



Εξεταστική Επιτροπή για τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης

2022/2077(INI)

28.11.2022

ΣΧΕΔΙΟ ΕΚΘΕΣΗΣ

σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης
(2022/2077(INI))

Εξεταστική Επιτροπή για τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης

Εισηγήτρια: Sophie in 't Veld

ΠΕΡΙΕΧΟΜΕΝΑ

	Σελίδα
ΣΧΕΔΙΟ ΑΠΟΤΕΛΕΣΜΑΤΩΝ	3
ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ.....	57

ΣΧΕΔΙΟ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (2022/2077(INI))¹

Το Ευρωπαϊκό Κοινοβούλιο,

- έχοντας υπόψη το άρθρο 226 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ),
- έχοντας υπόψη την απόφασή του της 10ης Μαρτίου 2022 σχετικά με τη σύσταση εξεταστικής επιτροπής για τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης, και τον καθορισμό του αντικειμένου της έρευνας, καθώς και των αρμοδιοτήτων, της αριθμητικής σύνθεσης και της διάρκειας της θητείας της επιτροπής,
- έχοντας υπόψη την έκθεση της εξεταστικής επιτροπής για τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (A9-0000/2022),

I. Η χρήση κατασκοπευτικού λογισμικού στην ΕΕ

I.A Πολωνία

1. Η χρήση εμπορικού κατασκοπευτικού λογισμικού στην Πολωνία έγινε για πρώτη φορά ευρέως γνωστή στο κοινό τον Δεκέμβριο του 2021. Οι κίνδυνοι που εγκυμονεί μπορούν να γίνουν πλήρως κατανοητοί μόνο εντός του πλήρους πλαισίου στο οποίο εντάσσεται. Το εμπορικό κατασκοπευτικό λογισμικό δεν είναι απλώς ένα τεχνικό μέσο που χρησιμοποιείται μεμονωμένα και σε τυχαίες καταστάσεις. Αποτελεί αναπόσπαστο και ζωτικό μέρος ενός συστήματος ειδικά σχεδιασμένου για την ανενόχλητη παρακολούθηση και τον έλεγχο των πολιτών. Τα νομικά, θεσμικά και πολιτικά δομικά στοιχεία του συστήματος αυτού συγκροτήθηκαν σκόπιμα και μεθοδικά για να δημιουργήσουν ένα συνεκτικό και ιδιαίτερα αποτελεσματικό πλαίσιο. Η πλήρης εικόνα αυτού του προσεκτικά σχεδιασμένου συστήματος καθίσταται ορατή μόνο με τη σύνδεση των επιμέρους στοιχείων.
2. Το πεδίο της νόμιμης παρακολούθησης στην Πολωνία έχει επεκταθεί σε σχεδόν απεριόριστο βαθμό. Τα δικαιώματα των θυμάτων έχουν ελαχιστοποιηθεί και τα ένδικα μέσα προσφυγής έχουν καταστεί άνευ νοήματος στην πράξη. Ο αποτελεσματικός εκ των προτέρων και κατασταλτικός έλεγχος, καθώς και η ανεξάρτητη εποπτεία, έχουν σχεδόν καταργηθεί. Τα μέλη της πολωνικής κυβέρνησης και οι πιστοί του κόμματος ελέγχουν, άμεσα ή έμμεσα, τις κύριες θέσεις εντός του συστήματος. Οι πληροφορίες που συλλέγονται με κατασκοπευτικό λογισμικό χρησιμοποιούνται σε εκστρατείες

¹ The draft report is based on the document where the rapporteur set her findings. Any person named in the course of the inquiry to whom this might prove prejudicial shall have the right to be heard by the Committee. The Secretariat may be reached at pega-secretariat@europarl.europa.eu.

δυσφήμισης κατά επικριτών της κυβέρνησης καθώς και κατά της αντιπολίτευσης, μέσω των κρατικών μέσων ενημέρωσης που τελούν υπό τον έλεγχο της κυβέρνησης. Όλες οι διασφαλίσεις έχουν εξαλειφθεί, τα κυβερνητικά κόμματα έχουν πλήρη έλεγχο και τα θύματα δεν έχουν πού να στραφούν.

Αγορά του Pegasus

3. Τον Νοέμβριο του 2016, η πρώην πρωθυπουργός και εν ενεργεία βουλευτής του ΕΚ Beata Szydło και ο πρώην υπουργός Εξωτερικών Witold Waszczykowski παρέστησαν σε δείπνο στο σπίτι του τότε πρωθυπουργού του Ισραήλ Benjamin Netanyahu². Το επόμενο έτος τον Ιούλιο, η Szydło και ο Netanyahu συναντήθηκαν με τους αρχηγούς κυβερνήσεων των χωρών της ομάδας Βίσεγκραντ. Υποτίθεται ότι συζήτησαν για την «ενίσχυση της συνεργασίας στον τομέα της καινοτομίας και των τεχνολογιών αιχμής» και για «θέματα που σχετίζονται με την ασφάλεια των πολιτών, υπό ευρεία έννοια»³. Λίγο μετά τη συνάντηση αυτή το 2017, η πολωνική κυβέρνηση απέκτησε το Pegasus μετά από συνάντηση μεταξύ του πρωθυπουργού Mateusz Morawiecki, του πρωθυπουργού της Ουγγαρίας Viktor Orbán και του Netanyahu⁴. Παρά τις αρχικές διαψεύσεις, τον Ιανουάριο του 2022, ο ηγέτης του PiS Jarosław Kaczyński επιβεβαίωσε την αγορά κατασκοπευτικού λογισμικού από την πολωνική κυβέρνηση⁵⁶⁷.

Νομικό πλαίσιο

4. Το 2014 το Συνταγματικό Δικαστήριο προέβη σε επανεξέταση του νόμου περί αστυνομίας και άλλων υφιστάμενων νόμων που διέπουν την παρακολούθηση πολιτών, οι οποίοι κρίθηκαν ασύμβατοι με το πολωνικό Σύνταγμα⁸. Το δικαστήριο κατέληξε με την έκδοση απόφασης που περιείχε συγκεκριμένες συστάσεις και προθεσμία 18 μηνών εντός της οποίας έπρεπε να εφαρμοστούν οι νομοθετικές αλλαγές⁹. Μετά τις εκλογές του 2015, η νέα κυβέρνηση εισήγαγε νομοθετικές αλλαγές. Ωστόσο, ο συνακόλουθος νόμος της 15ης Ιανουαρίου 2016 για την τροποποίηση του νόμου περί αστυνομίας του 1990 και ορισμένων άλλων νόμων (εφεξής ο νόμος του 2016 περί αστυνομίας) δεν διόρθωσε κανένα από τα κενά του νόμου, όπως απαιτούσε το Συνταγματικό Δικαστήριο¹⁰. Αντ' αυτού, ο νόμος του 2016 περί αστυνομίας αποδυνάμωσε τις ήδη ανεπαρκείς διατάξεις που δεν προστατεύουν τα δικαιώματα των πολιτών ούτε δημιουργούν κατάλληλη εποπτεία και ενίσχυσε τη διαρκώς αυξανόμενη απόσταση μεταξύ της πολωνικής νομοθετικής εξουσίας και του κράτους δικαίου.

² Gazeta, <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html>, 29 January 2022.

³ Gazeta, <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html>, 29 January 2022.

⁴ Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.', 7 January, 2022.

⁵ Financieele Dagblad, 'Liberalen Europarlement eisen onderzoek naar spionagesoftware', 12 January 2022.

⁶ Politico, <https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/>, 7 January 2022.

⁷ Financial Times, <https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e>, 8 February 2022.

⁸ Venice Commission Report June 2016, [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2016\)012-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e).

⁹ <https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani>

¹⁰ Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

Αντιτρομοκρατικός νόμος του 2016

5. Εκτός από τον νόμο περί αστυνομίας του 2016, η πολωνική κυβέρνηση θέσπισε επίσης νόμο που διέπει την παρακολούθηση αλλοδαπών πολιτών το 2016, τον οποίο χαρακτηρίζει ως τον «αντιτρομοκρατικό νόμο». Τα άρθρα του νόμου ορίζουν ότι οι μη Πολωνοί πολίτες μπορούν να παρακολουθούνται χωρίς τη συγκατάθεσή τους για περίοδο τριών μηνών εάν η ταυτότητά τους είναι «αμφίβολη», μεταξύ άλλων μέσω υποκλοπής τηλεφώνων, λήψης δακτυλικών αποτυπωμάτων, βιομετρικών φωτογραφιών και DNA, καθώς και την υποχρέωση να καταχωρίζονται οι προπληρωμένες τηλεφωνικές κάρτες¹¹. Ο γενικός εισαγγελέας είναι αρμόδιος να διατάξει την καταστροφή μη συναφών υλικών και, επί του παρόντος, ασκεί το αξίωμα αυτό ο Zbigniew Ziobro, υπουργός Δικαιοσύνης του PiS¹²¹³.

Κώδικας Ποινικής Δικονομίας

6. Τον Ιούλιο του 2015, θεσπίστηκε στην Πολωνία ο νόμος για την τροποποίηση του κώδικα ποινικής δικονομίας, ώστε να διασφαλιστεί ότι τα αποδεικτικά στοιχεία που αποκτήθηκαν παράνομα δεν θα μπορούν να συμπεριληφθούν σε ποινικές διαδικασίες. Ωστόσο, ο νόμος αναδιατυπώθηκε αργότερα τον Μάρτιο του 2016 προκειμένου να συμπεριληφθεί το άρθρο 168α¹⁴. Η προσθήκη αυτή διασφαλίζει πλέον ότι τα αποδεικτικά στοιχεία που συλλέγονται κατά παράβαση του νόμου ή οι «καρποί του δηλητηριώδους δένδρου», όπως οι πληροφορίες που συλλέγονται μέσω της χρήσης του Pegasus, μπορούν να υποβληθούν στο δικαστήριο¹⁵.

Νόμος περί τηλεπικοινωνιών της 16ης Ιουλίου 2004

7. Ο νόμος που διέπει τις τηλεπικοινωνίες στην Πολωνία περιλαμβάνει διατάξεις για την πρόσβαση της αστυνομίας σε τηλεπικοινωνιακά δεδομένα δωρεάν και, σε ορισμένες περιπτώσεις, χωρίς τη συμμετοχή των υπαλλήλων¹⁶. Αυτό μπορεί να γίνει στο πλαίσιο της αόριστης αιτιολόγησης της «ανακάλυψης εγκλημάτων». Ο εισαγγελέας αποφασίζει στη συνέχεια πώς θα κινηθεί όσον αφορά τη λήψη των εν λόγω δεδομένων, και μάλιστα διαθέτει σημαντική εξουσία στο πλαίσιο του νόμου, παρόλο που η ανάθεση της θέσης αποτελεί πολιτική απόφαση, δεδομένου ότι ο Ziobro έχει αναλάβει αυτόν τον ρόλο¹⁷¹⁸.

Εκ των προτέρων έλεγχος

¹¹ Act of 10 June 2016 on Anti-terrorism Operations, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf>.

¹² Act of 10 June 2016 on Anti-terrorism Operations, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf>.

¹³ EDRi, <https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/>, 29 June 2016.

¹⁴ Act of 11 March 2016 amending the Act - Code of Criminal Procedure and certain other acts <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf>

¹⁵ <https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings>

¹⁶ Telecommunications Act of 16 July 2004 <https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004>.

¹⁷ Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

¹⁸ Helsinki Foundation for Human Rights, https://www.hfhr.pl/wp-content/uploads/2016/05/HFHR_hand_out_Venice_Commission_Act_on_Police_FNL.pdf, 28 April 2016 at pg. 18 [hereinafter HFHR Report].

8. Μολονότι για την παρακολούθηση απαιτείται κατ' αρχήν δικαστική άδεια στην Πολωνία, στην πράξη η διαδικασία χορήγησης άδειας δεν χρησιμεύει πλέον ως εγγύηση κατά των καταχρήσεων, αλλά ως μέσο για να προσδίδεται μια επίφαση νομιμότητας στην παρακολούθηση για πολιτικούς σκοπούς. Δεν έχει καταστεί σαφές μέχρι σήμερα αν κάποιο από τα θύματα του Pegasus κατασκοπεύονταν με δικαστική άδεια. Οι αιτήσεις για τη χορήγηση δικαστικής άδειας σε επιχείρηση παρακολούθησης υποβάλλονται από τις ειδικές υπηρεσίες¹⁹. Για την αξιολόγηση της αίτησης, οι δικαστές έχουν στη διάθεσή τους μόνο τις πληροφορίες που παρέχονται από τον αιτούντα (δηλαδή τις ειδικές υπηρεσίες), και ο εισαγγελέας είναι εκείνος που αποφασίζει ποιο υλικό είναι σχετικό προς υποβολή²⁰. Συχνά, οι πληροφορίες είναι απλώς συνοπτικές και ενίοτε δεν περιλαμβάνουν ούτε τις βασικότερες λεπτομέρειες σχετικά με τον στόχο (όνομα, επάγγελμα, αξιόποινη πράξη για την οποία είναι ύποπτος/ύποπτη) και τις μεθόδους παρακολούθησης που πρόκειται να χρησιμοποιηθούν.

Κατασταλτικός έλεγχος

9. Η κοινοβουλευτική εποπτεία είναι ουσιαστικά ανύπαρκτη στην Πολωνία. Όταν το PiS ανέλαβε την εξουσία το 2015, το παραδοσιακό σύστημα που προέβλεπε ότι το κόμμα της αντιπολίτευσης αναλαμβάνει την προεδρία της επιτροπής κοινοβουλευτικής εποπτείας για τις ειδικές υπηρεσίες (KSS) απορρίφθηκε, και τα κυβερνώντα κόμματα τοποθέτησαν τα μέλη του PiS Waldemar Andzel ως πρόεδρο και τον κ. Jarosław Krajewski ως αντιπρόεδρο²¹. Τα κυβερνητικά κόμματα έχουν την απόλυτη πλειοψηφία στην επιτροπή²². Επιπλέον, η κυβερνητική πλειοψηφία στην Πολωνική Δίαιτα απέρριψε τις εκκλήσεις για κοινοβουλευτική έρευνα σχετικά με τους ισχυρισμούς για παράνομη χρήση κατασκοπευτικού λογισμικού²³²⁴²⁵²⁶²⁷. Από την άλλη πλευρά, η Γερουσία, όπου τα κυβερνητικά κόμματα δεν έχουν την πλειοψηφία, συγκρότησε εξεταστική επιτροπή, αλλά η Γερουσία δεν διαθέτει τις εξουσίες έρευνας της Πολωνικής Δίαιτας²⁸.

Υποβολή εκθέσεων

10. Σύμφωνα με τον νόμο περί αστυνομίας του 2016, η αστυνομία υποχρεούται απλώς να υποβάλλει εξαμηνιαίες εκθέσεις στα δικαστήρια σχετικά με τον αριθμό των συλλογών τηλεπικοινωνιακών, ταχυδρομικών ή διαδικτυακών δεδομένων μαζί με το νομικό σκεπτικό τους (σχετικά με την προστασία της ανθρώπινης ζωής ή υγείας ή την

¹⁹ Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

²⁰ Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

²¹ <https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS>

²² <https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS>

²³ AP, <https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422> 17 January 2022.

²⁴ European Commission Rule of Law 2022 Report, Poland Specific Chapter, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 27.

²⁵ AP, <https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab>, 23 December 2021.

²⁶ The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 January 2022.

²⁷ Politico, <https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/>, 18 January 2022.

²⁸ European Commission Rule of Law 2022 Report, Poland Specific Chapter, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 27, footnote 220.

υποστήριξη της έρευνας και διάσωσης)²⁹. Οι εκθέσεις αυτές μπορούν να υποβάλλονται μόνο εκ των υστέρων και δεν δημοσιοποιούνται. Σε περίπτωση που ανακύψει ζήτημα με την υποβληθείσα έκθεση, το δικαστήριο θα υποβάλει σε απάντηση τα πορίσματά του εντός 30 ημερών, αλλά δεν μπορεί να διατάξει την καταστροφή δεδομένων ακόμη και αν διαπιστώσει ασυμβατότητες με τον νόμο. Είναι ζωτικής σημασίας το γεγονός ότι οι εν λόγω εποπτικές ενέργειες είναι μόνο προαιρετικές και όχι υποχρεωτικές³⁰.

Μέσα προσφυγής

11. Μέχρι στιγμής, ο Πολωνός εισαγγελέας δεν έχει κινήσει έρευνα, παρά τα πολυάριθμα αποδεικτικά στοιχεία ότι έχουν διαπραχθεί σοβαρά εγκλήματα. Φαίνεται ότι τα δικαστήρια έχουν επιληφθεί μόνο της υπόθεσης της εισαγγελέως Ewa Wrzosek. Η Wrzosek κατέθεσε αρχικά την υπόθεσή της στην Εισαγγελία, ωστόσο, μετά την επίσημη άρνησή της να επιληφθεί της υπόθεσης, μπόρεσε να προσφύγει στα δικαστήρια. Στα τέλη Σεπτεμβρίου 2022, το περιφερειακό δικαστήριο της Βαρσοβίας (Mokotów) διέταξε τον εισαγγελέα να κινήσει έρευνα³¹.

Δημόσιος έλεγχος

12. Τα ανεξάρτητα μέσα ενημέρωσης αποτελούν ένα ακόμη στοιχείο δημοκρατικών ελέγχων και ισορροπιών, που ασκούν δημόσιο έλεγχο. Ωστόσο, στην περίπτωση της χρήσης κατασκοπευτικού λογισμικού, ο δημόσιος ραδιοτηλεοπτικός φορέας της Πολωνίας, ο οποίος ελέγχεται σε μεγάλο βαθμό από τα κυβερνητικά κόμματα, στην πραγματικότητα κατέστη συνένοχος στο παράνομο σκάνδαλο παρακολούθησης, δημοσιοποιώντας υλικό προερχόμενο από τα έξυπνα τηλέφωνα πολλών από τους στόχους, συμπεριλαμβανομένου του γερουσιαστή Brejza. Η δημοσιοποίηση των πληροφοριών που λαμβάνονται στο πλαίσιο επιχείρησης παρακολούθησης των ειδικών υπηρεσιών συνιστά ήδη από μόνη της εγκληματική πράξη. Ωστόσο, δεν έχει ληφθεί κανένα μέτρο από την αστυνομία ή την εισαγγελική αρχή.

Πολιτικός έλεγχος

13. Πολλές καίριες θέσεις σε ολόκληρη την αλυσίδα κατέχονται από μέλη ή πιστούς υποστηρικτές των κυβερνητικών κομμάτων. Ο υπουργός Εσωτερικών και συντονιστής των Ειδικών Υπηρεσιών Kamiński καταδικάστηκε το 2015 για κατάχρηση εξουσίας και του επιβλήθηκε ποινή κάθειρξης τριών ετών³². Ωστόσο, αμέσως μετά τις βουλευτικές εκλογές του 2015, ο πρόεδρος Duda του χορήγησε χάρη με εξαιρετικά παράτυπο τρόπο, ο οποίος καταδικάστηκε, μεταξύ άλλων, από το Ανώτατο Δικαστήριο της Πολωνίας, το ΔΕΕ, την Επιτροπή της Βενετίας και το Υπουργείο Εξωτερικών των ΗΠΑ. Τούτο εγείρει ανησυχίες σχετικά με την ανεξαρτησία και την ουδετερότητα του. Ο κ.

²⁹ Act of 15 January 2016 Amending the Police Act and Certain Other Acts at Art. 20c, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf>.

³⁰ HFHR Report at pg.4.

³¹ Wyborcza, <https://wyborcza.pl/7,75398,28963729,pegasus-w-telefonie-ewy-wrzosek-prokuratura-odmowila-sad-kaze.html>, 28 September 2022.

³² Reuters, <https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117>, 17 November 2015.

Kaminski αρνήθηκε να συναντηθεί ή να συνεργαστεί με την ειδική εξεταστική επιτροπή Pegasus του Ευρωπαϊκού Κοινοβουλίου³³.

Οι στόχοι

14. Μετά τις έρευνες από μέλη του Associated Press και του Citizen Lab στο Πανεπιστήμιο του Τορόντο, αποκαλύφθηκε ότι τουλάχιστον τρία άτομα είχαν στοχοποιηθεί στην Πολωνία το 2019³⁴. Οι στόχοι αυτοί ήταν ο γερουσιαστής της αντιπολίτευσης Krzysztof Brejza, ο δικηγόρος Roman Giertych, και η εισαγγελέας Ewa Wrzosek, οι επικοινωνίες των οποίων παρακολούθηθηκαν με κατασκοπευτικό λογισμικό Pegasus το οποίο απέκτησε η κυβέρνηση το 2017³⁵. Ενώ η κυβέρνηση επιβεβαίωσε την αγορά του λογισμικού από τον όμιλο NSO, δεν έχει παραδεχθεί επίσημα ότι στοχοποιήθηκαν συγκεκριμένα πρόσωπα. Κανένας από τους στόχους που αναφέρονται κατωτέρω, δεν έχει κατηγορηθεί επισήμως για οποιοδήποτε έγκλημα, ούτε έχει κληθεί για ανάκριση, ούτε έχει υποβληθεί αίτημα άρσης της ασυλίας των στόχων που κατέχουν πολιτικό αξίωμα.

