ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΠΛΗΡΟΦΟΡΙΚΗ»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Κυβερνοασφάλεια και Ψηφιακός Μετασχηματισμός: Συστηματική Ανασκόπηση** **Cybersecurity & Digital Transformation: A systematic review**
Ονοματεπώνυμο Φοιτητή	**ΨΑΡΡΑΚΗΣ ΣΤΑΥΡΟΣ-ΧΡΗΣΤΟΣ**
Πατρώνυμο	**ΙΩΑΝΝΗΣ**
Αριθμός Μητρώου	**ΜΠΠΛ19066**
Επιβλέπων	**ΠΑΤΣΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ, Αν. Καθηγητής**

Ημερομηνία Παράδοσης **Νοέμβριος 2023**

Τριμελής Εξεταστική Επιτροπή

Πατσάκης Κωνσταντίνος	Αλέπης Ευθύμιος	Σωτηρόπουλος Διονύσιος
Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής	Επίκουρος Καθηγητής

Ευχαριστίες

Στον Καθηγητή μου Κύριο Πατσάκη Κωνσταντίνο

Περίληψη

Αυτή η περιεκτική ανασκόπηση της υπάρχουσας βιβλιογραφίας εμβαθύνει στις προεκτάσεις του ψηφιακού μετασχηματισμού και της ασφάλειας στον κυβερνοχώρο για την επίτευξη επιχειρηματικής ανθεκτικότητας. Ο ψηφιακός μετασχηματισμός περιλαμβάνει τη μετατόπιση των οργανωτικών διαδικασιών προς λύσεις πληροφορικής, οι οποίες μπορούν να οδηγήσουν σε ουσιαστικές αλλαγές σε διάφορες πτυχές ενός οργανισμού. Ωστόσο, η παγκόσμια ώθηση για ψηφιακό μετασχηματισμό, με γνώμονα τις αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη, τα μεγάλα δεδομένα και τα αναλυτικά στοιχεία, το blockchain και το cloud computing, ενισχύει επίσης τους κινδύνους για την ασφάλεια στον κυβερνοχώρο για τις επιχειρήσεις που υφίστανται αυτόν τον μετασχηματισμό. Αυτό το άρθρο, που επικεντρώνεται στην έρευνα της υπάρχουσας βιβλιογραφίας, υπογραμμίζει την κρίσιμη σημασία της εκτενούς κατανόησης των απειλών για την ασφάλεια στον κυβερνοχώρο κατά την εφαρμογή του ψηφιακού μετασχηματισμού για την αποτροπή διαταραχών που προκαλούνται από κακόβουλες δραστηριότητες ή μη εξουσιοδοτημένη πρόσβαση από άτομα με σκοπό την παραποίηση ευαίσθητων πληροφοριών, που προκαλούν ζημιά ή αναζήτηση εκβιασμού από τους χρήστες. Η ασφάλεια στον κυβερνοχώρο διαδραματίζει ζωτικό ρόλο στη διαφύλαξη των ψηφιακών περιουσιακών στοιχείων από απειλές στον κυβερνοχώρο. Για τη διεξαγωγή αυτής της έρευνας, πραγματοποιήσαμε μια συστηματική ανασκόπηση της βιβλιογραφίας ακολουθώντας τη μεθοδολογία PRISMA. Η ανασκόπησή μας αποκάλυψε ότι ενώ ο ψηφιακός μετασχηματισμός ενισχύει την αποτελεσματικότητα και την παραγωγικότητα, εισάγει νέες προκλήσεις που σχετίζονται με τους κινδύνους της κυβερνοασφάλειας, όπως παραβιάσεις δεδομένων και επιθέσεις στον κυβερνοχώρο. Ολοκληρώνουμε αντιμετωπίζοντας τις πιθανές ευπάθειες που σχετίζονται με την εφαρμογή του ψηφιακού μετασχηματισμού και προσφέροντας συστάσεις για το πώς οι οργανισμοί μπορούν να μετριάσουν αυτούς τους κινδύνους μέσω της εφαρμογής αποτελεσματικών μέτρων κυβερνοασφάλειας. Το έγγραφο προτείνει την υιοθέτηση ενός δομημένου πλαισίου ετοιμότητας για την κυβερνοασφάλεια για τις επιχειρηματικές οργανώσεις, ώστε να διασφαλίζεται η ετοιμότητα καθώς ξεκινούν το ταξίδι τους στον ψηφιακό μετασχηματισμό.

Λέξεις-Κλειδιά: Ψηφιακός Μετασχηματισμός, Κυβερνοασφάλεια, επιχειρηματική ανθεκτικότητα, απειλές κυβερνοχώρου, στρατηγικές ασφαλείας

Abstract

This comprehensive review of existing literature delves into the ramifications of digital transformation and cybersecurity for achieving business resilience. Digital transformation involves the shift of organizational processes toward IT solutions, which can lead to substantial changes across various facets of an organization. Nonetheless, the global push for digital transformation, driven by emerging technologies like artificial intelligence, big data and analytics, blockchain, and cloud computing, also amplifies cybersecurity risks for businesses undergoing this transformation. This article, focused on surveying the existing literature, underscores the critical importance of having an extensive understanding of cybersecurity threats during the implementation of digital transformation to prevent disruptions caused by malicious activities or unauthorized access by individuals with the intent of tampering with sensitive information, causing damage, or seeking extortion from users. Cybersecurity plays a vital role in safeguarding digital assets from cyber threats. To conduct this research, we conducted a systematic literature review following the PRISMA methodology. Our review revealed that while digital transformation enhances efficiency and productivity, it introduces new challenges related to cybersecurity risks, such as data breaches and cyber-attacks. We conclude by addressing the prospective vulnerabilities associated with the implementation of digital transformation and offering recommendations on how organizations can mitigate these risks through the implementation of effective cybersecurity measures. The paper proposes the adoption of a structured cybersecurity readiness framework for business organizations to ensure preparedness as they embark on their digital transformation journey.

Keywords: Digital Transformation, Cybersecurity, Business Resilience, Cyber Threats, Mitigation Strategies

Αφιέρωση

Στην Οικογενειά μου
Ιωάννη , Νικολέτα

Πίνακας Περιεχομένων

Κατάλογος Διαγραμμάτων

Κατάλογος Πινάκων

1 Εισαγωγή

Ο ψηφιακός μετασχηματισμός αναφέρεται στην υιοθέτηση ψηφιακών λύσεων στις επιχειρηματικές διαδικασίες των οργανισμών, οι οποίες μπορούν να οδηγήσουν σε σημαντικές αλλαγές στις επιχειρηματικές τους λειτουργίες. Μια τέτοια τροποποίηση μπορεί να επηρεάσει διάφορες πτυχές ενός οργανισμού, για παράδειγμα, την εμπειρία του χρήστη, τις επιχειρηματικές διαδικασίες, τις αγορές-στόχους, τους πελάτες, τις σχέσεις με τους πελάτες, ακόμη και διάφορες πολιτιστικές επιπτώσεις. Η επιταχυνόμενη υιοθέτηση τεχνολογίας από επιχειρηματικούς οργανισμούς κατά τη διάρκεια της πανδημίας COVID-19 οδήγησε επίσης σε πολλές απότομες προκλήσεις [1]. Οι αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη, τα μεγάλα δεδομένα και τα αναλυτικά στοιχεία, το blockchain, το cloud computing, το Διαδίκτυο των πραγμάτων και το βιομηχανικό Διαδίκτυο των πραγμάτων αποτελούν κρίσιμους παράγοντες για τον ψηφιακό μετασχηματισμό. Λόγω των εκτεταμένων πλεονεκτημάτων, οι επιχειρήσεις επιταχύνουν την κίνηση του ψηφιακού μετασχηματισμού. Ωστόσο, η κυβερνοασφάλεια έχει εξελιχθεί σε μια σημαντική πρόκληση για τις εταιρείες και για να αποκτήσουν επιχειρηματική συνέχεια, οι οργανισμοί πρέπει να εξασφαλίσουν τα εργαλεία ψηφιακού μετασχηματισμού και τα τεχνουργήματα τους. Ως εκ τούτου, είναι ζωτικής σημασίας για τους οργανισμούς που υποβάλλονται σε υιοθέτηση ψηφιακού μετασχηματισμού να δώσουν προτεραιότητα στα μέτρα κυβερνοασφάλειας και να διασφαλίσουν ότι τα συστήματά τους είναι ασφαλή από πιθανές απειλές [2,3].

Οι εγκληματίες του κυβερνοχώρου ενδέχεται να εκμεταλλευτούν τις ευπάθειες στις ψηφιακές τεχνολογίες. Ως εκ τούτου, οι οργανισμοί πρέπει να διασφαλίζουν ότι οι τεχνολογικές λύσεις είναι ασφαλείς από ψηφιακές επιθέσεις. Η κυβερνοασφάλεια μπορεί να επιτευχθεί με την εφαρμογή μέτρων κρυπτογράφησης, ελέγχου ταυτότητας και ελέγχου πρόσβασης για την προστασία δεδομένων και δικτύων από μη εξουσιοδοτημένη πρόσβαση ή κακόβουλες δραστηριότητες. Επιπλέον, οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο να επενδύσουν σε ασφαλιστήρια συμβόλαια στον κυβερνοχώρο που μπορούν να παρέχουν οικονομική προστασία έναντι ζημιών λόγω μιας επιτυχημένης επίθεσης στα συστήματά τους. Ένα άλλο κρίσιμο ζήτημα είναι η ευαισθητοποίηση των εργαζομένων σχετικά με τις επιθέσεις στον κυβερνοχώρο, καθώς η υψηλότερη ευαισθητοποίηση οδηγεί σε αξιόπιστη συμπεριφορά ασφάλειας πληροφοριών [4,5]. Οι επιθέσεις στον κυβερνοχώρο έχουν κλιμακωθεί δραστικά. Ως εκ τούτου, οι επιχειρηματικές οργανώσεις πρέπει να κατανοήσουν τις απειλές για την ασφάλεια στον κυβερνοχώρο και τον καλύτερο τρόπο να τις μετριάσουν συνολικά. Αυτές οι επιθέσεις συνήθως στοχεύουν στην αξιολόγηση, αλλαγή ή καταστροφή ευαίσθητων πληροφοριών. εκβιάζουν χρηματικά οφέλη από τους χρήστες· ή να διακόψουν τις συνήθεις επιχειρηματικές διαδικασίες. Η κυβερνοασφάλεια περιλαμβάνει τεχνικές για την προστασία των υπολογιστών και των δικτύων από μη εξουσιοδοτημένη πρόσβαση και κακόβουλες δραστηριότητες όπως η κλοπή και η καταστροφή δεδομένων.

Το κόστος κυβερνοασφάλειας και τα εγκλήματα στον κυβερνοχώρο παρουσιάζουν αυξητική τάση παγκοσμίως [6]. Οι Haislip et al. [7] τόνισε ότι το οικονομικό κόστος των παραβιάσεων της κυβερνοασφάλειας είναι υποτιμημένο, καθώς δεν περιορίζεται μόνο στη στοχευμένη μορφή· μεταδίδονται στον ενδιαφερόμενο κλάδο μέσω αρνητικών αποδόσεων και υψηλότερου κόστους ασφάλισης. Ο Garg [8] έχει επισημάνει επτά κρίσιμα οφέλη από την επένδυση στην ασφάλεια στον κυβερνοχώρο για να παρακινήσει τους οργανισμούς να κάνουν επενδύσεις στον κυβερνοχώρο. Αυτά περιλαμβάνουν την προστασία της πνευματικής ιδιοκτησίας, την καλύτερη ικανοποίηση των απαιτήσεων των πελατών, την ελαχιστοποίηση του κύκλου εργασιών των πελατών, την επωνυμία ασφαλών προϊόντων, τη συμμετοχή ασφαλών προμηθευτών σε ένα ολοκληρωμένο δίκτυο, τη φήμη της εταιρείας και την ελαχιστοποίηση των παράπλευρων ζημιών στον κλάδο. Ο Lee [9] παρουσίασε ένα πλαίσιο διαχείρισης κινδύνου που εστιάζει στη συνεχή βελτίωση των πρακτικών κυβερνοασφάλειας και στην ανάλυση κόστους-οφέλους για επενδύσεις στον κυβερνοχώρο. Πολλοί οργανισμοί χρησιμοποιούν το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) για την ασφάλεια στον κυβερνοχώρο για τη διαχείριση κινδύνων στον κυβερνοχώρο. Ωστόσο, το πρότυπο δεν διαθέτει ανάλυση κόστους-οφέλους. Το μοντέλο Gordon-Loeb έχει προταθεί για να προσδιορίσει ποιο επίπεδο NIST είναι πιο αποτελεσματικό για έναν συγκεκριμένο οργανισμό όσον αφορά τη μελέτη κόστους-οφέλους [10]. Οι Krutilla et al. [11] βελτίωσε το μοντέλο Gordon-Loeb λαμβάνοντας υπόψη το κόστος απόσβεσης των περιουσιακών στοιχείων στον κυβερνοχώρο, το οποίο μπορεί να επηρεάσει την ανάλυση κόστους-οφέλους των πρωτοβουλιών για την ασφάλεια στον κυβερνοχώρο. Οι Simon και Omar [12] τόνισαν ότι οι εταιρείες μπορεί να επηρεαστούν από κινδύνους κυβερνοασφάλειας μέσω επιθέσεων κυβερνοασφάλειας στους συνεργάτες τους στην αλυσίδα εφοδιασμού, επομένως υποστηρίζουν ότι οι επενδύσεις στον κυβερνοχώρο πρέπει να λαμβάνουν υπόψη

τόσο τις συντονισμένες όσο και τις ασυντόνιστες επιθέσεις. Οι Uddin et al. [13] τόνισε ότι οι αδυναμίες στον κυβερνοχώρο επηρεάζουν την οργανωτική ανάπτυξη και απόδοση και, ειδικά για τον τραπεζικό τομέα, οι λειτουργικοί κίνδυνοι έχουν αυξηθεί λόγω των απειλών για την ασφάλεια στον κυβερνοχώρο. Οι Curti et al. [14] τόνισε ότι οι επιθέσεις κυβερνοασφάλειας αυξάνονται στον κυβερνητικό τομέα και για να μετριάσουν αυτές τις απειλές, οι κυβερνήσεις αυξάνουν το κυβερνητικό λειτουργικό κόστος και το συνολικό κόστος χρηματοδότησης.

Σε αυτό το έγγραφο, πραγματοποιήσαμε μια συστηματική βιβλιογραφική ανασκόπηση που τεκμηριώνει πώς ο ψηφιακός μετασχηματισμός άλλαξε τον επιχειρηματικό τομέα και τις επιπτώσεις της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό. Ερευνήσαμε τις εργασίες που δημοσιεύθηκαν κατά την περίοδο 2019–2023 χρησιμοποιώντας τις οδηγίες PRISMA για τη διεξαγωγή βιβλιογραφικής ανασκόπησης. Έχουμε προτείνει ένα πλαίσιο ετοιμότητας για την κυβερνοασφάλεια για τις επιχειρηματικές οργανώσεις που επιδιώκουν τον ψηφιακό μετασχηματισμό. Τα ευρήματα αυτής της εργασίας θα βοηθήσουν τους επιχειρηματικούς οργανισμούς, τους επαγγελματίες και τους ερευνητές να κατανοήσουν την κατάσταση της τέχνης σε αυτόν τον τομέα και θα αποτελέσουν τη βάση για περαιτέρω έρευνα.

2 Βιβλιογραφική Ανασκόπηση

Τις τελευταίες δύο δεκαετίες, η υποδομή Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ) έχει εξελιχθεί σε μεγάλο βαθμό, η οποία είναι πανταχού παρούσα και είναι εξαιρετικά ενσωματωμένη στη σύγχρονη κοινωνία μας. Ως εκ τούτου, η προστασία των συστημάτων και των εφαρμογών ΤΠΕ από επιθέσεις στον κυβερνοχώρο έχει ζητηθεί από τους υπεύθυνους χάραξης πολιτικής ασφαλείας εδώ και μέρες [22]. Η πράξη προστασίας της δομής των ΤΠΕ από διάφορες απειλές ή επιθέσεις στον κυβερνοχώρο έχει ονομαστεί κυβερνοασφάλεια [9]. Διαφορετικές πτυχές συνδέονται με την ασφάλεια στον κυβερνοχώρο, όπως μέτρα για την προστασία των ΤΠΕ, τα ακατέργαστα δεδομένα και πληροφορίες που περιέχουν και η επεξεργασία και μετάδοσή τους· συσχέτιση εικονικών και φυσικών στοιχείων των συστημάτων. το επίπεδο προστασίας που προκύπτει από την εφαρμογή αυτών των μέτρων· και τελικά το σχετικό πεδίο επαγγελματικής προσπάθειας [23]. Σύμφωνα με τον ερευνητή Craigen, η κυβερνοασφάλεια αποτελείται από διαφορετικά εργαλεία, κατευθυντήριες γραμμές και πρακτικές που χρησιμοποιούνται για την προστασία προγραμμάτων λογισμικού, δικτύων υπολογιστών και δεδομένων από επίθεση, μη εξουσιοδοτημένη πρόσβαση ή ζημιά [24]. Ο ερευνητής Aftergood et al. [12], όρισε ότι, η κυβερνοασφάλεια χρησιμοποιεί διαφορετικές διαδικασίες και τεχνολογίες που είναι χρήσιμες για την προστασία δικτύων, προγραμμάτων υπολογιστών και δεδομένων από επιθέσεις, αλλαγές και μη εξουσιοδοτημένη πρόσβαση ή καταστροφή. Με λίγα λόγια, η κυβερνοασφάλεια αφορά την κατανόηση διαφορετικών επιθέσεων στον κυβερνοχώρο και την ανάπτυξη αντίστοιχων αμυντικών στρατηγικών που προστατεύουν διάφορες ιδιότητες που αναφέρονται παρακάτω [24, 25, 26].

