Π.Μ.Σ. ΣΤΙΣ ΔΙΕΘΝΕΙΣ ΣΠΟΥΔΕΣ ΤΟΥ ΤΜΗΜΑΤΟΣ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ ΤΡΟΥΠΚΟΥ ΑΝΤΩΝΙΟΥ

Α.Μ.: MAD21037

ΘΕΜΑ: «Παγκόσμια Πολιτική Οικονομία του Κυβερνο-εγκλήματος στα πλαίσια της πανδημίας Covid-19: Η περιπτωσιολογική μελέτη της «Κυβερνο-Βιοασφάλειας(Cyber-Biosecurity)».

ΘΕΣΣΑΛΟΝΙΚΗ, ΜΑΪΟΣ 2023

«*Δηλώνω υπευθύνως ότι όλα τα στοιχεία σε αυτήν την εργασία τα απέκτησα, τα επεξεργάστηκα και τα παρουσιάζω σύμφωνα με τους κανόνες και τις αρχές της ακαδημαϊκής δεοντολογίας, καθώς και τους νόμους που διέπουν την έρευνα και την πνευματική ιδιοκτησία. Δηλώνω επίσης υπευθύνως ότι όπως απαιτείται από αυτούς τους κανόνες, αναφέρομαι και παραπέμπω στις πηγές όλων των στοιχείων που χρησιμοποιώ και τα όποια δεν συνιστούν πρωτότυπη δημιουργία μου*» .

-Ο-
ΔΗΛΩΝ
ΤΡΟΥΠΚΟΣ ΑΝΤΩΝΙΟΣ

Ευχαριστίες

Ένα ενδιαφέρον ταξιδί από το οποίο αποκόμισα γνώσεις, απέκτησα νέα επιστημονικά ενδιαφέροντα και είχα την τιμή να γνωρίσω αξιόλογους καθηγητές και ανθρώπους έφτασε στο τέλος του. Τελευταίος σταθμός αυτού του ταξιδιού της γνώσης και της συμμετοχής μου στο μεταπτυχιακό πρόγραμμα σπουδών «Διεθνείς Σπουδές» του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Μακεδονίας, είναι η εκπόνηση της διπλωματικής μου εργασίας.

Θα ήθελα ευχαριστήσω τον καθηγητή μου και επιβλέποντα στην παρούσα διπλωματική εργασία, κ. Αθανάσιο Μποζίνη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, για την επιστημονική και συμβουλευτική καθοδήγηση και τις εύστοχες και εποικοδομητικές παρατηρήσεις του. Η πρωτοποριακή επιστημονική του ενασχόληση με τα θέματα των ψηφιακών διεθνών σχέσεων, της βιοασφάλειας και των υδριβικών και νέων παγκόσμιων απειλών, αποτέλεσε το εφαλτήριο για την συνεργασία μας. Έχοντας ως πυξίδα την παρούσα αγαστή συνεργασία και το κοινό μας επιστημονικό ενδιαφέρον ευελπιστώ και σε μελλοντική μας συνεργασία.

Τέλος θα ήθελα να εκφράσω τις ευχαριστίες μου στην σύζυγο μου και στους γονείς μου για την στήριξή τους σε όλη την διαδρομή μου μέχρι σήμερα.

Περίληψη

Αντικείμενο της εργασίας είναι να αναδείξει την σημασία της κυβερνοβιοασφάλειας και να καταδείξει τα κενά της στους διάφορους τομείς που εμπεριέχεται. Προκειμένου να γίνει κατανοητός ο όρος της κυβερνοβιοασφάλειας, η εργασία αρχικά θα αναλύσει στο πρώτο κεφάλαιο το κυβερνοέγκλημα και τις κατηγορίες των κυβενροεγκλημάτων. Στο δεύτερο κεφάλαιο θα αναλυθεί η βιοασφάλεια και οι κατηγορίες των βιολογικών απειλών. Στην συνέχεια, στο τρίτο κεφάλαιο, θα γίνει αναφορά στον όρο την κυβερνοβιοασφάλειας και την σημασία της, η οποία αναδείχθηκε στην περίοδο της πανδημίας του COVID-19. Ακολούθως, θα αναπτυχθούν τα κενά στο τομέα της κυβερνοβιασφάλειας σε διάφορους τομείς, όπως στα νοσηλευτικά ιδρύματα, στα βιοφαρμακευτικά προϊόντα, την γεωργία και σε εθνικό και διακρατικό επίπεδο, ενώ θα γίνει αναφορά και στο νομικό πλαίσιο προστασίας των βιολογικών δεδομένων σε διεθνές και εθνικό επίπεδο. Στο επόμενο κεφάλαιο θα γίνει αναλυτική επεξήγηση της κυβερνοβιοασφάλειας στις βάσεις δεδομένων που αφορούν το ανθρώπινο γονιδίωμα (dna), τα είδη των κυβερνοεπιθέσων που μπορούν να δεχτούν, τις απειλές που διατρέχουν και την συμβολή που είχαν στην αντιμετώπιση της πανδημίας του COVID-19, ενώ παράλληλα θα γίνει μια περιληπτική παράθεση του σημαντικότερων βάσεων δεδομένων ανθρώπινου γονιδιώματος (dna) σε παγκόσμιο επίπεδο. Στο πέμπτο και τελευταίο κεφάλαιο θα αναλυθεί το επίπεδο της κυβερνοβιοασφάλειας στα εργαστήρια προηγμένης τεχνολογίας και οι προκλήσεις που θα θέσει η χρήση της τεχνητής νοημοσύνης στα εργαστήρια αυτά, όσο αναφορά την κυβερνοβιοασφάλεια. Τέλος θα παρατεθούν οι προτάσεις για την βελτίωση και την ενίσχυση του επιπέδου της κυβερνοβιοασφάλειας.

Λέξεις κλειδιά: κυβερνοασφάλεια, βιοασφάλεια, κυβερνοβιοασφάλεια, κυβερνοέγκλημα.

Abstract

The purpose of this thesis is to demonstrate the importance of cyber-biosecurity and to highlight its gaps in the various areas it includes. In order to understand the term cyber-security, the paper will initially analyze in the first chapter cybercrime and the categories of cybercrimes. In the second chapter, biosecurity and the categories of biological threats will be analyzed. Then, in the third chapter, reference will be made to the term cyber-biosecurity and its importance, which emerged during the period of the COVID-19 pandemic. Next, cybersecurity gaps will be developed in various sectors, such as healthcare, biopharmaceuticals, agriculture, and at national and transnational level, while reference will also be made to the legal framework for the protection of biological data at international and domestic level. In the next chapter, there will be a detailed explanation of cyber-biosecurity in databases related to the human genome (dna), the types of cyber-attacks they can face up, the threats they face, the contribution they had in dealing with the COVID-19 pandemic, while at the same time will be a summary statement of the most important human genome (dna) databases at global level. In the fifth and last chapter, the level of cyberbiosecurity in advanced technology laboratories and the challenges posed by the use of artificial intelligence in these laboratories will be analyzed, as far as cybersecurity is concerned. Finally, the proposals for improving and strengthening the level of cybersecurity will be listed.

Key words: cybersecurity, biosecurity, cyberbiosecurity, cybercrime.

Περιεχόμενα

ΣΕΛΙΔΑ

Εισαγωγή

Δεν υπάρχει αμφιβολία ότι έχουμε εισέλθει σε μια περίοδο ψηφιακού μετασχηματισμού σε όλες τις πτυχές και τις εκφάνσεις της ύπαρξής μας. «Ο ψηφιακός μετασχηματισμός είναι η αλλαγή που συνδέεται με την εφαρμογή των ψηφιακών τεχνολογιών σε όλες τις πτυχές της ανθρώπινης προσπάθειας» (Shelly Palmer 2018). Μέσω αυτού του μετασχηματισμού, η τεχνολογία έχει γίνει μια θεμελιώδης πτυχή της ζωής μας. Η τεχνολογία αγγίζει τώρα όλα όσα έχουν σημασία στον κόσμο μας και όλα τα σημαντικά έχουν πλέον ένα στοιχείο στον κυβερνοχώρο. Είναι κοινώς αποδεκτό ότι η αποδοτικότητα και η παραγωγικότητά μας αυξάνονται σημαντικά όταν οι συσκευές και τα συστήματα είναι δικτυωμένα και συνδεδεμένα στο διαδίκτυο. Αυτή η αποτελεσματικότητα, με τη σειρά της, επιταχύνει τον ρυθμό της ανατρεπτικής καινοτομίας. « Ο κυβερνοχώρος σε μεγάλο βαθμό μετουσιώνει την έννοια της παγκοσμιοποίησης και συγκροτεί ένα τεράστιο πεδίο δράσης το οποίο βιώνει μια άμεση διασυνδεσιμότητα αλλά παράλληλα είναι και ένας πολιτικά κατακερματισμένος χώρος που αντανακλά τις ετερογένειες του διεθνούς συστήματος. Ο κυβερνοχώρος συνιστά ένα παγκόσμιο ψηφιακό περιβάλλον που ρυθμίζει την καθημερινότητά μας, αλλά στερείται ενός κοινά αποδεκτού συστήματος δικυβέρνησης…ο υπερεθνικός του χαρακτήρας θέτει σε αμφισβήτηση μια σειρά από έννοιες όπως η ισχύς, η κυριαρχία, ασφάλεια και η διακυβέρνηση» (Λιαρόπουλος Α. και Μποζίνης Α. (Επιμ.), 2022).

Παρά λοιπόν το τεράστιο όφελος, η τεχνολογία και ο κυβερνοχώρος παρουσιάζουν σημαντικές ευπάθειες ασφαλείας στον τομέα των βιοεπιστημών, οι οποίες αναδείχθηκαν με την πανδημία του Covid-19. Αυτά τα τρωτά σημεία πρέπει να αντιμετωπιστούν αποτελεσματικά για να αποφευχθεί η υπαρξιακή απειλή, οι κίνδυνοι για την εθνική ασφάλεια, τη δημόσια υγεία και τις επιχειρήσεις.

1. Κυβερνοέγκλημα (cybercrime):

Δεν υπάρχει ένας σαφής ορισμός του. Σύμφωνα με το Συμβούλιο της Ευρώπης, κυβερνοέγκλημα είναι κάθε αδίκημα κατά συστημάτων ηλεκτρονικών υπολογιστών αλλά και κάθε αδίκημα μέσω συστημάτων ηλεκτρονικών υπολογιστών (COE:Cybercrime). Για την Ευρωπαϊκή Ένωση το κυβερνοέγκλημα συνίσταται σε εγκληματικές πράξεις που διαπράττονται στο διαδίκτυο με τη χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών (EU: Cybercrime). Τα χαρακτηριστικά του κυβερνοεγκλήματος είναι τα εξής:

- Ευκολία για την διάπραξή του καθώς μπορεί να πραγματοποιηθεί από οπουδήποτε και απαιτεί την διασύνδεση του δράστη με μια συσκευή στο διαδίκτυο.
- Για την διάπραξή του απαιτούνται ειδικές γνώσεις.
- Αμεσότητα και ταχύτητα, παρέχει την δυνατότητα γρήγορης τέλεσης του, χωρίς την μετακίνηση του δράστη.
- Παρέχει την δυνατότητα συγκάλυψης και χρήσης ψευδών στοιχείων από δράστη.
- Έχει διασυνοριακό χαρακτήρα.
- Η έρευνα και η εξιχνίαση του από τις διωκτικές αρχές απαιτεί χρόνο, καθώς στην πλειοψηφία των περιπτώσεων χρειάζεται συνεργασία φορέων από τουλάχιστον δύο κράτη.
- Η εγκληματικότητα στον κυβερνοχώρο δεν μπορεί να καταγραφεί με ακρίβεια καθώς υπάρχουν περιπτώσεις εγκλημάτων του κυβερνοχώρου που δεν καταγγέλλονται.

Κυβερνοασφάλεια: Είναι άρρηκτα συνδεδεμένη με το κυβερνοέγκλημα και ουσιαστικά αποτελεί το μέσο για την καταπολέμησή του. Τυποποιημένος ορισμός της κυβερνοασφάλειας δεν υπάρχει, αλλά ο όρος αυτός καλύπτει «το σύνολο των διασφαλίσεων και των μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών και των χρηστών τους έναντι μη εξουσιοδοτημένης πρόσβασης, επιθέσεων και ζημίας, ώστε να εξασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων. Η κυβερνοασφάλεια δεν καλύπτει μόνο την ασφάλεια δικτύων και πληροφοριών, αλλά και κάθε παράνομη

δραστηριότητα με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο» (ECA.EU: Cybersecurity).

Οι έννοιες της κυβερνοεπίθεσης και του κυβερνοπόλεμου και της κυβερνοτρομοκρατίας.

Κυβερνοεπίθεση (cyber attack): «Είναι μια επίθεση, μέσω του κυβερνοχώρου, με σκοπό τη διακοπή, την απενεργοποίηση, την καταστροφή ή τον κακόβουλο έλεγχο ενός υπολογιστικού περιβάλλοντος/υποδομής ή την καταστροφή της ακεραιότητας των δεδομένων ή την κλοπή ελεγχόμενων πληροφοριών. (NIST: cyber attack).

Κυβερνοπόλεμος (cyber warfare): «Είναι η χρήση κυβερνοεπιθέσεων στον κυβερνοχώρο από ένα κράτος εναντίον εχθρικού κράτους, προκειμένου να προκληθεί ζημιά ή/και διαταραχές σε ζωτικής σημασίας σε συστήματα υπολογιστών και έχει ως στόχο την κατασκοπεία, την δολιοφθορά, την προπαγάνδα, την χειραγώγηση ή τον οικονομικό πόλεμο.

Κυβερνοτρομοκρατία (cyberterrorism): Είναι μια εγκληματική ενέργεια που διαπράττεται μέσω της χρήσης του κυβερνοχώρου ή των πληροφοριακών συστημάτων που χρησιμοποιούν οι συσκευές τεχνολογίας από μια τρομοκρατική οργάνωση ή για τρομοκρατικό σκοπό. Το Γραφείο του ΟΗΕ για την Αντιτρομοκρατία (UNOCT) έχει αρκετές πρωτοβουλίες στον τομέα των νέων τεχνολογιών, συμπεριλαμβανομένου ενός προγράμματος για τη χρήση των μέσων κοινωνικής δικτύωσης και τη συλλογή πληροφοριών ανοιχτού κώδικα και ψηφιακών στοιχείων για την καταπολέμηση της τρομοκρατίας και του βίαιου εξτρεμισμού. Οι κυβερνοτρομοκράτες χρησιμοποιούν το διαδίκτυο για επιθέσεις σε κρίσιμες υποδομές ή/και συσκευές, για την διάδοση του περιεχομένου, για τις διαδικτυακές τους επικοινωνίες και την ψηφιακή χρηματοδότηση της τρομοκρατία (UN: cybersecurity).

1.1. <u>Οι κατηγορίες των Κυβερνοεγκλήματων:</u>

Τα κυβερνοεγκλήματα χωρίζονται σε δύο μεγάλες κατηγορίες στα γνήσια και τα μη γνήσια. Τα γνήσια κυβερνοεγκλήματα αφορούν τις κατηγορίες των εγκλημάτων που αν δεν υπήρχε το διαδίκτυο και η τεχνολογία πληροφοριών και επικοινωνιών δεν θα μπορούσαν να πραγματοποιηθούν, ενώ μη γνήσια είναι τα εγκλήματα που χρησιμοποιούν το διαδίκτυο απλά ως μέσο για την διάπραξή τους και θα μπορούσαν να τελεστούν και με άλλο τρόπο-μέσο.

Τα γνήσια κυβερνοεγκλημάτα χωρίζονται στις εξής κατηγορίες:

1. <u>Απάτες (Fraud).</u>

Είναι τα εγκλήματα εκείνα κατά τα οποία «ο δράστης προσπορίζει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτοντας ξένη περιουσία επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή με διάφορους τρόπους (Άρθρο 386^{Α} του Π.Κ.). Χαρακτηριστικά είδη τέτοιων εγκλημάτων είναι υποκλοπή στοιχείων πιστωτικών καρτών ή στοιχείων εισόδου σε web banking, με τη χρήση μεθόδων κοινωνικής μηχανικής ή με την αξιοποίηση κακόβουλου λογισμικού, οι απάτες CEO όταν ένας υπάλληλος που πραγματοποιεί πληρωμές της εταιρείας εξαπατάται ώστε πληρώσει ένα πλαστό τιμολόγιο ή να μεταφέρει χρήματα από εταιρικό λογαριασμό της επιχείρησης.

1.1 Διαφημιστικές απάτες (Ad-Fraud)

Είναι αρκετά συχνές καθώς αυτές οι απάτες συνήθως δεν καταγγέλλονται και κατά συνέπεια δεν διώκονται ενώ είναι προσοδοφόρες για τους εγκληματίες. Χωρίζονται σε τρεις κατηγορίες: την απάτη ταυτότητας όπου στην ουσία μέσω της δημιουργίας πλαστών προσώπων-χρηστών αυξάνεται ο αριθμός του κοινού π.χ. ψεύτικη επισκεψιμότητα στα μέσα κοινωνικής δικτύωσης. Η απάτη απόδοσης στοχεύει στην πλαστοπροσωπία της συμπεριφοράς πραγματικών χρηστών (κλικ, δραστηριότητες, συνομιλίες κ.λπ.). και τις υπηρεσίες απάτης διαφημίσεων οι οποίες περιλαμβάνουν τις «διαδικτυακές υποδομές» που χρειάζονται για την πραγματοποίηση της απάτης ταυτότητας ή απόδοσης(Jean-Loup Richet 2022).

2. Κακάβουλο λογισμικό (Ransomware).

Οι δράστες εγκαθιστούν κακόβουλο λογισμικό στην συσκευή του θύματος και με τον τρόπο αυτό αποκτούν πρόσβαση στις προσωπικές του πληροφορίες, τις οποίες είτε απειλούν να δημοσιεύσουν είτε να καταστρέψουν, απαιτώντας την καταβολή ανταλλαγμάτων συνήθως οικονομικών για να μην το πράξουν (Steve Morgan 2019).

3. Κυβερνοεκβιασμός (Cyberexortion).

Οι δράστες απαιτούν την καταβολή χρηματικού ανταλλάγματος ώστε να σταματήσουν τις κυβερνοεπιθέσεις και να παρέχουν «προστασία» από αυτές στο θύμα.

4. Hacking.

Είναι η παραβίαση των συστημάτων ασφαλείας που διαθέτουν οι υπολογιστές και οι συσκευές τεχνολογίας και πληροφοριών, η οποία πραγματοποιείται μέσω του διαδικτύου για την αποκόμιση χρηματικού ωφελήματος, συλλογής πληροφοριών ή συμβολικής διαμαρτυρίας και επιτυγχάνεται με την χρήση κακόβουλων λογισμικών (malware) και λογισμικών κατασκοπείας (spyware).

5. Διακίνηση παιδικής πορνογραφίας.

Είναι ένα συνεχώς εξελισσόμενο φαινόμενο και διαμορφώνεται από τις εξελίξεις στην τεχνολογία. Η συνδεσιμότητα κινητής τηλεφωνίας, η αυξανόμενη κάλυψη του Διαδικτύου στις αναπτυσσόμενες χώρες παρέχουν υψηλό βαθμό ανωνυμίας στον θεατή, ενισχύουν την τάση στην εμπορική ζωντανή ροή της σεξουαλικής κακοποίησης παιδιών (EUROPOL: child sexual exploitation).

6. Κοινωνική μηχανική (Social engineering).

Στην ουσία είναι το λεγόμενο ηλεκτρονικό ψάρεμα, με το οποίο οι δράστες προκαλούν τεχνηέντως το θύμα να τους αποκαλύψει ευαίσθητα προσωπικά δεδομένα. Υπάρχουν διάφοροι τύποι ψαρέματος με το πιο γνωστό το email-phishing. (Ross J. Anderson 2008). Ενώ υπάρχουν και άλλοι τύποι όπως το (vishing), η απόσπαση πληροφοριών γίνεται μέσω του τηλεφώνου, η απομίμηση (impersonation), η προσποίηση ενός ως άλλου ατόμου με στόχο τη λήψη

πληροφοριών και τέλος το SmiShing κατά το οποίο χρησιμοποιούνται μηνύματα (SMS) ή η λήψη κακόβουλου λογισμικού ώστε να αποσπάσουν από τα θύματα τις ευαίσθητες πληροφορίες που επιθυμούν (social-engineer).

7. Η αποστολή ανεπιθύμητου περιεχόμενου (Spam).

Είναι οποιοσδήποτε τύπος ανεπιθύμητων δεδομένων τα οποία αποστέλλονται μαζικά κυρίως μέσω email στους χρήστες τους. Το spam συνήθως δεν είναι επικίνδυνο για τον υπολογιστή ή την συσκευή του χρήστη, ωστόσο αποστέλλεται σε αυτόν χωρίς την θέλησή του και καταλαμβάνει πολύτιμο χώρο αποθήκευσης.

8. Cryptojacking.

Είναι μια πράξη κατά την οποία κυριεύεται ένας υπολογιστής με σκοπό την απόκτηση κρυπτονομισμάτων από τον χρήστη, μέσω ιστοτόπων ή χωρίς ο χρήστης να το γνωρίζει, με κίνητρο το κέρδος, ενώ σε αντίθεση με άλλες απειλές, το λογισμικό που χρησιμοποιείται είναι σχεδιασμένο ώστε να παραμένει κρυφό και να μην γίνεται αντιληπτό από τον χρήστη.

9. Εγκλήματα που αφορούν τα πληροφοριακά συστήματα.

9.1 Ιοί υπολογιστών (computer viruses):

Είναι προγράμματα υπολογιστών τα οποία προκαλούν «μόλυνση»- ζημία στα υπολογιστικά συστήματα που εγκαθίστανται και τα καθιστούν με λειτουργικά.

9.2 Επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service attacks (DoS)):

Είναι μια κυβερνοεπίθεση κατά την οποία ο δράστης επιδιώκει να καταστήσει μια μηχανή ή ένα δίκτυο μη διαθέσιμο στους χρήστες για τους οποίους προορίζεται, διακόπτοντας προσωρινά ή επ' αόριστον τις υπηρεσίες ενός κεντρικού υπολογιστή που είναι συνδεδεμένος σε αυτό (CISA: Denial of Service attacks).

9.3 Κακόβουλο λογισμικό (Malware):

Είναι λογισμικό που δημιουργήθηκε και μπορεί να χρησιμοποιηθεί ώστε διακόψει την λειτουργία ενός υπολογιστή διακομιστή ή δίκτυο υπολογιστών, να αποκτήσει πρόσβαση σε πληροφορίες και συστήματα, με σκοπό να τα δημοσιεύσει, να στερήσει την πρόσβαση σε

πληροφορίες ή να παρεμβαίνει εν αγνοία του χρήστη στην ασφάλεια και το απόρρητο του υπολογιστή του (RossBrewer 2016). Το κακόβουλο λογισμικό μπορεί να κατηγοριοποιηθεί, σε διάφορους τύπους όπως, οι ιοί υπολογιστών, τα σκουλήκια (worms), οι δούρειοι ίπποι (Trojan horses), ransomware, κατασκοπευτικό λογισμικό (spyware), adware, rogue software, wiper και keylogger).

Τα μη γνήσια εγκλήματα κατηγοριοποιούνται ως εξής:

1. Εγκλήματα σχετικά με την πνευματική ιδιοκτησία.

Αυτή η κατηγορία εγκλημάτων μπορεί να διαιρεθεί σε δύο υποκατηγορίες, η μια αφορά τα πνευματικά δικαιώματα και η άλλη τα εμπορικά σήματα. Όσο αναφορά την παραβίαση των πνευματικών δικαιωμάτων, αυτή έχει πλήξει κυρίως την βιομηχανία του θεάματος (μουσική, ταινίες), καθώς ο ανεξέλεγκτος διαμοιρασμός και αναπαραγωγή τους στο διαδίκτυο, πραγματοποιείται χωρίς την εφαρμογή της νομοθεσίας περί πνευματικών δικαιωμάτων. Τα εμπορικά σήματα από την άλλη, χρησιμοποιούνται είτε για να προσελκύσουν του χρήστες με σκοπό να τους ξεγελάσουν για να αποκτήσουν πρόσβαση σε πληροφορίες τους, είτε ευρέως γνωστά εμπορικά σήματα χρησιμοποιούνται αυθαιρέτως και παρανόμως από εταιρείες με σκοπό να αποκτήσουν τους πελάτες της πραγματικής εταιρείας και να παρέχουν τα προϊόντα τους σε χαμηλότερες τιμές.

2. Διαδικτυακές παρενοχλήσεις.

Στην κατηγορία αυτή, οι χρήστες διακινούν περιεχόμενο το οποίο είναι προσβλητικό με αισχρολογίες, με υποτιμητικά ή ρατσιστικά σχόλια είτε γενικώς είτε σε συγκεκριμένα άτομα με βάση το φύλο, τη φυλή, τη θρησκεία, την εθνικότητα ή τον σεξουαλικό προσανατολισμό.

3. Η διασπορά ψευδών ειδήσεων και δυσφήμησης.

Η παραπληροφόρηση και η δημιουργία ψευδών ειδήσεων αποτελεί την σύγχρονη μάστιγα του διάδικου. Η ψευδής είδηση ενός γεγονότος ή η είδηση σχετικά με ένα πρόσωπο διαδίδεται ταχύτατα κα ανεξέλεγκτα και μπορεί να έχει σοβαρό αντίκτυπο σε διάφορους τομείς όπως τον

κοινωνικό ή οικονομικό, τους οποίους μπορεί να πλήξει ανεπανόρθωτα. Από την στιγμή την διάδοσής της είναι δύσκολο να διαγράφει από τον αχανές διαδίκτυο.

4. Παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ο όρος «επεξεργασία» «καλύπτει ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα. Κάποια παραδείγματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι η διαχείριση των στοιχείων του προσωπικού και μισθοδοσίας τους, η προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων, η καταστροφή διά τεμαχισμού εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα, η δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο και η αποθήκευση διευθύνσεων IP ή διευθύνσεων MAC (EU COMMISION: Data protection).

5. Το ξέπλυμα χρήματος από εγκληματικές δραστηριότητες.

Επιτυγχάνεται κυρίως μέσω του σκοτεινού διαδικτύου (dark web), το οποίο αναφέρεται σε ιστότοπους στους οποίους οι χρήστες δεν μπορούν να έχουν πρόσβαση μέσω κανονικών προγραμμάτων περιήγησης. Στο σκοτεινό διαδίκτυο η τοποθεσία και οι δραστηριότητες των χρηστών είναι «κρυμμένες» και οι αρχές δεν μπορούν να τις ελέγξουν. Έτσι, όταν οι αρχές διενεργούν διάφορους ελέγχους, οι χρήστες δεν μπορούν να εντοπιστούν. Οι δύο παράγοντες που κάνουν το σκοτεινό διαδίκτυο δημοφιλές είναι το απόρρητο και η ανωνυμία για αυτό και χρησιμοποιείται αδιάκοπα για το ξέπλυμα χρημάτων.

6. Η διεξαγωγή άλλων εγκληματικών δραστηριοτήτων.

Άλλες εγκληματικές δραστηριότητες που διεξάγονται σε μεγάλη κλίμακα μέσω του διαδικτύου και κυρίως του σκοτεινού διαδικτύου, είναι το εμπόριο παράνομων ναρκωτικών και όπλων ώστε

να διαφύγουν της προσοχής των αρχών επιβολής του νόμου. Οι εμπλεκόμενοι καταβάλλουν προσπάθεια ώστε να κρατήσουν μυστική την ταυτότητά τους, ενώ βρίσκονται στο διαδίκτυο για αυτό και χρησιμοποιούν ειδικά εργαλεία, όπως είναι τα εικονικά ιδιωτικά δίκτυα, τα Tails και το πρόγραμμα περιήγησης Tor, τα οποία βοηθούν στην απόκρυψη της παρουσίας τους στο διαδίκτυο. Τέλος το πιο σημαντικό στοιχείο που προσφέρει επιπρόσθετη ανωνυμία και ασφάλεια είναι η χρήση του νομίσματος Bitcoin, το οποίο επιτρέπει να πραγματοποιούνται οι συναλλαγές ανώνυμα, με τις μοναδικές πληροφορίες που είναι διαθέσιμες στα εμπλεκόμενα μέρη να είναι το αρχείο ότι πραγματοποιήθηκε η μεταξύ τους συναλλαγή.

7. <u>Παράνομος στοιχηματισμός και τυχερά παιχνίδια.</u>

Με τον ερχομό και την διάδοση του διαδικτύου, ο στοιχηματισμός και τα τυχερά παιχνίδια μεταφέρθηκαν online και παράλληλα μεταφέρθηκε και η παράνομη δραστηριότητα εκεί, με χιλιάδες παράνομες ιστοσελίδες που προσφέρουν ανεξέλεγκτο στοιχηματισμό. Ωστόσο, ο στοιχηματισμός σε μια παράνομη ιστοσελίδα στοιχηματισμού εγκυμονεί κινδύνους. Η αξιοπιστία των παιχνιδιών, των αποδόσεων και των χρημάτων που θα επιστραφούν στον χρήστη σε περίπτωση νίκης του είναι αμφίβολη, ενώ και τα προσωπικά του δεδομένα όπως τα προσωπικά του στοιχεία και ο αριθμός του τραπεζικού του λογαριασμού αποστέλλονται σε άγνωστες εταιρείες που δεν εφαρμόζουν τις ισχύουσες πολιτικές ασφαλείας και προστασίας-επεξεργασίας των προσωπικών δεδομένων.

2. Ο ορισμός της Βιοασφάλειας (biosecurity)

Αρχικά ό όρος, χρησιμοποιήθηκε κυρίως στην άμυνα σε σχέση με την πρόληψη των βιολογικών όπλων, ενώ ορισμένα επίσημα έγγραφα και ιστοσελίδες εξακολουθούν να χρησιμοποιούν αυτόν τον αρχικό ορισμό της βιοασφάλειας. Στο Βέλγιο, για παράδειγμα, η βιοασφάλεια ορίζεται ως «η πρόληψη και η μη χρήση μέσω απώλειας, κλοπής, εκτροπής ή σκόπιμης απελευθέρωσης μολύνσεων, δηλητηρίων και οποιωνδήποτε άλλων βιολογικών υλικών» (Véronique Renault κ.α. 2022). Στις Η.Π.Α. τη δεκαετία του 1980, άρχισαν να χρησιμοποιούν για πρώτη φορά τον όρο βιοασφάλεια σε σχέση με την υγεία των ζώων και των συστημάτων παραγωγής ως «ζωτικής σημασίας στρατηγική στην προσπάθεια για τον σχεδιασμό της προστασίας της υγείας των ανθρώπων, των ζώων και του περιβάλλοντος από βιολογικές απειλές». Το 1987, ο όρος «βιοασφάλεια» αναφέρθηκε για πρώτη φορά στο PubMed. Η ευρεία χρήση του επεκτάθηκε σταδιακά, σε πολλά κράτη και με την πάροδο του χρόνου περιλαμβάνεται σε πολλά στρατηγικά έγγραφα κυβερνήσεων, διεθνών οργανισμών, μη κυβερνητικών οργανώσεων και σε διάφορες βιομηχανίες. Σαφής ορισμός της βιοασφάλειας δεν υπάρχει. Ο κανονισμός 2016/429, της Ε.Ε., αναφέρεται στον όρο biosecurity ως «ένα σύνολο διαχειριστικών και φυσικών μέτρων που έχουν σχεδιαστεί για τη μείωση του κινδύνου εισαγωγής, εγκατάστασης και εξάπλωσης ζωικών ασθενειών, μολύνσεων ή προσβολών προς, από και εντός ενός ζωικού πληθυσμού». Ενώ συνυπάρχουν αρκετοί ορισμοί, γίνονται προσπάθειες να καθιερωθεί ένας ενιαίος ορισμός της βιοασφάλειας (biosecurity). Σύμφωνα με τον Οργανισμό Τροφίμων και Γεωργίας των Ηνωμένων Εθνών (FAO) και τον Παγκόσμιο Οργανισμό Υγείας (WHO), η βιοασφάλεια (biosecurity) είναι «μια στρατηγική και ολοκληρωμένη έννοια που περιλαμβάνει την πολιτική και τα κανονιστικά πλαίσια (συμπεριλαμβανομένων των μέσων και των δραστηριοτήτων) που αναλύουν και διαχειρίζονται κίνδυνους για την ασφάλεια των τροφίμων, τη δημόσια υγεία, τη ζωή και την υγεία των ζώων και τη ζωή και την υγεία των φυτών, συμπεριλαμβανομένου του σχετικού περιβαλλοντικού κινδύνου». Από το 2007, η βιοασφάλεια έχει συμπεριληφθεί ως βασικό στοιχείο στη

στρατηγική της Ευρωπαϊκής Ένωσης για την υγεία των ζώων και στο σχέδιο ετοιμότητας για κάθε χώρα του Ευρωπαϊκού Κέντρου Πρόληψης και Ελέγχου Νοσημάτων (ECDC). Νωρίτερα, είχε περιληφθεί στον Διεθνή Κανονισμό Υγείας που εγκρίθηκε από τον ΠΟΥ το 2005. Η βιοασφάλεια περιλαμβάνει όλα τα μέτρα για την πρόληψη και τη μείωση της εξάπλωση των ασθενειών (βιοαποκλεισμός και βιοπεριορισμός). Ο κύριος στόχος της βιοασφάλειας είναι η προστασία από κινδύνους που προκαλούνται από ασθένειες και οργανισμούς. Τα κύρια μέτρα με τα οποία επιτυγχάνει τον στόχο της, είναι ο αποκλεισμός, η εξάλειψη και ο έλεγχος, τα οποία στηρίζονται στην διαχείριση ειδικών συστημάτων, σε χρήσιμα πρωτόκολλα και στην ταχεία και αποτελεσματική διασφάλιση και ανταλλαγή κρίσιμων πληροφοριών. Επομένως, ένα προηγμένο επίπεδο βιοασφάλειας ελαχιστοποιεί τον αντίκτυπο των μολυσματικών ασθενειών στη δημόσια υγεία, την υγεία των ζώων και των φυτών, καθώς και στην οικονομία, στο περιβάλλον αλλά και στην κοινωνία γενικότερα.