Γερουσιαστής Krzysztof Brejza

15. Ο γερουσιαστής Krzysztof Brejza ηγείτο της εκστρατείας της Πλατφόρμας Πολιτών του κόμματος της αντιπολίτευσης όταν έπεσε θύμα χάκινγκ με κατασκοπευτικό λογισμικό³⁶. Πραγματοποιήθηκαν 33 επιθέσεις στο τηλέφωνο του Brejza κατά τη διάρκεια της εκστρατείας της Πλατφόρμας Πολιτών το 2019, με τις επιθέσεις να ξεκινούν στις 26 Απριλίου 2019 και να συνεχίζονται έως τις 23 Οκτωβρίου 2019, λίγες ημέρες μετά το τέλος του εκλογικού κύκλου³⁷.

Roman Giertych

16. Ο Roman Giertych στοχοποιήθηκε με κατασκοπευτικό λογισμικό Pegasus κατά τις τελευταίες εβδομάδες των βουλευτικών εκλογών του 2019. Από τον Σεπτέμβριο έως τον Δεκέμβριο του 2019, ο Giertych παραβιάστηκε (χακαρίστηκε) 18 φορές, οι περισσότερες από τις οποίες πραγματοποιήθηκαν αμέσως πριν από την ημερομηνία των εκλογών της 13ης Οκτωβρίου 2019. Τότε, υπηρέτούσε ως δικηγόρος του ηγέτη της αντιπολίτευσης Donald Tusk. Κατά την περίοδο αυτή, ο Giertych εκπροσωπούσε επίσης τον Radek Sikorski, πρώην υπουργό Εξωτερικών και νυν βουλευτή του ΕΚ με το Ευρωπαϊκό Λαϊκό Κόμμα (ΕΛΚ). Ο Sikorski επιχειρούσε να πραγματοποιήσει έρευνα για τη συμμετοχή του Kaczynski και των συμμάχων του σε παράνομες παρακολουθήσεις τηλεφωνικών συνδιαλέξεων, πράγμα που είχε ως αποτέλεσμα την καταγραφή και τη δημοσίευση των συνομιλιών του υπουργού³⁸.

³³ EU Observer, <https://euobserver.com/rule-of-law/156063>, 15 September 2022.

³⁴ The Guardian, <https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware>, 17 February 2022.

³⁵ Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.' 7 January, 2022.

³⁶ Haaretz, <https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000>, 5 April 2022.

³⁷ The Guardian, 'More Polish opposition figures found to have been targeted by Pegasus spyware', 17 February, 2022.

³⁸ AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e> 21 December 2021.

Ewa Wrzosek

17. Η εισαγγελέας Ewa Wrzosek υπήρξε θύμα χάκινγκ με κατασκοπευτικό λογισμικό Pegasus 6 φορές μεταξύ της 24ης Ιουνίου και της 19ης Αυγούστου 2020³⁹. Η Wrzosek είναι μέλος της Lex Super Omnia, ομάδας αποτελούμενης από εισαγγελείς που εργάζονται για την ανεξαρτησία της εισαγγελικής αρχής. Διερευνούσε την ασφάλεια της διεξαγωγής προεδρικών εκλογών εν μέσω της παγκόσμιας πανδημίας COVID-19, όταν της αφαίρεσαν την υπόθεση, η οποία στη συνέχεια εγκαταλείφθηκε, και τη μετέθεσαν στην πόλη Srem με προειδοποίηση 48 ωρών. Εμπίπτει στην αυξανόμενη εξουσία του γενικού εισαγγελέα του PiS, Zbigniew Ziobro, να επιλέξει να μην ασκήσει δίωξη σε ορισμένες υποθέσεις ή να απομακρύνει τους ιεραρχικά κατώτερους εισαγγελείς από τις υποθέσεις⁴⁰. Μετά την επιστροφή της Wrzosek στη Βαρσοβία, στοχοποιήθηκε με κατασκοπευτικό λογισμικό. Οι πολωνικές αρχές για ακόμη μια φορά ούτε επιβεβαίωσαν ούτε αρνήθηκαν την ευθύνη τους^{41,42}.

Άλλοι πιθανοί στόχοι

Ανώτατο Ελεγκτικό Συνέδριο

18. Η λειτουργία του Najwyższa Izba Kontrol (NIK) ή Ανώτατου Ελεγκτικού Συνεδρίου, ως ενός από τα παλαιότερα θεσμικά όργανα στην Πολωνία, είναι η διαφύλαξη των δημόσιων δαπανών και της διαχείρισης των δημόσιων υπηρεσιών. Η Marian Banās είναι σήμερα επικεφαλής του οργάνου⁴³ και αντιστέκεται στη διάβρωση του κράτους δικαίου, αναλαμβάνοντας την ηγεσία της προσπάθειας να λογοδοτήσει η κυβέρνηση του PiS σε αυτές τις περιπτώσεις χάκινγκ, παρά το γεγονός ότι ήταν πρώην σύμμαχος του κόμματος⁴⁴.

PiS Associates

19. Ορισμένοι πιστεύουν ότι το Pegasus χρησιμοποιήθηκε για την «προληπτική υποκλοπή» των συνδιαλέξεων ηγετών και διοργανωτών διαδηλώσεων, μετά τις μεταρρυθμίσεις του Συνταγματικού Δικαστηρίου που εφάρμοσε το κόμμα PiS. Ωστόσο, δεν έπεσαν μόνο οι αντίπαλοι του κυβερνώντος κόμματος θύματα του Pegasus. Ο Adam Hofman, πρώην εκπρόσωπος του κόμματος PiS, ισχυρίζεται επίσης ότι οι συνάδελφοί του τον κατασκόπευσαν το 2018, πράγμα που σημαίνει ότι ήταν ένας από τους πρώτους στόχους μετά την αγορά του κατασκοπευτικού λογισμικού. Ο Hofman ίδρυσε την R4S,

³⁹ AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e> 21 December 2021.

⁴⁰ European Commission Rule of Law 2022 Report, Poland Specific Chapter, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 16.

⁴¹ AP, <https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e>, 21 December 2021.

⁴² The Guardian, <https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony>, 24 January 2022.

⁴³ <https://www.nik.gov.pl/en/about-us/>

⁴⁴ Politico, <https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/>, 18 January 2022.

εταιρεία δημοσίων σχέσεων, μετά την αποπομπή του από το κόμμα PiS⁴⁵⁴⁶. Σύμφωνα με πληροφορίες, η εν λόγω ενέργεια αναστάτωσε το κυβερνών κόμμα και κατέστησε τον Hofman στόχο παρακολούθησης. Δηλώνει ότι οι συλλεγείσες πληροφορίες χρησιμοποιήθηκαν στη συνέχεια σε εκστρατεία δυσφήμισης του.

Σύνδεση με εκστρατείες δυσφήμισης

20. Για πολλές εβδομάδες, ο γερουσιαστής Brejza ήταν στόχος εκστρατείας δυσφήμισης που χρησιμοποιούσε υλικό αποκτηθέν μέσω της χρήσης κατασκοπευτικού λογισμικού. Είναι αξιοσημείωτο το γεγονός ότι το υλικό αυτό δημοσιοποιήθηκε μέσω της δημόσιας τηλεόρασης. Πώς μπορεί να εξηγηθεί η πρόσβαση ενός δημόσιου ραδιοτηλεοπτικού φορέα σε τέτοιο υλικό; Εάν το χάκινγκ του γερουσιαστή Brejza με το Pegasus ήταν πράγματι ζήτημα εθνικής ασφάλειας, όπως φαίνεται να υπονοεί η κυβέρνηση, η διαρροή του υλικού που αποκτήθηκε στο πλαίσιο μυστικής επιχείρησης ασφαλείας θα συνιστούσε ιδιαίτερα σοβαρό έγκλημα. Το γεγονός ότι ο δημόσιος ραδιοτηλεοπτικός φορέας βρίσκεται επίσης υπό τον έλεγχο του κυβερνητικού κόμματος μάλλον δείχνει ότι πρόκειται για εκστρατεία δυσφήμισης που ενορχηστρώθηκε από τα κυβερνητικά κόμματα.

I.B. Ουγγαρία

21. Η Ουγγαρία ήταν μία από τις πρώτες χώρες που ενεπλάκη στο σκάνδαλο των ευρωπαϊκών κατασκοπευτικών λογισμικών. Το 2021, το «Pegasus Project» αποκάλυψε ότι ορισμένοι ουγγρικοί αριθμοί τηλεφώνου περιλαμβάνονταν μεταξύ των 50 000 αριθμών τηλεφώνου που προσδιορίστηκαν ως δυνητικώς παραβιασθέντες από το προϊόν της NSO. Έκτοτε έχει επιβεβαιωθεί από τη Διεθνή Αμνηστία⁴⁷ ότι πάνω από 300 Ούγγροι έχουν πέσει θύματα του Pegasus, συμπεριλαμβανομένων πολιτικών ακτιβιστών, δημοσιογράφων, δικηγόρων, επιχειρηματιών και ενός πρώην υπουργού της κυβέρνησης⁴⁸.

Αγορά του Pegasus

22. Το ουγγρικό Υπουργείο Εσωτερικών αγόρασε το Pegasus από τον όμιλο NSO το 2017 λίγο μετά τη συνάντηση του Orbán με τον πρωθυπουργό της Πολωνίας Mateusz Morawiecki και τον πρώην πρωθυπουργό του Ισραήλ Benjamin Netanyahu⁴⁹⁵⁰. Το ουγγρικό Υπουργείο Εσωτερικών επιβεβαίωσε το γεγονός αυτό μόλις στις 8 Απριλίου 2021, όταν ο πρόεδρος της κοινοβουλευτικής επιτροπής άμυνας και επιβολής του νόμου, Lajos Kósa, παραδέχθηκε την αγορά του Pegasus από την κυβέρνηση Fidesz⁵¹

⁴⁵ <https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true>

⁴⁶ Rzeczpospolita, <https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana>, 11 October 2014.

⁴⁷ Euractiv, [Hungary employed Pegasus spyware in hundreds of cases, says government agency](#), 1 February 2022.

⁴⁸ DW, [‘Pegasus scandal: In Hungary, journalists sue state over spyware’](#), 29 January 2022.

⁴⁹ Financieel Dagblad, [De wereld deze week: het beste uit de internationale pers](#), 7 January, 2022.

⁵⁰ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

⁵¹ DW, [Hungary admits to using NSO Group’s Pegasus spyware](#), 4 November 2021.

—ο Κόσα επέμεινε ωστόσο ότι το κατασκοπευτικό λογισμικό δεν έχει χρησιμοποιηθεί ποτέ εναντίον Ούγγρων πολιτών⁵².

Νομικό πλαίσιο

23. Οι νομικές πράξεις που διέπουν το κατασκοπευτικό λογισμικό στην Ουγγαρία είναι από τις πιο αδύναμες αυτού του είδους διατάξεις στην Ευρώπη⁵³. Το σύστημα λειτουργεί σε κατάφωρη παραβίαση των ευρωπαϊκών απαιτήσεων και προτύπων που ορίζονται για την παρακολούθηση των πολιτών από την ΕΣΔΑ και τις αποφάσεις του ΕΔΑΔ⁵⁵, παρά την επιμονή της κυβέρνησης ότι έχουν ενεργήσει νόμιμα σε όλες τις περιπτώσεις και ότι συμμορφώνονται πλήρως με τον νόμο⁵⁶. Ο νόμος CXXV του 1995 για τις υπηρεσίες εθνικής ασφάλειας (εφεξής «ο νόμος») διέπει επί του παρόντος τη χρήση κατασκοπευτικού λογισμικού στην Ουγγαρία⁵⁸ και αποτελεί πολύ περισσότερο εργαλείο ελέγχου και εξουσίας για την κυβέρνηση παρά ασπίδα για τα δικαιώματα και την ιδιωτική ζωή των πολιτών. Όχι μόνο παραλείπει την υποχρέωση ενημέρωσης των αντικειμένων της παρακολούθησης, αλλά ορίζει ρητά ότι οι στόχοι δεν πρέπει να ενημερώνονται από το μέρος που παρέχει την εξουσιοδότηση ότι κατασκοπεύονται⁵⁹. Η απαίτηση ενημέρωσης των θυμάτων διαπιστώθηκε σαφώς στην υπόθεση *Klass και άλλοι κατά Γερμανίας*⁶⁰ στο ΕΔΑΔ και η ουγγρική κυβέρνηση δεν εφάρμοσε την εν λόγω απόφαση όπως και η Πολωνία και πολλές άλλες χώρες εντός της ΕΕ.

Εκ των προτέρων έλεγχος

24. Σύμφωνα με τον νόμο, η παρακολούθηση που διενεργείται από τις ειδικές υπηρεσίες εθνικής ασφάλειας (SNSS) με τη χρήση κατασκοπευτικού λογισμικού εξαρτάται από την άδεια του υπουργού Δικαιοσύνης στις περισσότερες περιπτώσεις, και από τον δικαστή που ορίζεται από τον πρόεδρο του περιφερειακού δικαστηρίου Βουδαπέστης-Πρωτεύουσας σε ορισμένες ειδικές περιπτώσεις⁶¹. Δεν μπορεί να ασκηθεί προσφυγή

⁵² DW, *Hungary admits to using NSO Group's Pegasus spyware*, 4 November 2021

⁵³ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

⁵⁴ DW, *Pegasus scandal: In Hungary, journalists sue state over spyware*, 29 January 2022.

⁵⁵ See, inter alia, *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015 39; *Klass and others v. Germany*, 6 September 1978, § 50, Series A no. 28. 40; *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003; *Liberty and others v. United Kingdom*, no. 58243/00, § 62, 1 July 2008.

⁵⁶ AP, <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, 4 November 2021.

⁵⁷ Euractiv, *Hungary employed Pegasus spyware in hundreds of cases, says government agency*, 1 February 2022.

⁵⁸ Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.

⁵⁹ Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Section 58.

⁶⁰ *Klass and others v. Germany*, 6 September 1978, § 50, Series A no. 28. 40.

⁶¹ Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 56-58.

⁶² Europe's PegasusGate: Countering Spyware Abuse - EPRS Report, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU\(2022\)729397_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf), July 2022 at pg. 20.

κατά των αποφάσεων αυτών και δεν υπάρχει ουσιαστικά καμία εποπτεία της διαδικασίας⁶³⁶⁴.

Κατασταλτικός έλεγχος

25. Τον Νοέμβριο του 2021, κατόπιν επιμονής της αντιπολίτευσης, δύο επιτροπές στη Γερουσία διεξήγαγαν ακροάσεις σχετικά με τη χρήση κατασκοπευτικού λογισμικού στην Ουγγαρία και, ειδικότερα, την εικαζόμενη πολιτικά υποκινούμενη στοχοποίηση πολιτών από την κυβέρνηση. Στη συνέχεια αναφέρθηκε ότι οι εκπρόσωποι της κυβέρνησης επέμεναν ότι όλες οι παρακολουθήσεις είχαν εγκριθεί μέσω των κατάλληλων διαύλων, αλλά αρνήθηκαν να σχολιάσουν κατά πόσον στοχοποιήθηκαν δημοσιογράφοι ή πολιτικοί. Ωστόσο, δεν είναι δυνατόν να γνωρίζουμε επακριβώς τι ειπώθηκε, δεδομένου ότι το κυβερνών κόμμα διαβάθμισαν τα πρακτικά της συνεδρίασης έως το έτος 2050.

Μέσα προσφυγής

26. Όταν ξέσπασε το σκάνδαλο Pegasus στην Ουγγαρία, κατέστη σαφές ότι οι δημοσιογράφοι ήταν μία από τις ομάδες που στοχοποιήθηκαν περισσότερο από την κυβέρνηση, αν και η εν λόγω χώρα ούτε επιβεβαιώνει ούτε διαψεύδει κάτι τέτοιο. Συνεπώς, στις αρχές του 2022 μια ομάδα έξι δημοσιογράφων και ακτιβιστών κίνησε νομικές διαδικασίες στην Ουγγαρία τόσο κατά του κράτους όσο και κατά της ΝΑΙΗ. Η Ουγγρική Ένωση Πολιτικών Ελευθεριών (HCLU) θα εκπροσωπήσει τους δημοσιογράφους Brigitta Csikász, Dávid Dercsényi, Dániel Németh και Szabolcs Panyi, καθώς και τον Adrien Beauduin, έναν ακτιβιστή και υποψήφιο διδάκτορα, βελγοκαναδικής ιθαγένειας. Το έκτο μέρος επέλεξε να διατηρήσει την ανωνυμία του. Η HCLU συνεργάζεται επίσης με την Eitay Mack στο Ισραήλ για να υποβάλει υπόθεση στον γενικό εισαγγελέα προκειμένου να κινηθεί έρευνα για τον όμιλο NSO⁶⁵.

Πολιτικός έλεγχος

27. Ο πολιτικός έλεγχος της χρήσης της παρακολούθησης στην Ουγγαρία είναι πλήρης και συνολικός. Το καθεστώς Fidesz υπό την ηγεσία του Orbán έχει διαμορφώσει την κατάσταση έτσι ώστε να μπορεί να στοχεύσει δικηγόρους, δημοσιογράφους, πολιτικούς αντιπάλους και οργανώσεις της κοινωνίας των πολιτών με ευκολία και χωρίς φόβο προσφυγής. Επιπλέον, ο έλεγχός τους σε όλα σχεδόν τα ουγγρικά μέσα ενημέρωσης τους επιτρέπει να συνεχίσουν να προωθούν τη δική τους εκδοχή της αλήθειας, εμποδίζοντας μεγάλο μέρος του δημόσιου ελέγχου που διενεργούν τα μέσα ενημέρωσης να φτάσει στους Ούγγρους πολίτες.

Οι στόχοι

28. Είναι πολύ σαφές ότι οι ενέργειες της κυβέρνησης είχαν πολιτικά κίνητρα από τη στιγμή που ξέσπασε το σκάνδαλο του κατασκοπευτικού λογισμικού στην Ουγγαρία.

⁶³ Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf at Sections 57 and 58.

⁶⁴ European Commission Rule of Law Report 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf, at pg. 26.

⁶⁵ The Guardian, <https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state>, 28 January 2022.

Αναφέρθηκε ότι οι τηλεφωνικοί αριθμοί άνω των 300 ατόμων περιλαμβάνονταν στα πορίσματα του «Pegasus project»⁶⁶. Μεταξύ αυτών περιλαμβάνονταν τουλάχιστον πέντε δημοσιογράφοι, δέκα δικηγόροι και ένας πολιτικός της αντιπολίτευσης, καθώς και ακτιβιστές και επιχειρηματίες υψηλής προβολής⁶⁷. Μολονότι η περίληψη αριθμών τηλεφώνου στον εν λόγω κατάλογο δεν σημαίνει κατ' ανάγκη ότι έγινε χάκινγκ των εν λόγω τηλεφώνων, είναι μια αποκαλυπτική εικόνα των μεθοδικών και συστηματικών ενεργειών και της στάσης της κυβέρνησης της Ουγγαρίας έναντι των θεμελιωδών δικαιωμάτων και της ελευθερίας των μέσων ενημέρωσης. Έκτοτε από το 2021, έχει επιβεβαιωθεί ότι ορισμένοι στόχοι έχουν παραβιαστεί επιτυχώς με κατασκοπευτικό λογισμικό.

Szabolcs Panyi

29. Η παραβίαση του τηλεφώνου του δημοσιογράφου και συντάκτη Szabolcs Panyi συνέβη κατά τη διάρκεια της εργασίας του στο Direkt36. Ως μία από τις λίγες ανεξάρτητες πηγές ειδήσεων που έχουν απομείνει στην Ουγγαρία, αποτελεί σημαντικό στόχο του κυβερνώντος κόμματος. Ο Panyi είναι γνωστός, έγκριτος δημοσιογράφος και, κατά συνέπεια, εκτός από τη συλλογή βασικών πληροφοριών απευθείας από τον ίδιο τον Panyi, πολλές από τις επαφές και τις πηγές στο τηλέφωνό του θα αποτελούσαν πολύτιμα παρεμπόδιοντα ευρήματα για την κυβέρνηση.

Zoltán Varga

30. Ως διευθύνων σύμβουλος και πρόεδρος του ομίλου Central Media, ο Zoltán Varga είναι ιδιοκτήτης του 24.hu., του μεγαλύτερου εναπομένοντος ανεξάρτητου ειδησεογραφικού ιστότοπου της Ουγγαρίας. Αφού η κυβέρνηση Orbán δρομολόγησε την εξαγορά του κύριου ανταγωνιστή του, του Index.hu, το 2020, ο Varga έμεινε να αψηφά μόνος του το κυβερνών κόμμα.

Adrien Beauduin

31. Ο Adrien Beauduin εμφανίστηκε στο ραντάρ του καθεστώτος Orbán το 2018, ενώ ολοκλήρωνε το διδακτορικό δίπλωμα του σε σπουδές για θέματα φύλου στο Πανεπιστήμιο Κεντρικής Ευρώπης (CEU). Το εν λόγω πανεπιστήμιο ιδρύθηκε από τον George Soros και η κυβέρνηση προσπαθούσε να το απομακρύνει από την Ουγγαρία την εποχή εκείνη, μαζί με ολόκληρο το αντικείμενο των σπουδών για θέματα φύλου⁶⁸. Μετά τη συμμετοχή του σε διαμαρτυρία στη Βουδαπέστη, ο Beauduin συνελήφθη σε μια κίνηση που θεωρείται εξαιρετικά πολιτικά υποκινούμενη και αντιμετώπισε κατηγορίες για επίθεση κατά αστυνομικού, τις οποίες αρνείται κατηγορηματικά⁶⁹. Αναφέρθηκε ότι ουσιαστικά δεν υπήρχαν αποδεικτικά στοιχεία κατά του Beauduin και

⁶⁶Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/> , 19 July 2021.

