ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ 'ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ'

ΔΙΠΛΩΜΑΤΙΚΗ ΔΙΑΤΡΙΒΗ

ΠΛΑΙΣΙΟ ΓΙΑ ΤΗ ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΤΩΝ ΠΟΛΙΤΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

του

Φώτιου Παπαγιαννίδη

Υπεύθυνος καθηγητής: Ηλιούδης Χρήστος

Θεσσαλονίκη, Φεβρουάριος, 2023

Εκπονηθείσα Διπλωματική Εργασία απαραίτητη
για τη λήψη του Μεταπτυχιακού Διπλώματος

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ 'ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ'

ΔΙΠΛΩΜΑΤΙΚΗ ΔΙΑΤΡΙΒΗ

ΠΛΑΙΣΙΟ ΓΙΑ ΤΗ ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΤΩΝ ΠΟΛΙΤΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

του

Φώτιου Παπαγιαννίδη

Υπεύθυνος καθηγητής: Ηλιούδης Χρήστος

Θεσσαλονίκη, Φεβρουάριος, 2023

Εκπονηθείσα Διπλωματική Εργασία απαραίτητη
για τη λήψη του Μεταπτυχιακού Διπλώματος

Η παρούσα διπλωματική εργασία
εγκρίνεται για παρουσίαση.

Ηλιούδης Χρήστος,

Υπογραφή: ……..

Ημερομηνία: ……..

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών ‘Ευφυείς Τεχνολογίες Διαδικτύου’ του Τμήματος Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος. Η έγκριση της δεν υποδηλώνει απαραιτήτως και την αποδοχή των απόψεων του συγγραφέα εκ μέρους του Διεθνούς Πανεπιστημίου της Ελλάδος.

Βεβαιώνω ότι είμαι αποκλειστικός συγγραφέας της παρούσας μεταπτυχιακής διπλωματικής εργασίας και ότι κάθε βοήθεια που είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία.

Βεβαιώνω, επίσης, ότι έχω σαφώς αναφέρει όλες τις δευτερογενείς πηγές συλλογής δεδομένων τις οποίες χρησιμοποίησα για την συγγραφή της παρούσας εργασίας. Το κείμενο της εργασίας είναι γραμμένο με τα δικά μου λόγια και δεν αποτελεί προϊόν λογοκλοπής από τρίτες πηγές. Σε περίπτωση αυτούσιας αντιγραφής προτάσεων από τρίτες πηγές έχω χρησιμοποιήσει εισαγωγικά.

Φώτιος Παπαγιαννίδης,

Υπογραφή: ……..

Ημερομηνία: ……..

ΑΦΙΕΡΩΣΗ

Η παρούσα διπλωματική εργασία αφιερώνεται στα παιδιά μου, Νικόλαο - Παΐσιο και Βασιλική.

Θεσσαλονίκη, Φεβρουάριος, 2023

ΠΡΟΛΟΓΟΣ - ΕΥΧΑΡΙΣΤΙΕΣ

Από τη θέση αυτή θα ήθελα να ευχαριστήσω θερμά τον υπεύθυνο καθηγητή κ. Ηλιούδη για τις παρατηρήσεις και την καθοδήγηση που μου παρείχε σε όλη τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας. Ευχαριστώ επίσης τα υπόλοιπα μέλη της εξεταστικής επιτροπής για την προσεκτική ανάγνωση της εργασίας.

ΠΛΑΙΣΙΟ ΓΙΑ ΤΗ ΒΕΛΤΙΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΤΩΝ ΠΟΛΙΤΩΝ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Φώτιος Παπαγιαννίδης, pap_fotis@hotmail.com

Διεθνές Πανεπιστήμιο της Ελλάδος, Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων,

Π.Μ.Σ. 'Ευφυείς Τεχνολογίες Διαδικτύου', 2023

Επόπτης Καθηγητής: Ηλιούδης Χρήστος

Περίληψη

Οι μεγάλες τεχνολογικές ανακαλύψεις τα τελευταία χρόνια έχουν επιφέρει μία σημαντική αλλαγή στη καθημερινότητα των πολιτών μέσα από μία μεγάλη γκάμα υπηρεσιών που στοχεύουν στην ικανοποίηση τους. Οι εφαρμογές αυτές προσπαθούν να λειτουργούν όσο το δυνατόν καλύτερα και αποτελεσματικά προς όφελος των πολιτών μίας έξυπνης πόλης καθώς αναπτύσσονται μέσα από τις τεράστιες ποσότητες δεδομένων που παράγονται από τη καθημερινή χρήση. Η ανάπτυξη μίας έξυπνης πόλης σε συνδυασμό με τις νέες τεχνολογίες μπορεί να βελτιώσει αισθητά τη ποιότητα ζωής των πολιτών καθώς έρχονται σε άμεση επαφή με το ψηφιακό κόσμο της τεχνολογίας (IoT). Η εμπιστοσύνη και η ικανοποίηση των πολιτών προς τις νέες αυτές τεχνολογίες είναι το κύριο στοιχείο για να μπορέσει να αναπτυχθεί αυτή η επικοινωνία και να δώσει νέες πτυχές στις υπηρεσίες. Επομένως, μία έξυπνη πόλη πρέπει να διαφυλάξει σε κάθε περίπτωση την ασφάλεια και την ιδιωτική ζωή των πολιτών προστατεύοντας όλα τα προσωπικά δεδομένα τους ώστε να διατηρείται το απόρρητο. Φυσικά, σε όλο αυτό το οικοδόμημα λαμβάνονται αυστηρά μέτρα προστασίας και πιθανές ευπάθειες που μπορούν να αναπτυχθούν αλλά μέσα από μία σειρά ενεργειών και μεθόδων αναπτύσσεται μία στρατηγική κουλτούρα για την αποτελεσματική εφαρμογή των μέτρων ώστε να μην χαθούν τα οφέλη από την έξυπνη πόλη και να προφυλαχθούν οι πολίτες νιώθοντας ασφάλεια και εμπιστοσύνη.

Λέξεις Κλειδιά – Έξυπνη Πόλη, Ασφάλεια, Ιδιωτικό Απόρρητο, Πλαίσιο Ασφάλειας, Απαιτήσεις Ασφάλειας

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΜΣ 'ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ'

ΔΙΠΛΩΜΑΤΙΚΗ ΔΙΑΤΡΙΒΗ

Abstract

Technological advancements in recent years have brought significant change to the life of citizens through a wide range of services aimed at improving their quality of life. Innovative applications aim to effective and efficiently benefit citizens of a smart city, by making the most of large amounts of data generated by daily use. The development of a smart city combined with new technologies can significantly improve the quality of life of citizens as they come into direct contact with the digital world of information technology (IoT). The trust and satisfaction of citizens towards these new technologies is the main element to their acceptance and successful utilization. Therefore, a smart city must in every case safeguard the security and privacy of citizens by protecting all their personal data to maintain user privacy. Throughout this edifice strict protection measures are taken and possible vulnerabilities identified. Through such a series of actions and methods a strategic culture is developed for the effective implementation of the measures so that the benefits of the smart city are realized and citizens feel safe.

Keywords – Smart City, Security, Private Privacy, Security Framework, Security Requirements

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

DOS	Επίθεση άρνησης εξυπηρέτησης
IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
ISO	
IOT	Internet of Things
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Οι μεγάλες και ραγδαίες τεχνολογικές αλλαγές έχουν καταφέρει να προσελκύσουν ένα μεγάλο αριθμό ανθρώπων του πληθυσμού στις πόλεις. Η αυξητική τάση που καταγράφεται από τις μετακινήσεις των ανθρώπων έχει να κάνει και σε ένα βαθμό με την ικανοποίηση των αναγκών τους και με την εξασφάλιση μίας ποιοτικά καλύτερης ζωής. Σίγουρα, αυτές οι συστηματικές μετακινήσεις των ανθρώπων δημιουργούν και τις αντίστοιχες πιέσεις στο εκάστοτε σύστημα μίας πόλης καθώς θα πρέπει να ληφθούν όλα τα αναγκαία μέτρα που θα εξασφαλίσουν αρμονικά την ισορροπία του συστήματος και την άμεση επίλυση διαφόρων προβλημάτων που υπάρχουν. Έτσι, η εκάστοτε πόλη αναλαμβάνει να επεξεργαστεί και να μελετήσει όλα τα δεδομένα που έχει στη διάθεση της ώστε να εφαρμόσει κατάλληλα μέτρα και κανόνες που θα αφορούν το σχεδιασμό της πόλης και τους πιθανούς τρόπους αντιμετώπισης των προκλήσεων. Η αναβάθμιση και ανάπτυξη των υποδομών είναι το σημαντικότερο στοιχείο της υπόθεσης καθώς μέσα από τις υφιστάμενες υποδομές λειτουργούν οι τεχνολογίες που σχετίζονται με τις παρεχόμενες υπηρεσίες μίας πόλης.

Τα τελευταία χρόνια έχει καταγραφεί μεγάλη αύξηση των παραγόμενων δεδομένων στις έξυπνες πόλεις από τους πολίτες καθώς δημιουργούνται διαρκώς νέες ανάγκες που μπορούν να επηρεάσουν σημαντικά την καθημερινότητα τους και να δώσουν λύσεις στα προβλήματα τους. Μέσα από τη τεχνολογία οι άνθρωποι ψάχνουν λύσεις για να βελτιώσουν τη ζωή τους αλλά και να προφυλάξουν όλα όσα έχουν καταφέρει να ‘’χτίσουν’’ σε αυτό το ψηφιακό σχεδιασμό. Ο ψηφιακός κόσμος και οι αμέτρητες εφαρμογές που δημιουργούνται μέσα σε αυτόν έχουν ως κύριο αποδέκτη τον πολίτη που χρησιμοποιεί αυτές τις δυνατότητες και τον καθιστούν ως βασικό χρήστη για να μπορεί να στηριχθεί και η τεχνολογία. Η συνύπαρξη αυτή έχει σημασία γιατί παράγονται δεδομένα που αναλύονται και επεξεργάζονται από τους ειδικούς ώστε να εξειδικεύσουν τις λειτουργίες των υπηρεσιών και να προσφέρουν αποτελεσματικά μέσα στις έξυπνες πόλεις.

Ο σχεδιασμός, η έρευνα και η εφαρμογή τέτοιων υπηρεσιών είναι αρκετά σύνθετα ζητήματα λόγω της πολυπλοκότητας και της δομής των λειτουργιών και διαρκώς αλλάζουν για να μπορούν να ανταποκρίνονται στις πιθανές αδυναμίες και ευπάθειες που μπορούν να προκύψουν μέσα στη ροή των εφαρμογών. Σίγουρα, γίνεται ένας αυστηρός έλεγχος και ενημέρωση σε καθημερινή βάση ώστε να διασφαλίζεται και η

ασφάλεια των υπηρεσιών για τους χρήστες. Η ασφάλεια και το απόρρητο των χρηστών είναι ψηλά στη λίστα των προτεραιοτήτων των ειδικών που σχετίζονται με αυτά τα θέματα γιατί πρέπει να αποδεικνύουν πως μπορούν να εμπιστευτούν αυτές τις τεχνολογίες που αναπτύσσονται στις έξυπνες πόλεις.

Η αξιοποίηση των δεδομένων σε συνδυασμό με τα ψηφιακά εργαλεία που υπάρχουν μπορούν να επηρεάσουν σημαντικά και τις απαιτήσεις των πολιτών και να περιορίσουν πιθανούς κινδύνους παραβιάσεων. Η βιωσιμότητα των υπηρεσιών έχει να κάνει σε ένα βαθμό και με τα μέτρα ασφαλείας που καλείται μία έξυπνη πόλη να λάβει και να ‘’μάθει’’ ώστε να εφαρμόσει σωστά όλες τις πιθανές μεθόδους και πρακτικές που θα εξασφαλίσουν την αξιοπιστία των υποδομών σε κρίσιμα ζητήματα.

Οι κύριοι στόχοι μίας έξυπνης πόλης είναι να συμβάλουν στη κοινωνία και κατ’ επέκταση σε όλες τις λειτουργίες της (π.χ. οικονομικές δραστηριότητες) που αυτομάτως την καθιστούν ως ένα χρήσιμο εργαλείο για την ανάπτυξη και τη βιωσιμότητα των υπηρεσιών. Ο εκσυγχρονισμός και η αναδιοργάνωση μίας έξυπνης πόλης είναι σίγουρα μία πρόκληση αλλά και ένας ‘’γρίφος’’ που αν αναλυθούν και μελετηθούν σωστά όλα τα εμπλεκόμενα μέρη μπορούν να προσφέρουν σημαντικά οφέλη και να ικανοποιήσουν τις απαιτήσεις των πολιτών σε ένα βαθμό και να δημιουργηθούν πιθανώς μελλοντικές βάσεις λαμβάνοντας όλα τα αναγκαία μέτρα για τις υποδομές σε θέματα ανθεκτικότητας και βιωσιμότητας. Σε κάθε περίπτωση, μία πόλη εφόσον επιλέγει να αναβαθμίσει τις υποδομές της και να προσφέρει στους πολίτες υψηλού επιπέδου εξυπηρέτηση ώστε να χαρακτηρίζεται ‘’έξυπνη’’ θα πρέπει να προσαρμόζεται άμεσα σε όλα τα ζητήματα επεκτείνοντας συστηματικά τις υποδομές της καθώς υπάρχει μεγάλος κίνδυνος να αντιμετωπίσει προβλήματα που δεν υπήρχαν ή ήταν σε χαμηλά επίπεδα.

Αυτά τα προβλήματα έχουν να κάνουν λόγω της μαζικής μετακίνησης των πολιτών σε μεγάλα και ανεπτυγμένα κέντρα που ενδέχεται να επηρεάσουν την οικονομία, την ενέργεια και το περιβάλλον δημιουργώντας πίεση στο σύστημα. Επομένως, θα πρέπει να γνωρίζει μία έξυπνη πόλη πως μεταβάλλοντας ένα παράγοντα μέσα σε αυτό το οικοσύστημα μπορεί να χαθεί η ισορροπία και να παραβιαστούν οι υποδομές σε πιθανές επιθέσεις από το περιβάλλον της (άμεσο και έμμεσο) και να υποβαθμίσουν τις τεχνολογικές λύσεις που σχεδιάστηκαν και εφαρμόστηκαν με σκοπό τη διαχείριση των πόλεων.

Η ασφάλεια και το απόρρητο των πολιτών καθώς και τα δεδομένα που παράγονται είναι η προτεραιότητα όλων και εργάζονται οι έξυπνες πόλεις συστηματικά επάνω σε αυτό το θέμα γιατί μπορούν να προκύψουν μεγάλα προβλήματα που θα είναι ικανά να καταρρεύσουν αυτό το οικοσύστημα και να ‘’στρέψουν’’ αρνητικά τους πολίτες στις τεχνολογίες και κατ’ επέκταση να μην τις χρησιμοποιούν. Οι ψηφιακές επιθέσεις που γίνονται σε αυτά τα πεδία έχουν να κάνουν κυρίως με τη δύναμη που μπορούν να αποκτήσουν οι επιτιθέμενοι και τις αρνητικές συνέπειες που μπορούν να προκαλέσουν στο σύστημα της πόλης υπονομεύοντας και τις λειτουργίες της στο κοινωνικό σύνολο καθιστώντας την ως αναξιόπιστη να προφυλάξει αυτό το οικοσύστημα και τις σχέσεις εμπιστοσύνης των πολιτών προς την έξυπνη πόλη.

Φυσικά, δεν είναι καθόλου εύκολο να προστατευτεί μία έξυπνη πόλη σε άγνωστες επιθέσεις, χωρίς δεδομένα και χωρίς να γνωρίζει τον επιτιθέμενο. Η ασφάλεια και η αξιοπιστία λοιπόν είναι σύνθετα ζητήματα και καθόλου επιφανειακά εστιάζοντας μονάχα στις βασικές εφαρμογές και ενημερώσεις που αναπτύχθηκαν και μπορούν να δώσουν λύσεις σε συγκεκριμένα ζητήματα αλλά να καταφέρουν να αποκλείσουν ζημίες που μπορούν να οδηγήσουν σε καταστροφικές συνέπειες για την έξυπνη πόλη.

ΚΕΦΑΛΑΙΟ 1.1: ΣΤΟΧΟΙ

Η διπλωματική εργασία έχει στόχο να εξετάσει όλες τις πιθανές υπηρεσίες που παρέχονται στους πολίτες μίας έξυπνης πόλης καθώς και τις λύσεις που προτείνονται για την αποτελεσματική χρήση. Η σημασία του απορρήτου και η ασφάλεια για τους πολίτες είναι μερικά από τα βασικά χαρακτηριστικά που θα εξεταστούν και θα αναζητηθούν όλες οι πιθανές βελτιώσεις που μπορούν να ικανοποιήσουν την ασφάλεια και το ιδιωτικό απόρρητο της ζωής ενός πολίτη μέσα σε μία τεχνολογικά εξελίξιμη πόλη που προσφέρει νέες υπηρεσίες. Η ανάλυση και καταγραφή των μεθόδων είναι σημαντικά στοιχεία για την έρευνα καθώς μπορούν να αποτυπώσουν καλύτερα τα δεδομένα και να περιορίσουν τυχόν λάθη στη διάρκεια της έρευνας. Η σημασία της έρευνας παίζει καθοριστικό ρόλο και θα δώσει αξία στα αποτελέσματα της εργασίας και φυσικά θα έχει σαν στόχο να βελτιώσει τις πληροφορίες που υπάρχουν έως σήμερα.

Μέσω της βιβλιογραφικής ανασκόπησης έγινε η μελέτη του συγκεκριμένου θέματος για να αναλυθούν σ’ ένα βαθμό τα ποιοτικά και ποσοτικά χαρακτηριστικά που

επηρεάζουν τις έξυπνες πόλεις. Μέσα από την έρευνα και την αξιοποίηση όλων των διαθέσιμων μέσων θα προσπαθήσει η παρούσα διατριβή να αξιολογήσει όλα τα κριτήρια που έχουν επηρεάσει το συγκεκριμένο θέμα και να προταθούν πιθανές λύσεις για μία διαφορετική αντιμετώπιση σε μελλοντικά ζητήματα ασφαλείας και απορρήτου που σχετίζονται με τις έξυπνες πόλεις. Τέλος, όταν ολοκληρωθεί η βιβλιογραφική ανασκόπηση και μελετηθούν όλα τα διαθέσιμα δεδομένα θα γίνει μία προσπάθεια για να καταγραφούν και τα συμπεράσματα της διατριβής και τα πιθανά οφέλη που μπορούν να προκύψουν μέσα από τις διαθέσιμες ερευνητικές υποθέσεις σε μία μελέτη περίπτωσης (έξυπνης πόλης) προσφέροντας μελλοντικά στις επόμενες έρευνες και ταξινομώντας τα προβλήματα γύρω από την έξυπνη πόλη σε θέματα ασφάλειας, τις ευπάθειες και τους κινδύνους που αναπτύσσονται τεχνολογικά και τα μέτρα που λαμβάνονται από μία έξυπνη πόλη από την αρχή της ανάπτυξης και της στρατηγικής που ακολουθεί για να αντιμετωπίσει τις επιθέσεις αυτές και να εξουδετερώσει κινδύνους που θα προσπαθήσουν να παραβιάσουν το σύστημα διαχείρισης που έχει δημιουργηθεί για αυτό το σκοπό.

ΚΕΦΑΛΑΙΟ 2: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

2.1 ΕΞΥΠΝΗ ΠΟΛΗ

Τα τελευταία χρόνια, η έννοια της έξυπνης πόλης έχει προσελκύσει το ενδιαφέρον τόσο του ακαδημαϊκού χώρου όσο και της βιομηχανίας. Εννοιολογικά, θα μπορούσαμε να ισχυριστούμε ότι με την πάροδο των χρόνων ο βασικός πυρήνας της έννοιας έχει πλέον μετατεθεί και ενώ αρχικά η έξυπνη πόλη επικεντρωνόταν κατά κόρον στις ψηφιακές τεχνολογίες στη συνέχεια η έννοια αυτή εξελίχθηκε και πλέον κινείται γύρω από την από την ποιότητα ζωής, τη βιωσιμότητα καθώς επίσης και την οικονομική ανάπτυξη (Kummitha & Crutzen, 2017). Έτσι στο κεφάλαιο αυτό θα επιχειρήσουμε να προσεγγίσουμε την έννοια της «έξυπνης πόλης» (smart city), καθώς επίσης και την εξέλιξη της έννοιας αυτής, η οποία θεωρείται ταυτόσημη με την έννοια της πόλης της πληροφορίας, της ψηφιακής πόλης και της αειφόρου πόλης (Yigitcanlar 2006).

Όπως θα δούμε στη συνέχεια, η δημιουργία των «έξυπνων πόλεων» υπήρξε αποτέλεσμα της ταχείας αστικής ανάπτυξης, καθώς οι πόλεις προσαρμόζονταν με τέτοιον τρόπο, ώστε να βελτιώνουν τις υποδομές τους και παράλληλα να ανταπεξέρχονται στις αυξανόμενες προκλήσεις. Πρέπει επίσης να τονίσουμε ότι, επειδή η εξεταζόμενη έννοια προσεγγίζεται με διαφορετική οπτική από τον εκάστοτε μελετητή, είναι αναμενόμενο ότι οι ήδη υφιστάμενοι ορισμοί να αναθεωρούνται, συνδυάζοντας άλλοτε τον ανθρώπινο παράγοντα με την τεχνολογική υποδομή και άλλοτε όχι. Μία από τις πρώτες προσπάθειες ορισμού της έξυπνης πόλης ήταν του Hall (2000), ο οποίος επιχειρώντας να ορίσει ποιες είναι οι έξυπνες πόλεις, θα καταλήξει στο συμπέρασμα ότι είναι αυτές που συνδυάζουν όλες φυσικές υποδομών της, συμπεριλαμβανομένων των δρόμων, των γεφυρών, των σηράγγων, του μετρό, των αεροδρομίων, των λιμανιών, των τηλεπικοινωνιών, του νερού, της ενέργειας, ακόμη και των μεγάλων κτιρίων, έχοντας ως κύριο σκοπό τη βελτίωση των πόρων της και μεγιστοποιώντας φυσικά τις προσφερόμενες υπηρεσίες προς τους πολίτες της.

Ωστόσο, στον ορισμό αυτό, ο οποίος επικεντρώνεται στην τεχνολογική και θεσμική διάσταση των έξυπνων πόλεων, δεν υπάρχει σαφής διαχωρισμός των φυσικών αυτών υποδομών που χρησιμοποιούνται για την ανάπτυξη μίας έξυπνης πόλης. Όπως ήδη αναφέραμε η έννοια της έξυπνης πόλης είναι ταυτόσημη με την έννοια της ψηφιακής πόλης, γεγονός που θα οδηγήσει τον Schuler (2002), ο οποίος εστιάζοντας στην

τεχνολογική διάσταση της, θα καταλήξει στο συμπέρασμα ότι μία ψηφιακή πόλη έχει τουλάχιστον δύο έννοιες. Σύμφωνα με την πρώτη, μια ψηφιακή πόλη είναι αυτή που μετασχηματίζεται ή επαναπροσανατολίζεται μέσω των ψηφιακών τεχνολογιών, ενώ σύμφωνα με τη δεύτερη η έννοια της ψηφιακής πόλης σχετίζεται με τη ψηφιακή αναπαράσταση ή ανάκλαση ορισμένων πτυχών μιας πραγματικής ή φανταστικής πόλης. Την ίδια χρονιά και ο Ishida (2002), εστιάζοντας και ο ίδιος στην τεχνολογική διάσταση της έξυπνης πόλης, θα καταλήξει στο συμπέρασμα ότι η ψηφιακή πόλη είναι ουσιαστικά μία ενσύρματη ψηφιακή πόλη, της οποίας οι λειτουργίες στηρίζονται στη χρήση των ΤΠΕ τόσο για την επεξεργασία δεδομένων όσο και για την ανταλλαγή πληροφοριών.

Οι Mustard και Ostendorf (2004) θα προσθέτουν στον ορισμό της έξυπνης πόλης νέα χαρακτηριστικά, αυτά της προσαρμοστικότητας, της καινοτομίας και της δημιουργικότητας, ως προϋποθέσεις για την οικονομική και κοινωνική ανάπτυξη. Ο Hartley (2005) θα συμπληρώσει τον ορισμό του Hall (2000), δίνοντας έναν πιο τεχνολογικό ορισμό, χαρακτηρίζοντας μία πόλη ως έξυπνη, όταν αυτή συνδέει την υλική, την πληροφορική, την κοινωνική καθώς επίσης και την επιχειρηματική υποδομή της, προκειμένου να στοχεύσει τη μόχλευση της συλλογικής νοημοσύνης της πόλης. Οι Giffinger et al. (2007) επιχειρώντας να προσεγγίσουν το ζήτημα της έξυπνης, εστιάζουν την προσοχή τους στην οικονομία και το περιβάλλον. Έτσι, θα καταλήξουν στο συμπέρασμα πως έξυπνη πόλη είναι αυτή που προνοεί για τον άνθρωπο, το περιβάλλον και την οικονομική ανάπτυξη, συνδυάζοντας με έξυπνο τρόπο τις δραστηριότητες και τις ικανότητες των συνειδητοποιημένων και ενεργών πολιτών της, έχοντας ως βάση της τους φυσικούς πόρους που διαθέτει. Όσον αφορά στον επιχειρησιακό σκοπό της, σύμφωνα με τους ίδιους, αυτός δεν είναι άλλος από το να συμβάλει στην επίτευξη των στόχων μίας βιώσιμης ανάπτυξης.

Σε αντιδιαστολή με τον Hartley, ο Rios (2008) στο άρθρο του με τίτλο ‘‘How to Strategize Smart Cities: Revealing the Smart Model’’, προσέγγισε τη συγκεκριμένη έννοιά περισσότερο ανθρωποκεντρικά, χαρακτηρίζοντας ως έξυπνη την πόλη εκείνη που εμπνέει, μοιράζεται την κουλτούρα της, τη γνώση και τη ζωή της. Παράλληλα, σύμφωνα με τον ίδιο, μία πόλη είναι έξυπνη, όταν παρακινεί τους κατοίκους της να δημιουργήσουν μέσω του καθημερινού τρόπου ζωής τους. Έναν χρόνο αργότερα οι Caragliu et al. (2009) στην προσπάθεια τους να την ορίσουν, συνέδεσαν την ανθρώπινη με την κοινωνική πτυχή, υπογραμμίζοντας πως «οι επενδύσεις σε

ανθρώπινο και κοινωνικό κεφάλαιο και στην παραδοσιακή υποδομή επικοινωνιών και σύγχρονης επικοινωνίας (ΤΠΕ) συμβάλλουν στη βιώσιμη οικονομική ανάπτυξη και στην υψηλή ποιότητα ζωής, με σοφή διαχείριση των φυσικών πόρων, μέσω συμμετοχικής διακυβέρνησης». Από τον ορισμό αυτό εύκολα αντιλαμβανόμαστε ότι τόσο οι στόχοι, που δεν είναι άλλοι από τη βιωσιμότητα, την ανάπτυξη και φυσικά την ευημερία και τα εργαλεία, δηλαδή τις επενδύσεις σε ανθρώπινο κεφάλαιο όσο και η διαδρομή που απαιτείται για να φτάσουμε σε αυτούς στόχους (ορθή διαχείριση πόρων και συμμετοχικότητα) είναι διακριτά στοιχεία.

Οι ίδιοι λίγα χρόνια αργότερα (2011) εστιάζοντας το ενδιαφέρον του στην έξυπνη πόλη θα συνέδεσαν την ανθρώπινη, τη θεσμική και τεχνολογική πτυχή, χαρακτηρίζοντας μία πόλη ως έξυπνη, όταν οι επενδύσεις σε ανθρώπινο και κοινωνικό κεφάλαιο και η παραδοσιακή υποδομή επικοινωνίας (Τ.Π.Ε.) και η σύγχρονη επικοινωνία Τ.Π.Ε. συμβάλλουν στη βιώσιμη οικονομική ανάπτυξη και στην υψηλή ποιότητα ζωής. Φυσικά, για να επιτευχθεί ο στόχος αυτός, θα πρέπει να γίνεται σωστή διαχείριση των φυσικών πόρων και πάντοτε μέσω της συμμετοχικής διακυβέρνησης. Οι Anthopoulos & Fitsilis (2010) μελετώντας την έννοια της έξυπνης πόλης, την οποία ονομάζουν ως πανταχού παρούσα πόλη (U-City), θα καταλήξουν στο συμπέρασμα ότι η U-City αποτελεί επέκταση της έννοιας της ψηφιακής πόλης, καταλήγοντας εν τέλει ότι στη συγκεκριμένη μορφή πόλης είναι παρούσα η τεχνολογία πληροφοριών. Ακόμη μία έρευνα εστιάζει την προσοχή της στην τεχνολογική διάσταση των έξυπνων πόλεων καταλήγοντας στο συμπέρασμα ότι οι πόλεις έξυπνες είναι το προϊόν της ψηφιακής πόλης σε συνδυασμό με το Διαδίκτυο των πραγμάτων (Su, 2011). Για τους Kourtit και Nijkamp (2012) η έξυπνη πόλη είναι αυτή στην οποία η οικονομία και η διακυβέρνηση της καθοδηγούνται και διαμορφώνονται από την καινοτομία, την επιχειρηματικότητα και σαφώς από τους ‘‘έξυπνους’’ ανθρώπους. Παράλληλα, οι ίδιοι θα ορίσουν ότι οι έξυπνες πόλεις είναι αυτές που παρουσιάζουν υψηλή παραγωγικότητα, καθώς οι άνθρωποί της έχουν υψηλό μορφωτικό επίπεδο, υπάρχουν θέσεις εργασίας και συστήματα προγραμματισμού προσανατολισμένα προς την παραγωγή, ενώ οι πρωτοβουλίες που λαμβάνονται βασίζονται στην αειφορία. Ο Dameri (2013) στο άρθρο του ‘‘Searching for smart city definition: a comprehensive proposal’’, συνδυάζοντας και τις τέσσερις διαστάσεις, δηλαδή την τεχνολογική, την ανθρώπινη, την περιβαλλοντική και τέλος τη θεσμική, θα καταλήξει στο συμπέρασμα ότι η έξυπνη πόλη είναι μία σαφώς

οριοθετημένη γεωγραφική περιοχή, στην οποία οι υψηλές τεχνολογίες, όπως είναι για παράδειγμα οι ΤΠΕ και η παραγωγή ενέργειας, όχι μόνο συνυπάρχουν αλλά ταυτόχρονα συνεργάζονται προς όφελος των πολιτών, στοχεύοντας στην ευημερία, στην κοινωνική ένταξη και την συμμετοχή, στην περιβαλλοντική ποιότητα καθώς επίσης και στην ευφυή ανάπτυξη.

Την επόμενη χρονιά (2014), η μελέτη της Γενικής Διεύθυνσης Εσωτερικής Πολιτικής της Ευρωπαϊκής Ένωσης, εστιάζοντας την προσοχή της στη χρήση των ΤΠΕ, έδωσε έναν πιο ολιστικό ορισμό της εξεταζόμενης έννοιας, καθορίζοντας ταυτόχρονα τα δομικά συστατικά της έξυπνης πόλης. Έτσι, σύμφωνα με τη μελέτη αυτή, η έξυπνη πόλη βασίζεται στη χρήση των τεχνολογιών, κυρίως των ΤΠΕ, έχοντας ως πρωταρχικό σκοπό της όχι μόνο την αύξηση της ανταγωνιστικότητας αλλά και τη διασφάλιση ενός πιο βιώσιμου μέλλοντος. Παράλληλα, η ίδια μελέτη θα υπογραμμίσει ότι μία έξυπνη πόλη είναι αυτή που επιλύει, μέσω της χρήσης των ΤΠΕ, διάφορα δημόσια προβλήματα, έχοντας ως βάση της την κοινοτική συνεργασία πολλών τομέων. Ουσιαστικά, σύμφωνα με την προσέγγιση αυτή, το τεχνολογικό, το ανθρώπινο και τέλος το θεσμικό στοιχείο είναι τα τρία συστατικά στοιχεία που οικοδομούν τις πρωτοβουλίες των έξυπνων πόλεων.

Για τους Anagnostopoulos et al., (2015) μία πόλη είναι έξυπνη, όταν πραγματοποιεί, μέσων μακροπρόθεσμων τρόπων, θεμελιώδεις έξυπνες λειτουργίες, όπως η οικονομία, η κινητικότητα, το περιβάλλον και οι άνθρωποι, και ταυτόχρονα είναι αυτή που βασίζεται στον «έξυπνο» συνδυασμό των προικοδοτήσεων και των δραστηριοτήτων αυτορρυθμιζόμενων, ανεξάρτητων και ευαισθητοποιημένων πολιτών. Το 2017 ο Anthopoulos θα ανακεφαλαιώσει τους ήδη υφιστάμενους ορισμούς έχοντας ως στόχο τη δημιουργία ενός νέου και πιο περιεκτικού ορισμού, σύμφωνα με τον οποίο, η εκμετάλλευση των ΤΠΕ και η καινοτομία από τις πόλεις (νέες ή υπάρχουσες περιοχές) ως μέσο οικονομικής, κοινωνικής και περιβαλλοντικής υποστήριξης αντιμετωπίζουν διάφορες προκλήσεις που αφορούν έξι (6) διαστάσεις (άνθρωποι, οικονομία, διακυβέρνηση, κινητικότητα, περιβάλλον και διαβίωση).

