



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Gender and Cybersecurity: Theoretical considerations, Tools
and Guidance**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Αικατερίνης Παπαβέντση

Επιβλέπουσα: Βασιλική Διαμαντοπούλου

Μέλη εξεταστικής επιτροπής: Μαρία Καρύδα, Ευαγγελία Μήτρου

Σάμος, Οκτώβριος 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια της διπλωματικής μου, κυρία Βασιλική Διαμαντοπούλου, για την συνεχή καθοδήγηση και τις συμβουλές της κατά την διάρκεια της εκπόνησης της εργασίας αυτής.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, τους γονείς και την αδερφή μου για την στήριξη, την κατανόηση και την ενθάρρυνσή τους καθ' όλη την διάρκεια των σποδών μου.

© 2024

της

Αικατερίνης Παπαβέντση

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1	Εισαγωγή	12
1.1	Το πλαίσιο της διπλωματικής εργασίας.....	12
1.2	Αντικείμενο διπλωματικής	13
1.3	Δομή της διπλωματικής	13
2	Διαχωρισμός των φύλων στον επαγγελματικό τομέα της επιστήμης της πληροφορικής.....	15
2.1	Η αντιμετώπιση των γυναικών στον τομέα της πληροφορικής.....	15
2.2	Η αντιμετώπιση των φύλων στον κλάδο της κυβερνοασφάλειας.	16
2.3	Τα φύλα σε διευθυντικές θέσεις στον τομέα της κυβερνοασφάλειας	18
3	Απαιτούμενες δεξιότητες στον εργασιακό χώρο της κυβερνοασφάλειας	22
3.1	Απαιτούμενες δεξιότητες στον χώρο της κυβερνοασφάλειας: κάτι παραπάνω από τεχνολογικές γνώσεις.....	22
3.2	Απαραίτητες τεχνολογικές γνώσεις στον κυβερνοχώρο.	24
3.2.1	Ασφάλεια Cloud	25
3.2.2	Γνώση λειτουργικών συστημάτων	26
3.2.3	Ασφάλεια δικτύου.....	27
3.2.4	Διαδίκτυο των Πραγμάτων (IoT)	28
3.2.5	Γνώση τεχνολογίας Blockchain.....	29
3.3	Δεξιότητες κυβερνοασφάλειας και ποικιλομορφία των φύλων	31
4	Κυβερνοασφάλεια και εκπαίδευση.....	33
4.1	Προκλήσεις που αντιμετωπίζουν τα φύλα στην εκπαίδευση για την κυβερνοασφάλεια	33
4.1.1	Κοινωνικά εμπόδια	33
4.1.2	Έλλειψη οικογενειακής υποστήριξης.....	35
4.1.3	Έλλειψη σχολικής υποστήριξης	36
4.2	Εκπαιδευτικές προσεγγίσεις κυβερνοασφάλειας.....	37
4.2.1	Πανεπιστημιακή εκπαίδευση	37
4.2.2	Συνεργασία Πανεπιστημίων και εργοδοτών.	40
4.2.3	Η Παιχνιδοποίηση της εκπαίδευσης (Gamification)	42
4.2.4	Cybercompetitions.....	45
5	Σύνοψη και Συμπεράσματα	47
5.1	Σύνοψη.....	47
5.2	Συμπεράσματα	49
5.3	Προτάσεις για αύξηση των γυναικών στον τομέα της πληροφορικής και της κυβερνοασφάλειας	50

5.4	Προτάσεις για ενίσχυση της εκπαίδευσης στην κυβερνοασφάλεια	51
5.5	Προτάσεις για μελλοντική έρευνα.....	53
Βιβλιογραφία		54

Λίστα Σχημάτων

Σχήμα 1. Πτώση ποσοστού γυναικών στο πεδίο της επιστήμης της πληροφορικής ανά τα χρόνια.....	21
Σχήμα 2. Σύνθεση του εργατικού δυναμικού κυβερνοασφάλειας, ανά περιοχή.....	22
Σχήμα 3. Ποσοστά γυναικών (που εκτιμώνται στο εργασιακό περιβάλλον και που δεν εκτιμώνται) που επωφελήθηκαν από χορηγίες.....	25
Σχήμα 4. Κατανομή των φύλων σε διοικητικές θέσεις στον τομέα της κυβερνοασφάλειας παγκοσμίως...25	
Σχήμα 5. Ο hacker μπορεί εύκολα να πάρει τα δεδομένα που μεταφέρονται από τον χρήστη. Εδώ έχουμε απώλεια σημαντικών δεδομένων.....	31
Σχήμα 6. Functions of Operating Systems.....	32
Σχήμα 7. Το τείχος προστασίας αναχαιτίζει την κυκλοφορία δικτύου στο σημείο εισόδου ενός υπολογιστή.....	33
Σχήμα 8. Οι 4 σημαντικές ευπάθειες IoT συσκευών.....	34
Σχήμα 9. Ο ρόλος του Blockchain στην ενίσχυση και βελτίωση της ασφάλειας σε ένα δίκτυο εφοδιαστικής αλυσίδας.....	36
Σχήμα 10. «Οι ρόλοι της ασφάλειας στον κυβερνοχώρο θεωρούνται ως “ανδρικές δουλειές” στην κοινωνία».....	39
Σχήμα 11. «Με ενθάρρυνε η οικογένειά μου να δουλέψω στην κυβερνοασφάλεια».....	41
Σχήμα 12. «Είχα αποτελεσματική πρόσβαση σε πληροφορίες σχετικά με το πώς να ενταχθώ στον τομέα της κυβερνοασφάλειας. ».....	42
Σχήμα 13. Μεταπτυχιακά προγράμματα Κυβερνοασφάλειας σε διάφορες χώρες.....	44
Σχήμα 14. Πώς λειτουργεί η Παιχνιδοποίηση.....	47

Λίστα Πινάκων

Πίνακας 1. Διαγωνισμοί που σχετίζονται με θέματα κυβερνοασφάλειας.....	50-51
--	-------

Ακρωνύμια

AWS	Amazon Web Services
TΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
STEM	Science, Technology, Engineering and Mathematics
AAUW	American Association of University Women
IHL	Institutes of Higher Learning
NCSC	National Cyber Security Centre
(ISC) ²	International Information System Security Certification Consortium
CAE	Centers for Academic Excellence
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
ISACA	Information Systems Audit and Control Association.
VMs	Virtual Machines
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΕΕ	Ευρωπαϊκή Ένωση

Περίληψη

Στη σύγχρονη εποχή ένας από τους ταχύτερα αναπτυσσόμενους κλάδους της πληροφορικής είναι αυτός της κυβερνοασφάλειας. Η κυβερνοασφάλεια διαδραματίζει έναν κρίσιμο ρόλο στην προστασία των επιχειρήσεων, αλλά και των ανθρώπων και πλήττεται καθημερινά από πολλές επιθέσεις. Η ζήτηση για την κάλυψη των θέσεων εργασίας στον τομέα αυτόν είναι μεγάλη, όμως οι διαθέσιμοι εξειδικευμένοι επαγγελματίες δεν είναι αρκετοί για να καλύψουν τα κενά αυτά. Οι γυναίκες σήμερα καλύπτουν ένα πολύ μικρό ποσοστό των θέσεων αυτών.

Στα πλαίσια της εργασίας αυτής εξετάζουμε την αντιμετώπιση του επαγγελματικού κλάδου της πληροφορικής απέναντι στα φύλα. Η εργασία βασίζεται σε έρευνες για να αξιολογήσει τις διαφορές, λόγω φύλου, στον τομέα της κυβερνοασφάλειας. Πιο συγκεκριμένα, ερευνούμε κατά πόσο οι γυναίκες έχουν τις ίδιες ευκαιρίες με τους άντρες στον χώρο αυτόν αλλά και αν αντιμετωπίζονται ισάξια με αυτούς. Το φύλο ενός ανθρώπου ορίζει την ατομική του ταυτότητα και δημιουργεί τις ανάλογες προσδοκίες στους ανθρώπους, οι οποίοι τις περισσότερες φορές είναι προκατειλημμένοι και έχουν στερεοτυπικές αντιλήψεις στον χώρο της πληροφορικής.

Στην συνέχεια της διπλωματικής εργασίας, αναλύουμε τις τεχνολογικές και μη τεχνολογικές δεξιότητες και γνώσεις που θα πρέπει να έχει ένας επαγγελματίας κυβερνοασφάλειας. Αναφέρονται συγκεκριμένα κάποια κοινωνικά χαρακτηριστικά που είναι σημαντικά αλλά και πιο αναλυτικά κάποιοι τεχνολογικοί τομείς της πληροφορικής των οποίων η γνώση είναι απαραίτητη για την επίτευξη της ασφάλειας στον κυβερνοχώρο ανεξάρτητα από το φύλο του εργαζομένου.

Τέλος, εξετάζουμε εάν υπάρχουν ισάξιες ευκαιρίες για τα φύλα στην εκπαίδευση για την απόκτηση δεξιοτήτων κυβερνοασφάλειας καθώς και τις προκλήσεις και τα εμπόδια που παρουσιάζονται στον δρόμο της εκμάθησης της ασφάλειας στον κυβερνοχώρο. Δίνουμε έμφαση στον κοινωνικό περίγυρο των μαθητών, στην σχολική αλλά και οικογενειακή υποστήριξη που τους παρέχεται. Επίσης, παρουσιάζονται εργαλεία και εκπαιδευτικές προσεγγίσεις της κυβερνοασφάλειας, τα οποία μπορούν να καθοδηγήσουν τους σπουδαστές και να τους δώσουν τα απαραίτητα εφόδια και γνώσεις ώστε να εξειδικευτούν στον τομέα αυτόν, με στόχο την κάλυψη των κενών θέσεων εργασίας στην ασφάλεια στον κυβερνοχώρο.

Λέξεις Κλειδιά: κυβερνοασφάλεια, φύλα, γυναίκες, στερεοτυπικές αντιλήψεις, δεξιότητες, εργαλεία-τρόποι εκπαίδευσης, προκλήσεις-εμπόδια.

Abstract

In modern times, one of the fastest growing IT industries is cybersecurity. Cybersecurity plays a critical role in protecting businesses, as well as people, and is affected by many attacks every day. The demand for jobs in this field is high, but the skilled professionals available are not enough to fill these gaps. Women currently fill a very small percentage of these positions.

In the context of this paper, we examine the gendered approach of the IT profession. The paper relies on surveys to evaluate gender differences in the cybersecurity sector. More specifically, we investigate whether women have the same opportunities as men in this field and whether they are treated equally with men. A person's gender defines their individual identity and creates the corresponding expectations in people, who are most often prejudiced and have stereotypical perceptions in the IT field.

In the following part of the thesis, we analyze the technological and non-technological skills and knowledge that a cybersecurity professional should have. We specifically mention some social characteristics that are important but also elaborate on some technological areas of IT whose knowledge is necessary to achieve cybersecurity regardless of the gender of the employee.

Finally, we examine whether there are equal opportunities for gender in education to acquire cybersecurity skills as well as the challenges and barriers presented on the path to learning cybersecurity. We focus on the social environment of the students, the school and family support provided to them. We also present tools and educational approaches of cybersecurity, which can guide students and provide them with the necessary skills and knowledge to specialize in this field, with the aim of filling the job gaps in cybersecurity.

Keywords: *cybersecurity, gender, women, stereotypical perceptions, skills, tools-methods of training, challenges-barriers.*

1 *Εισαγωγή*

1.1 Το πλαίσιο της διπλωματικής εργασίας

Η ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας για την εθνική, την ομοσπονδιακή και τοπική κυβέρνηση, για τον στρατό, τις βιομηχανίες, ακόμη και για την προσωπική ιδιωτική ζωή κάθε ανθρώπου. Για την υπεράσπιση των όλων αυτών έναντι των απειλών στον κυβερνοχώρο, υπάρχει μια σημαντική ζήτηση για εξειδικευμένο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας σε ακαδημαϊκό επίπεδο. Στην σύγχρονη εποχή, η ανισότητα μεταξύ των φύλων στον κυβερνοχώρο είναι ένα αποθαρρυντικό γεγονός για τις γυναίκες που επιδιώκουν να εξελιχθούν στον τομέα αυτόν. Μελέτες αποκαλύπτουν ότι οι γυναίκες αντιπροσωπεύουν ένα αρκετά μικρό ποσοστό του παγκόσμιου εργατικού δυναμικού στον τομέα της ασφάλειας των πληροφοριών, και ότι πολύ λίγες κατέχουν ηγετικές θέσεις. Το ποσοστό των γυναικών που εργάζονται στον τομέα της πληροφορικής είναι χαμηλό, και είναι ακόμη χαμηλότερο για την ασφάλεια στον κυβερνοχώρο. Λόγω έλλειψης ενθάρρυνσης, οι γυναίκες έχουν αμφιβολίες σχετικά με το αν έχουν τη σωστή εξειδικευμένη ικανότητα ή το επιχειρηματικό όραμα για να διαπρέψουν στο επάγγελμα αυτό.

Οι παραβιάσεις της ασφάλειας είναι διαδεδομένες στους οργανισμούς και πολλές από αυτές αποδίδονται σε ανθρώπινα λάθη. Για αυτόν τον λόγο, οι οργανισμοί πρέπει να αυξήσουν την ευαισθητοποίηση των υπαλλήλων τους σε θέματα ασφάλειας και να ενισχύσουν τις ικανότητές τους στην ασφάλεια στον κυβερνοχώρο. Η κυβερνοασφάλεια αποτελεί πλέον απαραίτητη προϋπόθεση για τους σύγχρονους οργανισμούς, αλλά υπάρχει έλλειψη εξειδικευμένου προσωπικού για την υποστήριξη των απαιτούμενων ρόλων και αρμοδιοτήτων. Παρόλο που διατίθενται πολυάριθμα σχετικά προσόντα και πιστοποιήσεις, είναι καίριας σημασίας να κατανοήσουμε τις δεξιότητες που είναι απαραίτητες να έχει κάποιος για να προσληφθεί στο επάγγελμα αυτό. Τα ακαδημαϊκά πτυχία και οι επαγγελματικές πιστοποιήσεις υποδηλώνουν ότι έχει επιτευχθεί ένα συγκεκριμένο επίπεδο γνώσεων. Ωστόσο, λόγω των ταχέων αλλαγών στη ζήτηση δεξιοτήτων κυβερνοασφάλειας, οι άνθρωποι που εργάζονται στον τομέα χρειάζονται ένα συνδυασμό τεχνικών και μη τεχνικών δεξιοτήτων καθώς και κοινωνικής νοημοσύνης για να κάνουν σωστά και αποτελεσματικά την δουλειά τους.

Όσο αναφορά την εκπαίδευση στον τομέα της κυβερνοασφάλειας, τα φύλα δεν έχουν πάντα τις ίδιες ευκαιρίες. Το ποσοστό των γυναικών που σπουδάζουν στην επιστήμη της πληροφορικής είναι αρκετά μικρότερο σε σχέση με αυτό των ανδρών. Από πολύ μικρή ηλικία αποθαρρύνονται από τον περίγυρό τους να ασχοληθούν σοβαρά με τον τομέα αυτόν πόσο μάλλον πιο συγκεκριμένα με τον τομέα της κυβερνοασφάλειας.

Υπάρχουν αρκετά πανεπιστήμια στον κόσμο που εξειδικεύονται στον τομέα της κυβερνοασφάλειας, αν και θα μπορούσαν να υπάρχουν και περισσότερα. Με λίγη έρευνα μπορεί κανείς να βρει πολλά διπλώματα, μεταπτυχιακά σεμινάρια και διαγωνισμούς μέσω των οποίων μπορούν να εκπαιδευτούν στον τομέα της ασφάλειας στον κυβερνοχώρο.

1.2 Αντικείμενο διπλωματικής

Αντικείμενο της παρούσας διπλωματικής, όπως αναφέρεται και στον τίτλο, είναι να παρατηρήσουμε την αντιμετώπιση των φύλων μέσα στον εργασιακό τομέα της κυβερνοασφάλειας. Πιο συγκεκριμένα, ερευνούμε την θέση των φύλων στην κυβερνοασφάλεια, την αντιμετώπισή τους από τους συναδέλφους τους και τις προοπτικές του καθενός στην εξέλιξη της καριέρας του στον τομέα αυτόν.

Στην έρευνά μας για την διπλωματική, αναγνωρίζουμε τις σημαντικές ικανότητες που πρέπει να έχει κάποιος στον χώρο της κυβερνοασφάλειας ανεξαρτήτως φύλου. Οι ικανότητες αυτές δεν πρέπει να είναι μόνο τεχνολογικές αλλά και μη-τεχνολογικές. Σκοπός είναι να τονίσουμε το πόσο σημαντική είναι η ποικιλομορφία στο εργατικό δυναμικό ενός οργανισμού. Άλλωστε, τις απαραίτητες δεξιότητες μπορούν να τις κατέχουν όλοι οι άνθρωποι που έχουν εκπαιδευτεί, ανεξαρτήτως φύλου. Για αυτόν τον λόγο, οι εργοδότες δεν πρέπει να κάνουν φυλετικές διακρίσεις καθώς οι πολλές και διαφορετικές γνώσεις και γνώμες μπορούν να δημιουργήσουν μία πολύ δυνατή ομάδα κυβερνοασφάλειας.

Μέσα από την έρευνα μας προσπαθούμε να αναδείξουμε τα εμπόδια που μπαίνουν στον δρόμο της εκπαίδευσης των φύλων στον τομέα της κυβερνοασφάλειας. Καταγράφουμε τις προκλήσεις που αντιμετωπίζει κάθε φύλο, από μικρή ακόμη ηλικία, αν θέλει να ασχοληθεί με την τεχνολογία και την πληροφορική. Στόχος είναι να καταγράψουμε τρόπους και εργαλεία με τα οποία μπορεί κάποιος που ενδιαφέρεται για την κυβερνοασφάλεια να εκπαιδευτεί πάνω σε αυτήν. Η πανεπιστημιακή εκπαίδευση είναι ένα μικρό κομμάτι της εκπαίδευσης των φοιτητών, καθώς αν συνδυαστεί με πρακτική άσκηση και συμμετοχή σε διαγωνισμούς μπορεί να επεκτείνει τις ικανότητες και δεξιότητες τους.

1.3 Δομή της διπλωματικής

Στο κεφάλαιο 1 της παρούσας εργασίας γίνεται μια αναφορά στο αντικείμενο και το περιεχόμενο της διπλωματικής. Στο Κεφάλαιο 2 αναλύεται ο διαχωρισμός των φύλων στον εργασιακό τομέα της κυβερνοασφάλειας. Πιο συγκεκριμένα, αναφέρουμε τις προκαταλήψεις που αντιμετωπίζουν τα φύλα στην δουλειά τους στον χώρο αυτό αλλά και τις πιθανότητες επαγγελματικής εξέλιξης και κατάκτησης ανώτερων θέσεων στον τομέα της ασφάλειας στον κυβερνοχώρο. Στο Κεφάλαιο 3 αναφέρουμε τις απαραίτητες δεξιότητες που πρέπει κάποιος να κατέχει για να εργαστεί στην κυβερνοασφάλεια, τεχνολογικές και μη. Γίνεται επίσης μια πιο λεπτομερής περιγραφή κάποιων

τεχνολογικών γνώσεων που απαιτεί ο τομέας αυτός. Επιπλέον, γίνεται αναφορά στους λόγους που είναι απαραίτητη η ποικιλομορφία του εργατικού δυναμικού ενός οργανισμού. Στο Κεφάλαιο 4 ερευνούμε το κομμάτι της εκπαίδευσης στην κυβερνοασφάλεια. Αναφέρονται οι προκλήσεις που αντιμετωπίζει το κάθε φύλο στην εκπαίδευση του στον κυβερνοχώρο. Ακόμη γίνεται μια ανάλυση των εκπαιδευτικών προσεγγίσεων της κυβερνοασφάλειας και με ποια μέσα μπορεί κάποιος να αποκτήσει τις καλύτερες δυνατές ικανότητες για να εργαστεί στον χώρο. Τέλος, η διπλωματική αυτή εργασία ολοκληρώνεται με το Κεφάλαιο 5 το οποίο περιέχει τα συμπεράσματα και την σύνοψη της εργασίας, καθώς και κάποιες προτάσεις για μελλοντική έρευνα που θα ήταν απαραίτητο να γίνει.

2

Διαχωρισμός των φύλων στον επαγγελματικό τομέα της επιστήμης της πληροφορικής

2.1 Η αντιμετώπιση των γυναικών στον τομέα της πληροφορικής

Στην σύγχρονη κοινωνία, η επιστήμη της πληροφορικής κυριαρχείται κυρίως από άνδρες. Αυτό όμως δεν ήταν πάντα έτσι, καθώς οι άνθρωποι οι οποίοι προγραμματίσαν τους πρώτους ψηφιακούς υπολογιστές ήταν γυναίκες. Για αρκετές δεκαετίες ο αριθμός των γυναικών που σπούδαζαν πληροφορική και κατά επέκταση εργάζονταν σε αυτόν τον τομέα αυξανόταν ταχύτερα από τον αριθμό των ανδρών. Το 1984 αυτό άλλαξε και το ποσοστό των γυναικών στις σπουδές πληροφορικής έπεσε κατακόρυφα. Οι γυναικείες θέσεις στον κλάδο της πληροφορικής άρχισαν να μειώνονται την ίδια στιγμή που άρχισαν να εμφανίζονται οι προσωπικοί υπολογιστές σε έναν μεγάλο αριθμό σπιτιών. Οι πρώτοι αυτοί προσωπικοί υπολογιστές δεν ήταν κάτι περισσότερο από παιχνίδια τα οποία απευθύνονταν κυρίως σε αγόρια και άνδρες. Έτσι, αναπτύχθηκε η γενικότερη αντίληψη ότι οι υπολογιστές είναι για τους άνδρες. Από τότε λοιπόν, το γενικότερο κοινωνικό περιβάλλον ξεκίνησε να τροφοδοτεί τη χαμηλή αυτοεκτίμηση των γυναικών σχετικά με τις δυνατότητές τους στους υπολογιστές [1].

Στον χώρο εργασίας της πληροφορικής, ο οποίος είναι κυρίως ανδροκρατούμενος, οι γυναίκες έρχονται πλέον αντιμέτωπες με διαφυλικές διακρίσεις και πολύ σπάνια δέχονται υποστήριξη από μέντορες. Σε μία έρευνα του Πανεπιστημίου Πατρών, οι απόφοιτοι του Τμήματος Μηχανικών Η/Υ και Πληροφορικής, της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών που συμμετείχαν, αναφέρουν πως ως γυναίκες στην αρχή της καριέρας τους χρειάστηκε να προσπαθήσουν πολύ περισσότερο από τους άνδρες συναδέλφους τους για να κερδίσουν την εμπιστοσύνη των υπολοίπων. Επίσης, οι γνώσεις και τα προσόντα τους δεν αναγνωρίζονται τόσο εύκολα, οι συνάδελφοί τους τις αντιμετωπίζουν με δυσπιστία και αυτές πρέπει να αποδείξουν την αξία τους με σκληρή δουλειά. Στην ίδια έρευνα αναφέρεται επιπλέον, πως ορισμένες εταιρείες προωθούν κυρίως άνδρες και δεν προάγουν τις γυναίκες καθώς οι εργοδότες θεωρούν πως εάν αυτές αποφασίσουν να δημιουργήσουν οικογένεια θα παραμελήσουν την δουλειά τους [2]. Σύμφωνα με την εταιρεία στατιστικής Bureau of Labor Statistics (BLS) οι θέσεις εργασίας στον

τομέα της έρευνας στην επιστήμη των υπολογιστών θα αυξηθούν κατά 19% έως το 2026. Παρά την υψηλή ζήτηση θέσεων εργασίας, η επιστήμη της πληροφορικής παραμένει ένας ανδροκρατούμενος τομέας στις Ηνωμένες Πολιτείες [3]. Οι γυναίκες τείνουν να εγκαταλείπουν τους τομείς της μηχανικής και της πληροφορικής εν μέρει λόγω της απομόνωσης που βιώνουν σε σύγκριση με τους άνδρες συναδέλφους τους. Ενώ κάποιοι μπορεί να υποστηρίζουν ότι οι γυναίκες απλώς δεν ενδιαφέρονται τόσο πολύ για την πληροφορική, άλλοι είναι πιο τολμηροί και υποστηρίζουν ότι οι άνδρες μπορεί να επιδιώκουν στην πραγματικότητα να κρατήσουν τις γυναίκες μακριά από τον τομέα της πληροφορικής, ακόμη και αν ο αποκλεισμός αυτός είναι ακούσιος [57]. Μπορούμε λοιπόν να συμπεράνουμε ότι τα κοινωνικά στερεότυπα και οι πολιτισμικές προκαταλήψεις περιορίζουν τις επιλογές των γυναικών και θέτουν φραγμούς στη καριέρα τους.

