1. QUIS CUSTODIET IPSOS CUSTODES ?

Μέσο: . . . . . .ΤΑ ΝΕΑ
Ημ. Έκδοσης: . . .06/09/2022 Ημ. Αποδελτίωσης: . . .06/09/2022
Σελίδα: 12

Innews ΑΕ - Αποδελτίωση Τύπου - http://www.innews.gr

Quis custodiet ipsos custodes?

ΓΝΩΜΗ

ΤΟΥ ΜΙΧΑΛΗ ΚΡΗΤΙΚΟΥ

Οι πρόσφατες διεθνείς αποκαλύψεις για τη χρήση κατασκοπευτικού λογισμικού μας θυμίζουν ότι βιώνουμε ίσως την πιο βαθιά μεταμόρφωση του πληροφοριακού μας περιβάλλοντος από την εφεύρεση της τυπογραφίας. Και το πρόβλημα όπως σε όλες τις μεγάλες τεχνολογικές ανακατατάξεις είναι ότι είναι αδύνατο να προβλέψεις τις συνέπειες, να αντιληφθείς το πού οδηγούν και κυρίως να αποδεχθείς ότι κάποιες από τις επιμέρους χρήσεις αυτής της τεχνολογίας ενδέχεται να διαφύγουν κάθε έλεγχο. Αυτό ισχύει και στην περίπτωση της λογισμικών παρακολούθησης καθώς επιτρέπουν στους παρόχους τέτοιων υπηρεσιών και στα ίδια τα κράτη τη δυνατότητα παρακολούθησης με μια λεγόμενη «επίθεση μηδενικού κλικ» («sandboxing») να παρακολουθούν τις κινήσεις σχεδόν οποιουδήποτε όσο μακριά και εάν βρίσκεται, μετατρέποντας τα ίδια τα κινητά τηλέφωνα σε τέλειους κοριούς.

Αυτό το μοντέλο που η Zuboff αποκάλεσε «καπιταλισμό επιτήρησης» μεταλλάσσεται διαρκώς τεχνολογικά (εκμεταλλευόμενη ασυνήθιστα τρωτά σημεία/zero-days) και πλέον εργαλειοποιείται για νεφελώδεις σκοπούς απειλώντας να υπομονεύσει τις ίδιες τις σχέσεις κράτους - πολίτη. Ενώ οι περισσότεροι από εμάς πιστεύουμε ότι έχουμε να κάνουμε απλώς με δυσερμήνευτα αλγοριθμικά μοντέλα, στην πραγματικότητα αυτό που αντιμετωπίζουμε στην περίπτωση των λογισμικών spyware είναι οι απαρχές μιας δυστοπικής γιγάντωσης ενός νέου τεχνολογικού μοντέλου που αναπτύσσεται με γεωμετρικό τρόπο μακριά από τον δημόσιο έλεγχο, εκμεταλλευόμενο το ασαφές νομοθετικό πλαίσιο και την ακόρεστη επιθυμία πολλών κρατών να εγκαταστήσουν «έξυπνα» συστήματα παρακολούθησης. Οι τεχνολογίες που χρησιμοποιούνται έχουν τεράστια επεξεργαστική ισχύ και θεωρούνται διπλής χρήσης, που πρακτικά σημαίνει ότι μπορούν να χρησιμοποιηθούν για καλό και για κακό σκοπό, γεγονός που δυσκολεύει την πλήρη απαγόρευσή τους.

