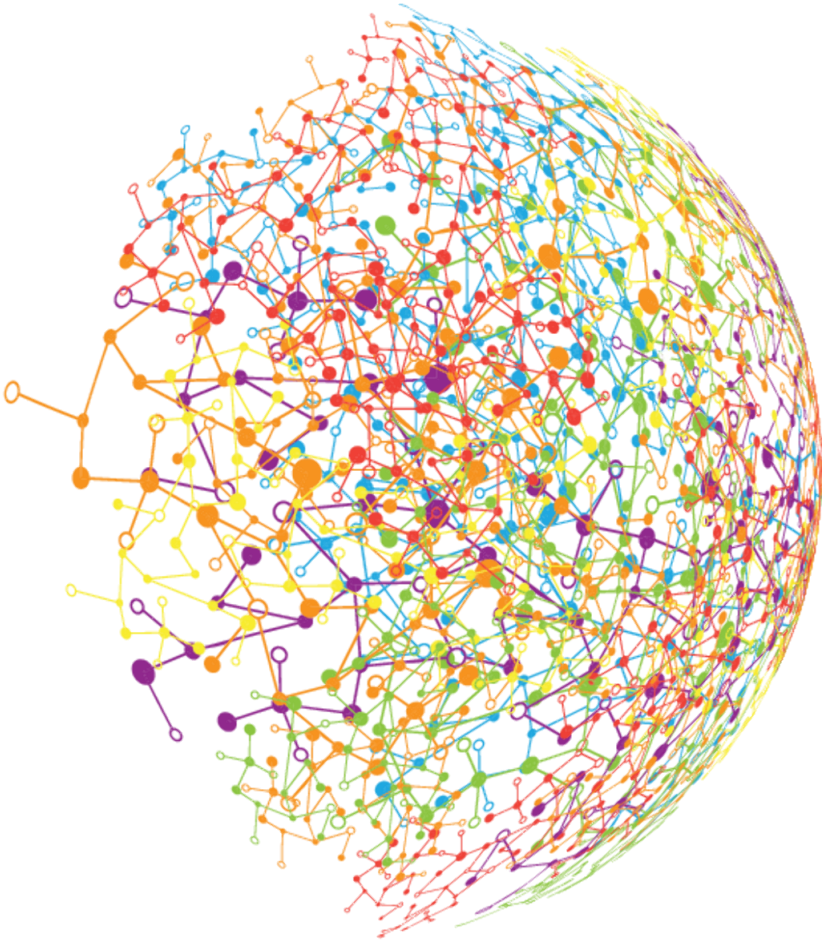


Στρατηγική για το Διαδίκτυο των Πραγμάτων (IoT)

Τεύχος Διαβούλευσης

Μάρτιος 2025

Περιεχόμενα

Περιβάλλον και αντικείμενο του έργου

Περιβάλλον του έργου

Το Υπουργείο Ψηφιακής Διακυβέρνησης και η Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων εστιάζει στην ανάπτυξη μιας ολοκληρωμένης εθνικής στρατηγικής για τη χρήση της τεχνολογίας Διαδικτύου των Πραγμάτων - Internet of Things (IoT) και τη θέσπιση ενός σαφούς και συνεκτικού πλαισίου για την ασφαλή, υπεύθυνη και ρυθμιζόμενη ενσωμάτωσή του στην Ελλάδα. Στόχος της μελέτης είναι η δημιουργία ενός ευνοϊκού περιβάλλοντος για την ανάπτυξη και χρήση της συγκεκριμένης τεχνολογίας σε εθνικό επίπεδο, η υποστήριξη της ανάπτυξης μιας ανταγωνιστικής και καινοτόμου βιομηχανίας Διαδικτύου των Πραγμάτων και η μεγιστοποίηση των οφελών για την κοινωνία και την οικονομία.

Για την επίτευξη αυτών των στόχων, η εθνική στρατηγική για το τα Μη-Επανδρωμένα Οχήματα θα αξιοποιήσει μια πολύπλευρη προσέγγιση που περιλαμβάνει τις παρακάτω βασικές συνιστώσες:

- **Κανονιστικό πλαίσιο**: Ανάπτυξη και των βασικών πυλώνων ενός ολοκληρωμένου και συνεκτικού συνόλου κανονισμών και κατευθυντήριων γραμμών για την ασφαλή και υπεύθυνη χρήση του Διαδικτύου των Πραγμάτων. Ενδεικτικά, μπορεί να περιλαμβάνει απαιτήσεις για την εκπαίδευση των χειριστών και την αδρανοποίηση, καθώς και τα τεχνικά πρότυπα για το σχεδιασμό και τη λειτουργία τους.
- **Έρευνα και ανάπτυξη**: Ενθάρρυνση και υποστήριξη της ανάπτυξης τεχνολογιών αιχμής και εφαρμογών IoT μέσω ερευνητικών επιχορηγήσεων και χρηματοδοτικών προγραμμάτων.
- **Ανάπτυξη της βιομηχανίας**: Προώθηση της ανάπτυξης της βιομηχανίας IoT μέσω της στήριξης της ανάπτυξης των μικρών και μεσαίων επιχειρήσεων και της ενθάρρυνσης των επενδύσεων στον τομέα.
- **Διεθνής συνεργασία**: Συνεργασία με διεθνείς εταίρους και ενδιαφερόμενα μέρη για την προώθηση της ασφαλούς και υπεύθυνης χρήσης του IoT και για τη διευκόλυνση της ανταλλαγής βέλτιστων πρακτικών και τεχνικής εμπειρογνωμοσύνης.

Τρέχουσα κατάσταση του έργου

Το παρόν έγγραφο της διαβούλευσης αποτελεί ένα συνοπτικό κείμενο που επικεντρώνεται στα πιο βασικά σημεία της προτεινόμενης στρατηγικής. Στόχος είναι να αποτελέσει ένα κείμενο συνοπτικό και πρακτικό που θα εξυπηρετήσει τη διαδικασία συγκέντρωσης σχολίων και προτάσεων για τη βελτίωση της στρατηγικής από όλα τα εμπλεκόμενα μέρη.

Το παρόν έγγραφο δεν αποτελεί την πλήρη στρατηγική. Η τελευταία θα περιλαμβάνει μεταξύ άλλων, και επιπρόσθετα του παρόντος εγγράφου:

- Εκτενείς πληροφορίες αναφορικά με όλες τις ενότητες που παρουσιάζονται στο κείμενο της διαβούλευσης (π.χ. κλάδοι με την μεγαλύτερη ωριμότητα, SWOT ανάλυση, προτεινόμενες δράσεις)
- Οδικό χάρτη για την υλοποίηση της στρατηγικής
- Τρόπους χρηματοδότησης των προτεινόμενων δράσεων
- Διακυβέρνηση της υλοποίησης της στρατηγικής

Συντομογραφίες

Ακρωνύμιο	Περιγραφή
BLE	Bluetooth Low Energy
GDPR	General Data Protection Regulation
LPWAN	Low Power Wide Area Network
NB-IoT	Narrowband Internet of Things
NFV	Network Function Virtualization
SDN	Software-Defined Networking
ΕΕ	Ευρωπαϊκή Ένωση
IoT	Internet of Things
ΤΝ	Τεχνητή Νοημοσύνη

Διεθνές και εθνικό ρυθμιστικό πλαίσιο

Το ισχύον ευρωπαϊκό νομικό πλαίσιο καλύπτει πολλές πτυχές της χρήσης των IoT μέσω κανονισμών για την κυβερνοασφάλεια, την προστασία προσωπικών δεδομένων και την προμήθεια ψηφιακού περιεχομένου. Ωστόσο, δεν υπάρχει ειδική και σαφής ρύθμιση αποκλειστικά για τα IoT, δημιουργώντας ρυθμιστικά κενά και ζητήματα νομικής σαφήνειας. Παρακάτω παρατίθεται το εφαρμοστέο δίκαιο, διακρίνοντας μεταξύ ειδικών και γενικών διατάξεων, στο πλαίσιο της ενωσιακής και εθνικής νομοθεσίας.

Ειδικές διατάξεις

α. Ενωσιακή νομοθεσία

- **Κανονισμός (ΕΕ) 2023/2854 (Data Act):** Ρυθμίζει τη δίκαιη χρήση δεδομένων συνδεδεμένων προϊόντων, επιβάλλοντας υποχρεώσεις σε κατασκευαστές και παρόχους για διαφάνεια, προστασία δεδομένων και διαλειτουργικότητα, προωθώντας την καινοτομία και την ανταγωνιστικότητα.
- **Κανονισμός (ΕΕ) 2024/2847 (Cyber Resilience Act):** Θεσπίζει απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία, διασφαλίζοντας την ανθεκτικότητά τους σε κυβερνοεπιθέσεις. Επιβάλλει υποχρεώσεις σε κατασκευαστές, ενισχύει τη διαφάνεια και θεσπίζει μηχανισμούς εποπτείας, βελτιώνοντας την ασφάλεια των IoT συσκευών.
- **Κανονισμός (ΕΕ) 2024/1689 (AI Act):** Θεσπίζει κανόνες για την ανάπτυξη και χρήση συστημάτων ΤΝ στην ΕΕ, διασφαλίζοντας ασφάλεια και θεμελιώδη δικαιώματα. Επιβάλλει υποχρεώσεις σε παρόχους και χρήστες, κατηγοριοποιεί τα συστήματα βάσει κινδύνου και προβλέπει μηχανισμούς εποπτείας και κυρώσεων.
- **Κανονισμός (ΕΕ) 2022/2065 (Digital Services Act):** θεσπίζει κανόνες για τις ψηφιακές πλατφόρμες, ενισχύοντας τη διαφάνεια, την ασφάλεια χρηστών και τη διαχείριση περιεχομένου. Επιβάλλει υποχρεώσεις σε πλατφόρμες που διαχειρίζονται δεδομένα, συμπεριλαμβανομένων IoT συσκευών, διασφαλίζοντας την προστασία της ιδιωτικότητας και την κυβερνοασφάλεια.
- **Κανονισμός (ΕΕ) 2024/2547**: Ενισχύει την προστασία των καταναλωτών σε ψηφιακές υπηρεσίες και προϊόντα, όπως τα IoT. Προβλέπει διαφάνεια, ασφάλεια και προστασία δεδομένων, καθορίζοντας ευθύνες προμηθευτών και διασφαλίζοντας την ασφαλή χρήση των ψηφιακών τεχνολογιών.
- **Κανονισμός (ΕΕ) 2017/745 (MDR)**: Ρυθμίζει την κυκλοφορία των ιατρικών προϊόντων στην ΕΕ, διασφαλίζοντας την ασφάλεια, την ποιότητα και την προστασία των δεδομένων των χρηστών. Ισχύει και για IoT ιατρικές συσκευές, επιβάλλοντας αυστηρούς κανόνες συμμόρφωσης, σήμανσης CE και παρακολούθησης μετά την κυκλοφορία.
- **Κανονισμός (ΕΕ) 2024/1747:** τροποποιεί τους Κανονισμούς 2019/942 και 2019/943, ενισχύοντας την ευρωπαϊκή αγορά ηλεκτρικής ενέργειας και την ενεργειακή μετάβαση. Προβλέπει τη χρήση δεδομένων από έξυπνες μετρητικές συσκευές με συναίνεση καταναλωτών και προωθεί την εγκατάσταση έξυπνων συστημάτων για ενεργή συμμετοχή στις ενεργειακές αγορές.
- **Κανονισμός (ΕΕ) 2019/941**: θεσπίζει κοινό πλαίσιο για την πρόληψη και διαχείριση κρίσεων ηλεκτρικής ενέργειας, διασφαλίζοντας τον ενεργειακό εφοδιασμό. Προβλέπει συνεργασία μεταξύ κρατών μελών, σχέδια ετοιμότητας και μέτρα συμβατά με την εσωτερική αγορά.
- **Κανονισμός (ΕΕ) 2022/1925**: ρυθμίζει την ευρωπαϊκή αγορά ψηφιακών προϊόντων και υπηρεσιών, ενισχύοντας την ψηφιακή ασφάλεια και την προστασία των καταναλωτών. Επιβάλλει αυστηρούς κανόνες για την ασφάλεια των συνδεδεμένων συσκευών, διασφαλίζοντας την προστασία δεδομένων και την ανθεκτικότητα απέναντι σε κυβερνοεπιθέσεις.
- **Οδηγία 2023/1791/ΕΕ:** ενισχύει τους κανόνες ενεργειακής απόδοσης στην Ε.Ε., μειώνοντας την κατανάλωση ενέργειας και τις εκπομπές CO2. Επιβάλλει στα κράτη μέλη την ανάπτυξη εθνικών στρατηγικών, επηρεάζοντας και τις IoT συσκευές, όπου η ενεργειακή απόδοση είναι κρίσιμη, με προθεσμία ενσωμάτωσης την 11η/10/2025.
- **Οδηγία 2024/2853/ΕΕ**: ρυθμίζει την ευθύνη για ελαττωματικά προϊόντα και τα δικαιώματα αποζημίωσης, καλύπτοντας και IoT συσκευές. Ορίζει τα είδη ζημίας, τις προϋποθέσεις ελαττωματικότητας και τους υπεύθυνους οικονομικούς φορείς, με προθεσμία ενσωμάτωσης την 9η/12/2026.
- **Οδηγία 2024/1788/ΕΕ:** Ρυθμίζει την αγορά ανανεώσιμων αερίων, φυσικού αερίου και υδρογόνου, ενισχύοντας την προστασία των καταναλωτών. Προβλέπει την εγκατάσταση έξυπνων μετρητικών συστημάτων με δυνατότητα μετάδοσης δεδομένων, διασφαλίζοντας συμμόρφωση με την κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων με προθεσμία ενσωμάτωσης την 5η/8/2026.

