

# Κυβερνοβιοασφάλεια: Κίνδυνοι και Προκλήσεις στη Διασφάλιση της εξατομικευμένης θεραπείας στο σύγχρονο κοινωνικοοικονομικό γίγνεσθαι

Ιωάννης Γ. Χατζής<sup>1\*</sup>, Αγγελική Γριβοπούλου<sup>2</sup>, Περικλής Ρόμπολας<sup>3</sup>

<sup>1</sup>Δημόσιο Ινστιτούτο Επαγγελματικής Κατάρτισης Μεσολογγίου, Μεσολόγγι

<sup>2</sup>Σχολείο Δεύτερης Ευκαιρίας Μεσολογγίου, Μεσολόγγι

<sup>3</sup>Τμήμα Νοσηλευτικής, Τεχνολογικό Πανεπιστήμιο Κύπρου, Λεμεσός

## ΠΕΡΙΛΗΨΗ

Η Κυβερνοβιοασφάλεια αποτελεί ένα νέο αναδυόμενο πεδίο της παγκόσμιας βιοασφάλειας που δίνει έμφαση στη συνεχώς αυξανόμενη αλληλεξάρτηση του κυβερνοχώρου και της βιοασφάλειας. Η ανάπτυξη αυτού του επιστημονικού και επιχειρησιακού πεδίου προκύπτει παράλληλα με τη σύγχρονη πραγματικότητα ψηφιοποίησης των οικονομικών, κοινωνικών και πολιτικών δραστηριοτήτων που καθίσταται ζωτική στην πραγματοποίηση εξατομικευμένων θεραπευτικών σχημάτων και η σημασία της θα αυξάνει καθώς η τεχνητή νοημοσύνη και η ψηφιοποίηση θα επιταχύνονται ποσοτικά και ποιοτικά. Ταυτόχρονα η κυβερνοβιοασφάλεια θέτει τις βάσεις για νέες προ-

σεγγίσεις και προτεραιότητες σε επείγοντα και πολύπλοκα θέματα διεθνούς και εθνικής βιοασφάλειας, ειδικά σε καταστάσεις όπως η πανδημία COVID-19 και άλλες ταχέως εξελισσόμενες και μεταδιδόμενες επιδημίες, με πιθανή υπαρξιακή επίπτωση, όπως οι Βιοκίνδυνοι Πλανητικά Καταστρεπτικής Επίπτωσης (ΒΠΚΕ-GCBR). Σε ένα τέτοιο πλαίσιο αναδύονται διάφοροι κίνδυνοι ασφάλειας και σημεία τρωτότητας για τους πολίτες και τα κράτη. Υπό αυτή την έννοια είναι ποικίλες οι προκλήσεις που κάθε χώρα καλείται να αντιμετωπίσει για έγκαιρη ανίχνευση και αντιμετώπιση τέτοιων απειλών, τόσο σε εθνικό αλλά και σε διεθνές επίπεδο.

**ΛΕΞΕΙΣ ΕΥΡΕΤΗΡΙΟΥ:** Κυβερνοβιοασφάλεια, Βιοκίνδυνοι Πλανητικά Καταστρεπτικής Επίπτωσης, εξατομικευμένη θεραπεία, τεχνητή νοημοσύνη

\* Αντεπιστέλλων Συγγραφέας

Δημόσιο Ινστιτούτο Επαγγελματικής Κατάρτισης Μεσολογγίου, Τέρμα Σπύρου Τρικούπη, 302 00, Μεσολόγγι. Τηλ: 26310-50100  
Email: yhatzis@gmail.com

## Εισαγωγή

Η Κυβερνοασφάλεια είναι μια αναδυόμενη υβριδική επιστήμη στο πεδίο της οποίας συζεύγνυται η Κυβερνοασφάλεια και η Βιοασφάλεια (1) αλλά και η φυσική ασφάλεια στον κυβερνοχώρο που σχετίζεται με τα βιολογικά συστήματα (2). Ουσιαστικά η Κυβερνοασφάλεια αποτελεί μέρος ενός συστήματος μέτρων που συλλογικά στοχεύουν στη «Διαφύλαξη της Βιοοικονομίας», ένας στόχος που περιγράφεται από τις Εθνικές Ακαδημίες Επιστημών, Μηχανικής και Ιατρικής των Ηνωμένων Πολιτειών της Αμερικής (3).