- Η εμπιστευτικότητα είναι μια ιδιότητα που χρησιμοποιείται για την αποτροπή της αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες, άτομα ή συστήματα.
- Η ακεραιότητα είναι μια ιδιότητα που χρησιμοποιείται για την αποτροπή οποιασδήποτε μη εξουσιοδοτημένης καταστροφής ή τροποποίησης πληροφοριών.
- Η διαθεσιμότητα είναι μια ιδιότητα που χρησιμοποιείται για τη διασφάλιση έγκαιρης και αξιόπιστης πρόσβασης σε στοιχεία και συστήματα πληροφοριών σε μια εξουσιοδοτημένη οντότητα.

Υπάρχουν τρεις κύριοι παράγοντες ασφάλειας που συνήθως θεωρούνται κίνδυνοι. Αυτοί οι παράγοντες είναι οι επιθέσεις, δηλαδή ποιος επιτίθεται, τα τρωτά σημεία του συστήματος, δηλαδή οι αδυναμίες ή ο θύλακας ασφαλείας στον οποίο επιτίθενται και οι επιπτώσεις, δηλαδή το τι κάνει η επίθεση [9]. Παραβίαση ασφάλειας είναι μια πράξη που απειλεί την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των στοιχείων και των συστημάτων πληροφοριών. Διαφορετικοί τύποι συμβάντων κυβερνοασφάλειας που μπορεί να οδηγήσουν σε κινδύνους για την ασφάλεια στα συστήματα και τα δίκτυα ενός οργανισμού ή σε ένα άτομο [2].

2.1 Κακόβουλο λογισμικό

Είναι ένα κακόβουλο λογισμικό που έχει σχεδιαστεί για να προκαλεί ζημιά σε ένα προσωπικό σύστημα, πελάτη, διακομιστή ή δίκτυο υπολογιστών. Το κακόβουλο λογισμικό περιλαμβάνει spyware, ransomware, ιούς και worms. Το κακόβουλο λογισμικό παραβιάζει ένα δίκτυο δημιουργώντας μια ευάλωτη κατάσταση,

όπως το να κάνει κλικ ο χρήστης σε έναν επικίνδυνο σύνδεσμο ή ένα συνημμένο email και ως εκ τούτου εγκαθιστά ένα επικίνδυνο λογισμικό. Συνήθως, το κακόβουλο λογισμικό επηρεάζει το δίκτυο καθώς: • Τα στοιχεία κλειδιού δικτύου είναι αποκλεισμένα (Ransomware) • Εγκαθιστά πρόσθετο επιβλαβές λογισμικό για κατασκοπεία με το ίδιο το κακόβουλο λογισμικό. • Αποκτήστε πρόσβαση σε προσωπικά δεδομένα και μετάδοση πληροφοριών. • Διαταράσσει ορισμένα στοιχεία και καθιστά το σύστημα μη λειτουργικό για τους χρήστες. Το Ransomware εμποδίζει την πρόσβαση στα δεδομένα του θύματος και απειλεί τον πελάτη να τα καταστρέψει, εκτός εάν τα λύτρα είναι επώδυνα. Ο Δούρειος ίππος είναι το πιο επικίνδυνο κακόβουλο λογισμικό που φαίνεται να είναι χρήσιμο και συνηθισμένο λογισμικό και ως επί το πλείστον έχει σχεδιαστεί για την κλοπή οικονομικών πληροφοριών. Η επίθεση ημέρας οδήγησης είναι μια κοινή μέθοδος για τη διανομή κακόβουλου λογισμικού. Δεν απαιτούν την ενεργοποίηση των ενεργειών των χρηστών. Οι χρήστες πρέπει απλώς να επισκεφτούν έναν καλοήθη ιστότοπο και το προσωπικό τους σύστημα μολύνεται σιωπηλά και μετατρέπεται σε IFRAME που ανακατευθύνει το πρόγραμμα περιήγησης του θύματος σε έναν ιστότοπο που ελέγχεται από τον εισβολέα.

2.2 Phishing

Το ηλεκτρονικό ψάρεμα (phising) είναι μια πρακτική αποστολής δόλιων επικοινωνιών ή κοινωνικής μηχανικής που διαδίδονται κυρίως μέσω email. Ο στόχος είναι να κλέψουν δεδομένα του θύματος, όπως αριθμούς πιστωτικών καρτών και διαπιστευτήρια σύνδεσης. Αυτή η επίθεση χρησιμοποιείται συχνά για να αποκτήσει βάση σε κυβερνητικά ή εταιρικά δίκτυα ως μέρος σημαντικής πλοκής ως προηγμένη επίμονη απειλή (apt). Το Spear phishing στοχεύει σε συγκεκριμένο άτομο ή οργανισμούς, κυβερνήσεις, στρατιωτικές πληροφορίες για την απόκτηση εμπορικών μυστικών, οικονομικών κερδών ή πληροφοριών. Το ψάρεμα φαλαινών απευθύνεται κυρίως σε υπαλλήλους υψηλού προφίλ, όπως CFO ή Διευθύνοντα Σύμβουλο, προκειμένου να αποκτήσουν ζωτικής σημασίας πληροφορίες σχετικά με τα ευαίσθητα δεδομένα της εταιρείας.

2.3 Επίθεση Man-in-Middle

Ο άνθρωπος στη μέση (MITM) γνωστός και ως υποκλοπή εμφανίζεται όταν οι εισβολείς συμπεριλαμβάνονται επιτυχώς σε συναλλαγή ή επικοινωνία δύο μερών. Η πιο κοινή καταχώρηση για εισβολείς MITM είναι:

- Μη ασφαλές δημόσιο WiFi όπου οι εισβολείς παρεμβάλλονται μεταξύ της συσκευής του επισκέπτη και του δικτύου.
- Εάν το κακόβουλο λογισμικό του εισβολέα παραβιάσει με επιτυχία το σύστημα του θύματος, μπορεί να εγκαταστήσει πολύ λογισμικό για να αποκτήσει ασφαλείς πληροφορίες για τα θύματα.

2.4 Επίθεση άρνησης υπηρεσίας

Το denial-of-service (DDoS) τερματίζει τη λειτουργία ενός δικτύου ή μιας υπηρεσίας με τεράστια κίνηση για την εξάντληση πόρων και εύρους ζώνης, με αποτέλεσμα το σύστημα να μην μπορεί να εκπληρώσει τα νόμιμα αιτήματα. Τα DDoS συχνά έχουν σχεδιαστεί για να στοχεύουν διακομιστές ιστού οργανισμών υψηλού προφίλ, όπως πλατφόρμα συναλλαγών, μέσα ενημέρωσης, τραπεζικές υπηρεσίες και κυβέρνηση.

2.5 SQL Injection

Το SQL Injection (SQLI) στοχεύει στη χρήση κακόβουλου κώδικα για τον χειρισμό πληροφοριών πρόσβασης στη βάση δεδομένων backend που δεν προορίζονταν για εμφάνιση. Οι εισβολείς θα μπορούσαν να πραγματοποιήσουν μια ένεση SQL απλώς υποβάλλοντας κακόβουλο κώδικα σε ευάλωτο πλαίσιο αναζήτησης ιστότοπου.

2.6 Επίθεση Zero-day Exploit

Η επίθεση Zero-day Exploit θεωρείται ως ο όρος που χρησιμοποιείται για να περιγράψει την απειλή μιας άγνωστης ευπάθειας ασφαλείας για την οποία η ενημέρωση κώδικα δεν έχει κυκλοφορήσει ακόμη ή οι

προγραμματιστές εφαρμογών δεν γνωρίζουν. Για τον εντοπισμό αυτής της απειλής, οι προγραμματιστές απαιτούν συνεχή επίγνωση.

2.7 DNS-Tunneling

Το DNS Tunneling χρησιμοποιεί το πρωτόκολλο DNS για να επικοινωνεί κίνηση εκτός DNS μέσω της θύρας 53, στέλνοντας κίνηση HTTP και άλλου πρωτοκόλλου μέσω DNS. Δεδομένου ότι η χρήση του DNS Tunneling είναι μια κοινή και νόμιμη διαδικασία, επομένως η χρήση του για κακόβουλους λόγους είναι πολύ συχνά. Οι εισβολείς μπορούν να το χρησιμοποιήσουν για να συγκαλύψουν την εξερχόμενη κίνηση ως DNS, αποκρύπτοντας δεδομένα που μοιράζονται μέσω μιας σύνδεσης στο Διαδίκτυο.

2.8 Στρατηγικές Άμυνας

Απαιτούνται αμυντικές στρατηγικές για τη διατήρηση δεδομένων ή πληροφοριών, συστημάτων πληροφοριών και δικτύων για την αποτροπή κυβερνοεπιθέσεων ή εισβολών. Πιο συγκεκριμένα, είναι υπεύθυνοι για την πρόληψη παραβιάσεων δεδομένων ή συμβάντων ασφαλείας, παρακολούθηση και αντίδραση σε απειλή, η οποία μπορεί να οριστεί ως κάθε είδους μη εξουσιοδοτημένη δραστηριότητα που προκαλεί ζημιά σε ένα δίκτυο και σε προσωπικά συστήματα [37]. Ένα σύστημα ανίχνευσης εισβολής (IDS) περιγράφεται ως «λογισμικό, συσκευή ή εφαρμογή που παρακολουθεί ένα σύστημα ή ένα δίκτυο υπολογιστών για κακόβουλη δραστηριότητα ή παραβιάσεις πολιτικής» [39]. Ωστόσο, οι καθιερωμένες λύσεις ασφαλείας, όπως ο έλεγχος ταυτότητας χρήστη, ο έλεγχος πρόσβασης, η προστασία από ιούς, τα τείχη προστασίας, τα συστήματα κρυπτογράφησης και η κρυπτογράφηση δεδομένων ενδέχεται να μην είναι αποτελεσματικές σύμφωνα με τις σημερινές ανάγκες της βιομηχανίας του κυβερνοχώρου [16–19]. Επιπλέον, το IDS επιλύει τα ζητήματα αναλύοντας δεδομένα ασφαλείας από πολλά βασικά σημεία ενός δικτύου ή συστήματος [38, 40]. Επιπλέον, το IDS μπορεί να χρησιμοποιηθεί για τον εντοπισμό τόσο εσωτερικών όσο και εξωτερικών επιθέσεων. Τα συστήματα ανίχνευσης εισβολής είναι διαφόρων κατηγοριών ανάλογα με το εύρος χρήσης. Για παράδειγμα, ένα σύστημα ανίχνευσης εισβολής που βασίζεται σε κεντρικό υπολογιστή (HIDS) και ένα σύστημα ανίχνευσης εισβολής δικτύου (NIDS) είναι οι πολύ γνωστοί τύποι που βασίζονται στην εμβέλεια μεμονωμένων υπολογιστών σε μεγάλα δίκτυα. Σε ένα HIDS, το σύστημα παρακολουθεί δεδομένα, αρχεία, ασφαλείς πληροφορίες σε ένα μεμονωμένο σύστημα, ενώ παρακολουθεί και αναλύει συνδέσεις δικτύου για ύποπτη κίνηση σε ένα NIDS. Ομοίως, με βάση τις θεωρίες, το IDS που βασίζεται στην υπογραφή και το IDS που βασίζεται σε ανωμαλίες είναι οι πιο καθιερωμένες παραλλαγές [37].

Η μηχανική μάθηση στην ασφάλεια στον κυβερνοχώρο καθοδηγείται σε μεγάλο βαθμό από τη διαθεσιμότητα δεδομένων κυβερνοασφάλειας [48]. Τα σύνολα δεδομένων αντιπροσωπεύουν συνήθως μια συλλογή εγγραφών που αποτελούνται από πληροφορίες ως πολλά χαρακτηριστικά ή χαρακτηριστικά και σχετικά γεγονότα, στα οποία βασίζονται οι τεχνικές μηχανικής μάθησης στην ασφάλεια στον κυβερνοχώρο. Επομένως, είναι σημαντικό να κατανοήσουμε τη φύση των δεδομένων κυβερνοασφάλειας που περιέχουν διάφορους τύπους περιστατικών στον κυβερνοχώρο και σχετικά χαρακτηριστικά. Ο λόγος πίσω από αυτό είναι ότι τα ανεπεξέργαστα δεδομένα ασφαλείας που συλλέγονται από παρόμοιες πηγές στον κυβερνοχώρο μπορούν να χρησιμοποιηθούν για την ανάλυση των διαφορετικών προτύπων συμβάντων ασφαλείας ή κακόβουλης συμπεριφοράς, για τη δημιουργία ενός μοντέλου ασφάλειας βάσει δεδομένων για την επίτευξη του στόχου μας. Υπάρχουν διαφορετικά σύνολα δεδομένων στον τομέα της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένης της ανάλυσης εισβολής δικτύου, της ανάλυσης κακόβουλου λογισμικού, του εντοπισμού ηλεκτρονικού ψαρέματος, της απάτης, της ανωμαλίας ή της ανάλυσης ανεπιθύμητης αλληλογραφίας που χρησιμοποιούνται για διάφορους σκοπούς. Στον Πίνακα 2.2, συνοψίζουμε διαφορετικούς τύπους συνόλων δεδομένων, συμπεριλαμβανομένων των διαφόρων χαρακτηριστικών και περιστατικών τους που είναι προσβάσιμα στο διαδίκτυο και τονίζουμε τη χρήση τους με βάση τεχνικές μηχανικής εκμάθησης σε διαφορετικές εφαρμογές στον κυβερνοχώρο. Η αποτελεσματική ανάλυση και επεξεργασία αυτών των δικτυακών και τυπικών χαρακτηριστικών, η δημιουργία στοχευόμενου μοντέλου ασφάλειας που βασίζεται στη μηχανική μάθηση σύμφωνα με τις αμυντικές απαιτήσεις και, τελικά, η λήψη αποφάσεων βάσει δεδομένων, θα μπορούσε να παίξει ρόλο στην παροχή ευφυών υπηρεσιών κυβερνοασφάλειας.

3 Μεθοδολογία

Σε αυτή την ενότητα, εξηγούμε τη μεθοδολογία. Κάναμε μια συστηματική ανασκόπηση της βιβλιογραφίας χρησιμοποιώντας τις οδηγίες PRISMA [15]. Όπως φαίνεται στην Εικόνα 1, χρησιμοποιήσαμε τη βάση δεδομένων Google Scholar. Οι πρωτογενείς μελέτες εξήχθησαν χρησιμοποιώντας συγκεκριμένες λέξεις-κλειδιά στα κριτήρια αναζήτησης. Οι λέξεις-κλειδιά επιλέχθηκαν για να διευκολυνθεί η δημιουργία ερευνητικών άρθρων σχετικά με το θέμα μας. Οι όροι αναζήτησης που χρησιμοποιήθηκαν ήταν (επιχειρηματικός μετασχηματισμός) AND (ασφάλεια), (ψηφιακός μετασχηματισμός) AND (κυβερνοασφάλεια), (ψηφιακός μετασχηματισμός) AND (ασφάλεια στον κυβερνοχώρο), (ψηφιακός μετασχηματισμός) ΚΑΙ (προστασία) και (ψηφιοποίηση) ΚΑΙ (ασφάλεια) . Για να βελτιώσουμε τα αποτελέσματα αναζήτησής μας, χρησιμοποιήσαμε τα ακόλουθα κριτήρια συμπερίληψης:

- Το έγγραφο θα πρέπει να σχετίζεται με τις ψηφιακές επιχειρήσεις και την ασφάλεια στον κυβερνοχώρο.
- Η εργασία δημοσιεύτηκε μεταξύ 2019-2023.

Διάγραμμα 1 Διάγραμμα Prisma για τη συστηματική βιβλιογραφική ανασκόπηση.

Επιπλέον, εφαρμόστηκαν τα ακόλουθα κριτήρια αποκλεισμού στα αποτελέσματα αναζήτησης:

- Οι εργασίες δεν είναι γραμμένες στην αγγλική γλώσσα.
- Η εργασία δεν σχετίζεται με την κυβερνοασφάλεια και τον ψηφιακό μετασχηματισμό.
- Η εργασία είναι μια ανασκόπηση.