Συνήθως υπάρχει μια σύγχυση μεταξύ των όρων biosafety και biosecurity, καθώς σε πολλές γλώσσες όπως και στην ελληνική οι δύο όροι αποδίδονται με την ίδια λέξη. Ωστόσο μεταξύ τους υπάρχει διαφορά και ο όρος biosafety συμπληρώνει τον ορό biosecurity, ο οποίος είναι και ευρύτερος. Ειδικότερα, ο όρος biosafety αναφέρεται στην εφαρμογή εργαστηριακών πρωτοκόλλων (πρακτικών, διαδικασιών, ειδικών κατασκευαστικών χαρακτηριστικών, εργαστηριακών εγκαταστάσεων, εξοπλισμού ασφαλείας και κατάλληλων προγραμμάτων υγείας) κατά την εργασία με δυνητικά μολυσματικούς μικροοργανισμούς και άλλους βιολογικούς κινδύνους. Για παράδειγμα ο όρος biosafety περιγράφεται στο Βέλγιο ως «η ασφάλεια για την ανθρώπινη υγεία και το περιβάλλον, συμπεριλαμβανομένης της προστασίας της βιοποικιλότητας, κατά τη χρήση γενετικά τροποποιημένων οργανισμών (ΓΤΟ) ή μικροοργανισμών (ΓΤΜ) και κατά την περιορισμένη χρήση παθογόνων οργανισμών για τον άνθρωπο». Η σημασία της βιοασφάλειας άρχισε να φαίνεται στις αρχές του 2000. Συγκεκριμένα, στις 10 Ιανουαρίου 2000, το Συμβούλιο Ασφαλείας των Ηνωμένων Εθνών (ΗΕ) συνεδρίασε με θέμα μια νέα απειλή για τη διεθνή ειρήνη και ασφάλεια, καθώς εξέτασε τον

αντίκτυπο του ιού (HIV) στην Αφρική. Για πρώτη φορά στην ιστορία των Ηνωμένων Εθνών, το Συμβούλιο Ασφάλειας αντιμετώπισε ένα ζήτημα υγείας ως απειλή για τη διεθνή ασφάλεια (UN: Impact of AIDS on Peace and Security in Africa). Τον Φεβρουάριο του ίδιου έτους το Συμβούλιο Εθνικής Ασφάλειας των ΗΠΑ όρισε και αυτό με την σειρά του, τον HIV ως απειλή για την εθνική ασφάλεια. Ήταν η πρώτη φορά που μια ασθένεια χαρακτηρίστηκε ως απειλή (Barton Gellman 2000) και προκείμενου το Συμβούλιο Εθνικής Ασφάλειας των ΗΠΑ να προβεί σε αυτόν τον χαρακτηρισμό βασίστηκε σε μια έκθεση πληροφοριών σχετικά με τις επιπτώσεις μιας μολυσματικής νόσου στην εθνική ασφάλεια. Σύμφωνα λοιπόν με την έκθεση αυτή: «Νέες και επανεμφανιζόμενες μολυσματικές ασθένειες θα δημιουργήσουν μια ανερχόμενη απειλή για την παγκόσμια υγεία και θα περιπλέξουν την ασφάλεια των ΗΠΑ αλλά και την παγκόσμια ασφάλεια τα επόμενα 20 χρόνια. Αυτές οι ασθένειες θα θέσουν σε κίνδυνο τους πολίτες των ΗΠΑ στο εσωτερικό και στο εξωτερικό, θα απειλήσουν ένοπλες δυνάμεις των ΗΠΑ που αναπτύσσονται στο εξωτερικό και θα επιδεινώσουν την κοινωνική και πολιτική αστάθεια σε χώρες και περιοχές στις οποίες οι Ηνωμένες Πολιτείες έχουν σημαντικά συμφέροντα» (National Intelligence Council 2000). Ακολούθως, το 2006 η Στρατηγική Εθνικής Ασφάλειας των ΗΠΑ συμπεριέλαβε την πανδημία ως απειλή για την εθνική ασφάλεια στην ίδια κατηγορία με την απόκτηση πυρηνικών, βιολογικών και χημικών όπλων από την τρομοκρατία (Geoge W. Bus 2006).

Οι λόγοι για τους οποίους τα θέματα υγείας άρχισαν να συμπεριλαμβάνονται στον όρο της διεθνούς ασφάλειας ήταν οι εξής:

- Ο πρώτος ήταν ο επαναπροσδιορισμός του όρου της ασφάλειας ώστε να συμπεριλάβει μη στρατιωτικές απειλές όπως η υποβάθμιση του περιβάλλοντος, η κλιματική αλλαγή, το οργανωμένο έγκλημα, οι προσφυγικές ροές και η τρομοκρατία.
- Ο δεύτερος ήταν η αναγνώριση ότι αυτές οι απειλές δεν προέρχονται κατά κύριο λόγο από τα κράτη, αλλά έχουν διεθνικό και ή μη κρατικό χαρακτήρα.

- Τέλος, προέκυψε μια νέα πτυχή ασφάλειας των ατόμων και των ομάδων εντός των κρατών και όχι μόνο των ίδιων κρατών (Gregory D. Koblentz 2010).

Επιπλέον, την ανάδειξη των βιολογικών απειλών σε σημαντικό παράγοντα της διεθνούς ασφάλειας καθόρισαν η πρόοδος της επιστήμης και της τεχνολογίας, η εμφάνιση νέων ασθενειών, η παγκοσμιοποίηση και η αλλαγή στο πεδίο των συγκρούσεων των κρατών. Ειδικότερα, η ανάπτυξη της τεχνολογίας και η πρόοδος των επιστημών όπως η βιολογία και η βιοτεχνολογία οδήγησε την ανθρωπότητα στην λεπτομερή ανάλυση γονιδιομάτων και της γενετικής πληροφορίας (dna) ιών και μικροβίων. Αυτό από την μια οδήγησε στην ανακάλυψη και την δημιουργία φαρμάκων για την αντιμετώπισή τους, από την άλλη όμως αποτέλεσε και αποτελεί απειλή για την δημιουργία εργαστηριακών ιών, που μπορεί να χρησιμοποιηθούν ως βιολογικά όπλα. Η εξέλιξη των μικροοργανισμών, έχει ως αποτέλεσμα την ανάπτυξη νέων μικροβιακών απειλών και ασθενειών για την ανθρώπινη υγεία. Για παράδειγμα ο ιός (H1N1) εμφανίστηκε στη Βόρεια Αμερική το 2009 και πυροδότησε την πρώτη πανδημία μετά από σαράντα σχεδόν χρόνια, ενώ σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ) από τον ιό μολύνθηκαν περισσότεροι από 620.000 άνθρωποι και τουλάχιστον 7.800 απεβίωσαν (WHO: H1N1). Η παγκοσμιοποίηση και ο διεθνικός χαρακτήρας πολλών φαρμακευτικών και βιοτεχνολογικών εταιρειών συνετέλεσε στην διάχυση της γνώσης, των πληροφοριών και της τεχνολογίας σε επιστημονικό επίπεδο. Επιπλέον, το ελεύθερο εμπόριο οδήγησε στην δημιουργία μιας παγκόσμιας αγροτοδιατροφικής αλυσίδας, κάνοντας ευκολότερη την ταχύτερη διάδοση των ασθενειών. Τέλος, η μετανάστευση και ο τουρισμός αποτελούν επιβαρυντικούς παράγοντες για την διάδοση μιας ασθένειας από μια περιοχή σε πολλές χώρες (Institute of Medicine and National Research Council: Biosecurity, and the Future of the Life Sciences) .

Όσο αναφορά τις συγκρούσεις, αυτές στη σύγχρονη εποχή, συνήθως δεν πραγματοποιούνται μεταξύ των κρατών αλλά εντός αυτών, με τους εμφύλιους πολέμους να είναι μια μορφή τους κυρίως στις αναπτυσσόμενες χώρες, με καταστροφικές συνέπειες, οι οποίες τελούν σε απόλυτη συνάφεια με την βιοασφάλεια. Ειδικότερα, μια εμφύλια σύγκρουση

συνήθως καταστρέφει τις κρατικές υποδομές, δημιουργεί μεγάλο όγκο εκτοπισμένων πληθυσμών, οι οποίοι στερούνται επαρκούς τροφής, στέγης, υγειονομικής και ιατρικής περίθαλψης, με αποτέλεσμα να διευκολύνουν την εμφάνιση ασθενειών (Michael Moodie and William J. Taylor Jr., 2000). Επιπροσθέτως, η εμφάνιση τρομοκρατικών οργανώσεων και το ενδιαφέρον τους να αποκτήσουν πυρηνικά, χημικά και βιολογικά όπλα, αποτελεί απειλή για διεθνή ασφάλεια. Για παράδειγμα στις 20-03-1995, στο Τόκιο μέλη της τρομοκρατικής-παραθρησκευτικής οργάνωση «Aum Shinrikyo», επιβιβάστηκαν σε βαγόνια του μετρό και απελευθέρωσαν το νευροτοξικό αέριο σαρίν, προκαλώντας το θάνατο σε 13 ανθρώπους και αφήνοντας 5.500 τραυματίες (BRITANICCA). Επίσης, οι επιθέσεις με επιστολές άνθρακα το φθινόπωρο του 2001 στις ΗΠΑ, σκότωσαν πέντε ανθρώπους, διέκοψαν την ταχυδρομική υπηρεσία των ΗΠΑ και έκλεισαν προσωρινά τη Γερουσία των ΗΠΑ (FBI: anthrax-amerithrax).

2.1. Οι κατηγορίες των βιολογικών απειλών

Βιολογικός πόλεμος.

Είναι ο πόλεμος κατά τον οποίο χρησιμοποιούνται παθογόνοι μικροοργανισμοί (π.χ. ιοί, βακτήρια) προκειμένου να πλήξουν τον εχθρό. Τα βιολογικά όπλα ανάλογα με την «ισχύ» τους χωρίζονται σε τρείς κατηγορίες. Στην πρώτη κατηγορία ανήκουν παθογόνοι οργανισμοί, που δεν έχουν ως βασικό σκοπό το θάνατο, αλλά την εξασθένηση των γραμμών του αντιπάλου. Στην δεύτερη κατηγορία, γίνεται η εκτεταμένη χρήση τους για την εξόντωση του εχθρού, με θανατηφόρες ασθένειες, για τις οποίες υπάρχει θεραπεία. Στην τελευταία κατηγορία εντάσσονται μεταλλαγμένοι ιοί, οι οποίοι αποστέλλονται με συμβατικά όπλα, όπως διηπειρωτικοί πύραυλοι και βόμβες και προκαλούν ασθένειες για τις οποίες δεν υπάρχει άμεση θεραπεία. Τα βιολογικά όπλα θεωρούνται όπλα μαζικής καταστροφής και είναι μη συμβατικά όπλα. Αναπτύχθηκαν κατά τον 20^{ο} αιώνα από αρκετά κράτη και αποτελούν μια από τις σημαντικότερες απειλές για την διεθνή ασφάλεια. (Gregory D. Koblentz 2009).

Βιοτρομακρατία.

Η χρήση των βιολογικών όπλων από τρομοκρατικές οργανώσεις προκειμένου να πετύχουν έναν από τους στόχους τους αποτελεί την δεύτερη κατηγορία βιολογικών απειλών. Ωστόσο, το αυξημένο κόστος, η έλλειψη κατάλληλων υποδομών, η απουσία ειδικών επιστημονικών γνώσεων και η ανάπτυξη της βιοάμυνας από τα κράτη, καθιστούν την χρήση βιολογικών όπλων από τρομοκρατικές οργανώσεις λιγότερο απειλητική από όσο την πρώτη κατηγορία καθώς και από αυτή που θα ακολουθήσει.

Οι έρευνες διπλής χρήσης.

Όπως ανέφερε η Επιτροπή των ΗΠΑ για την πρόληψη της διάδοσης των όπλων μαζικής καταστροφής: «οι Ηνωμένες Πολιτείες θα πρέπει να ανησυχούν λιγότερο για το αν οι τρομοκράτες γίνουν βιολόγοι και να ανησυχούν πολύ περισσότερο για αν οι βιολόγοι γίνουν τρομοκράτες» (Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism: World at Risk). Η ανάπτυξη της τεχνολογίας και η πρόοδος των επιστημών,

οδήγησαν και στην πρόοδο των βιοεπιστημών, οι οποίες με την σειρά τους συνέβαλαν στην αντιμετώπιση των ασθενειών και στην δημιουργία νέων φαρμάκων, βοηθώντας την ανθρωπότητα. Ωστόσο, οι γνώσεις και η τεχνολογία που αποκτώνται από αυτές τις έρευνες, μπορούν να χρησιμοποιηθούν για την ανάπτυξη βιολογικών όπλων τα οποία θα χρησιμοποιηθούν είτε σ' ένα βιολογικό πόλεμο είτε σε από βιοτρομοκράτες. (Institute of Medicine and National Research Council, Globalization, Biosecurity, and the Future of the Life Sciences, 2006).

Βιοεγκλήματα.

Ορίζονται τα εγκλήματα εκείνα που υποκινούνται από προσωπικούς λόγους όπως π.χ. η ζήλια και στα οποία η χρήση παθογόνων μικροοργανισμών μπορεί να προκαλεί τον θάνατο, την ασθένεια ή να προκαλέσει πανικό σε ένα συγκεκριμένο άτομο ή μια περιορισμένη ομάδα ατόμων. Οι διαφορές μεταξύ της βιοτρομοκρατίας και του βιοεγκλήματος είναι ο αριθμός των ατόμων που επηρεάζονται και το κίνητρο πίσω από την επίθεση. Συνήθως, οι δράστες αυτών των εγκλημάτων έχουν τις εξιδικευμένες επιστημονικές γνώσεις και την πρόσβαση στον βιολογικό παράγοντα που θα χρησιμοποιηθεί (Manuela Oliveira κ.α. 2020).

Εργαστηριακά ατυχήματα.

Η ανάπτυξη των ερευνών γύρω από την καταπολέμηση των παθογόνων ιών και ραγδαία αύξηση των βιοεργαστηρίων σε όλο τον κόσμο είναι τα αίτια αυτής της κατηγορίας. Τα χιλιάδες βιοεργαστήρια ανά τον κόσμο, δεν εφαρμόζουν τα ίδια αυστηρά πρωτόκολλα ασφαλείας, εγείροντας ανησυχίες για τη βιοασφάλεια και ειδικότερα την πιθανότητα γενετικοί ή τροποποιημένοι παθογόνοι οργανισμοί να διαφύγουν από κάποιο εργαστήριο, προκαλώντας σημαντικό κίνδυνο για την δημόσια υγεία με την επαναφορά μιας μεταδοτικής ασθένειας που έχει εξαλειφθεί ή με την μετάδοση μιας νέας η οποία δημιουργήθηκε εντός του εργαστηρίου.

Πανδημικές ασθένειες.

Εμφανίζονται σε μια γεωγραφική περιοχή, όπως σε μια ήπειρο ή σε ολόκληρο τον κόσμο και μολύνουν ένα υψηλό ποσοστό του πληθυσμού. Η εμφάνισή τους, έχει σημαντικές επιπτώσεις

για την δημόσια υγεία καθώς και σε άλλους τομείς όπως την οικονομία και την σταθερότητα και τη ασφάλεια των κρατών. Χαρακτηριστικές πανδημικές ασθένειες είναι η πανδημική γρίπη του 1918-1919, ο HIV/AIDS στις αρχές του 2000 και ο COVID-19 στις μέρες μας. Στην κατηγορία αυτή μπορούν να ενταχθούν και οι ενδημικές ασθένειες οι οποίες εμφανίζονται σε μία μικρότερη γεωγραφική περιοχή όπως π.χ. σε ένα κράτος και οι οποίες έχουν τις ίδιες συνέπειες με την πανδημία σε μικρότερη κλίμακα.

Οι προκλήσεις της βιοασφάλειας και τα προβλήματα που ανακύπτουν είναι τα εξής:

- Ο σχεδιασμός και η πρόβλεψη της πιθανότητας και των συνεπειών των περισσότερων βιολογικών απειλών είναι εξαιρετικά δύσκολα. Εκτός από τις φυσικές μολυσματικές ασθένειες όπως τον HIV/AIDS και τον COVID-19, αυτές οι απειλές είναι σπάνιες.
- Η αντιμετώπιση αυτών των απειλών απαιτεί μια διεπιστημονική προσέγγιση σε διεθνικό επίπεδο. Ένας ευρύς, σαφής και ενιαίος ορισμός της βιοασφάλειας είναι πολύτιμος για την δημιουργία ενός θεσμικού πλαισίου ώστε οι επιστήμονες, οι υπεύθυνοι χάραξης πολιτικής καθώς και όλοι οι εμπλεκόμενοι να καταφέρουν να συνεργαστούν ώστε συμπληρώσουν τα κενά.
- Οι συνέπειες των κινδύνων δεν μπορούν να υπολογιστούν αξιόπιστα, καθώς υπάρχει ο αστάθμητος παράγοντας του φόβου για την αντίληψη του κινδύνου που διατρέχουν οι άνθρωποι από τις μολυσματικές ασθένειες και την μετάδοσή τους.
- Δεν υπάρχει ενιαία στρατηγική που να περιλαμβάνει το σύνολο ή ένα μεγάλο μέρος αυτών των απειλών, καθώς στην πλειοψηφία των περιπτώσεων αυτές μελετώνται ξεχωριστά και σε περίοδο ηρεμίας, (όπου δεν υφίστανται αυτές οι απειλές). Αυτό μπορεί να έχει ως αποτέλεσμα να επιλεγούν μέτρα που υποκαθιστούν νέους κινδύνους με παλιούς στον ίδιο πληθυσμό ή να μεταφέρουν κινδύνους σε νέους πληθυσμούς ή να δημιουργήσουν νέους κινδύνους σε νέους πληθυσμούς.
- Σε πολλά κράτη δεν υπάρχει σαφής σύνδεση της εθνικής ασφάλειας με την βιοασφάλεια.

- Υπάρχει αυξημένο κόστος για τη διασύνδεση της βιοασφάλειας με την δημόσια υγεία και την εθνική ασφάλεια, από την οποία ωστόσο θα προκύψουν οφέλη.

3. Η κυβερνοβιοασφάλεια (cyberbiosecurity)

Αποτελεί μια νέα πτυχή της αλληλεπίδρασης μεταξύ της βιοασφάλειας (biosecurity) και της κυβερνοασφάλειας (cybersecurity) (Lauren C κ.α. 2019) Ο στόχος της κυβερνοβιοασφάλειας έχει περιγραφεί ως η αντιμετώπιση «δυνητικής ή πραγματικής κακόβουλης καταστροφής, κακής χρήσης ή εκμετάλλευσης πολύτιμων πληροφοριών, διαδικασιών και υλικού στη διεπαφή των βιοεπιστημών και των ψηφιακών τεχνολογιών» (Peccoud, J κ.α. 2018). Η κυβερνοβιοασφάλεια είναι μέρος ενός συστήματος μέτρων που στοχεύουν συλλογικά στην «Διασφάλιση της Βιοοικονομίας», έναν στόχο που περιγράφεται από τις Εθνικές Ακαδημίες Επιστημών, Μηχανικής και Ιατρικής των Ηνωμένων Πολιτειών. Ο στόχος της επιτυγχάνεται μέσω της κατανόησης των τρωτών σημείων που προκύπτουν από τον συγκερασμό των πολλών κλάδων που την αποτελούν όπως τα βιοϊατρικά συστήματα, τα εργαλεία βιοπληροφορικής και της ανάπτυξης και εφαρμογής μέτρων που θα προστατεύσουν από απειλές που στοχεύουν σε άτομα ή οργανισμούς. Ουσιαστικά, η κυβερνοβιοασφάλεια συμβάλλει στην ενίσχυση της κατανόησης των κινδύνων ασφάλειας, λόγω της αυξημένης χρήσης της πληροφορικής στον τομέα των βιοεπιστημών και των ιατρικών επιστημών (Saadia Arshad κ.α. 2021).

Το 2010 το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ, δημιούργησε ένα λεξικό κινδύνου με διάφορες ορολογίες, σύμφωνα με το οποίο για την βιοασφάλεια και την κυβερνοβιοασφάλεια πρέπει να ληφθεί υπόψη συνάρτηση τριών στοιχείων: οι απειλές στις οποίες είναι επιρρεπής ένα στοιχείο ή ένα σύστημα, τα τρωτά σημεία του στοιχείου ή του συστήματος στην απειλή και οι πιθανές συνέπειες που προκύπτουν από την υποβάθμιση του στοιχείου ή του συστήματος. Καθένα από αυτά τα στοιχεία ορίζεται ως εξής: Απειλή: Είναι ένα φυσικό ή ανθρωπογενές συμβάν, μια ατομική ή μαζική ενέργεια που έχει ή υποδεικνύει τη δυνατότητα να βλάψει τη ζωή, τις πληροφορίες, τις λειτουργίες, το περιβάλλον ή/και την ιδιοκτησία. Ευπάθεια: είναι ένα φυσικό ή λειτουργικό χαρακτηριστικό που καθιστά μια οντότητα ανοιχτή σε εκμετάλλευση ή επιρρεπής σε έναν δεδομένο κίνδυνο. Συνέπειες: Είναι η

επίδραση ενός γεγονότος, περιστατικού ή συμβάντος. Η συνέπεια συνήθως αποδομείται και μετριέται σε τέσσερις κατηγορίες: την ανθρώπινη, την οικονομική, το είδος της αποστολής και την ψυχολογική. Μια άλλου είδους ανάλυση που βοήθα στην κατανόηση της σημασίας της κυβερνοβιοασφάλειας είναι αυτή μεταξύ των εξαρτήσεων και των αλληλεξαρτήσεων. Οι αλληλεξαρτήσεις είναι σημαντικές για το πώς ο δημόσιος και ο ιδιωτικός τομέας κατανοούν, αναλύουν και διαχειρίζονται τον κίνδυνο σε κρίσιμους τομείς υποδομής και άλλα πολύπλοκα συστήματα. Η εξάρτηση είναι μια μονόδρομη σχέση μεταξύ δύο στοιχείων, στα οποία οι λειτουργίες ενός στοιχείου επηρεάζουν τις δραστηριότητες του άλλου (Daniel S. κ.α. 2019). Για παράδειγμα, μια μονάδα επεξεργασίας νερού μπορεί να εξαρτάται από μια εξωτερική πηγή δεδομένων για την επεξεργασία του νερού της για το εάν είναι πόσιμο. Η αλληλεξάρτηση είναι μια αμφίδρομη σχέση μεταξύ δύο στοιχείων, στα οποία οι λειτουργίες και των δύο στοιχείων επηρεάζουν η μία την άλλη. Για παράδειγμα, η μονάδα επεξεργασίας νερού χρειάζεται να επικοινωνεί με το σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων που επεξεργάζεται την καταλληλότητα του νερού, το οποίο με τη σειρά του, παρέχει το νερό που χρησιμοποιείται από το σύστημα, για να ψύξει τον εξοπλισμό του. Μια αλληλεξάρτηση είναι ουσιαστικά ο συνδυασμός δύο εξαρτήσεων και επομένως, η κατανόηση μιας αλληλεξάρτησης απαιτεί την ανάλυση και κατανόηση των εξαρτήσεων.

Συνοψίζοντας και όπως θα αναλυθεί στα επόμενα κεφάλαια αναλυτικά η κυβερνοβιοασφάλεια:

- «Επικεντρώνεται στην στρατηγική χρήση του κυβερνοχώρου και των πληροφοριών που αφορούν τις βιολογικές απειλές»,
- «Αναλύει και εξειδικεύει τις πολιτικές κυβερνοασφάλειας που έχουν ως στόχο…την προστασία των κρίσιμων πληροφοριών σε θέματα βιοτεχνολογίας και φαρμακευτικών δεδομένων μεταξύ των εμπλεκόμενων φορέων»,

- «Προωθεί με ασφάλεια αλλά και με ηθική προσέγγιση τη δημιουργία, τη διαβίβαση και τη διαχείριση των ψηφιακών ιατρικών δεδομένων από τους διάφορους φορείς που παράγονται και διακινούνται ψηφιακά σε κεντρικές βάσεις δεδομένων»,
- «Εξασφαλίζει την αποτελεσματική και ασφαλή εφαρμογή βιομετρικών συσκευών αλλά και των βιομετρικών δεδομένων που είναι ενσωματωμένα στις σύγχρονες συσκευές (π.χ. κινητά) καθώς και την αποτελεσματική διαχείριση και προστασία των βιομετρικών πληροφοριών των ανθρώπων σε βάσεις δεδομένων»,
- «Εξασφαλίζει τη σωστή και ηθική χρήση των αναδυόμενων ψηφιακών τεχνολογιών που συνδέονται με τον κυβερνοχώρο όπως π.χ. της τεχνητής νοημοσύνης»,
- « Προσπαθεί να διασφαλίσει τη συνεχή και αξιόπιστη ροή πληροφοριών σχετικά με μια πανδημία και γενικότερα για όσα εστιάζουν σε παγκόσμια θέματα βιοασφάλειας και βιοπολιτικής»,
- «Αναλύει και ελέγχει τις πιθανές επιπτώσεις των νέων ψηφιακών τεχνολογιών στο πλαίσιο του κυβερνοχώρου και στην ανθρώπινη βιοασφάλεια…στο πλαίσιο της ευρείας ανάπτυξης του διαδικτύου των πραγμάτων (Internet of things), στο οποίο άνθρωποι, συσκευές και μηχανές θα είναι δια-συνδεδεμένοι και θα αλληλεπιδρούν μέσα από ένα σύστημα ψηφιακών τεχνολογιών και αισθητήρων»,
- «Ελέγχει τη συνεχόμενη αλληλεξάρτηση μεταξύ των νέων ψηφιακών τεχνολογιών και της βιοασφάλειας, ειδικά στο πλαίσιο χρήσης των αναδυόμενων αυτών τεχνολογιών ως βασικών τεχνολογικών στοιχείων στην εκδήλωση υβριδικού πολέμου»,
- «Προστατεύει τα αποτελέσματα κλινικών, ιατρικών και φαρμακευτικών μελετών τα οποία καταχωρούνται σε βάσεις δεδομένων ή σε εξυπηρετές (servers), από την κατασκοπεία ή τις κυβερνοεπιθέσεις από εξωτερικούς χρήστες (hackers)» και
- «Αναλύει θέματα Αστρο-κυβερνο-ασφάλειας που έχει ως στόχο την έρευνα της αυξημένης αλληλεξάρτησης μεταξύ της στρατηγικής χρήσης του διαστήματος και των δορυφόρων με τον κυβερνοχώρο και την βιοασφάλεια». (Λιαρόπουλος Α. και Μποζίνης Α. (Επιμ.), 2022)

3.1. Η σημασία και το αντικείμενο της κυβερνοβιοασφάλειας

Το ενδιαφέρον της βιομηχανίας για την τεχνητή νοημοσύνη έχει αυξηθεί κατακόρυφα τα τελευταία χρόνια λόγω της προηγμένης πληροφορικής, των εφαρμογών νευρωνικών δικτύων και της εμφάνισης νέων τεχνικών μηχανικής στον τομέα της βιολογίας. Οι εταιρείες βιοτεχνολογίας αξιοποιούν με επιτυχία αυτές τις εξελίξεις για το σχεδιασμό φαρμάκων και γενόσημων. Η γρήγορη και εξελισσόμενη τεχνολογία της τεχνητής νοημοσύνης και ευκολία στην πρόσβασή της, δημιούργησε νέες απειλές που σχετίζονται με το απόρρητο και την αποθήκευση πληροφοριών, την ιδιοκτησία σε βιολογικά και γενετικά δεδομένα και τις εφαρμογές ισχυρών τεχνολογιών. Η τεχνητή νοημοσύνη και η ρομποτική οδήγησαν σε αυτοματοποιημένες διαδικασίες την επιστήμη της βιολογίας (Lauren C.Richardson κ.α., 2019).

Οι βελτιωμένες τεχνικές βιολογικής μηχανικής και τα εργαστήρια χρησιμοποιούν όλο και περισσότερο ρομπότ για καλύτερη απόδοση και λιγότερα ανθρώπινα χέρια. Τα ρομπότ συνδέονται όλο και περισσότερο με δίκτυα και άλλα ηλεκτρονικά συστήματα, δημιουργώντας αυτοματοποιημένα εργαστήρια, τα οποία με την σειρά τους δημιουργούν νέες προκλήσεις για την κυβερνοβιοασφάλεια, καθώς υπάρχει πιθανότητα για μη εξουσιοδοτημένη και απομακρυσμένη πρόσβαση σε ένα αυτοματοποιημένο σύστημα παραγωγής. Αντίστοιχες προκλήσεις υπάρχουν στην συνθετική βιολογία, η οποία χρησιμοποιώντας τις προαναφερόμενες τεχνολογίες σχεδιάζει γενετικά κυκλώματα, νέα μόρια και αγαθά όπως καύσιμα, ηλεκτρική ενέργεια, ζωοτροφές και ανανεώσιμες πηγές ενέργειας, κάνοντας τις τεχνικές του εργαστηριακού αυτοματισμού πιο διαδεδομένες.

Επιπλέον, οι περισσότεροι οργανισμοί-επιχειρήσεις πλέον εξαρτώνται από την επιστήμη και την τεχνολογία, ενώ η δομή και το εύρος τους, γίνεται όλο και πιο σύνθετο και δικτυωμένο όσο αναφορά τις εγκαταστάσεις τους, οι οποίες περιλαμβάνουν μεταξύ άλλων, την γραμμή παραγωγής, την γραμμή προμηθειών, τον μηχανισμό μεταφοράς και διανομής των προϊόντων τους. (House, T. W. 2012). Τα αποκεντρωμένα δίκτυα παραγωγής μπορεί να βρίσκονται ακόμη

και σε διαφορετικές ηπείρους και να συνδέονται μεταξύ τους την τεχνολογία. Έτσι και οι παραγωγικές διαδικασίες και η δημιουργία βιολογικών προϊόντων μπορεί να πραγματοποιηθεί ασύγχρονα, από γεωγραφικά διαφορετικές τοποθεσίες.

Στις βιοϊατρικές επιστήμες η ψηφιοποίηση των δεδομένων υγείας τα τελευταία χρόνια έχει αυξηθεί κατακόρυφα. Απόρρητες και προσωπικές ιατρικές πληροφορίες, όπως η διαχείριση της θεραπείας των ασθενών, της πιθανής αλληλεπίδρασης φαρμάκων, τα σχετικά πρωτόκολλα και ειδικές ευαισθησίες και το ιατρικό ιστορικό του ασθενούς, έχουν ψηφιοποιηθεί. (in.go, Μποζίνης, Κυβερνο-βιοασφάλεια και βιο-υβριδικές απειλές). Η εξατομικευμένη ιατρική και τα διαγνωστικά και θεραπευτικά κέντρα διατηρούν ψηφιακά την πλειοψηφία αν όχι το σύνολο όλων των πληροφοριών και δεδομένων τους. Ωστόσο, όπως θα αναλυθεί και στην συνέχεια, οι παραβιάσεις βιοϊατρικών δεδομένων έχουν αυξηθεί ραγδαία τα τελευταία χρόνια. Αυτές οι παραβιάσεις παρέχουν στους δράστες πολύτιμες πληροφορίες για κλινικά δεδομένα, τα οποία θα μπορούσαν να χρησιμοποιηθούν από τους ίδιους ή να πωληθούν για χρηματικό κέρδος. Εκτός από τη διευκόλυνση της συλλογής παράνομων δεδομένων, η διακοπή των ψηφιακά προγραμματισμένων συστημάτων διαγνωστικών ελέγχων και των ιατροτεχνολογικών συσκευών αποτελεί έναν ακόμη τομέα ενδιαφέροντος για την κυβερνοβιοασφάλεια. Για τις βιοεπιστήμες, τα μεγαδεδομένα (big data), αναφέρονται σε σύνολα δεδομένων που περιλαμβάνουν συνδυασμό δεδομένων ή δημοσιευμένα δεδομένα που προέρχονται από το σύστημα υγειονομικής περίθαλψης, την φαρμακευτική βιομηχανία και παραπλήσιους τομείς (Kozminski, K. G. 2015).

Τέλος στον τομέα της γεωργίας, η ασφάλεια των τροφίμων αποτελεί υψηλή προτεραιότητα, καθώς οποιαδήποτε επίπτωση στην ασφάλεια τους έχει άμεσες επιπτώσεις στην οικονομική και κοινωνική ανθεκτικότητα μιας χώρας. Ωστόσο, η γεωργία πλέον σε πολλές χώρες βασίζεται σε ηλεκτρονικά συστήματα και τεχνολογίες για πολλές πτυχές της, όπως η διαχείριση αγροκτημάτων και η παρακολούθηση της παραγωγής. Η προστασία και η ασφάλεια

αυτής της διάστασης της γεωργίας και των συστημάτων που χρησιμοποιεί είναι ασαφή και σχεδόν άγνωστη από την πλευρά της κυβερνοβιοασφάλειας.

3.2. Κυβερνοέκγλημα και COVID-19

Η πανδημία COVID-19 φανέρωσε τα τεχνολογικά κενά και τις ευπάθειες των χρηστών τις οποίες οι εγκληματίες επιδιώκουν να εκμεταλλευτούν στον κυβερνοχώρο. Ο περιορισμός των μετακινήσεων, η φυσική απόσταση και τα άλλα μέτρα δημόσιας υγείας που ελήφθησαν μεταμόρφωσαν τόσο την εγκληματική συμπεριφορά όσο και τις μορφές θυματοποίησης σε μακροοικονομική κλίμακα, μειώνοντας ορισμένες εγκληματικές συμπεριφορές όπως π.χ. οικιακή διάρρηξη και αυξάνοντας κάποιες άλλες όπως π.χ., το κυβερνοέγκλημα. Η τηλεργασία των εργαζομένων για την επικοινωνία και την ανταλλαγή πληροφοριών μέσω του διαδικτύου, σε συνδυασμό με τις μη επαρκείς, περιορισμένες ή μηδενικές γνώσεις σε θέματα χειρισμού των νέων τεχνολογιών αποτελέσαν έναν από τους παράγοντες που συνετέλεσαν σε αυτήν την αύξηση (Steven Kemp κ.α., 2021).