Εξάλλου η ανάπτυξη δικτύων συνεργασίας οργανισμών τα τελευταία χρόνια, έχει επιτρέψει τη δημιουργία δικτυακών υποδομών που είναι ειδικά προσαρμοσμένες στις ανάγκες διαφορετικών εφαρμογών δικτύου. Παράλληλα δύναται να υποστηρίξει τη δημιουργία ευνοϊκών περιβαλλόντων για την ανάπτυξη και αξιολόγηση νέων αρχιτεκτονικών δικτύων και πρωτοκόλλων (4). Παρά την ευρεία εφαρμογή των δικτύων, η κοινή χρήση συσκευών δρομολόγησης και καναλιών επικοινωνίας οδηγεί σε μια σειρά ανησυχιών που σχετίζονται με την ασφάλεια. Έτσι λοιπόν είναι απαραίτητο να παρέχεται προστασία στις υποδομές αυτών των δικτύων, προκειμένου να καταστεί δυνατή η χρήση τους σε πραγματικά, μεγάλης κλίμακας περιβάλλοντα (5), όπως είναι οι πληθυσμιακής κλίμακας υγειονομικές και κλινικές πληροφορίες, ιδίως εκτελεστικής μορφής.

## Απειλές και προκλήσεις Κυβερνοβιοασφάλειας

Οι απειλές Κυβερνοβιοασφάλειας γίνονται όλο και πιο σημαντικές στο σύγχρονο κόσμο, καθώς σημειώνεται μεγάλη τεχνολογική πρόοδος η οποία συνεχίζει να επιταχύνεται σε τομείς όπως η τεχνητή νοημοσύνη, η αυτοματοποίηση και η Συνθετική Βιολογία. Χαρακτηριστικό παράδειγμα αποτελούν οι κακόβουλες κυβερνοεπιθέσεις (6). Υπό αυτή την έννοια τα μέτρα Κυβερνοβιοασφάλειας αποκτούν ολοένα και μεγαλύτερη σημασία για την πρόληψη ή την προστασία των εφαρμογών των Βιοεπιστημών (7). Εξάλλου οι νέες προκλήσεις της Κυβερνοβιοασφάλειας σχετίζονται με την κατανόηση του εξελισσόμενου πεδίου των απειλών και τον προσδιορισμό νέων κινδύνων, την ανάπτυξη κατάλληλων μέτρων διασφάλισης των δεδομένων, την επικύρωση και εφαρμογή τους και τους ειδικούς κρίσιμους κινδύνους και συνέπειες, σχετιζόμενες με τις επιστήμες της ζωής (6).

Το ερευνητικό ενδιαφέρον για το συγκεκριμένο πεδίο τα τελευταία χρόνια είναι αυξημένο μιας και ένας σημαντικός αριθμός μελετών πραγματοποιούνται ζητήματα απειλών Κυβερνοβιοασφάλειας με έμφαση στους κινδύνους στον τομέα της Βιοτεχνολογίας, αλλά και συ-

στάσεων όσον αφορά προληπτικά μέτρα και προστασία από σχετικές απειλές των νέων ψηφιακών εργαλείων των επιστημών ζωής και υγείας, ιδία δε στην παροχή υγειονομικών υπηρεσιών μέσω ψηφιακού ορίζοντα, με χαρακτηριστικό αλλά όχι αποκλειστικό παράδειγμα την τηλεϊατρική (2).

