ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Προκλήσεις Ασφάλειας και Κυβερνοέγκλημα σε Κρίσιμες Υποδομές

Δημήτριος Χριστόπουλος
Α.Μ. 18033

Εισηγητής: Δημήτριος Καλλέργης, Λέκτορας Εφ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Προκλήσεις Ασφάλειας και Κυβερνοέγκλημα σε Κρίσιμες Υποδομές

Δημήτριος Χριστόπουλος
Α.Μ. 18033

Τριμελής εξεταστική επιτροπή

1. **<u>Επιβλέπων καθηγητής</u>: Δημήτριος Καλλέργης**, Λέκτορας Εφ. Πανεπιστημίου Δυτικής Αττικής

   Digitally signed by Dimitrios Kallergis
   Date: 2021.07.12 18:39:14 +03'00'

2. **<u>Μέλος</u>: Αντώνιος Μπόγρης,** Καθηγητής Πανεπιστημίου Δυτικής Αττικής

   Antonios Bogris Digitally signed by Antonios Bogris
   Date: 2021.07.13 15:07:49 +03'00'

3. **<u>Μέλος</u>: Ιωάννα Καντζάβελου**, Επίκ. Καθηγήτρια Πανεπιστημίου Δυτικής Αττικής

   Ioanna Kantzavelou Digitally signed by Ioanna Kantzavelou
   Date: 2021.07.13 12:33:13 +03'00'

Αθήνα, 12 Ιουλίου 2021

Δήλωση περί μη λογοκλοπής

Δηλώνω ότι είμαι ο συγγραφέας της παρούσας εργασίας με τίτλο:

«**Προκλήσεις Ασφάλειας και Κυβερνοέγκλημα σε Κρίσιμες Υποδομές**»

και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς, είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 30.06.2022 και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο Δηλών

Digitally signed by Dimitrios Kallergis
Date: 2021.07.12 18:39:46 +03'00'

Δημήτριος Χριστόπουλος

Αριθμός Μητρώου : 18033

Ημερομηνία : 12 Ιουλίου 2021

Περίληψη

Η ψηφιακή εποχή επηρεάζει την καθημερινή ζωή του ανθρώπου, τα θεμελιώδη δικαιώματά του, τις κοινωνικές αλληλεπιδράσεις και τις οικονομίες. Καθώς συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) χρησιμοποιούνται για τη σωστή λειτουργία των Υποδομών Ζωτικής Σημασίας, ευνοείται η εμφάνιση κινδύνων και απειλών στον κυβερνοχώρο. Σημαντικό ρόλο για την επίτευξη της ασφάλειας του κυβερνοχώρου έχουν οι κυβερνήσεις, οι οποίες αναπτύσσουν την ασφάλεια εισάγοντας κανονισμούς, στρατηγικές και μέτρα ασφαλείας. Στην παρούσα εργασία, αφού οριστεί η έννοια των Υποδομών Ζωτικής Σημασίας και πώς αυτές λειτουργούν με συστήματα που περιλαμβάνουν ΤΠΕ, περιγράφονται διάφορες προκλήσεις ασφάλειας και τα μέτρα που πρέπει να λαμβάνονται για την αντιμετώπισή τους. Επίσης, μελετώνται τα πρότυπα ασφάλειας που ισχύουν για την Ευρωπαϊκή Ένωση και συνεπώς την Ελλάδα, τις Η.Π.Α, την Κίνα και την Ρωσία καθώς και συμβάντα επιθέσεων σε τομείς κρίσιμων υποδομών στις χώρες αυτές. Τέλος, πραγματοποιείται συγκριτική αποτίμηση των συμβάντων κυβερνοεγκλήματος στις τέσσερις περιοχές μελέτης, εξάγονται χρήσιμα συμπεράσματα και διαμορφώνονται συγκεκριμένες προτάσεις προς μελλοντική έρευνα, με σκοπό να συνεισφέρουν σε βελτιώσεις των συστημάτων ασφαλείας των Υποδομών Ζωτικής Σημασίας.

Abstract

The digital era affects fundamental rights, social interactions, and economies. Cyberthreats emerge as Information and Communication Technologies (ICT) systems are utilised for the proper operation of Critical Infrastructures. An important and recognised role in achieving cybersecurity is adopted by governments, which develop security by introducing regulations, strategies, and other security measures. In this postgraduate thesis, following the definition of the concept of Critical Infrastructure and how they work with systems that include ICT, various security challenges are described as well as the measures that need to be taken in order to address them. Furthermore, the security standards that apply to the European Union (and therefore Greece), USA, China and Russia are studied, as well as incidents of attacks on critical infrastructure sectors in these countries. Finally, as a result of a comparative assessment of cybercrime incidents in these four study areas, useful conclusions are drawn, and specific proposals are formulated for future research in order to contribute to improvements in the security systems of critical infrastructures.

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ ιδιαιτέρως, τον επιβλέποντα καθηγητή μου, Λέκτορα Εφ. κ. Δημήτριο Καλλέργη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα και την επιστημονική του καθοδήγηση, τις υποδείξεις του, την επιμονή του και το αμείωτο ενδιαφέρον του από την αρχή μέχρι το τέλος.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για όλη τη στήριξη, τη συμπαράσταση και την κατανόησή της, καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας περιεχομένων

Περίληψη 4

Abstract 5

Ευχαριστίες 6

Πίνακας περιεχομένων 7

Κατάλογος Εικόνων 8

Κατάλογος Πινάκων 8

Κεφάλαιο 1 - Εισαγωγή 9

1.1 Πρόλογος 9

1.2 Σκοπός και Αντικείμενο Μελέτης 11

1.3 Δομή Μεταπτυχιακής Εργασίας 12

Κεφάλαιο 2 - Κρίσιμες Υποδομές και Εισαγωγή Νέων Τεχνολογιών 13

2.1 Κρίσιμες Υποδομές 13

2.2 Διαδίκτυο των Πραγμάτων και Έξυπνο Πλέγμα 15

2.2.1 Διαδίκτυο των Πραγμάτων (IoT) 15

2.2.2 Έξυπνο Πλέγμα 20

2.3 Νέες Τεχνολογίες στις Κρίσιμες Υποδομές και IoT Πλαίσιο Ασφαλείας για Έξυπνες Υποδομές 22

Κεφάλαιο 3 - Κυβερνοέγκλημα 28

3.1 Κυβερνοέγκλημα στο IoT 28

3.2 Πολιτική Κυβερνοασφάλειας IoT [6] [13] 29

3.3 Κυβερνοέγκλημα και Σχέδιο Δράσης για την Ασφάλεια στον Κυβερνοχώρο και την Εθνική Ασφάλεια στις Διάφορες Κυβερνήσεις 30

3.3.1 Στρατηγικές για την Ασφάλεια στον Κυβερνοχώρο των eUnations [13] 31

3.3.2 Σχέδιο Δράσης για την Εθνική Ασφάλεια στον Κυβερνοχώρο (Ελλάδα) [16] 32

3.3.3 Σχέδιο Δράσης Ηνωμένων Πολιτειών Αμερικής [14] 36

3.3.4 Σχέδιο Δράσης Κίνας 38

3.3.5 Σχέδιο Δράσης Ρωσίας [18] 40

3.4 Κυβερνοέγκλημα σε Εθνικές Κυβερνήσεις και Διεθνείς Οργανισμούς [19] 41

3.4.1 Ασφάλεια Στρατιωτικού Τομέα [19] 41

3.4.2 Ασφάλεια Κυβερνοχώρου για Επιχειρήσεις 42

3.4.3 Ασφάλεια Κυβερνοχώρου για Κυβερνητικά Ιδρύματα [19] 43

3.5 Σημασία της Ασφάλειας στον Κυβερνοχώρο [21] 43

3.5.1 Κυβερνητικές Προσπάθειες για την Πρόληψη του Εγκλήματος στον Κυβερνοχώρο 44

Κεφάλαιο 4 - Κυβερνητική Ασφάλεια για Υποδομές Ζωτικής Σημασίας: Μοντελοποίηση Επίθεσης και Άμυνας 48

4.1 SCADA (Supervisory Control and Data Acquisition) Πλαίσιο Ασφαλείας 48

4.1.1 Παρακολούθηση σε Πραγματικό χρόνο [22] 53

4.1.2 Ανίχνευση Ανωμαλιών και Ανάλυση Επιπτώσεων [22] 54

4.1.3 Στρατηγικές Μετριασμού [22] 56

4.2 Μοντελοποίηση Επίθεσης Δέντρου [22] 57

Κεφάλαιο 5 - Συγκριτική Αποτίμηση – Συμπεράσματα 59

5.1 Συγκριτική Αποτίμηση 59

5.2 Συμπεράσματα 60

Κεφάλαιο 6 - Μελλοντική Εργασία – Επίλογος 64

6.1 Μελλοντική Εργασία 64

6.2 Επίλογος 65

Βιβλιογραφία 66

Κατάλογος Εικόνων

Εικόνα 1. IoT Αρχιτεκτονική [5] 18

Εικόνα 2. Έξι Βασικά Στοιχεία του IoT [11] 19

Εικόνα 3. Γενική Αρχιτεκτονική SCADA σε περιβάλλον IoT-Cloud 49

Εικόνα 4. Τομείς εφαρμογών συστημάτων SCADA 49

Εικόνα 5. Η εξέλιξη των συστημάτων SCADA 53

Εικόνα 6. Φύλλα επίθεσης με κόμβους“AND” και “OR”. (α) Φύλλο επίθεσης με κόμβο “AND”. (β) Φύλλο επίθεσης με κόμβο “OR”. 57

Κατάλογος Πινάκων

Πίνακας 1. Κανόνες για τις συνθήκες 1, 2 και 3 58

Πίνακας 2. Συγκριτική Αποτίμηση Συμβάντων Μελέτης 59

Κεφάλαιο 1 - Εισαγωγή

1.1 Πρόλογος

Η ανάπτυξη του διαδικτύου έχει διαμορφώσει εντελώς την καθημερινότητα για όλους τους πολίτες των ανεπτυγμένων κρατών, δημιουργώντας πληθώρα νέων ευκαιριών. Στον κυβερνοχώρο μπορούν να πραγματοποιηθούν δραστηριότητες και συναλλαγές που να αφορούν π.χ. στην διαχείριση οικονομικών πόρων, στο διεθνές εμπόριο, στις δημόσιες υπηρεσίες κ.α. Η εξέλιξη στην ψηφιακή εποχή επηρεάζει σημαντικά την ασφάλεια στον κυβερνοχώρο. Οι κυβερνοεπιθέσεις ή τα κυβερνοεγκλήματα που διαπράττονται στον κυβερνοχώρο, αυξάνονται εκθετικά και γίνονται όλο και πιο σύνθετα με αποτέλεσμα να θέτουν σε κίνδυνο την λειτουργικότητα κρίσιμων υποδομών που παρέχουν απαραίτητες υπηρεσίες για την εύρυθμη λειτουργία της κοινωνίας.

Με τον όρο κρίσιμες υποδομές περιγράφονται οι υποδομές και οι υπηρεσίες των οποίων, εάν η ομαλή δραστηριότητα διαταραχθεί, αναμένεται να υπάρξουν σημαντικές επιπτώσεις στην εύρυθμη λειτουργία του κρατικού μηχανισμού και της ζωής των πολιτών. Παραδείγματα κρίσιμων υποδομών συναντάμε πολλά, όπως είναι τα *δίκτυα ενέργειας και μεταφοράς*, *οι δομές υγείας*, οι *ψηφιακές υποδομές, κυβερνητικά ιδρύματα και επιχειρήσεις κ.α*. Λόγω της παγκόσμιας φύσης του διαδικτύου, συμβάντα κυβερνοεγκλήματος υπερβαίνουν τα εθνικά σύνορα και το αντίκτυπο μπορεί να είναι παγκόσμιας κλίμακας.

Η επιτακτική ανάγκη ασφάλειας στον κυβερνοχώρο, οδήγησε στην δημιουργία ειδικών συστημάτων ασφάλειας, προκειμένου να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων. Οι μέθοδοι, τα εργαλεία και οι τεχνολογίες, πάνω στις οποίες στηρίζονται τα συστήματα αυτά, εξελίσσονται συνεχώς ώστε να ανταποκρίνονται στις ολοένα και αυξανόμενες απαιτήσεις της ραγδαίας εξέλιξης της τεχνολογίας, για την αντιμετώπιση των προκλήσεων που συνεχώς ανακύπτουν.

Επειδή οι κρίσιμες υποδομές διαφέρουν για κάθε κράτος και επειδή κάθε κράτος πρέπει να είναι σε θέση να αντιμετωπίσει τους κινδύνους ασφάλειας που ελλοχεύουν για τις δικές του κρίσιμες υποδομές, έχουν θεσπιστεί νομικά πλαίσια με συγκεκριμένες προδιαγραφές, διαδικασίες, μέτρα και οδηγίες, με την συνεργασία των εμπλεκόμενων φορέων. Όσον αφορά στο τεχνολογικό επίπεδο συστημάτων ασφάλειας των υποδομών, εφαρμόζονται διάφορες λύσεις λογισμικών με εξειδίκευση σε μεθόδους

κρυπτογράφησης ώστε να εξασφαλίζεται η ακεραιότητα των πληροφοριών. Παρακάτω, περιγράφουμε εν συντομία τα πρότυπα ασφάλειας που ισχύουν για την Ευρωπαϊκή Ένωση, τις Η.Π.Α, την Κίνα και την Ρωσία. Εκτενέστερα θα αναφερθούμε σε κεφάλαιο της παρούσης εργασίας.

Η **Ευρωπαϊκή Ένωση** αντιλήφθηκε γρήγορα, πως η ασφάλεια των συστημάτων ασφαλείας και των πληροφοριών, παίζουν σημαντικό ρόλο για αυτό και δημιούργησε τον **ENISA**. Ο ENISA ενδυναμώνει την δυνατότητα των κρατών μελών της Ε.Ε. να διευθύνουν και να ανταποκρίνονται στα προβλήματα που αφορούν στην ασφάλεια των δικτύων και των πληροφοριών. Αποτελεί ένα κέντρο εμπειρογνωμοσύνης σε θέματα ασφάλειας των Δικτύων και προωθεί την συνεργασία ανάμεσα στον ιδιωτικό και δημόσιο τομέα.

Στην **Αμερική** ιδρύθηκε η **Cisa** (**C**ybersecurity **and I**nfrastructure **S**ecurity **A**gency). Μια αυτόνομη ομοσπονδιακή υπηρεσία, υπό την εποπτεία του Υπουργείου Εσωτερικής Ασφάλειας(DHS). Οι δραστηριότητές της αποτελούν συνέχεια της Διεύθυνσης Εθνικής Προστασίας και Προγραμμάτων (NPPD). Ο ρόλος της CISA είναι να βελτιώσει την ασφάλεια στον κυβερνοχώρο σε όλα τα επίπεδα της κυβέρνησης, να συντονίσει τα προγράμματα ασφάλειας στον κυβερνοχώρο με τα κράτη και να βελτιώσει την προστασία της κυβέρνησης από την ασφάλεια του κυβερνοχώρου έναντι ιδιωτών και εθνικών χάκερ.

Στην **Κίνα** ιδρύθηκε το **CAC** (Cyberspace Administration of China). Σύμφωνα με σχέδιο νόμου, το CAC είναι υπεύθυνο για την ασφάλεια στον κυβερνοχώρο και συνεργάζεται με άλλες κινεζικές ρυθμιστικές αρχές για τη διαμόρφωση ενός καταλόγου "βασικού εξοπλισμού δικτύου" και "εξειδικευμένων προϊόντων ασφάλειας δικτύων" για πιστοποίηση. Η CAC συμμετέχει επίσης στην αναθεώρηση της προμήθειας προϊόντων ή υπηρεσιών δικτύου για λόγους εθνικής ασφάλειας. Τα δεδομένα που αποθηκεύονται εκτός Κίνας από κινεζικές εταιρείες πρέπει επίσης να υποβληθούν σε έγκριση της CAC.

Η FSB ή FSS είναι η Ομοσπονδιακή Υπηρεσία Ασφαλείας της **Ρωσικής Ομοσπονδίας**. Η FSS είναι κυρίως υπεύθυνη για την εσωτερική ασφάλεια του ρωσικού κράτους. Πρωταρχική ευθύνη αποτελεί η υπερεθνική κατασκοπία για την καταπολέμηση του οργανωμένου εγκλήματος, της τρομοκρατίας, του λαθρεμπορίου, ναρκωτικών κ.α. Η FSS είναι αυτή που καθοδηγεί όλες τις υπηρεσίες επιβολής του νόμου και της υπηρεσίες πληροφοριών στην Ρωσία.

Παρόλο που η σωστή χρήση των προτύπων ασφαλείας στον κυβερνοχώρο ωφελεί σίγουρα την επίτευξη μιας ισχυρής προσέγγισης ασφάλειας, εξακολουθούν να υπάρχουν αρκετές προκλήσεις που πρέπει να αντιμετωπιστούν στην πράξη. Ορισμένες από αυτές τις προκλήσεις αφορούν στους τομείς:

- Αρχιτεκτονικής(επίπεδο αντίληψης εφαρμογής, δικτύου)
- Threat vector (φυσικές επιθέσεις, επιθέσεις επικοινωνίας, επιθέσεις λογισμικών)
- Εμπιστευτικότητα (Απόρρητο, διαθεσιμότητα, αξιοπιστία)
- Συμμόρφωση (Έλεγχος πολιτικής απορρήτου, κυβερνητική επίβλεψη, μη κυβερνητική επίβλεψη)

Ορισμένες λύσεις που εξετάζονται για να μετριάσουν το πρόβλημα των προκλήσεων, είναι μεταξύ άλλων η δημιουργία Firewalls, τα συστήματα ανίχνευσης (IDS), τα συστήματα πρόληψης εισβολών (IPS), η χρήση λογισμικών προστασίας από ιούς και η κρυπτογράφηση.

1.2 Σκοπός και Αντικείμενο Μελέτης

Σκοπός αυτής της μεταπτυχιακής διατριβής είναι να διερευνηθούν οι προκλήσεις ασφάλειας και τα συμβάντα κυβερνοεγκλήματος σε κρίσιμες υποδομές (critical infrastructures).

Οι κρίσιμες υποδομές που θα εξεταστούν, αφορούν στα δίκτυα ενέργειας και μεταφοράς και γενικά σε ψηφιακές υποδομές, όπως αυτές ισχύουν στην χώρα μας, στην Ευρωπαϊκή Ένωση, στην Αμερική, στην Κίνα και στην Ρωσία. Επιλέχθηκαν οι συγκεκριμένες χώρες καθώς έχουν τον μεγαλύτερο στρατηγικό αντίκτυπο παγκοσμίως.

Αντικείμενο της μελέτης είναι να δοθεί έμφαση στα τεχνικά χαρακτηριστικά των συστημάτων και των τεχνικών που ακολουθούνται στις απόπειρες κακόβουλης επίθεσης από κυβερνοεγκληματίες, αφήνοντας εκτός μελέτης τις υπόλοιπες συνιστώσες που εμπίπτουν σε άλλα γνωστικά πεδία (π.χ. το νομικό πλαίσιο). Θα εξετάσουμε τα κενά των συστημάτων αυτών και θα αναλύσουμε τις προτεινόμενες λύσεις που απαιτούνται για την κάλυψη των κενών αυτών.

1.3 Δομή Μεταπτυχιακής Εργασίας

Η μεθοδολογική προσέγγιση για την εκπόνηση της παρούσας εργασίας, θεμελιώνεται πάνω στην συλλογή δεδομένων από ένα σύνολο έγκριτων επιστημονικών άρθρων, γύρω από δύο κεντρικούς άξονες: τις κρίσιμες υποδομές αφενός και ένα σύνολο αλληλοσυνδεόμενων εννοιών αφετέρου, την έννοια της κυβερνοασφάλειας, της κυβερνοεπίθεσης, του κυβερνογκληματία και άλλες αντίστοιχες. Τα άρθρα που κάλυπταν σε μεγάλο βαθμό διάφορες πτυχές του θέματος, αφού μελετήθηκαν, έγινε μία ποιοτική συσχέτιση ώστε να δοθεί απάντηση στο ερώτημα που καλείται να απαντήσει η μεταπτυχιακή διατριβή, σχετικά με το ποιες είναι οι προκλήσεις ασφαλείας και η φύση του κυβερνοεγκλήματος για τις κρίσιμες υποδομές.

Στο **κεφάλαιο 1** αναφέρονται το πλαίσιο και οι ερευνητικοί στόχοι της εργασίας.

Στο **κεφάλαιο 2** περιγράφονται οι Κρίσιμες Υποδομές, πώς ο χώρος του διαδικτύου των αντικειμένων εντάσσεται μέσα σε αυτές και γενικά πώς οι Κρίσιμες Υποδομές αξιοποιούν τις καινοτομίες που φέρνουν οι νέες τεχνολογίες.

Στο **κεφάλαιο 3**, αφού οριστεί τι θεωρείται Κυβερνοέγκλημα, θα αναφερθεί η επίδραση αυτού και η αντιμετώπιση του σε τέσσερις περιοχές μελέτης (ΕΕ, Η.Π.Α., Ρωσία, Κίνα) περιγράφοντας συμβάντα Κυβερνοεγκλήματος για τρείς διαφορετικούς τομείς (Στρατιωτικός Τομέας, Επιχειρήσεις, Κυβερνητικά Ιδρύματα).

Στο **κεφάλαιο 4** αναλύεται η αρχιτεκτονική του μοντέλου SCADA σε Κρίσιμες Υποδομές καθώς αποτελεί μια πολύ σημαντική τεχνολογική περίπτωση εφαρμογής. Επίσης καταγράφονται οι τύποι επιθέσεων, με ποιες μεθόδους ανιχνεύονται και αναλύονται ώστε να προκύψουν οι στρατηγικές πρόληψης και μετριασμού για τα μοντέλα αυτά.

Στο **κεφάλαιο 5** παρουσιάζεται η συγκριτική αποτίμηση των συμβάντων κυβερνοεγκλήματος στις περιοχές μελέτης που αναλύθηκαν στο κεφάλαιο 3. Επιπλέον, παρατίθενται τα συμπεράσματα που ανακύπτουν από τη μελέτη αυτή και παρατίθενται λίστες προτάσεων για την προαγωγή της κυβερνοασφάλειας στο νέφος –ιδίως για τα συστήματα υποδομών ζωτικής σημασίας– αλλά και τη διευκόλυνση της εγκληματολογικής έρευνας σε αυτό. Συγκεκριμένα παρατίθεται μια λίστα προτάσεων για τεχνικά ζητήματα και μια αντίστοιχη για θεσμικά ζητήματα.

Στο **κεφάλαιο 6** παρατίθεται μια σειρά από προτάσεις προς μελλοντική έρευνα και η μελέτη ολοκληρώνεται με τον Επίλογο.

Κεφάλαιο 2 - Κρίσιμες Υποδομές και Εισαγωγή Νέων Τεχνολογιών

2.1 Κρίσιμες Υποδομές

Ο προσδιορισμός του όρου Κρίσιμων Υποδομών έχει καταστεί κορυφαία προτεραιότητα για κυβερνήσεις και οργανισμούς και αποτελεί κρίσιμο στοιχείο για μία υγιή πολιτική ασφάλεια στον κυβερνοχώρο.