⁶⁷ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests> , 18 July 2021 and Washington Post, <https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/> , 19 July 2021.

⁶⁸ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests> , 18 July 2021.

⁶⁹ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests> , 18 July 2021.

ότι τα αποδεικτικά στοιχεία που υποβλήθηκαν είχαν αντιγραφεί αυτολεξεί από την αστυνομική μαρτυρία σε άλλη υπόθεση⁷⁰.

Πονα Ρατόcs

32. Η δικηγόρος Πονα Ρατόcs υπήρξε ύποπτο θύμα παρακολούθησης με Pegasus το καλοκαίρι του 2019, ενώ εκπροσωπούσε πελάτη σε μια μακροχρόνια υπόθεση δολοφονίας με μεγάλη προβολή⁷¹. Ωστόσο, λόγω του τύπου της κινητής συσκευής που χρησιμοποιούσε, δεν ήταν δυνατόν να επιβεβαιωθεί αν η παραβίαση ήταν πλήρως επιτυχής ή ποτέ ακριβώς συνέβη. Ο πελάτης της, István Hatvani, είχε ήδη εκτίσει επτά έτη για δολοφονία, με βάση, κατά την Ρατόcs, μια «πολιτικά υποκινούμενη» καταδίκη⁷². Παρά το γεγονός ότι ένας άλλος διάδικος ισχυρίστηκε αργότερα ότι ευθύνεται για τη δολοφονία, το ουγγρικό εφετείο έστειλε τον Hatvani πίσω στη φυλακή για να ολοκληρώσει την αρχική του ποινή. Πολλοί άλλοι αριθμοί τηλεφώνου δικηγόρων έχουν καταγραφεί ως δυνητικοί στόχοι του Pegasus, συμπεριλαμβανομένου του προέδρου του ουγγρικού δικηγορικού συλλόγου János Bánáti⁷³. Ειδικότερα, αυτή η στόχευση δείχνει σαφή αδιαφορία από την κυβέρνηση για το προνόμιο που υφίσταται μεταξύ των δικηγόρων και των πελατών τους.

Άλλοι στόχοι

33. Άτομα εντός του κύκλου του κυβερνώντος κόμματος έχουν επίσης στοχοποιηθεί με κατασκοπευτικό λογισμικό. Το ανεξάρτητο ουγγρικό μέσο ενημέρωσης Direkt36 ανέφερε τον Δεκέμβριο του 2021 ότι ένας σωματοφύλακας του János Áder, προέδρου και στενού συμμάχου του Orbán, έπεσε θύμα του κατασκοπευτικού λογισμικού Pegasus. Ο δημοσιογράφος του Direkt36 και θύμα του κατασκοπευτικού λογισμικού Szabolcs Panyí ανέφερε ότι αυτό το είδος κατασκοπείας οφείλεται κυρίως στην αυξανόμενη παράνοια του πρωθυπουργού της Ουγγαρίας.

Εταιρείες κατασκοπευτικού λογισμικού

34. Η ουγγρική κυβέρνηση όχι μόνο αγόρασε και χρησιμοποίησε κατασκοπευτικό λογισμικό Pegasus κατά του λαού της, αλλά και φιλοξενεί και άλλες εταιρείες στην αγορά πληροφοριών. Η Black Cube είναι μια ισραηλινή ιδιωτική υπηρεσία πληροφοριών που αποτελείται από πρώην υπαλλήλους της Mossad, του ισραηλινού στρατού και των ισραηλινών υπηρεσιών πληροφοριών⁷⁴. Ο ίδιος ο δικτυακός τόπος της εταιρείας τους περιγράφει ως «δημιουργική υπηρεσία πληροφοριών» που βρίσκει «προσαρμοσμένες λύσεις σε σύνθετες επιχειρηματικές και δικαστικές προκλήσεις»⁷⁵. Η Black Cube έχει εμπλακεί σε μια σειρά δημόσιων αντιπαραθέσεων σε σχέση με

⁷⁰ The Guardian, <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>, 18 July 2021.

⁷¹ Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

⁷² Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

⁷³ Direkt36, <https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

⁷⁴ The New Yorker, <https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators>, 7 October 2019.

⁷⁵ <https://www.blackcube.com/>

υποθέσεις χάκινγκ, μεταξύ άλλων στις ΗΠΑ και τη Ρουμανία⁷⁶. Ιδιαίτερα σημαντικό είναι ότι αποκαλύφθηκε επίσης πως οι εν λόγω υποθέσεις συνδέονται με τον όμιλο NSO και το κατασκοπευτικό λογισμικό Pegasus. Μετά από μεγάλη δημόσια πίεση σχετικά με την πρόσληψη της NSO από την Black Cube για να στοχεύσει τους αντιπάλους τους, ο πρώην διευθύνων σύμβουλος της NSO Shalev Hulio παραδέχθηκε ότι προσέλαβε την Black Cube σε τουλάχιστον μία περίπτωση στην Κύπρο.

I. Γ. Ελλάδα

35. Φέτος, η Ελλάδα κλονίστηκε από μια σειρά αποκαλύψεων σχετικά με την προφανώς πολιτικά υποκινούμενη χρήση κατασκοπευτικού λογισμικού. Στις 26 Ιουλίου 2022, ο βουλευτής του Ευρωπαϊκού Κοινοβουλίου και ηγέτης του κόμματος ΠΑΣΟΚ της ελληνικής αντιπολίτευσης Νίκος Ανδρουλάκης υπέβαλε καταγγελία στην Εισαγγελία του Αρείου Πάγου για απόπειρες μόλυνσης του κινητού του τηλεφώνου με το κατασκοπευτικό λογισμικό Predator⁷⁷. Η απόπειρα μόλυνσης από κατασκοπευτικό λογισμικό ανακαλύφθηκε κατά τη διάρκεια ελέγχου του τηλεφώνου του Ανδρουλάκη από την υπηρεσία ΤΠ του Ευρωπαϊκού Κοινοβουλίου⁷⁸. Οι απόπειρες χάκινγκ έγιναν ενώ ο Ανδρουλάκης ήταν υποψήφιος για την ηγεσία του κόμματος της αντιπολίτευσης. Η αποκάλυψη αυτή έφερε στο προσκήνιο τις καταγγελίες που είχαν υποβληθεί νωρίτερα, τον Απρίλιο και τον Μάιο του 2022, από τον δημοσιογράφο οικονομικών θεμάτων Θανάση Κουκάκη σχετικά με τη μόλυνση του τηλεφώνου του με το Predator. Τον Σεπτέμβριο αποκαλύφθηκε ότι ο πρώην υπουργός Υποδομών και βουλευτής του κόμματος ΣΥΡΙΖΑ, Χρήστος Σπίρτζης⁷⁹, είχε επίσης αποτελέσει στόχο κατασκοπευτικού λογισμικού. Επιπλέον, αργότερα τον ίδιο μήνα αποκαλύφθηκε ότι η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ) φέρεται να είχε στοχεύσει δύο από τους υπαλλήλους της με κατασκοπευτικό λογισμικό⁸⁰. Στις 5 και 6 Νοεμβρίου, τα ελληνικά μέσα ενημέρωσης αποκάλυψαν λίστα με 33 στόχους, όλοι τους διακεκριμένες προσωπικότητες⁸¹. Ο κατάλογος —εάν επιβεβαιωθεί— μοιάζει με εντυπωσιακό ευρετήριο σημαντικών προσώπων από τους τομείς της πολιτικής, των επιχειρήσεων και των μέσων ενημέρωσης στην Ελλάδα. Ο αντίκτυπος αυτής της μεγάλης κλίμακας πολιτικής χρήσης του κατασκοπευτικού λογισμικού εκτείνεται αναπόφευκτα πέραν των ατόμων που περιλαμβάνονται στον κατάλογο, καθώς όλες οι αντίστοιχες επαφές και συνδέσεις τους «εμπλέκονται» έμμεσα και στην κατασκοπευτική επιχείρηση, συμπεριλαμβανομένων των επαφών τους στα όργανα της ΕΕ. Η έντονη παρουσία κατασκοπευτικού λογισμικού ήταν ήδη εμφανής στην έκθεση Meta του 2021, η οποία αναφέρει στο παράρτημά της 310 συνδέσμους προς ψευδεπίγραφους ιστότοπους που σχετίζονταν με την εταιρεία κατασκοπευτικού λογισμικού Cytrox, εκ των οποίων οι 42 δημιουργήθηκαν για να παραπλανήσουν στόχους μόνο στην Ελλάδα⁸²⁸³.
36. Οι αποκάλυψεις σχετικά με τη χρήση κατασκοπευτικού λογισμικού και την παρακολούθηση δημοσιογράφων από την ΕΥΠ σκιαγραφούν μια πολύ ανησυχητική

⁷⁶ The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

⁷⁷ Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

⁷⁸ Tagesspiegel. [Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.](#)

⁷⁹ Reuters. [One more Greek lawmaker files complaint over attempted phone hacking.](#)

⁸⁰ Efsyn. [Targeting the disliked.](#)

⁸¹ Documento. [Apocalypse: They Watched - This Sunday in Document.](#)

⁸² Meta. [Threat Report on the Surveillance-for-Hire Industry.](#)

⁸³ InsideStory. [Who was tracking the mobile phone of journalist Thanasis Koukakis?](#)

ιστορία ενός περίπλοκου και αδιαφανούς δικτύου σχέσεων, πολιτικών και επιχειρηματικών συμφερόντων, ευνοιών και νεποτισμού, καθώς και πολιτικής επιρροής. Είναι εύκολο να χαθεί κανείς στον λαβύρινθο. Ωστόσο, εμφανίζονται ορισμένα μοτίβα. Η πολιτική πλειοψηφία χρησιμοποιείται για την προώθηση συγκεκριμένων συμφερόντων και όχι για το γενικό συμφέρον, ιδίως με τον διορισμό συνεργατών και πιστών σε καίριες θέσεις όπως στην ΕΥΠ, την ΕΑΔ και την Krikel. Λαμβάνοντας υπόψη ότι το κατασκοπευτικό λογισμικό, ενδεχομένως σε συνδυασμό με τη νόμιμη παρακολούθηση, χρησιμοποιείται ως εργαλείο πολιτικής εξουσίας και ελέγχου στα χέρια της ανώτατης πολιτικής ηγεσίας της χώρας. Οι μηχανισμοί εκ των προτέρων ελέγχου και κατασταλτικού ελέγχου έχουν αποδυναμωθεί σκόπιμα και αποφεύγεται η διαφάνεια και η λογοδοσία. Δημοσιογράφοι που ασκούν κριτική ή υπάλληλοι που καταπολεμούν τη διαφθορά και την απάτη αντιμετωπίζουν εκφοβισμό και εμπόδια και δεν υπάρχει προστασία των μαρτύρων δημοσίου συμφέροντος.

37. Η κατασκοπεία για πολιτικούς λόγους δεν είναι νέο φαινόμενο για την Ελλάδα, αλλά οι νέες τεχνολογίες κατασκοπευτικού λογισμικού καθιστούν πολύ ευκολότερη την παράνομη παρακολούθηση, ιδίως σε ένα πλαίσιο σοβαρής αποδυνάμωσης των διασφαλίσεων. Σε αντίθεση με άλλες περιπτώσεις, όπως η Πολωνία, η κατάχρηση του κατασκοπευτικού λογισμικού δεν φαίνεται να αποτελεί μέρος μιας ολοκληρωμένης αυταρχικής στρατηγικής, αλλά εργαλείο που χρησιμοποιείται σε ad hoc βάση για πολιτικά και οικονομικά οφέλη. Ωστόσο, διαβρώνει εξίσου τη δημοκρατία και το κράτος δικαίου και αφήνει μεγάλα περιθώρια για διαφθορά, ενώ αυτή η περίοδος κρίσεων απαιτεί αξιόπιστη και υπεύθυνη ηγεσία.

Αγορά

38. Η κυβέρνηση αρνείται την αγορά κατασκοπευτικού λογισμικού Predator⁸⁴. Ωστόσο, εάν η αγορά δεν έγινε από την ελληνική κυβέρνηση, τότε θα πρέπει να συναχθεί το συμπέρασμα ότι ένας μη κρατικός φορέας ήταν υπεύθυνος για τις (απόπειρες) παραβίασης των τηλεφώνων των Κουκάκη και Ανδρουλάκη. Αυτό θα συνιστούσε έγκλημα κατά το ελληνικό δίκαιο και θα ανέμενε κανείς από τις ελληνικές αρχές να διερευνήσουν άμεσα και αποφασιστικά μια τόσο σοβαρή υπόθεση. Ωστόσο, μέχρι στιγμής δεν υπάρχει αστυνομική έρευνα, αλλά μόνο εισαγγελικές έρευνες κατόπιν καταγγελιών. Δεν έχει κατασχεθεί κανένα υλικό αποδεικτικό στοιχείο. Επιπλέον, η υπόθεση ότι πίσω από τις επιθέσεις με Predator κρύβονται ιδιωτικοί φορείς είναι εξαιρετικά απίθανη, καθώς δεν εξηγεί την επιλογή των στόχων.
39. Μια άλλη πιθανότητα είναι η αγορά του Predator μέσω της Ketyak, μιας ειδικής οντότητας που συστάθηκε από τον πρώην διευθυντή της ΕΥΠ, Κοντολέων. Η εν λόγω οντότητα λειτουργεί σε απόσταση από την ΕΥΠ.
40. Ελλείπει αποδεικτικών στοιχείων σχετικά με την ταυτότητα του αγοραστή και του χρήστη του Predator στις ελληνικές υποθέσεις, δεν μπορεί να διαπιστωθεί με βεβαιότητα αν ή με ποιον τρόπο η κυβέρνηση ή άλλος φορέας απέκτησε το Predator. Ωστόσο, κατ' αρχήν, δεν είναι αδύνατον να αποκτηθεί ή να χρησιμοποιηθεί κατασκοπευτικό λογισμικό χωρίς οι κρατικοί φορείς να αγοράσουν στην πραγματικότητα απευθείας το λογισμικό. Το κατασκοπευτικό λογισμικό μπορεί να αγοραστεί μέσω πληρεξουσίων, εταιρειών μεσολάβησης ή μεσαζόντων, όπως έχουμε

⁸⁴ Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

δει σε άλλες περιπτώσεις, ή μπορεί να γίνει συμφωνία με πωλητές κατασκοπευτικού λογισμικού για την παροχή ορισμένων υπηρεσιών που σχετίζονται με κατασκοπευτικό λογισμικό. Δεν υπάρχει αμφιβολία ότι υπήρξαν στενές διασυνδέσεις και αλληλεξαρτήσεις μεταξύ ορισμένων προσώπων και συμβάντων που σχετίζονται με την κυβέρνηση, την ΕΥΠ και τους παρόχους κατασκοπευτικού λογισμικού, ιδίως την Krikel, προτιμώμενο προμηθευτή εξοπλισμού επικοινωνιών και παρακολούθησης, μεταξύ άλλων, στην αστυνομία και την ΕΥΠ. Η Krikel συνδέεται στενά με άτομα από το περιβάλλον του πρωθυπουργού Μητσοτάκη.

Γρηγόρης Δημητριάδης

41. Ο Δημητριάδης είναι ανιψιός του πρωθυπουργού Μητσοτάκη και μέχρι τον Αύγουστο του 2022 ο Γενικός Γραμματέας στο γραφείο του. Υπό την ιδιότητά του αυτή, ήταν υπεύθυνος για τις κυβερνητικές επαφές με την ΕΥΠ.

Φέλιξ Μπίτζιος

42. Ο επιχειρηματίας Φέλιξ Μπίτζιος είχε εμπλακεί στην τεράστια παραβίαση του σκανδάλου ελέγχου κεφαλαίων της Τράπεζας Πειραιώς. Εν αναμονή των ερευνών, τα περιουσιακά στοιχεία του Μπίτζιου δεσμεύθηκαν⁸⁵. Ο Μπίτζιος επωφελήθηκε από νομοθετική τροποποίηση που εισήγαγε ο πρωθυπουργός Μητσοτάκης λίγο μετά την ανάληψη της εξουσίας το 2019. Η αμφιλεγόμενη τροποποίηση έθεσε χρονικό όριο για τη δέσμευση περιουσιακών στοιχείων, επιτρέποντας έτσι την αποδέσμευση δεσμευμένων περιουσιακών στοιχείων μετά από δεκαοκτώ μήνες κατ' ανώτατο όριο⁸⁶. Χάρη στην τροπολογία της κυβέρνησης Μητσοτάκη, τα περιουσιακά στοιχεία του Μπίτζιου θα μπορούσαν να αποδεσμευθούν.
43. Ο Μπίτζιος κατείχε το 35 % των μετοχών της Intellexa, μέσω της εταιρίας του Santinomo. Ωστόσο, στις 4 Αυγούστου 2022, καταχώρισε τη μεταβίβαση του συνόλου των μετοχών του στην Thalestris, μητρική εταιρία της Intellexa⁸⁷. Αυτό που είναι αξιοσημείωτο δεν είναι μόνο η ημερομηνία καταχώρισης της μεταβίβασης —μόλις ημέρες μετά τις αποκαλύψεις για το χάκινγκ Ανδρουλάκη— αλλά το γεγονός ότι η μεταβίβαση φέρεται να πραγματοποιήθηκε στις 18 Δεκεμβρίου 2020, δηλαδή πάνω από 19 μήνες νωρίτερα. Συνεπώς, ο Μπίτζιος αποστασιοποιήθηκε αναδρομικά από το ιδιοκτησιακό καθεστώς 1/3 της Intellexa. Ωστόσο, ο Μπίτζιος είχε συνδεθεί με την Intellexa από τον Μάρτιο του 2020 έως τον Ιούνιο του 2021 ως αναπληρωτής διευθυντής.

Γιάννης Λαβράνος

44. Ο Γιάννης Λαβράνος είχε κατηγορηθεί για φοροδιαφυγή και ο δημοσιογράφος Κουκάκης έκανε ρεπορτάζ για την υπόθεση του Λαβράνου.

Intellexa

⁸⁵ Lexocology. [Cyprus court offers directions to bank on ambit of freezing injunction.](#)

⁸⁶ Financial Times. [Greek law change viewed as backtracking on money laundering.](#)

⁸⁷ Inside Story. [Predatorgate: The second shareholder of Intellexa SA.](#)

45. Το κατασκοπευτικό λογισμικό Predator πωλείται μέσω της Intellexa, μιας κοινοπραξίας πωλητών κατασκοπευτικού λογισμικού με παρουσία, μεταξύ άλλων, στην Κύπρο, την Ελλάδα, την Ιρλανδία και τη Γαλλία. Ο Tal Dilian, ο οποίος είχε προηγούμενη σταδιοδρομία στην Ισραηλινή Αμυντική Δύναμη, ίδρυσε την κοινοπραξία στην Κύπρο. Η δεύτερη πρώην σύζυγός του, Πολωνή υπήκοος, Sara Hamou, είναι κεντρική προσωπικότητα στο περίπλοκο δίκτυο εταιρειών. Ο Tal Dilian έχει αποκτήσει επίσης τη μαλτέζικη ιθαγένεια. Το Υπουργείο Εξωτερικών της Ελλάδας, το οποίο είναι αρμόδιο για τη διανομή των αδειών εξαγωγής, δήλωσε ότι δεν χορηγήθηκαν άδειες εξαγωγής στον όμιλο εταιρειών Intellexa⁸⁸. Ωστόσο, σύμφωνα με πληροφορίες, οι εταιρείες Intellexa με έδρα την Ελλάδα εξήγαγαν τα προϊόντα τους στο Μπανγκλαντές και σε τουλάχιστον μία αραβική χώρα^{89,90}. Για λεπτομερή περιγραφή σχετικά με την Intellexa, βλ. το κεφάλαιο για τη βιομηχανία κατασκοπευτικού λογισμικού.

Krikel

46. Η Krikel είναι η προτιμώμενη προμηθεύτρια εξοπλισμού για τις ελληνικές αρχές ασφάλειας και επιβολής του νόμου. Είναι επίσης η αντιπρόσωπος στην Ελλάδα της RCS Lab, μιας ιταλικής εταιρείας που πωλεί λογισμικό παρακολούθησης. Επιπλέον, ο Γιάννης Λαβράνος φέρεται ότι κατέχει το 50 % της Krikel, μέσω μιας άλλης εταιρείας που ονομάζεται Mexal⁹¹. Ωστόσο, δεν φαίνεται να είναι δυνατόν να προσδιοριστεί με βεβαιότητα ποιος είναι ο τελικός πραγματικός δικαιούχος της Krikel, παρά τις πολυάριθμες συμβάσεις της με τις κρατικές αρχές.
47. Το 2014, η εταιρία Ιωνική Τεχνική του Γιάννη Λαβράνου πωλήθηκε στην Tetra Communications στο Λονδίνο. Κατά το ίδιο έτος, η Ιωνική Τεχνική είναι μία από τις τρεις εταιρείες που δώρισαν τα συστήματα επικοινωνίας Tetra στο ελληνικό Υπουργείο Προστασίας του Πολίτη⁹². Η δωρεά της Tetra διευκολύνθηκε από εταιρεία με έδρα τη Φλόριντα, επιτρέποντας την παράκαμψη των τακτικών διαδικασιών υποβολής προσφορών. Η δωρεά στην ελληνική κυβέρνηση έγινε δεκτή το 2017. Το 2018, η Krikel υπέγραψε σύμβαση συντήρησης και παροχής τεχνικής υποστήριξης ύψους €10,8 εκατομμυρίων EUR. Ο διαχειριστής της Krikel Stanislaw Pelczar υπέγραψε εξ ονόματος της Krikel, αλλά φαίνεται ότι ο Λαβράνος συμμετείχε ανεπίσημα στις διαπραγματεύσεις καθ' όλη τη διάρκειά τους⁹³. Η Κρίκελ έγινε σημαντική προμηθεύτρια του ελληνικού Υπουργείου Προστασίας του Πολίτη. Από το 2018, υπέγραψε επτά συμβάσεις με την ελληνική κυβέρνηση, έξι εκ των οποίων είναι απόρρητες⁹⁴.