Source: National Science Foundation, American Bar Association, American Association of Medical Colleges
Credit: Quoc Trung Bui/NPR

Σχήμα 1. Πτώση ποσοστού γυναικών στο πεδίο της επιστήμης της πληροφορικής ανά τα χρόνια. [1]

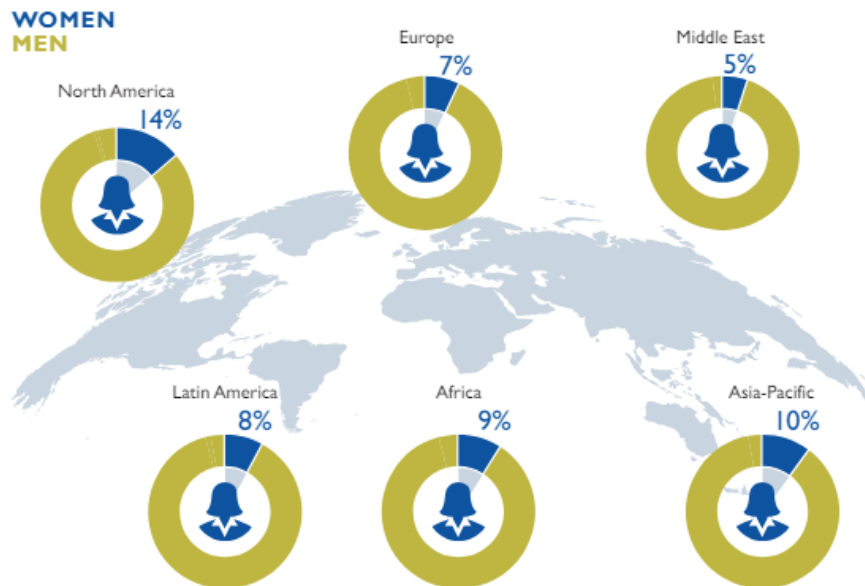
2.2 Η αντιμετώπιση των φύλων στον κλάδο της κυβερνοασφάλειας.

Ένας από τους κλάδους της πληροφορικής είναι η κυβερνοασφάλεια. Στόχος της κυβερνοασφάλειας είναι η προστασία των ψηφιακών πόρων και η διασφάλιση της ακεραιότητας των δεδομένων και των ψηφιακών υπηρεσιών [4].

Υπάρχει ένα σαφές χάσμα μεταξύ των δύο φύλων στον τομέα της ασφάλειας στον κυβερνοχώρο. Σήμερα, μόνο το 10% του παγκόσμιου εργατικού δυναμικού στον τομέα της ασφάλειας πληροφοριών είναι γυναίκες. Στη Βόρεια Αμερική, οι γυναίκες αποτελούν το 14% του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας, την υψηλότερη περιφερειακή συγκέντρωση στον κόσμο. Οι γυναίκες στις Ηνωμένες Πολιτείες αποτελούσαν το 48% του

εργατικού δυναμικού. Μια εξέταση άλλων περιοχών του κόσμου δείχνει ότι η συμμετοχή των γυναικών είναι μικρότερη από αυτή της Βόρειας Αμερικής, γεγονός που οδηγεί σε μια απορία αν πολιτισμικά ζητήματα, διακρίσεις, πρόσβαση στην εκπαίδευση ή ένας συνδυασμός αυτών συμβάλλουν σε αυτό [8].

Exhibit #1: Male and Female Cybersecurity Workforce Composition, by Region



Source: 2017 Global Information Security Workforce Study, (n=19,641)

Σχήμα 2. Σύνθεση του εργατικού δυναμικού κυβερνοασφάλειας, ανά περιοχή. [8]

Υπάρχουν πολλά διαφορετικά κοινωνικά, θεσμικά και προσωπικά εμπόδια που μπορούν να σταθούν απέναντι στην πρόοδο των γυναικών στον τομέα της κυβερνοασφάλειας. Για παράδειγμα, πολλές μελέτες επισημαίνουν ότι η πληροφορική εξακολουθεί να είναι ένας ανδροκρατούμενος τομέας και το γεγονός αυτό μπορεί να είναι ένας από τους λόγους για τους οποίους τόσες λίγες νέες γυναίκες ακολουθούν καριέρα στην ψηφιακή ασφάλεια. [6] Οι εργαζόμενοι στον πεδίο της κυβερνοασφάλειας αμείβονται γενικά με πολύ ικανοποιητικούς μισθούς. Έρευνες όμως έχουν δείξει πως γυναίκες με ίσως περισσότερα πτυχία και γνώσεις από κάποιους άνδρες έχουν χαμηλότερους μισθούς και καταλαμβάνουν χαμηλότερες θέσεις στις εταιρείες πληροφορικής. Η κατάσταση αυτή δημιουργεί στις γυναίκες το αίσθημα της κατωτερότητας, κάνοντάς τις να πιστεύουν πως δεν έχουν τα απαραίτητα προσόντα όσο και αν έχουν προσπαθήσει και όσα πτυχία και αν έχουν. Οι γυναίκες στον χώρο της κυβερνοασφάλειας πρέπει καθημερινά να αποδεικνύουν την ποιότητα της δουλειάς τους και το επίπεδο των γνώσεων τους. Σημαντικό είναι να επισημάνουμε πως την επιφυλακτική αυτή στάση απέναντι στις γυναίκες που θέλουν να εργαστούν στο πεδίο της ασφάλειας του κυβερνοχώρου δεν την έχουν απαραίτητως μόνο οι άνδρες. Οι γυναίκες που δουλεύουν ήδη αρκετό καιρό στον χώρο και έχουν

ίσως δυσκολευτεί αρκετά να φτάσουν σε ένα υψηλό επίπεδο, είναι εξίσου ψυχρές στο να υποδεχτούν νέες γυναίκες στην δουλειά αυτή. Τέλος, όπως αναφέρθηκε και στην προηγούμενη υπό-ενότητα, στο γενικότερο κομμάτι εργασίας στην επιστήμη της πληροφορικής, έτσι και στον τομέα της κυβερνοασφάλειας μόνο πολύ μεγάλες εταιρείες, όπως η Microsoft και η Google, δίνουν άδειες εγκυμοσύνης στις γυναίκες. Οι μικρότερες εταιρείες δεν μπορούν να το αντέξουν οικονομικά αυτό και έτσι δύσκολα θα δώσουν κάποια θέση εργασίας σε γυναίκες [7].

Σε έρευνα που διεξήγαγε το Center for Cyber Safety and Education, ερωτήθηκαν άνδρες και γυναίκες από την Βόρεια και την Λατινική Αμερική σχετικά με την ποικιλομορφία των εργαζομένων στον χώρο της κυβερνοασφάλειας. Σε αυτές τις περιοχές ένα πολύ σημαντικό 51% των γυναικών δήλωσε ότι έχει βιώσει διακρίσεις στον εργασιακό χώρο. Από την άλλη μόνο το 15% των ανδρών δήλωσαν το αντίστοιχο. Οι διακρίσεις αυτές μπορεί να συμβαίνουν υποσυνείδητα ή και εντελώς απροκάλυπτα. Ένα μεγάλο ποσοστό γυναικών δέχονται μία ανεξήγητη άρνηση ή καθυστέρηση στην επαγγελματική τους προαγωγή. Επίσης, αξιοσημείωτο είναι και το ποσοστό αυτών που στοχοποιούνται και τους τονίζονται συνεχώς και σε υπερβολικό βαθμό τα λάθη τους [8].

2.3 Τα φύλα σε διευθυντικές θέσεις στον τομέα της κυβερνοασφάλειας

Τα τελευταία χρόνια παρατηρείται μια μεγάλη ανισορροπία μεταξύ των φύλων, ιδίως όσον αναφορά τις ηγετικές/ διευθυντικές θέσεις στον τομέα της ασφάλειας στον κυβερνοχώρο. Οι γυναίκες αποτελούν ένα μεγάλο μέρος του εργατικού δυναμικού, αλλά ως επί το πλείστον υπό-εκπροσωπούνται στον τομέα της ασφάλειας στον κυβερνοχώρο. Αν αναλογιστούμε πως οι γυναίκες που εργάζονται στον κυβερνοχώρο αποτελούν μόνο ένα 10%, το ποσοστό γυναικών σε ηγετικές θέσεις είναι σίγουρα πολύ μικρότερο. Με ελάχιστους γυναικείους ηγετικούς ρόλους στον τομέα αυτόν, οι γυναίκες το βρίσκουν δύσκολο να συνδεθούν με έναν μέντορα ή ένα πρότυπο. Αυτή η τόσο μεγάλη διαφορά μεταξύ των δύο φύλων στις ηγετικές θέσεις, δεν είναι ένα απλό τοπικό ζήτημα που ισχύει σε μία συγκεκριμένη χώρα. Αντίθετα, είναι ένα φαινόμενο που ξεπερνά τα διεθνή σύνορα υπογραμμίζοντας την ανάγκη να εξεταστούν τα βαθύτερα αίτια αυτής της υπό-εκπροσώπησης των γυναικών [9].

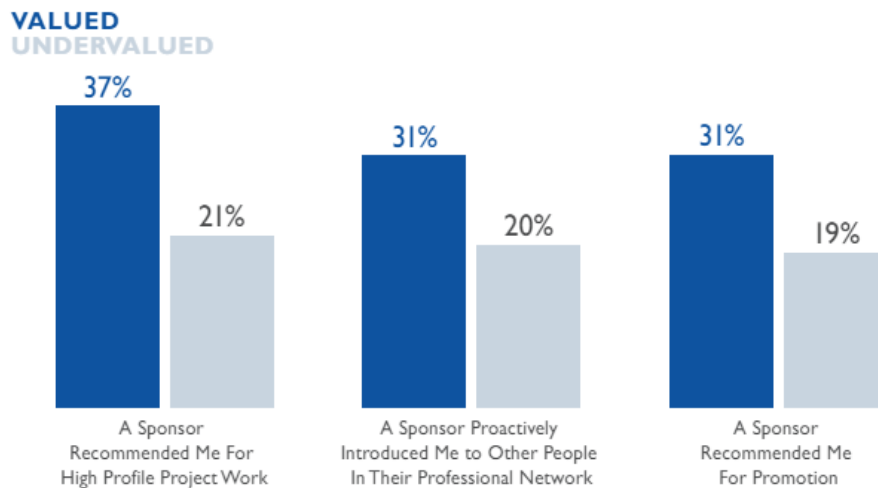
Οι ερευνητές έχουν καταλήξει πως ο χώρος εργασίας στον κλάδο της κυβερνοασφάλειας συμβάλει σημαντικά στην έμφυλη ανισότητα που παρατηρείται στους ηγετικούς ρόλους. Αρχικά, οι προκηρύξεις θέσεων εργασίας στον κλάδο συχνά περιέχουν λέξεις που έχουν συνδεθεί με την αρρενωπότητα, γεγονός που αποθαρρύνει, χωρίς όμως να το επιδιώκει, τις γυναίκες. Λέξεις όπως ‘κυρίαρχος’ και ‘ηγέτης’ κάνουν τις γυναίκες να πιστεύουν ότι δεν ανήκουν στον τομέα αυτόν και πως δεν θα καταφέρουν ποτέ να φτάσουν σε ένα υψηλότερο επίπεδο στην καριέρα τους. Σε περίπτωση που οι γυναίκες τα καταφέρουν και βρεθούν σε κάποια ηγετική θέση, πολλές φορές προσκρούουν σε προκαταλήψεις λόγω φύλου επειδή δεν ταιριάζουν με τις ρατσιστικές αντιλήψεις που υποστηρίζουν ότι οι γυναικείοι ρόλοι δεν συνάδουν με τους ηγετικούς ρόλους. Η κοινωνία αποδίδει τα χαρακτηριστικά ενός ηγέτη στις ιδιότητες των ανδρών και με αυτόν τον τρόπο επηρεάζει την προώθηση των γυναικών σε διευθυντικούς ρόλους. Επιπλέον, οι άνδρες αποκτούν την πεποίθηση πως έχουν πιο κατάλληλες δεξιότητες για να ηγηθούν μιας τεχνολογικής θέσης [5][9].

Μπορούμε να πούμε πως υπάρχουν κάποιες γενικές διαπιστώσεις που συμβάλλουν στην ανισότητα των φύλων σε ηγετικές θέσεις στον κυβερνοχώρο:

- Ασυνείδητες προκαταλήψεις: προκαταλήψεις και στερεότυπα τα οποία οι άνθρωποι ακολουθούν χωρίς να καταλαβαίνουν ότι αυτά μπορούν να σταθούν εμπόδιο στην καριέρα και την πρόοδο των γυναικών. Τις εμποδίζουν στο να πάρουν προαγωγή και να αναλάβουν ηγετικούς ρόλους [5].
- Η έλλειψη προτύπων: καθώς δεν υπάρχουν πολλές γυναίκες που κατέχουν ηγετικές θέσεις στον τομέα της ασφάλειας στον κυβερνοχώρο, το γυναικείο φύλο που θέλει να εργαστεί στον τομέα αυτόν αποθαρρύνεται και περιορίζει τις ιδέες του για το πώς μπορεί να φτάσει ψηλά στην δουλειά αυτή. Επίσης, δεδομένου ότι οι έρευνες για την ανάδειξη των επιτυχημένων γυναικών είναι σχετικά ελάχιστες, υπάρχουν ακόμη λιγότερες για τις γυναίκες που έχουν πετύχει σε διευθυντικούς ρόλους στον τομέα της κυβερνοασφάλειας. Αυτό έχει ως αποτέλεσμα να μην κατανοείται η συμβολή τους και τα εμπόδια που αντιμετώπισαν μέχρι να τα καταφέρουν [5].
- Ισορροπία μεταξύ εργασίας και ζωής: οι γυναίκες συχνά έρχονται αντιμέτωπες με το πρόβλημα εξισορρόπησης των επαγγελματικών και οικογενειακών τους υποχρεώσεων. Αυτό το γεγονός δυσχεραίνει την δυνατότητα να δώσουν στην καριέρα και στον ηγετικό τους ρόλο τον χρόνο και την ενέργεια που αυτά απαιτούν [9].
- Η κουλτούρα στον χώρο εργασίας: τα γυναικεία ταλέντα και οι υψηλές γνώσεις τους απορρίπτονται από χώρους εργασίας που δεν εκτιμούν και δεν αναγνωρίζουν τον ρόλο της ποικιλομορφίας στον εργασιακό χώρο. Αυτό μπορεί να οδηγήσει σε έλλειψη των γυναικών σε ηγετικές θέσεις [9].

Σε συνέχεια της έρευνας του Center for Cyber Safety and Education, το 28% των γυναικών που ρωτήθηκαν ανέφεραν ότι η γνώμη τους στο εργασιακό περιβάλλον δεν εκτιμάται. Οι γυναίκες που πιστεύουν ότι εκτιμώνται αναφέρουν πως η εταιρεία στην οποία εργάζονται τους παρέχει επαρκείς πόρους κατάρτισης και ανάπτυξης των ηγετικών τους ικανοτήτων. Επίσης ένα μεγάλο ποσοστό των γυναικών αυτών, δηλώνουν πως έχουν υψηλότερες πιθανότητες να έρθουν σε επαφή με χορηγούς. Οι χορηγοί είναι αυτοί που στην συνέχεια τις προωθούν σε άλλα μεγαλύτερα project, σε άλλους ανθρώπους του χώρου και τέλος θα τις προτείνουν για προαγωγή σε μια ηγετική θέση [8].

Exhibit #13: Percentage of Women (Who Feel Valued Versus Undervalued) Who Benefited From Sponsorship Options, Globally

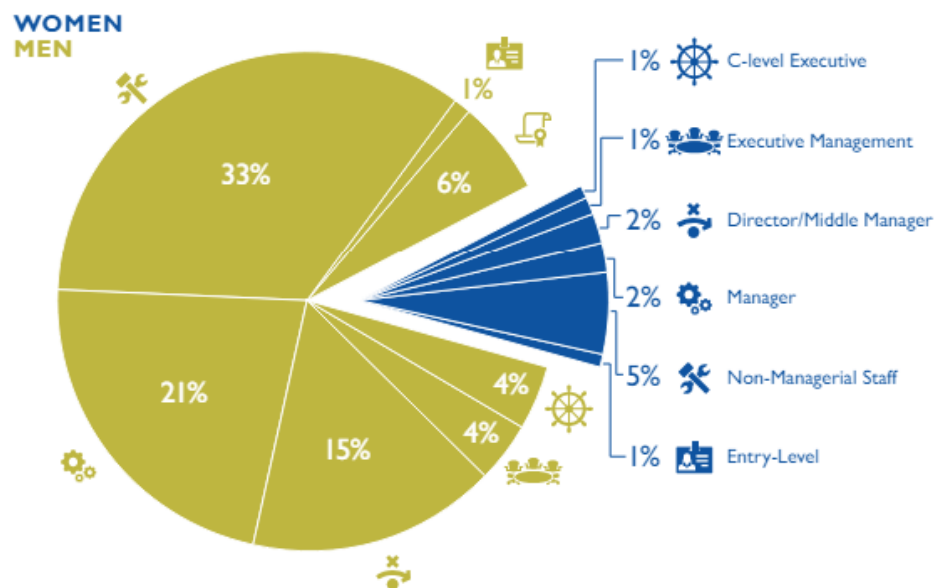


Source: 2017 Global Information Security Workforce Study

Σχήμα 3. Ποσοστά γυναικών (που εκτιμώνται στο εργασιακό περιβάλλον και που δεν εκτιμώνται) που επωφελήθηκαν από χορηγίες [8]

Συνολικά οι άνδρες υπερτερούν των γυναικών κατά περίπου εννέα προς ένα. Οι άνδρες κυριαρχούν σε όλους τους ανώτερους ρόλους, συμπεριλαμβανομένων των διευθυντικών και διοικητικών θέσεων [8].

Exhibit #2: Gender Distribution of the Cybersecurity Workforce, by Organizational Positions Globally



Source: 2017 Global Information Security Workforce Study

Σχήμα 4. Κατανομή των φύλων σε διοικητικές θέσεις στον τομέα της κυβερνοασφάλειας παγκοσμίως. [8]

Ισότητα μεταξύ ανδρών και γυναικών/ Νομοθεσία

Η ισότητα μεταξύ γυναικών και ανδρών είναι ένας από τους στόχους της Ευρωπαϊκής Ένωσης. Με την πάροδο του χρόνου, η νομοθεσία, η νομολογία και οι τροποποιήσεις των Συνθηκών συνέβαλαν στην ενίσχυση αυτής της αρχής και της εφαρμογής της στην ΕΕ. Από το 1957, η αρχή σύμφωνα με την οποία άνδρες και γυναίκες πρέπει να λαμβάνουν ίση αμοιβή για εργασία ίσης αξίας κατοχυρώθηκε στις Συνθήκες (σήμερα: άρθρο 157 ΣΛΕΕ). Το άρθρο 153 ΣΛΕΕ επιτρέπει στην ΕΕ να δρα στον ευρύτερο τομέα των ίσων ευκαιριών και της ίσης μεταχείρισης σε θέματα εργασίας, και, στο πλαίσιο αυτό, το άρθρο 157 ΣΛΕΕ επιτρέπει τη θετική δράση για την ενίσχυση της θέσης των γυναικών. Επιπλέον, το άρθρο 19 ΣΛΕΕ προβλέπει την θέσπιση νομοθεσίας για την καταπολέμηση των πάσης φύσεως διακρίσεων, περιλαμβανομένων των διακρίσεων λόγω φύλου. Σύμφωνα με το άρθρο 23 του Χάρτη, η ισότητα γυναικών και ανδρών πρέπει να εξασφαλίζεται σε όλους τους τομείς, μεταξύ άλλων στην απασχόληση, την εργασία και τις αποδοχές [58].

3

Απαιτούμενες δεξιότητες στον εργασιακό χώρο της κυβερνοασφάλειας

3.1 Απαιτούμενες δεξιότητες στον χώρο της κυβερνοασφάλειας: κάτι παραπάνω από τεχνολογικές γνώσεις

Η ασφάλεια στον κυβερνοχώρο αποτελεί πλέον απαραίτητη προϋπόθεση για τους σύγχρονους οργανισμούς. Η ασφάλεια των συστημάτων και των δεδομένων καθώς και η προστασία τους από επιθέσεις, είναι ένα θέμα που απασχολεί τον τομέα των πληροφοριακών συστημάτων από την πρώτη κιόλας στιγμή που αυτά δημιουργήθηκαν. Οι συνέπειες των επιθέσεων στον κυβερνοχώρο ποικίλλουν και μπορεί να είναι καταστροφικές όχι μόνο για τους οργανισμούς αλλά και για την κοινωνία ολόκληρη. Για αυτόν τον λόγο απαιτούνται νέες τεχνικές και όχι μόνο τεχνολογικές δεξιότητες, για τη βελτίωση της ανθεκτικότητας στον κυβερνοχώρο εντός των οργανισμών [12].

Χάρη στην ανάπτυξη του διαδικτύου και την πρόοδο της τεχνολογίας, η ασφάλεια στον κυβερνοχώρο κερδίζει καθημερινά ολοένα και μεγαλύτερη αναγνώριση ως βασικό θέμα στο πλαίσιο της πληροφορικής, αλλά και ως μια σημαντική απαίτηση για τις επιχειρήσεις και τους οργανισμούς. Τα τελευταία χρόνια παρατηρούμε το επάγγελμα της κυβερνοασφάλειας να ωριμάζει. Η κυβερνοασφάλεια υποστηρίζεται από πολυάριθμες επαγγελματικές πιστοποιήσεις αλλά και από ένα αυξανόμενο αριθμό ακαδημαϊκών προσόντων που εξειδικεύονται στον τομέα αυτόν. Όσον αφορά το εύρος του επαγγέλματος αυτού, αξίζει να αναφέρουμε ότι η ασφάλεια στον κυβερνοχώρο καλύπτει ένα ευρύ φάσμα δεξιοτήτων, τόσο τεχνικών όσο και μη τεχνικών. Είναι σημαντικό, να κατανοήσουμε την συμβολή που έχουν στην ασφάλεια στον κυβερνοχώρο κάποιοι διαφορετικοί ακαδημαϊκοί κλάδοι με παρόμοιες εισροές, όπως αυτοί των επιχειρήσεων, της μηχανικής, του δικαίου αλλά και της ψυχολογίας. Ταυτόχρονα όμως αναγνωρίζουμε ότι η πρωταρχική βάση του θέματος βρίσκεται στους κλάδους της τεχνολογίας και των πληροφοριακών συστημάτων [10-11].