β. Εθνική νομοθεσία

- **Ν. 4961/2022**: θεσπίζει πλαίσιο για την ασφαλή εκμετάλλευση προηγμένων τεχνολογιών, όπως το IoT και τα Μη-Επανδρωμένα Αεροσκάφη, ενισχύοντας τον ψηφιακό μετασχηματισμό. Προβλέπει απαιτήσεις κυβερνοασφάλειας, υποχρεώσεις συμμόρφωσης για κατασκευαστές και διανομείς, καθώς και Μητρώο Διασυνδεδεμένων Συσκευών υπό την Εθνική Αρχή Κυβερνοασφάλειας.
- **Ν. 5099/2024:** Ορίζει παράταση έναρξης ισχύος των ρυθμίσεων του ν. 4961/2022 για τις εφαρμογές τεχνολογίας IoT, και ως νέα ημερομηνία έναρξης των ρυθμίσεων ορίστηκε η 1η.09.2024.
- **Ν. 4967/2022**: συνιστά μεταφορά στην εθνική έννομη τάξη των Οδηγιών (ΕΕ) 2019/770 και 2019/771.
- **Ν. 4727/2020:** ενσωματώνει την Οδηγία 2018/1972/ΕΕ, θεσπίζοντας τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών. Ρυθμίζει την εναρμόνιση των κανόνων επικοινωνίας, ενισχύει τα δικαιώματα χρηστών και προωθεί δίκτυα 5G, διασφαλίζοντας τη διαλειτουργικότητα και ασφάλεια των IoT συσκευών.
- **Κοινή Υπουργική Απόφαση υπ' αριθμ. ΟΙΚ.37764/873/Φ342/2016:** ενσωματώνει την Οδηγία 2014/30/ΕΕ, ρυθμίζοντας την ηλεκτρομαγνητική συμβατότητα (EMC) ηλεκτρικών και ηλεκτρονικών συσκευών. Διασφαλίζει ότι οι συσκευές, συμπεριλαμβανομένων των IoT, δεν προκαλούν ή επηρεάζονται από ηλεκτρομαγνητικές παρεμβολές, εξασφαλίζοντας την ομαλή λειτουργία τους.
- **Προεδρικό Διάταγμα 98/2017:** ενσωματώνει την Οδηγία 2014/53/ΕΕ, ρυθμίζοντας τη διάθεση συσκευών ραδιοεπικοινωνιών στην ΕΕ. Διασφαλίζει τη συμμόρφωσή τους με τεχνικές προδιαγραφές, αποτρέποντας παρεμβολές στο ραδιοφάσμα, και καλύπτει και IoT συσκευές που χρησιμοποιούν ραδιοκύματα για επικοινωνία.
- **Κοινή Υπουργική Απόφαση υπ' αριθμ. Η.Π. 23615/651/Ε.103/2014**: ενσωματώνει την Οδηγία 2012/19/ΕΕ (WEEE) και ρυθμίζει τη διαχείριση των αποβλήτων ηλεκτρικού και ηλεκτρονικού εξοπλισμού, προωθώντας την ανακύκλωση και την κυκλική οικονομία. Ισχύει και για IoT συσκευές, διασφαλίζοντας τη σωστή συλλογή και επεξεργασία τους για τη μείωση του περιβαλλοντικού αντίκτυπου.
- **Ν. 4996/2022:** ενσωματώνει την Οδηγία 2019/790/ΕΕ, ενισχύοντας την προστασία πνευματικών δικαιωμάτων στην ψηφιακή εποχή. Ρυθμίζει την αδειοδότηση και αποζημίωση δημιουργών για περιεχόμενο που διανέμεται μέσω IoT συσκευών, διασφαλίζοντας διαφάνεια και δίκαιη κατανομή εσόδων.
- **Ν. 4967/2022:** ενσωματώνει α) την Οδηγία 2019/770/ΕΕ και ρυθμίζει τις συμβάσεις για την προμήθεια ψηφιακού περιεχομένου και υπηρεσιών. Καθορίζει τη συμμόρφωση, τις επανορθώσεις και τις τροποποιήσεις, ισχύοντας και για IoT συσκευές, όπως smartwatches και smartphones, β)Οδηγία 2019/771/ΕΕ και ρυθμίζει τις συμβάσεις πώλησης αγαθών, θέτοντας κανόνες για συμμόρφωση, επανόρθωση και εγγυήσεις. Καλύπτει και ψηφιακό περιεχόμενο ή υπηρεσίες που συνδέονται με αγαθά, όπως λογισμικό cloud και δεδομένα IoT συσκευών.
- **Προεδρικό Διάταγμα 50/2012:** ενσωματώνει την Οδηγία 2010/40/ΕΕ, θεσπίζοντας το πλαίσιο για τα ευφυή συστήματα μεταφορών (ITS) στις οδικές μεταφορές. Προωθεί διαλειτουργικές τεχνολογίες, όπως διαχείριση κυκλοφορίας και ηλεκτρονικά διόδια, αξιοποιώντας IoT συσκευές για συλλογή και ανταλλαγή δεδομένων σε πραγματικό χρόνο.

Γενικές διατάξεις

α. Ενωσιακή νομοθεσία

- **Κανονισμός (ΕΕ) 679/2016 (GDPR):** θεσπίζει ενιαίο πλαίσιο για την προστασία προσωπικών δεδομένων στην ΕΕ, δίνοντας στους πολίτες έλεγχο στα δεδομένα τους. Καθορίζει νομικές βάσεις, αρχές επεξεργασίας, δικαιώματα χρηστών και αυστηρές κυρώσεις για μη συμμόρφωση, ισχύοντας και για οργανισμούς εκτός ΕΕ που επεξεργάζονται δεδομένα Ευρωπαίων πολιτών..
- **Κανονισμός (ΕΕ) 2019/881 (Cybersecurity Act):** θεσπίζει ενιαίο πλαίσιο για την κυβερνοασφάλεια στην ΕΕ, εισάγοντας σύστημα πιστοποίησης για την ασφάλεια ψηφιακών προϊόντων, υπηρεσιών και IoT συσκευών. Ενισχύει την προστασία δεδομένων, την ιδιωτικότητα και την εμπιστοσύνη των χρηστών, συμβάλλοντας στην ασφάλεια και την ενοποίηση της ενιαίας αγοράς.
- **Εκτελεστικός Κανονισμός (ΕΕ) 2023/203:** καθορίζει απαιτήσεις για τη διασφάλιση της ασφάλειας πληροφοριών με αντίκτυπο στην αεροπορία. Ρυθμίζει την ανίχνευση και αντιμετώπιση συμβάντων ασφαλείας, εφαρμόζοντας τον Κανονισμό (ΕΕ) 2018/1139 για την προστασία κρίσιμων δεδομένων και υποδομών.
- **Κανονισμός (ΕΕ) 2018/1807:** θεσπίζει πλαίσιο για την ελεύθερη ροή δεδομένων μη προσωπικού χαρακτήρα στην ΕΕ, καταργώντας γεωγραφικούς περιορισμούς. Ενισχύει την ψηφιακή αγορά, προωθώντας την καινοτομία και τη διαλειτουργικότητα, επηρεάζοντας άμεσα τις IoT συσκευές που απαιτούν αποθήκευση και επεξεργασία δεδομένων.

- **Οδηγία 2002/58/ΕΚ**: ρυθμίζει την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καλύπτοντας και τις IoT συσκευές ως «τερματικό εξοπλισμό». Προβλέπει κανόνες για τη χρήση δεδομένων, τα cookies, την ανάλυση πληροφοριών και την προστασία από αθέμιτες παρακολουθήσεις, διασφαλίζοντας τον έλεγχο των χρηστών στα προσωπικά τους δεδομένα.

β. Εθνική νομοθεσία

- **Ν. 4624/2019:** Συμπληρώνει τον κανονισμό GDPR (ΕΕ/2016/679) και ενσωματώνει την Οδηγία 2016/680/ΕΕ, ρυθμίζοντας την προστασία προσωπικών δεδομένων από αρχές επιβολής του νόμου για σκοπούς έρευνας και δίωξης εγκλημάτων.
- **Ν. 3471/2006:** ενσωματώνει την Οδηγία 2002/58/ΕΚ στην ελληνική νομοθεσία, ρυθμίζοντας την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Καθορίζει κανόνες για τη διαχείριση δεδομένων, τη χρήση cookies και την προστασία των χρηστών από αθέμιτες παρακολουθήσεις και επεξεργασία προσωπικών δεδομένων.
- **Ν. 5160/2024:** ενσωματώνει την Οδηγία 2022/2555/ΕΕ (NIS 2) στην ελληνική νομοθεσία, ενδυναμώνοντας την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ). Επεκτείνει τις εποπτικές και ελεγκτικές της αρμοδιότητες, διασφαλίζοντας τη συμμόρφωση φορέων, την ανταλλαγή πληροφοριών και την επιβολή κυρώσεων για παραβιάσεις κυβερνοασφάλειας.
- **Ν. 5002/2022**: Καθορίζει τη διαδικασία άρσης απορρήτου επικοινωνιών, προβλέπει τη σύσταση Επιτροπής Συντονισμού για θέματα κυβερνοασφάλειας και επιβάλλει νέες υποχρεώσεις στις αρμόδιες αρχές για την προστασία δεδομένων.
- **Ν. 2251/1994 (Νόμος Προστασίας Καταναλωτών):** όπως εκάστοτε ισχύει, ρυθμίζει τα δικαιώματα καταναλωτών σε συμβάσεις με προμηθευτές, καλύπτοντας και την προμήθεια ψηφιακού περιεχομένου ή υπηρεσιών. Επεκτείνεται σε περιπτώσεις όπου ο καταναλωτής παρέχει προσωπικά δεδομένα ως αντάλλαγμα, διασφαλίζοντας την προστασία του.
- **Ν. 4933/2022:** ενσωματώνει την Οδηγία 2019/2161/ΕΕ, εκσυγχρονίζοντας τη νομοθεσία προστασίας καταναλωτών στην ΕΕ. Ενισχύει τη διαφάνεια στις ηλεκτρονικές αγορές, ρυθμίζει καταχρηστικές πρακτικές, προβλέπει αυστηρότερα πρόστιμα και καλύπτει ψηφιακές υπηρεσίες, συμπεριλαμβανομένων IoT προϊόντων..