Ως κρίσιμες υποδομές (Critical Infrastructures - CI) ορίζονται τα συστήματα ή μέρη αυτών, τα οποία είναι απαραίτητα για την διατήρηση ζωτικών κοινωνικών λειτουργιών, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των ανθρώπων. Μία ενδεχόμενη διακοπή ή αποτυχία της λειτουργίας των συστημάτων αυτών, θα είχε ως αποτέλεσμα την καταστροφή τους, συνεπώς το αντίκτυπο στην ζωή και την υγεία του πληθυσμού θα ήταν σημαντικό [1]. Θα μπορούσε κανείς να συγκρίνει τις κρίσιμες υποδομές με τα ζωτικά όργανα του ανθρώπου, τα οποία πρέπει να είναι στη θέση τους για να εξασφαλίζεται η υγεία του [2].

Οι κρίσιμες υποδομές ενός κράτους είναι οι φυσικοί, μη φυσικοί και κυβερνητικοί πόροι ή υπηρεσίες που είναι θεμελιώδεις για την ελάχιστη λειτουργία μιας κοινωνίας και της οικονομίας της [2].

Τα κρίσιμα συστήματα υποδομής (CIS) μπορούν να χωριστούν σε δύο τομείς ανάλογα με τις λειτουργικές τους ιδιαιτερότητες: τεχνικές και κοινωνικοοικονομικές υποδομές. Η αλληλεξάρτηση μεταξύ αυτών των τομέων υποδομής, είναι σημαντική καθώς όλοι οι τομείς της κοινωνικοοικονομικής περιοχής απαιτούν τις απεριόριστες δυνατότητες διάθεσης υπηρεσιών σε τομείς τεχνικής υποδομής και, αντιθέτως, οι τομείς τεχνικής υποδομής - σε περίπτωση κρίσης - εξαρτώνται πλήρως από τις υπηρεσίες κοινωνικοοικονομικών τομέων [3]. Τα δίκτυα ενέργειας καθώς και τα δίκτυα μεταφοράς στο σύνολό τους, οι τράπεζες, οι χρηματοοικονομικές αγορές, η υγεία, τα δίκτυα ύδρευσης και οι ψηφιακές υποδομές, αποτελούν τους τομείς που συμπεριλαμβάνουν υποδομές και υπηρεσίες που εντάσσονται στις κρίσιμες υποδομές. Τα συστήματα και οι εφαρμογές των τομέων αυτών, εγκαθίστανται, αναπτύσσονται και διαχειρίζονται λαμβάνοντας υπόψη τις αρχές της ασφάλειας “από τον σχεδιασμό”, οι οποίες τηρούνται σε όλο τον κύκλο της ζωής τους. Συνεπώς διασφαλίζεται και η συντήρηση τους.

Οι χειριστές και οι ιδιοκτήτες των υποδομών είναι υπεύθυνοι για την σταθερότητα και την ασφάλεια των συστημάτων τόσο τεχνικά όσο και φροντίζοντας την οργανική

ανθεκτικότητα τους. Η διαχείριση της οργανικής ανθεκτικότητας συνίσταται κυρίως στη συνεχή αξιολόγηση των υποδομών, προκειμένου να εντοπίζονται αδύνατα σημεία νωρίς, ώστε να μπορούν να ληφθούν εγκαίρως επαρκή μέτρα ασφαλείας για την ενίσχυσή τους [1].

Το ενδεχόμενο επιτυχής επίθεσης σε κρίσιμες υποδομές μπορεί να οδηγήσει σε μια καταστροφική οικονομία και κοινωνία των χωρών. Μια επίθεση που εξαρτάται από τον κυβερνοχώρο, όπως οι παράνομες εισβολές σε δίκτυα υπολογιστών και η διακοπή της λειτουργικότητας του υπολογιστή και του χώρου του δικτύου, είναι οι πιο συνηθισμένοι τρόποι επίθεσης που ποικίλλουν στο πεδίο εφαρμογής και αυτές είναι οι μεγάλες προκλήσεις που πρέπει να επιλυθούν σε κρίσιμες υποδομές [4]. Οι τρεις τομείς αξιοπιστίας της ασφάλειας (Προβλεπόμενη λειτουργικότητα, λειτουργική ασφάλεια και ασφάλεια στον κυβερνοχώρο) είναι ζωτικής σημασίας για την επίλυση των προκλήσεων που αντιμετωπίζει η κρίσιμη ασφάλεια των υποδομών [4].

Οι τύποι επιθέσεων σε κρίσιμες υποδομές μπορούν να διακριθούν με βάση τα μέσα επίθεσης [2]:
α)Σε απλές επιθέσεις στον κυβερνοχώρο με φυσικό συστατικό
β)Με βάση την έκβαση της ζημίας, η οποία μπορεί να είναι είτε φυσική είτε λειτουργική.

Οι κρίσιμες υποδομές που θα εξεταστούν σε αυτή την μεταπτυχιακή διατριβή, αφορούν στον τομέα της υγείας, της δικτύων ενέργειας και μεταφορών καθώς επίσης και των ψηφιακών υποδομών, όπως αυτές ισχύουν στην χώρα μας, στην Ευρωπαϊκή Ένωση, στις Η.Π.Α, στην Κίνα και στην Ρωσία. Επιλέχθηκαν οι συγκεκριμένες χώρες καθώς έχουν τον μεγαλύτερο στρατηγικό αντίκτυπο παγκοσμίως.

Εν συντομία περιγράφοντας τους τομείς αυτούς:

- ***Τομέας Υγεία***

Στον τομέα της υγείας, οι κρίσιμες υποδομές έχουν να κάνουν με υπηρεσίες που διασφαλίζουν την εύρυθμη λειτουργία της επείγουσας περίθαλψης, της νοσοκομειακής περίθαλψης, του εφοδιασμού και της διάθεσης φαρμάκων, εμβολίων, αίματος και ιατρικών προμηθειών καθώς και τον έλεγχο λοιμώξεων και επιδημιών.

- ***Τομέας Δικτύων Ενέργειας***

Στον τομέα των Δικτύων Ενέργειας, οι κρίσιμες υποδομές αφορούν στα συστήματα εκείνα που διασφαλίζουν την αγορά ή την παραγωγή, την διανομή-μεταφορά και την αποθήκευση της Ηλεκτρικής Ενέργειας, του Πετρελαίου και του Φυσικού Αερίου.

- ***Τομέας Δικτύων Μεταφορών***

Στον τομέα των Δικτύων Μεταφοράς, οι κρίσιμες υποδομές αφορούν σε υπηρεσίες ελέγχου, διαχείρισης και συντήρησης των δικτύων αερομεταφοράς, των οδικών μεταφορών, της ναυσιπλοΐας, των σιδηροδρομικών μεταφορών καθώς και των ταχυδρομικών μεταφορών.

- ***Τομέας Δικτύων Ψηφιακών Υποδομών.***

Στον τομέα των Ψηφιακών Υποδομών, τις κρίσιμες υποδομές αποτελούν οι υπηρεσίες Διαδικτύου-Web, οι υπηρεσίες Cloud, οι υπηρεσίες λογισμικού (SaaS) και γενικά όλες οι υπηρεσίες που αφορούν στις Τεχνολογίες Πληροφορικής & Επικοινωνιών (ΤΠΕ).

Όλα τα συστήματα που περιλαμβάνονται σε κρίσιμες υποδομές βασίζονται σε δίκτυα και υπηρεσίες ΤΠΕ, συνεπώς οι κοινωνίες εξαρτώνται όλο και περισσότερο από τα δημόσια δίκτυα ΤΠΕ και τις υπηρεσίες τους. Μείζον θέμα εθνικής ασφάλειας είναι η εξασφάλιση όσον αφορά στην σταθερότητα, στην ασφάλεια και στην ανθεκτικότητα.

2.2 Διαδίκτυο των Πραγμάτων και Έξυπνο Πλέγμα

2.2.1 Διαδίκτυο των Πραγμάτων (IoT)

Διανύοντας την ψηφιακή επανάσταση με την ραγδαία εξέλιξη της τεχνολογίας, η κοινωνία μας έχει επηρεαστεί σημαντικά σε όλους τους τομείς της. Ένα σημαντικό στάδιο στην ψηφιακή επανάσταση αποτελεί το «Internet of Things-IoT» [5].

Το IoT - Διαδίκτυο των Πραγμάτων, είναι ένα δίκτυο στο οποίο μπορεί να έχει πρόσβαση ένας μεγάλος ή μικρός αριθμών συσκευών που διαθέτουν ενσωματωμένους αισθητήρες, με την δυνατότητα να συνδέονται μεταξύ τους ανταλλάσσοντας πληροφορίες και δεδομένα. Οι συσκευές IoT είναι εξοπλισμένες με αισθητήρες και ισχύ επεξεργασίας που τις επιτρέπουν να αναπτυχθούν σε πολλά περιβάλλοντα [5].

Η βελτίωση της ποιότητας των υπηρεσιών που παρέχονται στους ανθρώπους, η ανάπτυξη της χρήσης δημοσίων πόρων και η μείωση του λειτουργικού κόστους των υπηρεσιών αποτελούν το κίνητρο για την δημιουργία του IoT. Βασικός στόχος όμως παραμένει η καλυτέρευση της ποιότητας της ζωής του ανθρώπου [5].

Επειδή το IoT χρησιμοποιείται συχνά σε τομείς που ανήκουν στις κρίσιμες υποδομές π.χ. υγειονομική περίθαλψη, δίκτυα ενέργειας και μεταφορών κ.α. , θα πρέπει να εξασφαλίζεται η ασφάλεια των πληροφοριών του δικτύου με ταυτοποίηση, εμπιστευτικότητα και ακεραιότητα [5].

Θεωρώντας δεδομένο ότι η ουσία του IoT είναι η διασύνδεση του φυσικού κόσμου των πραγμάτων με το Διαδίκτυο, οι πλατφόρμες λογισμικού και υλικού καθώς και τα πρότυπα που χρησιμοποιούνται συνήθως για την ενεργοποίηση αυτής της διασύνδεσης μπορεί να καταστούν πυρήνας ενός οικοσυστήματος IoT [6]. Λόγω των δισεκατομμυρίων συνδεδεμένων συσκευών, υπάρχει μεγάλος κίνδυνος κλοπής ταυτότητας και δεδομένων, χειραγώγησης συσκευών, παραποίησης δεδομένων, χειραγώγησης διακομιστή / δικτύου και επακόλουθου αντίκτυπου στις πλατφόρμες εφαρμογών. Ενώ ο αριθμός αυτών των διασυνδεδεμένων συσκευών συνεχίζει να αυξάνεται καθημερινά, το ίδιο ισχύει και για τον αριθμό των απειλών ασφαλείας και των ευπαθειών που τίθενται σε αυτές τις συσκευές. . Ένα από τα πιο βασικά ζητήματα έρευνας στην τεχνολογία του IoT είναι η ασφάλεια. Η ασφάλεια έχει πολλές πτυχές - ασφάλεια ενσωματωμένη στη συσκευή, ασφάλεια μετάδοσης δεδομένων και αποθήκευση δεδομένων εντός των συστημάτων και των εφαρμογών της [7]. Η ασφάλεια του IoT περιλαμβάνει ένα ευρύ φάσμα εργασιών όπως την ενσωμάτωση υλικού κλειδώματος στην κατασκευή της συσκευής αλλά και στην λειτουργία της, τον έλεγχο πρόσβασης σε δίκτυα και υπηρεσίες, την εξασφάλιση διαδικασιών ανάπτυξης λογισμικού, την διαχείριση ενημερώσεων λογισμικού, την αποτελεσματική κρυπτογράφηση δεδομένων, την ανάπτυξη λειτουργικών μονάδων ασφαλείας υλικού κλειδώματος στις παραβιάσεις [6].

Η γενική αρχιτεκτονική του συστήματος IoT περιέχει τρία βασικά επίπεδα (όπως φαίνεται και στην εικόνα 1.), το επίπεδο Αντίληψης, το επίπεδο Δικτύου και το επίπεδο Εφαρμογής. Κάθε επίπεδο προσφέρει διαφορετική λειτουργικότητα αλλά συγχρόνως συνδέεται και βασίζεται στα άλλα επίπεδα προκειμένου να λειτουργήσει. Επομένως, για να είναι ασφαλές ένα από αυτά τα επίπεδα, τα άλλα στρώματα πρέπει επίσης να είναι ασφαλισμένα.

1) <u>Επίπεδο Αντίληψης</u>:

Σε αυτό το επίπεδο συλλέγονται όλων των ειδών οι πληροφορίες, μέσω φυσικού εξοπλισμού όπως είναι το RFID reader, οι αισθητήρες, το GPS ή οποιουδήποτε άλλου εξοπλισμού. Το βασικό στοιχείο αυτού του επιπέδου, είναι ο αισθητήρας του οποίου

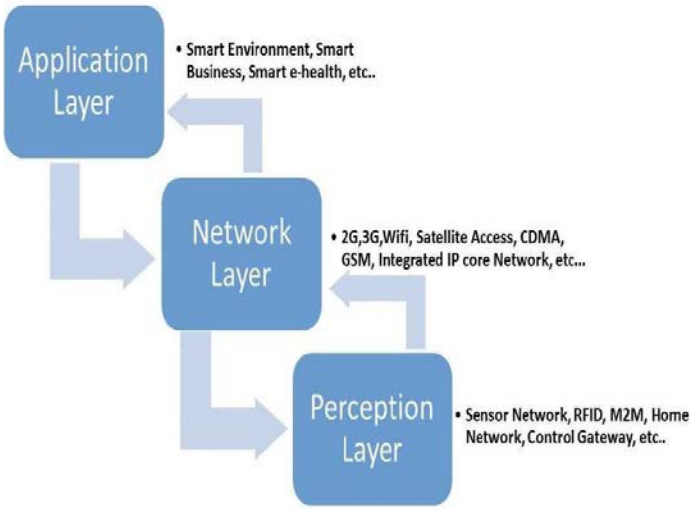
ιδιότητα είναι να αναπαριστά τον φυσικό κόσμο σε ψηφιακό. Επειδή σε αυτό το επίπεδο υπάρχει περιορισμένη ισχύς και χωρητικότητα αποθήκευσης, είναι δύσκολο να δημιουργηθεί σύστημα προστασίας για την ασφάλεια των δεδομένων. Συνεπώς, οι απαιτήσεις για την αντιμετώπιση των προκλήσεων ασφαλείας σε αυτό το επίπεδο είναι αυξημένες. Δεδομένου ότι οι συσκευές IoT είναι γενικά αυτόνομες, μπορούν εύκολα να παραβιαστούν από τους εισβολείς [5].

2) <u>Επίπεδο Δικτύου</u>:

Το επίπεδο δικτύου εμπλέκεται στη μετάδοση δεδομένων. Κύριος ρόλος του είναι η αξιόπιστη μετάδοση των πληροφοριών από το επίπεδο αντίληψης. Αποτελείται από ασύρματο δίκτυο αισθητήρων (WSN) [5]. Το επίπεδο δικτύου στο IoT λειτουργεί το ίδιο με το επίπεδο δικτύου στο TCP / IP [6]. Έχει σχετικά υψηλή ικανότητα να παρέχει προστασία ασφάλειας, ωστόσο μερικές από τις κοινές απειλές ασφαλείας, είναι δυνατές. Όπως για παράδειγμα, η κατανεμημένη επίθεση άρνηση υπηρεσίας (DDoS) που οδηγεί σε μη διαθεσιμότητα του δικτύου, η επίθεση Man-in-the-middle που στοχεύει στον έλεγχο όλων των ιδιωτικών επικοινωνιών μεταξύ των μερών, η επίθεση Sybil στην οποία ο εισβολέας παρουσιάζει πολλές ταυτότητες κ.λ.π. [5].

3) <u>Επίπεδο Εφαρμογής</u>:

Το επίπεδο εφαρμογής είναι το πιο διαφορετικό και περίπλοκο από τα αρχιτεκτονικά στρώματα του IoT καθώς παρέχει εξατομικευμένες υπηρεσίες σύμφωνα με τις ανάγκες των χρηστών. Η πρόσβαση από τους χρήστες γίνεται με προσωπικό υπολογιστή ή κινητό εξοπλισμό. Οι προκλήσεις στο επίπεδο εφαρμογής έχουν να κάνουν ως επί το πλείστων με προβλήματα απορρήτου δεδομένων. Τόσο ο έλεγχος ταυτότητας και η διαχείριση των κωδικών πρόσβασης, όσο και η ασφάλεια των δεδομένων του χρήστη, είναι βασικά ζητήματα σε αυτό το επίπεδο. Επιθέσεις που μπορεί να εμφανιστούν είναι για παράδειγμα η επίθεση με έγχυση κακόβουλου κώδικα προκειμένου να κλέψει δεδομένα, η επίθεση DDoS που θέτει σε κίνδυνο το απόρρητο των δεδομένων του χρήστη, η επίθεση phear-fishing που είναι μια επίθεση πλαστογράφησης μέσω email που ανοίγει το θύμα ώστε να οδηγηθεί ο εισβολέας σε πρόσβαση δεδομένων. Ακόμα μια επίθεση μπορεί να είναι η επίθεση sniffing, στην οποία, ο εισβολέας χρησιμοποιώντας μια εφαρμογή sniffer, συλλέγει πληροφορίες για το δίκτυο που προκαλούν την καταστροφή του συστήματος [5].



Εικόνα 1. IoT Αρχιτεκτονική [5]

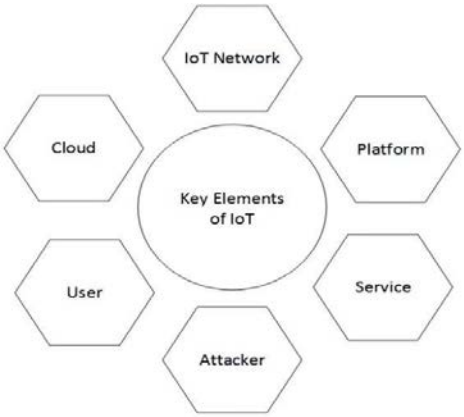
Το δίκτυο IoT έχει τρία τυπικά χαρακτηριστικά. Την ετερογένεια, τον περιορισμό πόρων και το δυναμικό περιβάλλον [8]. Στο δίκτυο IoT, οι συνδεδεμένες συσκευές που επικοινωνούν μεταξύ τους, ενδέχεται να χρησιμοποιούν πρωτόκολλα επικοινωνίας όπως MQTT και CoAP σύμφωνα με το IEEE 802.15.4 [8]. Για τις συσκευές με τους περισσότερους περιορισμούς πόρων, ιδίως εκείνες που συμμορφώνονται με το πρότυπο IEEE 802.15.4, το IETF (Internet Engineering Task Force**)** πρότεινε διάφορα πρωτόκολλα για την αποτελεσματική ενσωμάτωσή τους στο Διαδίκτυο, δηλαδή να είναι σε θέση να επικοινωνούν με συσκευές διαφορετικής αρχιτεκτονικής και εφαρμογών [9]:

- 6LowPAN4: Είναι ένα πρωτόκολλο IPv6 το οποίο καταναλώνει χαμηλή ενέργεια σε συσκευές, οι οποίες συνδέονται ασύρματα στο διαδίκτυο αλλά έχουν περιορισμένη ικανότητα επεξεργαστή.
- RPL4: Πρόκειται για ένα ελαφρύ πρωτόκολλο δρομολόγησης που υποστηρίζεται σε δίκτυα χαμηλής ισχύος.
- CoAP4: Είναι ένα εξειδικευμένο πρωτόκολλο μεταφοράς ιστού για χρήση με περιορισμένους κόμβους και περιορισμένα δίκτυα.

Για τα αντικείμενα που ακόμα δεν μπορούν να υποστηρίξουν πρωτόκολλο IP, λόγω των εξαιρετικά περιορισμένων πόρων, η ολοκλήρωση στο σφαιρικό δίκτυο Διαδικτύου είναι ακόμα δυνατή μέσω των πυλών, όπου τα ιδιόκτητα πρωτόκολλα στοίβας μη-IP (Zigbee

v1, HART, Z-Wave, κ.λπ.), μεταφράζονται σε / από πρωτόκολλα στοίβας IP, με ιδιαίτερο κόστος και χωρίς επίτευξη end-to-end επικοινωνία [10].

Το διαδίκτυο των πραγμάτων διαχωρίζεται σε έξι βασικά στοιχεία. Το δίκτυο, το Cloud, τον χρήστη, τον εισβολέα, την υπηρεσία που το υποστηρίζει και την πλατφόρμα που χρησιμοποιείται, όπως φαίνεται στην εικόνα 2 [11].



Εικόνα 2. Έξι Βασικά Στοιχεία του IoT [11]

1) Δίκτυο IoT Network [11]

Ένα δίκτυο IoT έχει πολλά κοινά με ένα δίκτυο Lan, άρα τα προβλήματα όπως κατακερματισμός και επιθέσεις ασφαλείας είναι συχνό φαινόμενο. Μπορεί να χρησιμοποιηθεί οπουδήποτε, οποτεδήποτε με οτιδήποτε. Οι συσκευές που είναι συνδεδεμένες στο IoT θα πρέπει να έχουν την δυνατότητα της ενσωματωμένης ασφάλειας, που προληπτικά να ανιχνεύει, να διαγιγνώσκει και να απομονώνει τα κενά ασφαλείας.

2) Υπολογιστικό Νέφος (Cloud) [11]

Το Cloud είναι το σημείο που δίνει την δυνατότητα να αποθηκεύονται δεδομένα από συνδεδεμένες συσκευές στο IoT, οι οποίες δεν διαθέτουν μεγάλης χωρητικότητας μνήμη RAM. Στο ενδεχόμενο αποστολής μαζικών δεδομένων ταυτόχρονα από πολλές συσκευές, θα πρέπει να γίνεται ο κατάλληλος έλεγχος διαπιστευτηρίων του χρήστη στην συσκευή, χρησιμοποιώντας την κρυπτογράφηση για την διατήρηση της ανωνυμίας.

3) Χρήστης(User) [11]

Ο χρήστης είναι ένα από τα πιο σημαντικά στοιχεία σε ένα δίκτυο IoT, καθώς με την οποιαδήποτε απροσεξία του επηρεάζει την ασφάλεια του δικτύου. Η εμπειρία του χρήστη στην συμμόρφωση των κανόνων ασφαλείας, αποτελεί το βασικό στοιχείο για την ομαλότητα λειτουργίας ενός συστήματος ασφαλείας. Για παράδειγμα, σε ένα

μοντέλο ελέγχου ταυτότητας με κωδικό πρόσβασης ID, εάν ένας χρήστης φτιάξει τον κωδικό πρόσβασης με μια απλή φράση, οι εισβολείς θα μπορούσαν να τον σπάσουν εύκολα, χρησιμοποιώντας επίθεση με brute force ή επίθεση λεξικού που είναι γνωστή επίθεση ασφαλείας.

4) Εισβολέας (Attacker) [11]

Λόγω ότι οι συσκευές είναι συνδεδεμένες στο δίκτυο και σε συνδυασμό με τους περιορισμένους πόρους ισχύος που διαθέτουν, μπορούν να είναι θύματα εισβολέων ακόμα και αν οι χρήστες τηρούν τους κανόνες ασφαλείας. Οι επιθέσεις διακρίνονται σε φυσικές και σε μη φυσικές. Φυσικές απειλές μπορούν να θεωρηθούν οι απειλές που έχουν να κάνουν κυρίως με το δίκτυο στο οποίο είναι τοποθετημένη η συσκευή και μη φυσικές απειλές είναι εκείνες, στις οποίες ο εισβολέας έχει πρόσβαση τόσο στο λογισμικό της συσκευής και στο πρωτόκολλο επικοινωνίας όσο και στην πλατφόρμα της συσκευής. Οι μη φυσικές απειλές έχουν να κάνουν κυρίως με την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα.