Η κοινωνική επαφή των ανθρώπων, η οποία πραγματοποιούνταν κατά την περίοδο της πανδημίας σε μεγάλο βαθμό μέσω του διαδικτύου, η ανησυχία και η διαρκής συζήτηση για τον COVID-19 με μηνύματα ηλεκτρονικού ταχυδρομείου και στον ιστό, σε συνάρτηση με την συναισθηματική ανησυχία που προκλήθηκε στους ανθρώπους από την αβεβαιότητα και τις δυσκολίες της πανδημίας, αποτέλεσε άλλον έναν παράγοντα που εκμεταλλευτήκαν οι κυβερνοεγκληματίες (Johannes Wiggen, 2020). Υπολογίζεται ότι περισσότερο από το 80% των εγκλημάτων είναι επιτυχή λόγω των τεχνικών κοινωνικής μηχανικής που χρησιμοποιούνται από τους εγκληματίες, επιβεβαιώνοντας το γεγονός ότι οι χρήστες του διαδικτύου παραμένουν «ο πιο αδύναμος κρίκος» για την ασφάλεια στον κυβερνοχώρο (Brumfield, 2020).

Ο ανθρώπινος παράγοντας αποτελεί κεντρικό συστατικό της κυβερνοασφάλειας και λαμβάνει υπόψη του, τις ατομικές συμπεριφορές, την προσωπικότητα και τα χαρακτηριστικά της, τις διαδικτυακές δραστηριότητες και την στάση απέναντι στην τεχνολογία (Scott Monteith κ.α., 2021). Η πανδημία αποτέλεσε μια ιδανική ευκαιρία ώστε να αλλάξει το πλαίσιο των κυβερνοεγκλημάτων, καθώς αναθεώρησε τους στόχους τις μεθόδους επίθεσης και αναπροσάρμοσε τις τεχνικές της κοινωνικής μηχανικής, η οποία έλαβε υπόψη της

περιστασιακούς παράγοντες που επέφερε ο COVID-19, όπως η ανάγκη για κοινωνική συνδεσιμότητα, η εξ αποστάσεως εργασία, η αύξηση της ανεργίας, η ανάγκη για ψυχαγωγία/αναψυχή ως αποτέλεσμα του lockdown, οι παραγγελίες προϊόντων από το σπίτι και η αυξανόμενη υποστήριξη των φιλανθρωπικών οργανώσεων. Υπολογίζεται ότι μεταξύ Φεβρουαρίου και Μαρτίου 2020, καταχωρήθηκαν 116.000 νέα ονόματα ιστοσελίδων με θέμα τον κορωνοϊό, με περισσότερες από 2000 κακόβουλες εγγραφές και πάνω από 40.000 εγγραφές υψηλού κινδύνου με στοιχεία συσχέτισης με κακόβουλες διευθύνσεις URL (Szurdi J κ.α., 2020). Σύμφωνα με την έρευνα του Πανεπιστημίου της Πρετόρια, οι κορυφαίοι διεθνείς οργανισμοί αποτέλεσαν στόχο πλαστοπροσωπίας μέσω των δικτύων κοινωνικής δικτύωσης, με την πλειοψηφία των απατών να πραγματοποιούνται στο Facebook σε ποσοστό 82%. Από την ανάλυση των κυβερνοεγκλημάτων σχετικά με τον COVID-19 προέκυψε ότι οι εγκληματίες χρησιμοποιούσαν μια δυναμική διαδικασία που περιλαμβάνει τέσσερα στάδια: α) τον εντοπισμό του στόχου με βάση τους περιστασιακούς παράγοντες-πλαίσιο, β) την συλλογή πληροφοριών σχετικά με τον στόχο, γ) την μέθοδο επίθεσης και δ) την χρήση τεχνικής κοινωνικής μηχανικής. Αυτή η μελέτη είναι από τις πρώτες που υιοθέτησε μια προσέγγιση για το έγκλημα στον κυβερνοχώρο που αναγνωρίζει τη σημασία του πλαισίου διευκόλυνσης, όπως μια παγκόσμια πανδημία και της ενσωμάτωσης περισσότερων περιστασιακών παραγόντων στα σχέδια απάτης τους (Rennie Naidoo, 2020).

Στην επεξήγηση και την κατανόηση της αλλαγής της εγκληματικής συμπεριφοράς συνέβαλε και η θεωρία καθημερινής δραστηριότητας (RAT) (Holt και Bossler, 2008). Αν και η θεωρία της καθημερινής δραστηριότητας προέρχεται από τα ληστρικά εγκλήματα, αναφέρει ότι για τα εγκλήματα που διαπράττονται, πρέπει να υπάρχει η συμβολή τριών παραγόντων σε χρόνο και χώρο: ο πιθανός παραβάτης, ο κατάλληλος στόχος και την απουσία ικανού φύλακα κατά το έγκλημα (Felson και Clarke 1998). Έτσι, με το ξέσπασμα του κορωνοϊού, ένας ειδικός στον κυβερνοχώρο, ένας εμπειρογνώμονας της τεχνητής νοημοσύνης ή οποιοσδήποτε ειδικεύεται στην ασφάλεια στον κυβερνοχώρο και την ανάλυση της διαδικτυακής απάτης ή συνεργάτες σε

συναφείς τομείς θα λειτουργούσε ως φύλακάς εναντίον αυτών που πέφτουν θύματα των εγκληματιών του κυβερνοχώρου, ιδιαίτερα κατά τη διάρκεια του COVID-19 (Sogo Angel Olofinbiyi and Shanta Balgobind Singh 2020).

Τα αποτελέσματα δείχνουν πως τα εγκλήματα στον κυβερνοχώρο λειτουργούν συντονισμένα με δημόσια διαθέσιμες πληροφορίες σχετικά με τον COVID-19. Για παράδειγμα, η κοινωνική αξιοπιστία του Π.Ο.Υ. τον έχει κάνει τέλειο στόχο για πλαστοπροσωπία. Επίσης, οι εγκληματίες στοχεύουν στους απομακρυσμένους εργαζόμενους, μιμούμενοι τις εταιρείες τεχνολογίας που προσφέρουν βιντεοτηλεφωνία, υπηρεσίες διαδικτυακής συνομιλίας και υπηρεσίες φιλοξενίας αρχείων cloud. Τα ανωτέρω επιβεβαιώνονται και από έτερη έρευνα που διεξήχθη από το Ινστιτούτο μοριακής βιολογίας και Βιοτεχνολογίας του Πανεπιστήμιου Baha Uddin του Πακιστάν κατά την διάρκεια του πρώτου περιορισμού των μετακινήσεων. Σύμφωνα με την εν λόγω έρευνα το 95% των συμμετεχόντων χρησιμοποιούσε κατά την διάρκεια της πανδημίας κινητό ή άλλη ψηφιακή συσκευή, εκ των οποίων το 53,1 % των συμμετεχόντων παρείχε σε διάφορες ιστοσελίδες περισσότερα προσωπικά στοιχεία αυτό το διάστημα, ενώ το 43.90% των ατόμων θεωρεί σίγουρα ότι οι ιστότοποι που χρησιμοποιούσε (google meet, zoom κ.α) δεν ήταν ασφαλής και κλαπήκαν τα προσωπικά τους δεδομένα με το 35,7% να εκφράζει τις αμφιβολίες του σχετικά με την ασφάλεια και την χρήση των προσωπικών του δεδομένων. (Muhammad Kashan Javed, 2020).

Στο Ηνωμένο Βασίλειο σύμφωνα με τα επίσημα στατιστικά στοιχεία, τα κυβερνοεγκλήματα αυξήθηκαν κατακόρυφα κατά την διάρκεια των περιορισμών σε σχέση με την προηγούμενη χρονιά. Ειδικότερα, η υποκλοπή προσωπικών δεδομένων αυξήθηκε κατά 77,4% και οι διαδικτυακές απάτες κατά 50,9%. Ενώ από την έρευνα προέκυψε ότι τα κυβερνοεγκλήματα έναντι ιδιωτών αυξήθηκαν κατά 40,9% σε σχέση με αυτά που πραγματοποιήθηκαν σε βάρος των επιχειρήσεων και των οργανισμών όπου η αύξηση ήταν 3,9%, γεγονός που συνδέεται με το προσωρινό κλείσιμο της πλειοψηφίας τους κατά την διάρκεια των περιορισμών (David Buil-Gil κ.α., 2020). Η πανδημία COVID-19 δημιούργησε

ιδανικές κοινωνικές και οικονομικές συνθήκες που επηρέασαν τους εγκληματίες στον κυβερνοχώρο. Πολλές ανακοινώσεις και ειδήσεις στα μέσα ενημέρωσης συνδυάστηκαν με μια αντίστοιχη εκστρατεία κυβερνοεπιθέσεων χρησιμοποιώντας ένα συμβάν ή μια είδηση για να το επιτύχουν. Για παράδειγμα, την 11-03-2020 η κυβέρνηση του Ηνωμένου Βασιλείου ανακοίνωσε ένα ευρύ φάσμα οικονομικών μέτρων για την ενίσχυση των πολιτών. Ακολούθως, εμφανίστηκαν διάφοροι ιστότοποι, οι οποίοι εκμεταλλευόμενοι την είδηση αυτή, παρείχαν δήθεν οικονομικές αποζημιώσεις στους πολίτες, οι οποίοι έπρεπε να συμπληρώσουν τα προσωπικά τους τραπεζικά στοιχεία, προκειμένου να λάβουν τις αποζημιώσεις με αποτέλεσμα στο τέλος να πέφτουν θύματα απάτης και να αφαιρούνται από τους λογαριασμούς τους χρηματικά ποσά (Collier B., 2020). Άλλες κυβερνο-επιθέσεις λειτουργούσαν με μια phishing καμπάνια που κατεύθυνε τα θύματα να κατεβάσουν ένα αρχείο ή προσπελάσουν μια διεύθυνση URL. Το αρχείο ή διεύθυνση URL ενεργούσαν ως φορέας κακόβουλου λογισμικού το οποίο μετά την εγκατάστασή του λειτουργούσε ως δούρειος ίππος για την οικονομική απάτη (Harjinder Singh κ.α., 2020).

Επίσης, μια άλλη σημαντική παράμετρος της πανδημίας COVID-19 ήταν η παραπληροφόρηση που προκλήθηκε σχετικά με την επιδημία, τα αίτια, τις θεραπείες ή τις παρενέργειες του εμβολίου, το οποίο αναφέρεται πλέον όλο και περισσότερο με τον όρο infodemic (ajtmh.org:infodemic). Το διαδίκτυο από την μια πλημμυρισμένο με διαφορετικά μηνύματα και αναφορές και από την άλλη με έλλειψη πρόσβασης σε αξιόπιστες πηγές πληροφοριών, κατέστησε τους χρήστες του, επιρρεπείς στην παραπληροφόρηση και τις ψευδείς ειδήσεις (fake news). Από τον Νοέμβριο του 2020 όταν έγινε το εμβόλιο για τον COVID-19 διαθέσιμο, σημειώθηκε σημαντική αύξηση της παραπληροφόρησης σχετικά με τις παρενέργειες του εμβολίου, ειδήσεις σχετικά με το εμβόλιο και τις αρνητικές του επιπτώσεις του, οι οποίες κατέκλυσαν τους ιστότοπους κοινωνικής δικτύωσης. Τον Δεκέμβριο του 2020, στην Πολωνία, βρέθηκαν ιστοσελίδες, οι οποίες ζητούσαν από τους χρήστες να συνδεθούν με το προσωπικό τους e-mail, εισάγοντας και τον προσωπικό κωδικό πρόσβασης (του e-mail), ώστε να

συμπληρώσουν μια φόρμα για να εξαιρεθούν από τον εμβολιασμό κατά του COVID-19 τα παιδιά τους (Agnieszka GRYSZCZYŃSKA 2021).

3.3. Κυβερνοβιοασφάλεια και Νοσηλευτικά Ιδρύματα

Αύξηση των επιθέσεων στον κυβερνοχώρο υπήρξε σε οργανισμούς και ιδρύματα υγειονομικής περίθαλψης. Οι κυβερνοεπιθέσεις σε νοσοκομεία, σχετίζονται πρωτίστως με την λήψη δημογραφικών και οικονομικών πληροφοριών, προκειμένου οι δράστες αυτών των επιθέσεων, να αποκτήσουν χρήματα με δεδομένα ψηφιακής ταυτότητας (Michigan University: Data hackers). Στις 13 Μαρτίου 2020, το δεύτερο μεγαλύτερο νοσοκομείο της Τσεχίας, έγινε στόχος απροσδιόριστης κυβερνοεπίθεσης από αγνώστους δράστες. Το νοσοκομείο, το οποίο είχε την ευθύνη για τη διεξαγωγή των τεστ COVID-19, έπρεπε να κλείσει το σύστημα πληροφορικής του και να αναβάλει τις προγραμματισμένες λειτουργίες, εκτελώντας μόνο τις βασικές του λειτουργίες (cyberscoop: hospital-cyberattack-coronavirus).

Επιπλέον, τα νοσοκομεία και άλλες εγκαταστάσεις του τομέα της υγειονομικής περίθαλψης γίνονται στόχος των λεγόμενων «ransomware». Οι εγκληματίες χρησιμοποιούν κακόβουλο λογισμικό για να κρυπτογραφήσουν τα αποθηκευμένα δεδομένα των θυμάτων τους ώστε να τους εκβιάσουν και στην συνέχεια τα δεδομένα αποκρυπτογραφούνται ως αντάλλαγμα της πληρωμής λύτρων. Στο Λονδίνο, για παράδειγμα, ένα εργαστήριο που ήταν έτοιμο να δοκιμάσει ένα εμβόλιο κατά του κορωνοϊού, έπεσε θύμα επίθεσης ransomware. Ενώ η εταιρεία ήταν σε θέση να προστατεύσει τα συστήματα πληροφορικής της επιτυχώς, οι επιτιθέμενοι κατάφεραν να αποσπάσουν τα αρχεία ασθενών τα οποία και δημοσίευσαν στο Διαδίκτυο (forbes:cyber-attack-stolen-data).

Η κυβερνοβιοασφάλεια στον τομέα τον νοσηλευτικών ιδρυμάτων αφορά κυρίως την πρόσβαση ή την διαγραφή των δεδομένων υγειονομικής περίθαλψης των ασθενών, την αδυναμία παροχής υπηρεσιών υγείας όταν μια εγκατάσταση-μηχάνημα υπόκειται σε κυβερνοεπίθεση, ακόμη και τις λανθασμένες διαγνώσεις ασθενειών όταν έχουν παραβιαστεί ιατρικές συσκευές και παρουσιάζουν λανθασμένες πληροφορίες. Τα νοσοκομεία πλέον διαθέτουν πολλές ιατρικές συσκευές συνδεδεμένες στο διαδίκτυο στις οποίες περιλαμβάνονται οι μαγνητική τομογράφοι, οι ηλεκτρονικοί τομογράφοι καθώς και άλλοι νευροδιεγέρτες και

συσκευές νευροχειρουργικής και ρομπότ και έχουν γίνει εδώ και καιρό στόχοι κυβερνοεπιθέσεων (ransomware) που έχουν ως αποτέλεσμα την απώλεια και τη διαγραφή αρχείων ασθενών. Για παράδειγμα η Hancock Health πλήρωσε σε χάκερ 55,000 $ για να ξεκλειδώσει συστήματα μετά από μόλυνση από ransomware. Ειδικότερα, το νοσοκομείο που εδρεύει στο Γκρίνφιλντ, ανέφερε ότι «μια επιτυχημένη επίθεση ransomware κράτησε ομήρους τα συστήματα πληροφορικής του νοσοκομείου, απαιτώντας πληρωμή λύτρων σε Bitcoin (BTC) σε αντάλλαγμα για ένα κλειδί αποκρυπτογράφησης. Οι εγκληματίες ζήτησαν την πληρωμή τεσσάρων Bitcoin, αξίας περίπου 55.000 δολαρίων εκείνη την εποχή. Όταν πραγματοποιήθηκε επίθεση, οι εργαζόμενοι παρατήρησαν αμέσως την παρουσία κακόβουλου λογισμικού, ωστόσο ήταν πολύ αργά για να αποφευχθεί η εξάπλωση του στο σύστημα ηλεκτρονικού ταχυδρομείου του νοσοκομείου, στα ηλεκτρονικά αρχεία υγείας και στα εσωτερικά λειτουργικά συστήματα με αποτέλεσμα πάνω από 1.400 αρχεία ασθενών να μετονομαστούν σε «Λυπάμαι» ως μέρος της επίθεσης» (zdnet: US Hospital pays 55.000$ to hackers).

Προκειμένου να προστατευθούν υποδομές ζωτικής σημασίας, όπως σταθμοί ηλεκτροπαραγωγής, διοικητικές δομές ή νοσοκομεία, η Ευρωπαϊκή Ένωση υιοθέτησε οδηγία για την ασφάλεια των πληροφοριών η οποία και αναπροσαρμόστηκε το 2020, λαμβάνοντας υπόψη και την πανδημία COVID-19. Βάσει αυτής της οδηγίας, τα κράτη μέλη απαιτούν από τους φορείς εκμετάλλευσης «βασικών υπηρεσιών» να εισαγάγουν και να συμμορφώνονται με τεχνικά πρότυπα ασφαλείας, μεταξύ άλλων, για την ενίσχυση της ασφάλειας των συστημάτων πληροφορικής (Οδηγία (2020) 829, 2020/0365). Η πανδημία COVID-19 έδειξε ποιοι οργανισμοί και ιδρύματα είναι πραγματικά κρίσιμοι και σε κρίση. Τα νοσοκομεία είναι σχετικά ήπιοι στόχοι και συχνά πρέπει να μειώσουν το κόστος για να παραμείνουν εντός προϋπολογισμών, κάτι που αντικατοπτρίζεται από ξεπερασμένα και μη ασφαλή συστήματα πληροφορικής, ωστόσο θα έπρεπε να διαθέτουν περισσότερη χρηματοδότηση για την καλύτερη προστασία των συστημάτων πληροφορικής τους. Ο COVID-19 θα μπορούσε επίσης να

χρησιμεύσει ως έναυσμα για τον εντοπισμό νέων οργανισμών που χρειάζονται προστασία ή αξιολόγηση των υφιστάμενων διασφαλίσεών τους.

3.4. Η κυβερνοβιοασφάλεια σε εθνικό και διακρατικό επίπεδο.

Η βιολογία, βιοτεχνολογία, η συνθετική βιολογία και η βιοϊατρική αξιοποιώντας πλέον σύγχρονες μεθόδους, έχουν δώσει την δυνατότητα στα κράτη και τις ιδιωτικές επιχειρήσεις να αναπτύξουν αλγόριθμους για την ανάλυση και την οπτικοποίηση δεδομένων, να δημιουργήσουν νέους βιολογικούς οργανισμούς που έχουν συγκεκριμένες λειτουργίες, να επεξεργαστούν γονιδιωματικές πληροφορίες ασθενών και να δημιουργήσουν νέα φαρμακευτικά και βιοτεχνολογικά προϊόντα. Πολλές υποδομές ζωτικής σημασίας μιας χώρας, μπορούν να επηρεαστούν από αυτές τις εξελίξεις και ως εκ τούτου, διαδραματίζουν σημαντικό ρόλο στη διασφάλιση της κυβερνοβιασφάλειας, όπως είναι η αμυντική βιομηχανία, οι υπηρεσίες έκτακτης ανάγκης, οι επιχειρήσεις ενέργειας, τροφίμων και γεωργίας και οι δομές υγειονομικής περίθαλψης και δημόσιας υγείας (Asha M. 2019). Ο ανταγωνισμός μεταξύ των κρατών σε οικονομικό, υγειονομικό και επιχειρηματικό επίπεδο καθώς και σε επίπεδο εθνικής ασφάλειας, τα έχει οδηγήσει σε ένα διαρκή αγώνα και μια προσπάθεια απόκτησης με οποιαδήποτε τρόπο αυτών των αποτελεσμάτων της επιστημονικής έρευνας. Τα ψηφιακά συστήματα αποθήκευσης και ανάλυσης δεδομένων και οι τεράστιες ποσότητες δεδομένων που είναι προσβάσιμες μέσω του διαδικτύου και διαφόρων εφαρμογών Cloud, με ανεπαρκή ασφάλεια στον κυβερνοχώρο αποτελούν μια από τις μεγαλύτερες απειλές καθώς η διασύνδεση μεταξύ του ψηφιακού και του βιολογικού κόσμου μπορεί να αξιοποιηθεί από κρατικούς παράγοντες, με διάφορα μέσα και επιβλαβείς συνέπειες όπως η κλοπή πληροφοριών, η δημοσίευση εσφαλμένων πληροφοριών ή διακοπή δραστηριοτήτων. Οι απειλές για την εθνική ασφάλεια μιας χώρας αλλά και οι λόγοι για την απόκτηση αυτών των δεδομένων, μπορεί να αφορούν την ενίσχυση της δικής τους οικονομικής ανταγωνιστικότητας έναντι της ζημίας της οικονομίας ενός άλλου κράτους, την δημιουργία-τροφοδότηση βιολογικών όπλων, την αύξηση της σοβαρότητας νόσησης μιας ασθένειας ή και την δημιουργίας μιας νέας ασθένειας, την στοχοποίηση συγκεκριμένων ομάδων του πληθυσμού των αντιπάλων για επίθεση (Kavita M. Berger και Phyllis A. Schneck, 2019).

Ιστορικά η σύνδεση μεταξύ υγείας και διεθνούς ασφάλειας βασιζόταν στην εξάπλωση των ασθενειών και στα θύματα που σχετίζονται με ασθένειες σε πολέμους. Η πολιτική σταθερότητα και οι δημοκρατίες απαιτούν επίσης οικονομική και κοινωνική ευημερία. Η επιδείνωση της δημόσιας υγείας έχει τη δυνατότητα να επηρεάζει την πολιτική αστάθεια και τις δημόσιες αναταραχές στα δημοκρατικά έθνη. Αυτή η άμεση σχέση μεταξύ δημόσιας υγείας και πολιτικής σταθερότητας επιτρέπει στους διεθνείς παράγοντες και τα κράτη να χρησιμοποιούν τη δημόσια υγεία ως εργαλείο σε διεθνές επίπεδο. Ένας άλλος παράγοντας που επηρεάζει τη γενική δημόσια υγεία είναι παγκοσμιοποίηση με τις θετικές και αρνητικές επιρροές της. Όλα αυτά φυσικά προκαλούν ανησυχίες σχετικά με την διασύνδεση της δημόσιας υγείας και της πολιτικής σταθερότητας και αποδεικνύουν ότι η κυβερνοβιοασφάλεια αποτελεί σημαντικό παράγοντα για τις διεθνείς σχέσεις. Επίσης, ενώ πολλές χώρες από την μια επενδύουν μεγάλα ποσά σε βιολογικές έρευνες που θα μπορούσαν να χρησιμοποιηθούν και για την παραγωγή βιολογικών όπλων από την άλλη είναι υπεύθυνες, χωρίς βέβαια αυτό να μπορεί να αποδειχθεί, για πολλά από τα περιστατικά κυβερνοεπιθέσων σε δημόσιους και ιδιωτικούς φορείς άλλων χωρών. Η κλοπή πληροφοριών από μια φαρμακευτική ή βιοτεχνολογική εταιρεία μπορεί να αποκαλύψει εμπορικά μυστικά και να επιτρέψει στους ανταγωνιστές να αναπτύξουν ανώτερα προϊόντα ή/και να φέρουν τα υπάρχοντα προϊόντα στην αγορά πιο γρήγορα, κερδίζοντας την μάχη στην παγκόσμια εμπορική αγορά, ενισχύοντας την εθνική οικονομία μιας χώρας έναντι της άλλης. Τα επιστημονικά δεδομένα που παράγονται σε εργαστήρια έρευνας στον ακαδημαϊκό χώρο, σε μη κερδοσκοπικούς ερευνητικούς οργανισμούς, σε παρόχους υπηρεσιών συνήθως προορίζονται για την δημοσίευση τους για δημόσιο όφελος. Αυτά τα δεδομένα δεν είναι απαραίτητα ευαίσθητα, αλλά αντιπροσωπεύουν τα αποτελέσματα σημαντικών επενδύσεων από μια κυβέρνηση, την βιομηχανία και τους επενδυτές (Xavier-Lewis Palmer, Lucas Potter και Saltuk Karahan 2020).

Επομένως, η κλοπή ή η μεγάλης κλίμακας απόκτηση αυτών των δεδομένων μπορεί να έχει δυσμενείς οικονομικές συνέπειες για τον οργανισμό ή το κράτος, ειδικά εάν αντίπαλα κράτη

απέκτησαν τα δεδομένα με στόχο το ανταγωνιστικό πλεονέκτημα σε έναν δεδομένο τομέα. Ένας τρόπος για να το πετύχουν, πέραν της απομακρυσμένης πρόσβασης, είναι η εγγραφή στρατιωτικών επιστημόνων σε πανεπιστήμια μιας άλλης χώρας με σκοπό την συλλογή και αποστολή πληροφοριών εκ των έσω. Χαρακτηριστικό παράδειγμα είναι η Κίνα, η οποία έχει εγγράψει κρυφά πάνω από 2.500 στρατιωτικούς επιστήμονες σε δυτικά πανεπιστήμια με στόχο την κατασκοπεία ή την κλοπή πνευματικής ιδιοκτησίας κατά τη διάρκεια της θητείας τους (Defense One: China is Secretly Enrolling Military Scientists). Ένα άλλο παράδειγμα κρατικής παρέμβασης τέτοιου είδους είναι η κλοπή ηλεκτρονικών αρχείων υγειονομικής περίθαλψης ασθενών.

3.4.1. COVID-19 και χάκερ που χρηματοδοτούνται από το κράτος

Οι κρατικοί παράγοντες που προσπαθούν να λειτουργήσουν κρυφά στον κυβερνοχώρο για να αποφύγουν πολιτική ευθύνη, εκμεταλλεύονται την κατάσταση χρησιμοποιώντας στοχευόμενο ηλεκτρονικό ψάρεμα ηλεκτρονικά μηνύματα – το λεγόμενο «ψάρεμα με δόρυ» – για σκοπούς κατασκοπείας. Ομάδες χάκερ που πιστεύεται ότι χρηματοδοτούνται από τη Ρωσία, την Κίνα και τη Βόρεια Κορέα χρησιμοποιούσαν εξατομικευμένα μηνύματα ηλεκτρονικού ταχυδρομείου που περιείχαν αναφορές στην πανδημία προκειμένου να μολύνουν τους στόχους τους με κακόβουλο λογισμικό (Cyberscoop: coronavirus-phishing-scams-iran-china).

Η εθνική ασφάλεια δεν ασχολείται μόνο με τις παραδοσιακές στρατιωτικές απειλές στην εποχή της πανδημία του COVID-19, γεγονός αποδεικνύεται από το γεγονός ότι η συλλογή διαδικτυακών πληροφοριών από τις υπηρεσίες πληροφοριών, η λεγόμενη Signals Intelligence (SIGINT), στρέφει την εστίασή της σε νέους στόχους. Οι κλασικοί στόχοι SIGINT είναι πολιτικοί και στρατιωτικοί θεσμοί που θα μπορούσαν, για παράδειγμα, να παρέχουν πληροφορίες σχετικά με τις διαδικασίες λήψης πολιτικών αποφάσεων ή τις στρατιωτικές δυνατότητες μιας χώρας. Εκτός από την αντικατασκοπεία, δηλαδή την προστασία από τις δραστηριότητες άλλων υπηρεσιών πληροφοριών, η βιομηχανική κατασκοπεία είναι ένας άλλος σημαντικός τομέας λειτουργίας για τις υπηρεσίες πληροφοριών στο διαδίκτυο. Οι κυβερνήσεις ενδιαφέρονταν για τις πληροφορίες σχετικά με την εξάπλωση του κορωνοϊού, για τις διαφορετικές εθνικές πολιτικές για τον περιορισμό του ιού και πιθανά φάρμακα καθώς και εμβόλια. Αυτές οι πληροφορίες τους παρείχαν βασικά στρατηγικά οφέλη για την καταπολέμηση της πανδημίας. Κατά συνέπεια, ιδιαίτερα τα ιδρύματα και οργανισμοί του κλάδου της υγείας, της φαρμακευτικής και της βιοτεχνολογίας και οι κρατικοί φορείς σε αυτούς τους τομείς καθώς και οι υποδομές logistics κινούνται στο στόχαστρο των υπηρεσιών πληροφοριών. Για αυτό και δεν αποτελεί έκπληξη το γεγονός ότι, τον Μάρτιο του 2020, μέλη του προσωπικού του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ), ήταν στόχος ηλεκτρονικών μηνυμάτων ψαρέματος (spear-phishing), που πιστεύεται ότι προέρχονταν από το Ιράν. Στα μέσα Μαΐου, το FBI και η

Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών (CISA) προειδοποίησαν από κοινού για ομάδες χάκερ που συνδέονταν με την Κίνα. Η δουλειά τους ήταν να συλλέγουν ψηφιακές πληροφορίες από αμερικανικά ιδρύματα που διεξάγουν έρευνες για τον κορωνοϊό και στόχος τους ήταν ο εντοπισμός και η απόκτηση δεδομένων δημόσιας υγείας που σχετίζονται με εμβολιασμούς, θεραπείες και τεστ κορωνοϊού. Οι ομάδες αυτές που πιστεύεται ότι συνδέονταν με την Κίνα απέστειλαν email με συνημμένα έγγραφα με γνήσιες πληροφορίες υγείας σε στόχους στο Βιετνάμ, τη Μογγολία και τις Φιλιππίνες προκειμένου να τα μολύνουν με λογισμικό υποκλοπής spyware.

Καθώς εκείνο το χρονικό διάστημα δεν μπορούσαν να πραγματοποιηθούν φυσικές συναντήσεις, μεταξύ επιχειρήσεων, κυβερνήσεων και ανθρώπων, όλοι χρησιμοποιούσαν προγράμματα τηλεδιάσκεψης, ανάλογα με τη διαθεσιμότητα και τη φιλικότητα προς τον χρήστη. Στο παρελθόν, αυτά τα κανάλια επικοινωνίας αποτελούσαν ελκυστικό στόχο για τις υπηρεσίες πληροφοριών, όπως φαίνεται από την υπόθεση της Swiss Crypto AG. Οι κυβερνήσεις και οι δημόσιες αρχές συνήθως έχουν ασφαλή κανάλια επικοινωνίας. Στην πανδημία COVID-19 όμως πολλά μέλη κυβερνήσεων και κυβερνητικοί αξιωματούχοι εργάζονταν χωριστά από διαφορετικές τοποθεσίες και συχνά δεν υπήρχαν αρκετά ασφαλείς γραμμές επικοινωνίας. Αυτό φαίνεται από το γεγονός ότι η βρετανική κυβέρνηση, για παράδειγμα, χρησιμοποίησε για συνδιάσκεψη το Zoom, που αναπτύχθηκε από την ομώνυμη αμερικανική εταιρεία. Η εταιρεία που έχει 700 υπαλλήλους στην Κίνα που εργάζονται στην έρευνα και την ανάπτυξη είδε τον αριθμό των χρηστών της να εκτοξεύεται από 10 εκατομμύρια την ημέρα τον Δεκέμβριο του 2019 σε περισσότερα από 200 εκατομμύρια την ημέρα τον Μάρτιο του 2020. Η Zoom προώθησε το προϊόν της υποστηρίζοντας ότι η υπηρεσία διαθέτει κρυπτογράφηση από άκρο σε άκρο, πράγμα που σημαίνει ότι μόνο τα άτομα που εμπλέκονται στην επικοινωνία μπορεί να διαβάσει τις κοινές πληροφορίες. Λόγω ανεπαρκών προτύπων προστασίας δεδομένων και κακής κρυπτογράφησης των μεταδιδόμενων συνομιλιών, στην εταιρεία ασκήθηκε κριτική στις αρχές Απριλίου 2020 (Citizenlab: a quik look at the confidentiality of zoom meetings). Το Zoom

αντέδρασε αμέσως σε αυτά τα παράπονα εφαρμόζοντας ενέργειες για την ενίσχυση της διαφάνειας και της προστασίας δεδομένων και την παροχή των πρώτων ενημερώσεων λογισμικού, παρουσιάζοντας ένα ολοκληρωμένο σχέδιο για τον τρόπο προστασίας δεδομένων και ασφάλειας του προγράμματος που θα μπορούσε να βελτιωθεί στο μέλλον, μεταξύ άλλων με την προγραμματισμένη εφαρμογή πραγματικής κρυπτογράφησης από άκρο σε άκρο. Σύμφωνα με δημοσίευμα, το Γερμανικό Υπουργείο Εξωτερικών απαγόρευσε τη χρήση του Zoom από το προσωπικό του σε κινητές συσκευές μετά από εσωτερικό έλεγχο ασφαλείας.