Εξετάζοντας τη σχετική ζήτηση, δεν υπάρχει κανένας τομέας που να μην έχει ανάγκη την ασφάλεια στον κυβερνοχώρο, και κατ' επέκταση κανένας τομέας που να μην έχει τουλάχιστον έμμεση εξάρτηση από σχετικές δεξιότητες κυβερνοασφάλειας. Πολλοί όμως οργανισμοί αντιμετωπίζουν ένα σημαντικό περιορισμό όσον αφορά την έλλειψη εξειδικευμένου προσωπικού για την υποστήριξη των απαιτούμενων ρόλων και αρμοδιοτήτων. Παρατηρούμε πως υπάρχουν δύο προκλήσεις οι οποίες προκύπτουν εδώ:

- Πρώτον, οι δεξιότητες οι ίδιες είναι ανεπαρκείς και
- Δεύτερον, η ποικιλομορφία του τομέα της ασφάλειας στον κυβερνοχώρο μπορεί να περιπλέξει τον προσδιορισμό των προσόντων ή των πιστοποιήσεων που μπορούν να συμβάλουν στη ανάδειξη των δεξιοτήτων κάποιου που θέλει να ασχοληθεί με τον τομέα αυτόν.

Οι άνθρωποι που δραστηριοποιούνται στον τομέα του κυβερνοχώρου χρειάζονται ένα συνδυασμό τεχνικών δεξιοτήτων, ειδικών γνώσεων και κοινωνικής νοημοσύνης για να είναι επιτυχείς. Αυτοί, όπως και τα δίκτυα τα οποία χειρίζονται, πρέπει να είναι αξιόπιστοι, ευέλικτοι και ανθεκτικοί. Ο καθορισμός των γνώσεων, των δεξιοτήτων, και των χαρακτηριστικών των ανθρώπων που θέλουν να ασχοληθούν με την κυβερνοασφάλεια δεν είναι τόσο απλός όσο ο ορισμός μιας ομάδας τεχνικών δεξιοτήτων. Καταλαβαίνουμε λοιπόν, πως απαραίτητο δεν είναι μόνο να αναγνωρίσουμε την ανάγκη των γνώσεων στο κομμάτι της κυβερνοασφάλειας αλλά και το είδος των γνώσεων και των δεξιοτήτων αυτών. Πολλά από τα ιδρύματα που χορηγούν πτυχία κυβερνοασφάλειας δίνουν έμφαση μόνο στις τεχνικές δεξιότητες και αγνοούν τις σημαντικές κοινωνικές και οργανωτικές επιρροές που καθορίζουν την επιτυχία ή την αποτυχία σε καθημερινά πλαίσια. Η ανάπτυξη ενός μελλοντικού εργατικού δυναμικού στον κυβερνοχώρο που θα λαμβάνει υπόψη τόσο τις τεχνικές όσο και τις κοινωνικές δεξιότητες, θα παράγει πιθανότατα το είδος εμπειρογνομosύνης που θα καταστήσει την πραγματική δημιουργικότητα και την αριστεία στην απόδοση ενός οργανισμού [11].

Οι επαγγελματίες που εργάζονται στον κυβερνοχώρο πρέπει να έχουν καλή νοητική ευελιξία και ικανότητα αντιστοίχισης μοτίβων. Σίγουρα θα πρέπει να διαθέτουν σημαντικές δεξιότητες και γνώσεις σχετικά με τα λειτουργικά συστήματα υπολογιστών και τη χρήση αναλυτικών εργαλείων, όπως η σάρωση δικτύου, η χαρτογράφηση και ανάλυση ευπαθειών. Αυτά όμως δεν αρκούν. Η ασφάλεια στον κυβερνοχώρο προσεγγίζεται συχνότερα από μια τεχνική άποψη, με την καινοτόμο τεχνολογία και τους τεχνικούς εργαζόμενους να θεωρούνται ο δρόμος για την επίλυση των προβλημάτων ασφάλειας [11]. Πολλές φορές όμως, η ύπαρξη μιας ολοκληρωμένης προσέγγισης και αντιμετώπισης των κοινωνικών παραγόντων μπορεί να είναι πιο αναγκαία από τις τεχνικές λύσεις και μόνο. Αυτές οι δεξιότητες αναφέρονται συχνά ως “soft skills” και αποτελούνται από προσωπικά χαρακτηριστικά όπως η θετική συμπεριφορά, η συνεργασία, η κριτική σκέψη, η προσαρμοστικότητα και η ομαδική εργασία. Επιπλέον, “soft skills” μπορούν να θεωρηθούν οι ανθρώπινες δεξιότητες όπως η ενσυναίσθηση και η οικοδόμηση σχέσεων και οι δεξιότητες επικοινωνίας. Οι επαγγελματίες πρέπει να είναι σε θέση να “πουλήσουν” την ασφάλεια. Χρησιμοποιώντας μια ποικιλία επικοινωνιακών προσεγγίσεων προσαρμοσμένων στο κοινό τους, όπως για παράδειγμα χρήση εικόνων, μεταφορών και βίντεο, οι εργαζόμενοι στον χώρο της κυβερνοασφάλειας πρέπει να είναι ικανοί να εξηγήσουν τεχνικές έννοιες σε ένα ακροατήριο το οποίο δεν έχει γνώσεις σε τεχνικά ζητήματα. Ιδιαίτερη σημασία έχει

η καλλιέργεια συνεργασιών και οικοδόμησης συναίνεσης. Σε έναν πολύπλοκο, δυναμικό τομέα, οι επαγγελματίες πρέπει να βασίζονται στην συλλογική εμπειρογνωμοσύνη και την καθιέρωση κοινών στόχων ασφαλείας, καθώς θα υπάρχουν πολλές απόψεις και λύσεις πάνω σε κάποιο πρόβλημα. Επιπρόσθετα, μια σημαντική κατηγορία δεξιοτήτων στον χώρο της κυβερνοασφάλειας ονομάζεται “people skills”. Σε αυτόν τον όρο εντοπίζουμε την κατανόηση των ανθρώπινων συμπεριφορών και την ικανότητα οικοδόμησης ανθρώπινων σχέσεων. Για να πετύχει κάποιος σε αυτόν τον τομέα πρέπει να μπορεί να κάνει συζητήσεις με τους ανθρώπους που πρόκειται να δουλέψει και να μπορέσει να τους δώσει αποτελεσματικές συμβουλές, χωρίς να τους προσβάλει επειδή μπορεί να μην γνωρίζουν ορισμένα πράγματα [13].

Δυστυχώς, αυτές οι δεξιότητες οι οποίες αναφέρθηκαν παραπάνω είναι δύσκολο να βρεθούν σε επαγγελματίες ασφαλείας στον κυβερνοχώρο. Είναι όμως απαραίτητο να κατανοήσουμε πως εάν οι τεχνικές γνώσεις συνδυαστούν με τις ατομικές δεξιότητες, η δημιουργία ενός ισχυρού εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας είναι μονόδρομος [13].

3.2 Απαραίτητες τεχνολογικές γνώσεις στον κυβερνοχώρο.

Ο τομέας του κυβερνοχώρου είναι μια συνεργασία της επιστήμης των υπολογιστών, των μαθηματικών, των οικονομικών, του δικαίου, της ψυχολογίας και της μηχανικής. Περιλαμβάνει όχι μόνο τη δικτύωση διαδικτυακών συσκευών μεταξύ τους, αλλά και τον τρόπο με τον οποίο οι άνθρωποι αλληλοεπιδρούν και επηρεάζονται από αυτές τις συσκευές. Η ασφάλεια στον κυβερνοχώρο επηρεάζει κάθε πτυχή της σύγχρονης ζωής, από το ηλεκτρικό ρεύμα που τροφοδοτεί εκατομμύρια σπίτια μέχρι το δίκτυο μεταφορών που μετακινεί καθημερινά εκατομμύρια ανθρώπους. Καθώς ο αριθμός και οι χρήσεις των συνδεδεμένων συσκευών αυξάνονται, η πολυπλοκότητα της υποδομής του κυβερνοχώρου αυξάνεται εκθετικά, όπως και ο αριθμός των ευάλωτων συσκευών. Το εργατικό δυναμικό της κυβερνοασφάλειας υποστηρίζει αυτή την υποδομή και υπερασπίζεται τα δίκτυα. Το συγκεκριμένο περιβάλλον εργασίας περιλαμβάνει την σάρωση μεγάλου αριθμού συμβάντων δικτύου και συναγερμών σε πολλαπλές οθόνες υπολογιστών, με σκοπό τον εντοπισμό απειλών και ταυτόχρονα την μείωση των λανθασμένων συναγερμών. Επιπλέον, σημαντικό είναι οι επαγγελματίες του κυβερνοχώρου να μπορούν να χειριστούν ταυτόχρονα πολλές πηγές πληροφοριών και να έχουν πλήρη επίγνωση της κατάστασης του δικτύου, εκτελώντας συνεχόμενες αξιολογήσεις κινδύνων [11]. Συγκεκριμένα, οι επαγγελματίες στον χώρο της κυβερνοασφάλειας πρέπει να κατέχουν τις παρακάτω τεχνολογικές δεξιότητες επιγραμματικά:

- Κατανόηση των πρωτοκόλλων δικτύου, της αρχιτεκτονικής και του τρόπου ασφάλισης των δικτύων.
- Εξειδίκευση σε διάφορα λειτουργικά συστήματα, γνώση ασφαλείας και διαχείρισή τους.
- Διαμόρφωση και διαχείριση τειχών προστασίας και συσκευών ασφαλείας συστημάτων για ανίχνευση και πρόληψη εισβολών.
- Γνώση τεχνικών κρυπτογράφησης για την προστασία δεδομένων κατά τη μεταφορά.
- Ανίχνευση και επιδιόρθωση ευπαθειών σε συστήματα και εφαρμογές.
- Ανάλυση και μετριάσμός των απειλών κακόβουλου λογισμικού.
- Κατανόηση των βέλτιστων πρακτικών ασφαλείας για πλατφόρμες cloud.

- Ασφάλιση υπολογιστών, κινητών συσκευών και διακομιστών.
- Ασφάλεια στο διαδίκτυο των πραγμάτων [23].

Στην επόμενη ενότητα θα αναλύσουμε κάποιες από αυτές τις τεχνολογικές δεξιότητες που είναι απαραίτητες για την δημιουργία ενός ισχυρού επαγγελματικού δυναμικού στον κλάδο της κυβερνοασφάλειας.

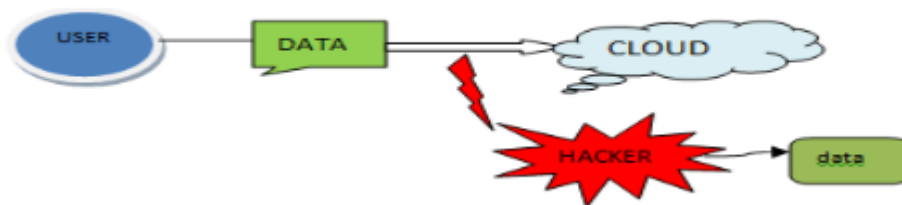
3.2.1 Ασφάλεια Cloud

Το cloud έχει αναδειχθεί ως ένα επιτυχημένο υπολογιστικό πρότυπο που επιτρέπει στους χρήστες να βασίζονται σε εξωτερικούς παρόχους για την αποθήκευση και την επεξεργασία των δεδομένων τους. Τα βασικά χαρακτηριστικά του cloud computing είναι η ευελιξία, το χαμηλό κόστος, η ανεξαρτησία συσκευής-τοποθεσίας, η υψηλή αξιοπιστία, η υψηλή επεκτασιμότητα, η ασφάλεια και η βιωσιμότητα. Την μέγιστη σημασία όμως στο cloud έχει η εγγύηση ασφάλειας. Αυτό σημαίνει ότι πρέπει να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, η πρόσβαση σε αυτά και η επεξεργασία τους. Επίσης, διασφαλίζεται η διαθεσιμότητα των δεδομένων και των υπηρεσιών στους νόμιμους χρήστες. Ανάλογα με τον τύπο των παρεχόμενων δυνατοτήτων, οι υπηρεσίες του cloud computing χωρίζονται σε τρεις κατηγορίες: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) και Software-as-a-Service (SaaS) [14].

Η ασφάλεια στο cloud εξακολουθεί να αποτελεί μια πρόκληση για τους παρόχους και τους χρήστες των αναδυόμενων τεχνολογιών παγκοσμίως. Πρόσφατα υπήρξε μια διαρροή δεδομένων που αφορούσε την Cambridge Analytical στην οποία συμμετείχαν περισσότερα από 86 εκατομμύρια δεδομένα πελατών του Facebook και τα οποία χρησιμοποιήθηκαν παράνομα χωρίς την άδειά τους. Αυτό το συμβάν αποτελεί μια απόδειξη για το γεγονός πως υπάρχουν ορισμένες αδυναμίες ασφάλειας σε πολλές διαδικτυακές πλατφόρμες. Πολλοί χρήστες γίνονται γρήγορα επιφυλακτικοί απέναντι στο cloud λόγω των ζητημάτων προστασίας της ιδιωτικής ζωής. Παρόλο που υπάρχουν άφθονα οφέλη που συνδέονται με την τεχνολογία νέφους, φαίνεται να υπάρχουν και πολλές σοβαρές ανησυχίες σχετικά με την ασφάλεια των δεδομένων του σε όλα τα επίπεδα. Πολλά από τα χαρακτηριστικά του νέφους που το κάνουν τόσο δελεαστικό, δημιουργούν νέες δοκιμασίες στο σύστημα ασφαλείας και το εκθέτουν σε νέους κινδύνους. Σε έρευνες που έχουν γίνει αναφέρεται ότι στο κοντινό μέλλον η ευπάθεια του υπολογιστικού νέφους σε ιούς, worms, hackers και επιθέσεις στον κυβερνοχώρο θα αυξηθούν. Αυτό θα συμβεί επειδή οι εγκληματίες και τα εχθρικά έθνη θα προσπαθήσουν να κλέψουν ιδιωτικές πληροφορίες και να βλάψουν τις υπηρεσίες και το υπολογιστικό δίκτυο. Το υπολογιστικό νέφος είναι ευάλωτο σε πολλές απειλές ασφαλείας. Αυτές οι απειλές και τα τρωτά σημεία εμφανίζονται σε διάφορες μορφές ανάλογα με το δίκτυο και το μοντέλο υπηρεσιών που χρησιμοποιείται. Η διατήρηση της ασφάλειας του κυβερνοχώρου στο υπολογιστικό νέφος απαιτεί τον προσδιορισμό του είδους των πληροφοριών που ανταλλάσσονται [15].

Όλο και περισσότεροι οργανισμοί αναζητούν υποδομές cloud για την αποθήκευση δεδομένων και την εκτέλεση εφαρμογών. Όλες οι εταιρείες σήμερα ζητούν επαγγελματίες με δεξιότητες ασφάλειας που να εφαρμόζονται σε δημόσιες πλατφόρμες cloud, όπως το AWS και το Azure. Είναι σημαντικό κάποιος που θέλει να εργαστεί στον χώρο της κυβερνοασφάλειας να έχει όσες περισσότερες γνώσεις γίνεται, αλλά και εμπειρία, στην διαχείριση πλατφορμών cloud. Με

αυτές τις γνώσεις ένας υπάλληλος κυβερνοασφάλειας θα μπορέσει να εφαρμόσει σωστά τις πολιτικές ασφαλείας και να προστατεύσει τις συσκευές και τα συστήματα που βασίζονται στο cloud. Η επιτυχής εφαρμογή απλών μέτρων για την προστασία από γνωστά ζητήματα ασφαλείας αποτελεί σημαντικό έργο κάποιου που θα εργαστεί στον τομέα της ασφαλείας στον κυβερνοχώρο [16].



Σχήμα 5. Ο hacker μπορεί εύκολα να πάρει τα δεδομένα που μεταφέρονται από τον χρήστη. Εδώ έχουμε απώλεια σημαντικών δεδομένων [28]

3.2.2 Γνώση λειτουργικών συστημάτων

Λειτουργικό Σύστημα (Operating System – OS) είναι το σύνολο των προγραμμάτων ενός υπολογιστικού συστήματος το οποίο λειτουργεί ως σύνδεσμος ανάμεσα στα προγράμματα του χρήστη και το υλικό. Το λειτουργικό σύστημα είναι υπεύθυνο για τη δημιουργία του περιβάλλοντος επικοινωνίας του χρήστη με το σύστημα, τη διαχείριση και το συντονισμό των εργασιών του συστήματος, καθώς και για την κατανομή των διαθέσιμων πόρων [17]. Παρόλο που τα συστήματα αυτά φαίνεται να είναι το απόλυτο εργαλείο για τον χρήστη, υπάρχουν αρκετά τρωτά σημεία τα οποία μπορούν να εκμεταλλευτούν hackers. Οι επιθέσεις στον κυβερνοχώρο σε λειτουργικά συστήματα υπάρχουν από την πρώτη κιόλας μέρα της δημιουργίας των υπολογιστών και του παγκόσμιου ιστού. Οι πιο συνηθισμένες επιθέσεις έχουν τη μορφή κακόβουλων προγραμμάτων τα οποία επιτίθενται με διάφορες μορφές. Τα κακόβουλα προγράμματα μπορούν να προκαλέσουν ζημιά στο λειτουργικό σας σύστημα αλλάζοντας ή διαγράφοντας σημαντικά αρχεία που απαιτούνται για τη σωστή λειτουργία του συστήματός. Αυτός ο τύπος επίθεσης μπορεί να εμποδίσει την εκκίνηση του λειτουργικού συστήματος, την εκτέλεση ενός λογισμικού. Μπορεί επίσης να πολλαπλασιαστεί και ως αποτέλεσμα να γεμίσει το χώρο στο σκληρού δίσκου. Επιπλέον, οι κακόβουλες επιθέσεις προκαλούν την απώλεια πολλών εκατομμυρίων σε εταιρείες λόγω της ζημιάς που προκαλείται, όπως χαμένα αρχεία, αρχεία που κλάπηκαν αλλά και ο χρόνος που απαιτείται για την επίλυση αυτού του ζητήματος [18].

Όπως μπορούμε λοιπόν να καταλάβουμε, η ασφάλεια των λειτουργικών συστημάτων είναι απαραίτητη λόγω της σημασίας των δεδομένων. Για αυτόν τον λόγο οι περισσότερες εταιρείες είναι πρόθυμες να δαπανήσουν πολλά χρήματα σε επαγγελματίες που έχουν τις γνώσεις για να προστατεύσουν ένα λειτουργικό σύστημα και τα δεδομένα που αυτό περιλαμβάνει. Μηχανικοί λογισμικού και εμπειρογνώμονες σε θέματα ασφαλείας στον κυβερνοχώρο πρέπει να είναι ικανοί να βρουν τρόπους και μέσα για να εμποδίσουν κάθε ευπάθεια. Ένας εμπειρογνώμονας

κυβερνοασφάλειας, θα πρέπει να εργάζεται άνετα σε οποιοδήποτε λειτουργικό σύστημα. Ένας επαγγελματίας στον τομέα της κυβερνοασφάλειας πρέπει να έχει καλή γνώση λειτουργικών περιβαλλόντων όπως τα Windows, το Linux και το Mac OS [18].



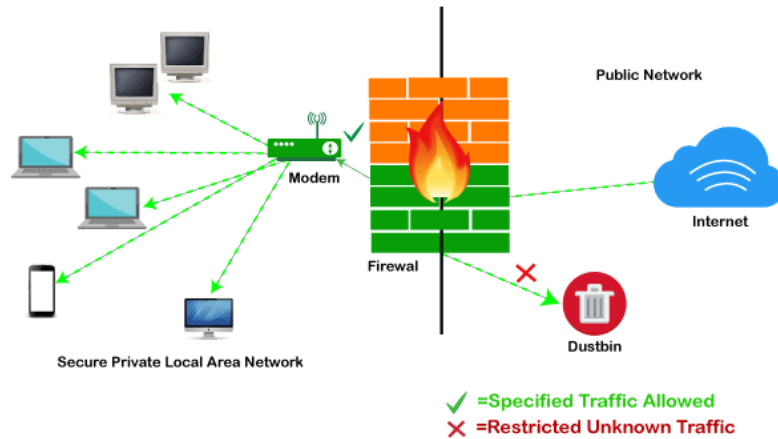
Σχήμα 6. Functions of Operating Systems [31]

3.2.3 Ασφάλεια δικτύου

Η ασφάλεια δικτύου είναι κάθε δραστηριότητα που αποσκοπεί στην προστασία της χρήσης και της ακεραιότητας του δικτύου και των δεδομένων. Περιλαμβάνει τεχνολογίες υλικού και λογισμικού. Στοχεύει σε ποικίλες απειλές και εμποδίζει την είσοδο ή την εξάπλωσή τους στο δίκτυο. Επιπροσθέτως, η ασφάλεια δικτύου είναι η διαδικασία λήψης προληπτικών μέτρων λογισμικού για την προστασία της υποκείμενης υποδομής δικτύωσης από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση, δυσλειτουργία, τροποποίηση, καταστροφή ή αθέμιτη αποκάλυψη. Με αυτόν τον τρόπο δημιουργείται μια ασφαλής πλατφόρμα για τους υπολογιστές, τους χρήστες και τα προγράμματα ώστε να εκτελούν τις επιτρεπόμενες κρίσιμες λειτουργίες τους μέσα σε ένα ασφαλές περιβάλλον. Κάθε οργανισμός που θέλει να παρέχει τις υπηρεσίες που απαιτούν οι πελάτες του πρέπει να προστατεύει το δίκτυό του και τις απόρρητες πληροφορίες που αυτό περιλαμβάνει, από επιθέσεις [19].

Κάποιος λοιπόν που θέλει να δουλέψει στον χώρο της κυβερνοασφάλειας είναι σημαντικό να γνωρίζει, να σχεδιάζει, να εφαρμόζει και να συντονίζει μέτρα ασφαλείας δικτύου, να εγκαθιστά λογισμικό ασφαλείας και να παρακολουθεί τα δίκτυα για τυχόν παραβιάσεις. Επίσης, θα πρέπει να αξιολογεί τα προβλήματα του δικτύου για να διασφαλίζει ότι είναι διαθέσιμο στους χρήστες και να προσδιορίζει τις ανάγκες του πελάτη. Υπάρχουν πολλά επίπεδα που πρέπει να εξεταστούν κατά την αντιμετώπιση της ασφάλειας δικτύου σε έναν οργανισμό. Οι επιθέσεις μπορούν να συμβούν σε οποιοδήποτε επίπεδο ασφαλείας δικτύου, επομένως το υλικό, το λογισμικό και οι πολιτικές ασφαλείας δικτύου πρέπει να είναι σχεδιασμένες για να αντιμετωπίζουν κάθε περιοχή. Ο υπάλληλος κυβερνοασφάλειας πρέπει να είναι σε θέση να ρυθμίζει δρομολογητές, τείχη προστασίας (firewall) και ένα σύστημα ανίχνευσης εισβολών με αποδοτικό και αποτελεσματικό τρόπο. Η ασφάλεια δικτύων αρχικά επικεντρώθηκε σε

αλγοριθμικές πτυχές όπως η κρυπτογράφηση και οι τεχνικές κατακερματισμού. Παρόλα αυτά, αυτές οι δεξιότητες από μόνες τους είναι ανεπαρκείς για την προστασία των δικτύων υπολογιστών. Πολλοί εκπαιδευτικοί πιστεύουν ότι για να εκπαιδευτούν οι άνθρωποι στην ασφάλεια των δικτύων, πρέπει να μάθουν να σκέφτονται σαν να είναι οι ίδιοι hackers [20].