5) Υπηρεσία (Service) [11]

Προκειμένου μια υπηρεσία να θεωρείται ωφέλιμη, ο χρήστης πρέπει να εμπιστεύεται τον διακομιστή και ο διακομιστής θα πρέπει να παρέχει ασφάλεια απορρήτου στον χρήστη. Όταν λοιπόν εξασφαλιστεί η εμπιστευτικότητα του χρήστη προς τον διακομιστή, τότε η χρήση της υπηρεσίας, παρέχεται μέσω μιας έξυπνης συσκευής, αφού πρώτα προηγηθεί ο έλεγχος πρόσβασης, δηλαδή έλεγχος ταυτότητας και εξουσιοδότησης.

6) Πλατφόρμα (Platform) [11]

Η πλατφόρμα είναι το στοιχείο του δικτύου IoT στο οποίο συνδέονται οι συσκευές εφαρμόζοντας διάφορα πρότυπα ανταλλαγής πληροφοριών. Επειδή οι εισβολείς μπορούν να καταλάβουν τη συσκευή και να αναλύσουν την ευπάθεια της πλατφόρμας, πρέπει να χρησιμοποιείται μία αξιόπιστη μονάδα πλατφόρμας που θα ελαχιστοποιεί την ευπάθεια της και να επαληθεύεται από μόνη της.

2.2.2 Έξυπνο Πλέγμα

Το Smart Grid (Ε.Π), το έξυπνο δίκτυο / πλέγμα ηλεκτρικής ενέργειας, θα μπορούσε να θεωρηθεί ως η μεγαλύτερη δημιουργία του δικτύου IoT στο άμεσο μέλλον. Ολόκληρη η αλυσίδα δικτύων ηλεκτρικής ενέργειας, από την παραγωγή ενεργειακών σταθμών μέχρι τους τελικούς καταναλωτές της (σπίτια, κτίρια, εργοστάσια, δημόσιες υπηρεσίες,

ηλεκτρικά οχήματα, έξυπνες συσκευές κ.λπ.), συμπεριλαμβανομένων των δικτύων μεταφοράς και διανομής ηλεκτρικής ενέργειας, θα είναι γεμάτη με δυνατότητες ευφυΐας και αμφίδρομης επικοινωνίας [12].

Η τεχνολογία του Έξυπνου δικτύου μειώνει τις ενεργειακές απαιτήσεις και κατά συνέπεια το κόστος χρήσης, καθότι αλλάζει εντελώς τον τρόπο λειτουργίας των παραδοσιακών ηλεκτρικών δικτύων. Για την παρακολούθηση και τον έλεγχο του δικτύου ηλεκτρικής ενέργειας οπουδήποτε, απαιτείται λεπτομέρεια και υψηλή ακρίβεια που προσφέρουν οι έξυπνες συσκευές και οι έξυπνοι μετρητές [12].

Στόχος του Έξυπνου Πλέγματος είναι, χρησιμοποιώντας τα έξυπνα αντικείμενα (μετρητές, συσκευές, αισθητήρες κ.α.) να ισορροπεί την παραγωγή και την κατανάλωση ηλεκτρικής ενέργειας [6].

Επειδή το έξυπνο πλέγμα χρησιμοποιεί το IoT είναι ευάλωτο σε επιθέσεις στον κυβερνοχώρο και συνεπώς μπορεί να οδηγηθεί σε καταστροφές. Για τον λόγο αυτό θα πρέπει να βρεθούν λύσεις μέσω τυποποιημένων πρωτοκόλλων που βασίζονται σε υποδομές προκειμένου να μπορεί να γίνει ο απαραίτητος έλεγχος. Τα έξυπνα πλέγματα είναι ευάλωτα σε επιθέσεις που αφορούν στην διασύνδεση και την επικοινωνία των συσκευών μεταξύ τους. Αυτό γιατί, όλες αυτές οι συσκευές είναι εκτεθειμένες στο δίκτυο με αποτέλεσμα να υπάρχουν αρκετά σημεία εισόδου διείσδυσης από εισβολείς. Κατά συνέπεια, ένας εισβολέας θα μπορούσε να προκαλέσει οικονομικές απώλειες από το βοηθητικό πρόγραμμα και ζημιά στα ηλεκτρικά περιουσιακά στοιχεία, διαταράσσοντας την ισορροπία σε πραγματικό χρόνο, μεταξύ της κατανάλωσης ενέργειας / παραγωγής, μέσω του χειρισμού των δεδομένων, που παράγονται από τα έξυπνα αντικείμενα ή αποστέλλονται από το βοηθητικό πρόγραμμα. Τις απειλές ενός έξυπνου δικτύου, θα τις κατηγοριοποιούσαμε σε αυτές που αφορούν στην διαθεσιμότητα του δικτύου, την ακεραιότητα των δεδομένων και το απόρρητο των πληροφοριών [12].

Το έξυπνο πλέγμα ενισχύεται με τη μαζική χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνίας (Τ.Π.Ε.) όπως λογισμικό, υλικό, δίκτυα, εκτός από την ενσωμάτωση των κατανεμημένων ανανεώσιμων πηγών ενέργειας και των δυνατοτήτων αποθήκευσης. Στο Έξυπνο πλέγμα υπάρχουν δυο ροές [12]:

- **Ηλεκτρική ροή:** πρόκειται για την κύρια ροή ενός δικτύου ηλεκτρικής ενέργειας με αφετηρία την παραγωγή στο εργοστάσιο έως τον πελάτη που αποτελεί τον

τελικό προορισμό. Δηλαδή, ο τελικός πελάτης θα μπορούσε να αγοράσει και επίσης να πουλήσει ενέργεια.

- **Ροή πληροφοριών:** Πρόκειται για μια ροή επικοινωνίας στην οποία χρησιμοποιούνται αισθητήρες και έξυπνα αντικείμενα στους χώρους μετάδοσης και διανομής.

Δύο βασικά στοιχεία του έξυπνου πλέγματος είναι οι έξυπνοι μετρητές και οι προηγμένη υποδομή μέτρησης. Έξυπνοι μετρητές παρέχουν την δυνατότητα να καταγράφουν πληροφορίες κατανάλωσης για την εκάστοτε χρέωση και διαχείριση της υπηρεσίας σε πραγματικό χρόνο. Έχουν την ικανότητα να διαχειρίζονται την ενέργεια σε έξυπνες συσκευές όπως στο ψυγείο, στο κλιματιστικό μέχρι και στα αυτόνομα ηλεκτρικά αυτοκίνητα [12].

Η Προηγμένη Υποδομή Μέτρησης (ΠΥΜ), είναι υπεύθυνη για τη συλλογή, την ανάλυση, την αποθήκευση και την παροχή στοιχείων μέτρησης. Τα στοιχεία αποστέλλονται με SMS στα αρμόδια εξουσιοδοτημένα μέρη (π.χ. πάροχος ενέργειας, Υπηρεσία Διαχείρισης Δεδομένων Μετρητών κ.λ.π.), ώστε να μπορούν να προχωρήσουν σε διάφορες εργασίες όπως είναι η τιμολόγηση, η διαχείριση διακοπής ρεύματος. Η Προηγμένη Υποδομή Μέτρησης, διαβιβάζει μέσω SMS τα αιτήματα, τις εντολές, τις πληροφορίες τιμολόγησης και τις ενημερώσεις των λογισμικών [12].

2.3 Νέες Τεχνολογίες στις Κρίσιμες Υποδομές και IoT Πλαίσιο Ασφαλείας για Έξυπνες Υποδομές

Ο ρόλος της τεχνολογίας είναι κεντρικός στο έργο της διασφάλισης ότι η επένδυση σε κρίσιμες υποδομές έχει σχέση με το είδος της κοινωνίας και το είδος των δυνατοτήτων αυτής, πράγμα που πρέπει να λάβουμε υπόψη προκειμένου να συνδυάσουμε την ανάπτυξη, τη βιωσιμότητα, την ένταξη και την καινοτομία που απαιτεί ο «κόσμος του μέλλοντος» [8].

Στις κρίσιμες υποδομές εφαρμόζονται συστήματα τα οποία βασίζονται σε δίκτυα και υπηρεσίες ΤΠΕ [1]. Παρακάτω θα αναφερθούμε συνοπτικά σε κάποιες από τις νέες τεχνολογίες που μπορούν να βασιστούν τα συστήματα και οι εφαρμογές των κρίσιμων υποδομών όπως για παράδειγμα το Διαδίκτυο των Πραγμάτων (IoT) , η Τεχνητή Νοημοσύνη (Artificial Intelligence), το Δίκτυο 5G και τα συστήματα αναγνώρισης FRSs [8].

- **IoT**

Το Διαδίκτυο των πραγμάτων (IoT) είναι η τεχνολογία που αφενός θα συνδέσει υπολογιστές και κινητές συσκευές, αφετέρου θα συνδέονται επίσης σπίτια, πόλεις, ηλεκτρικά δίκτυα, δίκτυα ύδρευσης , δίκτυα μεταφοράς κ.α. Τα κέντρα δεδομένων (Data Centers) θα πρέπει να είναι ικανά να αντέξουν μεγάλης κλίμακας δεδομένων σε πραγματικό χρόνο, αφού το IoT είναι το επίκεντρο της τέταρτης Βιομηχανικής Επανάστασης, μιας και εξελίσσεται σε αναπόσπαστο μερίδιο της σύγχρονης ζωής με προηγμένες υπηρεσίες και πληροφορίες. Η ενοποίηση του IoT με το Cloud και το Fog Computing επιφέρει την απαιτούμενη υπολογιστική ισχύ και χωρητικότητα αποθήκευσης, επιτρέποντας στις υπηρεσίες να είναι διάχυτες και οικονομικά αποδοτικές. Πλέον υπάρχει πρόσβαση από οποιαδήποτε έξυπνη συσκευή είτε σταθερή είτε κινητή [4]. Ωστόσο, οι υποδομές και οι υπηρεσίες που βασίζονται σε τεχνολογία IoT, αυξάνουν την ανάγκη για ασφάλεια σε προκλήσεις επιθέσεων που μπορεί να δημιουργηθούν λόγω της πολυπλοκότητας, της ετερογένειας και του αριθμού των πόρων. Για παράδειγμα, επιθέσεις που γίνονται ενάντια στους αισθητήρες IoT οι οποίες ανιχνεύονται και ταξινομούνται με συστήματα ABA-IDS (Anomaly Behaviour Analysis-Intrusion Detection System) [8].

Υπάρχουν διάφορα πλαίσια IoT που μπορούν να χρησιμοποιηθούν για να δημιουργήσουν ένα πρότυπο απειλής και να εφαρμόσουν τις στρατηγικές μετριασμού. Αυτά τα πλαίσια περιλαμβάνουν όλες τις απαιτούμενες δυνατότητες για την υποστήριξη cloud και άλλες ανάγκες που απαιτούνται για την ικανοποίηση της τεχνολογίας του IoT. Τα πιο διαδεδομένα στην χρήση πλαίσια είναι [2]:

- KAA IoT
- Cisco IoT Cloud Connect
- Zetta IoT
- Sap IoT

Η ασφάλεια των έξυπνων υποδομών του IoT εξασφαλίζεται με την χρήση του Framework το οποίο αποτελείται από 4 επίπεδα [2]:

1. Το δίκτυο

2. Τις υπηρεσίες
3. Τις εφαρμογές
4. Τους τελικούς κόμβους IoT

Οι μηχανισμοί μετριασμού περιλαμβάνουν ελαφριά κρυπτογράφηση, έλεγχο ταυτότητας αισθητήρα, φιλτράρισμα πακέτων, έλεγχο συμφόρησης, συστήματα ανίχνευσης εισβολής IDS (Intrusion Detection Systems), αναγνώριση επιθέσεων απάρνησης υπηρεσίας DoS (Denial of Service), παραμόρφωση δεδομένων, αντί εμπλοκή και ανάλυση συμπεριφοράς [2].

Ένα δίκτυο IoT έχει δύο πλευρές. Η μία είναι για το τοπικό δίκτυο (πρόσωπα που κατέχουν εμπιστευτικές πληροφορίες) και η άλλη για τα δημόσια δίκτυα (ξένοι) . Τα τοπικά δίκτυα περιλαμβάνουν τελικές συσκευές, δίκτυα IP και δίκτυα εκτός IP, ελεγκτές και πύλες. Τα δημόσια δίκτυα περιλαμβάνουν υπηρεσίες IoT και εφαρμογές [2].

Τα συστήματα αυτοματισμού κτιρίων (BAS) και τα συστήματα εποπτείας ελέγχου και απόκτησης δεδομένων (SCADA) αποτελούν την πιο κοινή αρχιτεκτονική ελέγχου των έξυπνων υποδομών [2].

- **Δίκτυο 5G - Slicing Networks** [2]

Τα δίκτυα 5ης γενιάς (5G) είναι σε θέση να ικανοποιήσουν τις διαφορετικές απαιτήσεις ποιότητας των υπηρεσιών (QoS) των χρηστών. Το Slicing Network είναι μία τεχνολογία που επιτρέπει στη δημιουργία πολλαπλών τμημάτων δικτύου και υπηρεσιών 5G μέσα από μια κοινόχρηστη υποδομή. Κάθε τμήμα του μπορεί να είναι ανεξάρτητο.

Αναπτύσσεται σύμφωνα με την αυξημένη μαζική ασύρματη κίνηση δεδομένων από διαφορετικά σενάρια εφαρμογών, τα οποία αξιοποιούν αποτελεσματικά συστήματα για τη βελτίωση και την ευελιξία της κατανομής των πόρων δικτύου, της χωρητικότητας των δικτύων 5G.

Λόγω της ποικιλομορφίας των σεναρίων εφαρμογής 5G, απαιτούνται σε μεγάλο βαθμό νέα προγράμματα διαχείρισης της κινητικότητας που να εγγυώνται την απρόσκοπτη μετάδοση των συστημάτων 5G.

Στα δίκτυα 5G έχουν την δυνατότητα να συνδέονται πολλές συσκευές ταυτόχρονα, με χαμηλή κατανάλωσης ενέργειας και κόστους, αρκεί οι συνδέσεις να θεωρούνται αξιόπιστες.

Με το τεμαχισμό ενός φυσικού δικτύου σε πολλαπλά δίκτυα, υποστηρίζονται προσαρμοσμένες ανάγκες υπηρεσιών για ξεχωριστές εφαρμογές κατά τη χρήση των ίδιων των υλικών στο δίκτυο. Η αύξηση της αυτοματοποίησης σε συστήματα όπως τα Smart Grids (SGs), το Διαδίκτυο των πραγμάτων (IoT) και η Βιομηχανία 4ης Γενιάς (Industry 4.0) , απαιτεί την ανάγκη για στιβαρή τεχνολογία των Πληροφοριών και των Επικοινωνιών (ΤΠΕ). Παραδοσιακά, για την κάλυψη διαφορετικών απαιτήσεων ανά περίπτωση χρήσης σχετικά με τον ρυθμό δεδομένων δικτύου, την καθυστέρηση, την ασφάλεια, την αξιοπιστία και την ευελιξία, χρησιμοποιούνται ειδικές υποδομές επικοινωνίας.

Με τον τεμαχισμό δικτύου μια κοινή υποδομή χωρίζεται σε πολλαπλά δίκτυα ανεξάρτητα μεταξύ τους. Με αυτόν τον τρόπο οι υπηρεσίες των χρηστών είναι απομονωμένες, διασφαλίζοντας την εγγύηση της σκληρής απόδοσης. Για την αξιοποίηση των δυνατοτήτων των δικτύων 5G, αναπτύσσονται λύσεις που βασίζονται στην δυναμική κατανομή ρυθμού δεδομένων SDN ως μια τεχνική για την υλοποίηση του τεμαχισμού του δικτύου με βάση την εικονικοποίηση λειτουργιών δικτύου (NFV).Οι Virtual Machines συνδέονται σε δίκτυα 5G με την χρήση του SDN Επιπλέον, οι ελεγκτές SDN μπορούν να έχουν κεντρικά τον έλεγχο του δικτύου.

Το δίκτυο 5G προσφέρει οφέλη όπως γρήγορες ταχύτητες, αυξημένη χωρητικότητα και μικρότερη καθυστέρηση, που όμως αυξάνουν την δυνατότητα επιθέσεων για παράδειγμα μια επίθεση τύπου DDos (Distributed Denial of Service), βρίσκει πρόσφορο έδαφος λόγω της αυξημένης ταχύτητας του δικτύου 5G. Στην περίπτωση των αυτόνομων οχημάτων που απαιτείται μεγάλος όγκος δεδομένων και πληροφορίας, χρησιμοποιούνται δίκτυα 5G. Αυτό συνεπάγεται ότι οι επιθέσεις στο δίκτυο θα είναι απειλή για την ανθρώπινη ζωή.

- **Τεχνητή νοημοσύνη** [2]

Η τεχνητή νοημοσύνη ή αλλιώς A.I (Artificial Intelligence) θα αλλάξει τον τρόπο λειτουργίας πολλών υπηρεσιών. Η τεχνητή νοημοσύνη και ο αυτοματισμός της, αυξάνει την ταχύτητα και την παραγωγικότητα, μαθαίνει συνεχώς να αναπτύσσεται με βάση τις τεράστιες ποσότητες δεδομένων που επεξεργάζεται. Με την τεχνητή νοημοσύνη η

παρακολούθηση των δεδομένων ασφάλειας αυξάνεται και λιγοστεύουν να χρησιμοποιούνται οι παλιοί μέθοδοι επεξεργασίας. Βέβαια είναι κάτι που οι κακόβουλοι παράγοντες αναγνωρίζουν και αναπτύσσουν νέες μεθόδους επίθεσης για να επωφεληθούν.

Οι τεχνολογίες τεχνητής νοημοσύνης βασίζονται στην αναγνώριση προσώπου και στην ικανότητα δημιουργίας συνθετικών εικόνων και ήχων. Παραδείγματος χάρη μπορεί να προσδιοριστεί το βιομετρικό προφίλ ενός πολίτη, χρησιμοποιώντας την διαδικτυακή συμπεριφορά του. Η Τεχνητή Νοημοσύνη μπορεί να βοηθήσει στην εύρεση των κενών ασφαλείας ενός λογισμικού. Αυτό δεν σημαίνει ότι εντοπίζοντας τα κενά ασφαλείας, μπορεί να προστατέψει από τις απειλές του κυβερνοχώρου. Ο ρόλος της είναι κυρίως προληπτικός.

Ένα κακόβουλο πρόγραμμα είναι ικανό, χρησιμοποιώντας την τεχνητή Νοημοσύνη, να προκαλέσει καταστροφικές συνέπειες όπως έγινε και με την εταιρία Darktrace το 2017 υιοθετώντας συμπεριφορές χρηστών του δικτύου της. Αυτό έγινε ώστε να μπορεί να μιμείται το συγκεκριμένο μοτίβο συμπεριφοράς, και να μην εντοπίζεται από τα εργαλεία της ασφάλειας. Όσο καθυστερεί να εντοπιστεί μία επίθεση σε ένα δίκτυο, τόσο μεγαλύτερη πρόσβαση μπορεί να έχουν οι εισβολείς σε σοβαρά δεδομένα.

- **Τα συστήματα αναγνώρισης προσώπου (FRSs)** [2]

Για να εντοπιστούν ύποπτοι, οι αστυνομικές υπηρεσίες και τα αεροδρόμια κάνουν χρήση του λογισμικού Face Recognition Systems (FRSs). Με βάση αυτό, συλλέγονται πληροφορίες σχετικά με το ποινικό μητρώο των επιβατών. Ο κύριος λόγος για τον οποίο οι FRSs απασχολούνται όλο και περισσότερο από κρατικές υπηρεσίες είναι ότι, εντοπίζουν ένα «πρόσωπο στο πλήθος» ή εντοπίζουν έναν ύποπτο από φωτογραφίες γνωστών παραβατών. Οι FRSs αυτοματοποιούν αυτήν την εργασία, συνεπώς, απαλλάσσουν τους κρατικούς υπαλλήλους για πιο πολύτιμες εργασίες. Τα FRSs προτιμώνται ως βιομετρικά για ψηφιακή παρακολούθηση, καθώς είναι αθόρυβα, μη επεμβατικά και πάνω από όλα είναι οι μόνες βιομετρικές τεχνικές που χρησιμοποιούνται επί του παρόντος για την επιβολή του νόμου.

Ωστόσο, η απόδοση των FRSs μειώνεται σε μεγάλο βαθμό σε ένα ανεξέλεγκτο περιβάλλον «πρόσωπο-με-το-πλήθος», στην περίπτωση μιας μεγάλης βάσης δεδομένων και στην περίπτωση που έχει παρέλθει μεγάλο χρονικό διάστημα, μεταξύ της εικόνας της βάσης δεδομένων. Τα FRSs είναι σχεδιασμένα από ανθρώπους όπου

αυτό σημαίνει ότι οι προκαταλήψεις των αλγορίθμων των FRSs μπορούν να υπάρχουν σε κάθε φάση του σχεδιασμού του αλγορίθμου. Για τον λόγο αυτό ο σχεδιασμός των αλγορίθμων πρέπει να είναι ιδιαίτερα προσεκτικός, έτσι ώστε τα συστήματα να επιτυγχάνονται με ίση μεταχείριση και χωρίς ατομικές προκαταλήψεις, ενώπιον του νόμου.

Κεφάλαιο 3 - Κυβερνοέγκλημα

3.1 Κυβερνοέγκλημα στο IoT

Στο Διαδίκτυο των Πραγμάτων, με την πάροδο του χρόνου δημιουργούνται προβλήματα ηθικής στην καθημερινότητα του χρήστη. Η κλοπή ταυτότητας, η πρόσβαση σε προσωπικά δεδομένα με σκοπό της παραβίαση τους, η απώλεια εμπιστοσύνης και ο περιορισμός της ελευθερίας του λόγου και της έκφρασης, είναι μερικά από τα πιο συχνά προβλήματα που μπορούμε να συναντήσουμε κατά την χρήση του διαδικτύου. Η ανάπτυξη του IoT έχει μεγιστοποιήσει τα προαναφερόμενα προβλήματα [6].

Τα εγκλήματα στον κυβερνοχώρο έχουν πολλές πτυχές και εμφανίζουν μεγάλη ποικιλία. Ως κυβερνοέγκλημα θεωρείται η εγκληματική δραστηριότητα σε ένα συγκεκριμένο τόπο του διαδικτύου. Μπορεί αυτός ο τόπος να είναι ένας προσωπικός υπολογιστής, είτε ένα δίκτυο, είτε ακόμη και μια ευάλωτη συσκευή που χρησιμοποιείται στο διαδίκτυο. Για την διάπραξη ενός κυβερνοεγκλήματος, χρησιμοποιούνται μέσα και τεχνικές που διευκολύνονται με συσκευές υλικού, δικτύων και υπολογιστών [6]. Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο διατυπώνει τέσσερις διαφορετικούς τύπους αδικημάτων, τα όρια των οποίων δεν είναι πάντα ευδιάκριτα:

1. αδικήματα κατά της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων του υπολογιστή και των συστημάτων των υπολογιστών,
2. αδικήματα που σχετίζονται με τον υπολογιστή,
3. αδικήματα που σχετίζονται με το περιεχόμενο,
4. αδικήματα που σχετίζονται με τα πνευματικά δικαιώματα.