Εκτός από την κατασκοπεία, τα κράτη μπορούν επίσης να χρησιμοποιούν κυβερνοεπιχειρήσεις για σκοπούς δολιοφθοράς σε περιόδους ειρήνης, δηλαδή να πετύχουν απλά την αλλοίωση του λογισμικού ή την παύση λειτουργίας με σκοπό την αποδυνάμωση του πολιτικού ή οικονομικού συστήματος ενός άλλου κράτους. Με αυτόν τον τρόπο το κράτος που κάνει τη δολιοφθορά αναμένει να επωφεληθεί από μια δεδομένη κατάσταση που θα δημιουργήσει. Σε μια υπάρχουσα κρίση όπως μια πανδημία, τέτοιες επιθέσεις στον κυβερνοχώρο, π.χ. στσ συστήματα πληροφορικής των υποδομών ζωτικής σημασίας, μπορούν να αποτελέσουν πρόσθετη επιδείνωση σε μια ήδη τεταμένη κατάσταση. Το 2017, για παράδειγμα η κυβερνοεπίθεση με το κακόβουλο λογισμικό NotPetya έδειξε ότι οι επιθέσεις στον κυβερνοχώρο μπορούν να έχουν μεγάλη εμβέλεια και συνέπειες ακόμη και χωρίς να προκαλείται άμεση σωματική βλάβη, έχοντας αρνητικό αντίκτυπο στην λειτουργικότητα των υπολογιστών. Η Ουκρανία ήταν ο κύριος στόχος αυτής της επίθεσης, όπου περισσότερες από 80 εταιρείες δέχθηκαν αρχικά επίθεση, συμπεριλαμβανομένης της Εθνικής Τράπεζας της Ουκρανίας. Επίσης, κατά τη διάρκεια της επίθεσης το σύστημα παρακολούθησης της ακτινοβολίας στον πυρηνικό σταθμό του Τσερνομπίλ τέθηκε εκτός λειτουργίας, ενώ ουκρανικά υπουργεία, τράπεζες και συστήματα μετρό επηρεάστηκαν επίσης. Λέγεται ότι ήταν η πιο καταστροφική κυβερνοεπίθεση που έγινε ποτέ και η συνολική ζημιά υπολογίστηκε σε δέκα δισεκατομμύρια δολάρια ΗΠΑ. Η επίθεση έλαβε χώρα μια ημέρα πριν την εθνική εορτή της Ουκρανίας και σύμφωνα με τις κυβερνήσεις των ΗΠΑ και του Ηνωμένου Βασιλείου, πίσω από

την εν λόγω κυβερνοεπίθεση κρύβονταν οι ρώσικες ένοπλες δυνάμεις (CNET: uk said russia is behind destructive 2017 cyberattack in Ukraine).

Εν κατακλείδι, οι προκλήσεις των τρωτών σημείων κυβερνοβιοασφαλείας για τα κράτη πρέπει επί της ουσίας να απαντούν αρχικά στο ερώτημα με ποιον τρόπο τα δεδομένα μπορούν να αξιοποιηθούν από τους αντιπάλους και ποιες συνέπειες προκύπτουν από αυτήν την εκμετάλλευση και στην συνέχεια ποιες θα είναι οι πιθανές αρνητικές επιπτώσεις που μπορεί να προκύψουν για το ίδιο το κράτος. Ακολούθως, κάθε κράτος οφείλει να έχει πρόγραμμα για τον εντοπισμό και την αξιολόγηση του κυβερνοβιολογικού κινδύνου, ώστε να εντοπίζει νέες απειλές, τρωτά σημεία και συνέπειες. Αυτό το πρόγραμμα θα πρέπει να προκύπτει από μια σύμπραξη δημόσιου-ιδιωτικού τομέα μεταξύ όλων των κυβερνητικών υπηρεσιών και εταιρειών του ιδιωτικού τομέα, ακαδημαϊκών ιδρυμάτων και άλλων μη κυβερνητικών οργανώσεων.

3.5. Η προστασία των βιολογικών δεδομένων σε διεθνές και εθνικό επίπεδο

Σε πολιτικό επίπεδο η προστασία των βιολογικών δεδομένων από κυβερνοεπιθέσεις είναι περιορισμένη. Σε διεθνές επίπεδο, το πρωτόκολλο της Ναγκόγια της σύμβασης για τη βιοποικιλότητα που τέθηκε σε ισχύ στις 12 Οκτωβρίου 2014, προωθεί τη διακυβέρνηση όσον αφορά την πρόσβαση και τον δίκαιο και ισότιμο επιμερισμό των οφελών από τη χρήση βιολογικών δεδομένων, πλην ωστόσο των ανθρωπίνων γενετικών πόρων. Το πρωτόκολλο της Ναγκόγια καθορίζει τις βασικές υποχρεώσεις των συμβαλλομένων μερών να λαμβάνουν μέτρα σχετικά με την πρόσβαση στους γενετικούς πόρους, τον καταμερισμό των οφελών και τη συμμόρφωση. Οι υποχρεώσεις πρόσβασης σε εγχώριο επίπεδο έχουν ως εξής:

- Δημιουργία ασφάλειας δικαίου, σαφήνειας και διαφάνειας.
- Παροχή δίκαιων και μη αυθαίρετων κανόνων και διαδικασιών.
- Θέσπιση σαφών κανόνων και διαδικασιών για συναίνεση μετά από ενημέρωση και αμοιβαία συμφωνημένους όρους.
- Πρόβλεψη έκδοσης άδειας ή ισοδύναμου εγγράφου όταν χορηγείται πρόσβαση.
- Δημιουργία συνθηκών για την προώθηση και την ενθάρρυνση της έρευνας που συμβάλλει στη διατήρηση της βιοποικιλότητας και τη βιώσιμη χρήση.
- Να λαμβάνουν δεόντως υπόψη περιπτώσεις υφιστάμενων ή επικείμενων καταστάσεων έκτακτης ανάγκης που απειλούν την υγεία των ανθρώπων, των ζώων ή των φυτών.
- Εξέταση της σημασίας των γενετικών πόρων για τα τρόφιμα και τη γεωργία για την επισιτιστική ασφάλεια.

Οι υποχρεώσεις καταμερισμού των οφελών σε εθνικό επίπεδο αποσκοπούν στην εξασφάλιση της δίκαιης και ισότιμης κατανομής των οφελών που προκύπτουν από τη χρησιμοποίηση των γενετικών πόρων με το συμβαλλόμενο μέρος που παρέχει τους γενετικούς πόρους. Η αξιοποίηση περιλαμβάνει έρευνα και ανάπτυξη σχετικά με τη γενετική ή βιοχημική σύνθεση των γενετικών πόρων, καθώς και μεταγενέστερες εφαρμογές και εμπορευματοποίηση. Η κοινή χρήση υπόκειται σε αμοιβαία συμφωνημένους όρους. Τα οφέλη μπορεί να είναι χρηματικά ή μη

χρηματικά, όπως τα δικαιώματα εκμετάλλευσης και η ανταλλαγή των αποτελεσμάτων της έρευνας.

Οι υποχρεώσεις συμμόρφωσης με την εθνική νομοθεσία ή τις κανονιστικές απαιτήσεις του συμβαλλόμενου μέρους που παρέχει γενετικούς πόρους, καθώς και οι συμβατικές υποχρεώσεις που αντικατοπτρίζονται σε αμοιβαία συμφωνηθέντες όρους, αποτελούν σημαντική καινοτομία του πρωτοκόλλου της Ναγκόγια. Τα συμβαλλόμενα μέρη:

- Λαμβάνουν μέτρα που προβλέπουν ότι η πρόσβαση στους γενετικούς πόρους που χρησιμοποιούνται εντός της δικαιοδοσίας τους έχει γίνει σύμφωνα με προηγούμενη συναίνεση μετά από ενημέρωση και ότι έχουν καθοριστεί αμοιβαία συμφωνημένοι όροι, όπως απαιτείται από άλλο συμβαλλόμενο μέρος.
- Συνεργασία σε περιπτώσεις εικαζόμενης παραβίασης των απαιτήσεων ενός άλλου συμβαλλόμενου μέρους.
- Ενθάρρυνση των συμβατικών διατάξεων για την επίλυση διαφορών με αμοιβαία αποδεκτούς όρους.
- Διασφάλιση της δυνατότητας προσφυγής στο πλαίσιο των νομικών τους συστημάτων όταν προκύπτουν διαφορές από αμοιβαία συμφωνημένους όρους.
- Λήψη μέτρων σχετικά με την πρόσβαση στη δικαιοσύνη.
- Λήψη μέτρων για την παρακολούθηση της χρησιμοποίησης των γενετικών πόρων μετά την αναχώρησή τους από μια χώρα, μεταξύ άλλων με τον καθορισμό αποτελεσματικών σημείων ελέγχου σε οποιοδήποτε στάδιο της αλυσίδας αξίας: έρευνα, ανάπτυξη, καινοτομία, προ-εμπορευματοποίηση ή εμπορευματοποίηση (Convention on Biological Diversity).

Σε επίπεδο Ευρωπαϊκής Ένωσης το ως άνω πρωτόκολλο ενσωματώθηκε στην Ενωσιακή νομοθεσία με τον κανονισμό 511/2014 «σχετικά με τα μέτρα συμμόρφωσης των χρηστών βάσει του Πρωτοκόλλου της Ναγκόγια για την πρόσβαση στους γενετικούς πόρους και τον δίκαιο και ισότιμο καταμερισμό των οφελών που απορρέουν από τη χρησιμοποίησή τους». Ο εν λόγω κανονισμός επικεντρώνεται σε 2 πυλώνες που αφορούν αρχικά τα μέτρα για την πρόσβαση

όπου τα κράτη μέλη είναι ελεύθερα να θεσπίζουν τέτοια μέτρα, εφόσον το κρίνουν σκόπιμο και σε περίπτωση που το κάνουν τα μέτρα αυτά πρέπει να είναι σύμφωνα με τη λοιπή σχετική νομοθεσία της ΕΕ και μέτρα για τη συμμόρφωση των χρηστών όπου επιβάλλει σε όλα τα συμβαλλόμενα μέρη την υποχρέωση να λαμβάνουν μέτρα που εξασφαλίζουν ότι στην περιοχή δικαιοδοσίας τους, χρησιμοποιούνται μόνο γενετικοί πόροι και σχετικές παραδοσιακές γνώσεις που έχουν αποκτηθεί νόμιμα (Κανονισμός 511/2014 της Ε.Ε.)

Σε εθνικό επίπεδο τα παραπάνω ενσωματώνονται με τον ν. 3937/2011 «Διατήρηση της βιοποικιλότητας και άλλες διατάξεις», όπου στο άρθρο 15 αναφέρεται ότι «το σύνολο των γενετικών πόρων της Ελλάδας λογίζεται ως προστατευμένο εθνικό κεφάλαιο. Η χρήση του υπόκειται στους όρους και περιορισμούς, για την πρόσβαση στους γενετικούς πόρους, καθώς και το δίκαιο και ισότιμο καταμερισμό των ωφελειών που προκύπτουν από τη χρήση τους..» (ν. 3937/2011, ΦΕΚ 60/Α/31-3-2011).

3.6. Κυβερνοβιοασφάλεια και βιοφαρμακευτικά προϊόντα

Τα βιοφαρμακευτικά προϊόντα ή τα βιολογικά προϊόντα χρησιμοποιούν μηχανικά συστήματα ως πλατφόρμες για την κατασκευή θεραπευτικών προϊόντων για την πρόληψη ή τη θεραπεία ασθενειών, όπως ο καρκίνος, ο διαβήτης, οι αυτοάνοσες διαταραχές και οι μικροβιακές λοιμώξεις. Αυτά τα προϊόντα περιλαμβάνουν τα εμβόλια, τα μονοκλωνικά αντισώματα, καθώς και αναδυόμενες βιοτεχνολογίες, όπως κυτταρικές και γονιδιακές θεραπείες. Αν και οι διάφορες κατηγορίες θεραπευτικών μεθόδων διαφέρουν στον τρόπο παρασκευής τους, σε κάθε διαδικασία, οι πληροφορίες «ρέουν» επανειλημμένα μεταξύ βιολογικών πληροφοριών (δηλαδή γενετικών) και διαδικτυακών (δηλαδή ψηφιακών) πληροφοριών.

Η διασφάλιση αυτής της ροής πληροφοριών μέσω της προσεκτικής αξιολόγησης των τρωτών σημείων και των απειλών για τη βιοφαρμακευτική παραγωγή είναι κρίσιμη για τη δημόσια υγεία, την οικονομική ασφάλεια και την εθνική ασφάλεια και εδώ εντοπίζονται δύο τρωτά σημεία. Το πρώτο έχει να κάνει με την φύση της πλατφόρμας βιολογικής παραγωγής, καθώς οι πληροφορίες που περιέχονται στα βιολογικά συστήματα εξελίσσονται και αλλάζουν περιεχόμενο με τρόπους που μπορεί να μην είναι κατανοητοί ή προβλέψιμοι, με αποτέλεσμα να παρουσιάζονται κίνδυνοι για τη συνοχή του προϊόντος (Jennifer L κ.α., 2019). Η δυναμική φύση των γενετικών πληροφοριών που βοηθούν στην επιβίωση σε φυσικά περιβάλλοντα θέτει προκλήσεις σε ένα τεχνητό περιβάλλον. «Για παράδειγμα, κάποια αλλαγή στις γενετικές πληροφορίες ενός κυτταρικού πληθυσμού είναι αναπόφευκτη κατά τη διάρκεια της επέκτασης και της ανάπτυξης σε έναν βιοαντιδραστήρα, οπότε οι διαδικασίες βιοκατασκευής πρέπει να αντιμετωπίσουν ετερογενείς πληθυσμούς κυττάρων που μπορεί να αποδώσουν ένα ετερογενές προϊόν, είτε βιομοριακό είτε κυτταρικό» (NIST: Framework for Improving Critical Infrastructure Cybersecurity). Η ικανότητα των βιολογικών συστημάτων να μεταβάλλουν το περιεχόμενο και την έκφραση των γενετικών τους πληροφοριών παρουσιάζει σημαντική πολυπλοκότητα για τη βιοφαρμακευτική παραγωγή, η οποία πρέπει να λαμβάνεται υπόψη στις

στρατηγικές για τον μετριασμό του κινδύνου κυβερνοβιοασφάλειας. Το ζήτημα της εγγενούς βιολογικής διακύμανσης αποτελεί κρίσιμη πρόκληση στην παρασκευή αναδυόμενων κατηγοριών γονιδιακών και κυτταρικών θεραπειών, όπου η τυπική παραγωγή μικρών παρτίδων σε μια ευρύτερη ποικιλία προϊόντων αποκλείει την εξάρτηση από μεγάλα ιστορικά σύνολα δεδομένων για τον εντοπισμό λεπτών αποκλίσεων της διαδικασίας. Για αυτά τα προϊόντα μικρής παρτίδας, η λεπτή γενετική απόκλιση κατά τη διάρκεια των σταδίων κυτταρικής επέκτασης μπορεί να μεγεθυνθεί λόγω των διαφορών μεταξύ του ξενιστή και του ασθενούς.

Η ασφάλεια των γενετικών πληροφοριών στην κυβερνο-βιολογική διεπαφή διασφαλίζεται αρχικά μέσω της ακεραιότητας τους, καθώς χρησιμοποιούνται για τη μετάδοση μιας κυτταρικής σειράς. Αυτή η διαδικασία μεταφέρει αποτελεσματικά ψηφιακές πληροφορίες σε μια «παραγωγική διαδικασία». Σε όλες αυτές τις ροές εργασίας, χρησιμοποιούνται συνεπή πρωτόκολλα επέκτασης της κυτταρικής καλλιέργειας για την επίτευξη σταθερού πλαισίου για τις γενετικές πληροφορίες, με σκοπό την ελαχιστοποίηση των φυσικών μεταλλάξεων. Η ασφάλεια των γενετικών πληροφοριών κατά τη διάρκεια της παραγωγής μεγιστοποιείται επίσης μέσω σαφώς καθορισμένων στρατηγικών ελέγχου της διαδικασίας. Αυτό το πλαίσιο περιλαμβάνει συνθήκες ανάπτυξης βιοαντιδραστήρα, όπως η στρατηγική τροφοδοσίας, η συγκέντρωση διαλυμένου οξυγόνου, η ροή αερίου, το pH και η θερμοκρασία. Οι κυτταρικοί πληθυσμοί που παρουσιάζουν γενετική αστάθεια κατά τη διάρκεια της ανάπτυξης του βιοαντιδραστήρα εντοπίζονται μέσω αποκλίσεων από τις καθιερωμένες παραμέτρους της διεργασίας, έτσι ώστε οι διαδικασίες να μπορούν να ματαιωθούν σε πρώιμα στάδια και να μην υπάρχει κίνδυνος για την ποιότητα του προϊόντος (Donovan Guttieres κ.α., 2019). Η βιομηχανία μετριάζει τους κινδύνους που σχετίζονται με την αβεβαιότητα στα προφίλ ασφάλειας των προϊόντων λόγω φυσικής διακύμανσης ή μόλυνσης στο βιολογικό σύστημα, μέσω εκτεταμένων στρατηγικών ελέγχου και διασφάλισης ποιότητας, ακολουθώντας καθιερωμένες βέλτιστες πρακτικές και αυστηρές κανονιστικές οδηγίες. Επιπλέον, καθώς η πρόσβαση στις εγκαταστάσεις είναι περιορισμένη για να διασφαλίσει τόσο την προστασία των εμπορικών

μυστικών όσο και τη συμμόρφωση με τους ισχύοντες κανονισμούς ορθής παρασκευαστικής πρακτικής είναι δύσκολο να υπάρξουν σενάρια με κακόβουλες πράξεις κατά την βιοεπεξεργασία. Ωστόσο, μια κακόβουλη εισβολή αυξάνει την αβεβαιότητα στη κυβερνο-βιολογική διεπαφή και θα μπορούσε να προκαλέσει απώλειες παρτίδων, με σημαντικές οικονομικές επιπτώσεις για τη βιομηχανία και θα μπορούσε ενδεχομένως να οδηγήσει σε ελλείψεις φαρμάκων. Κατά τη διάρκεια της παραγωγής θεραπευτικών π.χ. πρωτεϊνών, υπάρχουν ευπάθειες κυβερνοασφάλειας σε κάθε σημείο όπου οι γενετικές πληροφορίες αποθηκεύονται, εκφράζονται, αναπαράγονται ή παρακολουθούνται μέσω διαδικτυακών ή κυβερνοφυσικών συστημάτων. Τέτοια παραδείγματα είναι η αποθήκευση κυττάρων σε καταψύκτη με συστήματα συναγερμού και παρακολούθησης θερμοκρασίας συνδεδεμένα σε δίκτυο, όπου μία αποτυχία στο δίκτυο μπορεί να έχει ως συνέπεια την αβεβαιότητα στη βιωσιμότητα αυτών των κυττάρων ή μια εισβολή στον κυβερνοχώρο που μπορεί να καταστρέψει την ψηφιακή εγγραφή που τεκμηριώνει τις συνθήκες αποθήκευσης των κυττάρων. Και στις δύο περιπτώσεις, η αβεβαιότητα της βιωσιμότητας των κυττάρων παρουσιάζει ευπάθεια, ακόμη και αν η πραγματική επίδραση στα αποθηκευμένα κύτταρα ήταν αμελητέα. Η συστηματική αξιολόγηση των τρωτών σημείων και των απειλών στις κυβερνο-βιολογικές διεπαφές για αυτές τις διαδικασίες, μειώνει τα εναπομείναντα τρωτά σημεία από κακόβουλες πράξεις.

Το δεύτερο σημείο, είναι η ακεραιότητα των δεδομένων που σχετίζονται με τη διαδικασία παρασκευής φαρμακευτικών προϊόντων, συμπεριλαμβανομένων των δεδομένων που σχετίζονται με την αλυσίδα εφοδιασμού και τα κυβερνοφυσικά συστήματα. Οι φαρμακευτικοί κατασκευαστές βασίζονται στην τεχνολογία ως μέρος των καθημερινών λειτουργιών τους, για την παρακολούθηση και τον έλεγχο των διαδικασιών παραγωγής των προϊόντων τους. Η παρασκευή φαρμακευτικών προϊόντων περιλαμβάνει δεδομένα που υποστηρίζουν την ανάπτυξη και την αύξηση της διαδικασίας παρασκευής, κλινικά δεδομένα, δεδομένα μετά την έγκριση και τον εξοπλισμό που χρησιμοποιείται για την κατασκευή του προϊόντος (Peccoud, J. κ.α., 2018). Καθώς αυξάνεται ο αριθμός των διασυνδεδεμένων συσκευών και συστημάτων που

ενημερώνουν όλη την διαδικασία, η ευπάθεια στον κυβερνοχώρο αυξάνεται, επειδή μια ευάλωτη συσκευή μπορεί να οδηγήσει σε απειλή που θέτει σε κίνδυνο ένα μόνο σημείο ή ολόκληρη την διαδικασία, το σύστημα ή την αλυσίδα του εφοδιασμού. Επιπλέον, ως αποτέλεσμα της μεγαλύτερης εξάρτησης από τον αυτοματισμό, η ασφάλεια της μεταφοράς πληροφοριών από τοποθεσία σε τοποθεσία είναι κρίσιμη για τη διασφάλιση της αποτελεσματικότητας της παραγωγικής διαδικασίας.

Οι συνέπειες μιας αποτυχίας στον τομέα της κυβερνοβιοασφάλειας μπορούν να έχουν σημαντικό αντίκτυπο στην προμήθεια φαρμάκων και στην υγεία των ασθενών. Οι ασθενείς που βασίζονται σε φαρμακευτικά προϊόντα μπορεί να επηρεαστούν ιδιαίτερα από ελλείψεις ή ανακλήσεις. Μια παραβίαση της ασφάλειας στον κυβερνοχώρο έχει τη δυνατότητα να «σπάσει» ένα ολοκληρωμένο σύστημα και εάν θεμελιώδεις δραστηριότητες σταματήσουν ή παραβιαστούν, οι φαρμακευτικές δραστηριότητες παραγωγής θα έπρεπε είτε να κλείσουν είτε να υποβληθούν σε λεπτομερή, χειροκίνητη αναθεώρηση και αξιολόγηση. Αυτή η πρακτική στην καλύτερη περίπτωση αυξάνει το κόστος και τις διακυμάνσεις που προέρχονται από τον άνθρωπο και στη χειρότερη θέτει σε κίνδυνο την ποιότητα του παραγόμενου προϊόντος. Οι μη ανιχνεύσιμες «μολύνσεις» κυβερνοβιοασφάλειας θα μπορούσαν να εκδηλωθούν, για παράδειγμα, με εσφαλμένα αποτελέσματα δοκιμών ή ημερομηνίες λήξης, εσφαλμένους βρόχους και αλγόριθμους ελέγχου διαδικασίας, ακατάλληλη συμπεριφορά συντήρησης στη μονάδα ή ακόμη και διακοπή μέσω παρουσίασης ψευδών αστοχιών κατά την επιθεώρηση από τις ρυθμιστικές αρχές (Kathryn Millett, κ.α., 2019).

Για τους λόγους αυτούς, η αξιολόγηση των τρωτών σημείων κυβερνοβιοασφάλειας θα πρέπει να ενσωματώνεται στο σχέδιο συντήρησης και ελέγχου. Τέλος ο κίνδυνος και ο αντίκτυπος μιας αποτυχίας της κυβερνοβιοασφάλειας στην αλυσίδα εφοδιασμού ή σε έναν βασικό προμηθευτή θα μπορούσε να έχει απρόβλεπτο, αρνητικό αντίκτυπο τόσο στη διασφάλιση συνεπούς προμήθειας φαρμακευτικών προϊόντων υψηλής ποιότητας όσο και να θέσει σε κίνδυνο το ίδιο το φαρμακευτικό προϊόν με κακόβουλες επιθέσεις

κυβερνοβιοασφάλειας στη διατήρηση αποστειρωμένων λειτουργιών ή στην ψυκτική αλυσίδα που μπορεί να οδηγήσουν στην απώλεια-καταστροφή του προϊόντος και να θέσουν σε κίνδυνο την ζωή των ασθενών που τα λαμβάνουν.

Τα φαρμακευτικά προϊόντα διαδραματίζουν σημαντικό ρόλο για την δημόσια υγεία. Με την αυξανόμενη ψηφιοποίηση των πληροφοριών που σχετίζονται με τέτοια προϊόντα και τον τρόπο κατασκευής τους, καθίσταται σημαντικό να εξεταστούν οι πιθανές επιπτώσεις από απειλές που σχετίζονται με την ασφάλεια στον κυβερνοχώρο. Μεταξύ των πιθανών επιπτώσεων είναι:

• Οικονομική απώλεια για τη βιομηχανία λόγω παραγωγικής διαδικασίας εκτός προδιαγραφών, κακής ποιότητας προϊόντος ή απώλειας εμπιστοσύνης στην ακεραιότητα της διαδικασίας.

• Επιπτώσεις στους ασθενείς και τη δημόσια υγεία λόγω αναποτελεσματικών, επικίνδυνων ή χαμένων παρτίδων παραγωγής.

• Έκθεση των εργαζομένων σε επιβλαβείς παράγοντες, για παράδειγμα, μέσω της σκόπιμης εισαγωγής ενός παθογόνου στη διαδικασία παρασκευής.

• Αδυναμία ταχείας αντίδρασης σε αναδυόμενες απειλές για τη δημόσια υγεία.

Δεδομένης της σημασίας των ζητημάτων που εγείρονται από τους κινδύνους για την ασφάλεια στον κυβερνοχώρο, απαιτείται συντονισμός και επικοινωνία σε ολόκληρο το οικοσύστημα για την ανάπτυξη μιας ολοκληρωμένης κατανόησης του πεδίου, καθώς και κατάλληλες στρατηγικές μετριασμού. Το πλαίσιο θα μπορούσε ενδεχομένως να προσαρμοστεί ή να διαμορφωθεί με τη συμβολή των ενδιαφερόμενων μερών ώστε να περιλαμβάνει σχετικά πρότυπα, κατευθυντήριες γραμμές και βέλτιστες πρακτικές για τη διαχείριση των κινδύνων κυβερνοβιοασφάλειας. Οι ανησυχίες σχετικά με την ασφάλεια στον κυβερνοχώρο θα πρέπει να αποτελούν μέρος των σύγχρονων συστημάτων διαχείρισης της ποιότητας και θα πρέπει να λαμβάνονται υπόψη κατά την ανάπτυξη και τη διατήρηση στρατηγικών ελέγχου καθ' όλη τη

διάρκεια του κύκλου ύπαρξης του προϊόντος. Η εκπαίδευση και η ευαισθητοποίηση στις βέλτιστες πρακτικές για την ασφάλεια των συστημάτων παραγωγής στον κυβερνοχώρο είναι ουσιαστικής σημασίας για το προσωπικό που συμμετέχει στις διαδικασίες. Η δημιουργία τυποποιημένων πρακτικών για την ασφάλεια στον κυβερνοχώρο σε κάθε στάδιο της διαδικασίας παραγωγής μπορεί να οδηγήσει σε ασφαλέστερη προμήθεια φαρμάκων που σώζουν ζωές, βελτιώνοντας τελικά τη ζωή μέσω μιας υγιούς κοινωνίας και μιας ισχυρής οικονομίας (Sokolov κ.α., 2017). Καθώς η βιομηχανία εξετάζει όλο και περισσότερο την προηγμένη παραγωγή, ιδίως για νέες θεραπευτικές μεθόδους, η κυβερνοβιοασφάλεια πρέπει να έχει τον πρωταγωνιστικό ρόλο στον σχεδιασμό ψηφιακών στρατηγικών, επιχειρηματικών μοντέλων, τεχνολογιών, προτύπων και κανονισμών που διασφαλίζουν την ασφάλεια όλων των σταδίων παραγωγής.

Το παράδειγμα της Merck: Τον Ιούνιο του 2017, η βιοφαρμακευτική εταιρεία Merck &Co. δέχτηκε επίθεση από το κακόβουλο σκουλήκι NotPetya (έχει ξαναφερθεί στο κεφάλαιο 3.4.1.). με αποτέλεσμα να επηρεαστούν τα συστήματα υπολογιστών που χρησιμοποιούνται για τον έλεγχο της διαδικασίας παρασκευής που είχε ως συνέπεια την έλλειψη του εμβολίου Gardasil το οποίο χρησιμοποιείται κυρίως για την πρόληψη του καρκίνου του τραχήλου της μήτρας, με το συνολικό εκτιμώμενο κόστος της κυβερνοεπίθεσης να ανέρχεται κοντά στο 1 δισεκατομμύριο δολάρια (Reuters: Merck says cyber attack halted production, will hurt profits).

3.7. Γεωργία και κυβερνο-βιοασφάλεια

Η γεωργία στις μέρες μας υιοθετεί νέες έξυπνες τεχνολογίες που επιτρέπουν την απομακρυσμένη παρακολούθηση των καλλιεργειών και του ζωικού κεφαλαίου. Στο πλαίσιο αυτό, η χρήση βιολογικών και γενετικών αναλυτικών τεχνολογιών στα ερευνητικά εργαστήρια είναι ευρέως διαδεδομένη για την αξιολόγηση της ποιότητας των τροφίμων, τον εντοπισμό ζωονόσων και την υγεία των ζώων και των φυτών. Επιπλέον, η χρήση της βιοπληροφορικής και των γενετικών τεχνολογιών ενισχύει το ρυθμό ανάπτυξης νέων προϊόντων και καλλιεργειών.

Η διασύνδεση αυτών των τεχνολογιών σε ένα ενιαίο κέντρο ή μια μονάδα παραγωγής και η ανταλλαγή δεδομένων με τους προμηθευτές και τους πωλητές δημιουργεί δίκτυα πληροφοριών και βάσεις δεδομένων που λειτουργούν χωρίς ιδιαίτερη ασφάλεια (Geil A., κ.α., 2018). Με την υιοθέτηση αυτών των τεχνολογιών αυξάνονται οι κίνδυνοι για κυβερνοεπιθέσεις σε αγροτικές επιχειρήσεις. Αυτές οι επιθέσεις έχουν τη δυνατότητα να διαταράξουν την αλυσίδα εφοδιασμού τροφίμων, βλάπτοντας τη βιοοικονομία και την ευρύτερη κοινότητα. Η προστασία της γεωργίας περιλαμβάνει πλέον τόσο τον τομέα της κυβερνοασφάλειας και της βιοασφάλειας, ο συνδυασμός των οποίων συγκροτεί την κυβερνοβιοασφάλεια.

Η κυβερνοβιοασφάλεια εστιάζει στην πρόληψη παράνομων και απομακρυσμένων εισβολέων και στην προστασία των δεδομένων, των πληροφοριών και άλλων διαδικτυακών πόρων που σχετίζονται με τη γεωργία και τις επιστήμες τροφίμων. Η προστασία της γεωργίας και της αλυσίδας εφοδιασμού τροφίμων θεωρείται υψηλής προτεραιότητας, ιδίως με τον αυξανόμενο κίνδυνο επισιτιστικής κρίσης που υπάρχει τόσο λόγω της πανδημίας Covid-19, της ταχείας αύξησης του παγκόσμιου πληθυσμού, όσο και της πολιτικής αστάθειας και της ενεργειακής κρίσης λόγω της εισβολής της Ρωσίας στην Ουκρανία και των κυρώσεων που έχουν επιβληθεί από τις Δυτικές χώρες στην Ρωσία. Δυστυχώς, θεωρείται πρωτόγνωρο για τα αγροτικές επιχειρήσεις να έχουν θωρακιστεί έναντι των κυβερνοεπιθέσων που μπορεί να τις

πλήξουν τόσο λόγω της ανεπαρκούς εκπαίδευσης των ανθρώπων πάνω στον τομέα αυτό όσο και της έλλειψης ή της μη επάρκειας κεφαλαίων, χρόνου και κατάλληλου προσωπικού για την θωράκιση στην κυβερνοβιοασφάλεια. Επίσης, άλλη μια σημαντική παράμετρος που πρέπει να ληφθεί υπόψη είναι ότι οι επιθέσεις στον κυβερνοχώρο που αφορούν στη γεωργία αναφέρονται στις Αρχές από ελάχιστα ως καθόλου λόγω της μη ανίχνευσης του από τα χρησιμοποιηθέντα λογισμικά και δίκτυα.

Ενδεικτική της κατάστασης, αποτέλεσε μια έρευνα που διενεργήθηκε στις ΗΠΑ το φθινόπωρο του 2020, στην οποία συμμετείχαν εμπλεκόμενοι με τον τομέα της αγροοικονομίας σύμφωνα με την οποία μία από τις κύριες προκλήσεις της κυβερνοβιοασφάλειας στον εν λόγω τομέα, είναι η έλλειψη υποδομών και τεχνογνωσίας. Επίσης, σύμφωνα με την ίδια έρευνα οι «έξυπνες φάρμες» δεν κατασκευάζονται πάντα με γνώμονα την κυβερνοβιοασφάλεια και τα μηχανήματα και οι υπολογιστές τους ενδέχεται να μην έχουν εγκατεστημένα και ενημερωμένα μέτρα ασφαλείας για την προστασία των ίδιων και των δεδομένων τους. Εργαζόμενοι ή αγροκτήματα, ανεξαρτήτως μεγέθους δεν έχουν την εκπαίδευση και την ευαισθητοποίηση για την κυβερνοβιοασφάλεια και τον περιορισμό των απειλών της και αυτό μπορεί να οδηγήσει σε προβλήματα όσον αφορά την προστασία των δεδομένων. Τέλος, διαπιστώθηκε ότι υπάρχει έλλειψη συνεννόησης και χρήσης μιας κοινής γλώσσας μεταξύ επαγγελματιών στον τομέα της γεωργίας και της κυβερνοβιοασφάλειας (Susan E. Duncan, κ.α., 2019). Οι κύριες απειλές που αφορούν τομέα της γεωργίας είναι οι εξής:

- «Η έκθεση δεδομένων όπως για παράδειγμα η αφελής έκθεση δεδομένων από άτομα ή από τα κενά ασφάλειας στον κυβερνοχώρο σε μικρές επιχειρήσεις ή εργαστήρια».
- «Η καταγραφή ιδιωτικών δεδομένων με σκοπό τη συγκέντρωση δεδομένων για κέρδος ή προγνωστικό πλεονέκτημα».
- «Η κλοπή πνευματικής ιδιοκτησίας όπως παραδείγματος χάρη σε νέα φυτικά και ζωικά είδη».