Όλα τα αποτελέσματα του Μελετητή Google ελέγχθηκαν για συμμόρφωση με αυτά τα κριτήρια. Η διαδικασία αναγνώρισης των εξαγόμενων μελετών πέρασε από το στάδιο αξιολόγησης ποιότητας, ξεκινώντας με μια γρήγορη σάρωση του τίτλου και της γλώσσας της εργασίας (αγγλικά ή μη). Δεύτερον, διασφαλίστηκε επίσης ότι αυτές οι εργασίες σχετίζονται και σχετίζονται με την έρευνά μας. Το Σχήμα 1 δείχνει τον αριθμό των τελικών εργασιών που επιλέχθηκαν μετά από αυτά τα στάδια.

4 Αποτελέσματα

Σε αυτήν την ενότητα, επισημαίνουμε τα ευρήματα των ληφθέντων εγγράφων.

4.1 Χρηματοοικονομικός τομέας

Ο χρηματοοικονομικός τομέας είναι ένα κρίσιμο συστατικό μιας οικονομίας και έχουν γίνει πολλές εμπειρικές μελέτες σε διαφορετικά γεωγραφικά πλαίσια. Για παράδειγμα, οι Al-Alawi και Al-Bassam διεξήγαγαν εμπειρική έρευνα στο Μπαχρέιν και διαπίστωσαν ότι τα χρηματοπιστωτικά ιδρύματα εκτίθενται σε διαδικτυακή κλοπή ταυτότητας, ζημιά στο σύστημα υπολογιστών και απόπειρες πειρατείας που οδηγούν σε λειτουργικές διαταραχές [16]. Ομοίως, οι Hasan και Al-Ramadan [17] διεξήγαγαν μια εμπειρική μελέτη με πελάτες τραπεζών στο Ιράκ και διαπίστωσαν ότι παρόλο που οι τράπεζες υιοθετούν σημαντικά μέτρα ασφαλείας, ορισμένοι πελάτες εξακολουθούν να είναι δύσπιστοι σχετικά με την ηλεκτρονική τραπεζική. Σε μια άλλη μελέτη, οι Joveda et al. [18] ερεύνησαν τον τραπεζικό τομέα στο Μπαγκλαντές. Τόνισαν την ανάπτυξη ενός συστήματος κυβερνοασφάλειας για τον εντοπισμό συναλλαγών για ξέπλυμα χρήματος που επηρεάζουν αρνητικά την οικονομική ανάπτυξη. Υπάρχει τεράστιο δυναμικό στις σύγχρονες τεχνολογίες για τη στήριξη του χρηματοπιστωτικού τομέα. Οι Almudaires και Almaiah [19] περιέγραψαν σημαντικές απειλές για τις εταιρείες πιστωτικών καρτών και συναφείς λύσεις για τις εταιρείες πιστωτικών καρτών για να βελτιώσουν την εφαρμογή τους στον κυβερνοχώρο. Οι Smith και Dhillon [20] τόνισαν ότι το blockchain είναι μια κρίσιμη τεχνολογία για την ελαχιστοποίηση των απειλών ασφαλείας στις χρηματοοικονομικές συναλλαγές. Ωστόσο, υπάρχει ανάγκη για αυστηρή ανάλυση της εφαρμογής blockchain στον χρηματοπιστωτικό τομέα. Ομοίως, οι Kuzmenko et al. [21] χρησιμοποίησαν μοντέλα μηχανικής μάθησης για να αναλύσει μεγάλους όγκους οικονομικών δεδομένων για να εντοπίσει πιθανές απειλές σε πρώιμο στάδιο.

Οι Rodrigues et al. [22] ανέπτυξαν ένα μοντέλο υποστήριξης αποφάσεων για την ενσωμάτωση της τεχνητής νοημοσύνης (AI), του ψηφιακού μετασχηματισμού και της ασφάλειας στον κυβερνοχώρο στον τραπεζικό τομέα, διασφαλίζοντας παράλληλα ότι η ασφάλεια των δεδομένων δεν τίθεται σε κίνδυνο. Οι συγγραφείς διαπίστωσαν ότι οι παραδοσιακές τράπεζες υφίστανται πίεση από τους μετόχους τους να προσαρμοστούν στις νέες τεχνολογίες και πρέπει επίσης να διασφαλίσουν ότι τυχόν πιθανές παραβιάσεις δεδομένων ή άλλα ζητήματα ασφάλειας δεν θέτουν σε κίνδυνο τη φήμη τους. Οι συγγραφείς χρησιμοποίησαν τη γνωστική χαρτογράφηση και τη δοκιμαστική μέθοδο λήψης αποφάσεων και την εργαστηριακή μέθοδο αξιολόγησης για να αντιμετωπίσουν αυτό το περίπλοκο ζήτημα με μια ομάδα ειδικών σε ομαδικές συνεδρίες. Αυτό οδήγησε σε ένα ρεαλιστικό πλαίσιο για τη λήψη αποφάσεων σχετικά με την εφαρμογή της τεχνητής νοημοσύνης στον τραπεζικό κλάδο, διασφαλίζοντας παράλληλα ότι δεν διακυβεύεται η ασφάλεια των δεδομένων. Η μελέτη ανέπτυξε ένα πλαίσιο με γνώμονα τη γνώση πολλών συμμετόχων χρησιμοποιώντας γνωστική χαρτογράφηση σε συνδυασμό με τη μεθοδολογία DEMATEL. Αυτή η προσέγγιση τους επέτρεψε να εντοπίσουν κρίσιμους παράγοντες που επηρεάζουν την υιοθέτηση της τεχνητής νοημοσύνης εντός των τραπεζών, όπως η εμπιστοσύνη των πελατών προς τις υπηρεσίες που βασίζονται στην τεχνολογία που προσφέρονται από τις τράπεζες. κανονιστικές απαιτήσεις συμμόρφωσης· και διαθεσιμότητα ειδικευμένου εργατικού δυναμικού, τα οποία στη συνέχεια ταξινομήθηκαν με βάση τη σχετική σημασία τους χρησιμοποιώντας την ανάλυση DEMATEL.

Ομοίως, οι Fedorov et al. [23] τόνισε πώς οι γνωστικές τεχνολογίες θα μπορούσαν να εξασφαλίσουν την ασφάλεια των δεδομένων κατά τη χρήση της τεχνολογίας βιομετρικής ταυτοποίησης σε απομακρυσμένες τραπεζικές συναλλαγές. Το άρθρο εξέτασε πώς ο ψηφιακός μετασχηματισμός και η βιομετρική ταυτοποίηση θα επηρεάσουν τις χρηματοπιστωτικές υπηρεσίες στη Ρωσία. Τόνισε ότι απαιτούνται προηγμένα μέτρα ασφαλείας για την προστασία ευαίσθητων δεδομένων πελατών κατά τη διάρκεια αυτών των συναλλαγών. Η προτεινόμενη λύση είναι μέσω γνωστικών τεχνολογιών που εστιάζονται στις ανθρώπινες διανοητικές ικανότητες ως μία κατεύθυνση για τη διασφάλιση της ασφάλειας των πληροφοριών σε αυτό το πλαίσιο.

Μια άλλη ερευνητική μελέτη από τους Patil και Bharath [24] διερεύνησε τις τεχνολογικές εξελίξεις στον χρηματοπιστωτικό τομέα. Τα ευρήματα της μελέτης έδειξαν ότι η Fintech έχει βελτιώσει τις επιχειρήσεις και οι επενδυτές έχουν μεγαλύτερη εμπιστοσύνη στην τεχνολογία. Παρουσίασαν επίσης τις νέες τεχνολογίες που υιοθετήθηκαν από τη Fintech και τα σχετικά θέματα. Η επίδραση της χρηματοοικονομικής τεχνολογίας ήταν θετική στους παράγοντες εμπιστοσύνης και εξουσιοδότησης επιχειρήσεων. Η παραδοσιακή χρηματοοικονομική έχει παρατηρήσει τα πιο σημαντικά κρίσιμα ζητήματα, όπως οι κίνδυνοι

απάτης και οι χαμηλές επιδόσεις, καθώς και διαφορές και περιορισμοί. Η έρευνα διεξήχθη σε περιορισμένο δείγμα περίπου 160.

Επιπλέον, οι Rãƒdulescu et al. [25] εξήγησε τους κινδύνους που συνδέονται με την ψηφιοποίηση όσον αφορά την οικονομική ανάπτυξη και τη διασφάλιση της κοινωνικής ασφάλειας και της ασφάλειας των πληροφοριών. Τόνισαν ότι η ψηφιοποίηση επηρεάζει σημαντικά την οικονομική ανάπτυξη, την κοινωνική ένταξη και τη βιώσιμη ανάπτυξη. Ωστόσο, εισάγει επίσης νέα τρωτά σημεία που μπορούν να οδηγήσουν σε επιθέσεις στον κυβερνοχώρο και απαιτούν έξυπνους ελέγχους για την αποτροπή τους. Οι συγγραφείς πρότειναν ότι οι ειδικοί της τεχνολογίας και άλλοι ενδιαφερόμενοι θα πρέπει να συμμετέχουν στην αξιολόγηση αυτών των κινδύνων, καθώς μπορούν να αυξηθούν και να γίνουν πιο περίπλοκοι με την πάροδο του χρόνου. Οι διαχειριστές κινδύνων πρέπει να αναπτύξουν μια ολοκληρωμένη στρατηγική που να περιλαμβάνει λύσεις μετριασμού και μεταφοράς κινδύνου, δίνοντας προτεραιότητα σε ποιες επιλογές ασφάλειας IT μετριάζουν καλύτερα τον κίνδυνο του οργανισμού.

Επιπλέον, η διεθνής συνεργασία είναι απαραίτητη για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο λόγω του εξελισσόμενου παγκόσμιου εγκλήματος και των τρομοκρατικών απειλών που συνδέονται με τον ψηφιακό μετασχηματισμό. Τέλος, τόνισε την αυξανόμενη σημασία της τεχνολογίας των πληροφοριών στην ανάπτυξη των επιχειρήσεων, τις ανθρώπινες σχέσεις και την επικοινωνία μεταξύ ανθρώπων και κυβερνήσεων. Ως εκ τούτου, η διαχείριση του ψηφιακού κινδύνου θα πρέπει να αποτελεί προτεραιότητα για όλους τους εμπλεκόμενους φορείς.

4.2 Τομέας Υγείας

Η κυβερνοασφάλεια στον τομέα της υγείας ασχολείται με το απόρρητο των δεδομένων ασθενών [26] και την ασφάλεια των ιατρικών συσκευών [27-30]. Μια ασφαλής κίνηση ψηφιακού μετασχηματισμού μπορεί να βοηθήσει στη βελτίωση της οργανωτικής διακυβέρνησης των οργανισμών υγείας [31-33]. Garcia-Perez et al. [34] συζήτησε πώς ο ψηφιακός μετασχηματισμός των συστημάτων υγειονομικής περίθαλψης πρέπει να αντιμετωπίζεται αποτελεσματικά από την οπτική της κυβερνοασφάλειας. Αυτό το έγγραφο ανέλυσε δεδομένα από ανώτερα στελέχη στο Ηνωμένο Βασίλειο κατά τη διάρκεια της πανδημίας COVID-19. Σύμφωνα με τα ευρήματά τους, μια ισορροπημένη βάση που λαμβάνει υπόψη την ανάπτυξη γνώσεων στον κυβερνοχώρο, τη διαχείριση αβεβαιότητας και την υψηλή συστηματική και οργανωτική αλληλεξάρτηση του τομέα που έχει επιπτώσεις στην έρευνα και τις πρακτικές διαχείρισης είναι απαραίτητη για τις προσπάθειες ψηφιακής ανθεκτικότητας και βιωσιμότητας στον τομέα της υγείας.

Από την άλλη, οι Paul et al. [35] συζήτησε τη χρήση της ψηφιακής τεχνολογίας στον τομέα της υγειονομικής περίθαλψης και τόνισε θέματα ιδιωτικότητας και ασφάλειας που σχετίζονται με αυτές τις τεχνολογίες. Αυτή η μελέτη εξέτασε πώς η ψηφιοποίηση μεταμορφώνει τον τομέα της υγειονομικής περίθαλψης, τον αντίκτυπό της στην περίθαλψη ασθενών και ευκαιρίες για νέα επιχειρηματικά μοντέλα με προσεγγίσεις Industry 4.0 και επιχειρηματικής ευφυΐας. Η αύξηση των χρόνιων ασθενειών και η τρέχουσα πανδημία έχουν αυξήσει την ανάγκη για ατομοκεντρική φροντίδα που ενθαρρύνει τα άτομα να συμμετέχουν στην υγειονομική τους φροντίδα. Ψηφιακές λύσεις, όπως βιοαισθητήρες και λογισμικό εισάγονται για να καλύψουν την αυξανόμενη ανάγκη για υπηρεσίες υγειονομικής περίθαλψης κατά παραγγελία. Η ανάλυση μεγάλων δεδομένων έχει επίσης επηρεάσει σημαντικά τους οργανισμούς υγειονομικής περίθαλψης παρέχοντας πρόσβαση σε δεκαετίες αποθηκευμένων δεδομένων, τα οποία χρησιμεύουν ως τεκμηριωμένο φάρμακο για καλύτερη λήψη αποφάσεων κατά τη θεραπεία ασθενών, διασφαλίζοντας παράλληλα την προστασία του απορρήτου των ασθενών. Υπάρχουν πολλοί τρόποι αντιμετώπισης των ανησυχιών για την ασφάλεια και το απόρρητο που σχετίζονται με την ψηφιοποίηση στην υγειονομική περίθαλψη. Καλύπτει διάφορες λύσεις, όπως αμοιβαίο έλεγχο ταυτότητας, συμφωνία κλειδιού, ελαφριά κρυπτογραφία, λύσεις που βασίζονται σε blockchain κ.λπ., οι οποίες μπορούν να συμβάλουν στη διασφάλιση του ασφαλούς χειρισμού των ιατρικών δεδομένων. Οι συγγραφείς προτείνουν επίσης την ανάπτυξη προγραμμάτων διαχείρισης για ιατρικό εξοπλισμό και τη διερεύνηση του τρόπου με τον οποίο η δέσμευση των ασθενών μπορεί να επηρεάσει τα μέτρα απορρήτου και ασφάλειας. Τέλος, συνιστούν περαιτέρω έρευνα σχετικά με τους κανονισμούς σχετικά με το απόρρητο και την ασφάλεια στον τομέα της υγειονομικής περίθαλψης και τη διερεύνηση του ρόλου της τεχνητής νοημοσύνης (AI) και της τεχνολογίας blockchain στη βελτίωση των αποτελεσμάτων της υγειονομικής περίθαλψης διατηρώντας παράλληλα την ασφάλεια των δεδομένων. Η υιοθέτηση της τεχνολογίας που βασίζεται στο cloud συζητείται επίσης ως πιθανή λύση για καλύτερη αρχειοθέτηση και χρήση δεδομένων ασθενών,

χαμηλότερο κόστος αποθήκευσης, ταχύτερους κύκλους καινοτομίας, πιο απλή συνεργασία και αυξημένες δυνατότητες τηλεϊατρικής.

Οι Nwaiwu και Mbelu [36] τόνισαν ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων GDPR είναι απαραίτητος για να συμμορφώνονται οι επιχειρήσεις και οι κυβερνήσεις για την παρακολούθηση και την παρακολούθηση της υγείας των ανθρώπων, την ανάπτυξη επιχειρηματικών μοντέλων και την ανακάλυψη ευκαιριών στην αγορά. Οι στατιστικές δείχνουν ότι η Ευρώπη έχει καταγράψει 1,92 εκατομμύρια επιβεβαιωμένα κρούσματα COVID-19 και ο εντοπισμός επαφών με προσωπικά δεδομένα είναι απαραίτητος για τον περιορισμό και τον περιορισμό της εξάπλωσης του ιού.

Οι Maleh και Mellal [37] παρείχαν πληροφορίες σχετικά με τον τρόπο με τον οποίο ο ψηφιακός μετασχηματισμός και η κυβερνοασφάλεια επηρεάζονται από τη διάδοση του COVID-19. Ο συγγραφέας συζήτησε πώς ο COVID-19 έχει επιταχύνει τις τάσεις ψηφιακού μετασχηματισμού, όπως το cloud computing, η έκρηξη των IoT και η συσσώρευση μεγάλων δεδομένων, ενώ επίσης αύξησε τις επιθέσεις στον κυβερνοχώρο που σχετίζονται με προσωπικά δεδομένα Οι Maleh και Mellal [37] παρείχαν πληροφορίες για τον τρόπο με τον οποίο ο ψηφιακός μετασχηματισμός και η κυβερνοασφάλεια επηρεάζονται από τη διάδοση του COVID-19. Ο συγγραφέας συζήτησε πώς ο COVID-19 έχει επιταχύνει τις τάσεις ψηφιακού μετασχηματισμού, όπως το cloud computing, η έκρηξη του IoT και η συσσώρευση μεγάλων δεδομένων, ενώ παράλληλα έχει αυξήσει τις επιθέσεις στον κυβερνοχώρο που σχετίζονται με προσωπικά δεδομένα.