Οι προκλήσεις σε σχέση με απειλές Κυβερνοβιοασφάλειας είναι υπαρκτές λόγω και των πιθανών κοινωνικών, οικονομικών, ψυχολογικών επιπτώσεων και άλλων δυσμενών συνεπειών που μπορεί να προκύψουν από τέτοιου είδους συμβάντα (8). Έτσι έμφαση θα πρέπει να δοθεί στις τυπικές αρχιτεκτονικές δικτύων και στους πιθανούς τρόπους εκμετάλλευσης των τρωτών σημείων τους από εισβολείς, μέσω μελέτης δεικτών έκθεσης και ανάπτυξης συστημάτων ανίχνευσης εισβολών (1).

## Κίνδυνοι Κυβερνοβιοασφάλειας

Η Κυβερνοασφάλεια για μια βιολογική εφαρμογή έχει διαφορετικές πτυχές από την κανονική ασφάλεια στον κυβερνοχώρο (6). Η διευρυνόμενη ψηφιοποίηση των βιολογικών επιστημών δίνει υπεραξία στα δεδομένα που προκύπτουν, στις πληροφορίες που αλιεύονται, συγκεντρώνονται ή εξορύσσονται και στη γνώση που αποκτάται. Η αδυναμία προστασίας των δεδομένων θα επηρεάσει την ικανότητα μιας εταιρείας ή μιας χώρας να μετάσχει επωφελώς στην επικείμενη τέταρτη βιομηχανική επανάσταση (7) διότι η αυξημένη εξάρτηση από την αυτοματοποίηση διαδικασιών και τη διακίνηση μεγάλου όγκου πληροφορίας με χρήση διαδικτύου καθιστά τις σχετικές υποδομές ευάλωτους στόχους εξαιρετικά υψηλής επίπτωσης (3).

Η έλλειψη προστασίας αυτών των ανθρωποσχετιζόμενων πόρων και των πόρων υλικού και λογισμικού από εισβολή αυξάνει τον κίνδυνο τυχαίας ή εσκεμμένης βλάβης, για παράδειγμα από την απώλεια του ελέγχου της παραγωγικής αλυσίδας ή των αυτοματισμών Βιοασφάλειας και ποιοτικού ελέγχου των βιολογικών προϊόντων. Ως εκ τούτου, τα ισχυρά μέτρα Κυβερνοβιοασφάλειας είναι ζωτικής σημασίας τόσο για την ασφάλεια των δεδομένων που παράγονται από τον τομέα της Βιοτεχνολογίας όσο και για τη διασφάλιση βασικών υποδομών και των προϊόντων/υπηρεσιών που αυτές προσφέρουν, δηλαδή εκτείνεται στο πλήρες φάσμα παροχών και παραγωγής (1). Η διατήρηση μικροβιακών πληθυσμών βιοτεχνολογικού ενδιαφέροντος σε αποδεκτά επίπεδα, ο έλεγχος της τοξινοπαραγωγής τους σε συνδυασμό με την θαλλική ή βλαστική τους μορφή (αερομεταφερόμενη ή μη) γενικώς ελέγχονται στη βιομηχανία, από εξελιγμένα συστήματα περιβαλλοντικού ελέγχου που λειτουργούν υπό κυβερνοέλεγχο.

Ένα πλαίσιο επιτυχίας της Βιοασφάλειας στον τομέα της γεωργίας και των τροφίμων περιλαμβάνει συμμετοχή των εμπλεκόμενων μερών, συνεργασία στην επίλυση του προβλήματος, απλούστευση του ορισμού της Κυβερνοβιοασφάλειας και ανάπτυξη κοινής γλώσσας μεταξύ των ειδικών. Παράλληλα απαιτείται ευαισθητοποίηση σχετικά με την Κυβερνοβιοασφάλεια εντός και μεταξύ των τομέων του συμπλέγματος γεωργίας και τροφίμων. Η αντιμετώπιση των κινδύνων για το σύστημα γεωργίας και τροφίμων δεν είναι απλώς ένα ζήτημα της επιστήμης της πληροφορικής καθότι εμπλέκονται και άλλες πτυχές ασφάλειας (9), ιδίως η Αγροασφάλεια/Αντιαγροτρομοκρατία.