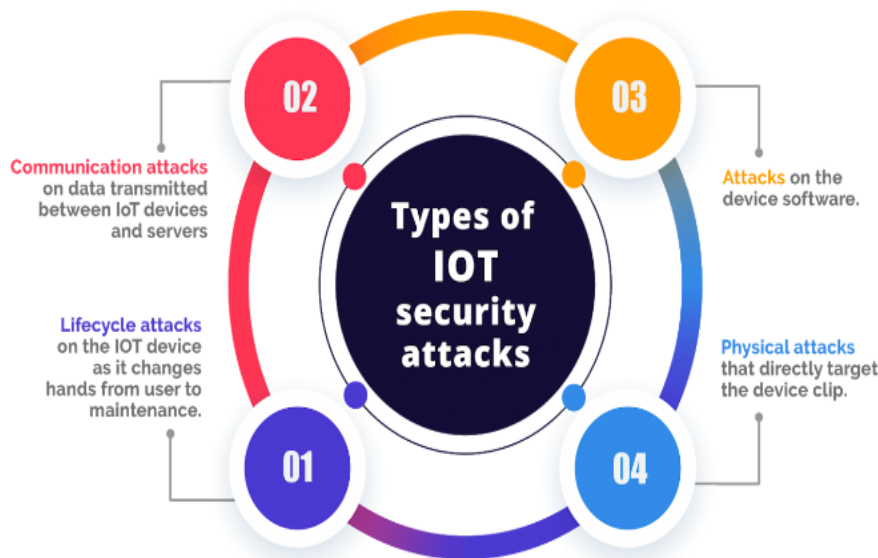
Σχήμα 7. Το τείχος προστασίας αναχαιτίζει την κυκλοφορία δικτύου στο σημείο εισόδου ενός υπολογιστή [30]

3.2.4 Διαδίκτυο των Πραγμάτων (IoT)

Σύμφωνα με τα στατιστικά στοιχεία που έχουμε, μέχρι το 2025 θα υπάρχουν πάνω από 30 δισεκατομμύρια συσκευές Internet of Things συνδεδεμένες παγκοσμίως. Με έναν τέτοιο τεράστιο αριθμό συσκευών προκύπτουν πολύ περισσότερες ευκαιρίες για την δημιουργία ευπαθειών στην ασφάλεια. Ως εκ τούτου, η ασφάλεια του IoT θα αποτελέσει μεγαλύτερη προτεραιότητα στο εγγύς μέλλον και ουσιαστικό μέρος της διατήρησης της ακεραιότητας και της ασφάλειας του συνολικού συστήματος του Διαδικτύου. Πολλές συσκευές IoT συλλέγουν προσωπικά δεδομένα, γεγονός που αυξάνει το ρίσκο για τη διατήρηση ασφαλών δικτύων και τη διατήρηση της εμπιστοσύνης των καταναλωτών. Η ασφάλεια στον κυβερνοχώρο είναι μία από τις κύριες προκλήσεις που αντιμετωπίζουν οι εταιρείες στο πλαίσιο του διαδικτύου των πραγμάτων, στο οποίο ένας αριθμός έξυπνων συσκευών συνδέονται με μηχανές, υπολογιστές και ανθρώπους, δικτυώνονται και επικοινωνούν μεταξύ τους [21].

Σε αυτό το βιομηχανικό σενάριο των IoT, το προσωπικό πρέπει να γνωρίζει τα θέματα κυβερνοασφάλειας προκειμένου να αποτρέψει ή να ελαχιστοποιήσει την εμφάνιση περιστατικών και την παραβίαση εταιρικών δεδομένων και, συνεπώς, να καταστήσει τις εταιρείες ανθεκτικές στις κυβερνοεπιθέσεις. Η ασφάλεια του IoT δίνει έμφαση στην προστασία των συνδεδεμένων συσκευών και δικτύων μέσω του Διαδικτύου, ιδίως επειδή οι περισσότερες από αυτές τις συσκευές έχουν πρόσβαση στα δίκτυα χωρίς ανθρώπινη παρέμβαση ή επίβλεψη. Για αυτόν τον λόγο, καθίσταται σημαντικό να διασφαλιστεί ότι εφαρμόζονται τα κατάλληλα μέτρα ασφαλείας, ώστε οι συσκευές IoT να μπορούν να αφεθούν μόνες τους να εκτελούν τις λειτουργίες τους αυτόματα, χωρίς οι ειδικοί σε θέματα ασφάλειας στον κυβερνοχώρο να χρειάζεται να ανησυχούν

για τους μη εξουσιοδοτημένους εισβολείς [21]. Τα συστήματα IoT μεταδίδουν συνεχώς σημαντικές πληροφορίες, όπως την τοποθεσία ενός ατόμου, τραπεζικούς λογαριασμούς και ιατρικές πληροφορίες, οι οποίες μπορεί να είναι εξαιρετικά ευαίσθητες για τέτοιου είδους επιθέσεις [22][24]. Εάν συνεργαστούν μεταξύ τους οι τομείς της βιομηχανίας, της ακαδημαϊκής κοινότητας και της κυβέρνησης, οι ενδιαφερόμενοι μελλοντικοί επαγγελματίες κυβερνοασφάλειας μπορούν να συγκεντρώσουν τις γνώσεις, τους πόρους και την εμπειρογνώμοσύνη που χρειάζονται για να αναπτύξουν ολοκληρωμένες, προσαρμόσιμες και αποτελεσματικές λύσεις για τις πολύπλοκες προκλήσεις της κυβερνοασφάλειας του IoT [25].



Σχήμα 8. Οι 4 σημαντικές ευπάθειες IoT συσκευών [29]

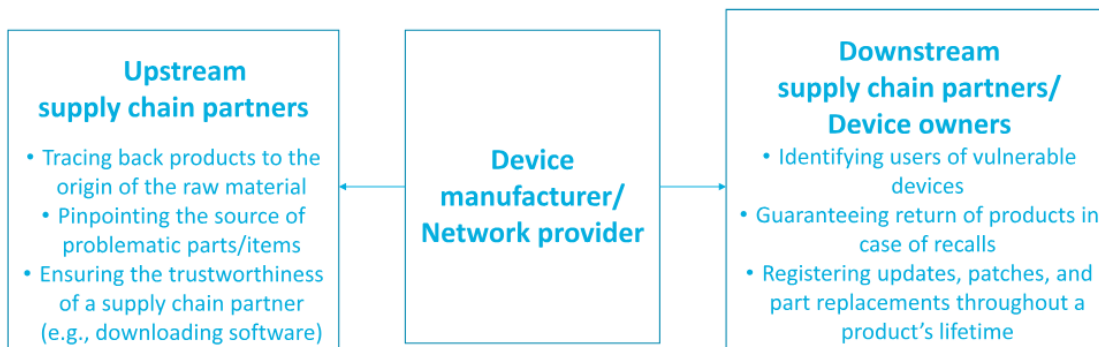
3.2.5 Γνώση τεχνολογίας Blockchain

Η αναφορά της CB Insights έχει εκτιμήσει ότι μεταξύ του 2017 και του 2018 κλάπηκαν περίπου 6 δισεκατομμύρια απόρρητα αρχεία. Επίσης, ο αριθμός των επιθέσεων στον κυβερνοχώρο έχει αυξηθεί. Αυτές οι περίπλοκες επιθέσεις έχουν καταρρεύσει τις συμβατικές μεθόδους ασφάλειας δεδομένων, δημιουργώντας έτσι προκλήσεις για την προστασία της ιδιωτικής ζωής και για τους επιχειρηματικούς οργανισμούς. Στον απόηχο της επιδημίας Covid-19, οι υπάλληλοι εκατομμυρίων εταιρειών εργάστηκαν από το σπίτι και αναγκαστικά συνδέθηκαν με το διαδίκτυο. Το γεγονός αυτό έχει επίσης δημιουργήσει έναν νέο τρόπο απειλών των δεδομένων των εταιρειών και των υπαλλήλων. Για αυτό τον λόγο, πολλοί επιχειρηματικοί οργανισμοί έχουν αρχίσει να επανεξετάζουν τα υπάρχοντα συστήματα που διαμόρφωσαν αυτά τα τρωτά σημεία, αντί να αναπτύξουν περισσότερα πιθανά εργαλεία. Υπάρχουν τεχνολογίες όπως η τεχνητή νοημοσύνη (AI), η ανάλυση μεγάλων δεδομένων, το Διαδίκτυο των πραγμάτων (IoT), και η τεχνολογία Blockchain που έχουν αναπτυχθεί για την ενίσχυση των επιχειρήσεων με αποτελεσματικό τρόπο. Η τεχνολογία Blockchain είναι μία από τις τεχνολογίες που έχουν

διαδραματίζει σημαντικό ρόλο και διασφαλίζει την ομαλή ροή της επιχειρηματικής διαδικασίας με επαρκή ασφάλεια δεδομένων στις ηλεκτρονικές επιχειρήσεις.

Το Blockchain είναι μια τεχνολογία που λειτουργεί με ομάδες μπλοκ τα οποία συνδέονται μεταξύ τους μέσω αλυσίδων. Κάθε μπλοκ λειτουργεί ως αρχείο που συγκρατεί τα δεδομένα που σχετίζονται με κάθε συναλλαγή. Περαιτέρω τα αποθηκευμένα δεδομένα μπορούν να μεταφερθούν από ένα μπλοκ σε πολλαπλά μπλοκ και με τον ίδιο τρόπο ένα μπλοκ μπορεί επίσης να συλλέξει τα δεδομένα από διαφορετικά μπλοκ ταυτόχρονα. Τα δεδομένα που αποθηκεύονται στα μπλοκ είναι μόνιμα και μη αναστρέψιμα. Έτσι, ο αριθμός των μπλοκ μπορεί να προστεθεί στην αλυσίδα ανάλογα με τον αριθμό των συναλλαγών και κάθε συναλλαγή θα επαληθεύεται για να διασφαλίζεται η αυθεντικότητα των δεδομένων. Η τεχνολογία blockchain διασφαλίζει την ασφάλεια των δεδομένων μέσω ενός ολοκληρωμένου συστήματος με το οποίο συλλέγει, τακτοποιεί, αποθηκεύει και διαδίδει τις πληροφορίες σε διάφορα μπλοκ. Με τον τρόπο αυτόν, επιτρέπεται η προσθήκη των δεδομένων στο δίκτυο. Από τη στιγμή που τα δεδομένα έχουν προστεθεί στο δίκτυο, κανείς δεν μπορεί να μεταβάλει το σύνολο των δεδομένων, είτε προσθέτοντας είτε διαγράφοντας το. Επιπλέον, η τεχνολογία αυτή βοηθά στην παρακολούθηση και τον έλεγχο των αλλαγών, εάν γίνει κάτι σε μια αλυσίδα μπλοκ, καθώς οι αλλαγές παραμένουν στη βάση δεδομένων για πάντα. Δεδομένου ότι αυτή η τεχνολογία χρησιμοποιεί πολλά συστήματα σε μια αλυσίδα μπλοκ, κατεβάζει τακτικά τα δεδομένα της, τακτοποιώντας και διατηρώντας το αντίγραφο τοπικά. Ο αλγόριθμος της τεχνολογίας Blockchain συμβάλλει στην εξάλειψη των παραδοσιακών απειλών δεδομένων, παρατηρώντας τις κακόβουλες δραστηριότητες και τις παρατυπίες. Έτσι, αυτή η τεχνολογία καθιστά ισχυρότερη την επικύρωση των δεδομένων και τα προστατεύει διατηρώντας ένα ψηφιακό μητρώο. Παρόλο που η τεχνολογία Blockchain διαθέτει διάφορα φουτουριστικά χαρακτηριστικά, δεν λειτουργεί μόνη της και χρειάζεται την υποστήριξη της τεχνολογίας της κρυπτογράφησης. Τεχνολογία Blockchain μπορεί να προστατεύσει διάφορους συνδεδεμένους θερμοστάτες, κάμερες ασφαλείας, έξυπνα κουδούνια και άλλες ευαίσθητες τεχνολογίες με κρυπτογράφηση και ψηφιακές υπογραφές. Μια έκθεση που δημοσιεύθηκε από την Palo Alto Networks αποκαλύπτει ότι το 98 τοις εκατό των κινήσεων μιας έξυπνης συσκευής IoT δεν είναι κρυπτογραφημένες και έτσι ανοίγουν ένα το δρόμο για κυβερνοεπιθέσεις.

Ως εκ τούτου, όλες οι βιομηχανίες, ανεξάρτητα από τις υπηρεσίες που προσφέρουν απαιτούν μια εξαιρετική λύση κυβερνοασφάλειας και εξαρτώνται από την τεχνολογία Blockchain για να διανέμουν τα αγαθά και τις υπηρεσίες χωρίς λάθη και απάτες. Περαιτέρω, η τεχνολογία αυτή υποστηρίζει την ψηφιοποίηση των δεδομένων των επιχειρήσεων και των πελατών. Για αυτούς τους λόγους οι βιομηχανίες, ιδίως οι διαδικτυακοί επιχειρηματικοί οίκοι, χρειάζονται έμπειρο προσωπικό που γνωρίζει να χρησιμοποιεί αυτή την εκπληκτική τεχνολογία για να καταστήσουν ισχυρότερες τις επιχειρηματικές τους διαδικασίες εξασφαλίζοντας ασφάλεια στον κυβερνοχώρο. Ακόμη και οι πάροχοι υπηρεσιών αποθήκευσης cloud έχουν αρχίσει να χρησιμοποιούν αυτή την τεχνολογία Blockchain για να διατηρούν τα δεδομένα ασφαλή από κυβερνοεπιθέσεις [26-27].



Σχήμα 9. Ο ρόλος του Blockchain στην ενίσχυση και βελτίωση της ασφάλειας σε ένα δίκτυο εφοδιαστικής αλυσίδας. [27]

3.3 Δεξιότητες κυβερνοασφάλειας και ποικιλομορφία των φύλων

Σε αντίθεση με ορισμένους άλλους τομείς της πληροφορικής, η ασφάλεια στον κυβερνοχώρο απλά δεν θα λειτουργήσει αν γίνει με λανθασμένο τρόπο. Μπορούμε να γράψουμε ένα κακό λογισμικό που θα εξακολουθεί να τρέχει για να εκπληρώσει τη λειτουργία του, αλλά η κακή τεχνική ασφάλειας δεν θα μπορέσει να παρέχει την αναμενόμενη προστασία. Για αυτόν τον λόγο, η ανάθεση των καθηκόντων ασφαλείας σε κατάλληλα καταρτισμένους επαγγελματίες είναι πολύ σημαντική. Υπάρχουν ταλαντούχοι άνθρωποι μέσα στον εργασιακό χώρο της κυβερνοασφάλειας, οι οποίοι διαθέτουν τις δεξιότητες που χρειάζεται το επάγγελμα αυτό αλλά και την ικανότητα να αναβαθμίσουν τις δεξιότητες αυτές ώστε να γίνουν ολοκληρωμένοι επαγγελματίες της ασφάλειας στον κυβερνοχώρο [32].

Σύμφωνα με έρευνες, οι γυναίκες κατά τη διάρκεια της εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο, εξακολουθούν να αντιμετωπίζουν εσφαλμένες αντιλήψεις ότι αυτός ο τομέας συνδέεται με το ανδρικό φύλο. Το γεγονός αυτό πολλές φορές τις αποτρέπει από το να επιχειρήσουν να ασχοληθούν και να εξειδικευτούν στην ασφάλεια στον κυβερνοχώρο. Παρόλα αυτά δεν είναι λίγες οι γυναίκες που έχουν γνώσεις και πτυχία στην κυβερνοασφάλεια καθώς και ικανότητες αντίστοιχες με αυτές των ανδρών. Οι γυναίκες προσθέτουν αξία στα διοικητικά συμβούλια μέσω της εμπειρίας, των γνώσεων και των δεξιοτήτων κοινωνικής αλληλεπίδρασης που κατέχουν. Έρευνες δείχνουν ότι οι γυναίκες προσθέτουν αξία στους οργανισμούς επειδή λαμβάνουν υπόψη τα συμφέροντα των ενδιαφερομένων πελατών και τα ευθυγραμμίζουν με εκείνα της επιχείρησης.

Η ενθάρρυνση της ποικιλομορφίας των φύλων στον τομέα της ασφάλειας στον κυβερνοχώρο θα συμβάλει όχι μόνο στην ανάπτυξη ενός εργατικού δυναμικού που θα έχει περισσότερα προσόντα, αλλά και που θα είναι καλύτερα προετοιμασμένο για την παροχή λύσεων ασφαλείας στον κυβερνοχώρο. Η πρωτοβουλία αυτή θα βοηθήσει επίσης τα διάφορα ενδιαφερόμενα άτομα να κατανοήσουν καλύτερα τους ρόλους και τις ευθύνες τους. Ακόμη, θα συμβάλει στη μείωση του χάσματος μεταξύ των φύλων στον τομέα της ασφάλειας στον κυβερνοχώρο και στην αντιμετώπιση της διαδικτυακής κατάχρησης λόγω φύλου [32-33].

Εμπειρικές μελέτες αναδεικνύουν τα πολλά υποσχόμενα πλεονεκτήματα της υιοθέτησης αυτών των μετασχηματισμών, όπως η αυξημένη ικανότητα για την επινόηση δημιουργικών λύσεων για τους διαρκώς παρόντες κινδύνους στον κυβερνοχώρο. Για να εξασφαλιστεί ένα ανθεκτικό εργατικό δυναμικό κυβερνοασφάλειας που θα μπορεί να προσαρμόζεται αβίαστα στο αδιάκοπα μεταβαλλόμενο περιβάλλον απειλών στον κυβερνοχώρο, είναι ζωτικής σημασίας να αντιμετωπιστεί το υφιστάμενο χάσμα μεταξύ των φύλων στον τομέα της κυβερνοασφάλειας. [9] Αυτή η έλλειψη ποικιλομορφίας στο επάγγελμα αυτό είναι επιζήμια για το παγκόσμιο εργατικό δυναμικό και τη συνεχιζόμενη μάχη κατά των κυβερνοεπιθέσεων σε ευάλωτες παγκόσμιες κοινότητες. Προφανώς, η μη ισορροπημένη εκπροσώπηση αποτελεί έναν ανεξέλεγκτο μηχανισμό κατά των μειονοτήτων και μαρτυρά της απροθυμία των γυναικών να αποτελέσουν ενεργά μέλη της λύσης για τις κυβερνοεπιθέσεις και το κυβερνοέγκλημα. Για να ξεπεραστούν αυτά τα εμπόδια, οι μειονότητες και οι γυναίκες πρέπει να ενδυναμωθούν ως πρότυπα με ικανότητα να δείξουν στη νέα γενιά ότι το επάγγελμα της κυβερνοασφάλειας είναι ένα πραγματικό εργαλείο για την προστασία των ιδιωτικών και δημόσιων οργανισμών από τους δράστες κυβερνοεπιθέσεων, ανεξάρτητα από την ισότητα και την ανισότητα των φύλων. Η κουλτούρα του επαγγελματικού μετασχηματισμού είναι επιβεβλημένη και πρέπει να περιέχει μια μετάβαση προς όφελος της πόλης, του κράτους, του έθνους και της παγκόσμιας οικονομίας κάτι το οποίο αναπόφευκτα απαιτεί τη συνδυασμένη τεχνογνωσία και τα talέντα των μειονοτήτων και των γυναικών και των ανδρών. Οι μειονότητες, ιδίως οι μειονότητες φύλου, είναι συχνά έτοιμες και ικανές να εργαστούν ανεξάρτητα και επαγγελματικά με πρωταρχική περιορισμένη επίβλεψη για να ολοκληρώσουν τα καθήκοντα που τους έχουν ανατεθεί ακριβώς όπως οι άνδρες συνάδελφοί τους εν μέσω προκλήσεων [56].

Οι οργανισμοί και οι εταιρείες που αναζητούν ειδικευμένους επαγγελματίες πρέπει να γνωρίζουν τις ικανότητες που αναζητούν, τις σχετικές πιστοποιήσεις και προσόντα και όχι να περιορίζονται σε προκαταλήψεις φύλου. Οι επαγγελματίες της ασφάλειας στον κυβερνοχώρο καλούνται έντονα να σχηματίσουν ένα ενιαίο μέτωπο για να συμπεριλάβουν τις μειονότητες γυναικών σε όλες τις πτυχές της εκπαίδευσης στον κυβερνοχώρο που ενθαρρύνουν την πνευματική διέγερση και τις επαγγελματικές ευκαιρίες. Αν θέλουμε να αντιμετωπίσουμε την έλλειψη δεξιοτήτων, πρέπει να ενθαρρύνουμε τους ανθρώπους να ενταχθούν στο επάγγελμα αυτό, από ένα ευρύ φάσμα υποβάθρων και να ψάξουμε μέσα στο σημερινό εργατικό δυναμικό. Υπάρχουν όπως αναφέρθηκε παραπάνω, ταλαντούχοι άνθρωποι ανεξαρτήτως φύλου, που έχουν δεξιότητες οι οποίες είναι απαραίτητες στο επάγγελμα αυτό. Πρέπει, λοιπόν, οι οργανισμοί να επενδύσουν σε αυτούς και να τους βοηθήσουν να αναβαθμιστούν κατάλληλα [32][56].

4

Κυβερνοασφάλεια και εκπαίδευση

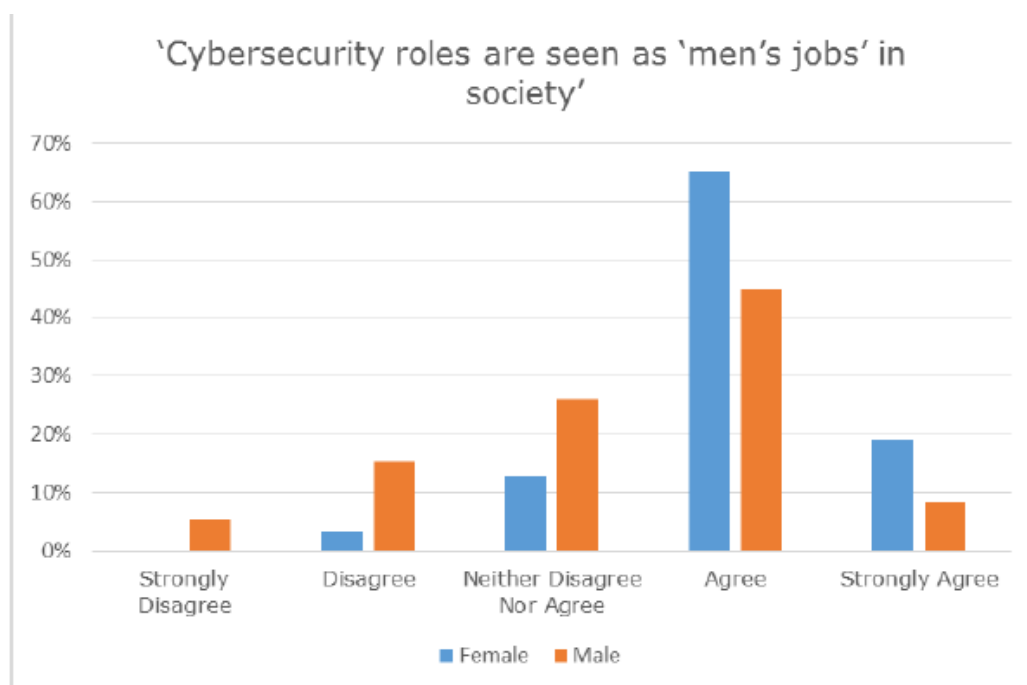
4.1 Προκλήσεις που αντιμετωπίζουν τα φύλα στην εκπαίδευση για την κυβερνοασφάλεια

Όπως αναφέρθηκε και στα προηγούμενα κεφάλαια το έγκλημα και οι επιθέσεις στον κυβερνοχώρο καθημερινά αυξάνονται. Η αντιμετώπιση αυτού του ζητήματος είναι μια από τις πιο κρίσιμες ανάγκες στον τομέα της πληροφορικής. Ωστόσο, η βιομηχανία κυβερνοασφάλειας αντιμετωπίζει σημαντικά κενά απασχόλησης, με ακάλυπτες θέσεις. Το 2019, υπήρχαν πάνω από 313.000 κενές θέσεις εργασίας που σχετίζονται με την κυβερνοασφάλεια στις Ηνωμένες Πολιτείες. Παρόλο που οι γυναίκες αντιπροσωπεύουν περίπου το 50% του συνολικού εργατικού δυναμικού, αποτελούν μόνο το 11% των εργαζομένων στον τομέα της ασφάλειας στον κυβερνοχώρο. Σε πιο πρόσφατες αναφορές ο αριθμός των γυναικών στην κυβερνοασφάλεια ανέρχεται στο 20% του εργατικού δυναμικού, το οποίο δείχνει μια σαφή βελτίωση, αλλά εξακολουθεί να είναι πολύ χαμηλό. Τα προηγούμενα οκτώ χρόνια, υπήρξε σταθερή αύξηση του αριθμού των πτυχίων που σχετίζονται με STEM, που αποκτήθηκαν από γυναίκες φοιτήτριες. Υπήρξε μια αύξηση 48% για τις γυναίκες από το 2008 έως το 2016, ενώ ο αριθμός των ανδρών που απέκτησαν το ίδιο πτυχίο είχε μια αύξηση 38% την ίδια χρονική περίοδο. Το γεγονός αυτό, είναι ενθαρρυντικό και υποδηλώνει περαιτέρω κίνηση προς την κατεύθυνση της κάλυψης του χάσματος μεταξύ των δύο φύλων στον κυβερνοχώρο, αν και το χάσμα εξακολουθεί να υφίσταται. Για να αντιμετωπίσουμε το χάσμα αυτό, είναι απαραίτητο να κατανοήσουμε τις προκλήσεις που αντιμετωπίζουν οι μαθητές, που αργότερα θα γίνουν φοιτητές, οι οποίοι επιδιώκουν να εκπαιδευτούν στον τομέα της πληροφορικής και ειδικότερα της κυβερνοασφάλειας [34]. Είναι λοιπόν σημαντικό να εξετάσουμε αν έχουν τις ίδιες ευκαιρίες στην εκπαίδευση του τομέα αυτού όλα τα φύλα.