Κάποια παραδείγματα είναι τα εγκλήματα που περιλαμβάνουν την παρακολούθηση δεδομένων όπου π.χ. ένας εισβολέας παρακολουθεί την ροή δεδομένων προς ή από έναν στόχο για τη συλλογή πληροφοριών, την τροποποίηση δεδομένων (παρακολούθηση δεδομένων κατά τη διαμετακόμιση και την τροποποίηση τμημάτων αυτών των δεδομένων πριν από την αναμετάδοση) και την κλοπή δεδομένων (παράνομο αντίγραφο ή κλοπή δεδομένων), την παρεμβολή στην λειτουργία ενός

δικτύου υπολογιστών με την εισαγωγή, τη μετάδοση, την καταστροφή ή την τροποποίηση δεδομένων δικτύου [7].

Το κυβερνοέγκλημα αποτελεί την εξέλιξη των παραδοσιακών εγκλημάτων και είναι αποτέλεσμα της τεχνολογικής προόδου, η οποία έδωσε περισσότερες ευκαιρίες και νέους λόγους δράσης και στόχους. Οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ), μεγιστοποιούν την ταχύτητα για τις κυβερνοεπιθέσεις στο διαδίκτυο. Για να διαπραχθεί μία εγκληματική ενέργεια πρέπει να εντοπιστεί η ευκαιρία η οποία θεωρείται πρωταρχικός παράγοντας. Στο Διαδίκτυο παρέχονται πολλές ευκαιρίες για εγκληματική ενέργεια, στοιχείο απαραίτητο για την πραγματοποίηση ενός εγκλήματος. Εξάλλου το διαδίκτυο δεν κατασκευάστηκε με γνώμονα την ασφάλεια. Λόγω του ότι το IoT είναι χτισμένο πάνω από την υπάρχουσα υποδομή του Διαδικτύου, τα προβλήματα των κυβερνοεπιθέσεων πολλαπλασιάζονται και μεγεθύνονται, όσο αυξάνει το πλήθος των κόμβων και των υπηρεσιών που συνδέονται στο διαδίκτυο, καθώς παρέχονται όλο και περισσότερες ευκαιρίες. Είναι σημαντικό να τονιστεί ότι λόγω της εικονικής φύσης των εγκληματικών μεθόδων, είναι εφικτή η απόκρυψη των αδικημάτων, πολλά από τα οποία γίνονται αντιληπτά μετά την πάροδο αρκετών εβδομάδων ή και μηνών [6].

Το IoT θέτει νέες προκλήσεις για την προστασία των δεδομένων και του απορρήτου των τελικών χρηστών με την ασφάλεια των ανθρώπων και των συσκευών που εμπλέκονται στο IoT, να τίθενται στο επίκεντρο από τις κυβερνήσεις όλων των κρατών [6].

3.2 Πολιτική Κυβερνοασφάλειας IoT [6]

Ενώ το IoT είναι το θεμέλιο πάνω στο οποίο οικοδομούνται τα έξυπνα συστήματα η μειωμένη ασφάλεια καθιστά αυτό το θεμέλιο ευάλωτο σε κυβερνοεπιθέσεις και εγκλήματα στον κυβερνοχώρο.

Η ασφάλεια του IoT είναι ένα περίπλοκο φαινόμενο, καθώς περιλαμβάνει ένα ευρύ φάσμα πτυχών: κλείδωμα των συσκευών, πολιτικές ελέγχου στην πρόσβαση σε δίκτυα και υπηρεσίες, εξασφάλιση απορρήτου στις διαδικασίες ανάπτυξης λογισμικού, ανάπτυξη λειτουργικών μονάδων ασφαλείας για προστασία από παραβιάσεις στην πρόσβαση, και ανάπτυξη αποτελεσματικών κρυπτογραφικών προτύπων.

Στον τομέα της ασφάλειας του IoT, οι προκλήσεις της κυβερνοασφάλειας έχουν λάβει σημαντική ερευνητική προσοχή, συμπεριλαμβανομένης της κυβερνοασφάλειας στην κατασκευή “συστημάτων φυσικής ασφάλειας (cyber-physical-systems - CPS)”, της έλλειψης ολοκληρωμένων προτύπων, των επιμέρους λύσεων κυβερνοασφάλειας στα

έξυπνα κτίρια, της προστασίας της ιδιωτικής ζωής στα έξυπνα σπίτια, της κυβερνοασφάλειας στο μάρκετινγκ και στα ποικίλα δίκτυα υπολογιστών.

Υπάρχουν διάφοροι παράγοντες που συνεισφέρουν στην επιδείνωση των προκλήσεων κυβερνοασφάλειας, όπως η περιορισμένη ορατότητα, η κοινωνικο-τεχνολογική πολυπλοκότητα, η δυσκολία στην καταπολέμησης της κυβερνοασφάλειας, καθιστώντας τη χάραξη αντίστοιχης πολιτικής πιο κρίσιμη από ποτέ.

Αρκετοί ομοσπονδιακοί οργανισμοί προσπαθούν να υποστηρίξουν την ασφάλεια του IoT, μέσα από την ανάπτυξη διαφόρων προτύπων. Πρότυπα που σχετίζονται με την αρχιτεκτονική των δικτύων, την προστασία των δεδομένων της ιδιωτικής ζωής και την χρήση αυτών, δημοσιεύθηκαν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST), τον Μάιο του 2016, ως ολοκληρωμένες τεχνικές πληροφοριών σε μείζονα θέματα ασφάλειας IoT. Στις Η. Π. Α. , οι αρμοδιότητες της διακυβέρνησης του "Υπουργείου Άμυνας (Department of Defence - DoD)" που σχετίζονται με το IoT δεν συγκεντρώνονται σε ένα γραφείο, αλλά αντίθετα, διάφοροι οργανισμοί έχουν ρόλους και ευθύνες που σχετίζονται με τους κινδύνους της ασφάλειας IoT. Εντοπίζονται διάφοροι κίνδυνοι ασφάλειας στις συσκευές του IoT, που ξεκινούν με τον τρόπο σχεδιασμού, κατασκευής και διαμόρφωσης των ίδιων των συσκευών.

3.3 Κυβερνοέγκλημα και Σχέδιο Δράσης για την Ασφάλεια στον Κυβερνοχώρο και την Εθνική Ασφάλεια στις Διάφορες Κυβερνήσεις

Ο κυβερνοχώρος προσφέρει μια εξαιρετική ευκαιρία για κοινωνική και οικονομική ανάπτυξη, προτρέποντας τα κράτη μέλη και τους διεθνείς οργανισμούς να αντιμετωπίσουν το ζήτημα της ασφάλειας στον κυβερνοχώρο στη βάση της αμοιβαίας συνεργασίας και της ανταλλαγής πληροφοριών. Η ευθύνη βαραίνει τις εθνικές κυβερνήσεις πού καλούνται να οργανώσουν την πρόληψη και την αντιμετώπιση των κυβερνοεπιθέσεων [13].

Η στρατηγική για την προστασία του κυβερνοχώρου προσδιορίζει τους ακόλουθους τρεις στρατηγικούς στόχους [14]:

1. Την πρόληψη κυβερνοεπιθέσεων σε κρίσιμες υποδομές.
2. Το μετριασμό των επιπτώσεων σε επιθέσεις του κυβερνοχώρου και

3. Την ελαχιστοποίηση των χτυπημάτων καθώς και του χρόνος αποκατάστασης από επιθέσεις στον κυβερνοχώρο.

Οι βασικές αρχές που διέπουν μία στρατηγική και ένα στρατηγικό σχέδιο δράσης είναι οι ακόλουθες [15]:

- Όλες οι ενέργειες που θα περιγράφουν το σχέδιο δράσης θα πρέπει να αποσκοπούν στην προστασία των πολιτών, δομών και φορέων.
- Θα πρέπει να αναγνωρίζονται, καταγράφονται, κατηγοριοποιούνται και αντιμετωπίζονται όλες οι κυβερνοαπειλές και οι παράγοντες που πιθανόν θα επηρεάσουν την λειτουργία της Δημόσιας Διοίκησης.
- Η προστασία των προσωπικών δεδομένων, συνεπώς της ανθρώπινης ζωής και δικαιωμάτων, αποτελεί ύψιστη σημασία και για αυτό τον λόγο πρέπει να διασφαλίζεται με κάθε μέτρο, κανονισμούς και νομοθεσία.
- Η συνεργασία μεταξύ ιδιωτικών και δημοσίων φορέων (ανταλλαγή πληροφοριών, ενίσχυση έρευνας) κρίνεται επιβεβλημένη, με γνώμονα την διαρκή βελτιστοποίηση της στρατηγικής και των μέτρων υλοποίησης της.
- Ως προς την αποτελεσματικότητα του σχεδίου δράσης, θα πρέπει να διασφαλίζεται η διαρκής ενημέρωση και εκπαίδευση όλων των εμπλεκόμενων φορέων.
- Η στρατηγική και το σχέδιο δράσης θα πρέπει να είναι σε απόλυτη ευθυγράμμιση με το μεταβαλλόμενο περιβάλλον ΤΠΕ και απειλών, ορίζοντας συγκεκριμένους στόχους, ρόλους, αρμοδιότητες που συνδράμουν στην διαρκή αξιολόγηση και αναθεώρηση τους.

3.3.1 Στρατηγικές για την Ασφάλεια στον Κυβερνοχώρο των eUnations [13]

Τον Μάιο του 2017, μια επίθεση τύπου ransomware, έθεσε σε κίνδυνο την ασφάλεια των νοσοκομείων στην Αγγλία και εξαπλώθηκε σε περισσότερες από 150 χώρες σε όλο τον κόσμο. Σύμφωνα με το Ευρωπαϊκό Κέντρο Εγκλήματος στον Κυβερνοχώρο (European Cybercrime Centre - EC3), ιδρύθηκε ένα παρατηρητήριο το 2013, για να ενισχύσει έμπρακτα την επιβολή κυρώσεων που ρυθμίζονται από τον Νόμο για εγκλήματα στον κυβερνοχώρο σε χώρες της ΕΕ, δηλαδή να βοηθήσει στην προστασία των ευρωπαίων πολιτών, των επιχειρήσεων και των κυβερνήσεων από το ηλεκτρονικό έγκλημα.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, η "ασφάλεια στον κυβερνοχώρο" αναφέρεται συχνά σε ενέργειες που στοχεύουν στην προστασία του κυβερνοχώρου, τόσο στον πολιτικό όσο και στον στρατιωτικό τομέα, από τις απειλές που ενδέχεται να βλάψουν τα δίκτυα στα οποία διακινούνται ευαίσθητες πληροφορίες. Η εμπιστευτικότητα των πληροφοριών, η διαθεσιμότητα και η ακεραιότητα των δικτύων και των υποδομών διαφυλάσσονται με την ασφάλεια στον κυβερνοχώρο.

Το 2004 συστάθηκε ο οργανισμός ENISA. Σκοπός ήταν να ενδυναμωθεί η ασφάλεια των δικτύων και των πληροφοριών, εντός της Ευρωπαϊκής ένωσης. Υποστηρίζει την συνεργασία των κρατών-μελών σχετικά με την πρόληψη κυβερνοεπιθέσεων ενισχύοντας την πολιτική της Ευρωπαϊκής ένωσης. Ταυτόχρονα, ενισχύει την ικανότητα των κρατών μελών, των θεσμικών οργάνων, των οργανισμών και των φορέων της ΕΕ και προσδιορίζει τις αναδυόμενες τάσεις και ανάγκες ενόψει των εξελισσόμενων προτύπων κυβερνοεγκλήματος και ασφάλειας στον κυβερνοχώρο.

Για τον ENISA, η εφαρμογή μιας κοινής πολιτικής ασφάλειας, θεωρείται προτεραιότητα. Ως εκ τούτου, τα τελευταία χρόνια όλο και περισσότερο η ΕΕ σκληραίνει τις πολιτικές στον τομέα της ασφάλειας των πληροφοριών, της προστασίας των δεδομένων και της ασφάλειας στις ηλεκτρονικές επικοινωνίες. Πρόσφατα, αναλήφθηκαν πολλαπλές δράσεις για την προώθηση της ευρωπαϊκής ψηφιακής ενιαίας αγοράς και την ενδυνάμωση της ασφάλειας στον τομέα των απειλών που σχετίζονται με τον κυβερνοχώρο

Το ζήτημα που διακυβεύεται είναι ακόμη πιο ευαίσθητο εάν λάβουμε υπόψη ότι ο ENISA καλείται να διαδραματίσει έναν ακόμη μεγαλύτερο ρόλο, με περιορισμούς στο χρονικό πλαίσιο, τους δημοσιονομικούς πόρους και το ανθρώπινο δυναμικό.

3.3.2 Σχέδιο Δράσης για την Εθνική Ασφάλεια στον Κυβερνοχώρο (Ελλάδα) [16]

Οι εμπλεκόμενοι φορείς για το σχέδιο δράσης σύμφωνα με το πλαίσιο της 3ης Αναθεώρησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας, είναι οι εξής :

- Γενική Διεύθυνση Κυβερνοασφάλειας – Εθνική Αρχή Κυβερνοασφάλειας (National Cybersecurity Authority)
- Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – ΕΘΝΙΚΟ CERT (Ε.Υ.Π.)
- Διεύθυνση Κυβερνοάμυνας (ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ) (ΓΕΕΘΑ/ΔΙΚΥΒ)
- Δίωξη ηλεκτρονικού εγκλήματος (ΕΛ.ΑΣ)

- Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα (Α.Π.Δ.Π.Χ.)
- Αρχή διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε.)
- Κέντρο Μελετών Ασφάλειας (Κ.Ε.Μ.Ε.Α.)

Αναλυτικά:

1) Η Γενική Διεύθυνση Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης κάτω από απαιτούμενα μέτρα, διαχειρίζεται τον συντονισμό των φορέων μέσω στρατηγικού σχεδίου, διαχειρίζεται την εθνική στρατηγική της κυβερνοασφάλειας. Καθορίζει τις βασικές απαιτήσεις της ασφάλειας, αξιολογεί τις υπηρεσίες και τις λειτουργίες που επηρεάζουν την ασφάλεια των πληροφοριών όπως π.χ υπηρεσίες cloud, τρόποι εφαρμογών αλληλογραφίας αλλά και επικοινωνίας μέσω κινητής τηλεφωνίας. Διαχειρίζεται επίσης τα μητρώα συμβάντων, αξιολογεί τις βασικές απαιτήσεις της ασφάλειας, συνεργάζεται με ακαδημαϊκούς φορείς σε θέματα κυβερνοασφάλειας, επιμορφώνει και ενημερώνει τα στελέχη του.

2) Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων- ΕΘΝΙΚΟ CERT (Ε.Υ.Π.) η οποία αφορά στην οργάνωση των υπηρεσιών της ΕΥΠ με καθορισμό των αρμοδιοτήτων όπως θέματα στην ασφάλεια εθνικών επικοινωνιών, συστημάτων τεχνολογίας πληροφοριών, την αξιολόγηση τηλεπικοινωνιακών και πληροφοριακών συστημάτων αλλά και την πιστοποίηση κρυπτοσυστημάτων, υποστηρίζοντας τις Ένοπλες Δυνάμεις και τις υπηρεσίες του δημόσιου τομέα σε θέματα κρυπτασφάλειας (Εθνική Αρχή Crypto). Είναι επίσης υπεύθυνη για την εξασφάλιση των εθνικών ηλεκτρικών συσκευών τηλεπικοινωνιών από διαρροές, λόγω ανεπιθύμητων ηλεκτρομαγνητικών και μη μεταδόσεων. Γενικά, για την αντιμετώπιση κυβερνοεπιθέσεων εναντίων των δημόσιων φορέων της χώρας που δεν αφορούν στην αρμοδιότητα της Διεύθυνσης της Κυβερνοασφάλειας. Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων παρέχει υπηρεσίες που άπτονται στο αντικείμενο της ασφάλειας των Πληροφοριακών Συστημάτων του ευρύτερου Δημόσιου Τομέα.

3) Η Διεύθυνση Κυβερνοάμυνας του Υπουργείου Εθνικής Άμυνας (ΓΕΕΘΑ/ΔΙΚΥΒ) έχει επιτελικό ρόλο σε εθνικό επίπεδο. Αποτελεί την Ελληνική Αρμόδια Ομάδα Απόκρισης Κυβερνοπεριστατικών (Computer Security Incident Response Team – CSIRT) και αφορά σε περιστατικά στρατιωτικού τομέα και κυβερνοάμυνας. Η Διεύθυνση Κυβερνοάμυνας είναι αρμόδια για την μείωση κινδύνου εθνικών προκλήσεων σε τομείς κυβερνοασφάλειας των επικοινωνιών.

4) Η Δίωξη Ηλεκτρονικού Εγκλήματος είναι αρμόδια για την πρόληψη την έρευνα και την καταστολή εγκλημάτων που διαπράττονται στο διαδίκτυο ή σε άλλα ηλεκτρονικά μέσα επικοινωνίας. Υπάγεται στο κ. Αρχηγό της ΕΛ.ΑΣ. Η Διεύθυνση Δίωξης αποτελείται από πέντε τμήματα τα οποία είναι:

– Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,

– Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,

– Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας

Λογισμικού και Πνευματικών Δικαιωμάτων,

– Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης,

– Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

5) Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ) είναι μία ανεξάρτητη αρχή η οποία εποπτεύει την εφαρμογή του γενικού κανονισμού προστασίας δεδομένων που αφορά στην προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Προστατεύει τα θεμελιώδη δικαιώματα ελευθερίας φυσικών προσώπων, έναντι της επεξεργασίας των δεδομένων που τα αφορούν. Παρακολουθεί και επιβάλλει την εφαρμογή του ΓΚΠΔ (Γενικού Κανονισμού Προστασίας Δεδομένων).

– Έχει την δυνατότητα να παρέχει πληροφορίες έπειτα από αίτημα, στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους.

– Συμβάλει στην ευαισθητοποίηση του κοινού σχετικά με τα ζητήματα προστασίας προσωπικών δεδομένων και των υπευθύνων, με ειδική προσοχή σε δραστηριότητες που απευθύνονται σε παιδικές ηλικίες.

– Μέσω ανταλλαγής πληροφοριών, μπορεί να συνεργαστεί με άλλες εποπτικές αρχές και να παρέχει αμοιβαία συνδρομή με σκοπό τη διασφάλιση της συνεκτικότητας εφαρμογής του ΓΚΠΔ.

– Μπορεί να διεξάγει έρευνες όσον αφορά στην εφαρμογή του ΓΚΠΔ.

– Είναι υπεύθυνη για να συμβουλεύει το εθνικό κοινοβούλιο, την κυβέρνηση και τους οργανισμούς, για νομοθετικά και διοικητικά μέτρα, που αφορούν στην προστασία των προσωπικών δεδομένων.

– Έχει στην διάθεση της διορθωτικές, συμβουλευτικές και αδειοδοτικές εξουσίες, όπως αυτές εξειδικεύονται και αναλύονται στο άρθρο 58 του ΓΚΠΔ.

– Έχει την δυνατότητα να εγκρίνει κριτήρια πιστοποίησης και κώδικες δεοντολογίας και να μπορεί να σχεδιάζει κριτήρια διαπίστευσης.

– Μπορεί να συμβάλλει στις δραστηριότητες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων – ΕΣΠΔ.

– Διαχειρίζεται τις υποβληθείσες καταγγελίες για παράβαση διατάξεων του ΓΚΠΔ.

6) Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε) είναι μία ανεξάρτητη αρχή που εδρεύει στην Αθήνα, μπορεί όμως με απόφασή της να λειτουργήσει και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της Α.Δ.Α.Ε. κοινοποιούνται στον Υπουργό Δικαιοσύνης και στο τέλος κάθε έτους υποβάλλει Έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο. Προστατεύει τα απόρρητα των επιστολών, την ελεύθερη επικοινωνία με οποιονδήποτε τρόπο καθώς και την ασφάλεια των δικτύων και των πληροφοριών.

Οι κύριες αρμοδιότητες της Α.Δ.Α.Ε. είναι:

– Να διενεργεί ακροάσεις παρόχων ηλεκτρονικών και ταχυδρομικών υπηρεσιών, για παραβάσεις της επικείμενης νομοθεσίας για την διασφάλιση του απορρήτου των επικοινωνιών.

– Να επιβάλει τα προβλεπόμενες κυρώσεις στην περίπτωση που παρατηρείται παραβίαση της επικείμενης νομοθεσίας, για το προσωπικό απόρρητο των επικοινωνιών.

– Να εξετάζει καταγγελίες όταν υπάρχουν ενδείξεις παραβίασης τηλεφωνικού και διαδικτυακού απορρήτου.

– Να διενεργεί τακτικούς και έκτακτους ελέγχους σε δημόσιους φορείς, υπηρεσίες και ιδιωτικές επιχειρήσεις που ασχολούνται με τηλεπικοινωνιακές και ταχυδρομικές υπηρεσίες.

– Να ελέγχει τους όρους και τις διαδικασίες που ακολουθούνται κατά την εφαρμογή των διατάξεων της άρσης του απορρήτου.

7) Το Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α) είναι νομικό πρόσωπο ιδιωτικού δικαίου, υπό την εποπτεία του Υπουργού Προστασίας του Πολίτη. Ως συμβουλευτικός ερευνητικός και επιστημονικός φορέας, έχει σκοπό την εκπόνηση μελετών και την διεξαγωγή εφαρμοσμένης έρευνας σε στρατηγικό επίπεδο για την παροχή υπηρεσιών σε θέματα Πολιτικής Ασφάλειας. Σκοπός του είναι:

- Να έχει την δυνατότητα να προτείνει λύσεις με βάση την τεχνογνωσία που έχει

- Να πραγματοποιεί εκπαιδεύσεις και να εκπονεί πιστοποιημένες μελέτες

- Να αξιολογεί νέα επιτεύγματα στο χώρο, παρακολουθώντας την τεχνολογική εξέλιξη του στα συστήματα ασφαλείας

- Να μπορεί να εφαρμόζει διαδικασίες που να επιτρέπουν την διασυνοριακή συνεργασία με άλλα κράτη ή διεθνείς οργανισμούς

- Να προτείνει μέτρα πρόληψης κατά του εγκλήματος έχοντας υπόψη τα ατομικά και πολιτικά δικαιώματα εφαρμόζοντας πάντα τις συνταγματικές αρχές.

3.3.3 Σχέδιο Δράσης Ηνωμένων Πολιτειών Αμερικής [14]

Το 2016, ο Μπαράκ Ομπάμα, πρότεινε το "Σχέδιο δράσης για την εθνική κυβερνοασφάλεια (Cybersecurity National Security Action Plan - CNAP)". Το CNAP ενθαρρύνει κυρίως τον ιδιωτικό τομέα να ενημερώνει την κυβέρνηση για κρούσματα και απειλές στον κυβερνοχώρο. Μακροπρόθεσμα, αυτό μπορεί να οδηγήσει στην προστασία των ΗΠΑ από απειλές στον κυβερνοχώρο. Η σχεδίαση αφορούσε στα γενικά πλαίσια ενημέρωσης των αμερικανών πολιτών για την ψηφιακή ασφάλεια, την προστασία των ευαίσθητων προσωπικών δεδομένων αλλά και την ανοδική τάση που έχουν οι απειλές στο κυβερνοέγκλημα. Ένα από τα σημαντικότερα σημεία αυτού του σχεδίου περιλαμβάνει τη δημιουργία μιας επιτροπής που θα ενισχύσει την εθνική κυβερνοασφάλεια, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ένα δεύτερο σημαντικό σημείο αυτού του σχεδίου περιλαμβάνει την αλλαγή των κρατικών πληροφοριακών συστημάτων και την αντικατάστασή τους με νέα και πιο ασφαλή. Παράλληλα, το σχέδιο αυτό μπορεί εν δυνάμει να παρέχει στους Αμερικανούς πολίτες τη διασφάλιση των διαδικτυακών λογαριασμών τους και την αποφυγή κρουσμάτων διαδικτυακών κλοπών και παραχάραξης λογαριασμών.