⁸⁸ Inside Story. [Who signs the exports of spyware from Greece and Cyprus?](#)

⁸⁹ Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

⁹⁰ Inside Story. [Who signs the exports of spyware from Greece and Cyprus?](#)

⁹¹ There are several connections of interest here. Lavranos sold his in Athens based family home at a price below market value to Albitrum Properties in April 2021. The representative of Albitrum Properties during the sale was Felix Bitzios' half-brother Theodoros Zervos. Albitrum is a Cypriot company and has as its shareholder Mexal Services Ltd. Mexal Services owns 100% of Eneross Holdings ltd. Eneross Holdings in addition owns Krikel. Giannis Lavranos' registered office is at the same address as Eneross Holdings and Mexal Services in Cyprus. See: InsideStory. [Predatorgate's invisible privates.](#) and tvxs. [G.Lavranos behind KRIKEL - How the deception of the Parliament was attempted \[Revealing documents\].](#)

⁹² Inside Story. [Predatorgate's invisible privates.](#)

⁹³ Inside Story. [Predatorgate's invisible privates.](#)

⁹⁴ InsideStory. [Predatorgate's invisible privates.](#)

48. Η εταιρεία Krikel έγινε επίσης τοπική αντιπρόσωπος της ιταλικής εταιρείας RCS Lab. Τον Ιούνιο του 2021, η ΕΥΠ αγόρασε ένα σύστημα παρακολούθησης τηλεφωνικών συνδιαλέξεων από το RCS lab μέσω της Krike⁹⁵⁹⁶. Την εποχή εκείνη, ο Δημητριάδης ήταν υπεύθυνος για τις επαφές μεταξύ της κυβέρνησης και της ΕΥΠ. Ορισμένες πηγές έχουν τεκμηριώσει ότι κατά την εγκατάσταση αυτού του νέου συστήματος χάθηκε υλικό που περιείχε πληροφορίες σχετικά με την παρακολούθηση των Ανδρουλάκη και Κουκάκη, κάτι που φέρεται να προκλήθηκε από τεχνικό πρόβλημα⁹⁷. Ωστόσο, άλλες πηγές ισχυρίστηκαν ότι ο Κοντολέων διέταξε την καταστροφή των αρχείων στις 29 Ιουλίου 2022⁹⁸.
49. Αξίζει να σημειωθεί ότι παρατηρήθηκε πως εργαζόμενοι της Krikel εργάζονταν στην Ketyak, υποτίθεται αφιλοκερδώς. Φαίνεται ότι χορηγήθηκε στην Ketyak ποσό 40 εκατ. EUR από τον Μηχανισμό Ανάκαμψης και Ανθεκτικότητας, μέσω εμπιστευτικής διαδικασίας υποβολής προσφορών βάσει μυστικής απόφασης του πρωθυπουργού.

Εμπλοκή Μπίτζιου και Λαβράνου

50. Οι Μπίτζιος και Λαβράνος συμμετείχαν ενεργά στη σύσταση της Krikel το 2017. Από κοινού διοργάνωσαν τον διορισμό του Πολωνού δικηγόρου Stanislaw Pelczar ως διαχειριστή της Krikel τον Οκτώβριο του 2017⁹⁹. Η εταιρεία του Μπίτζιου Viniato Holdings Limited προσελήφθη στη συνέχεια από την Krikel ως σύμβουλος από τον Ιανουάριο έως τον Αύγουστο του 2018 έναντι αμοιβής περίπου 550 000 EUR (μολονότι η Krikel είχε κύκλο εργασιών μόνο 840 000 EUR κατά το ίδιο έτος)¹⁰⁰.
51. Οι Μπίτζιος και Λαβράνος αποτελούν δύο βασικά πρόσωπα για την παροχή υλικού επικοινωνίας και παρακολούθησης σε κρατικούς φορείς, όπως η αστυνομία και η ΕΥΠ. Ο Μπίτζιος διαδραμάτισε καθοριστικό ρόλο στην εταιρεία που πωλεί το Predator. Ήταν αμφότεροι κοντά στον Δημητριάδη και επωφελήθηκαν και οι δυο τους από επικερδείς δημόσιες συμβάσεις. Επωφελήθηκαν από τη νομική τροποποίηση της νέας κυβέρνησης με την οποία αποδεσμεύθηκαν τα δεσμευμένα περιουσιακά τους στοιχεία. Είχαν κίνητρο για τη χρήση κατασκοπευτικού λογισμικού κατά του Κουκάκη. Υπάρχει πολύ προφανής και υψηλός κίνδυνος σύγκρουσης συμφερόντων και διαφθοράς στο πλαίσιο της εμπλοκής επιχειρηματικών συμφερόντων, προσωπικών σχέσεων και πολιτικών δεσμών. Επιπλέον, θα είναι σε θέση να παράσχουν κρίσιμες πληροφορίες σχετικά με την απόκτηση και τη χρήση του Predator στην Ελλάδα.

Νομικό πλαίσιο

52. Η Ελλάδα διαθέτει κατ' αρχήν ένα αρκετά ισχυρό νομικό πλαίσιο. Ωστόσο, οι νομικές τροποποιήσεις έχουν αποδυναμώσει τις κρίσιμες διασφαλίσεις και οι πολιτικοί διορισμοί σε βασικές θέσεις αποτελούν εμπόδιο για τον έλεγχο και τη λογοδοσία.

Εκ των προτέρων έλεγχος

⁹⁵ Hellas Posts English. [The EYP supplier contaminates smartphones in Greece as well.](#)

⁹⁶ TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

⁹⁷ TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

⁹⁸ [Euractiv. Greek MEP spyware scandal takes new turn.](#)

⁹⁹ TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

¹⁰⁰ InsideStory. [From Koukakis to Androulakis: A new twist in the Predator spyware case.](#)

53. Στην Ελλάδα, η μόλυνση συσκευής με κατασκοπευτικό λογισμικό αποτελεί ποινικό αδίκημα, όπως ορίζεται σε διάφορα άρθρα του ελληνικού ποινικού κώδικα, συμπεριλαμβανομένου του άρθρου 292 σχετικά με τα εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών, του άρθρου 292B σχετικά με την παρεμπόδιση της λειτουργίας των συστημάτων πληροφοριών, καθώς και του άρθρου 370 σχετικά με τις παραβιάσεις του απορρήτου των επιστολών. Επιπλέον, η παραγωγή, πώληση, προμήθεια, χρήση, εισαγωγή, κατοχή και διανομή κακόβουλου λογισμικού (συμπεριλαμβανομένου του κατασκοπευτικού λογισμικού) αποτελεί επίσης ποινικό αδίκημα, όπως περιγράφεται στο άρθρο 292Γ του ελληνικού Ποινικού Κώδικα¹⁰¹.

Πράξη νομοθετικού περιεχομένου

54. Μετά τις αποκαλύψεις για τις παρακολουθήσεις, ο πρωθυπουργός Μητσοτάκης πρότεινε αλλαγές στο πλαίσιο λειτουργίας της ΕΥΠ. Μία από τις αλλαγές αυτές είναι η θέσπιση της Πράξης Νομοθετικού Περιεχομένου από την κυβέρνηση στις 9 Αυγούστου 2022. Η παράγραφος 2 του άρθρου 9 του νόμου 3649/2008 επικαιροποιείται και πλέον απαιτείται γνωμοδότηση της Μόνιμης Επιτροπής Θεσμών και Διαφάνειας σχετικά με τον διορισμό του διοικητή της ΕΥΠ¹⁰². Ωστόσο, δεδομένου ότι το κυβερνών κόμμα διαθέτει επί του παρόντος απόλυτη πλειοψηφία στην Ειδική Μόνιμη Επιτροπή Θεσμών και Διαφάνειας του Κοινοβουλίου, ενέκρινε τον διορισμό του κ. Δεμίρη ως νέου διοικητή της ΕΠΝ, ενώ όλα τα άλλα κόμματα της αντιπολίτευσης τάχθηκαν κατά του διορισμού αυτού¹⁰³. Παρεμπιπτόντως, ο δεύτερος υποδιοικητής της ΕΥΠ είναι ο Διονύσης Μελιτσιώτης¹⁰⁴, πρώην μέλος του ιδιαίτερου γραφείου του πρωθυπουργού, ενώ ένας άλλος υποδιοικητής είναι ο Αναστάσιος Μητσιάλης, πρώην υπάλληλος της Νέας Δημοκρατίας¹⁰⁵.

Κατασταλτικός έλεγχος

55. Από το 2019, οι ενέργειες της ΕΥΠ. τελούν υπό τον άμεσο έλεγχο του πρωθυπουργού Κυριάκου Μητσοτάκη έπειτα από αλλαγή του νόμου μετά τη νίκη της Νέας Δημοκρατίας το 2019¹⁰⁶.
56. Το απόρρητο των επικοινωνιών, όπως προβλέπεται στον νόμο 2225/1994, ορίζει ότι το εν λόγω απόρρητο μπορεί να αρθεί μόνο σε περιπτώσεις εθνικής ασφάλειας και για τη διερεύνηση σοβαρών εγκλημάτων. Μετά την άρση του απορρήτου, το άρθρο 5 του εν λόγω νόμου ορίζει ότι η ΑΔΑΕ. μπορεί να ενημερώσει τους στόχους των ερευνών, υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός της έρευνας¹⁰⁷. Το δικαίωμα του ατόμου να έχει πρόσβαση σε πληροφορίες σχετικά με το κατά πόσον το εν λόγω πρόσωπο αποτέλεσε αντικείμενο παρακολούθησης περιγράφεται στον νόμο 2472/1997¹⁰⁸. Ωστόσο, όταν τον Μάρτιο του 2021 η ΑΔΑΕ κοινοποίησε στην ΕΥΠ το δικαίωμα ενημέρωσης του Κουκάκη, η κυβέρνηση κατέθεσε αμέσως την τροποποίηση

¹⁰¹ ICLG. [Cybersecurity Laws and Regulation Greece 2022](#).

¹⁰² Efsyn. [What \(does not\) change with the Act of Legislative Content for EYP](#).

¹⁰³ Kathemirini. [Themistoklis Demiris: His appointment to the management of EYP was approved by a majority](#).

¹⁰⁴ Ekathimerini. [National security takes center stage](#).

¹⁰⁵ Greek City Times. [Greek PM appoints new security and intelligence chiefs](#).

¹⁰⁶ Euractiv. [Another Greek opposition lawmaker victim of Predator](#).

¹⁰⁷ Constitutionalism. [Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications](#).

¹⁰⁸ Dpa. [Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data](#).

826/145 στις 31 Μαρτίου 2021, με την οποία καταργήθηκε η δυνατότητα της ΑΔΑΕ. να ενημερώνει τους πολίτες για την άρση του απορρήτου των επικοινωνιών¹⁰⁹. Τούτο στερεί εκ των πραγμάτων από το άτομο το δικαίωμά του στην ενημέρωση. Η τροποποίηση εισήχθη με εξαιρετικά παράτυπο τρόπο. Προστέθηκε σε έναν εντελώς άσχετο νόμο (νομοσχέδιο για τα μέτρα covid) και δεν τηρήθηκαν οι προθεσμίες που απαιτούνται από το Σύνταγμα¹¹⁰¹¹¹¹¹². Ως εκ τούτου, δεν υπήρξε κατάλληλη διαδικασία διαβούλευσης.

57. Οι δυνατότητες κατασταλτικού ελέγχου αποδυναμώνονται περαιτέρω από το γεγονός ότι η Ελλάδα δεν έχει ακόμη εφαρμόσει πλήρως την οδηγία της ΕΕ για τους μάρτυρες δημοσίου συμφέροντος¹¹³.

Δημόσιος έλεγχος

58. Η Ελλάδα κατατάσσεται στη χαμηλότερη θέση μεταξύ όλων των χωρών της ΕΕ στον Παγκόσμιο Δείκτη Ελευθερίας του Τύπου για το 2022: 108η στις 180¹¹⁴. Το 2021 δολοφονήθηκε ο δημοσιογράφος Γιώργος Καραϊβάζ. Η δολοφονία δεν έχει ακόμη επιλυθεί. Οι δημοσιογράφοι αντιμετωπίζουν εκφοβισμό και στρατηγικές αγωγές προς αποθάρρυνση της συμμετοχής του κοινού. Ο Γρηγόρης Δημητριάδης¹¹⁵ υπέβαλε στρατηγικές αγωγές κατά της συμμετοχής του κοινού κατά των ειδησεογραφικών πρακτορείων Reporters United και «Εφημερίδα των Συντακτών» (Εφ.Συν)¹¹⁶ αφού αναγκάστηκε να παραιτηθεί. Ο υπουργός Οικονομίου επιδίωξε να δυσφημίσει την δημοσιογράφο του Politico, Νεκταρία Σταμούλη, υπονοώντας ότι τα άρθρα της σχετικά με το σκάνδαλο του κατασκοπευτικού λογισμικού ήταν πολιτικά υποκινούμενα¹¹⁷. Όντως, δύο από τα θύματα του Predator, οι Κουκάκης και Μαλιχούδης, είχαν κάνει επικριτικά ρεπορτάζ σχετικά με υποθέσεις διαφθοράς και απάτης, καθώς και την κακομεταχείριση των μεταναστών. Ο Τάσος Τέλλογλου και η Ελίζα Τριανταφύλλου αναφέρθηκαν στο σκάνδαλο του κατασκοπευτικού λογισμικού και εικάζεται ότι τέθηκαν υπό παρακολούθηση¹¹⁸.

Μέσα προσφυγής

Η Εθνική Αρχή Διαφάνειας

59. Στις 22 Ιουλίου 2022, η Εθνική Αρχή Διαφάνειας (ΕΑΔ) ξεκίνησε έρευνα σχετικά με την εικαζόμενη αγορά του κατασκοπευτικού λογισμικού Predator από το Υπουργείο Προστασίας του Πολίτη και την ΕΥΠ. Στο πλαίσιο του ελέγχου εξετάστηκαν η Ελληνική Αστυνομία, η ΕΥΠ και οι εταιρείες Intellexa και Krikel. Η ΕΑΔ ολοκλήρωσε την έκθεσή της στις 10 Ιουλίου 2022, αλλά υπέβαλε την έκθεση στην ΕΥΠ για προηγούμενη έγκριση. Η επίσημη έκθεση που εστάλη στον Κουκάκη στις 22 Ιουλίου

¹⁰⁹ <https://www.reportersunited.gr/8646/eyp-koukakis/>

¹¹⁰ Hellenic Parliament. [Constitution](#).

¹¹¹ Hellenic Parliament. [Rules of Procedure of the House](#).

¹¹² Govwatch. [Violation of the legislative process for amendments in law 4790/2021](#).

¹¹³ https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768

¹¹⁴ <https://rsf.org/en/index>

¹¹⁵ Tagesspiegel. .

¹¹⁶ EUobserver. [Greece accused of undermining rule of law in wiretap scandal](#).

¹¹⁷ <https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/>

¹¹⁸ Heinrich-Böll-Stiftung. [In conditions of absolute loneliness](#).

περιλάμβανε μόνο κλάσματα του πλήρους ελέγχου που διενεργήθηκε από την ΕΑΔ. Στο πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα, αφαιρέθηκαν διάφορα ονόματα από την έκθεση, συμπεριλαμβανομένων των ονομάτων των ελεγκτών της ΕΑΔ, του εισαγγελέα της ΕΥΠ που έλεγξε την αρχική έκθεση της ΕΑΔ και των δικηγόρων και λογιστών των εμπλεκόμενων νομικών προσώπων¹¹⁹.

60. Η έκθεση της ΕΑΔ κατέληξε στο συμπέρασμα ότι τόσο η ΕΥΠ όσο και το Υπουργείο Προστασίας του Πολίτη δεν είχαν συνάψει συμβάσεις με την Intellexa και άλλες συνδεδεμένες εθνικές εταιρείες. Επίσης, δεν είχαν αγοράσει ούτε χρησιμοποιήσει το κατασκοπευτικό λογισμικό Predator¹²⁰. Ωστόσο, η ΕΑΔ δεν διερεύνησε τους τραπεζικούς λογαριασμούς της Intellexa και της Krikel, ούτε τις συνδεδεμένες υπεράκτιες εταιρείες. Επιπλέον, η ΕΑΔ επισκέφθηκε τα γραφεία της Intellexa και του Krikel μόνο μετά από 2 μήνες, οπότε οι εργαζόμενοι εργάζονταν κατ' οίκον λόγω της πανδημίας COVID-19. Επιπρόσθετα, η ΕΑΔ δεν συναντήθηκε με νόμιμους εκπροσώπους των εν λόγω εταιρειών¹²¹.
61. Υπάρχουν ερωτηματικά σχετικά με την ανεξαρτησία της ηγεσίας της ΕΑΔ. Πρόσφατα, η ΕΑΔ έγινε πρωτοσέλιδο καθώς διατυπώθηκαν υπόνοιες για φιλοκυβερνητική μεροληψία κατά την εκπόνηση έκθεσης σχετικά με τις επαναπροωθήσεις μεταναστών¹²². Ο διευθυντής της ΕΑΔ, πρώην υπάλληλος του Μητσοτάκη, δεν συναντήθηκε με την PEGA κατά τη διάρκεια της αποστολής τον Νοέμβριο του 2022.

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

62. Τον Ιούλιο του 2022, ο Νίκος Ανδρουλάκης επιβεβαίωσε ότι είχε υποβάλει καταγγελία στην Εισαγγελία Αρείου Πάγου ότι φέρεται να στοχοποιήθηκε με το κατασκοπευτικό λογισμικό Predator στις 21 Σεπτεμβρίου 2021. Μετά την καταγγελία του Ανδρουλάκη, η ΑΔΑΕ δρομολόγησε έρευνα τον Αύγουστο του 2022, ξεκινώντας με τη λήψη πληροφοριών από τον τηλεπικοινωνιακό πάροχο του Ανδρουλάκη.

Επιτροπή Θεσμών και Διαφάνειας

63. Τον Ιούλιο του 2022, η Επιτροπή Θεσμών και Διαφάνειας κάλεσε τον Κοντολέοντα και τον πρόεδρο της ΑΔΑΕ, Χρήστο Ράμμο σε κοινοβουλευτική ακρόαση. Κατά τη διάρκεια της ακρόασης αυτής, ο Κοντολέων παραδέχθηκε ότι η ΕΥΠ είχε κατασκοπεύσει τον Θανάση Κουκάκη για λόγους εθνικής ασφάλειας, αλλά δήλωσε ότι δεν γνώριζε την απόπειρα χάκινγκ της συσκευής του Ανδρουλάκη με το Predator. Ο κυβερνητικός εκπρόσωπος, Γιάννης Οικονόμου ανέφερε ότι οι ελληνικές αρχές δεν απέκτησαν ούτε χρησιμοποίησαν ποτέ το κατασκοπευτικό λογισμικό Predator¹²³.