Ειδικότερα στον 21ο αιώνα, καθώς το πεδίο της βιοάμυνας διασταυρώνεται με τον κυβερνοχώρο οι κυβερνοασφάλεις μπορούν να έχουν σοβαρή οικονομική και κοινωνική επίπτωση. Στον τομέα της Κυβερνοβιοασφάλειας, η σύζευξη της βιοτεχνολογίας και της Κυβερνοασφάλειας προκαλεί ποικίλα σημεία συνδυαστικής τρωτότητας- ένα ασύμμετρο και νεοφανές, σοβαρότατο πρόβλημα για τη βιοάμυνα: Νέες απειλές μπορούν να προκύψουν/σχηματιστούν/παραχθούν και να διαδοθούν με τρόπους που συνδυάζουν τις οδούς των επιθέσεων στον τομέα της Βιοασφάλειας και της Κυβερνοασφάλειας (3). Χαρακτηριστικό παράδειγμα είναι η κακόβουλη υποβάθμιση δικτύου που ελέγχει, αυτοματοποιημένα ή υβριδικά, διαδικασίες συνθετικής βιολογίας που δημιουργούν νέους οργανισμούς. Η κακόβουλη παραποίηση δεδομένων μπορεί να δημιουργήσει υπερπαθόγνο η υπεραλλοιογόνο αντί ενός νέου, αποτελεσματικού παραγωγικού μικροοργανισμού. Ο τελευταίος μπορεί να είναι ένα στέλεχος βιοεπεξεργασίας (πχ ζύμωσης) και, το σημαντικότερο, να αποτελεί το βασικό συστατικό ενός βιοτεχνολογικού θεραπευτικού σκευάσματος ή βιοφαρμακευτικών θεραπευτικών σχημάτων, με συναφές παράδειγμα την παραγωγή προβιοτικών.

Για τον προσδιορισμό των αντιληπτικών κινδύνων κατά τη διεπαφή μεταξύ Κυβερνοασφάλειας και Βιοασφάλειας, η Biosecure διεξήγαγε διαδικτυακά μια πιλοτική μελέτη που εξέτασε τις απόψεις ενός διακριτού διεθνούς συνόλου πρωτοπόρων στον τομέα της Βιοτεχνολογίας και της Κυβερνοασφάλειας το διάστημα Οκτωβρίου – Νοεμβρίου 2017. Τα βασικά ευρήματα της έρευνας έδειξαν ότι οι κίνδυνοι Βιοασφάλειας στον κυβερνοχώρο θεωρούνταν δύσκολο να διακριθούν λόγω των διαφοροποιήσεων στους τύπους απειλών, των στόχων και των πιθανών επιπτώσεων τους σε πτυχές της κοινωνικής ζωής. Επίσης φάνηκε ότι οι κίνδυνοι γίνονται μεγαλύτεροι όσο αυξάνει το επίπεδο πολυπλοκότητάς τους σε συνάρτηση με τα υπαρκτά μη αποτελεσματικά

μέτρα αντιμετώπισής τους (1).

Φαίνεται λοιπόν ότι είναι απαραίτητη η συνεχής έρευνα για τη συνεργασία και διεπαφή των διαφορετικών τομέων δραστηριότητας που ενέχονται σε αυτά τα ζητήματα για την ανάπτυξη μιας κοινής γλώσσας επικοινωνίας – και πιθανώς περιληπτικής ορολογίας - αλλά και για τον καλύτερο προσδιορισμό των απειλών και τη συζήτηση πιθανών τρόπων, μεθόδων και πρακτικών αντιμετώπισης των κινδύνων (10). Η ανάπτυξη κατάλληλων στρατηγικών για την προληπτική μείωση των κινδύνων/τρωτότητας Κυβερνοβιοασφάλειας απαιτεί επίσης μια διεπιστημονική προσέγγιση στα συναφή ζητήματα (5). Υπό αυτή την έννοια μια καλή πρακτική αποτελεί η πλατφόρμα Cybersecurity Atlas της Ευρωπαϊκής Επιτροπής. Η πλατφόρμα αυτή υποστηρίζει τη διαχείριση της γνώσης για τη χαρτογράφηση, την κατηγοριοποίηση και την τόνωση της συνεργασίας μεταξύ ευρωπαίων εμπειρογνομόνων στον τομέα της Κυβερνοασφάλειας για την υποστήριξη της ψηφιακής στρατηγικής της Ευρωπαϊκής Ένωσης (11).