Αποτύπωση ενδιαφερόμενων μερών

Η αποτύπωση των ενδιαφερόμενων μερών για το Διαδίκτυο των Πραγμάτων (IoT) είναι κρίσιμη για την κατανόηση του οικοσυστήματος και των επιπτώσεών του. Η χαρτογράφηση αυτών των μερών είναι κρίσιμη για τη διαμόρφωση ενός ολοκληρωμένου πλαισίου ανάπτυξης, χρήσης και εποπτείας του IoT. Ακολουθεί πίνακας με τους βασικούς ενδιαφερόμενους διεθνείς και εθνικούς φορείς:

ΔΙΕΘΝΕΙΣ ΦΟΡΕΙΣ	ΕΘΝΙΚΟΙ ΦΟΡΕΙΣ	
• Ευρωπαϊκός Οργανισμός για την Ασφάλεια της Αεροπορίας (EASA) • European Union Agency for Cybersecurity (ENISA) • Institute of Electrical and Electronics Engineers (IE.E.E) • European Telecommunications Standards Institute (ETSI) • International Telecommunication Union Internet Engineering Task Force (IETF) • ISO/ IEC JTC 1 • Internet of Things Alliance (IoTA) • Industry IoT Consortium (IIC) • Open Connectivity Foundation (OCF) • LoRa Alliance • Alliance for Internet of Things Innovation (AIOTI) • IoT Security Foundation (IoTSF) • GSMA • Wi-SUN Alliance	• Υπουργείο Εθνικής Άμυνας - Εθνική Μετεωρολογική Υπηρεσία • Υπουργείο Εσωτερικών - Δήμοι και Περιφέρειες • Υπουργείο Υγείας • Υπουργείο Προστασίας του Πολίτη • Υπουργείο Υποδομών και Μεταφορών • Υπουργείο Κλιματικής Κρίσης και Πολιτικής Προστασίας • Υπουργείο Περιβάλλοντος και Ενέργειας • Υπουργείο Ανάπτυξης • Υπουργείο Αγροτικής Ανάπτυξης • Υπουργείο Ναυτιλίας και Νησιωτικής Πολιτικής • Υπουργείο Ψηφιακής Διακυβέρνησης - Γενική Γραμματεία Τηλεπικοινωνίων και Ταχυδρομείων - Κοινωνία της Πληροφορίας - Εθνική Αρχή Κυβερνοασφάλειας	• Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων • Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα • Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών • Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας (ΚΕ.Τ.Υ.Α.Κ.), • Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.) • Ακαδημαϊκά Ιδρύματα και Ερευνητικά Κέντρα

• Connectivity Standards Alliance (CSA) • Bluetooth Special Interest Group (SIG)		

Πίνακας 1: Ενδιαφερόμενα μέρη για το IoT

Επιπρόσθετα των παραπάνω φορέων, ο ιδιωτικός τομέας διαδραματίζει έναν εξαιρετικά σημαντικό ρόλο στην ανάπτυξη και την χρήση του IoT. Η συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα είναι επίσης πολύ σημαντική για την επιτυχή υλοποίηση της στρατηγικής. Μέσω αυτής της συνεργασίας, μπορούν να αξιοποιηθούν οι πόροι, η τεχνογνωσία και η καινοτομία του ιδιωτικού τομέα, ενώ ο δημόσιος τομέας παρέχει το θεσμικό πλαίσιο και την υποστήριξη που απαιτείται για την υλοποίηση των στρατηγικών. Οι συνέργειες αυτές ενισχύουν την αποτελεσματικότητα και την αποδοτικότητα των δράσεων, οδηγώντας σε βιώσιμη ανάπτυξη και μακροχρόνια επιτυχία.

Αποτύπωση κλάδων με τη μεγαλύτερη ωριμότητα ωφέλειας υλοποίησης δράσεων

Το Διαδίκτυο των Πραγμάτων (IoT) αποτελεί μία από τις πλέον καινοτόμες τεχνολογίες, προσφέροντας τη δυνατότητα διασύνδεσης και επικοινωνίας μεταξύ των συσκευών, συστημάτων και χρηστών. Η εξέλιξη του διαμορφώνει ένα μέλλον όπου η διαχείριση της πληροφορίας και η αλληλεπίδραση μεταξύ των συστημάτων γίνονται όλο και πιο έξυπνες και αυτοματοποιημένες επηρεάζοντας πολλούς τομείς, όπως τα Έξυπνα Κτίρια, την Ασφάλεια στον Κυβερνοχώρο, τη Διαχείριση Φυσικών Πόρων, τις Μεταφορές, την Αντιμετώπιση καταστάσεων έκτακτης ανάγκης, την Άμυνα, την Εθνική Ασφάλεια, τη Βιομηχανία, την Ενέργεια, την Ανθρωπιστική Βοήθεια, τη Γεωργία, την Υγεία, το Περιβάλλον και τη Βιωσιμότητα.
Στο παρακάτω συνοπτικό διάγραμμα, αποτυπώνονται οι κλάδοι μεγαλύτερη ωριμότητα για την αξιοποίηση τεχνολογιών IoT:

Εικόνα 1: Διάγραμμα: Κλάδοι με τη μεγαλύτερη ωριμότητα για την αξιοποίηση IoT

SWOT Ανάλυση

Η SWOT ανάλυση για το IoT, παρέχει μια συνοπτική αποτύπωση των δυνατών σημείων, αδυναμιών, ευκαιριών και απειλών εξετάζοντας τόσο τις ίδιες τις τεχνολογίες, όσο και τις ιδιαιτερότητες της Ελλάδας που επηρεάζουν την υιοθέτησή τους, λαμβάνοντας υπόψη το εσωτερικό και εξωτερικό περιβάλλον. Τα ευρήματα συμβάλλουν στη στρατηγική αξιοποίησης των πλεονεκτημάτων και διαχείρισης των προκλήσεων.

Στο παρόν έγγραφο παρουσιάζονται πολύ συνοπτικά και επιγραμματικά τα βασικά σημεία της SWOT ανάλυσης. Η πλήρης περιγραφή της ανάλυσης SWOT θα περιλαμβάνεται σε πλήρη ανάπτυξη στο τελικό κείμενο της στρατηγικής.

Στον πίνακα που ακολουθεί παρουσιάζεται συνοπτικά η SWOT ανάλυση για τον τομέα του IoT:

S

Δυνατά Σημεία (Strengths)

Για την Τεχνολογία:

- Η υιοθέτηση της τεχνολογίας αυξάνει την αποτελεσματικότητα και την παραγωγικότητα
- Η χρήση της τεχνολογίας οδηγεί σε ταχύτερη και καλύτερη λήψη αποφάσεων
- Η ανάπτυξη της τεχνολογίας επιτρέπει τη δημιουργία καινοτόμων προϊόντων και υπηρεσιών
- Η χρήση της τεχνολογίας επιτρέπει τη βελτίωση της εμπειρίας του χρήστη
- Η αξιοποίηση της τεχνολογίας βελτιώνει τη διαχείριση και την εξοικονόμηση πόρων
- Η εφαρμογή της τεχνολογίας βελτιώνει την ασφάλεια και την προστασία
- Η χρήση της τεχνολογίας ενισχύει την συνεργασία και την επικοινωνία

Για την Ελλάδα:

- Η Ελλάδα έχει ευνοϊκό περιβάλλον που προσελκύει επενδύσεις σε ΤΠΕ

W

Αδυναμίες (Weaknesses)

Για την Τεχνολογία:

- Η χρήση της τεχνολογίας αυξάνει τον κίνδυνο κυβερνοεπιθέσεων, και παραβίασης της ιδιωτικότητας
- Η έλλειψη προτύπων μπορεί να δυσχεράνει τη διαλειτουργικότητα
- Η υιοθέτηση της τεχνολογίας απαιτεί υψηλό κόστος επένδυσης και λειτουργίας
- Η διαχείριση μεγάλου όγκου δεδομένων από τις IoT συσκευές ενδεχομένως μπορεί να είναι περίπλοκη
- Η χρήση της τεχνολογίας προϋποθέτει σταθερή και αξιόπιστη σύνδεση σε ευρυζωνικές υποδομές
- Πολλές IoT συσκευές έχουν περιορισμένες τεχνικές δυνατότητες, οι οποίες μπορεί να περιορίζουν την απόδοσή τους

Για την Ελλάδα:

- Η περιορισμένη πρόσβαση στη χρηματοδότηση περιορίζει την έρευνα και την καινοτομία, τη δημιουργία νεοφυών επιχειρήσεων και την

	υιοθέτηση τεχνολογιών αιχμής στις επιχειρήσεις και οργανισμούς • Η περιορισμένη ευαισθητοποίηση του κοινού για τις δυνατότητες της τεχνολογίας περιορίζουν την υιοθέτησή της
O **Ευκαιρίες (Opportunities)** Για την Τεχνολογία: • Η τεχνολογία ενισχύει τις ευκαιρίες για τη δημιουργία νέων επιχειρηματικών ευκαιριών και ανάπτυξη νέων αγορών • Η τεχνολογία παρέχει ευκαιρίες για βελτίωση της ποιότητας της ζωής των πολιτών, της υγείας και της ευεξίας • Η τεχνολογία παρέχει ευκαιρίες για βελτίωση της ενεργειακής αποδοτικότητας • Η τεχνολογία δημιουργεί ευκαιρίες για την προώθηση βιώσιμων πρακτικών Για την Ελλάδα: • Η ανάπτυξη συνεργασιών και διασύνδεση οικοσυστημάτων • Η βελτίωση της συμμόρφωσης της χώρας και των οργανισμών στο κανονιστικό και θεσμικό πλαίσιο • Η βελτίωση των υπηρεσιών από τη δημόσια διοίκηση • Η γεωμορφολογία της χώρας ενισχύει την ανάγκη για ταχύτερη αξιοποίηση της τεχνολογίας • Η αναβάθμιση των ευρυζωνικών υποδομών της χώρας να συμβάλει στην περαιτέρω αξιοποίηση της τεχνολογίας • Η ανάπτυξη, υιοθέτηση και εξαγωγή καινοτόμων υπηρεσιών στον τουρισμό • Η ανάπτυξη, υιοθέτηση και εξαγωγή καινοτόμων υπηρεσιών στην ναυτιλία • Η ανάπτυξη, υιοθέτηση και εξαγωγή καινοτόμων υπηρεσιών για έξυπνες πόλεις	**T** **Απειλές (Threats)** Για την Τεχνολογία: • Η γρήγορη εξέλιξη της τεχνολογίας μπορεί να αυξήσει το ρίσκο της υιοθέτησής της Για την Ελλάδα: • Η αυξημένη διασυνδεσιμότητα των συσκευών αυξάνει την απειλή από επιθέσεις σε περίπτωση πολεμικής εμπλοκής • Η αυξημένη χρήση της τεχνολογίας μπορεί να επιβαρύνει το περιβάλλον με αύξηση της κατανάλωσης ενέργειας και αύξηση ηλεκτρονικών αποβλήτων

Πίνακας 2: SWOT ANALYSIS για IoT

Όραμα και κατευθυντήριες αρχές

Όραμα

Το **οραμά** για το IoT είναι:

«Η δημιουργία μιας πιο ενοποιημένης και πιο συνδεδεμένης χώρας, στην οποία οι τεχνολογίες IoT χρησιμοποιούνται για τη βελτίωση της ζωής των ανθρώπων, τη δημιουργία νέων επιχειρηματικών ευκαιριών και την υποστήριξη της βιώσιμης οικονομικής ανάπτυξης»

Βασικά **στοιχεία του οράματος** αποτελούν:

- **Πλαίσιο**. Η ανάπτυξη ενός ολοκληρωμένου και συνεκτικού συνόλου κανονισμών και κατευθυντήριων γραμμών για την ανάπτυξη και χρήση του IoT.
- **Έρευνα και ανάπτυξη**. Η ενθάρρυνση και υποστήριξη της ανάπτυξης νέων τεχνολογιών και εφαρμογών IoT, μέσω ερευνητικών επιχορηγήσεων και χρηματοδοτικών προγραμμάτων και η ανάπτυξη των ανθρωπίνου δυναμικού.
- **Βιομηχανία**. Η προώθηση της ανάπτυξης μιας ανταγωνιστικής και καινοτόμου βιομηχανίας IoT, μέσω της στήριξης των μικρών και μεσαίων επιχειρήσεων και της ενθάρρυνσης των επενδύσεων στον τομέα.
- **Κοινωνία και οικονομία.** Η μεγιστοποίηση των οφελών για την κοινωνία και την οικονομία.