Η στρατηγική που αφορά στον κυβερνοχώρο της Αμερικής είχε διεθνή χαρακτήρα και η κυκλοφορία της πραγματοποιήθηκε τον Μάιο του 2011 Η στρατηγική αυτή περιλαμβάνει δραστηριότητες όπως:

- η οικονομία στην οποία προωθούνται καινοτόμες ανοικτές αγορές
- η προστασία δικτύων που βελτιώνει την ασφάλεια, την αξιοπιστία και την ανθεκτικότητα,
- η επιβολή του νόμου που επεκτείνει τη συνεργασία και το κράτος δικαίου,
- ο στρατιωτικός τομέας που προετοιμάζει για διάφορες προκλήσεις ασφάλειας του 21ου αιώνα,
- η διακυβέρνηση Διαδικτύου η οποία προωθεί αποτελεσματικές και χωρίς αποκλεισμούς δομές,
- η διεθνής ανάπτυξη η οποία βοηθά στην ανάπτυξη ικανοτήτων, ασφάλειας και ευημερίας και
- η ελευθερία στο Διαδίκτυο η οποία επιτρέπει την υποστήριξη θεμελιωδών ελευθεριών και απορρήτου.

Για την επίτευξη των παραπάνω στόχων, η στρατηγική των Η. Π. Α. θέτει τις παρακάτω προτεραιότητες:

Α. Την ανάπτυξη ενός εθνικού συστήματος απόκρισης στον κυβερνοχώρο, ώστε η κυβέρνηση να ανταποκρίνεται πιο άμεσα και αποτελεσματικά στα περιστατικά κυβερνοασφάλειας και στη μείωση της πιθανής ζημίας από τέτοια γεγονότα.

Β. Την ανάπτυξη ενός εθνικού προγράμματος, για την ενημέρωση όλων για την απειλή της κυβερνοασφάλειας

Γ. Την ανάπτυξη ενός εθνικού προγράμματος κατάρτισης των εμπλεκομένων, ώστε να αποκτήσουν πιο ενεργητικό ρόλο στην κυβερνοασφάλεια.

Δ. Την καθαυτή διασφάλιση του κυβερνοχώρου.

Ε. Την θέσπιση ενός συστήματος για την ασφάλεια του κυβερνοχώρου στα πλαίσια διεθνούς συνεργασίας

Έχουν προταθεί ορισμένοι κανονισμοί σε ομοσπονδιακό επίπεδο για την κυβερνοασφάλεια, οι οποίοι επικεντρώνονται σε συγκεκριμένους κλάδους. Οι βασικοί κανονισμοί είναι οι εξής:

- Ο “νόμος φορητότητας και λογοδοσίας για την ασφάλιση υγείας του 1996 (Health Insurance Portability and Accountability Act - HIPAA)”,
- Ο Νόμος Gramm - Leach – Bliley (1999),
- Ο Νόμος περί εσωτερικής ασφάλειας, στον οποίο περιλαμβάνεται ο ομοσπονδιακός “νόμος διαχείρισης ασφάλειας πληροφοριών (Federal Information Security Management Act – FISMA, 2002)”.

Οι υπεύθυνοι για τις πληροφορίες και την προστασία των συστημάτων είναι οι ίδιοι οι ομοσπονδιακοί οργανισμοί, τα χρηματοπιστωτικά ιδρύματα και οι οργανισμοί υγειονομικής περίθαλψης. Το FISMA (Federal Information Security Management Act) το οποίο ψηφίστηκε από το Κογκρέσο των ΗΠΑ το 2002 ζητάει υποχρεωτικά από τις ομοσπονδιακές υπηρεσίες να εφαρμόζουν σχέδια ασφάλειας πληροφοριών για την προστασία ευαίσθητων δεδομένων. Για την ασφάλεια των πληροφοριών απαιτείται η εφαρμογή υποχρεωτικών προτύπων αλλά και γραμμών καθοδήγησης. Ωστόσο οι πάροχοι ίντερνετ διαδικτύου αλλά και οι βιομηχανίες ανάπτυξης λογισμικού δεν τηρούν τους εν λόγω κανονισμούς. Επιπλέον, δεν προσδιορίζουν τον τρόπο που θα εφαρμόζονται τα μέτρα κυβερνοασφάλειας.

3.3.4 Σχέδιο Δράσης Κίνας

Στην Κίνα, η καταπολέμηση του κυβερνοεγκλήματος γίνεται με την πολύτιμη συνεισφορά της συμβουλευτικής εταιρείας Klynveld Peat Marwick Goerdeler (KPMG) η οποία έχει πλήρη επίγνωση των νόμων και των κανονισμών της χώρας, και ως εκ τούτου αντιλαμβάνεται καλά τον χώρο της κυβερνοασφάλειας. Η KPMG παρέχει τέσσερις τύπους υπηρεσιών στη διαχείριση της κυβερνοασφάλειας [14]:

1. Διαχείριση επικινδυνότητας των προσωπικών δεδομένων και προστασία του απορρήτου στον κυβερνοχώρο
2. Μετασχηματισμός ασφαλείας μέσα από αλλαγή στην αρχιτεκτονική των δικτύων, αλλαγή στην ταυτότητα πρόσβασης, στα μέσα εκπαίδευσης.
3. Υπηρεσίες κυβερνοάμυνας δηλαδή ασφάλεια των εφαρμογών, και η αντίδραση σε περιστατικά κυβερνοεπιθέσεων
4. Αξιολογήσεις του επιπέδου ασφάλειας, σε διάφορα επίπεδα του δικτύου και των συστημάτων των ιδιωτικών και δημόσιων οργανισμών, ιδίως δε των κρίσιμων υποδομών [14].

Τα τελευταία χρόνια η Κίνα έχει ενισχύσει τις πολιτικές της για την προστασία των προσωπικών δεδομένων και την προστασία των καταναλωτών, ενώ έχει επίσης δώσει σημαντική έμφαση και έχει καταναλώσει πόρους για το μετριασμό του κυβερνοεγκλήματος, και τη διατήρηση της δημόσιας τάξης. Συνολικά, η Κίνα, είναι η δεύτερη μεγαλύτερη οικονομία του κόσμου και για αυτό είναι αρκετά ευάλωτη στον κυβερνοχώρο. Η Κίνα έχει κατορθώσει να οικοδομήσει τις τελευταίες δύο δεκαετίες το μοναδικό κυβερνοοικοσύστημα που μπορεί να ανταγωνιστεί τις ΗΠΑ. Παρά την κόντρα στην οποία βρίσκονται οικονομικά οι δύο χώρες, είναι αδιαμφισβήτητο ότι οι ΗΠΑ είναι η πιο τεχνολογικά προηγμένη χώρα με ασύγκριτη στρατιωτική ικανότητα και αποδεδειγμένα μπορεί να ανταπεξέλθει καλύτερα από οποιαδήποτε άλλη χώρα σε διαδικτυακές επιθέσεις [17].

Προσπαθώντας να βελτιώσει τη θέση της στην διεθνή κυβερνοασφάλεια, η Κίνα έχει προβεί σε αρκετές σημαντικές θεσμικές, νομοθετικές και αναπτυξιακές προσαρμογές. Πρώτον, η κινεζική κυβέρνηση εδραίωσε τη διαδικασία λήψης αποφάσεων για την πολιτική στον κυβερνοχώρο, η οποία προηγουμένως συντελούταν μεταξύ διαφόρων υπουργείων, σε μια κεντρική ρυθμιστική αρχή, την Διοίκηση Κυβερνοχώρου της Κίνας (Cyberspace Administration of China - CAC). Το CAC αποτελεί την επίσημη ρυθμιστική αρχή του Διαδικτύου και είναι επιφορτισμένο με το ρόλο της εποπτείας του κυβερνοχώρου. Είναι υπόλογο στην Κεντρική Επιτροπή Κυβερνοχώρου, το οποίο αποτελεί μια διυπουργική κυβερνητική υπηρεσία, με επικεφαλής τον Πρόεδρο Xi. Η ίδρυσή του σηματοδοτήθηκε το 2014, ενώ σήμερα διατηρεί 31 γραφεία σε διάφορες επαρχίες της Κίνας, τα οποία σχετίζονται σε μεγάλο βαθμό με την προπαγάνδα και τον έλεγχο περιεχομένου, με την αυξανόμενη εποπτεία της ασφάλειας στον κυβερνοχώρο [18].

Πέρα από το CAC, υπάρχουν και άλλες δομές που εξυπηρετούν τα σχέδια της χώρας για κυριαρχία στον κυβερνοχώρο. Μια σειρά νόμων και πολιτικών για τον κυβερνοχώρο συντάχθηκαν και ψηφίστηκαν σε διάφορα επίπεδα τα τελευταία χρόνια στην Κίνα για να αντιμετωπιστούν προβλήματα που σχετίζονται με την κυβερνοασφάλεια, όπως η εισαγωγή του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation - GDPR) το 2018. Μεταξύ των νέων νόμων και πολιτικών που θεσπίστηκαν, το πιο σημαντικό είναι ο νόμος για την ασφάλεια στον κυβερνοχώρο της Επαγγελματικής Κανονιστικής Επιτροπής (Professional Regulation Commission – PRC), ο

οποίος τέθηκε σε ισχύ το 2017 και αποτελέσει το θεμέλιο λίθο της πολιτικής της Κίνας για την ασφάλεια στον κυβερνοχώρο [18].

Τέλος, πέρα από το επίπεδο της πολιτικής, η κινεζική κυβέρνηση έδωσε έμφαση στην ενίσχυση της χώρας σε επίπεδο τεχνολογικής ανάπτυξης. Το σχέδιο "Made in China 2025" στοχεύει να μετατρέψει την Κίνα στον ηγέτη της τεχνολογικής ανάπτυξης και να αποτινάξει την ετικέτα της χώρας που έχει συνδυαστεί με μεγάλη παραγωγή αμφιβόλου ποιότητας, ανεβάζοντας τον πήχη της ποιότητας κατακόρυφα, ενώ παράλληλα το σχέδιο "Internet Plus" που δημοσιεύθηκε το 2015 στοχεύει στην αναβάθμιση των παραδοσιακών βιομηχανιών της χώρας, στις οποίες πέρα από την γεωργία, εξέχουσα θέση θα κατέχουν οι βιομηχανίες παραγωγής τεχνολογικών συσκευών και ανάπτυξης λογισμικών οι οποίες θα επεκταθούν σε νέες αγορές σε όλο τον κόσμο. Με το σχέδιο αυτό, προβλέπονται αναβαθμίσεις στις υποδομές του διαδικτύου, καθιερώνονται κοινά τεχνολογικά πρότυπα και ενώ βελτιώνονται τα αστυνομικά συστήματα για πάταξη του ηλεκτρονικού εγκλήματος [18].

3.3.5 Σχέδιο Δράσης Ρωσίας [18]

Η Ρωσία, έχει απορρίψει τη "Σύμβαση του συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (Council of Europe Convention on Cybercrime – CoECoC)" υποστηρίζοντας ότι παραβιάζει το σύνταγμα της χώρας, διότι με αυτόν τον τρόπο επιτρέπει σε ξένες υπηρεσίες να διεξάγουν έρευνες στο Διαδίκτυο εντός των συνόρων της. Από το 1998, η Ρωσία έχει υποβάλει ψηφίσματα για να εξεταστούν από τα Ηνωμένα Έθνη ζητώντας την απαγόρευση της επέμβασης σε ευαίσθητες πληροφορίες, που υπονομεύουν τη σταθερότητα του καθεστώτος. Η Ρωσία το 1998 υπέβαλε νομοσχέδιο προς ψήφιση στο Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών με τον τίτλο "Εξελίξεις στον τομέα της πληροφόρησης και των τηλεπικοινωνιών στα πλαίσια της ασφάλειας".

Τους πρώτους μήνες του 2013 ο υπουργός άμυνας Sergei Shoigu έδωσε το πράσινο φως για την δημιουργία στρατιωτικής διοίκησης που θα αφορούσε καθαρά στον κυβερνοχώρο. Ένα χρόνο μετά, ιδρύεται το τμήμα κυβερνοπολέμου, διεξάγοντας επιθετικές και αμυντικές επιχειρήσεις και συγκεντρώνοντας πληροφορίες από ξένες πηγές, παρακολουθεί και καταπολεμά τις απειλές και τις επιθέσεις στον κυβερνοχώρο. Η επένδυση αυτή στοίχισε 500 εκατομμύρια δολάρια.

Η γραμμή που ακολουθεί η Ρωσία δημιούργησε αλυσιδωτές αντιδράσεις σε έναν εμπορικό πόλεμο μεταξύ εκ νέου της Ρωσίας και των Η. Π. Α. . Τα μέλη του υπουργικού συμβουλίου της Ρωσίας δεν χρησιμοποιούσαν πλέον Ipad ύστερα από απαγόρευση.

Αντίθετα, προωθήθηκαν συσκευές της εταιρίας Samsung, υποστηρίζοντας ότι παρέχουν περισσότερη ασφάλεια και προστασία των ευαίσθητων πληροφοριών.

Τον Οκτώβριο του 2014 δημιουργήθηκαν οι ομάδες SOPKA (Σύστημα Ανίχνευσης και Πρόληψης Υπολογιστών) με σκοπό τον εντοπισμό επιθέσεων έναντι συστημάτων πληροφορικής και την πρόληψη αυτών. Λόγω της μεγάλης αναγκαιότητας στην προστασία των ρωσικών όπλων, οι Ρωσικές Στρατηγικές Πυραυλικές Δυνάμεις MSF (Strategic Missile Forces) χρησιμοποιούν όλο και περισσότερο τις ψηφιακές τεχνολογίες όπως η διαχείριση ηλεκτρονικών εγγράφων, προκειμένου να έχουν τον έλεγχο των στρατευμάτων τους και να επιβλέπουν τα πυρηνικά όπλα της χώρας.

3.4 Κυβερνοέγκλημα σε Εθνικές Κυβερνήσεις και Διεθνείς Οργανισμούς [19]

Η επικοινωνιακή υποδομή σε όλο τον κόσμο βασίζεται σε μεγάλο βαθμό στο Διαδίκτυο και στον κυβερνοχώρο. Η ανάπτυξη πολιτικών και πρακτικών ασφάλειας ύστερα από έρευνα είναι επιτακτική ανάγκη προκειμένου να διασφαλιστεί η ροή πληροφοριών στα δίκτυα επικοινωνίας, καθώς οποιαδήποτε διαταραχή θέτει σε κίνδυνο την ανθρωπότητα. Διεθνής οργανισμοί όπως κυβερνητικά ινστιτούτα, επιχειρήσεις, στρατιωτικά τμήματα θα πρέπει να λειτουργούν άψογα σε ασφαλή δίκτυα επικοινωνίας. Επιπλέον, οι ερευνητές θα πρέπει να παρακολουθούν τις αυξανόμενες δυνατότητες των εγκληματιών στον κυβερνοχώρο. Για να δοθεί έμφαση στην εκτεταμένη ανάγκη ενός ισχυρού και αποτελεσματικού συστήματος ασφάλειας στον κυβερνοχώρο, αναφέρονται παρακάτω διάφορες θανατηφόρες και καταστροφικές παρεμβάσεις στον κυβερνοχώρο σε στρατιωτικά, επιχειρηματικά, νοσοκομεία και κυβερνητικά ιδρύματα σε όλο τον κόσμο.

3.4.1 Ασφάλεια Στρατιωτικού Τομέα [19]

Με την εμφάνιση του κυβερνοχώρου ως ουσιαστικής απειλής για την εθνική και παγκόσμια ασφάλεια, ο πόλεμος/πολεμικές επιχειρήσεις/εχθροπραξίες στον κυβερνοχώρο έγιναν επίσης τομέας ενδιαφέροντος και σκοπού για το Στρατιωτικό Τομέα.

Τον Οκτώβριο του 2012, το ΝΑΤΟ εντόπισε μια εκτεταμένη επίθεση κατασκοπείας στη Ρωσία που διήρκεσε για πέντε χρόνια. Αυτή η επίθεση στόχευε κυρίως σε ουκρανικά και ευρωπαϊκά κυβερνητικά ιδρύματα. Τα δεδομένα των αρχείων καταγραφής είναι κυρίως διαθέσιμα για σύντομο χρονικό διάστημα λόγω νομικών κανονισμών, συνεπώς δε μπορεί να εκτιμηθεί με ακρίβεια η ποσότητα ή η φύση των δεδομένων που έχουν

κλαπεί από αυτήν την επίθεση. Τέτοιες επιθέσεις αυξάνουν την σημασία ισχυροποίησης του συστήματος ασφαλείας και ειδικά στον πόλεμο. Για τον λόγο αυτό οι στρατιωτικές δυνάμεις βασίζονται στην άμεση και ταχεία ανταλλαγή πληροφοριών, προκειμένου να λαμβάνονται αποφάσεις γρήγορα και αποτελεσματικά στο πεδίο μάχης. Αυτό σημαίνει ότι το δίκτυο επικοινωνίας θα πρέπει να είναι εξαιρετικά ισχυρό στην ασφάλεια του, που θα μπορεί να εμποδίσει επιθέσεις στον κυβερνοχώρο και ταυτόχρονα να προστατεύει ευαίσθητα δεδομένα και πληροφορίες.

3.4.2 Ασφάλεια Κυβερνοχώρου για Επιχειρήσεις

Το 2008, σε βρετανικά σούπερ μάρκετ, διαπιστώθηκαν επιθέσεις στις οποίες γίνονταν κλοπές πιστωτικών καρτών. Οι εγκληματίες χρησιμοποιούσαν ασύρματες συσκευές οι οποίες μπορούσαν να μεταδώσουν δεδομένα που τα υπέκλεπταν μία φορά την ημέρα και στη συνέχεια έθεταν τη συσκευή σε κρυφή λειτουργία για να αποφύγουν τον εντοπισμό. Η ενέργεια αυτή είχε καταστροφικές συνέπειες τόσο στην αλυσίδα εφοδιασμού των λιανεμπόρων όσο και στους καταναλωτές του Ηνωμένου Βασιλείου [19].

Πιο πρόσφατα, το 2018, πάλι στο Ηνωμένο Βασίλειο, μια βιομηχανία κεραμικών ειδών βρέθηκε στο στόχαστρο εγκληματιών στον κυβερνοχώρο για εκβιασμό. Μια ομάδα από χάκερς κρυπτογράφησαν τα δεδομένα τους, και πιο συγκεκριμένα αρχεία πληρωμών των υπαλλήλων και ζήτησαν 79 Bitcoin (2500£ / Bitcoin) ως λύτρα. Η εταιρεία, βέβαια, είχε προνοήσει και διατηρούσε backup για όλα τα δεδομένα της, για αυτό δεν επηρεάστηκε από την επίθεση. Το τμήμα IT της εταιρείας εργάστηκε πολύ αποτελεσματικά για να δημιουργήσει έναν νέο server και να αποθηκεύσει τα δεδομένα τους με αποτέλεσμα να μην χρειαστεί να πληρώσει τα λύτρα, και το σύστημα είχε άμεση λειτουργία μετά την επίθεση. Τέτοιου είδους επιθέσεις έχουν κάνει τους ιδιοκτήτες μεγάλων εταιρειών να δίνουν μεγάλη σημασία στην δημιουργία ενός ασφαλούς δικτύου. Αυτά τα παραδείγματα έχουν οδηγήσει στην δημιουργία μιας τεράστιας βιομηχανίας που εστιάζει στην παροχή ασφάλειας στον κυβερνοχώρο προσφέροντας υπηρεσίες αποτελεσματικής ασφάλειας στον κυβερνοχώρο επί 24ώρου βάσεως σε μικρότερες και μεγαλύτερες επιχειρήσεις [19].

Το 2014, οι Η.Π.Α. μέσω του υπουργείου Δικαιοσύνης, κατηγόρησαν την Κίνα για δραστηριότητες κατασκοπείας οι οποίες προκάλεσαν σοβαρές απώλειες σε εταιρίες, με σκοπό την αποδυνάμωση της διεθνούς ανταγωνιστικότητας της οικονομίας των Η.Π.Α. Συγκεκριμένα, διαπιστώθηκε επίθεση εισβολής σε συστήματα δικτύου αμερικανικών

εταιριών, από 5 κινέζους, κλέβοντας εμπορικά μυστικά και ευαίσθητες πληροφορίες. Η Κίνα από την μεριά της, εκμεταλλευόμενη την δυσκολία ανιχνευσιμότητας της συμπεριφοράς του δικτύου στην περίπτωση της κατασκοπείας, γεγονός που καθιστά δύσκολη την απόδειξη κατηγοριών, απάντησε άμεσα με αναστολή των δραστηριοτήτων της ομάδας δικτύων Κίνας-Η.Π.Α, φέρνοντας την σχέση των 2 χωρών σε αδιέξοδο [20].

Το 2016, η κινεζική εταιρία προστασίας διαδικτύου, Qihoo, ανέφερε 197 εκατομμύρια επιθέσεις τύπου phishing σε Android τηλεφωνικές συσκευές, που είχαν ως αποτέλεσμα τεράστιες χρηματικές απώλειες. Αυτός ο τύπος εγκλημάτων θεωρείται ο πιο διαδεδομένος στην Κίνα [17].

3.4.3 Ασφάλεια Κυβερνοχώρου για Κυβερνητικά Ιδρύματα [19]

Χαρακτηριστικές είναι οι εγκληματικές επιθέσεις στον κυβερνοχώρο στα ινστιτούτα της Ευρωπαϊκής κυβέρνησης.

Τον Δεκέμβριο του 2015, στην Ουκρανία, εντοπίστηκε επίθεση στον κυβερνοχώρο σε πολλά κέντρα διανομής ηλεκτρικής ενέργειας, πράγμα που προκάλεσε διακοπές ρεύματος και επηρέασε περίπου 225.000 πελάτες. Παράλληλα με αυτήν την επίθεση, επιθέσεις τύπου DoS (Disk Operating System)" πραγματοποιήθηκαν σε τηλεφωνικά κέντρα με σκοπό οι πελάτες να μην μπορούν να επικοινωνήσουν με εταιρείες παροχής ενέργειας για βοήθεια.

Τον Μάιο του 2017, μια διαδικτυακή επίθεση δεδομένων είχε ως αποτέλεσμα να βρεθούν εκτός σύνδεσης 61 νοσοκομεία της Εθνικής Υπηρεσίας Υγείας στο Ηνωμένο Βασίλειο. Την συγκεκριμένη επίθεση σταμάτησε ένα εξαιρετικό και ασυνήθιστο βήμα που έκανε η Microsoft όταν παρείχε μια επείγουσα ενημέρωση για τα προαναφερθέντα συστήματα.

3.5 Σημασία της Ασφάλειας στον Κυβερνοχώρο [21]

Η ασφάλεια στον κυβερνοχώρο είναι μια έννοια που συζητείται έντονα παγκοσμίως και έχει διάφορες πολιτικές διαστάσεις. Η ασφάλεια των πληροφοριών ορίζεται ως "η κατάσταση προστασίας των εθνικών συμφερόντων της στον τομέα της πληροφόρησης που ορίζεται από το σύνολο των ισορροπημένων συμφερόντων του ατόμου, της κοινωνίας και του κράτους". Ένας και μοναδικός σκοπός είναι να αυξάνεται ο έλεγχος και η λογοκρισία στον κυβερνοχώρο σύμφωνα πάντα με τις αρχές που διέπουν την νομιμότητα του κράτους.