### **Κυβερνοβιοασφάλεια και πανδημία COVID-19**

Η Βιολογία και η Βιοτεχνολογία έχουν αλλάξει δραματικά τα τελευταία χρόνια, αφού η εξάρτησή τους από την ψηφιοποίηση και τον αυτοματισμό αλλά και οι επικαλύψεις τους στον κυβερνοχώρο έχουν δημιουργήσει νέα τρωτά σημεία για ακούσιες συνέπειες και δυνατότητες σκοπούμενης εκμετάλλευσης που σε μεγάλο βαθμό υποτιμώνται (6). Στο πλαίσιο της πανδημίας COVID-19, το ερευνητικό ενδιαφέρον έχει επικεντρωθεί στις επιπτώσεις της πανδημίας στον κυβερνοχώρο (3).

Με βάση την υπαρκτή τεχνογνωσία και την τρέχουσα κατάσταση της Βιοοικονομίας υπάρχουν ποικίλες αιτιολογικές πτυχές ως συνάρτηση των μοναδικών χαρακτηριστικών της που δύνανται να προκαλέσουν ακούσια ή εκούσια βλάβη στην ανθρώπινη υγεία ή στο περιβάλλον με διαστάσεις που σχετίζονται με τη δημόσια υγεία ή την εθνική ασφάλεια. Ειδικότερα μέσω των θεωρητικών προσεγγίσεων της ανθρώπινης ασφάλειας και της Βιοασφάλειας σε έρευνα στις Ηνωμένες Πολιτείες της Αμερικής προκύπτει ότι, μέσα από τη θέαση των απειλών για την ασφάλεια υπό το πρίσμα του ατόμου και του κράτους η πανδημία COVID-19 αποτελεί απειλή για την παγκόσμια ασφάλεια (2).

Κατά τη διάρκεια της πανδημίας COVID-19, υπήρξαν αναφορές για αυξανόμενες απειλές στον κυβερνοχώρο για τις ερευνητικές βάσεις δεδομένων και τις σχετιζόμενες δραστηριότητες (π.χ. παραγωγή θεραπευτικών, εμβολίων, χημικών αντισηπτικών κ.λπ.). Ο έλεγχος των δεδομένων δημιουργεί το πλαίσιο ελέγχου στον κλάδο

της υγειονομικής περιθάλψης, την παγκόσμια οικονομία και την εθνική ασφάλεια, γι' αυτό και δεν θα πρέπει να διακυβεύεται (3). Είναι προφανές το ότι η αλλοίωση των βάσεων εμβολιαστικών δεδομένων, θα μπορούσε να προκαλέσει πραγματικό χάος και πολλές απώλειες υγείας αν ακυρώνονταν τα εμβολιαστικά πιστοποιητικά, ή αν εμφανίζονταν άτομα υψηλού κινδύνου μετάδοσης ως εμβολιασμένα και ως εκ τούτου αποκλείονταν από το εμβολιαστικό πρόγραμμα ενώ διατηρούνταν, λόγω ψηφιακού σφάλματος στην εμβολιαστική κατατομή, ενεργά σε εργασία με μεγάλο αριθμό πιθανών μεταδοτών. Με βάση ότι το πιστοποιητικό εμβολιασμού είναι μια πρώτη και σχετικά ακατέργαστη μορφή εξατομικευμένης θεραπείας/ιατρικής μέριμνας που εκτείνεται στο σύνολο του πληθυσμού ενός κράτους, μπορούν να αντληθούν χρησιμότητα διδάγματα και τις πιθανές επιπτώσεις και τις περιοχές τρωτότητας υπό το πρίσμα της Κυβερνοβιοασφάλειας, τόσο έναντι αυθόρμητων/ατυχηματικών όσο και εναντίον εσκεμμένων προκλήσεων και απειλών.