Κοινοβουλευτική εξεταστική επιτροπή

¹¹⁹ InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case.](#)

¹²⁰ InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case.](#)

¹²¹ InsideStory. [From Koukakis to Androulakis: A new twist in the Predator Spyware case.](#)

¹²² <https://www.politico.eu/article/greek-transparency-agency-report-data-breach-migration-european-commission/>

¹²³ Reuters. [Greek intelligence service admits spying on journalist - sources.](#)

64. Η πρόταση του κόμματος ΠΑΣΟΚ-ΚΙΝΑΛ για τη σύσταση εξεταστικής επιτροπής σχετικά με την εικαζόμενη χρήση κατασκοπευτικού λογισμικού¹²⁴ εγκρίθηκε από 142 βουλευτές της αντιπολίτευσης, ενώ οι 157 βουλευτές της Νέας Δημοκρατίας απείχαν¹²⁵. Ωστόσο, η ΝΔ είχε απόλυτη πλειοψηφία στην εξεταστική επιτροπή. Οι εκκλήσεις για ένα διμερές Προεδρείο απορρίφθηκαν. Η ΝΔ καθόρισε το πρόγραμμα εργασίας και τον κατάλογο των μαρτύρων που θα κληθούν, και απέρριψε αρκετούς από τους μάρτυρες που πρότειναν τα κόμματα της αντιπολίτευσης. Η επιτροπή συστάθηκε στις 29 Αυγούστου 2022. Άρχισε τις εργασίες της στις 7 Σεπτεμβρίου 2022 και ολοκλήρωσε τις εργασίες της στις 10 Οκτωβρίου 2022.
65. Η κυβερνητική πλειοψηφία στην επιτροπή αρνήθηκε να προσκαλέσει τους Μπίτζιο και Λαβράνο, αλλά προσκάλεσε τον Σταμάτη Τρίμπαλη —νυν διαχειριστή της Krikel— και τη Sara Hamou. Στις 22 Σεπτεμβρίου, ο Τρίμπαλης κατέθεσε ενώπιον της εν λόγω κοινοβουλευτικής επιτροπής. Ο Τρίμπαλης παρουσίασε κατάφωρα ψευδείς πληροφορίες σχετικά με τη συμμετοχή του Μπίτζιου και του Λαβράνου στην Krikel, ισχυριζόμενος, μεταξύ άλλων, ότι ο ίδιος ήταν ιδιοκτήτης της Krikel¹²⁶.
66. Μία μάρτυρας, η Sarah Hamou της Intellexa, ισχυρίστηκε ότι δεν είναι σε θέση να εμφανιστεί αυτοπροσώπως (αν και ζει στην Κύπρο), και της επετράπη να υποβάλει γραπτές απαντήσεις. Δεδομένου ότι δεν κατέστη δυνατή η εξαγωγή κοινών συμπερασμάτων, κάθε μέρος δημοσίευσε τη δική του έκθεση. Περίπου 5 500 σελίδες εγγράφων, συμπεριλαμβανομένων των πρακτικών και της κατάθεσης της Χάμου έχουν διαβαθμιστεί, αν και εμπίπτει εξ ολοκλήρου στην αρμοδιότητα του Κοινοβουλίου να τα αποχαρκτηρίσει. Παραδόξως, επομένως, η εξεταστική επιτροπή χρησιμεύει για την προστασία των πληροφοριών, και όχι για την παροχή πρόσβασης σε αυτές.

Οι στόχοι

67. Κατά τον χρόνο σύνταξης του παρόντος εγγράφου, είχε δημοσιευθεί κατάλογος 33 ονομάτων στόχων. Δεν είναι δυνατή η λεπτομερής ανάλυση και δεν έχουν κινηθεί ακόμη επίσημες έρευνες. Ωστόσο, η ανάλυση των λίγων περιπτώσεων που είναι γνωστές μέχρι στιγμής παρέχει μια αρκετά σαφή εικόνα των υπό εξέταση ζητημάτων.

Θανάσης Κουκάκης

68. Το καλοκαίρι του 2020, η ΕΥΠΗ έθεσε υπό παρακολούθηση τις τηλεφωνικές συνδιαλέξεις του δημοσιογράφου Θανάση Κουκάκη. Κατά τη διάρκεια της περιόδου αυτής, έκανε ρεπορτάζ για οικονομικά θέματα, μεταξύ των οποίων το σκάνδαλο της Libra/Τράπεζας Πειραιώς, στο οποίο εμπλέκεται ο Φέλιξ Μπίτζιος, και την εικαζόμενη φοροδιαφυγή του Έλληνα επιχειρηματία Γιάννη Λαβράνου, καθώς και αμφιλεγόμενους τραπεζικούς νόμους που θεσπίστηκαν από την κυβέρνηση Μητσοτάκη, οι οποίοι παρεμπόδιζαν τη δίωξη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και άλλων οικονομικών παραπτωμάτων (πράγματι, η αναδρομική ισχύς είχε ως αποτέλεσμα την εγκατάλειψη δώδεκα εκκρεμών υποθέσεων)¹²⁷. Ο Κουκάκης ερευνούσε επίσης την προμήθεια νέων δελτίων ταυτότητας, όπου οι Λαβράνος και Μπίτζιος είχαν επιχειρηματικό συμφέρον. Κοντά στην ημερομηνία που Κουκάκης παρουσιάστηκε για

¹²⁴ Tovina. [Interceptions: Committee of Inquiry to monitor Androulakis - Pasok's proposal in detail.](#)

¹²⁵ Tovina. [Parliament: The examination for the attendances from 2016 was passed - With 142 'yes'.](#)

¹²⁶ TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.](#)

¹²⁷ Inside Story. [Who was tracking the mobile phone of journalist Thanasis Koukakis.](#)

πρώτη φορά ενώπιον της επιτροπής PEGA, η πρόσκληση υποβολής προσφορών ξαφνικά αποσύρθηκε και παραιτήθηκε ο αρμόδιος γενικός γραμματέας.

Νίκος Ανδρουλάκης

69. Στις 21 Σεπτεμβρίου 2021, ο Νίκος Ανδρουλάκης, ηγέτης του κεντροαριστερού ΠΑΣΟΚ-ΚΙΝΑΛ και βουλευτής του Ευρωπαϊκού Κοινοβουλίου, στοχοποιήθηκε με το κατασκοπευτικό λογισμικό του Predator όταν στάλθηκε κακόβουλη σύνδεση στο τηλέφωνό του¹²⁸. Ο Ανδρουλάκης έλαβε ένα μήνυμα το οποίο έγραφε «Let's get a little serious, man, we've got a lot to gain». Επιπλέον, το μήνυμα περιλάμβανε σύνδεσμο για την εγκατάσταση του κατασκοπευτικού λογισμικού Predator στο τηλέφωνό του, αλλά, σε αντίθεση με τον Κουκάκη, ο Ανδρουλάκης δεν έκανε κλικ στον σύνδεσμο που του είχε αποσταλεί¹²⁹.
70. Η παρακολούθηση ενός πολιτικού είναι εξαιρετικά ασυνήθιστη και το ελληνικό Σύνταγμα προβλέπει ειδική προστασία των πολιτικών. Η ΕΥΠ αρνείται οποιαδήποτε εμπλοκή στην παρακολούθηση με Predator. Η κυβέρνηση ανέφερε αρχικά ως πιθανά σενάρια ξένες δυνάμεις που υποτίθεται ότι ζήτησαν την παρακολούθηση των τηλεφωνικών συνδιαλέξεων του Ανδρουλάκη ή ότι λόγος μπορεί να ήταν η συμμετοχή του σε επιτροπή του ΕΚ αρμόδια για τις σχέσεις με την Κίνα. Καμία από αυτές τις υποθέσεις δεν ήταν ιδιαίτερα αξιόπιστη. Η παρακολούθηση πραγματοποιήθηκε σε πολιτικό πλαίσιο επικείμενων εκλογών. Οι δημοσκοπήσεις προέβλεπαν ότι η Νέα Δημοκρατία θα έχανε την απόλυτη πλειοψηφία της. Το ΠΑΣΟΚ θα ήταν το προτιμώμενο κόμμα συνεργασίας σε τυχόν συνασπισμό. Το φθινόπωρο του 2021 υπήρχαν τέσσερις υποψήφιοι για την ηγεσία του ΠΑΣΟΚ, καθένας από τους οποίους είχε διαφορετικές απόψεις σχετικά με έναν τέτοιο συνασπισμό. Λέγεται ότι ο Ανδρουλάκης ήταν ανοικτός στην ιδέα, αλλά όχι υπό την πρωθυπουργία του Μητσοτάκη. Ένας άλλος υποψήφιος, ο Ανδρέας Λοβέρδος, είχε υπηρετήσει νωρίτερα ως υπουργός σε συνασπισμό Νέας Δημοκρατίας-ΠΑΣΟΚ, και θεωρήθηκε ότι θα ήταν πιο υποστηρικτικός. Επίσης, γνώριζε τον Δημητριάδη. Ο Μανώλης Όθωνας, το δεξί χέρι ενός άλλου υποψηφίου, αναφέρθηκε επίσης ότι συγκαταλέγεται μεταξύ εκείνων που είχαν στενότερες σχέσεις με τη Νέα Δημοκρατία και τον Δημητριάδη. Η δημοσίευση του καταλόγου άλλων εικαζόμενων στόχων από την Documento ενισχύει την υποψία πολιτικών λόγων για την παρακολούθηση. Δεν υπάρχουν αποδείξεις για καμία από αυτές τις υποθέσεις, αλλά είναι σημαντικό αυτά τα ενδεχόμενα να διερευνηθούν και να αποκλειστούν όπου είναι δυνατόν.

Σταύρος Μαλιχούδης

71. Στις 13 Νοεμβρίου 2021, η Εφημερίδα των Συντακτών (Εφ.Συν) αποκάλυψε ότι η ΕΥΠ φέρεται να παρακολουθούσε τις τηλεφωνικές συνδιαλέξεις πολλών δημοσιογράφων που έκαναν ρεπορτάζ σχετικά με υποθέσεις προσφύγων. Εσωτερικό έγγραφο της ΕΥΠ έδειξε ότι η ΕΥΠ διέταξε την παρακολούθηση και τη συλλογή δεδομένων για τον Έλληνα δημοσιογράφο Σταύρο Μαλιχούδη¹³⁰¹³¹. Ο Μαλιχούδης έγραφε για ένα

¹²⁸ InsideStory. [From Koukakis to Androulakis: A new twist in the Predator spyware case.](#)

¹²⁹ Euractiv. [EU Commission alarmed by new spyware case against Greek socialist leader.](#)

¹³⁰ Efsyn. [Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ](#)

¹³¹ Solomon. [Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'.](#)

12χρονο παιδί από τη Συρία που εξαναγκάστηκε να ζήσει για αρκετούς μήνες σε στρατόπεδο κράτησης στην Κω¹³².

Χρήστος Σπίρτζης

72. Στις 15 Νοεμβρίου 2021, ο πρώην υπουργός Υποδομών και βουλευτής του κόμματος ΣΥΡΙΖΑ, Χρήστος Σπίρτζης στοχοποιήθηκε στο κινητό του τηλέφωνο με το κατασκοπευτικό λογισμικό Predator¹³³.

Τάσος Τέλλογλου, Ελίζα Τριανταφύλλου και Θεοδωρής Χονδρόγιαννος

73. Ο Τάσος Τέλλογλου και η Ελίζα Τριανταφύλλου εικάζεται ότι έχουν κατασκοπευθεί κατά τη διάρκεια των ερευνητικών τους εργασιών για το Inside Story.

Άλλοι στόχοι

74. Στις 29 Οκτωβρίου 2022 αναφέρθηκε ότι και άλλοι πολιτικοί είχαν στοχοποιηθεί με το κατασκοπευτικό λογισμικό Predator, συμπεριλαμβανομένου ενός υπουργού της κυβέρνησης ο οποίος δεν είχε καλές σχέσεις με τον πρωθυπουργό. Επιπλέον, ένα άλλο μέλος της Νέας Δημοκρατίας φέρεται να έλαβε σύνδεσμο για την εγκατάσταση του Predator¹³⁴. Ο κ. Οικονόμου —κυβερνητικός εκπρόσωπος— δήλωσε ότι το άρθρο δεν βασίζεται σε συγκεκριμένα αποδεικτικά στοιχεία¹³⁵.
75. Στις 5 και 6 Νοεμβρίου 2022, η Documento ανέφερε κατάλογο που περιείχε 33 ονόματα προσώπων που στοχοποιήθηκαν με κατασκοπευτικό λογισμικό Predator¹³⁶. Μεταξύ αυτών περιλαμβάνονταν πολλοί υψηλόβαθμοι πολιτικοί, συμπεριλαμβανομένων μελών της σημερινής κυβέρνησης, ο πρώην πρωθυπουργός Σαμαράς, ο πρώην Επίτροπος της ΕΕ Αβραμόπουλος, ο αρχισυντάκτης μιας φιλικής προς την κυβέρνηση εφημερίδας, και άτομα στο περιβάλλον του Βαγγέλη Μαρινάκη, πλοιοκτήτη, μεγιστάνα των μέσων ενημέρωσης και ιδιοκτήτη των ποδοσφαιρικών συλλόγων Ολυμπιακός και Nottingham Forest. Οι αποκαλύψεις του καταλόγου προκαλούν μεγάλη ανησυχία όχι μόνο λόγω των ιδιαίτερα προβεβλημένων ονομάτων που περιλαμβάνει, αλλά και επειδή υποδηλώνουν ότι η κατάχρηση του κατασκοπευτικού λογισμικού είναι συστηματική, μεγάλης κλίμακας και αποτελεί μέρος μιας πολιτικής στρατηγικής.

1.4. Κύπρος

76. Η Κύπρος αποτελεί σημαντικό ευρωπαϊκό εξαγωγικό κόμβο για τον κλάδο της παρακολούθησης. Στα χαρτιά, υπάρχει ένα ισχυρό νομικό πλαίσιο, συμπεριλαμβανομένων των κανόνων της ΕΕ, αλλά στην πράξη η Κύπρος αποτελεί ελκυστικό τόπο για τις εταιρείες που πωλούν τεχνολογίες παρακολούθησης. Ωστόσο, πρόσφατα σκάνδαλα έπληξαν τη φήμη της χώρας και αναμένεται να ολοκληρωθεί το

¹³² BalkanInsight. [Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.](#)

¹³³ Ekathimerini. [Former SYRIZA minister says he was targeted by Predator.](#)

¹³⁴ Ta Nea. [Four illegal manipulations by suspicious center.](#)

¹³⁵ Politico. [Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.](#)

¹³⁶ Documento, edition 6 November 2022.

2023 μια σειρά νέων νομοθετικών πρωτοβουλιών για την αυστηροποίηση του νομικού πλαισίου για τις εξαγωγές και τη βελτίωση της συμμόρφωσης.

77. Στα χαρτιά, υπάρχει νομικό πλαίσιο που προβλέπει την προστασία των ιδιωτικών επικοινωνιών, την επεξεργασία δεδομένων προσωπικού χαρακτήρα και το δικαίωμα του ατόμου στην ενημέρωση. Ωστόσο, στην πράξη, όταν γίνεται επίκληση της εθνικής ασφάλειας, δεν υπάρχουν σαφείς κανόνες που να προβλέπουν τη χρήση συσκευών παρακολούθησης και την προστασία των συνταγματικών δικαιωμάτων των πολιτών.
78. Η Κύπρος φαίνεται να έχει πολύ στενή συνεργασία με το Ισραήλ στον τομέα των τεχνολογιών παρακολούθησης. Η Κύπρος διαβουλευθήκε με το Ισραήλ και τις ΗΠΑ σχετικά με τη μεταρρύθμιση του νομικού της πλαισίου. Η Κύπρος είναι δημοφιλής προορισμός για πολλές ισραηλινές εταιρείες κατασκοπευτικού λογισμικού.

Νομικό πλαίσιο

Κανονισμός για τα είδη διπλής χρήσης

79. Σε σύγκριση με το ισχύον νομικό πλαίσιο, η Κύπρος φέρεται να είναι μάλλον επιεικής όσον αφορά την παροχή αδειών εξαγωγής σε εταιρείες κατασκοπευτικού λογισμικού¹³⁷. Οι εταιρείες χρησιμοποιούν τεχνάσματα για να παρακάμπτουν τους κανόνες. Δηλαδή, το υλισμικό του προϊόντος αποστέλλεται σε αποδέκτρια χώρα χωρίς να έχει φορτωθεί το λογισμικό σε αυτό¹³⁸. Στη συνέχεια, το λογισμικό ενεργοποίησης (το οποίο αναφέρεται επίσης ως «κλειδί άδειας») αποστέλλεται χωριστά μέσω ενός USB στη χώρα προορισμού¹³⁹. Ένας άλλος τρόπος είναι να δηλωθεί ότι το προϊόν εξάγεται μόνο για σκοπούς επίδειξης, αν και προστίθεται λεπτομερής περιγραφή του προϊόντος¹⁴⁰.
80. Πολλές ισραηλινές εταιρείες έρχονται στην Κύπρο για να ξεκινήσουν την ευρωπαϊκή τους δραστηριότητα¹⁴¹. Διάφορες πηγές ανέφεραν επίσης ότι η χώρα φιλοξενεί περίπου 29 ισραηλινές εταιρείες¹⁴². Το εμπόριο κατασκοπευτικού λογισμικού και οι διπλωματικές σχέσεις συνδέονται στενά. Ως αντάλλαγμα για τη διευκόλυνση των αδειών για ισραηλινές εταιρείες, η Κύπρος φέρεται να έχει λάβει ορισμένα από τα προϊόντα που αναπτύσσουν και εξάγουν οι εν λόγω εταιρείες, όπως το κατασκοπευτικό λογισμικό Pegasus από την NSO¹⁴³, καθώς και υλικό κατασκοπευτικού λογισμικού από την WiSpear¹⁴⁴.

Εκ των προτέρων έλεγχος

¹³⁷ InsideStory. [Who signs the exports of spyware from Greece and Cyprus?](#)

¹³⁸ InsideStory. [Who signs the exports of spyware from Greece and Cyprus?](#)

¹³⁹ Philenews. [This is how interception patents are exported from Cyprus.](#)

¹⁴⁰ Philenews. [Export of monitoring software confirmed.](#)

¹⁴¹ Philenews. [Revelations in Greece: Predator came from Cyprus.](#)

¹⁴² Makarios Drousiotis. [Κράτος Μαφία](#). Chapter 6. Published 2022

¹⁴³ Makarios Drousiotis. [Κράτος Μαφία](#). Chapter 6. Published 2022.

¹⁴⁴ Inside Story. [Predator: The 'spy' who came from Cyprus.](#)

81. Ο νόμος για την προστασία του απορρήτου των ιδιωτικών επικοινωνιών 92 (I)/1996 ορίζει ότι η αίτηση για τη χορήγηση άδειας παρακολούθησης ιδιωτικών επικοινωνιών πρέπει να υποβάλλεται στο δικαστήριο¹⁴⁵.

Κατασταλτικός έλεγχος

82. Στα χαρτιά, η παραβίαση της προστασίας των ιδιωτικών επικοινωνιών συνιστά εκ του νόμου ποινικό αδίκημα. Εκ των πραγμάτων, η παρανομία αυτή συχνά κρύβεται πίσω από την επίκληση της εθνικής ασφάλειας¹⁴⁶. Δεν υπάρχει νομοθεσία που να καλύπτει τον τρόπο με τον οποίο η αστυνομία ή άλλες υπηρεσίες πληροφοριών χρησιμοποιούν τις συσκευές παρακολούθησης, ποιος ρυθμίζει τις διαδικασίες παρακολούθησης και τον τρόπο με τον οποίο διασφαλίζεται η προστασία των συνταγματικών δικαιωμάτων των πολιτών. Οι σχετικοί κανονισμοί και πρωτόκολλα εκκρεμούν επί του παρόντος στη Βουλή των Αντιπροσώπων προς συζήτηση και έγκριση. Προς το παρόν, οι διατάξεις αυτές εκφεύγουν του ελέγχου¹⁴⁷.

Μέσα προσφυγής

83. Ο πρόεδρος της Κύπρου έχει σημαντικό λόγο στον σχηματισμό της επιτροπής που είναι σε θέση να ξεκινήσει έρευνες για τις ενέργειες της ΚΥΠ. Επιπλέον, οι ετήσιες εκθέσεις με τα πορίσματα της επιτροπής αποστέλλονται πρώτα στον Πρόεδρο¹⁴⁸.

Βασικά πρόσωπα στον κλάδο του κατασκοπευτικού λογισμικού

84. Ο Tal Dilian έχει διαδραματίσει καίριο ρόλο σε πολλές από τις εξελίξεις που σημειώθηκαν στην Κύπρο και την Ελλάδα. Απέκτησε τη μαλτέζικη ιθαγένεια το 2017¹⁴⁹. Επίσης, υπηρέτησε σε διάφορες ηγετικές θέσεις στην Ισραηλινή Αμυντική Δύναμη για 25 χρόνια προτού αποστρατευθεί το 2002¹⁵⁰. Ξεκινώντας τη σταδιοδρομία του ως «εμπειρογνώμονας σε θέματα πληροφοριών, δημιουργός κοινοτήτων και κατά συρροήν επιχειρηματίας» στην Κύπρο, ο Dilian ίδρυσε την Aveledo Ltd., αργότερα γνωστή ως Ws WiSpear Systems ltd. και μετά, ως Passitora Ltd¹⁵¹.
85. Στην Κύπρο, ο Dilian συνεργάστηκε στενά με τον Abraham Sahak Avni. Ο Avni έχει συνεργαστεί στο παρελθόν με τις Ειδικές Δυνάμεις της Ισραηλινής Αστυνομίας ως ειδικός ντετέκτιβ¹⁵². Τον Νοέμβριο του 2015 απέκτησε την κυπριακή ιθαγένεια και ένα χρυσό διαβατήριο λόγω επένδυσης ύψους 2,9 εκατομμυρίων EUR σε ακίνητα¹⁵³. Ο Avni ίδρυσε την κυπριακή NCIS Intelligence Services ltd¹⁵⁴, εταιρεία η οποία φέρεται

¹⁴⁵ CyLaw. [The Protection of Privacy of Private Communications \(Interception and Access to Recorded Private Communications Content\) Law of 1996 \(92\(I\)/1996\)](#)

¹⁴⁶ Makarios Drousiotis. [Κράτος Μαφία..](#) Chapter 6. Published 2022.

