια κατά τους προσεχείς μήνες. Θα υποβάλλουν τακτικά εκθέσεις σχετικά με την πρόοδο που σημειώνεται και θα ενημερώνουν πλήρως το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ευρωπαϊκής Ένωσης και τα ενδιαφερόμενα μέρη για όλες τις

σχετικές δράσεις, ενώ θα ενθαρρύνεται η συμμετοχή τους σε αυτές. Επιπλέον, σε ό, τι αφορά την οδηγία NIS2, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θα την εξετάσουν και θα την εγκρίνουν. Μόλις επιτευχθεί συμφωνία και εγκριθούν οι προτάσεις, τα κράτη μέλη θα πρέπει να τις μεταφέρουν στο εθνικό τους δίκαιο εντός 18 μηνών από την έναρξη ισχύος τους. Τέλος, η Επιτροπή θα επανεξετάζει περιοδικά την οδηγία NIS2 και θα υποβάλλει εκθέσεις σχετικά με τη λειτουργία τους. Και στην Ελλάδα αντίστοιχα, η υλοποίηση των στρατηγικών στόχων της Εθνικής Στρατηγικής Κυβερνοασφάλειας παρακολουθείται από την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αξιολόγηση και την ανατροφοδότηση της Στρατηγικής. Λαμβάνοντας δε υπόψη την ανάγκη διαμόρφωσης ενός πιο μακροπρόθεσμου ορίζοντα στην υλοποίηση των περιγραφόμενων πρωτοβουλιών και δράσεων, προτείνεται η παρούσα στρατηγική να επικαιροποιείται ανά πέντε έτη.

ΑΝΑΛΥΣΗ

5. Τεχνολογία, το 5G και το μέλλοντικό πλαίσιο τεχνολογικής ανάπτυξης και μέσα κυβερνοάμυνας στο Δημόσιο Σύστημα Υγείας.

Οι τεχνολογικές εξελίξεις παρουσιάζουν ταχύτατους ρυθμούς σε παγκόσμιο επίπεδο, περνώντας σε μια νέα τροχιά εφαρμογών και δικτύωσης. Στο πλαίσιο της νέας τεχνολογίας δικτύων 5ηςγενιάς, όπου οι ταχύτητες συνδεσιμότητας εκτιμάται να φτάσουν έως και 20 Gigabits ανά δευτερόλεπτο4, επιτρέπεται η βελτιστοποίηση της αξιοποίησης νέων τεχνολογιών από τη μονάδα του νοικοκυριού (smarthome) και της επιχείρησης (smartbusiness) μέχρι το επίπεδο των πόλεων, τις λεγόμενες έξυπνες πόλεις (smartcities), αλλά και ολόκληρους τομείς υπηρεσιών. Παράλληλα με τις εξελίξεις αυτές, η πανδημία COVID-19 έθεσε νέα δεδομένα και νέες απαιτήσεις σε όλο το φάσμα της οικονομικής και κοινωνικής ζωής. Οι προκλήσεις και οι αδυναμίες λειτουργίας της φυσικής επαφής των ανθρώπων υπό το φως των αυξημένων κινδύνων μετάδοσης της ασθένειας, τα μέτρα περιορισμού που λαμβάνονται σε παγκόσμια κλίμακα, η παύση λειτουργίας καταστημάτων και χώρων συνάθροισης κοινού, αναζητούν εναλλακτικές μέσα στον ψηφιακό κόσμο: την τηλεδιάσκεψη (teleconference, telco), τη βιντεο-κλήση (videocall), την απομακρυσμένη πρόσβαση (remoteaccess),το ηλεκτρονικό κατάστημα (e-shop), το ψηφιακό κράτος (digitalstate). Όλες οι ανωτέρω ταχύτατες εξελίξεις, σε συνδυασμό με την αυξανόμενη ζήτηση για ψηφιακές εφαρμογές και υπηρεσίες, ενέχουν σημαντικές προκλήσεις. Όσο ταχύτερα εξαπλώνεται ο ψηφιακός κόσμος σε κάθε έκφανση της καθημερινής οικονομικής και κοινωνικής ζωής, τόσο εξαπλώνεται και η επιφάνεια (surface) για κακόβουλες και παράνομες ενέργειες. Όσο οι νέες υπηρεσίες μας επιτρέπουν μεγαλύτερη προσωποποίηση και εστίαση στις δικές μας ανάγκες, τόσο αυξάνονται οι κίνδυνοι για την εκμετάλλευση ή παραβίαση των προσωπικών μας δεδομένων. Όσο ευχερέστερη καθίσταται η επικοινωνία μας με φίλους και συνεργάτες σε όλο τον πλανήτη, τόσο εξίσου εύκολη μπορεί να καταστεί η αξιοποίηση της έκθεσής μας σε ιστότοπους κοινωνικής δικτύωσης (socialnetworking) για την πραγματοποίηση έκνομων ενεργειών. Πρόκειται για ελάχιστα παραδείγματα, που καταδεικνύουν ότι όχι μόνο η ίδια η τεχνολογία, αλλά κυρίως ο τρόπος που τη χρησιμοποιούμε, κρύβουν κινδύνους. Για τους λόγους αυτούς, ο σχεδιασμός και η εφαρμογή μιας ολιστικής Στρατηγικής Κυβερνοασφάλειας, οφείλουν να εστιάζουν στη διαρκή εισροή γνώσης και κατανόησης των σύγχρονων τεχνολογικών εξελίξεων, την πρόβλεψη ειδικών δικλείδων ασφαλείας, αλλά και τη διαρκή

ενημέρωση και ευαισθητοποίηση των χρηστών στο πλαίσιο της προαγωγής της κυβερνο-υγιεινής (cyber-hygiene).

5.1 Ευρωπαϊκός Οργανισμός ENISA και PESCO για την καταπολέμηση κυβερνοαπειλών το 2022

Σύμφωνα με το επίσημο φύλλο της εφημερίδας της Ευρωπαϊκής Ενώσεως συστάθηκε επιτροπή για την ασφάλεια στον κυβερνοχώρο με σκοπό την προστασία των προκλήσεων στον τομέα της κυβερνοασφάλειας. Στην επίσημη ιστοσδελίδα της επιτροπής της Ευρωπαικής Ενωσεως παρουσιάζονται αναλυτικά οι δραστηριότητες για την ασφάλεια και προστασία των πληροφοριών μέσω της χρήσης του διαδικτύου.

- να ενισχύσει την κυβερνοανθεκτικότητα
- να καταπολεμήσει το κυβερνοέγκλημα
- να ενισχύσει την κυβερνοδιπλωματία
- να ενδυναμώσει την κυβερνοάμυνα
- να τονώσει την έρευνα και την καινοτομία
- να προστατεύσει τις υποδομές ζωτικής σημασίας

Παρά το γεγονός πως η πρόοδος της τεχνολογίας και η ανάγκη για ψηφιοποίησης όλων των κρατικών υπηρεσιών θεωρείται θεμελιώδη στοιχείο για την σύσταση ενός εκσυγχρονισμένου κράτους. Ο κυβερνητικός μηχανισμός έρχεται αντιμέτωπος με κινδύνους κυβερνοαπειλών και κυβερνοεγκλημάτων. Ωστόσο για την αντιμετώπιση τους τον Οκτώβριο του 2020 οι ηγέτες και οι ηγέτιδες της ΕΕ ζήτησαν να ενισχυθεί η ικανότητα της ΕΕ:

- να αυτοπροστατεύεται από κυβερνοαπειλές
- να παρέχει ασφαλές περιβάλλον επικοινωνίας, ιδίως μέσω της κβαντικής κρυπτογράφησης
- να διασφαλίζει την πρόσβαση σε δεδομένα για δικαστικούς σκοπούς και για σκοπούς επιβολής του νόμου

Τον Δεκέμβριο του 2020 η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) παρουσίασαν μια νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια. Στόχος της στρατηγικής αυτής είναι να ενισχυθεί η ανθεκτικότητα της Ευρώπης απέναντι στις κυβερνοαπειλές και να μπορέσουν να ωφεληθούν πλήρως όλοι οι πολίτες και οι επιχειρήσεις από έγκυρες και αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία. Η νέα στρατηγική περιλαμβάνει συγκεκριμένες προτάσεις για τη χρήση κανονιστικών και επενδυτικών μέσων καθώς και μέσων πολιτικής.

Στις 22 Μαρτίου 2021, το Συμβούλιο ενέκρινε συμπεράσματα σχετικά με τη στρατηγική κυβερνοασφάλειας, υπογραμμίζοντας ότι η κυβερνοασφάλεια είναι αναγκαία για μια ανθεκτική, πράσινη και ψηφιακή Ευρώπη. Οι υπουργοί της ΕΕ έθεσαν ως βασικό στόχο την επίτευξη στρατηγικής αυτονομίας με διατήρηση μιας ανοικτής οικονομίας. Στο πλαίσιο αυτό περιλαμβάνεται η ενίσχυση της ικανότητας για αυτόνομες επιλογές στον τομέα της κυβερνοασφάλειας με σκοπό να ενισχυθεί ο ηγετικός ρόλος της ΕΕ στον ψηφιακό τομέα και οι στρατηγικές της ικανότητες.