4.1.1 Κοινωνικά εμπόδια

Υπάρχουν διάφοροι λόγοι για την ανισορροπία των φύλων στον τομέα των ΤΠΕ. Ξεκινώντας, παρά το γεγονός ότι τα κορίτσια είναι περισσότερα και καλύτερα από τα αγόρια στον

τομέα των STEM, δεν φιλοδοξούν να εμβαθύνουν στον κλάδο της τεχνολογίας, καθώς αυτός θεωρείται ότι είναι «για αγόρια». Ακόμη, ο τρόπος με τον οποίον η τεχνολογία έχει κατασκευαστεί κοινωνικά, χρησιμοποιώντας μια «βίαιη» γλώσσα μπορεί να μην απασχολεί τους περισσότερους άνδρες, αλλά μπορεί να αποτελέσει πρόβλημα για τις γυναίκες. Για παράδειγμα, το ψυχαγωγικό ή ακόμη και το εκπαιδευτικό λογισμικό για παιδιά συχνά περιλαμβάνει λέξεις όπως «attack» ή «war» [35]. Η κοινωνία έχει βαθύτατο αντίκτυπο στις εικόνες των νεαρών κοριτσιών για την εαυτό τους και την επιστήμη των υπολογιστών, πόσο μάλλον για την εμβάθυνση στον κλάδο της κυβερνοασφάλειας. Δυστυχώς, οι περισσότερες από τις εικόνες της επιστήμης της πληροφορικής είναι αρνητικές και υπονοούν ότι η πληροφορική είναι για σπασίκλης (geeks) ή μόνο για άνδρες. Το κοινωνικό περιβάλλον και οι γονείς διδάσκουν στα παιδιά πώς να συμπεριφέρονται σαν αγόρια ή κορίτσια, παρόλο που η σωματική ανάπτυξη όλων των παιδιών είναι περίπου η ίδια μέχρι την εφηβεία. Στην περίοδο της εφηβείας, η πίεση των συνομηλίκων είναι στο υψηλότερο σημείο της και είναι η αιτία για πολλά ταλαντούχα νεαρά κορίτσια να χάσουν κάθε ενδιαφέρον για την επιστήμη και την τεχνολογία, ιδίως για τους υπολογιστές [38]. Όσες από τις γυναίκες συνεχίζουν στην τριτοβάθμια εκπαίδευση σπουδές σε επιστημονικά και τεχνικά πεδία, όπως αυτό της κυβερνοασφάλειας, υποφέρουν από τις συνέπειες συνεχούς παρενόχλησης. Αρχίζουν να αμφιβάλλουν για τις ικανότητές τους παρά τις ενδείξεις ότι έχουν την ικανότητα να επιτύχουν στον τομέα που επιλέγουν. Παρόλο που η υποβάθμιση της γυναικείας ακαδημαϊκής συνεισφοράς είναι συχνά ακούσια, πολλά μικρά περιστατικά έχουν αθροιστικό αποτέλεσμα και για πολλές γυναίκες, αυτό οδηγεί στην απώλεια της αυτοεκτίμησης, την πεποίθηση ότι είναι λιγότερο ικανές από τους άλλους γύρω τους και την απροθυμία να ξεκινήσουν σπουδές στην ασφάλεια του κυβερνοχώρου [35].



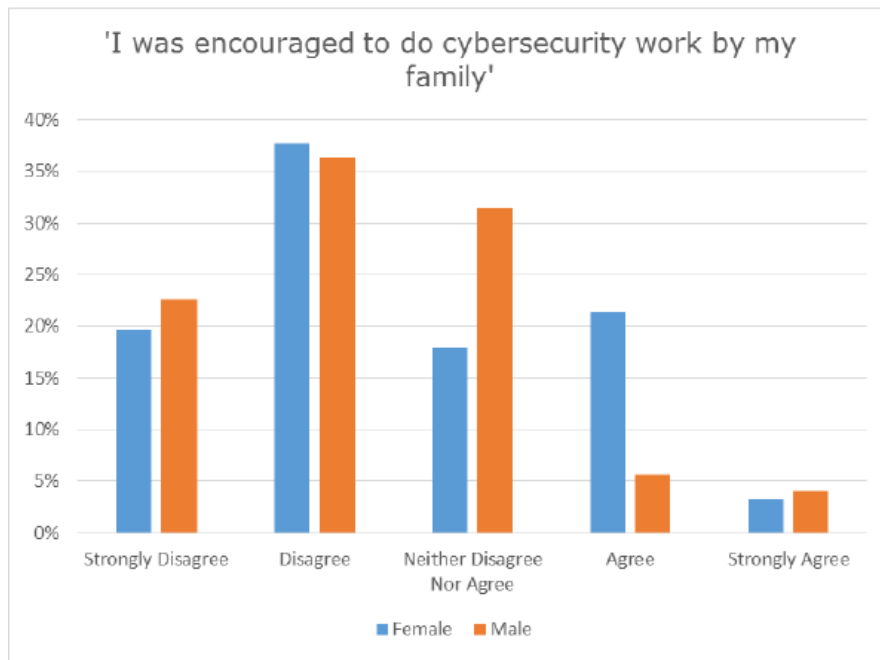
Σχήμα 10. «Οι ρόλοι της ασφάλειας στον κυβερνοχώρο θεωρούνται ως “ανδρικές δουλειές” στην κοινωνία» [36]

Όπως φαίνεται στον Σχήμα 10, υπάρχει η σημαντική αντίληψη ότι οι θέσεις εργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο θεωρούνται «ανδρικές θέσεις εργασίας» από την κοινωνία. Η αντίληψη αυτή είναι σημαντικά ισχυρότερη μεταξύ των γυναικών ερωτηθέντων απ' ό,τι μεταξύ των ανδρών ερωτηθέντων, με 84,1% των γυναικών ερωτηθέντων να συμφωνούν ή να συμφωνούν απόλυτα με τη δήλωση σε σύγκριση με το 53,4% των ανδρών ερωτηθέντων.

Η αντίληψη που προκύπτει από το Σχήμα 10 είναι ότι τα στερεότυπα φύλου είναι περισσότερο εμφανή στην ευρύτερη κοινωνία παρά στον ίδιο τον κλάδο. Αυτό μπορεί να συμβάλλει στην ενίσχυση της ανισότητας στον κλάδο. Οι εργοδότες μπορεί να είναι απρόθυμοι να προσλάβουν άτομα που θεωρούν ότι δεν ταιριάζουν με τις αντιλήψεις των καταναλωτών ή των πελατών τους. Υπάρχει αντιληπτή ανισότητα στις προσλήψεις και τις προαγωγές και διατυπώνεται επίσης η άποψη ότι υπάρχουν στερεότυπα φύλου σε σχέση με τους ρόλους εργασίας. Οι ανισότητες που γίνονται αντιληπτές σε αυτούς τους τομείς θεωρούνται μεγαλύτερες από τις γυναίκες ερωτηθέντες. Οι γυναίκες μπορεί να έχουν υψηλότερο επίπεδο ευαισθητοποίησης σχετικά με την ανισότητα στον κλάδο, καθώς είναι πιθανότερο να την έχουν βιώσει άμεσα [36].

4.1.2 Έλλειψη οικογενειακής υποστήριξης

Προχωρώντας, η έλλειψη οικογενειακής υποστήριξης των μαθητών στο να εκπαιδευτούν στο τεχνολογικό κομμάτι της κυβερνοασφάλειας, τους αποθαρρύνει από κάθε προσπάθεια. Αυτό συμβαίνει λόγω έλλειψης γνώσεων ή και εμπιστοσύνης των γονέων στο κομμάτι των τεχνολογιών. Έρευνες δείχνουν ότι η υποστήριξη των γονέων έχει μεσολαβητική επίδραση στα παιδιά. Όσο μεγαλύτερη υποστήριξη έχουν από τους γονείς τους για να ακολουθήσουν την πληροφορική, τόσο μεγαλύτερη είναι η τεχνολογική τους περιέργεια. Δεδομένα από αυτές τις έρευνες δείχνουν ότι τα κορίτσια βλέπουν τους γονείς και άλλα μέλη της οικογένειάς τους, ως τη μεγαλύτερη επιρροή στα επαγγελματικά και εκπαιδευτικά τους ενδιαφέροντα και στόχους. Τα παιδιά μπορούν να εκτεθούν σε έμφυλες προκαταλήψεις και μέσα στην ίδια τους την οικογένεια. Δυστυχώς, ορισμένοι γονείς παρέχουν ακούσια εμπόδια στις ίδιες τους τις κόρες και μέσω ανεπαίσθητων προκαταλήψεων υποστηρίζουν περισσότερο τα αρσενικά παιδιά τους. Για παράδειγμα, η πλειονότητα των «οικογενειακών» υπολογιστών είναι συνήθως εγκατεστημένη στο υπνοδωμάτιο του γιου [38]. Ωστόσο, όπως έχει διαπιστωθεί, ακόμη και όταν οι γονείς υποστηρίζουν τα παιδιά τους στην εκπαίδευσή τους στην κυβερνοασφάλεια, η φύση της υποστήριξης αυτής φαίνεται να είναι περισσότερο συναισθηματική (ενθάρρυνση να επιδιώξουν τα όνειρά τους), παρά εργαλειακή (παροχή πληροφοριών σχετικά με τον τρόπο επίτευξης των στόχων τους) [35].

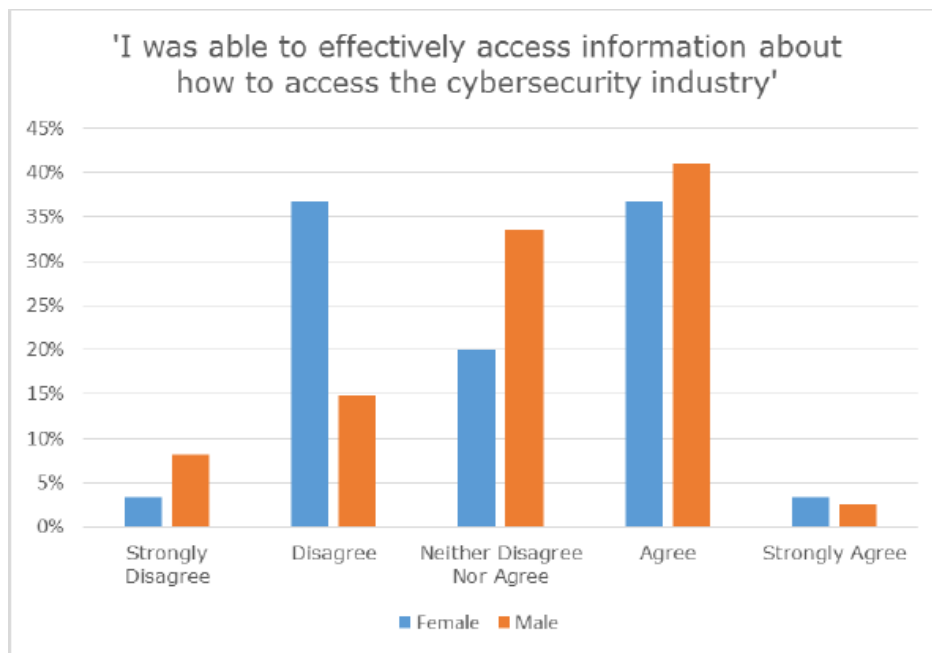


Σχήμα 11. «Με ενθάρρυνε η οικογένειά μου να δουλέψω στην κυβερνοασφάλεια»[36]

Το διάγραμμα στο Σχήμα 11 δείχνει ότι κάτι παραπάνω από το 35% των γυναικών που απάντησαν σε έρευνα που έγινε, διαφώνησαν απόλυτα ότι ενθαρρύνθηκαν από την οικογένειά τους να ασχοληθούν με την ασφάλεια στον κυβερνοχώρο, ενώ μόνο το 9,6% των ανδρών συμφώνησαν ή συμφώνησαν απόλυτα.

4.1.3 Έλλειψη σχολικής υποστήριξης

Η έλλειψη ενθάρρυνσης και υποστήριξης κυριαρχεί και μέσα στα σχολεία, όπου δεν υπάρχουν τα κατάλληλα εκπαιδευτικά μέσα, τα οποία θα μεταδώσουν τις απαραίτητες γνώσεις κυβερνοασφάλειας στα παιδιά που βρίσκουν κάποιο ενδιαφέρον στον τομέα αυτόν. Πολλοί μαθητές δεν έχουν ιδέα για το τι συνεπάγεται η πληροφορική, και μόνο όταν την βιώνουν τυχαία, συνειδητοποιούν ότι είναι κάτι που τους ενδιαφέρει και απολαμβάνουν. Είναι αξιοσημείωτο όμως να αναφέρουμε, ότι δεν παρατηρείται διαφορά που να γίνεται αντιληπτή από τα δύο φύλα όσον αφορά τα επίπεδα ενθάρρυνσης στην εκπαίδευση. Παρόλα αυτά, στα σχολεία δεν υπάρχουν αρκετά γυναικεία πρότυπα από τα οποία θα μπορούσαν τα κορίτσια να πάρουν θάρρος και να τα έχουν ως παράδειγμα για την ενασχόληση τους με τον τομέα της πληροφορικής και αργότερα της κυβερνοασφάλειας. Αν και τα κορίτσια σήμερα έρχονται αντιμέτωπα με λιγότερα στερεότυπα των φύλων σε σχέση με τα προηγούμενα χρόνια, αυτές οι πεποιθήσεις έχουν μια ισχυρή σύνδεση με τις προσδοκίες τους για επιτυχία, καθώς και με τον τρόπο με τον οποίο βλέπουν την πληροφορική και ειδικά την κυβερνοασφάλεια, ως σημαντική ή σχετική με τα ενδιαφέροντά τους. Όταν μάλιστα στα σχολεία δεν υπάρχουν εκπρόσωποι του γυναικείου φύλου, το αίσθημα της κατωτερότητας ενισχύεται. Παρά αυτή την αντιληπτή ισότητα των φύλων στην ενθάρρυνση τους, στο εκπαιδευτικό σύστημα και στον κλάδο της κυβερνοασφάλειας παρατηρούμε σημαντικές διαφορές στην ικανότητά τους να έχουν πρόσβαση σε πληροφορίες σχετικά με τον τρόπο εισόδου στον κλάδο. Οι γυναίκες έχουν σχεδόν τις μισές πιθανότητες να μπορέσουν να το κάνουν αυτό αποτελεσματικά [36-37].



Σχήμα 12. «Είχα αποτελεσματική πρόσβαση σε πληροφορίες σχετικά με το πώς να ενταχθώ στον τομέα της κυβερνοασφάλειας. » [36]

Οι γυναίκες ήταν πιο πιθανό να αναφέρουν ότι δεν μπορούσαν να έχουν αποτελεσματική πρόσβαση σε πληροφορίες σχετικά με τον τρόπο εισαγωγής στον κλάδο της κυβερνοασφάλειας. Όπως βλέπουμε στο σχήμα 12, οι γυναίκες αυτές αποτελούν το 40% σε σύγκριση με το 15% των ανδρών που βρήκαν επίσης δύσκολη την πρόσβασή τους σε πληροφορίες σχετικές με το επάγγελμα. Οι γυναίκες που συμμετείχαν στην έρευνα ανέφεραν ότι είχαν περιορισμένες ευκαιρίες ή πρόσβαση στη χρήση ηλεκτρονικών υπολογιστών. Γενικά, τα κορίτσια στο σχολείο μαθαίνουν πώς να χρησιμοποιούν το Διαδίκτυο. Ωστόσο, σύμφωνα με μια μελέτη που έγινε από την AAUW τα κορίτσια δεν μαθαίνουν προγραμματισμό και ασφάλεια ηλεκτρονικών υπολογιστών στο σχολείο ώστε να εμβαθύνουν στον τομέα αυτόν, αλλά μόνο βασικές δεξιότητες χρήσης υπολογιστών που επικεντρώνονται σε γραφειοκρατικές εργασίες και εισαγωγή δεδομένων [36].

4.2 Εκπαιδευτικές προσεγγίσεις κυβερνοασφάλειας

4.2.1 Πανεπιστημιακή εκπαίδευση

Για την ανάπτυξη μιας επιτυχημένης εκπαίδευσης στον τομέα της κυβερνοασφάλειας, απαιτείται διεπιστημονική προσέγγιση η οποία θα περιλαμβάνει τόσο τεχνικούς όσο και μη τεχνικούς κλάδους. Το 2014, το Ινστιτούτο Ponemon προσδιόρισε τις δώδεκα κορυφαίες σχολές για την κυβερνοασφάλεια και η τοποθέτηση των πτυχίων τους στον τομέα της κυβερνοασφάλειας είναι αποκαλυπτική. Ένα από τα σημαντικότερα ευρήματα αυτής της μελέτης ήταν ότι η εκπαίδευση στον τομέα της κυβερνοασφάλειας σε αυτές τις δώδεκα σχολές τέμνει και άλλα επιστημονικά πεδία εκτός της επιστήμης των υπολογιστών, όπως η μηχανική, η διοίκηση και οι

μελέτες πολιτικής. Δόθηκε επίσης έμφαση σε μαθήματα που περιλάμβαναν την ηγεσία, τη διακυβέρνηση και την πολιτική ασφάλειας πληροφοριών, καθώς και στην ανάπτυξη σταδιοδρομίας και την επαγγελματική ανέλιξη των σπουδαστών. Ενώ πολλοί κλάδοι εξελίσσονται με την πάροδο του χρόνου, η ασφάλεια στον κυβερνοχώρο αντιμετωπίζει ένα συνεχώς μεταβαλλόμενο τοπίο απειλών, τρωτών σημείων και αντίμετρων που μπορούν να επηρεάσουν τα προγράμματα σπουδών. Ακριβώς όπως οι επαγγελματίες της κυβερνοασφάλειας πρέπει να συμμετέχουν σε συνεχή εκπαίδευση για να διασφαλίσουν ότι παραμένουν επίκαιρες οι δεξιότητές τους, τα IHL με προγράμματα ασφάλειας στον κυβερνοχώρο πρέπει επίσης να είναι προετοιμασμένα και να αξιολογούν συνεχώς το πρόγραμμα σπουδών τους για να παρέχουν στους φοιτητές τις πιο πρόσφατες και σχετικές γνώσεις για να επιτύχουν στο τομέα αυτόν. Προγράμματα μεταπτυχιακού επιπέδου στην κυβερνοασφάλεια προσφέρονται πλέον ευρέως από πανεπιστήμια σε όλο τον κόσμο [39].

Είναι ενδιαφέρον να αναφέρουμε ότι μόνο ένα από τα είκοσι κορυφαία πανεπιστήμια στις ΗΠΑ προσφέρει ένα πτυχίο που σχετίζεται με την ασφάλεια στον κυβερνοχώρο, συγκεκριμένα, BSc. in Computer Science Engineering with a concentration in Cybersecurity. Επιπλέον, ενώ εννέα πανεπιστήμια προσφέρουν μεταπτυχιακό τίτλο σπουδών στην κυβερνοασφάλεια, μόνο ένα προσφέρει διδακτορικό δίπλωμα στον τομέα αυτόν. Ένα από τα πανεπιστήμια προσφέρει μεταπτυχιακό πρόγραμμα στην Δημόσια Πολιτική με εστίαση στην κυβερνοασφάλεια, όπου οι φοιτητές μελετούν τα νομικά ζητήματα που αφορούν τον έλεγχο πρόσβασης, ιδιωτικότητας των χρηστών και την ανάλυση απειλών. Παρομοίως, ένα άλλο πανεπιστήμιο προσφέρει μεταπτυχιακό πρόγραμμα στις Διεθνείς Σπουδές με έμφαση στην Κυβερνοασφάλεια που καλύπτει θέματα όπως οι άνθρωποι και η τεχνολογία, η απειλή της τρομοκρατίας και του εγκλήματος, και εγκληματολογία υπολογιστών και κυβερνοχώρου. Η πλειονότητα των πανεπιστημίων στις ΗΠΑ προσφέρει επίσης προγράμματα πιστοποίησης για επαγγελματίες στην κυβερνοασφάλεια. Ακόμη, υπάρχει ένα εκπαιδευτικό πρόγραμμα 24 εβδομάδων για την ασφάλεια στον κυβερνοχώρο. Αυτά τα προγράμματα για επαγγελματίες φαίνεται να είναι αρκετά δημοφιλή μεταξύ αυτών των μεγάλων πανεπιστημίων αλλά σίγουρα απαιτούν να υπάρχουν ήδη γνώσεις πληροφορικής και δικτύωσης. Στο Ηνωμένο Βασίλειο, μόνο πέντε από τα δέκα κορυφαία πανεπιστήμια προσφέρουν πτυχία στην κυβερνοασφάλεια ή την ασφάλεια πληροφοριών. Ένα από αυτά τα πέντε πανεπιστήμια προσφέρει τόσο μεταπτυχιακά όσο και διδακτορικά πτυχία, ενώ τα άλλα τέσσερα προσφέρουν μόνο μεταπτυχιακό. Στην Ευρώπη, τρία από τα δέκα κορυφαία πανεπιστήμια προσφέρουν μεταπτυχιακά πτυχία στην κυβερνοασφάλεια. Ενώ σχεδόν όλα τα πανεπιστήμια προσφέρουν βασικές γνώσεις πληροφορικής, μόνο λίγα περιλαμβάνουν την ασφάλεια στον κυβερνοχώρο ως υποχρεωτικό μάθημα. Πολλά πανεπιστήμια επιλέγουν να προσφέρουν μαθήματα που σχετίζονται με την κυβερνοασφάλεια μόνο ως μαθήματα επιλογής για το τμήμα Πληροφορικής Επιστήμης ή Μηχανικών και τους φοιτητές που μπορεί να ενδιαφέρονται για αυτά [40].