¹⁴⁷ Philenews. [Legal but uncontrolled interceptions.](#)

¹⁴⁸ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁴⁹ Government of Malta. Persons Naturalised Registered Gaz 21.12

<https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf>

¹⁵⁰ <https://taldilian.com/about/>

¹⁵¹ Opencorporates. [Passitora ltd.](#)

¹⁵² ShahakAvni. [About Shahak Avni.](#)

¹⁵³ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁵⁴ Philenews. [FILE: The state insulted Avni and Dilian.](#)

να εμπλέκεται με τις ισχυρότερες εταιρείες με τεχνολογικό προσανατολισμό στον κόσμο¹⁵⁵. Η NCIS παρείχε λογισμικό ασφαλείας στο Αρχηγείο της Αστυνομίας από το 2014 έως το 2015 και κατάρτισε υπαλλήλους του Γραφείου Εγκληματολογικής Ανάλυσης και Στατιστικής μεταξύ 2015 και 2016¹⁵⁶. Το κυβερνητικό κόμμα ΔΗΣΥ (Δημοκρατικός Συναγερμός) συγκαταλέγεται επίσης στους πελάτες της εταιρείας. Σύμφωνα με πληροφορίες, ο Avni είχε εγκαταστήσει εξοπλισμό ασφαλείας στα γραφεία του κόμματος¹⁵⁷. Εκτός από τον εξοπλισμό ασφαλείας του Avni, εξοπλισμός του Dilian πωλήθηκε επίσης στο Γραφείο Καταστολής Ναρκωτικών και στην Αστυνομία Της Κύπρου¹⁵⁸.

86. Οι συνδέσεις μεταξύ Dilian και Avni είναι πολυάριθμες. Η εταιρεία WiSpear του Dilian μοιραζόταν ένα κτίριο στη Λάρνακα και μέρος του προσωπικού της με τον Avni¹⁵⁹. Το 2018, οι δύο άνδρες ίδρυσαν την εταιρεία Poltrex, η οποία μετονομάστηκε αργότερα σε Alchemycorp Ltd. Η Poltrex φιλοξενείται στον Novel Tower τον οποίο μοιράζεται με τον Avni¹⁶⁰ και αποτελεί επίσης μέρος της Intellexa Alliance. Σύμφωνα με πληροφορίες, οι σχέσεις του Avni με το κόμμα ΔΗΣΥ δημιούργησαν το πεδίο δοκιμής για τα προϊόντα του Dilian¹⁶¹.

Κατασκοπευτικό βαν του Ντίλιαν

87. Μετά την πώληση της εταιρείας Circles technologies και την ίδρυση της WiSpear, ο Tal Dilian ίδρυσε επιπλέον το 2019 την Intellexa Alliance, η οποία περιγράφεται στον ιστότοπο ως «εταιρεία με έδρα στην ΕΕ και ρυθμιζόμενη από το δίκαιο της ΕΕ με σκοπό την ανάπτυξη και την ενσωμάτωση τεχνολογιών για την ενδυνάμωση των υπηρεσιών πληροφοριών»¹⁶². Υπάρχουν διάφοροι προμηθευτές εξοπλισμού παρακολούθησης που περιλαμβάνονται στην εμπορική επωνυμία της Intellexa Alliance, όπως η Cytrox, η WiSpear -που στη συνέχεια μετονομάστηκε σε Passitora Ltd.- η Nexa technologies και η Poltrex ltd. Αυτοί οι διαφορετικοί πωλητές που περιλαμβάνονται στην Intellexa Alliance του Dilian επιτρέπουν στην Intellexa να προσφέρει, μεταξύ άλλων και με διάφορους συνδυασμούς, ένα ευρύ φάσμα λογισμικού και υπηρεσιών παρακολούθησης στους πελάτες της¹⁶³. Λεπτομερέστερες πληροφορίες σχετικά με την εταιρική δομή περιλαμβάνονται στο κεφάλαιο για τη βιομηχανία κατασκοπευτικού λογισμικού.
88. Μετά τις καταγγελίες κατά του Dilian, κατέστη σαφές ότι η ισραηλινή εταιρεία Go Networks συνδεόταν, σύμφωνα με πληροφορίες, με την Intellexa μέσω εταιρικής συνιδιοκτησίας στην Ιρλανδία. Εικάζεται ότι πρώην ανώτεροι εκπρόσωποι είχαν αναλάβει κορυφαία καθήκοντα στην Intellexa¹⁶⁴. Επιπλέον, οι αστυνομικές έρευνες διαπίστωσαν ότι είχαν χορηγηθεί άδειες εξαγωγής στην WiSpear για «εξοπλισμό

¹⁵⁵ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁵⁶ Philenews. [FILE: The state insulted Avni and Dilian.](#)

¹⁵⁷ Tovima. [The unknown “bridge” between Greece and Cyprus for the eavesdropping system.](#)

¹⁵⁸ Inside Story. [Predator: The “spy” who came from Cyprus.](#)

¹⁵⁹ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁶⁰ CyprusMail. [Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal.](#)

¹⁶¹ Inside Story. [Predator: The “spy” who came from Cyprus.](#)

¹⁶² <https://intellexa.com/>

¹⁶³ Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

¹⁶⁴ Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

υποκλοπών σχεδιασμένο για την εξαγωγή φωνής ή δεδομένων, που μεταδίδονται διαμέσου της ραδιοδιεπαφής»¹⁶⁵¹⁶⁶.

89. Το 2011, ο Avni ίδρυσε εταιρεία με τον Μιχαήλ Αγγελίδη, αδελφό του πρώην υπουργού και νυν αναπληρωτή γενικού εισαγγελέα Σάββα Αγγελίδη. Η εταιρεία τους, S9S, καταχωρίστηκε στο μητρώο εταιρειών στις 10 Νοεμβρίου 2011¹⁶⁷ με τη βοήθεια του πρώην δικηγορικού γραφείου του Σάββα Αγγελίδη¹⁶⁸. Ωστόσο, η εταιρική τους σχέση λύθηκε το 2012. Ωστόσο, ο Σάββας Αγγελίδης ήταν ο υπεύθυνος για τον έλεγχο των Avni και Dillian στην περίπτωση του βαν παρακολούθησης¹⁶⁹.
90. Το κόμμα της αντιπολίτευσης ΑΚΕΛ εξέφρασε την οργή του για το γεγονός ότι οι υποθέσεις κατά του Dillian και του προσωπικού που αποσύρθηκαν, και κατήγγειλε τη νομική απόφαση ως συγκάλυψη από τον γενικό εισαγγελέα¹⁷⁰. Άλλωστε, σύμφωνα με πληροφορίες, η κυπριακή κυβέρνηση είχε αγοράσει εξοπλισμό από την εταιρεία του Dillian και ένας από τους κατηγορούμενους υπαλλήλους είχε εργαστεί για λογαριασμό της NSO, παρέχοντας στην ΚΥΠ οδηγίες σχετικά με τον τρόπο χρήσης του κατασκοπευτικού λογισμικού Pegasus¹⁷¹. Η απόσυρση των κατηγοριών διασφάλισε την προστασία των πληροφοριών σχετικά με τους δεσμούς μεταξύ της εταιρείας του Dillian και της κυπριακής κυβέρνησης¹⁷². Το παράδειγμα αυτό δείχνει ότι η προστασία των δεδομένων των προσώπων ενάντια σε παραβιάσεις από εξοπλισμό μαζικής παρακολούθησης δεν διασφαλίζεται πλήρως. Ενώ στο χαρτί υπάρχουν μέσα προσφυγής, τα δικαστικά αποτελέσματα επηρεάζονται από κυβερνητικές παρεμβάσεις, αφήνοντας απροστάτευτο το μεμονωμένο θύμα.

Η μεταφορά στην Ελλάδα

91. Μετά το επεισόδιο με το βαν και την αγωγή, ο Dillian μετέφερε τις δραστηριότητες της Intellexa στην Ελλάδα, αν και δεν εγκατέλειψε ποτέ την Κύπρο και εξακολουθεί να είναι κάτοικος. Οι έμμεσες σχέσεις μεταξύ διαφόρων φυσικών και νομικών προσώπων όπως είναι καταχωρισμένα στην Κύπρο και την Ελλάδα αποκαλύπτουν τη διευκόλυνση των επιχειρήσεων του Dillian στην Αθήνα¹⁷³.
92. Σύμφωνα με πρόσφατες μαρτυρίες υπό το φως των δικαστικών ερευνών στην υπόθεση του βαν, ο δικηγόρος Αλέξανδρος Σίνκα είχε σημαντική επιρροή στη μεταφορά στην Ελλάδα. Ο Sinka —ο οποίος στο παρελθόν διαδραμάτισε καίριο ρόλο στο κεντροδεξιό κόμμα ΔΗΣΥ— είχε προφανώς καλές σχέσεις τόσο με τον Dillian όσο και με τον Avni¹⁷⁴. Φαίνεται ότι ο Σίνκα γνώριζε επίσης τον Δημητριάδη, τον πρώην γενικό γραμματέα της ελληνικής κυβέρνησης. Και οι δυο τους κατείχαν θέσεις στο Προεδρείο των Ευρωπαίων Δημοκρατών Φοιτητών, της φοιτητικής οργάνωσης του Ευρωπαϊκού Λαϊκού Κόμματος (ΕΛΚ). Μεταξύ 2003 και 2004, ο Σίνκα διετέλεσε πρόεδρος και ο

¹⁶⁵ Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.

¹⁶⁶ Philenews. Export of tracking software from Cyprus.

¹⁶⁷ Politis. “Interceptions” file: Classified Police Report (2016) shows he knew everything about Avni

¹⁶⁸ Press Release Deputy Attorney General of 10.08.2022 as acquired on the PEGA mission to Cyprus on 02.11.2022.

¹⁶⁹ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁷⁰ Financial Mirror. Anger after ‘spy van’ charges dropped.Le

¹⁷¹ Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

¹⁷² Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.

¹⁷³ Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

¹⁷⁴ Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.

Δημητριάδης αντιπρόεδρος¹⁷⁵. Ο Δημητριάδης φέρεται να σύστησε τον φίλο του και Έλληνα επιχειρηματία Φέλιξ Μπίτζιο στον Σίνκα, λόγω της μακροχρόνιας διαμάχης του Μπίτζιου ενόπιον κυπριακού δικαστηρίου. Ο Σίνκα με τη σειρά του συνέστησε τον δικηγόρο Χάρη Κυριακίδη για να βοηθήσει τον Μπίτζιο στη διαμάχη του. Ο Κυριακίδης επίσης είχε καλές σχέσεις με το ΔΗΣΥ¹⁷⁶.

Όμιλος NSO και Κύπρος

93. Εκτός από την Intellexa Alliance, η Κύπρος φέρεται να φιλοξενούσε και τον όμιλο NSO. Το 2010, ο Tal Dilian, μαζί με τους Boaz Goldman και Eric Banoun, ίδρυσαν την εταιρεία Circles Technologies, η οποία ειδικευόταν στην πώληση συστημάτων που εκμεταλλεύονται τρωτά σημεία της SS7¹⁷⁷. Έξι χρόνια αργότερα, η Circles Technologies πωλήθηκε στην Francisco Partners έναντι σχεδόν 130 εκατομμυρίων δολαρίων, εκ των οποίων 21,5 εκατομμύρια δολάρια διατέθηκαν στον Dilian. Η εν λόγω εταιρεία επενδύσεων ιδιωτικών κεφαλαίων με έδρα την Καλιφόρνια απέκτησε ομοίως το 90 % του ομίλου NSO, με αποτέλεσμα τη συγχώνευση της Circles Technologies και του ομίλου NSO υπό την επωνυμία L.E.G.D Company Ltd., γνωστή ως Q Cyber Technologies Ltd. από τις 29 Μαρτίου 2016¹⁷⁸.
94. Ωστόσο, ο ισχυρισμός της κυπριακής κυβέρνησης που αρνείται την εξαγωγή και την ανάπτυξη του Pegasus στη χώρα φαίνεται ότι δεν ισχύει. Στις 21 Ιουνίου 2022, ο υπάλληλος Chaim Gelfad της NSO δήλωσε ότι οι εταιρείες του ομίλου NSO στην Κύπρο και τη Βουλγαρία ασχολούνται με λογισμικό που παρέχει υπηρεσίες πληροφοριών¹⁷⁹. Σύμφωνα με έγγραφο που κοινοποίησε το κόμμα της αντιπολίτευσης ΑΚΕΛ στο Ευρωπαϊκό Κοινοβούλιο, ο όμιλος NSO φέρεται να εξήγαγε το κατασκοπευτικό λογισμικό Pegasus μέσω μιας από τις θυγατρικές του στην Κύπρο σε εταιρεία στα Ηνωμένα Αραβικά Εμιράτα. Μία από τις θυγατρικές φαίνεται να έχει εκδώσει τιμολόγιο ύψους 7 εκατ. δολαρίων για υπηρεσίες προς την εν λόγω εταιρεία¹⁸⁰.
95. Σύμφωνα με πληροφορίες, ο όμιλος NSO είχε επίσης ενεργό εταιρεία στην Κύπρο, η οποία υποτίθεται ότι φιλοξενούσε κέντρο εξυπηρέτησης πελατών. Το 2017 πραγματοποιήθηκε συνάντηση με στελέχη της NSO και πελάτες από τη Σαουδική Αραβία στο ξενοδοχείο Four Seasons στη Λεμεσό για να τους παρουσιάσουν τις τελευταίες δυνατότητες του κατασκοπευτικού λογισμικού Pegasus 3. Η έκδοση αυτή είχε τη νέα δυνατότητα «χωρίς κλικ» (zero-click), πράγμα που σημαίνει ότι μπορούσε να μολύνει μια συσκευή χωρίς να χρειάζεται να γίνει κλικ σε σύνδεσμο, για παράδειγμα μέσω μιας αναπάντητης κλήσης WhatsApp. Οι Σαουδάραβες πελάτες αγόρασαν αμέσως την τεχνολογία για ποσό 55 εκατομμυρίων EUR¹⁸¹¹⁸². Στο σημείο αυτό θα πρέπει να σημειωθεί ότι ένα έτος αργότερα, στις 2 Οκτωβρίου 2018, το καθεστώς της Σαουδικής Αραβίας σκότωσε τον Jamal Khashoggi στο προξενείο της Σαουδικής Αραβίας στην Τουρκία, αφού είχε παρακολουθήσει αυτόν και τους οικείους του με το Pegasus.

¹⁷⁵ EDS. 2003/2004 Bureau.

¹⁷⁶ Tovima. [The unknown “bridge” between Greece and Cyprus for the eavesdropping system.](#)

¹⁷⁷ Amnesty International. [Operating from the Shadows.](#)

¹⁷⁸ Amnesty International. [Operating from the Shadows.](#)

¹⁷⁹ Report by Fanis Makridis. PEGA Mission to Cyprus on 01.11.2022.

¹⁸⁰ Akel report. PEGA mission to Cyprus.

¹⁸¹ Makarios Drousiotis. [Κράτος Μαφία..](#) Chapter 6. Published 2022.

¹⁸² Haaretz. [Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.](#)

Black Cube

96. Η Black Cube είναι εταιρεία που απασχολεί πρώην αξιωματικούς των ισραηλινών υπηρεσιών πληροφοριών, όπως η Mossad. Η εταιρεία χρησιμοποιεί πράκτορες με ψευδείς ταυτότητες. Σύμφωνα με το περιοδικό New Yorker, ο πρώην διευθύνων σύμβουλος του ομίλου NSO Shalev Hulio προσέλαβε τη Black Cube αφότου τρεις δικηγόροι— Mazen Masri, Alaa Mahajna και Χριστιάνα Μάρκου— κατέθεσαν μήνυση κατά της NSO και μιας συνδεδεμένης θυγατρικής της στο Ισραήλ και την Κύπρο¹⁸³.

Αγορά και χρήση κατασκοπευτικού λογισμικού από την Κύπρο

97. Εκτός από την καλλιέργεια ενός ευνοϊκού εξαγωγικού κλίματος για εταιρείες κατασκοπευτικού λογισμικού, η κυπριακή κυβέρνηση έχει η ίδια ιστορικό αγοράς κατασκοπευτικού λογισμικού. Εικάζεται επίσης ότι χρησιμοποίησε τα ίδια συστήματα παρακολούθησης. Κατά τον χρόνο σύνταξης του παρόντος εγγράφου, παραμένει ασαφές σε ποιες περιπτώσεις η Κύπρος έκανε χρήση συμβατικών μεθόδων παρακολούθησης ή κατασκοπευτικού λογισμικού.

Θύμα: Μακάριος Δρουσιώτης

98. Από τον Φεβρουάριο του 2018, εικάζεται ότι η κυπριακή κυβέρνηση κατασκόπευε τον δημοσιογράφο Μακάριο Δρουσιώτη. Η εν λόγω υπόθεση κατασκοπείας ξεκίνησε κατά τη διάρκεια της προηγούμενης θητείας του κ. Δρουσιώτη ως βοηθού του Κύπριου Επιτρόπου Ανθρωπιστικής Βοήθειας και Διαχείρισης Κρίσεων, Χρήστου Στυλιανίδη και κατά τη διάρκεια των ερευνών του σχετικά με τις οικονομικές σχέσεις μεταξύ του προέδρου Αναστασιάδη και προσωπικοτήτων της Ρωσίας, όπως ο ολιγάρχης Dmitri Rybolonlev. Σύμφωνα με τον Δρουσιώτη, ο τελευταίος αυτός ρόλος του ήταν αυτός που πυροδότησε την πρώτη απόπειρα παρακολούθησης¹⁸⁴.

Συμπληρωματικές παρατηρήσεις

99. Η Κύπρος φαίνεται να διαθέτει ισχυρό νομικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής, για την έγκριση της παρακολούθησης, και για τις εξαγωγές. Ωστόσο, στην πράξη, φαίνεται ότι οι κανόνες είναι εύκολο να παρακαμφθούν και υπάρχουν στενοί δεσμοί μεταξύ της πολιτικής, των υπηρεσιών ασφαλείας και της βιομηχανίας παρακολούθησης. Φαίνεται ότι η χαλαρή εφαρμογή των κανόνων είναι που καθιστά την Κύπρο τόσο ελκυστική για το εμπόριο κατασκοπευτικού λογισμικού. Η Κύπρος παρουσιάζει επίσης σημαντικό στρατηγικό ενδιαφέρον για τη Ρωσία, την Τουρκία και τις ΗΠΑ. Επιπλέον, οι στενές σχέσεις με το Ισραήλ φαίνεται να παρουσιάζουν ιδιαίτερο αμοιβαίο όφελος όσον αφορά το εμπόριο κατασκοπευτικού λογισμικού. Οι άδειες εξαγωγής για κατασκοπευτικό λογισμικό έχουν καταστεί νόμισμα στις διπλωματικές σχέσεις.

1.E Ισπανία

100. Οι αποκαλύψεις του Ιουλίου 2021 από το «Pegasus project» έδειξαν μεγάλο αριθμό στόχων στην Ισπανία. Ωστόσο, φαίνεται ότι στοχοποιήθηκαν από διάφορους φορείς και

¹⁸³ The New Yorker. How Democracies Spy on their Citizens.

¹⁸⁴ Makarios Drousiotis. Κράτος Μαφία. Chapter 5. Published 2022.

για διαφορετικούς λόγους. Πιστεύεται ευρέως ότι οι μαροκινές αρχές στοχοποίησαν τον πρωθυπουργό Pedro Sanchez, την υπουργό Άμυνας Margarita Robles και τον υπουργό Εσωτερικών Fernando Grande-Marlaska, παρόμοια με την περίπτωση του Γάλλου προέδρου και των υπουργών της κυβέρνησής του¹⁸⁵. Η στόχευση μιας δεύτερης ομάδας θυμάτων αναφέρεται ως «CatalanGate»¹⁸⁶. Περιλαμβάνει Καταλανούς βουλευτές, βουλευτές του Ευρωπαϊκού Κοινοβουλίου, δικηγόρους, μέλη οργανώσεων της κοινωνίας των πολιτών και ορισμένους συγγενείς και προσωπικό που συνδέεται με τα θύματα αυτά¹⁸⁷. Το σκάνδαλο παρακολούθησης «CatalanGate» αναφέρθηκε για πρώτη φορά το 2020, αλλά μόλις τον Απρίλιο του 2022 το Citizen Lab ολοκλήρωσε τη διεξοδική έρευνά του και τότε ήταν που αποκαλύφθηκε η κλίμακα του σκανδάλου. Τα αποτελέσματα της έρευνας αυτής έδειξαν ότι είχαν τεθεί στο στόχαστρο τουλάχιστον 65 άτομα¹⁸⁸. Τον Μάιο του 2020, οι ισπανικές αρχές παραδέχθηκαν ότι στόχευσαν 18 από τα εν λόγω 65 θύματα με έγκριση δικαστηρίου¹⁸⁹.

Αγορά κατασκοπευτικού λογισμικού

101. Η προηγούμενη αγορά διαφόρων προϊόντων κατασκοπευτικού λογισμικού όπως η SITEL το 2001 και το κατασκοπευτικό λογισμικό της Hacking Team το 2010 από το Υπουργείο Εσωτερικών, την Εθνική Υπηρεσία Πληροφοριών της Ισπανίας (CNI) και την αστυνομία έχουν δημοσιοποιηθεί ευρέως¹⁹⁰. Στο παρελθόν είχε επίσης αναφερθεί από το CitizenLab ότι υπήρχαν υποψίες πως η Ισπανία ήταν πελάτης της Finfisher¹⁹¹. Το 2020, η ισπανική εφημερίδα *El Pais* ανέφερε ότι η Ισπανία έχει συνεργαστεί με τον όμιλο NSO και ότι το CNI χρησιμοποιεί συστηματικά το Pegasus¹⁹². Η ισπανική κυβέρνηση φέρεται να αγόρασε το κατασκοπευτικό λογισμικό κατά το πρώτο ήμισυ της δεκαετίας του 2010 για εκτιμώμενο ποσό 6 εκατομμυρίων EUR¹⁹³¹⁹⁴. Επιπλέον, πρώην υπάλληλος της NSO επιβεβαίωσε περαιτέρω ότι η Ισπανία έχει λογαριασμό στην εταιρεία, παρά το γεγονός ότι οι ισπανικές αρχές αρνήθηκαν να σχολιάσουν ή να επιβεβαιώσουν¹⁹⁵.