- «Ο χειρισμός κρίσιμων αυτοματοποιημένων διαδικασιών οι οποίες βασίζονται σε υπολογιστή, (π.χ. χρόνος θερμικής επεξεργασίας και θερμοκρασία για την ασφάλεια των τροφίμων)».
- «Ανάκτηση του ελέγχου ρομποτικών ή αυτόνομων οχημάτων».
- «Η παραπληροφόρηση που επηρεάζει την εμπιστοσύνη και τη συνεργασία μεταξύ των επιχειρήσεων ή/και των καταναλωτών».
- «Η έλλειψη εξοπλισμού, προμηθειών ή τελικών προϊόντων για την κάλυψη των προσδοκιών».
- «Η έλλειψη της ικανότητας διενέργειας αξιολογήσεων τρωτότητας και ανάπτυξης σχεδίων αντιμετώπισης καταστάσεων έκτακτης ανάγκης όπως η προστασία της παροχής πόσιμου νερού» (Tiffany Drape, κ.α., 2021).

Ενδεικτικές είναι οι κατηγορίες προϊόντων που μπορεί να επηρεαστούν είναι:

Τα γαλακτοκομικά προϊόντα: Η γενετική συντελεί στην αναπαραγωγή και την υψηλή παραγωγή γάλακτος στη γαλακτοκομική βιομηχανία. Τα γενετικά δεδομένα αξιολογούνται ιδιαίτερα ως μέρος της διαδικασίας αναπαραγωγής. Τα αρχεία παραγωγής γάλακτος είναι σημαντικά για τη δημιουργία ζώων υψηλής απόδοσης. Επίσης, τα υπολογιστικά συστήματα χρησιμοποιούνται για τη διατήρηση των θερμοκρασιών επεξεργασίας, των προσθηκών συστατικών, της απολύμανσης και των βημάτων καθαρισμού (Tiffany Drape, κ.α., 2021) .

Τα ζώα διατροφής: Για παράδειγμα, πολλές σειρές φυλών ενσωματώνονται στην παραγωγή χοίρων για να ενισχύσουν την ετερογένεια. Οι γενεαλογικές πληροφορίες των φυλών επηρεάζουν σημαντικά την επιλογή των ιδρυτών για το σύστημα παραγωγής. Η παραβίαση ή η χειραγώγηση των πληροφοριών μπορεί να οδηγήσει σε καταστροφική απώλεια για τους παραγωγούς. Η πιθανή εφαρμογή της τεχνολογίας επεξεργασίας του γονιδιώματος σε ζώα που προορίζονται για τροφή μπορεί επίσης να δημιουργήσει νέες γενετικές πληροφορίες που θα μπορούσαν να βελτιώσουν δραματικά την παραγωγικότητα των ζώων που τρέφονται με τροφή (Tiffany Drape, κ.α., 2021).

Οι καλλιέργειες: Ο τομέας των καλλιεργειών χρησιμοποιεί την τεχνολογία για συλλογή και την ανάλυση δεδομένων που αφορούν από τις συνθήκες του εδάφους έως την απόδοση και τη θέση των μηχανημάτων (Tiffany Drape, κ.α., 2021).

Φρούτα και λαχανικά: Τα φρέσκα φρούτα και λαχανικά είναι προϊόντα που διατίθενται προς πώληση στις τοπικές αγορές και μπορεί να έχουν παραχθεί σε μία από τις πολλές τοποθεσίες σε μια χώρα ή σε άλλες χώρες σε όλο τον κόσμο. Η παραγωγή, η διαλογή, η ταξινόμηση, η ανάμειξη, η μεταφορά, η εμπορία και η πώληση φρέσκων φρούτων και λαχανικών είναι πολύπλοκη και περιλαμβάνει πολλούς παράγοντες της βιομηχανίας με διαφορετικούς ρόλους. Η παρακολούθηση των νωπών προϊόντων από την αρχική παραγωγή έως την κατανάλωση είναι ζωτικής σημασίας για τον περιορισμό της πιθανότητας και των επιπτώσεων των εστιών τροφιμογενών ασθενειών. Οι ακριβείς πληροφορίες για τα προϊόντα και η ταχεία πρόσβαση σε δεδομένα είναι ουσιαστικής σημασίας για τον εντοπισμό μολυσμένων προϊόντων στην αγορά, την πρόληψη ή τον περιορισμό των τροφιμογενών ασθενειών, τον περιορισμό της ζημίας σε μη εμπλεκόμενους παραγωγούς και τη διατήρηση της εμπιστοσύνης των καταναλωτών. Η πρόσβαση στην παρακολούθηση προϊόντων και στα μικροβιολογικά δεδομένα αυξάνεται στη βιομηχανία φρέσκων προϊόντων (Tiffany Drape, κ.α., 2021).

Περιβαλλοντικοί πόροι (νερό): Η ασφάλεια του πόσιμου νερού είναι εξαιρετικά σημαντική για την γεωργία, την επεξεργασία των τροφίμων, τη διασφάλιση της υγείας των καταναλωτών και για την ορθή λειτουργία του οικοσυστήματος. Το ποσοστό του παγκόσμιου πληθυσμού που καταναλώνει πόσιμο νερό από πιστοποιημένες και ελεγχόμενες πηγές νερού είναι περίπου 90%. Ωστόσο, 2,3 δισεκατομμύρια άνθρωποι παγκοσμίως πάσχουν από ασθένειες που σχετίζονται με το πόσιμο νερό. (David G. Schmale, κ.α.,2019). Δεδομένης της σοβαρότητας του κινδύνου και της δυνητικής βλάβης, πρέπει να δοθεί υψηλή προτεραιότητα στη βιοασφάλεια στον κυβερνοχώρο για τον τομέα της διαχείρισης και επεξεργασίας πόσιμου νερού. Ένα ισχυρό πρόγραμμα ασφάλειας στον κυβερνοχώρο για το νερό είναι απαραίτητο για την προστασία της δημόσιας υγείας και την πρόληψη διαταραχών των υπηρεσιών (Panguluri, S., κ.α., 2017).

Η γεωργία εξαρτάται όλο και περισσότερο από την έξυπνη τεχνολογία ώστε να είναι ακριβής και αποτελεσματική. Η κυβερνοβιοασφάλεια είναι επιτακτική για τη μελλοντική ασφάλεια της αλυσίδας εφοδιασμού και της βιοοικονομίας, καθώς οι επιθέσεις στον κυβερνοχώρο που σχετίζονται με αυτή, είναι θέμα χρόνου για το πότε θα συμβούν και όχι πλέον για το αν θα συμβούν. Θα ήταν λοιπόν, συνετό και ωφέλιμο να βελτιωθεί η ασφάλεια στον τομέα αυτό για να αποτραπεί η επιτυχία μιας επίθεσης παρά να έρθει ως αντίδραση σε μια επιτυχημένη επίθεση.

4. Κυβερνοβιοασφάλεια και ανθρώπινο dna

Η αποκρυπτογράφηση του ανθρώπινου γονιδιώματος υπήρξε ωφέλιμη καθώς με βάση τις γονιδιωματικές πληροφορίες και τις πληροφορίες υγείας ενός ατόμου, σε συνδυασμό με την πρόοδο της τεχνολογίας και της πληροφορικής ξεκίνησε η νέα εποχή της μοριακής ιατρικής. Επίσης τα οφέλη της αποκρυπτογράφησης συνέβαλαν στην κατανόηση και αντιμετώπιση των ιών και των μεταλλάξεων τους, την κατανόηση διάφορων μορφών καρκίνου, την ανάπτυξη φαρμάκων, έως και την ανάπτυξη των βιοκαυσίμων. Πολλές χώρες όπως το Ηνωμένο Βασίλειο (genomics: 100000 genomes project), οι ΗΠΑ και η Σαουδική Αραβία έχουν καταβάλει προσπάθειες ώστε να αποθηκεύουν το γενετικό υλικό των πολιτών οι οποίοι πάσχουν από σπάνιες ασθένειες. Σύμφωνα με μια έρευνα εκτιμάται ότι έως το 2025 περίπου 1 δισεκατομμύριο άνθρωποι θα έχουν δώσει γενετικό υλικό το οποίο θα έχει αποθηκευτεί και αποκρυπτογραφηθεί (journal: Big Data Astronomical or Genomical). .

Επιπλέον, σύμφωνα με το MIT μέχρι τις αρχές του 2019 περισσότεροι από 26 εκατομμύρια πελάτες είχαν προσθέσει τις πληροφορίες DNA τους στο διαδίκτυο σε βάσεις δεδομένων που διατηρούνται από τις τέσσερις κορυφαίες εταιρείες δοκιμών DNA (technologyreview: more than 26 million people have taken an at home ancestry test). Ωστόσο, αυτή η αύξηση των ιδιωτικών εταιρειών με απευθείας πρόσβαση στον καταναλωτή (DTC) δημιουργεί ανησυχίες για την ασφάλεια και το απόρρητο όταν πρόκειται για τις γενετικές πληροφορίες ενός ατόμου, για μια σειρά από λόγους. Αρχικά, οι ιδιωτικές εταιρείες (Direct-to-Consumer DTC) ενδέχεται να μοιράζονται τα γονιδιωματικά δεδομένα με τρίτα μέρη χωρίς οι ίδιοι οι δότες να το γνωρίζουν. Μια πρόσφατη μελέτη στις ΗΠΑ ανέφερε ότι περίπου το 67% των εταιρειών DTC παρείχαν ανεπαρκή πληροφορίες σχετικά με το πού χρησιμοποιούν τις συλλεγμένες γονιδιωματικές πληροφορίες του κάθε ατόμου (tandfonline).

Επίσης, οι παραβιάσεις του απορρήτου των προσωπικών δεδομένων έχει σοβαρές αρνητικές επιπτώσεις σε γονιδιωματικές έρευνες ή έρευνες που βασίζονται στο DNA, καθώς τα άτομα θα δεν νιώθουν σίγουρα για την συμμετοχή τους σε αυτές. Τέλος, οι ιδιωτικές εταιρείες, έχοντας μεγάλο όγκο γενετικών δεδομένων γίνονται επικερδής στόχος για τους κυβερνοεγκληματίες τόσο για την υποκλοπή των δεδομένων τους όσο και για την καταβολή λύτρων (ramsware) με την χρήση ψηφιακών τεχνολογιών ή της η κοινωνικής μηχανικής ή μέσω άλλων μεθόδων. Βέβαια, η παραβίαση τέτοιων δεδομένων θα μπορούσε να δημιουργήσει βιογονιδιωματικά όπλα για τη βιοτρομοκρατία (health21initiative: genomics data requires better data protection). Για παράδειγμα, οι πρόσφατες εξελίξεις στη γενετική μηχανική όπως π.χ η τεχνολογία γονιδιακής επεξεργασίας επέτρεψε την εισαγωγή τεχνητών ή ανθρωπογενών κλώνων DNA στα ζωντανά κύτταρα των οργανισμών, με σκοπό την εξέρευση νέων θεραπειών για γενετικές ασθένειες. Εάν όμως βρεθούν σε λάθος χέρια μπορεί να αποδειχθούν καταστροφικές, καθώς μπορεί να χρησιμοποιηθούν π.χ. για την επεξεργασία και τη δημιουργία μεταλλαγμένων ζώων. Ως εκ τούτου, η ασφάλεια, οι μέθοδοι και οι μηχανισμοί που αναλύουν τα γενετικά δεδομένα είναι πρωταρχικής σημασίας για την αποφυγή των πιθανών παραβιάσεων των δεδομένων Dna.

Επίσης, πολλές πρόσφατες βιολογικές έρευνες βασίζονται σε δημόσια διαθέσιμες βάσεις γενετικών δεδομένων και διαφορετικά εργαλεία λογισμικού. Πολλά από τα εργαλεία λογισμικού που χρησιμοποιούνται από τους βιοπληροφορικούς για την αλληλουχία (ανάγνωση, σύνθεση μεγέθους, γραφή, ανάλυση, κοινή χρήση και αποθήκευση δεδομένων DNA/γονιδιώματος) συχνά αναπτύσσονται από ερευνητικές ομάδες οι οποίες δίνουν προτεραιότητα στη λειτουργικότητα του λογισμικού και όχι στην ασφαλή λειτουργία του. Επομένως, εργαλεία που επεξεργάζονται πολύτιμα δεδομένα δεν δημιουργούνται σύμφωνα με τους κανόνες και τα πρότυπα ασφαλείας των λογισμικών, ενώ τα περισσότερα μέχρι πρότινος ήταν εργαλεία ανοιχτού κώδικα που χρησιμοποιούν τις γλώσσες προγραμματισμού C, C++, οι οποίες διδάσκονται στα πρώτα έτη του πανεπιστημίου.

Επιπλέον, παρόλο που οι περισσότερες βάσεις δεδομένων, (οι οποίες θα παρουσιαστούν παρακάτω στη ενότητα 4.3.), απαιτούσαν όνομα χρήστη και κωδικό πρόσβασης για τη είσοδο σε αυτές, σχεδόν καμιά από αυτές δεν απαιτούσε από τον χρήστη να επιλέξει έναν ισχυρό κωδικό πρόσβασης (μακρύς και συμπεριλαμβανομένης της χρήσης κεφαλαίων γραμμάτων, ειδικών χαρακτήρων, συμβόλων και αριθμών).

Συνεπώς, ένας αδύναμος κωδικός πρόσβασης καθιστά αυτές τις βάσεις πολύ ευαίσθητες σε μια κυβερνο-επίθεση που μπορεί να οδηγήσει σε παραβίαση του κωδικού πρόσβασης και κλοπή δεδομένων. Ενδεικτικά τα προβλήματα που προέκυψαν από την μελέτη και την ταξινόμηση της ιδιωτικότητας και της ασφάλειας σχετικά με τα εργαλεία και τις βάσεις δεδομένων βιοπληροφορικής που επεξεργάζονται ή αποθηκεύουν DNA και γονιδιωματικά δεδομένα είναι τα εξής:

1. Κακή κωδικοποίηση των δεδομένων και έλλειψη επικύρωσης εισόδου: Ο κωδικοποίηση των δεδομένων και η επικύρωση εισόδου μπορεί να συνυπάρχουν και να αλληλοσυμπληρώνονται. Πολλές διαδικτυακές πλατφόρμες που επεξεργάζονται ή αποθηκεύουν δεδομένα DNA και γονιδιώματος δεν περιέχουν τέτοιο μηχανισμό. Από την άλλη πλευρά, η κωδικοποίηση των δεδομένων είναι επίσης απαραίτητη αφού το DNA και τα γονιδιωματικά δεδομένα είναι εξαιρετικά ευαίσθητα.

2. Χρήση μη ασφαλών, απαγορευμένων ή απαρχαιωμένων λειτουργιών: Η χρήση μη ασφαλών, απαγορευμένων ή απαρχαιωμένων λειτουργιών, είναι ένα από τα πιο κοινά προβλήματα που παρατηρήθηκαν κατά την ανάλυση των εργαλείων βιοπληροφορικής. Η χρήση μη ασφαλών λειτουργιών μπορεί να οδηγήσει κενά ασφαλείας, όπως π.χ. η υπερχείλιση buffer.

3. Ανεπαρκής μηχανισμός ελέγχου ταυτότητας: Υπάρχουν ανεπαρκείς μηχανισμοί ελέγχου ταυτότητας που εφαρμόζονται για την είσοδο των χρηστών σε πολλές από αυτές τις βάσεις δεδομένων. Οι έλεγχοι συνήθως εφαρμόζονται κατά την μεταφόρτωση δεδομένων αλλά σπάνια εφαρμόζεται κατά τη λήψη DNA και γονιδιωματικών δεδομένων, τα οποία θεωρούνται προσωπικά και ευαίσθητα δεδομένα. Αυτό είναι σημαντικό καθώς οι οργανισμοί έχουν νομική

υποχρέωση να αναλάβουν όλα τα μέτρα για την ασφάλεια των προσωπικών δεδομένων. Επιπλέον, ο μηχανισμός όπως ο κωδικός πρόσβασης που χρησιμοποιείται για την ασφαλή πρόσβαση, είναι σημαντικός.

4. Η χρήση σελίδων με την μορφή HTTP αντί για HTTPS: Ορισμένες διαδικτυακές πλατφόρμες που περιέχουν αυτές τις βάσεις δεν χρησιμοποιούν την μορφή HTTPS, με αποτέλεσμα να εξακολουθούν να είναι ευάλωτες σε κυβερνοεπιθέσεις, όπου μπορούν να υποκλαπούν δεδομένα κατά τη μετάδοση απλού κειμένου, δηλαδή, δεν είναι κρυπτογραφημένες ή ασφαλής.

5. Γονιδιωματικά δεδομένα διαθέσιμα δημόσια: Πλήρη ή μερικά δεδομένα DNA, δημοσιευμένες αλληλουχίες DNA, SNPS, φαινότυπος ή γονότυπος είναι διαθέσιμα μέσω διαδικτυακών βάσεων δεδομένων ή άλλων διαδικτυακών ιστότοπων.

6. Χρήση μη ασφαλών γραμμών εντολών: Μη ασφαλής γραμμές εντολών βρέθηκαν επίσης να χρησιμοποιούνται σε πολλά εργαλεία τέτοιου είδους.

4.1. Είδη κυβερνοεπιθέσεων και κυβερνοεγκλημάτων και τρόποι αντιμετώπισής τους

Πέρα από τα κυβερνοεγκλήματα και τα είδη των κυβερνοεπιθέσεων που αναλύθηκαν στο 1ο κεφάλαιο, υπάρχουν και ειδικότερες κυβερνοεπιθέσεις που αφορούν τις γενετικές βάσεις δεδομένων. Ειδικότερα τέτοιες είναι:

- Επιθέσεις αποκάλυψης χαρακτηριστικών με χρήση DNA (Attribute disclosure attacks using DNA (ADAD): Είναι οι επιθέσεις που χρησιμοποιούν γενετικούς δείκτες ή χαρακτηριστικά προκειμένου να αναγνωρίσουν άτομα και να αποκαλύψουν περαιτέρω πληροφορίες σχετικά με αυτά. Οι επιθέσεις ADAD με το λογισμικό της βιοπληροφορικής χωρίζονται σε τρείς κατηγορίες:

  (α) Γονιδιακή έκφραση: Ένας τύπος επίθεσης ADAD, κατά την οποία αποκτάται πρόσβαση στην γονιδιακή έκφραση των προφίλ των ατόμων που έχουν ένα δεδομένο γενότυπο. Μόλις αποκτήσουν αυτή την πληροφορία μπορούν να συγκρίνουν τα δεδομένα γονιδιακής έκφρασης με ιατρικά δεδομένα και πληροφορίες ασθενών.

  (β) Συνοπτικά στατιστικά στοιχεία: Σύνολα δεδομένων που αποτελούνται μόνο από τις συχνότητες αλληλόμορφων των συμμετεχόντων στην εκάστοτε μελέτη.

  (γ) n=1 σενάριο: n = 1 είναι ένα σενάριο όπου το ευαίσθητο χαρακτηριστικό στο σύνολο δεδομένων σχετίζεται με το γενότυπο ενός ατόμου. Σε αυτή την περίπτωση, ο αντίπαλος μπορεί απλώς να αντιστοιχίσει τα δεδομένα γονότυπου που σχετίζονται με την ταυτότητα του ατόμου και που συνδέεται με αυτό χαρακτηριστικό.

- Επιθέσεις εντοπισμού ταυτότητας: Είναι οι επιθέσεις ανίχνευσης ταυτότητας οι οποίες προσπαθούν να αναγνωρίσουν μοναδικά ένα ανώνυμο δείγμα DNA χρησιμοποιώντας οποιαδήποτε αναγνωριστικά από το σύνολο δεδομένων και διακρίνονται σε τρείς υποκατηγορίες (Peter Ney, κ.α., 2019):

  (α) Επιθέσεις συσχέτισης: Με την χρήση υπηρεσιών DNA τρίτων μπορεί να είναι εφικτή η κλοπή των δεδομένων DNA ενός ατόμου από μια βάση δεδομένων χωρίς την συγκατάθεσή του. Ερευνητές από το πανεπιστήμιο της Ουάσινγκτον, δημιούργησαν μια ψευδή επίθεση χρησιμοποιώντας έναν μικρό αριθμό ειδικά σχεδιασμένων αρχείων και κατάφεραν να εξάγουν γενετικούς δείκτες συμπεριλαμβανομένων και των ιατρικά ευαίσθητων δεικτών από άλλους χρήστες. Οι επιτιθέμενοι μπορούν να κάνουν το ίδιο δημιουργώντας ένα ψευδές σχετικό δείγμα που μιμείται ψευδώς τον συγγενή του υπάρχοντος δείγματος και κλέβει ευαίσθητα δεδομένα.

  (β) Αξιοποίηση μεταδεδομένων[1]: Συχνά δημοσιεύονται σύνολα δεδομένων γονιδιωμάτων με πρόσθετα μεταδεδομένα, τα οποία μπορούν να αξιοποιηθούν για τον εντοπισμό της ταυτότητα ενός άγνωστου γονιδιώματος στο δείγμα. Τα δημογραφικά μεταδεδομένα είναι μια ισχυρή πηγή πληροφοριών αναγνώρισης. Σύμφωνα με μια προηγούμενη μελέτη στις ΗΠΑ, εκτιμήθηκε ότι ο συνδυασμός φύλου, ημερομηνίας γέννησης και ταχυδρομικού κώδικα είναι αρκετός για να ταυτοποιήσουν μοναδικά το 60% των υπηκόων τους.

  (γ) Γενεαλογικός τριγωνισμός: Με την δημιουργία και την ανάπτυξη των διαδικτυακών πλατφορμών και βάσεων δεδομένων για την αναζήτηση γενετικών αντιστοιχιών, ο γενεαλογικός τριγωνισμός έχει γίνει μια εφικτή επίθεση για την εξέρευση μιας ταυτότητας. Τα επώνυμα περνούν από πατέρα σε γιο στις περισσότερες κοινωνίες και αυτό δημιουργεί μια παροδική συσχέτιση με συγκεκριμένο χρωμόσωμα Y που ονομάζεται απλότυπος. Οι επιτιθέμενοι μπορούν επωφεληθούν από τη συσχέτιση του επωνύμου του χρωμοσώματος Y και να συγκρίνουν τον απλότυπο του χρωμοσώματος Y του αγνώστου με εγγραφές γονιδιώματος σε απλότυπο σε αντίστοιχες βάσεις δεδομένων (L. Sweeney κ.α., 2000) και (Peter Ney, κ.α., 2019).

[1] είναι δεδομένα τα οποία περιγράφουν άλλα δεδομένα. Κατά κανόνα, ένα σύνολο μεταδεδομένων περιγράφει ένα άλλο σύνολο δεδομένων, το οποίο αποτελεί μια πηγή.

Τρόποι αντιμετώπισης επίλυσης των προβλημάτων:

1) Θωράκιση του νομικού πλαισίου και διαχείρισης των δεδομένων: Η αύξηση της χρήσης της τεχνολογίας δημιούργησε σημαντικές προκλήσεις σε νομικό και ηθικό επίπεδο, οδηγώντας και σε παραβιάσεις της ιδιωτικής ζωής και κατάχρηση αυτής. Σε αυτό το πλαίσιο, υπάρχει ανάγκη για ένα επαρκές πλαίσιο διακυβέρνησης το οποίο θα μετριάσει την ευκολία της κοινής χρήσης και επεξεργασίας, έχοντας ως αντίβαρο την ασφάλεια και το απόρρητο των γονιδιωματικών δεδομένων. Η υιοθέτηση αυτών των πολιτικών ασφαλείας των οργανισμών που ασχολούνται με γονιδιωματικά δεδομένα είναι ζωτικής σημασίας.
2) Η χρήση κρυπτογράφησης: Ένα από τα κύρια προβλήματα που εντοπίστηκαν είναι η μη ασφαλής αποθήκευση δεδομένων και η κοινή τους χρήση. Λαμβάνοντας μια ολιστική άποψη του τοπίου της απειλής για την επεξεργασία γονιδιωματικών δεδομένων, με την αύξηση της χρήσης των τεχνολογιών που βασίζονται στο διαδίκτυο για την επίτευξη αποτελεσματικής επεξεργασίας των γονιδιωματικών δεδομένων, χρήση κρυπτογραφικών τεχνικών για την ασφάλεια των δεδομένων είναι επιτακτική.
3) Στοιχεία ελέγχου ταυτότητας και αυθεντικοποίησης-ταυτοποίησης: Η αναγνώριση και ο έλεγχος ταυτότητας αποτελεί την πρώτη γραμμή άμυνας για σχεδόν όλες τις εφαρμογές του διαδικτύου. Ωστόσο, λόγω της πολυπλοκότητας και της ανάγκης ισχυρών μηχανισμών και κωδικών πρόσβασης για την ταυτοποίηση, τα βιομετρικά στοιχεία, χρησιμοποιούνται όλο και περισσότερο για την επίτευξη του μηχανισμού ελέγχου ταυτότητας, τα οποία και είναι ανθεκτικά σε κυβερνοεπιθέσεις, έναντι των κωδικών και των ονομάτων.
4) Έλεγχοι πρόσβασης: Οι έλεγχοι πρόσβασης από τις αρμόδιες αρχές εντός των οργανισμών υγειονομικής περίθαλψης που φιλοξενούν DNA και οι βάσεις δεδομένων γονιδιώματος θα μπορούσαν να βελτιώσουν σημαντικά την ασφάλεια των βάσεων αυτών.
5) Ανίχνευση εισβολής και καταγραφή: Η ανίχνευση εισβολής και τα συστήματα παρακολούθησης αποτελούν σημαντικά στοιχεία για την αρχιτεκτονική ασφάλειας και παρέχουν άμυνα σε βάθος. Η χρήση προηγμένων συστημάτων πληροφορικής που επικεντρώνεται στην καταγραφή

γεγονότων του συστήματος και στον εντοπισμό κακής χρήσης του, αποτελούν σημαντικό πλεονέκτημα.

4.2. Οι προκλήσεις της κυβερνοβιοασφάλειας για τις γενετικές βάσεις δεδομένων.

Η ανίχνευση, η ταυτοποίηση και η παρακολούθηση παθογόνων μικροοργανισμών βασίζεται σε μεθόδους δακτυλικών αποτυπωμάτων DNA και μεθόδους γονιδιωμάτων. Τα δεδομένα του γονιδιώματος του ιού Έμπολα και της γρίπης και προσφάτως του COVID-19, χρησιμοποιούνται για παρακολούθηση σε πραγματικό χρόνο, όπως επίσης και τα τροφιμογενή νοσήματα[2] από βακτηριακούς παθογόνους μικροοργανισμούς και τα νοσοκομειακά ξεσπάσματα λοιμώξεων. Επιπλέον, τα γονιδιώματα παθογόνων φυτών χρησιμοποιούνται για τη διερεύνηση επιδημιών και ασθενειών των φυτών, όπως η επιδημία έκρηξης σιταριού στο Μπαγκλαντές το 2016. Ενώ αυτές οι προσεγγίσεις που βασίζονται στο γονιδίωμα παρέχουν πρωτοφανή πλεονεκτήματα σε σχέση με όλες τις προηγούμενες προσεγγίσεις όσον αφορά τη δημόσια υγεία και τη βιοασφάλεια, ενέχουν επίσης νέα τρωτά σημεία και κινδύνους όσον αφορά την ασφάλεια στον κυβερνοχώρο. «Όσο περισσότερο βασιζόμαστε σε βάσεις δεδομένων γονιδιώματος, τόσο πιο πιθανό είναι αυτές οι βάσεις δεδομένων να γίνουν στόχοι κυβερνοεπιθέσεων για να παρέμβουν στη δημόσια υγεία και τα συστήματα βιοασφάλειας θέτοντας σε κίνδυνο την ακεραιότητά τους, παίρνοντάς τους ομήρους ή χειραγωγώντας τα δεδομένα που περιέχουν».

Επίσης, ενώ υπάρχει η δυνατότητα συλλογής γονιδιωματικών δεδομένων παθογόνων από μολυσμένα άτομα ή γεωργικά προϊόντα και προϊόντα διατροφής κατά τη διάρκεια επιδημιών και ασθενειών για τη βελτίωση της μοντελοποίησης και της πρόβλεψης ασθενειών, ο τρόπος προστασίας της ιδιωτικής ζωής των ατόμων, είναι άλλη μια σημαντική πρόκληση για

[2] τροφιμογενές νόσημα είναι κάθε νόσημα που προκαλείται από την κατανάλωση τροφίμου ή νερού [i]. Έχουν περιγραφεί περισσότερα από 250 διαφορετικά τροφιμογενή νοσήματα. https://eody.gov.gr/cat-disease/trofimogeni-nosimata/

την ασφάλεια στον κυβερνοχώρο. Καθώς τα δεδομένα καθίστανται συνδεδεμένα με άλλες πηγές δεδομένων, τα άτομα και οι ομάδες καθίστανται αναγνωρίσιμα και οι πιθανές κακόβουλες δραστηριότητες που στοχεύουν αυτά που εντοπίζονται καθίστανται εφικτές. Οι δημόσιες βάσεις δεδομένων γονιδιώματος κατέχουν το σύνολο της γνώσης της έρευνας του γονιδιώματος που αποκτήθηκε τα τελευταία τριάντα χρόνια και θα λέγαμε ότι είναι ανάλογες με τις δεκάδες χιλιάδες δημόσιες βιβλιοθήκες που κατέχουν τη γνώση της ανθρωπότητας με τη μορφή σχολικών βιβλίων. Οι δημόσιες βάσεις δεδομένων γονιδιώματος αποτελούν τον μοναδικό τρόπο για την έρευνα στον κυβερνοχώρο που στοχεύει στην προστασία της βιοοικονομίας και για τον λόγο αυτό διευκολύνουν την ανοικτή πρόσβαση σε όλους τους χρήστες.

Επιπλέον, οι σημαντικές καινοτομίες στις υπολογιστικές μεθόδους για την ανάλυση γονιδιωματικών δεδομένων καθοδηγούνται επίσης σε μεγάλο βαθμό από τη δημόσια έρευνα και το λογισμικό ανοιχτού κώδικα. Πολλές εταιρείες, ακαδημαϊκά ιδρύματα και κυβερνητικές οντότητες, χρησιμοποιούν λογισμικό ανοιχτού κώδικα και βάσεις δεδομένων που αναπτύχθηκαν στη δημόσια ερευνητική κοινότητα, επειδή οι τελευταίες καινοτομίες στη γονιδιωματική προέρχονται συνήθως από ακαδημαϊκή έρευνα. Αρκετές από τις μεγαλύτερες εταιρείες σύνθεσης DNA ενώθηκαν για να σχηματίσουν τη Διεθνή Κοινοπραξία Γονιδιακής Σύνθεσης (International Gene Synthesis Consortium (IGSC)), μια οργάνωση της εμπορικής βιομηχανίας που αποσκοπεί στην προώθηση της ευεργετικής εφαρμογής της τεχνολογίας σύνθεσης γονιδίων, διασφαλίζοντας παράλληλα τη βιοασφάλεια. Η IGSC δημοσίευσε το Εναρμονισμένο Πρωτόκολλο Διαλογής, για να παρέχει πρόσθετες τακτικές λεπτομέρειες σχετικά με την εφαρμογή του ελέγχου πελατών και αλληλουχιών που συμμορφώνεται με την ισχύουσα νομοθεσία. Το πρωτόκολλο ορίζει ότι οι εντολές συνθετικής αλληλουχίας γονιδίων θα ελέγχονται από ένα σύνολο δεδομένων που συγκεντρώνεται και διατηρείται από την IGSC και υπόκεινται σε κανονιστικό έλεγχο ή αδειοδότηση. Το πρωτόκολλο διευκρινίζει ότι οι εταιρείες που συμμετέχουν στην IGSC θα προμηθεύουν γονίδια μόνο σε «*καλόπιστα* κυβερνητικά

εργαστήρια, πανεπιστήμια, μη κερδοσκοπικά ερευνητικά ιδρύματα ή βιομηχανικά εργαστήρια που αποδεδειγμένα ασχολούνται με νόμιμη έρευνα» (James Diggans και Emily Leprost 2019).

4.3. Βάσεις δεδομένων γενικής χρήσης με πληροφορίες για παθογόνους παράγοντες.

Σχεδόν όλα τα δεδομένα μοριακών αλληλουχιών κατατίθενται στα δύο μεγάλα αποθετήρια γονιδιωματικών δεδομένων, οι οποίες είναι οι βάσεις δεδομένων γονιδιώματος που υπάρχουν στο Εθνικό Κέντρο Βιοτεχνολογικών Πληροφοριών (NCBI) του Εθνικού Ινστιτούτου Υγείας των ΗΠΑ και βάσεις δεδομένων γονιδιώματος που υπάρχουν στο Ευρωπαϊκό Εργαστήριο Μοριακής Βιολογίας (EMBL). Το NCBI και το EMBL παρέχουν βάσεις δεδομένων για αλληλουχίες νουκλεοτιδίων, αλληλουχίες πρωτεϊνών, συγκροτήματα γονιδιώματος κ.α.. Και οι δύο βάσεις δεδομένων έχουν υπολογιστικά εργαλεία για τους χρήστες, ώστε να μπορούν να αναζητούν αυτές τις βάσεις δεδομένων δεδομένα που είναι αποθηκευμένα με την χρήση της γραμμής εντολών ή μιας γλώσσας προγραμματισμού (Saadia Arshad, κ.α.. 2021))

4.3.1. Βάσεις δεδομένων στο NCBI

Η βάση δεδομένων NCBI Assembly, είναι μια βάση δεδομένων για γονιδιώματα διαφορετικών οργανισμών και περιέχει 4.055 σύνολα μυκήτων, 180.914 βακτηρίων και 23.816 συγκροτημάτων ιϊκού γονιδιώματος. Ειδικότερα παρέχει βάσεις δεδομένων, λήψεις, προγράμματα και εργαλεία για την επεξεργασία αυτών των βάσεων, οι οποίες και παρουσιάζονται παρακάτω.