Η κοινή ανακοίνωση υπογραμμίζει τον ισχυρό εσωτερικό-εξωτερικό δεσμό για την ασφάλεια στον κυβερνοχώρο και εξισορροπεί ταυτόχρονα την τεχνολογική κυριαρχία και την ανάγκη για διεθνή συνεργασία. Η νέα Στρατηγική Κυβερνοασφάλειας καλύπτει πέντε τομείς πολιτικής με περισσότερες από 20 συγκεκριμένες προτάσεις που συμβάλλουν σε μια ισχυρότερη Ευρώπη στον κυβερνοχώρο, όπως:

- Ενίσχυση της διεθνούς ασφάλειας για τη συμβολή στην υπεύθυνη συμπεριφορά του κράτους στον κυβερνοχώρο.
- Ενίσχυση της εργαλειοθήκης της ΕΕ για την κυβερνοδιπλωματία για την πρόληψη, την αποτροπή και την απόκριση σε κυβερνοεπιθέσεις·

- Ενίσχυση του συντονισμού και της συνεργασίας για την άμυνα στον κυβερνοχώρο και οικοδόμηση ικανοτήτων άμυνας στον κυβερνοχώρο·
- Ενίσχυση και επέκταση διεθνών συνεργασιών και ανταλλαγών με διεθνείς οργανισμούς, χώρες εταίρους και την κοινωνία των πολιτών, τον ακαδημαϊκό κόσμο και τον ιδιωτικό τομέα·
- Αύξηση του εύρους, της κλίμακας, της αποτελεσματικότητας και της αποδοτικότητας της εξωτερικής ανάπτυξης ικανοτήτων στον κυβερνοχώρο της ΕΕ.

Η νέα Στρατηγική Κυβερνοασφάλειας στοχεύει στη διασφάλιση ενός παγκόσμιου και ανοιχτού Διαδικτύου, ενώ ταυτόχρονα προσφέρει εγγυήσεις, όχι μόνο για τη διασφάλιση της ασφάλειας αλλά και για την προστασία των ευρωπαϊκών αξιών και των θεμελιωδών δικαιωμάτων όλων. Με βάση τα επιτεύγματα των τελευταίων μηνών και ετών, περιέχει συγκεκριμένες προτάσεις για ρυθμιστικές, επενδυτικές και πολιτικές πρωτοβουλίες, σε τρεις τομείς δράσης της ΕΕ.

Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγεσία. Στο πλαίσιο αυτού του σκέλους δράσης, η Επιτροπή προτείνει τη μεταρρύθμιση των κανόνων για την ασφάλεια των συστημάτων δικτύων και πληροφοριών, στο πλαίσιο μιας οδηγίας για μέτρα για υψηλό κοινό επίπεδο ασφάλειας στον κυβερνοχώρο σε ολόκληρη την Ένωση (αναθεωρημένη οδηγία NIS ή «NIS 2»), προκειμένου να αυξηθεί το επίπεδο ανθεκτικότητας στον κυβερνοχώρο κρίσιμων δημόσιων και ιδιωτικών τομέων: νοσοκομεία, ενεργειακά δίκτυα, σιδηρόδρομοι, αλλά και κέντρα δεδομένων, δημόσιες διοικήσεις, ερευνητικά εργαστήρια και κατασκευή κρίσιμων ιατρικών συσκευών και φαρμάκων, καθώς και άλλες κρίσιμες υποδομές και υπηρεσίες, πρέπει να παραμείνει αδιαπέραστο , σε ένα όλο και πιο γρήγορα κινούμενο και πολύπλοκο περιβάλλον απειλής. Η Επιτροπή προτείνει επίσης τη δημιουργία ενός δικτύου Επιχειρησιακών Κέντρων Ασφάλειας σε ολόκληρη την ΕΕ, που θα τροφοδοτούνται από τεχνητή νοημοσύνη (AI), το οποίο θα αποτελέσει μια πραγματική «ασπίδα ασφάλειας στον κυβερνοχώρο» για την ΕΕ, ικανή να ανιχνεύσει σημάδια κυβερνοεπίθεσης αρκετά νωρίς και να επιτρέψει την προληπτική δράση, πριν προκληθεί βλάβη. Πρόσθετα μέτρα θα περιλαμβάνουν την αποκλειστική υποστήριξη των μικρομεσαίων επιχειρήσεων (ΜΜΕ), στο πλαίσιο των Κόμβων Ψηφιακής Καινοτομίας , καθώς και αυξημένες προσπάθειες για την αναβάθμιση του εργατικού δυναμικού, την προσέλκυση και διατήρηση των καλύτερων ταλέντων στον τομέα της κυβερνοασφάλειας και την επένδυση στην έρευνα και την καινοτομία που είναι ανοιχτή, ανταγωνιστικές και βασισμένες στην αριστεία. Αδιαμφισβήτητα η δημιουργία επιχειρησιακής ικανότητας για πρόληψη, αποτροπή και αντίδραση
Η Επιτροπή προετοιμάζει, μέσω μιας προοδευτικής και χωρίς αποκλεισμούς διαδικασίας με τα κράτη μέλη, μια νέα κοινή μονάδα κυβερνοχώρου, για την ενίσχυση της συνεργασίας μεταξύ των οργάνων της ΕΕ και των αρχών των κρατών μελών που είναι αρμόδιες για την πρόληψη, την αποτροπή και την απόκριση σε κυβερνοεπιθέσεις, συμπεριλαμβανομένων των μη στρατιωτικών, της επιβολής του νόμου. κοινότητες διπλωματικής και κυβερνοάμυνας. Η Ύπατη Εκπρόσωπος υποβάλλει προτάσεις για την ενίσχυση της εργαλειοθήκης κυβερνοδιπλωματίας της ΕΕ για την πρόληψη, την αποθάρρυνση, την αποτροπή και την αποτελεσματική απάντηση σε κακόβουλες δραστηριότητες στον κυβερνοχώρο, ιδίως εκείνες που επηρεάζουν τις κρίσιμες υποδομές, τις αλυσίδες εφοδιασμού, τους δημοκρατικούς θεσμούς και τις διαδικασίες μας. Η ΕΕ θα επιδιώξει επίσης να ενισχύσει περαιτέρω τη συνεργασία στον κυβερνοχώρο άμυνας και να αναπτύξει υπερσύγχρονες ικανότητες άμυνας στον κυβερνοχώρο,Ευρωπαϊκό Ταμείο Άμυνας.

Η προώθηση ενός παγκόσμιου και ανοιχτού κυβερνοχώρου μέσω της αυξημένης συνεργασίας θεωρείται βασικό στοιχείο για την θεμελίωση ενός ασφαλούς συστήματος προστασίας δεδομένων.Η ΕΕ θα εντείνει τη συνεργασία με διεθνείς εταίρους για την ενίσχυση της παγκόσμιας τάξης που βασίζεται σε κανόνες, την προώθηση της διεθνούς ασφάλειας και σταθερότητας στον κυβερνοχώρο και την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στο Διαδίκτυο. Θα προωθήσει διεθνείς κανόνες και πρότυπα που αντικατοπτρίζουν αυτές τις βασικές αξίες της ΕΕ, συνεργαζόμενος με τους διεθνείς εταίρους της στα Ηνωμένα Έθνη και άλλα σχετικά φόρουμ. Η ΕΕ θα ενισχύσει περαιτέρω την

εργαλειοθήκη της ΕΕ για την κυβερνοδιπλωματία και θα αυξήσει τις προσπάθειες ανάπτυξης ικανοτήτων στον κυβερνοχώρο σε τρίτες χώρες αναπτύσσοντας ένα εξωτερικό θεματολόγιο της ΕΕ για την ανάπτυξη ικανότητας στον κυβερνοχώρο. Θα ενταθούν οι διάλογοι στον κυβερνοχώρο με τρίτες χώρες, περιφερειακούς και διεθνείς οργανισμούς καθώς και με την πολυμερή κοινότητα. Η ΕΕ θα σχηματίσει επίσης ένα Δίκτυο Κυβερνοδιπλωματίας της ΕΕ σε όλο τον κόσμο για να προωθήσει το όραμά της για τον κυβερνοχώρο. Η ΕΕ έχει δεσμευτεί να υποστηρίξει τη νέα Στρατηγική Κυβερνοασφάλειας με ένα άνευ προηγουμένου επίπεδο επενδύσεων στην ψηφιακή μετάβαση της ΕΕ κατά τα επόμενα επτά χρόνια, μέσω του επόμενου μακροπρόθεσμου προϋπολογισμού της ΕΕ, ιδίως του προγράμματος Digital Europe και του Horizon Europe , καθώς και της Ανάκαμψης Σχέδιο για την Ευρώπη . Ως εκ τούτου, τα κράτη μέλη ενθαρρύνονται να κάνουν πλήρη χρήση της διευκόλυνσης ανάκαμψης και ανθεκτικότητας της ΕΕ για την ενίσχυση της ασφάλειας στον κυβερνοχώρο και την αντιστοίχιση των επενδύσεων σε επίπεδο ΕΕ. Ο στόχος είναι να φτάσουμε έως και 4,5 δισεκατομμύρια ευρώ συνδυασμένων επενδύσεων από την ΕΕ, τα κράτη μέλη και τον κλάδο, ιδίως στο πλαίσιο του Κέντρου Αρμοδιοτήτων για την Κυβερνοασφάλεια και του Δικτύου Κέντρων Συντονισμού , και να διασφαλιστεί ότι ένα μεγάλο μέρος θα φτάσει στις ΜΜΕ.Η Επιτροπή στοχεύει επίσης στην ενίσχυση των βιομηχανικών και τεχνολογικών ικανοτήτων της ΕΕ στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων μέσω έργων που υποστηρίζονται από κοινού από κοινοτικούς και εθνικούς προϋπολογισμούς. Η ΕΕ έχει τη μοναδική ευκαιρία να συγκεντρώσει τα πλεονεκτήματά της για να ενισχύσει τη στρατηγική της αυτονομία και να προωθήσει την ηγεσία της στον τομέα της κυβερνοασφάλειας σε ολόκληρη την ψηφιακή αλυσίδα εφοδιασμού (συμπεριλαμβανομένων δεδομένων και cloud, τεχνολογιών επεξεργαστών επόμενης γενιάς, εξαιρετικά ασφαλούς συνδεσιμότητας και δικτύων 6G), σύμφωνα με αξίες και προτεραιότητες.