Σχεδόν όλα τα μεταπτυχιακά προγράμματα κυβερνοασφάλειας απαιτούν από τους υποψηφίους να έχουν πτυχίο πληροφορικής ή ισοδύναμο, όπως πληροφοριακά συστήματα, μηχανική λογισμικού, μηχανική υπολογιστών, μαθηματικά ή στατιστική. Ο διεπιστημονικός χαρακτήρας των μεταπτυχιακών προγραμμάτων κυβερνοασφάλειας δικαιολογεί την αποδοχή υποψηφίων με διαφορετικό υπόβαθρο. Επιπλέον, το Πανεπιστήμιο Ben-Gurion του The Negev, το Πανεπιστήμιο George Mason και το Πανεπιστήμιο Queen's του Μπέλφαστ, το Πανεπιστήμιο του

Waikato και το Πανεπιστήμιο George Washington, απαιτούν οι υποψήφιοι να έχουν βαθμούς ενός υψηλού επιπέδου σε μαθήματα STEM. Ορισμένα πανεπιστήμια προχωρούν ένα βήμα ακόμη πιο μπροστά και δηλώνουν τις απαιτούμενες βασικές γνώσεις. Μπορεί να περιλαμβάνουν άλγεβρα, προγραμματισμό υπολογιστών, δίκτυα, θεωρία υπολογισμού, λειτουργικά συστήματα και Linux. Το Πανεπιστήμιο John Hopkins παρουσιάζει λεπτομερείς πληροφορίες σχετικά με το απαιτούμενο υπόβαθρο: η προηγούμενη εκπαίδευση των υποψηφίων θα πρέπει να περιλαμβάνει ένα έτος μαθηματικών ένα μάθημα προγραμματισμού σε Java ή C++, ένα μάθημα στις δομές δεδομένων, και ένα μάθημα οργάνωσης υπολογιστών [41].

Στο παρακάτω Σχήμα 13 μπορεί κανείς να παρατηρήσει ότι το Ηνωμένο Βασίλειο και οι ΗΠΑ έχουν τα περισσότερα μεταπτυχιακά προγράμματα που αφορούν την ασφάλεια στον κυβερνοχώρο. Το Ηνωμένο Βασίλειο έχει 16 μεταπτυχιακά προγράμματα και οι ΗΠΑ έχουν 25. Στον ίδιο πίνακα μπορεί κανείς να παρατηρήσει ότι η Ισπανία ακολουθεί με μόνο 2 προγράμματα και η Εσθονία, η Φινλανδία, η Γαλλία και οι Κάτω Χώρες με μόνο 2 προγράμματα η καθεμία, επίσης.

Country	Number of Programs
Australia	1
Cyprus	1
Czech Republic	1
Estonia	2
Finland	2
France	2
Germany	1
India	1
Italy	1
Lithuania	1
Malaysia	1
Malta	1
Netherlands	2
New Zealand	1
Spain	2
UK	16
USA	25
Total	61

Σχήμα 13. Μεταπτυχιακά προγράμματα Κυβερνοασφάλειας σε διάφορες χώρες [42]

- Στο Ηνωμένο Βασίλειο το διάστημα 2011-2016 συμπεριλήφθηκε η ασφάλεια στον κυβερνοχώρο σε όλα τα πτυχία που πιστοποιούνται από τη Βρετανική Εταιρεία Υπολογιστών και το Institution of Engineering & Technology. Επιπλέον, δημιουργήθηκαν υποτροφίες CyberFist για την υποστήριξη και την προετοιμασία των προπτυχιακών φοιτητών για μια καριέρα στην ασφάλεια στον κυβερνοχώρο, οι οποίες χρηματοδοτήθηκαν από την Ακαδημία Ανώτατης Εκπαίδευσης. Τέλος, το NCSC πιστοποίησε μεταπτυχιακά και προπτυχιακά. Όσον αφορά την έρευνα, δημιουργήθηκαν νέα ερευνητικά ινστιτούτα, διάφορα Ακαδημαϊκά Κέντρα Αριστείας στην έρευνα για την ασφάλεια στον κυβερνοχώρο και κέντρα διδακτορικής εκπαίδευσης.
- Στις ΗΠΑ η κυβέρνηση πρότεινε την αύξηση της ομοσπονδιακής χρηματοδότησης για το «CyberCorps: Υποτροφία για την αύξηση των φοιτητών στον τομέα της ασφάλειας στον

κυβερνοχώρο που εισέρχονται στο ομοσπονδιακό εργατικό δυναμικό. Σύμφωνα με το (ISC)², ο σημερινός αριθμός των Κέντρων Ακαδημαϊκής Αριστείας (CAE) στις Ηνωμένες Πολιτείες δεν επαρκεί για να δημιουργήσει το αριθμό εμπειρογνομόνων κυβερνοασφάλειας που χρειάζεται ο κλάδος.

- Στην Εσθονία, μια κοινή σύμπραξη μεταξύ του Τεχνικού Πανεπιστημίου του Τάλλιν, της Εθνικής Άμυνας της Εσθονίας και του Κέντρου Εκπαίδευσης και Ανάπτυξης στα συστήματα επικοινωνίας και πληροφοριών των εσθονικών αμυντικών δυνάμεων, δημιούργησε ένα διεθνές μεταπτυχιακό δίπλωμα στην ασφάλεια στον κυβερνοχώρο με ετήσια εισαγωγή 50 φοιτητών. Ένα νέο μεταπτυχιακό πρόγραμμα σπουδών στην ψηφιακή εγκληματολογία άνοιξε το 2014. Η κυβέρνηση σχεδιάζει επίσης να παράσχει στήριξη για την αύξηση του αριθμού των φοιτητών που ολοκληρώνουν μεταπτυχιακά στην ασφάλεια στον κυβερνοχώρο και να αυξήσει τον αριθμό των διδακτορικών διατριβών.
- Στην Αυστραλία, δημιουργήθηκαν ακαδημαϊκά κέντρα ασφάλειας στον κυβερνοχώρο στα πανεπιστήμια και υπάρχουν ετήσιοι διαγωνισμοί κυβερνοασφάλειας για την ανάπτυξη δεξιοτήτων.
- Στην Γαλλία η κυβέρνηση θέλει να ενσωματώσει την ευαισθητοποίηση σε θέματα ασφάλειας στον κυβερνοχώρο σε όλα τα προγράμματα ανώτερης εκπαίδευσης, καθώς και σε ειδική επιμόρφωση σε όλη την τριτοβάθμια εκπαίδευση που περιλαμβάνει κάποια τεχνολογία πληροφοριών [43].

Μπορούμε λοιπόν να δούμε πως η διαθεσιμότητα προπτυχιακών πτυχίων της Κυβερνοασφάλειας είναι αρκετά ελλιπής παγκοσμίως, παρά τις κάποιες προσπάθειες που έχουν γίνει. Ενώ ορισμένα πανεπιστήμια προσφέρουν μαθήματα κυβερνοασφάλειας σε προπτυχιακό επίπεδο, τα μαθήματα αυτά δεν είναι επαρκώς διαθέσιμα για την ανάπτυξη δεξιοτήτων ασφάλειας στον κυβερνοχώρο που απαιτούνται για την κάλυψη των κενών θέσεων εργασίας στον κυβερνοχώρο [40].

4.2.2 Συνεργασία Πανεπιστημίων και εργοδοτών.

Η συνεργασία εργοδοτών, πανεπιστημίων και κολεγίων δίνει την δυνατότητα στους ανθρώπους να συνδυάσουν τόσο τις ακαδημαϊκές σπουδές ενός παραδοσιακού πανεπιστημιακού πτυχίου όσο και την πρακτική εμπειρία και τις ευρύτερες δεξιότητες απασχόλησης, οι οποίες είναι ζωτικής σημασίας για την επιτυχία και την σταδιοδρομία των φοιτητών. Οι μαθητευόμενοι με πτυχίο μοιράζουν το χρόνο τους μεταξύ των πανεπιστημιακών σπουδών και του χώρου εργασίας και απασχολούνται καθ' όλη τη διάρκεια σε προγράμματα μαθητείας που διαρκούν περίπου τέσσερα χρόνια [44]. Για να ανταπεξέλθουν στην εξελισσόμενη αγορά εργασίας και για να μπορέσουν οι απόφοιτοι να διαφοροποιηθούν από τους υπόλοιπους, τα πανεπιστήμια αναζητούν συνεχώς βιώσιμους τρόπους ενίσχυσης της επαγγελματικής απασχόλησης των φοιτητών. Η επαγγελματική απασχόληση των φοιτητών πριν αποκτήσουν το πτυχίο τους, μπορεί να διευκολύνει την πρακτική εφαρμογή των γνώσεων και δεξιοτήτων που βασίζονται στο γνωστικό αντικείμενο. Με αυτόν τον τρόπο οι φοιτητές ενισχύουν την αυτοπεποίθησή τους, εντοπίζουν τα κενά στην τεχνική τους εξειδίκευση και ενθαρρύνονται να φέρουν καινοτόμες ιδέες, από τη μάθησή τους μέσα στην τάξη, καθώς και να μεταφέρουν επιτυχώς δεξιότητες και γνώσεων όταν τελικά εισέλθουν στο

εργατικό δυναμικό ως νέοι απόφοιτοι [45]. Οι έρευνες δείχνουν σταθερά ότι οι εταιρείες αξιολογούν την πρακτική εμπειρία πάνω από όλους τους άλλους παράγοντες όταν αξιολογούν άτομα για νέες προσλήψεις. Η ενσωμάτωση ενός πρακτικού περιβάλλοντος μάθησης όπου οι φοιτητές εργάζονται πάνω σε ρεαλιστικές προκλήσεις κυβερνοασφάλειας έχει αναγνωριστεί ως ένας από τους πιο βασικούς παράγοντες που ξεχωρίζουν τους κορυφαίους επαγγελματίες της κυβερνοασφάλειας [46].

Η PwC δέχεται φοιτητές του πρώτου έως τέταρτου έτους προπτυχιακών σπουδών και η πρακτική άσκηση διαρκεί τουλάχιστον οκτώ εβδομάδες κατά τη διάρκεια των θερινών ή χειμερινών διακοπών. Το πρόγραμμα αυτό προσφέρει επίσης την ευκαιρία οι φοιτητές να εξασφαλίσουν μια θέση στο πρόγραμμα μεταπτυχιακών σπουδών της εταιρείας, το οποίο είναι ένα από τα πιο αναγνωρισμένα στην επιχειρηματική κοινότητα. Το πρόγραμμα πρακτικής άσκησης της PwC παρέχει απaráμιλλες ευκαιρίες στους φοιτητές να εργαστούν δίπλα σε έμπειρους επαγγελματίες για να αναπτύξουν νέες δεξιότητες και ιδιότητες, να εφαρμόσουν στην πράξη όσα έχουν μάθει στο πανεπιστήμιο και να γνωρίσουν πώς είναι η εργασιακή ζωή στην πραγματικότητα [47].

Το NICE Cybersecurity Apprenticeship Program Finder είναι ένα εργαλείο που βοηθά στον εντοπισμό προγραμμάτων πρακτικής άσκησης στον κυβερνοχώρο στις Ηνωμένες Πολιτείες. Η πρακτική άσκηση παρέχει στους εκπαιδευόμενους πρόσβαση σε υψηλής ποιότητας μονοπάτια, ευθυγραμμισμένα με τις ανάγκες των εργοδοτών. Για την ασφάλεια στον κυβερνοχώρο, όπου υπάρχει έλλειψη εργαζομένων που είναι έτοιμοι για εργασία, η πρακτική άσκηση μπορεί να συμβάλει στην παροχή εξειδικευμένων ταλέντων στον κυβερνοχώρο. Οι συμμετέχοντες σε προγράμματα μαθητείας λαμβάνουν αμειβόμενη εργασιακή εμπειρία και μάθηση με βάση την μελλοντική εργασία και με την ολοκλήρωση του προγράμματος καταλαμβάνουν ένα αναγνωρισμένο σε εθνικό ή κρατικό επίπεδο πιστοποιητικό κυβερνοασφάλειας [48].

Η CISA, στις ΗΠΑ, προσλαμβάνει φοιτητές εγγεγραμμένους σε αναγνωρισμένα εκπαιδευτικά ιδρύματα από το λύκειο έως το μεταπτυχιακό επίπεδο για αμειβόμενη πρακτική άσκηση στον κυβερνοχώρο/στην πληροφορική. Η CISA συνεργάζεται με βιομηχανικούς και κυβερνητικούς εταίρους για την άμυνα κατά των σημερινών απειλών στον κυβερνοχώρο και την οικοδόμηση μιας πιο ασφαλούς και ανθεκτικής υποδομής στον κυβερνοχώρο του μέλλοντος. Ως ασκούμενος στην CISA, οι φοιτητές αναπτύσσουν τις δεξιότητές τους και ενισχύουν τις δυνατότητες της καριέρας τους, καθώς συνεργάζονται στενά με επαγγελματίες του κυβερνοχώρου σε διάφορα έργα. Ακόμη, οι φοιτητές αποκτούν μια ποικιλία από ισχυρές και πλούσιες εμπειρίες, όπως η έκθεση σε δραστηριότητες κυβερνοασφάλειας και η ακρόαση των υπευθύνων του προγράμματος που συζητούν σημαντικές πρωτοβουλίες της CISA και του DHS για την ασφαλή διατήρηση των συστημάτων. Μπορούν επίσης, να περιηγηθούν στα εργαστήριά της εταιρείας, να συμμετάσχουν σε ανεπίσημες συναντήσεις με ανώτερα στελέχη και να παρακολουθήσουν τοπικά συνέδρια και φόρουμ για να ακούσουν από εμπειρογνώμονες και ειδησεογράφους άλλων εκτελεστικών οργανισμών, του Κογκρέσου, της βιομηχανίας και της ακαδημαϊκής κοινότητας τη σημασία της κυβερνοασφάλειας για την προστασία από τις διάφορες απειλές [49].

4.2.3 Η Παιχνιδοποίηση της εκπαίδευσης (Gamification)

Οι υποδομές ζωτικής σημασίας έχουν γίνει επίκεντρο των κυβερνοεπιθέσεων, λόγω της αυξημένης συνδεσιμότητας με δίκτυα πληροφορικής. Επιπλέον, η ανεπαρκής προσφορά εργασίας στον κυβερνοχώρο επιδεινώνει τις προκλήσεις για τους οργανισμούς να υπερασπιστούν τα συστήματά τους. Η μάθηση με βάση τα παιχνίδια κερδίζει έδαφος και μελέτες έχουν δείξει ότι είναι ένα αποτελεσματικό εκπαιδευτικό στοιχείο. Η παιχνιδοποίηση στην κυβερνοασφάλεια είναι μια στρατηγική που δίνει κίνητρα στους ανθρώπους να επιλύουν προκλήσεις που σχετίζονται με την ασφάλεια μέσω διαγωνισμών και ανταμοιβών για τη βελτίωση της πρακτικής, τεχνικής τους εμπειρίας και των δεξιοτήτων τους. Η παιχνιδοποίηση του hacking χρησιμοποιεί τη θεωρία παιγνίων και τη μηχανική των παιγνίων όχι απλώς για διασκέδαση, αλλά και για την κατανόηση και τη βελτίωση της λήψης αποφάσεων στον τομέα της κυβερνοασφάλειας.

Η παιχνιδοποίηση των μαθησιακών πόρων είναι μια μέθοδος που δεν είναι πλήρως κατανοητή. Σύμφωνα με μελέτες που έγιναν, αξιολογήθηκε η επίδραση της παιχνιδοποίησης στην εκπαίδευση και στις περισσότερες περιπτώσεις διαπιστώθηκε ότι οι συμμετέχοντες θεώρησαν ότι είναι πιο αποτελεσματική και διασκεδαστική. Σε αυτές τις μελέτες, χρησιμοποιήθηκαν διάφορα στοιχεία παιχνιδοποίησης για την επίτευξη μαθησιακών στόχων. Η προσομοίωση, ο ανταγωνισμός και οι γρίφοι είχαν ως αποτέλεσμα μια θετική ανατροφοδότηση από τους συμμετέχοντες. Ένα χαρακτηριστικό που μοιράζονται όλα αυτά τα στοιχεία είναι ότι καθιστούν την παιχνιδοποίηση ιδιαίτερα διαδραστική. Επιπλέον, τα στοιχεία αυτά μπορούν να παρακινήσουν τους συμμετέχοντες επειδή ενισχύουν το ενδιαφέρον τους.



Σχήμα 14. Πως λειτουργεί η Παιχνιδοποίηση [54]

Η έννοια της παιχνιδοποίησης στις επιχειρήσεις δεν είναι καινούργια. Πολλές εταιρείες τη χρησιμοποιούν για την εισαγωγή νέων υπαλλήλων, τη διαχείριση της απόδοσης και τα προγράμματα πιστότητας πελατών. Το ποσοστό διατήρησης της γνώσης των εργαζομένων με παραδοσιακές μεθόδους μάθησης είναι μόνο περίπου 5%. Αλλά με τη βιωματική μάθηση, η διατήρηση μπορεί να φτάσει το 90%. Μέσω πρακτικών μορφών μάθησης, όπως η παιχνιδοποίηση, οι συμμετέχοντες είναι πιο πιθανό να θυμούνται τις δεξιότητες και να μπορούν να τις χρησιμοποιήσουν. Το *hacking gamification* βάζει τους εργαζόμενους σε πραγματικά σενάρια και τους κάνει να σκέφτονται υπό πίεση. Βασίζεται στην κριτική σκέψη και τη συνεργασία για την επίτευξη βέλτιστων αποτελεσμάτων. Ορισμένοι οργανισμοί προσφέρουν ακόμη και κίνητρα, όπως ανταμοιβές για επιτεύγματα εντός του παιχνιδιού, ενθαρρύνοντας τους εργαζόμενους να συμμετέχουν. Το να έχει διαβάσει κάποιος για την ασφάλεια στον κυβερνοχώρο ή ακόμη και να έχει περάσει τις εξετάσεις στο πανεπιστήμιο του, δεν τον κάνει απαραίτητα εμπειρογνώμονα στη μάχη εναντίον ενός εγκληματία στον κυβερνοχώρο. Η καλύτερη άμυνα είναι να γνωρίζει τον εχθρό και όχι μόνο να ξέρει τι είναι πιθανό να σκέφτεται ένας επιτιθέμενος, αλλά και τις προτιμώμενες τεχνικές του. Η παιχνιδοποίηση διδάσκει στους ανθρώπους να μαθαίνουν πώς σκέφτονται και ενεργούν οι εγκληματίες του κυβερνοχώρου, ώστε να μπορούν να εφαρμόζουν νέες στρατηγικές για την καταπολέμησή τους. Αυτό είναι πολύ σημαντικό επειδή οι *hacker* συχνά σκέφτονται έξω από το κουτί για να διεισδύσουν σε δίκτυα και να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Σκεπτόμενοι σαν *hacker*, μπορούμε ενδεχομένως να προβλέψουμε τις κινήσεις ενός δράστη και να λάβουμε προληπτικά μέτρα για να ανατρέψουμε τα σχέδιά τους.

Πιο συγκεκριμένα κάποια από τα οφέλη της παιχνιδοποίησης της εκπαίδευσης της κυβερνοασφάλειας είναι:

- Η παιχνιδοποίηση δίνει στους ανθρώπους μια πλατφόρμα για να παρουσιάσουν τις δεξιότητές τους στον τομέα της κυβερνοασφάλειας και να γίνουν αντιληπτοί από μια κοινότητα επαγγελματιών. Πολλές πλατφόρμες παιχνιδοποίησης διαθέτουν πίνακα κατάταξης για να δείχνουν ποιος έχει κερδίσει τους περισσότερους πόντους με βάση την πρόοδο στις προκλήσεις. Πολλές εταιρείες δημιουργούν πλέον προκλήσεις για να ανακαλύψουν τα καλύτερα talέντα. Αυτό μπορεί να οδηγήσει σε νέες ευκαιρίες καριέρας για τους επαγγελματίες της κυβερνοασφάλειας, ενώ παράλληλα βοηθά τις εταιρείες να ανακαλύψουν κρυμμένα talέντα και να καλύψουν θέσεις εργασίας.
- Οι στρατηγικές και τα εργαλεία που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου αλλάζουν συνεχώς και οι επιθέσεις στον κυβερνοχώρο γίνονται όλο και πιο πολύπλοκες. Όταν ένας οργανισμός ανακαλύψει μια νέα ευπάθεια, μπορεί να χρησιμοποιήσει την παιχνιδοποίηση της κυβερνοασφάλειας για να μάθει για την ευπάθεια αυτή, τον τρόπο εκμετάλλευσής της και τι μπορεί να κάνει για να μειώσει τους κινδύνους κατά του οργανισμού.
- Η παιχνιδοποιημένη εκπαίδευση συμβάλλει στη διάσπαση των διαχωρισμών και αυξάνει την ομαδική εργασία μεταξύ διαφορετικών επιχειρηματικών μονάδων και ομάδων δεξιοτήτων. Αυτό, με τη σειρά του, φέρνει τις ομάδες πιο κοντά και αυξάνει τις ευκαιρίες μάθησης. Επιπλέον, είναι καλό να αναμειγνύονται άτομα με διαφορετικά επίπεδα γνώσεων και ικανοτήτων. Η παιχνιδοποίηση επαναφέρει τη διασκέδαση στην

κυβερνοασφάλεια και δίνει τη δυνατότητα στις ομάδες να συνεργάζονται, να επιλύουν προκλήσεις και να μαθαίνουν νέες δεξιότητες η μία από την άλλη [50-51].

Το Network Defense Training Game (NDTG) είναι μια εκπαιδευτική πλατφόρμα κυβερνοασφάλειας που περιλαμβάνει μια σειρά από γεγονότα τα οποία ο παίκτης πρέπει να αξιολογήσει και να αντιδράει καθ' όλη τη διάρκεια του σεναρίου για να υπερασπιστεί το δίκτυο αποτρέποντας την επίθεση του αντιπάλου. Το NDTG χρησιμοποιεί αφηγήσεις σεναρίων που βασίζονται σε ιστορικά περιστατικά στον κυβερνοχώρο. Το NDTG χρησιμοποιεί καθένα από τα στοιχεία της παιχνιδοποίησης (δηλαδή προσομοίωση, ανταγωνισμό και γρίφους) για τη δημιουργία ενός αποτελεσματικού και διασκεδαστικού εργαλείου κατάρτισης κυβερνοασφάλειας που μπορεί να χρησιμοποιηθεί για την ανάπτυξη του εργατικού δυναμικού κυβερνοασφάλειας σε ομοσπονδιακές εγκαταστάσεις.

Βέβαια υπάρχουν πολλά πρόσθετα εργαλεία βασισμένα σε παιχνίδια που είναι διαθέσιμα για την εκπαίδευση στην κυβερνοασφάλεια τα οποία θα αναφέρουμε παρακάτω.