4.3 Κυβερνητικός Τομέας

Ο ψηφιακός μετασχηματισμός σε κυβερνητικούς οργανισμούς υιοθετείται σε όλο τον κόσμο, όπως στο Μπαχρέιν [38], στο Ηνωμένο Βασίλειο [39] και στη Σαουδική Αραβία [40]. Ωστόσο, η ταχύτητα υιοθέτησης δεν είναι ομοιόμορφη. Οι Al Shobaki et al. [41] ερεύνησε πώς ο ψηφιακός μετασχηματισμός επηρεάζει τις πρακτικές κυβερνοασφάλειας στο Υπουργείο Εσωτερικών και Εθνικής Ασφάλειας στην Παλαιστίνη. Οι ερευνητές χρησιμοποίησαν μια περιγραφική-αναλυτική προσέγγιση με κύριο ερευνητικό εργαλείο ένα ερωτηματολόγιο. Βρήκαν μια στατιστικά σημαντική συσχέτιση μεταξύ όλων των διαστάσεων του ψηφιακού μετασχηματισμού και των πρακτικών κυβερνοασφάλειας του υπουργείου. Επιπλέον, ορισμένοι οργανωτικοί παράγοντες βρέθηκε να έχουν ισχυρό αντίκτυπο σε αυτές τις πρακτικές. Για παράδειγμα, η αποτελεσματική ανταλλαγή δεδομένων μεταξύ διαφορετικών τμημάτων προσδιορίστηκε ως ζωτικής σημασίας για τη διατήρηση ισχυρών μέτρων κυβερνοασφάλειας σε όλους τους τομείς λειτουργίας. Τα συνολικά αποτελέσματα έδειξαν ότι υπάρχει πράγματι αντίκτυπος του ψηφιακού μετασχηματισμού στην ασφάλεια στον κυβερνοχώρο σε αυτό το πλαίσιο, ειδικά στις επαρχίες της Γάζας, όπου είχε συντελεστή αντίκτυπου (0,897). Με βάση αυτά τα ευρήματα, διατυπώθηκαν συστάσεις για τη βελτίωση των ηλεκτρονικών υπηρεσιών που προσφέρονται από κρατικούς φορείς, ενώ παράλληλα αντιμετωπίζονται τα κενά στην απόδοση των εργαζομένων που σχετίζονται με τη χρήση της τεχνολογίας ή τα κενά γνώσης σχετικά με τις βέλτιστες πρακτικές κατά την αντιμετώπιση ευαίσθητων πληροφοριών στο διαδίκτυο. Συμπερασματικά: αυτό το έγγραφο παρέχει πολύτιμες πληροφορίες για το πώς οι επιχειρήσεις μπορούν να προσαρμόσουν τις στρατηγικές τους στον κυβερνοχώρο όταν υφίστανται σημαντικές αλλαγές λόγω τεχνολογικών προόδων, όπως αυτές που σχετίζονται με «ψηφιακούς μετασχηματισμούς», εντοπίζοντας βασικούς οργανωτικούς παράγοντες που επηρεάζουν τα μέτρα κυβερνοασφάλειας σε οργανισμούς όπως υπουργεία.

Μια άλλη μελέτη των Al Najjar et al. [42] στόχευε στον εντοπισμό της πραγματικότητας του ψηφιακού μετασχηματισμού στο Παλαιστινιακό Υπουργείο Εσωτερικών και Εθνικής Ασφάλειας από τη σκοπιά των εργαζομένων σε μονάδες υπολογιστών και τεχνολογίας πληροφοριών. Η μελέτη χρησιμοποίησε μια ολοκληρωμένη μέθοδο έρευνας, διανέμοντας ερωτηματολόγια μεταξύ των εργαζομένων, με 61 που ανακτήθηκαν (που αντιπροσωπεύουν ποσοστό ανταπόκρισης 87,1%). Μέσω αυτών των ερωτηματολογίων μετρήθηκαν διάφορες διαστάσεις που σχετίζονται με τον ψηφιακό μετασχηματισμό, συμπεριλαμβανομένης της υποστήριξης ανώτερων στελεχών, των στρατηγικών κατευθύνσεων, της τεχνικής υποδομής που είναι απαραίτητη για τον ψηφιακό μετασχηματισμό, του συντονισμού των ανθρώπινων πόρων, της ιδιωτικής ζωής και της ασφάλειας δεδομένων, της οργανωτικής δομής και της περιγραφής εργασίας. Τα αποτελέσματα έδειξαν ότι οι περισσότερες διαστάσεις που σχετίζονται με τον ψηφιακό μετασχηματισμό είναι διαθέσιμες εντός του υπουργείου σε μεγάλο βαθμό. Ωστόσο, υπάρχουν ακόμη περιθώρια βελτίωσης, όπως η παροχή περισσότερων κεφαλαίων για την ανάπτυξη ηλεκτρονικών

υπηρεσιών ή τις δαπάνες για καινοτομία. Η υποστήριξη της ανώτερης διοίκησης έλαβε υψηλό βαθμό έγκρισης μαζί με στρατηγικές κατευθύνσεις. Ταυτόχρονα, η απαραίτητη τεχνική υποδομή για τον ψηφιακό μετασχηματισμό πέτυχε επίσης μεγάλο βαθμό έγκρισης, ακολουθούμενη από τον συντονισμό του ανθρώπινου δυναμικού, ο οποίος σημείωσε χαμηλότερη βαθμολογία από άλλες διαστάσεις, αλλά εξακολουθεί να έχει σημαντική σχετική βαρύτητα. Συμπερασματικά, αυτό το έγγραφο υπογραμμίζει πόσο σημαντικό είναι για τους οργανισμούς που αναζητούν ανταγωνιστικό πλεονέκτημα μέσω βελτιωμένης αποδοτικότητας ή ευκαιριών ανάπτυξης ηλεκτρονικών υπηρεσιών χαμηλού κόστους που εκμεταλλεύονται τις δυνατότητες τεχνολογικής επανάστασης που προσφέρονται σε όλα τα επίπεδα, εσωτερικά ή εξωτερικά, με διάφορους συνεργαζόμενους οργανισμούς, να εξετάσουν το ενδεχόμενο να επενδύσουν σε προσπάθειες για την επίτευξη επιτυχημένων πρωτοβουλιών ψηφιακού μετασχηματισμού.

Σε μια άλλη μελέτη, οι Fjord και Schmidt [43] εξέτασαν τις δυνατότητες και τις προκλήσεις της χρήσης ψηφιακών εργαλείων για την απλούστευση της εκτίμησης και είσπραξης φόρων και τη βελτίωση της διαφάνειας. Οι πρακτικές εμπειρίες στη Δανία έδειξαν ότι τα κράτη είχαν σημειώσει πρόοδο όσον αφορά τη βελτίωση της αποτελεσματικότητας των φορολογικών διαδικασιών, αλλά έπρεπε να λάβουν μέτρα για τη διασφάλιση της νομιμότητας και της διαφάνειας μέσω της ασφάλειας στον κυβερνοχώρο.

Οι Mijwil et al. [44] τόνισε τη σημασία της διακυβέρνησης της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό για τις δημόσιες υπηρεσίες που παρέχονται από εταιρείες ή ιδρύματα. Η εργασία υποστήριξε οι Mijwil et al. [44] τόνισε τη σημασία της διακυβέρνησης της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό για τις δημόσιες υπηρεσίες που παρέχονται από εταιρείες ή ιδρύματα. Η εφημερίδα μάλωνε

Maglaras et al. [45] επικεντρώθηκε στην προστασία της ζωτικής σημασίας υποδομής για τη δημόσια ασφάλεια και την εθνική ασφάλεια. Πρότειναν μια μεθοδολογία για την προστασία της εθνικής υποδομής ζωτικής σημασίας που βασίζεται σε επιθέσεις χωρίς αρχεία έναντι τεχνικών ομάδας Advanced Persistent Threat (APT) που χρησιμοποιούνται σε τέτοιες επιθέσεις. Η μελέτη που χρησιμοποιεί αυτή τη μεθοδολογία είχε ως στόχο να ποσοτικοποιήσει και να βαθμολογήσει τις επιθέσεις στον κυβερνοχώρο από μια επιθετική προοπτική της κυβερνοασφάλειας.

4.4 Επαγγελματικός τομέας

Οι επιχειρηματικές οργανώσεις είναι πολύ ετερογενείς, με αποτέλεσμα τα τεχνολογικά συστήματα που αναπτύσσονται στους οργανισμούς. Οι σύγχρονες τεχνολογίες όπως το Διαδίκτυο των Πάντων μπορούν να βοηθήσουν τους οργανισμούς να βελτιώσουν την ασφάλεια στον κυβερνοχώρο [46]. Ο Gonchar [47] ανέπτυξε θεωρητικές και πρακτικές συστάσεις για τη βελτίωση της οικονομικής ασφάλειας στην ψηφιακή οικονομία. Οι ερευνητές διεξήγαγαν μια μελέτη σχετικά με τον αντίκτυπο των ψηφιακών τεχνολογιών στην επιχειρηματική δραστηριότητα στην Ουκρανία, διαπιστώνοντας ότι οι επιχειρήσεις χρησιμοποιούν όλο και περισσότερο τεχνολογίες πληροφοριών και επικοινωνιών. Ωστόσο, υπήρχαν διαφορές με βάση το μέγεθος και τον τομέα. Το έγγραφο πρότεινε μια μεθοδολογία για την αξιολόγηση του επιπέδου ψηφιακού μετασχηματισμού μιας χώρας σε αυτό το πλαίσιο, η οποία θα μπορούσε να βοηθήσει στην ενοποίηση της μελέτης των συνθηκών που σχετίζονται με την επιχειρηματικότητα και την καινοτομία. Ωστόσο, η εργασία δεν βρήκε σημαντική σχέση μεταξύ των επιπέδων απόδοσης των εταιρειών που μελετήθηκαν και του βαθμού ψηφιοποίησής τους λόγω της χαμηλής συμμετοχής του προσωπικού σε αυτά τα έργα. Το συμπέρασμα που προκύπτει από αυτήν την έρευνα είναι ότι ενώ οι επιχειρήσεις υιοθετούν περισσότερη τεχνολογία σε όλους τους τομείς, συμπεριλαμβανομένου του τραπεζικού, καθώς αυξάνει την ευελιξία και τις ευκαιρίες πωλήσεων ενώ μειώνει το κόστος που προκύπτει εσωτερικά, όπως ο χρόνος που αφιερώνεται στην επανεκπαίδευση εργαζομένων που μπορεί να μην έχουν εξοικειωθεί ακόμη ή να μην έχουν επαρκείς δεξιότητες. Είναι απαραίτητο επί του παρόντος, δεδομένων των ραγδαίων αλλαγών που συμβαίνουν παγκοσμίως, πρέπει να υπάρχει μεγαλύτερη συμμετοχή των εργαζομένων σε αυτά τα έργα, εάν πρόκειται να έχουν αντίκτυπο στα επίπεδα επιχειρηματικής απόδοσης. Ως εκ τούτου, οι δραστηριότητες θα πρέπει να επικεντρώνονται όχι μόνο στην υποστήριξη της ανθεκτικότητας των επιχειρήσεων έναντι των κινδύνων που σχετίζονται με απειλές για την ασφάλεια στον κυβερνοχώρο, αλλά και στην προώθηση καλύτερων προσόντων των εργαζομένων που απαιτούνται από πιο σύνθετα καθήκοντα που προκύπτουν από την αυτοματοποίηση των επιχειρηματικών διαδικασιών μέσω της υιοθέτησης τεχνολογίας σε όλους τους τομείς, συμπεριλαμβανομένων των τραπεζών, όπου αυξάνει την

ευελιξία και τις πωλήσεις ευκαιρίες, ενώ παράλληλα μειώνεται το κόστος που προκύπτει εσωτερικά, όπως ο χρόνος που αφιερώνεται στην επανεκπαίδευση των εργαζομένων.

Σε άλλη εργασία, οι Kuzior et al. [48] περιέγραψε τη σύγκλιση των διαδικασιών ψηφιοποίησης μεταξύ των χωρών με βάση παράγοντες όπως η χρήση του διαδικτύου, οι μετρήσεις της υποδομής και η πρόσβαση στις ΤΠΕ. Αυτή η μελέτη χρησιμοποίησε τον συντελεστή διακύμανσης για τον προσδιορισμό της σύγκλισης. Ανέπτυξε ένα οικονομετρικό μοντέλο που περιέγραψε τον αντίκτυπο των εθνικών επιπέδων κυβερνοασφάλειας, της ευκολίας επιχειρηματικής δραστηριότητας και των δεικτών κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες στην ψηφιακή ανάπτυξη. Αυτή η μελέτη είχε στόχο να κατανοήσει τους βασικούς καθοριστικούς παράγοντες που διαμορφώνουν τον κίνδυνο κατά τη χρήση χρηματοπιστωτικών μέσων για ξέπλυμα χρήματος και χρηματοδότηση της τρομοκρατίας σχετικά με τις παγκόσμιες τάσεις ψηφιοποίησης.

Επιπλέον, μια άλλη εργασία των Putri et al. [49] παρουσίασε ένα παράδειγμα χρησιμοποιώντας την αλλαγή από κατάλογο σε ψηφιοποίηση στην Ινδονησία. Χρησιμοποιήθηκαν προσεγγίσεις ποιοτικής έρευνας, όπως η εξέταση και η περιγραφή γεγονότων μέσω αλληλεπιδράσεων με άλλους, νοητικών εικόνων και αντιλήψεων. Αυτά συντάχθηκαν με βάση τη γνώμη του ευρύτερου κοινού για την ενθάρρυνση της χρήσης της ψηφιοποίησης στις δημόσιες επιχειρήσεις και υπηρεσίες και για την παρακολούθηση των τάσεων που παρατηρούνται από συνδεδεμένα μέρη, καθώς και για την ενθάρρυνση του κυβερνητικού τομέα να αναπτύξει υπηρεσίες και να αξιολογήσει την αποτελεσματικότητα των εννοιών χρησιμοποιώντας το six-ware πλαίσιο ασφάλειας στον κυβερνοχώρο (SWCSF) και Ηλεκτρονικό Κυβερνητικό Σύστημα (SPBE) που έχουν χρησιμοποιήσει πολλές κρατικές υπηρεσίες.

Επιπλέον, μια άλλη μελέτη από τον Shitta-Bey [50] έδειξε την επίδραση του ψηφιακού μετασχηματισμού μέσω του υπολογιστικού νέφους στον επιχειρηματικό μετασχηματισμό ανάλογα με τους παράγοντες απαιτήσεων που επιλέγουν οι οργανισμοί για δημοσίευση ή άλλα μοντέλα που διαφέρουν μεταξύ τους. Το μοντέλο και το πεδίο ελέγχου καθορίστηκαν μεταξύ των παρόχων υπηρεσιών cloud και των συνοδών καταναλωτών. Ως εκ τούτου, υπήρχαν κίνδυνοι για την ασφάλεια και ευρείες απειλές που συνδέονται με αυτό, καθώς και αύξηση του όγκου των εμπιστευτικών δεδομένων σε διαφορετικά περιβάλλοντα cloud, και αυτό αποτελεί σημαντική ανησυχία για τις εταιρείες που εξετάζουν το ενδεχόμενο μετασχηματισμού επιχειρήσεων χρησιμοποιώντας μια ποιοτική μέθοδο για να αποκτήσουν μια πλήρη αντίληψη του τάσεις και πρακτικές υπηρεσιών υπολογιστικού νέφους. Μεταξύ αυτών των απειλών για το περιβάλλον cloud, είτε από το εσωτερικό είτε από το εξωτερικό, όπως η διείσδυση δεδομένων, η απώλεια ή η διαρροή, οι κίνδυνοι μπορεί επίσης να περιλαμβάνουν αδυναμίες στην υποδομή ή ασφαλή πρόσβαση ή μπορεί να είναι άλλοι προορισμοί που είναι νεκροί χρησιμοποιώντας την εφαρμογή διεπαφή προγραμματισμού. Δεκαοκτώ απειλές εντοπίστηκαν σε αυτή τη μελέτη της πλήρους μετανάστευσης του νέφους. Για την αντιμετώπιση αυτών των κινδύνων ασφαλείας και τη λήψη μέτρων για τη μείωσή τους και τη δημιουργία στρατηγικών με χρήση κατάλληλου εξοπλισμού και διαδικασιών καταγραφής για την παρακολούθηση των κινδύνων, πρέπει να ληφθούν κατάλληλα μέτρα κατά τη μετάβαση ή τη μετάβαση στο cloud. Στο στρατηγικό σχέδιο περιλαμβάνονται πρωτόκολλα που καθορίζουν το εύρος της μετανάστευσης και προσδιορίζουν τις βασικές παραμέτρους και δείκτες απόδοσης.