Σύμφωνα με τον οργανισμό ECSM και την ετήσια εκστρατεία ευαισθητοποίησης για την κυβερνοασφάλεια που συντονίζεται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και υποστηρίζεται από την Ευρωπαϊκή Επιτροπή, τα κράτη μέλη της ΕΕ, την Ευρωπόλ, την Ευρωπαϊκή Κεντρική Τράπεζα, τις χώρες της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών (ΕΖΕΣ) και περισσότερους από 300 εταίρους από τον δημόσιο και τον ιδιωτικό τομέα. Η εκστρατεία διάρκειας ενός μήνα προωθεί επικαιροποιημένες συστάσεις για την κυβερνοασφάλεια με σκοπό την οικοδόμηση εμπιστοσύνης στις διαδικτυακές υπηρεσίες και την υποστήριξη των πολιτών όσον αφορά την προστασία των προσωπικών, οικονομικών και επαγγελματικών τους δεδομένων στο διαδίκτυο. Η Margrethe Vestager, Εκτελεστική Αντιπρόεδρος για μια Ευρώπη έτοιμη για την ψηφιακή εποχή, δήλωσε: «Δεν θα χρησιμοποιήσουμε την τεχνολογία αν δεν την εμπιστευτούμε. και η εμπιστοσύνη προέρχεται από την αίσθηση ασφάλειας. Αυτός είναι ο λόγος για τον οποίο η κυβερνοασφάλεια είναι πραγματικά κεντρική για την ψηφιοποίηση μας και για τη χρήση της τεχνολογίας. Ειδικά στις μέρες μας όταν λόγω της πανδημίας κάναμε τόσα πολλά πράγματα στο διαδίκτυο: εργασία, μάθηση, ψώνια και πολλά άλλα. Υιοθετώντας καλές συνήθειες στον κυβερνοχώρο, χτίζουμε μια ασφαλή και ασφαλή ψηφιακή ζωή». Ο αντιπρόεδρος της Ευρωπαϊκής Επιτροπής για την Προώθηση του Ευρωπαϊκού Τρόπου Ζωής μας, Μαργαρίτης Σχοινάς, δήλωσε: «Οι κυβερνοεπιθέσεις θέτουν σε κίνδυνο τις επιχειρήσεις μας, τις υποδομές ζωτικής σημασίας, τα δεδομένα μας και τη λειτουργία των δημοκρατιών μας. Οι κυβερνοεγκληματίες εκμεταλλεύονται την παραμικρή τρωτότητα στο ψηφιακό μας περιβάλλον. Η εκστρατεία ECSM έχει ως στόχο να βοηθήσει όλους μας να αποκτήσουμε τις απαραίτητες δεξιότητες για να προστατεύσουμε τον εαυτό μας και τον τρόπο ζωής μας κατά των κυβερνοαπειλών. Το σύνθημα της εκστρατείας «Σκέψου πριν κάνεις κλικ!» είναι φέτος πιο επίκαιρο από ποτέ.»Ο εκτελεστικός διευθυντής του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια, Juhan Lepassaar, δήλωσε: «Στόχος της φετινής εκστρατείας ECSM είναι να προσφέρει στους πολίτες της ΕΕ τις πληροφορίες που θα πρέπει να χρησιμοποιούν στην καθημερινότητά τους και να τους παρέχει συμβουλές για την προστασία από κυβερνοαπειλές. Συνεργαζόμαστε με τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ για την προώθηση της ευαισθητοποίησης σχετικά με αυτές τις απειλές και για την οικοδόμηση μιας αξιόπιστης και

κυβερνοασφαλούς Ευρώπης.» Η πανδημία COVID-19 υπογράμμισε τη σημασία της κυβερνοασφάλειας. Σήμερα, περισσότερο από ποτέ, η εκπαίδευση σχετικά με την ψηφιακή ασφάλεια είναι καίριας σημασίας προκειμένου οι πολίτες να εντοπίζουν τους κινδύνους και να αντιδρούν αποτελεσματικά στις κυβερνοαπειλές. Κάθε χρόνο, καθ' όλη τη διάρκεια του Οκτωβρίου, ο ECSM φέρνει σε επαφή πολίτες της ΕΕ, κράτη μέλη, την Ευρωπαϊκή Επιτροπή, φορείς της ΕΕ και κυβερνητικούς οργανισμούς, τον ιδιωτικό τομέα και την ακαδημαϊκή κοινότητα με σκοπό την προώθηση καλών συνηθειών κυβερνοασφάλειας με το σύνθημα «Σκέψου πριν κάνεις κλικ!». Σ' όλη την Ευρώπη και πέραν αυτής, διοργανώνονται διαδικτυακές δραστηριότητες, συμπεριλαμβανομένων προγραμμάτων κατάρτισης, συνεδρίων, κουίζ, παρουσιάσεων και εθνικών εκστρατειών, με σκοπό την ενίσχυση της ευαισθητοποίησης σχετικά με τους κινδύνους κυβερνοασφάλειας και την ανταλλαγή επικαιροποιημένων κατευθυντήριων γραμμών και συμβουλών για τον μετριασμό των εν λόγω κινδύνων. Η φετινή εκστρατεία ECSM θα ασχοληθεί εκ νέου με την αντιμετώπιση ζητημάτων ασφάλειας που αφορούν την ψηφιοποίηση της καθημερινής ζωής, η οποία επιταχύνθηκε λόγω της πανδημίας COVID-19. Η εκστρατεία του 2021, η οποία ενθαρρύνει τους πολίτες να «σκέφτονται πριν κάνουν κλικ», παρουσιάζει δύο θεματικές σχετικά με την κυβερνοασφάλεια με σκοπό να βοηθήσει τους πολίτες της ΕΕ να αναγνωρίζουν τις κυβερνοαπειλές και να προετοιμάζονται για αυτές. Η πρώτη θεματική επικεντρώνεται στην πρωτοβουλία *«Προστατέψου από κυβερνοαπειλές στο σπίτι»* και παρέχει συμβουλές σχετικά με το πώς μπορούμε να παραμείνουμε ασφαλείς στον κυβερνοχώρο κατά την πραγματοποίηση διαδικτυακών συναλλαγών, την επικοινωνία, την εργασία ή τις σπουδές μέσω διαδικτύου. Θα παρέχονται συμβουλές καλής κυβερνουγιεινής όσον αφορά τις καθημερινές δραστηριότητες στο διαδίκτυο. Η δεύτερη θεματική παρέχει κατευθυντήριες γραμμές *«πρώτων βοηθειών»* σχετικά με τις ενέργειες που πρέπει να γίνουν σε περίπτωση κυβερνοσυμβάντος. Στόχος αυτής της θεματικής είναι να ενθαρρύνει τους πολίτες να έχουν αυξημένη εγρήγορση σχετικά με τις πιο κοινές κυβερνοαπειλές και να τους παρέχει συμβουλές σχετικά με τον τρόπο αντίδρασης σε περίπτωση που πέσουν θύματα απάτης στις διαδικτυακές αγορές, σε περίπτωση που έχει διακυβευτεί η ασφάλεια της πιστωτικής κάρτας και/ή του τραπεζικού λογαριασμού τους και έχει παραβιαστεί ο λογαριασμός τους στα μέσα κοινωνικής δικτύωσης. Οι πραγματικές ιστορίες των θυμάτων θα κοινοποιηθούν υπό μορφή συνεντεύξεων και βίντεο.Φέτος, ο ECSM ενώνει τις δυνάμεις του με τον ευρωπαϊκό διαγωνισμό κυβερνοασφάλειας (ECSC) — η νικήτρια ομάδα του ECSC 2021 θα είναι η πρέσβειρα της φετινής εκστρατείας ECSM.Ο επίσημος ιστότοπος της εκστρατείας ECSM είναι cybersecuritymonth.eu. Ο ιστότοπος λειτουργεί ως κόμβος πληροφοριών για την κυβερνοασφάλεια και περιλαμβάνει μία σελίδα για την καταχώριση δραστηριοτήτων που σχετίζονται με την ευαισθητοποίηση του κοινού, καθώς και ειδικό υλικό της εκστρατείας των κρατών μελών σε κάθε γλώσσα (εκπροσωπούνται και οι 24 επίσημες γλώσσες της ΕΕ), όπως και οι οπτικές κατευθυντήριες γραμμές της εκστρατείας για τηλεφόρτωση. Ο ιστότοπος του ECSM περιλαμβάνει επίσης ένα κουίζ για την κυβερνοασφάλεια, το οποίο επιτρέπει στους χρήστες να δοκιμάσουν τις γνώσεις τους, καθώς και έναν διαδραστικό χάρτη των συμμετεχουσών χωρών, με πληροφορίες σχετικά με τις υπηρεσίες που είναι διαθέσιμες σε κάθε χώρα για την παροχή συμβουλών και την υποβολή καταγγελίας σε περίπτωση κυβερνοεπίθεσης.