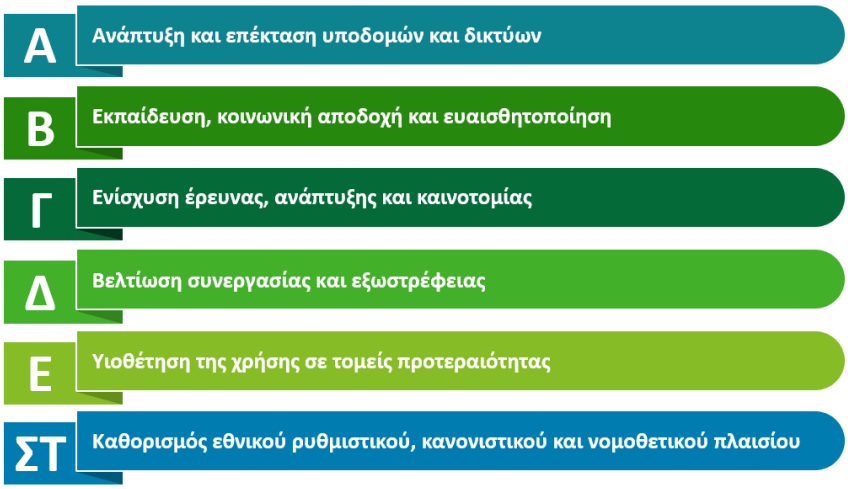
Κατευθυντήριες αρχές

Για την πραγματοποίηση του παραπάνω οράματος, θα ακολουθηθούν οι παρακάτω **κατευθυντήριες αρχές**:

- **Διαλειτουργικότητα και ανοικτά πρότυπα.** Το IoT θα πρέπει να προωθεί κοινά τεχνολογικά πρότυπα που θα επιτρέπουν τη συνεργασία μεταξύ συσκευών, συστημάτων και παρόχων, εξασφαλίζοντας ένα ανοιχτό οικοσύστημα.
- **Ασφάλεια και προστασία προσωπικών δεδομένων**. Το IoT θα πρέπει να ενσωματώνει υψηλά πρότυπα ασφαλείας και προστασίας το προσωπικών δεδομένων.
- **Σεβασμός βασικών ανθρωπίνων δικαιωμάτων**. Το IoT θα πρέπει να σέβεται και να προάγει τα βασικά δικαιώματα των ανθρώπων, συμπεριλαμβανομένων μεταξύ άλλων (και όχι περιοριστικά) το δικαίωμα: στην ζωή, στην ελευθερία, στην ισότητα, στην προσωπική ασφάλεια, στην ιδιωτικότητα, στην αποφυγή διακρίσεων, στην ίση προστασία από τον νόμο, στην εκπαίδευση, στην υγεία.
- **Βιώσιμη οικονομική ανάπτυξη**. Το IoT θα πρέπει να προάγει την οικονομική ευημερία, καθώς και να σέβεται και να προάγει τους στόχους βιώσιμης ανάπτυξης.
- **Συνεργασία.** Το IoT θα πρέπει να προάγει και να αξιοποιεί τη συνεργασία, τις συνέργειες την ανταλλαγή βέλτιστων πρακτικών, και την ανταλλαγή τεχνικής εμπειρογνωμοσύνης μεταξύ:
  α) φορέων εντός της Ελλάδος,
  β) φορέων της Ευρωπαϊκής Ένωσης, και
  γ) φορέων σε διεθνές επίπεδο.
- **Βιωσιμότητα και περιβαλλοντική προστασία**. Το IoT θα πρέπει να σέβεται το περιβάλλον και να προάγει τους εθνικούς περιβαντολογικούς στόχους και στόχους βιωσιμότητας, συμπεριλαμβανομένου και της ενεργειακής αποδοτικότητας.
- **Προσαρμοστικότητα**. Η εθνική πολιτική αναφορικά με το IoT θα πρέπει ταυτόχρονα: α) να προσαρμόζεται δυναμικά με βάσει τις τεχνολογικές και λοιπές εξελίξεις, αλλά και β) να παρέχει ένα σταθερό και προβλέψιμο περιβάλλον που να επιτρέπει τις επενδύσεις και την χρήση του.

Στρατηγικές προτεραιότητες και δράσεις

Η εθνική στρατηγική για το IoT περιλαμβάνει **6 στρατηγικές προτεραιότητες**:



Η κάθε στρατηγική προτεραιότητα εξειδικεύεται σε επιμέρους δράσεις προς υλοποίηση.

Οι προτεινόμενες δράσεις προέκυψαν ακολουθώντας μια ολοκληρωμένη μεθοδολογία διαμόρφωσης της στρατηγικής και λαμβάνοντας υπόψη:

- Την ανάλυση των κλάδων με τη μεγαλύτερη ωριμότητα ωφέλειας υλοποίησης δράσεων
- Την ανάλυση των διεθνών πρακτικών και στρατηγικών
- Την ανάλυση SWOT
- Το όραμα της Ελλάδος και τις κατευθυντήριες αρχές

Στις παρακάτω παραγράφους παρουσιάζονται συνοπτικά οι δράσεις. Η πλήρης περιγραφή των δράσεων θα περιλαμβάνεται σε πλήρη ανάπτυξη στο τελικό κείμενο της στρατηγικής.

1. Επέκταση δικτυακών υποδομών

Η δράση επικεντρώνεται στην επέκταση των δικτυακών υποδομών για την υποστήριξη λύσεων και υπηρεσιών IoT. Η επέκταση αυτή θα γίνει σε ευθυγράμμιση με τις δράσεις που προβλέπονται στο εθνικό ευρυζωνικό σχέδιο 2021-2027 και κάποιες εκ των οποίων είναι ήδη σε εξέλιξη.

Η δράση περιλαμβάνει:

- Επέκταση δικτύων 5G για επικοινωνία υψηλής ταχύτητας και χαμηλής καθυστέρησης (π.χ. σε αυτοκινητόδρομους, υποθαλάσσιο καλωδιακό σύστημα, νησιά)
- Επέκταση δικτύων BLE (Bluetooth Low Energy) και LPWAN (Low Power Wide Area Network) για σύνδεση συσκευών IoT με χαμηλή ισχύ και ευρεία εμβέλεια, όπως το Narrowband IoT (NB-IoT)
- Επέκταση δικτύων Wi-Fi και Zigbee για υποστήριξη IoT συσκευών σε εσωτερικούς και εξωτερικούς χώρους
- Ανάπτυξη και επέκταση δορυφορικών δικτύων χαμηλής τροχιάς (low earth orbit) σε εθνικό ή σε ευρωπαϊκό επίπεδο
- Ανάπτυξη και επέκταση υποδομών για τον συνδυασμό των πολλαπλών δικτύων, όπως ενδεικτικά σε επίπεδο κεντρικής σχεδίασης δικτύων, multi-protocol gateways, shared physical infrastructure, software-defined networking (SDN) και network function virtualization (NFV)

Με αυτή τη δράση, επιτυγχάνεται η ευρεία χρήση των συσκευών IoT σε όλη την επικράτεια, καλύπτοντας τόσο τις αστικές, όσο και τις μη-αστικές περιοχές.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων, Υπουργείο Υποδομών και Μεταφορών, Υπουργείο Ανάπτυξης, Υπουργείο Εθνικής Άμυνας, Υπουργείο Προστασίας του Πολίτη, Υπουργείο Ναυτιλίας και Νησιωτικής Πολιτικής,.

2. Ανάπτυξη ανοικτών χώρων δεδομένων (open data spaces)

Η δράση επικεντρώνεται στην ανάπτυξη ανοικτών χώρων δεδομένων (open data spaces) που μπορούν να χρησιμοποιούνται από ερευνητικούς και ακαδημαϊκούς φορείς, καθώς και από επιχειρήσεις που σχετίζονται με λύσεις πάνω στο διαδίκτυο των πραγμάτων.

Η δράση περιλαμβάνει:

- Διεξαγωγή μελέτης για α) εντοπισμό βέλτιστων διεθνών πρακτικών, β) επικοινωνία και συνεργασία με τους αρμόδιους φορείς, γ) προτεραιοποίηση των πιο χρήσιμων ανοικτών χώρων δεδομένων για εφαρμογές IoT, δ) καθορισμό οδικού χάρτη για υλοποίηση
- Εξασφάλιση χρηματοδότησης για την υλοποίηση των ανοικτών χώρων δεδομένων
- Δημιουργία μονάδων συντονισμού για τη συλλογή και διακυβέρνηση δεδομένων και τη διαμόρφωση και εκτέλεση στρατηγικής για την τεχνητή νοημοσύνη εντός της Ελληνικής κυβέρνησης. Οι μονάδες μπορεί να είναι κοινές με αυτές που έχουν προταθεί στο πλαίσιο του εμβληματικού έργου 1 στο σχέδιο για την μετάβαση στην τεχνητή νοημοσύνη
- Υλοποίηση των ανοικτών χώρων δεδομένων

Με αυτή τη δράση, επιτυγχάνεται η βελτίωση της διαθεσιμότητας των δεδομένων που θα επιτρέψει την ανάπτυξη εφαρμογών IoT.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Υπουργείο Ανάπτυξης, Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας, Υπουργείο Παιδείας, Ακαδημαϊκά Ιδρύματα και Ερευνητικά Κέντρα

3. Καθορισμός ελάχιστων τεχνικών προδιαγραφών και πρωτοκόλλων ελέγχου για δίκτυα

Η δράση επικεντρώνεται στη θεσμοθέτηση και εφαρμογή ελάχιστων τεχνικών προδιαγραφών και πρωτοκόλλων ελέγχου για τα δίκτυα, με σκοπό τη διασφάλιση της ορθής λειτουργίας και της αξιοπιστίας των δικτύων αυτών, τόσο σε δημόσιες όσο και σε ιδιωτικές υποδομές.

Η δράση περιλαμβάνει:

- Καθορισμό ελάχιστων τεχνικών προδιαγραφών για την υλοποίηση των δικτύων, απαίτηση χρήσης ελεγμένων και πιστοποιημένων συσκευών
- Καθιέρωση πρωτοκόλλου ελέγχου για τα νέα δίκτυα με σκοπό την υποχρεωτική δοκιμή δικτύων πριν την παράδοση των έργων, έλεγχο ορθής επικοινωνίας με τις συσκευές σε κρίσιμα σημεία του δικτύου για προκαθορισμένο χρονικό διάστημα
- Υιοθέτηση μηχανισμού συνεχούς ελέγχου και συμμόρφωσης για την πρόληψη παρεμβολών μεταξύ δικτύων, λανθασμένων ρυθμίσεων συσκευών, υποβάθμιση απόδοσης λόγω κορεσμού και διασφάλιση ομαλής λειτουργίας κατάστασης περιαγωγής

Με αυτή τη δράση, επιτυγχάνεται η διασφάλιση της αξιοπιστίας, η μείωση των αποτυχιών, η βελτιστοποίηση απόδοσης και η αρμονική λειτουργία δικτύων σε δημόσιες και ιδιωτικές υποδομές.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

4. Εναρμόνιση με την εθνική στρατηγική κυβερνοασφάλειας

Το Υπουργείο Ψηφιακής Διακυβέρνησης και η Εθνική Αρχή Κυβερνοασφάλειας έχουν καθορίσει την εθνική στρατηγική κυβερνοασφάλειας 2020-2025. Στη στρατηγική αυτή περιλαμβάνονται σημαντικές δράσεις για την ενίσχυση της ασφάλειας και της προστασίας δεδομένων, οι οποίες καλύπτουν μεταξύ άλλων και θέματα IoT.

Η δράση επικεντρώνεται στην επέκταση και την ενίσχυση των δράσεων που περιλαμβάνονται στην εθνική στρατηγική κυβερνοασφάλειας 2020-2025, ώστε να διασφαλιστεί πως αυτές καλύπτουν τις νέες ανάγκες για ασφάλεια και προστασία σε θέματα IoT.