Το ηλεκτρονικό εμπόριο είναι μια σημαντική εφαρμογή όπου ο ψηφιακός μετασχηματισμός έχει μεταμορφώσει τον επιχειρηματικό τομέα. Οι Trung et al. [51] ανέλυσε τις εφαρμογές του ψηφιακού μετασχηματισμού, της τεχνητής νοημοσύνης, του IoT και του blockchain στη διαχείριση εμπορικών μυστικών από την προοπτική SWOT. Οι συγγραφείς χρησιμοποίησαν ποιοτική ανάλυση, σύνθεση, επαγωγικές μεθόδους και στατιστικά δεδομένα για τη διεξαγωγή της έρευνάς τους. Διαπίστωσαν ότι αυτές οι τεχνολογίες προσφέρουν πολλά οφέλη, όπως αυξημένη αποτελεσματικότητα, διαφάνεια και ασφάλεια για τις επιχειρήσεις που τις υιοθετούν. Ωστόσο, υπάρχουν επίσης προκλήσεις που σχετίζονται με την εφαρμογή τους, όπως το υψηλό κόστος και η τεχνική πολυπλοκότητα, οι οποίες πρέπει να αντιμετωπιστούν από τους οργανισμούς προτού μπορέσουν να συνειδητοποιήσουν πλήρως τα πιθανά οφέλη. Συμπερασματικά, η εργασία τόνισε πώς θα μπορούσαν να εφαρμοστούν μαθηματικές λύσεις για βιομηχανικές χρήσεις μέσω μιας ανάλυσης SWOT της τεχνολογίας blockchain. Τόνισε πώς οι επιχειρήσεις θα πρέπει να εξετάσουν το ενδεχόμενο υιοθέτησης αυτών των τεχνολογιών ενώ γνωρίζουν τα πλεονεκτήματα και τους περιορισμούς τους για να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την αποτελεσματική εφαρμογή τους στις δραστηριότητές τους, ελαχιστοποιώντας ταυτόχρονα τους κινδύνους για την ασφάλεια στον κυβερνοχώρο στην εποχή του κλάδου 4.0 ή μετά.

Οι Gul et al. [52] ερεύνησαν τους ιστότοπους ηλεκτρονικού εμπορίου της Σαουδικής Αραβίας για να κατανοήσει τις αντιλήψεις για την ασφάλεια των πελατών χρησιμοποιώντας ως κύρια κριτήρια την αξιοπιστία, τις ανησυχίες σχετικά με τη χρήση πιστωτικών καρτών και τις αξιολογήσεις των καταναλωτών. Οι συγγραφείς διαπίστωσαν ότι οι ιστότοποι ηλεκτρονικού εμπορίου της Σαουδικής Αραβίας στερούνται εμπιστοσύνης των πελατών στο πλαίσιο της ασφάλειας και υπάρχει ανάγκη να ενισχυθούν τα χαρακτηριστικά ασφαλείας των ιστοσελίδων της Σαουδικής Αραβίας. Ομοίως, ο Saeed [5] διερεύνησε τη συμπεριφορά των χρηστών των πελατών ηλεκτρονικού εμπορίου στο Πακιστάν χρησιμοποιώντας τη θεωρία κινήτρων προστασίας ως θεωρητικό μοντέλο. Τα αποτελέσματα τόνισαν ότι τα συναισθήματα των πελατών, η αξιοπιστία, οι παράγοντες κινήτρων και οι ανησυχίες για τις πιστωτικές κάρτες επηρεάζουν την εμπιστοσύνη των πελατών κατά τη διάρκεια των διαδικτυακών αγορών.

4.5 Βιομηχανικός Τομέας

Το Industry 5.0 υποστηρίζει την καθιέρωση ευφυών συστημάτων παραγωγής, τα οποία απαιτούν το Διαδίκτυο των πραγμάτων με βάση την τεχνολογική εφαρμογή. Υπάρχουν πολλές τεχνολογικές εξελίξεις για την ασφάλεια των βιομηχανικών οργανισμών, όπως η αυτοματοποιημένη ανίχνευση επιθέσεων [53,54], τα αυτοματοποιημένα δωμάτια ελέγχου [55-57], η αρχιτεκτονική μηδενικής εμπιστοσύνης [58] και τα ψηφιακά δίδυμα [59]. Οι Osak και Buzina [60] διερεύνησαν τρόπους αξιολόγησης της ευελιξίας και της ασφάλειας των συστημάτων ισχύος υπό νέες συνθήκες που επιφέρει ο ψηφιακός μετασχηματισμός και οι αλλαγές στις βιομηχανικές πρακτικές, όπως η αύξηση των ανανεώσιμων πηγών ενέργειας και των ηλεκτρικών αυτοκινήτων. Οι συγγραφείς συζήτησαν αρχές για τον αυτόματο έλεγχο των συστημάτων ισχύος κατά τη διάρκεια του ψηφιακού μετασχηματισμού, ενώ εξέτασαν τις διαφορές μεταξύ των διαφόρων ηλεκτρικών εγκαταστάσεων.

Σε μια άλλη μελέτη, οι Mayhuasca και Sotelo [61] συνόψισαν πώς οι κβαντικές τεχνολογίες θα μπορούσαν να φέρουν επανάσταση σε διάφορες βιομηχανίες βελτιώνοντας τις δυνατότητες επεξεργασίας δεδομένων και ενισχύοντας την ασφάλεια έναντι των απειλών στον κυβερνοχώρο. Ωστόσο, οι συγγραφείς αναγνώρισαν ότι απαιτείται περαιτέρω έρευνα για να μπορέσουν αυτές οι τεχνολογίες να υιοθετηθούν ευρέως λόγω της πολυπλοκότητάς τους και του υψηλού κόστους που συνδέονται επί του παρόντος με αυτές. Συνολικά, οι συγγραφείς πρότειναν ότι η συνεχής εξερεύνηση στην κβαντική τεχνολογία πιθανότατα θα οδηγήσει σε καινοτομίες που θα μπορούσαν να μεταμορφώσουν την κοινωνία μας ακόμη περισσότερο από αυτό που έχουμε δει με τα παραδοσιακά συστήματα υπολογιστών.

Σε μια άλλη μελέτη, οι Raza et al. [62] διερεύνησαν πώς οι οργανισμοί εξισορροπούν την πρόληψη ζητημάτων ασφάλειας με την ανταπόκρισή τους σε έργα ψηφιακού μετασχηματισμού. Αυτή η έρευνα πιθανότατα παρουσιάζει πρωτότυπες γνώσεις σχετικά με τον τρόπο με τον οποίο οι οργανισμοί προσεγγίζουν τη διαχείριση της συμμόρφωσης με την ασφάλεια IS κατά τη διάρκεια πρωτοβουλιών ψηφιακού μετασχηματισμού. Αυτή η εργασία επικεντρώθηκε στον αυτοματισμό ρομποτικής διαδικασίας (RPA) στον ψηφιακό μετασχηματισμό και στον αντίκτυπό του στη συμμόρφωση με την ασφάλεια πληροφοριών. Ομοίως, οι Trung et al. [63] διερεύνησε πώς το IoT, η μηχανική μάθηση (ML), η τεχνητή νοημοσύνη και ο ψηφιακός μετασχηματισμός επηρεάζουν τις βιομηχανίες υπηρεσιών, όπως η εκπαίδευση, η ιατρική-νοσοκομεία, ο τουρισμός και οι τομείς της μεταποίησης. Οι συγγραφείς διαπίστωσαν ότι στον τομέα της εκπαίδευσης, το ML και το IoT έχουν επηρεάσει τις μεθόδους διδασκαλίας αξιολογώντας την απόδοση των μαθητών, κάτι που μπορεί να βοηθήσει τους δασκάλους να επιλέξουν κατάλληλες διαδρομές εξέλιξης σταδιοδρομίας για τους μαθητές. Στον τομέα της υγείας, η επεξεργασία δεδομένων δημόσιας υγείας είναι ταχύτερη με τα μεγάλα δεδομένα λόγω της τεχνολογίας ML που εφαρμόζεται. Με βάση τα ευρήματα της εμπειρικής έρευνας, οι συγγραφείς πρότειναν επιπτώσεις για μελλοντικές μελέτες σχετικά με τις εφαρμογές της μηχανικής μάθησης σε κάθε συγκεκριμένο τομέα. Τόνισαν επίσης τους κινδύνους για την ασφάλεια στον κυβερνοχώρο που συνδέονται με την εφαρμογή αυτών των τεχνολογιών που χρειάζονται λύσεις διαχείρισης. Αυτή η μελέτη έδειξε πώς οι αναδυόμενες τεχνολογίες όπως το IoT, η μηχανική μάθηση (ML) και η τεχνητή νοημοσύνη μεταμορφώνουν τις βιομηχανίες. Ωστόσο, ταυτόχρονα, τόνισε πιθανούς κινδύνους ασφάλειας που συνδέονται με αυτά, οι οποίοι χρήζουν προσοχής από ερευνητές και επαγγελματίες που εφαρμόζουν αυτά τα συστήματα στους οργανισμούς ή τις επιχειρήσεις τους.

4.6 Διαφορετικά οργανωτικά πλαίσια

Σε μια μελέτη, οι Di et al. [64] πρότεινε μια δικτυωμένη οργανωτική δομή για τη διαχείριση της ασφάλειας των πληροφοριών της επιχείρησης βασισμένη σε γενετικούς αλγόριθμους και ανέλυσε τα οφέλη της σε σύγκριση με τις παραδοσιακές προσεγγίσεις. Οι συγγραφείς εντόπισαν τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στη διαχείριση της ασφάλειας των πληροφοριών τους κατά τη διάρκεια των προσπαθειών ψηφιακού μετασχηματισμού, όπως κινδύνους από επιθέσεις στον κυβερνοχώρο και παραβιάσεις δεδομένων. Πρότειναν μια νέα προσέγγιση γενετικού αλγορίθμου για τη βελτίωση της αποδοτικότητας της εργασίας, τη μείωση του κόστους και τη διατήρηση ισχυρής ασφάλειας πληροφοριών. Τα πειράματά τους που συνέκριναν τις παραδοσιακές δομές οργάνωσης του δικτύου με εκείνες που βασίζονται σε γενετικούς αλγόριθμους διαπίστωσαν ότι ο τελευταίος ήταν πολύ πιο αποτελεσματικός όσον αφορά την αποδοτικότητα της εργασίας. Επιπλέον, παρείχαν δεδομένα που δείχνουν πλεονεκτήματα, όπως εξοικονόμηση κόστους και περιθώρια ανάπτυξης κατά την εφαρμογή αυτής της προσέγγισης στις επιχειρήσεις. Συνολικά, τα αποτελέσματα υποδεικνύουν ότι η χρήση μιας δικτυωμένης οργανωτικής δομής για τη διαχείριση της ασφάλειας πληροφοριών της επιχείρησης που βασίζεται σε ψηφιακούς μετασχηματισμούς και γενετικούς αλγόριθμους μπορεί να διατηρήσει αποτελεσματικά ισχυρή ασφάλεια πληροφοριών βελτιώνοντας παράλληλα την αποδοτικότητα εργασίας σε επιχειρήσεις που υφίστανται τεχνολογικές αλλαγές.

Ο Alenezi [65] εξέτασε τον ρόλο της μηχανικής λογισμικού στον ψηφιακό μετασχηματισμό και τη σημασία του για ασφαλείς πρακτικές ανάπτυξης. Οι συγγραφείς υποστήριξαν ότι η μηχανική λογισμικού έχει καταστεί απαραίτητη για τη διασφάλιση της αποτελεσματικής λειτουργίας καθώς οι οργανισμοί υιοθετούν όλο και περισσότερο ψηφιακές λύσεις για τη βελτίωση των λειτουργιών τους. Τόνισαν επίσης ότι οι ανησυχίες για την ασφάλεια είναι κρίσιμες κατά τη διάρκεια αυτής της διαδικασίας λόγω των αυξημένων απειλών στον κυβερνοχώρο. Αναλύοντας τις τάσεις στη μηχανική λογισμικού και εξετάζοντας περιπτωσιολογικές μελέτες από διάφορους κλάδους, όπως η υγειονομική περίθαλψη και η χρηματοδότηση, καταλήγουν στο συμπέρασμα ότι όλα τα ψηφιακά συστήματα βασίζονται σε λογισμικό για αποτελεσματική απόδοση, ενώ τονίζουν πώς οι ασφαλείς πρακτικές ανάπτυξης μπορούν να μετριάσουν τους κινδύνους που συνδέονται με την υιοθέτηση νέων τεχνολογιών.

Επιπλέον, σε άλλη εργασία, ο Marelli [66] συζήτησε πώς η ψηφιοποίηση και οι νέες τεχνολογίες γίνονται όλο και πιο σημαντικές στις ανθρωπιστικές επιχειρήσεις, καθιστώντας τους οργανισμούς ευάλωτους σε κυβερνοεπιθέσεις που μπορούν να επηρεάσουν την ικανότητά τους να προστατεύουν και να βοηθούν όσους πλήττονται από ένοπλες συγκρούσεις και βία.

Σε μια άλλη μελέτη, οι Dvojmoˇc και Verboten [67] τόνισαν ότι οι εργοδότες έχουν ορισμένες υποχρεώσεις για τη διασφάλιση της ασφάλειας των πληροφοριών των εργαζομένων, όπως η χρήση κατάλληλου υλικού και λογισμικού, η διαμόρφωση τείχη προστασίας και η εφαρμογή προγραμμάτων προστασίας από ιούς. Επιπλέον, τόνισαν την ανάγκη συμμόρφωσης των εταιρειών με διεθνή μέσα όπως ο GDPR όταν ασχολούνται με θέματα προστασίας προσωπικών δεδομένων που σχετίζονται με νέες τεχνολογίες που εφαρμόζονται.

Από την άλλη πλευρά, στον τομέα του περιβάλλοντος, οι Mukhlynina et al. [68] εξέτασε το πρόβλημα της εισαγωγής ψηφιακών τεχνολογιών στο σύστημα περιβαλλοντικής ασφάλειας και προστασίας στη Ρωσία. Οι συγγραφείς επικεντρώθηκαν στον ρόλο και τα συγκεκριμένα βήματα που γίνονται επί του παρόντος από τις κρατικές αρχές σε ομοσπονδιακό επίπεδο. Τόνισαν επίσης νομικά προβλήματα που υπάρχουν σε αυτό το πλαίσιο. Τα λεπτομερή ευρήματα πρότειναν αρκετές προκλήσεις που σχετίζονται με την εφαρμογή προσπαθειών ψηφιακού μετασχηματισμού που σχετίζονται με την περιβαλλοντική ασφάλεια στη Ρωσία. Αυτά περιελάμβαναν έλλειψη σαφών κανονιστικών πλαισίων, ανεπαρκή χρηματοδότηση για δραστηριότητες έρευνας και ανάπτυξης, ανεπαρκή υποστήριξη υποδομών και περιορισμένη ευαισθητοποίηση του κοινού σχετικά με αυτά τα ζητήματα. Όσον αφορά τα αποτελέσματα, με βάση την ανάλυσή τους χρησιμοποιώντας τη μέθοδο της παραγοντικής ανάλυσης, εντόπισαν ζωτικούς παράγοντες που επηρεάζουν τις προσπάθειες ψηφιοποίησης, όπως η τεχνολογική ετοιμότητα, η διαθεσιμότητα ειδικευμένου εργατικού δυναμικού, οι κυβερνητικές πολιτικές και κανονισμοί κ.λπ., οι οποίοι μπορούν να χρησιμοποιηθούν από τους υπεύθυνους χάραξης πολιτικής κατά το σχεδιασμό στρατηγικές για την επίτευξη βιώσιμων περιβαλλοντικών στόχων μέσω της ψηφιοποίησης. Επιπλέον, οι Halabi et al. υποστήριξε πράσινες πρακτικές κυβερνοασφάλειας για εξοικονόμηση ενέργειας [69].

Ο Voskresenskaya [70] διερεύνησε την τρέχουσα κατάσταση του ψηφιακού μετασχηματισμού στη διακυβέρνηση, την οικονομία και τους κοινωνικούς τομείς ως παράγοντα ανάπτυξης και ασφάλειας. Οι ερευνητές διαπίστωσαν ότι η ψηφιοποίηση έχει γίνει αναπόσπαστο μέρος της σύγχρονης κοινωνίας.

Προσδιόρισαν ζωτικά χαρακτηριστικά όπως ο μηχανισμός μετατροπής της οικονομικής συνεργασίας σε χώρο πληροφοριών/τηλεπικοινωνιών, η ενεργή εισαγωγή/εφαρμογή του ηλεκτρονικού χρήματος/έξυπνων συμβάσεων στις αστικές συναλλαγές και η ανάπτυξη της ηλεκτρονικής διακυβέρνησης. Σημείωσαν επίσης ότι προβλήματα σε αυτούς τους τομείς θα μπορούσαν να επηρεάσουν τη συμβατότητα με άλλες οικονομίες λόγω καθυστερήσεων στις δυνατότητες επεξεργασίας δεδομένων ή της αδυναμίας αποτελεσματικής χρήσης ψηφιακών πόρων. Με βάση την ανάλυσή τους χρησιμοποιώντας τόσο ποιοτικές (νόμους/κανονισμούς) όσο και ποσοτικές (στατιστικές/συγκριτικές) μεθόδους σε εθνικό/διεθνές επίπεδο, κατέληξαν στο συμπέρασμα ότι υπάρχουν σημαντικά οφέλη που συνδέονται με την υιοθέτηση της ψηφιοποίησης σε διάφορους τομείς, συμπεριλαμβανομένης της αυξημένης αποτελεσματικότητας / παραγωγικότητας στις διαδικασίες παροχής υπηρεσιών , που τελικά οδηγεί σε βιώσιμη ανάπτυξη/ασφάλεια.