- ENISA

Ο ENISA είναι προσηλωμένος στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Οργανισμός συνεργάζεται με οργανώσεις και επιχειρήσεις για να ενισχύσει την εμπιστοσύνη στη ψηφιακή οικονομία, να τονώσει την ανθεκτικότητα των υποδομών της Ευρωπαϊκής Ένωσης και να διατηρήσει, τελικά, την ψηφιακή ασφάλεια για τους πολίτες της Ευρωπαϊκής Ένωσης. Αυτό το επιτυγχάνει μέσω της ανταλλαγής γνώσεων, της ανάπτυξης προσωπικού και δομών και της αύξησης της ευαισθητοποίησης. Η πράξη της ΕΕ για την κυβερνοασφάλεια έχει ενισχύσει το έργο του Οργανισμού. Τα τελευταία χρόνια ο οργανισμός κατέχει βασικό ρόλο στις διακρατικές σχέσεις σε περιπτώσεις παραβίασης των ορίων στον κυβερνοχώρο. Ο ENISA λειτουργεί κυρίως προς όφελος των δημόσιων οργανισμών όπως

παραδείγματος χάρη για την προστασία των αρχών, των θεσμικών οργάνων και των αποκεντρωμένων οργάνων και οργανισμών των χωρών της ΕΕ. ΕΠίσης σημαντική χαρακτηριζεται η συμβολή του οργανισμού στα θεσμικα και λοιπά οργανα και των οργανισμών της ΕΕ.Ο Οργανισμός βοηθά επίσης κατά βάσει στον κλάδο των ΤΠ (τηλεπικοινωνίες, παρόχους υπηρεσιών διαδικτύου και εταιρείες ΤΠ), στην επιχειρηματική κοινότητα – ιδίως μικρές και μεσαίες επιχειρήσεις, τους εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας (π.χ. ομάδες αντιμετώπισης κυβερνοπεριστατικών), την ακαδημαϊκή κοινότητα και τέλος το κοινό.

- PESCO

Κομβικής σημασίας για την ενίσχυση του περιβάλλοντος ασφάλειας της Ένωσης είναι η επιτυχής πρωτοβουλία για την αντιμετώπιση των προβλημάτων στην κυβερνοασφάλεια υπό τον τίτλο Μόνιμη Δομημένη Συνεργασία ή Permanent Structured Cooperation (PESCO). Η PESCO αποτελεί τμήμα της Παγκόσμιας Στρατηγικής της ΕΕ για την πολιτική ασφαλείας της και εμπίπτει, συνεπώς, στον τομέα της εξωτερικής πολιτικής της. Αναλυτικότερα, στις 13 Νοεμβρίου 2017, Υπουργοί Εξωτερικών και Άμυνας από 23 κράτη μέλη υπέγραψαν κοινή ανακοίνωση για τη Μόνιμη Δομημένη Συνεργασία (Μ.Δ.Σ.-PESCO) και την απέστειλαν στην Ύπατο Εκπρόσωπο και στο Συμβούλιο. Την κοινή αυτή ανακοίνωση προσυπέγραψαν δύο επιπλέον χώρες στις 7 Δεκεμβρίου 2017. Τα 25 κράτη – μέλη είναι: Αυστρία, Βέλγιο, Βουλγαρία, Τσεχική Δημοκρατία, Κροατία, Κύπρος, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Ολλανδία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβενία, Σλοβακία, Ισπανία, Ιρλανδία και Σουηδία. Η δυνατότητα της Μόνιμης Διαρθρωμένης Συνεργασίας στον τομέα της ασφάλειας και αμυντικής πολιτικής εισήχθη με τη Συνθήκη της Λισαβόνας και προβλέπει τη δυνατότητα περισσότερων κρατών μελών της ΕΕ να συνεργάζονται στενότερα στον τομέα της ασφάλειας και της άμυνας. Υπό το πρίσμα ενός μεταβαλλόμενου περιβάλλοντος ασφαλείας, η ΕΕ στο πλαίσιο της παγκόσμιας στρατηγικής για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (EUGS), ξεκίνησε μια διαδικασία ενισχυμένης συνεργασίας για την ασφάλεια και την άμυνα. Τα κράτη μέλη συμφώνησαν η Ευρωπαϊκή Ένωση να εντείνει τις εργασίες της στον τομέα αυτό και αναγνώρισαν ότι ο ενισχυμένος συντονισμός, οι αυξημένες επενδύσεις στην άμυνα και η συνεργασία στην ανάπτυξη των αμυντικών δυνατοτήτων, είναι οι βασικές απαιτήσεις για την επίτευξή του. Μέσω PESCO, τα κράτη μέλη αυξάνουν την αποτελεσματικότητά τους στην αντιμετώπιση των προκλήσεων ασφαλείας, προχωρώντας προς την περαιτέρω ενσωμάτωση και ενίσχυση της αμυντικής τους συνεργασίας, εντός του πλαισίου της ΕΕ.

• Η Μ.Δ.Σ - PESCO είναι ένα μόνιμο πλαίσιο για στενότερη λειτουργία και μια δομημένη διαδικασία για σταδιακή εμβάθυνση της αμυντικής συνεργασίας στο πλαίσιο της Ένωσης. Θα είναι ένας οδηγός για ολοκλήρωση στον τομέα της άμυνας.

• Κάθε συμμετέχον κράτος μέλος παρέχει ένα σχέδιο για τις εθνικές συνεισφορές και τις προσπάθειες, που έχει συμφωνήσει να κάνει. Αυτά τα εθνικά σχέδια εφαρμογής υπόκεινται σε τακτική αξιολόγηση. Αυτό που είναι διαφορετικό από την εθελοντική προσέγγιση είναι, ο κανόνας εντός της Ευρωπαϊκής Ένωσης κοινής ασφάλειας και αμυντικής πολιτικής.

• Η Μ.Δ.Σ - PESCO σχεδιάζεται για να καταστεί αποτελεσματικότερη η ευρωπαϊκή άμυνα και να παρέχει μεγαλύτερη απόδοση, παρέχοντας ενισχυμένο συντονισμό και συνεργασία στους τομείς των επενδύσεων, την ανάπτυξη δυνατοτήτων και την επιχειρησιακή ετοιμότητα. Η ενισχυμένη συνεργασία σε αυτόν τον τομέα θα επιτρέψει, μειώνοντας τον αριθμό των διαφορετικών οπλικών συστημάτων στην Ευρώπη και ως εκ τούτου, ενισχύοντας την επιχειρησιακή συνεργασία μεταξύ των κρατών μελών, να αυξάνουν τη διαλειτουργικότητα και τη βιομηχανική ανταγωνιστικότητα.

• Η Μ.Δ.Σ - PESCO θα βοηθήσει να ενισχυθεί η στρατηγική αυτονομία της ΕΕ να δράσει μόνη της, όταν είναι απαραίτητο και με συνεργάτες οσάκις είναι δυνατόν. Ενισχύεται από την ιδέα ότι η κυριαρχία μπορεί να ασκείται καλύτερα όταν εργάζονται από κοινού, ενώ η εθνική κυριαρχία παραμένει ουσιαστικά άθικτη.

• Πρόκειται για παροχή μιας ομπρέλας τέτοιων παραδειγμάτων περιφερειακής αμυντικής ολοκλήρωσης όπως το Ναυτικό Βελγίου – Ολλανδίας ή της Διοίκησης Ευρωπαϊκής Αερομεταφοράς.

• Στρατιωτικές ικανότητες, που αναπτύχθηκαν εντός PESCO παραμένουν στα χέρια των κρατών μελών, οι οποίες μπορούν επίσης να γίνουν διαθέσιμες σε άλλα πλαίσια, όπως τα Ηνωμένα Έθνη ή το ΝΑΤΟ. Η Μ.Δ.Σ. - PESCO συνδέεται στενά με τη νέα συντονισμένη ετήσια αναθεώρηση άμυνας (CARD - Coordinated Annual Review on Defence) και το Ευρωπαϊκό Ταμείο Άμυνας (ΕΤΑ), το οποίο αναπτύσσεται επί του παρόντος στο πλαίσιο του προγράμματος της Ευρωπαϊκής Αμυντικής Βιομηχανικής ανάπτυξης. Είναι συμπληρωματικά και αμοιβαία ενισχυόμενα εργαλεία, που συμβάλλουν στον ίδιο πολιτικό στόχο:

• Coordinated Annual Review on Defence (CARD) πρέπει να εκτελεστούν από τον Ευρωπαϊκό Οργανισμό Άμυνας, μέσα από συστηματική παρακολούθηση των σχεδίων των εθνικών αμυντικών δαπανών και βοηθούν στον εντοπισμό ευκαιριών για νέες πρωτοβουλίες συνεργασίας.

• Το ΕΤΑ θα παρέχει οικονομικά κίνητρα για την προώθηση της αμυντικής συνεργασίας από την έρευνα στη φάση της ανάπτυξης των ικανοτήτων, περιλαμβανομένων των πρωτοτύπων.

• Η Μ.Δ.Σ - PESCO θα αναπτύξει ικανότητα έργων, ταυτοποιημένων ιδίως μέσω της διαδικασίας της CARD σε τομείς προτεραιότητας. Επιλέξιμα έργα θα μπορούσαν επίσης να επωφεληθούν από χρηματοδότηση από το ΕΤΑ, το οποίο θα προβλέπει ένα πρόσθετο 10% χρηματοδότηση για τη φάση της βιομηχανικής ανάπτυξης άμυνας των έργων, που αναπτύχθηκαν στο πλαίσιο της Μ.Δ.Σ. - PESCO.