Η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο ελέγχεται από ένα ολοκληρωμένο έγγραφο που αποσκοπεί στην παροχή της διαβεβαίωσης της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Ο κύριος στόχος του ΝΑΤΟ είναι η άμυνα, και η κυβερνοασφάλεια έχει γίνει μέρος αυτού όπως δηλώνεται σε πολλά έγγραφα. Η στρατηγική του ΝΑΤΟ συγκριτικά με αυτή της Ευρωπαϊκής Ένωσης σχετικά με την κυβερνοασφάλεια στον κυβερνοχώρο, αποτελείται από διατάξεις λιγότερο λεπτομερής καλύπτοντας μικρότερη γκάμα θεμάτων.

Τα στρατηγικά έγγραφα της ΕΕ και του ΝΑΤΟ στον τομέα της ασφάλειας στον κυβερνοχώρο διαφέρουν ως προς τη μορφή, τη δομή και το πεδίο εφαρμογής τους. Αν και η στρατηγική του ΝΑΤΟ για την ασφάλεια στον κυβερνοχώρο δεν είναι ακόμα παγιωμένη, η σημασία της ολοένα και αυξάνεται και η ασφάλεια στον κυβερνοχώρο αποτελεί ένα από τα κρισιμότερα ζητήματα στην πολιτική του ΝΑΤΟ. Η ασφάλεια στον κυβερνοχώρο αποτελεί την άμεση προτεραιότητα και για τους δύο οργανισμούς, παρά τις όποιες διαφορές στις πολιτικές που εφαρμόζουν. Βέβαια, οι γραμμές πάνω στις οποίες πατούν οι πολιτικές ασφαλείας των δύο ενώσεων δεν ευθυγραμμίζονται πάντα. Αυτό μπορεί να σημαίνει ότι οι στρατηγικές που εφαρμόζονται σε κάθε χώρα επικεντρώνονται περισσότερο στις λεπτομέρειες, αλλά στερούνται εννοιολογικών και ουσιαστικών στοιχείων, όπως αρχές, βάσεις της κυβερνοάμυνας, κλπ. Ως εκ τούτου κάποιες χώρες δυσκολεύονται να εφαρμόσουν μακροπρόθεσμες στρατηγικές ασφάλειας στον κυβερνοχώρο. Επίσης, έχει αναγνωριστεί η ανάγκη ενοποίησης των εθνικών στρατηγικών, παρά τις διαφορές που υπάρχουν ανά κράτος. Ωστόσο δεν είναι εύκολη μιας κοινής πολιτικής ασφάλειας στον κυβερνοχώρο καθότι τα κριτήρια που θέτει η κάθε χώρα είναι διαφορετικά και αποκλίνουν μεταξύ τους. Η ενοποίηση των εθνικών στρατηγικών, σύμφωνα με την οδηγία για τις NIS (Network and Information Security) και την στρατηγική της Ευρωπαϊκής Ένωσης, είναι αδύνατη. Τα έγγραφα της ΕΕ ισχύουν μόνο εντός της ΕΕ, ενώ, από την άλλη πλευρά, όταν πρόκειται για την ανάλυση των διατάξεων των προαναφερθέντων εγγράφων της ΕΕ, υπάρχει μεγάλη σύγχυση. Σε κάθε περίπτωση, η ασφάλεια στον κυβερνοχώρο αποτελεί πρώτη προτεραιότητα και η συνεργασία των χωρών μπορεί να είναι το όχημα για την επίτευξή της.

3.5.1 Κυβερνητικές Προσπάθειες για την Πρόληψη του Εγκλήματος στον Κυβερνοχώρο

Η ασφάλεια στον κυβερνοχώρο είναι ένα καίριο ζήτημα για πολλές χώρες, καθώς οι οργανισμοί αλλά και οι πολίτες είναι εξαιρετικά συνδεδεμένες με τον κυβερνοχώρο σε εμπορικές, πολιτικές, αστικές κοινωνίες και στρατιωτικές υποθέσεις [17].

Γεγονός είναι ότι δεν είναι λίγες οι περιπτώσεις που τα μεμονωμένα κράτη διαφέρουν στον τρόπο που αντιμετωπίζουν την κυβερνοασφάλεια σε σχέση με τις διεθνείς στρατηγικές ασφάλειας που αναπτύσσονται σε επίπεδο οργανισμών (ΕΕ και ΝΑΤΟ). . Οι εθνικές με τις διεθνείς στρατηγικές διαφέρουν ως προς τις αρχές, την έρευνα, την εφαρμογή προτύπων και τις διατάξεις που προστατεύουν τα ανθρώπινα δικαιώματα. Οι εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο, παραμένουν σταθερές και οι κατευθυντήριες γραμμές της ΕΕ και του ΝΑΤΟ προσπάθησαν μάλλον ανεπιτυχώς να συνδυάσουν το γενικό καλό με τα συμφέροντα κάθε κράτους [21].

Αυτές οι διαφορές στις εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο, είναι ο λόγος που δεν καθίσταται εφικτή η επίτευξη μιας ενοποιημένης πολιτικής ασφάλειας. Δεδομένου ότι όλες οι στρατηγικές εξακολουθούν να είναι πολύ διαφορετικές, απαιτείται περαιτέρω συντονισμός με τη βοήθεια μιας κοινής οδηγίας για την ασφάλεια δικτύων και πληροφοριών και άλλων πιθανών νομικών μέσων, ιδίως από τη στιγμή που η ασφάλεια στον κυβερνοχώρο έχει καταστεί ένα παγκόσμιο ζήτημα [21].

Η προετοιμασία και η πρόταση ενός ενοποιημένου εθνικού προτύπου στρατηγικής για την ασφάλεια στον κυβερνοχώρο θα μπορούσε να αποτελέσει μια νέα, ξεχωριστή πρόταση. Έτσι θα διασφαλίζεται μια κοινή πολιτική ασφάλειας στον κυβερνοχώρο σε επίπεδο περιφερειακής οργάνωσης (ΕΕ και ΝΑΤΟ) η οποία θα ενίσχυε την κουλτούρα ασφάλειας όσο το δυνατόν πιο ομοιόμορφα. Σε ένα ενοποιημένο εθνικό πρότυπο στρατηγικής για την ασφάλεια στον κυβερνοχώρο θα πρέπει να λαμβάνονται υπόψη και οι διαφορές των εθνικών χαρακτηριστικών. Από την άλλη πλευρά, η πρόταση ενός ενοποιημένου εθνικού προτύπου στρατηγικής για την ασφάλεια στον κυβερνοχώρο θα μπορούσε να δημιουργήσει το κατάλληλο έδαφος για την ενοποίηση των διατάξεων των στρατηγικών ασφάλειας στον κυβερνοχώρο [21].

Τα στρατηγικά έγγραφα ασφάλειας της ΕΕ και του ΝΑΤΟ στον κυβερνοχώρο διαφέρουν τόσο ως προς το πεδίο εφαρμογής όσο και ως προς τις πτυχές που τονίζονται από την κάθε ένωση. Ωστόσο, η επίλυση του κοινού «εχθρού», δηλαδή του κυβερνοεγκλήματος, δείχνει ότι η προσέγγιση της ΕΕ και του ΝΑΤΟ σε περιστατικά στον κυβερνοχώρο και η καταπολέμηση αυτού είναι παρόμοια. Έτσι, είναι επιδίωξη τόσο της ΕΕ όσο και του ΝΑΤΟ να υπάρχει συνεργασία σε όλες τις χώρες για την υιοθέτηση, την ενημέρωση και

την τροποποίηση διατάξεων των εθνικών στρατηγικών ασφάλειας προκειμένου να διασφαλιστεί η ασφάλεια στον κυβερνοχώρο. Τα στρατηγικά έγγραφα ασφάλειας στον κυβερνοχώρο τόσο της ΕΕ όσο και του ΝΑΤΟ διακρίνουν τα γενικά ζητήματα που πρέπει να ρυθμιστούν, τα οποία συνοψίζονται στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο, την άμυνα στον κυβερνοχώρο, την επιστημονική έρευνα, και σε ένα γενικότερο πλαίσιο, την υποστήριξη των θεμελιωδών αξιών [21].

Οι συνεχόμενοι εμπορικοί και τεχνολογικοί πόλεμοι τροφοδοτούν ένα διεθνές περιβάλλον που είναι αυξανόμενα πιο ανταγωνιστικό και επιρρεπές σε συγκρούσεις. Εν πολλοίς, η κυριαρχία στον κυβερνοχώρο είναι μια σημαντική κατάκτηση που επιδιώκουν τα κράτη, ωστόσο ο στόχος είναι κοινός για όλους οπότε η συνεργασία είναι ένα στοιχείο που θα πρέπει να διέπει όλες τις χώρες. Τα συμφέροντα, σε επίπεδο διαδικτυακής ασφάλειας, μεταξύ Κίνας, Η. Π. Α., Ρωσίας, Ινδίας κ. λπ. είναι αλληλένδετα και αυτό είναι κάτι που έχουν ήδη αναγνωρίσει οι κυβερνήσεις των κρατών αλλά και ανεξάρτητες οργανώσεις. Ωστόσο, κάθε χώρα προσπαθεί να κερδίσει όσο περισσότερο έλεγχο μπορεί έναντι των υπολοίπων χωρών [17].

Η απροθυμία συνεργασίας μεταξύ των κρατών ανά τον κόσμο για το ευαίσθητο και κρίσιμο ζήτημα της κυβερνοασφάλειας δεν σταματούν εδώ. Τον Σεπτέμβριο του 2011, η Ρωσία και άλλα μέλη του SCO (Shanghai Cooperation Organization) υπέβαλαν επίσης σχέδιο για την θέσπιση ενός Διεθνούς Κώδικα Συμπεριφοράς που θα φροντίζει για την Ασφάλεια των Πληροφοριών στην 66η συνεδρίαση της Γενικής Συνέλευσης του ΟΗΕ, σύμφωνα με τον οποίο θα περιοριζόταν η διάδοση πληροφοριών που υποκινούν την τρομοκρατία και υπονομεύουν την πολιτική, οικονομική και κοινωνική σταθερότητα των εθνικών κρατών που καλούνται να συνεργαστούν. Με αυτόν τον τρόπο, τα κράτη αυτά συμφωνούσαν ότι οι ρυθμίσεις ασφάλειας πρέπει να τεθούν σε πρώτο πλάνο, ενώ θεωρήθηκε από πολλούς ότι απώτερος σκοπός ήταν να μειωθεί η δύναμη των ΗΠΑ στον κυβερνοχώρο. Το 2011 η Ρωσία εναντιώθηκε ακόμα πιο ξεκάθαρα στις Η.Π.Α. καθώς δήλωσε ότι προτεραιότητα της ήταν να καθιερωθεί ο διεθνής έλεγχος στο διαδίκτυο με βάση την ITU (International Telecommunication Union). Έτσι για άλλη μια φορά, οι σχέσεις μεταξύ των δύο μεγάλων κρατών φάνηκε ότι διέπονταν περισσότερο από ανταγωνισμό παρά από διάθεση για υγιή συνεργασία [18].

Γενικότερα, αυτό που υποστηρίζει πιο ανοιχτά η Ρωσία είναι κάτι που υποστηρίζουν και άλλες χώρες, οι οποίες προσπαθούν να πάρουν την εξουσία του κυβερνοχώρου από τα χέρια των ΗΠΑ. Για το λόγο αυτό, προσπαθούν να δημιουργήσουν νέες συμμαχίες και

να καταβάλλουν προσπάθειες για την αναδιανομή των μεριδίων στον παγκόσμιο χάρτη. Προς αυτή την κατεύθυνση, η Ρωσία έχει δείξει την διάθεσή της να αποφεύγει τις εταιρείες με έδρα τις ΗΠΑ, επιλέγοντας να διατηρήσει μια διμερή συνεργασία με την Κίνα. Η Κίνα και η Ρωσία δεσμεύονται για συνεργασία στους τομείς των ICT και των επικοινωνιών, θέτοντας έτσι μία μεγάλη συμφωνία που αφορούσε στις τηλεπικοινωνίες. Το 2014 η κινεζική εταιρεία Huawei υπογράφει συμφωνία με την Ρωσική κρατική εταιρεία τηλεπικοινωνιών στην οποία θα κατασκευαστεί υποθαλάσσια γραμμή επικοινωνίας στην Άπω Ανατολή της Ρωσίας. Καθώς η διεθνής κυβερνοασφάλεια πολώνεται, παρατηρείται προσπάθεια πολλών χωρών να κρατήσουν μια ουδέτερη θέση [18].

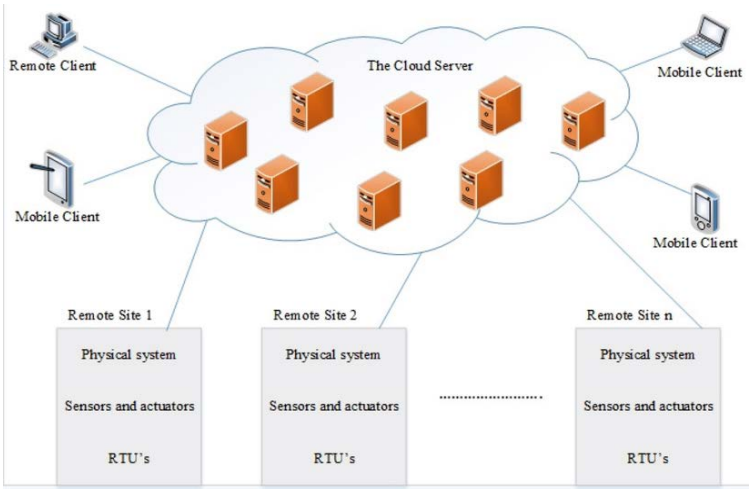
Κεφάλαιο 4 - Κυβερνητική Ασφάλεια για Υποδομές Ζωτικής Σημασίας: Μοντελοποίηση Επίθεσης και Άμυνας

Ο αποτελεσματικός τρόπος αντιμετώπισης των ζητημάτων ασφαλείας ενός δικτύου, για το πόσο ευάλωτο είναι στις επιθέσεις, εξαρτάται από την ανθεκτικότητα του. Τα μοντέλα αντιπάλων περιγράφουν τους στόχους επίθεσης και τις οικονομικές τους επιπτώσεις. Για τον βέλτιστο χειρισμό τους, κύριος παράγοντας είναι η τεχνική συστημάτων ασφαλείας που ορίζει τους κινδύνους σε κόμβους αναφοράς σε ένα δίκτυο. Προκειμένου να οριστεί η τεχνική συστημάτων ασφαλείας, είναι σημαντικό να αναγνωριστούν οι ιδιότητες του συστήματος, καθώς επίσης και να αναλυθούν οι επιπτώσεις οι οποίες θα βοηθήσουν στο να ληφθούν κατάλληλα μέτρα μετριασμού των κινδύνων στους κόμβους αναφοράς [22].

4.1 SCADA (Supervisory Control and Data Acquisition) Πλαίσιο Ασφαλείας

Οι μεγάλες δυνατότητες του συνδυασμού IoT με το Cloud δημιουργούν λύσεις για την απόδοση, την ευελιξία, την σταθερότητα, αλλά και την ανοχή σφαλμάτων. Σε αυτό το πλαίσιο αναπτύσσονται τα Κυβερνοφυσικά Συστήματα CPS (Cyper Physical System). Φυσικά αλλά και ψηφιακά συστήματα επικοινωνούν μεταξύ τους, καταγράφοντας πληροφορίες, που εξασφαλίζουν την ορθή αλλά και ευφυή λειτουργία τους. Αυτό, για να γίνει εφικτό, τα CPS αξιοποιούν αισθητήρες επικοινωνίας για να ικανοποιήσουν τις εκάστοτε ανάγκες και απαιτήσεις. Αυτά τα συστήματα είναι τα λεγόμενα SCADA, που έχουν ως άμεση ευθύνη την παρακολούθηση διαδικασιών με την εφαρμογή κατάλληλων ελέγχων. Με τον όρο SCADA περιγράφεται μια κατηγορία συστημάτων αυτομάτου βιομηχανικού ελέγχου και τηλεμετρίας. Το χαρακτηριστικό των συστημάτων SCADA είναι ότι αποτελούνται από τοπικούς ελεγκτές, που ελέγχουν επιμέρους στοιχεία και μονάδες μιας εγκατάστασης, συνδεδεμένους σε ένα κεντρικό τερματικό. Όπως φαίνεται και στην εικόνα 1, η γενική αρχιτεκτονική των συστημάτων SCADA σε περιβάλλον IoT περιέχει τα εξής [23]:

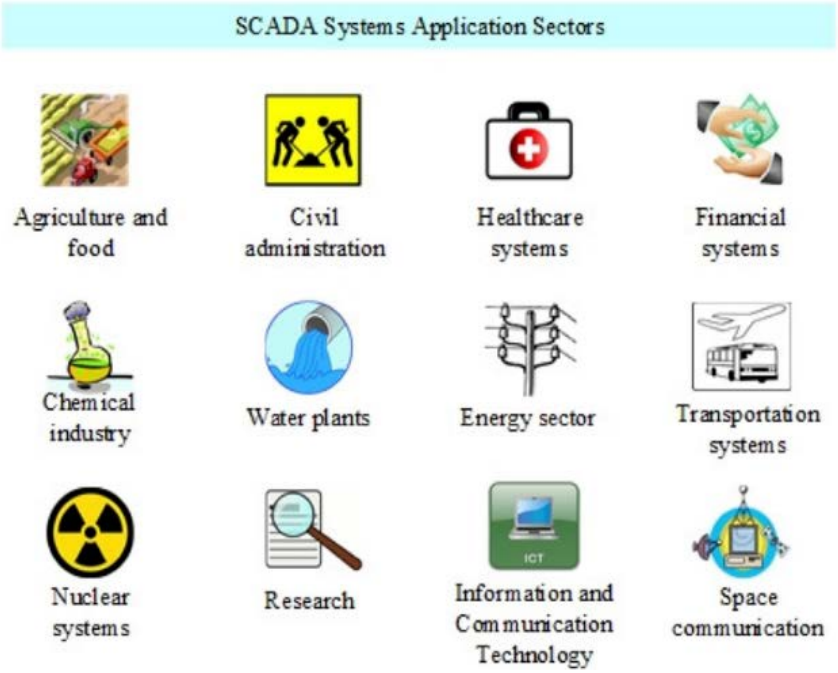
1. Μια διεπαφή ανθρώπινου μηχανήματος HMI (Human Machine Interface)
2. Εξοπλισμό και λογισμικό σε απομακρυσμένες μονάδες τερματικού RTUs (Remote Terminal Units)
3. Έναν εποπτικό σταθμό
4. Αισθητήρες



Εικόνα 3. Γενική Αρχιτεκτονική SCADA σε περιβάλλον IoT-Cloud

Οι τομείς εφαρμογών των συστημάτων SCADA ποικίλουν. Μπορεί να είναι ο τομέας της ενέργειας, των μεταφορών, της έρευνας, της επικοινωνίας σηράγγων και αυτοκινητοδρόμων κ.α.

Μία εφαρμογή ενός συστήματος SCADA, όπως είναι το WebSCADA, στον τομέα της υγειονομικής περίθαλψης, επιτρέπει σε γιατρούς και συναφή μέλη της ομάδας υγειονομικής περίθαλψης, να παρακολουθούν και να ελέγχουν την κατάσταση υγείας των ασθενών [23].



Εικόνα 4. Τομείς εφαρμογών συστημάτων SCADA

Τα συστήματα SCADA πρωτοεμφανίστηκαν, χρησιμοποιώντας τυποποιημένα πρωτόκολλα και ενσύρματες επικοινωνίες με αποκλειστικό σκοπό την παρακολούθηση

και τον έλεγχο των διαδικασιών ενός συστήματος. Όταν όμως τα συστήματα αυτά εκτέθηκαν σε περιβάλλον IoT, με Cloud Web Interface και σε περιβάλλον δικτύου, έγιναν πιο ευάλωτα σε απειλές και επιθέσεις. Στην εικόνα 3, φαίνεται η εξέλιξη των συστημάτων SCADA από την 1η γενιά έως την 4η σε περιβάλλον Cloud [23].

Όταν τα συστήματα είναι ενσωματωμένα σε περιβάλλον IoT και Cloud, είναι πολύ ευάλωτα με αποτέλεσμα να παρουσιάζουν ευπάθειες. Αρνητικό αντίκτυπο στην απόδοση των SCADA προκαλούν οι ευπάθειες όπως [23]:

1. Εντολές και πληροφορίες ενός συστήματος, μπορούν να τροποποιηθούν και να χαθούν κατά την διάρκεια μιας επικοινωνίας για αυτό τον λόγο η επικοινωνία Cloud κάνει τα συστήματα SCADA πιο εκτεθειμένα.
2. Τα συστήματα SCADA που είναι ενσωματωμένα στο Cloud κινδυνεύουν το ίδιο όπως μια τυπική υποδομή Cloud.
3. Οι εφαρμογές συστημάτων SCADA μπορούν εύκολα να αναζητηθούν και να παραβιαστούν από εισβολείς.
4. Τα πρωτόκολλα IEC40 και DNP3 που χρησιμοποιούνται στον έλεγχο και στον αυτοματισμό των συστημάτων SCADA είναι ευάλωτα σε επιθέσεις.
5. Λογισμικά τρίτων κατασκευαστών που χρησιμοποιούνται στις συσκευές IoT προκαλούν σφάλματα στα λειτουργικά συστήματα των συσκευών αυτών όπως η έλλειψη κρυπτογραφίας.
6. Τα συστήματα SCADA δεν διαθέτουν ελέγχους ασφαλείας

Λόγω των ευπαθειών οι κίνδυνοι-απειλές που συναντάμε σε περιβάλλοντα IoT-Cloud όπως [23]:

1. Advanced Persistent Threats (APTs): Οι APTs είναι επιθέσεις σε δίκτυο που χρησιμοποιείται από μη εξουσιοδοτημένο άτομο, χρησιμοποιώντας κρυφές και εξελιγμένες τεχνικές εισβολής, προκειμένου να αποκτήσει πρόσβαση σε ένα σύστημα και να παραμείνει μέσα για μεγάλη χρονική διάρκεια, με δυνητικά καταστροφικές συνέπειες.
2. Φυσική παραβίαση ή παρεμβολή: Η ακεραιότητα δεδομένων μπορεί να χαθεί όταν υπάρξει φυσική παραβίαση ή παρεμβολή .

3. Επιθέσεις Man-in-the-Middle(MITM): Επίθεση spoofing και επίθεση sniffing είναι αποτέλεσμα επίθεσης πλαστογράφησης από πρόγραμμα ή όταν ένα άτομο μεταμφιέζεται ως άλλο άτομο για να αποκτήσει πρόσβαση στο σύστημα ή στο δίκτυο. Ένας εισβολέας, σε μια επίθεση sniffing, έχει πρόσβαση στο σύστημα τόσο στα μηνύματα που διαβιβάζονται όσο και στις δραστηριότητες που εκτελούνται.