1. Το Cyber Threat Defender (CTD) είναι ένα ανταγωνιστικό επιτραπέζιο παιχνίδι καρτών που αναπτύχθηκε από το Center for Infrastructure Assurance and Security του Πανεπιστημίου του Τέξας στο Σαν Αντόνιο. Ο παίκτης χτίζει το δίκτυό του τοποθετώντας περιουσιακά στοιχεία και άμυνες μπροστά του και μπορεί επίσης να παίξει επίθεση για να νικήσει τον αντίπαλό του. Η τράπουλα καρτών που χρησιμοποιείται από κάθε παίκτη μπορεί να προσαρμοστεί ώστε να χρησιμοποιεί διαφορετικές στρατηγικές για να κερδίσει το παιχνίδι. Ενώ αυτό ξεκίνησε ως επιτραπέζιο παιχνίδι, έχει εικονικοποιηθεί.
2. Το CyberCIEGE είναι ένα εκπαιδευτικό εργαλείο βασισμένο σε παιχνίδι για τη διδασκαλία εννοιών κυβερνοασφάλειας πληροφορικής σε μαθητές. Πρόκειται για μια τρισδιάστατη προσομοίωση ενός χώρου γραφείου, στον οποίο ο χρήστης διαχειρίζεται μια πολιτική ασφαλείας. Ένα βασικό συστατικό της μηχανικής του CyberCIEGE είναι ότι, στο πλαίσιο της προσομοίωσης, ο παίκτης αλληλοεπιδρά με τους εικονικούς υπαλλήλους για να κατανοήσει τις απαιτήσεις τους κατά την εφαρμογή των πολιτικών ασφαλείας.
3. Στο παιχνίδι Cyber Exchange, ο παίκτης υπερασπίζεται το δίκτυο αγοράζοντας και αναπτύσσοντας εργαλεία. Καθώς συμβαίνουν κυβερνοεπιθέσεις, δίνεται μια αναφορά στον παίκτη η οποία του υποδεικνύει τι έχουν κάνει οι επιτιθέμενοι και του παρέχει ανατροφοδότηση σχετικά με τις εφαρμοστέες άμυνες και τον μετριασμό των απειλών.
4. Δίκτυο υπολογιστών CyberNEXS Defense Centralized είναι μια προσομοίωση με στόχο την υπεράσπιση του προσομοιωμένου δικτύου έναντι μιας επίθεσης στον κυβερνοχώρο, με πρωταρχικό στόχο τη διατήρηση της διαθεσιμότητας των κρίσιμων υπηρεσιών. Ο παίκτης πρέπει να εντοπίζει τις απειλές για το δίκτυο, να εφαρμόσει μέτρα μετριασμού και να επικοινωνήσει και να τα κοινοποιήσει στον διαχειριστή του δικτύου [51].

4.2.4 Cybercompetitions

Καθώς οι διαγωνισμοί στον κυβερνοχώρο έχουν αυξηθεί την τελευταία δεκαετία, το περιεχόμενο που καλύπτεται σε κάθε διαγωνισμό έχει επεκταθεί. Η χρήση των διαγωνισμών αποτελεί μία μέθοδο για τη βελτίωση των μαθησιακών αποτελεσμάτων και την παροχή μιας νέας πνοής στην εκπαίδευση. Οι διαγωνισμοί υπόσχονται να διδάξουν τους συμμετέχοντες πώς να εργάζονται ως ομάδα σε μια έντονη ατμόσφαιρα και υπό πίεση. Υπάρχουν πολλοί διαφορετικοί τύποι διαγωνισμών στον κυβερνοχώρο που φιλοξενούνται κάθε χρόνο. Νέοι τύποι διαγωνισμών αναπτύσσονται συνεχώς, ορισμένοι από τους οποίους έχουν σημειώσει μεγάλη επιτυχία και γίνονται επαναλαμβανόμενες εκδηλώσεις (όπως το CPTC5 του Ινστιτούτου Τεχνολογίας του Rochester). Έχουν επίσης υπάρξει πανεπιστήμια που αντικατέστησαν εξ ολοκλήρου ένα παραδοσιακό μάθημα με μάθηση βασισμένη σε διαγωνισμούς, για τα εκπαιδευτικά οφέλη και τα βελτιωμένα μαθησιακά αποτελέσματα που αυτή παρέχει. Οι διαγωνισμοί που επικεντρώνονται στην κυβερνοασφάλεια έχουν λάβει ευρεία δημοσιότητα, με το CTFTIME, το 2018 και το 2019 να διαφημίζει πολύ περισσότερους από 100 διαγωνισμούς ανά έτος στην πλατφόρμα του (CTFTIME, 2020). Οι διαγωνισμοί κυβερνοασφάλειας έχουν καταγραφεί και μελετήθηκαν στην ακαδημαϊκή έρευνα την τελευταία δεκαετία, με πολυάριθμες δημοσιεύσεις σχετικά με την επανεξέταση των μαθησιακών αποτελεσμάτων και την έρευνα των συμμετεχόντων. Γενικά, οι διαγωνισμοί στον κυβερνοχώρο παρέχουν στους συμμετέχοντες ανάπτυξη δεξιοτήτων σε εργαλεία, συστήματα και τεχνολογίες.

Ο πίνακας 1 παρακάτω καταγράφει κάποια είδη διαγωνισμών για την ασφάλεια στον κυβερνοχώρο και περιγράφει τα μαθησιακά αποτελέσματα καθώς και τα αναμενόμενα οφέλη κάθε διαγωνισμού [52].

Τύπος Διαγωνισμού	Γνωστικά αποτελέσματα
Penetration Testing	• Ικανότητα χρήσης εργαλείων δοκιμών διείσδυσης που συναντάμε συνήθως σε Kali και Linux. • Απόκτηση εμπειρίας στη συγγραφή μιας ολοκληρωμένης δοκιμής διείσδυσης • Ανάπτυξη ικανότητας επικοινωνίας και συνεργασίας εταιρείες και τα μέλη τους.
Forensics	• Εμπειρία στη χρήση δημοφιλών εγκληματολογικών εργαλείων όπως Autopsy, FTK Imager, Volatility και SANS SIFT. • Γνώση αξιολόγησης του κόστους της επίθεσης και του χρόνου διακοπής λειτουργίας ενός οργανισμού καθώς και δημιουργία σχεδίων αποκατάστασης.

	• Εμπειρία διαχείρισης αρχείων καταγραφής (log files).
Capture the Flag (CTF)	• Κάθε τύπος προβλήματος CTF απαιτεί οι συμμετέχοντες να χρησιμοποιήσουν ένα διαφορετικό σύνολο δεξιοτήτων, διδάσκοντάς τους έτσι μια μεγάλη ποικιλία εννοιών κυβερνοασφάλειας. • Μαθαίνουν βασικές γνώσεις πληροφορικής, όπως η χρήση της γραμμής εντολών και το περιβάλλον των Linux. • Διαθέτει ποικιλία προκλήσεων και διδάσκει από τα πιο βασικά προβλήματα έως τα πιο σύνθετα.
Cyber Defense	• Ικανότητα ανίχνευσης απειλών δικτύου με ανάλυση αρχείων καταγραφής. • Εμπειρία επαναδιαμόρφωσης υπηρεσιών, και αφαίρεση επίμονων απειλών συστήματος. • Εμπειρία συντήρησης μεγάλου δικτύου συστημάτων και τειχών προστασίας.

Πίνακας 1. Διαγωνισμοί που σχετίζονται με θέματα κυβερνοασφάλειας [52]

5

Σύνοψη και Συμπεράσματα

5.1 Σύνοψη

Βασικός στόχος της έρευνας αυτής ήταν να διερευνήσει τα θέματα ισότητας φύλων στον εργασιακό χώρο της κυβερνοασφάλειας. Η ανισότητα μεταξύ των φύλων στην επιστήμη της πληροφορικής και της κυβερνοασφάλειας αποτελεί ένα σύνθετο και διαχρονικό πρόβλημα στην σημερινή εποχή. Οι καταγραφές του παρελθόντος και η σημερινή κατάσταση δείχνουν ότι μια μειοψηφία γυναικών ασχολείται με την κυβερνοασφάλεια, καθώς υπάρχουν πολλά εμπόδια στην πρόοδό τους στον τομέα αυτό.

Η ενασχόληση με την ασφάλεια στον κυβερνοχώρο εξαρτάται από το ενδιαφέρον του ατόμου για την επιστήμη, την τεχνολογία, τη μηχανική και τα μαθηματικά (STEM). Τα στερεότυπα καριέρας και οι λανθασμένες αντιλήψεις σχετικά με τη φύση της επιστήμης της πληροφορικής είναι κάποιοι από τους βασικούς λόγους για την υπό-εκπροσώπηση των γυναικών σε επαγγέλματα στον τομέα αυτόν. Ενώ οι γυναίκες αρχικά κυριαρχούσαν στην επιστήμη των υπολογιστών, αργότερα το ποσοστό τους άρχισε να μειώνεται λόγω της σύνδεσης των υπολογιστών με τους άνδρες. Καθώς η τεχνολογία στις μέρες μας συνεχώς εξελίσσεται, η ασφάλεια των συστημάτων και των δεδομένων και η προστασία τους από επιθέσεις αποτελεί ένα μεγάλο ζήτημα. Στον εργασιακό χώρο της κυβερνοασφάλειας, οι γυναίκες έρχονται αντιμέτωπες με διακρίσεις και πρέπει να προσπαθούν καθημερινά για να αποδείξουν τις ικανότητές τους, κάτι που δεν συμβαίνει αντίστοιχα με τους άνδρες συναδέλφους τους. Στην έρευνα που κάναμε διαπιστώσαμε επίσης πως δεν είναι εξίσου εύκολο με τους άνδρες οι γυναίκες να πάρουν μια προαγωγή σε υψηλότερη θέση στον χώρο της κυβερνοασφάλειας επειδή οι εργοδότες θεωρούν πως αυτές θα παραμελήσουν την δουλειά τους για να δημιουργήσουν οικογένεια. Ο κοινωνικός φραγμός αναφέρεται στις γυναίκες που μπορεί να είναι κοινωνικά απομονωμένες ή αποκομμένες από την τομέα της πληροφορικής, σε αντίθεση με τους άνδρες που θεωρούνται εμπειρογνώμονες, καθώς είναι πιο εξοικειωμένοι με τον τομέα των υπολογιστών. Επιπλέον, ο τομέας της ασφάλειας στον κυβερνοχώρο θα μπορούσε να απαιτεί ξενύχτια σε εργαστήρια υπολογιστών ή ακόμα και εργασία κατά τη διάρκεια του Σαββατοκύριακου. Το γεγονός αυτό μπορεί να μην είναι αποδεκτό για τις γυναίκες σε πολλές πατριαρχικές κουλτούρες, καθώς μια τέτοια εργασία θα μπορούσε να επηρεάσει την ασφάλειά τους, τη φήμη τους και τον χρόνο που αφιερώνουν σε οικογενειακά θέματα [55]. Εκτός από αυτή

την προκατάληψη οι γυναίκες αντιμετωπίζουν και άλλες υποσυνείδητες προκαταλήψεις οι οποίες συνεχίζουν να τις βασανίζουν ακόμη και αν καταφέρουν να πάρουν την δουλειά. Αντιλαμβανόμαστε λοιπόν, πως οι απόψεις ενός μεγάλου ποσοστού γυναικών δεν εκτιμώνται εύκολα στον εργασιακό χώρο της κυβερνοασφάλειας.

Σε συνέχεια της έρευνάς μας, αναζητήσαμε τις δεξιότητες που είναι απαραίτητες να έχει κάποιος ανεξαρτήτως φύλου στον τομέα της κυβερνοασφάλειας. Πολλοί σύγχρονοι οργανισμοί αντιμετωπίζουν έλλειψη εξειδικευμένου προσωπικού για την υποστήριξη των απαιτούμενων ρόλων. Η μαθητεία, τα ακαδημαϊκά πτυχία και οι επαγγελματικές πιστοποιήσεις προσφέρουν δομημένες διαδρομές ανάπτυξης ικανοτήτων και τα πτυχία υποδηλώνουν πως ένα συγκεκριμένο επίπεδο γνώσεων έχει επιτευχθεί. Παρόλα αυτά, μέσα από την έρευνα της εργασίας αυτής διαπιστώνουμε πως η ασφάλεια στον κυβερνοχώρο απαιτεί έναν συνδυασμό τεχνικών και μη τεχνικών δεξιοτήτων, συμπεριλαμβανομένων της κοινωνικής νοημοσύνης της συνεργασίας, της επικοινωνίας και της κριτικής σκέψης. Η ποικιλομορφία των φύλων στον τομέα της κυβερνοασφάλειας είναι αναγκαία και η ενθάρρυνση της ισότητας των φύλων μπορεί να οδηγήσει σε καλύτερα προετοιμασμένο εργατικό δυναμικό. Οι γυναίκες διαθέτουν και αυτές σημαντικές δεξιότητες για τον χώρο παρά τις προκαταλήψεις που δεν τις συνδέουν με την κυβερνοασφάλεια. Για αυτόν τον λόγο οι εργοδότες και οι εταιρείες πρέπει να αξιολογούν τις πραγματικές ικανότητες και τα προσόντα των επαγγελματιών ανεξαρτήτως φύλου, ώστε να είναι έτοιμοι απέναντι στις προκλήσεις που θα χρειαστεί να αντιμετωπίσουν.

Προχωρώντας, αναζητήσαμε τις προκλήσεις που αντιμετωπίζουν τα φύλα σχετικά με την εκπαίδευσή τους στον τομέα της κυβερνοασφάλειας. Είναι λοιπόν γεγονός πως δεν έχουν όλοι τις ίδιες ευκαιρίες στην εκπαίδευση. Καταγράψαμε συγκεκριμένα τρεις παράγοντες που επηρεάζουν την σταδιοδρομία των φύλων σε επιστήμες STEM και πιο συγκεκριμένα στην ασφάλεια στον κυβερνοχώρο. Αρχικά, τα κοινωνικά στερεότυπα αποθαρρύνουν τις γυναίκες να ασχοληθούν με την πληροφορική και πλήττουν την αυτοπεποίθησή τους, η οικογένεια συνήθως υποστηρίζει περισσότερο τα αγόρια και τα προωθεί στην τεχνολογία και τέλος στα σχολεία δεν υπάρχουν γυναικεία πρότυπα και κατάλληλη εκπαίδευση για κάποιον που θέλει να ασχοληθεί με την κυβερνοασφάλεια.

Στο τελευταίο κομμάτι της διπλωματικής, καταγράψαμε τους εκπαιδευτικούς τρόπους με τους οποίους μπορεί κάποιος να εξειδικευτεί στην κυβερνοασφάλεια. Τα πανεπιστημιακά πτυχία ανά τον κόσμο που εστιάζουν σε αυτές τις σπουδές δεν είναι πάρα πολλά. Παρόλα αυτά, πολλές είναι οι εταιρείες και οι οργανισμοί που δίνουν την ευκαιρία στους φοιτητές να κάνουν πρακτική άσκηση ταυτόχρονα με τις σπουδές και να έρθουν σε κοντινότερη επαφή με το αντικείμενο αυτό. Τέλος, τονίσαμε πως η πρακτική άσκηση, η παιχνιδιοποίηση της εκπαίδευσης και η συμμετοχή σε διαγωνισμούς κυβερνοασφάλειας είναι κάποιοι από τους τρόπους μέσω των οποίων οι μαθητές μπορούν να αναπτύξουν τις δεξιότητες τους στην κυβερνοασφάλεια σε ένα πολύ ικανοποιητικό επίπεδο.

5.2 Συμπεράσματα

Μέσα από την έρευνα που κάναμε, καταλήγουμε στο συμπέρασμα πως υπάρχει έλλειψη επαγγελματιών με τις απαραίτητες δεξιότητες για να μας προστατεύσουν από κυβερνοεπιθέσεις. Η κυβερνοασφάλεια έχει σημασία για όλους τους ανθρώπους. Από κυβερνήσεις, μεγάλες εταιρείες έως μικρές επιχειρήσεις, εργαζόμενους ακόμη και άτομα στο σπίτι. Ο αριθμός των κυβερνοεπιθέσεων αυξάνεται καθημερινά. Αυτό σημαίνει ότι είναι ακόμη πιο σημαντικό να διατηρούμε το λογισμικό μας ενημερωμένο, την υλικοτεχνική υποδομή προστατευμένη και τα δεδομένα ασφαλή.

Βρισκόμαστε σε έναν παγκόσμιο κυβερνοπόλεμο και οι επιτιθέμενοι γνωρίζουν ότι δεν είμαστε επαρκώς προετοιμασμένοι για να κερδίσουμε αυτόν τον πόλεμο. Αυτό συμβαίνει επειδή υπάρχει σοβαρή έλλειψη τεχνικού ταλέντου. Η καλύτερη επιλογή μας είναι να εκπαιδεύσουμε περισσότερα κορίτσια στον τομέα της τεχνολογίας και της κυβερνοασφάλειας. Η προώθηση αυτών των θέσεων εργασίας στις νέες γυναίκες δεν γίνεται σε μεγάλο βαθμό. Πρέπει να πληροφορήσουμε τη νεολαία και ιδιαίτερα τις γυναίκες, για το γεγονός ότι οι θέσεις εργασίας στην κυβερνοασφάλεια καλύπτουν ευρεία και διαφορετικά καθήκοντα. Σήμερα, η εργασία ως ειδικός στην κυβερνοασφάλεια είναι μια πολύ επιθυμητή δουλειά, ενώ στα μέσα ενημέρωσης εξακολουθεί να περιγράφεται ως περίπλοκη και περίεργη. Πρέπει να αλλάξουμε αυτήν την άποψη, καθώς τα αρνητικά στερεότυπα απομακρύνουν όλο και περισσότερο τις γυναίκες από το επάγγελμα αυτό. Είναι σημαντικό να διευκρινίσουμε γιατί υπάρχει ανάγκη αύξησης του αριθμού των γυναικών στην ασφάλεια στον κυβερνοχώρο. Η ύπαρξη περισσότερων γυναικών στον χώρο εργασίας έχει θετικό αποτέλεσμα στις επιχειρήσεις και την εθνική ασφάλεια. Χρειαζόμαστε ποικιλία. Η ποικιλομορφία της σκέψης παρέχει καινοτόμες λύσεις για προβλήματα κυβερνοασφάλειας. Επιπλέον, η ζήτηση επαγγελματιών ασφαλείας είναι τόσο υψηλή και η εμπλοκή περισσότερων γυναικών, οι οποίες φυσικά δεν υστερούν σε γνωστικό επίπεδο σε σχέση με τους άνδρες, θα είχε μεγάλο αντίκτυπο στην κάλυψη αυτών των κενών θέσεων.

Το χάσμα μεταξύ των δύο φύλων δεν είναι κάτι καινούργιο, ωστόσο η έρευνα δείχνει ότι η τάση αυτή συνεχίζεται στον τομέα της κυβερνοασφάλειας και εξακολουθούν να υπάρχουν προβλήματα ρατσιστικών αντιλήψεων. Οι γυναίκες συχνά δεν βλέπουν την τεχνολογία ή την κυβερνοασφάλεια ως καριέρα, επειδή θεωρούνται “ανδρικά” επαγγέλματα.. Παρόλα αυτά, οι συνθήκες αυτές φαίνεται πως σιγά σιγά μπορούν να αλλάξουν και οι μειονότητες και οι γυναίκες θα μπορέσουν να κάνουν σταθερή και καινοτόμο πρόοδο προς το επάγγελμα της ασφάλειας στον κυβερνοχώρο, συμβάλλοντας σε μεγαλύτερο ρόλο στην παγκόσμια οικονομία σε σύγκριση με την παλαιότερα. Οι επιχειρήσεις κυβερνοασφάλειας αντικατοπτρίζουν το ήθος της προστασίας και της υπεράσπισης των παγκόσμιων οργανισμών από τις απειλές στον κυβερνοχώρο, τους δράστες, τους hacker και την προστασία των θυμάτων των εγκλημάτων στον κυβερνοχώρο. Σε εθνική και παγκόσμια κλίμακα, η καταπολέμηση του εγκλήματος στον κυβερνοχώρο, των κυβερνοεπιθέσεων και των κυβερνοαπειλών πρέπει να είναι μια ολοκληρωμένη κοινοτική ευθύνη που απαιτεί συντονισμένη δράση, συμμετοχή και συμβολή όλων των πολιτών (ανδρών, μειονοτήτων και γυναικών).

Τα προβλήματα διάκρισης φύλων, είναι δύσκολο να επιλυθούν επειδή είναι πολύπλοκα από την ίδια τους την φύση, αφορούν ζητήματα πολιτισμού και εκπαίδευσης. Δεν υπάρχει μια απλή απάντηση για την επίλυση της έλλειψης εργατικού δυναμικού στον κυβερνοχώρο, αλλά ένα βήμα

προς τη σωστή κατεύθυνση είναι σίγουρα να εκπαιδεύσουμε και να προσελκύσουμε τα κορίτσια στην ανακάλυψη αυτού του τομέα. Τα εμπόδια έλλειψης επαγγελματιών μπορούν να ξεπεραστούν όταν οι μειονότητες και οι γυναίκες υποστηρίζονται, προωθούνται σε ανώτερα επίπεδα διοικητικών θέσεων, εκπαιδεύονται με ικανότητα να καθοδηγούν τη νέα γενιά και να διευκολύνουν τη σημαντική εισροή μειονοτήτων και γυναικών. Απαιτείται εκπαίδευση σε όλους τους τομείς σχετικά με την ποικιλομορφία, τις δεξιότητες και την τεχνογνωσία για τον μετριασμό των προβλημάτων της κυβερνοασφάλειας. Ο δρόμος για την άμβλυνση της παραβίασης των δικαιωμάτων κατά των εξειδικευμένων υποψήφιων για την ασφάλεια στον κυβερνοχώρο πρέπει να απέχει από την ανισότητα των φύλων [59].

5.3 Προτάσεις για αύξηση των γυναικών στον τομέα της πληροφορικής και της κυβερνοασφάλειας

Όπως αναφέρθηκε στα προηγούμενα κεφάλαια, το ποσοστό των γυναικών σε θέσεις εργασίας στον τομέα της ασφάλειας στον κυβερνοχώρο παγκοσμίως είναι αρκετά μικρό. Η αντιμετώπιση αυτού του ζητήματος θα συμβάλει στην αντιμετώπιση της παγκόσμιας έλλειψης δεξιοτήτων στον τομέα. Αυτό είναι σημαντικό για τον κλάδο και για την κοινωνία, προκειμένου να αντιμετωπιστεί η αυξανόμενη απειλή που συνιστά το έγκλημα στον κυβερνοχώρο. Πρέπει να κατανοήσουμε πως είναι θέμα κοινωνικής δικαιοσύνης να υπάρχει ισότητα ευκαιριών όσον αφορά την πρόσβαση και την εξέλιξη σε ένα καλά αμειβόμενο και πνευματικά διεγερτικό εργασιακό περιβάλλον. Πολλές γυναίκες στον τομέα αυτό αισθάνονται παρείσακτες, αλλά αυτό ελπίζουμε ότι θα αλλάξει στο προσεχές μέλλον, καθώς οι γυναίκες αποκτούν την απαραίτητη εκπαίδευση, ανταγωνίζονται τους άνδρες για την απόκτηση ηγετικών θέσεων και εφαρμόζουν στρατηγικές κυβερνοασφάλειας μέσω των καθηκόντων τους [36][56].