5.3 Νομοθετικό πλαίσιο, πολιτικές και πρακτικές στην Ελλάδα και την Κύπρο

Το πρώτο νομοθέτημα, που θεσπίστηκε για να αντιμετωπίσει το φαινόμενο της τρομοκρατίας, ήταν ο νόμος 774/1978 «περί καταστολής της τρομοκρατίας και προστασίας του δημοκρατικού πολιτεύματος», στον οποίο δεν υπήρχε ορισμός της τρομοκρατίας, αλλά μόνον μια γενική αναφορά στον όρο «ομάδα». Δεύτερο νομοθέτημα ήταν αυτό του Ν. 1916/1990 με τίτλο «για την προστασία της κοινωνίας από το οργανωμένο έγκλημα», όπου δε γινόταν λόγος ούτε για οργανωμένο έγκλημα, παρά τον οξύμωρο τίτλο του, ενώ έλειπαν από τις αξιόποινες πράξεις του εντελώς τα οικονομικά εγκλήματα, που χαρακτηρίζουν κατ' εξοχήν την οργανωμένη εγκληματικότητα και που αργότερα καταργήθηκε με τον ν. 2172/1993. Ακολούθησαν ο Ν. 2928/2001 και 3251/2004, ενώ με τον τελευταίο δημιουργείται αυτοτελές τρομοκρατικό αδίκημα, χωρίς την προϋπόθεση ύπαρξης οργάνωσης ή ομάδας. Η βασική καινοτομία του Ν. 3251/2004 συνίσταται στην εισαγωγή για πρώτη φορά στο ελληνικό δίκαιο του ευρωπαϊκού εντάλματος σύλληψης, ενώ δια του νόμου αυτού η ελληνική έννομη τάξη επιχειρεί να συμμορφωθεί στην ουσία με την απόφαση – πλαίσιο της Ευρωπαϊκής Ένωσης 2002/584/ΔΕΥ, όπως ίσχυε μετά την τροποποίηση από την απόφαση – πλαίσιο 2009/299/ΔΕΥ και να ενσωματώσει, περαιτέρω, τις Οδηγίες 2012/13/ΕΕ και 2013/48/ΕΕ για την αντιμετώπιση της τρομοκρατίας. Τυποποιούνται πλέον ως τρομοκρατικές πράξεις μια σειρά από κοινά εγκλήματα (πράξεις ποινικά κολάσιμες κατά τις διατάξεις του Ειδικού Μέρους του ΠΚ), εφόσον αυτά χαρακτηρίζονται από ένα αντικειμενικό στοιχείο, ότι δηλαδή τελούνται με τρόπο, σε έκταση ή υπό συνθήκες που είναι δυνατόν να βλάψουν σοβαρά μία χώρα ή έναν διεθνή οργανισμό και από ένα υποκειμενικό στοιχείο, ότι δηλαδή τελούνται με σκοπό να εκφοβίσουν σοβαρά έναν πληθυσμό, να εξαναγκάσουν μία δημόσια αρχή ή έναν διεθνή οργανισμό να εκτελέσει οποιαδήποτε πράξη ή να απόσχει από αυτήν ή να βλάψουν σοβαρά ή να καταστρέψουν τις θεμελιώδεις συνταγματικές, πολιτικές, οικονομικές

δομές μιας χώρας ή ενός διεθνούς οργανισμού. Τα εγκλήματα των άρθρων 187 Α και 187 Β ΠΚ Σε συμμόρφωση με την Οδηγία (ΕΕ) 2017/541 του ΕΚ και του Συμβουλίου της Ευρώπης, η οποία ενσωματώθηκε στην ελληνική νομοθεσία με τον Ν. 4689/2020, ποινικοποιήθηκαν νέα εγκλήματα που σχετίζονται με τρομοκρατικές δραστηριότητες. Στον ελληνικό Ποινικό Κώδικα σήμερα οι τρομοκρατικές ενέργειες και δη το έγκλημα της τρομοκρατικής οργάνωσης τυποποιούνται στο άρθρο 187 Α και 187 Β αυτού. • Άρθρο 187 Α ΠΚ Στο άρθρο αυτό προβλέπεται ότι τρομοκρατικό έγκλημα μπορεί να είναι οποιοδήποτε κακούργημα ή οποιοδήποτε κοινώς επικίνδυνο έγκλημα, εφόσον τελείται υπό συνθήκες ή με τέτοιο τρόπο ή σε τέτοια έκταση που να προκαλεί σοβαρό κίνδυνο για τη χώρα ή για διεθνή οργανισμό και με τους σκοπούς που περιγράφονται στο συγκεκριμένο άρθρο. Επέρχεται κατ' αυτό τον τρόπο μία ουσιώδης αλλαγή, η οποία συνίσταται στην κατάργηση του καταλόγου των αξιόποινων πράξεων που μπορούν να χαρακτηριστούν ως τρομοκρατικές. Σημαντική είναι και η αλλαγή που υιοθετείται για την σύσταση τρομοκρατικής οργάνωσης ή τη συμμετοχή σε αυτή. Ενώ η σύσταση της οργάνωσης ή συμμετοχή σε αυτή για την τέλεση τρομοκρατικού εγκλήματος που έχει τη μορφή κακουργήματος διατηρεί τον κακουργηματικό της χαρακτήρα και απειλείται με ποινή κάθειρξης ως δέκα έτη, η σύσταση τρομοκρατικής οργάνωσης ή η συμμετοχή σε αυτή προκειμένου να τελεστεί τρομοκρατικό έγκλημα που έχει τη μορφή πλημμελήματος αντιμετωπίζεται ως πλημμέλημα και τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους, σε αντίθεση με όσα προέβλεπε η προϊσχύσασα διάταξη, στο πλαίσιο της οποίας απειλείτο η ποινή του κακουργήματος μειωμένη στο μέτρο του άρθρου 83 ΠΚ5 . Επιπλέον, προστίθενται πλέον στο άρθρο αυτό οι παράγραφοι 4 έως 6 σε συμμόρφωση της χώρας μας προς την Απόφαση - Πλαίσιο 2008/919/ΔΕΥ του Συμβουλίου της 28ης Νοεμβρίου 2008. Στην παρ. 4 τυποποιείται, ειδικότερα, η πράξη της *(Α. Χαραλαμπάκης, Ο Νέος Ποινικός Κώδικας – Συνοπτική Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Νομική Βιβλιοθήκη, 2η έκδοση, σελ. 175)*. στρατολόγησης άλλου σε τρομοκρατική οργάνωση ή σε τέλεση τρομοκρατικών πράξεων, ενώ στην παράγραφο 5 τυποποιείται η εκπαίδευση άλλου για την τέλεση συγκεκριμένης τρομοκρατικής πράξης. Τέλος, στην παράγραφο 6 έχει μεταφερθεί η διάταξη της παρ. 3 του προϊσχύσαντος άρθρου με αρκετές αλλαγές, που ήταν αναγκαίες προκειμένου να προσδιοριστούν με μεγαλύτερη σαφήνεια τα στοιχεία της αξιόποινης συμπεριφοράς. Πιο συγκεκριμένα, στην παράγραφο αυτή τιμωρείται όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου απειλεί με τέλεση τρομοκρατικών πράξεων ή προκαλεί ή διεγείρει σε διάπραξή τους και έτσι εκθέτει σε κίνδυνο τη δημόσια τάξη. Τέλος, με τη διάταξη του άρθρου 3 παρ. 14 Ν 4637/2019, προστέθηκε στο άρθρο 187Α ΠΚ έβδομη παράγραφος, η οποία έχει ως εξής: «Με την ποινή της προηγούμενης παραγράφου τιμωρείται και όποιος με σκοπό να τελέσει ή να συμβάλει στην τέλεση τρομοκρατικού εγκλήματος, να συμμετάσχει στις δραστηριότητες τρομοκρατικής ομάδας, με επίγνωση του γεγονότος ότι η εν λόγω συμμετοχή θα συμβάλει στις εγκληματικές δραστηριότητες αυτής της ομάδας ή με σκοπό να προσφέρει ή να παρακολουθήσει εκπαίδευση για τέλεση τρομοκρατικών πράξεων, πραγματοποιεί ταξίδι το οποίο διευκολύνει την πραγμάτωση του σκοπού του». Άρθρο 187 Β ΠΚ Στο άρθρο αυτό τυποποιείται ως αυτοτελές έγκλημα η αξιόποινη υποστήριξη, μια πράξη που τυποποιείται σήμερα εν μέρει στο άρθρο 187 παρ. 2 και 4 και εν μέρει στο άρθρο 187Α παρ. 6-8 ΠΚ. Στην προτεινόμενη διάταξη, ως πρώτη μορφή αξιόποινης υποστήριξης, προβλέπεται η παροχή ουσιωδών πληροφοριών ή υλικών μέσων με σκοπό να διευκολυνθεί ή να υποβοηθηθεί εγκληματική ή τρομοκρατική οργάνωση για τη διάπραξη των επιδιωκόμενων από αυτήν κακουργημάτων. Στην παρ. 2 επαναλαμβάνεται κατά βάση αυτούσια η διάταξη του άρθρου 187Α παρ. 6 ΠΚ, ενώ στην παρ. 3 επαναλαμβάνεται η διάταξη του άρθρου 187 παρ. 4 ΠΚ, η οποία, με βάση το άρθρο 187Α παρ. 8 ΠΚ ισχύει τόσο για το τρομοκρατικό έγκλημα όσο και για τις τρομοκρατικές οργανώσεις. Αντίθετα, δεν κρίθηκε αναγκαία η αυτοτελής τυποποίηση των πράξεων που περιγράφονται στο άρθρο 187Α παρ. 7 ΠΚ (διακεκριμένη κλοπή, ληστεία, πλαστογραφία και εκβίαση). Αν από τα προϊόντα που θα προκύψουν από τις συγκεκριμένες πράξεις ενισχυθεί πράγματι η δράση των εγκληματικών ή τρομοκρατικών οργανώσεων, οι πράξεις υπάγονται ούτως ή άλλως στις προβλεπόμενες στο άρθρο 187Β του νέου ΠΚ πράξεις Με τη διάταξη του άρθρου 3 παρ. 16 Ν 4637/2019, προστέθηκε στο άρθρο 187Β νέα παρ. 4, η οποία έχει ως εξής: «Κατά την επιμέτρηση της ποινής των

εγκλημάτων της παραγράφου 1 λαμβάνονται υπόψη ως επιβαρυντικές περιστάσεις οι αμετάκλητες καταδικαστικές αποφάσεις που εκδίδουν δικαστήρια άλλων κρατών - μερών της Σύμβασης της Βαρσοβίας της 16ης Μαΐου 2005 του Συμβουλίου της Ευρώπης για τη νομιμοποίηση, ανίχνευση, κατάσχεση και δήμευση εσόδων από εγκληματικές δραστηριότητες και για τη χρηματοδότηση της τρομοκρατίας».