### **Κυβερνοβιοασφάλεια και βάσεις δεδομένων υγείας/ Ηλεκτρονικός Φάκελος Υγείας και άυλη συνταγογράφηση**

Η Ηλεκτρονική Υγεία αφορά τα εργαλεία και τις υπηρεσίες που βασίζονται σε Τεχνολογίες Πληροφορίας και Επικοινωνίας και μπορούν να βελτιώσουν την πρόληψη, τη διάγνωση, τη θεραπεία, την παρακολούθηση και τη διαχείριση της υγείας (12). Η Ηλεκτρονική Υγεία αποτελεί προτεραιότητα και για την Ευρωπαϊκή Ένωση γεγονός που αποτυπώνεται στο σχέδιο δράσης 2012 – 2020 για την ανάπτυξη της Ηλεκτρονικής Υγείας που διέθεσε στα κράτη – μέλη της. Στο σχέδιο αυτό, εξέχουσα θέση έχει ο σχεδιασμός, η εφαρμογή και υλοποίηση του Ηλεκτρονικού Φακέλου Υγείας με έμφαση στις διασυνοριακές υπηρεσίες όπως η ανάπτυξη και διακίνηση μητρώων υγείας ασθενών και η ηλεκτρονική συνταγογράφηση (13,14).

Οι εφαρμογές Ηλεκτρονικής Υγείας στα συστήματα υγείας διεθνώς όπως η χρήση του Ηλεκτρονικού Φακέλου Υγείας εγείρει πλήθος νομικών, ηθικών και οικονομικών ερωτημάτων καθώς και ζητημάτων ασφάλειας. Ειδικότερα, λόγω του μεγάλου όγκου των πληροφοριών υγείας διευκολύνεται η λήψη της κατάλληλης κλινικής απόφασης κατά περίπτωση, καθώς επίσης και η έγκαιρη αναγνώριση του λάθους των επαγγελματιών υγείας. Παράλληλα, η μη υιοθέτηση τεκμηριωμένων θεραπευτικών πρωτοκόλλων από τους επαγγελματίες υγείας μπορεί να εγείρει επίσης νομικά ζητήματα σε περίπτωση βλάβης του ασθενούς (15), αλλά από την άλλη μεριά εξασφαλίζει την προσαρμογή της θεραπείας στον ασθε-

νή η οποία ακόμη, και για το ορατό μέλλον, δεν μπορεί να βασιστεί σε διαγνωστικούς αλγόριθμους αποκλειστικά. Κι αυτό επειδή η ποικιλομορφία στους ανθρώπινους παθοφαινότυπους είναι εξαιρετικά εκτεταμένη και εν πολλοίς ασυνεχής ως συνάρτηση και συνεπώς μη επακριβώς προβλέψιμη. Δηλαδή τελικά είναι απαραίτητος ο ιατρός ως ανθρώπινος παράγοντας, και όχι μόνο οι αλγόριθμοι και οι κλινικές οδηγίες.

Βέβαια το απόρρητο και η ασφάλεια των δεδομένων και πληροφοριών υγείας αποτελούν κυρίαρχα ζητήματα στο πλαίσιο εφαρμογής υπηρεσιών Ηλεκτρονικής Υγείας στα συστήματα υγείας. Η ανάπτυξη νομικών πλαισίων για την ιδιωτικότητα και την εμπιστευτικότητα των δεδομένων ασθενών και η χρήση προτύπων ενισχύει την ασφαλή ανταλλαγή δεδομένων και την υποστήριξη κλινικών αποφάσεων (16).