Η επέκταση και ενίσχυση των δράσεων θα λαμβάνει υπόψη της:

- Τις εξελίξεις (τεχνολογικές, κοινωνικές, οικονομικές) που έχουν συντελεστεί τα τελευταία χρόνια, μετά την διαμόρφωση της στρατηγικής κυβερνοασφάλειας
- Τις ευρύτερες ανάγκες που προκύπτουν από την υλοποίηση των υπόλοιπων δράσεων της στρατηγικής IoT

Η δράση περιλαμβάνει:

- Αξιολόγηση της προόδου υλοποίησης των δράσεων της εθνικής στρατηγικής κυβερνοασφάλειας (π.χ. δραστηριότητα "Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)"
- Αξιολόγηση των προσαρμογών που ενδεχομένως απαιτούνται για την κάλυψη νέων θεμάτων IoT (π.χ. καταγραφή πληροφορίας όταν τα συμβάντα ασφαλείας αφορούν συσκευές IoT, συμμόρφωση με διεθνή πρότυπα, πλαίσιο πιστοποίησης συσκευών και λογισμικού, διαχείριση και ενημέρωση λογισμικού, καθορισμός προδιαγραφών ασφαλείας κατά την ανάπτυξη συστημάτων IoT από δημόσιους φορείς, κλπ.)
- Υλοποίηση προσαρμογών για την ενίσχυση της κυβερνοασφάλειας για το IoT
- Παρακολούθηση υλοποίησης προσαρμογών και δυναμικός επανακαθορισμός

Με αυτή τη δράση, επιτυγχάνεται η ενίσχυση της κυβερνοασφάλειας και η προστασία δεδομένων για το IoT.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

5. Καθορισμός και εφαρμογή εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων

Η δράση επικεντρώνεται στον καθορισμό και την εφαρμογή εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων αναφορικά με το IoT, εξασφαλίζοντας τη συμβατότητα και την επικοινωνία μεταξύ διαφορετικών συσκευών και συστημάτων.

Η δράση περιλαμβάνει:

- Καθορισμό εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων
- Εφαρμογή εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων
- Παρακολούθηση εφαρμογής εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων

Με αυτή τη δράση, διασφαλίζεται η συμβατότητα και η επικοινωνία μεταξύ των IoT συσκευών, βελτιώνοντας την απόδοση και την εμπιστοσύνη των χρηστών.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

6. Ανάπτυξη edge data centres

Η δράση επικεντρώνεται στην ανάπτυξη edge data centres για τη διαχείριση, επεξεργασία και αποθήκευση δεδομένων κοντά στην πηγή τους, μειώνοντας τη χρονοκαθυστέρηση (latency) και τη συμφόρηση των κεντρικών υποδομών cloud.

Η δράση περιλαμβάνει:

- Χαρτογράφηση των υφιστάμενων edge data centers και των μελλοντικών αναγκών
- Επιλογή του βέλτιστου τρόπου ανάπτυξης των edge data centers (π.χ. συνεργασία μεταξύ του δημόσιου και ιδιωτικού τομέα, αγορά υπηρεσιών από ιδιωτικό τομέα, ανάπτυξη δημόσιων)

- Δημιουργία edge data centers σε στρατηγικές τοποθεσίες (π.χ. έξυπνες πόλεις, βιομηχανικές ζώνες, αγροτικές περιοχές) για την επεξεργασία IoT δεδομένων κοντά στην πηγή

Με αυτή τη δράση, επιτυγχάνεται μείωση χρονοκαθυστέρησης, βελτιωμένη επεξεργασία δεδομένων και αποσυμφόρηση του cloud.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας, Ακαδημαϊκά Ιδρύματα και Ερευνητικά Κέντρα, Υπουργείο Ανάπτυξης.

7. Πιστοποίηση των IoT συσκευών

Η δράση επικεντρώνεται στην προώθηση της πιστοποίησης των IoT συσκευών για την ασφάλεια, τη συμμόρφωση με τα πρότυπα της ΕΕ και τη διασφάλιση της προστασίας δεδομένων, προκειμένου να εξασφαλιστεί η ασφάλεια των καταναλωτών και η βελτίωση της εμπιστοσύνης στις τεχνολογίες IoT.

Η δράση περιλαμβάνει:

- Εφαρμογή της υποχρεωτικής οδηγίας RED (Radio Equipment Directive (2014/53/EU)) που θα τεθεί σε εφαρμογή από τον Αύγουστο του 2025. Οι IoT συσκευές που διατίθενται στην ελληνική αγορά θα πρέπει να πληρούν τις απαιτήσεις ασφαλείας και κυβερνοασφάλειας που θα ορίζονται από την οδηγία RED
- Προώθηση συστήματος πιστοποίησης που θα επιτρέπει στους κατασκευαστές και τους προμηθευτές IoT συσκευών να πιστοποιούν τα προϊόντα τους σύμφωνα με το πρότυπο ETSI EN 303 645

Η δράση θα ενισχύσει την ασφάλεια των καταναλωτών, θα βελτιώσει την εμπιστοσύνη στις IoT τεχνολογίες και θα διασφαλίσει τη συμμόρφωση με τα πρότυπα της ΕΕ.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων, Υπουργείο Ανάπτυξης.

B Εκπαίδευση, κοινωνική αποδοχή και ευαισθητοποίηση

8. Δημιουργία μηχανισμού υποστήριξης για χρήστες και επαγγελματίες IoT

Η δράση επικεντρώνεται στη δημιουργία ενός μηχανισμού υποστήριξης και στοχεύει στη διευκόλυνση της χρήσης και ανάπτυξης IoT εφαρμογών τόσο για επαγγελματίες όσο και για τελικούς χρήστες.

Η δράση περιλαμβάνει:

- Ανάπτυξη πλατφόρμας για ανταλλαγή γνώσης και πληροφορίας για θέματα που αφορούν IoT, σε αντιστοιχία με παρόμοιες πρωτοβουλίες σε άλλες χώρες, όπως η Γερμανία, και σε ευθυγράμμιση με το σχέδιο μετάβασης της Ελλάδας στην εποχή της τεχνητής νοημοσύνης
- Ανάπτυξη chatbot με χρήση GenAI που να αφορά συσκευές IoT προς εξυπηρέτηση των χρηστών
- Ανάπτυξη forum χρηστών για θέματα του IoT
- Παροχή υπηρεσιών mentor support και καθοδήγησης για ανάπτυξη IoT λύσεων, με εξατομικευμένες συμβουλές και απαντήσεις σε τεχνικά ζητήματα
- Παροχή offline σεμιναρίων, video tutorials και whitepapers, που καλύπτουν τις πτυχές των IoT εφαρμογών από την αρχική εγκατάσταση έως την προηγμένη χρήση και βελτιστοποίηση
- Ενίσχυση με εκπαιδευτικό υλικό IoT της εκπαιδευτικής πλατφόρμας που έχει προταθεί στο πλαίσιο του εμβληματικού έργου 3 στο σχέδιο για την μετάβαση στην τεχνητή νοημοσύνη

Με αυτή τη δράση, οι χρήστες και επαγγελματίες θα έχουν την αναγκαία τεχνογνωσία και υποστήριξη, βελτιώνοντας την απόδοση και αξιοπιστία των IoT λύσεων που αναπτύσσουν ή χρησιμοποιούν.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Παιδείας, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

9. Ενίσχυση προγραμμάτων σπουδών και εκπαίδευσης για IoT

Η δράση επικεντρώνεται στην ενσωμάτωση εξειδικευμένων εκπαιδευτικών προγραμμάτων σε πανεπιστήμια και επαγγελματικές σχολές, προετοιμάζοντας ένα εξειδικευμένο εργατικό δυναμικό σε θέματα IoT.

Η δράση περιλαμβάνει:

- Υποστήριξη των πανεπιστημίων για την ανάπτυξη μαθημάτων σε προπτυχιακό και μεταπτυχιακό επίπεδο καθώς και πιστοποιήσεων, με έμφαση σε θέματα διαλειτουργικότητας, ασφάλειας, ανάπτυξης και καινοτομίας για IoT
- Δημιουργία εργαστηριακών υποδομών για πρακτική εξάσκηση σε IoT
- Εξειδίκευση σε εφαρμογές IoT
- Ενσωμάτωση νέων τεχνολογιών IoT για την εκπαίδευση (π.χ. AR/VR)
- Συνεργασίες με τον ιδιωτικό τομέα για πρακτική άσκηση και σύνδεση της εκπαίδευσης με την αγορά εργασίας

Με αυτήν τη δράση, η Ελλάδα ενισχύει την εκπαίδευση στις τεχνολογίες IoT, δημιουργώντας ένα δυναμικό και εξειδικευμένο οικοσύστημα που ενισχύει την καινοτομία και την ανταγωνιστικότητα.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Παιδείας, Υπουργείο Ψηφιακής Διακυβέρνησης.

Γ Ενίσχυση έρευνας, ανάπτυξης και καινοτομίας

10. Δημιουργία εθνικού IoT testbed για έλεγχο νέων τεχνολογιών και υπηρεσιών

Η δράση επικεντρώνεται στην ανάπτυξη ενός εθνικού testbed για την αξιολόγηση, δοκιμή και χρηματοδότηση νέων IoT λύσεων και τεχνολογιών.

Η δράση περιλαμβάνει:

- Καθορισμό πλάνου ανάπτυξης υποδομών testbed (π.χ. στόχοι, τεχνολογίες, εφαρμογές, τοποθεσίες)
- Ανάπτυξη υποδομών testbed που θα επιτρέπουν τη δοκιμή και αξιολόγηση IoT λύσεων σε πραγματικές συνθήκες
- Δημιουργία διαδικασιών για την επιλογή νέων έργων προς πιθανή χρηματοδότηση
- Σύνδεση με χρηματοδοτικά εργαλεία και φορείς για χρηματοδότηση των έργων

Με αυτή τη δράση, ενισχύεται η έρευνα και η ανάπτυξη νέων IoT τεχνολογιών, διασφαλίζοντας την ποιότητα και αξιοπιστία των λύσεων που αναπτύσσονται στην Ελλάδα.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ανάπτυξης, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

11. Δημιουργία κόμβου και θερμοκοιτίδων καινοτομίας για τεχνολογίες IoT

Η δράση επικεντρώνεται στην ανάπτυξη IoT τεχνολογιών στην Ελλάδα μέσω της δημιουργίας κόμβου και θερμοκοιτίδων καινοτομίας και τεχνολογίας.

- Δημιουργία κόμβου και θερμοκοιτίδων καινοτομίας για την υποστήριξη νεοφυών επιχειρήσεων που δραστηριοποιούνται σε τεχνολογίες IoT
- Ανάπτυξη πιλοτικών έργων και δοκιμαστικών εφαρμογών IoT σε πραγματικές συνθήκες, ώστε να επιταχυνθεί η εμπορική αξιοποίησή τους
- Δημιουργία δικτύου συνεργασίας μεταξύ επιχειρήσεων, startups και φορέων του δημοσίου, με στόχο τη διάδοση και υιοθέτηση καινοτόμων IoT λύσεων

Με αυτή τη δράση, ενισχύεται η ενσωμάτωση των IoT τεχνολογιών τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, δημιουργώντας γόνιμο έδαφος για συνέργειες και καινοτομία, όπως προκύπτει και από την SWOT ανάλυση.

Παράλληλα, προωθείται η ανταλλαγή γνώσεων και βέλτιστων πρακτικών, επιταχύνοντας την ανάπτυξη και υιοθέτηση προηγμένων τεχνολογικών λύσεων που μπορούν να αλλάξουν κλάδους της οικονομίας και της κοινωνίας.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ανάπτυξης, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

Δ Βελτίωση συνεργασίας και εξωστρέφειας

12. Θεσμοθέτηση επιτροπής εμπειρογνωμόνων για το IoT

Η δράση επικεντρώνεται στη θεσμοθέτηση μιας επιτροπής εμπειρογνωμόνων στόχο έχει τη διευκόλυνση της επικοινωνίας και συνεργασίας μεταξύ εμπλεκομένων φορέων στον τομέα του IoT.