Η μεγαλύτερη πρόκληση όμως παραμένει η απόλυτη έλλειψη διαφάνειας σχετικά με τον τρόπο με τον οποίο αναπτύσσονται, αγοράζονται, πωλούνται και χρησιμοποιούνται από το κράτος αυτά τα εργαλεία ψηφιακής επιτήρησης. Καθώς η κρατική προμήθεια αυτών των συστημάτων συνοδεύεται από ρήτρες εμπιστευτικότητας και η χρήση τους καλύπτεται από την επίκληση λόγων εθνικής ασφαλείας, ο αποτελεσματικός έλεγχος αυτών των παρεμβατικών τεχνολογιών καθίσταται ακόμα πιο δύσκολος. Κατά τα φαινόμενα, οι διάφορες μορφές ελέγχου αυτών των τεχνολογιών που έχουν αναπτυχθεί (ο πρόσφατος ευρωπαϊκός Κανονισμός για την εξαγωγή τεχνολογιών διπλής χρήσης, τα διάφορα μοντέλα εισαγγελικής εποπτείας που έχουν προταθεί και δοκιμαστεί και οι κατά καιρούς προσπάθειες κοινοβουλευτικού ελέγχου) δεν φαίνεται να εξασφαλίζουν διαφάνεια, λογοδοσία και να εμπεδώνουν μια αίσθηση υπεύθυνης χρήσης της τεχνολογίας.

Κυρίως δεν είναι ξεκάθαρο εάν οι προαναφερόμενοι ελεγκτικοί μηχανισμοί διαθέτουν την τεχνική ικανότητα ουσιαστικού ελέγχου των συγκεκριμένων τεχνολογιών παρακολούθησης, δεδομένου ότι η επεξεργασία των πληροφοριών γίνεται πλέον με τη βοήθεια λογισμικών που κρύβουν επιμελώς τις κακόβουλες δυνατότητές τους και βασίζονται σε εξελιγμένες τεχνικές μηχανικής μάθησης. Πού καταλήγουν όλες οι πληροφορίες που συγκεντρώνονται από αυτά τα τεχνολογικά συστήματα; Στα ψηφιακά αρχεία κρατικών υπηρεσιών ή/και στον ίδιο τον πάροχο/δημιουργό των ψηφιακών υπηρεσιών και στις δικές του βάσεις δεδομένων; Εχουν πρόσβαση τα κράτη εκείνα όπου εδρεύουν οι εν λόγω εταιρείες σε στοιχεία που συγκεντρώνονται μέσω τέτοιων εργαλείων παρακολούθησης; Γιατί τα κράτη-μέλη της ΕΕ δεν ακολουθούν τα βήματα των ΗΠΑ, οι οποίες τον περασμένο Νοέμβριο έθεσαν συγκεκριμένες εταιρείες δημιουργίας spyware στη μαύρη λίστα των εταιρειών που απαγορεύεται να δραστηριοποιούνται στην Αμερική ή ακόμα και το παράδειγμα της εταιρείας Meta του Facebook και της Apple που έχουν στραφεί δικαστικά εναντίον αυτών των εταιρειών; Και γιατί δεν απαιτούν μεγαλύτερη διαφάνεια από προμηθευτές λογισμικού τέτοιου είδους σχετικά με το ποιος και πώς χρησιμοποιεί το λογισμικό τους; Με άλλα λόγια ποιος ελέγχει τους ελέγχοντες;

Για να δοθούν πειστικές και κυρίως βιώσιμες απαντήσεις σε αυτά τα ερωτήματα, απαιτείται η δημιουργία ενωσιακών ανεξάρτητων δομών που θα έχουν όχι μόνο βαθιά γνώση των τρομακτικών δυνατοτήτων των τεχνολογιών αυτών, αλλά και θα διαθέτουν ισχυρές εξουσίες επαλήθευσης του τρόπου απόκτησης και χρήσης μιας τέτοιας παρεμβατικής τεχνολογίας προτού τα συστήματα αυτά αυτονομηθούν περαιτέρω – τεχνολογικά και πολιτικά – και κρίσιμες πληροφορίες περιέλθουν σε λάθος χέρια ή γίνουν μέσο επίτευξης ανομολόγητων σκοπών.

**Λατινικό ρητό που σημαίνει «Ποιος θα φρουρήσει τους φρουρούς;»*

Ο δρ Μιχάλης Κρητικός είναι ερευνητής του ΕΛΙΑΜΕΠ και ερευνητικός εταίρος σε θέματα Τεχνητής Νοημοσύνης και Ψηφιακής Μετάβασης στη Σχολή Διακυβέρνησης του Ελεύθερου Πανεπιστημίου των Βρυξελλών.