Συμπληρώνει πως ανάλογα με την απόδοση των ΤΠΕ και της καινοτομίας, καθώς και με τις ανάγκες και τις προτεραιότητες κάθε τόπου, κάθε πόλη λειτουργεί διαφορετικά και εφαρμόζει εναλλακτικές πρακτικές έξυπνων πόλεων. Πιο πρόσφατα, ο Παντελίδης (2017), εξετάζοντας το ζήτημα των έξυπνων πόλεων στη διπλωματική

του εργασία, θα δώσει έναν άλλον ορισμό για το τι είναι οι έξυπνες πόλεις, προσεγγίζοντας το θέμα μέσω της περιβαλλοντικής διάστασης (Eco - Green City). Έτσι, σύμφωνα με τον ορισμό που δίνει, σκοπός της οικολογικής-πράσινης πόλης δεν είναι άλλος από την αειφόρο ανάπτυξη και την προστασία του περιβάλλοντος, όπου οι περιβαλλοντικές μετρήσεις πραγματοποιούνται με αισθητήρες των ΤΠΕ με τα έξυπνα κτήρια και τις ανανεώσιμες πηγές να έχουν τον πρωταγωνιστικό ρόλο.

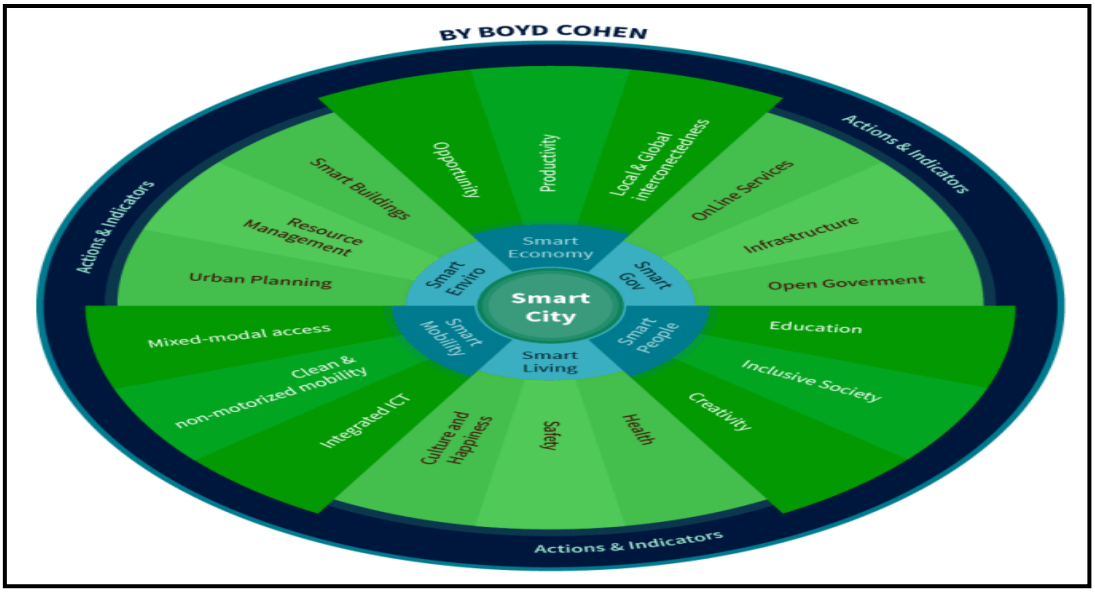
Η δημιουργία ψηφιακών μέσων παροχής υπηρεσιών σε συνδυασμό με τις ανάγκες μίας πόλης μπορούν να περιορίσουν τα προβλήματα σε διάφορους τομείς (οικονομία, περιβάλλον κτλ) και να υποστηρίξουν έμπρακτα το σύστημα της πόλης (Kumar & Dahiya, 2017). Μάλιστα, παρατηρείται αρκετά το τελευταίο διάστημα πως οι πόλεις μέσα από τους τοπικούς παράγοντες προσπαθούν να αναπτύξουν τις υποδομές και τα μέσα για να οργανώσουν από την αφετηρία μία ‘’έξυπνη πόλη’’ που θα απλοποιεί τη καθημερινότητα των πολιτών παρέχοντας λύσεις. Οι μεγάλες μετακινήσεις στα αστικά κέντρα έφεραν και τις αντίστοιχες αλλαγές μέσα στο σύστημα καθώς έπρεπε να αναδιοργανωθεί το σύστημα της πόλης και να ενσωματώσει νέες τεχνολογίες που θα βοηθούσαν στη καθημερινότητα των πολιτών (Pereira et al., 2018). Με τις τελευταίες αλλαγές της τεχνολογίας πληροφοριών και επικοινωνιών, η έξυπνη πόλη προσπάθησε να αναβαθμίσει τις υποδομές της αξιοποιώντας καλύτερα τους πόρους που έχει στη διάθεση της όπως για παράδειγμα σε συσκευές, σε δίκτυα, σε βάσεις δεδομένων και γενικότερα σε κέντρα ανάλυσης και επεξεργασίας δεδομένων καθώς παράγονται εκατομμύρια δεδομένα και οι αποφάσεις πρέπει να είναι άμεσες και ξεκάθαρες. Η αυξητική τάση της αστικοποίησης σε παγκόσμιο επίπεδο ανέρχεται σήμερα κοντά στο 55% και υπολογίζεται πως θα ξεπεράσει το 70% τα επόμενα χρόνια λόγω και άλλων παραγόντων όπως για παράδειγμα το φαινόμενο της κλιματικής αλλαγής (United Nations, 2018). Φυσικά, μία έξυπνη πόλη για να φτάσει σε ένα ικανοποιητικό επίπεδο ώστε να εφαρμόζει καινοτόμες λύσεις θα πρέπει να περάσει από κάποια στάδια ανάπτυξης.

Σύμφωνα με τον Boyd Cohen (2012) υπάρχουν τρεις γενιές έξυπνων πόλεων και έχουν καταγραφεί ως εξής:

1. **Smart Cities 1.0:** το όραμα κολοσσών εταιριών τεχνολογίας για τη δημιουργία καινοτόμων πόλεων.

2. **Smart Cities 2.0:** το όραμα κυβερνήσεων και πόλεων για τη βελτίωση της ποιότητας ζωής με τη βοήθεια της τεχνολογίας.
3. **Smart Cities 3.0:** ένα ανθρωποκεντρικό όραμα που θα εστιάζει στις ανάγκες των πολιτών με τις καταλληλόλητες λύσεις μέσω των νέων τεχνολογιών.

Στη παρακάτω εικόνα καταγράφονται τα κυριότερα χαρακτηριστικά μίας έξυπνης πόλης και οι παράγοντες που συνθέτουν αυτό το οικοσύστημα σύμφωνα με τον Boyd Cohen (2012). Η αξιοποίηση όλων των διαθέσιμων πηγών μπορούν να προσφέρουν ποιοτικές λύσεις σε διαφορετικά ζητήματα που έχει να αντιμετωπίσει μία έξυπνη πόλη και να προσφέρει νέες καινοτόμες και αποτελεσματικές πρακτικές. Πριν από μερικά χρόνια δεν θα μπορούσε πιθανόν κανένας να είναι σε θέση να καταλάβει αυτό το οικοσύστημα και τις δυνατότητες που μπορεί να προσφέρει στον άνθρωπο μέσα χωρίς να εφαρμόσει κάτι από όλα αυτά σε έξυπνα κτήρια, έξυπνους δρόμους, σε θέματα που σχετίζονται με την υγεία ή την εκπαίδευση (Appio et al., 2018). Η αξιοποίηση όλων αυτών των διαθέσιμων τεχνολογιών μπορεί να δώσει μία νέα εκδοχή στο σχεδιασμό και τη στρατηγική υλοποίησης των έξυπνων πόλεων και να συμβάλει στις απαιτήσεις των πολιτών στοχεύοντας στην ανάπτυξη όλων των υποδομών που μπορούν να προσφέρουν λύσεις στις ανάγκες των πολιτών μίας πόλης.



Εικόνα 1: Οικοσύστημα έξυπνης πόλης

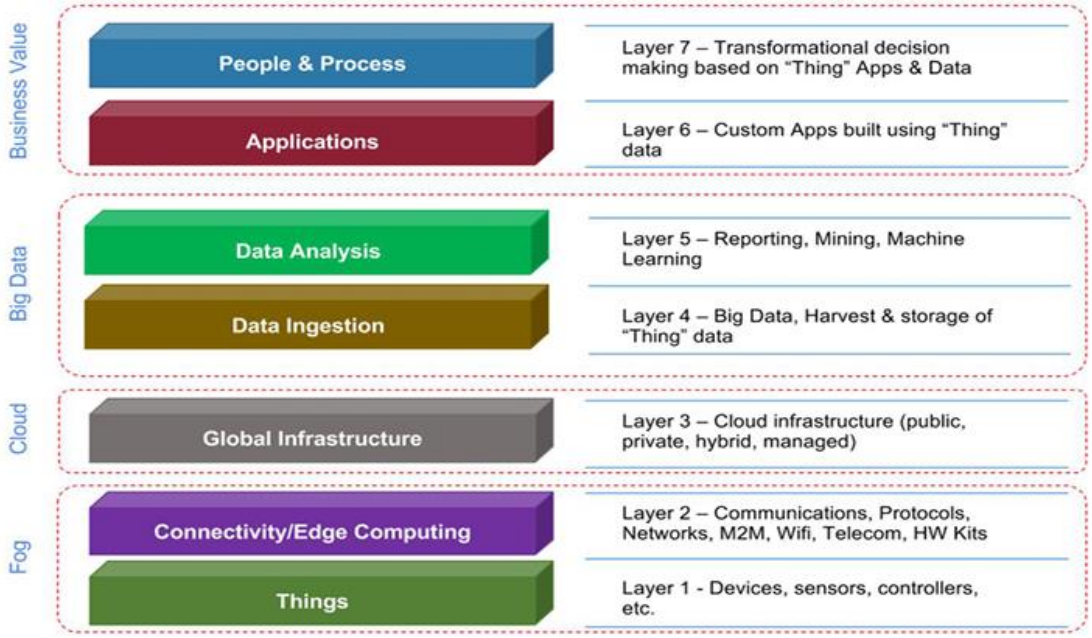
Σίγουρα, υπάρχουν αρκετοί τομείς που αναπτύσσονται μέσα σε μία έξυπνη πόλη αλλά για να είναι ολοκληρωμένη και αποτελεσματική μία λειτουργία θα πρέπει να

ελέγχεται συστηματικά η ασφάλεια και το απόρρητο λόγω των πιθανών προκλήσεων και της ιδιωτικότητας που υπάρχει μέσα στις έξυπνες πόλεις (Laufs et al., 2020). Επομένως, μία έξυπνη πόλη ενσωματώνει νέες και έξυπνες τεχνολογίες που αυξάνουν την αποτελεσματικότητα, την ασφάλεια και τις ευκολίες που υπάρχουν προστατεύοντας το απόρρητο των πολιτών και ενισχύοντας την αποδοτικότητα της έξυπνης πόλης καθώς οι πολίτες που συμμετέχουν ενισχύουν τις λειτουργίες της.

Ολοκληρώνοντας τη βιβλιογραφική ανασκόπηση του θέματος καταλήγουμε στο συμπέρασμα ότι για την έννοια της έξυπνης πόλης, η οποία αναπτύσσεται με ραγδαίους ρυθμούς, δεν υπάρχει ένας μόνος ορισμός, καθώς οι διάφοροι μελετητές του θέματος την προσεγγίζουν κάθε φορά από διαφορετική σκοπιά και οπτική γωνία. Ωστόσο, παρά την πληθώρα των ορισμών, όλοι περιστρέφονται γύρω από τρεις κύριες κατευθύνσεις: την τεχνολογία, τους ανθρώπους και τέλος την κοινότητα.

2.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Για να μπορέσει κάποιος να κατανοήσει τις διαβαθμίσεις και τα επίπεδα από τα οποία αποτελείται η έξυπνη πόλη θα πρέπει να δει στη πράξη αυτό το οικοσύστημα. Σύμφωνα με τους Salman & Jain (2019) η έξυπνη πόλη αποτελείται από επτά στρώματα και έχουν καταγραφεί ως εξής: στο πρώτο στρώμα του συστήματος είναι οι συσκευές και τα περιφερειακά μέσα που θα συνδεθούν στο έξυπνο δίκτυο. Στο δεύτερο στρώμα βρίσκονται τα πρωτόκολλα και οι ασύρματες επικοινωνίες. Στο τρίτο στρώμα βρίσκεται ένα κέντρο δεδομένων και απαιτεί μεγάλη υπολογιστική ισχύ. Στο τέταρτο στρώμα είναι τα μεγάλα δεδομένα που συγκεντρώνονται και αναλύονται μέσω των εργαλείων. Στο πέμπτο στρώμα υπάρχει ένα τμήμα προηγμένης τεχνολογίας που αναλύει και επεξεργάζεται τα δεδομένα μέσω της μηχανικής μάθησης και εκπαιδεύει τους αντίστοιχους αλγορίθμους. Στο έκτο στρώμα βρίσκονται οι εφαρμογές και στο τελευταίο στρώμα βρίσκονται οι υπηρεσίες που εκτελούνται για να φέρουν το τελικό αποτέλεσμα. Η διαδικασία αυτή επαληθεύεται μέσων των μηχανισμών που υπάρχουν ανάμεσα στα στρώματα και εάν προκύψει κάποιο πρόβλημα τότε τα υπόλοιπα στρώματα πραγματοποιούν αυτόματα εσωτερικό έλεγχο για να βεβαιωθούν για την ορθότητα των διεργασιών.



Εικόνα 2: Στρώματα οικοσυστήματος έξυπνων πόλεων.

2.3 ΔΟΜΗ ΠΡΩΤΟΚΟΛΛΩΝ

Για την ομαλή λειτουργία ενός έξυπνου δικτύου μέσα στην έξυπνη πόλη είναι αρκετά σύνθετο και πολύπλοκο ζήτημα καθώς υπάρχουν πολλές εφαρμογές που εκτελούνται ταυτόχρονα και απαιτούνται μεγάλες υπολογιστικές δυνάμεις που θα μπορέσουν να διαχειριστούν αυτές τις λειτουργίες καθώς υπάρχουν πολλά στρώματα και δεν είναι καθόλου εύκολο να ταξινομηθούν σε μία σειρά. Για να μπορέσουν λοιπόν να επιτευχθούν οι επικοινωνίες και να καλυφθούν όλες οι τεχνικές δυσκολίες χρησιμοποιούνται αυτά τα πρωτόκολλα επικοινωνίας καθώς έχουν περάσει διάφορες φάσεις προτυποποίησης από μεγάλους οργανισμούς (I3E και W3C) και έχουν δοθεί οι κατάλληλες οδηγίες στοχεύοντας στην ασφάλεια και τη διασύνδεση όλων των πιθανών συσκευών που θα επικοινωνούν χωρίς να υπάρχουν ευάλωτα σημεία και θα υπήρχε ο κίνδυνος διαρροής πληροφοριών. Παρακάτω καταγράφονται τα επίπεδα λειτουργίας ενός έξυπνου δικτύου που υπάρχει σε μία έξυπνη πόλη:

1. Υποδομή (π.χ.: 6LowPAN, IPv4/IPv6, RPL)
2. Αναγνώριση (π.χ.: EPC, uCode, IPv6, URI)
3. Επικοινωνίας / Μεταφοράς (π.χ.Wifi, Bluetooth, LPWAN)
4. Αναζήτησης (π.χ. υλικό δίκτυο, mDNS, DNS-SD)
5. Πρωτόκολλα δεδομένων (π.χ.: MQTT, CoAP, AMQP, Websocket, Κόμβος)
6. Διαχείριση συσκευών (π.χ.: TR-069, OMA-DM)
7. Σημασιολογία (π.χ.: JSON-LD, Web Thing Model)
8. Πλαίσια πολλαπλών επιπέδων (π.χ.: Alljoyn, IoTivity, Weave, Homekit)

2.4 IoT– SMART CITY

Η τεχνολογική επανάσταση στο Διαδίκτυο των Πραγμάτων (Internet of Things /IoT) είναι η αναβάθμιση και εξέλιξη της Πληροφορικής μέσα από καινοτόμες εφευρέσεις που εξυπηρετούν αποτελεσματικά τους χρήστες. Όσο εξελίσσεται η κοινωνία και εμπλουτίζονται οι συσκευές μέσα σε μία έξυπνη πόλη τόσα περισσότερα οφέλη προκύπτουν από τη χρήση. Η τεχνολογία καθώς αναβαθμίζεται είναι λογικό να χρησιμοποιούνται προϊόντα και υπηρεσίες σε καθημερινή βάση που επιφέρουν μεγάλη οικονομική και βιομηχανική σημασία καθώς όλα δουλεύουν συντονισμένα για να υπάρχουν αυτές οι παροχές. Προφανώς, αυτή η εξέλιξη με τις χρήσιμες λειτουργίες του IoT έχουν ήδη αναπτύξει ένα σύνολο συσκευών που συνδέονται μέσω εξαρτημάτων, αισθητήρων ή υπολογιστικών μέσων σε λίγα χρόνια θα ξεπεράσουν τα 100 δις διασυνδεμένων συσκευών και μίας οικονομικής αύξησης πάνω από 12 τρις σε παγκόσμια κλίμακα (Sicari et al., 2015).

Με τον όρο IoT περιγράφεται η συνδεσιμότητα των δικτύων και η υπολογιστική ικανότητα να μεταφέρεται σε συσκευές και αισθητήρες με σκοπό τη δημιουργία, συλλογή, επεξεργασία και ανάλυση των δεδομένων χωρίς να υπάρχει καθυστέρηση στο χρόνο (Caputo et al., 2016). Παρακάτω καταγράφονται επίσης κάποιοι από τους σημαντικότερους ορισμούς για το Διαδίκτυο των πραγμάτων (IoT):

1. Το IoT αποσκοπεί στην αλληλεπίδραση του ψηφιακού κόσμου με τον πραγματικό μέσα από μία μεγάλη γκάμα συσκευών, υπηρεσιών και επικοινωνιών μεταξύ Μηχανής προς Μηχανής (M2M) και αφορούν την αλληλεπίδραση στο σύστημα.
2. Πλήθος συσκευών που επικοινωνούν μέσω πρωτοκόλλων ασφαλείας και παρέχουν έξυπνες λύσεις ακόμη και όταν δεν υπάρχει η παρέμβαση του ανθρώπου στο σύστημα.
3. Σύγχρονες υποδομές καινοτόμων τεχνολογιών που βασίζονται στις έξυπνες συσκευές και στην επικοινωνία που αναπτύσσεται στο δίκτυο. Η συλλογή, ανάλυση, επεξεργασία και αξιοποίηση των δεδομένων είναι η αποτελεσματική λειτουργία του συνόλου.

2.4.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ IoT

1. Διαθεσιμότητα: όλες οι συσκευές μπορούν να συνδεθούν στο δίκτυο και να επικοινωνούν απευθείας.
2. Συνύπαρξη των Πραγμάτων: υπάρχει δηλαδή μία ισορροπία στο ψηφιακό κόσμο με το πραγματικό κόσμο.
3. Διαφορετικότητα: παρότι είναι διαφορετικά τα δεδομένα μπορούν να συνεργάζονται άρτια χωρίς τεχνικά προβλήματα.
4. Ασφάλεια: προτεραιότητα είναι η προφύλαξη των δεδομένων και η απομάκρυνση κακόβουλων ενεργειών.
5. Μεταβολές: ένα τεράστιο εύρος συσκευών που προστίθεται καθημερινά στο δίκτυο και συνεργάζεται αρμονικά ακολουθώντας ομαλά τη ροή του δικτύου.
6. Χρήστες: άμεσα συνδεδεμένοι με το σύστημα και τις συσκευές που χρησιμοποιούν καθημερινά και ικανοποιούν τις ανάγκες τους λόγω και της συνδεσιμότητας που έχουν και επικοινωνούν μέσα από ένα σύνολο πρωτοκόλλων.

2.4.2 ΤΟΜΕΙΣ IoT

Η σημασία του IoT και η ανάπτυξη των δραστηριοτήτων του σε διάφορους τομείς δείχνει και τη δυναμική που υπάρχει και τις λύσεις καθώς φαίνεται ότι τεχνολογία σε συνδυασμό με τον άνθρωπο μπορούν να δώσουν αποτελέσματα για το κοινό καλό. Παλαιότερα θα ήταν εξαιρετικά δύσκολο να αντιληφθεί κανείς σε βιομηχανικό

επίπεδο αν οι μηχανές για παράδειγμα ήθελαν κάποια επισκευή χωρίς κάποια φανερό πρόβλημα ή να ήταν σε θέση να προβλέψουν πιθανές δυσλειτουργίες στα μηχανήματα. Επίσης, θα ήταν αρκετά δύσκολο να προβλέπουν και να παρακολουθούν τις καιρικές αλλαγές και να μετράνε οι άνθρωποι τις κλιματικές αλλαγές χωρίς τα κατάλληλα μέσα και τις έγκαιρες ενημερώσεις. Ένας ακόμη εξίσου σημαντικός τομέας είναι η υγεία που μπορεί να παρέμβει άμεσα και να σώσει έναν άνθρωπο που βρίσκεται σε κίνδυνο όπως για παράδειγμα να έχει καρδιακά προβλήματα και να έχει επάνω του μηχάνημα υποστήριξης και να ενημερώνει ανά πάσα στιγμή για τη κατάσταση του και να μπορεί απομακρυσμένα να δεχτεί βοήθεια. Ακόμη, η συνεισφορά του IoT σε θέματα ενέργειας που δίνει λύσεις μέσα από τη παρακολούθηση και διαχείριση της κατανάλωσης, για τις ποσότητες που παρήγαγαν οι ανανεώσιμες πηγές και το όφελος των πόλεων σε πραγματικό χρόνο. Τέλος, η έξυπνη γεωργία που μπορεί να μεγιστοποιήσει τις καλλιέργειες και να μειώσει φθορές που κοστίζουν στις σοδειές αυξάνοντας τη ποιότητα των τροφών.

Εικόνα 3: Οικοσύστημα IoT

Αξίζει να σημειωθεί ότι η τεχνολογία δεν είναι το βασικό στοιχείο σε αυτή την αλυσίδα αλλά ένα σημαντικό χαρακτηριστικό ώστε να αναπτυχθεί η έξυπνη πόλη καθώς αποτελείται από τον άνθρωπο, το περιβάλλον, την οικονομία και τη τεχνολογία που όλα μαζί αποτελούν μία βιώσιμη έξυπνη πόλη που συνυπάρχουν και συνεργάζονται όλα τα στοιχεία σωστά (Kyriazis & Varvarigou, 2013). Η διαρκής συνεργασία και η συστηματική εργασία θα δώσουν μελλοντική αξία καθώς θα

μεγαλώνει αυτό το οικοδόμημα και θα εξελίσσεται μέσα από αυτούς τους τομείς και θα προσφέρει ικανοποίηση στις ανάγκες των πολιτών μιας και θα αναπτύσσεται μέσα από τις νέες τεχνολογίες και τα νέα πρότυπα. Οι εφαρμογές αυτές έχουν να προσφέρουν στις κοινωνίες ένα καλύτερο επίπεδο ζωής και πάνω από όλα μία διαρκή αύξηση όλων των παραγόμενων υπηρεσιών αρκεί να κατανοούνται και να αντιμετωπίζονται τα ζητήματα της πόλης (Alawadhi et al., 2012).

Εικόνα 4: Χαρακτηριστικά βιωσιμότητας έξυπνης πόλης

2.5 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΠΟΡΡΗΤΟΥ

Η ανάγκη για προστασία και ασφάλεια των πολιτών είναι από τις σημαντικότερες υπηρεσίες που πρέπει να εξετάσει μία έξυπνη πόλη καθώς χτίζεται και η εμπιστοσύνη των πολιτών σε όλες τις παρεχόμενες υποδομές και φυσικά δίνουν τη δυναμική που υπάρχει στο σύστημα. Τα δεδομένα που παράγονται μεταφέρονται σε βάσεις δεδομένων και επικοινωνούν με πολλά και διαφορετικά εργαλεία ή αισθητήρες ώστε να δώσουν μία έγκυρη ενημέρωση (Zhang et al., 2017). Προφανώς, υπάρχουν σοβαρά

σημεία που πρέπει να εξετάζονται σε κάθε περίπτωση και να αναλύονται προσεκτικά καθώς μεταφέρονται πληροφορίες και τα ρίσκα για πιθανές απώλειες ή παρεμβολές ή επιθέσεις είναι μεγάλα. Η προστασία της ιδιωτικής ζωής ενός πολίτη μέσα σε μία έξυπνη πόλη είναι άμεση προτεραιότητα γιατί όσο αυξάνονται οι δυνατότητες που δίνονται στους πολίτες τόσο αυξάνονται οι πιθανότητες για πιθανές επιθέσεις (Losavio, 2014).

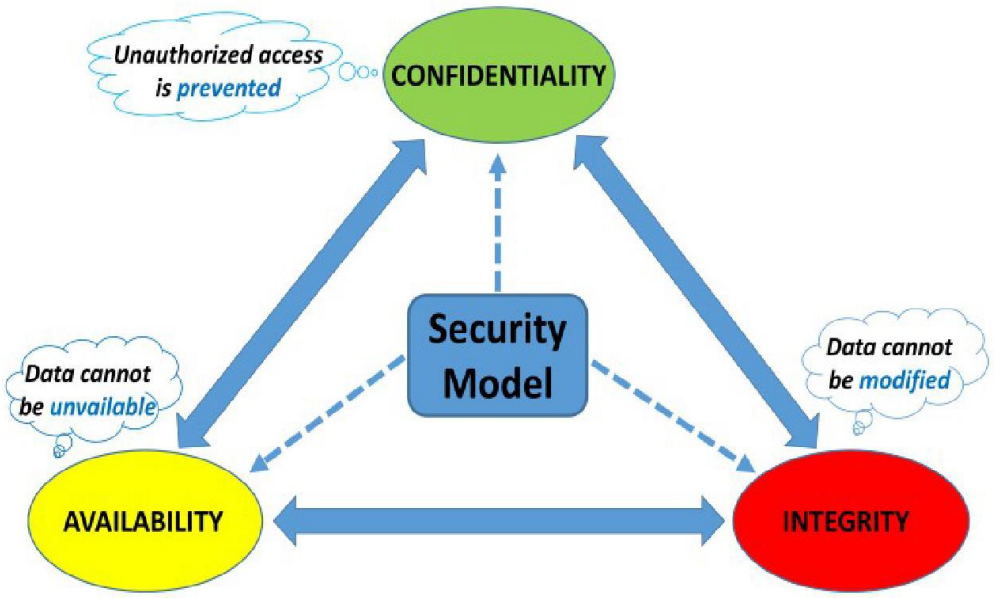
Η συνεργασία των ιδιωτικών επιχειρήσεων με το Κράτος είναι αναγκαία σε αυτό το κομμάτι της τεχνολογίας καθώς μέσα από αυτήν τη συνεργασία μπορούν να αναπτυχθούν οι υποδομές και να δημιουργηθούν ακόμη καλύτερα κέντρα. Η επίτευξη της προστασίας της ιδιωτικής ζωής και η ασφάλεια του απορρήτου δεν είναι σε καμία περίπτωση εύκολη υπόθεση καθώς υπάρχουν πολλές τεχνικές και συνδυασμοί που μπορούν να επηρεάσουν τα δεδομένα και να προκληθούν ζημίες (Turjman et al., 2022). Μάλιστα, σε ορισμένα σημεία των λειτουργιών που υπάρχουν μέσα σε μία έξυπνη πόλη ένας πιθανός συνδυασμός των δεδομένων θα μπορούσε να βοηθήσει και να αναπτύξει καλύτερα αποτελέσματα γιατί θα ήταν μικρότερος ο όγκος διαχείρισης και ο χρόνος ανταπόκριση που θα απαιτούσαν τα συστήματα για να αναλύσουν.

Σε ένα έξυπνο περιβάλλον μίας πόλης, το απόρρητο διατηρείται σε υψηλά επίπεδα από το συνδυασμό να μοιράζονται και να έχουν πρόσβαση χωρίς περιορισμούς (Braun et al., 2018). Φυσικά, από μόνο του σαν πρακτική έχει και αυτό τον κίνδυνο για να εκτεθεί το σύστημα σε μία επίθεση και να αποκαλύψει πληροφορίες. Εδώ θα πρέπει να εφαρμόζεται μία στρατηγική διαφορετική και να ‘’κομματιάζονται’’ τα δεδομένα σε ένα σύνολο δεδομένων με πολλαπλά στρώματα που θα γενικεύουν ορισμένα χαρακτηριστικά χωρίς να δίνουν συγκεκριμένα αναγνωριστικά. Έτσι, ακόμα και αν ο εισβολέας αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα δεν θα μπορεί άμεσα να διασταυρώσει τις πληροφορίες και να εξάγει χρήσιμα δεδομένα (Butt & Afzaal, 2019).

Η έξυπνες πόλεις προσπαθούν να προβλέψουν μέσα από διαδικασίες και μεθόδους τις πιθανές απειλές και να προβλέψουν τις επιθέσεις απορρήτου και δεδομένων μέσα στο σύστημα διαχείρισης (Theodorou & Sklavos, 2019). Το ιδιωτικό απόρρητο των πολιτών και η ασφάλεια είναι ουσιαστικά η ‘’δέσμευση’’ για συνεχή ανάπτυξη των επιπέδων ασφαλείας από την έξυπνη πόλη καθώς προσπαθεί να αναπτύξει τις γνώσεις της και να δημιουργήσει νέες τεχνικές γενίκευσης με K-ανωνυμία υψηλών

διαστάσεων που θα διατηρήσουν εμπιστευτικές τις πληροφορίες και θα αποφύγει τις πιθανές υποκλοπές δεδομένων. Ένας άλλος σημαντικός τρόπος αντιμετώπισης του απορρήτου των δεδομένων υψηλών διαστάσεων είναι η ανάλυση σε μειωμένο αριθμό χαρακτηριστικών, δηλαδή να προ-επεξεργαστεί λιγότερα χαρακτηριστικά με τέτοιο τρόπο που η διαδρομή που θα ακολουθεί το σύστημα να επικεντρώνεται σε μία αυστηρή μέθοδο ανίχνευσης συλλογής δεδομένων (Mora et al., 2018).

Η ασφάλεια ενός δικτύου περιγράφεται πάντα με την ακεραιότητα, την εμπιστευτικότητα και την αυθεντικότητα μέσα σε ένα μοντέλο ασφαλείας και παρέχονται μέσω της κρυπτογράφησης που ακολουθείται για την ορθή χρήση του μοντέλου ενώ σε διαφορετική περίπτωση δεν ανταποκρίνεται και δεν δίνει πρόσβαση στους πιθανούς εισβολείς προστατεύοντας τα δεδομένα και τις πληροφορίες που έχει.



Εικόνα 5: Μοντέλο ασφαλείας δικτύου.

Μία έξυπνη πόλη για να μπορέσει επομένως να προχωρήσει σωστά θα πρέπει να αναπτύξει μία στρατηγική και ένα σχεδιασμό που θα αποβλέπει σε ένα νέο μετασχηματισμό με περισσότερες λειτουργίες και ευκαιρίες. Το βασικό εργαλείο για να αλλάξει όλη αυτή η φιλοσοφία είναι να επαναξιολογηθούν τα αστικά κέντρα και να καταγραφούν τα προβλήματα που υπάρχουν και να εστιάσουν σε ένα δυναμικό περιβάλλον που θα αλληλεπιδρά με τους χρήστες και θα δίνει λύσεις σε όλα τα θέματα με ασφάλεια εξασφαλίζοντας και το ιδιωτικό απόρρητο του καθενός. Αυτές οι

προκλήσεις κυρίως του σχεδιασμού ενός συστήματος μίας έξυπνης πόλης έχει να κάνει με τα δυνατά και αδύναμα σημεία που μπορεί να υπάρχουν επιδιώξεις από εισβολείς προσπαθώντας να εκμεταλλευτούν κάθε ευπάθεια.