4. Επανάληψη επιθέσεων: Πρόκειται για επιθέσεις με μεγάλη συχνότητα στις οποίες ένα έγκυρο μήνυμα περιέχει έγκυρα δεδομένα. Τέτοιου είδους επιθέσεις επηρεάζουν την απόδοση των συστημάτων SCADA και χαρακτηρίζεται ως σοβαρή απειλή μιας και δημιουργεί μεγάλο φόρτο καθυστέρησης σε μηνύματα που αποστέλλονται σε άλλες συσκευές.

5. Κατανεμημένη Επίθεση Άρνησης Εξυπηρέτησης ή Denial Of Service(DoS) : Στόχος αυτής της επίθεσης είναι να μην λειτουργεί ώστε να βγαίνει εκτός η υπηρεσία που έχει επιλέξει ο χρήστης. Στο απλούστερο επίπεδο τέτοιες επιθέσεις υπερφορτώνουν πόρους υπολογιστών σε ένα δίκτυο μιας εταιρίας ακόμα και ενός μεγάλου data center, με αποτέλεσμα το κάθε μηχάνημα να μην μπορεί να εκτελέσει τις προβλεπόμενες εργασίες του.

Οι επιθέσεις DoS έχουν εξελιχθεί σε διάφορες κατανεμημένες μορφές. Προκειμένου να μπορούν να εντοπίζονται οι διάφορες επιθέσεις, είναι απαραίτητο να δημιουργείται ένα προφίλ έτσι ώστε ο εντοπισμός να γίνεται μέσω αναγνώρισης των αλλαγών. Σε ένα σύστημα ηλεκτρικής ενέργειας, οι επιθέσεις DoS είναι πιθανές, καθώς αποτελεί υποδομή πληροφοριών και επικοινωνίας. Οι επιθέσεις DoS βρίσκουν πρόσφορο έδαφος σε συστήματα κρίσιμων υποδομών [22].

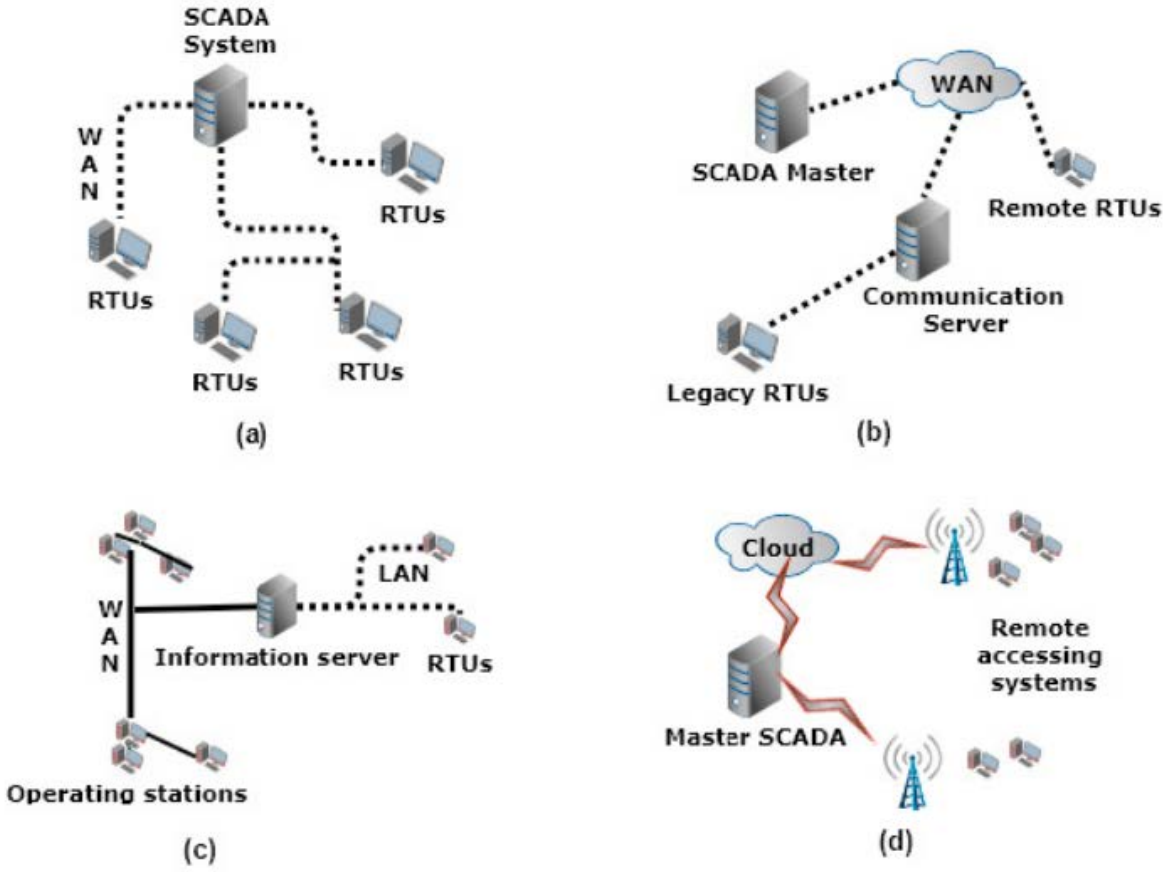
Για παράδειγμα, σε συστήματα υποδομής ισχύος όπου λειτουργούν τα συστήματα SCADA και άλλες κρίσιμες λειτουργίες όπως εκτίμηση κατάστασης, προληπτικοί ή έκτακτοι έλεγχοι και επεξεργασία προειδοποίησης, οι επιθέσεις DoS έχουν σοβαρή επίπτωση στο δίκτυο επικοινωνίας, στο κέντρο ελέγχου και στον υποσταθμό. Οι επιθέσεις DoS με βάση την εξάντληση πόρων θα μπορούσαν να έχουν τις ακόλουθες μορφές σε περιβάλλον δικτύου ηλεκτρικής ενέργειας [22]:

- Να επιβραδύνουν ή να ρίχνουν το δίκτυο του κέντρου ελέγχου, προκαλώντας μείωση απόδοσης ελέγχου σε πραγματικό χρόνο.

- Να επιβραδύνουν ή να ρίχνουν τα Αυτόματα Συστήματα Υποσταθμού (Substation Automation Systems – SASs) προκαλώντας υποβάθμιση της ανίχνευσης πραγματικού χρόνου και της απόδοσης ενεργοποίησης.
- Να προκαλέσουν συμφόρηση στους διαύλους επικοινωνίας, με αποτέλεσμα οι καθυστερήσεις επικοινωνίας να υπερβαίνουν το όριο που μπορεί να γίνει ανεκτό για τη λειτουργία SCADA σε πραγματικό χρόνο.

Ακόμη και αν τα συστήματα SCADA χρησιμοποιούν ασφαλή πρωτόκολλα επικοινωνίας όπως Modbus και ICCP (Inter Control Center Communications) οι επιθέσεις DoS με βάση την εξάντληση πόρων μπορούν να δράσουν [22].

Οι επιθέσεις (DoS) είναι μία από τις πιο επιζήμιες, οι οποίες επηρεάζουν την απόδοση του υπολογιστή και της επικοινωνίας μέσω εξάντλησης πόρων από την άποψη των κύκλων υπολογισμού, της προσωρινής αποθήκευσης (buffers) και του εύρους ζώνης επικοινωνίας. Μια τυπική επίθεση εξάντλησης πόρων, όπως για παράδειγμα μία επίθεση εκατομμυρίων πακέτων, περιλαμβάνει παραβιασμένες μηχανές που στέλνουν μεγάλο αριθμό ψεύτικων πακέτων σε στοχευμένους servers και σε στοχευμένα δίκτυα που είναι τα πιθανά θύματα. Τα συστήματα υποδομής πληροφοριών διαταράχθηκαν από διάδοση του ιού trojan, καθώς καταναλώνουν μεγάλο αριθμό υπολογιστικών πόρων και πόρων δικτύου [22].



Εικόνα 5. Η εξέλιξη των συστημάτων SCADA

Οι τέσσερις θεμελιώδεις συνιστώσες σε ένα προτεινόμενο πλαίσιο ασφαλείας SCADA είναι [22]:

1. Παρακολούθηση σε πραγματικό χρόνο
2. Ανίχνευση ανωμαλιών
3. Ανάλυση επιπτώσεων και
4. Στρατηγικές μετριασμού RAIM ((Real-time Anomaly Impact Mitigation).

4.1.1 Παρακολούθηση σε Πραγματικό χρόνο [22]

Τα συστήματα SCADA παρακολουθούν on-line μέσω μονάδων Προγραμματιζόμενων Λογικών Ελεγκτών και καταγράφουν συνεχώς όλες τις σημαντικές παραμέτρους της παραγωγικής διαδικασίας, για την επίτευξη εποπτείας σε πραγματικό χρόνο. Τα γεγονότα και τα δεδομένα που καταγράφονται σε πραγματικό χρόνο σε βάσεις δεδομένων, παρέχουν στον χρήστη την δυνατότητα να δημιουργεί στατιστικές

αναφορές ανά πάσα στιγμή. Για παράδειγμα σε ένα δίκτυο ηλεκτρικής ενέργειας ένα σύστημα SCADA περιλαμβάνει ένα κέντρο ελέγχου, αισθητήρες που πραγματοποιούν μετρήσεις στο δίκτυο, έξυπνες συσκευές σε υποσταθμούς και διάφορους συνδέσμους για να επικοινωνούν οι υποσταθμοί με τα κέντρα ελέγχου. Η δικτύωση όλων αυτών αποτελείται από ενσύρματα καλωδιακά κυκλώματα, μικροκυματικά κανάλια ή γραμμές μεταφοράς ηλεκτρικής ισχύος. Τα δεδομένα που συλλέγονται μέσω του SCADA εκτιμώνται και αναλύονται σε πραγματικό χρόνο σε πολλές λειτουργίες ενός συστήματος διαχείρισης ενέργειας (Energy Management System – EMS).

4.1.2 Ανίχνευση Ανωμαλιών και Ανάλυση Επιπτώσεων [22]

Προκειμένου να ανιχνευτεί μία απειλή, χρησιμοποιούνται τεχνικές που συσχετίζουν συμβάντα με εξαγωγή και ανάλυση δεδομένων ελέγχου από όργανα ισχύος. Οι κατηγορίες των συσχετίσεων συμβάντων είναι οι εξής:

- Χρονικές (Temporal)
- Χωρικές (Spatial) ή
- Υβριδικές (Hybrid)

Αυτοί οι συνδυασμοί ανωμαλιών, παρατηρούνται είτε σε ένα τοπικό LAN δίκτυο, είτε σε ένα world wide web δίκτυο.

Η στρατηγική ανίχνευση ανωμαλιών είναι αναγκαία για την αντιμετώπιση των ελλιπών δεδομένων, ιδίως για τον εντοπισμό σκόπιμης εξαπάτησης ή σφαλμάτων δεδομένων. Με την ανάλυση συσχέτισης εντοπίζονται οι επιθέσεις και οι απόπειρες επιθέσεων όπως π.χ. οι επιθέσεις DoS.

Αναλύοντας τις συσχετίσεις που μπορούν να εφαρμοστούν διαπιστώνουμε:

- **Χρονική συσχέτιση:** Αφορά στην εξαγωγή δεδομένων από ένα τοπικό περιβάλλον που μπορεί να βασίζεται στην εκπαίδευση των συσκευών, για την ανίχνευση κακόβουλης τροποποίησης στις ρυθμίσεις. Μια τροποποίηση στις ρυθμίσεις ανιχνεύεται με την κατάλληλη προσθήκη ευφυΐας. Ωστόσο, μια τέτοια υλοποίηση έχει εξεταστεί μόνο σε μερικές προοπτικές ανωμαλίας, οι οποίες μπορούν να βελτιωθούν μέσω συσχετίσεων μεταξύ άλλων τοπικών πηγών.
- **Χωρική συσχέτιση:** Αυτή η συσχέτιση περιλαμβάνει ιδιότητες για την ανάλυση συμβάντων που συμβαίνουν σε πολλαπλούς υποσταθμούς και/η σε κέντρα

ελέγχου ή έτσι ώστε να εξασφαλιστεί υψηλότερο επίπεδο ασφαλείας όταν ένα σύστημα βρίσκεται υπό εξελιγμένες επιθέσεις που μπορεί να προκαλέσουν σημαντικές ζημιές όσον αφορά στις οικονομικές απώλειες και στον εξοπλισμό.

- **Υβριδική συσχέτιση:** Η υβριδική προσέγγιση συνδυάζει χρονικούς και χωρικούς συσχετισμούς για τον προσδιορισμό και τη σύγκριση της πιθανότητας έντασης των επιθέσεων. Με τον τρόπο αυτό μπορεί να βελτιωθεί η υπόθεση συσχέτισης, σε σχέση πάντα με την αξιοπιστία των τρεχουσών συνθηκών από τις διάφορες πηγές.

Για να πραγματοποιηθεί ανίχνευση ανωμαλιών και σχετική ανάλυση επιπτώσεων, τα διάφορα αρχεία καταγραφής του δικτύου SCADA πρέπει να παρακολουθούνται και να συσχετίζονται περιοδικά. Τα αρχεία αυτά μπορούν να ληφθούν είτε από πραγματικά περιβάλλοντα SCADA, είτε από πλατφόρμες δοκιμών που εξομοιώνουν λειτουργίες SCADA και περιλαμβάνουν τα ακόλουθα συστήματα:

- **Συστήματα επικοινωνιών:** Τα συστήματα επικοινωνιών δείχνουν την κατάσταση σύνδεσης. Αν αυτή είναι προσωρινή ή μόνιμη, αν είναι αποτυχημένη σύνδεση, ή ακόμα αν έχει πραγματοποιηθεί μία αδρανής σύνδεση και σε ποιο χρονικό πλαίσιο. Επιπλέον, εφόσον έχει καθοριστεί ο μέγιστος αριθμός των επιτρεπόμενων συνδέσεων και το χρονικό πλαίσιο αυτών, ανιχνεύουν απειλές τύπου DOS με επιτυχία. Μπορούν να διαπιστώσουν αν υπάρχει κάποια ασυνήθιστη συχνότητα σύνδεσης, καθώς επίσης και τον όγκο χρήσης μιας εφαρμογής.
- **Συστήματα υπολογιστών:** Πρόκειται για συστήματα τα οποία μπορούν εύκολα να προειδοποιήσουν επικείμενες απόπειρες εισβολής. Καταγράφοντας των αριθμό των επανεκκινήσεων, των τερματισμών λειτουργίας ή της διακοπής των εφαρμογών, είναι ικανά να προειδοποιήσουν και για τυχόν μόνιμες βλάβες.

Προκειμένου να είναι εφικτή η ανάλυση των επιπτώσεων θα πρέπει πρώτα να έχουν αναλυθεί οι συμπεριφορές εισβολής σε ένα σύστημα SCADA και ταυτόχρονα να έχουν αξιολογηθεί οι συνέπειες της. Με την ανάλυση των συμπεριφορών αξιολογείται και η ευπάθεια των συστημάτων ισχύος σε ένα δίκτυο υπολογιστών. Μια επίθεση στην κυβερνο-ασφάλεια ενός συστήματος SCADA μπορεί να προκαλέσει σοβαρή ζημιά που θα οδηγήσουν ακόμα και σε καταστροφή στον εξοπλισμό. Μια ολοκληρωμένη προσέγγιση μοντελοποίησης κινδύνου που καταγράφει τόσο τις ευπάθειες του

συστήματος ελέγχου ισχύος όσο και τις επιπτώσεις που προκύπτουν στη λειτουργία σε πραγματικό χρόνο του συστήματος ισχύος, έχει τα ακόλουθα τέσσερα βασικά βήματα:

1. **Cybernet:** Πρόκειται για ένα δίκτυο το οποίο καταγράφοντας την διαμόρφωση του συστήματος, τον έλεγχο ταυτότητας, το μοντέλο τείχους προστασίας και το μοντέλο σύνδεσης / κωδικού πρόσβασης, μπορεί και φτιάχνει συνδυασμούς σεναρίων εισβολής στο σύστημα SCADA.
2. **Προσομοίωση ροής ισχύος:** Για να αξιολογηθεί μία κατάσταση ενός συστήματος ισχύος, υπό το καθεστώς κυβερνοεπίθεσης, χρησιμοποιούνται μοντέλα εισβολής και προσομοιώσεις ροής ισχύος, απομονώνοντας τα παραβιασμένα υποσυστήματος. Εάν απομονώνοντας το παραβιασμένο υποσύστημα, δεν καταστεί δυνατό να βρεθεί λύση ροής ισχύος τότε είναι πολύ πιθανό το σύστημα ισχύος να καταρρεύσει.
3. **Υπολογισμός δείκτη ευπάθειας:** Ο δείκτης ευπάθειας υπολογίζεται λαμβάνοντας υπόψη την ανάλυση Cybernet που δείχνει την πιθανότητα της εισβολής και την προσομοίωση ροής ισχύος που δείχνει τον συντελεστή επίπτωσης.
4. **Βελτιώσεις της ασφάλειας:** Αφού έχουν αξιολογηθεί τα αποτελέσματα ευπάθειας ενός συστήματος SCADA βάσει των διαθέσιμων τεχνολογιών, υπάρχει δυνατότητα βελτίωσης της κυβερνοασφάλειας.

4.1.3 Στρατηγικές Μετριασμού [22]

Ο κίνδυνος και η σοβαρότητα αυτού είναι το αποτέλεσμα της ανάλυσης των επιπτώσεων με συσχέτιση των συμβάντων. Εάν ο κίνδυνος είναι υψηλός, τότε γίνονται οι απαραίτητες ενέργειες ελέγχου για την εφαρμογή τεχνικών πρόληψης/μετριασμού του. Ανάλογα με τον κίνδυνο, εξαρτώνται οι τεχνικές πρόληψης και μετριασμού. Οι κίνδυνοι μπορεί να είναι:

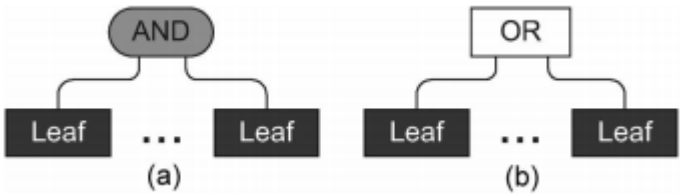
- Επαναλαμβανόμενες επιθέσεις DoS
- Σενάρια εισβολής
- Απόπειρες εισβολής

Σε περίπτωση απόπειρας εισβολής, πρέπει να γίνουν κατάλληλες βελτιώσεις ασφαλείας σύμφωνα με το σενάριο ευπάθειας που προσδιορίστηκε. Προκειμένου να γίνουν οι κατάλληλες βελτιώσεις ασφαλείας, θα πρέπει να ανιχνευθεί η φύση του κινδύνου και

έπειτα να αξιολογηθούν τα στοιχεία που χρειάζονται βελτίωση. Η αξιολόγηση τόσο των μελετών για τον ποσοτικό προσδιορισμό των ευπαθειών όσο και της αποτελεσματικότητας του μετριασμού των κινδύνων , υλοποιείται με ένα προτεινόμενο πλαίσιο εξελιγμένων σεναρίων επίθεσης. Η εφαρμογή μίας στρατηγικής ανάκαμψης με μηχανισμούς αυτοθεραπείας, μετριάζει σημαντικά τις κυβερνοεπιθέσεις.

4.2 Μοντελοποίηση Επίθεσης Δέντρου [22]

Η ανάλυση των επιπτώσεων ενός συστήματος δικτύου υπολογιστών είναι ένας τρόπος για την αξιολόγηση των συνεπειών μιας επίθεσης και μπορεί να γίνει με απλοποιημένες μεθοδολογίες αναγνώρισης των στόχων του αντιπάλου που είναι τα δέντρα επίθεσης. Ένας γράφος που αποτελείται από κόμβους με πάνω από ένα φύλλα επίθεσης σε κάθε ένα από αυτούς, θεωρείται ένα δέντρο επίθεσης. Αποτελείται από μια πολύ-επίπεδη ιεραρχία που καταγράφει τους πιθανούς τρόπους για την επίτευξη των στόχων. Σε ένα δέντρο επίθεσης, ο αρχικός κόμβος θεωρείται τελικός στόχος κάποιων δευτερευόντων στόχων. Ένα φύλλο επίθεσης προέρχεται από κάποιο αμυντικό κόμβο, που περιέχει αντίμετρα, με ένα ή περισσότερα φύλλα επίθεσης. Ανάλογα με τον κόμβο και την συνδεσιμότητα του, το φύλλο επίθεσης μπορεί να είναι στοιχείων από διάφορα σενάρια εισβολής. Οι προκάτοχοι κάθε φύλλου επίθεσης είναι κόμβοι που τους αποδίδονται λογικοί τελεστές "AND" ή "OR". Στην εικόνα 4 φαίνονται δέντρα επίθεσης με κόμβους "AND" και "OR". Όλα τα φύλλα που οδηγούν σε ένα κουτί "AND" θα πρέπει να διαπεραστούν για να προσπελαστεί προς τα πάνω το δέντρο επίθεσης, δηλαδή, ένα υποσύστημα έχει παραβιαστεί. Από την άλλη πλευρά, στην περίπτωση (b), εάν μόνο ένα από τα φύλλα επίθεσης διαπεραστεί, τότε αυτό είναι επαρκές για να προσπελαστεί προς τα πάνω το δέντρο επίθεσης.



Εικόνα 6. Φύλλα επίθεσης με κόμβους “AND” και “OR”. (α) Φύλλο επίθεσης με κόμβο “AND”. (β) Φύλλο επίθεσης με κόμβο “OR”.

Το πόσο ευάλωτο για κυβερνοεπιθέσεις είναι ένα φύλλο ή ένα δέντρο επίθεσης, φαίνεται από τον δείκτη ευπάθειας του κυβερνοχώρου. Ο δείκτης ευπάθειας παίρνει

τιμές από 0 έως 1, όπου 0 θεωρείται η πιο άτρωτη τιμή και 1 θεωρείται η πιο ευάλωτη τιμή. Κάθε φύλλο επίθεσης, έχει διαφορετικό δείκτη ευπάθειας, ανάλογα με το σενάριο εισβολής. Ωστόσο υπάρχει και ένας γενικός δείκτης ευπάθειας για όλο το σύστημα.

Ένας δείκτης ευπάθειας καθορίζεται με βάση τρεις συνθήκες που παρατίθενται στον Πίνακα 1. Η συνθήκη 1 ικανοποιείται όταν δεν υπάρχουν αποδείξεις για απόπειρες εισβολής σε ένα σύστημα που βασίζεται σε ηλεκτρονικά δεδομένα. Η συνθήκη 2 ικανοποιείται όταν για κάθε φύλλο επίθεσης μπορεί να εφαρμοστεί ένα ή περισσότερα αντίμετρα οποιασδήποτε τεχνολογίας. Η συνθήκη 3 ικανοποιείται όταν εφαρμόζονται μία ή περισσότερες πολιτικές που αντιστοιχούν σε κάθε ένα φύλλο επίθεσης. Οι συνθήκες 2 και 3 σαφώς επηρεάζουν την συνθήκη 1.

Για παράδειγμα όταν ένας server έχει εγκατεστημένο κάποιο σύστημα προστασίας τύπου Firewall έχει την ικανότητα να παρατηρεί και να αποτρέπει τυχόν επιθέσεις που αφορούν στην πρόσβαση. Κάθε ένα φύλλο επίθεσης αξιολογείται και εφαρμόζεται διαφορετικός κωδικός πρόσβασης σε αυτό. Άρα, δεν προσφέρεται εξουσιοδοτημένη πρόσβαση σε έναν εισβολέα που λανθασμένα υποβάλει διάφορους κωδικούς πρόσβασης. Παρόλο που ένα σύστημα μπορεί να διαθέτει προστασία τύπου Firewall, μπορεί εύκολα να κινδυνεύσει από χρήστες μη εξουσιοδοτημένης πρόσβασης.