Συμπερασματικά, προτάθηκε στις κυβερνήσεις να δώσουν προτεραιότητα στις επενδύσεις σε υποδομές που είναι απαραίτητες για την αποτελεσματική εφαρμογή/υιοθέτηση νέων τεχνολογιών, διασφαλίζοντας παράλληλα την ύπαρξη επαρκών κανονιστικών πλαισίων/πολιτικών για την υποστήριξη της καινοτομίας χωρίς να διακυβεύονται τα δικαιώματα ιδιωτικής ζωής/προστασίας δεδομένων των πολιτών. Επιπλέον, δεδομένου του γρήγορου ρυθμού των αλλαγών, οι επιχειρήσεις πρέπει να προσαρμοστούν γρήγορα για να παραμείνουν ανταγωνιστικές. Σε μια άλλη μελέτη, οι Kuchumov et al. [71] πρότεινε ότι ενώ υπάρχουν πιθανά οφέλη από τις πρωτοβουλίες ψηφιοποίησης, όπως η αυξημένη αποδοτικότητα και τα κέρδη παραγωγικότητας, ενέχονται σημαντικοί κίνδυνοι, όπως απειλές για την ασφάλεια στον κυβερνοχώρο ή εκτόπιση θέσεων εργασίας λόγω αυτοματοποίησης. Επιπλέον, ο αντίκτυπος αυτών των πρωτοβουλιών ποικίλλει ανάλογα με τις περιφερειακές πολιτικές για την ψηφιοποίηση. Συμπερασματικά, αυτό το έγγραφο τόνισε ότι είναι σημαντικό οι υπεύθυνοι χάραξης πολιτικής στις περιοχές της Ρωσίας να εξετάζουν τα πιθανά οφέλη και να αξιολογούν προσεκτικά τις πιθανές αρνητικές επιπτώσεις κατά την εφαρμογή στρατηγικών ψηφιακού μετασχηματισμού. Με αυτόν τον τρόπο, μπορούν να αναπτύξουν επαρκείς δημόσιες πολιτικές που βασίζονται σε συστημικές αναλύσεις που λαμβάνουν υπόψη και τα δύο θετικά αποτελέσματα μαζί με σοβαρούς παράγοντες κινδύνου που επηρεάζουν την περαιτέρω ανάπτυξη σε κάθε περιοχή ξεχωριστά αντί να εφαρμόζουν ενιαίες λύσεις σε όλους τους τομείς αδιακρίτως χωρίς να λαμβάνεται υπόψη τοπικές συνθήκες ή ιδιαιτερότητες των αναγκών, οι οποίες θα μπορούσαν να οδηγήσουν σε ακούσιες συνέπειες εάν δεν αντιμετωπιστούν επαρκώς εκ των προτέρων μέσω προσεκτικών διαδικασιών σχεδιασμού με τη συμμετοχή ενδιαφερομένων σε διαφορετικά επίπεδα (τοπικές κοινότητες/επιχειρήσεις/κυβερνητικές υπηρεσίες).

Ο Alahmadi et al. [72] τόνισε ότι η ψηφιακή γεωργία βοήθησε στην αυτοματοποίηση θέσεων εργασίας υψηλής έντασης εργασίας. Ωστόσο, πολλές απειλές και τρίτα σημεία συνδέονται με την ψηφιακή γεωργία. Τόνισαν τις πιθανές επιθέσεις πλευρικού καναλιού που σχετίζονται με τον ψηφιακό μετασχηματισμό. Ομοίως, οι Song et al. [73] τόνισε ότι το Διαδίκτυο των πραγμάτων και τα δίκτυα 5G έχουν μεγάλη ανάπτυξη της ψηφιακής γεωργίας. Ωστόσο, η δημοσίευση μεγάλου όγκου δεδομένων είναι επιρρεπής σε ανησυχίες για την ασφάλεια. Ως αποτέλεσμα, οι συγγραφείς προτείνουν ένα σύστημα συγκέντρωσης δεδομένων διατήρησης της ιδιωτικής ζωής που είναι πιο ασφαλείς και ευέλικτο.

Ο Gonçalves [74] τόνισε ότι ο ψηφιακός μετασχηματισμός στον λογιστικό τομέα των μικρομεσαίων επιχειρήσεων βρίσκεται στα αρχικά του στάδια. Ωστόσο, τα οφέλη αναγνωρίζονται ευρέως. Η προστασία δεδομένων και οι απειλές για την ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας προκλήσεις που πρέπει να αντιμετωπιστούν από επαγγελματίες λογιστές. Σε μια άλλη μελέτη, οι Tiron-Tudor et al. [75] τόνισε ότι οι τεχνολογίες τεχνητής νοημοσύνης, blockchain και GPS μπορούν να βοηθήσουν τα λογιστικά τμήματα των εταιρειών να εφαρμόσουν συστήματα ελέγχου σε πραγματικό χρόνο. Ωστόσο, οι εταιρείες πρέπει να διαθέσουν σημαντικούς πόρους για τον μετριασμό των κινδύνων στον κυβερνοχώρο που συνδέονται με τις προηγμένες τεχνολογίες.

Οι Rodríguez-Abitia και Bribiesca-Correa [76] τόνισαν το γεγονός ότι οι τεχνολογικές εξελίξεις, όπως η τεχνητή νοημοσύνη, το Διαδίκτυο των πραγμάτων, το blockchain, η τρισδιάστατη εκτύπωση και η ασφαλής τεχνική υποδομή, θα αλλάξουν επίσης τα πανεπιστήμια. Ο καθένας μπορεί να υιοθετήσει έναν νέο ρόλο, όπως παραγωγός περιεχομένου, επιρροή κ.λπ., για να συνεισφέρει στον τομέα της εκπαίδευσης. Ομοίως, η Pavlova [77] τόνισε ότι η κουλτούρα βασίζεται συνήθως στην ελεύθερη και ανοιχτή ανταλλαγή γνώσεων σε ένα εκπαιδευτικό περιβάλλον. Ωστόσο, οι απειλές για την ασφάλεια απαιτούν ισορροπία μεταξύ διαφάνειας και μηχανισμών ασφάλειας. Ο Πίνακας 1 παρέχει μια περίληψη όλης της βιβλιογραφίας που συζητήθηκε.

Τα συστήματα ισχύος είναι πολύπλοκες υποδομές στη σύγχρονη κοινωνία και είναι ευάλωτα σε απειλές για την ασφάλεια στον κυβερνοχώρο [78,79]. Ο Νταγκούμας [80] χρησιμοποίησε το σύστημα ισχύος IEEE RTS 96 και ο συγγραφέας τόνισε ότι ένας συνδυασμός συνθηκών λειτουργίας και κυβερνοεπιθέσεων θα πρέπει να χρησιμοποιηθεί για την αξιολόγηση της σταθερότητας του συστήματος. Οι Diaba et al. [81] τόνισε ότι τα πρωτόκολλα επικοινωνίας του συστήματος ισχύος είναι επιρρεπή σε επιθέσεις στον κυβερνοχώρο από χάκερ. Οι συγγραφείς έχουν προτείνει έναν αλγόριθμο που ξεπερνά τις συμβατικές προσεγγίσεις βαθιάς μάθησης χρησιμοποιώντας SVM, ANN και CNN. Ομοίως, οι Presekal et al. [82] ανέπτυξε ένα υβριδικό μοντέλο μηχανικής μάθησης χρησιμοποιώντας Graph Convolutional Long-Short-Term Memory (GC-LSTM) και ένα βαθύ συνελικτικό δίκτυο για ανίχνευση ανωμαλιών σε δίκτυα ηλεκτρικής ενέργειας.

Ο Κεχαγιάς κ.ά. [83] τόνισε ότι η κυβερνοασφάλεια στη ναυτιλιακή βιομηχανία έχει γίνει πολύ σημαντική. Οι συγγραφείς παρουσίασαν μια λεπτομερή περίπτωση του τρόπου με τον οποίο μια ναυτιλιακή εταιρεία υιοθέτησε μια συστηματική προσέγγιση για την αναθεώρηση των στρατηγικών πολιτικών της στον κυβερνοχώρο, εντόπισε κενά και στη συνέχεια πραγματοποίησε τον μετριασμό του κινδύνου.

Πίνακας 1 Βασικά ευρήματα της βιβλιογραφίας

Έγγραφο	Τομέας εφαρμογής	Βασικές Τεχνολογίες / Θεωρίες	Σημαντικά ευρήματα
[22]	Χρηματοοικονομικός τομέας	Τεχνητή νοημοσύνη, γνωστική χαρτογράφηση, τεχνικές DEMATEL	Παροχή μοντέλου υποστήριξης αποφάσεων συνδυάζοντας τη μέθοδο λήψης αποφάσεων δοκιμής και εργαστηρίου αξιολόγησης (DEMATEL) και τη γνωστική χαρτογράφηση.
[23]		Γνωστικές τεχνολογίες	Παρείχε οδηγίες για τη χρήση γνωστικών τεχνολογιών στον ψηφιακό μετασχηματισμό της ρωσικής οικονομίας.
[24]		Τεχνητή νοημοσύνη, blockchain, τεχνολογία που βασίζεται στη φωνή ή επεξεργασία φυσικής γλώσσας	Υψηλότερη εμπιστοσύνη στη Fintech από τους ενδιαφερόμενους στον χρηματοπιστωτικό τομέα.
[25]	Δημόσια ιδρύματα, χρηματοπιστωτικά ιδρύματα, τραπεζικά ιδρύματα, βιομηχανία, μεταφορές και γεωργία	Διαφορετικές τεχνολογίες που σχετίζονται με την ψηφιοποίηση	Επισήμανση της ανάγκης για ασφάλεια πληροφοριών σε διαφορετικούς τομείς εφαρμογών.
[34]	Τομέας Υγείας	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Η βιωσιμότητα του ψηφιακού μετασχηματισμού στον τομέα της υγειονομικής περίθαλψης απαιτεί δεξιότητες κυβερνοασφάλειας, διαχείριση αβεβαιότητας και αλληλεξάρτηση του τομέα της υγειονομικής

			περίθαλψης.
[35]		Ηλεκτρονικά αρχεία υγείας, απομακρυσμένη παρακολούθηση ασθενών, τεχνητή νοημοσύνη, τηλεϊατρική και ομοσπονδιακή μάθηση	Προτάσεις απορρήτου και ασφάλειας για τον τομέα της υγείας.
[36]		Οι εφαρμογές για smartphone και τα φορετά προϊόντα τεχνολογίας επιτρέπουν την κοινή χρήση δεδομένων	Ανάγκη απορρήτου δεδομένων ασθενών σε εφαρμογές υγειονομικής περίθαλψης.
[37]		Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Ανάγκη για ενισχυμένη ασφάλεια στον κυβερνοχώρο στον ψηφιακό μετασχηματισμό μετά τον COVID-19.
[41]	Κυβερνητικός τομέας	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Σύσταση για χρήση ασφαλούς δικτύου από το υπουργείο στην Παλαιστίνη
[42]		Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Καθιέρωση σαφών πολιτικών ανταλλαγής δεδομένων και σαφείς περιγραφές θέσεων εργασίας για υπαλλήλους πληροφορικής.
[43]	Πληρωμές κρατικών φόρων	Πλήρης υπηρεσία εφαρμογών για κινητά και κανάλι ηλεκτρονικών πληρωμών	Ανάγκη για ενέργειες για να καταστεί η διαδικασία διαφανής και νόμιμη στην πληρωμή φόρων στη Δανία.
[44]	Κυβερνητικές και άλλες δημόσιες υπηρεσίες	AI και άλλες κορυφαίες τεχνολογίες	Δίνει έμφαση στη διακυβέρνηση της κυβερνοασφάλειας.
[45]	Κυβερνητική υποδομή ζωτικής σημασίας	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Δίνει έμφαση στην κυβερνοασφάλεια των υποδομών ζωτικής σημασίας.
[47]	Επαγγελματικός τομέας	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία.	Δίνει έμφαση στις κρατικές ρυθμίσεις για τον μετασχηματισμό των οικονομικών clusters σε διεθνές επίπεδο.
[48]		Η προηγμένη κρυπτογράφηση και η ανάλυση δεδομένων είναι απαραίτητα για την ασφάλεια στον	Ανάλυσε τις καταστάσεις ψηφιακού μετασχηματισμού και ασφάλειας στον κυβερνοχώρο σε διάφορες χώρες

		κυβερνοχώρο και την αποτελεσματικότητα της AML	
[49]		Η προηγμένη κρυπτογράφηση και η ανάλυση δεδομένων του επιχειρηματικού τομέα είναι απαραίτητα για την ασφάλεια στον κυβερνοχώρο και την αποτελεσματικότητα της AML	Ψηφιακός μετασχηματισμός στην Ινδονησία και πλαίσιο ασφάλειας στον κυβερνοχώρο έξι λογισμικών.
[50]		Ασφάλεια πληροφορικής και προστασία δεδομένων, μετεγκατάσταση cloud, υπολογιστικό νέφος	Ανησυχίες για την ασφάλεια για τον μετασχηματισμό των επιχειρήσεων στο cloud.
[51]		Blockchain, IoT, AI και άλλες αναδυόμενες τεχνολογίες	Ανάλυση SWOT του blockchain και άλλων τεχνολογιών.
[52]	Ηλεκτρονικό εμπόριο	Αξιοπιστία, ανησυχίες σχετικά με τη χρήση πιστωτικών καρτών, αξιολόγηση καταναλωτή	Αντίληψη ασφάλειας πληροφοριών χρήστη σε εφαρμογές ηλεκτρονικού εμπορίου της Σαουδικής Αραβίας.
[5]		Θεωρία κινήτρων προστασίας	Αντίληψη ασφάλειας πληροφοριών χρήστη για το ηλεκτρονικό εμπόριο στο Πακιστάν.
[60]	Βιομηχανικός τομέας	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Επιπτώσεις στην ασφάλεια των μικρών σταθμών ηλεκτροπαραγωγής.
[61]		Συζητούνται οι κβαντικοί υπολογιστές, η κρυπτογραφία, οι οπτικές ίνες και οι σχετικές τεχνολογίες	Επιπτώσεις στην ασφάλεια των πληροφοριών στις κβαντικές τεχνολογίες.
[62]		Ρομποτική Αυτοματοποίηση Διαδικασιών (RPA)	Συμμόρφωση με την ασφάλεια του συστήματος πληροφοριών και συνέπειες απόκρισης.
[63]	Βιομηχανία υπηρεσιών	IoT, μηχανική μάθηση, AI και ψηφιακός μετασχηματισμός	Επιπτώσεις της κυβερνοασφάλειας του IoT, της μηχανικής μάθησης και του ψηφιακού μετασχηματισμού.
[64]	Δικτυωμένη οργανωτική δομή	Γενετικοί αλγόριθμοι	Παράγοντες που επηρεάζουν την ποιότητα

			στις συνθήκες παραγωγής.
[65]	Εργασιακό περιβάλλον	Υπολογιστικό νέφος	Τονίζει τη σημασία της ασφαλούς ανάπτυξης λογισμικού στον ψηφιακό μετασχηματισμό.
[66]	Επιχειρήσεις	Κινητές συσκευές, cloud computing, πλατφόρμες μέσων κοινωνικής δικτύωσης	Επιπτώσεις της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό των ανθρωπιστικών οργανώσεων.
[67]	Εργασιακό περιβάλλον	Τείχη προστασίας, λογισμικό κρυπτογράφησης, συστήματα ανίχνευσης εισβολών	Δίνει έμφαση στην ασφάλεια δεδομένων των δεδομένων των εργαζομένων σε οργανισμούς.
[68]	το περιβάλλον	Δεν επικεντρώνεται σε συγκεκριμένη τεχνολογία	Ψηφιακός μετασχηματισμός και περιβαλλοντική ασφάλεια στη Ρωσία
[69]		IoT	Πράσινο IoT και προσαρμοστικές επιπτώσεις στον κυβερνοχώρο.
[70]	Διακυβέρνηση, οικονομία και κοινωνικοί τομείς	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Ψηφιακός μετασχηματισμός και ασφάλεια στη Ρωσία.
[71]	Οικονομία	Δεν αναφέρθηκε συγκεκριμένη τεχνολογία	Οικονομική ασφάλεια και ψηφιακός μετασχηματισμός στη Ρωσία.
[72]	Ψηφιακή γεωργία	Έξυπνοι αισθητήρες, Διαδίκτυο των πραγμάτων, μηχανική μάθηση	Επιθέσεις πλευρικών καναλιών στην ψηφιακή γεωργία.
[73]	Ψηφιακή γεωργία	Internet of Things, δίκτυα 5G	Σύστημα συγκέντρωσης δεδομένων για τη διατήρηση του απορρήτου.
[74]	Ψηφιακή λογιστική	Ρομποτική, προγραμματισμός πόρων επιχειρήσεων, τεχνητή νοημοσύνη, οπτική αναγνώριση χαρακτήρων	Ψηφιακός μετασχηματισμός και μέλλον της λογιστικής.
[75]	Ψηφιακή λογιστική	AI, blockchain, υπολογιστικό νέφος	Έμφαση στα οφέλη για τις λογιστικές εταιρείες στον ψηφιακό μετασχηματισμό.
[76]	Εκπαίδευση	Τεχνητή νοημοσύνη, Διαδίκτυο των πραγμάτων, blockchain, τρισδιάστατη εκτύπωση, ασφάλεια στον	Φουτουριστικά πανεπιστήμια στην εποχή του ψηφιακού μετασχηματισμού.