Στη συνέχεια, ένα ακόμη σημαντικό δεδομένο είναι η συνεχής ενημέρωση των χρηστών και η αντιμετώπιση εντάσεων λόγω πιθανών συμφερόντων από τη μία πλευρά και αντίστροφα λόγω των δεδομένων που παρέχονται και τέλος η αδιάλειπτη συνεργασία όλων των εμπλεκόμενων τμημάτων και φορέων που θα παρέχουν υποστήριξη και τεχνολογικά εργαλεία που θα βοηθούν στη προστασία του συστήματος (Beurden, 2011). Για την ανάπτυξη της έξυπνης πόλης και τον τεχνολογικό σχεδιασμό των υποδομών θα πρέπει να μελετηθούν αρκετά σημεία και να εφαρμοστούν πολλές δοκιμές ώστε να προκύψει μία πιθανή λύση ως καταλληλότερη. Η χρήση πολλών μικρών αισθητήρων, ψηφιακά κέντρα, δίκτυα και υβριδικές ασύρματες μορφές τεχνολογίας μπορούν να αναβαθμίσουν τις υφιστάμενες υποδομές και να συγκεντρώσουν τις λειτουργίες της πόλης ώστε να διαχειρίζονται όλα σωστά (IBM, 2012). Η αποτελεσματικότητα και η αποδοτικότητα αυτών των συστημάτων μπορούν να οδηγήσουν μία έξυπνη πόλη στην επίτευξη των στόχων της μέσα από μία σειρά ενεργειών που θα εξασφαλίσουν την επιτυχία αυτού του οικοσυστήματος. Έτσι, ένα υψηλό επίπεδο ασφαλείας για τους πολίτες έχει να κάνει και με τον τρόπο που συμπεριφέρονται μέσα σε ένα αντίστοιχο περιβάλλον, σε ποιο βαθμό προστατεύουν τα προσωπικά δεδομένα τους, η εμπιστοσύνη στα συστήματα που προτείνονται, η αποδοτικότητα των υπηρεσιών και αν χρησιμοποιούνται τα διεθνή πρότυπα ασφαλείας.

2.6 ΔΙΑΤΗΡΗΣΗ ΕΜΠΙΣΤΟΣΥΝΗΣ ΤΩΝ ΠΟΛΙΤΩΝ

Η σχέση εμπιστοσύνης των πολιτών μέσα σε μία έξυπνη πόλη αναφορικά με τις δυνατότητες που τους παρέχονται παίζουν καθοριστικό ρόλο από τις ενέργειες που κάνει μία έξυπνη πόλη και οι αλληλεπιδράσεις που δημιουργούνται. Οι νέες τεχνολογίες, οι καινοτόμες λύσεις, οι έξυπνες συσκευές και αισθητήρες είναι μερικά από τα σημαντικότερα στοιχεία αυτού του συστήματος. Για να μπορέσει όμως να ικανοποιήσει μία έξυπνη πόλη τις ανάγκες των πολιτών θα πρέπει να μεριμνήσει και για τα θέματα ασφαλείας, πιθανές επιθέσεις και ευπάθειες που μπορούν να προκύψουν και το ιδιωτικό απόρρητο που θα προστατεύει τα προσωπικά δεδομένα

των πολιτών (Braun et al., 2018). Η εμπιστοσύνη που δημιουργείται μέσα από τη χρήση είναι η βάση για να συνεχίσει να χρησιμοποιεί ο πολίτης αυτές τις εφαρμογές.

Μέσα από αυτό το ψηφιακό κόσμο και τις τεχνολογίες που αναπτύσσονται μπορεί κανείς να αντιληφτεί ότι η ανάγκη για ασφάλεια είναι καθοριστική για το σύστημα αυτό γιατί οι φορείς και ιδιωτικές επιχειρήσεις (πάροχοι τηλεπικοινωνιών) επενδύουν δεκάδες δις ευρώ για να φτιάξουν πολλαπλά επίπεδα ασφαλείας ώστε να μη θέσουν σε κίνδυνο το σύστημα και να μην βρεθούν σε μειονεκτική θέση (Bernabe et al., 2014). Επίσης, από τη πλευρά της Πολιτείας θεσπίζονται νόμοι για το ιδιωτικό απόρρητο και υπάρχουν αυστηρά πλαίσια για τη διασφάλιση και τη τήρηση της Αρχής Προστασίας των Προσωπικών Δεδομένων (GDPR). Επομένως, δεν είναι ένα απλό θέμα που αφήνει ‘’αδιάφορο’’ το σύστημα αυτό και λαμβάνονται υψηλά και αυστηρά πρότυπα για να προφυλάξουν ευαίσθητα δεδομένα. Μάλιστα, όσο εξελίσσεται και η τεχνολογία μέσα από τα έξυπνα δίκτυα διαμορφώνεται σιγά – σιγά μία αντίληψη και στους χρήστες πως πρέπει να συμμορφώνονται με το νόμιμο και ηθικό κομμάτι της τεχνολογίας λειτουργώντας με σεβασμό και λειτουργώντας συλλογικά για το καλό όλων μέσα στη κοινωνία (Ahmad et al., 2021).

Τα προσωπικά δεδομένα των πολιτών είναι διαρκώς σε μία ‘’κίνηση’’ λόγω της επεξεργασίας που γίνεται και της χρήσης και προφανώς πρέπει να τηρούνται μέτρα προστασίας για να μην αποκαλυφθούν σε λάθος πλευρές. Για παράδειγμα, θα μπορούσαν οι πολίτες να μην επιθυμούν να επεξεργάζονται 3^{ες} ομάδες τα δεδομένα τους χωρίς τη συναίνεση τους και το δίκτυο διαχείρισης να κοινοποιούσε πληροφορίες σε πιθανούς ενδιαφερόμενους με αποτέλεσμα να γινόταν ανάλυση και επεξεργασία των δεδομένων προς όφελος τους. Έτσι, δημιουργούνται πολλαπλά στρώματα και πολλές παραμέτρους που θα ‘’φιλτράρουν’’ τις ροές και τις ενέργειες που γίνονται ώστε να αποτρέψουν πιθανά λάθη και να εξυπηρετήσουν καλύτερα (Vojkovic, 2018). Επίσης, λαμβάνονται μέτρα προστασίας που έχουν θεσπιστεί με νόμους και συμμορφώνουν με δημοκρατικά μέσα τους εμπλεκόμενους που διαχειρίζονται τα προσωπικά δεδομένα των πολιτών ώστε να σέβονται το ιδιωτικό απόρρητο και να δίνουν το δικαίωμα της επιλογής στους πολίτες για το που και ποιος θα επεξεργαστεί τα δεδομένα τους και σε ποιο βαθμό θα αποκτήσει πρόσβαση.

Η τεχνολογία κατάφερε τα τελευταία χρόνια να σταματήσει ή να περιορίσει σε κάποιες περιπτώσεις τέτοιου είδους ζητήματα μέσα από συντονισμένες δράσεις και

αναπτύξεις των υποδομών με ευφυή συστήματα και δίκτυα τεχνητής νοημοσύνης που βοήθησαν αποτελεσματικά στην ασφάλεια. Τα παραδείγματα που υπάρχουν είναι πολλά και ενδεικτικά αναφέρεται ότι μέσα σε μία πόλη της Γερμανίας σε ένα εργοστάσιο παραγωγής πυρομαχικών έγινε η απόπειρα να αποσπάσουν δεδομένα από υπολογιστές που ήταν απομονωμένοι από το κεντρικό σύστημα για λόγους ασφαλείας και δεν είχαν πρόσβαση στο διαδίκτυο. Η αρχική πρόσβαση πάρθηκε από τις περιφερειακές συσκευές που επικοινωνούσαν στο δίκτυο της έξυπνης πόλης και μέσα από μεγάλες και περίπλοκες διαδρομές οδηγούνταν στο εργοστάσιο (Al-Turjman and Zahmatkesh, 2022). Μία επίθεση άρνησης εξυπηρέτησης (DoS) σταμάτησε την επίθεση μέσα στο δίκτυο και απέτρεψε στους εισβολείς να έχουν πρόσβαση και ανάγκασε τους εισβολείς να εγκαταλείψουν τη προσπάθεια.

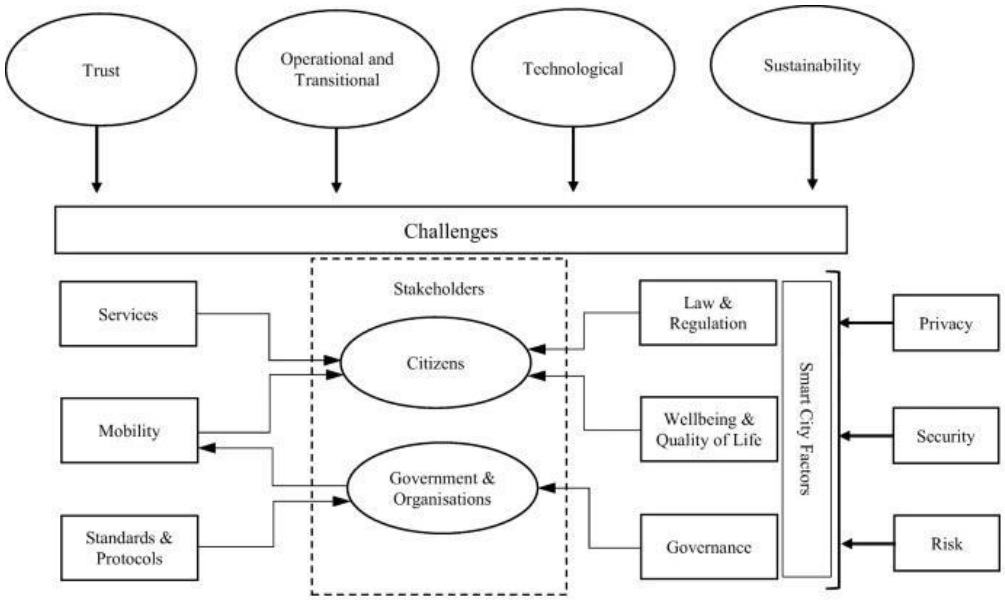
Στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) έγινε πρόσφατα μία έρευνα για την εμπιστοσύνη που υπάρχει ανάμεσα στους πολίτες και τις έξυπνες πόλεις και τα 2/3 των ερωτηθέντων απάντησαν πως δεν νιώθουν σιγουριά και ασφάλεια για τα προσωπικά δεδομένα τους και αν διασφαλίζεται το ιδιωτικό απόρρητο τους καθώς έβλεπαν καθημερινά να ανακοινώνονται κυβερνο – επιθέσεις σε μεγάλες εταιρίες ή φορείς. Στη συνέχεια της έρευνας έβλεπαν πως η μία πλευρά ‘’κατηγορούσε’’ την άλλη για έλλειψη μέτρων και μεθόδων που θα απέκλειαν πιθανές επιθέσεις (Κοσμόπουλος, 2016). Οι απειλές στον κυβερνοχώρο για την ακεραιότητα των δεδομένων αποτελούν μία αυξανόμενη ανησυχία για όλους τις έξυπνες πόλεις και τις ιδιωτικές επιχειρήσεις καθώς μπορούν να βλάψουν αρνητικά τις προσπάθειες που κάνουν και να υπονομεύσουν μελλοντικές κινήσεις τους.

Η μεγάλη εξάρτηση από ένα δίκτυο πληροφοριών μέσα σ’ ένα έξυπνο δίκτυο μπορεί να προκαλέσει εξίσου μεγάλα προβλήματα αφού όλα διαχειρίζονται σε ένα μεγάλο βαθμό μέσω διαδικτύου και υπάρχουν πιθανά ευάλωτα σημεία στο περιβάλλον με αποτέλεσμα οι επιθέσεις να στοχεύουν σε αυτές τις ευπάθειες από πολλά και διαφορετικά σημεία μέχρι να αποκτήσουν πρόσβαση στο σύστημα (Ma, 2021). Το έξυπνο δίκτυο είναι ένα σύνολο νέων τεχνολογιών με κύριο σκοπό τον εκσυγχρονισμό του δικτύου ενσωματώνοντας σε αυτό συστήματα τηλεπικοινωνιών και τεχνολογίας πληροφοριών.

Η υποδομή πληροφοριών έξυπνου δικτύου αποτελείται από ένα σύνολο λογισμικού και βάσεων δεδομένων. Για τη βελτιστοποίηση της απόδοσης του έξυπνου δικτύου

λαμβάνονται κατάλληλα μέτρα για την αποτελεσματική λειτουργία του δικτύου (Baig et al., 2017). Τα πρωτόκολλα ασφαλείας και ελέγχου σε συνδυασμό με το ιδιωτικό απόρρητο αποτελούν προτεραιότητα για τις έξυπνες πόλεις καθώς η κρυπτογράφηση που αναπτύσσεται μέσα από τις διάφορες μεθόδους έχει δώσει μία ικανοποιητική λύση στις επιθέσεις που δέχονται τα συστήματα. Οι μεγάλες ροές στο σύστημα δικτύου μπορούν να προκαλέσουν ανά πάσα στιγμή προβλήματα που να θίξουν ζητήματα ασφαλείς και κατ' επέκταση να μην αφορά μόνο το απόρρητο αλλά και την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (Ferraz and Gomes, 2016).

Στη παρακάτω εικόνα (4) φαίνεται η αλληλεπίδραση που υπάρχει και ανάμεσα στους εμπλεκόμενα τμήματα και τις σχέσεις που δημιουργούνται από τις πιθανές μεταβολές. Η εμπιστοσύνη, τα συστήματα, η τεχνολογία και η βιωσιμότητα συνδέονται άμεσα τις προκλήσεις και τις δυσκολίες που έχουν να διαχειριστούν καθώς επηρεάζονται από διαφορετικούς παράγοντες. Η ασφάλεια, η εμπιστοσύνη και το απόρρητο έχουν καθοριστικό ρόλο στις υπόλοιπες λειτουργικές μονάδες αφού καταλήγουν να επηρεάζουν σημαντικά τον πολίτη που χρησιμοποιεί τις υπηρεσίες. Ακόμα και εάν υπήρχε το ''ιδανικό'' προϊόν / υπηρεσία δεν θα ήταν αρκετό αν δεν υπήρχε η κατάλληλη ασφάλεια και πρότυπα που θα έδιναν σταθερότητα και σιγουριά στον πολίτη και αυτό θα είχε ως αποτέλεσμα να μην χρησιμοποιεί καμία υπηρεσία.



Εικόνα 6: Πλαίσιο ασφάλειας και απορρήτου της έξυπνης πόλης.

Η κινητικότητα, τα πρωτόκολλα και πρότυπα, τα νομικά πλαίσια, η ποιότητα ζωής και η λειτουργία της έξυπνης πόλης είναι αναγκαία και χρήσιμα όταν λειτουργούν και συνυπάρχουν – συνεργάζονται για το μοναδικό αποτέλεσμα, δηλαδή την εξυπηρέτηση και ασφάλεια του πολίτη (Ismagilova et al., 2022). Μία πιθανή και επιτυχημένη επίθεση σ' ένα τέτοιο σύστημα θα είχε αρνητικές επιπτώσεις στις σχέσεις των πολιτών με τις παροχές της έξυπνης πόλης και αυτομάτως θα την καθιστούσε ανίκανη να διαχειριστεί τα προσωπικά δεδομένα των πολιτών. Η αποτελεσματική διαχείριση και προφύλαξη των δεδομένων, η προστασία της ιδιωτικότητας και ισχυρή άμυνα των υποδομών μπορούν να δώσουν άλλες δυνατότητες και να αναπτύξουν νέους και τεχνολογικά καινοτόμες λύσεις ώστε οι πολίτες να αντιμετωπίζουν θετικά τις ενέργειες αυτές και να αποτελούν ενεργά μέρη του συστήματος με σκοπό την ανάπτυξη της πόλης και των υποδομών.

Φυσικά, σε αυτή τη σχέση εμπιστοσύνης και της ασφάλειας του απορρήτου ο πολίτης πρέπει να συμμετέχει ουσιαστικά και να μην αντιμετωπίζει τις αλλαγές καχύποπτα ή να βρίσκεται σε μία αμυντική στάση αφού όλες οι τεχνολογικές αναβαθμίσεις έχουν κύριο σκοπό την προστασία του πολίτη και όχι να τον εγκαταλείψουν (Bergh & Viaene, 2015). Η τεχνολογική ισχύς, τα κέντρα δεδομένων, οι έξυπνες συσκευές και οι νέες τεχνολογίες (τεχνητή νοημοσύνη, διαδίκτυο των πραγμάτων κτλ) είναι τα εργαλεία που έχει στα χέρια της η έξυπνη πόλη για να μπορέσει να προφυλάξει κάθε πολίτη και να σταματήσει πιθανές επιθέσεις για λογαριασμό του πολίτη που είναι εκτεθειμένος. Παρότι, οι δυσκολίες είναι πολλές και σε ορισμένες περιπτώσεις μπορεί να ''φαίνονται'' ακατόρθωτες αυτό το οικοσύστημα μπορεί να ανταπεξέλθει και να δώσει λύσεις.

2.7 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Η ελευθερία και προάσπιση των δικαιωμάτων ενός πολίτη κατοχυρώνονται από τους νόμους του Κράτους και τις αντίστοιχες νομοθετικές διατάξεις που προστατεύουν την ιδιωτικότητα και τα προσωπικά δεδομένα και δεν επιτρέπει σε κανέναν να παραβιάσει αυτό ιδιωτικό απόρρητο όπως κατοχυρώθηκε στο άρθρο 9^{A} /2001 του Συντάγματος (Hellenic Parliament, 2001). Ο νόμος είναι αυστηρός θέλοντας να τονίσει το ιδιωτικό απόρρητο και να διασφαλίσει τυχόν παρερμηνείες που θα έδιναν αρνητικές διαστάσεις στο θέμα. Φυσικά, όσο εξελίσσεται η τεχνολογία, η κοινωνία

αλλάζει και εκπαιδεύεται σε νέους τρόπους και εφαρμογές (λόγω της αλληλεπίδρασης με έξυπνες συσκευές) και προσπαθεί να κατανοήσει τις αλλαγές.

Η διαφορά που προκύπτει ανάμεσα στη ψηφιακή παρουσία σε σχέση με τη φυσική ενός πολίτη είναι ότι στη ψηφιακή παρουσία του σε κάποια υπηρεσία ενδέχεται να αποκαλύψει ευκολότερα προσωπικά δεδομένα ή να γίνει μέρος ενός συνόλου που θα διαχειρίζονται προσωπικές του πληροφορίες καθώς δεν θα έχει ενημερωθεί πλήρως ή θα περιορίζεται η ελευθερία του για να μπορέσει να κάνει χρήση της υπηρεσίας. Η συγκριτικά μεγαλύτερη αποστολή και λήψη πληροφοριών στο ψηφιακό κόσμο σε σχέση με το παραδοσιακό τρόπο (φυσική παρουσία) είναι χαοτική καθώς μέσα από τις ροές των έξυπνων δικτύων και των νέων τεχνολογιών μεταφέρονται σε κέντρα αποθήκευσης και επεξεργασίας με σκοπό να ‘’φιλτραριστούν’’ και να προωθηθούν συγκεκριμένα στις κατάλληλες επιχειρήσεις/φορείς κτλ. Αξίζει να σημειωθεί πως η Ελλάδα σαν μέλος της Ευρωπαϊκής Ένωσης ασπάζεται και λειτουργεί αντίστοιχα με τις Ευρωπαϊκές Άξιες και Ήθη για τα Ανθρώπινα Δικαιώματα όπως ισχύουν και στην Ένωση (European Union, 2007). Μέσα από μία σειρά ενεργειών της Ευρωπαϊκής Ένωσης το 2014 αναδιοργανώθηκε το νομικό κυρίως πλαίσιο για τη Προστασία των Προσωπικών Δεδομένων ώστε να ενημερωθούν καλύτερα οι πράξεις νόμου αλλά και να συμμορφωθεί η Κοινωνία στο σύνολο (πολίτες – επιχειρήσεις – κράτος). Τα βασικότερα χαρακτηριστικά του νέου κανονισμού είναι η νομική και ηθική τήρηση των νόμων περί προστασίας και ασφάλειας του πολίτη, η σωστή επεξεργασία των προσωπικών δεδομένων, η εξακρίβωση των δεδομένων, η νομιμότητα και η πιστοποίηση γνησιότητας των δεδομένων (ΓΚΠΔ, 2022).

2.8 ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Τα τελευταία χρόνια έγιναν μεγάλα βήματα για να μπορέσει ένα πολίτης – χρήστης να αξιοποιήσει όλες τις δυνατότητες που του δόθηκαν από τις νέες τεχνολογίες (5G, Cloud, NFC, IoT, AI) μέσα στις έξυπνες συσκευές που χρησιμοποιεί στη καθημερινότητα του. Ένας επιπλέον λόγος που αύξησε τη συχνότητα αυτή τα τελευταία χρόνια είναι λόγω της υγειονομικής κρίσης (Covid-19) όπου ήταν αναγκαίο και χρήσιμο για τη προστασία της ζωής των πολιτών. Έτσι, μέσα από αυτές τις φάσεις προωθήθηκε η ασύρματη και ευέλικτη τεχνολογία με υπηρεσίες νέφους, ασύγχρονα δίκτυα και ψηφιακές λύσεις και υπηρεσίες όπου οι πολίτες ‘’ανέβασαν’’ αρκετά στοιχεία από τα προσωπικά τους δεδομένα όπως για παράδειγμα είναι η

ταυτότητα, ο φορολογικός αριθμός, μία κάρτα υγείας, τα τραπεζικά στοιχεία και οι λογαριασμοί (Badii et al., 2020). Η μετακίνηση λοιπόν από τη παραδοσιακή μορφή χρήσης στο ψηφιακό κόσμο έχει σαν αποτέλεσμα να μεταφέρονται τεράστιες ποσότητες δεδομένων που αυτομάτως αυξάνονται όλες οι πιθανότητες στον αντίστοιχο βαθμό για μία κυβερνο – επίθεση καθώς είναι δύσκολο να ληφθούν όλες οι πιθανές επιθέσεις ακόμη και από τις προηγμένες τεχνολογίες (AI). Ουσιαστικά, θα μπορούσε κανείς να φανταστεί ένα γιγάντιο εικονικό ‘’εγκέφαλο’’ που λαμβάνει, επεξεργάζεται και μαθαίνει τα πάντα για τους πολίτες και ξαφνικά δέχεται μαζικές επιθέσεις καθώς είναι στο επίκεντρο της τεχνολογίας και η προσοχή των εισβολέων είναι στραμμένη επάνω του (Παντελοπούλου, 2021).

Μέσα από τις νέες τεχνολογίες και τους τρόπους αποθήκευσης των δεδομένων υπάρχουν αρκετά θέματα που χρειάζονται επιπλέον μέτρα για την ασφάλεια των πληροφοριών καθώς όλα βρίσκονται σε απομακρυσμένες βάσεις δεδομένων. Η ανάπτυξη του υπολογιστικού νέφους (cloud computing) για παράδειγμα είναι μία έξυπνη και ευέλικτη τεχνολογία που δίνει τη δυνατότητα στους χρήστες να αποθηκεύουν τα δεδομένα τους και να έχουν παράλληλα πρόσβαση από διαφορετικά σημεία. Έτσι, οι επιχειρήσεις κυρίως που διαχειρίζονται αυτές τις βάσεις έχουν αναπτύξει το δικό τους μοντέλο – γράφο όπου συνεργάζονται και με τρίτες εταιρίες δίνοντας πρόσβαση στα δεδομένα των χρηστών (Nowicka, 2014). Η συγκατάθεση πολλές φορές είναι υποχρεωτική για την ‘’αδιάλειπτη’’ χρήση της πρόσβασης και της ασφάλειας με όλα τα λογισμικά που χρησιμοποιούνται και τις τεχνικές. Πιθανόν, οι έξυπνες πόλεις να υστερούν σε αρκετά θέματα τεχνογνωσίας / ειδίκευσης στα θέματα αυτά καθώς υπάρχουν ακόμη και σήμερα σοβαρά προβλήματα στις υποδομές, στους πόρους που δεν επαρκούν για να αυξήσουν ποιοτικά τα εργαλεία τους, στο λογισμικό, στις εφαρμογές κρυπτογραφίας, σε νέους μηχανισμούς και στη προτυποποίηση μεθόδων. Τα προβλήματα και οι αρνητικές επιπτώσεις που προκύπτουν είναι η παραβίαση των συστημάτων, η κακή διαχείριση των υποδομών, η έλλειψη μηχανισμών αποτροπής και οι περιορισμοί στις λύσεις.

2.9 ΠΑΡΑΒΙΑΣΗ ΙΔΙΩΤΙΚΟΥ ΑΠΟΡΡΗΤΟΥ

Υπάρχουν αρκετές πόλεις στην Ευρώπη όπως η Κοπεγχάγη, η Στοκχόλμη, Άμστερνταμ και η Βιέννη που προσπαθούν να αναβαθμίσουν τις υποδομές τους μέσα από τη τεχνολογία καθώς έχουν εστιάσει σε έξυπνους δρόμους, βιομηχανικά λιμάνια,

ηλεκτρικά αυτοκίνητα, συσκευές κατάλληλες για το περιβάλλον και την ενέργεια στοχεύοντας στη καλύτερη διαχείριση των πόρων και της βελτίωσης της ποιότητας ζωής των πολιτών (TVXS, 2019). Όλες οι λειτουργίες που προαναφέρθηκαν περνάνε από τους αντίστοιχους πίνακες ελέγχου και συστημάτων διαχείρισης μαζί με όλα τα προσωπικά δεδομένα των πολιτών αφού νωρίτερα έκαναν χρήση των υπηρεσιών. Αξίζει να σημειωθεί ότι αυτές οι βάσεις δεδομένων δεν υπολειτουργούν ή βρίσκονται σε κάποια μορφή αδράνειας αλλά εργάζονται 24/7 και τις 365 του χρόνου. Έτσι, βρίσκονται διαρκώς σε μία μόνιμη και σταθερή θέση, αυτή της επεξεργασίας και ανάλυσης των δεδομένων που συλλέχθηκαν και πιθανόν να διαμοιραστούν σε τρίτα μέρη εν αγνοία των πολιτών. Ενδεικτικά παραδείγματα κοινοποίησης προσωπικών δεδομένων ήταν η μεταφορά δεδομένων από εταιρία παροχής ηλεκτρικής ενέργειας σε άλλη εταιρία με σκοπό τις διαφημιστικές τους ανάγκες να αυξήσουν το πελατολόγιο τους δίνοντας πρόσβαση σε (διευθύνσεις, αριθμούς επικοινωνίας και στοιχεία επικοινωνίας). Επίσης, ένα ακόμη περιστατικό που καταγράφτηκε με τη κοινοποίηση δεδομένων ήταν όταν δόθηκαν σε άλλη αντίστοιχες πληροφορίες και είχε ως αποτέλεσμα να επηρεάσουν μαζικά τις γνώμες των πολιτών σε πολιτικό επίπεδο (Caputo et al., 2016). Η διασφάλιση του απορρήτου είναι σημαντικοί για τους χρήστες καθώς ανησυχούν για πιθανές παραβιάσεις από τις έξυπνες συσκευές που μελετούν τις συμπεριφορές τους και τις κινήσεις τους μέσα από τη συλλογή των δεδομένων.

Ο ξαφνικός κίνδυνος της παραβίασης σαν υποψία απομακρύνει σε αρκετές περιπτώσεις τους χρήστες καθώς πιστεύουν πως δεν τηρούνται τα μέτρα ασφαλείας ή δεν υπάρχει πλήρες έλεγχος και μπορούν να εκτεθούν ανά πάσα στιγμή. Επομένως, οι συσκευές IoT που υπάρχουν μέσα στις έξυπνες πόλεις έχουν δύο κύριες προκλήσεις: η τήρηση ασφαλείας των δεδομένων και ο τρόπος διαχείρισης των δεδομένων. Είναι σημαντικό να νιώθει ένας χρήστης το ίδιο ασφαλής όταν βρίσκεται και εκτός σπιτιού αφού υπάρχουν αμέτρητες εφαρμογές που τον εντοπίζουν μέσω GPS καθώς δίνει τη συγκατάθεση του για να χρησιμοποιήσει την υπηρεσία. Εφόσον υπάρχει το νομοθετικό πλαίσιο που εγγυάται την ασφάλεια των υπηρεσιών και τη συμμόρφωση των εταιριών προς όφελος των πολιτών περιορίζεται η μετακίνηση των πληροφοριών σε ένα βαθμό. Δεν είναι τυχαίο που σε αρκετές περιπτώσεις αλλάζουν τα μέτρα ασφαλείας και διαφοροποιούνται για να τονίσουν τη μοναδικότητα του κάθε χρήστη και να σεβαστούν το ιδιωτικό απόρρητο (Lucic et al., 2018). Η καταγραφή και

παρακολούθηση του χρήστη μέσα από τις συσκευές μπορεί να οδηγήσει σε αρνητικά σενάρια καθώς μπορεί να μάθει μία συσκευή εύκολα τις συνήθειες του χρήστη, να εξάγει δεδομένα και συμπεράσματα και να κοινοποιηθούν χωρίς τη συγκατάθεση του παραβιάζοντας τους νόμους. Ως εκ τούτου, η προστασία των προσωπικών δεδομένων είναι ζωτικής σημασίας και επηρεάζει άμεσα την εμπειρία του χρήστη – πολίτη και τις σχέσεις εμπιστοσύνης με την έξυπνη πόλη που δραστηριοποιείται. Έτσι, δεν πρέπει να συνδέονται οι χρήστες με τις εφαρμογές άμεσα και να αποκαλύπτονται οι πληροφορίες τους (π.χ. τοποθεσία, ταυτότητα κτλ) και να προστατεύονται άμεσα από τους νόμους καθώς έχει προτεραιότητα η ανάπτυξη της κοινωνίας.

ΚΕΦΑΛΑΙΟ 3: ΤΟ ΠΛΑΙΣΙΟ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

3.1 ΚΑΤΗΓΟΡΙΕΣ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια και η προστασία των πολιτών μέσα στις έξυπνες πόλεις είναι η μέγιστη προτεραιότητα ώστε να διαφυλάσσεται αυτό το οικοσύστημα και να αναπτύσσεται διαρκώς καλύπτοντας όλες τις ανάγκες των πολιτών. Η ανάπτυξη των έξυπνων πόλεων έχει να κάνει άμεσα με το πλαίσιο της αρχιτεκτονικής και ασφάλειας που θα σχεδιαστεί η πόλη καθώς και τις επιμέρους λειτουργίες και εφαρμογές που θα αναπτύξει. Επίσης έχουν δημιουργηθεί κανόνες που συμβάλλουν και ενισχύουν τους νόμους και τους κανονισμούς και δίνουν κατευθυντήριες γραμμές ώστε να οργανώνονται καλύτερα οι έξυπνες πόλεις και να παρέχουν ολοκληρωμένες λύσεις στους πολίτες διαμορφώνοντας κατάλληλα μέτρα και υπηρεσίες (Alaba et al., 2017).

Η έννοια της ασφάλειας χωρίζεται σε τέσσερις κατηγορίες και αναφέρονται παρακάτω. Αρχικά, είναι η Διακυβέρνηση, δηλαδή μία κατηγορία που δείχνει τον τρόπο λειτουργίας μέσα από ένα σύνολο κανόνων και εφαρμογών δίνοντας μία κατεύθυνση στους πολίτες. Υπάρχουν κανόνες και πολιτικές που προσπαθούν να ενισχύσουν την οργάνωση και τη οικοδόμηση της έξυπνης πόλης μέσα στις αλλαγές αυτές και να δώσουν ένα επιπλέον όφελος στους πολίτες. Επίσης, είναι σημαντικό να αναφερθεί ο τρόπος που θα γίνουν, τι είδους πολιτικές ασφαλείας θα αναπτυχθούν και θα διαμορφωθούν, πως θα λειτουργούν, η δομή και η οργάνωση (HaddadPajouh et al., 2021). Η διαμόρφωση τέτοιων πρακτικών ασφαλείας είναι σημαντικά συνδεδεμένα με το νόμο περί προστασίας Προσωπικών Δεδομένων και ενισχύεται διαρκώς από την εκάστοτε νομοθεσία καθώς γίνεται προσπάθεια για να αποφευχθούν παραβατικές συμπεριφορές και καταστάσεις που θα δημιουργούσαν επιπλέον θέματα στην ασφάλεια και την εμπιστοσύνη των πολιτών μέσα στις έξυπνες πόλεις αλλάζοντας τις ισορροπίες αρνητικά.

Ακόμη, μία σημαντική κατηγορία που επηρεάζεται σημαντικά και σχετίζεται με την ασφάλεια είναι η υπηρεσία που παρέχεται και οι διάφορες λειτουργίες της καθώς υπάρχουν σημαντικά δεδομένα που αναπαράγονται μέσα από τη χρήση και δημιουργούν χρήσιμες πληροφορίες που μπορούν να καθορίσουν το σχηματισμό στις υποδομές. Επίσης, μία υπηρεσία σχεδιάζεται και αναπτύσσεται μέσα σε μία έξυπνη πόλη για να επιφέρει σημαντικά οικονομικά οφέλη καθώς μελετούνται τα πιθανά

μοντέλα που μπορούν να ενισχύσουν την οικονομία. Η ασφάλεια που απαιτείται είναι υψηλή και σε καμία περίπτωση δεν πρέπει να μένει ‘’πίσω’’ στις πολιτικές ενημέρωσης και ελέγχου καθώς αυξάνεται ο κίνδυνος να προκληθούν απώλειες. Θα πρέπει σε κάθε περίπτωση η τεχνολογία που αναπτύσσεται να ακολουθείται από την υπηρεσία και την ασφάλεια ώστε να ενισχύεται και ο ρόλος τους και να διευκολύνουν στη καθημερινότητα τους πολίτες σε ένα συνεχόμενο και μεταβαλλόμενο περιβάλλον. Μέσα από την τεχνολογία μπορεί η υπηρεσία να δώσει και τεράστια οικονομικά οφέλη που να είναι σε θέση μία έξυπνη πόλη να ενισχύσει τα διάφορα επιχειρηματικά μοντέλα και να προσφέρουν νέες ευκαιρίες και δυνατότητες καθώς εξελίσσεται η πόλη.