Η δράση περιλαμβάνει:

- Σύσταση επιτροπής εμπειρογνωμόνων, η οποία θα αποτελείται από επιστήμονες, ερευνητές, νομικούς εκπροσώπους της βιομηχανίας, της ακαδημαϊκής κοινότητας και δημόσιων φορέων
- Η επιτροπή θα καλύπτει θέματα τεχνολογικά, κοινωνικά, οικονομικά και νομικά
- Συντονισμός δραστηριοτήτων και πρωτοβουλιών στον τομέα του IoT, προωθώντας την ανταλλαγή γνώσεων και πρακτικών μέσω συντονισμένων πρωτοβουλιών και δράσεων
- Δημιουργία πλατφορμών για τη διευκόλυνση της συνεργασίας και ενίσχυση των συνεργασιών μεταξύ των μελών και την υλοποίηση κοινών έργων
- Διοργάνωση σεμιναρίων, εργαστηρίων και εκδηλώσεων για εκπαίδευση και ενημέρωση των εμπλεκομένων, συμβάλλοντας στη διαρκή μάθηση και εξέλιξη των μελών

Με αυτή τη δράση, βελτιώνεται η συνεργασία στον τομέα του IoT, προωθώντας την καινοτομία, την ανάπτυξη, την ασφάλεια και την διαλειτουργικότητα μέσω ανταλλαγής γνώσεων και εμπειριών.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ανάπτυξης, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

13. Συμμετοχή σε εθνικές, ευρωπαϊκές και διεθνείς πρωτοβουλίες που περιλαμβάνουν το IoT

Η δράση επικεντρώνεται στη συμμετοχή σε ευρωπαϊκές και διεθνείς πρωτοβουλίες που προωθούν μεταξύ άλλων την ανταλλαγή τεχνογνωσίας και την ανάπτυξη IoT τεχνολογιών.

Η δράση περιλαμβάνει:

- Ενεργή συμμετοχή σε εθνικές πρωτοβουλίες που αφορούν θέματα που σχετίζονται με το IoT (π.χ. πρωτοβουλίες τεχνητής νοημοσύνης, ανάπτυξης πληροφορικής και τηλεπικοινωνιών, προτυποποίησης, ασφάλειας κλπ.)
- Ενεργή συμμετοχή σε διεθνείς οργανισμούς και προγράμματα που προωθούν την ανάπτυξη, την ασφάλεια και τα πρότυπα των IoT τεχνολογιών, επιτρέποντας στην Ελλάδα να συμβάλλει και να επωφεληθεί από τις διεθνείς προσπάθειες σε αυτόν τον τομέα
- Ενεργή συμμετοχή σε διεθνείς οργανισμούς και προγράμματα που προωθούν την ανάπτυξη, την ασφάλεια και τα πρότυπα των IoT τεχνολογιών, επιτρέποντας στην Ελλάδα να συμβάλλει και να επωφεληθεί από τις διεθνείς προσπάθειες σε αυτόν τον τομέα
- Συμμετοχή σε ευρωπαϊκά και διεθνή προγράμματα έρευνας και ανάπτυξης για την υιοθέτηση καινοτόμων τεχνολογιών και πρακτικών και ανταλλαγή γνώσεων και βέλτιστων πρακτικών
- Δικτύωση με διεθνείς φορείς για συνεργασίες και ανταλλαγή τεχνογνωσίας
- Προώθηση της ανταλλαγής τεχνογνωσίας μεταξύ της ελληνικής και διεθνούς κοινότητας IoT

Με αυτή τη δράση, βελτιώνεται η διεθνή συνεργασία, ενισχύεται η ανταλλαγή τεχνογνωσίας και προωθείται η καινοτομία στον τομέα του IoT.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

14. Δημιουργία εθνικού κέντρου για το IoT

Η δράση επικεντρώνεται στη δημιουργία ενός εθνικού κέντρου για το Διαδίκτυο των Πραγμάτων (IoT). Ο στόχος του κέντρου θα περιλαμβάνει:

- Παρακολούθηση των εξελίξεων στον τομέα του IoT
- Προώθηση της καινοτομίας σε δημόσια και ιδιωτικά έργα IoT με παροχή τεχνογνωσίας
- Ενημέρωση των δημόσιων και ιδιωτικών φορέων για θέματα IoT (π.χ. τεχνολογία, συμμόρφωση)
- Επικαιροποίηση της στρατηγικής IoT

Η δράση περιλαμβάνει:

- Ανάλυση και επιλογή της νομικής και οργανωτικής φύσης του κέντρου (π.χ. επέκταση υφιστάμενου οργανισμού, δημιουργία σύμπραξης)
- Σχεδίαση του κέντρου
- Στελέχωση του κέντρου
- Λειτουργία του κέντρου

Με αυτή τη δράση, επιτυγχάνεται η ενίσχυση της καινοτομίας, η βελτίωση της στρατηγικής και η παρακολούθηση των εξελίξεων στο IoT.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

E Υιοθέτηση της χρήσης σε τομείς προτεραιότητας

15. Υιοθέτηση χρήσης IoT στις έξυπνες πόλεις

Η δράση επικεντρώνεται στην ενσωμάτωση του IoT στις έξυπνες πόλεις, με στόχο τη βελτίωση της διαχείρισης του αστικού περιβάλλοντος και της καθημερινότητας των πολιτών. Προτεραιότητα θα δοθεί στους 20 πιο μεγάλους δήμους και περιφέρειες της Ελλάδος.

Η υιοθέτηση της χρήσης IoT στις έξυπνες πόλεις είναι μια ευκαιρία για την Ελλάδα, όπως αυτή αποτυπώνεται και στην ανάλυση SWOT. Ο λόγος είναι ότι στην Ελλάδα ένα πολύ μεγάλο ποσοστό του πληθυσμού είναι συγκεντρωμένο σε λίγες μεγάλες πόλεις. Ως εκ τούτου, η ανάπτυξη λύσεων IoT στις πόλεις αυτές μπορεί να βελτιώσει το επίπεδο ζωής πολλών πολιτών.

Η ενέργειες που θα μπορούσαν να αποφασιστούν να υλοποιηθούνε από το Υπουργείο Εσωτερικών σε συνεργασία με την επιτροπή εμπειρογνωμόνων και εθνικό κέντρο για το IoT περιλαμβάνουν μεταξύ άλλων:

- Συλλογή διεθνών βέλτιστων πρακτικών έξυπνων πόλεων από πόλεις του εξωτερικού
- Αξιοποίηση τεχνογνωσίας διεθνών συντονιστικών ομάδων όπως π.χ. οι ISO, IEC και ITU-T καθώς και η Global Standards Collaboration
- Συλλογή ελληνικών βέλτιστων πρακτικών έξυπνων πόλεων από πόλεις της Ελλάδος (π.χ. Τρίκαλα)
- Συλλογή και οργάνωση υποστηρικτικού υλικού για την επίσπευση των διαδικασιών (π.χ. παλαιότερες διακηρύξεις, προδιαγραφές, εμπειρίες από το τι λειτούργησε και τι όχι σε προηγούμενες υλοποιήσεις)
- Επικοινωνία με τους μεγαλύτερους δήμους και περιφέρειες για ανταλλαγή πληροφοριών

Η ενέργειες που θα μπορούσαν να αποφασιστούν να υλοποιηθούν από τους επιμέρους δήμους και περιφέρειες, περιλαμβάνουν ενδεικτικά μεταξύ άλλων:

- Ανάλυση των αναγκών του συγκεκριμένου δήμου
- Προκήρυξη και ανάθεση έργων έξυπνης πόλης
- Υλοποίηση έργων έξυπνης πόλης

Η ενσωμάτωση IoT στις έξυπνες πόλεις αναμένεται να βελτιώσει την εμπειρία των κατοίκων, την ποιότητα ζωής, την ασφάλεια και τη καθημερινότητα τους.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Εσωτερικών - Δήμοι και Περιφέρειες, Υπουργείο Ανάπτυξης, Υπουργείο Υποδομών και Μεταφορών, Υπουργείο Περιβάλλοντος και Ενέργειας, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

16. Υιοθέτηση χρήσης IoT στον τουρισμό

Η δράση επικεντρώνεται στην ενσωμάτωση του IoT στον τουρισμό, με στόχο την αναβάθμιση των τουριστικών υπηρεσιών.

Η υιοθέτηση της χρήσης IoT στον τουρισμό είναι μια ευκαιρία για την Ελλάδα, όπως αυτή αποτυπώνεται και στην ανάλυση SWOT. Ο τουριστικός κλάδος της χώρας έχει ένα σημαντικό μέγεθος το οποίο επιτρέπει την ανάπτυξη καινοτόμων IoT λύσεων. Οι λύσεις αυτές μπορούν να βελτιώσουν το τουριστικό προϊόν καθώς και να εξαχθούν παγκοσμίως.

Η δράση και οι ενέργειες που θα μπορούσαν να αποφασιστούν να υλοποιηθούνε από το Υπουργείο Τουρισμού περιλαμβάνουν ενδεικτικά μεταξύ άλλων την αξιοποίηση του IoT για:

- Εγκατάσταση έξυπνων συστημάτων πλοήγησης για την παροχή πληροφοριών σε πραγματικό χρόνο σχετικά με αξιοθέατα, εστιατόρια και εκδηλώσεις
- Χρήση αισθητήρων σε τουριστικά σημεία για την παρακολούθηση της επισκεψιμότητας και τη διαχείριση του πλήθους, βελτιώνοντας την ασφάλεια και την άνεση των επισκεπτών

Η ενσωμάτωση IoT στον τουρισμό αναμένεται να βελτιώσει την εμπειρία των επισκεπτών, την ασφάλεια και τη διαχείριση του πλήθους.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Τουρισμού, Υπουργείο Πολιτισμού, Υπουργείο Ανάπτυξης, Υπουργείο Υποδομών και Μεταφορών.

17. Υιοθέτηση χρήσης IoT στην ναυτιλία

Η δράση επικεντρώνεται στην ενσωμάτωση του IoT στη ναυτιλία, με στόχο τη βελτίωση της διαχείρισης των πλοίων και των λιμένων μέσω της χρήσης IoT τεχνολογιών.

Η υιοθέτηση της χρήσης IoT στην ναυτιλία είναι μια ευκαιρία για την Ελλάδα, όπως αυτή αποτυπώνεται και στην ανάλυση SWOT. Η Ελλάδα παραμένει η μεγαλύτερη ναυτιλιακή χώρα στον κόσμο. Αυτό αποτελεί μεγάλη ευκαιρία για ανάπτυξη καινοτόμων IoT λύσεων που θα μπορούσαν να βελτιώσουν την ναυσιπλοΐα και τον εφοπλισμό καθώς και να εξαχθούν παγκοσμίως.

Οι ενέργειες που θα μπορούσαν να αποφασιστούν να υλοποιηθούνε από το Υπουργείο Ναυτιλίας και Νησιωτικής Πολιτικής περιλαμβάνουν ενδεικτικά μεταξύ άλλων την αξιοποίηση του IoT για:

- Δημιουργία δικτύων αισθητήρων για μέτρηση ρύπων, θορύβου & ποιότητας νερού εντός των λιμένων και σε σημεία αγκυροβολίας πλοίων
- Έξυπνα συστήματα ελέγχου ναυσιπλοΐας, που επιτρέπουν την αποφυγή συγκρούσεων και τη δυναμική καθοδήγηση των πλοίων σε πραγματικό χρόνο, ιδιαίτερα σε πυκνοκίνητες θαλάσσιες περιοχές
- Παρακολούθηση και ανάλυση της κατάστασης του εξοπλισμού και των υποδομών των λιμένων, που βοηθούν στον προγραμματισμό συντήρησης και στην αποφυγή προβλημάτων
- Αυτοματοποίηση και παρακολούθηση σε πραγματικό χρόνο της φόρτωσης και εκφόρτωσης εμπορευμάτων, επιτρέποντας ταχύτερη και πιο ακριβή διαχείριση των λιμενικών υποδομών και των φορτίων

Η ενσωμάτωση IoT στη ναυτιλία αναμένεται να βελτιώσει την αποδοτικότητα, την ασφάλεια και τη διαχείριση φορτίου και εξοπλισμού.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Ναυτιλίας και Νησιωτικής Πολιτικής, Υπουργείο Ανάπτυξης, Υπουργείο Υποδομών και Μεταφορών, Υπουργείο Εσωτερικών, Υπουργείο Περιβάλλοντος και Ενέργειας.

18. Υιοθέτηση χρήσης IoT στην δημόσια διοίκηση

Η δράση επικεντρώνεται στην ενσωμάτωση του IoT στη δημόσια διοίκηση, με στόχο τη βελτίωση της αποδοτικότητας, της διαφάνειας και της εξυπηρέτησης των πολιτών μέσω έξυπνων τεχνολογιών. Η υιοθέτηση της χρήσης IoT στην δημόσια διοίκηση είναι μια ευκαιρία για την Ελλάδα, όπως αυτή αποτυπώνεται και στην ανάλυση SWOT.