Συνθήκη 1:	Το σύστημα είναι απαλλαγμένο από απόπειρα εισβολής που συνάγεται από τις ηλεκτρονικές αποδείξεις στο σύστημα
Συνθήκη 2:	Εφαρμόζονται τουλάχιστον ένα ή περισσότερα αντίμετρα για την προστασία μιας επίθεσης
Συνθήκη 3:	Εφαρμόζονται τουλάχιστον μία ή περισσότερες πολιτικές που αντιστοιχούν σε κάθε επίθεση

Πίνακας 1. Κανόνες για τις συνθήκες 1, 2 και 3

Κεφάλαιο 5 - Συγκριτική Αποτίμηση – Συμπεράσματα

5.1 Συγκριτική Αποτίμηση

Στον πίνακα που ακολουθεί συνοψίζονται όσα συμβάντα έχουν καταγραφεί στο κεφάλαιο 3 και αφορούν συμβάντα επιθέσεων στις τέσσερις περιοχές μελέτης. Στον πίνακα σημειώνεται ο τομέας που αφορούσε η επίθεση, το είδος της επίθεσης καθώς και το αποτέλεσμα της.

Κρίσιμες Υποδομές / Χώρες	ΗΠΑ	Ε.Ε	ΡΩΣΙΑ	ΚΙΝΑ
ΣΤΡΑΤΙΩΤΙΚΟΣ ΤΟΜΕΑΣ			2012 Επίθεση κατασκοπείας με αποτέλεσμα την κλοπή Δεδομένων	
ΕΠΙΧΕΙΡΗΣΕΙΣ	2014 Επίθεση κατασκοπείας (APTs) από κινέζους με αποτέλεσμα την κλοπή δεδομένων.	α) 2008 Επίθεση κρυπτογράφησης σε Βρετανικά σούπερ μάρκετ με αποτέλεσμα την κλοπή δεδομένων. β)2018 Επίθεση κρυπτογράφησης σε εταιρία κεραμικών ειδών στο Ηνωμένο Βασίλειο με αποτέλεσμα την κλοπή δεδομένων.		2016 Επίθεση Phishing σε εταιρία κινητής τηλεφωνίας με αποτέλεσμα μεγάλες χρηματικές απώλειες.
ΚΥΒΕΡΝΗΤΙΚΑ ΙΔΡΥΜΑΤΑ		α) 2015 Επίθεση DoS σε κέντρα διανομής ηλεκτρικής ενέργειας της Ουκρανίας με αποτέλεσμα διακοπή λειτουργίας των υπηρεσιών. β) 2017 Επίθεση Ransomware σε νοσοκομεία της Εθνικής Υπηρεσίας Υγείας του Ηνωμένου Βασιλείου με αποτέλεσμα την εκτός σύνδεση δικτύου 61 νοσοκομείων.		

Πίνακας 2. Συγκριτική Αποτίμηση Συμβάντων Μελέτης

5.2 Συμπεράσματα

Η ανάπτυξη του διαδικτύου συμβάλλει σημαντικά στην εξέλιξη της ψηφιακής εποχής και ως εκ τούτου έχει διαμορφώσει εντελώς την καθημερινότητα των πολιτών, δημιουργώντας νέες ευκαιρίες. Το IoT- Διαδίκτυο των πραγμάτων είναι μια τεχνολογία, η οποία διεισδύει σε τομείς κρίσιμων υποδομών με αποκλειστικό στόχο την βελτίωση της ποιότητας των υπηρεσιών που παρέχονται στους ανθρώπους. Ένα από τα πιο βασικά ζητήματα έρευνας στην τεχνολογία του IoT που αφορά στις κρίσιμες υποδομές είναι η ασφάλεια και η προστασία των υποδομών αυτών. Αυτό μπορεί να γίνει με τον εντοπισμό ευπαθειών των συστημάτων και την ανάλυση των απειλών τους. Αφού διερευνηθούν οι προκλήσεις ασφάλειας και τα συμβάντα κυβερνοεγκλήματος σε κρίσιμες υποδομές, μοναδικός σκοπός είναι να βρεθούν όλοι οι πιθανοί τρόποι αντιμετώπισης, προκειμένου να αποφευχθούν παρόμοιες επιθέσεις. Οι Η.Π.Α, η Ευρωπαϊκή Ένωση, η Κίνα και η Ρωσία είναι οι χώρες οι οποίες έχουν συμβάλλει καθοριστικά στην αντιμετώπιση του κυβερνοεγκλήματος παγκοσμίως, καθώς τα στρατηγικά σχέδια που έχουν αναπτύξει, έχουν δημιουργήσει πρότυπα προστασίας δεδομένων και αποτελούν ολοκληρωμένες τεχνικές σε μείζονα θέματα ασφαλείας. Τα παρακάτω συμπεράσματα προέκυψαν από την μελέτη που έγινε για την εκπόνηση της εργασίας αυτής:

1. Ο προσδιορισμός των Κρίσιμων Υποδομών είναι απαραίτητο στοιχείο μιας υγιούς πολιτικής ασφάλειας στον κυβερνοχώρο. Για αυτό και η δυνατότητα της ομαλής λειτουργίας τους με ασφάλεια είναι απαραίτητη για την ζωτική λειτουργία μιας κοινωνίας. Η ενίσχυση των συστημάτων των κρίσιμων υποδομών γίνεται με την λήψη των απαραίτητων μέτρων ασφάλειας, ύστερα από τον έγκυρο εντοπισμό και την αξιολόγηση των αδύνατων σημείων τους.
2. Καθώς τα συστήματα που περιλαμβάνονται σε κρίσιμες υποδομές βασίζονται σε δίκτυα και υπηρεσίες ΤΠΕ, η δημιουργία του IoT συνέβαλε σημαντικά στην βελτίωση της ποιότητας των υπηρεσιών των κρίσιμων υποδομών, καθότι πρόκειται για ένα δίκτυο στο οποίο συνδέονται πολλές συσκευές με ενσωματωμένους αισθητήρες ανταλλάσσοντας πληροφορίες και δεδομένα. Όμως, όσο μεγαλύτερος είναι ο αριθμός των συνδεδεμένων συσκευών, τόσο μεγαλώνει και ο κίνδυνος απειλών ασφαλείας και ευπαθειών που εκτίθενται οι συσκευές αυτές.

3. Μια από τις μεγαλύτερες δημιουργίες του IoT, θεωρείται το έξυπνο πλέγμα (Smart Grid), καθότι πρόκειται για ένα δίκτυο ηλεκτρικής ενέργειας που μειώνει το κόστος χρήσης ηλεκτρικών δικτύων. Όμως είναι εξαιρετικά ευάλωτο σε επιθέσεις, αφού χρησιμοποιεί το IoT. Επιθέσεις που αφορούν σε διαθεσιμότητα του δικτύου, την ακεραιότητα των δεδομένων και το απόρρητο των πληροφοριών.

4. Οι τύποι των αδικημάτων που σχετίζονται με το κυβερνοέγκλημα είναι αρκετοί και έχουν κατηγοριοποιηθεί από την Σύμβαση της Ευρώπης, προκειμένου να μπορεί να γίνει πιο συγκεκριμένη η έρευνα και η ανάλυση τους. Παρόλα αυτά, καθώς αυξάνεται η τεχνολογική εξέλιξη του Διαδικτύου, ο κίνδυνος και οι ευκαιρίες για να διαπραχθεί μια εγκληματική ενέργεια ελλοχεύουν.

5. Η δημιουργία και η εφαρμογή στρατηγικών σχεδίων είναι απαραίτητη για την προστασία του κυβερνοχώρου και προσδιορίζει τρεις στόχους: Την πρόληψη, τον Μετριασμό και την Ελαχιστοποίηση των κυβερνοεπιθέσεων σε κρίσιμες υποδομές. Ο σχεδιασμός ενός στρατηγικού σχεδίου βασίζεται σε αρχές οι οποίες θα πρέπει να τηρούνται στο ακέραιο χωρίς να παραβλέπεται καμία.

6. Υπάρχουν αρκετοί ομοσπονδιακοί οργανισμοί που έχουν αναπτύξει πρότυπα που έχουν δημοσιευτεί και σχετίζονται με την αρχιτεκτονική των δικτύων και την προστασία των δεδομένων της ιδιωτικής ζωής.

7. Οι κρίσιμες υποδομές δεν είναι ίδιες για όλα τα κράτη, καθώς κάθε κράτος θέτει δικά του κριτήρια που χαρακτηρίζουν μία κρίσιμη υποδομή. Αυτό έχει ως αποτέλεσμα να είναι αδύνατον να εφαρμοστεί μία παγκόσμια κοινή πολιτική κυβερνοασφάλειας και κάθε χώρα να πρέπει να σχεδιάσει και να εφαρμόσει δικό της στρατηγικό σχέδιο, που αφενός το διέπουν οι βασικές αρχές προστασίας και αφετέρου, στηρίζεται σε νόμους και κανόνες της συγκεκριμένης χώρας που το σχεδιάζει.

8. Στο κεφάλαιο 3 έγινε εκτενής αναφορά στα στρατιωτικά πλαίσια που εφαρμόζονται στην Ευρωπαϊκή Ένωση και κατ᾽επέκταση στην Ελλάδα, στις Η.Π.Α, στην Ρωσία και στην Κίνα. Διαπιστώσαμε ότι οι εθνικές στρατηγικές ασφαλείας εκτός του ότι διαφέρουν σημαντικά μεταξύ τους, έχουν και αντικρουόμενα συμφέροντα. Για παράδειγμα, η Ρωσία βλέπει τα ζητήματα

κυβερνοασφάλειας ως μια ευκαιρία για να συμμετέχει σε στρατιωτικές δράσεις και επιχειρήσεις.

9. Σε επίπεδο Ευρωπαϊκής Ένωσης, έχει συσταθεί ο οργανισμός ENISA με αποκλειστικό ρόλο την ενδυνάμωση της ασφάλειας των δικτύων και των πληροφοριών εντός της Ευρωπαϊκής Ένωσης. Προτεραιότητα του θεωρείται η εφαρμογή μιας κοινής πολιτικής ασφάλειας της Ευρωπαϊκής Ένωσης με την συνεργασία των κρατών-μελών, όσον αφορά στην πρόληψη των κυβερνοεπιθέσεων. Οι οδηγίες της Ευρωπαϊκής Ένωσης προβλέπουν ότι τα κράτη-μέλη μπορούν να ζητήσουν την συνδρομή του ENISA για την ανάπτυξη εθνικών στρατηγικών, για την ασφάλεια των συστημάτων δικτύων και πληροφοριών.

10. Στην Ελλάδα, προκειμένου να δημιουργηθεί και να εφαρμοστεί στρατηγικό σχέδιο δράσης, εμπλέκονται αρκετοί κρατικοί φορείς οι οποίοι έχουν και την ευθύνη παρακολούθησης του, ενώ στην Αμερική το σχέδιο δράσης ενθαρρύνει κυρίως ιδιωτικούς φορείς να ενημερώνουν την κυβέρνηση για κρούσματα και απειλές στον κυβερνοχώρο.

11. Η Κίνα καθώς αποτελεί την δεύτερη μεγαλύτερη οικονομία του κόσμου, είναι αρκετά ευάλωτη στον κυβερνοχώρο. Για αυτό και η συνεισφορά δομών και οργανισμών που παρέχουν υπηρεσίες προστασίας στην διαχείριση της κυβερνοασφάλειας, είναι πολύτιμη. Τέτοιοι είναι η εταιρεία KPMG και η ρυθμιστική αρχή CAC.

12. Η Ρωσία έχοντας απορρίψει την Σύμβαση του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα, καθώς υποστηρίζει ότι παραβιάζεται το Σύνταγμα της χώρας, δημιούργησε ειδικό τμήμα κυβερνοπολέμου το οποίο παρακολουθεί και καταπολεμά τις απειλές και τις επιθέσεις στον κυβερνοχώρο, διεξάγοντας επιθετικές και αμυντικές επιχειρήσεις, συγκεντρώνοντας πληροφορίες από ξένες πηγές.

13. Σημαντικά παραδείγματα κυβερνοεγκλήματος που αναφέρονται στην παρούσα εργασία στο 3ο κεφάλαιο, αποτελούν αφορμή για εκτεταμένη έρευνα παγκοσμίως στον τομέα της κυβερνοασφάλειας. Η ανάλυση των ιδιοτήτων των συστημάτων που έλαβαν χώρα οι επιθέσεις, καθώς και η ανάλυση των επιπτώσεων οδήγησαν στο να οριστούν τεχνικές συστημάτων ασφαλείας και

μετριασμού των κινδύνων. Τέτοιες τεχνικές εφαρμόζονται στα συστήματα SCADA.

14. Τα συστήματα SCADA αποτελούνται από τοπικούς ελεγκτές συνδεδεμένους σε ένα κεντρικό τερματικό. Πρόκειται για συστήματα βιομηχανικού ελέγχου και τηλεμετρίας που μπορούν να εφαρμόζονται σε κρίσιμες υποδομές, καταγράφοντας πληροφορίες που εξασφαλίζουν την ορθή και ευφυή λειτουργία των υποδομών. Επειδή όμως εκτίθενται σε περιβάλλοντα IoT και Cloud είναι πολύ ευάλωτα και παρουσιάζουν ευπάθειες. Οι συνηθέστερες απειλές που συναντάμε στα συστήματα SCADA είναι οι APTs (Advanced Persistent Threats) επιθέσεις, οι επιθέσεις MITM(Man in the middle) και οι επιθέσεις άρνησης εξυπηρέτησης DoS (Denial of Service). Ένα προτεινόμενο πλαίσιο ασφάλειας SCADA βασίζεται σε 4 συνιστώσες οι οποίες είναι:
    i. Παρακολούθηση σε πραγματικό χρόνο
    ii. Ανίχνευση Ανωμαλιών
    iii. Ανάλυση Επιπτώσεων
    iv. Στρατηγικές μετριασμού RAIM (Real Time Anomaly Impact Mitigation)
15. Η ανάλυση των επιπτώσεων ενός συστήματος προσδιορίζει τον τρόπο αξιολόγησης των συνεπειών μέσω μεθοδολογικής αναγνώρισης των στόχων του αντιπάλου που ονομάζονται δέντρα επίθεσης. Ένα δέντρο επίθεσης, είναι ένας γράφος αποτελούμενος από κόμβους, όπου κάθε κόμβος είναι ένα φύλλο επίθεσης. Το δέντρο ακολουθεί μία πολυεπίπεδη ιεραρχία που καταγράφει τους πιθανούς τρόπους για την επίτευξη των στόχων.

Κεφάλαιο 6 - Μελλοντική Εργασία – Επίλογος

6.1 Μελλοντική Εργασία

Για τον σχεδιασμό και την υλοποίηση της παρούσας εργασίας παρατέθηκαν στοιχεία που αφορούν αμιγώς σε βιβλιογραφική επισκόπηση. Αυτό σημαίνει ότι δεν διενεργήθηκε έρευνα με αποδεικτική ισχύ αναφορικά με το θέμα της εργασίας, για τον λόγο ότι ο σκοπός της εργασίας ήταν η θεωρητική επισκόπηση των κυβερνοεγκλημάτων στον τομέα των Κρίσιμων Υποδομών. Παρόλα αυτά, μιας και η ραγδαία ανάπτυξη της τεχνολογίας, οδηγεί ταυτόχρονα και σε παράλληλη αύξηση των κρουσμάτων επιθέσεων στον κυβερνοχώρο, παρακάτω προτείνονται κάποια θέματα, που θα μπορούσαν να αποτελέσουν έμπνευση για μελλοντική εξέταση σχετικά με απειλές γύρω από τις κρίσιμες υποδομές:

- Δημιουργία αυτόματων μηχανισμών εργασίας περιστατικών, για ενίσχυση της Εθνικής Κυβερνοασφάλειας με προσαρμογή των κατάλληλων μέτρων ασφάλειας στο συνεχές εναλλασσόμενο τοπίο των απειλών. Αυτός ο τρόπος μπορεί να βοηθήσει σε μία εκτενή ανάλυση των σεναρίων αποτυχίας, με την χρήση αλγορίθμων ανάλυσης γράφων οι οποίοι, θα εντοπίζουν όχι μόνο το κρίσιμο μονοπάτι αλλά και άλλα εναλλακτικά μονοπάτια μετριάζοντας την επικινδυνότητα [22].

- Συνεργασία μεταξύ του ιδιωτικού και δημόσιου τομέα. Όπως αναφέρθηκε μέσα στην εργασία, ήδη στις Η.Π.Α. ο ιδιωτικός τομέας παρέχει σημαντικές υπηρεσίες στο κράτος, ενημερώνοντας για τα περιστατικά Κυβερνοεπιθέσεων. Μια έρευνα γύρω από την παροχή κινήτρων στον ιδιωτικό τομέα για επενδύσεις σε μέτρα ασφάλειας, θα βοηθήσει στην καλύτερη συνεργασία μεταξύ ιδιωτικού και δημόσιου τομέα, καθώς θα αποτελεί ένα χρήσιμο εργαλείο για την αποτελεσματική χρήση των κοινών ικανοτήτων και εμπειριών [14].

- Έμφαση στην επιρροή της Νέας Τεχνολογίας και πως διασφαλίζεται η προστασία και η ανθεκτικότητα των κρίσιμων υποδομών. Σε μια εποχή όπου ο τεχνολογικός παράγοντας κατέχει κυρίαρχη θέση, η αναγκαιότητα για διαρκής έρευνα γύρω από την προστασία των πληροφοριακών συστημάτων είναι επιβεβλημένη και θα πρέπει συνεχώς να διασφαλίζεται με νέα πρότυπα ασφάλειας περί διαχείρισης επικινδυνότητας τύπο ISO [2] [5] [8].

- Η τεχνητή Νοημοσύνη να συμβάλλει περισσότερο στον έλεγχο εξοπλισμού μέσω ρομπότ επιθεώρησης, μειώνοντας έτσι το χρόνο τυχόν επισκευών της βλάβης από μία επίθεση αλλά και μακροπρόθεσμα από το επιπλέον κόστος [2].

6.2 Επίλογος

Η παρούσα εργασία υπογράμμισε την ανάγκη για αποτελεσματικές λύσεις στον τομέα της ασφάλειας των Κρίσιμων Υποδομών δίνοντας ιδιαίτερη σημασία στην προστασία των συστημάτων πληροφοριών από κακόβουλες επιθέσεις.

Η ραγδαία εξελισσόμενη τεχνολογία και η υπερεθνική διάσταση που παίρνουν κάποια κυβερνοεγκλήματα, είναι οι βασικότεροι παράγοντες που δυσχεραίνουν το έργο της κάθε χώρας σχετικά με τον σχεδιασμό και την λήψη μέτρων ενάντια στις κυβερνοεπιθέσεις.

Η ασφάλεια και η άμυνα εναντίον των απειλών στον κυβερνοχώρο, είναι ένα επίμονο πρόβλημα παγκοσμίως και απαιτεί την επισταμένη προσοχή των Κρατικών Υπηρεσιών. Για την ενίσχυση του επιπέδου της ασφάλειας του κυβερνοχώρου και τη διαφύλαξη των δικαιωμάτων των πολιτών απαιτείται όμως και η ισχυρή υποστήριξη και δέσμευση από τον ιδιωτικό τομέα καθώς οι προκλήσεις που έχουν να αντιμετωπίσουν και ο ιδιωτικός και ο δημόσιος τομέας έχουν εντυπωσιακές ομοιότητες.

Καθώς οι σύγχρονες εγκληματικές απειλές χαρακτηρίζονται από την χρήση υψηλής τεχνογνωσίας συστημάτων, η πρόληψη εκδήλωσης των επιθέσεων, η ανίχνευσή τους και τελικώς η άμεση αντιμετώπισή τους επιβάλλει τον συνεχή εκσυγχρονισμό των συστημάτων, που εφαρμόζουν οι Κρίσιμες Υποδομές, με τις νέες τεχνολογίες.

Κλείνοντας, πρέπει να τονιστεί η ανάγκη για συνεργασία και ο συντονισμός των προσπαθειών σε παγκόσμιο επίπεδο καθώς το μόνο σίγουρο είναι ότι μία απειλή/στόχος μπορεί να καταστραφεί ταχύτερα και πιο εύκολα όταν είναι πολλοί οι «σκοπευτές» που βάλλουν.

Βιβλιογραφία

[1] D. Rehak, “Assessing and strengthening organisational resilence in a critical infrastructure system: Case study of the Slovac Republic.,” 2020.

[2] E. Vigano, E. Yaghmaei and M. Loi, “Cybersecurity of Critical Infrastructure,” 2019.

[3] D. Rehak, M. Hromada and T. Lovecek, “Personnel threats in the electric power critical infrastacture sector and their effect on depentent sector: Overview in the Czech Republic,” *Safety Science,* no. 127, 2020.

[4] T. E. Ademilua, “Challenge in Critical Infrastructures Security,” 2019.

[5] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, “CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques,” *IEEE,* 2019.

[6] A. T. Chatfield and C. Reddick, “A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government,” *Government Information Quarterly,* 2019.

[7] S. Rizvi, J. Pfeffer, A. Kurtz and M. Rizvi, “Securing the Internet of Things(IoT): A Security Taxonomy for IoT,” *IEEE,* 2018.

[8] J. Pacheco and S. Hariri, “IoT Security Framework for Smart Cyber Infrastructures,” *IEEE,* 2016.

[9] A. Tewari and B. Gupta, “Security, Privacy and Trust of different layers in Internet-of-Things(IoTs) Framework,” *Future Generation Computer System,* 2018.

[10] K. Sollins, “IoT Big Data Security and Privacy vs. Innovation,” *Internet of Things Journal,* 2018.

[11] S.-h. Oh and Y.-G. Kim, “Security Requirements Analysis for the IoT,” *IEEE,* 2017.

[12] Z. Baig, P. Szewczyk, G. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed and M. Peacock, “Future

Challenges for smart cities: Cyber-Security and digital forensics.," *Digital Investigation,* 2017.

[13] E. Pauri, "Agency Reform in the time of Cybersecurity Governance: ENISA," https://iris.luiss.it/retrieve/handle/11385/185996/77841/ENISA%20Pauri%20pubblicato.pdf, 2017.

[14] J. Srinivas, A. K. Das and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generations Computer Systems,* 2019.

[15] S. Helfenstein and P. Saariluoma, How Cyber Breeds Crime and Criminals, SDIWC, 2014.

[16] "ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ," 2020. [Online]. Available: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1.

[17] M. Jiang, "Cybersecurity Policies in China," *CyberBRICS: Mapping cybersecurity frameworks in the BRICS,* 2020.

[18] N. Kshetri, "Cybersecurity in Russia," *The Quest to Cyber Superiority,* 2016.

[19] M. Saleem, "Brexit Impact on Cyber Security of United Kingdom," 2019.

[20] X. Qian, "Cyberspace Security and U.S.- China Relations," *Association for Computing Machinnery,* 2019.

[21] D. Stitilis, P. Pakutinskas and I. Malinauskaite, "EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis," *Security Journal,* 2016.

[22] C.-W. Ten, G. Manimaran and C.-C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” no. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2010.

[23] A. Sajid, H. Abbas and K. Saleem, “Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges,” 2016.