Βάσεις δεδομένων:

Συνέλευση: Μια βάση δεδομένων που παρέχει πληροφορίες για τη δομή των συναρμολογημένων γονιδιωμάτων, ονόματα συγκροτημάτων και άλλα μεταδεδομένα, στατιστικές αναφορές και συνδέσμους προς δεδομένα γονιδιωματικής αλληλουχίας.

BioProject (πρώην Genome Project): Μια συλλογή μελετών γονιδιωματικής, λειτουργικής γονιδιωματικής και γενετικής και συνδέσμων με τα προκύπτοντα σύνολα δεδομένων τους. Αυτός ο πόρος περιγράφει το εύρος, το υλικό και τους στόχους του έργου και παρέχει έναν μηχανισμό για την ανάκτηση συνόλων δεδομένων που είναι συχνά δύσκολο να βρεθούν λόγω ασυνεπούς σχολιασμού, πολλαπλών ανεξάρτητων υποβολών και της ποικίλης φύσης διαφορετικών τύπων δεδομένων που συχνά αποθηκεύονται σε διαφορετικές βάσεις δεδομένων.

Βάση δεδομένων γονιδιωματικής δομικής παραλλαγής (dbVar)**:** Η βάση δεδομένων dbVar έχει αναπτυχθεί για την αρχειοθέτηση πληροφοριών που σχετίζονται με μεγάλης κλίμακας γονιδιωματικές παραλλαγές, συμπεριλαμβανομένων μεγάλων εισαγωγών και διαγραφών,. Εκτός από την αρχειοθέτηση της ανακάλυψης παραλλαγών, το dbVar αποθηκεύει επίσης συσχετίσεις καθορισμένων παραλλαγών με πληροφορίες φαινοτύπου.

Γονιδίωμα: Περιέχει δεδομένα αλληλουχίας και χαρτών από ολόκληρα γονιδιώματα περισσότερων από 1000 οργανισμών. Τα γονιδιώματα αντιπροσωπεύουν τόσο οργανισμούς με πλήρη αλληλουχία όσο και αυτούς για τους οποίους η αλληλουχία βρίσκεται σε εξέλιξη. Αντιπροσωπεύονται και οι τρεις κύριοι τομείς της ζωής (βακτήρια, αρχαία και ευκαρυώτες), καθώς και πολλοί ιοί, φάγοι, ιοειδή, πλασμίδια και οργανίδια.

Genome Reference Consortium (GRC): Διατηρεί την ευθύνη για το γονιδίωμα αναφοράς ανθρώπου και ποντικού. Το GRC εργάζεται για να διορθώσει παραπλανημένους τόπους και να κλείσει τα εναπομείναντα κενά συναρμολόγησης. Επιπλέον, το GRC επιδιώκει να παρέχει εναλλακτικές συναρμολογήσεις για πολύπλοκους ή δομικά παραλλαγμένους γονιδιωματικούς τόπους. Στον ιστότοπο του GRC (http://www.genomereference.org), το κοινό μπορεί να δει τις γονιδιωματικές περιοχές υπό εξέταση, να αναφέρει προβλήματα που σχετίζονται με το γονιδίωμα και να επικοινωνήσει με το GRC.

HIV-1, Βάση δεδομένων αλληλεπίδρασης ανθρώπινης πρωτεΐνης: Μια βάση δεδομένων γνωστών αλληλεπιδράσεων των πρωτεϊνών HIV-1 με πρωτεΐνες από ανθρώπινους

ξενιστές. Παρέχει σχολιασμένες βιβλιογραφίες δημοσιευμένων αναφορών αλληλεπιδράσεων πρωτεϊνών, με συνδέσμους προς τις αντίστοιχες εγγραφές PubMed και δεδομένα αλληλουχίας.

Ιός γρίπης: Μια συλλογή δεδομένων που παρέχει εργαλεία για ανάλυση αλληλουχίας γρίπης, σχολιασμό και υποβολή. Αυτός ο πόρος έχει επίσης συνδέσμους με άλλους πόρους αλληλουχίας γρίπης και δημοσιεύσεις και γενικές πληροφορίες σχετικά με τους ιούς της γρίπης.

NCBI Pathogen Detection Project: Ένα έργο που περιλαμβάνει τη συλλογή και ανάλυση γονιδιωματικών αλληλουχιών βακτηριακών παθογόνων που προέρχονται από απομονώσεις τροφίμων, περιβάλλοντος και ασθενών.

Βάση δεδομένων νουκλεοτιδίων: Μια συλλογή αλληλουχιών νουκλεοτιδίων από διάφορες πηγές.

PopSet: Βάση δεδομένων σχετικών αλληλουχιών DNA που προέρχονται από συγκριτικές μελέτες: φυλογενετικές, πληθυσμιακές, περιβαλλοντικές και, σε μικρότερο βαθμό, μεταλλάξεις. Κάθε εγγραφή στη βάση δεδομένων είναι ένα σύνολο αλληλουχιών DNA. Για παράδειγμα, ένα σύνολο πληθυσμού παρέχει πληροφορίες για τη γενετική παραλλαγή μέσα σε έναν οργανισμό, ενώ ένα φυλογενετικό σύνολο μπορεί να περιέχει αλληλουχίες και την ευθυγράμμισή τους, ενός μεμονωμένου γονιδίου που λαμβάνεται από πολλούς συγγενείς οργανισμούς.

Καθετήρας: Ένα δημόσιο μητρώο αντιδραστηρίων νουκλεϊκών οξέων σχεδιασμένο για χρήση σε μια μεγάλη ποικιλία εφαρμογών βιοϊατρικής έρευνας, μαζί με πληροφορίες σχετικά με τους διανομείς αντιδραστηρίων, την αποτελεσματικότητα του ανιχνευτή και τις ομοιότητες της υπολογισμένης αλληλουχίας.

Πόροι ρετροϊών: Μια συλλογή πόρων ειδικά σχεδιασμένων για την υποστήριξη της έρευνας ρετροϊών.

SARS CoV: Μια σύνοψη δεδομένων για τον κορωνοϊό SARS (CoV), συμπεριλαμβανομένων συνδέσμων με τα πιο πρόσφατα δεδομένα αλληλουχίας και δημοσιεύσεις, συνδέσμους σε άλλους πόρους που σχετίζονται με το SARS.

Αρχείο ανάγνωσης ακολουθίας (SRA): Αποθηκεύει δεδομένα αλληλουχίας από την επόμενη γενιά πλατφορμών αλληλουχίας.

Αρχείο Ιχνών: Μια αποθήκη χρωματογραφημάτων αλληλουχίας DNA (ίχνη), για αναγνώσεις από διάφορα έργα αλληλουχίας μεγάλης κλίμακας.

Ιικά γονιδιώματα: Ένα ευρύ φάσμα πόρων, συμπεριλαμβανομένης μιας σύντομης περίληψης της βιολογίας των ιών, συνδέσμων με αλληλουχίες ιικού γονιδιώματος και πληροφορίες σχετικά με τις αλληλουχίες αναφοράς ιών, μια συλλογή από αλληλουχίες αναφοράς για χιλιάδες ϊϊκά γονιδιώματα.

Παραλλαγή ιού: Μια επέκταση του πόρου του ιού της γρίπης σε άλλους οργανισμούς, παρέχοντας μια διεπαφή για τη λήψη συνόλων ακολουθιών επιλεγμένων ιών, εργαλείων ανάλυσης.

Για την αναζήτηση δεδομένων από τη βάση δεδομένων NCBI, παρέχεται μια ενοποιημένη διεπαφή ιστού που επιτρέπει την υποβολή ερωτημάτων σε όλες τις βάσεις δεδομένων από οποιονδήποτε ανώνυμο χρήστη. Το NCBI επιτρέπει επίσης σε έναν χρήστη να συνθέτει και να χρησιμοποιεί διευθύνσεις URL για την άμεση ανάκτηση δεδομένων από ορισμένες βάσεις δεδομένων. Πολλά σύνολα δεδομένων στο NCBI μπορούν επίσης να μεταφορτωθούν ανώνυμα χρησιμοποιώντας τον διακομιστή FTP. Ένας χρήστης συνιστάται να εκτελεί έως 3 ερωτήματα ανά δευτερόλεπτο, διαφορετικά η διεύθυνση IP του χρήστη θα αποκλειστεί. Εάν η διεύθυνση IP του χρήστη είναι αποκλεισμένη, ο χρήστης πρέπει να εγγραφεί μέσω NCBI παρέχοντας πρόσθετες πληροφορίες, όπως τη διεύθυνση ηλεκτρονικού ταχυδρομείου του και το όνομα του εργαλείου που πρόκειται να αναπτύξει ο χρήστης. Από τον Δεκέμβριο του 2018, απαιτείται ένα κλειδί API (Application Programming Interface) για την εκτέλεση περισσότερων από 3 ερωτημάτων ανά δευτερόλεπτο χρησιμοποιώντας ηλεκτρονικά βοηθητικά προγράμματα. Ένα κλειδί API μπορεί να ληφθεί από εγγεγραμμένους χρήστες του NCBI και συσχετίζεται με έναν μοναδικό λογαριασμό χρήστη.

Η υποβολή δεδομένων στη βάση δεδομένων NCBI είναι μια καλά ελεγχόμενη διαδικασία πολλαπλών βημάτων. Για παράδειγμα, για να υποβληθεί μια συναρμολόγηση γονιδιώματος σε βάση δεδομένων, παρέχονται λεπτομερείς οδηγίες στον ιστότοπο του NCBI. Πρώτον, ο χρήστης πρέπει να συνδεθεί, χρησιμοποιώντας προεγγεγραμμένα διαπιστευτήρια για να δημιουργήσει ένα αναγνωριστικό έργου και να συμπληρώσει ένα αρχείο προτύπου υποβολής. Μετά την απόκτηση του αναγνωριστικού έργου, ο χρήστης πρέπει να οργανώσει τα δεδομένα και τα μεταδεδομένα του έργου σε συγκεκριμένες μορφές. Ορισμένα αρχεία δεδομένων πρέπει να μετατραπούν σε συγκεκριμένη μορφή χρησιμοποιώντας βοηθητικά προγράμματα λογισμικού που αναπτύχθηκαν από το NCBI. Στη συνέχεια, μόλις τα αρχεία δεδομένων είναι στη σωστή μορφή, ο χρήστης θα χρησιμοποιήσει μια άλλη διαδικτυακή πύλη από το NCBI για να υποβάλει και να ανεβάσει τα δεδομένα. Μετά την υποβολή, ο χρήστης θα πρέπει να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε έναν λογαριασμό διαχειριστή στο NCBI που περιλαμβάνει την περιγραφή του έργου (NCBI: Datadases). https://www.ncbi.nlm.nih.gov/guide/all/

4.3.2. Βάσεις δεδομένων στο EMBL

Το Ευρωπαϊκό Εργαστήριο Μοριακής Βιολογίας αποτελείται από 28 κράτη μέλη, και διαθέτει περισσότερες από 110 ανεξάρτητες ερευνητικές ομάδες. Το Συμβούλιο του EMBL αποτελείται από εθνικούς εκπροσώπους των κρατών μελών και είναι το διοικητικό όργανο του. Στόχος του είναι η έρευνα, οι υπηρεσίες κατάρτισης, μεταφοράς τεχνολογίας και η ανάπτυξη πολιτικών, ενώ διαθέτει και αυτό πληθώρα βάσεων δεδομένων.

Βάσεις δεδομένων:

Το Ευρωπαϊκό Αρχείο Νουκλεοτιδίων (ENA): είναι μια ανοιχτή, υποστηριζόμενη πλατφόρμα για τη διαχείριση, την κοινή χρήση, την ενοποίηση, την αρχειοθέτηση και τη διάδοση δεδομένων αλληλουχίας. Περιλαμβάνει δεδομένα ακολουθίας δημόσιου τομέα όσο και ένα πλούσιο χαρτοφυλάκιο εργαλείων και υπηρεσιών για την υποστήριξη της διαχείρισης της ακολουθίας δεδομένων, καλύπτοντας τομείς όπως η γονιδιωματική των ζώων, η θαλάσσια βιοτεχνολογία, η βιοποικιλότητα, η επιτήρηση παθογόνων και η βιολογία των βλαστοκυττάρων.

Ensembl Genomes: Περιλαμβάνει γονιδιώματα φυτών, μυκήτων, ασπόνδυλων, βακτηριδίων και και παρέχει ταξινομικά σημεία αναφοράς δίνοντας το εξελικτικό πλαίσιο στο οποίο μπορούν να γίνουν κατανοητά τα γονίδια, καθώς και κάλυψη όλων των μεγάλων πειραματικών οργανισμών μη σπονδυλωτών, ειδών γεωργικής σημασίας, παθογόνων και φορέων. Μέχρι το 2020, υποστήριξε πάνω από 50.0000 γονιδιώματα, παρέχοντας πρόσβαση στο γονιδίωμα SARS-CoV2.

Το ArrayExpress: είναι μια βάση δεδομένων που περιέχει δεδομένα γονιδιακής έκφρασης και αποτελέσματα από άλλες λειτουργικές γονιδιωματικές δοκιμασίες που παράγονται από ανάλυση μικροσυστοιχιών, η βάση δεδομένων περιέχει στην πραγματικότητα δεδομένα RNA και DNA.

Ο Άτλας Έκφρασης: είναι μια επιμελημένη βάση δεδομένων μόνο για δεδομένα γονιδιακής έκφρασης.

BioStudies: περιέχει περιγραφές βιολογικών μελετών, συνδέσμους προς δεδομένα από αυτές τις μελέτες σε άλλες βάσεις δεδομένων και μπορεί να δεχθεί ένα ευρύ φάσμα τύπων μελετών που περιγράφονται μέσω μιας απλής μορφής. Επιτρέπει επίσης στους συγγραφείς χειρογράφων να υποβάλλουν συμπληρωματικές πληροφορίες και να συνδέονται με αυτές από τη δημοσίευση.

Σελόσαυρος : είναι ένας πόρος γνώσης για τις κυτταρικές σειρές. Προσπαθεί να περιγράψει όλες τις κυτταρικές σειρές που χρησιμοποιούνται στη βιοϊατρική έρευνα.

ChEMBL: είναι μια βάση δεδομένων μικρών μορίων που μοιάζουν με βιοενεργά φάρμακα, περιέχει δισδιάστατες δομές, υπολογισμένες ιδιότητες.

European Genome-phenome Archive (EGA): είναι μια υπηρεσία για μόνιμη αρχειοθέτηση και κοινή χρήση όλων των τύπων γενετικών και φαινοτυπικών δεδομένων προσωπικά αναγνωρίσιμα που προκύπτουν από βιοϊατρικά ερευνητικά έργα.

Τράπεζα δεδομένων Ηλεκτρονικής Μικροσκοπίας: είναι ένα δημόσιο αποθετήριο για χάρτες όγκου ηλεκτρονιακής κρυομικροσκοπίας και τομογράμματα μακρομοριακών συμπλεγμάτων και υποκυτταρικών δομών. Καλύπτει μια ποικιλία τεχνικών, συμπεριλαμβανομένης της ανάλυσης ενός σωματιδίου, της ηλεκτρονικής τομογραφίας και της κρυσταλλογραφίας ηλεκτρονίων.

Δημόσιο Αρχείο Εικόνων Ηλεκτρονικής Μικροσκοπίας: είναι ένας δημόσιος πόρος για ακατέργαστες εικόνες που υποστηρίζουν τρισδιάστατους χάρτες και τομογραφήματα ενώ φιλοξενεί επίσης τρισδιάστατα σύνολα δεδομένων που λαμβάνονται με μαλακή και σκληρή τομογραφία ακτίνων Χ. Όλα τα δεδομένα που αρχειοθετούνται μπορούν να επαναχρησιμοποιηθούν ελεύθερα χωρίς όρους ή περιορισμούς.

Ευρώπη PMC: παρέχει ολοκληρωμένη πρόσβαση στη βιβλιογραφία των βιοεπιστημών από αξιόπιστες πηγές. Είναι διαθέσιμο σε οποιονδήποτε, οπουδήποτε δωρεάν και περιλαμβάνει 40,2 εκατομμύρια δημοσιεύσεις, προεκτυπώσεις και άλλα έγγραφα εμπλουτισμένα με συνδέσμους προς υποστηρικτικά δεδομένα, κριτικές, πρωτόκολλα και άλλους σχετικούς πόρους.

European Variation Archive (EVA): είναι μια βάση δεδομένων ανοιχτής πρόσβασης όλων των τύπων δεδομένων γενετικών παραλλαγών από όλα τα είδη. Όλοι οι χρήστες μπορούν να

κατεβάσουν δεδομένα από οποιαδήποτε μελέτη ή να υποβάλουν τα δικά τους δεδομένα στο αρχείο. Οι χρήστες μπορούν επίσης να αναζητήσουν όλες τις παραλλαγές ανά μελέτη, γονίδιο, χρωμοσωμική θέση ή αναγνωριστικό χρησιμοποιώντας πρόγραμμα περιήγησης παραλλαγής.

Κατάλογος GWAS: ιδρύθηκε το 2008, ως απάντηση στην ταχεία αύξηση του αριθμού των δημοσιευμένων μελετών συσχέτισης γονιδιωμάτων. Αυτές οι μελέτες παρέχουν μια άνευ προηγουμένου ευκαιρία για τη διερεύνηση της επίδρασης κοινών παραλλαγών σε πολύπλοκες ασθένειες και παρέχουν μια συνεπή, οπτικοποιήσιμη και ελεύθερα διαθέσιμη βάση δεδομένων συσχετίσεων χαρακτηριστικών, η οποία μπορεί εύκολα να ενσωματωθεί με άλλους πόρους και είναι προσβάσιμη από επιστήμονες, κλινικούς ιατρούς και άλλους χρήστες σε όλο τον κόσμο.

Βάση δεδομένων μοριακής αλληλεπίδρασης IntAct: παρέχει ένα δωρεάν, ανοιχτού κώδικα σύστημα βάσης δεδομένων και εργαλεία ανάλυσης για δεδομένα μοριακής αλληλεπίδρασης.

InterPro: είναι ένας πόρος που παρέχει λειτουργική ανάλυση αλληλουχιών πρωτεϊνών ταξινομώντας τες σε οικογένειες και προβλέποντας την παρουσία τομέων και σημαντικών τοποθεσιών.

Τράπεζα Δεδομένων Πρωτεϊνών στην Ευρώπη (PDBE) - Γνωσιακή Βάση: είναι ιδρυτικό μέλος της Worldwide Protein Data Bank, η οποία συλλέγει, οργανώνει και διαδίδει δεδομένα σχετικά με τις βιολογικές μακρομοριακές δομές. Σε συνεργασία με τους άλλους εταίρους της Worldwide Protein Data Bank (wwPDB), αυτή η βάση εργάζεται για τη συλλογή, τη διατήρηση και την παροχή πρόσβασης στο παγκόσμιο αποθετήριο μοντέλων μακρομοριακής δομής, την Τράπεζα Δεδομένων Πρωτεϊνών (PDB).

Βάση δεδομένων Proteomics Identifications (PRIDE): είναι μια κεντρική, συμβατή με πρότυπα, δημόσια αποθήκη δεδομένων για δεδομένα πρωτεϊνικής μάζας, συμπεριλαμβανομένων των ταυτοποιήσεων πρωτεϊνών και πεπτιδίων.

Reactome: είναι μια βάση δεδομένων ανοιχτού κώδικα, ανοιχτής πρόσβασης, χειροκίνητα επιμελημένη, η οποία παρέχει διαισθητικά εργαλεία βιοπληροφορικής για την οπτικοποίηση,

ερμηνεία και ανάλυση της γνώσης, για την υποστήριξη της βασικής και κλινικής έρευνας, της ανάλυσης γονιδιώματος, της μοντελοποίησης, της βιολογίας συστημάτων και της εκπαίδευσης.

Ο Άτλας της ανθρώπινης πρωτεΐνης: είναι ένα πρόγραμμα με βάση τη Σουηδία που ξεκίνησε το 2003 με στόχο να χαρτογραφήσει όλες τις ανθρώπινες πρωτεΐνες σε κύτταρα, ιστούς και όργανα χρησιμοποιώντας μια ενοποίηση διαφόρων τεχνολογιών omics, συμπεριλαμβανομένης της απεικόνισης με βάση αντισώματα. Όλα τα δεδομένα είναι σε ανοιχτή πρόσβαση για να επιτρέψουν στους επιστήμονες τόσο στον ακαδημαϊκό χώρο όσο και στη βιομηχανία να έχουν ελεύθερη πρόσβαση στα δεδομένα για εξερεύνηση του ανθρώπινου είδους.

UniProt: είναι μια ολοκληρωμένη πηγή για δεδομένα αλληλουχίας πρωτεϊνών και σχολιασμού.

Για την αναζήτηση δεδομένων από βάσεις δεδομένων του EMBL, υπάρχουν διάφορες μέθοδοι, ωστόσο όλες οι βάσεις δεδομένων υποστηρίζουν ερωτήματα που βασίζονται σε κείμενο. Η βάση ENA επιτρέπει επίσης αναζητήσεις βάσει ακολουθίας. Αρκετές βάσεις δεδομένων παρέχουν πρόσβαση μέσω προγραμματισμού, η οποία επιτρέπει στο χρήστη να ανακτά δεδομένα χρησιμοποιώντας μια διεύθυνση URL ακολουθώντας μια συγκεκριμένη σύνταξη, ενώ υπάρχει όριο 30 ερωτημάτων κάθε φορά. Επίσης, όλες οι ανωτέρω βάσεις παρέχουν πρόσβαση FTP[3] στους χρήστες για σκοπούς μαζικής λήψης.

Για την υποβολή δεδομένων σε οποιαδήποτε από τις βάσεις δεδομένων ακολουθίας EMBL απαιτούνται διαδικασίες παρόμοιες με την υποβολή δεδομένων στο NCBI. Για παράδειγμα, εάν ένας χρήστης θέλει να υποβάλει ένα σύνολο δεδομένων σε μια βάση δεδομένων, πρέπει πρώτα να καταχωρήσει έναν λογαριασμό που σχετίζεται με μια διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν κωδικό πρόσβασης που παρέχεται από το χρήστη. Ο χρήστης πρέπει να προετοιμάσει μεταδεδομένα, ανεπεξέργαστα δεδομένα και επεξεργασμένα δεδομένα σύμφωνα με μια συγκεκριμένη μορφή.

[3] Το **Πρωτόκολλο Μεταφοράς Αρχείων** (*File Transfer Protocol (FTP)*) είναι ένα ευρέως χρησιμοποιούμενο σε δίκτυα όπως το διαδίκτυο ή εσωτερικά δίκτυα. Ένα πρόγραμμα FTP μόλις συνδεθεί με το διακομιστή μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως αποστολή αρχείων από και προς το διακομιστή, μετονομασία ή διαγραφή αρχείων. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου.

Και οι δύο βάσεις δεδομένων φιλοξενούν terabytes γονιδιωματικών δεδομένων σε πολλές συγκεκριμένες μορφές δεδομένων. Οι τύποι δεδομένων περιλαμβάνουν μεταδεδομένα, ανεπεξέργαστα δεδομένα και επεξεργασμένα δεδομένα. Ορισμένα δεδομένα βρίσκονται σε αρχεία κειμένου με συγκεκριμένες δομές. Ορισμένα δεδομένα είναι δυαδικά δεδομένα, τα οποία απαιτούν εργαλεία λογισμικού για την εξαγωγή πληροφοριών σε μορφές αναγνώσιμες από τον άνθρωπο. Οι χρήστες μπορούν να έχουν πρόσβαση σε δεδομένα χρησιμοποιώντας μια πληθώρα μεθόδων. Ορισμένα όρια λήψης εφαρμόζονται και στις δύο βάσεις δεδομένων για τον περιορισμό του όγκου των δεδομένων ή της ταχύτητας λήψης δεδομένων από τους χρήστες. Για να υποβάλει δεδομένα σε αυτές τις βάσεις δεδομένων, ένας χρήστης θα πρέπει να προεγγραφεί με μια διεύθυνση ηλεκτρονικού ταχυδρομείου και να συνδεθεί για να χρησιμοποιήσει μια διεπαφή ιστού συγκεκριμένου ιστότοπου για να ανεβάσει δεδομένα. Τα μεταδεδομένα, τα ανεπεξέργαστα δεδομένα και τα επεξεργασμένα δεδομένα μπορούν να μεταφορτωθούν και οι φόρμες ιστού θα πρέπει να συμπληρωθούν για να περιγράψουν τα δεδομένα. Αν και δεν αναφέρεται ρητά στην κατευθυντήρια γραμμή της διαδικασίας υποβολής, και για τους δύο ιστότοπους, υπάρχουν επιμελητές που ελέγχουν την τελική διαδικασία ενσωμάτωσης δεδομένων που υποβάλλονται από χρήστες στη βάση δεδομένων (EMBL-EBI:Data-resources).

Εκτός από τα κύρια αποθετήρια αλληλουχιών που περιγράφονται παραπάνω, υπάρχουν πολλές βάσεις δεδομένων και διαδικτυακές υπηρεσίες που είναι μικρότερης κλίμακας και εστιάζουν πιο συγκεκριμένα σε ορισμένες πτυχές. Το Κέντρο Ενοποίησης Πόρων Pathosystems (PATRIC) είναι ένα κέντρο βακτηριακής βιοπληροφορικής. Η κύριος στόχος του PATRIC είναι ο σχολιασμός και η ανάλυση του βακτηριακού γονιδιώματος. Υπάρχουν 202.602 βακτηριακά γονιδιώματα που φιλοξενούνται στο PATRIC (NGDC: atabasecommons). Η βάση δεδομένων eukaryotic pathogen genomics database (EuPathDB) είναι μια συλλογή βάσεων δεδομένων για ευκαρυωτικά παθογόνα (veupathdb). Το ViPR είναι μια βάση δεδομένων παθογόνων ιών, η οποία παρέχει μια διαδικτυακή διεπαφή για την αναζήτηση αλληλουχιών γονιδιώματος, αλληλουχιών γονιδίων, πρωτεϊνικών αλληλουχιών και πρωτεϊνικών δομών. Η PHI-βάση είναι

μια επιμελημένη βάση δεδομένων για γονίδια που σχετίζονται με αλληλεπιδράσεις ξενιστή-παθογόνου. Το PHIDIAS είναι μια επιμελημένη διαδικτυακή βάση δεδομένων που επικεντρώνεται σε δεδομένα γονιδιώματος, που σχετίζονται με αλληλεπιδράσεις παθογόνων και ξενιστών. Το Victors επικεντρώνεται στους λοιμογόνους παράγοντες και υπάρχουν 5.296 λοιμογόνοι παράγοντες αποθηκευμένοι στη βάση. Το PAMDB είναι μια βάση δεδομένων και ένας ιστότοπος για τα μικρόβια που και έχει σχεδιαστεί για την αποθήκευση και αναζήτηση δεδομένων για την τυποποίηση αλληλουχίας πολλαπλών τόπων για παθογόνα βακτήρια φυτών. Το PhytoPath είναι μια διαδικτυακή βάση δεδομένων για δεδομένα γονιδιώματος φυτικών παθογόνων (Bacterial and Viral Bioinformatics resource center).https://www.bv-brc.org/ .

4.4. Η Κυβερνο-βιοασφάλεια και οι απειλές στις βάσεις δεδομένων

Ένα χαρακτηριστικό αυτών των βάσεων δεδομένων είναι ότι όλες απαιτούν έλεγχο πρόσβασης όταν οι χρήστες ζητούν μεταφόρτωση δεδομένων στην κύρια βάση δεδομένων και έλεγχο ταυτότητας του χρήστη πριν από την ενσωμάτωση των δεδομένων στη βάση δεδομένων. Σε αντίθεση με τον έλεγχο της μεταφόρτωσης, δεν ζητείται ο πλήρης έλεγχος της πρόσβασης στα δεδομένα που σημαίνει ότι ένας χρήστης πρέπει να εγγραφεί και στη συνέχεια να συνδεθεί πριν κατεβάσει οποιαδήποτε δεδομένα από μια βάση. Οι περισσότερες βάσεις δεδομένων παρέχουν ανώνυμη λήψη χωρίς κανέναν έλεγχο, ενώ ορισμένες βάσεις δεδομένων παρέχουν μηχανισμούς για τον περιορισμό της ταχείας λήψης πολλαπλών εγγραφών. Επίσης το πιο ανησυχητικό πρόβλημα είναι ότι καμία από τις βάσεις δεδομένων δεν απαιτεί ισχυρούς κωδικούς πρόσβασης, γεγονός που μπορεί να οδηγήσει σε πολλαπλούς κινδύνους για την ασφάλεια στον κυβερνοχώρο Τέλος, ορισμένες από τις βάσεις δεδομένων παρέχουν μεθόδους για προγραμματική πρόσβαση, η οποία είναι να βοηθήσει τους χρήστες να εκτελέσουν δομημένα ερωτήματα με γλώσσες προγραμματισμού ή να παρέχουν ταχύτερη ταχύτητα λήψης με εξωτερικές υπηρεσίες ή πρωτόκολλα γρήγορης λήψης. Ο κίνδυνος χρήσης αυτών των εργαλείων λογισμικού τρίτων σχετίζεται με κάθε μεμονωμένο λογισμικό, δεδομένου ότι πολλά από αυτά τα εργαλεία χρησιμοποιούνται ευρέως εκτός της γονιδιωματικής ερευνητικής κοινότητας.

Δεν έχει υπάρξει συστηματική μελέτη σχετικά με παραβιάσεις της ασφάλειας των βάσεων δεδομένων γονιδιώματος και επομένως η ασφάλεια επικεντρώνεται γενικότερα στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ψηφιακών πληροφοριών.

Ένα σημαντικό κίνητρο πίσω από τις κυβερνοεπιθέσεις είναι η πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες. Οι περισσότερες δημόσιες βάσεις δεδομένων γονιδιώματος δεν περιέχουν ευαίσθητες προσωπικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών ή αριθμούς κοινωνικής ασφάλισης, ωστόσο περιέχουν δεδομένα ατόμων, τα πιο «προσωπικά» δεδομένα

από όλα. Δύο λόγοι για τους οποίους οι βάσεις δεδομένων γονιδιώματος δεν είχαν γίνει έως τώρα στόχος κυβερνοεπιθέσεων είναι ότι οι χρήστες αυτών των βάσεων δεδομένων είναι κυρίως ερευνητές επιστήμονες που αντιπροσωπεύουν ένα μικρό ποσοστό του πληθυσμού καθώς και η τεχνολογία που απαιτείται για την εκμετάλλευση των δεδομένων ήταν εξελιγμένη και δαπανηρή. Ωστόσο, όσο η γνώση και η κατάρτιση εξαπλώνονται και διαχέονται με τις τεχνολογικές εξελίξεις, ο εξοπλισμός γίνεται λιγότερο ακριβός και ευκολότερος στη χρήση. Επιπλέον, αδιάκριτες επιθέσεις μπορούν πάντα να συμβούν και μπορούν να προκαλέσουν ζημιά στις βάσεις δεδομένων. Όπως αναφέρθηκε πολλές βάσεις δεδομένων απαιτούν μόνο το email χρήστη και κωδικό πρόσβασης για να δημιουργήσουν έλεγχο πρόσβασης και οι χρήστες επαναλαμβάνουν τους συνδυασμούς email και κωδικού πρόσβασης. Έτσι, τα διαπιστευτήρια που διακυβεύονται σε ένα σύστημα και ενδιαφέρουν τυχόν επιτιθέμενους για να αποκτήσουν πρόσβαση σε άλλους λογαριασμούς του ίδιου χρήστη. Μεταξύ των βάσεων δεδομένων καμία βάση δεν απαιτεί ισχυρούς κωδικούς πρόσβασης, επιβάλλοντας έναν αρκετά μεγάλο κωδικό πρόσβασης επαρκούς πολυπλοκότητας (που περιλαμβάνει κεφαλαία γράμματα, αριθμούς και σύμβολα) για να καταστήσει ανέφικτες τις επιθέσεις κωδικού πρόσβασης λογαριασμού (Jacob Caswell, κ.α. 2019).

Ένα άλλο σημαντικό ζήτημα με τις βάσεις δεδομένων είναι η χρήση της ιδέας των επιθέσεων συσχέτισης. Ο εισβολέας επιθυμεί να συσχετίσει βιολογικά δεδομένα με συγκεκριμένους χρήστες ή ομάδες χρηστών. Η απειλή μπορεί να προέρχεται από κακόβουλους υπολογιστές-πελάτες με έλεγχο ταυτότητας ή/και χωρίς έλεγχο ταυτότητας. Στην πρώτη περίπτωση, ένας υπολογιστής-πελάτης με έλεγχο ταυτότητας είναι αυτός που έχει πρόσβαση στη βάση δεδομένων και μπορεί να διαβάσει και να συσχετίσει εγγραφές σε πολλές βάσεις δεδομένων. Αυτό συνήθως αναφέρεται ως εσωτερική απειλή και απαιτεί μια προσεκτική διαδικασία ελέγχου και παρακολούθησης χρηστών για τον εντοπισμό πιθανών υποψηφίων. Στη δεύτερη περίπτωση, ο εισβολέας χρησιμοποιεί μια κλασική εξωτερική επίθεση, για παράδειγμα εκμεταλλευόμενος τα διαπιστευτήρια ενός υπάρχοντος χρήστη ή στέλνοντας μηνύματα

ηλεκτρονικού ταχυδρομείου σε γνωστούς χρήστες του συστήματος με ενσωματωμένο κακόβουλο λογισμικό, (επίσης γνωστό ως "phishing") για να αποκτήσει πρόσβαση σε λογαριασμούς συστήματος και στη συνέχεια να προχωρήσει σε μια επίθεση συσχέτισης (Brown A., κ.α. 2018).