Οι ενέργειες που θα μπορούσαν να αποφασιστούν να υλοποιηθούνε από το Υπουργείο Εσωτερικών περιλαμβάνουν ενδεικτικά μεταξύ άλλων την αξιοποίηση του IoT για:

- Εγκατάσταση έξυπνων συστημάτων διαχείρισης κτιρίων για την ενεργειακή απόδοση, την ασφάλεια και τη βελτιστοποίηση των δημόσιων κτιρίων
- Ανάπτυξη έξυπνων συστημάτων εξυπηρέτησης πολιτών, όπως διαδραστικοί σταθμοί πληροφόρησης και αυτοματοποιημένες διαδικασίες για αιτήσεις και πληρωμές
- Ανάπτυξη συστημάτων παρακολούθησης και ανάλυσης δεδομένων για την αποδοτικότητα των δημόσιων υπηρεσιών με στόχο την αναγνώριση σημείων βελτίωσης και την ενίσχυση της διαφάνειας στη διαχείριση των πόρων

Σε κεντρικό επίπεδο, μπορεί να καθοριστούν προδιαγραφές για την υλοποίηση έργων IoT

- Συλλογή και οργάνωση υποστηρικτικού υλικού για την επίσπευση των διαγωνιστικών διαδικασιών (π.χ. απαιτήσεις, προδιαγραφές, παλαιότερες διακηρύξεις)
- Παροχή πρόσβασης και τεχνογνωσίας στους φορείς του δημοσίου που αναλαμβάνουν τη διενέργεια σχετικών διαγωνισμών
- Διασφάλιση και έλεγχο ότι όλα τα έργα IoT ακολουθούν τις κατευθυντήριες γραμμές λειτουργίας με τεχνητή νοημοσύνη, όπως αυτές προτάθηκαν στο σχέδιο για την μετάβαση στην ΤΝ

Η ενσωμάτωση IoT στη Δημόσια Διοίκηση αναμένεται να βελτιώσει την ποιότητα ζωής των πολιτών, την αποδοτικότητα των υπηρεσιών και τη βιωσιμότητα των δημόσιων υποδομών.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Εσωτερικών, Υπουργείο Ψηφιακής Διακυβέρνησης, Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων.

ΣΤ Καθορισμός εθνικού ρυθμιστικού, κανονιστικού και νομοθετικού πλαισίου

Το κανονιστικό πλαίσιο που διέπει τη χρήση συσκευών και εφαρμογών Διαδικτύου των Πραγμάτων (Internet of Things και εφεξής IoT) πρέπει να γίνεται κατανοητό, να ερμηνεύεται, να ενισχύεται και να εμπλουτίζεται υπό το φως βασικών αρχών που διασφαλίζουν την ισορροπία μεταξύ των ωφελειών από τη χρήση αυτών των τεχνολογιών με δικαιώματα και έννομα συμφέροντα άλλων προσώπων καθώς και το δημόσιο συμφέρον.

- **Αρχή της μη βλάβης**. Η αρχή της μη βλάβης (do no harm) επιβάλλει τον σχεδιασμό και τη χρήση των IoT με τρόπο τέτοιο ώστε να ελαχιστοποιούνται οι αρνητικές συνέπειες στην ασφάλεια των πολιτών, το περιβάλλον, τα δικαιώματα των προσώπων ή και την κοινωνία στο σύνολό της. Η εν λόγω αρχή πρέπει να τηρείται τόσο από τους σχεδιαστές και κατασκευαστές των σχετικών εφαρμογών IoT όσο και από τους χρήστες/ χειριστές αυτών.
- **Αρχή ενημέρωσης – διαφάνειας της χρήσης των IoTs.** Η αρχή της ενημέρωσης και της διαφάνειας στη χρήση των IoT διασφαλίζει ότι οι πολίτες και οι ενδιαφερόμενοι φορείς είναι επαρκώς και καταλλήλως ενημερωμένοι για τη χρήση των IoT, τους σκοπούς των χρήσεων, τις δυνατότητες και τους περιορισμούς τους, καθώς και για τον αντίκτυπο που μπορεί να έχουν στην κοινωνία, την ασφάλεια και σε δικαιώματα όπως η ιδιωτικότητα.
- **Αρχή προστασίας της προσωπικότητας και της ιδιωτικότητας**. Όταν γίνεται χρήση IoT, θα πρέπει να διασφαλίζεται η προστασία δικαιωμάτων που συνδέονται με την προσωπικότητα και την ιδιωτικότητα των ατόμων. Η διασφάλιση αυτή καθίσταται επιτακτική, καθώς οι εν λόγω συσκευές μπορούν να συλλέγουν δεδομένα, συμπεριλαμβανομένων δεδομένων εικόνας ή ήχου, συχνά χωρίς να γίνονται αντιληπτές από τα πρόσωπα.
- **Αρχή της πρόληψης και της προφύλαξης.** Οι ανωτέρω αρχές επιβάλλουν τη λήψη προληπτικών μέτρων για την ελαχιστοποίηση γνωστών κινδύνων που σχετίζονται με την ασφάλεια, την ιδιωτικότητα και την

κυβερνοασφάλεια. Στην περίπτωση των IoT, η πρόληψη απαιτεί όχι μόνο την ύπαρξη και τήρηση ενός αυστηρού ρυθμιστικού πλαισίου που θα διασφαλίζει την ασφαλή λειτουργία αυτών των τεχνολογιών, αλλά κυρίως την «εξατομικευμένη» μελέτη, σε προγενέστερο στάδιο, των πιθανών επιπτώσεων ενός έργου μεγάλης κλίμακας.

- **Αρχή εμπιστοσύνης και αποδοχής.** Η ένταξη και διάδοση της χρήσης των τεχνολογιών αυτών σε διάφορες ιδιωτικές και δημόσιες δραστηριότητες και δράσεις αλλά και στην καθημερινότητα προϋποθέτει την εμπιστοσύνη και την αποδοχή των πολιτών και εν γένει των ενδιαφερομένων μερών. Συνεπώς για τον σχεδιασμό, προγραμματισμό και υλοποίηση τέτοιων χρήσεων θα πρέπει να λαμβάνονται υπόψιν ανησυχίες και επιφυλάξεις για την ασφάλεια, τα δικαιώματα και τις επιπτώσεις στη ζωή και την κοινωνία και αντίστοιχα να επιδιώκεται η αντιμετώπισή τους ή/και η ενημέρωση των πολιτών ως προς τις περιστάσεις και διαστάσεις των χρήσεων, ώστε να υπάρξει μια εξορθολογισμένη στάση έναντι των τεχνολογιών αυτών.
- **Αρχή "by design".** Αναφορικά με τις τεχνολογίες IoT, η συγκεκριμένη αρχή αποτυπώνεται στην ενσωμάτωση σε αυτά μηχανισμών ασφαλείας προκειμένου να επιτυγχάνεται η προστασία από επιθέσεις και η ασφαλής διαχείριση δεδομένων, στην διασφάλιση της by default προστασίας των προσωπικών δεδομένων μέσω τεχνολογιών παρακολούθησης, όπως κάμερες και αισθητήρες, οι οποίες κατ' εφαρμογή της βασικής αρχής της ελαχιστοποίησης περιορίζουν τη συλλογή δεδομένων σε αυτό που είναι απολύτως απαραίτητο για τη λειτουργία του συστήματος.
- **Αρχή της ασφάλειας δικτύων, υπηρεσιών και δεδομένων.** Η ανωτέρω αρχή καθίσταται απαραίτητη, καθώς η συνεχής διασύνδεση συσκευών αυξάνει τους κινδύνους κυβερνοεπιθέσεων, απειλώντας την ιδιωτικότητα, τη λειτουργικότητα των συστημάτων και την κοινωνική εμπιστοσύνη στα συστήματα IoT. Η ασφάλεια δικτύου, μέσω κρυπτογράφησης και ασφαλούς ταυτοποίησης, προστατεύει από επιθέσεις όπως Man-in-the-Middle (όπου τρίτος εισβολέας παρεμβάλλεται στην επικοινωνία μεταξύ δύο μερών εν αγνοία τους), ενώ η προστασία υπηρεσιών και δεδομένων, με ενημερώσεις λογισμικού, ελέγχους ταυτότητας και κρυπτογράφηση, αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση και διαρροές.

Με βάση τις παραπάνω αρχές, οι προτεινόμενες δράσεις περιλαμβάνουν:

19. Ενημέρωση τελικών χρηστών σχετικά με τα δικαιώματα και τις υποχρεώσεις τους από τη χρήση τεχνολογιών IoT

Η δράση επικεντρώνεται στη κατάρτιση και δημοσίευση μιας σαφούς και αναλυτικής πολιτικής στην επίσημη ιστοσελίδα κάθε φορέα που ενδέχεται να χρησιμοποιεί τεχνολογίες IoT για την παροχή των υπηρεσιών του.

Οι σχετικές ενημερώσεις, σε συμμόρφωση με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και άλλων σχετικών νομοθετικών πλαισίων, θα πρέπει να παρέχουν επαρκείς πληροφορίες στους τελικούς χρήστες σχετικά με την πιθανή συλλογή και επεξεργασία των προσωπικών δεδομένων τους μέσω των εν λόγω τεχνολογιών.

Συγκεκριμένα, η σχετική ανάρτηση θα πρέπει κατ' ελάχιστον να αναφέρει τις κατηγορίες των προσωπικών δεδομένων που συλλέγονται, τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, τον σκοπό αυτής της συλλογής, καθώς και τη νομική βάση της επεξεργασίας (συγκατάθεση, σύμβαση, νομική υποχρέωση, ζωτικό συμφέρον, δημόσιο συμφέρον, έννομο συμφέρον) και να ενημερώνει τα πρόσωπα που αφορά η επεξεργασία προσωπικών δεδομένων μέσω IoT για τα δικαιώματά τους.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

20. Θέσπιση νομοθετικών μέτρων σχετικά με την ευθύνη των μερών του κύκλου εργασίας συσκευών IoT

Η δράση επικεντρώνεται στη θέσπιση νομοθετικών μέτρων σχετικά με την ευθύνη των μερών του κύκλου εργασίας συσκευών IoT.

Με δεδομένο ότι η χρήση συστημάτων IoT μπορεί να επιφέρει προσβολή δικαιωμάτων των προσώπων, ζημία ή ηθική βλάβη προτείνεται η εξέταση της εισαγωγής ενός πλέγματος κανόνων ποινικής και αστικής ευθύνης ή/και επιβολής διοικητικών κυρώσεων που θα αφορούν σε όλο το φάσμα των εμπλεκομένων μερών, εκτεινόμενης της σχετικής ευθύνης από τους κατασκευαστές συσκευών IoT, τους χειριστές του λογισμικού τους, έως και τους διαθέτοντες τις εν λόγω συσκευές στην αγορά.

Ο σκοπός δεν είναι να προστεθούν επιπλέον ρυθμίσεις πέραν αυτών που γενικώς ισχύουν αλλά να εξεταστεί η ειδικότητα και η επάρκεια των τελευταίων για την αντιμετώπιση των ζητημάτων που θέτει η χρήση IoT. Ενδεικτικά, δύναται να προβλεφθεί:

- Αστική ευθύνη των κατασκευαστών/κατόχων λογισμικού IoT για αποζημίωση ατόμων επί των οποίων διενεργήθηκε λανθασμένη ιατρική διάγνωση μέσω φορητής συσκευής παρακολούθησης της υγείας τους,
- Ποινική ευθύνη για τη μη επίδειξη δέουσας επιμέλειας /αμέλεια κατά την υποστήριξη ενάσκησης τηλεϊατρικής μέσω συστημάτων IoT, η οποία προκάλεσε – ακόμη και απλή – βλάβη ατόμου

Οι διοικητικές κυρώσεις μπορεί να συνίστανται σε επιβολή διοικητικών προστίμων. Σε κάθε περίπτωση, η πρόβλεψη των σχετικών κυρώσεων πρέπει να είναι σαφής και ανάλογη της σοβαρότητας της παράβασης.