Όμως τα νομικά πλαίσια ανεπαρκούν: σε περίπτωση κακόβουλης επέμβασης είναι προφανές ότι, στους ηλεκτρονικούς φακέλους υγείας ενός πληθυσμού όπου εφαρμόζεται η εξατομικευμένη θεραπεία, η μαζική αλλαγή μερικών μόνο, επιλεκτικών σημείων/καταγραφών (πχ η απαλοιφή κλινικών σημείων αντένδειξης έναντι συχνά συνταγογραφούμενου φαρμάκου) θα οδηγήσει, ιδίως όταν χρησιμοποιούνται θεραπευτικά πρωτόκολλα και κατευθυντήριες οδηγίες, σε χορήγηση λανθασμένων θεραπειών με τεράστιο κόστος και πιθανότητα εξαιρετικά μεγάλου εύρους απώλειες ζωής και υγείας. Αν και μικρότερης καταστροφικότητας, μια άλλη αντίστοιχη επέμβαση μπορεί να ευνοήσει ένα συγκεκριμένο φαρμακευτικό σκεύασμα ως προς τη συνταγογράφηση, αυξάνοντας το φαρμακευτικό κόστος/δαπάνη, καταστρέφοντας τον ανταγωνισμό και πιθανόν υποβαθμίζοντας την παράμετρο ασφάλειας και εν γένει ποιότητας.

### **Συμπεράσματα**

Συμπερασματικά οι απειλές της Κυβερνοβιοασφάλειας μπορούν να προκύψουν μέσα στο διεθνές πλαίσιο είτε εκούσια, είτε ακούσια. Κάθε χώρα, ή μάλλον πολιτική οντότητα (με λειτουργικό ορισμό, στην συγκεκριμένη περίπτωση βασισμένο στην ύπαρξη ανεξάρτητου συστήματος καταγραφής φακέλου υγείας, που μπορεί να είναι σε τοπικό επίπεδο, πχ Αμερικανικές Πολιτείες ή στην Ευρώπη σε επίπεδο περιφερειών) καλείται να λειτουργήσει προληπτικά για την έγκαιρη ανίχνευση και αντιμετώπιση τους, τόσο μεμονωμένα σε θεσμικό επίπεδο όσο και σε συνεργασία με άλλες χώρες/πολιτικές οντότητες. Η συνεργασία είναι ιδιαίτερα σημαντική όπου οι έλεγχοι μετακινήσεων ανθρώπων και αγαθών πιθανόν προκαλούν κινδύνους βιοασφάλειας και τα πρωτόκολλα τηλεπικοινωνιών και κυβερνοδραστηρι-

οτήτων (πχ κοινοί πάροχοι διαδικτυακής πρόσβασης) δημιουργούν θέματα Κυβερνοασφάλειας.

Παράλληλα είναι αναγκαία η ενίσχυση των γνώσεων, δεξιοτήτων και ικανοτήτων πολλαπλών ενδιαφερομένων για να εργαστούν στη διασύνδεση μεταξύ της Κυ-

βερνοασφάλειας και Βιοασφάλειας. Τέλος θα πρέπει να επενδυθούν υποστήριξη και πόροι για την περαιτέρω κατανόηση των κινδύνων στον τομέα της Κυβερνοασφάλειας στον τομέα της βιοτεχνολογίας προκειμένου να αναπτυχθούν κατάλληλα μέτρα αντιμετώπισης. ●

## ABSTRACT

# Cybersecurity: risks and challenges in safeguarding Individualized therapy within the current socioeconomic continuum

**Eloannis G. Hatzis<sup>\*</sup>, Angeliki Grivopoulou<sup>2</sup>, Periklis Rompolas<sup>1</sup>**

<sup>1\*</sup> Public Institute of Vocational Training of Messolonghi, Messolonghi, Greece

<sup>2</sup> Second Change School of Messolonghi, Messolonghi, Greece

<sup>3</sup> Department of Nursing, Cyprus University of Technology, Limassol, Cyprus

Cyberbiosecurity is a new emerging field of Global Biosecurity that emphasizes the ever-increasing interdependence of Cyberspace and Biosecurity. The development of this scientific field occurs in parallel with the digitization of economic, social and political activities and as the individualized therapy proposes a quantum leap in health services but with serious security liabilities due to ever increasing impact of Artificial Intelligence amenities in a more extensively and deeply networked setting. At the same time, the cyberbiosecurity lays the foundations for new,

nimbler and streamlined approaches and optimized priorities in international and national biosecurity, especially in situations such as the COVID-19 pandemic and other rapidly evolving and speedily communicated infectious diseases of potentially existential threat level. In such a context, various security risks emerge for individuals and states at large, while in this sense the challenges that each country might tackle in terms of timely detection and response to such threats, both nationally and internationally, vary.