Άλλη μια ανησυχία για τις βάσεις δεδομένων γονιδιώματος παθογόνων είναι ότι η γνώση των αλληλουχιών παθογόνων μπορεί να οδηγήσει σε κακόβουλη χρήση. Αυτή η κακοπροαίρετη χρήση δεδομένων και τεχνολογίας αποτελεί μείζον πρόβλημα βιοασφάλειας. Επί του παρόντος, πολλά γονιδιώματα ζωικών και φυτικών παθογόνων είναι ελεύθερα προσβάσιμα σε οποιονδήποτε χρήστη μέσω βάσεων δεδομένων. Ακόμη και η αλληλουχία του γονιδιώματος ενός παθογόνου υψηλού κινδύνου όπως ο ιός της ευλογιάς, μπορεί εύκολα να προσεγγιστεί στις βάσεις το NCBI από οποιονδήποτε ανώνυμο χρήστη (Colston S.M., κ.α., 2014).

Είναι γεγονός, ότι οι βάσεις δεδομένων με γενετικά στοιχεία αναπτύσσονται ραγδαία λόγω του αυξανόμενου όγκου δεδομένων. Πολλές βάσεις δεδομένων διαθέτουν πρωτόκολλα για τον έλεγχο της ποιότητας των δεδομένων και τη χειροκίνητη επιμέλεια, για τη διασφάλιση της ακεραιότητας των δεδομένων. Σε όλες τις βάσεις δεδομένων που αναφερθήκαμε, για να υποβάλει κανείς ένα νέο σύνολο δεδομένων, πρέπει να καταχωρήσει ένα λογαριασμό με μια διεύθυνση ηλεκτρονικού ταχυδρομείου, ενώ τα δεδομένα δεν μπορούν να εισαχθούν απευθείας στην κύρια βάση δεδομένων. Υπάρχει πάντα ένας επιμελητής ή ένας διαχειριστής για να επιβλέπει τη διαδικασία. Είναι ενδιαφέρον ότι δεν φαίνεται να υπάρχει περίπτωση όπου η ακεραιότητα των δεδομένων ελέγχεται κατά τη διάρκεια της διαδικασίας μεταφοράς για να διασφαλιστεί ότι τα δεδομένα που παρέχονται από τον χρήστη δεν τροποποιούνται κατά την διάρκεια της διαδικασίας μεταφοράς δεδομένων. Η ταχεία ανάπτυξη των πεδίων της γονιδιωματικής και της βιοπληροφορικής έχουν δημιουργήσει μια πρόκληση που αφορά στην επεξεργασία του όγκου για τους επιμελητές και έχει αφήσει τα ιδρύματα να αγωνίζονται να φέρουν τεράστιες υπολογιστικές υποδομές "μεγάλων δεδομένων" στο διαδίκτυο. Οι επιτιθέμενοι έχουν πολλές επιλογές για να εκμεταλλευτούν μια μη επαληθευμένη διαδικασία

μεταφοράς δεδομένων. Μια πιθανότητα επίθεσης είναι η παροχή μη έγκυρων δεδομένων, με κίνητρο την καθοδήγηση μελλοντικών μελετών προς συγκεκριμένα αποτελέσματα. Αυτή η επίθεση απαιτεί προσεκτική δημιουργία εγγραφών στη βάση δεδομένων για τη διατήρηση έγκυρης μορφής, αλλά περιέχει δεδομένα χωρίς πειραματικά στοιχεία. Αυτή η επίθεση μπορεί να γίνει κατά τη διάρκεια μιας μεμονωμένης μεταφοράς δεδομένων. Η επαλήθευση της εγκυρότητας των δεδομένων είναι ιδιαίτερα δύσκολη και δεν μπορεί να πραγματοποιηθεί εύκολα με τις υπάρχουσες μεθόδους. Ένας άλλος τύπος επίθεσης συνίσταται στη σταδιακή εισαγωγή μη έγκυρων εγγραφών μέσα σε ένα μεγαλύτερο έγκυρο σύνολο δεδομένων. Για παράδειγμα, ο εισβολέας θα μπορούσε να κάνει λήψη υπαρχόντων δεδομένων από τη βάση δεδομένων, να εξαγάγει ένα υποσύνολο των δεδομένων και να εισαγάγει μη έγκυρα δεδομένα. Σε αυτήν την περίπτωση, οι μηχανισμοί ανίχνευσης που χρησιμοποιούν πιθανοτική ανάλυση μπορεί να αποτύχουν να εντοπίσουν τις μη έγκυρες εγγραφές. Μόνο αρχεία με σαφή παραβίαση της ακεραιότητας των δεδομένων μπορούν να εντοπιστούν (Boris A, κ.α., 2019).

Τέλος, καθυστέρηση στην πρόοδο των πειραμάτων που είναι ευαίσθητα στο χρόνο προκαλεί η μειωμένη διαθεσιμότητα δεδομένων. Για παράδειγμα, σε ένα διαγνωστικό εργαστήριο που χρησιμοποιεί αλληλουχίες DNA ως μέθοδο για τον εντοπισμό παθογόνων, η διακοπή μιας βάσης δεδομένων θα προκαλέσει καθυστερήσεις στην ταυτοποίηση του παθογόνου. Επίσης, ακόμη ένας λόγος απώλειας δεδομένων είναι ότι μια βάση δεδομένων μπορεί να είναι ελεύθερα προσβάσιμη στον καθένα, αλλά δεν υπάρχουν πάντα πόροι για να διατηρηθεί η βάση δεδομένων online, ώστε να είναι διαθέσιμη για χρήση σε μελλοντικούς χρήστες. Η διατήρηση αυτών των δεδομένων, απαιτεί ένα κατανεμημένο δίκτυο μόνιμων παρόχων που περιλαμβάνει ένα σύστημα ελέγχου που παρέχει εγγυήσεις και μπορεί να διατηρήσει τη διαθεσιμότητά τους, όταν ορισμένοι πάροχοι δεδομένων δεν ανταποκρίνονται πλέον (Peccoud J, κ.α. 2019). Τέλος όπως είδαμε παραπάνω, σε ορισμένες βάσεις δεδομένων παρέχεται η δυνατότητα σε απομακρυσμένους χρήστες να υποβάλλουν ερωτήματα σε δεδομένα απευθείας, με αποτέλεσμα οι βάσεις να είναι ευαίσθητες σε κυβερνο-επιθέσεις. Πολλά μεγάλα

ερευνητικά πανεπιστήμια είναι εξοπλισμένα με διακομιστές υπολογιστών και αυτοί οι διακομιστές είναι ελκυστικοί στόχοι για κακόβουλη χρήση, όπως η εξόρυξη κρυπτονομισμάτων.

4.5. Η ασφάλεια και οι δυνατότητες για την λήψη νέων μέτρων

Καθώς τα γονιδιωματικά δεδομένα γίνονται αναπόσπαστο μέρος του σχεδίου υγειονομικής περίθαλψης και θεραπείας ενός ατόμου, το παραδοσιακό τείχος προστασίας μεταξύ βιοπληροφορικής και ιατρικής τεχνολογίας γίνεται πορώδες και διάτρητο στις κυβερνο-απειλές. Τα μέτρα ασφαλείας που χρησιμοποιούνται από τις βάσεις δεδομένων γονιδιώματος παθογόνων που θα μπορούσαν να ελαχιστοποιήσουν αυτές τις απειλές είναι:

1) Ο έλεγχος της πρόσβασης. Πολλές βάσεις δεδομένων περιέχουν στοιχεία που δεν απαιτούν σύνδεση. Οι χρήστες μπορούν απλά να χρησιμοποιήσουν μια διεπαφή ιστού για να αναζητήσουν δεδομένα από βάσεις δεδομένων. Οι χρήστες μπορούν επίσης να χρησιμοποιήσουν μια γλώσσα προγραμματισμού για πρόσβαση σε δεδομένα. Για μαζική λήψη, παρέχεται ανώνυμη πρόσβαση σε πολλές περιπτώσεις. Τόσο το NCBI όσο και το EMBL-EBI, έχουν εφαρμόσει όρια ταχύτητας για μαζική λήψη χρησιμοποιώντας προγραμματιζόμενες διεπαφές. Σχεδόν όλες οι βάσεις δεδομένων απαιτούν από τους χρήστες να χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο και τον κωδικό πρόσβασης ως μεθόδους σύνδεσης για να αποκτήσουν πρόσβαση στη μεταφόρτωση δεδομένων και στη δυνατότητα ανάλυσης δεδομένων. Παρατηρούμε ότι οι περισσότερες βάσεις δεδομένων δεν απαιτούν ισχυρούς κωδικούς πρόσβασης, όπως συνδυασμούς μεγάλων φράσεων, κεφαλαίων γραμμάτων, συμβόλων και αριθμών. Καμία βάση δεδομένων δεν απαιτεί έλεγχο ταυτότητας δύο παραγόντων ή σύνδεση μέσω λογαριασμών τρίτων. Η απαίτηση ισχυρών κωδικών πρόσβασης, η εφαρμογή ελέγχου ταυτότητας θα μπορούσαν να παρέχουν πρόσθετα μέτρα ασφαλείας για την τρέχουσα γενιά γονιδιωματικών βάσεων δεδομένων.

2) Ο έλεγχος της ακεραιότητας και της προστασίας δεδομένων. Οι περισσότερες βάσεις δεδομένων επιτρέπουν στους χρήστες να συνεισφέρουν δεδομένα και να εφαρμόζουν πρότυπα μεταδεδομένων.

Ωστόσο, δεν είναι σαφές πώς οι βάσεις δεδομένων διασφαλίζουν ότι τα δεδομένα είναι άθικτα κατά τη διαδικασία μεταφοράς. Απλές μέθοδοι, όπως κρυπτογραφικά αθροίσματα ελέγχου, θα μπορούσαν να εφαρμοστούν για τη διασφάλιση της ακεραιότητας των δεδομένων. Οι υφιστάμενοι μηχανισμοί ποιοτικού ελέγχου δεν επιτρέπουν στους επιμελητές να ελέγχουν την ποιότητα των δεδομένων σε σχέση με την προαναφερθείσα, υποθετική κατάσταση. Ένα άλλο μοντέλο για την προστασία των δεδομένων είναι η χρήση κρυπτογραφημένων βάσεων δεδομένων ή η χρήση ασφαλούς πολυκομματικού υπολογισμού. Για παράδειγμα, η πρόσβαση σε βάσεις δεδομένων δεν χρειάζεται να είναι δυαδική, επιτρέποντας ή απαγορεύοντας την πρόσβαση με βάση μοντέλα ελέγχου πρόσβασης. Μπορεί κανείς να αποκαλύψει μερικές προβολές της βάσης δεδομένων ανάλογα με τις ανάγκες. Διαθεσιμότητα δεδομένων και μακροζωία. Η απώλεια πρόσβασης στη βάση δεδομένων συνεπάγεται απώλεια πολύτιμων ερευνητικών αποτελεσμάτων και σπατάλη χειρωνακτικής εργασίας στη διαδικασία επιμέλειας δεδομένων. Δεδομένου ότι η συντήρηση των βάσεων δεδομένων απαιτεί συνεχή υποστήριξη, είναι σύνηθες ότι ορισμένες βάσεις δεδομένων δεν μπορούν να διατηρηθούν λόγω έλλειψης χρηματοδοτικής στήριξης. Μια λύση σε αυτό το πρόβλημα είναι η κατάθεση δεδομένων σε δημόσιες βάσεις δεδομένων που διατηρούνται από τις εθνικές κυβερνήσεις. Η προσέγγιση αυτή παρέχει καλύτερες εγγυήσεις για τη μακροπρόθεσμη διαθεσιμότητα των ερευνητικών δεδομένων (James Diggans and Emily 2019).

4.6. COVID-19 και οι βάσεις δεδομένων

Το Ομοσπονδιακό «EGA» (θα αναφερθεί παρακάτω), είναι ο πρωταρχικός παγκόσμιος πόρος για την ανακάλυψη και πρόσβαση σε ευαίσθητα ανθρώπινα omics[4] και συναφή δεδομένα που εγκρίνονται για δευτερογενή χρήση, μέσω ενός δικτύου εθνικών αποθετηρίων ανθρώπινων δεδομένων για την επιτάχυνση της έρευνας ασθενειών και τη βελτίωση της ανθρώπινης υγείας. Τα τελευταία 10 χρόνια, τα περισσότερα δεδομένα έχουν δημιουργηθεί στο πλαίσιο ερευνητικών κοινοπραξιών και έχουν κοινοποιηθεί μέσω παγκόσμιων αποθετηρίων όπως το Ευρωπαϊκό Αρχείο Γονιδιώματος «EGA». Πολλές χώρες έχουν πλέον αναδυόμενα εξατομικευμένα προγράμματα ιατρικής που παράγουν δεδομένα από εθνικές ή περιφερειακές πρωτοβουλίες. Έτσι, η ανθρώπινη γονιδιωματική υφίσταται μια σταδιακή αλλαγή από μια δραστηριότητα με γνώμονα την έρευνα σε μια δραστηριότητα που χρηματοδοτείται μέσω πρωτοβουλιών υγειονομικής περίθαλψης. Τα γενετικά δεδομένα που παράγονται σε ένα πλαίσιο υγειονομικής περίθαλψης υπόκεινται σε πιο αυστηρή διαχείριση πληροφοριών από τα ερευνητικά δεδομένα και συχνά πρέπει να συμμορφώνονται με την εθνική νομοθεσία. Για την αντιμετώπιση αυτής της ανάγκης, η Ομοσπονδιακή «EGA» παρέχει ένα δίκτυο συνδεδεμένων πόρων για να επιτρέψει τη διεθνική ανακάλυψη και πρόσβαση σε ανθρώπινα δεδομένα για έρευνα, ενώ παράλληλα σέβεται τους κανονισμούς περί προστασίας δεδομένων δικαιοδοσίας.

Το Ομοσπονδιακό «EGA» είναι μια υποδομή που βασίζεται στο European Genome-phenome Archive (EGA), έναν πόρο δεδομένων, για ασφαλή αρχειοθέτηση και κοινή χρήση ευαίσθητων ανθρώπινων βιομοριακών και φαινοτυπικών δεδομένων που προκύπτουν από βιοϊατρικά ερευνητικά έργα. Υποστηρίζει την ελεγχόμενη κοινή χρήση πρόσβασης σε βιομοριακά και φαινοτυπικά δεδομένα για τον COVID-19. Εκτός από τους κόμβους δεδομένων SARS-CoV2 και την πύλη δεδομένων COVID-19, αποτελεί το τρίτο στοιχείο της Ευρωπαϊκής Πλατφόρμας Δεδομένων COVID-19. Με τεχνικά εργαλεία για την ανάπτυξη εθνικών ασφαλών

[4] Οι κλάδοι της επιστήμης γνωστοί ανεπίσημα ως ωμική είναι διάφοροι κλάδοι της βιολογίας των οποίων τα ονόματα τελειώνουν στο επίθημα -omics, όπως γονιδιωματική, πρωτεϊνομική, μεταβολομική, μεταγονιδιωματική, φαινομενική και μεταγραφομική.

κόμβων βάσεων δεδομένων και κατάλληλα πρωτόκολλα για τη σύνδεση κόμβων σε ολόκληρη την ομοσπονδία για αιτήματα αναζήτησης και πρόσβασης, το σύστημα υποστηρίζει εθνικές απαιτήσεις διαχείρισης δεδομένων για γονιδιωματικά και κλινικά δεδομένα που συλλέγονται από πολίτες ως μέρος ερευνητικών έργων υγειονομικής περίθαλψης ή βιοϊατρικής . Στο πλαίσιο της Ευρωπαϊκής Πλατφόρμας Δεδομένων για τον COVID-19, η Ομοσπονδιακή «EGA» υποστήριξε τις βιομοριακές μελέτες υποδοχής COVID-19 σε όλη την Ευρώπη.

Το «EGA» περιλαμβάνει έναν ασφαλή εξουσιοδοτημένο μηχανισμό πρόσβασης για την υποστήριξη της ερευνητικής χρήσης των συνόλων των δεδομένων σε όλη την Ευρώπη, όπου το τελικό αποτέλεσμα είναι μια συντονισμένη και εναρμονισμένη συλλογή εθνικών συνόλων δεδομένων κεντρικού υπολογιστή COVID-19 για ερευνητικούς σκοπούς. Η πρόσβαση στα σύνολα δεδομένων παρέχεται σε εξουσιοδοτημένους ερευνητές χρησιμοποιώντας διαδικασίες που επικεντρώνονται στην Επιτροπή Πρόσβασης Δεδομένων και ασφαλή πρωτόκολλα που έχουν ήδη αναπτυχθεί για την υπηρεσία «EGA» και εφαρμόζονται σε εθνικό επίπεδο ως μέρος του ομοσπονδιακού μοντέλου «EGA». Οι επιχειρησιακές διαδικασίες του «EGA» βοηθούν τους εθνικούς κόμβους να μοιράζονται γρήγορα και με ασφάλεια τα δεδομένα COVID-19 που φιλοξενούν τον άνθρωπο. Επιπλέον, παρέχεται πρόσβαση σε εξουσιοδοτημένους ερευνητές χρησιμοποιώντας ασφαλή πρωτόκολλα που έχουν ήδη αναπτυχθεί για την υπηρεσία «EGA» και εφαρμόζονται πλέον σε εθνικό επίπεδο ως μέρος του ομοσπονδιακού μοντέλου «EGA» (Federated-Ega).

5. Κυβερνοβιοασφάλεια σε εργαστήρια προηγμένης τεχνολογίας.

Τα εργαστήρια βιοεπιστημών βρίσκονται στο στάδιο μετάβασης σε «έξυπνα εργαστήρια» του μέλλοντος. Τα περισσότερα υπάρχοντα εργαστήρια διαθέτουν ήδη κοινά χαρακτηριστικά με τα «έξυπνα σπίτια». Οι χρήστες μπορούν να λαμβάνουν αυτόματη ειδοποιήσεις για την κατάσταση των συσκευών (π.χ. ενεργοποίηση / απενεργοποίηση) καθώς και φυσικές αλλαγές στο περιβάλλον, όπως θερμοκρασία, κίνηση ή ήχο. Αυτό είναι παρόμοιο με τα συστήματα αυτοματισμού κτιρίων και το λογισμικό διαχείρισης ενέργειας που βρίσκονται συνήθως σε σύγχρονες εργαστηριακές εγκαταστάσεις. Αυτά τα συστήματα παρέχουν έλεγχο του κλίματος και της υγρασίας και, κυρίως, έλεγχο των διαφορών πίεσης μεταξύ των χώρων εργασίας.

Ορισμένα έξυπνα συστήματα μπορούν να προγραμματίσουν επαναλαμβανόμενες εργασίες προληπτικής συντήρησης, να αναθέσουν αυτές τις εργασίες σε συγκεκριμένα άτομα και να παραγγείλουν αυτόματα ανταλλακτικά και προμήθειες για τη διατήρηση των αποθεμάτων. Η διαχείριση τέτοιων έξυπνων συστημάτων περιλαμβάνει την διασύνδεση με προσωπικές κινητές συσκευές επικοινωνίας. Οι κακές συνήθειες προστασίας και ασφάλειας δεδομένων στην προσωπική ζωή σε συνδυασμό με την αξιοσημείωτη υποτίμηση των προσωπικών μας δεδομένων μπορεί να μεταφραστούν σε παρόμοιες συμπεριφορές και συνήθειες στο εργασιακό περιβάλλον (J Craig Reed and Nicolas Dunaway, 2017) .

Η χρήση προσωπικών συσκευών, όπως προσωπικοί φορητοί υπολογιστές και κινητά τηλέφωνα, για την πρόσβαση σε συστήματα που σχετίζονται με την εργασία έχει ως αποτέλεσμα να προστίθενται τρωτά σημεία για την κυβερνοβιοασφάλεια για διάφορους λόγους. Πρώτον, θα πρέπει οι εργοδότες είτε να απαγορεύσουν την χρήση προσωπικών συσκευών και να προβούν στη αγορά συσκευών που ανήκουν στην εταιρεία είτε να εφαρμόσουν μια πολιτική ασφαλείας στις προσωπικές συσκευές που έχουν πρόσβαση στα δίκτυα του οργανισμού. Η αποτελεσματική πολιτική ασφάλειας στον κυβερνοχώρο περιλαμβάνει κρυπτογράφηση, ισχυρή χρήση κωδικού πρόσβασης, χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων με βιομετρικά στοιχεία και κρυπτογράφηση δεδομένων σε κατάσταση αδράνειας και κατά τη μεταφορά. Ενώ

ορισμένα άτομα ακολουθούν τέτοιες διαδικασίες στις προσωπικές τους συσκευές, τα περισσότερα δεν το κάνουν, με αποτέλεσμα να υπάρχουν ευπάθειες κυβερνοβιοασφάλειας στα συστήματα δεδομένων των επιχειρήσεων βιοεπιστημών καθώς και στον διασυνδεδεμένο εργαστηριακό εξοπλισμό. Δεύτερον, οι προσωπικές συσκευές μπορούν να χρησιμοποιηθούν σε μη ασφαλή δημόσια δίκτυα, όπως σε καφετέριες ή δωμάτια ξενοδοχείων, για πρόσβαση σε εργαστηριακά συστήματα και δεδομένα. Χωρίς τη χρήση εικονικού ιδιωτικού δικτύου (VPN) ή κρυπτογραφημένων δεδομένων, τα μη ασφαλή δίκτυα επιτρέπουν σε άλλα μέρη να έχουν πρόσβαση και να υποκλέπτουν τα μεταδιδόμενα δεδομένα. Τρίτον, όταν οι προσωπικές συσκευές συνδέονται σε εξωτερικά δίκτυα και μεταφέρονται στο εργαστήριο, μπορούν να χρησιμοποιηθούν για την αφαίρεση-κλοπή ευαίσθητων δεδομένων εργασίας και την κοινοποίησή τους σε άλλους χωρίς ανίχνευση. Η εξαγωγή δεδομένων ή η κλοπή δεδομένων είναι ένα τέλειο παράδειγμα της εσωτερικής απειλής. Τέταρτον, η χρήση Wi-Fi σε εργαστήριο ή άλλη εγκατάσταση αποτελεί συχνά σοβαρή ευπάθεια και αυτό επιδεινώνεται όταν επιτρέπονται προσωπικές συσκευές. Εάν μια προσωπική συσκευή είναι συνδεδεμένη στο εσωτερικό δίκτυο ενός οργανισμού και επιτρέπεται να εκπέμπει ως σημείο πρόσβασης Wi-Fi, δημιουργείται ένα νέο σημείο εισόδου για μια κακόβουλη ενέργεια. Τέλος, οποιαδήποτε προσωπική κινητή συσκευή μπορεί να χαθεί ή να κλαπεί. Και να εκθέσει τα συστήματα και τα δεδομένα του οργανισμού σε εισβολή, καταστροφή και κλοπή. Τα άτομα, οι επιχειρήσεις και οι κυβερνητικές υπηρεσίες διαπιστώνουν ότι τα οφέλη αποτελεσματικότητας και παραγωγικότητας της δικτύωσης κινητών συσκευών, εργαστηριακού εξοπλισμού και συστημάτων εγκαταστάσεων αντισταθμίζονται από τις ευπάθειες ασφαλείας που παρουσιάζουν (Kruse C.S., κ.α., 2017).

Η διείσδυση μέσω του διαδικτύου στον διασυνδεδεμένο εργαστηριακό εξοπλισμό και τον έλεγχο εγκαταστάσεων παρέχει πρόσβαση στα ευαίσθητα επιστημονικά και επιχειρηματικά δεδομένα του οργανισμού καθώς και στην πνευματική ιδιοκτησία. Εκτός από την άρνηση υπηρεσιών και την εισαγωγή κακόβουλου λογισμικού, οι επιθέσεις στον κυβερνοχώρο μπορούν να οδηγήσουν σε μια σειρά καταστροφικών αποτελεσμάτων η όπως εξαγωγή

δεδομένων, η δυσφήμιση και απώλεια οικονομικών στοιχείων που μπορούν να θέσουν υπό αμφισβήτηση τη βιωσιμότητα ενός οργανισμού. Αυτά τα αποτελέσματα, μπορεί να είναι η καταστροφή, η κλοπή, η δημόσια διάδοση ή η κακόβουλη αλλοίωση ηλεκτρονικών επιστημονικών δεδομένων, ή/και εγγράφων εγκαταστάσεων που είναι ευαίσθητα στην ασφάλεια (όπως έγγραφα προϋπολογισμού, σχέδια προγραμμάτων, κατόψεις εγκαταστάσεων, διαδικασίες έκτακτης ανάγκης, σχέδια συνέχειας επιχειρήσεων κ.λπ.). Η πρόσβαση σε έναν συνδεδεμένο εργαστηριακό εξοπλισμό, όπως καταψύκτες, ψυγεία και θερμοκοιτίδες, μπορεί να έχει ως αποτέλεσμα την καταστροφή πολύτιμων αντιδραστηρίων και μικροοργανισμών. Ο δικτυωμένος εξοπλισμός μπορεί να απενεργοποιηθεί και να οδηγήσει σε απώλεια δεδομένων και χρόνου εργασίας. Οι αλλαγές στο φως, τη θερμοκρασία ή την υγρασία στους χώρους μπορεί να οδηγήσουν στην καταστροφή και την αλλοίωση πολύτιμων και δαπανηρών ερευνητικών πόρων, όπως π.χ. φυτών, ζώων και μικροοργανισμών (J Craig Reed and Sharpe D.C., 2013).

Όπως είπαμε και παραπάνω τα έξυπνα εργαστήρια θα λειτουργούν, αν δεν έχουν ήδη ξεκινήσει να λειτουργούν, όπως τα έξυπνα σπίτια. Τα έξυπνα ηχεία που χρησιμοποιούνται στα σπίτια (π.χ. Alexa) είναι συνδεδεμένες συσκευές στο διαδίκτυο που διαθέτουν ηχεία και μικρόφωνα. Η κύρια είσοδος και έξοδος τους είναι φωνή (ή φωνή και βίντεο για συσκευές με δυνατότητα βίντεο). Μέσω της επεξεργασίας φυσικής γλώσσας, των δεδομένων τοποθεσίας και της πρόσβασης σε δεδομένα που είναι αποθηκευμένα στο cloud, αυτές οι συσκευές παρέχουν πληροφορίες ήχου απευθείας στους χρήστες και επιτρέπουν στους χρήστες να έχουν πρόσβαση, να ελέγχουν και να παρακολουθούν προϊόντα συνδεδεμένα στο διαδίκτυο, όπως θερμοστάτες, φωτισμό, συστήματα ασφαλείας και οικιακές συσκευές. Η επεξεργασία φυσικής γλώσσας είναι ένας από τους πέντε υποτομείς της τεχνητής νοημοσύνης (AI) και είναι η τεχνολογία που επιτρέπει σε έναν υπολογιστή να κατανοεί και να ανταποκρίνεται σε οποιαδήποτε ανθρώπινη γλώσσα. Η επεξεργασία φυσικής γλώσσας είναι αυτό που επιτρέπει σε ένα τέτοιο σύστημα να λαμβάνει προφορικές οδηγίες και να ανταποκρίνεται με ανθρώπινη φωνή. Όπως τα έξυπνα ηχεία χρησιμοποιούνται στο σπίτι για να παίζουν μουσική, να παραγγέλνουν πίτσα ή να καλούν

κάποιον, είναι θέμα χρόνου να χρησιμοποιηθούν έξυπνα ηχεία στο εργαστήριο για παρόμοιες λειτουργίες. Τα έξυπνα ηχεία θα τοποθετηθούν σε όλους τους χώρους των εργαστηρίων και οι χρήστες θα ζητήσουν από έξυπνα ηχεία να παρουσιάσουν τυποποιημένες διαδικασίες λειτουργίας, εκπαιδευτικά βίντεο, γραπτά έγγραφα και ηλεκτρονικά σημειωματάρια εργαστηρίου. Για να μειωθούν ή να εξαλειφθούν οι διαταραχές των άλλων στο χώρο εργασίας, τα έξυπνα ηχεία θα συζευχθούν με ακουστικά με δυνατότητα Bluetooth για να επιτρέψουν τη διακριτή επικοινωνία και τη λήψη περιεχομένου ήχου από το δικτυωμένο σύστημα ηχείων. Τα άτομα θα μπορούν να χρησιμοποιούν έξυπνα ηχεία για να ειδοποιούν την ηγεσία για καταστάσεις έκτακτης ανάγκης σχετικά με την ασφάλεια και την προστασία (Burnette R.N., Reed J.C. and Delarosa P., 2013).

Η τεχνητή νοημοσύνη είναι η ευρεία επιστήμη της εκπαίδευσης και εκμάθησης μιας μηχανής για να μιμηθεί τις ανθρώπινες ικανότητες για την εκτέλεση ανθρώπινων εργασιών και περιλαμβάνει πολυάριθμα υποπεδία: μηχανική μάθηση, ομιλία, υπολογιστική όραση, ρομποτική, σχεδιασμός, προγραμματισμός, βελτιστοποίηση και επεξεργασία φυσικής γλώσσας. Η μηχανική μάθηση εφαρμόζει διάφορες μορφές ανάλυσης δεδομένων σε τεράστιους όγκους εξαιρετικά λεπτομερών και ποικίλων κομματιών δεδομένων για τον εντοπισμό ευρέων μοτίβων και την εξαγωγή συμπερασμάτων. Ένα εργαστήριο με τεχνητή νοημοσύνη θα μπορεί να ειδοποιήσει το γραφείο ασφαλείας για ένα συμβάν ή ένα ατύχημα και θα έχει τη δυνατότητα να αναλύσει τις πληροφορίες ώστε άλλα εργαστήρια να αποφύγουν τα ζητήματα που οδήγησαν στο συμβάν ή το ατύχημα. Παρόλο που απαιτούνται τεράστιοι όγκοι δεδομένων για να καταστούν αποτελεσματικά τα εργαλεία ανάλυσης δεδομένων και τεχνητής νοημοσύνης, μόλις συγκεντρωθούν επαρκή ιστορικά και ζωντανά εργαστηριακά δεδομένα, τα εργαλεία αυτά θα βοηθήσουν τις θεσμικές επιτροπές ασφάλειας και προστασίας στον εντοπισμό και τη διόρθωση των τρωτών σημείων που σχετίζονται με διοικητικούς ελέγχους, όπως οι τυπικές διαδικασίες λειτουργίας και διαδικασίες ασφαλείας. Τελικά, οι συστάσεις και οι συμβουλές που δημιουργούνται από την τεχνητή νοημοσύνη, θα παρέχονται απευθείας στο προσωπικό του

εργαστηρίου σε πραγματικό χρόνο μέσω του έξυπνου ηχείου ή άλλης συσκευής για την πρόληψη μη ασφαλών πρακτικών που ενδέχεται να προκαλέσουν επικείμενη βλάβη στους εργαζόμενους (Shubhendu S. and Vijay J., 2013).

Πέρα από τα εργαστήρια του μέλλοντος προς το παρόν τα εργαστήρια πρέπει να εφαρμόσουν ένα σύστημα διαχείρισης και ασφάλειας στον κυβερνοχώρο για την προστασία, την παρακολούθηση και τη σκλήρυνση όλων των πτυχών της κυβερνοβιοασφάλειας. Για να επιτευχθεί αυτό, οι οργανισμοί πρέπει να αναπτύξουν ένα σχέδιο ασφάλειας που να περιλαμβάνει όλα τα πιθανά τρωτά σημεία κυβερνοβιοασφάλειας που σχετίζονται με τις επικοινωνίες, τις ευαίσθητες πληροφορίες, τα δεδομένα από τις εργαστηριακές συσκευές και συστήματα εγκαταστάσεων και τη φυσική πρόσβαση σε τερματικά υπολογιστών. Ένα αποτελεσματικό σχέδιο ασφάλειας στον κυβερνοχώρο περιλαμβάνει ένα εγχειρίδιο κυβερνοβιοασφάλειας που ευαισθητοποιεί τους χρήστες στις επιπτώσεις πιθανών τρωτών σημείων, τονίζει τη σημασία της επαγρύπνησης για την ασφάλεια (Greninger A.L., κ.α., 2019).

Επιπλέον, το σχέδιο ασφάλειας πρέπει να βασίζεται σε σαφή πολιτική που να δηλώνει ότι όλα τα εταιρικά δεδομένα θα προστατεύονται σθεναρά, θα περιορίζονται στη διανομή, θα παρακολουθούνται ενεργά για εισβολή, κλοπή και διαρροή και δεν θα είναι ποτέ διαθέσιμα στο κοινό στο διαδίκτυο. Αυτό σημαίνει ότι οι ηλεκτρονικές επικοινωνίες, οι ροές δεδομένων και οι οργανωτικές πληροφορίες κρυπτογραφούνται σε όλα τα στάδια για την πρόληψη της διαφθοράς ή της κλοπής και υπόκεινται σε ασφαλή αποθήκευση στο cloud ή ασφαλή αποθήκευση εκτός ιστότοπου και δημιουργούνται αντίγραφα ασφαλείας. Όλες πληροφορίες πρέπει να λαμβάνουν διαβαθμισμένη προστασία ασφαλείας μέσω συστηματικής ταξινόμησης (δηλ. δημόσια, ευαίσθητα, μόνο για επαγγελματική χρήση, περιορισμένα, άκρως εμπιστευτικά) και να υπόκεινται σε αυστηρές διαδικασίες ελέγχου πρόσβασης, συμπεριλαμβανομένης της διαχείρισης δικαιωμάτων για τον έλεγχο της δυνατότητας των ατόμων να βλέπουν, να επεξεργάζονται, να κατεβάζουν, να εκτυπώνουν και να διανέμουν ηλεκτρονικά πληροφορίες τόσο εσωτερικά όσο και εξωτερικά. Η πρόσβαση των εργαζομένων θα πρέπει να περιορίζεται

μόνο στις πληροφορίες που είναι απαραίτητες για την εκτέλεση της εργασίας τους. Οι αυτοματοποιημένες δραστηριότητες πληροφορικής θα πρέπει να περιλαμβάνουν αυτοματοποιημένες σαρώσεις ιών και κακόβουλου λογισμικού, σε ολόκληρη την επιχείρηση για όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου και τις λήψεις, ενώ θα πρέπει να γίνει εκπαίδευση του προσωπικού για την αναγνώριση και την αναφορά απάτης ηλεκτρονικού "ψαρέματος", την παρακολούθηση όλων των δραστηριοτήτων του προσωπικού σε εσωτερικό ηλεκτρονικό υλικό και την παρακολούθηση όλων των λήψεων δεδομένων και των δραστηριοτήτων διαδικτύου στα δίκτυα του οργανισμού για τον εντοπισμό της εσωτερικής απειλής. Η διανομή ευαίσθητων πληροφοριών σε προμηθευτές, εργολάβους και παρόχους υπηρεσιών πρέπει να υπόκειται σε συμφωνίες εμπιστευτικότητας και πρέπει πάντα να ελέγχεται, να περιορίζεται και να κρυπτογραφείται. Τα ζητήματα ασφάλειας στον κυβερνοχώρο πρέπει να αποτελέσουν κορυφαία προτεραιότητα πριν από την ανάπτυξη οποιασδήποτε τεχνολογίας στον χώρο των βιοεπιστημών, όπου κάθε σημείο ηλεκτρονικής διεπαφής παρουσιάζει ευπάθεια ώστε να καταστήσουν την κυβερνοβιοασφάλεια άμεσο και θεμελιώδες στοιχείο των προσπαθειών σχεδιασμού λογισμικού και προϊόντων τους (Kwok R., 2018).