Στη συνέχεια, υπάρχει η τρίτη κατηγορία που εμπλέκεται με την ασφάλεια και λέγεται ‘’City OS’’ δηλαδή είναι η κατηγορία που συγκεντρώνει όλες τις χρήσιμες πληροφορίες που συλλέγονται από τη κατηγορία ‘’Assets’’ και διαχειρίζεται ως πλατφόρμα παροχής δεδομένων. Θεωρείται σημαντική κατηγορία καθώς εδώ μέσα αναπτύσσονται υπηρεσίες cloud, IoT εφαρμογές, διαδικτυακοί servers και ένα σύνολο μέτρων ασφαλείας που ελέγχουν την ορθότητα των στοιχείων, προσωπικά δεδομένα, συστήματα ασφαλείας, πιθανές ευπάθειες και ταυτότητες χρηστών ώστε να υπάρχει η ασφάλεια που απαιτείται στο σύστημα. Το σύστημα επικοινωνεί τόσο εσωτερικά αλλά και εξωτερικά ανατροφοδότηση και ενημέρωση καθώς και να τηρούνται όλα τα πρωτόκολλα ασφαλείας και κρυπτογράφησης για να είναι σε θέση το σύστημα να εγγυηθεί τη διαθεσιμότητα και την ακεραιότητα των υπηρεσιών καθώς και την ορθότητα των δεδομένων.

Τέλος, τα περιουσιακά στοιχεία που υπάρχουν μέσα στο οικοσύστημα και οι διάφορες συσκευές που ενισχύουν τα δίκτυα, την αναμετάδοση και ανατροφοδότηση και είναι απαραίτητα καθώς η παρεχόμενη υπηρεσία μπορεί να μη λειτουργήσει επαρκώς και να προκύψουν πιθανές ανωμαλίες ή απώλειες στο σύστημα επικοινωνίας. Η κατηγορία αυτή είναι σημαντική λόγω της ακεραιότητας. Η μεταφορά δεδομένων είναι σύνθετη και δύσκολη διαδικασία και απαιτεί αρκετές διεργασίες και μηχανισμούς ασφαλείας ώστε να προστατεύσουν επαρκώς όλα τις πληροφορίες και να ανιχνεύσουν άλλες απώλειες (Popescul & Radu, 2016). Η επικοινωνία εσωτερικά και εξωτερικά με το σύστημα έχει να κάνει κυρίως με τους μηχανισμούς ασφαλείας και την εμπιστευτικότητα των περιουσιακών στοιχείων τόσο

σε επίπεδο διαθεσιμότητας όσο και της ακεραιότητας καθώς είναι η κύρια πηγή δεδομένων.

Η ασφάλεια από μόνη της σαν κατηγορία δεν μπορεί να προσφέρει τις ιδανικές λύσεις μέσα σε ένα οικοσύστημα εάν δεν έχουν ληφθεί και τα κατάλληλα μέτρα που θα ενισχύσουν και θα αποτρέψουν πιθανούς κινδύνους που υπάρχουν μέσα στις έξυπνες πόλεις και τους μηχανισμούς ασφαλείας που αναπτύσσονται για αυτούς τους λόγους (Weber, 2010). Το πλαίσιο της ασφάλειας δεν πρέπει να περιορίζεται αλλά ούτε και να απαξιώνεται καθώς πολύ εύκολα μπορεί να δημιουργηθεί ένα ‘’κενό’’ και να διαρρεύσουν δεδομένα και να αλλάξουν τις ισορροπίες αρνητικά. Για αυτούς τους λόγους λαμβάνονται και πολιτικές ασφαλείας αξιολογώντας τους κινδύνους και αναπτύσσοντας ρόλους και μηχανισμούς που θα διαχειρίζονται σωστά τα πληροφοριακά συστήματα και φυσικά τα προσωπικά δεδομένα των πολιτών καθώς αποτελούν ένα από τους κύριους λόγους πιθανών επιθέσεων μέσα σε μία έξυπνη πόλη (Toh, 2020). Αυτές οι κατηγορίες περιγράφουν την έννοια της ασφάλειας και τους στόχους – ρόλους της μέσα στην έξυπνη πόλη και τις ανάγκες που υπάρχουν ώστε να λειτουργούν όλα σωστά και να αξιοποιούν οι πολίτες τις υπηρεσίες προς όφελος τους χωρίς να διστάζουν ή να ανησυχούν για πιθανές παραβιάσεις ή κινδύνους από εξωτερικούς παράγοντες. Η ασφάλεια τους πρέπει να είναι στο επίκεντρο όλων των εφαρμογών και υπηρεσιών και να προσφέρουν συνεχώς τη βέλτιστη εμπειρία στους πολίτες καθώς και αυτοί είναι μέρος αυτού του οικοσυστήματος και δεν υπάρχει άλλος τρόπος να επιβιώσει χωρίς τον άνθρωπο (Ministry of Internal Affairs and Communication, 2020).

Εικόνα 7: Κατηγοριοποίηση αρχιτεκτονικής στην έξυπνη πόλη.

3.2 ΚΙΝΔΥΝΟΙ ΚΑΙ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα προβλήματα που δημιουργούνται μέσα στην έξυπνη πόλη ποικίλουν και διαφέρουν καθώς υπάρχουν αρκετοί κίνδυνοι. Ο πάροχος υπηρεσιών, οι εφαρμογές, το σύστημα διαχείρισης, μία ευπάθεια, ένας μη εξουσιοδοτημένος χρήστης που καταγράφτηκε, μία επίθεση στο σύστημα με απώλειες δεδομένων μπορούν να επηρεάσουν σοβαρά τις λειτουργίες ενός οικοσυστήματος ειδικά αν δεν είναι ενημερωμένα τα πληροφοριακά συστήματα και δεν επικοινωνούν μεταξύ τους (Biswas, 2016). Είναι αρκετά σύνθετο ζήτημα η ασφάλεια που μπορεί να αναπτυχθεί μέσα σε μία έξυπνη πόλη καθώς και ποιους μηχανισμούς θα χρειαστούν για να μπορέσουν να αντέξουν σε πιθανές παραβιάσεις ή ευπάθειες. Φυσικά, οι κίνδυνοι είναι πολλοί και δεν έχουν τον ίδιο βαθμό δυσκολίας ως προς την αντιμετώπιση ή ζημία. Επομένως, μία έξυπνη πόλη πρέπει να γνωρίζει κάθε πιθανό σημείο παραβίασης και να είναι σε θέση να μπορεί να αντισταθεί σε αρκετές επιθέσεις που μπορούν να προσβάλουν τις λειτουργίες (Jeong & Park, 2019). Αναπτύσσοντας τους κατάλληλους μηχανισμούς και τις αντίστοιχες αμυντικές ζώνες μπορεί να σταματήσει μία επίθεση και να απομακρύνει τους κακόβουλους ιούς ώστε να μην περάσουν στο εσωτερικό του δικτύου και προκαλέσουν επιπλέον ζημίες.

Μερικές φορές οι πολιτικές διαχείρισης των δεδομένων μπορεί να επιφέρει ένα καλύτερο αποτέλεσμα μέσα στο σύστημα καθώς θα είναι σε θέση οι φορείς να

γνωρίζουν καλύτερα την εκάστοτε κατάσταση και φυσικά να μπορούν να διαχειριστούν άμεσα το πρόβλημα. Σε αυτό το σημείο αξίζει να τονιστεί η σπουδαιότητα των δεδομένων καθώς επηρεάζουν σημαντικά και τα αποτελέσματα κυρίως από τη δομή τους, δηλαδή αν είναι ανοιχτά ή κλειστά δεδομένα και αν έχουν ταυτοποιηθεί μέσα από μία σειρά που ορίζει το σύστημα . Έτσι, μπορεί να δημιουργηθούν κενά και ευπάθειες μέσα στο σύστημα και να επηρεάσουν τις βασικές λειτουργίες των συστημάτων (Jameel et al., 2019). Για παράδειγμα, αν μία έξυπνη πόλη ανέθετε τη κατασκευή του δικτύου σε ένα πάροχο τηλεπικοινωνιών χωρίς να κοινοποιήσει πιθανές αλλαγές ή μέτρα μέσα στο σύστημα και ο πάροχος έδινε σε τρίτους ένα μέρος των εργασιών χωρίς να αποκαλύψει με τη σειρά του τα δικά του ‘’μυστικά’’ τότε θα ήταν λογικό να υπάρχουν προβλήματα και ευπάθειες που δεν θα είχαν προβλεφτεί από κανέναν και θα είχαν σίγουρα δυσάρεστες εκπλήξεις για την έξυπνη πόλη και παράλληλα την έλλειψη εμπιστοσύνης των πολιτών αφού θα έβλεπαν τα προβλήματα και δεν θα ήθελαν να συμμετέχουν ξανά σε κάτι που πιθανόν να μην τους προστατεύει ή λειτουργεί σωστά για το καλό τους μέσα στη πόλη (Cui et al., 2018).

Η λήψη κατάλληλων μέτρων ασφαλείας με κύριο γνώμονα την εξυπηρέτηση των πολιτών και τη προστασία τους έχει να κάνει και με τις απαιτήσεις που υπάρχουν ή έχουν δημιουργηθεί από τους χρήστες καθώς μαθαίνουν μέσα σε αυτό το οικοσύστημα. Η έξυπνη πόλη προσπαθεί να βοηθήσει τους πολίτες και να τους δώσει μία καλύτερη οργάνωση ώστε να προστατεύονται από κάθε εξωτερική επίθεση και να λαμβάνουν ενημερώσεις για τις πιθανές παραβιάσεις. Έτσι, μία έξυπνη πόλη δεν λαμβάνει απλώς μέτρα για να επιβιώσει αλλά για να μπορέσει να οικοδομήσει και μελλοντικά τις υπηρεσίες της και να διαμορφώσει νέες και καινοτόμες λύσεις που θα έχουν ως σκοπό τον πολίτη . Τα μέτρα ασφαλείας που εφαρμόζονται έχουν να κάνουν και σε ένα βαθμό για το πόσο καλά μπορεί κάποιος να κατανοήσει τις δυσκολίες και να εξάγει σημαντικές πληροφορίες που θα δώσουν μία στρατηγική στην έξυπνη πόλη (Laufs et al., 2020). Ο προσδιορισμός των δεδομένων, η προστασία του συστήματος, οι υποδομές, οι συνεργαζόμενες λειτουργίες, τα περιουσιακά στοιχεία και τις απαιτήσεις των χρηστών μέσα στην έξυπνη πόλη είναι κάποια από τα σημαντικότερα στοιχεία για να ληφθούν και τα κατάλληλα μέτρα ασφαλείας. Ένα ακόμα σημαντικό σημείο στην έξυπνη πόλη είναι η διασφάλιση της αξιοπιστίας των δεδομένων και των υπηρεσιών καθώς εμπλέκονται αρκετά τμήματα και φορείς και σε διαφορετικά

επίπεδα επηρεάζοντας και το σύστημα ανάλογα και με πιθανές διαρροές σε πληροφορίες που θα βλάψουν την οργάνωση και ασφάλεια της έξυπνης πόλης. Η ψηφιοποίηση των διαδικασιών και η χρήση έξυπνων συσκευών μπορούν να διασφαλίσουν την ακεραιότητα, την αυθεντικότητα και την αξιοπιστία των υπηρεσιών μέσα στη πόλη (Sengan et al., 2020). Επομένως, ένας ψηφιακός μετασχηματισμός δεν αρκεί για να προχωρήσουν οι παρεχόμενες υπηρεσίες στους πολίτες. Τα μεγάλα δεδομένα, οι ψηφιακές πλατφόρμες, οι τυποποιήσεις των επικοινωνιών κ.α. είναι μερικά από τα χρήσιμα εργαλεία που έχει μία έξυπνη πόλη ώστε να λειτουργήσει και να παρέχει αποτελεσματικά λύσεις που θα αναπτύξουν και τους υπόλοιπους τομείς και φυσικά τις μελλοντικές συνεργασίες καθώς η τεχνολογία και η καινοτομία δεν σταματούν ποτέ αφού εστιάζουν στον άνθρωπο. Τα μέτρα που λαμβάνονται σε κάθε περίπτωση θα πρέπει να είναι δομημένα σωστά και φυσικά να έχουν προηγηθεί δοκιμές για πιθανές ευπάθειες καθώς η επίθεση μπορεί να είναι συνεχόμενη και ξαφνική. Τα αμυντικά συστήματα και οι μηχανισμοί που μπαίνουν σε ένα οικοσύστημα έχουν να κάνουν με αρκετά πράγματα γιατί απαιτεί συγχρονισμό και αμεσότητα στις λειτουργίες και αποτελεσματικές λύσεις στις πιθανές απειλές.

3.3 ΑΠΑΙΤΗΣΕΙΣ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια είναι η δύναμη της ισορροπίας μέσα σε ένα σύστημα καθώς όσο πιο ασφαλή είναι το σύστημα τόσο περισσότερο θα γίνει η προσπάθεια για να εξελιχθεί τεχνολογικά. Η ασφάλεια λοιπόν μέσα σε μία έξυπνη πόλη μπορεί να ‘’καταρρεύσει’’ από αρκετά σημεία καθώς οι πιθανές παραβιάσεις μπορούν να γίνουν μέσα από το δίκτυο, από υπολογιστές, αισθητήρες και τους servers. Η απαραίτητο να υπάρχει ένα ολοκληρωμένο σύστημα που θα ελέγχει και θα ανιχνεύει πιθανές παραβιάσεις (Τσανή, 2021). Παρακάτω καταγράφονται ορισμένες απειλές για την ασφάλεια μέσα σε μία έξυπνη πόλη (υποκλοπές, παραποίηση στοιχείων χρηστών, απώλεια δεδομένων, αποκάλυψη). Επιθέσεις υπάρχουν επίσης σε υλικό ή λογισμικό μέσα από κόμβους ή κακόβουλα λογισμικά που προκαλούν ζημίες. Ακόμη, υπάρχουν οι επιθέσεις phishing με παράνομα λογισμικά και παρακολουθήσεις από μη εξουσιοδοτημένα άτομα, επιθέσεις κρυπτογράφησης, δηλαδή επιθέσεις που έχουν σκοπό να πλήξουν την ασφάλεια και την ακεραιότητα των υπηρεσιών και τέλος η επιθέσεις hacking με παραπλανητικές ενημερώσεις, ανεπιθύμητα μηνύματα, αλληλογραφία και ψεύτικες ειδήσεις στοχεύοντας να αποσπάσουν σημαντικές

πληροφορίες από τους χρήστες. Για να μειωθεί η πιθανότητα μίας επίθεσης θα πρέπει να ληφθούν και τα κατάλληλα μέτρα για τις αντίστοιχες περιπτώσεις ασφαλείας. Αρχικά θα πρέπει να διασφαλιστεί η εμπιστευτικότητα, η ιδιωτικότητα, η ακεραιότητα και διαθεσιμότητα. Έτσι θα υπάρχει ένα επίπεδο ελέγχου και δεν θα παραβιάζονται στα συστήματα. Αξίζει να σημειωθεί ότι η αυθεντικοποίηση είναι η διαδικασία της επιβεβαίωσης των προσωπικών δεδομένων και συνήθως γίνεται με τη δημιουργία ενός προφίλ (username / password). Επίσης, ένας άλλος μηχανισμός αποτροπής και πρόληψης της ασφάλειας και της ιδιωτικότητας είναι η εξουσιοδότηση, δηλαδή η ελεγχόμενη πρόσβαση του χρήστη σε ένα μέρος ή συγκεκριμένες υπηρεσίες όπου δεν έχει πλήρη δικαιώματα στο σύστημα και αναμένει την έγκριση πάντα από τον διαχειριστή. Ακόμη σαν μηχανισμός ασφαλείας είναι η αναγνώριση, δηλαδή αν τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση για να συνεχίσουν την αναγνώριση στο σύστημα (Μενεγάτος, 2021). Ακόμη μία κατηγορία μηχανισμού ασφαλείας που χρησιμοποιείται είναι τα μη συνδεδεμένα, δηλαδή αν προστατεύουν την ιδιωτικότητα του πολίτη μέσα στην έξυπνη πόλη από πιθανούς κινδύνους και αν αποκαλύπτουν τη ταυτότητα του και τέλος η κρυπτογραφία και η ανωνυμία που προσπαθούν να αμυνθούν και να προστατέψουν τα προσωπικά δεδομένα χωρίς να παραποιηθούν τα δεδομένα και να μην επεξεργαστούν από μη εξουσιοδοτημένους χρήστες καθώς δημιουργούνται ισχυροί μηχανισμοί που εξασφαλίζουν την αποτελεσματική λειτουργία μέσω αλγορίθμων και κλειδιών που έχουν δημιουργηθεί για να προστατέψουν τους πολίτες από επιθέσεις και πιθανούς κινδύνους (Ζαχαροπούλου, 2020). Προφανώς, και όλοι οι μηχανισμοί επηρεάζουν και επηρεάζονται και από άλλες παραμέτρους και για αυτό δημιουργούνται επιπλέον και διαφορετικά επίπεδα ασφαλείας ώστε να αποτρέψουν ή να καθυστερήσουν μία επίθεση. Έτσι, μία έξυπνη πόλη έχοντας κάνει μία στατιστική πρόβλεψη και μοιράζοντας τους διαθέσιμους πόρους μέσα στο οικοσύστημα μπορεί να μη προβλέψει κάποια αλλαγή ή ακόμα χειρότερα να μην επαρκούν οι πόροι και να εκτεθεί σε μία επίθεση. Η απώλεια των δεδομένων, η αναγνώριση άγνωστων λογαριασμών και οι συνεχόμενες – αυξανόμενες ροές στο δίκτυο είναι μερικά στοιχεία που θα πρέπει να αναγνωρίζονται και να εξετάζονται καθώς μπορεί να κρύβεται ένας πιθανός κίνδυνος που έχει ως στόχο να ‘’βλάψει’’ τις εφαρμογές ή υπηρεσίες και να προκαλέσει δυσπιστία στους χρήστες καθώς δεν θα έχουν την πλήρη κάλυψη.

3.4 ENISA - ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ

3.4.1 ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Για να μπορέσει ένα σύστημα να προστατευτεί από μία κακόβουλη επίθεση θα πρέπει αρχικά να λάβει κάποια σημαντικά μέτρα φυσικής ασφαλείας ώστε να περιορίσει τις πιθανές φυσικές καταστροφές, τις κλοπές ή μία πιθανή διακοπή στο δίκτυο. Είναι απαραίτητο να προστατευτούν όλα τα κρίσιμα σημεία ώστε να μην έχει πρόσβαση κανένας μη εξουσιοδοτημένος χρήστης και φυσικά να είναι αποτρεπτικό να πλησιάσει με σκοπό να καταστρέψει ή να προκαλέσει υλικές ζημιές. Έτσι, όταν βρίσκεται μία έξυπνη πόλη στην αρχική φάση της υλοποίησης και του σχεδιασμού θα πρέπει να λάβει σοβαρά υπόψη της πως θα προφυλάξει τις υποδομές σε ασφαλή σημεία και να διασφαλίσει μελλοντικά ότι δεν θα χρειαστεί ξανά κάποια επιπλέον κίνηση. Η ζημιές που μπορούν να προκληθούν μπορεί να επηρεάσουν άλλες σημαντικές υποδομές και να προκαλέσουν προβλήματα στους χρήστες. Η διαρκής ενημέρωση των πολιτών και του προσωπικού είναι απαραίτητη καθώς δίνεται η ενημέρωση στους ανθρώπους και είναι πιο προσεκτικοί στις απειλές που μπορεί να δεχτούν μέσα στον κυβερνοχώρο. Το προσωπικό που εργάζεται θα πρέπει να ενθαρρύνει τους πολίτες να αντιμετωπίζουν με σοβαρότητα και ψυχραιμία τις απειλές καθώς και να συμμορφώνονται με τους κανόνες ασφαλείας όπως ορίζονται. Υπάρχουν πολλά μέτρα που χρησιμοποιούνται για την αντιμετώπιση των απειλών από επιδιωκόμενες διαδικτυακές επιθέσεις. Γενικότερα, θα πρέπει να επισημανθεί ότι οι επιτιθέμενοι θα αναζητούν πάντα τον πιο αδύναμο κρίκο. Επομένως, δεν είναι απίθανο οι φορείς επίθεσης να περιλαμβάνουν όχι μόνο την τεχνολογία και τις εφαρμογές αλλά και τους ίδιους τους εργαζόμενους. Επομένως, δεν αρκεί η τεχνολογία και η εφαρμογή να σχεδιάζονται από την αρχή για να είναι ασφαλείς, αλλά είναι απαραίτητο και οι εργαζόμενοι να γνωρίζουν τις απειλές για την ασφάλεια στον κυβερνοχώρο, ώστε να είναι καλά εκπαιδευμένοι για να ενεργούν σωστά. Τελευταίος αλλά εξίσου σημαντικός είναι και ο στενός συντονισμός μεταξύ τις CSIRT και των αρχών δημόσιας ασφάλειας, όπως είναι για παράδειγμα η αστυνομία.

3.4.2 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Ένα σημαντικό εργαλείο για την ασφάλεια είναι η διαρκής επιτήρηση των συστημάτων και των ενεργειών - δραστηριοτήτων που καταγράφονται στο σύστημα.

Η παρακολούθηση και η καταγραφή αυτή εξυπηρετεί στο κέντρο ελέγχου ώστε να γνωρίζει τις κινήσεις που εκτελούνται μέσα στο έξυπνο δίκτυο. Η ασφάλεια ενός δικτύου είναι απαραίτητη και οφείλει κάθε έξυπνη πόλη ή οργανισμός να ακολουθήσει κάθε φυσικό και εικονικό δίκτυο που θα δώσει τη μέγιστη λύση καθώς το μέγεθος και η πολυπλοκότητα των συστημάτων σε συνδυασμό με τη διαχείριση των δεδομένων είναι τεράστια και πρέπει να προστατεύονται όλα τα προσωπικά δεδομένα των πολιτών που συμμετέχουν στο οικοσύστημα αυτό καθώς υπάρχουν πολλές πιθανότητες να δεχτούν κακόβουλες επιθέσεις. Έτσι, θα περιοριστούν οι διαρροές πληροφοριών και δεδομένων σε ένα σημαντικό βαθμό. Η πολιτική/πλαίσιο ασφάλειας πληροφοριών εφαρμόζεται για την αποτελεσματική διαχείριση της ασφάλειας πληροφοριών σε έναν οργανισμό. Η πολιτική αυτή ορίζει για παράδειγμα τα στοιχεία που πρέπει να προστατεύονται, τις διαδικασίες που πρέπει να ακολουθούνται καθώς επίσης και την οργάνωση της ασφάλειας. Χαρακτηριστικό παράδειγμα αποτελεί το ISO 270001.26

3.4.3 ΠΕΡΙΟΡΙΣΜΟΣ ΛΕΙΤΟΥΡΓΙΩΝ

Σε ορισμένες περιπτώσεις όταν ξαφνικά αλλάζει η ροή και η συμπεριφορά του δικτύου και των υπηρεσιών και εμφανίζονται πολλές και ταυτόχρονα διαφορετικές λειτουργίες τότε το σύστημα οφείλει να λάβει τα μέτρα του και να μειώσει τις κινήσεις και για να αυξήσει την ανθεκτικότητα του και να αμυνθεί στις πιθανές απειλές. Η άμυνα αυτή θα βοηθήσει την έξυπνη πόλη και τις υπηρεσίες της ώστε να αποφύγει καταστροφικές συνέπειες και βλάβες καθώς θα είναι σε θέση να διαχειριστεί επαρκώς κάθε πιθανή συνέπεια που θα έχει σκοπό να βλάψει τις υποδομές του δικτύου. Η ζημία που μπορεί να προκληθεί μέσα από τις επιθέσεις αυτές είναι η διακοπές στο έξυπνο δίκτυο και η υπολειτουργίες στα συστήματα και οι αρνητικές καθυστερήσεις στις εφαρμογές που θα δυσκολέψουν τους πολίτες. Ένα εικονικό ιδιωτικό δίκτυο μετατρέπει ένα ιδιωτικό δίκτυο σε δημόσιο και επιτρέπει να επωφεληθείτε από τις πολιτικές λειτουργικότητας, ασφάλειας και διαχείρισης του ιδιωτικού δίκτυο. Τα εικονικά ιδιωτικά δίκτυα προσφέρουν ασφάλεια από άκρο σε άκρο, τα οποία προσαρμόζονται, προσφέροντας συγκεκριμένες απαιτήσεις για την προστασία ανταλλαγής δεδομένων.

Οι διαδικασίες τερματισμού λειτουργίας είναι μέθοδοι για την απενεργοποίηση μιας συσκευής. Οι διαδικασίες τερματισμού συνήθως ενσωματώνουν μια λίστα ενεργειών

που πρέπει να εκτελεστούν πριν, κατά τη διάρκεια και μετά τον τερματισμό. Πρέπει να ενσωματώσουν τη λίστα των εξαρτήσεων προκειμένου να περιορίσουν τις επιπτώσεις στην υπηρεσία. Ο τακτικός έλεγχος είναι μια επιθεώρηση ή εξέταση της υποδομής (ψηφιακής ή φυσικής) για την αξιολόγηση ή τη βελτίωση της καταλληλότητας, της ασφάλειας, της αποτελεσματικότητάς της ή παρόμοια. Οι έλεγχοι συνήθως παρέχουν μια έκθεση που επισημαίνει τις αδυναμίες και προτείνει διορθωτικές ενέργειες.

3.4.4 ΠΡΟΒΛΕΨΗ ΚΑΙ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ

Η πρόβλεψη των πιθανών κινδύνων είναι ένα στοιχείο της οργάνωσης της έξυπνης πόλης που γίνεται σε αρχικό στάδιο του σχεδιασμού και προσπαθεί να μάθει και να αναλύσει όλες τις πιθανότητες που θα διαφυλάξουν την ασφάλεια των χρηστών. Η αποτελεσματικότητα της πρόβλεψης μπορεί να μεγιστοποιηθεί όταν υπάρχουν διαθέσιμοι πόροι που θα εργάζονται αποκλειστικά σε αυτό το κομμάτι της ασφάλειας και θα δίνουν πολιτικές και πρότυπα που θα ενισχύουν αυτές τις πρακτικές και θα περιορίζουν κακόβουλες επιθέσεις που θα έχουν ως στόχο να πλήξουν την ακεραιότητα και τη διαθεσιμότητα των υποδομών. Η ανάλυση των κινδύνων μπορεί να βοηθήσει περισσότερο τις έξυπνες πόλεις και να μάθουν να αναγνωρίζουν πιθανές ευπάθειες και τρωτά σημεία που χρειάζονται επιπλέον ενίσχυση σε επίπεδα ασφαλείας. Διατηρούνται αντίγραφα ασφαλείας δεδομένων, ιδανικά σε ασφαλείς διακομιστές εκτός τοποθεσίας που επιτρέπουν την ανάκτηση δεδομένων σε περίπτωση φθοράς/απώλειας. Η σωστή συντήρηση των αντιγράφων ασφαλείας διασφαλίζει ότι η ανάκτηση δεδομένων διατηρεί την ακεραιότητα, δηλαδή χωρίς απώλεια δεδομένων

3.4.5 ΑΠΟΜΑΚΡΥΣΜΕΝΟΣ ΕΛΕΓΧΟΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΣΥΣΤΗΜΑΤΩΝ

Ένα ακόμη σημαντικό στοιχείο της οργάνωσης αυτής των έξυπνων πόλεων είναι η εφαρμογή και ανάπτυξη επιχειρησιακών διαδικασιών και κατευθυντήριων γραμμών που θα πρέπει να ακολουθήσει και να εφαρμόσει. Η συμμετοχή και ανάπτυξη δεξιοτήτων του προσωπικού είναι αναγκαία και πρέπει να έχουν πιο ενεργό ρόλο καθώς συμμετέχουν σε ένα δυναμικά μεταβαλλόμενο οικοσύστημα και προφανώς πρέπει να έχουν πρόσβαση σε κάθε περίπτωση ακόμα και στα πιο απομακρυσμένα σημεία (γεωγραφικά) ώστε ακόμα και σε περίπτωση κλοπής ή βλάβης να μπορούν να

επέμβουν οι υπάλληλοι και να επιδιορθώσουν τις ζημίες. Για να ενεργοποιηθούν οι άμεσες αντιδράσεις από τους χειριστές των συστημάτων, η δυνατότητα είτε απομακρυσμένου τερματισμού είτε απενεργοποίησης ορισμένων δυνατοτήτων αυτών των στοιχείων μπορεί να ελαχιστοποιήσει τη ζημιά. Τα συστήματα ανίχνευσης εισβολής (δίκτυο) ελέγχουν όλες τις εισερχόμενες και εξερχόμενες δραστηριότητες του δικτύου, εντοπίζοντας ύποπτα μοτίβα που μπορεί να υποδεικνύουν επίθεση του δικτύου ή του συστήματος. Για την αποτελεσματική απόδοση, τα συστήματα ανίχνευσης εισβολών δικτύου θα πρέπει να διαμορφωθούν κατάλληλα (παρακολούθηση ανταλλαγής δεδομένων κλειδιών, γνώση εξουσιοδοτημένων συνδέσεων).

3.4.6 ΕΛΕΓΧΟΣ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ

Μία έξυπνη πόλη πρέπει να είναι συνεχώς συνδεδεμένη από άκρη σε άκρη με τις υποδομές και τα συστήματα, τις εφαρμογές και τις λειτουργίες της καθώς όλα λειτουργούν αρμονικά και συνεργάζονται μαζί για να δίνουν τη βέλτιστη λύση στους πολίτες. Ο συντονισμός των διεργασιών και η κατανομή τους έχει να κάνει με τις απαιτήσεις που υπάρχουν μέσα στα συστήματα και τις πιθανές απειλές που έχουν να αντιμετωπίσουν εφόσον εντοπιστούν μέσα στα συστήματα και έχουν σκοπό να πλήξουν κρίσιμες υποδομές. Ο έλεγχος σε πραγματικό επίπεδο δίνει επίσης και τη δυνατότητα στις έξυπνες πόλεις να γνωρίζουν αν υπάρχουν προβλήματα και ποια είναι αυτά και τις δυσκολίες που μπορεί να προκύψουν αν δεν λάβουν τα απαραίτητα μέτρα και γίνουν σε δεύτερο χρόνο που μπορεί να φανεί ένα πρόβλημα.

Η φυσική προστασία στοχεύει στον περιορισμό της παραβίασης και της μη εξουσιοδοτημένης πρόσβασης στη φυσική υποδομή. Τα μέτρα φυσικής προστασίας περιλαμβάνουν κλειδαριές, συναγερμούς, εξοπλισμό επιτήρησης, αισθητήρες και συστήματα ελέγχου πρόσβασης. Είναι ιδιαίτερα σημαντική η προστασία του εξοπλισμού που δεν βρίσκεται σε ασφαλή τοποθεσία (π.χ. εξοπλισμός πεδίου). Τα στοιχεία ελέγχου πρόσβασης αναφέρονται στις μεθόδους με τις οποίες ένα σύστημα χορηγεί/απορρίπτει την έγκριση πρόσβασης σε ένα θέμα με βάση τον επιτυχή έλεγχο ταυτότητας. Ο έλεγχος πρόσβασης είναι συνήθως ένας συνδυασμός φυσικών μέτρων (π.χ. κλειδί, κλειδαριά) και λογικών μέτρων (έλεγχος ταυτότητας, λίστα ελέγχου πρόσβασης). Ο έλεγχος πρόσβασης περιορίζει τη μη εξουσιοδοτημένη πρόσβαση και παρέχει στοιχεία σε περίπτωση παραβίασης. Η επιτήρηση αναφέρεται στην

παρακολούθηση της συμπεριφοράς ή άλλων μεταβαλλόμενων πληροφοριών. Οι συναγερμοί δίνουν σήμα μόλις παρουσιαστεί ένα πρόβλημα ή μια συγκεκριμένη κατάσταση. Οι συναγερμοί πρέπει να ορίζονται σύμφωνα με τις απαιτήσεις ασφαλείας. Παρακολουθούν βασικούς δείκτες απόδοσης και μπορούν να ειδοποιήσουν μόλις εντοπίσουν μια απειλή. Για βέλτιστη ασφάλεια, οι συναγερμοί συνδέονται με οργανωτικές διαδικασίες.