		κυβερνοχώρο, μεγάλα δεδομένα	
[77]		Δεν επικεντρώνεται σε συγκεκριμένη τεχνολογία	Έμφαση στην κουλτούρα της κυβερνοασφάλειας στα πανεπιστήμια.

5 Συζήτηση

Ο Πίνακας 1 υπογραμμίζει ότι οι προηγμένες τεχνολογίες όπως τα δίκτυα IoT [51,53], blockchain [63,74] και 5G [84,85] μπορούν να διευκολύνουν τους οργανισμούς να διασφαλίσουν τις επιχειρηματικές διαδικασίες και να τις καταστήσουν αποτελεσματικές [1,2]. Επιπλέον, οι προσεγγίσεις μηχανικής μάθησης [63,72,86] μπορούν να βοηθήσουν στον εντοπισμό κακόβουλης κίνησης στο δίκτυο, κάτι που μπορεί να βοηθήσει στον προληπτικό εντοπισμό απειλών στον κυβερνοχώρο. Ωστόσο, τέτοιες τεχνολογικές παρεμβάσεις θα πρέπει να είναι καλά μελετημένες και κατάλληλα σχεδιασμένες [9]. Ενώ οι νέες τεχνολογίες μπορούν να αυξήσουν την αποτελεσματικότητα και την ανταγωνιστικότητα των επιχειρήσεων, ενέχουν επίσης άγνωστους κινδύνους, όπως οι επιθέσεις στον κυβερνοχώρο [3]. Αυτό τους αφήνει ευάλωτους σε απειλές στον κυβερνοχώρο, οι οποίες θα μπορούσαν να έχουν σημαντικές οικονομικές συνέπειες. Ως εκ τούτου, είναι απαραίτητη η ευαισθητοποίηση των επαγγελματιών του κλάδου σχετικά με αυτούς τους κινδύνους.

Επιπλέον, θα πρέπει να υπάρχουν εύλογα μέτρα ασφαλείας για την προστασία των τεχνολογικών υποδομών από επιθέσεις στον κυβερνοχώρο [87]. Μια θεμελιώδης στρατηγική ασφάλειας θα μπορούσε να βοηθήσει τους οργανισμούς από επαναλαμβανόμενες επιθέσεις στον κυβερνοχώρο [88]. Ως εκ τούτου, είναι σημαντικό να αναλυθούν οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο κατά τη μετάβαση στην ψηφιακή οικονομία [89]. Οι κυβερνήσεις έχουν εκτεταμένο ρόλο στην ανάπτυξη και εφαρμογή πολιτικής σε εθνικό επίπεδο. Για παράδειγμα, η καθιέρωση μιας εθνικής στρατηγικής για την κυβερνοασφάλεια βοήθησε την Ελλάδα να επιδιώξει τον ψηφιακό μετασχηματισμό [90]. Θα πρέπει επίσης να ληφθεί υπόψη ότι ενώ στοχεύουμε στον ψηφιακό μετασχηματισμό, θα πρέπει να ληφθούν υπόψη και οι ανθρώπινοι παράγοντες. Η υποβάθμιση της ανθρώπινης απόδοσης είναι ένας κρίσιμος παράγοντας στις επιθέσεις στον κυβερνοχώρο [91].

Στη βιβλιογραφία, ορισμένα άρθρα ανασκόπησης έχουν επικεντρωθεί στον ψηφιακό μετασχηματισμό, όπως ένα άρθρο των Metawa et al. [92], η οποία διερεύνησε τον ρόλο της πληροφορίας στον ψηφιακό μετασχηματισμό στο πλαίσιο των αιγυπτιακών μικρομεσαίων επιχειρήσεων. Ομοίως, ο Özsungur [93] ερεύνησε την επιχειρηματική στρατηγική για την ασφάλεια στον κυβερνοχώρο στον ψηφιακό μετασχηματισμό και ο Nguyen Duc [94] τεκμηρίωσε τον κίνδυνο ασφάλειας από μηχανολογική άποψη. Επιπλέον, οι Hai et al. [1] τόνισε τις ευκαιρίες και τις προκλήσεις για τις αναδυόμενες χώρες σχετικά με τον ψηφιακό μετασχηματισμό και το έργο του Kour [95] επικεντρώθηκε στις επιπτώσεις της κυβερνοασφάλειας στον τομέα των σιδηροδρόμων. Παρά αυτές τις έρευνες στη βιβλιογραφία, καμία έρευνα δεν έχει παρουσιάσει ταξινόμηση τομέα και εξέτασε τις επιπτώσεις της κυβερνοασφάλειας σε διάφορους κλάδους, όπως έχει διερευνηθεί σε αυτό το έγγραφο. Με βάση την ανασκόπησή μας, προτείνουμε ένα πλαίσιο ετοιμότητας για την κυβερνοασφάλεια για επιχειρηματικούς οργανισμούς που επιδιώκουν ψηφιακό μετασχηματισμό, όπως φαίνεται παρακάτω:

Ad hoc: Δεν υπάρχει συγκεκριμένος μηχανισμός σχεδιασμού, προετοιμασίας, ανάπτυξης και επιτήρησης κυβερνοασφάλειας. Ίσως υπάρχουν περιστασιακές πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο.

Βασικό: Αναλαμβάνονται σποραδικές πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο. Ωστόσο, υπάρχει έλλειψη σχεδιασμού και οι βέλτιστες στρατηγικές ασφάλειας στον κυβερνοχώρο δεν στοχεύουν.

Προγραμματισμένος: Υπάρχει κατάλληλος σχεδιασμός, σχεδιασμός και διαδικασίες δοκιμών για τη συστηματική εφαρμογή της στρατηγικής κυβερνοασφάλειας του οργανισμού.

Βελτιστοποιημένο: οι δραστηριότητες κυβερνοασφάλειας μετρώνται ποσοτικά ως προς την αποτελεσματικότητα και η συνεχής βελτίωση στοχεύει στην υιοθέτηση βέλτιστων λύσεων.

Σε ad hoc επίπεδο, οι οργανισμοί δεν διαθέτουν μηχανισμούς σχεδιασμού, προετοιμασίας, ανάπτυξης και επιτήρησης για να ανταποκριθούν σε απειλές για την ασφάλεια στον κυβερνοχώρο. Η ανθεκτικότητα στην ασφάλεια στον κυβερνοχώρο εξαρτάται από τις προσωπικές πρωτοβουλίες των εργαζομένων. Οι

αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη, τα μεγάλα δεδομένα και τα αναλυτικά στοιχεία, το blockchain, το cloud computing και οι υπηρεσίες οδηγούν τον ψηφιακό μετασχηματισμό παγκοσμίως ενώ αυξάνουν τους κινδύνους για την ασφάλεια στον κυβερνοχώρο για τις επιχειρήσεις που υποβάλλονται σε αυτήν τη διαδικασία. Ως εκ τούτου, είναι ζωτικής σημασίας να αναλύονται τα μέτρα κυβερνοασφάλειας κατά την εφαρμογή τους για την επιδίωξη του ψηφιακού μετασχηματισμού, αλλά οι οργανισμοί σε αυτό το επίπεδο δεν εστιάζουν σε αυτές τις πτυχές.

Στο βασικό επίπεδο του πλαισίου μας, οι οργανισμοί διαθέτουν ουσιαστικές δραστηριότητες προγραμματισμού, προετοιμασίας, ανάπτυξης και επιτήρησης στον κυβερνοχώρο, αλλά δεν έχουν οργανωτική στρατηγική στρατηγική σχετικά με την ασφάλεια στον κυβερνοχώρο. Οι διαδικασίες δεν είναι ώριμες και γίνονται μεμονωμένες προσπάθειες. Δεν υπάρχουν διαθέσιμα δεδομένα σχετικά με την αποτελεσματικότητα των προσεγγίσεων που εφαρμόζονται στον κυβερνοχώρο.

Στο προγραμματισμένο επίπεδο του πλαισίου μας, οι οργανισμοί χρειάζονται μια καλά σχεδιασμένη οργανωτική στρατηγική κυβερνοασφάλειας που θα τεκμηριώνει τις διαδικασίες για την προετοιμασία, την ανάπτυξη και την επιτήρηση της κυβερνοασφάλειας. Κατά τη φάση της επιτήρησης, τα πιθανά τρωτά σημεία πρέπει να αξιολογούνται τακτικά μέσω δοκιμής διείσδυσης ή σάρωσης ευπάθειας. Επιπλέον, είναι σημαντικό για τους οργανισμούς που υφίστανται ψηφιακό μετασχηματισμό να λαμβάνουν υπόψη τον ανθρώπινο παράγοντα στην ασφάλεια στον κυβερνοχώρο. Αυτό σημαίνει την παροχή τακτικών προγραμμάτων εκπαίδευσης και ευαισθητοποίησης για τους υπαλλήλους ώστε να εντοπίζουν και να ανταποκρίνονται κατάλληλα σε πιθανές απειλές στον κυβερνοχώρο. Επιπλέον, καθώς η τεχνολογία προχωρά με ταχείς ρυθμούς, πιθανότατα θα προκύψουν νέοι κίνδυνοι ασφάλειας που δεν έχουν ακόμη κατανοηθεί πλήρως ή δεν αντιμετωπίζονται από τα τρέχοντα μέτρα ασφαλείας. Θα είναι ζωτικής σημασίας για τις επιχειρήσεις που υποβάλλονται σε ψηφιακό μετασχηματισμό που περιλαμβάνει συσκευές IoT ή άλλες αναδυόμενες τεχνολογίες όπως τα δίκτυα 5G ή ο κβαντικός υπολογιστής να δώσουν προτεραιότητα σε ολοκληρωμένες εκτιμήσεις κινδύνου πριν εφαρμόσουν τέτοιες λύσεις. Οι οργανισμοί που στοχεύουν σε ένα βελτιστοποιημένο επίπεδο πρέπει να μετρούν συνεχώς την αποτελεσματικότητα των μηχανισμών σχεδιασμού, προετοιμασίας, ανάπτυξης και επιτήρησής τους στον τομέα της κυβερνοασφάλειας. Καθώς η τεχνολογία εξελίσσεται ταχέως και εμφανίζονται συνεχώς νέες απειλές στον κυβερνοχώρο, μπορεί να προκύψουν τρωτά σημεία ακόμη και με ισχυρά μέτρα ασφαλείας. Ως εκ τούτου, είναι απαραίτητο για τους οργανισμούς που υποβάλλονται σε ψηφιακό μετασχηματισμό να πραγματοποιούν φουτουριστικές τεχνολογικές προβλέψεις και σχετικό σχεδιασμό κυβερνοασφάλειας να καινοτομούν συνεχώς τις διαδικασίες τους. Μια προληπτική προσέγγιση για βελτιστοποιημένες διαδικασίες ασφαλείας μπορεί να βοηθήσει στον μετριασμό των μελλοντικών κινδύνων που σχετίζονται με τις προσπάθειες ψηφιακού μετασχηματισμού.

6 Συμπεράσματα

Αυτή η συστηματική βιβλιογραφική ανασκόπηση έχει ρίξει φως στον κρίσιμο ρόλο της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό. Ο ψηφιακός μετασχηματισμός έχει μεταμορφώσει τον επιχειρηματικό τομέα με τη μετάβαση των οργανωτικών διαδικασιών σε λύσεις πληροφορικής, με αποτέλεσμα σημαντικές αλλαγές σε διάφορες πτυχές ενός οργανισμού. Επηρεάζει πολλαπλά στοιχεία, όπως εμπειρία χρήστη, λειτουργίες, αγορές, πελάτες, σχέσεις και πολιτισμικές διαφορές. Οι αναδυόμενες τεχνολογίες, συμπεριλαμβανομένης της τεχνητής νοημοσύνης (AI), των μεγάλων δεδομένων και των αναλυτικών στοιχείων, της τεχνολογίας blockchain, του υπολογιστικού νέφους και των υπηρεσιών, οδηγούν τον ψηφιακό μετασχηματισμό παγκοσμίως ενώ αυξάνουν τους κινδύνους για την ασφάλεια στον κυβερνοχώρο για τις επιχειρήσεις που υποβάλλονται σε αυτήν τη διαδικασία. Και οι επιπτώσεις της κυβερνοασφάλειας στον ψηφιακό μετασχηματισμό είναι σημαντικές. Καθώς οι επιχειρήσεις υποβάλλονται σε διαδικασία ψηφιακού μετασχηματισμού, γίνονται πιο ευάλωτες σε κυβερνοεπιθέσεις και παραβιάσεις ασφάλειας. Η κυβερνοασφάλεια είναι ένα ουσιαστικό συστατικό του ψηφιακού μετασχηματισμού, καθώς βοηθά στην αποφυγή διακοπών λόγω κακόβουλων δραστηριοτήτων ή μη εξουσιοδοτημένης πρόσβασης από εισβολείς που στοχεύουν στην αλλαγή, καταστροφή ή εκβιασμό ευαίσθητων πληροφοριών από τους χρήστες. Η πανδημία του COVID-19 έχει επισημάνει περαιτέρω τη σημασία της κυβερνοασφάλειας στην εφαρμογή του ψηφιακού μετασχηματισμού, καθώς οι κυβερνοεγκληματίες έχουν εκμεταλλευτεί τις ευπάθειες που δημιουργούνται από αυτή την ταχεία στροφή προς την ψηφιοποίηση. Ως εκ τούτου, οι οργανισμοί που υπόκεινται σε υιοθέτηση ψηφιακού μετασχηματισμού πρέπει να δώσουν προτεραιότητα

στα μέτρα κυβερνοασφάλειας για να εξασφαλίσουν μια επιτυχημένη μετάβαση χωρίς διακοπές που προκαλούνται από παραβιάσεις της ασφάλειας. Η μελέτη υπογραμμίζει ότι ο ψηφιακός μετασχηματισμός είναι μια σύνθετη και συνεχής διαδικασία που απαιτεί από τους οργανισμούς να γνωρίζουν τις αναδυόμενες τεχνολογίες και τους σχετικούς κινδύνους ασφάλειας. Καθώς οι επιχειρήσεις μεταβαίνουν τις κύριες δραστηριότητές τους σε λύσεις πληροφορικής, πρέπει να διασφαλίσουν ότι υπάρχουν κατάλληλα μέτρα για την προστασία των δεδομένων και των δικτύων από μη εξουσιοδοτημένη πρόσβαση ή κακόβουλες δραστηριότητες. Τα ευρήματα υποδηλώνουν ότι η εφαρμογή ασφαλιστηρίων συμβολαίων κρυπτογράφησης ή κυβερνοασφάλισης μπορεί να βοηθήσει στον μετριασμό αυτών των κινδύνων κατά την εφαρμογή του ψηφιακού μετασχηματισμού. Για μελλοντικές μελέτες, συνιστούμε τη σημασία των οργανισμών να έχουν ολοκληρωμένη γνώση των απειλών για την ασφάλεια στον κυβερνοχώρο σε όλη τη διαδικασία. Αυτό περιλαμβάνει τον εντοπισμό πιθανών τρωτών σημείων από νωρίς και την προληπτική αντιμετώπισή τους.

7 Προτάσεις

Αυτή η μελέτη αναφέρει την κυβερνοασφάλεια σε εφαρμογές ψηφιακού μετασχηματισμού. Με βάση τα αποτελέσματα αυτής της μελέτης, παρουσιάζονται ορισμένες ερευνητικές κατευθύνσεις που αφορούν την ασφάλεια στον κυβερνοχώρο. Η κυβερνοασφάλεια είναι καλά τοποθετημένη στη βιβλιογραφία και διάφορες πτυχές της έχουν διερευνηθεί σε διάφορες εφαρμογές της τεχνολογίας. Ωστόσο, εξακολουθεί να απαιτείται ένα σαφές πλαίσιο κυβερνοασφάλειας στη διαδικασία ψηφιακού μετασχηματισμού και το μεγαλύτερο μέρος της βιβλιογραφίας διερεύνησε λίγες πτυχές του ψηφιακού μετασχηματισμού, ενώ δεν τηρήθηκε ένα περιεκτικό πλαίσιο ψηφιακού μετασχηματισμού. Επομένως, η μελλοντική έρευνα πρέπει να αναπτύξει ολοκληρωμένες και ποσοτικοποιήσιμες κατευθυντήριες γραμμές για να καλυφθεί αυτό το κενό στη βιβλιογραφία.

Βιβλιογραφία

1. Hai, T.N.; Van, Q.N.; Thi Tuyet, M.N. Digital transformation: Opportunities and challenges for leaders in the emerging countries in response to COVID-19 pandemic. Emerg. Sci. J. 2021, 5, 21–36.