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

Με το άρθρο 37 του Ν. 4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις» ρυθμίζονται οι υποχρεώσεις που έχουν οι πάροχοι δικτύων/υπηρεσιών ηλεκτρονικών επικοινωνιών, για την ασφάλεια και ακεραιότητα των υπηρεσιών αυτών. Συγκεκριμένα, ο νόμος αναφέρει ρητά στο ως άνω άρθρο ότι οι πάροχοι οφείλουν να λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και των υπηρεσιών, εξασφαλίζοντας ένα επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο, διασφαλίζοντας την ακώλυτη και αδιάλειπτη παροχή των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών, ενώ οφείλουν και να κοινοποιούν στην ΕΕΤΤ κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που είχαν σημαντικό αντίκτυπο στη λειτουργία των ως άνω δικτύων ή υπηρεσιών. Αρμόδια για την εποπτεία της προστασίας του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας, καθώς και της ασφάλειας των δικτύων και πληροφοριών είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών («ΑΔΑΕ»), που συστάθηκε ως ανεξάρτητη συνταγματική Αρχή με το άρθρο 1 του Ν. 3115/2003 σε εκτέλεση του άρθρου 19 § 2 του Συντάγματος. Με την υπ’ αρ. 205/2013 απόφασή της με τίτλο «Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών», όπως δημοσιεύθηκε και στο ΦΕΚ 1742/Β΄/15-7-2013, η ΑΔΑΕ εξειδίκευσε/ερμήνευσε τις διατάξεις του άρθρου 37 του Ν. 4070/2012, αναφορικά με την ασφάλεια και την ακεραιότητα των δικτύων/υπηρεσιών ηλεκτρονικών επικοινωνιών, προβλέποντας ενδεικτικά τις ακόλουθες υποχρεώσεις για τους παρόχους:

Κατάρτιση/Σχεδιασμός και τήρηση πολιτικής ασφάλειας δικτύων και υπηρεσιών.

• Διορισμός υπευθύνου ασφάλειας δικτύων και υπηρεσιών.

• Κατάρτιση/Δημιουργία και τήρηση σχεδίου έκτακτων αναγκών.

• Συμμόρφωση με πρότυπα ασφαλείας, τεχνικές διεπαφές και στοιχεία λειτουργίας δικτύων που συμφωνούνται σε Ενωσιακό επίπεδο.

• ανάλυση επιχειρησιακών επιπτώσεων και αξιολόγησης επικινδυνότητας αναφορικά με την ασφάλεια και την ακεραιότητα των δικτύων.

• Κατάρτιση/Δημιουργία/Οργάνωση και τήρηση σχεδίου επιχειρησιακής συνέχειας/αδιάλειπτης λειτουργίας.

• Διεξαγωγή ελέγχων αποτελεσματικότητας και κατάρτιση σχετικών σχεδίων και διαδικασιών (δοκιμών, penetration tests, vulnerability assessments).

• Τήρηση κατάλληλων μέτρων φυσικής και λογικής/πληροφοριακής ασφάλειας.

• Σχεδιασμός/Επιλογή και τήρηση διαδικασίας διαχείρισης περιστατικών ασφαλείας.

• Σχεδιασμός/Επιλογή και τήρηση διαδικασίας εσωτερικού ελέγχου για την ασφάλεια και την ακεραιότητα των δικτύων / υπηρεσιών.

• Τήρηση σχετικών αρχείων.

6. Αποτελέσματα βάσει θεωρητικής μελέτης και πρακτικού εμπειρικού μελετητικού πλαισίου

Όσο ενθαρρυντική και αν είναι σήμεραη ραγδαία εξέλιξη των μέσων αντιμετώπισης των κυβερνοεπιθέσεων, παρ' όλα αυτά, είναι εξαιρετικά δύσκολο να προβλεφθεί ο τρόπος με τον οποίο θα διασφαλιστεί η απόλυτη και έγκαιρη προστασία του κυβερνοχώρου, απέναντι στην συνεχως εξελισσόμενη ακτίνα δράσης της κυβερνοτρομοκρατίας. Το μόνο το οποίο είμαστε σε θέση να συμπεράνουμε με ασφάλεια, αποτελεί η διαπίστωση πως σε διεθνές επίπεδο, οι ανωτέρω προκλήσεις παρουσιάζουν πλήθος κοινών στοιχείων, χωρίς ωστόσο να μπορούν να χαρακτηριστούν ως όμοιες. Ως εκ τούτου, το υπό συζήτηση φαινόμενο, όντας διαρκώς υπό εξέλιξη, θα πρέπει να εξετάζεται συστηματικά και με ιδιαίτερη προσοχή, καθώς οι συνέπειες της κυβερνοτρομοκρατίας δεν περιορίζονται μόνο σε μία χώρα ή μία ομάδα πολιτών. Γίνεται επομένως εμφανής η σπουδαιότητα της συνεχούς ενημέρωσης και η αποφυγή λήψης μέτρων αποκλειστικά σε επίπεδο κράτους. Με γνώμονα λοιπόν την ανωτέρω διαπίστωση, αξιολογώντας την διαδικασία έρευνας για την συγγραφή της μελέτης και επιχειρώντας μία κριτική αποτίμηση των δεδομένων της, συνολικά, καθίσταται αναγκαία η επισήμανση ορισμένων διευκρινιστικών παρατηρήσεων. Παρότι η ανάλυση έδωσε έμφαση στην αποτίμηση και την κριτική σύνθεση πληροφοριών από πρωτογενείς και δευτερογενείς πηγές, η χρήση αξιόπιστων δεδομένων ήταν δυσχερής, καθώς η εύρεση διαφορετικών στοιχείων από τις πηγές που αξιοποιήθηκαν αποτέλεσε συχνό φαινόμενο. Παρόλα αυτά, τα στοιχεία που χρησιμοποιήθηκαν καθ' όλη την έκταση της εργασίας έχουν διασταυρωθεί αφότου πηγάζουν κατά βάσει από ΕΥρωπαικούς και Εθνικούς Φορείς. Επομένως, λόγω της στρατηγικής σημασίας της κυβερνοασφάλειας και της κυβερνοισχύος, η ως άνω επιφύλαξη αποτέλεσε βασικό γνώμονα κατά την εξαγωγή των συμπερασμάτων της παρούσας μελέτης. Ολοκληρώνοντας, υπογραμμίζεται πως ήταν ιδιαίτερα δύσκολη η εύρεση αξιοποιήσιμης και αξιόπιστης βιβλιογραφίας στην ελληνική γλώσσα. Με το ως άνω δεδομένο, ήταν απαραίτητη η χρήση και ανάλυση πηγών στην αγγλική, κυρίως, γλώσσα. Δεδομένου του γεγονότος ότι η πληθώρα του υλικού που εντοπίστηκε αποτελούσε αναδημοσιεύσεις, σημαντική ποσότητα πληροφοριών αποκλείστηκε και διατηρήθηκαν μόνο επίσημες πηγές ώστε να μην υπάρξει κίνδυνος ακούσιας παραπληροφόρησης.

6.1 Δημόσια Υγεία και Τεχνολογία 2.0

Σύμφωνα με τον ορισμό που δίνει ο καθηγητής εφαρμοσμένης πληροφορικής και τεχνολογιών O'Reilly "*Το Web 2.0 είναι η επιχειρηματική επανάσταση στη βιομηχανία των υπολογιστών που προκλήθηκε από τη μετάβαση στο Διαδίκτυο ως πλατφόρμα και μια προσπάθεια κατανόησης των κανόνων επιτυχίας σε αυτήν τη νέα πλατφόρμα. Ο κύριος μεταξύ αυτών των κανόνων είναι ο εξής: Δημιουργήστε εφαρμογές που αξιοποιούν τα εφέ δικτύου για να βελτιώνονται όσο περισσότεροι άνθρωποι τις χρησιμοποιούν. (Αυτό το έχω ονομάσει αλλού "εκμετάλλευση συλλογικής νοημοσύνης"*. Συμπληρωματικός ορισμός αναφορικά με το Web 2.0 είναι αυτός του επιστήμονα ιδίου κλάδου Eric Schmidt ο οποίος αναφέρει χαρακτηριστικά πως "Μην σκοπεύσεις να πολεμήσεις το διαδίκτυο". Αυτός είναι πραγματικά ένας υπέροχος τρόπος να σκεφτείς τι πρόκειται να πολεμήσεις. Σκεφτείτε βαθιά τον τρόπο που λειτουργεί το Διαδίκτυο και δημιουργήστε συστήματα και εφαρμογές που το χρησιμοποιούν πιο πλούσια , απαλλαγμένο από τους περιορισμούς της σκέψης της εποχής του υπολογιστή και είστε σε καλό δρόμο. Κατά ειρωνικό τρόπο, το αρχικό Web 1.0 του Tim Berners-Lee είναι ένα από τα πιο "Web 2.0" συστήματα εκεί έξω που αξιοποιεί πλήρως τη δύναμη του χρήστη, τη συνεισφορά, τη συλλογική νοημοσύνη και τα εφέ δικτύου.