¹⁸⁵ Le Monde, https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-phone-hacking_5982990_4.html, 10 May 2022.

¹⁸⁶ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022.

¹⁸⁷ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 1.

¹⁸⁸ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 1.

¹⁸⁹ El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

¹⁹⁰ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 4 - 5.

¹⁹¹ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 5.

¹⁹² Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 5.

¹⁹³ Politico, <https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/>, 20 April 2022.

¹⁹⁴ El Pais, <https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html>, 20 April 2022.

¹⁹⁵ The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

Νομικό πλαίσιο

102. Το δικαίωμα στην ιδιωτική ζωή προστατεύεται από το άρθρο 18 του ισπανικού Συντάγματος του 1978, συμπεριλαμβανομένου του δικαιώματος απορρήτου στην «ταχυδρομική, τηλεγραφική και τηλεφωνική επικοινωνία»¹⁹⁶. Η χρήση κατασκοπευτικού λογισμικού όπως το Pegasus και το Candiru συνιστά παραβίαση του άρθρου 18· ωστόσο, υπάρχει εξαίρεση από το δικαίωμα αυτό στην περίπτωση που υπάρχει έγκριση από δικαστήριο¹⁹⁷. Το Σύνταγμα προβλέπει επίσης περαιτέρω εξαιρέσεις στα εν λόγω δικαιώματα στο μέρος Ι τμήμα 55, ορίζοντας ότι ορισμένες ελευθερίες μπορούν να ανασταλούν με τη «συμμετοχή των δικαστηρίων και τον κατάλληλο κοινοβουλευτικό έλεγχο» στην περίπτωση προσώπων που ερευνώνται για δραστηριότητες που αφορούν ένοπλες ομάδες ή τρομοκρατικές οργανώσεις¹⁹⁸.
103. Η ισπανική υπηρεσία πληροφοριών αποτελείται από τρεις κύριες υπηρεσίες. Πρώτον, την Εθνική Υπηρεσία Πληροφοριών (CNI), η οποία τελεί υπό τον έλεγχο του Υπουργείου Άμυνας. Ο διευθυντής της CNI διορίζεται από τον υπουργό Άμυνας και ενεργεί ως επικεφαλής σύμβουλος του πρωθυπουργού σε θέματα που αφορούν τις πληροφορίες και την αντικατασκοπεία¹⁹⁹. Ο δεύτερος φορέας είναι η υπηρεσία πληροφοριών εσωτερικού, το Κέντρο Πληροφοριών για την Καταπολέμηση της Τρομοκρατίας και του Οργανωμένου Εγκλήματος (CITCO). Το τρίτο και τελευταίο όργανο είναι το Κέντρο Πληροφοριών των Ενόπλων Δυνάμεων της Ισπανίας (CIFAS). Η CIFAS τελεί επίσης υπό την άμεση εποπτεία του Υπουργείου Άμυνας²⁰⁰²⁰¹.

Εκ των προτέρων έλεγχος

104. Μεγάλο μέρος της παρακολούθησης που πραγματοποιήθηκε στην Ισπανία πραγματοποιήθηκε από την CNI, φορέα που έχει εμπλακεί στο παρελθόν σε διάφορα σκάνδαλα σχετικά με την παρακολούθηση²⁰². Η CNI ιδρύθηκε με τον νόμο 11/2002 της 6ης Μαΐου και εξουσιοδοτεί την CNI να διεξάγει «έρευνες ασφαλείας»²⁰³. Ωστόσο, δεν υπάρχουν διευκρινίσεις σχετικά με τα μέσα ή τους περιορισμούς των εν λόγω δραστηριοτήτων²⁰⁴. Με τον νόμο 11/2002 θεσπίστηκε επίσης ο κοινοβουλευτικός, εκτελεστικός και νομοθετικός έλεγχος της CNI²⁰⁵. Η κοινοβουλευτική εποπτεία πρέπει να διενεργείται από την επιτροπή περί κρατικού απορρήτου της Ισπανικής Βουλής, η

¹⁹⁶ Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, at Section 18.

¹⁹⁷ Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, at Section 18.

¹⁹⁸ Constitution of Spain 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, at Section 55.

¹⁹⁹ <https://www.cni.es/en/intelligence>

²⁰⁰ https://emad.defensa.gob.es/en/?_locale=en

²⁰¹ Geneva Centre for Security Sector Governance report 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf at pg. 40.

²⁰² Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 2.

²⁰³ Law 11/2002 May 6, <https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html> at Article 5.5.

²⁰⁴ OMCT, <https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain>, 4 May 2022.

²⁰⁵ Law 11/2002 May 6, <https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html> at Article 11.

οποία συστάθηκε το 1995²⁰⁶. Η εντεταλμένη επιτροπή για ζητήματα πληροφοριών ασκεί τον εκτελεστικό έλεγχο του φορέα και συντονίζει τις δραστηριότητες συλλογής πληροφοριών της CNI²⁰⁷. Τέλος, η επιτροπή άμυνας της Ισπανικής Βουλής ασκεί νομοθετική εποπτεία επί της CNI²⁰⁸. Η ετήσια οδηγία για τις υπηρεσίες πληροφοριών καθορίζει τις προτεραιότητες της CNI όσον αφορά τις πληροφορίες για το έτος²⁰⁹.

Κατασταλτικός έλεγχος

105. Οι νόμοι για τη σύσταση της CNI ίδρυσαν επίσης την επιτροπή άμυνας της Βουλής των Αντιπροσώπων, η οποία είναι αρμόδια για τη διάθεση των εμπιστευτικών κονδυλίων για την CNI και για την εκπόνηση ετήσιας έκθεσης σχετικά με την CNI. Ωστόσο, το ισπανικό Σύνταγμα δεν ορίζει ότι θα παρέχεται πρόσβαση σε έγγραφα ή πληροφορίες που σχετίζονται με το έργο των υπηρεσιών πληροφοριών και είναι αξιοσημείωτο ότι η απαίτηση αυτή απουσιάζει επίσης από το νομικό πλαίσιο του νόμου περί διαφάνειας. Ως εκ τούτου, μεγάλο μέρος του έργου της CNI παραμένει απόρρητο και στερείται διαφάνειας²¹⁰.
106. Η επιτροπή περί κρατικού απορρήτου υποχρεούται να υποβάλλει ετήσια έκθεση σχετικά με τις δραστηριότητες των υπηρεσιών πληροφοριών, ωστόσο, όταν συγκλήθηκε ως αποτέλεσμα της παρακολούθησης από τη CNI, ήταν η πρώτη συνεδρίαση του οργάνου σε διάστημα άνω των δύο ετών. Ο επικεφαλής της CNI Paz Esteban εμφανίστηκε ενώπιον της επιτροπής στις 5 Μαΐου 2022 για να παρουσιάσει τις δικαστικές άδειες για τα 18 θύματα για τη στόχευση των οποίων οι αρχές έχουν αναλάβει την ευθύνη²¹¹. Η ακρόαση δεν ήταν δημόσια και δεν επιτράπη στους παριστάμενους να έχουν οποιοδήποτε ηλεκτρονικό εξοπλισμό μαζί τους²¹².

Δημόσιος έλεγχος

107. Το σκάνδαλο «CatalanGate» έχει αποτελέσει αντικείμενο μεγάλου δημόσιου ελέγχου από τότε που αποκαλύφθηκε τον Απρίλιο του 2022. Τα ισπανικά μέσα ενημέρωσης και τα μέσα ενημέρωσης σε ολόκληρο τον κόσμο συνεργάστηκαν εκτενώς με οργανώσεις της κοινωνίας των πολιτών για τον έλεγχο του συστήματος παρακολούθησης στην Ισπανία και την προάσπιση των θεμελιωδών δικαιωμάτων των θυμάτων. Αντιστρόφως, ορισμένοι Ισπανοί πολιτικοί προσπάθησαν να δυσφημίσουν το CitizensLab, υποδηλώνοντας ότι οι μέθοδοι του δεν είναι άρτιες ή ότι έχουν πολιτικά κίνητρα.

²⁰⁶ Law 11/1995 May 11, <https://www.boe.es/eli/es/l/1995/05/11/11/con>.

²⁰⁷ Law 11/2002 May 6, <https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html> at Article 6.

²⁰⁸ Law 11/2002 May 6, <https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html> at Article 11.

²⁰⁹ On Balance: Intelligence Democratization in Post-Franco Spain, <https://www.tandfonline.com/doi/full/10.1080/08850607.2018.1466588?scroll=top&needAccess=true>, *International Journal of Intelligence and Counter intelligence* [2018] Vol 31 issue 4, 769-804 at pg. 776.

²¹⁰ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 2.

²¹¹ El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

²¹² El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 May 2022.

Μεταξύ των στόχων συγκαταλέγονταν ένας συνεργάτης του CitizensLab, καταλανικής καταγωγής, μαζί με τους γονείς του, οι οποίοι δεν είναι καθόλου πολιτικά ενεργοί²¹³.

Μέσα προσφυγής

108. Μια νομική υπόθεση σχετικά με την παρακολούθηση του πρωθυπουργού Sanchez και του υπουργού Άμυνας Robles κατατέθηκε στη Μαδρίτη στο Audiencia Nacional, το Ισπανικό Εθνικό Δικαστήριο, από το γραφείο δικηγόρων του κράτους²¹⁴. Ο δικαστής Jose Luis Calama, επικεφαλής του κεντρικού πρωτοβάθμιου δικαστηρίου αριθ. 4, είναι υπεύθυνος για την εν εξελίξει υπόθεση²¹⁵. Στις 13 Οκτωβρίου 2022, ο δικαστής Calama απέστειλε ερωτηματολόγιο τόσο στη Robles καθώς και στον Grande-Marlaska, το οποίο περιελάμβανε αίτημα, το οποίο έπρεπε να επιβεβαιωθεί από νόμιμες πηγές, σχετικά με τον τρόπο εντοπισμού των λοιμώξεων από το Pegasus. Οι εισαγγελικές αρχές έστειλαν επίσης ερωτήσεις στους υπουργούς²¹⁶.
109. Σε αντίθεση με τον ταχύ χαρακτήρα της υπόθεσης που κατέθεσαν οι Sanchez κ.ά. στη Μαδρίτη, οι υποθέσεις που έχουν κατατεθεί στη Βαρκελώνη από τα θύματα κατασκοπευτικού λογισμικού της Καταλονίας κινούνται με αργό ρυθμό²¹⁷²¹⁸. Η πρώτη υπόθεση στην ανακριτική αρχή αριθ. 32 στη Βαρκελώνη υποβλήθηκε από δύο θύματα του Pegasus το 2020· τον πρώην πρόεδρο του Καταλανικού Κοινοβουλίου και νυν υπουργό Επιχειρήσεων και Εργασίας, Roger Torrent, και τον πρώην υπουργό Εξωτερικών, Θεσμικών Σχέσεων και Διαφάνειας της Καταλονίας και νυν πρόεδρος του ERC στο δημοτικό συμβούλιο της Βαρκελώνης, Ernest Maragall²¹⁹. Ο Andreu Van Den Eynde είναι ένας από τους δικηγόρους που εκπροσωπούν εν προκειμένω τους Torrent και Maragall και είναι και ο ίδιος θύμα του Pegasus. Ο Van Den Eynde επέκρινε τα δικαστήρια που καθυστερούν συστηματικά τη διαδικασία και ουσιαστικά «παραλύουν» την υπόθεση²²⁰. Η ένωση Omnium Cultural και το κόμμα CUP έχουν επίσης προσφύγει στο ίδιο δικαστήριο στη Βαρκελώνη. Ο δικηγόρος Benet Salellas, ο οποίος συμμετέχει και στις δύο υποθέσεις, ισχυρίζεται ότι η ισπανική κυβέρνηση βρίσκεται πίσω από τη στόχευση²²¹.
110. Δεδομένου ότι το Ισπανικό Εθνικό Δικαστήριο είναι αρμόδιο για υποθέσεις που αφορούν τα σοβαρότερα εγκλήματα σε όλα τα εδάφη, είναι πιθανό ο εισαγγελέας να

²¹³ Dit Kan Geen Toeval Zijn, De Volkskrant podcast series by Huib Modderkolk and Simone Eleveld, 2022.

²¹⁴ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²¹⁵ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²¹⁶ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²¹⁷ El Diario, https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje_1_9068271.html, 9 June 2022.

²¹⁸ El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 May 2022.

²¹⁹ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²²⁰ El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 May 2022.

²²¹ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

ζητήσει την ενοποίηση όλων των υποθέσεων Pegasus²²². Με άλλα λόγια, οι υποθέσεις των θυμάτων από την ισπανική κυβέρνηση και των θυμάτων του «CatalanGate» να εξεταστούν στο Ισπανικό Εθνικό Δικαστήριο της Μαδρίτης. Οι δικηγόροι που εκπροσωπούν τα θύματα από την Καταλονία ισχυρίζονται ότι δεν υπάρχει σχέση μεταξύ των υποθέσεων, εκτός εάν αποδειχθεί ότι ο δράστης είναι ο ίδιος σε όλες τις περιπτώσεις παρακολούθησης²²³.

111. Υπάρχουν ορισμένες άλλες εκκρεμείς νομικές υποθέσεις που συνδέονται με τα 65 θύματα της Καταλονίας. Ο δικηγόρος και θύμα του Pegasus Gonzalo Boye υπέβαλε μια τέτοια υπόθεση, εξ ονόματος τουλάχιστον 19 θυμάτων, κατά της NSO, των τριών ιδρυτών της NIV Karmi, Shalev Hulio και Omri Lavie, της Q Cyber Technologies, και της OSY, θυγατρικής εταιρείας με έδρα το Λουξεμβούργο²²⁴²²⁵. Έχουν επίσης κινηθεί νομικές διαδικασίες σε ορισμένα άλλα κράτη μέλη της ΕΕ ως αποτέλεσμα της παρακολούθησης που διενεργήθηκε εις βάρος των εν λόγω εξόριστων Καταλανών αυτονομιστών, μεταξύ των οποίων συγκαταλέγονται η Γαλλία, το Βέλγιο, η Ελβετία, η Γερμανία και το Λουξεμβούργο²²⁶.

Στόχοι

112. Σύμφωνα με πληροφορίες, η στόχευση Καταλλάνων πολιτών με κατασκοπευτικό λογισμικό ξεκίνησε ήδη από το 2015 και πραγματοποιείται σε μεγάλη κλίμακα από το 2017²²⁷. Μετά την αρχική κάλυψη από τα μέσα ενημέρωσης το 2020, το πλήρες σκάνδαλο ξέσπασε σε ολόκληρη την Ευρώπη τον Απρίλιο του 2022 με τη δημοσίευση της έκθεσης του CitizenLab του Πανεπιστημίου του Τορόντο. Λόγω του σημαντικού χρονικού διαστήματος που μεσολάβησε από την έναρξη του χάκινγκ και τις αποκαλύψεις αυτές αυτών, ορισμένοι στόχοι δεν μπόρεσαν να εντοπιστούν ή να διερευνηθούν περαιτέρω λόγω διαφόρων παραγόντων, μεταξύ των οποίων το γεγονός ότι ορισμένοι στόχοι είχαν απορρίψει την εν λόγω τηλεφωνική συσκευή²²⁸.
113. Ο πρωθυπουργός της Ισπανίας Pedro Sánchez, η υπουργός Άμυνας Margarita Robles και ο υπουργός Εσωτερικών Fernando Grande-Marlaska τέθηκαν στο στόχαστρο του Pegasus από τον Μάιο έως τον Ιούνιο του 2021²²⁹. Μέχρι στιγμής υπάρχουν λίγες διαθέσιμες πληροφορίες σχετικά με τις λεπτομέρειες αυτής της παραβίασης, δεδομένου ότι αυτές ανακοινώθηκαν από την κυβέρνηση και δεν ήταν αποτέλεσμα έρευνας του CitizenLab ή κάποιας ανάλογης ερευνητικής υπηρεσίας ή ερευνητών δημοσιογράφων. Οι Sánchez και Robles είναι οι επικεφαλής των δύο κυβερνητικών κλάδων που

²²² El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²²³ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

²²⁴ El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, 3 May 2022.

²²⁵ Catalan News, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

²²⁶ Catalan News, <https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab>, 19 April 2022.

²²⁷ <https://catalonia.citizenlab.ca/#targeting-puigdemont>

²²⁸ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 5.

²²⁹ El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 May 2022.

εποπτεύουν τη CNI, το όργανο που είναι αρμόδιο για τη διεξαγωγή παρακολουθήσεων στην Ισπανία. Οι μολυσμένες συσκευές των Sánchez και Robles είχαν παρασχεθεί από την κυβέρνηση και σαρώνονταν περιστασιακά για κατασκοπευτικό λογισμικό²³⁰. Ο Grande-Marlaska μολύνθηκε από την προσωπική του συσκευή²³¹. Ο υπουργός Γεωργίας Luis Planas, ο οποίος προηγουμένως διετέλεσε διπλωμάτης στο Μαρόκο, στοχοποιήθηκε επίσης με κατασκοπευτικό λογισμικό, αλλά δεν υπήρξε επιτυχής λοίμωξη. Έχει αναφερθεί ότι η μαροκινή κυβέρνηση θα μπορούσε δυνητικά να είναι υπεύθυνη για την εν λόγω στόχευση, ωστόσο οι πληροφορίες αυτές δεν έχουν επιβεβαιωθεί²³².

114. Συνολικά, επιβεβαιώθηκε ότι 65 Καταλανοί στοχοποιήθηκαν με μισθοφορικό κατασκοπευτικό λογισμικό, 63 με το Pegasus, τέσσερις με το Candiru και τουλάχιστον δύο άτομα στοχοποιήθηκαν και από τα δύο²³³. Τουλάχιστον 51 άτομα μολύνθηκαν με επιτυχία²³⁴. Η ισπανική κυβέρνηση αρνήθηκε να σχολιάσει κατά πόσον ήταν υπεύθυνη για την παρακολούθηση κάποιο από τα άλλα θύματα εκτός των 18 ατόμων που παραδέχονται ότι αποτέλεσαν στόχο²³⁵. Τα περισσότερα από τα εν λόγω 18 άτομα δεν κατηγορήθηκαν ποτέ για έγκλημα και, ωστόσο, συμπεριλήφθηκαν σε αυτόν τον κατάλογο. Η υπουργός Άμυνας Robles βασίστηκε σε μεγάλο βαθμό στον νόμο περί κρατικού απορρήτου και δεν επεκτάθηκε όσον αφορά τους λόγους για την παρακολούθηση των συγκεκριμένων στόχων²³⁶. Και οι 65 στόχοι από την Καταλονία είχαν έρθει κάποια στιγμή σε επαφή με τους Καταλανούς αυτονομιστές που ζουν εκτός Ισπανίας.

Βουλευτές του Ευρωπαϊκού Κοινοβουλίου

115. Μία από τις βασικές ομάδες που διαπιστώθηκε ότι στοχοποιήθηκαν είναι οι Καταλανοί βουλευτές του Ευρωπαϊκού Κοινοβουλίου που ήταν υπέρ της ανεξαρτησίας. Καθένας από αυτούς παραβιάστηκε με κατασκοπευτικό λογισμικό, είτε άμεσα είτε έμμεσα, μέσω αυτού που το CitizenLab χαρακτηρίζει ως σχεσιακή στόχευση²³⁷: Diana Riba i Giner, Antoni Comín i Oliveres, Jordi Solé, Carles Puigdemont και Clara Ponsati.

Καταλανοί πολιτικοί

116. Ο πρώην πρόεδρος του καταλανικού κοινοβουλίου και νυν υπουργός Επιχειρήσεων και Εργασίας Roger Torrent ήταν μεταξύ των πρώτων που δήλωσαν ότι έπεσαν θύματα

²³⁰ The Economist, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

²³¹ La Razon,

²³² The Economist, <https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099>, 7 May 2022.

²³³ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 1.

²³⁴ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg. 5.

²³⁵ El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5 May 2022.

²³⁶ El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5 May 2022.

²³⁷ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg.6.

μόλυνσης του κινητού τους με Pegasus το 2019 μέσω του WhatsApp²³⁸. Λίγο αργότερα, ο ηγέτης του υπέρ της ανεξαρτησίας κόμματος «Δημοκρατική Αριστερά της Καταλονίας», Ernest Maragall και η Anna Gabriel, πρώην μέλος του περιφερειακού κοινοβουλίου από το κόμμα «Υποψηφιότητα Λαϊκής Ενότητας» (CUP), δήλωσαν επίσης ότι υπήρξαν θύματα του Pegasus²³⁹. Όλοι οι πρόεδροι της Καταλονίας από το 2010 έχουν στοχοποιηθεί με κατασκοπευτικό λογισμικό είτε κατά τη διάρκεια της θητείας τους είτε μετά τη λήξη της θητείας τους²⁴⁰. Περίπου 12 μέλη του ERC ήταν μεταξύ των 65 στόχων, συμπεριλαμβανομένης της γενικής γραμματέως του κόμματος Marta Rovira, η οποία χακαρίστηκε τουλάχιστον δύο φορές τον Ιούνιο του 2020, σύμφωνα με το CitizenLab. Είναι εξαιρετικά σημαντικό το γεγονός ότι τόσο η Gabriel όσο και η Rovira ζούσαν στην Ελβετία την περίοδο της παρακολούθησής τους, που ακολούθησε τις εξελίξεις μετά το δημοψήφισμα του 2017.