3.4.7 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η κρυπτογράφηση είναι το κλειδί της ασφάλειας που μπορεί να εγγυηθεί την εμπιστευτικότητα των προσωπικών δεδομένων (π.χ. ταυτότητα χρήστη, συσκευή σύνδεσης, εντοπισμός κτλ) ασχέτως αν επικοινωνούν εσωτερικά ή εξωτερικά με τους διακομιστές. Η έξυπνες πόλεις πρέπει να χρησιμοποιούν εικονικά δίκτυα και πρότυπα κρυπτογράφησης για να διασφαλίσουν το απόρρητο των χρηστών και να προστατέψουν όλες τα δεδομένα. Σκοπός της κρυπτογράφησης είναι η εμπιστευτικότητα, δηλαδή η πληροφορία που μεταφέρει θα πάει μόνο σε εξουσιοδοτημένα μέλη και όχι σε τρίτους. Η ακεραιότητα, δηλαδή η πληροφορία δεν θα μπορεί να αλλοιωθεί από κανέναν τρίτο και μη εξουσιοδοτημένο χρήστη. Επίσης, είναι η μη απάρνηση, δηλαδή ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της πληροφορίας. Τέλος, υπάρχει η πιστοποίηση των χρηστών, δηλαδή ο αποστολέας και ο παραλήπτης μπορούν να εξακριβώσουν τις ταυτότητες τους και τη γνησιότητα των πληροφοριών που μεταφέρονται και όχι να λαμβάνουν πλαστές πληροφορίες. Έτσι, μέσα στα ιδιωτικά δίκτυα (VPN) μπορούν να ληφθούν σημαντικές γραμμές άμυνας μέσα από την κρυπτογράφηση και τις μεθόδους που χρησιμοποιούνται και να προστατευτούν τα προσωπικά δεδομένα των χρηστών από πιθανές επιθέσεις. Η κρυπτογράφηση είναι η μετατροπή ηλεκτρονικών δεδομένων σε κρυπτογραφημένο κείμενο που δεν μπορεί να γίνει εύκολα κατανοητό από κανέναν εκτός από εξουσιοδοτημένα μέλη. Τα ευαίσθητα δεδομένα πρέπει να προστατεύονται με (κατά προτίμηση ισχυρή) κρυπτογράφηση κατά τη μεταφορά. Η κρυπτογράφηση εγγυάται την εμπιστευτικότητα των δεδομένων καθώς προστατεύει από μη εξουσιοδοτημένη πρόσβαση (π.χ. υποκλοπές).

3.4.8 ΕΦΑΡΜΟΓΕΣ ISO ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Η τεχνολογία καθώς εξελίσσεται μέσα από τις καινοτόμες εφαρμογές, IoT, τα δίκτυα Παρόχων και τη τεχνητή νοημοσύνη έχουν δώσει λύσεις και βελτιώσεις στη ποιότητα των πολιτών καθώς προλαμβάνουν τις επιθέσεις και τους κινδύνους. Τα πρότυπα που δημιουργούνται και η συνεχής αναβάθμιση τους είναι ο οδηγός για τους τρόπους που μπορούν να μειώσουν τις ευπάθειες και να προφυλάξουν το προσωπικό απόρρητο. Οι οδηγίες που υπάρχουν για τις έξυπνες πόλεις αλλά και η καθοδήγηση από όλα τα εμπλεκόμενα μέρη στο οικοσύστημα της έξυπνης πόλης έχουν να κάνουν και με τη πολυπλοκότητα των προβλημάτων που έχουν να αντιμετωπίσουν και τις τεχνικές που έχουν να αναπτύξουν για να αμυνθούν καθώς τα προβλήματα έχουν διαφορετικό χαρακτήρα και δεν αποτελούν πάντα απειλή για το σύστημα. Υπάρχουν πολλά πρότυπα για την ασφάλεια και την ιδιωτικότητα και σίγουρα δεν είναι τα ίδια για κάθε περίπτωση καθώς εξετάζονται αρκετά στοιχεία για τη τελική επιλογή τους. Το ISO/IEC TS 27570 παρέχει οδηγίες για το πώς να επωφεληθεί η έξυπνη πόλη από τα διαθέσιμα πρότυπα με ποιος είναι ο καλύτερος τρόπος για να εφαρμοστεί. Θα ανοίξει το δρόμο για μελλοντικά πρότυπα απορρήτου για έξυπνες πόλεις, συμπεριλαμβανομένων εκείνων για την επικοινωνία, τα σχέδια διαχείρισης απορρήτου και τη χάραξη πολιτικής, καθώς και τη διαχείριση συναίνεσης. Η τεχνική προδιαγραφή αναπτύχθηκε από την υποεπιτροπή SC 27 , Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής , της μεικτής τεχνικής επιτροπής ISO/IEC JTC 1 , του κλάδου τεχνολογίας πληροφοριών του ISO και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC). Μία κακόβουλη επίθεση μπορεί να αντιμετωπιστεί με τη χρήση καλών πρακτικών με τη βοήθεια εικονικών ιδιωτικών δικτύων (VPN) και να σταματήσει τις υποκλοπές με των δεδομένων με τη χρήση κρυπτογράφησης και μηχανισμούς αποτροπής και ανίχνευσης. Η υποκλοπές μπορεί να είναι είτε φυσικά αντικείμενα (μέσω αισθητήρων και υπολογιστών) είτε από υπηρεσίες που θα μεταφέρουν προσωπικές πληροφορίες. Η συνεχής παρακολούθηση και η τήρηση των μέτρων μπορούν να σταματήσουν τις υποκλοπές ή τις πιθανές επιθέσεις και σε συνδυασμό με ψηφιακά μέτρα ασφαλείας να δημιουργήσουν τείχη προστασίας ικανά να αμυνθούν διασφαλίζοντας την έρρυθμη λειτουργία των συστημάτων που βασίζονται σε πολιτικές ασφαλείας πληροφοριών. Τα μέτρα αντιμετώπισης της προστασίας είναι ο διαρκής έλεγχος, επιτήρηση όλων των

κρίσιμων μονάδων, οι εφαρμογές πολιτικής ασφαλείας και η συνεχής παρακολούθηση των δικτύων για τυχόν απότομες αλλαγές.

Το απόρρητο και η ασφάλεια αντιμετωπίζονται σωστά από τις έξυπνες πόλεις μέσα από τις προκλήσεις που διαχειρίζονται οι υπηρεσίες στο σύνολο τους και έχουν ως στόχο να συμβάλλουν στην ανάπτυξη προτύπων. Πιο συγκεκριμένα, υπάρχουν ομάδες που αποτελούνται από εμπειρογνώμονες διαφορετικών πεδίων και αποτελούν τις ομάδες προτύπων (TC). Αυτές οι ομάδες μπορεί να είναι από τη βιομηχανία, διάφοροι φορείς και θεσμοί μίας πόλης. Κάθε TC ασχολείται με διαφορετικό θέμα, όπως διαχείριση ενέργειας, ποιότητα νερού ή έξυπνα συστήματα μεταφορών. Τ πρότυπα ISO δίνουν στις έξυπνες πόλεις ένα ρυθμιστικό και κανονιστικό πλαίσιο για το πως θα λειτουργούν, ποιες παραμέτρους πρέπει να πάρουν για την ασφάλεια και το απόρρητο και πως θα ενσωματωθούν στις υπόλοιπες λειτουργίες χωρίς να δημιουργηθούν προβλήματα. Για παράδειγμα, υπάρχει το ISO 37101, το οποίο ρυθμίζει τις απαιτήσεις για τη βιώσιμη ανάπτυξη σε μία έξυπνη πόλη και εφαρμόζει στρατηγικές για να επιτευχθούν οι στόχοι καθώς και τους τρόπους που θα αντιμετωπιστούν όλα τα κοινωνικά, οικονομικά και περιβαλλοντολογικά ζητήματα. Το ISO 37101 προσπαθεί ουσιαστικά μέσα από μία σειρά προτύπων (ISO 37105, ISO37120 κτλ) να αναβαθμίσει τη ποιότητα ζωής των ανθρώπων μέσα από βιώσιμες και έξυπνες πόλεις.

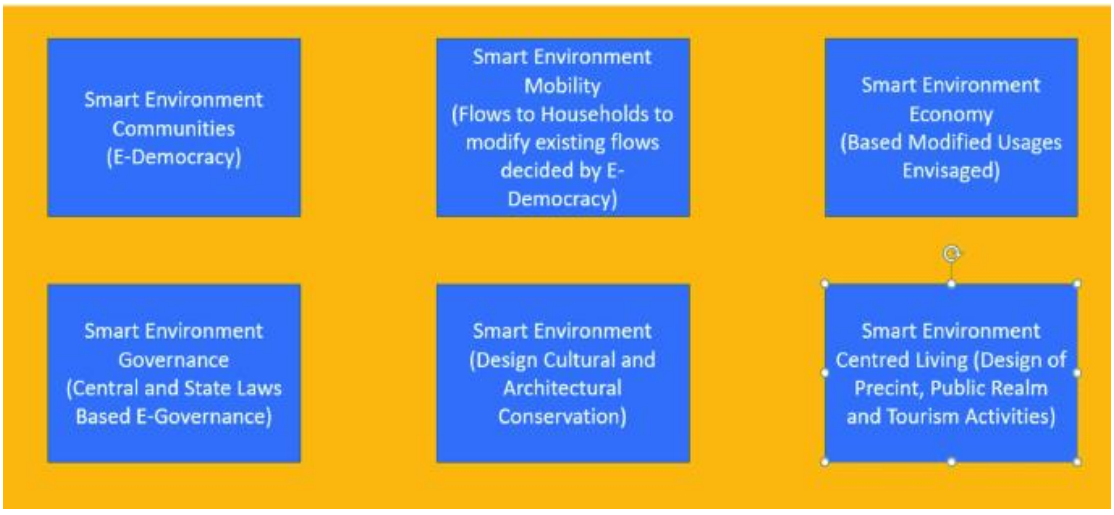
Ένα άλλο παράδειγμα μέσα στην έξυπνη πόλη είναι τα πρότυπα που έχουν γίνει σε θέματα γύρω από την ενέργεια. Η κάλυψη των αναγκών μίας έξυπνης πόλης σε σχέση με τον πληθυσμό μπορεί σε ορισμένες περιπτώσεις να είναι ένα σοβαρό πρόβλημα καθώς αν δεν σχεδιαστούν σωστά οι στρατηγικές που θα αναλάβουν να λύσουν αυτό το πρόβλημα δεν θα μπορεί μία έξυπνη πόλη να προχωρήσει. Ο υπολογισμός της ενεργειακής απόδοσης, η εξοικονόμηση ενέργειας βάσει δεικτών μέτρησης και οι ανάγκες από επιχειρήσεις και νοικοκυριά είναι μερικοί από τους παράγοντες που επηρεάζουν σημαντικά στη κατανάλωση της ενέργειας αλλά και στο τρόπο που θα διατεθεί. Υπάρχουν πολλά πρότυπα ISO που είναι αφιερωμένα σε λύσεις ανανεώσιμων πηγών ενέργειας, συμπεριλαμβανομένων εκείνων για οικιακή θέρμανση, όπως η σειρά ISO 9459 για ηλιακή ενέργεια σε συστήματα θέρμανσης νερού και η σειρά ISO 17225 για στερεά βιοκαύσιμα.

Ένα άλλο σημαντικό κομμάτι της έξυπνης πόλης είναι οι μεταφορές. Η μετακίνηση των ανθρώπων με ασφάλεια στους δρόμους είναι προτεραιότητα για κάθε έξυπνη πόλη. Τα πρότυπα ISO έχουν σημαντικό ρόλο στην ανάπτυξη νέων τεχνολογιών για καθαρές και αποτελεσματικές οδικές μεταφορές και διασφαλίζουν την καλύτερη δυνατή χρήση των δικτύων. Για παράδειγμα, το ISO 39001 αφορά τα συστήματα διαχείρισης οδικής ασφάλειας (RTS) και έχει αρκετές απαιτήσεις για τη σωστή και αποτελεσματική χρήση στους οδηγούς, δρόμους, μετακινήσεις και την οδική κυκλοφορία προσπαθώντας να μειώσει τα τροχαία ατυχήματα. Το ISO 39002, αφορά στην ασφάλεια οδικής κυκλοφορίας εφαρμόζοντας καλές πρακτικές για την αποτελεσματική διαχείριση και μεταφορά με ασφάλεια στους δρόμους προστατεύοντας τους ανθρώπους ανά πάσα στιγμή.

Στη συνέχεια της έρευνας μπορεί κανείς να δει τα πρότυπα που υπάρχουν σχετικά με τη διαχείριση του νερού από μία έξυπνη πόλη και τις ανάγκες που υπάρχουν. Τα πρότυπα ISO καλύπτουν σχεδόν όλες τις κατηγορίες για τη σωστή και καλή πρακτική της διαχείρισης των υδάτων. Το ISO 46001, έχει ως στόχο να βοηθήσει στη καλύτερη και πιο αποτελεσματική πρακτική για την αξιολόγηση και λογιστική παρακολούθηση του νερού καθώς και τον εντοπισμό νέων μέτρων για τη βελτιστοποίηση της χρήσης του νερού σε μία έξυπνη πόλη. Το ISO 24150, αναφέρεται κυρίως στις υπηρεσίες πόσιμου νερού και τα επίπεδα ποιότητας που πρέπει να επιτυγχάνονται από τις έξυπνες πόλεις καθώς αφορά ένα σημαντικό αγαθό που χρειάζεται για την επιβίβση του ανθρώπου. Επίσης, ένα σημαντικό κομμάτι μίας έξυπνης πόλης είναι η τεχνολογία. Η συνδεσιμότητα που υπάρχει ανάμεσα στις έξυπνες συσκευές που συμμετέχουν σε αυτό το οικοσύστημα, την ασφάλεια, το ιδιωτικό απόρρητο, τις απειλές, τις παραβιάσεις και τους κινδύνους από πιθανές ευπάθειες. Υπάρχουν πλέον πρότυπα όπως ISO 27001 και ISO 27002 που αφορούν σε συστήματα διαχείρισης ασφαλείας και πληροφοριών και βοηθούν τις έξυπνες πόλεις να αντιμετωπίσουν ζητήματα ασφαλείας και απορρήτου. Επίσης, το ISO 38500 αφορά την ηλεκτρονική διακυβέρνηση της τεχνολογίας και της πληροφορικής και παρέχει ένα πλαίσιο για την αποτελεσματική, αποδοτική και αποδεκτή χρήση της πληροφορικής εντός της έξυπνης πόλης. Τέλος, το ISO 27550 αφορά τις τεχνικές ασφαλείας και της ιδιωτικού απορρήτου και αφορά διαδικασίες μέσα στα συστήματα αυξάνοντας τα επίπεδα ασφαλείας μέσα στις έξυπνες πόλεις από πιθανές κακόβουλες επιθέσεις. Η ασφάλεια και η ανθεκτικότητα των υποδομών είναι σημαντική καθώς οι κίνδυνοι διαρκώς

αυξάνονται και πρέπει σε κάθε περίπτωση να υπάρχει ένα ολοκληρωμένο σχέδιο για ειδικές καταστάσεις ακόμη και καταστροφές των υποδομών σε μία έξυπνη πόλη. Το ISO έχει μία σειρά από πρότυπα που έχουν σχεδιαστεί και εφαρμοστεί για αυτό το σκοπό, δηλαδή να είναι προετοιμασμένα για τις χειρότερες συνθήκες. Το ISO 22300 αφορά τόσο για τη φυσική όσο και για την εικονική ασφάλεια και ανθεκτικότητα των υποδομών και συστημάτων και προωθείται διαρκώς καθώς περιλαμβάνει μία σειρά από επαρκή μέτρα που διασφαλίζουν κρίσιμες λειτουργίες. Το ISO 22301 έχει δημιουργηθεί για να υποστηρίξει τη βιωσιμότητα και τη παραγωγικότητα μίας έξυπνης πόλης σε εξαιρετικά δύσκολες συνθήκες.

Τέλος, υπάρχουν μία σειρά από πρότυπα που αφορούν τις έξυπνες υποδομές και έξυπνα κτήρια που προσπαθούν να αλλάξουν τη βιομηχανία και τους υπόλοιπους κλάδους καθώς δημιουργούνται ειδικές συμφωνίες και κανόνες ώστε να συμμορφώνονται με τις αρχικές οδηγίες και να ακολουθούν τις προδιαγραφές. Αυτά τα πρότυπα περιλαμβάνουν όλα τα είδη οικοδομικών υλικών, τον αποτελεσματικό σχεδιασμό, τις διασυνδέσεις, τηλεπικοινωνιακές υπηρεσίες, ψηφιακά εργαλεία, την ενεργειακή απόδοση των κτηρίων, μεθόδους δοκιμών υλικών για ανθεκτικότητα και ποιότητα και τέλος στο τρόπο κατασκευής. Το ISO 37151 που συμπεριλαμβάνει όλα τα παραπάνω και αποτελεί οδηγός για τις έξυπνες πόλεις είναι η αφετηρία για τις μελλοντικές αλλαγές που θα έρθουν καθώς θα έχουν δημιουργηθεί οι βάσεις. Η έξυπνη πόλη έχει ως στόχο να αναπτύξει τις υποδομές και να αναβαθμίσει τις υφιστάμενες υπηρεσίες και συστήματα με τις τεχνικές που ορίζονται από το ISO 37152 και τα μέτρα που προτείνει για να αποδώσουν οι διεργασίες σωστά οι λύσεις.



Εικόνα 8: Smart Environment

ΚΕΦΑΛΑΙΟ 4: ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Οι έξυπνες πόλεις αποτελούν ένα σημαντικό τεχνολογικό επίτευγμα των ανθρώπων καθώς αξιοποιούν τις δυνατότητες της τεχνολογίας μέσα από καινοτόμες ιδέες που βελτιώνουν τη καθημερινότητα τους με πολλαπλά οφέλη και σίγουρα με πολλές προκλήσεις. Οι πολίτες σταδιακά περνούν στο επόμενο βήμα της τεχνολογίας και χρησιμοποιούν όλες τις συσκευές που συνδέονται στο διαδίκτυο ώστε να βελτιώσουν το τρόπο ζωής και τις ανέσεις που μπορούν να προκύψουν. Για να μπορέσει όμως να αναπτυχθεί μία πόλη σε έξυπνη και να επωφεληθούν οι πολίτες τις δυνατότητες και τις παρεχόμενες υπηρεσίες χρειάζεται να αναπτυχθούν οι υποδομές και να αλλάξουν ουσιαστικά όλα τα διασυνδεδεμένα συστήματα παρακολούθησης, ελέγχου και αυτοματισμού (Angelidou, 2014). Για παράδειγμα, μία δυνατότητα σε μία έξυπνη πόλη όπως η μεταφορά με ένα δημόσιο ή και ιδιωτικό όχημα χρειάζεται ορισμένες πληροφορίες ώστε να ανταποκριθεί στις απαιτήσεις του πολίτη, δηλαδή από το μέσο χρόνο άφιξης, τη κυκλοφορία στους δρόμους, ενημερώσεις στο GPS, το καιρό και άλλες πιθανές μεταβλητές που μπορούν να επηρεάσουν τη μετακίνηση. Επομένως, δημιουργήθηκαν συστήματα που βοηθούν τον πολίτη ενημερώνοντας τον με όσες πληροφορίες χρειάζεται στους δρόμους μέσα από ένα τεράστιο σύστημα συσκευών που ανατροφοδοτούν με χρήσιμες πληροφορίες για κάθε πιθανή αλλαγή μέσα σε ελάχιστα δευτερόλεπτα (Angelidou, 2017). Σίγουρα, τα ανοιχτά δεδομένα μέσα στις έξυπνες πόλεις μπορούν να επηρεάσουν και αρνητικά τις καταστάσεις καθώς κρύβονται κίνδυνοι που έχουν σαν στόχο να παραβιάσουν τα προσωπικά δεδομένα των πολιτών, να προκαλέσουν προβλήματα στην ασφάλεια και την ιδιωτικότητα των πολιτών καθώς περιλαμβάνονται πληροφορίες που ενδέχεται να χρησιμοποιηθούν αρνητικά για τους πολίτες.

Η πόλη του Άμστερνταμ είναι από τις πρώτες στην Ευρώπη (2008) που ακολούθησαν μία στρατηγική ανάπτυξης γύρω από τις έξυπνες πόλεις με κύριο σκοπό την δημιουργία ολοκληρωμένων υπηρεσιών για τους πολίτες. Το Άμστερνταμ ανέπτυξε μία κουλτούρα γύρω από τις έξυπνες πόλεις και αξιοποίησε κάθε δυνατό σημείο και μέσο από όλους τους φορείς (Κράτος, επιχειρήσεις, πανεπιστήμια και τους πολίτες) ώστε να δημιουργήσει τις υπηρεσίες. Μέσα από τη καινοτομία και τη τεχνολογία οι υπηρεσίες βρήκαν γρήγορα τα επιθυμητά για τον άνθρωπο στοιχεία και έδωσαν νέες προοπτικές σε όλους τους τομείς (έξυπνοι άνθρωποι, έξυπνη οικονομία, έξυπνο περιβάλλον και έξυπνη διαβίωση). Τα οφέλη λοιπόν για τους πολίτες είναι πολλά και

σίγουρα αποτελεσματικά καθώς βελτιώνεται διαρκώς ο τρόπος ζωής τους μέσα στη πόλη έχοντας περισσότερα πράγματα να κάνουν (Capra, 2016). Η πλατφόρμα που υπάρχει για το ευρύ κοινό (Smart City - Amsterdam) είναι ο στρατηγικός πυλώνας της πόλης καθώς από εκεί μοιράζεται ένα μεγάλο σύνολο πληροφοριών και οργανώνονται οι υπηρεσίες καθώς ο κάθε ενδιαφερόμενος μπορεί να αντλήσει πληροφορίες για το τρόπο λειτουργίας της πόλης αλλά και να καταλάβει σε ένα βαθμό τις δυνατότητες που έχει διαθέσιμες σε υποδομές, τεχνολογία, ενέργεια, έξυπνη πόλη, έξυπνη διακυβέρνηση, έξυπνη διαβίωση, πολίτες κτλ. Φυσικά, η εφαρμογή τέτοιων λύσεων απαιτεί ισχυρές υποδομές και καινοτόμες τεχνολογίες για να μπορέσουν να αναπτυχθούν νέες ψηφιακές λύσεις και να βοηθήσουν στο μετασχηματισμό ώστε να ολοκληρωθούν και να λειτουργήσουν τέτοια έξυπνα οικοσυστήματα (Amsterdam Smart City, 2023).

Η τεχνολογία από μόνη της δεν επαρκεί για να αναπτυχθεί μία υπηρεσία. Στη προκειμένη περίπτωση υπάρχει διαρκής συνεργασία και μάλιστα το Internet of Things (IoT) προχώρησε δυναμικά καθώς δημιουργήθηκε ένα δίκτυο iBeacon σε μία έκταση περίπου 4 χιλιομέτρων με τεχνολογία δικτύου LPWA, που ονομάζεται LoRaWan (μηχανή προς μηχανή) για τη μετάδοση μικρών πακέτων χρησιμοποιώντας ραδιοσήματα χαμηλής συχνότητας που από εκεί αποστέλλονται σε cloud τα δεδομένα και οι χρήστες έχουν τη δυνατότητα να αντλήσουν χρήσιμες πληροφορίες για τις εφαρμογές της έξυπνης πόλης (Gharaibeh et al.,2017). Αυτό το οικοσύστημα της πόλης με τις δυνατότητες που έχει και τις πρωτοβουλίες που παίρνουν οι άνθρωποι ώστε να πάνε στο επόμενο βήμα έχει δώσει αυτά τα χρόνια στη πόλη την ευκαιρία να μάθει να χειρίζεται και τη τεχνολογία καλύτερα. Η άμεση εμπλοκή των ανθρώπων κρίνεται αναγκαία καθώς ο ρόλος τους επιβάλλεται να είναι πιο ενεργός και να συμμετέχει σε όλους τους τομείς.

Η αξία λοιπόν της τεχνολογίας έχει να κάνει και με τις δυνατότητες που μπορεί να πάρει ο πολίτης μέσα από τους στόχους που έχουν τεθεί. Η έξυπνη πόλη του Άμστερνταμ είχε θέσει ως πρώτο στόχο το 2010 τη μείωση των εκπομπών CO2 περίπου 45% κάτω και προσανατολιζόταν για τη βιωσιμότητα της πόλης. Η προώθηση νέων μοντέλων στρατηγικής για τη στέγαση, μεταφορά, ανοιχτά δεδομένα και εργασία έδωσαν εκπληκτικά αποτελέσματα άμεσα καθώς οι άνθρωποι προσπάθησαν να ανταποκριθούν και να αλλάξουν το τρόπο σκέψης τους για το γενικότερο καλό της πόλης και να ρυθμίσουν τις απαιτήσεις που είχαν και οι ίδιοι. . Η

εργασία στο κόσμο της Τεχνολογίας και των Επικοινωνιών (ΤΠΕ) είχε εξαρχής μεγάλη κινητικότητα καθώς εντάχθηκαν νέες έννοιες και λειτουργίες που απαιτούσε και νέους χρήστες που θα προχωρούσαν τις διεργασίες (Jameson et al., 2019) . Μέσα στην έξυπνη πόλη του Άμστερνταμ έχουν γίνει πολλές ρυθμίσεις σε όλες τις πιθανές λειτουργίες μίας πόλης για να εξοικονομηθεί ενέργεια και να μειωθούν οι πόροι που χρειάζονται για να καλύψουν αυτές τις ανάγκες και να είναι σίγουρα πιο φιλική πόλη στο περιβάλλον. Μία ακόμη σημαντική διεργασία είναι τα ανοιχτά δεδομένα που αναφέρονται στην έξυπνη διακυβέρνηση της πόλης και βοηθούν τους πολίτες ενημερώνοντας τους σωστά και γρήγορα παρέχοντας δημόσιες πληροφορίες μέσα από ένα σύνολο λειτουργιών στις εφαρμογές ώστε να ανταποκρίνονται οι υπηρεσίες στους ανθρώπους και φυσικά να μπορούν και οι ίδιοι μέσα από αυτή την αλληλεπίδραση να δίνουν χρήσιμα δεδομένα ώστε να εξάγονται χρήσιμες πληροφορίες για τους υπόλοιπους.

Στη συνέχεια λοιπόν της παρούσας διατριβής θα γίνει η προσπάθεια για να καταγραφούν τα περισσότερα εμπλεκόμενα μέρη της προστασίας και της ιδιωτικότητας των πολιτών σε σχέση με την έξυπνη πόλη και ποια μέτρα ασφαλείας λαμβάνονται για να αμυνθούν στις πιθανές και κακόβουλες επιθέσεις που έχουν ως στόχο να επηρεάσουν αρνητικά όλη την έξυπνη πόλη και κατ' επέκταση τους πολίτες που ζουν και αλληλεπιδρούν (Rawat & Ghafoor, 2018). Η ασφάλεια και το ιδιωτικό απόρρητο των πολιτών πρέπει και οφείλει η έξυπνη πόλη να το έχει ψηλά στην ατζέντα της καθώς αν κλονιστεί η εμπιστοσύνη των πολιτών προς την έξυπνη πόλη δεν θα μπορεί να υπάρχει συνέχεια και ανάπτυξη σε αυτό το οικοσύστημα καθώς δεν θα χρησιμοποιούνται οι υπηρεσίες και θα μένουν ανεκμετάλλευτες οι δυνατότητες που αναπτύχθηκαν. Οι πολίτες είναι το βασικότερο στοιχείο για να μπορέσει μία έξυπνη πόλη να λειτουργήσει και να αναπτύξει νέες και καινοτόμες ιδέες που θα δώσουν πολλά οφέλη προς κάθε κατεύθυνση και φυσικά να δημιουργηθούν νέες υπηρεσίες.

4.1 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΞΥΠΝΗ ΠΟΛΗ

Η πόλη του Άμστερνταμ έχει αναπτύξει τις τεχνολογίες που χρησιμοποιεί καθώς οι απειλές για την ασφάλεια και το απόρρητο έχουν αυξηθεί σημαντικά. Η βασικοί πυλώνες για την εφαρμογή και τη προστασία των πολιτών είναι σε θέματα που έχουν

να κάνουν με την αυθεντικότητα και την εμπιστευτικότητα, δηλαδή ο έλεγχος που γίνεται και η επαλήθευση της ταυτότητας ενός χρήστη που απαιτείται για να εισέλθει μέσα στο οικοσύστημα και να μπορέσει να χρησιμοποιήσει όλες τις δυνατότητες, να αλληλεπιδράσει με τις συσκευές IoT και να πάρει πληροφορίες μέσα από τα ανοιχτά δεδομένα που διαμοιράζονται ελεύθερα. Το κλειδί της υπόθεσης είναι η επαλήθευση της ταυτότητας του χρήστη σε πραγματικό χρόνο και ακριβή. Η ανάπτυξη προηγμένων τεχνολογιών έδωσε μία υπεροχή στην έξυπνη πόλη καθώς αναπτύχθηκαν σημαντικά όλες οι επιμέρους υποδομές (Ismagilova et al., 2013). Ο στόχος της εμπιστευτικότητας είναι η αποτροπή πληροφοριών από παθητικές επιθέσεις ή την έκθεση σε επιβλαβείς πηγές από λάθος χρήση. Οι εισβολείς προσπαθούν να πάρουν πληροφορίες από δυνατό σημείο και να κωδικοποιήσουν τα δεδομένα προς όφελος τους. Η προστασία λοιπόν του απορρήτου έχει να κάνει και με το ρυθμό μετάδοσης δεδομένων μεταξύ των κόμβων και τις τεχνολογίες κρυπτογράφησης που χρησιμοποιούν τα συστήματα.

Η διαφάνεια και η αξιοπιστία της έξυπνης πόλης έχουν να κάνουν και με το πλαίσιο της ασφάλειας και προστασίας των προσωπικών δεδομένων των χρηστών. Στη συνέχεια, υπάρχει η διαθεσιμότητα και η ακεραιότητα που στοχεύουν στην αμεσότητα και την αποτελεσματικότητα των υπηρεσιών την ώρα της επίθεσης από εισβολείς καθώς μέσα στο έξυπνο σύστημα υπάρχουν πολλές συσκευές και θα πρέπει να αξιολογηθούν όλες και να ανιχνευθούν τυχόν ύποπτες καταστάσεις που έχουν αλλάξει (Caragliu et al., 2011). Σκοπός του συστήματος είναι να λειτουργούν οι μηχανισμοί προστασίας σωστά και να μπορούν να αντιμετωπίσουν κάθε επίθεση ανεξαρτήτου κλίμακας καθώς τα δεδομένα ανταλλάσσονται διαρκώς καθώς μεταφέρονται από συσκευές σε συσκευές και προφανώς αν κατά τη διαδικασία μετάδοσης δεν προστατεύονται σωστά εύκολα μπορούν να παραβιαστούν. Οι συσκευές IoT είναι συνήθως οι από τις πρώτες που θα δεχτούν κάποια επίθεση και για αυτό το λόγο θα πρέπει να δίνεται ιδιαίτερη προσοχή στο σχεδιασμό και την αρχιτεκτονική που θα φιλοξενήσεις τις περιφερειακές συσκευές μέσα στο οικοσύστημα της έξυπνης πόλης και θα αλληλεπιδράσει με τις υπόλοιπες υποδομές. Η ανίχνευση των απειλών και η πρόβλεψη πιθανών ευπαθειών θα μπορούσε να δώσει μία επιπλέον ασφάλεια στα υποστηρικτικά συστήματα και να περιορίσει τις επιθέσεις. Δεν μπορεί σε καμία περίπτωση ένα σύστημα να θεωρηθεί ότι δεν κινδυνεύει ακόμα και αν λειτουργούν όλα εξαιρετικά καθώς οι συνθήκες λειτουργίας

αλλάζουν διαρκώς και προκύπτουν διαφορετικές επιθέσεις. Το παραδοσιακό σύστημα ανίχνευσης εισβολής IDS χρησιμοποιείται για την ανίχνευση κακής χρήσης, την ανίχνευση ανωμαλιών και την ανίχνευση βάσει προδιαγραφών των συστημάτων της έξυπνης πόλης. Λόγω της πρόβλεψης και της γνώσης που υπάρχουν μέσα στα δίκτυα χάρις την τεχνητή νοημοσύνη που έχει αναπτυχθεί μπορούν να απομακρυνθούν απειλές εκ των προτέρων και να εντοπιστούν σε όλη τη διαδικασία. Έτσι, τα συστήματα ανίχνευσης IPS βοηθούν για τη κατανόηση και επίγνωση της κατάστασης της ασφάλειας και προβλέπουν αυτόματα τις διάφορε επιθέσεις μέσα στις έξυπνες εφαρμογές.