2. Möller, D. Cybersecurity in Digital Transformation: Scope and Applications; Springer: Berlin/Heidelberg, Germany, 2020.

3. Matt, C.; Hess, T.; Benlian, A. Digital transformation strategies. Bus. Inf. Syst. Eng. 2015, 57, 339–343.

4. Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability 2023, 15, 6019.

5. Saeed, S. A Customer-Centric View of E-Commerce Security and Privacy. Appl. Sci. 2023, 13, 1020.

6. Sharif, M.H.U.; Mohammed, M.A. A literature review of financial losses statistics for cyber security and future trend. World J. Adv. Res. Rev. 2022, 15, 138–156.

7. Haislip, J.; Kolev, K.; Pinsker, R.; Steffen, T. The economic cost of cybersecurity breaches: A broad-based analysis. In Proceedings of the Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019; Volume 1, p. 37.

8. Garg, V. Covenants without the Sword: Market Incentives for Cybersecurity Investment. In Proceedings of the TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Virtual, 22–24 September 2021.

9. Lee, I. Cybersecurity: Risk management framework and investment cost analysis. Bus. Horiz. 2021, 64, 659–671.

10. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. J. Cybersecur. 2020, 6, tyaa005.

11. Krutilla, K.; Alexeev, A.; Jardine, E.; Good, D. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model. Risk Anal. 2021, 41, 1795–1808.

12. Simon, J.; Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. Eur. J. Oper. Res. 2020, 282, 161–171.

13. Uddin, M.H.; Ali, M.H.; Hassan, M.K. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Manag. 2020, 22, 239–309.

14. Curti, F.; Ivanov, I.; Macchiavelli, M.; Zimmermann, T. City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. The Financial Costs of Lax Cybersecurity. Available online: https://ssrn.com/abstract=4465071.

15. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, n71. [PubMed]

16. Al-Alawi, A.I.; Al-Bassam MS, A. The significance of cybersecurity system in helping managing risk in banking and financial sector. J. Xidian Univ. 2020, 14, 1523–1536.

17. Hasan, M.F.; Al-Ramadan, N.S. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. Soc. Sci. Humanit. J. 2021, 5, 2312–2323.

18. Joveda, N.; Khan, M.T.; Pathak, A.; Chattogram, B. Cyber laundering: A threat to banking industries in Bangladesh: In quest of effective legal framework and cyber security of financial information. Int. J. Econ. Financ. 2019, 11, 54–65.

19. Almudaires, F.; Almaiah, M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 732–738.

20. Smith, K.J.; Dhillon, G. Assessing blockchain potential for improving the cybersecurity of financial transactions. Manag. Financ. 2020, 46, 833–848.

21. Kuzmenko, O.; Kubálek, J.; Bozhenko, V.; Kushneryov, O.; Vida, I. An approach to managing innovation to protect financial sector against cybercrime. Pol. J. Manag. Stud. 2021, 24, 276–291.

22. Rodrigues, A.R.D.; Ferreira, F.A.; Teixeira, F.J.; Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Res. Int. Bus. Financ. 2022, 60, 101616.

23. Fedorov, B.M.; Fedorova, S.V.; Zhang, H.; Mamedova, N.A. Using Cognitive Technologies to Ensure the Information Security of Banks in the Conditions of Digital Transformation and Development of Biometrical Identification. WSEAS Trans. Bus. Econ. 2023, 20, 382–387.

24. Patil, R.; Bharathi, S.V. A Study on the Business Transformation, Security issues and Investors Trust in Fintech Innovation. Cardiometry 2022, 24, 918–932.

25. Rãƒdulescu, C.V.; Bodislav, D.A.; Negescu, M.D.O. The Risks of Digitization in the Context of Economic Development and of Ensuring Social and Informational Security. In Proceedings of the International Management Conference, Poznan, Poland, 27–29 June 2019; Faculty of Management, Academy of Economic Studies: Bucharest, Romania, 2019; Volume 13, pp. 1040–1050.

26. Mijwil, M.; Aljanabi, M.; Ali, A.H. Chatgpt: Exploring the role of cybersecurity in the protection of medical information. Mesopotamian J. Cybersecur. 2023, 2023, 18–21.

27. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber attacks on healthcare devices using unmanned aerial vehicles. J. Med. Syst. 2020, 44, 29.

28. Buzdugan, A. Integration of cyber security in healthcare equipment. In Proceedings of the 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, Chisinau, Moldova, 18–21 September 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 681–684.

29. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of medical things. Health Policy Technol. 2021, 10, 100549.

30. Abie, H. Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.

31. Loi, M.; Christen, M.; Kleine, N.; Weber, K. Cybersecurity in health–disentangling value tensions. J. Inf. Commun. Ethics Soc. 2019, 17, 229–245.

32. Ali, K.A.; Alyounis, S. Cybersecurity in healthcare industry. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 695–701.

33. Abbas HS, M.; Qaisar, Z.H.; Ali, G.; Alturise, F.; Alkhalifah, T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PLoS ONE 2022, 17, e0274550. [PubMed]

34. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. Technovation 2023, 121, 102583.

35. Paul, M.; Maglaras, L.; Ferrag, M.A.; AlMomani, I. Digitization of Healthcare Sector: A Study on Privacy and Security Concerns. ICT Express 2023, in press.

36. Nwaiwu, F.; Mbelu, S. Digital Transformation in Healthcare and Surveillance Capitalism: Comparative Assessment of Data and Privacy Protection Compliance across the European Union (5 July 2020). Available online: https://ssrn.com/abstract=3643838.

37. Maleh, Y.; Mellal, B. Digital transformation and cybersecurity in the context of COVID-19 proliferation. IEEE Technol. Policy Ethics 2021, 6, 1–4.

38. Shaheen, K.; Zolait, A.H. The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. Inf. Comput. Secur. 2023. ahead-of-print.

39. Montasari, R. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity; Springer Nature: Berlin/Heidelberg, Germany, 2023; pp. 7–25.

40. Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. Smart Cities 2023, 6, 1523–1544.

41. Al Shobaki, M.J.; El Talla, S.A.; Al Najjar, M.T. Digital Transformation and Its Impact on the Application of Cyber Security in the Ministry of Interior and National Security in Palestine. 2022. Available online: http://www.moi.gov.ps.

42. Al Najjar, M.T.; Al Shobaki, M.J.; El Talla, S.A. The Reality of Digital Transformation in the Palestinian Ministry of Interior and National Security. 2022. Available online: www.ijeais.org/ijamsr.

43. Fjord, L.B.; Schmidt, P.K. The Digital Transformation of Tax Systems: Progress, Pitfalls and Protection in a Danish Context. 2022. Available online: https://ssrn.com/abstract=4252832.

44. Mijwil, M.; Filali, Y.; Aljanabi, M.; Bounabi, M.; Al-Shahwani, H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. Mesopotamian J. Cybersecur. 2023, 2023, 1–6.

45. Maglaras, L.; Kantzavelou, I.; Ferrag, M.A. Digital Transformation and Cybersecurity of Critical Infrastructures. Appl. Sci. 2021, 11, 8357.

46. Bokhari, S.; Hamrioui, S.; Aider, M. Cybersecurity strategy under uncertainties for an IoE environment. J. Netw. Comput. Appl. 2022, 205, 103426.

47. Gonchar, V. The Transformation of Entrepreneurial Activity in the Conditions of the Development of the Digital Economy and a Methodology of Assessing Its Digital Security in Digital Technologies in the Contemporary Economy: Collective Monograph; Simanavi˘ciene, Ž., Ed.; ˙ Mykolas Romeris University Research: Vilnius, Lithuania, 2022; ISBN 9786094880506.

48. Kuzior, A.; Vasylieva, T.; Kuzmenko, O.; Koibichuk, V.; Brozek, P. Global Digital Convergence: Impact of Cybersecurity, Business ˙ Transparency, Economic Transformation, and AML Efficiency. J. Open Innov. Technol. Mark. Complex. 2022, 8, 195.

49. Putri MS, D.; Gultom, R.A.; Wadjdi, A.F. The Concept of an Electronic-Based Government System and the Six-Ware Cyber Security Framework in Supporting the Digitization of the Indonesian Government. Def. Secur. Stud. 2023, 4, 1–7.

50. Shitta-Bey, A.M. Security Concerns of Cloud Migration and Its Implications on Cloud-Enabled Business Transformation Effect of Quality Education on Poverty Alleviation View Project. Master's Thesis, Università della Svizzera Italiana, Lugano, Switzerland, 2023. Available online: https://www.researchgate.net/publication/369118961.

51. Trung, N.D.; Huy DT, N.; Van Thanh, T.; Thanh NT, P.; Dung, N.T.; Thanh Huong, L.T. Digital transformation, AI applications and IoT in Blockchain managing commerce secrets: And cybersecurity risk solutions in the era of industry 4.0 and further. Webology 2021, 18, 10–14704.

52. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. Electronics 2022, 11, 293.

53. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J. Inf. Secur. Appl. 2021, 58, 102717.

54. Meeran, Y.A.; Shyry, S.P. Resilient Detection of Cyber Attacks in Industrial Devices. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 564–569.

55. Ameri, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Design of a novel information system for semi-automated management of cybersecurity in industrial control systems. ACM Trans. Manag. Inf. Syst. 2023, 14, 1–35.

56. Buja, A.; Apostolova, M.; Luma, A. Enhancing Cyber Security in Industrial Internet of Things Systems: An Experimental Assessment. In Proceedings of the 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 14 June 2023; pp. 1–5.

57. Ramirez, R.; Chang, C.K.; Liang, S.H. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. Electronics 2023, 12, 1195.

58. Zanasi, C.; Russo, S.; Colajanni, M. Flexible Zero Trust Architecture for the Cybersecurity of Industrial Iot Infrastructures. Available online: https://ssrn.com/abstract=4481853.

59. Jacopo, P.; Graziana, C.; Federica, P.; Giarrè, L. Using Digital Twin to Detect Cyber-Attacks in Industrial Control Systems. In Proceedings of the IEEE Proceedings of 2023 EUROCON, Torino, Italy, 6–8 July 2023.

60. Osak, A.; Buzina, E. Flexibility and security of power systems, methods of analysis, and criteria for their evaluation in the conditions of digital transformation of the power industry. AIP Conf. Proc. 2023, 2552, 040008.

61. Mayhuasca, J.; Sotelo, S. Quantum Technologies for Digital Transformation and Informatica Security. Int. J. Eng. Sci. 2022, 15, 43–50.

62. Raza, H.; Baptista, J.; Constantinides, P. Conceptualizing the Role of IS Security Compliance in Projects of Digital Transformation: Tensions and Shifts between Prevention and Response Modes; ICIS: Houston, TX, USA, 2019.

63. Trung, N.D.; Huy DT, N.; Le, T.H. IoT, machine learning (ML), AI and digital transformation affects various industries-principles and cybersecurity risks solutions. Management 2021, 18, 10–14704.

64. Di, Z.; Liu, Y.; Li, S. Networked Organizational Structure of Enterprise Information Security Management Based on Digital Transformation and Genetic Algorithm. Front. Public Health 2022, 10, 921632.

65. Alenezi, M. Software and Security Engineering in Digital Transformation. arXiv 2021, arXiv:2201.01359. 66. Marelli, M. Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation. Int. Rev. Red Cross 2020, 102, 367–387.

67. Dvojmoˇc, M.; Verboten, M.T. Cyber (In) security of Personal Data and Information in Times of Digitization. Med. Law Soc. 2022, 15, 287–304.

68. Zarapina, L.; Mukhlynina, M.; Adamenko, A.; Mukhlynin, D.; Belokopytova, N. Issues of Legal Support of Socio-economic Policy and Environmental Security of Russia in the Context of Digital Transformation. In Proceedings of the International Scientific-Practical Conference “Ensuring the Stability and Security of Socio-Economic Systems: Overcoming the Threats of the Crisis Space” (SES 2021), Kirov, Russia, 17–18 June 2021; Sciete Press: Kirov, Russia, 2021; pp. 336–340, ISBN 978-989-758-546-3.

69. Halabi, T.; Bellaiche, M.; Fung, B.C. Towards Adaptive Cybersecurity for Green IoT. In Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 24–26 November 2022; pp. 64–69.

70. Voskresenskaya, E.; Vorona-Slivinskaya, L.; Panov, S. Digital transformation of social sector as the factor of development and security of the country. In E3S Web of Conferences; EDP Sciences: Les Ulis, France, 2019; Volume 135, p. 03075.

71. Kuchumov, A.; Pecherictsa, E.; Chaikovskaya, A.; Zhilyaeva, I. Digital transformation in the concept of economic security of Russia and its regions. In Proceedings of the 2nd International Scientific Conference on Innovations in Digital Economy, St. Petersburg, Russia, 22–23 October 2020; pp. 1–8.

72. Alahmadi, A.N.; Rehman, S.U.; Alhazmi, H.S.; Glynn, D.G.; Shoaib, H.; Solé, P. Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. Sensors 2022, 22, 3520.

73. Song, J.; Zhong, Q.; Wang, W.; Su, C.; Tan, Z.; Liu, Y. FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sens. J. 2020, 21, 17430–17438.

74. Gonçalves, M.J.A.; da Silva, A.C.F.; Ferreira, C.G. The Future of Accounting: How Will Digital Transformation Impact the Sector? Informatics 2022, 9, 19.

75. Tiron-Tudor, A.; Dont,u, A.N.; Bresfelean, V.P. Emerging Technologies' Contribution to the Digital Transformation in Accountancy Firms. Electronics 2022, 11, 3818.

76. Rodríguez-Abitia, G.; Bribiesca-Correa, G. Assessing digital transformation in universities. Future Internet 2021, 13, 52.

77. Pavlova, E. Enhancing the organisational culture related to cyber security during the university digital transformation. Inf. Secur. 2020, 46, 239–249.

78. Ribas Monteiro, L.F.; Rodrigues, Y.R.; Zambroni de Souza, A.C. Cybersecurity in Cyber–Physical Power Systems. Energies 2023, 16, 4556.

79. Liang, J.; Zhu, H.; Zhang, B.; Liu, L.; Liu, X.; Lin, H.; Tian, J.; Chen, Q. Research and Prospect of Cyber-Attacks Prediction Technology for New Power Systems. In Proceedings of the 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 24–26 February 2023; Volume 6, pp. 638–647.

80. Dagoumas, A. Assessing the impact of cybersecurity attacks on power systems. Energies 2019, 12, 725.

81. Diaba, S.Y.; Shafie-Khah, M.; Elmusrati, M. Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms. IEEE Access 2023, 11, 18660–18672.

82. Presekal, A.; ¸Stefanov, A.; Rajkumar, V.S.; Palensky, P. Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Trans. Smart Grid 2023. Early Access.

83. Kechagias, E.P.; Chatzistelios, G.; Papadopoulos, G.A.; Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. Int. J. Crit. Infrastruct. Prot. 2022, 37, 100526.

84. Khashan, O.A.; Alamri, S.; Alomoush, W.; Alsmadi, M.K.; Atawneh, S.; Mir, U. Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. Comput. Mater. Contin. 2023, 75, 3133–3158.

85. Sufyan, A.; Khan, K.B.; Khashan, O.A.; Mir, T.; Mir, U. From 5G to beyond 5G: A Comprehensive Survey of Wireless Network Evolution, Challenges, and Promising Technologies. Electronics 2023, 12, 2200.

86. Al-Taleb, N.; Saqib, N.A. Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. Appl. Sci. 2022, 12, 1863. 87. Sandhu, K. Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges. In Handbook of Research on Advancing Cybersecurity for Digital Transformation; IGI Global: Hershey, PA, USA, 2021; pp. 1–17.

88. Azizi, N.; Haass, O. Cybersecurity Issues and Challenges. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications; IGI Global: Hershey, PA, USA, 2023; pp. 21–48.

89. Lesmana, D.; Afifuddin, M.; Adriyanto, A. Challenges and Cybersecurity Threats in Digital Economic Transformation. Int. J. Humanit. Educ. Soc. Sci. 2023, 2.

90. Maglaras, L.; Drivas, G.; Chouliaras, N.; Boiten, E.; Lambrinoudakis, C.; Ioannidis, S. Cybersecurity in the era of digital transformation: The case of Greece. In Proceedings of the 2020 International Conference

on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, 27–29 November 2020; pp. 1–5.

91. Nobles, C. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA–J. Bus. Public Adm. 2022, 13, 49–72.

92. Metawa, N.; Elhoseny, M.; Mutawea, M. The role of information systems for digital transformation in the private sector: A review of Egyptian SMEs. Afr. J. Econ. Manag. Stud. 2022, 13, 468–479.

93. Özsungur, F. Business Management and Strategy in Cybersecurity for Digital Transformation. In Handbook of Research on Advancing Cybersecurity for Digital Transformation; IGI Global: Hershey, PA, USA, 2021; pp. 144–162.

94. Nguyen Duc, A.; Chirumamilla, A. Identifying security risks of digital transformation-an engineering perspective. In Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, 18–20 September 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 677–688.

95. Kour, R.; Patwardhan, A.; Thaduri, A.; Karim, R. A review on cybersecurity in railways. Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit 2023, 237, 3–20.