Ερχόμενοι στις ανακοινώσεις του έλληνα Υπουργού Ψηφιακής Διακυβέρνησης για τις αλλαγές που προκύπτουν στο σύστημα υγείας έγινε αναφορά στον όρο Web 2.0 και στις χρηστικές του ιδιότητες. Αυτός ο νέος ιστός χρησιμοποιείται για να περιγράψει την νέα γενιά Παγκόσμιου Ιστού όπου πραγματοποιείται η online μέθοδος περιήγησης. Μία τέτοια τεχνολογία νέας γενιάς μπορεί να υποστήριξει τα τεχνολογικά σχέδια για την εκσυγχρόνηση του συστήματος υγείας τόσο του ελληνικού όσο και και του κυπριακού

κράτους αλλά συγχρόνως στην απλούστευση των διαδικασιών που αφορά το κομμάτι της γραφειοκρατία και της πολιτικής εξυπηρέτησης. Στον τομέα της δημόσιας υγείας η εφαρμοσμένη χρήση του Web 2.0 διευκόλυνε την ζωή μας σε μία κρίσιμη περίοδο όπως αυτή της πανδημίας. Με βάσει τα κρούσματα που καταγράφονταν καθημερινώς από τα κλιμάκια του ΕΟΔΥ και σε συνεργασία με κολοσσούς τεχνολογικών επιτευγμάτων όπως facebook και instagram μπορούσαμε να ενημερωθούμε για τυχόν επιβεβαιωμένα κρούσματα που βρίσκονται δίπλα μας, το υιικό φορτίο κάθε περιοχής αλλά και τις οδηγίες χρήσης υγειονομικής προστασίας. Στην συνέχεια οι πλατφόρμες gov.gr και keplife.gr πρόκειται για τις δύο πιο πολυεπισκεπτόμενες online ιστοσελίδες εξυπηρέτησης των πολιτών είτε με απλή πρόσβαση για το κατέβασμα ενός εγγράφου, για την δήλωση μιας αίτησης ή και ακόμα online ραντεβού με υπάλληλο της εκάστοτε δημόσιας υπηρεσίας.

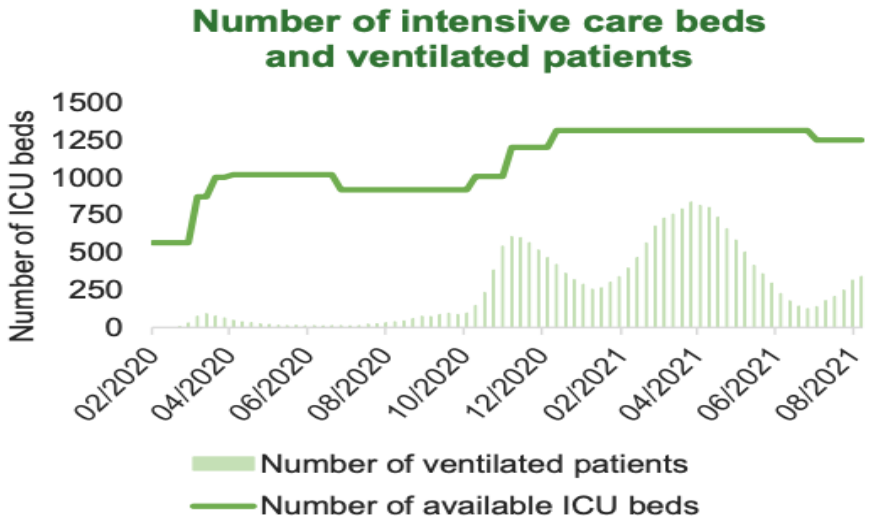
7. Προτάσεις εξέλιξης της κυβερνοασφάλειας στην δημόσια υγεία και αποτελέσματα

Με την υποστήριξη του Εθνικού Κέντρου Συντονισμού Κυβερνοασφάλειας σε συνεργασία με την Ευρωπαϊκή Ένωση έχοντας μοναδικό στόχο την προστασία των δεδομένων υγείας στον Δημόσιο Φορέα απαραίτητη θεωρείται η χρηματοδότηση κάθε συστηματος υγείας τόσο στην Ελλάδα όσο και στην Κύπρο. Με την συνεχή εξέλιξη της τεχνολογίας η προστασία των δημόσιων συστημάτων γίνεται ευκολότερη αλλά συγχρόνως πιο πολύπλοκη. Για αυτό τον λόγο η χρηματοδότηση νέων προγραμμάτων στον τομέα της κυβερνοασφάλειας τόσο στην ανάδειξη εφαρμόσιμων ιδεών δια μέσω των Ακαδημαϊκών Ιδρυμάτων όσο και στην πραγμάτωση διαγωνισμών που μπορούν να διοργανώθουν από Ιδιωτικούς και Δημόσιους Φορείς Τηλεπικοινωνιών με σκοπό την απόσπαση ιδεών από νέους επιστήμονες. Για την περίθαλψη Δημόσιων Ιδρυμάτων Κυβερνοασφάλειας με σκοπό τον περιορισμό της ζημίας κυβερνοασφάλειας τα οποία επηρεάζουν τα νοσοκομεία και τους παροχείς υπηρεσιών υγείας είναι η υποστήριξη για την υιοθέτηση εργαλείων λογισμικού, μεθόδων, πρακτικών οργάνωσης και διαχείρισης, και εκπαιδευτικού υλικού για την κυβερνοασφάλεια από τα ιδρύματα υγειονομικής περίθαλψης και τα δημόσια ιδρύματα υγείας, και κυρίως από τις μικρομεσαίες επιχειρήσεις. Εν συνεχεία ο Δημόσιος Φορέας θα μπορούσε να συνεργάζεται με Ιδιωτικές επιχειρήσεις Κυβερνοασφάλειας με σκοπό τον διαμοιρασμό του όγκου των πληροφοριών και την δυσκολία παραβίασης τους. Αυτόνομες ελληνικές είτε κυπριακές επιχειρησεις που εξειδιεκευονται σε θέματα κυβερνοασφάλειας θα μπορούσαν με μεγάλη επιτυχία να θωρακίσουν το ελληνικό είτε το κυπριακό σύστημα δημόσιας υγειας για την προστασία του από περιστατικά κυβερνοεπιθέσεων. Απαραίτητο φάινεται να είναι το γεγονός της προώθησης της εκπαίδευσης, της ευαισθητοποίησης και της ανάπτυξης δεξιοτήτων σε θέματα κυβερνοασφάλειας στα ιδρύματα υγειονομικής περίθαλψης και τα δημόσια ιδρύματα υγείας. Επιπροσθέτως η ηλεκτρονική υγεία είναι ένα πλάνο της κυβέρνησης το οποίο θα μπορούσε να λειτουργεί μέσω εφαρμογής στο κινητό είτε στον ηλεκτρονικό υπολογιστή συνδυάζοντας τις απαραίτητες επισκέψεις ασθενών είτε εξ αποστάσεως είτε δια ζώσης με την παράλληλη συνταγογράφηση φαρμάκων σε περίπτωση που χρήζει αναγκαιότητας. Σε περίπτωση νοσηλείας ασθενούς όλα τα απαραίτητα έγγραφα θα μπορούσαν να αρχειοθετούνται και να αποστέλλονται στον ασθενή μέσω παραθύρου της πλατφόρμας gov.gr με μοναδικά απαραίτητα στοιχεία τον αριθμό ΑΜΚΑ σε συνδυασμό με τα τελευταία ψηφία του αριθμού ΑΦΜ. Με έναν κωδικό μορφής OTP ο ασθενής θα μπορούσε να επιβεβαιώσει ότι έχει λάβει επιτυχώς τα κατάλληλα έγγραφα και συγχρόνως το ηλεκτρονικό σύστημα να προστατεύει με μια τέτοια διαδικασία εν μέρη τα προσωπικά δεδομένα του ασθενούς.

Αδιαμφισβήτητα σύμφωνα με όσα στοιχεία έχουμε μέσω της συγκεκριμένης διατριβής κατανοούμε πως η ψηφιοποίηση της δημόσιας υγείας στην Ελλάδα του 2022 βρίσκεται σε πρώιμο στάδιο. Απαραίτητο στοιχείο για την εξέλιξη της θεωρείται η άμεση εγκατάσταση δικτύων που λειτουργούν δια μέσου οπτικής ίνας και με ταχύτητες 5G σε όλη την Ελλάδα. Παρατηρώντας στατιστικά στοιχεία από την επίσημη

ιστοσελίδα της ευρωπαϊκής ενώσεως στην Ελλάδα είναι ευδιάκριτο το γεγονός πως ο κρατικός μηχανισμός δεν είναι τόσο ετοιμος όσο θεωρητικά πιστεύει. Η περίοδος της πανδημίας βοήθησε αρκετά στο να γίνει κατανοητό πως υπάρχουν αρκετά κενά και ελλείψεις στον τομέα της δημόσιας διοίκησης και πιο συγκεκριμένα στη δημόσια υγεία.