4.2 ΑΠΕΙΛΕΣ ΑΠΟΡΡΗΤΟΥ ΜΕΣΩ ΤΗΣ ΚΟΙΝΗΣ ΧΡΗΣΗΣ ΑΝΟΙΧΤΩΝ ΔΕΔΟΜΕΝΩΝ - ΑΝΤΛΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

Τα δεδομένα που παράγονται μέσα στις έξυπνες πόλεις είναι πολλά και φιλτράρονται διαρκώς με σκοπό να διασφαλιστεί το προσωπικό απόρρητο των ανθρώπων με τεχνικές και μεθόδους που επιτρέπουν τη μεγάλη διασύνδεση των πολιτών με τις υπηρεσίες της πόλης αλλά και να επικοινωνούν και με τους πολίτες. Η αλληλεπίδραση των πολιτών με εφαρμογές και υπηρεσίες είναι καθημερινή καθώς επικοινωνούν για να αποκτήσουν πρόσβαση σε πληροφορίες. Έτσι, μέσα από ένα σύνολο έξυπνων αισθητήρων και τη χρήση εφαρμογών τα δεδομένα μεταφέρονται προς κάθε κατεύθυνση και μπορεί να θέσουν σε κίνδυνο το προσωπικό απόρρητο των πολιτών. Δεδομένου ότι κάθε πολίτης έχει και διαφορετικές προτεραιότητες θα πρέπει να αντιληφτεί κανείς και τα πιθανά κενά που υπάρχουν καθώς δεν λαμβάνονται όλα τα αναγκαία μέτρα ασφαλείας. Καθώς εξελίσσεται η τεχνολογία και παρότι προκύπτουν πολλές διαφορές στα πρότυπα απορρήτου μεταξύ ιδιωτικού και δημοσίου οι πιθανοί κίνδυνοι παραμένουν ίδιοι. Μία επιχείρηση για παράδειγμα δίνει ένα σημαντικό ποσοστό των κεφαλαίων της για τη προστασία του ιδιωτικού απορρήτου καθώς υπάρχει ο κίνδυνος να αμαυρωθεί το κύρος και η αξιοπιστία της και να μην την επιλέγει στη συνέχεια κανένας (Basi, 2016).

Ένας δημόσιος φορέας διαχειρίζεται κρίσιμες υπηρεσίες για τους πολίτες και οφείλουν να προστατέψουν κάθε πληροφορία. Ο συνδυασμός είναι ακόμη πιο σύνθετος (δημόσιος και ιδιωτικός) καθώς πρέπει να παρθούν επιπλέον μέτρα για την ασφάλεια και το ιδιωτικό απόρρητο μέσα στην έξυπνη πόλη. Για παράδειγμα, σε θέματα που σχετίζονται με την υγεία μπορεί την φροντίδα και τη περίθαλψη να την

έχει ο δημόσιος φορέας και την διαχείριση ή μέρος των εργασιών μία ιδιωτική επιχείρηση και για να μπορέσουν να συνεργαστούν αποτελεσματικά να χρειαστεί να κοινοποιηθούν σε τρίτα μέρη πληροφορίες των πολιτών (φάρμακα, πρόγραμμα συναντήσεων σε ιατρείο, διεύθυνση διαμονής κτλ) και να μελετηθούν - αναλυθούν όλες αυτές οι πληροφορίες. Ο ανασυνδυασμός αυτός μπορεί να οδηγήσει σε τεχνικές ενοποίησης και να επιτρέψει στη κοινοποίηση ευαίσθητων πληροφοριών. Σε μία έξυπνη πόλη οι συνδυασμοί δεδομένων μπορεί να είναι πολλοί και να θέσουν σε κίνδυνο το ιδιωτικό απόρρητο αν όλοι οι εμπλεκόμενοι δεν τηρούν μέτρα ασφαλείας. Η αποκάλυψη ευαίσθητων πληροφοριών μπορεί να φέρει επιπλέον προβλήματα και να αποδυναμώσει την εμπιστοσύνη των πολιτών.

Ωστόσο, οι τρέχουσες πρακτικές συνδυασμού δεδομένων έχουν τις δικές τους προκλήσεις και προσπαθούν να περιορίσουν τα κενά όταν κοινοποιούν πληροφορίες σε τρίτα μέρη. Ακόμη, ένα σημαντικό στοιχείο είναι ότι αν υπήρχε ένα σύστημα ταυτοποίησης τότε θα βοηθούσε και στο ιδιωτικό απόρρητο να μην δίνουν πληροφορίες περισσότερες από όσες κρίνονταν απαραίτητες καθώς τα στοιχεία θα πρέπει να γενικεύονται και όχι να προσωποποιούνται με αποτέλεσμα να φανερώνουν προσωπικές πληροφορίες (Yang et al., 2019). Οι έξυπνες πόλεις δεν μπορούν να βασιστούν σε χαμηλά πρωτόκολλα ασφαλείας και παλιούς παραδοσιακούς τρόπους αντιμετώπισης σύνθετων ζητημάτων καθώς οι τεχνολογία έχει προχωρήσει σημαντικά και οι επιθέσεις πλέον είναι σε μεγάλη έκταση ταυτόχρονες και πιο σύνθετες και απαιτείται περισσότερη ασφάλεια για να αντιμετωπιστούν. Οι πιθανές ευπάθειες που μπορεί να υπάρχουν μέσα στις υποδομές μπορεί να μην έχουν αποκαλυφθεί και να θεωρείται πως δεν υπάρχουν. Το ιδιωτικό απόρρητο και η προστασία των δεδομένων θα πρέπει να αντιμετωπίζονται ανεξάρτητα και να μην θεωρείται ότι καλύπτοντας το ένα θέμα έχει καλυφθεί και το άλλο για αυτό και πρέπει με τεχνικές συνάθροισης και γενίκευσης με K- ανωνυμία να προστατεύονται σε υψηλά επίπεδα τα δεδομένα (Dwork, 2006).

Έτσι, σε κάθε χρήστη και κάθε συσκευή πρέπει να υπάρχουν μέτρα ασφαλείας και να λαμβάνονται μετρήσεις κατάλληλες ώστε να μελετώνται και να δημιουργούνται νέα σενάρια για τα επίπεδα ασφαλείας μέσα από τη χρήση και φυσικά από τη διαφορετικότητα των λειτουργιών. Η αξιοποίηση της γνώσης μπορεί να βοηθήσει στην εξαγωγή εμπιστευτικών πληροφοριών προς το συμφέρον των έξυπνων πόλεων. Τέλος, ένας ακόμη τρόπος αντιμετώπισης του ιδιωτικού απορρήτου των δεδομένων

είναι η διεξαγωγή ανάλυσης σε μειωμένο αριθμό χαρακτηριστικών, δηλαδή να χρειάζεται μία προ - επεξεργασία των δεδομένων πριν την έναρξη της ανάλυσης καθώς απαιτείται περισσότερος χρόνος για τη διαδικασία και μία σειρά εργασιών και θα χρειαστεί ένα σχετικό υποσύνολο χαρακτηριστικών για να διατηρηθούν τα δεδομένα (Matatov, Rokach, & Maimon, 2010).

4.3 ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΕΝΙΣΧΥΟΥΝ ΤΟ ΑΠΟΡΡΗΤΟ

Για να μπορέσει να αντιμετωπιστεί το πρόβλημα της ιδιωτικότητας σε μία έξυπνη πόλη πρέπει να παρθούν σοβαρά μέτρα ασφαλείας και να χαρτογραφηθεί το πρόβλημα και να εξεταστούν όλες οι ποσοτικές και ποιοτικές παράμετροι που επηρεάζουν στο θέμα. Στη πόλη του Άμστερνταμ οι άνθρωποι της πληροφορικής και της μηχανικής συνεργάστηκαν ώστε να δημιουργήσουν τα κατάλληλα μέτρα χρησιμοποιώντας μέτρα αβεβαιότητας, πληροφορίες, τυχόν λάθη και εκτιμήσεις για τα πιθανά προφίλ ενός εισβολέα που θα επιχειρήσει να επιτεθεί (Rebollo-Monedero et al., 2014). Σε περιπτώσεις αβεβαιότητα, η εντροπία που χρησιμοποιείται σαν στατιστικό εργαλείο που αξιολογεί τις πιθανότητες για πιθανές απειλές και παραβιάσεις και λειτουργεί ως βοηθητικός δείκτης για τη κατανόηση του απορρήτου. Λόγω των δυσκολιών που προκύπτουν και των τεχνικών διατήρησης της ιδιωτικής ζωής των πολιτών είναι σημαντικό να αξιοποιούνται όλα τα διαθέσιμα μοντέλα μέσα στο σύστημα καθώς μειώνεται η πιθανότητα να παραβιαστεί και οι κίνδυνοι ελαχιστοποιούνται. Για να μπορέσει η πόλη του Άμστερνταμ να διαχειριστεί αυτές τις δυσκολίες έχει κάνει ήδη μία επιπλέον κίνηση να χαρτογραφήσει τα δεδομένα και να αξιολογήσει τους κινδύνους και τις συνέπειες παραβίασης μέσα στην έξυπνη πόλη προκειμένου να διασφαλίσει το απόρρητο από επιθέσεις (Shafiq et al., 2020). Μάλιστα, για να πετύχει μεγαλύτερα ποσοστά στην ασφάλεια του απορρήτου συνεργάστηκαν αρκετοί δημόσιοι και ιδιωτικοί φορείς ώστε να πετύχουν τα επιθυμητά αποτελέσματα. Υπάρχουν πολλές προκλήσεις που αντιμετώπισαν ώστε να δημιουργηθεί η βάση δεδομένων μέσα στις υποδομές στη πόλη του Άμστερνταμ.

Οι ομάδες που συνεργάστηκαν για την ασφάλεια του απορρήτου και τις τεχνικές που εφάρμοσαν προσαρμόζοντας μεταξύ διαδραστικών και μη πλαισίων απορρήτου δημιούργησαν βάσεις δεδομένων όπου υπάρχουν σχετικές πληροφορίες που δημοσιεύει ο κάτοχος της βάσης στη πρώτη περίπτωση ενώ στη δεύτερη δεν κοινοποιούν τα δεδομένα και δεν επιτρέπεται η δημόσια πρόσβαση. Οι πάροχοι

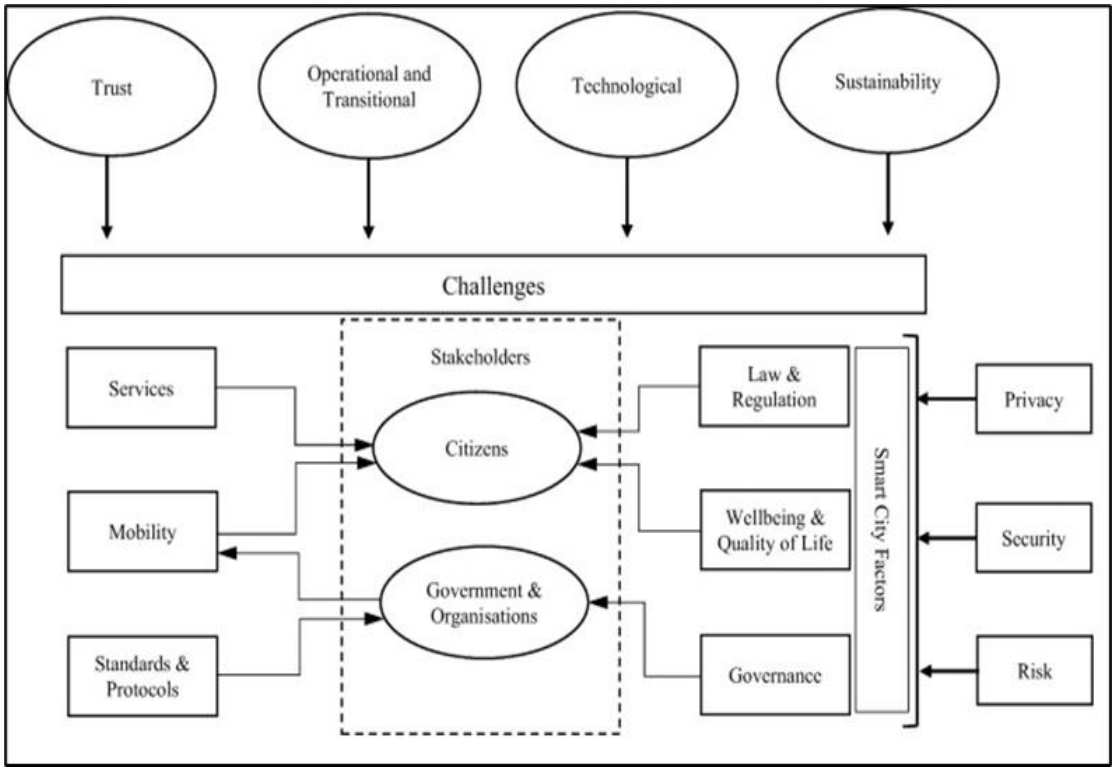
δεδομένων ως υπηρεσία (DaaS) μπορούν να χρησιμοποιούν μοντέλα mashup για να ενσωματώσουν πολλαπλούς κατόχους βάσεων δεδομένων χρησιμοποιώντας μη διαδραστικά πλαίσια. Όσον αφορά το συνολικό απόρρητο του δικτύου, τα μοντέλα απορρήτου W3 και 3D προσπαθούν να παρέχουν ένα πλαίσιο για την προστασία ολόκληρου του συστήματος. Το μοντέλο απορρήτου W3 για υπηρεσίες που βασίζονται στην τοποθεσία και επιδιώκει να προστατεύσει τρεις πτυχές του προσωπικού απορρήτου: πού, τι και ποιος (Martinez-Balleste et al., 2013). Το μοντέλο επιδιώκει να προστατεύσει ένα άτομο από την παρακολούθηση τοποθεσίας, τα συστήματα που μαθαίνουν τι κάνει ένας χρήστης και τις επεμβατικές προσπάθειες αναγνώρισης. Αυτό μπορεί να επιτευχθεί μέσω τεχνικών συσκότισης τοποθεσίας, τεχνικών ανάκτησης ιδιωτικών πληροφοριών και χρονικών ψευδωνύμων (Martinez-Balleste et al., 2013). Το τρισδιάστατο μοντέλο απορρήτου χωρίζει το απόρρητο σε τρεις διαστάσεις: ερωτηθέντες, χρήστες και ιδιοκτήτες (Martinez-Balleste et al., 2013). Έτσι, το μοντέλο είναι κατασκευασμένο ώστε το απόρρητο του ερωτώμενου να εστιάζει στην αποφυγή της αναγνώρισης του ατόμου, το απόρρητο του χρήστη εγγυάται το απόρρητο του ερωτήματος ενός χρήστη και το απόρρητο του ιδιοκτήτη επιδιώκει να προστατεύσει το απόρρητο των κατόχων μιας βάσης δεδομένων από εκείνους που κάνουν ερωτήσεις (Martinez-Balleste et al., 2013). Στη συνέχεια, οι τεχνικές λύσεις για το απόρρητο είναι αρκετές και εξίσου σημαντικές στη φάση που βρίσκονται. Έτσι, όταν χρησιμοποιούνται τεχνικές συγκέντρωσης δεδομένων στην έξυπνη πόλη μειώνεται ο απαραίτητος χρόνος για τη μεταφορά πρωτογενών δεδομένων στο σύστημα διαχείρισης.

Το επιθυμητό είναι να μπορεί να ενσωματωθεί μία τεχνική διαχείρισης δεδομένων στις έξυπνες συσκευές καθώς μέσα από τη χρήση μπορούν να παραχθούν επιπλέον δεδομένα και να βοηθήσουν στην αποτελεσματική αντιμετώπιση των ευπαθειών και τη καλύτερη λήψη αποφάσεων μιας και θα βρίσκεται ήδη μέσα στο έξυπνο δίκτυο και αποθηκεύει τις πληροφορίες. Είναι αρκετά δύσκολο και πολύπλοκο το ζήτημα του απορρήτου καθώς πρέπει να ακολουθήσει σύνθετες διαδρομές και να προφυλάξει τα δεδομένα από τους εισβολείς και να λάβει τα μέτρα προστασίας που χρειάζονται. Οι μέθοδοι που χρησιμοποιούνται μέσα στο έξυπνο δίκτυο για την αντιμετώπιση αυτών των διαδικασιών μπορεί να δώσει τη δύναμη που απαιτείται για να προφυλάξει τα δεδομένα καθώς για την υλοποίηση της ασφάλειας του απορρήτου στη πόλη του Άμστερνταμ συνεργάστηκαν πολλοί και διαφορετικοί φορείς ώστε να μην γνωρίζουν

από άκρο σε άκρο τις λειτουργίες του συστήματος και να προφυλαχθούν οι απαραίτητες ρυθμίσεις μέσα από μοντέλα ικανά να αποκρύψουν σημαντικές πληροφορίες (ταυτότητα χρήστη, τοποθεσία, δικαιώματα κτλ.) μέσα από τη κατάλληλη κρυπτογράφηση.

4.4 ΜΕΤΡΑ ΚΑΙ ΑΠΟΦΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟ ΑΜΣΤΕΡΝΤΑΜ

Όπως φαίνεται και παρακάτω στο διάγραμμα (εικόνα 8) η πόλη του Άμστερνταμ έχει λάβει τα απαραίτητα μέτρα ασφαλείας ώστε να προφυλάξει τους πολίτες κατά τη χρήση των υπηρεσιών που παρέχει σε μέσα μεταφοράς, στις ενημερώσεις που λαμβάνουν, σε υπηρεσίες μέσα σε μεγάλα εμπορικά κτήρια και στους δρόμους ώστε να καλύψουν τις πιθανές ευπάθειες και επιθέσεις που μπορούν να δεχτούν οι χρήστες. Οι λειτουργίες αυτές προφυλάσσονται μέσα στις έξυπνες υποδομές κυρίως από ιδιωτικά - απόρρητα δίκτυα που δρομολογούν με ασφάλεια τους χρήστες και περιορίζουν τις αρνητικές συνέπειες. Η τεχνολογία χρησιμοποιείται όπως φαίνεται και παρακάτω μέσα από ένα δίκτυο που επικοινωνεί άριστα στο εσωτερικό του και λαμβάνει όλες τις απαραίτητες ρυθμίσεις μέσα από πρωτόκολλα και πρότυπα ασφαλειών. Σίγουρα, οι χρήστες για να καταφέρουν να δείξουν εμπιστοσύνη στις υπηρεσίες αυτές ενημερώνονται διαρκώς και συμμορφώνονται στους νόμους όπως ορίζονται. Η έξυπνη πόλη απαιτεί ένα ασφαλές σύστημα που θα ανταποκρίνεται και παρακολουθεί διαρκώς και θα ρυθμίζει την επικοινωνία των χρηστών με τις διάφορες συσκευές μέσα στο οικοσύστημα της έξυπνης πόλης του Άμστερνταμ. Η τεχνολογία Blockchain διασφαλίζει τη μετάδοση μεγάλων δεδομένων στην έξυπνη πόλη και δημιουργεί ένα ασφαλές περιβάλλον συναλλαγών και αποτρέπει τις απάτες και τις πιθανές παραβιάσεις από τρίτους. Οι κυβερνοεπιθέσεις από την άλλη πλευρά μπορούν να επηρεάσουν συσκευές όπως IoT και να καταστρέφουν δεδομένα ή να διαρρέουν πληροφορίες απορρήτου μέχρι και τη κοινοποίηση κωδικών πρόσβασης και ταυτότητες των χρηστών.



Εικόνα 9: Τα χαρακτηριστικά της έξυπνης πόλης του Άμστερνταμ

Επίσης, ένα μεγάλο πρόβλημα που μπορεί να προκύψει μέσα στη κοινωνία είναι η υποβάθμιση τόσο σε βιοτικό αλλά και οικονομικό επίπεδο καθώς εφαρμόζονται τέτοιους μέτρα ώστε να σταματούν τις κακόβουλες επιθέσεις. Η διαρροή πληροφοριών μπορεί να οδηγήσει σε επιθέσεις spam και άλλων ειδών. Η υποδομές λοιπόν της πόλης του Άμστερνταμ βασίζονται σε συστήματα blockchain καθώς ανιχνεύονται και προβλέπονται αυτές οι επιθέσεις. Για αυτό πλέον σε ένα μεγάλο βαθμό οι υπηρεσίες που χρησιμοποιούνται απαιτούν ψηφιακά βιομετρικά στοιχεία ως επαλήθευση της ταυτότητας των χρηστών αλλά και της διασφάλισης του απορρήτου. Τα προσωπικά δεδομένα είναι σημαντικά και πρέπει να λαμβάνονται μέτρα ικανά να τα προφυλάξουν ειδικά μέσα από τις έξυπνες συσκευές που βρίσκονται μέσα στην έξυπνη πόλη.

Η ασφάλεια στην επικοινωνία, η διασύνδεση και ο διαμερισμός των πληροφοριών, η συλλογή και η ανάλυση των δεδομένων είναι μερικά από τις κύριες λειτουργίες ώστε να λειτουργεί το σύστημα. Η αξία όμως του οικοσυστήματος είναι η κρυπτογράφηση που θα ακολουθηθεί, η διαχείριση τεχνικών κρίσεων, οι εντοπισμοί αυτόματα στην ασφάλεια από ύποπτες συμπεριφορές, η ανίχνευση κακόβουλων ιών και ο έλεγχος

στο εσωτερικό των υποδομών. Υπάρχουν τεχνικές μέσα στην έξυπνη πόλη του Άμστερνταμ όπου ελέγχονται πλαστά δεδομένα, εικονικά στοιχεία και ύποπτες συμπεριφορές. Η στρατηγική που εφαρμόζεται στηρίζεται κυρίως στην πρόληψη και ανίχνευση και με τη βοήθεια προγραμματιστών εφαρμόζουν νέες καινοτομίες στο κώδικα σε όλα τα στάδια της σχεδίασης των υποδομών ακόμα και αν σταματήσει απροσδόκητα το σύστημα από μία επίθεση. Όπως φαίνεται και στο διάγραμμα οι τέσσερα βασικά χαρακτηριστικά της έξυπνης πόλης είναι η εμπιστοσύνη, το συνεχόμενο και μεταβαλλόμενο περιβάλλον, η τεχνολογία και η βιωσιμότητα. Αυτά τα χαρακτηριστικά έχουν άμεση επαφή με τις προκλήσεις που υπάρχουν μέσα στην έξυπνη πόλη και τις πιθανές δυσκολίες που υπάρχουν για να διαχειριστούν αυτά τα ζητήματα. Όπως φαίνεται και στο διάγραμμα, οι υπηρεσίες και η κινητικότητα έχουν άμεση επαφή με τους πολίτες και τα πρότυπα και πρωτόκολλα ασφάλειας με την έξυπνη πόλη και κατ' επέκταση το Κράτος και τους Θεσμούς. Οι πολίτες σε κάθε περίπτωση βρίσκονται στο επίκεντρο αυτής της εφαρμογής του οικοσυστήματος καθώς δεν θα μπορούσε να αναπτυχθεί περισσότερο αν δεν υπήρχε η συμμετοχή τους και φυσικά η εμπιστοσύνη τους στα συστήματα αυτά.

Στη συνέχεια, ένα σημαντικό στοιχείο για να μπορέσει να στηριχθεί αρχικά αυτό το σύστημα και να προχωρήσει είναι η τήρηση των νόμων και οι κανονισμοί καθώς όλοι πρέπει να συμμορφώνονται και να μην παρεμποδίζουν τις λειτουργίες καθώς ο κύριος σκοπός είναι η ασφάλεια τους. Η αναβάθμιση κι η ποιότητα ζωής των πολιτών σχετίζεται άμεσα με τις παροχές αλλά και γενικότερα με τη βιωσιμότητα της έξυπνης πόλης (οικονομία, κοινωνία και περιβάλλον) και έχει σαν στόχο να εμπλουτίσει σημαντικά όλους τους τομείς ώστε να βελτιωθεί και η ποιότητα ζωής των πολιτών. Όλα αυτά τα χαρακτηριστικά της έξυπνης πόλης υπάρχουν και συνεχίζουν να αναβαθμίζονται σε συνεργασία με τη ψηφιακή αλλαγή της Διακυβέρνησης της πόλης και των υπηρεσιών που παρέχει καθώς δίνει στους πολίτες πληροφορίες και εργαλεία για να τα αξιοποιήσουν στη καθημερινότητα τους. Η ασφάλεια και η διασφάλιση του απορρήτου των χρηστών είναι απαραίτητη και πρέπει να τηρείται καθώς υπάρχουν πολλοί κίνδυνοι και αν δεν παρθούν τα κατάλληλα μέτρα δεν θα μπορέσει καμία έξυπνη πόλη να συνεχίσει καθώς θα έχει χάσει το σημαντικό στοιχείο αυτού του οικοσυστήματος, τον άνθρωπο. Επομένως, πρέπει η έξυπνη πόλη να αυξήσει τους μηχανισμούς και τις άμυνες και να προστατέψει την ιδιωτικότητα του χρήστη και τις προσωπικές πληροφορίες που τον ακολουθούν. Η ανάπτυξη νέων τεχνολογιών είναι

μία διαρκής και συνεχής απαίτηση όλων των χρηστών καθώς όσο εξελίσσεται η τεχνολογία δεν μπορεί να μένει στάσιμη η στρατηγική άμυνας και χρειάζονται νέες πρακτικές που θα είναι σε θέση να ανταποκριθούν όλες τις κακόβουλες επιθέσεις που θα έχουν στόχο να προκαλέσουν βλάβες και ζημίες στα πληροφοριακά συστήματα και τις υποδομές της έξυπνης πόλης. Τέλος, όλο αυτό το οικοσύστημα για να μπορέσει να παραμείνει δυνατό θα πρέπει να ενοποιηθούν αυτά τα χαρακτηριστικά που το ενώνουν και να αξιοποιηθούν πλήρως όλες οι δυνατότητες καθώς το τελικό αποτέλεσμα είναι κοινό για την έξυπνη πόλη και τους πολίτες που αλληλεπιδρούν με τις εφαρμογές και υπηρεσίες.

4.5 ΚΕΝΑ ΚΑΙ ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ

Η πόλη του Άμστερνταμ στη πραγματικότητα έχει σχεδιαστεί αρκετά καλά σε σχέση με όταν ξεκίνησε πριν 13 χρόνια περίπου καθώς αξιοποίησε σωστά όλα τα τεχνολογικά και καινοτόμα αντικείμενα για να αυξήσει την ασφάλεια και να μπορέσει να σχεδιάσει σωστά όλες τις συσκευές που θα μπορούσαν να λειτουργήσουν μέσα σε αυτό το οικοσύστημα. Έξυπνες συσκευές, φορητοί υπολογιστές, αντικείμενα IoT, υπηρεσίες και εφαρμογές μπήκαν σε εφαρμογή για να μπορέσει να προχωρήσει η έξυπνη πόλη και να δώσει μία κατεύθυνση για τη συνέχεια. Έτσι, η ασφάλεια είναι προτεραιότητα καθώς ένας εισβολέας μπορεί να βρει μία ευπάθεια και να θελήσει να παρακολουθεί το σύστημα και να συλλέγει δεδομένα και θα εκθέσουν την έξυπνη πόλη και τις υποδομές της. Για παράδειγμα, αν το δίκτυο παραβιαζόταν από μία φορητή συσκευή που συμμετείχε στην ασφαλή σύνδεση και έπεφτε στα χέρια ενός εισβολέα τότε θα αποκαλυπτόταν πληροφορίες και τρωτά σημεία του δικτύου. Φυσικά, στα πλαίσια της ασφάλειας όλων όσων συμμετέχουν στις έξυπνες πόλεις πρέπει να είναι ενεργή η συμμετοχή του καθενός και να είναι προσεκτικός για τις επιλογές και τις ενημερώσεις που κάνει. Τα τελευταία χρόνια καθώς η τεχνολογία έχει φέρει τρομερές αλλαγές και προστίθενται επιπλέον συσκευές στο οικοσύστημα αυτό αυξάνονται και οι πιθανές απειλές από κακόβουλες έξυπνες εφαρμογές, λογισμικά παρακολούθησης και υπηρεσίες. Οι εισβολείς ανά διαστήματα προσπαθούν να παραπλανήσουν τους χρήστες δημιουργώντας ψεύτικα δίκτυα WI-FI ή άλλες υπηρεσίες που υποτίθεται θα έδινε η έξυπνη πόλη με σκοπό να αποσπάσουν πληροφορίες και να μολύνουν κρυφά τις συσκευές προκαλώντας προβλήματα στις διάφορες λειτουργίες και έμμεσα στην ασφάλεια και το απόρρητο. Τέτοιες ενέργειες

γίνονται από κακόβουλα λογισμικά που μπαίνουν στο σύστημα μίας έξυπνης συσκευής μέσω μη ασφαλών δικτύων ή ακόμη και χαμηλών συχνοτήτων (Bluetooth) ώστε να αποκαλυφθούν ευαίσθητες πληροφορίες. Ακόμη, και μία προσωπική ιστοσελίδα ενός χρήστη που φιλοξενεί τις προσωπικές του πληροφορίες είναι μέσον που μπορεί να χρησιμοποιηθεί αρνητικά και να χρησιμοποιηθεί το αναγνωριστικό της συσκευής ψευδώς για να προκαλέσει προβλήματα.

Ενώ τα έξυπνα κινητά συνδέουν τους πολίτες με την έξυπνη πόλη, το δίκτυο βασίζεται στην επικοινωνία μηχανής με μηχανή (M2M), η οποία αυτοματοποιεί πολλές διαδικασίες εντός της έξυπνης πόλης. Η επικοινωνία από μηχανή με μηχανή μπορεί να πραγματοποιηθεί αφού οι αισθητήρες έξυπνων αντικειμένων περάσουν μια πληροφορία ή αν λάβουν σήματα από άλλη συσκευή. Οι έξυπνες συσκευές που εμπλέκονται σε αυτή την επικοινωνία από μηχανή σε μηχανή μπορεί να θέτουν σε κίνδυνο τις έξυπνες πόλεις λόγω πιθανών προβλημάτων για την ασφάλεια, όπως φυσικές επιθέσεις, επιθέσεις ελέγχου ταυτότητας, επιθέσεις πρωτοκόλλου, απειλές στην ασφάλεια του δικτύου και παραβιάσεις απορρήτου. Οι φυσικές επιθέσεις που χρησιμοποιούν παραβιασμένη επικοινωνία M2M μπορούν να εκτελεστούν μέσω επιθέσεων που χρησιμοποιούν κακόβουλο λογισμικό για τη διάπραξη απάτης χειραγωγώντας την ακεραιότητα του υπάρχοντος λογισμικού M2M και των σχετικών δεδομένων (Ijaz et al., 2016). Τα διακριτικά ελέγχου ταυτότητας που παρέχουν πρόσβαση σε ορισμένα μηχανήματα στο έξυπνο δίκτυο μπορούν να αντικατασταθούν και να χρησιμοποιηθούν για διείσδυση στο δίκτυο. Οι απειλές στην ασφάλεια του δικτύου, όπως η πλαστοπροσωπία συσκευής και οι επιθέσεις άρνησης υπηρεσίας (DoS), μεταξύ έξυπνων συσκευών μπορούν είτε να διεισδύσουν είτε να διαταράξουν ένα έξυπνο δίκτυο. Οι επιθέσεις πρωτοκόλλου συμβαίνουν κυρίως εναντίον συσκευών, όπως οι επιθέσεις man-in-the-middle και denial-of-service (DoS) (Ijaz et al., 2016). Όλες αυτές οι επιθέσεις διακόπτουν τις γρήγορες, αυτοματοποιημένες επικοινωνίες μεταξύ έξυπνων συσκευών που καθιστούν δυνατή την ταχεία πρόσβαση σε πληροφορίες σε μια έξυπνη πόλη. Τέλος, άλλη μία πρόκληση για την ασφάλεια μέσα στην έξυπνη πόλη είναι οι ετικέτες αναγνώρισης ραδιοσυχνοτήτων (RFID) που χρησιμοποιούνται στο έξυπνο περιβάλλον, βιομηχανία και έξυπνη κινητικότητα.