Προκειμένου να ενθαρρυνθεί η συμμετοχή των γυναικών στον κυβερνοχώρο, υπάρχει ανάγκη για αύξηση των γυναικείων προτύπων που θα ενθαρρύνουν την ενασχόληση με την πληροφορική, μειώνοντας την πιθανότητα ανάπτυξης ταυτότητας απομακρυσμένη από τις επιστήμες STEM. Τα πρότυπα είναι πολύ σημαντικά. Οι γυναίκες πρέπει να βλέπουν τον εαυτό τους σε αυτόν τον τομέα καθώς αν δεν έχουν εικόνες από κάποιον που τους μοιάζει τότε αρχίζουν να σκέφτονται ότι δεν ανήκω σε αυτό το επάγγελμα. Επίσης τα μέσα μαζικής ενημέρωσης θα μπορούσαν να παρουσιάζουν περισσότερες εικόνες γυναικών που ασχολούνται με την πληροφορική και συγκεκριμένα την κυβερνοασφάλεια, πιο συχνά. Τα πρότυπα μπορούν να προβάλουν σε όσους θέλουν να ασχοληθούν με τον τομέα αυτόν τι μπορούν να επιτύχουν. Τα γυναικεία πρότυπα μπορούν να βοηθήσουν άλλες γυναίκες να μην αισθάνονται ότι είναι “οι μόνες στο δωμάτιο” και μπορούν να προσελκύσουν γυναίκες να ξεκινήσουν την σταδιοδρομία τους στην κυβερνοασφάλεια [7]

Λαμβάνοντας υπόψη τη σημασία της οικογενειακής υποστήριξης για την είσοδο στον κλάδο για τα κορίτσια και τις γυναίκες και το πρώιμο στάδιο στο οποίο τα κορίτσια διαμορφώνουν γνωστικά τους ενδιαφέροντα, πιθανές μελλοντικές λύσεις μπορεί να είναι η εκπαίδευση των γονέων και των οικογενειών σχετικά με τις ευκαιρίες που μπορεί να προσφέρει η πληροφορική και η ασφάλεια στον κυβερνοχώρο στις κόρες τους, όσον αφορά τη συναρπαστική, ενδιαφέρουσα,

δημιουργική και ποικίλη φύση της εργασίας. Για να διασφαλιστεί η παρουσία των γυναικών που συμμετέχουν στην κυβερνοασφάλεια, είναι ανάγκη να ενθαρρυνθούν τα κορίτσια και οι νεαρές γυναίκες στο σχολείο, στην περαιτέρω εκπαίδευση και στην τριτοβάθμια εκπαίδευση, να σπουδάσουν στους κλάδους της πληροφορικής και να τους δοθεί περαιτέρω η ευκαιρία να επικεντρωθούν στις ευκαιρίες της κυβερνοασφάλειας. Είναι επίσης σαφές πως πρέπει να τονιστούν οι ευκαιρίες εξέλιξης και οι αμοιβές στον τομέα αυτόν, προκειμένου να αυξηθεί η πιθανότητα να εισέλθουν γυναίκες στον κλάδο και να επιλέξουν να παραμείνουν σε αυτόν. Οι περισσότεροι άνθρωποι δεν γνωρίζουν αρκετά για την ασφάλεια στον κυβερνοχώρο. Ο μέσος πολίτης δεν καταλαβαίνει τι σημαίνει κυβερνοασφάλεια και νομίζει ότι είναι κάτι που δεν τον αφορά. Η ασφάλεια στον κυβερνοχώρο δεν έχει πάντα να κάνει μόνο με τις τεχνικές πτυχές, παρόλο που αυτές είναι σημαντικές για την κατανόηση της τεχνολογίας εξαρχής. Υπάρχουν τόσοι πολλοί διαφορετικοί τρόποι για να προχωρήσεις στην κυβερνοασφάλεια χωρίς αυτό να σημαίνει ότι πρέπει να γίνεις πληροφορικός, επιστήμονας πληροφορικής. Το επάγγελμα αυτό περιλαμβάνει την τεχνολογία, την πολιτική και το δίκαιο. Είναι λοιπόν πολύ σημαντικό να υπάρξει πλήρης ενημέρωση σχετικά με τον τομέα της ασφάλειας στον κυβερνοχώρο για να μπορέσει ο τομέας αυτός να προσελκύσει και άλλο κόσμο και πόσο μάλλον γυναίκες [7].

Για να δημιουργήσουν ισχυρές, επαρκώς στελεχωμένες ομάδες κυβερνοασφάλειας, οι εργοδότες και το επάγγελμα της κυβερνοασφάλειας στο σύνολό του, πρέπει να καταστήσουν την κυβερνοασφάλεια μία φιλόξενη καριέρα για όλους. Οι γυναίκες δεν θα πρέπει να μπαίνουν στο δίλημμα να αποφασίσουν αν μπορούν ή όχι να κάνουν οικογένεια και να εργαστούν σε αυτόν τον τομέα. Θα πρέπει να μπορούν να έχουν οικογένεια και ένα σεβαστό ωράριο εργασίας. Η κατανόηση των προκλήσεων που αντιμετωπίζει το επάγγελμά είναι ένα κρίσιμο πρώτο βήμα για την επίτευξη αυτού του στόχου και τελικά την αντιμετώπιση του διευρυμένου χάσματος εργατικού δυναμικού στον κυβερνοχώρο [7][36].

Τα αίτια της ανισότητας των φύλων στην ασφάλεια στον κυβερνοχώρο είναι πολύπλοκα. Οι ρίζες της ανισότητας εντοπίζονται στις κοινωνικές δομές του φύλου, στην ευρύτερη κοινωνία, στις οικογένειες, στην εκπαίδευση και στις βιομηχανίες ΤΠΕ, ασφάλειας και κυβερνοασφάλειας. Οποιαδήποτε προσπάθεια μείωσης του χάσματος μεταξύ των δύο φύλων θα πάρει χρόνο και θα πρέπει να εξετάσει το πρόβλημα από όλες αυτές τις πλευρές προκειμένου να δώσει λύση. Είναι καιρός να αμφισβητηθεί η αντίληψη ότι η ασφάλεια στον κυβερνοχώρο είναι μόνο «για αγόρια», ώστε ο κλάδος να μπορέσει να καλύψει την έλλειψη δεξιοτήτων, τα κορίτσια να έχουν πρόσβαση σε μια συναρπαστική και ενδιαφέρουσα σταδιοδρομία και η κοινωνία να είναι καλύτερα εξοπλισμένη για να αντιμετωπίσει την αυξανόμενη απειλή που συνιστά το έγκλημα στον κυβερνοχώρο [36].

5.4 Προτάσεις για ενίσχυση της εκπαίδευσης στην κυβερνοασφάλεια

Παρόλα τα διπλώματα κυβερνοασφάλειας, πολλοί οργανισμοί εξακολουθούν να διαπιστώνουν ότι οι φοιτητές που προέρχονται από προγράμματα κυβερνοασφάλειας δεν έχουν πρακτική εμπειρία. Σύμφωνα με την επαγγελματική ένωση ISACA, η εκπαίδευσή τους τις περισσότερες φορές βασίζεται και αυτή στη θεωρία. Ως αποτέλεσμα, η ίδια η αξία ενός πτυχίου κυβερνοασφάλειας έχει αρχίσει να μειώνεται στα μάτια των εργοδοτών, με έρευνες που δείχνουν

ότι το 80 τοις εκατό των διευθυντών δεν πιστεύουν πλέον ότι ένα πτυχίο τετραετούς κύκλου σπουδών προετοιμάζει επαρκώς τους φοιτητές για τις θέσεις εργασίας στον κυβερνοχώρο.

Μια στρατηγική με γνώμονα την κορυφή είναι σημαντική για την επιτυχία στην εκπαίδευση στον τομέα της κυβερνοασφάλειας. Ο γενικός στόχος είναι η αύξηση της ποιότητας και της ποσότητας των ταλέντων της κυβερνοασφάλειας, να συμβάλει στη δημιουργία μίας μεγάλης γκάμας επαγγελματιών για τη μείωση του χάσματος δεξιοτήτων και της ανεπάρκειας εξειδικευμένου προσωπικού. Ακόμη, είναι σημαντικό η εκπαίδευση να προσφέρει στους σπουδαστές μια πορεία σταδιοδρομίας που είναι τόσο ικανοποιητική όσο και μοναδική. Η διεπιστημονική εκπαίδευση για την ασφάλεια στον κυβερνοχώρο είναι απαραίτητη. Δεν πρόκειται μόνο για την επιστήμη των υπολογιστών και τη μηχανική. Τα πανεπιστήμια πρέπει να εργαστούν και να φέρουν σε επαφή πολλαπλά προγράμματα όπως η εγκληματολογία, η στατιστική, η ηθική, η υγειονομική περίθαλψη, η πληροφορική, τα οικονομικά και η ανάλυση κινδύνου για να αναπτύξουν πραγματικά μια ολοκληρωμένη προσέγγιση της σκέψης για την ασφάλεια. Τα εκπαιδευτικά ιδρύματα θα πρέπει να λαμβάνουν μέτρα για τον εντοπισμό κοντινών βιομηχανιών και οργανισμών που είναι πρόθυμοι να προσλάβουν ταλέντα στον τομέα της κυβερνοασφάλειας. Είναι σημαντικό να λαμβάνονται υπόψη οι ανάγκες της βιομηχανίας πριν από την έναρξη συγκεκριμένων προγραμμάτων. Αυτό όχι μόνο θα βοηθούσε μια σχολή να επιτύχει γρήγορα στα προγράμματα κυβερνοασφάλειας, αλλά θα άνοιγε επίσης τις πόρτες σε άλλες ευκαιρίες, όπως η πρακτική άσκηση και οι σχέσεις μεταξύ ακαδημαϊκών και επαγγελματιών.

Απαραίτητο κρίνεται να προσδιοριστούν οι πόροι που απαιτούνται για την παροχή αυτών των προγραμμάτων σπουδών. Οι πόροι αυτοί μπορεί να περιλαμβάνουν εργαστήρια πληροφορικής, πρακτικά προγράμματα εκμάθησης της κυβερνοασφάλειας, λογισμικό και εξειδικευμένο διδακτικό προσωπικό για τη διδασκαλία μαθημάτων κυβερνοασφάλειας. Οι συνεργασία μεταξύ ακαδημαϊκών και επαγγελματιών θα πρέπει να διερευνηθεί επίσης ως ένας πόρος. Το περιβάλλον του εργαστηρίου θα πρέπει να προσφέρει ένα ρεαλιστικό και ευέλικτο περιβάλλον, κάτι που μπορεί να επιτευχθεί μέσω της χρήσης πραγματικού υλικού και λογισμικού. Ωστόσο, είναι πιο ευέλικτο να γίνεται εικονικοποίηση λογισμικού, που επιτρέπει στους καθηγητές ή στους φοιτητές να διαμορφώνουν πιο εύκολα εικονικά δίκτυα ή εικονικές μηχανές (VMs) για να καλύπτουν τις ανάγκες τους. Επιπλέον, η παροχή απομακρυσμένης πρόσβασης στους φοιτητές μπορεί να βελτιώσει σημαντικά την προσβασιμότητα και να αυξήσει τον χρόνο που οι φοιτητές αφιερώνουν στην πρακτική. Με την παροχή απομακρυσμένης πρόσβασης, τα εκπαιδευτικά ιδρύματα μπορούν να αξιοποιήσουν τις πλατφόρμες τους για την εξ αποστάσεως εκπαίδευση.

Οι οργανισμοί αναγνωρίζουν πλέον την κυβερνοασφάλεια ως μια κορυφαία επιχειρηματική λειτουργία. Για αυτόν τον λόγο, τα ιδρύματα τριτοβάθμιας εκπαίδευσης θα πρέπει να δώσουν στην εκπαίδευση στην κυβερνοασφάλεια την ίδια σημασία. Μια σχολή με μια κορυφαία προσέγγιση στην κυβερνοασφάλεια τόσο σε επίπεδο ευαισθητοποίησης όσο και σε επίπεδο ανάπτυξης εκπαιδευτικών προγραμμάτων είναι σε θέση να επιτύχει στην ανάπτυξη ενός επιτυχημένου προγράμματος ασφάλειας στον κυβερνοχώρο.

Τα σχολεία πρέπει να διασφαλίζουν ότι χρησιμοποιούν κάθε διαθέσιμο μέσο για να προσελκύσουν και να αναπτύξουν ταλέντα στον τομέα της κυβερνοασφάλειας. Τα μέσα αυτά θα μπορούσαν να περιλαμβάνουν οργανισμούς και επαγγελματίες της κυβερνοασφάλειας οι οποίοι θα παρέχουν πρακτική άσκηση, απασχόληση και συνεργασίες μεταξύ ακαδημαϊκών και

βιομηχανιών που θα ενισχύσουν την ανάπτυξη μιας ζωντανής κοινότητας κυβερνοασφάλειας. Άλλοι πόροι θα μπορούσαν περιλαμβάνουν πρόσβαση σε πληροφορίες σχετικά με επιχορηγήσεις, υποτροφίες και διαγωνισμούς που μπορούν να εμπλουτίσουν την κοινότητα της κυβερνοασφάλειας εντός ενός πανεπιστημίου ή κολλεγίου. Οι εκπαιδευτικοί μπορούν να οργανώσουν μικρά εργαστήρια σε συνεργασία με βιομηχανικούς συμμάχους. Με αυτόν τον τρόπο, μπορούν να φέρουν στα σχολεία τους πρόσθετα πρότυπα ρόλων από διαφορετικούς πληθυσμούς και να εμπνεύσουν τους μαθητές να επιχειρήσουν να ασχοληθούν με τον τομέα της κυβερνοασφάλειας. Με την ενσωμάτωση εκδηλώσεων καθοδήγησης στα εργαστήρια, τόσο οι μέντορες όσο και οι καθοδηγούμενοι επωφελούνται από την οργανωμένη δομή που παρέχεται [53].

5.5 Προτάσεις για μελλοντική έρευνα

Πολλοί τομείς του κυβερνοχώρου απαιτούν πρόσθετη έρευνα. Υπάρχει ιδιαίτερη απουσία δεδομένων σχετικά με τα εμπόδια και τις ευκαιρίες που βιώνουν στο επάγγελμα της ασφάλειας στον κυβερνοχώρο (και στην εκπαίδευση τεχνολογικών επιστήμων) τα μη δυαδικά και LGBTQ+ άτομα. Οι πολιτικές που στοχεύουν στον μετασχηματισμό των φυλετικών εμποδίων θα πρέπει να υποστηρίζονται. Οι μελλοντικές εργασίες θα πρέπει να επικεντρωθούν στη μέτρηση της προσέλευσης, της επιτυχίας και της διατήρησης των μειονοτήτων, κατά τη μετάβαση των φοιτητών στον τομέα της κυβερνοασφάλειας, στην εκπαίδευση στον τομέα του κυβερνοχώρου.

Ένα μελλοντικό έργο θα πρέπει να περιλαμβάνει μια έρευνα που θα επιτρέψει στα ιδρύματα τριτοβάθμιας εκπαίδευσης να αυτοαξιολογήσουν τις προσπάθειές τους στα προγράμματα κυβερνοασφάλειας. Η έρευνα αυτή θα μπορούσε να δώσει πρόσθετα στοιχεία σχετικά με πιθανές βελτιώσεις στην εκπαίδευση της ασφάλειας στον κυβερνοχώρο.

Υπάρχει η ανάγκη για περεταίρω διερεύνηση των αντιλήψεων των γονέων, των εκπαιδευτικών και των συμβούλων σταδιοδρομίας για τις ΤΠΕ και την κυβερνοασφάλεια, καθώς και του αντίκτυπου αυτών των αντιλήψεων αυτών στις επαγγελματικές φιλοδοξίες των νέων.

Τέλος, έρευνες δείχνουν πως η συχνότερη πρόσβαση των κοριτσιών στους υπολογιστές θα αυξήσει το ενδιαφέρον τους για την πληροφορική. Ωστόσο, άλλες μελέτες δείχνουν ότι δεν είναι μόνο η συχνότητα, αλλά και ο τρόπος με τον οποίο τα κορίτσια χρησιμοποιούν τον υπολογιστή. Οι μελλοντικές μελέτες θα πρέπει να περιλαμβάνουν μετρήσεις τόσο της συχνότητας όσο και του εύρους χρήσης των υπολογιστών από τα κορίτσια, ώστε να προσδιοριστεί η μοναδική συμβολή του καθενός από αυτούς τους παράγοντες.

Βιβλιογραφία

- [1] NPR, 21 Οκτωβρίου 2014, 'When Women Stopped Coding', Προσβάσιμο: <https://www.npr.org/sections/money/2014/10/21/357629765/when-women-stoppedcoding>, Ανακτήθηκε: 4 Νοεμβρίου 2019
- [2] Τσαγαλά, Ε., and Μ. Κορδάκη. "Γυναίκες και Καριέρα στην Πληροφορική: Ενθαρρυντικοί και Ανασταλτικοί Παράγοντες." Συνέδρια της Ελληνικής Επιστημονικής Ένωσης Τεχνολογιών Πληροφορίας & Επικοινωνιών στην Εκπαίδευση (2008): 395-404.
- [3] Women in Computer Science: Getting Involved in STEM, Computerscience.org, Προσβάσιμο: <https://www.computerscience.org/resources/women-in-computerscience/>, Ανακτήθηκε: 4 Νοεμβρίου 2019
- [4] Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining cybersecurity." Technology innovation management review 4.10 (2014).
- [5] Plato, Toni C. "Women C-Suite Executives In Cybersecurity: Transformational Experiences And Gender Barriers On Their Leadership Journeys." (2021).
- [6] <https://thegfce.org/initiative/gender-and-cybersecurity-creating-a-more-inclusive-digital-world/>
- [7] Zahout, Marie. "Women in Cybersecurity." McCloy Fellowship on Global Trends (2017).
- [8] Reed, Jason et al. (2017): The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Presented by The Center for Cyber Safety and Education™ and Executive Women's Forum on Information Security, Risk Management & Privacy. Santa Clara: A Frost & Sullivan White Paper
- [9] Asiry, Yasser. "Closing the Gap: Boosting Women's Representation in Cybersecurity Leadership." *Journal of Information Security* 15.01 (2024): 15-23.
- [10] Furnell, Steven. "The cybersecurity workforce and skills." *Computers & Security* 100 (2021): 102080.
- [11] Dawson, Jessica, and Robert Thomson. "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance." *Frontiers in psychology* 9 (2018): 744.
- [12] Ruoslahti, Harri. "Business continuity for critical infrastructure operators." *Annals of Disaster Risk Sciences: ADRS 3.1* (2020): 0-0.
- [13] Haney, Julie M., and Wayne G. Lutters. "Skills and Characteristics of Successful Cybersecurity Advocates." *SOUPS*. 2017.

- [14] Samarati, Pierangela, and Sabrina De Capitani di Vimercati. "Cloud security: Issues and concerns." *Encyclopedia of cloud computing* (2016): 205-219.
- [15] Onyema, Edeh Michael, et al. "Cloud security challenges: implication on education." *Int J Comput Sci Mob Comput* 9.2 (2020): 56-73.
- [16] Duncan, Bob, Andreas Happe, and Alfred Bratterud. "Cloud cyber security: finding an effective approach with unikernels." *Security in Computing and Communications* (2017): 31.
- [17]http://ebooks.edu.gr/ebooks/v/html/8547/2716/Pliroforiki_B-Lykeiou_html-empl/index3_1.html
- [18] Vander-Pallen, Maame Araba, et al. "Survey on types of cyber attacks on operating system vulnerabilities since 2018 onwards." *2022 IEEE World AI IoT Congress (AIIoT)*. IEEE, 2022.
- [19]<https://luminisindia.com/cybersecurity-prism/354-what-is-networksecurity-and-what-skills-do-i-need>
- [20] Lincke, Susan J., and Andrew Holland. "Network security: Focus on security, skills, and stability." *2007 37th Annual Frontiers In Education Conference-Global Engineering: Knowledge Without Borders, Opportunities Without Passports*. IEEE, 2007.
- [21] <https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-skills>
- [22] KARIM, SAMSUL ARIFFIN ABDUL. "Security in Internet of Things: A Review." (2017).
- [23]<https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-career-path>
- [24] Corallo, Angelo, et al. "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review." *Computers in Industry* 137 (2022): 103614.
- [25] Mughal, Arif Ali. "Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges." *Applied Research in Artificial Intelligence and Cloud Computing* 2.1 (2019): 1-31.
- [26] Sriram, V. P., et al. "Enhancing Cybersecurity Through Blockchain Technology." *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*. IGI Global, 2023. 208-224.
- [27] Kshetri, Nir. "Blockchain's roles in strengthening cybersecurity and protecting privacy." *Telecommunications policy* 41.10 (2017): 1027-1038.
- [28] Kaur, Randeep, and Jagroop Kaur. "Cloud computing security issues and its solution: A review." *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2015.
- [29] <https://www.appsealing.com/iot-security/>
- [30] <https://www.javatpoint.com/firewall>
- [31] <https://logicmojo.com/functions-of-operating-system>
- [32] Furnell, Steven, Pete Fischer, and Amanda Finch. "Can't get the staff? The growing need for cyber-security skills." *Computer Fraud & Security* 2017.2 (2017): 5-10.
- [33]<https://thegfce.org/initiative/gender-and-cybersecurity-creating-a-more-inclusive-digital-world/>

- [34] Pinchot, Jamie, et al. "Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap." *Information Systems Education Journal* 18.3 (2020): 44-53.
- [35] Denner, J. (2011) "What Predicts Middle School Girls' Interest in Computing?" *International Journal of Gender, Science and Technology*, 3(1): 53-69.
- [36] Peacock, Donna, and Alastair Irons. "Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression." *International Journal of Gender, Science and Technology* 9.1 (2017): 25-44.
- [37] Teague, J. (2000). Women in Computing: What brings them to it, what keeps them in it? *GATES*, 5(1), 45-49.
- [38] Gürer, D. and Camp, T. (2002). An ACM-W Literature Review on Women in Computing. *Women and Computing*, 34(2), 121-127.
- [39] Knapp, Kenneth J., Christopher Maurer, and Miloslava Plachkinova. "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance." *Journal of Information Systems Education* 28.2 (2017): 101.
- [40] Ahmad, Norita, et al. "A cybersecurity educated community." *IEEE Transactions on Emerging Topics in Computing* 10.3 (2021): 1456-1463.
- [41] Cabaj, Krzysztof, et al. "Cybersecurity education: Evolution of the discipline and analysis of master programs." *Computers & Security* 75 (2018): 24-35.
- [42] Abu-Taieh, Evon MO. "Cyber security body of knowledge." *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*. IEEE, 2017.
- [43] De Zan, Tommaso. "Mind the gap: the cyber security skills shortage and public policy interventions." (2019).
- [44] Bishop, Daniel, and Jim Hordern. "Degree apprenticeships: higher technical or technical higher (education)." *Bath, GBR: Bath Spa University, Institute for Education* (2017).
- [45] Jackson, Denise, and David Collings. "The influence of work-integrated learning and paid work during studies on graduate employment and underemployment." *Higher Education* 76.3 (2018): 403-425.
- [46] Crumpler, William, and James A. Lewis. *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS), 2022.
- [47] <https://www.pwc.com/gr/en/careers/Internship-Programmes.html>
- [48] <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/apprenticeship-finder>
- [49] <https://www.cisa.gov/careers/work-rolescyber-and-it-interns>
- [50] <https://delinea.com/blog/cybersecurity-gamification>
- [51] Ashley, Travis D., et al. "Gamification of cybersecurity for workforce development in critical infrastructure." *Ieee Access* 10 (2022): 112487-112501.
- [52] Balon, Tyler, and Ibrahim Baggili. "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education." *Education and Information Technologies* 28.9 (2023): 11759-11791.

- [53] Tsado, Lucy. "Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach." *Journal of Cybersecurity Education, Research and Practice* 2019.1 (2019): 4.
- [54] <https://educationaltechnology.net/gamification-what-it-is-how-it-works-examples/>
- [55] Al-Alawi, Adel Ismail, Noora Ahmed Al-Khaja, and Arpita Anshu Mehrotra. "Women in cybersecurity: A study of the digital banking sector in Bahrain." *Journal of International Women's Studies* 25.1 (2023): 21.
- [56] Esin, Joseph O. "A call for concern: the unbalanced representation of minorities and women in cybersecurity profession." *J Women Minor Technol* 2 (2020): 1-11.
- [57] Woszczynski, Amy B., and Sherri Shade. "A call to IS educators to respond to the voices of women in information security." *Journal of Information Systems Education* 21.2 (2010): 223.
- [58] <https://www.europarl.europa.eu/factsheets/el/sheet/59/equality-between-men-and-women>
- [59] https://www.researchgate.net/publication/346574399_Journal_for_Women_and_Minority_in_Technology