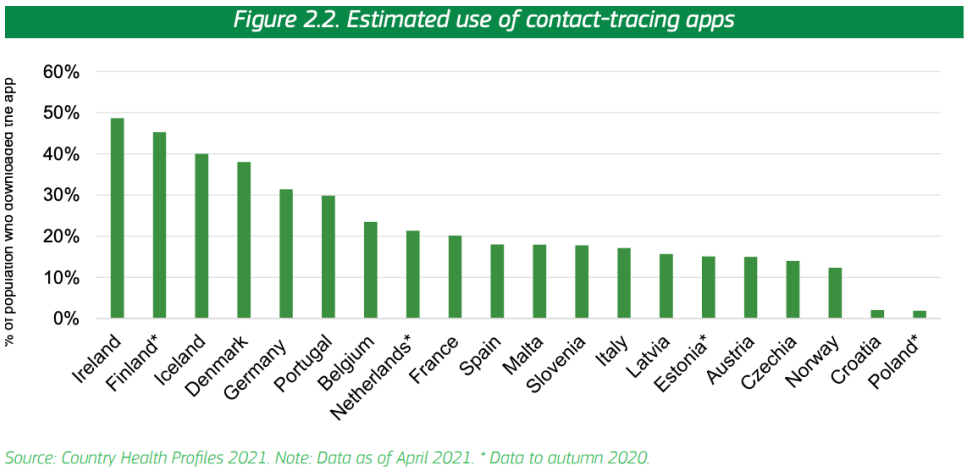
Στην παρακάτω στατιστική μελέτη μπορούμε να διαπιστώσουμε πως στον τομέα υγείας το ελληνικό κράτος αντιμετωπίζει αρκετές προβληματικές στο πρακτικό κομμάτι. Το 2021 φαίνεται να είναι μια δύσκολη χρονιά για την δημόσια υγεία μιας και τα θύματα της πανδημίας πολλαπλασιάστηκαν και ο ελληνικός κρατικός μηχανισμός δεν φανταζε έτοιμος για να βγάλει εις πέρας αξιοπρεπώς και ως μια ανερχόμενη αναπτυσσόμενη χώρα της Ε.Ε. μια δύσκολη και πρωτοφανή κατάσταση.



Βλ. Φωτογραφία europa.gr/covid-19/greece.

15/3/2020

Εν συνεχεία του λόγου παρατηρώντας άλλες στατιστικές μελέτες και όπως αναφορικά υποστηρίζει η επίσημη ιστοσελίδα της Ευρωπαϊκής Ένωσης κατά την διάρκεια της πανδημίας κρίθηκε αναγκαίο να επισπευσθεί η χρήση της τεχνολογίας για την εξυπηρέτηση των πολιτών μιας και η δια ζώσης επαφή κρίθηκε αδύνατη κατά της διάρκεια της πανδημίας. Από το αποτέλεσμα της μελέτης στην Ελλάδα μόνο το 23% των πολιτών κατά το 2019 εξοικειώθηκε και χρησιμοποίησε τις εφαρμογές της ψηφιακής πλατφόρμας gov.gr. Από τα δεδομένα που μελετάμε δια μέσω της ιστοσελίδας gov.gr η πλατφόρμα ξεκίνησε με 92 ονλάιν υπηρεσίες και το 2022 οι υπηρεσίες έφθασαν τις 1406. Σύμφωνα με αυτά τα στοιχεία βλέπουμε πως θεωρείται αναγκαιότητα σε μια εξελίξιμη εποχή η ψηφιοποίηση της γραφειοκρατίας. Βεβαίως απαραίτητη προϋπόθεση για την ομαλή λειτουργία των εφαρμογών αυτών είναι οι εγκαταστάσεις όπως η οπτική ίνα σε όλη την Ελλάδα και τα δίκτυα 5G. Επειδή γίνεται αναφορά σε προσωπικά δεδομένα όλων των Ελλήνων πολιτών χρήζει αναγκαιότητας ένα σύστημα κυβερνοασφάλειας που να προστατευει όσο γίνεται πιο πολύ τα δεδομένα.



*Source: Country Health Profiles 2021. Note: Data as of April 2021. * Data to autumn 2020.*

Βλ. Φωτογραφία europa.gr/covid-19/greece.

3/4/2021

Μελετώντας τα όσα δεδομένα έχουμε συλλέξει από διάφορες πηγές η Ελλάδα κάνει τα πρώτα της βήματα όσον αφορά τον ψηφιακό μετασχηματισμό και την ένταξη της στη νέα ψηφιακή εποχή. Ως τώρα η αλλαγή από την έγχαρτη μορφή γραφειοκρατίας σε ψηφιοποιημένη δεν είναι ο βασικός στόχος του Υπουργείου Ψηφιακής Διακυβέρνησης. Βασικός στόχος θεωρείται η αντιγραφή και η μετεξέλιξη μοντέλων άλλων ευρωπαϊκών και μη ευρωπαϊκών χωρών που έχουν συμβάλλει αποτελεσματικά στην απλούστευση και αμεσότητα του συστήματος υγείας. Δυστυχώς σε πρώτο στάδιο η Ελλάδα αντιμετωπίζει μεγάλες ελλείψεις αναφορικά με τον τομέα των εξελιγμένων εγκαταστάσεων και εξοπλισμών ώστε να μπορέσει να συμβαδίσει με τα δεδομένα της νέα ψηφιακής εποχής. Η ελληνική κυβέρνηση οφείλει να επενδύσει τόσο την εξασφάλιση των κατάλληλων εγκαταστάσεων όσο και στην προστασία των δεδομένων και συστημάτων.

8. Επίλογος

Οι επιδημικές λοιμώξεις και άλλες μορφές κρίσης, αναμενόμενες και απρόβλεπτες, είναι αναπόφευκτες. Ωστόσο, ο αντίκτυπός τους μπορεί να μετριαστεί μέσω καλύτερης ετοιμότητας και αποτελεσματικότερων απαντήσεων όπως με την . Η ιστορία δείχνει ότι οι αλλαγές που υιοθετούνται σε μια κρίση δεν είναι πάντα προσωρινές. Οι κρίσεις μπορούν, ουσιαστικά, να αναδιαμορφώσουν όχι μόνο τις πεποιθήσεις και τις συμπεριφορές μας, αλλά και τις επιχειρήσεις και τη βιομηχανία με πολλούς τρόπους. Και, η CTI θα διαδραματίσει ακόμη πιο σημαντικό ρόλο στη μετα-COVID εποχή. Η πληροφορική και οι άλλες βιομηχανίες πρέπει να συνεχίσουν να σχεδιάζουν προληπτικά, να εστιάζουν στην έρευνα και την ανάπτυξη σε βασικούς τομείς πρακτικής σημασίας και να επανεξετάζουν και να προσαρμόζουν τις πολιτικές τους. Πρέπει, επίσης, να επανεξετάσουν και να τροποποιήσουν τις απαραίτητες πολιτικές διαχείρισης κρίσεων και τις πολιτικές, στρατηγικές και πρακτικές διαχείρισης κινδύνων πληροφορικής και επιχειρήσεων, λαμβάνοντας διδάγματα από την τρέχουσα κρίση. Η ικανότητα ενός οργανισμού να ανταποκρίνεται αποτελεσματικά σε μια διαταραχή, όχι μόνο εξαρτάται από το πόσο αποτελεσματική ήταν στη διαδικασία σχεδιασμού, αλλά και από το πόσο αποτελεσματική ήταν με την προετοιμασία, τις δοκιμές και την εκπαίδευση του προσωπικού τους, η οποία συχνά παραμελείται. Η πανδημία COVID-19 είναι μια κλήση αφύπνισης σε όλους μας. Ο κόσμος, η κυβερνοαφάλεια, η ζωή και η δουλειά μας μετά τον κορονοϊό, δεν θα είναι τα ίδια. Στο πλαίσιο της κυβερνοασφάλειας, η πανδημία έχει αναδείξει ευκαιρίες και αδυναμίες των συστημάτων πληροφορικής.

Ασφαλίζοντας το Δημόσιο Σύστημα Υγείας με συστήματα Cyber Threat Intelligence, ένα από τα σημαντικότερα όπλα για την προάσπιση του κυβερνοχώρου αποδεικνύοντας έτσι η αναγκαιότητά της προάσπισης και ασφάλισης κατά τη διάρκεια αυτής της κρίσης αλλά και μετέπειτα. Για να την εκμεταλλευτούμε, στο έπακρον, πρέπει περισσότερες ιδιωτικέ ελληνικές επιχειρήσεις και οργανισμοί να ενσωματώσουν εργαλεία CTI για την βελτίωση της άμυνας της επιχείρησής τους αλλά και των κρατικών δομών Δημόσιας Υγείας.

9. Βιβλιογραφία

- **Hauben, M., & Hauben, R. (1998). Behind the Net: The Untold Story of the ARPANET and Computer Science. 7ed. Los Angeles.**
-
- ***Ostrom and Hess. (2007). Understanding Knowledge as a Commons, MIT Press.***
- ***Αθανάσιος Κοσμόπουλος. (2022). Ψηφιοποίηση της Δημόσιας Υγείας στην Ελλάδα, Προσωπική συνέντευξη, Αθήνα.***
- ***Hathaway et al. (2012) Roscini, (2014), Cyber Attacks Atittude. Columbia University, New York City.***
- **Giddens, Anthony (1990) The Consequences of Modernity. Cambridge : Polity.**
- ***Maris,G., Sklias, P., & Maravegias, N.(2020), The political ecomony of the Greek economic crisis in 2020. Athens.***
- ***Christensen & Lægreid, (2020),Balancing Governance Capacity and Legitimacy. Cambridge: Cambridge Press.***
- ***Mouroutsos, J. (2020). E-Journals.E-Publishing, Public Administration and Local Government in coronavirus crisis. University of Peloponnesse, Corinth.***
- **Herz, John. (1962). International Politics in the Atomic Age. Νέα Υόρκη : Columbia University Press.**

10. Ηλεκτρονικές πηγές

- https://mindigital.gr

Mindigital. 2020, Ηλεκτρονικές Υπηρεσίες 2020.

- https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/life-sciences-health-care/gr_health_4_0_noexp.pdf

Deloitte. 2021, Ψηφιακός Μετασχηματισμός ΣΕΒ.

- https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Digital-Strategy Ministry of Greece. 2021, Cybersecurity and policies.

- https://ec.europa.eu/reform-support/what-we-do/public-administration-and-governance_el

Europa. 2021, Public Administration, Greece, Athens

- https://konbriefing.com/en-topics/cyber-attacks-2021-by-country.html#cny-gr

Cyber Attacks 2021, Deutch, Länder.