**KEY WORDS:** PCyberbiosecurity, GCBR, Individualized therapy, Artificial intelligence

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- 1. Millett K, Dos Santos E, Millett PD. Cyber-Biosecurity Risk Perceptions in the Biotech Sector. *Front Bioeng Biotechnol.* 2019 Jun 19;7:136.
- 2. Albert C, Baez A, Rutland J. Human security as biosecurity. *Polit Life Sci.* 2021;40(1):83–105.
- 3. Potter L, Ayala O, Palmer X-L. Biocybersecurity: A Converging Threat as an Auxiliary to War. *Int Conf Cyber Warf Secur* [Internet]. 2021;291-298,XIV. Available from: <https://www.proquest.com/conference-papers-proceedings/biocybersecurity-converging-threat-as-auxiliary/docview/2505729708/se-2?accountid=17225>
- 4. George AM. The National Security Implications of Cyberbiosecurity. *Front Bioeng Biotechnol.* 2019;7(MAR):51.
- 5. Bays LR, Oliveira RR, Barcellos MP, Gaspary LP, Mauro Madeira ER. Virtual network security: threats, countermeasures, and challenges. *J Internet Serv Appl.* 2015;6(1):1–19.
- 6. Mueller S. Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosaf Heal* [Internet]. 2021;3(1):11–21. Available from: <https://doi.org/10.1016/j.bsheal.2020.09.007>
- 7. Mantle JL, Rammohan J, Romantseva EF, Welch JT, Kauffman LR, McCarthy J, et al. Cyberbiosecurity for Biopharmaceutical Products. *Front Bioeng Biotechnol.* 2019 May 31;7:116.
- 8. Craig Reed J, Dunaway N. Cyberbiosecurity Implications for the Laboratory of the Future. *Front Bioeng Biotechnol.* 2019;7(AUG):182.
- 9. Murch RS, So WK, Buchholz WG, Raman S, Peccoud J. Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Front Bioeng Biotechnol.* 2018 Apr 5;6(APR):39.
- 10. Richardson LC, Lewis SM, Burnette RN. Building Capacity for Cyberbiosecurity Training. *Front Bioeng Biotechnol.* 2019 Jun 26;7:112.
- 11. European Commission. European Cybersecurity Atlas | Cybersecurity Atlas [Internet]. 2022 [cited 2022 Jun 14]. Available from: <https://cybersecurity-atlas.ec.europa.eu/>
- 12. Επιτροπή των Ευρωπαϊκών Κοινοτήτων. ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ για την τηλεϊατρική, προς όφελος των ασθενών, των συστημάτων υγείας και της κοινωνίας [Internet]. COM(2008)689 τελικό. 2008 [cited 2021 Nov 10]. p. 1–16. Available from: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:EL:PDF>
- 13. European Commission. EHealth priorities and strategies in European countries : eHealth ERA report : March 2007 : towards the establishment of a European eHealth research area. Publications Office; 2006. 96 p.
- 14. European Union. e-Health Network Guidelines [Internet]. EU Member States and the European Commission. Bucharest; 2019. Available from: [https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev\\_20190611\\_co922\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co922_en.pdf)
- 15. Tsai CH, Eghdam A, Davoody N, Wright G, Flowerday S, Koch S. Effects of electronic health record implementation and barriers to adoption and use: A scoping review and qualitative analysis of the content. *Life.* 2020 Dec 1;10(12):1–27.
- 16. Chao WC, Hu H, Ung COL, Cai Y. Benefits and challenges of electronic health record system on stakeholders: A qualitative study of outpatient physicians. *J Med Syst.* 2013;37(4).