Σοβαρά ζητήματα τίθενται και ως προς τον καθορισμό της ενδοσυμβατικής ευθύνης, η οποία δύναται να ανακύψει από τη χρήση των εν λόγω συσκευών, όπως ο προσδιορισμός του φέροντος την ευθύνη συντήρησης και λειτουργίας συσκευών (κατασκευαστής, δημιουργός του λογισμικού, πωλητής), λαμβάνοντας υπόψη και τα ζητήματα ευθύνης από την πώληση ελαττωματικών προϊόντων.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

21. Υιοθέτηση κανόνων για τη δημιουργία καινοτόμων ρυθμιστικών πεδίων

Η δράση επικεντρώνεται στην αξιοποίηση κανόνων και τη συμπλήρωση του κανονιστικού πλαισίου για την ανάπτυξη, λειτουργία και υποστήριξη μορφωμάτων όπως τα Regulatory Sandboxes (Κανονιστικά Περιβλήματα Ελέγχου-Κανονιστικά Δοκιμαστήρια), τα οποία επιτρέπουν σε δημόσιους και ιδιωτικούς φορείς να δοκιμάσουν νέα προϊόντα και υπηρεσίες σε ελεγχόμενο περιβάλλον με χαλαρότερη ρυθμιστική εποπτεία, ή τα Open Data Spaces που επιτρέπουν τη συλλογή, ανταλλαγή και χρήση δεδομένων μεταξύ οργανισμών και επιχειρήσεων, προάγοντας τη διαφάνεια και την καινοτομία.

Ενδεικτικά, οι σχετικές ρυθμίσεις οφείλουν να διασφαλίζουν ότι οι χρήστες μπορούν να επωφελούνται από τα δεδομένα, χωρίς να παραβιάζουν δικαιώματα ιδιοκτησίας, διανοητικής ιδιοκτησίας ή προστασίας προσωπικών δεδομένων, να καθορίζουν τη διαδικασία υποβολής αιτήσεων από εταιρείες που επιθυμούν να συμμετάσχουν στο regulatory sandbox, να διασφαλίζουν τη συμμόρφωση αυτών με βασικές αρχές προστασίας καταναλωτών, καθώς και να ορίζουν το χρονικό διάστημα κατά το οποίο οι συμμετέχουσες επιχειρήσεις μπορούν να διεξάγουν τις δοκιμές τους.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

22. Δημιουργία Κεντρικού Αποθετηρίου πρωτοκόλλων και προτύπων συσκευών IoT

Η δράση επικεντρώνεται στη δημιουργία ενός ψηφιακού κεντρικού αποθετηρίου, στο οποίο θα συγκεντρώνονται όλα τα ισχύοντα και εφαρμόσιμα πρωτόκολλα και πρότυπα που σχετίζονται με τις IoT συσκευές, καλύπτοντας όλο το φάσμα του κύκλου ζωής τους, από την κατασκευή μέχρι τη λειτουργία και τη διάθεσή τους.

Στόχος της δράσης είναι ο μετριασμός του μεγάλου κατακερματισμού των διαφόρων πρωτοκόλλων και προτύπων κατασκευής και λειτουργίας IoT, τα οποία είναι ελεύθερα επιλέξιμα από τα ενδιαφερόμενα μέρη και τα οποία, εάν επιλεχθούν αυθαίρετα μπορούν να δημιουργήσουν ζητήματα συμμόρφωσης, διαλειτουργικότητας και ασφάλειας των συσκευών.

Ειδικότερα, το αποθετήριο, το οποίο θα τελεί υπό την επίβλεψη ενός φορέα τήρησης, προτείνεται να διαρθρωθεί με βάση την υποχρεωτικότητα ή μη των πρωτοκόλλων καθώς και το διαχωρισμό τους ανά τομέα ενδιαφέροντος (υγεία, γεωργία κ.α.). Επιπλέον, η εκάστοτε αρμόδια αρχή/φορέας προς έκδοση ενός νέου ή αναθεώρηση ενός υπάρχοντος πρωτοκόλλου θα υποχρεούται να ενημερώνει το Κεντρικό Αποθετήριο σχετικά, ώστε να διασφαλίζεται η συνεχής ενημέρωση των χρηστών αυτού.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

23. Διενέργεια εκτίμησης κινδύνου και αντικτύπου σε περιπτώσεις χρήσης IoT υψηλής επικινδυνότητας

Η δράση επικεντρώνεται στη καθιέρωση υποχρέωσης διενέργειας εκτίμησης κινδύνου και αντικτύπου προ της χρήσης τους. Η εκτίμηση κινδύνου θα λειτουργήσει ως εργαλείο προσδιορισμού κινδύνων και αποτελεσματικότητας και διασφάλισης της προστασίας των δικαιωμάτων όλων των εμπλεκόμενων μερών. Στόχος είναι η διαχείριση της επικινδυνότητας ενόψει της φύσης των IoT τεχνολογιών

Η εκτίμηση των κινδύνων και επιπτώσεων που συνεπάγεται μια απόφαση χρήσης τεχνολογίας IoT, ιδίως επί τη βάσει της ανάλυσης του κόστους και του οφέλους το οποίο προκαλεί, θεωρείται κομβική για την αξιολόγηση της σκοπιμότητάς και των συνεπειών της. Είναι επιπλέον κρίσιμη για τη διασφάλιση της τεχνολογικής βιωσιμότητας, της νομικής συμμόρφωσης και της κοινωνικής αποδοχής των εν λόγω τεχνολογιών.

Ειδικότερα, κατά τη διενέργεια της προαναφερθείσας μελέτης, θα πρέπει να λαμβάνονται υπόψιν ο επιδιωκόμενος σκοπός της χρήσης, οι δυνατότητες, τα τεχνικά χαρακτηριστικά και οι παράμετροι λειτουργίας του υπό κρίση συστήματος, οι κατηγορίες δεδομένων που συλλέγονται, τυγχάνουν επεξεργασίας ή εισάγονται στο σύστημα ή παράγονται από αυτό, καθώς και οι κίνδυνοι που ενδέχεται να προκύψουν για τα δικαιώματα, τις ελευθερίες και τα έννομα συμφέροντα των φυσικών ή νομικών προσώπων, στα οποία αφορά ή τα οποία επηρεάζει η λήψη της απόφασης. Εάν υφίστανται υποχρεώσεις διενέργειας εκτίμησης αντικτύπου με βάση άλλα κανονιστικά πλαίσια οι εκτιμήσεις αυτές θα μπορούσαν να διενεργηθούν συνδυαστικά.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

24. Εισαγωγή νομοθετικών ρυθμίσεων προς διασφάλιση συμμόρφωσης όλων των συσκευών IoT, ανεξαρτήτως προέλευσης, με τις υφιστάμενες απαιτήσεις κυβερνοασφάλειας

Η δράση επικεντρώνεται στη διασφάλιση ότι όλες οι συσκευές IoT, ακόμη και όσες κυκλοφόρησαν πριν τη δημοσίευση των Ευρωπαϊκών Κανονισμών για την Κυβερνοασφάλεια αλλά και όσες προέρχονται από τρίτες χώρες, συμμορφώνονται με τους σχετικούς κανόνες. Κρίνεται αναγκαία η συμπλήρωση του κανονιστικού πλαισίου, και συγκεκριμένα η υιοθέτηση αυστηρών και ενιαίων διαδικασιών πιστοποίησης, ώστε να διασφαλιστεί ότι οι συσκευές πληρούν τα απαραίτητα πρότυπα ασφάλειας.

Πιο συγκεκριμένα, απαιτείται η θέσπιση διαδικασιών αναβάθμισης των συσκευών που ήδη κυκλοφορούν, οι οποίες θα διασφαλίζουν ότι γίνεται σωστή διαχείριση των προσωπικών και ιδίως των ευπαθών δεδομένων, καθώς και εφαρμογή ενισχυμένων προτύπων κρυπτογράφησης και προστασίας από κυβερνοεπιθέσεις.

Προτεινόμενοι εμπλεκόμενοι φορείς: Υπουργείο Δικαιοσύνης, Υπουργείο Ψηφιακής Διακυβέρνησης.

Προτεραιοποίηση

Οι παραπάνω δράσεις προτεραιοποιούνται με βάση την εκτίμηση της χρονικής διάρκειας που απαιτείται για την υλοποίησή τους, ως βραχυπρόθεσμες, μεσοπρόθεσμες, ή μακροπρόθεσμες.

- Οι βραχυπρόθεσμες δράσεις αναμένεται να υλοποιηθούν σε συντομότερο χρονικό διάστημα, και έχουν ως στόχο την άμεση αντιμετώπιση προκλήσεων, ή/και την επίτευξη γρήγορων αποτελεσμάτων
- Οι μεσοπρόθεσμες δράσεις αναμένεται να απαιτήσουν περισσότερο χρόνο για την υλοποίησή τους
- Οι μακροπρόθεσμες δράσεις αφορούν στρατηγικές επενδύσεις και πρωτοβουλίες που εκτιμάται πως θα έχουν μακροχρόνιο ορίζοντα υλοποίησης

Η παρακάτω προτεραιοποίηση θα εξειδικευτεί κατά την διαμόρφωση της πλήρους στρατηγικής σε έναν προτεινόμενο οδικό χάρτη για την υλοποίηση των δράσεων.

Προτεραιότητα	#	Δράση	Βραχυπρόθεσμη	Μεσοπρόθεσμη	Μακροπρόθεσμη
Α	1	Επέκταση δικτυακών υποδομών		✓	
Α	2	Ανάπτυξη ανοικτών χώρων δεδομένων (open data spaces)		✓	
Α	3	Καθορισμός ελάχιστων τεχνικών προδιαγραφών και πρωτοκόλλων ελέγχου για δίκτυα	✓		
Α	4	Εναρμόνιση με την εθνική στρατηγική κυβερνοασφάλειας	✓		
Α	5	Καθορισμός και εφαρμογή εθνικών κατευθυντήριων οδηγιών, προτύπων διαλειτουργικότητας και πρωτοκόλλων	✓		
Α	6	Ανάπτυξη edge data centres			✓
Α	7	Πιστοποίηση των IoT συσκευών		✓	
Β	8	Δημιουργία μηχανισμού υποστήριξης για χρήστες και επαγγελματίες IoT		✓	
Β	9	Ενίσχυση προγραμμάτων σπουδών και εκπαίδευσης για IoT	✓		
Γ	10	Δημιουργία εθνικού IoT testbed για έλεγχο νέων τεχνολογιών και υπηρεσιών		✓	
Γ	11	Δημιουργία κόμβου και θερμοκοιτίδων καινοτομίας για τεχνολογίες IoT		✓	
Δ	12	Θεσμοθέτηση επιτροπής εμπειρογνωμόνων για το IoT	✓		
Δ	13	Συμμετοχή σε εθνικές, ευρωπαϊκές και διεθνείς πρωτοβουλίες που περιλαμβάνουν το IoT	✓		
Δ	14	Δημιουργία εθνικού κέντρου για το IoT		✓	
Ε	15	Υιοθέτηση χρήσης IoT στις έξυπνες πόλεις	✓		
Ε	16	Υιοθέτηση χρήσης IoT στον τουρισμό		✓	
Ε	17	Υιοθέτηση χρήσης IoT στην ναυτιλία		✓	
Ε	18	Υιοθέτηση χρήσης IoT στην δημόσια διοίκηση			✓
ΣΤ	19	Ενημέρωση τελικών χρηστών σχετικά με τα δικαιώματα και τις υποχρεώσεις τους από τη χρήση τεχνολογιών IoT	✓		
ΣΤ	20	Θέσπιση νομοθετικών μέτρων σχετικά με την ευθύνη των μερών του κύκλου εργασίας συσκευών IoT		✓	
ΣΤ	21	Υιοθέτηση κανόνων για τη δημιουργία καινοτόμων ρυθμιστικών πεδίων	✓		

Προτεραιότητα	#	Δράση	Βραχυπρόθεσμη	Μεσοπρόθεσμη	Μακροπρόθεσμη
ΣΤ	22	Δημιουργία κεντρικού αποθετηρίου πρωτοκόλλων και προτύπων συσκευών IoT	✓		
ΣΤ	23	Διενέργεια εκτίμησης κινδύνου και αντικτύπου σε περιπτώσεις χρήσης IoT υψηλής επικινδυνότητας	✓		
ΣΤ	24	Εισαγωγή νομοθετικών ρυθμίσεων προς διασφάλιση συμμόρφωσης όλων των συσκευών IoT, ανεξαρτήτως προέλευσης, με τις υφιστάμενες απαιτήσεις κυβερνοασφάλειας	✓		

Πίνακας 3: Προτεραιοποίηση δράσεων με βάση τον χρονικό ορίζοντα ολοκλήρωσης