Μπορούν να υποκλαπούν δεδομένα και να δώσουν πρόσβαση σε μη εξουσιοδοτημένους χρήστες αποσπώντας πληροφορίες για το απόρρητο των δεδομένων και προκαλώντας παρεμβολές στα σήματα επικοινωνίας ακόμη και στην

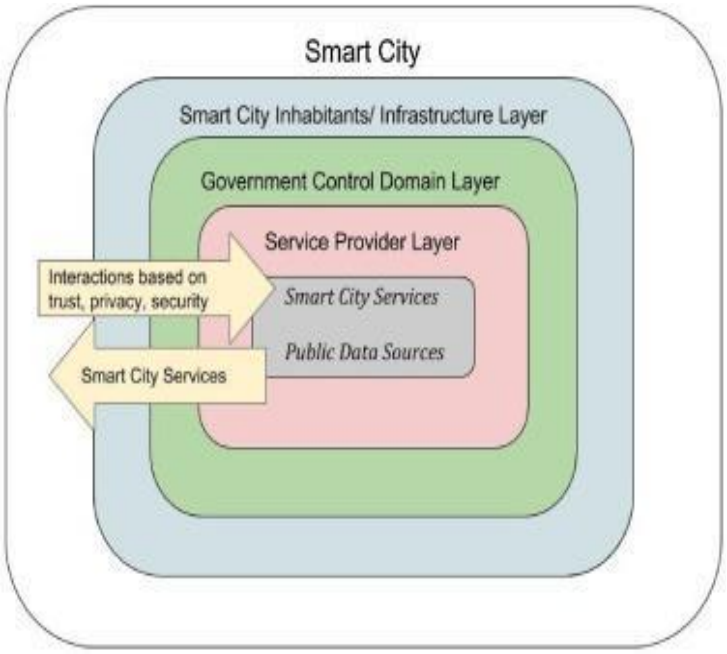
άρνηση της υπηρεσίας. Έτσι, η έξυπνη πόλη του Άμστερνταμ όταν αποφάσισε στρατηγικά και για τους οικονομικούς λόγους να στραφεί στις έξυπνες λύσεις έπρεπε και πρέπει μελλοντικά να ενισχύει διαρκώς την ασφάλεια σε όλα τα επίπεδα καθώς οι κίνδυνοι δεν θα σταματήσουν ποτέ έως ότου χαλαρώσει η ίδια η πόλη. Η επιθέσεις αυτές έχουν στόχο να πλήξουν την έξυπνη πόλη με κάθε τρόπο και αυτό έχει να κάνει με τις μελλοντικές συνέπειες που θα ακολουθήσουν καθώς θα είναι ένα τρομερό ζήτημα για την έξυπνη πόλη που σε ορισμένες περιπτώσεις πλήρωσαν ακόμη και τρίτους φορείς για να αντιμετωπίσουν αυτές τις ακραίες καταστάσεις καθώς δεν ήταν σε θέση να αντιμετωπίσουν το πρόβλημα λόγω των πολλαπλών χτυπημάτων και των ανέτοιμων υποδομών που δεν μπορούσαν να διαχειριστούν τέτοιου είδους καταστάσεις και προκλήσεις. Η συμμόρφωση και η πιστή τήρηση σε πρωτόκολλα ασφαλείας, η συνεχής ενημέρωση και η χρήση πολιτικών που υπάρχουν πλέον σαν εργαλεία αποτροπής είναι αναγκαία και επιβάλλεται η πιστή τήρηση αυτών των οδηγιών που βγαίνουν καθώς εξασφαλίζεται σε ένα ικανοποιητικό βαθμό η ασφάλεια και η ιδιωτικότητα των πολιτών από πιθανούς κινδύνους που βρίσκονται διαρκώς στη σκιά του συστήματος και περιμένουν να επιτεθούν στις υποδομές της έξυπνης πόλης.

4.6 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Για να αντιμετωπιστούν οι κυβερνοεπιθέσεις στο έξυπνο δίκτυο πρέπει να γίνουν σημαντικές αλλαγές και αναβαθμίσεις τόσο σε επίπεδο υλικού όσο και σε λογισμικού. Νέα δίκτυα, νέα μοντέλα και μηχανισμοί μπορούν να προσφέρουν σοβαρές λύσεις στο οικοσύστημα έχοντας λάβει νωρίτερα τα κατάλληλα μέτρα προστασίας και ελέγχου και πραγματοποιώντας διαρκής ελέγχους που θα δώσουν λύσεις σε τυχόν πιθανές απόπειρες. Το σημαντικό είναι να μπορούν να προλαμβάνουν τις επιθέσεις και να τις αναγνωρίζουν και όχι τόσο να έχουν το ρόλο του παρατηρητή και να επέμβουν σε δεύτερο χρόνο. Το σύστημα χρειάζεται προστασία των δεδομένων για ένα διακομιστή, ένα διαρκή έλεγχο για την αξιοπιστία των δεδομένων και ένα ασφαλές έξυπνο δίκτυο. Ο εντοπισμός κακόβουλων πληροφοριών και λογισμικών είναι η σημαντικότερη διεργασία που πρέπει να γίνει ώστε να αποτραπεί η είσοδος στο έξυπνο δίκτυο και να μη μολυνθούν οι συσκευές εξασφαλίζοντας έτσι την ασφάλεια γύρω από τη έξυπνη πόλη (Yang et al., 2019). Η ασφάλεια της έξυπνης πόλης στοχεύει στην ασφαλή παροχή υπηρεσιών και στην ικανοποίηση των πολιτών. Όπως φαίνεται και στη παρακάτω εικόνα τα στρώματα χωρίζονται σύμφωνα με τις διαδικασίες που ακολουθούνται και πιο συγκεκριμένα

όπως φαίνεται στη εικόνα υπάρχουν τρία επίπεδα: κυβερνητικός έλεγχος, έξυπνοι κάτοικοι / έξυπνες υποδομές και οι πάροχοι υπηρεσιών. Είναι απαραίτητο να συμμορφώνονται όλοι με τις πολιτικές που ορίζονται, οι πολίτες να επαληθεύουν την ταυτότητα τους και οι πάροχοι να ενισχύουν την ασφάλεια.

Η συνεργασία και των τριών κρίνεται αναγκαία καθώς δεν μπορεί να αντέξει κανένα σύστημα χωρίς την υποστήριξη και τη συνεργασία των υπολοίπων και θα δημιουργούνται συνέχεια κενά στην ασφάλεια και δεν είναι πάντα η ζημία στον ίδιο βαθμό. Η σπουδαιότητα λοιπόν είναι να υπάρχει εμπιστοσύνη, ασφάλεια και απόρρητο μέσα σε αυτό το οικοσύστημα και να τηρούνται οι κανόνες όπως ορίζονται χωρίς να παρερμηνεύει κάποιος τις λειτουργίες και να λειτουργεί αυτόνομα γιατί μπορεί μία αλλαγή να επηρεάσει και τις υπόλοιπες λειτουργίες και να δημιουργηθούν ακόμη περισσότερα προβλήματα στην έξυπνη πόλη. Σε αυτό το σημείο αξίζει να σημειωθεί πως όταν αναβαθμίζονται οι υποδομές και οι φορείς παίρνουν νέους εξοπλισμούς και λογισμικά θα πρέπει να πραγματοποιούν αρκετές δοκιμές έως ότου δουν τις δυνατότητες τους και φυσικά να γνωρίζουν όλες τις δυνατότητες και μειονεκτήματα που μπορούν να προκύψουν σε μία πιθανή επίθεση και πως θα αντιμετωπιστεί στον κυβερνοχώρο. Τα εργαλεία λοιπόν είναι χρήσιμα όταν γνωρίζει κάποιος πως λειτουργούν και πως θα αξιοποιηθούν σωστά όταν εντοπιστούν προβλήματα στην ασφάλεια από κακόβουλους εισβολείς.



Εικόνα 10: Υπηρεσίες έξυπνης πόλεις.

Υπάρχουν ορισμένες τεχνικές ασφαλείας που βοηθούν στην καταπολέμηση επιθέσεων στην έξυπνη πόλη. Τα έξυπνα κινητά που λειτουργούν εντός του έξυπνου δικτύου μπορούν να προστατευθούν περισσότερο μέσω προγραμμάτων προστασίας από ιούς, τείχους προστασίας, ασφαλών API, ελέγχου ταυτότητας, φίλτρων και λύσεων κινητής τηλεφωνίας M2M. Σύμφωνα με το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) μπορούν να βοηθήσουν στην ασφάλεια μιας έξυπνης πόλης με τους παρακάτω μηχανισμούς που περιλαμβάνουν τα IEEE 802.15.4, IEEE 802.15.1 και IEEE 802.15.11. Το IEEE 802.15.4 εξετάζει τη διαχείριση ενέργειας, την ανίχνευση ενέργειας και την ποιότητα σύνδεσης των έξυπνων αντικειμένων προκειμένου να αξιολογήσει τις απειλές ασφαλείας. Το IEEE 802.15.11 βοηθά στην ασφάλεια του Wi-Fi μέσω του πρωτοκόλλου ασφαλείας WIFI Protected Access (WPA) και το IEEE 802.15.1 χρησιμοποιείται στο Bluetooth (Martinez-Balleste et al., 2013).

4.7 ΠΡΟΣΤΑΣΙΑ ΥΠΗΡΕΣΙΩΝ ΣΤΟ CLOUD

Μέσα στην έξυπνη πόλη υπάρχουν αμέτρητες έξυπνες συσκευές που επικοινωνούν με στο σύνολο με το έξυπνο δίκτυο για την αποστολή, μεταφορά και επεξεργασία των δεδομένων. Η διαδικασία αυτή είναι άμεση και παρέχει εμπιστευτικά ένα μεγάλο

όγκο δεδομένων που συλλέγονται από τη καθημερινή χρήση. Η πόλη του Άμστερνταμ χρησιμοποιεί αυτές τις λύσεις και υπηρεσίες Cloud για να μπορούν γρήγορα και με ασφάλεια να αντλούν δεδομένα και να ενημερώνουν τις επιμέρους λειτουργίες. Αυτές που προκρίνονται αυτή τη στιγμή στην έξυπνη πόλη είναι τρεις και είναι οι εξής: Software as a Service (Saas), Platform as a Service (PaaS) και τέλος Infrastructure as a Service (IaaS). Το PaaS εφαρμόζεται κυρίως στις εφαρμογές με σκοπό τη παροχή υπηρεσιών στα λογισμικά που υπάρχουν, δηλαδή να καλύπτονται οι ανάγκες αν προκύψουν αυξημένα ζητήματα ενώ αντίστοιχα το IaaS δίνει πρόσβαση και παρακολουθεί τις απομακρυσμένες υποδομές, τις απαιτούμενες ρυθμίσεις και διαχειρίζεται τις επικοινωνίες για τους χρήστες σε σχέση με το σύστημα. Αυτές οι υπηρεσίες μαζί με τη παραδοσιακή λειτουργία της αποθήκευσης σε ένα Cloud μπορούν να προστατευτούν οι πολίτες μέσα στην έξυπνη σε οποιαδήποτε δραστηριότητα και αν κάνουν και να αξιοποιήσουν σωστά τις λειτουργίες. Η ασφάλεια και τα πρότυπα απορρήτου της ιδιωτικής χρήσης είναι η ουσία της απομακρυσμένης διασύνδεσης καθώς όλα βρίσκονται σε κάποιο υπολογιστικό νέφος. Η αποθήκευση πληροφοριών δημιουργεί πιθανόν πολλά ερωτηματικά για το αν πραγματικά προστατεύονται τα δεδομένα καθώς εγείρονται πολλά θέματα γύρω από τη ασφάλεια και το απόρρητο, για το ποιος πιθανόν να έχει πρόσβαση, αν έχουν παραβιαστεί και αν κοινοποιούνται προσωπικές πληροφορίες.

Η διαχείριση των δεδομένων πρέπει να γίνεται αποκλειστικά και μόνο από τους χρήστες και όχι να υπάρχουν πιθανά άλλα εμπλεκόμενα μέρη. Σίγουρα, πρέπει ο χρήστης να γνωρίζει αν για παράδειγμα υπάρχουν ή δημιουργούνται σε κάποιο άλλο υπολογιστικό νέφος ή τοπικά αντίγραφα και αν υπάρχουν και άλλες συσκευές που συμμετέχουν σε αυτό. Η ασφάλεια του καθενός μέσα σε ένα οικοσύστημα όπως είναι η έξυπνη πόλη έχει να κάνει με τις προσωπικές ελευθερίες που παραχωρεί ο χρήστης και τι θέλει να κοινοποιήσει ελεύθερα και όχι να παραχωρήσει τη συγκατάθεση του απλώς για να χρησιμοποιήσει μία υπηρεσία σαν και αυτή. Η έξυπνη πόλη σε κάθε περίπτωση χρησιμοποιεί τις υπηρεσίες Cloud για να μπορεί να μεταφέρει και να αποθηκεύει κυρίως τα δεδομένα, να ενημερώνει και να προλαμβάνει καταστάσεις και τέλος να συλλέγει δεδομένα για να μπορεί να τα μελετήσει κατά τη διάρκεια της συλλογής και να εκτιμηθούν τα δεδομένα μέσα από ένα σύνολο συσκευών, φορητών υπολογιστών, αισθητήρες, υπολογιστικά νέφη και λογισμικά. Η σημασία των

ψηφιακών λύσεων μπορεί και έχει αντέξει αρκετές επιθέσεις καθώς έγιναν έξυπνα τα δίκτυα και χρησιμοποιήθηκαν νέες τεχνολογίες και μέσα.

4.8 ΕΞΥΠΝΗ ΠΟΛΗ - ΛΟΝΔΙΝΟ

Το Λονδίνο τα τελευταία χρόνια προσπαθεί με κάθε τρόπο να αναβαθμίσει τις τεχνολογίες που χρησιμοποιεί σαν έξυπνη πόλη και να οργανωθεί μέσα από τα εργαλεία που έχει στη διάθεση του καθώς αυξάνονται και αλλάζουν οι ανάγκες διαρκώς. Η διαχείριση της έξυπνης πόλης γίνεται μέσα από τη πλατφόρμα Smart London και συντονίζεται απευθείας από τις Δημοτικές Αρχές της πόλης ώστε οι φορείς και το Κράτος να μπορούν να έχουν άμεση επαφή με τους πολίτες (Smart London, 2020). Στόχος της πόλης είναι να γίνει η πρώτη έξυπνη πόλη στο κόσμο και να προσελκύσει περισσότερους χρήστες για να χρησιμοποιούν τις εφαρμογές και τα μέσα που παρέχει η έξυπνη πόλη καθώς και να αναπτυχθούν νέα καινοτόμα εργαλεία. Η ανοιχτή πλατφόρμα καινοτομίας συγκεντρώνεται στο London Living. Η χρήση έξυπνων δεδομένων και η συνεργασία δεδομένων προωθείται στο πρόγραμμα ανάλυσης δεδομένων, το οποίο αποτελεί μέρος της ανοιχτής πύλης κοινής χρήσης δεδομένων του London Datastore (London Datastore, 2020). Ουσιαστικά είναι ένα κέντρο συλλογής δεδομένων που αναλύονται όλα τα δεδομένα με ψηφιακά μέσα και τεχνολογίες ώστε να βελτιώσουν τις υφιστάμενες παροχές και να δημιουργήσουν νέες και πιο σύγχρονες υπηρεσίες. Μάλιστα, ενθαρρύνεται η συνεργασία μεταξύ των φορέων (δημοσίου και ιδιωτικού) καθώς υπάρχουν πλατφόρμες (π.χ. το London Office of Technology and Innovation) συνεργασίας για την ενίσχυση της καινοτομίας και της επιχειρηματικότητας. Είναι σημαντικό το γεγονός πως η πόλη μέσα από τους θεσμούς της προσκαλεί διαρκώς όλους τους ενδιαφερόμενους να συμμετέχουν σε αυτές τις δράσεις μέσα από νεοφυείς τεχνολογίες και να δημιουργήσουν μαζί το σχεδιασμό και την αρχιτεκτονική της έξυπνης πόλης. Ο μετασχηματισμός της έξυπνης πόλης του Λονδίνου αφορά τη καινοτομία, την ψηφιακή τεχνολογία και την εξυπηρέτηση των πολιτών και λειτουργεί ως πόλος έλξης για τους ανθρώπους που θέλουν να επισκεφτούν την πόλη (Pozdniakova, 2018). Οι βασικότεροι παράγοντες που επηρεάζουν την έξυπνη πόλη του Λονδίνου έχουν να κάνουν με το σχεδιασμό των υπηρεσιών, με την ανάλυση και τη κοινή χρήση των δεδομένων, με την άρτια συνδεσιμότητα, τις έξυπνες παροχές από εφαρμογές και τη ψηφιακή διακυβέρνηση. Έτσι, η έξυπνη πόλη του Λονδίνου προσπαθεί σε κάθε υπηρεσία και εφαρμογή να

αυξήσει τις δυνατότητες που παρέχει και να μειώσει τις δυσκολίες που υπάρχουν, όπως για παράδειγμα την έξυπνη μεταφορά στους δρόμους που ενθαρρύνει τη χρήση των μέσων μαζικής μεταφοράς μειώνοντας την εισερχόμενη κίνηση των ιδιωτικών αυτοκινήτων στη πόλη που εκ των πραγμάτων δυσκολεύει τη καθημερινότητα των ανθρώπων ακόμη και στο πιο απλό πράγμα, την εύρεση μίας θέσης στάθμευσης.

Επίσης, δημιουργώντας ένα καλό σύστημα μέσων μαζικής μεταφοράς θα μπορούσε να μειωθούν οι περιβαλλοντολογικοί ρύποι και τα καυσαέρια και να συμβάλλουν έμπρακτα στο περιβάλλον. Τέλος, μέσα από την πλατφόρμα ενθαρρύνεται η χρήση των ποδηλάτων σε ορισμένες περιοχές και όπου είναι εφικτό για μετακίνηση ώστε να εξοικονομηθεί ενέργεια και να διατηρηθεί η ασφάλεια στους δρόμους. Η χρήση της βιώσιμης ενέργειας για τα κτήρια και τα μέσα μαζικής μεταφοράς τονίζεται και δίνεται ιδιαίτερη προσοχή από το Κράτος (Willems et al., 2017). Ένα ακόμη ζήτημα που προσπαθεί να επιλύσει η έξυπνη πόλη του Λονδίνου είναι το μεγάλο πρόβλημα της αστικοποίησης καθώς στη πόλη του Λονδίνου ζουν μόνιμα 9 εκατομμύρια άνθρωποι και οι ανάγκες τους διαρκώς μεταβάλλονται. Η βιωσιμότητα της κτιριακής κατασκευής και των δομικών υλικών που χρησιμοποιούνται δεν είναι εμφανώς αρκετή. Φαίνεται ότι το Λονδίνο έχει περισσότερα προβλήματα με τις παλαιότερες υποδομές του για να χτίσει απλώς νέα σπίτια για να αντιμετωπίσει τη γρήγορη αστικοποίηση. Στη συνέχεια, φαίνονται οι προσπάθειες που γίνονται από την έξυπνη πόλη του Λονδίνου να χρησιμοποιούνται οι νέες τεχνολογίες όπως της τεχνητής νοημοσύνης, ρομποτικής και υπηρεσίες Cloud για να καλυφθούν προβλήματα π.χ. στην έξυπνη κυκλοφορία και τη κινητικότητα των ανθρώπων. Με τη βοήθεια των εταιριών που ασχολούνται στη κατασκευή οχημάτων και παρέχουν νέες υπηρεσίες για τους οδηγούς σε συνδυασμό με τα έξυπνα εργαλεία που υπάρχουν στις έξυπνες πόλεις δίνουν μία λύση ικανή για τους πολίτες ώστε να βελτιώνουν τη ποιότητα ζωής τους και να εξοικονομούν χρόνο και πόρους. Οι πολίτες ενθαρρύνονται διαρκώς να συμμετέχουν και να είναι ενεργοί σε αυτό το οικοσύστημα και να έχουν πιο ενεργό ρόλο ώστε να διαμορφώνουν στη πραγματικότητα τις υπηρεσίες με την αλληλεπίδραση που υπάρχει. Το Λονδίνο, σε σχέση με τη πόλη του Άμστερνταμ προσπαθεί να αναπτύξει μία στρατηγική που θα ενσωματώνει όλες τις δυνάμεις τόσο στο εσωτερικό της όσο και στο εξωτερικό της περιβάλλον με πρωτοβουλίες που θα αναβαθμίσουν τις υποδομές (Song, 2020) . Η χρήση δικτύων, αισθητήρων IoT και υπηρεσίες τεχνητής νοημοσύνης είναι στα κύρια χαρακτηριστικά αυτής της

στρατηγικής που εφαρμόζεται λόγω της διαφοράς και του όγκου του πληθυσμού καθώς δημιουργούνται περισσότερα δεδομένα που αναλύονται. Οι δύο πόλεις προσπαθούν να αντιμετωπίσουν όλες τις δυσκολίες που εμφανίζονται καταναλώνοντας πόρους σε όλους τους τομείς προκειμένου να αναβαθμιστούν όλες οι υποδομές και να στηριχθούν στις νέες τεχνολογίες που έχουν αναπτύξει. Η υιοθέτηση τέτοιων πρακτικών δεν σημαίνει απαραίτητα πως έχουν επιλύσει όλα τα προβλήματα τους αλλά διαρκώς προσπαθούν να μάθουν από αυτά και να προχωρήσουν προς όφελος των πολιτών κάνοντας μία απλή πόλη σε έξυπνη.

Τα πλεονεκτήματα της αναβάθμισης αυτής που προκύπτουν για τους πολίτες του Λονδίνου είναι σημαντικά καθώς έχει βελτιωθεί η καθημερινότητα τους και δεν έχουν τοπικό χαρακτήρα μιας και είναι πόλος έλξης των ανθρώπων που επιλέγουν να την επισκεφτούν και απολαμβάνουν νέες και καινοτόμες υπηρεσίες. Η ανθεκτικότητα της πόλης σε τόσες μεγάλες και σύνθετες προκλήσεις σε όλο τον ιστό της φαίνεται και αποδεικνύεται στη πράξη καθώς καταγράφεται διαρκώς μία ανοδική τάση στη χρήση των υπηρεσιών της από τους πολίτες και φυσικά αυτό είναι ένα στοιχείο εμπιστοσύνης πως όλα λειτουργούν σωστά (Zvolska et al., 2019). Από την άλλη πλευρά, πρέπει να δει κανένας και τις πιθανές ευπάθειες που μπορεί να προκύψουν και τους πιθανούς τρόπους για να αντιμετωπιστούν. Η απλοποίηση της καθημερινότητας για μία έξυπνη πόλη δεν είναι σίγουρα μία εύκολη κατάσταση. Η αστικοποίηση των πόλεων και η αύξηση των ρυθμών σε όλους τους τομείς (οικονομία, κοινωνία, περιβάλλον κτλ) έχει οδηγήσει τις έξυπνες πόλεις στο σημείο να καταναλώνουν περισσότερους πόρους για να διαχειριστούν αυτά τα ζητήματα και σε ορισμένες περιπτώσεις να μην μπορούν να ανταποκριθούν στις απαιτήσεις προκαλώντας άλλα προβλήματα όπως στο περιβάλλον. Μέσα από την έρευνα που έγινε και τη προσπάθεια να συγκριθούν αυτές οι δύο έξυπνες πόλεις αναλύθηκαν όλα τα ποιοτικά χαρακτηριστικά των παρεχόμενων υπηρεσιών και με τη βοήθεια της βιβλιογραφίας να τονιστούν οι κύριες διαφορές τόσο στην εφαρμογή των στρατηγικών που ακολούθησαν αλλά και στη κουλτούρα που καλλιεργήθηκε για να αναπτυχθούν οι δύο πόλεις.

Αξιοποιώντας όλες τις διαθέσιμες πηγές και τη βιβλιογραφία και εφαρμόζοντας επαγωγικό συλλογισμό για την ανάδειξη κάποιων συμπερασμάτων γύρω από το θέμα της διατριβής αλλά και την εγκυρότητας των δεδομένων έγινε η προσπάθεια για να απαντηθούν μερικά από τα πιο σημαντικά στοιχεία της έξυπνης πόλης και των

εφαρμογών της. Μέσα από τα δεδομένα που αντλήθηκαν έγινε η προσπάθεια να μελετηθούν και να καταγραφούν οι σημαντικότερες πτυχές του θέματος εστιάζοντας στο κύριο αποτέλεσμα, δηλαδή στη διεξαγωγή έγκυρων συμπερασμάτων (Cowley & Caprotti, 2019). Η έρευνα που πραγματοποιήθηκε και η αξιοποίηση των δεδομένων έδειξαν ότι η έξυπνη πόλη αποτελείται από τον άνθρωπο, τις νέες τεχνολογίες και των θεσμικών διαστάσεων. Σίγουρα, με το πέρασμα των χρόνων οι ορισμοί για την έξυπνη πόλη έχουν αλλάξει αλλά στη πραγματικότητα όλοι αναφέρονται γύρω από την οικονομία, το περιβάλλον, τη διαβίωση, την επιβίωση και την διακυβέρνηση που μεταφράζονται σε έξυπνα χαρακτηριστικά για την πόλη. Έτσι, στις περισσότερες κατηγορίες που υπάρχουν μέσα σε μία έξυπνη πόλη μπορεί κανείς να διακρίνει σχεδόν τους ίδιους πυλώνες ανάπτυξης. Οι διαφορές ανάμεσα στη πόλη του Λονδίνου και του Άμστερνταμ έχουν να κάνουν με τον όγκο που έχει να διαχειριστεί αρχικά η πρώτη πόλη καθώς είναι μεγαλύτερος λόγω του πληθυσμού και δεύτερον η συμμετοχή των ανθρώπων σε αυτό το οικοσύστημα.

Υπάρχουν ορισμένες καταγραφές που δείχνουν ότι σε κάποιες κατηγορίες όπως είναι η έξυπνη κινητικότητα και η έξυπνη διαβίωση η πόλη του Λονδίνου έχει δώσει μεγάλη βαρύτητα και έχει διαθέσει περισσότερους πόρους ώστε να μειώσει τα προβλήματα και να δώσει ολοκληρωμένες λύσεις. Επίσης, στην έξυπνη βιωσιμότητα (οικονομία, κοινωνία και περιβάλλον) η πόλη του Λονδίνου προσπαθεί να αναπτύξει μέσα από τις υποδομές τις το ηλεκτρονικό εμπόριο και να ενθαρρύνει τους πολίτες στις νέες τεχνολογίες μειώνοντας τις αρνητικές συνέπειες που θα είχε για το περιβάλλον αν δεν είχαν αυτές τις εναλλακτικές εργασίας (Caird, 2016) . Η ανάπτυξη και χρήση νέων τεχνολογιών και δικτύων έχουν δώσει τα πληροφοριακά συστήματα μία διέξοδο ώστε να μεταφέρουν με ασφάλεια τα δεδομένα. Έτσι, η πόλη του Λονδίνου για να μπορέσει να εφαρμόσει όλες αυτές τις υπηρεσίες φρόντισε να αυξήσει τα πρωτόκολλα ασφαλείας και να δημιουργήσει άμυνες ικανές να ανταποκριθούν στις επιθέσεις. καθώς όλα στηρίζονται σε ιδιωτικά δίκτυα χρησιμοποιώντας και πρότυπα ISO 37120:2014 για την αειφόρο ανάπτυξη σε συνδυασμό με τους δείκτες των υπηρεσιών και της ποιότητας ζωής των πολιτών στη πόλη ώστε να καταγράφονται και να παρακολουθούνται οι αποδόσεις των δεικτών αλλά και η αποδοτικότητα της βιώσιμης ανάπτυξης. Η χρήση νέων τεχνολογιών 5G, η αναβάθμιση των δικτύων και η χρήση αισθητήρων IoT είναι ψηλά στην ατζέντα της έξυπνης πόλης του Λονδίνου καθώς οι μεγάλες ποσότητες που αναλύονται πρέπει να

δίνουν σε απειροελάχιστο χρόνο τη σωστή απάντηση. Η χρήση των βασικών προτύπων ασφαλείας και στις δύο πόλεις είναι ο ίδιος καθώς η έννοια της ασφάλειας δεν διαφέρει και τόσο από πόλη σε πόλη αλλά υπάρχει διαφορά στο βαθμό που θέλει μία έξυπνη πόλη να προστατέψει τις υποδομές της και τους χρήστες που συμμετέχουν. Η δυσκολία που υπάρχει στο Λονδίνο και τα ζητήματα που έχει να επιλύσει σαν πόλη δεν είναι τα ίδια με αυτά της πόλης του Άμστερνταμ καθώς διαφέρει η κουλτούρα των ανθρώπων, η οργάνωση της πολιτείας, οι θεσμοί αν συμμετέχουν και σε πιο βαθμό, οι συνεργασίες που υπάρχουν και τα τεχνολογικά μέσα που θέλουν να χρησιμοποιηθούν από τις έξυπνες πόλεις.

Οι κύριες ομοιότητες μεταξύ των δύο πόλεων είναι η συστηματική οργάνωση και συμμόρφωση με τους κανόνες και νόμους που υπάρχουν γύρω από τα θέματα ασφαλείας και απορρήτου και της τήρησης της αρχής των προσωπικών δεδομένων ώστε να διασφαλίζεται ο πολίτης μέσα σε αυτό το οικοσύστημα και να συμμετέχει δυναμικά. Από την άλλη πλευρά, οι διαφορές που υπάρχουν σε γενικές γραμμές είναι σημαντικές ως προς το σχεδιασμό και την εφαρμογή των δικτύων, των αναβαθμίσεων των υποδομών και των εργαλείων που θα τοποθετηθούν μέσα στο οικοσύστημα καθώς διαφέρουν στο τρόπο συλλογής και ανάλυσης αυτών των δεδομένων ώστε να εξάγουν χρήσιμες πληροφορίες μιας και δεν έχουν τα ίδια κέντρα ανάλυσης και επεξεργασίας τόσο μεγάλων και ανοιχτών δεδομένων να διαχειριστούν. Τέλος, να σημειωθεί ότι αν και η έξυπνη πόλη του Λονδίνου έχει περισσότερα πιθανά τρωτά σημεία λόγω του πληθυσμού και γεωγραφικά της θέσης της δεν σημαίνει ότι ο βαθμός των ευπαθειών είναι και απαραίτητα ο ίδιος ή αντίστοιχος με αυτόν της έξυπνης πόλης του Άμστερνταμ. Η κάθε απειλή είναι ξεχωριστή και αντιμετωπίζεται με συντονισμένες κινήσεις που γνωρίζει το εκάστοτε σύστημα διαχείρισης.

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

Οι έξυπνες πόλεις έχουν αλλάξει εντελώς το τρόπο σκέψης των ανθρώπων δημιουργώντας ακόμη περισσότερα οφέλη μέσα από τις νέες τεχνολογίες καθώς εργάζονται συνεχώς προς αυτή τη κατεύθυνση. Η αξιοποίηση της τεχνολογίας αλλά και των εργαλείων που είναι διαθέσιμα έδωσαν την ευκαιρία στις έξυπνες πόλεις να συνθέσουν ένα νέο οικοδόμημα και να εξασφαλίσουν σημαντικά οφέλη από τις εργασίες αυτές σε πολλούς τομείς (οικονομία, περιβάλλον και κοινωνία). Η έξυπνη πόλη αν και αναπτύχθηκε με τη βοήθεια πολλών και διαφορετικών δυνάμεων (ιδιωτικού και δημοσίου) αξίζει να σημειωθεί ότι όλοι οι εμπλεκόμενοι φορείς κέρδισαν (στο βαθμό που εργάστηκαν) και τις γνώσεις που αποκτήθηκαν. Η αξιοποίηση νέων τεχνολογιών, η αναβάθμιση δικτύων και αισθητήρων, η επενδύσεις σε νέες γενιές τεχνολογίας και οι πόροι που καταναλώθηκαν για να δημιουργηθεί αυτό το οικοσύστημα είναι πάρα πολλοί καθώς δεν θα ήταν εφικτό να μαζευτούν και να αναλυθούν τόσα πολλά μεγάλα δεδομένα ώστε να μπορούν να επιστρέφουν μέσα σε απειροελάχιστο χρόνο σωστές απαντήσεις στους χρήστες και να ρυθμίζουν αποτελεσματικά τις υπόλοιπες διεργασίες. Αν αναλογιστεί κανείς ότι οι πολίτες του Άμστερνταμ βρίσκονται διαρκώς εν κινήσει και αξιοποιούν τις δυνατότητες που τους παρέχει η πόλη τότε θα μπορεί να καταλάβει ο καθένας τι τεχνολογική δύναμη και οργάνωση απαιτείται για να μπορέσει η έξυπνη πόλη να ολοκληρώσει άμεσα τις διεργασίες. Το πλαίσιο της ασφάλειας και του απορρήτου που μελετήθηκαν γύρω από τις έξυπνες πόλεις μέσα από τη βιβλιογραφική ανασκόπηση και τη συστηματική συλλογή των δεδομένων ήταν ικανά σε ένα βαθμό ώστε να μελετηθούν τα δεδομένα και να βγουν ορισμένα συμπεράσματα με τη βοήθεια επαγωγικών συλλογισμών.