Η κυβέρνηση των ΗΠΑ έχει επενδύσει στην ανάπτυξη και παραγωγή κρίσιμων εμβολίων και βιοθεραπευτικών μεθόδων τόσο για πολιτικούς όσο και για στρατιωτικούς σκοπούς. Ταυτόχρονα, ειδικοί επισημαίνουν ότι οι βιοκατασκευές είναι δυνητικά ευάλωτες σε ανεπιθύμητες ή παράνομες δραστηριότητες που μπορεί να οδηγήσουν σε επιζήμια αποτελέσματα, όπως κλοπή πνευματικής ιδιοκτησίας, διακοπή της εφοδιαστικής αλυσίδας, χειραγώγηση της ανάπτυξης και της βιοπαραγωγής, κυβερνοεπιθέσεις σε βασικά στοιχεία της τεχνολογίας των πληροφοριών, καταστροφές κρίσιμων δεδομένων και χειραγώγηση συστημάτων και των υποδομών ασφαλείας από τις οποίες εξαρτάται η ασφαλής λειτουργία των εγκαταστάσεων. Η πολυδιάστατη ανάλυση μιας υπάρχουσας μονάδας βιοπαραγωγής-εργαστηρίου, για τον προσδιορισμό της ασφάλειας, των κενών και τρωτών σημείων, έθεσαν τις βάσεις για πιο συγκεκριμένα και ολοκληρωμένα μέτρα που πρέπει να ληφθούν. Αυτή η

προσέγγιση της ανάλυσης συστημάτων που χρησιμοποιήθηκε και σχεδιάστηκε για την αξιολόγηση της κατάστασης ασφάλειας, καθορίζοντας και ποια είναι η αποδεκτή κατάσταση ασφάλειας, παρέχοντας καθοδήγηση και συστάσεις, ώστε η κάθε εγκατάσταση να φτάσει στο επιθυμητό αποτέλεσμα. Αυτή η προσέγγιση-τεχνική της βιοπαραγωγής και των βιοδιαδικασιών που χρησιμοποιείται αναφέρεται ως το «κρεβάτι δοκιμής». Εάν τα αποτελέσματα από αυτό το «κρεβάτι δοκιμής» ανταποκρίνονται στις προσδοκίες του πελάτη και ο πελάτης λάβει κυβερνητική έγκριση, ο πελάτης παράγει το προϊόν το οποίο διατίθεται εν συνεχεία στην αγορά. Αυτή η εγκατάσταση μελετήθηκε ως σύστημα, που αποτελείται από τέσσερα βασικά, αλληλένδετα υποσυστήματα: την ανάπτυξη/βιοκατασκευή-βιοδιαδικασία, την εφοδιαστική αλυσίδα και τα υποστηρικτικά πληροφοριακά συστήματα, τις υποδομές και τις κυβερνο-φυσικές διεπαφές για την βιοδιεργασία. Η ανάλυση αυτών των συστημάτων ήταν μια σταδιακή διαδικασία που μελετήθηκε διεξοδικά. Η εγκατάσταση ή οποιαδήποτε από αυτά τα συστήματα ή λειτουργίες δεν παραβιάστηκαν, αλλά και όσα αλλοιώθηκαν ή τροποποιήθηκαν κατά τη διάρκεια αυτής της διαδικασίας με οποιονδήποτε τρόπο ή μορφή επίσης αξιολογήθηκαν και προέκυψαν τα εξής συμπεράσματα:

- «Τα τρωτά σημεία μπορεί να υπάρχουν σε ολόκληρο το σύστημα, από την αρχική διαδικασία, την αλυσίδα εφοδιασμού, στις υποδομές ή στα συστήματα που λειτουργούν στον κυβερνοχώρο».
- «Η επιτυχής εκμετάλλευση των τρωτών σημείων μπορεί να πραγματοποιηθεί μέσω παθητικών και ενεργητικών μέσων για παθητικούς και ενεργητικούς σκοπούς, ανάλογα με τις προθέσεις, τους στόχους, τις προσβάσεις των αντιπάλων, τις γνώσεις και τους πόρους καθώς και τα επιδιωκόμενα αποτελέσματα».
- «Η εκμετάλλευση ορισμένων τρωτών σημείων απαιτεί άμεση πρόσβαση σε εγκαταστάσεις ή εξαρτήματα και προσωπικό πτυχές που δεν πρέπει να παραβλέπονται».
- «Οι αντίπαλοι μπορούν να χρησιμοποιήσουν συνδυασμούς και αλληλουχίες μεθόδων με συγκριμένη στόχευση για να επιτύχουν τους στόχους τους».

- «Οι επιχειρησιακές δυνατότητες των αντιπάλων, όχι μόνο οι τεχνικές, πρέπει να ληφθούν υπόψη και να ληφθούν υπόψη και στον σχεδιασμό για την εφαρμογή μέτρων ασφαλείας» (Randall S. Murch, κ.α. 2018).

5.1. <u>Προτάσεις για ένα καλύτερο επίπεδο κυβερνοβιοασφάλειας.</u>

«Η κυβερνοβιοασφάλεια αποτελεί ένα εντελώς νέο επιστημονικό πεδίο των διεθνών σχέσεων και της διεθνούς ασφάλειας και βιοασφάλειας και έχει ως βασικό στόχο την ανάλυση της αλληλεξάρτησης μεταξύ του κυβερνοχώρου και των πολιτικών βιοασφάλειας στο πλαίσιο αντιμετώπισης των βιολογικών απειλών και βιο-υβριδικών απειλών» (Λιαρόπουλος Α. και Μποζίνης Α. (Επιμ.), 2022). Η ύπαρξή της επηρεάζει οργανισμούς σε πολλούς διαφορετικούς τομείς, από την γεωργία και τον μεταποιητικό τομέα μέχρι και την υγειονομική περίθαλψη. Αν και τα ενδιαφερόμενα μέρη έχουν εύλογο συμφέρον για μια αποτελεσματική κυβερνοβιοασφάλεια, παρόλα αυτά ένα σχετικά μικρό σύνολο ατόμων είναι κατάλληλα για να το πράξουν. Λόγω του πολυεπιστημονικού της χαρακτήρα, αυτοί που ενεργούν την αξιολόγηση, την ανάλυση την αναγνώριση και την προστασία των τρωτών σημείων της κυβερνοβιοασφάλειας θα πρέπει να είναι γνώστες τόσο των βιοεπιστημών όσο και της τεχνολογίας της πληροφορικής. Ακόμη και σήμερα ωστόσο, η βιοασφάλεια εμπίπτει συνήθως στην αρμοδιότητα των επαγγελματιών της θεσμικής ασφάλειας και της βιοασφάλειας, που εργάζονται με βάση μόνο την κατανόηση του τοπίου απειλών σε μια μόνο πτυχή (π.χ. αμελείς επιστήμονες χωρίς κακόβουλη πρόθεση ή με στοχευόμενη πρόθεση κλοπής ή καταστροφής για συγκεκριμένο κέρδος).

Από την άλλη η κυβερνοασφάλεια εκπροσωπείται σε θεσμικό επίπεδο από τους επαγγελματίες της πληροφορικής, με χιλιάδες θεμελιώδεις βάσεις γνώσεων για την ασφάλεια δικτύων και των συστημάτων. Στο τομέα της κυβερνοβιοαφάλειας όμως, απαιτείται, ανάπτυξη επαγγελματιών με εκπαίδευση από διαφορετικούς κλάδους των βιοεπιστημών και της πληροφορικής και των νέων τεχνολογιών. Ένα άτομο με κατανόηση της πληροφορικής και της κυβερνοασφάλειας, με υπόβαθρο στις βιολογικές επιστήμες, μπορεί και είναι σε θέση να γνωρίζει τις βασικές αρχές του κινδύνου, της απειλής και της ευαλωτότητας που αφορούν την κυβερνοβιοασφάλεια. Άλλη μια παράμετρος μεταξύ της βιοασφάλειας και της πληροφορικής αφορά τον τρόπο εκμάθησης και εκπαίδευσης. Η κατάρτιση στον τομέα της τεχνολογίας και της

πληροφορικής ποικίλει αλλά είναι καθιερωμένη. Είναι εφικτό να γίνεις ειδικός σε έναν από τους τομείς της πληροφορικής μέσω της παραδοσιακής εκπαίδευσης (δηλ. πανεπιστημιακά ή προγράμματα επαγγελματικής κατάρτισης), αλλά δεν απαιτείται κιόλας καθώς υπάρχουν πολλά μονοπάτια και ευκαιρίες για να γίνεις ειδικός σε έναν από τους κλάδους του ευρύτερου τομέα της πληροφορικής. Ανάλογα με τον κλάδο πληροφορικής στον οποίο κάποιος επιθυμεί ειδίκευση, υπάρχει μια σειρά από προγράμματα κατάρτισης που έχουν σχεδιαστεί και απευθύνονται σε άτομα με μικρή έως καθόλου εμπειρία. Σε ένα παραδοσιακό ακαδημαϊκό περιβάλλον, τα άτομα μπορούν να επιλέξουν να ειδικευτούν στα πρόγραμμα μηχανικής υπολογιστών και σε μια σειρά από κλάδους όπως η μηχανική δικτύων έως την ανάπτυξη λογισμικού.

Σε αντίθεση με τις βιοεπιστήμες, τεχνογνωσία πληροφορικής μπορεί επίσης να αποκτηθεί και μέσω μιας λιγότερο τυπικής διαδρομής καθώς ένα άτομο μπορεί να επιλέξει να παρακολουθήσει ένα πρόγραμμα κατάρτισης που φιλοξενείται από μη ακαδημαϊκό οργανισμό, χωρίς να μπορεί να παραληφθεί η εμπειρία και η εξειδίκευση που αποκομίζει κάποιος μέσω της εργασίας πάνω σε ένα συναφές αντικείμενο απασχόλησης. Στις βιοεπιστήμες, η εκπαίδευση αποτελείται από μια ευρεία και μικτή προσέγγιση διδασκαλίας, η οποία συμπεριλαμβάνει την παραδοσιακή διδασκαλία στην τάξη, την πρακτική άσκηση και τα εργαστήρια, ενώ μπορεί να περιλαμβάνει και διαδικτυακές ενότητες. Κοινό σημείο της κυβερνοασφάλειας και της βιοασφάλειας αποτελεί η διαχείριση και η αντιμετώπιση του κινδύνου και των απειλών.

Η υιοθέτηση πλαισίου πιστοποίησης και υλοποίησης αποτελεί άλλο ένα μέτρο με σκοπό την εκπαίδευση των ενδιαφερομένων επαγγελματιών που εργάζονται στον αναδυόμενο τομέα της κυβερνοβιοασφάλειας. Από την στιγμή που υπάρχουν διαφορετικές έννοιες σε καθέναν από τους κλάδους της κυβερνοασφάλειας και της βιοασφάλειας, τα ενδιαφερόμενα μέρη θα πρέπει να κατανοήσουν τις μοναδικές προκλήσεις που υπάρχουν και στους δύο τομείς. Η χρήση συστημάτων πιστοποίησης μπορεί να είναι επωφελής για την τυποποίηση της βάσης των

γνώσεων που απαιτούνται για να είναι κάποιος ειδικός στον τομέα αυτόν, κάτι που δεν αποκλείει την ύπαρξη υποπεδίων σε κάθε κλάδο που σχετίζεται με την κυβερνοβιοασφάλεια.

Τέλος, σημαντικότερα μέτρα που μπορούν να αναβαθμίσουν, να ενισχύσουν και να καταστήσουν την κυβερνοβιοασφάλεια ισχυρή είναι τα εξής:

- «Συμμετοχή και συνεργασία ειδικών-επιστημώνων στους τομείς της βιοτεχνολογίας, της βιοασφάλειας, της κυβερνοασφάλειας και της φυσικής ασφάλειας σε μια συνεργασία στη λήψη αποφάσεων».
- «Προσδιορισμός των σχετικών βιομηχανικών προτύπων, νομικών πλαισίων και ρυθμιστικών κανόνων που ισχύουν για την κυβερνοβιοασφάλεια».
- «Καθορισμός σαφών και κοινών προϋποθέσεων, απαιτήσεων και διαδικασιών αξιολόγησης, ώστε να γίνει ευρύτερα κατανοητό το πλαίσιο λειτουργίας και ασφάλειας εντός του οποίου θα πρέπει να λειτουργούν οι εμπλεκόμενοι».
- «Καθιέρωση μιας ολοκληρωμένης και ενιαίας ταξινόμησης χαρακτηριστικών των στοιχείων και των συστημάτων που χρησιμοποιούνται στον κυβερνοχώρο από την βιοτεχνολογία και επηρεάζουν την ασφάλεια και χρήση σχετικών μέτρων ασφαλείας».
- «Συλλογή των υφιστάμενων δεδομένων αξιολόγησης για τον τρόπο λειτουργίας του πλαισίου της κυβερνοβιοασφάλειας και επαναξιολόγησή της».
- «Η εκπαίδευση πάνω σε ζητήματα κυβερνοβιοασφάλειας θα βοηθούσε τους ανθρώπους να είναι περισσότεροι προσεκτικοί και καλύτερα προετοιμασμένοι ώστε αντιμετωπίσουν θέματα ασφάλειας».
- «Οι εμπλεκόμενοι οργανισμοί θα πρέπει να δημιουργήσουν πρωτόκολλα ασφαλείας τα οποία θα πρέπει να ακολουθήσουν σε περίπτωση που υπάρχει υποψία ή ένδειξη για παραβίαση ασφαλείας».
- «Σε πολιτειακό, ευρωπαϊκό και διεθνές επίπεδο, θα πρέπει να θεσπιστεί συναφής νομοθετικό πλαίσιο που να εντάσσει την κυβερνοβιοασφάλεια στις νομοθετικές ρυθμίσεις σε

συγκεκριμένους τομείς όπως στην γεωργία και την εφοδιαστική αλυσίδα αλλά και σε γενικό πλαίσιο».

- «Η παροχή επιδοτούμενου ειδικού εξοπλισμού και τεχνογνωσίας στις μικρομεσαίες επιχειρήσεις που θέλουν να βελτιώσουν την ασφάλεια τους».

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

1. Λιαρόπουλος Α. και Μποζίνης Α. (Επιμέλεια), 2022, Διακυβέρνηση του Κυβερνοχώρου και Κυβερνοασφάλεια στις Διεθνείς Σχέσεις, Αθήνα: Παπαζήση.

ΑΡΘΡΑ

1. Agnieszka GRYSZCZYŃSKA 2021, The impact of the COVID-19 pandemic on cybercrime doi:10.24425/bpasts.2021.137933
2. Asha M. George 2019, The National Security Implications of Cyberbiosecurity, https://doi.org/10.3389/fbioe.2019.00051
3. Boris A., Vinatzer Lenwood, S. Heath, Hussain M.J., Almohri, Michael J., Stulberg, Christopher Lowe and Song Li 2019 Cyberbiosecurity Challenges of Pathogen Genome Databases, https://doi.org/10.3389/fbioe.2019.00106
4. Brown A., Tuor A., Hutchinson B. and Nichols, N., 2018, Recurrent neural network attention mechanisms for interpretable system log anomaly detection in Proceedings of the First Workshop on Machine Learning for Computing Systems, https://dl.acm.org/doi/abs/10.1145/3217871.3217872
5. Burnette R.N., Reed J.C. and Delarosa P., 2013, The future of biosecurity: a global context" in Biosecurity – Understanding, Assessing, and Preventing the Threat, ed R. Burnette (Hoboken, NJ: John Wiley and Sons, Inc.),259–269. Burnette: Το μέλλον της βιοασφάλειας: ένα παγκόσμιο πλαίσιο - Μελετητής Google
6. Collier B., 2020, Boredom, routine activities, and cybercrime during the pandemic, https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-4.pdf)
7. Colston S.M., Fullmer M.S., Beka L., Lamy B., Gogarten J.P., and Graf J., 2014, Bioinformatic genome comparisons for taxonomic and phylogenetic assignments using Aeromonas as a test case, doi: 10.1128/mBio.02136-14

8. Daniel S. Schabacker, Leslie-Anne Levy Nate J. Evans, Jennifer M. Fowler and Ellen A. Dickey 2019, Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience. https://doi.org/10.3389/fbioe.2019.00061
9. David Buil-Gil, Fernando Miró-Llinares, Asier Moneva, Steven Kemp & Nacho Díaz-Castaño 2020, Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK, doi:10.1080/14616696.2020.1804973
10. David G. Schmale, Andrew P., Walid Saad, Durelle T. Scott and Judy A. Westrick, 2019 Perspectives on Harmful Algal Blooms (HABs) and the Cyberbiosecurity of Freshwater Systems, https://doi.org/10.3389/fbioe.2019.00128
11. Donovan Guttieres, Shannon Stewart, Jacqueline Wolfrum and Stacy L. Spring 2019, Cyberbiosecurity in Advanced Manufacturing Models, https://doi.org/10.3389/fbioe.2019.00210
12. Geil, A., Sagers, G., Spaulding, A. D., and Wolf, J.R., 2018, Cyber Security on the Farm: an Assessment of Cyber Security Practices in the United States Agriculture Industry doi:10.22434/ifamr2017.0045
13. Gregory D. Koblentz 2009, Living Weapons: Biological Warfare and International Security, Ithaca, N.Y.: Cornell University Press.
14. Gregory D. Koblentz 2010 Biosecurity Reconsidered Calibrating Biological Threats and Responses.
15. Greninger A.L., Zerr D.M., Qin X., Adler A.L., Sampoleo R., Kuypers J.M., 2017, Rapid metagenomic next-generation sequencing during an investigation of hospital-acquired human parainfluenza virus 3 infections, doi: 10.1128/JCM.01881-16
16. Harjinder Singh, Lallie Lynsay, A. Shepherd, Jason R. C., Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Belleken, 2020, Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic
17. House, T. W. 2012 National bioeconomy blueprint, doi: 10.1089/ind.2012.1524

18. Jacob Caswell, Jason D. Gans, Nicholas Generous, Corey M. Hudson, Eric Merkley, Curtis Johnson, Christopher Oehmen, Kristin Omberg , Emilie Purvine, Karen Taylor , Christina L. Ting, Murray Wolinsky and Gary Xie, 2019, Defending Our Public Biological Databases as a Global Critical Infrastructure https://doi.org/10.3389/fbioe.2019.00058
19. James Diggans και Emily Leprost, 2019, Next steps for Access to Safe, Secure DNA Synthesis, https://www.frontiersin.org/articles/10.3389/fbioe.2019.00086/full#B6:~:text=https%3A//doi.org/10.3389/fbioe.2019.00086
20. J Craig Reed and Nicolas Dunaway, 2019 Cyberbiosecurity Implications for the Laboratory of the Future, https://doi.org/10.3389/fbioe.2019.00182
21. J Craig Reed and Sharpe, D.C., 2013, Operational elements of biosecurity" in Biosecurity – Understanding, Assessing, and Preventing the Threat, ed R. Burnette (Hoboken, NJ: John Wiley and Sons, Inc., 71–88.
22. Jean-Loup Richet 2022 How cybercriminal communities grow and change: An investigation of ad-fraud communities https://doi.org/10.1016/j.techfore.2021.121282
23. Jennifer L. Mantle, Jayan Rammohan, Eugenia F. Romantseva , Joel T. Welch, Leah R. Kauffman, Jim McCarthy, John Schiel Jeffrey C. Baker, 2019, Cyberbiosecurity for Biopharmaceutical Products, https://doi.org/10.3389/fbioe.2019.00116
24. Johannes Wiggen 2020, The impact of COVID-19 on cyber crime and state-sponsored cyber activities: https://www.jstor.org/stable/resrep25300
25. Kathryn Millett, Eduardo dos Santos and Piers D. Millett, 2019, Cyber-Biosecurity Risk Perceptions in the Biotech Sector, https://doi.org/10.3389/fbioe.2019.00136
26. Kavita M. Berger and Phyllis A. Schneck, 2019, National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data, https://doi.org/10.3389/fbioe.2019.00021
27. Kozminski, K. G. 2015, Biosecurity in the age of Big Data: a conversation with the FBI., doi: 10.1091/mbc. E14-01-0027

28. Kruse C.S., Frederick B., Jacobson T. and Monticone D.K., 2017, Cybersecurity in healthcare: a systematic review of modern threats and trends, doi: 10.3233/THC-161263
29. Kwok R., 2018, How to pick an electronic laboratory notebook. Nature, https://doi.org/10.1038/d41586-018-05895-3
30. L. Sweeney 2000, Simple Demographics Often Identify People Uniquely, https://dataprivacylab.org/projects/identifiability/paper1.pdf
31. Lauren C. Richardson, Nancy D. Connell, Stephen M. Lewis, Eleonore Pauwels, and Randy S. Murch 2019, Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape, doi: 10.3389/fbioe.2019.00099
32. Lauren C. Richardson, Stephen M. Lewis and Ryan N. Burnette, 2019, Building Capacity for Cyberbiosecurity Training, https://doi.org/10.3389/fbioe.2019.00112
33. Manuela Oliveira, Gabriella Mason-Buck, David Ballard Wojciech Branicki and António Amorima, 2020 Biowarfare, bioterrorism and biocrime: A historical overview on microbial harmful applications, https://doi.org/10.1016/j.forsciint.2020.110366.
34. Marcus Felson Ronald V. Clarke, 1998, Opportunity Makes the Thief Practical theory for crime prevention, https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf
35. Michael Moodie and William J. Taylor Jr. 2000, Contagion and Conflict: Health as a Global Security Challenge (Washington, D.C.: Chemical and Biological Arms Control Institute and Center for Strategic and International Studies.
36. Muhammad Kashan Javed, 2020, A Surge in Cyber-Crime during COVID-19 Αύγουστος 2020Indonesian Journal of Social and Environmental Issues, https://doi.org/10.47540/ijsei.v1i2.22
37. Panguluri, S., Nelson, T. D. and Wyman, R.P., 2017, Creating a cyber security culture for your water/waste water utility in Cyber-Physical Security, doi: 10.1007/978-3-319-32824-9_7
38. Peccoud J., Gallegos J.E., Murch R., Buchholz W.G., and Raman S., 2018, Cyberbiosecurity: from naive trust to risk awareness. Trends Biotechnol, doi: 10.1016/j.tibtech.2017.10.012

39. Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., and Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. Trends Biotechnol, doi: 10.1016/j.tibtech.2017.10.012
40. Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., and Raman, S., 2018, Cyberbiosecurity: from naive trust to risk awareness. Trends Biotechnol. doi: 10.1016/j.tibtech.2017.10.012
41. Peter Ney, Luis Ceze, Tadayoshi Kohno Paul G., 2019, Allen Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference, https://www.ndss-symposium.org/ndss-paper/genotype-extraction-and-false-relative-attacks-security-risks-to-third-party-genetic-genealogy-services-beyond-identity-inference/
42. Peter Ney, Luis Ceze, Tadayoshi Kohno, 2019 Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference, ανακτήθηκε από https://dnasec.cs.washington.edu/genetic-genealogy
43. Randall S. Murch, William K. So, Wallace G. Buchholz, Sanjay Raman and Jean Peccoud 2018, Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy https://doi.org/10.3389/fbioe.2018.00039
44. Renault, V.; Humblet, M.-F.; Saegerman, C. Biosecurity Concept: Origins, Evolution and Perspectives. Animals 2022, 12, 63. https:// doi.org/10.3390/ani12010063
45. Rennie Naidoo 2020, A multi-level influence model of COVID-19 themed cybercrime Department of Informatics, University of Pretoria, Pretoria, South Africa https://doi.org/10.1080/0960085X.2020.1771222
46. Ross J. Anderson 2008, Security Engineering: A Guide to Building Dependable Distributed Systems.
47. RossBrewer 2016, Ransomware attacks: detection, prevention and cure.

48. Saadia Arshad, Junaid Arshad, Muhammad Mubashir Khan, Simon Parkinson 2021 Analysis of security and privacy challenges for DNA-genomics applications and databases Journal of Biomedical Informatics, doi: 10.1016/j.jbi.2021.103815
49. Saadia Arshad, Junaid Arshad, Muhammad Mubashir Khan, Simon Parkinson, 2021, Analysis of security and privacy challenges for DNA-genomics applications and databases, https://doi.org/10.1016/j.jbi.2021.103815
50. Shubhendu S. and Vijay J., 2013, Applicability of artificial intelligence in different fields of life, Intl. J. Sci. Eng. Res. 1, 2347–3878, MDExMzA5MTU_-libre.pdf (d1wqtxts1xzle7.cloudfront.net)
51. Scott Monteith , Michael Bauer & Martin Alda & John Geddes & Peter C Whybrow & Tasha Glenn 2021, Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry, https://doi.org/10.1007/s11920-021-01228-w
52. Sogo Angel Olofinbiyi and Shanta Balgobind Singh 2020, The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World's Upsurge in Cyber Crime https://www.researchgate.net/publication/342663258_The_Role_and_Place_of_Covid-19_An_Opportunistic_Avenue_for_Exponential_World's_Upsurge_in_Cyber_Crime
53. Sokolov, M., Feidl, F., Morbidelli, M., and Butté, A., 2017, Future challenges in BioPharma: the role of big data and digitalization technologies for drug manufacturing," in Presentation Presented at PharmaTalk, https://www.iottalk.eu/wp-content/uploads/2017/06/07.-Alessandro-Butte-ETH-Zurich.pdf
54. Steve Morgan 2019 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) by 2021, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
55. Steven Kemp David Buil-Gil, Asier Moneva, Fernando Miró-Llinares and Nacho Díaz-Castaño 2021, Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19, https://doi.org/10.1177/10439862211027986

56. Susan E. Duncan, Robert Reinhard, Robert C. Williams, Ford Ramsey , Wade Thomason, Kiho Lee, Nancy Dudek, Saied Mostaghimi, Edward Colbert and Randall Murch, 2019, Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System, https://doi.org/10.3389/fbioe.2019.00128
57. Szurdi J, Chen Z, Starov O, McCabe A, Duan R. Palo Alto Networks 2020, Studying how cybercriminals prey on the COVID-19 pandemic. https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic
58. Tiffany Drape, Noah Magerkorth, Anuradha Sen1, Joseph Simpson Megan Seibel , Randall Steven Murch and Susan E. Duncan, 2021, Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study, https://doi.org/10.3389/fbioe.2021.737927
59. Xavier-Lewis Palmer, Lucas Potter, and Saltuk Karahan 2020, On the Emerging Area of Biocybersecurity and Relevant Considerations.

ΔΙΑΔΥΚΤΙΑΚΕΣ ΠΗΓΕΣ

1. Ajtmh.org: infodemic, ανακτήθηκε από:https://www.ajtmh.org/view/journals/tpmd/103/4/article-p1621.xml.
2. Bacterial and Viral Bioinformatics resource center, ανακτήθηκε από: https://www.bv-brc.org/
3. BRITANICCA, ανακτήθηκε από: https://www.britannica.com/event/Tokyo-subway-attack-of-1995
4. CISA: Denial of Servisce Attacks, ανακτήθηκε από: https://www.cisa.gov/uscert/ncas/tips/ST04-015
5. Citizenlab: a quik look at the confidentiality of zoom meetings, ανακτήθηκε από: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
6. CNET: uk said russia is behind destructive 2017 cyberattack in Ukraine, ανακτήθηκε από:https://www.cnet.com/news/privacy/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

7. COE: Cybercrime, ανακτήθηκε από: https://www.coe.int/en/web/cybercrime
8. Cyberscoop: coronavirus-phishing-scams-iran-china, ανακτήθηκε από: https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china
9. cyberscoop: hospital-cyberattack-coronavirus, ανακτήθηκε από: https://www.cyberscoop.com/czech-hospital-cyberattack-coronavirus
10. Defense One: China is Secretly Enrolling Military Scientists, ανακτήθηκε από: China Is Secretly Enrolling Military Scientists in Western Universities - Defense One
11. ECA EUROPA: Cybersecurity, ανακτήθηκε από:https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf
12. EMBL-EBI:Data-resources, ανακτήθηκε από: https://www.ebi.ac.uk/services/data-resources-and-tools?query=ena
13. EU COMMISSION: Data protection, ανακτήθηκε από: https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_el
14. EU: Cybercrime, ανακτήθηκε από: https://home-affairs.ec.europa.eu/cybercrime_en
15. EUROPOL: Child sexual exploitation, ανακτήθηκε από: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation
16. FBI:anthrax-amerithrax, ανακτήθηκε από: https://archives.fbi.gov/archives/about-us/history/famous-cases/anthrax-amerithrax
17. Federated-Ega, ανακτήθηκε από: https://www.covid19dataportal.org/federated-ega
18. forbes: cyber-attack-stolen-data, ανακτήθηκε από: .https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/?sh=340cd8a618e5
19. Genomics: 100000 genomes project, ανακτήθηκε από: https://www.genomicsengland.co.uk/initiatives/100000-genomes-project

20. health21initiative:genomics data requires better data protection, ανακτήθηκε από: http://health21initiative.org/article/genomic-data-requires-better-protection/
21. IN. GR: Μποζίνης Α. Κυβερνο-βιοασφάλεια και βιο-υβριδικές απειλές, ανακτήθηκε από: https://www.in.gr/2020/12/21/b-science/gnomes/eidikoi/kyverno-vioasfaleia-kai-vio-yvridikes-apeiles/
22. Journal: Big Data Astronomical or Genomical, ανακτήθηκε από: https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.1002195
23. Michigan University: Data hackers, ανακτήθηκε από: https://msutoday.msu.edu/news/2019/heres-the-kind-of-data-hackers-get-about-you-from-hospitals
24. NCBI: Databases, ανακτήθηκε από: https://www.ncbi.nlm.nih.gov/guide/all/
25. NGDC: databasecommons, ανακτήθηκε από: https://ngdc.cncb.ac.cn/databasecommons/database/id/230
26. NIST: Framework for Improving Critical Infrastructure Cybersecurity, ανακτήθηκε από: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
27. Reuters: Merck says cyber attack halted production, will hurt profits, ανακτήθηκε από: Merck says cyber attack halted production, will hurt profits | Reuters
28. Shelly Palmer 2018, ανακτήθηκε από: https:// www.shellypalmer.com/events/ces-2018/media-tech-trend-report/
29. Social-engineer, ανακτήθηκε από: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/
30. tandfonline, ανακτήθηκε από: https://www.tandfonline.com/doi/full/10.1080/14636778.2016.1162092
31. technologyreview: more than 26 million people have taken an at home ancestry test, ανακτήθηκε από: https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/

32. UN: Cybersecurity, ανακτήθηκε από: https://www.un.org/counterterrorism/cybersecurity

33. Veupathdb, ανακτήθηκε από: https://veupathdb.org/veupathdb/app

34. WHO: H1N1 Pandemic, ανακτήθηκε από: http://www.who.int/csr/don/2009_11_27a/en/index.html.

35. zdnet: US Hospital pays 55.000$ to hackers, ανακτήθηκε από: https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

36. ανακτήθηκε από: https://www.amazon.com/Cybersecurity-Cyberwar-Everyone-Needs-Know%C2%AE/dp/0199918112

37. NIST: cyber attack, ανακτήθηκε από: https://csrc.nist.gov/glossary/term/cyber_attack

ΑΛΛΕΣ ΠΗΓΕΣ

1. Barton Gellman, "AIDS Is Declared Threat to Security," Washington Post, April 30, 2000.
2. Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism: World at Risk, ανακτήθηκε από: https://digital.library.unt.edu/ark:/67531/metadc123525/
3. Convention on Biological Diversity, ανακτήθηκε από: About the Nagoya Protocol (cbd.int)
4. George W. Bush, The National Security Strategy of the United States of America (Washington, D.C.: White House, 2006), p. 44.
5. Institute of Medicine and National Research Council, Globalization, Biosecurity, and the Future of the Life Sciences (Washington, D.C.: National Academies Press, 2006), pp. 79–112, ανακτήθηκε από https://nap.nationalacademies.org/catalog/11567/globalization-biosecurity-and-the-future-of-the-life-sciences

6. National Intelligence Council (NIC), The Global Infectious Disease Threat and Its Implications for the United States, NIE 99-17D (Washington, D.C.: NIC, January 2000), p. 5.
7. United Nations Security Council, “Security Council Holds Debate on Impact of AIDS on Peaceand Security in Africa,” press release, SC/6781, January 10, 2000.
8. Κανονισμός 511/2014 της Ε.Ε., ανακτήθηκε από: https://eur-lex.europa.eu/legalcontent/EL/TXT/HTML/?uri=CELEX:52019DC0013&from=IT
9. ν. 3937/2011, ΦΕΚ 60/A/31-3-2011.
10. Οδηγία (2020) 829, 2020/0365, ανακτήθηκε από: https://eur-lex.europa.eu/legalcontent/EL/TXT/HTML/?uri=CELEX:52020PC0829&from=EN