Οι έξυπνες πόλεις βασίζονται σε τρεις βασικούς πυλώνες: τις υποδομές, το ανθρώπινο κεφάλαιο και τις πληροφορίες. Η πόλη του Άμστερνταμ αν και ήταν από τις πρώτες χώρες που ξεκίνησε την εφαρμογή της δημιουργίας και της μετατροπής σε μία έξυπνη πόλη δεν τα κατάφερε τόσα καλά σε σχέση με άλλες πόλεις (π.χ. το Λονδίνο) και παρότι είναι μικρότερη σε έκταση και πληθυσμό καθώς αντιμετώπισε πολλές δυσκολίες στις υποδομές της καθώς έπρεπε να αλλάξει σχεδόν όλο τον αστικό κορμό και να ξανά εγκαταστήσει νέες και πιο σύγχρονες υποδομές που θα μπορούσαν να ανταπεξέλθουν στις υποχρεώσεις τους. Το σημαντικό στοιχείο όμως που ανέβασε γρήγορα τη πόλη του Άμστερνταμ είναι η πρωτοβουλία και η θέληση για μία αλλαγή, σαφώς καλύτερη για τη πόλη και τους πολίτες της. Τα κύρια αποτελέσματα της

μελέτης αυτής αναφορικά με την έξυπνη πόλη του Άμστερνταμ έδειξαν πως η συνεχόμενη και ενισχυμένη συνεργασία μαζί με την αξιοποίηση της καινοτομίας και της επιχειρηματικότητας μπορούν να συνεισφέρουν στην ανάπτυξη μίας πόλης και να αναβαθμίσουν το ρόλο της γενικότερα. Τα πλεονεκτήματα που θα προκύψουν σε επίπεδο οικονομίας, τεχνολογίας, κοινωνίας, περιβάλλοντος και κατ΄ επέκταση στους ανθρώπους είναι πολλά και πρέπει να αντιμετωπίζονται αυτές οι αλλαγές ως ευκαιρίες καθώς μπορούν να οδηγήσουν σε μελλοντικές συνεργασίες που θα αναβαθμίσουν τις υπηρεσίες. Σε κάθε περίπτωση, αν εξετάσει κανείς τις διαφορές με μιας έξυπνης πόλης με μιας άλλη θα δει τις διαφορές που υπάρχουν ως προς το τρόπο διαχείρισης σύνθετων καταστάσεων, έκτακτων συνθηκών, της κουλτούρας και της στρατηγικής που εφαρμόζουν καθώς μπορεί να υπάρχει το ίδιο πρόβλημα και να βρεθούν διαφορετικές λύσεις μιας και η τεχνολογία έχει φτάσει πλέον να προσφέρει λύσεις μέσα από συγκεκριμένες καταστάσεις και πρότυπα. Οι εφαρμογές και τα πρότυπα ISO που έχουν δημιουργηθεί για αυτό το σκοπό κυρίως και να μπορούν οι έξυπνες πόλεις να διαχειρίζονται και να αντιμετωπίζουν άμεσα τα προβλήματα δείχνει τη προδιάθεση των πόλεων να πάρουν όλα τα μέτρα που απαιτούνται για να εξασφαλίσουν θετικές λύσεις.

Στη παρούσα διατριβή, μελετήθηκε το πλαίσιο της ασφάλειας και του απορρήτου γύρω από τις έξυπνες πόλεις και τους τρόπους που αντιμετωπίζει μία έξυπνη πόλη αυτά τα προβλήματα. Η προτεραιότητα των έξυπνων πόλεων είναι να προστατέψει τους πολίτες μέσα από τις πιθανές και κακόβουλες επιθέσεις καθώς έχουν στόχο να πλήξουν κρίσιμες υποδομές και να αποσπάσουν σημαντικές προσωπικές πληροφορίες των πολιτών. Στόχος των έξυπνων πόλεων είναι να συμμορφώνονται αρχικά όλοι με τους νόμους και τους κανόνες ώστε να μία ισορροπία και να μπορούν να προφυλαχθούν από τις επιθέσεις. Οι νόμοι που ορίζονται και τα πρότυπα που αναβαθμίζονται γίνονται γιατί πρέπει λαμβάνονται τα ελάχιστα ως πρότυπα ασφαλείας για να προφυλάγονται οι πολίτες από πιθανές παραβιάσεις και απειλές. Έτσι, έχει δημιουργηθεί ένα τεράστιο σύνολο από αισθητήρες, ψηφιακά κέντρα, νέες τεχνολογίες δικτύων που συνεργάζονται με τεχνικές νοημοσύνης, υπηρεσίες Cloud, 5ης γενιάς δίκτυα και ιδιωτικά δίκτυα (VPN) που θα προστατέψουν από άκρο σε άκρο όλο το οικοσύστημα της έξυπνης πόλης. Η συνεργασία όλων τα παραπάνω είναι απαραίτητη καθώς αν χτυπηθεί ένα σημείο της άμυνας να μπορεί να είναι σε θέση και ετοιμότητα το υπόλοιπο σύστημα για να αντιμετωπιστεί η κακόβουλη επίθεση.

Η πόλη του Άμστερνταμ έχει αναπτύξει σημαντικά κέντρα παραγωγής και διαχείρισης των δεδομένων για να μπορεί να μαθαίνει και να επεξεργάζεται άμεσα όλες τις πληροφορίες και να ενημερώνει τους πολίτες έγκαιρα και με ασφάλεια. Οι διαφορές ανάμεσα στις δύο πόλεις (Άμστερνταμ και Λονδίνο) που μελετήθηκαν είναι κυρίως στις υποδομές και στο τρόπο που σχεδιάστηκαν οι υπηρεσίες καθώς είχαν να αντιμετωπίσουν διαφορετικά προβλήματα. Τα προβλήματα που είχε να αντιμετωπίσει το Λονδίνο ήταν κυρίως στις αλλαγές και αναβαθμίσεις των έξυπνων κτιρίων μιας και είναι πιο παλιά τα κτήρια και έπρεπε να γίνουν οι αλλαγές για να βελτιωθούν οι ενεργειακές αποδόσεις και να προφυλάξουν το περιβάλλον. Επίσης, η πόλη του Λονδίνου σε σχέση με το Άμστερνταμ πρέπει να διαχειριστεί περισσότερο τις υπηρεσίες που παρέχει στους πολίτες καθώς αν και έχει αναπτύξει ισχυρά κέντρα οι απαιτήσεις των χρηστών αλλάζουν διαρκώς και για αυτό απαιτείται περισσότερη υπολογιστική ισχύς για να μπορούν να ολοκληρώνονται τα αιτήματα. Κοινό σημείο και των δύο πόλεων είναι ότι αντιμετώπισαν τα προβλήματα ως ευκαιρίες και εργάστηκαν πραγματικά επάνω σε αυτά για να μπορέσουν να οικοδομήσουν νέα και πιο σύγχρονα κέντρα που θα ήταν πλήρως εξοπλισμένα και ρυθμισμένα για να υπερασπιστούν την ασφάλεια και τα προσωπικά δεδομένα των χρηστών. Η οργάνωση, ο σχεδιασμός, η αρχιτεκτονική και η υλοποίηση των φάσεων έγιναν σε κάθε περίπτωση με συντονισμένη προσπάθεια και επιστρατεύτηκαν ακόμη και φορείς από πανεπιστήμια για να μεταφέρουν τις γνώσεις τους στο αντικείμενο και να ολοκληρωθούν με επιτυχία τα έργα αυτά. Η έξυπνη πόλη είναι ένα πλαίσιο ουσιαστικά που συνδυάζει τις πολιτικές εκείνες που ενσωματώνουν τις νέες τεχνολογίες ως συμμάχους και ενισχύουν την επιχειρηματικότητα και τη καινοτομία συμβάλλοντας ενεργά στην ανάπτυξη. Η χρήση καλών πρακτικών και προτύπων σε συνδυασμό με τις νέες τεχνολογίες μπορούν να προσφέρουν μία ισορροπία στους πολίτες και να νιώσουν εμπιστοσύνη με τις εφαρμογές και τις υπηρεσίες και να συμμετέχουν ενεργά. Η σημασία της επικοινωνίας αυτής και της αλληλεπίδρασης μπορεί να μελετηθεί και να καλύψει ενδεχόμενα κενά που μπορούν να προκαλέσουν τυχόν προβλήματα. Στις δύο αυτές έξυπνες πόλεις που αναφέρθηκαν νωρίτερα οι άνθρωποι αγκάλιασαν σχετικά νωρίς τις υπηρεσίες αυτές και τις ενσωμάτωσαν από νωρίς καθώς και οι ίδιοι επιθυμούσαν λύσεις στη καθημερινότητα τους. Η τεχνολογία μπορεί να δώσει ανάσες μέσα σε μία έξυπνη πόλη και να αναβαθμίσει τις λειτουργίες της καθώς θα αναπτύσσονται νέα εργαλεία και θα ενισχύουν τις υπόλοιπες υποδομές. Έτσι, η βιώσιμη ανάπτυξη θα έρθει με εντατικότερους ρυθμούς και θα προκύψουν

καλύτερα αποτελέσματα καθώς θα στηρίζονται σε εναλλακτικές λύσεις που θα έχουν ως επίκεντρο τον άνθρωπο.

Τέλος, αξίζει να σημειωθεί πως και οι υπόλοιπες πόλεις που προσπαθούν να αλλάξουν και να αναβαθμίσουν τις υποδομές τους θα πρέπει να σκεφτούν σοβαρά τα μέτρα ασφαλείας που θα ακολουθήσουν και τους τρόπους που θα σχεδιάσουν αυτές τις υποδομές καθώς θα πρέπει να έχουν διαρκώς πρόσβαση σε ευαίσθητα δεδομένα και να προφυλάσσουν τα προσωπικά δεδομένα των πολιτών. Σε όλα τα επίπεδα ασφαλείας και απορρήτου πρέπει να ακολουθούν και να συμμορφώνονται με τις πολιτικές ασφαλείας και να αναβαθμίζουν τακτικά τα λογισμικά καθώς οι απειλές αλλάζουν μορφή και δεν έχουν την ίδια ένταση να χτυπήσουν τα συστήματα. Επομένως, δεν αρκεί μόνο να υπάρχουν τέλειες εφαρμογές και υπηρεσίες αλλά και όλα εκείνες οι υποδομές που στηρίζουν αυτές τις λειτουργίες να έχουν λάβει τα απαραίτητα μέτρα και να ενημερώνουν τόσο το προσωπικό που εργάζεται αλλά και τους πολίτες καθώς μπορούν να προκαλέσουν άθελα τους και άλλα προβλήματα. Η ασφάλεια και το απόρρητο αρχίζουν από εκεί που δεν επιτρέπεται στους εισβολείς να εισέλθουν και να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα και να καταστρέψουν τις λειτουργίες. Η πόλη του Άμστερνταμ έχει επιτύχει να διαμόρφωση σωστά τις υποδομές της με καλό συντονισμό και σχεδιασμό και έχει προσφέρει λύσεις στους πολίτες ακολουθώντας όλες τις μεθόδους που μπορούν να εγγυηθούν ασφάλεια έχοντας ως στόχο να εξελίσσεται διαρκώς και να μαθαίνει ακόμη και από τους πολίτες που προσφέρουν δεδομένα από τη καθημερινή επαφή τους.

Στη παρούσα εργασία έγινε η προσπάθεια για να τονιστούν τα τεχνολογικά επιτεύγματα των έξυπνων πόλεων καθώς και τα μέτρα ασφαλείας και απορρήτου που λαμβάνουν οι έξυπνες πόλεις ώστε να παρέχουν αποτελεσματικές λύσεις στους πολίτες. Με τη βοήθεια της τεχνολογίας και της καινοτομίας οι άνθρωποι δημιούργησαν νέες πτυχές και πρακτικές που θα μπορέσουν να δώσουν ακόμη καλύτερες λύσεις στο μέλλον εστιάζοντας στον άνθρωπο, έχοντας δηλαδή στο επίκεντρο των διεργασιών τον άνθρωπο προσπαθώντας να του παρέχουν λύσεις που θα ικανοποιούν κάθε ανάγκη. Σίγουρα, θα ήταν σημαντικό οι έξυπνες πόλεις να λαμβάνουν όλα τα απαραίτητα μέτρα και να είναι σε θέση να παρέχουν κάθε είδους υποστήριξη στους πολίτες.

5.1 ΣΥΖΗΤΗΣΗ

Οι μελλοντικές επεκτάσεις στη παρούσα διατριβή θα μπορούσαν να είναι σε συνδυασμό με την ασφάλεια και το απόρρητο η χρήση νέων πρακτικών και κανόνων που χρησιμοποιούνται σε νέες τεχνολογίες, τις αναβαθμίσεις σε αμυντικά συστήματα, στη χρήση νέων μηχανημάτων και λογισμικών που θα δίνουν νέες και πιο βελτιωμένες λύσεις και τέλος η εφαρμογή ενός μοντέλου σε μία πόλη που έχει λάβει διαφορετικά μέτρα ασφαλείας και απορρήτου και τις συνέπειες που θα καταγράφονταν αν είχαν ένα κοινό και σταθερό κανόνα στην ασφάλεια και όχι απλώς να χρησιμοποιούνται τα βασικά επίπεδα. Στη παρούσα διατριβή, μελετήθηκαν οι μεγάλες πόλεις της Ευρώπης και σε ορισμένα σημεία φαίνονται οι διαφορές που προκύπτουν καθώς και οι τρόποι που αντιμετωπίζουν τις καταστάσεις. Αν αναλογιστεί κανένας τις συνέπειες σε μία πιθανή επίθεση σε μία έξυπνη πόλη και τις αρνητικές συνέπειες που ακολουθούν θα πρέπει να φανταστεί ότι έτσι θα είναι στο γενικό κανόνα καθώς δεν αλλάζουν σε μεγάλο βαθμό αν γινόταν αυτό και σε άλλες πόλεις. Οι επιθέσεις έχουν τον ίδιο σκοπό σε κάθε περίπτωση, δηλαδή να βλάψουν μία έξυπνη πόλη και επομένως θα έπρεπε σε κάθε περίπτωση οι έξυπνες πόλεις να λαμβάνουν τα ίδια μέτρα ασφαλείας ώστε να αποφεύγονται τα προβλήματα. Ακόμη μία πιθανή επέκταση στην εργασία θα μπορούσε να είναι η χρήση νέων προτύπων και επικοινωνιών έκτης γενιάς (6G) που θα είναι σε θέση να καλύψουν σε μηδενικό χρόνο τις πιθανές επιθέσεις και θα μπορούν να απομακρύνουν πιθανές ευπάθειες. Τέλος, θα μπορούσε να γίνει μία προσομοίωση μίας έξυπνης πόλης και των μεθόδων που θα υπήρχαν σχετικά με τις κρίσιμες υποδομές και λειτουργίες της και να υπήρχαν πολλαπλές επιθέσεις στα συστήματα ώστε να αξιολογηθούν τα χαρακτηριστικά των δύο πλευρών και να φανούν τα αδύνατα σημεία της έξυπνης πόλης αλλά και οι πιθανές βελτιώσεις στις επιμέρους κατηγορίες. Η τεχνολογία είναι διαρκώς ένα βήμα μπροστά και αυτό αυτομάτως δημιουργεί μία κατάσταση που θέτει όλους τα εμπλεκόμενα τμήματα σε λειτουργία και συνεχή εκπαίδευση για να μπορούν να προστατεύουν τους πολίτες καθώς συμμετέχουν σε αυτό το οικοσύστημα και δείχνουν εμπιστοσύνη τις παρεχόμενες υπηρεσίες μιας και αποδέχονται τους όρους και τις προϋποθέσεις των υπηρεσιών μίας έξυπνης πόλης και υπάρχει πάντα ο κίνδυνος να εκτεθούν τα προσωπικά στοιχεία τους. Επομένως, θα πρέπει οι μελλοντικές έρευνες να θέσουν μία νέα πτυχή στο συγκεκριμένο ζήτημα εξετάζοντας τα προβλήματα μέσα από μία εικονική πραγματικότητα και τις πιθανές αλλαγές που

μπορούν να προκύψουν καθώς επηρεάζονται όλα άμεσα και δυναμικά. Η δύναμη που έχει ένας χρήστης - πολίτης μέσα στο οικοσύστημα αυτό και η αλληλεπίδραση τους είναι εξαιρετικά σημαντική καθώς ο ένας αποτελεί μέρος του άλλου ώστε να συνυπάρχουν μέσα σε αυτό το περιβάλλον. Οι μελλοντικές έρευνες αν συνδυάσουν τα σημερινά δεδομένα και τις τεχνολογίες μπορούν να παρακάμψουν τεχνικά ορισμένα προβλήματα και να δώσουν πιθανόν νέες εκδοχές στους τρόπους αντιμετώπισης της ασφάλειας και της διαχείρισης του ιδιωτικού απορρήτου των πολιτών. Μελλοντικές έρευνες που θα πραγματοποιηθούν σχετικά με τις έξυπνες πόλεις, την ασφάλεια και το ιδιωτικό απόρρητο θα πρέπει να έχουν ως προτεραιότητα τους να βρουν και να εφαρμόσουν καλές πρακτικές που θα βοηθήσουν σε αυτές τις κατηγορίες και θα δώσουν ακόμη περισσότερη ασφάλεια στους πολίτες καθώς οι κυβερνοεπιθέσεις διαρκώς αυξάνονται και απειλούνται τα προσωπικά δεδομένα των πολιτών. Οι μελλοντικές έρευνες στο συγκεκριμένο θέμα θα πρέπει να δώσουν νέα στοιχεία και προτάσεις καθώς θα έχει προχωρήσει η τεχνολογία αλλά και στο γεγονός ότι οι υφιστάμενες πηγές είναι οδηγοί στις έρευνες και δίνουν τις βασικές κατευθύνσεις στο θέμα. Η αξιοποίηση των δεδομένων αυτών μέσα από πηγές μπορούν να προσφέρουν σημαντικά οφέλη στις μελλοντικές έρευνες και να αναπτυχθούν τεχνολογίες μέσω της τεχνητής νοημοσύνης που θα εξασφαλίζουν την ομαλή λειτουργία των υπηρεσιών αυξάνοντας τ επίπεδα ασφαλείας και λειτουργίας προς όφελος των πολιτών. Με τη χρήση ψηφιακών εργαλείων, της εικονικής πραγματικότητας και της μηχανικής θα μπορούσαν να εφαρμοστούν μέτρα που θα προλάμβαναν σύνθετες καταστάσεις και θα μπορούσε η εκάστοτε πόλη να κάνει πιο στοχευόμενες υποθέσεις. Η ασφάλεια και το απόρρητο των υποδομών θα παρέμεναν στο σύνολο τους άθικτα και δεν θα αυξανόταν ο κίνδυνος επιθέσεων αν υπήρχαν μηχανισμοί που θα προστάτευαν τους τις έξυπνες πόλεις. Έτσι, μία σημαντική μελέτη θα βοηθούσε στην ανάπτυξη νέων δικτύων που θα μπορούν να εφαρμοστούν ακόμη περισσότερες διεργασίες. Η μελέτη και εφαρμογή πρότυπων δικτύων μπορούν να δώσουν επιπλέον αξία στα μέτρα πρόληψης της ασφάλειας όπως ορίζονται ώστε να υπάρχουν επιπλέον χαρακτηριστικά που συμβάλλουν προς αυτή τη κατεύθυνση της διαφάνειας, της ίσης μεταχείρισης, της ακεραιότητας και της ιδιωτικότητας των πολιτών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. (Amsterdam Smart City, n.d.) Amsterdam Smart City. (n.d.). Projects. Amsterdam Smart City. Retrieved January 2, 2023, from https://amsterdamsmartcity.com/updates/project
2. A. S. Elmaghraby and M. M. Losavio, 2014. Cyber security challenges in smart cities: Safety, security and privacy. Journal of advanced research.
3. Ahmad, I., Ashar, S. W., Khalid, U., Irfan, A., & Khalil, W. (2021). Blockchain for Sustainable Smart Cities. In Digital Cities Roadmap (pp. 127–161). Wiley.
4. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28.
5. Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., Nam, T., Pardo, T. A., Scholl, H. J., & Walker, S. (2012). Building understanding of smart city initiatives. In Lecture Notes in Computer Science (pp. 40–53).
6. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3).
7. Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3).
8. Anagnostopoulos, T., Zaslavsky, A. & Medvedev, A., 2015. Robust waste collection exploiting cost efficiency of IoT potentiality in Smart Cities. Singapore, International Conference on Recent Advances in Internet of Things.
9. Angelidou, M. (2014). Smart city policies: A spatial approach. *Cities (London, England)*, *41*, S3–S11.
10. Angelidou, M. (2017). The role of smart city characteristics in the plans of fifteen cities. *Journal of Urban Technology*, *24*(4), 3–28.
11. Anthopoulos, L., & Fitsilis, P. (2010). From digital to ubiquitous cities: defining a common architecture for urban development. IEEE 6th International conference on Intelligent Environments, (pp. 301–306).

12. Anthopoulos, L., (2017), Understanding Smart Cities: A tool of Smart government or an Induastrial Trick? Public Administration and Information Technology 22,The Rise of the Smart City, Chapter 2, 3 and 5, Springer International Publishing AG 2017.
13. Appio, F. P., Lima, M., & Paroutis, S. (2018). Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technological Forecasting and Social Change*, *142*, 1–14.
14. B. Zhang, N. Mohammed, V. S. Dave, and M. A. Hasan, 2017. Feature selection for classication under anonymity constraint. Transactions on Data Privacy.
15. Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. IEEE Access: Practical Innovations, Open Solutions, 8, 23601–23623.
16. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3–13.
17. Bernal Bernabe, J., Hernández, J. L., Moreno, M. V., & Skarmeta Gomez, A. F. (2014). Privacy-preserving security framework for a social-aware internet of things. In Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services (pp. 408–415).
18. Beurden H. (2011), 'Smart City Dynamics: Inspiring views from experts across Europe', Εκδόσεις HvB Communicative BV
19. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 1392–1393.
20. Boyd Cohen: 'the smart city wheel' – smart circle. (n.d.). Smart-circle.org. Retrieved October 12, 2022, from https://www.smart-circle.org/smart-city/boyd-cohen-smart-city-wheel/
21. Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499–507.

22. Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable Cities and Society, 39, 499–507.
23. Butt, T. A., & Afzaal, M. (2019). Security and privacy in smart cities: Issues and current solutions. In *Smart Technologies and Innovation for a Sustainable Future* (pp. 317–323). Springer International Publishing.
24. Caird, S. (2016). A tale of evaluation and reporting in UK smart cities. https://oro.open.ac.uk/46008/
25. Capra, C. F. (2016). The smart city and its citizens: Governance and citizen participation in Amsterdam Smart City. *International journal of e-planning research*, *5*(1), 20–38.
26. Caputo, A., Marzi, G., & Pellegrini, M. M. (2016). The Internet of Things in manufacturing innovation processes: Development and application of a conceptual framework. Business Process Management Journal, 22(2), 383–402.
27. Caragliu, A., Del Bo, C. and Nijkamp, P. (2011). 'Smart Cities in Europe'. Journal of Urban Technology, 18: 2, pp. 65–82.
28. Caragliu, A., Del Bo, C., Nijkamp, P., 2009. Smart cities in Europe, Serie Research Memoranda 0048, VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics.
29. Cowley, R., & Caprotti, F. (2019). Smart city as anti-planning in the UK. Environment and Planning. D, Society & Space, 37(3), 428–448.
30. Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE Access: Practical Innovations, Open Solutions, 6, 46134–46145.
31. Dameri, R. P. (2013). Searching for smart city definition: a comprehensive proposal. International Journal of Computers & Technology, 11(5), 2544–2551(Council for Innovative Research).
32. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography* (pp. 265–284).
33. Enisa, https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity
34. European Union Agency for Fundamental Rights (FRA) 168/2007: European Union. Retrieved October 15, 2022, from https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=legissum:l14169

35. European Union, 2014. Directorate General For Internal Policies, Policy Department A: Economic and Scientific Policy, European Parliament, Mapping Smart Cities in the EU, authors MANVILLE C. et all, IP/A/ITRE/ST/2013-02, PE 507.480, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(20 14)507480_EN.pdf
36. FS Ferraz, CAG Ferraz, A Gomes - ICSEA 2016, 2016. Smart Cities Security Issues: An Impeding Identity Crisis. Available from: https://tinyurl.com/2p8pmk74
37. Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (Fourthquarter 2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, *19*(4), 2456–2501.
38. Giffender, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., Meijers, E. (2007) "Smart cities: Ranking of European medium-sized cities". Vienna: Centre of Regional Science – Vienna University of Technology, http://www.smart-cities.eu/download/smart_cities_final_report.pdf, 4-11-2017.
39. HaddadPajouh, H., Dehghantanha, A., M. Parizi, R., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things.
40. Hall, P. (2000). 'Creative cities and economic development'. Urban Studies, 37(4), 633-649.
41. Hartley J., (2005), Innovation in governance and public services: Past and present. Public Money & Management, 25(1): 27-34.
42. https://chiefdigitalofficer4london.medium.com/introducing-the-smarter-london-together-report-cards-charting-smart-city-steps-openly-eefc7643eda0
43. https://data.london.gov.uk/
44. https://www.smartlondon.org.uk/
45. IBM Smarter Cities (2012): 'Creating opportunities through leadership and innovation', Εκδόσεις IBM corporation, USA, Διαθέσιμο στην ιστοσελίδα: https://tinyurl.com/4d4546me

46. Ijaz, A., Zhang, L., Grau, M., Mohamed, A., Vural, S., Quddus, A. U., Imran, M. A., Foh, C. H., & Tafazolli, R. (2016). Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations. *IEEE Access: Practical Innovations, Open Solutions*, *4*, 3322–3339.
47. IoT standards & protocols guide. (n.d.). Postscapes. Retrieved October 14, 2022, from https://www.postscapes.com/internet-of-things-protocols/
48. Ishida, T. (2002). Digital city kyoto. Communications of the ACM, 45(7), 76–81. / Komninos, N. (2008). Intelligent cities and globalisation of innovation networks. London: Routledge.
49. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers: A Journal of Research and Innovation, 24(2), 393–414.
50. Jameel, T., Ali, R., & Ali, S. (2019). Security in modern smart cities: An information technology perspective. 2019 2nd International Conference on Communication, Computing and Digital Systems (C-CODE), 293–298.
51. Jameson, S., Richter, C., & Taylor, L. (2019). People's strategies for perceived surveillance in Amsterdam Smart City. *Urban Geography*, *40*(10), 1467–1484.
52. Jeong, Y.-S., & Park, J. H. (2019). IoT and Smart City technology: Challenges, opportunities, and solutions. Journal of Information Processing Systems, 15(2), 233–238.
53. Keyur K Patel, Sunil M Patel, 2016. Department of Electrical Engineering Faculty of Technology and Engineering-MSU, Vadodara, Gujarat, India. Retrieved October 15, 2022, from https://tinyurl.com/mr2mpe98
54. Kourtit, K. P Nijkamp, Smart cities in the innovation age Innovation: The European Journal of Social Science Research 25 (2), 93-95
55. Kummitha, R. K. R., & Crutzen, N. (2017). How do we understand smart cities? An evolutionary perspective. *Cities (London, England)*, *67*, 43–52.
56. Kyriazis, D., & Varvarigou, T. (2013). Smart, autonomous and reliable internet of things. *Procedia Computer Science*, *21*, 442–448.
57. Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, *55*(102023), 102023.

58. Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. Sustainable Cities and Society, 55(102023), 102023.
59. Lucic, D., Boban, M., & Mileta, D. (2018). An impact of general data protection regulation on a smart city concept. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 0390–0394.
60. Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999–8012.
61. Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999–8012.
62. Martinez-Balleste, A., Perez-martinez, P., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136–141.
63. Matatov, N., Rokach, L., & Maimon, O. (2010). Privacy-preserving data mining: A feature set partitioning approach. *Information Sciences*, *180*(14), 2696–2720.
64. Mora, O. B., Rivera, R., Larios, V. M., Beltran-Ramirez, J. R., Maciel, R., & Ochoa, A. (2018). A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures.
65. Musterd, S. and Ostendorf, W. (2004). Creative cultural knowledge cities: Perspectives and planning strategies. Built Environment, 30(3), 188–193.
66. Nowicka, K. (2014). Smart city logistics on cloud computing model. Procedia, Social and Behavioral Sciences, 151, 266–281.
67. Parra-Arnau, J., Rebollo-Monedero, D., & Forné, J. (2014). Measuring the privacy of user profiles in personalized information systems. *Future Generations Computer Systems: FGCS*, *33*, 53–63.
68. Pereira, G. V., Eibl, G., Stylianou, C., Martínez, G., Neophytou, H., & Parycek, P. (2018). The role of smart technologies to support citizen engagement and decision making: The SmartGov case. International Journal of Electronic Government Research, 14(4), 1–17.
69. Popescul, D., & Radu, L. D. (2016). Data Security in Smart Cities: Challenges and Solutions. Informatica Economica, 20(1/2016), 29–38.

70. Pozdniakova, A. M. (2018). Smart city strategies “London-Stockholm-Vienna-Kyiv”: in search of common ground and best practices. Acta Innovations, 27, 31–45.
71. Rawat, D. B., & Ghafoor, K. Z. (2018). *Smart Cities Cybersecurity and privacy*. Elsevier.
72. Retrieved October 15, 2022, from http://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://thesai.org/Downloads/Volume10No6/Paper_11-Internet_of_Things_IOT_Research_Challenges.pdf
73. Rios, P. (2008), ‘Creating “the smart city’, Διαδικτυακό άρθρο στο ‘Udmercyr’, Διαθέσιμο στο: https://archive.udmercy.edu/handle/10429/393
74. Salman, T., & Jain, R. (2019). A survey of protocols and standards for internet of things.
75. Schuler, D. (2002). Digital cities and digital citizens. In: M. Tanabe, P. van den Besselaar, T. Ishida (Eds.), Digital cities II: computational and sociological approaches. LNCS, vol. 2362, (pp. 71–85). Berlin: Springer.
76. Sengan, S., Subramaniyaswamy, Nair, S. K., Indragandhi, Manikandan, & Ravi, L. (2020). Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future Generations Computer Systems: FGCS, 112, 724–737.
77. Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Generations Computer Systems: FGCS*, *107*, 433–442.
78. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.
79. Smart City Security Guideline (Ver 1.0). October, 2020. Ministry of Internal Affiars and Communications, Japan. Retrieved November 18, 2022, from http://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf

80. Song, M. (2020). A case study on energy focused smart city, London of the UK: Based on the framework of "business model innovation." International Journal of Advanced Smart Convergence, 9(2), 8–19.
81. Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. IEEE International Conference on Electronics, Communications and Control (ICECC), pp. 1028– 1031(IEEE Xplore).
82. Theodorou, S., & Sklavos, N. (2019). Blockchain-based security and privacy in smart cities. In D. B. Rawat & K. Z. Ghafoor (Eds.), *Smart Cities Cybersecurity and Privacy* (pp. 21–37).
83. Toh, C. K. (2020). Security for smart cities. IET Smart Cities, 2(2), 95–104.
84. United Nations, 2018 revision of world urbanization prospects. (n.d.). Www.un.org. Retrieved October 12, 2022, from https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html
85. Van den Bergh, J., & Viaene, S. (2015). Key challenges for the smart city: Turning ambition into reality. 2015 48th Hawaii International Conference on System Sciences, 2385–2394.
86. Vinod Kumar, T. M., & Dahiya, B. (2017). Smart Economy in Smart Cities. In Smart Economy in Smart Cities (pp. 3–76).
87. Vojkovic, G. (2018). Will the GDPR slow down development of smart cities? 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1295–1297.
88. Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law and Security Report, 26(1), 23–30.
89. Willems, J., Van den Bergh, J., & Viaene, S. (2017). Smart city projects and citizen participation: The case of London. In Public Sector Management in a Globalized World (pp. 249–266).
90. Yang, L., Elisa, N., & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In D. B. Rawat & K. Z. Ghafoor (Eds.), *Smart Cities Cybersecurity and Privacy* (pp. 89–102).
91. Yigitcanlar, T. (2006). Australian local governments' practice and prospects with online planning. URISA Journal, 18(2), 7–17.

92. Zvolska, L., Lehner, M., Voytenko Palgan, Y., Mont, O., & Plepys, A. (2019). Urban sharing in smart cities: the cases of Berlin and London. Local Environment, 24(7), 628–645.
93. Εθνικό Πλαίσιο Αξιολόγησης Ικανοτήτων, 2000, https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-el.pdf
94. Ευρωπαϊκή Ένωση, 2013, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0526&from=
95. Ζαχαροπούλου, Μ. (2020). Έξυπνες πόλεις και τεχνολογίες διασυνδεδεμένων συσκευών. Πανεπιστήμιο Πειραιώς.
96. Κοσμόπουλος, Λ. (2016, October 20). Έρευνα: Οι έξυπνες πόλεις είναι εκτεθειμένες σε κυβερνοεπιθέσεις. Autonomous.gr. https://www.autonomous.gr/smart-cities-have-no-cybersecurity-research-says-9124/
97. Κυβερνοεπιθέσεις μπορούν να κάνουν τις έξυπνες πόλεις… χαζές. (2019, September 12). TVXS - TV Χωρίς Σύνορα. https://tvxs.gr/news/kosmos/kybernoepitheseis-mporoyn-na-kanoyn-tis-eksypnes-poleis-xazes
98. Μενεγάτος, Α. (2021). Ζητήματα ασφάλειας και ιδιωτικότητας σε περιβάλλοντα έξυπνων μεταφορών. Πανεπιστήμιο Πειραιώς.
99. Παντελίδης Π., *Η έννοια της έξυπνης πόλης*, αδημ. Διπλωματική εργασία, Βόλος 2017.
100. Παντελοπούλου, Δ. (2021). Έξυπνες πόλεις και παράγοντες που επηρεάζουν την ανάπτυξή τους. https://hellanicus.lib.aegean.gr/handle/11610/23117.
101. Σύνταγμα. (n.d.). Hellenicparliament.gr. Retrieved October 15, 2022, from https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/
102. Τα δικαιώματά μου στο πλαίσιο του ΓΚΠΔ, 2022. (n.d.). dpa.gr. Retrieved October 15, 2022, from https://www.dpa.gr/polites/gkpd
103. Τσανή, Σ. (2021). Μελέτη και ανάλυση παραβιάσεων ιδιωτικότητας σε περιβάλλοντα έξυπνων σπιτιών και έξυπνων πόλεων. Πανεπιστήμιο Μακεδονίας.