Οργανώσεις της κοινωνίας των πολιτών

117. Ο Jordi Domingo ήταν ένας από τους πρώτους Καταλανούς ακτιβιστές που αναφέρθηκε ότι στοχοποιήθηκαν το 2020. Αν και υποστηρικτής της ανεξαρτησίας της Καταλονίας, ο Guardian ανέφερε ότι ο Domingo πίστευε ότι στοχοποιήθηκε κατά λάθος. Δεδομένου ότι δεν διαδραμάτισε σημαντικό ρόλο στα γεγονότα του 2017, πιστεύει ότι ο επιδιωκόμενος στόχος ήταν ένας δικηγόρος με το ίδιο όνομα που συνέβαλε στην κατάρτιση του συντάγματος της Καταλονίας²⁴¹.

Δικηγόροι

118. Ο Gonzalo Boye έχει εκπροσωπήσει πολλές προσωπικότητες υψηλού επιπέδου της Καταλονίας, συμπεριλαμβανομένων των πρώην προέδρων Puigdemont και Torras²⁴². Για πάνω από πέντε μήνες μεταξύ Ιανουαρίου και Μαΐου 2020, υπήρξε θύμα του Pegasus και ο ίδιος²⁴³. Ο Boye στοχοποιήθηκε έως και 18 φορές κατά τη διάρκεια αυτής της περιόδου μέσω γραπτών μηνυμάτων που εμφανίζονταν ως τουίτ από οργανώσεις της κοινωνίας των πολιτών ή εξέχοντα ειδησεογραφικά μέσα²⁴⁴. Το CitizenLab επιβεβαίωσε τουλάχιστον μία επιτυχή λοίμωξη στις 30 Οκτωβρίου 2020. Η μόλυνση πραγματοποιήθηκε μόλις 48 ώρες μετά τη σύλληψη ενός από τους πελάτες του²⁴⁵. Η στόχευση του Boye έθεσε υπό αμφισβήτηση τη νομιμότητα επιθέσεων στο δικηγορικό απόρρητο.

²³⁸ The Guardian, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

²³⁹ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg.5.

²⁴⁰ Artur Mas (after leaving office), Carles Puigdemont (relational targeting), Joaquim Torra (while in office), Pere Aragones (infected while serving as Torra's Vice President). <https://catalonia.citizenlab.ca/>

²⁴¹ The Guardian, <https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware>, 13 July 2020.

²⁴² <https://catalonia.citizenlab.ca/>

²⁴³ <https://catalonia.citizenlab.ca/>

²⁴⁴ <https://catalonia.citizenlab.ca/>

²⁴⁵ <https://catalonia.citizenlab.ca/>

119. Ο Andreu van den Eynde i Adroer μολύνθηκε επιτυχώς από το Pegasus στις 14 Μαΐου 2020²⁴⁶. Το χάκινγκ συνέβη όταν ενεργούσε ως δικηγόρος τόσο του Raul Romeva όσο και του Oriol Junqueras στην υπόθεσή τους ενώπιον του Ανωτάτου Δικαστηρίου.
120. Ομοίως, το τηλέφωνο του εξέχοντος δικηγόρου Jaume Alonso-Cuevillas μολύνθηκε, ενώ παράλληλα εκπροσωπούσε βασικές προσωπικότητες της Καταλονίας, όπως τον Carles Puigdemont. Ωστόσο, το CitizenLab δεν ήταν σε θέση να προσδιορίσει την ακριβή ημερομηνία της επιτυχούς μόλυνσης.

I.ΣΤ. Άλλα κράτη μέλη

121. Μέχρι στιγμής, οι εθνικές αρχές έχουν κοινοποιήσει ελάχιστες επίσημες πληροφορίες σχετικά με την απόκτηση και τη χρήση κατασκοπευτικού λογισμικού στις χώρες τους, ή σχετικά με τις δημοσιονομικές πτυχές ή το νομικό πλαίσιο που το διέπει. Οι πωλητές και οι χώρες που εκδίδουν άδειες εξαγωγής (ιδίως το Ισραήλ) δεν κοινοποιούν πληροφορίες σχετικά με τους πελάτες. Μόνο η Αυστρία, η Πολωνία και η Κύπρος απάντησαν στο ερωτηματολόγιο που απέστειλε η PEGA στις 15 Ιουλίου 2022, αλλά ως επί το πλείστον με πολύ γενικό, ακόμη και με υπεκφεύγοντα τρόπο.
122. Ωστόσο, με τη συγκέντρωση πληροφοριών από διάφορες πηγές, μπορεί να ανασυσταθεί μια μερική εικόνα και μπορούν να εντοπιστούν ζητήματα που εγείρουν ανησυχίες και χρήζουν περαιτέρω διερεύνησης.
123. Μπορεί να υποθεθεί με ασφάλεια ότι οι αρχές όλων των κρατών μελών χρησιμοποιούν κατασκοπευτικό λογισμικό με τον ένα ή τον άλλο τρόπο. Το κατασκοπευτικό λογισμικό μπορεί να αποκτηθεί απευθείας ή μέσω πληρεξουσίου, εταιρείας διαμεσολάβησης ή μεσάζοντος. Ενδέχεται επίσης να υπάρχουν συμφωνίες για συγκεκριμένες υπηρεσίες, αντί της πραγματικής αγοράς του λογισμικού. Μπορούν να προσφέρονται πρόσθετες υπηρεσίες, όπως η κατάρτιση του προσωπικού ή η παροχή εξυπηρετητών. Είναι σημαντικό να συνειδητοποιήσουμε ότι η αγορά και χρήση κατασκοπευτικού λογισμικού είναι ιδιαίτερα δαπανηρή και ανέρχεται σε εκατομμύρια ευρώ. Ωστόσο, σε πολλά κράτη μέλη, οι δαπάνες αυτές δεν περιλαμβάνονται στον τακτικό προϋπολογισμό και, ως εκ τούτου, ενδέχεται να διαφεύγουν του ελέγχου.
124. Από πληροφορίες που παρασχέθηκαν από τον όμιλο NSO, γνωρίζουμε ότι το Pegasus πωλήθηκε σε τουλάχιστον δεκατέσσερις χώρες της ΕΕ, μέχρι τον τερματισμό των συμβάσεων με δύο χώρες. Δεν είναι γνωστό ποιες, αλλά υπάρχει μια γενική υπόθεση ότι πρόκειται για την Πολωνία και την Ουγγαρία. Ωστόσο, εφόσον ο όμιλος NSO ή η ισραηλινή κυβέρνηση δεν προβούν σε κάποια επίσημη δήλωση σχετικά με τον τερματισμό της σύμβασης, δεν μπορεί να επαληθευτεί εάν αυτό ισχύει.
125. Μια πρόσθετη πληροφορία είναι ο κατάλογος συμμετεχόντων στην έκθεση ISS World (Intelligence Support Systems) για το 2013, γνωστή και ως «The Wiretappers Ball». Με εξαίρεση την Πορτογαλία και το Λουξεμβούργο, όλα τα σημερινά κράτη μέλη της ΕΕ εκπροσωπήθηκαν από ευρύ φάσμα οργανώσεων, συμπεριλαμβανομένων των τοπικών αστυνομικών δυνάμεων²⁴⁷. Τα τελευταία χρόνια, ο όμιλος NSO έχει καταστεί ο κύριος

²⁴⁶ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022 at pg.10.

²⁴⁷ <https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf>

χορηγός της εκδήλωσης, αλλά ο κατάλογος των χορηγών αναφέρει επίσης τις Intellexa, Candiru, RCS και πολλές άλλες εταιρείες²⁴⁸.

126. Τα κράτη μέλη δεν είναι μόνο πελάτες των προμηθευτών εμπορικού κατασκοπευτικού λογισμικού, αλλά έχουν και άλλους, διαφορετικούς ρόλους στο εμπόριο κατασκοπευτικού λογισμικού. Ορισμένοι φιλοξενούν προμηθευτές κατασκοπευτικού λογισμικού, ορισμένοι είναι ο προτιμώμενος προορισμός για τις χρηματοπιστωτικές και τραπεζικές υπηρεσίες, ενώ άλλοι προσφέρουν ιθαγένεια και διαμονή σε πρωταγωνιστές του κλάδου.
127. Το κατασκοπευτικό λογισμικό χρησιμοποιείται σαφώς και από τις αρχές επιβολής του νόμου και όχι μόνο από τις υπηρεσίες πληροφοριών. Δεν υπάρχουν πληροφορίες σχετικά με το υλικό που αποκτάται με τη χρήση κατασκοπευτικού λογισμικού και τον τρόπο με τον οποίο αυτό μπορεί να χρησιμοποιηθεί, και έχει χρησιμοποιηθεί για τον εντοπισμό, τη διερεύνηση και τη δίωξη εγκλημάτων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας της ΕΕ. Υπάρχουν σημαντικά ερωτηματικά σχετικά με το παραδεκτό ενώπιον δικαστηρίου τέτοιου είδους υλικού ως αποδεικτικών στοιχείων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας της ΕΕ, μεταξύ άλλων στο πλαίσιο της Ευρωπαϊκής και της Eurojust.

Κάτω Χώρες

128. Η συμφωνία συνασπισμού της ολλανδικής κυβέρνησης του 2017 αναφέρει ότι η ολλανδική αστυνομία δεν επιτρέπεται να αποκτήσει κατασκοπευτικό λογισμικό από παρόχους που προμηθεύουν τα προϊόντα τους σε «αμφιλεγόμενα καθεστώτα», τα οποία στη συνέχεια προσδιορίστηκαν ως «χώρες που ευθύνονται για σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων ή του διεθνούς ανθρωπιστικού δικαίου». Πριν από την απόκτηση κατασκοπευτικού λογισμικού, η ολλανδική αστυνομία πρέπει να ρωτήσει τον πάροχο αν έχει προμηθεύσει προϊόντα του σε χώρες στις οποίες έχουν επιβληθεί κυρώσεις από την ΕΕ ή τα Ηνωμένα Έθνη και να ελέγξει αν η χώρα στην οποία είναι εγκατεστημένος ο πάροχος διαθέτει καθεστώς ελέγχου των εξαγωγών με βάση το οποίο τα ανθρώπινα δικαιώματα αξιολογούνται στο πλαίσιο της διαδικασίας χορήγησης άδειας εξαγωγής. Η αξιολόγηση αυτή επαναλαμβάνεται περιοδικά. Θα πρέπει να σημειωθεί ότι ο περιορισμός αυτός φαίνεται να ισχύει μόνο για την απόκτηση κατασκοπευτικού λογισμικού από την αστυνομία. Οι υπηρεσίες πληροφοριών δεν αναφέρονται ρητά. Σύμφωνα με την κυβέρνηση, η αστυνομία χρησιμοποιεί λογισμικό χάκινγκ από το 2019, αν και οι αρχές δεν αναφέρουν ποιο είδος²⁴⁹. Φαίνεται ότι ο όμιλος NSO και το προϊόν κατασκοπευτικού λογισμικού Pegasus δεν πληρούν τα προαναφερθέντα πρότυπα, σε κάθε περίπτωση όχι πριν από την αυστηροποίηση του εξαγωγικού καθεστώτος του Ισραήλ τον Δεκέμβριο του 2021²⁵⁰. Δεν παρέχονται πληροφορίες σχετικά με τις δαπάνες τόσο της αστυνομίας όσο και των υπηρεσιών πληροφοριών για την αγορά και τη χρήση του συστήματος κατασκοπευτικού λογισμικού.

²⁴⁸ https://www.issworldtraining.com/iss_europe/sponsors.html

²⁴⁹ <https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland>

²⁵⁰ <https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021>

129. Στις 4 Οκτωβρίου 2022, αποκαλύφθηκε ότι τον Νοέμβριο του 2019 το ολλανδικό Υπουργείο Άμυνας επρόκειτο να υπογράψει συμφωνία με τη WiSpear, την εταιρεία που ανήκε στον Tal Dilian, που είχε αγοράσει προηγουμένως την Cytrox, κατασκευάστρια του κατασκοπευτικού λογισμικού Predator²⁵¹. Δεν είναι σαφές κατά πόσον η σύμβαση υπεγράφη ή όχι και αν παρασχέθηκε τυχόν κατασκοπευτικό λογισμικό στο ολλανδικό Υπουργείο Άμυνας.

Βέλγιο

130. Σε συνέντευξη με την The New Yorker, ένας πρώην αξιωματικός των ισραηλινών υπηρεσιών πληροφοριών αποκάλυψε ότι η βελγική αστυνομία χρησιμοποιεί το Pegasus στις επιχειρήσεις της²⁵². Σε απάντηση, η βελγική αστυνομία δήλωσε «ότι δεν γνωστοποιεί πληροφορίες σχετικά με τεχνικά ή/και τεχνολογικά μέσα που χρησιμοποιούνται για έρευνες και αποστολές». Τον Σεπτέμβριο του 2021, ο υπουργός Δικαιοσύνης Vincent Van Quickenborne ανέφερε ότι το Pegasus «μπορεί να χρησιμοποιηθεί με νόμιμο τρόπο» από τις υπηρεσίες πληροφοριών, αλλά δεν επιθυμούσε να επιβεβαιώσει κατά πόσον η βελγική υπηρεσία πληροφοριών είναι πελάτης της NSO ή χρησιμοποιεί κατασκοπευτικό λογισμικό κατά εγκληματιών²⁵³.

Γερμανία

131. Τον Σεπτέμβριο του 2021, αναφέρθηκε ότι η γερμανική ομοσπονδιακή αστυνομία δίωξης του εγκλήματος (BKA) είχε αποκτήσει το Pegasus στα τέλη του 2020. Είναι σημαντικό να σημειωθεί στο σημείο αυτό ότι το γερμανικό δίκαιο διακρίνει δύο μορφές χρήσης κατασκοπευτικού λογισμικού²⁵⁴: πρόσβαση σε όλες τις πληροφορίες (Online-Durchsuchung²⁵⁵) και πρόσβαση μόνο σε ζωντανή επικοινωνία (Quellen-TKÜ²⁵⁶). Δεδομένου ότι το αρχικό λογισμικό Pegasus μπορούσε να έχει πρόσβαση σε όλες τις πληροφορίες μιας συσκευής και όχι μόνο σε ζωντανή επικοινωνία, η χρήση του από την BKA θα παραβίαζε τον νόμο. Ως εκ τούτου, η BKA ζήτησε από την NSO να συντάξει πηγαίο κώδικα, ώστε το Pegasus να έχει πρόσβαση μόνο σε ό, τι επιτρέπεται από τον νόμο. Αρχικά, η NSO αρνήθηκε να το πράξει²⁵⁷. Μόνο μετά από νέες διαπραγματεύσεις, η NSO συμφώνησε, οπότε η BKA απέκτησε τροποποιημένη έκδοση²⁵⁸. Φέρεται να έχει αναπτυχθεί από τον Μάρτιο του 2021. Η έκδοση που αγόρασε η BKA απέκλειε ορισμένες λειτουργίες για την πρόληψη καταχρήσεων, μολοντί δεν είναι σαφές πώς αυτό λειτουργεί στην πράξη. Η BKA συνέταξε έκθεση σχετικά με την εν λόγω τροποποιημένη έκδοση, η οποία παραμένει διαβαθμισμένη²⁵⁹.

Χρήση του Finfisher

²⁵¹ <https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/>

²⁵² <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>

²⁵³ <https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spijonagetool-pegasus/10329450.html>

²⁵⁴ https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

²⁵⁵ https://www.gesetze-im-internet.de/stpo/___100b.html

²⁵⁶ https://www.gesetze-im-internet.de/stpo/___100a.html

²⁵⁷ <https://www.tagesschau.de/investigativ/ndr-wdr/spaech-software-pegasus-deutschland-101.html>

²⁵⁸ <https://www.tagesschau.de/investigativ/ndr-wdr/spaech-software-pegasus-smartphone-103.html>

²⁵⁹ <https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-pruefbericht-zur-pegasus-software/>

132. Το 2012 και το 2013, τόσο η ΒΚΑ όσο και η LKA του Βερολίνου αγόρασαν ανεξάρτητα το κατασκοπευτικό λογισμικό FinFisher (περισσότερα σχετικά με αυτό το κατασκοπευτικό λογισμικό στο κεφάλαιο για τη βιομηχανία του κατασκοπευτικού λογισμικού). Και εδώ, όπως και στην περίπτωση του Pegasus, η ΒΚΑ ζήτησε από την εταιρία να αναπτύξει το κατασκοπευτικό λογισμικό FinFisher κατά τρόπο που να μην έχει πρόσβαση σε όλα τα δεδομένα μιας συσκευής, αλλά μόνο σε ζωντανή επικοινωνία, ώστε να είναι σύμφωνη με το γερμανικό δίκαιο.

Μάλτα

133. Αρκετά άτομα που πρωταγωνιστούν στο εμπόριο κατασκοπευτικού λογισμικού έχουν καταχωρίσει μια επιχείρηση στη Μάλτα ή έχουν αποκτήσει μαλτέζικα διαβατήρια, αλλά φαίνεται ότι δεν διαμένουν εκεί, ούτε οι εταιρείες τους φαίνεται να είναι ενεργές. Μέχρι στιγμής έχουν εντοπιστεί ορισμένες βασικές προσωπικότητες από το εμπόριο κατασκοπευτικού λογισμικού: Tal Dilian, Anatoly Hurgin, Φέλιξ Μπίτζιος, Stanislaw Szymon Pelczar, Peter Thiel.

Γαλλία

Θύματα στη Γαλλία

134. Το καλοκαίρι του 2021, το «Pegasus Project» αποκάλυψε αρκετές περιπτώσεις απόπειρας χάκινγκ από το κατασκοπευτικό λογισμικό Pegasus στη Γαλλία²⁶⁰. Αυτό το σύνολο δεδομένων που διέρρευσε περιλάμβανε τον αριθμό τηλεφώνου του προέδρου Emmanuel Macron, καθώς και τους αριθμούς τηλεφώνου 14 μελών του ιδιαίτερου γραφείου του²⁶¹²⁶². Τα πορίσματα εγκληματολογικών αναλύσεων επιβεβαίωσαν ότι τα τηλέφωνα αρκετών υπουργών μολύνθηκαν από το κατασκοπευτικό λογισμικό Pegasus²⁶³.

Εταιρείες κατασκοπευτικού λογισμικού στη Γαλλία

135. Η Γαλλία φιλοξενεί επίσης τη βιομηχανία κατασκοπευτικού λογισμικού. Η Nexa technologies, μέρος της Intellexa Alliance του Tal Dilian, είναι γαλλική εταιρεία κυβερνοάμυνας και συλλογής πληροφοριών, η οποία ιδρύθηκε το 2000²⁶⁴. Η Nexa Technologies διοικείται από πρώην διευθυντικά στελέχη της Amesys. Η Amesys ιδρύθηκε το 1979²⁶⁵ και είναι γνωστή για την πώληση ενός προγράμματος που ονομάζεται Cerebro, ικανό να παρακολουθεί τις ηλεκτρονικές επικοινωνίες των θυμάτων του, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου και αριθμούς τηλεφώνου²⁶⁶.

²⁶⁰ The Guardian. [Pegasus spyware found on journalists' phones, French intelligence confirms.](#)

²⁶¹ The Guardian. [Spyware 'found on phones of five French cabinet members'.](#)

²⁶² Euractiv. [France's Macron targeted in project Pegasus spyware case.](#)

²⁶³ The Guardian. [Spyware 'found on phones of five French cabinet members'.](#)

²⁶⁴ Bloomberg. [Nexa Technologies Inc.](#)

²⁶⁵ PitchBook. [Amesys.](#)

²⁶⁶ Le Monde. [Vente de matériel de cybersurveillance à l'Égypte : la société Nexa Technologies mise en examen](#)

Ιρλανδία

136. Η Ιρλανδία έχει καταστεί το κράτος μέλος στο οποίο έχουν καταχωριστεί ορισμένες από τις κύριες εταιρείες κατασκοπευτικού λογισμικού που εμπλέκονται σε σκάνδαλα, λόγω της φορολογικής νομοθεσίας της. Στις 20 Σεπτεμβρίου 2022, η *The Currency*, ιρλανδική εκδότρια ερευνητικής δημοσιογραφίας, αποκάλυψε ότι τόσο η Thalestris Limited, μητρική εταιρεία της Intellexa, όσο και η ίδια η Intellexa έχουν την έδρα τους στην Ιρλανδία και είναι καταχωρισμένες σε δικηγορικό γραφείο στην πόλη Balbriggan. Είναι αξιοσημείωτο το γεγονός ότι η αίτηση για την ίδρυση της εταιρείας Thalestris Limited στην Ιρλανδία υποβλήθηκε τον Νοέμβριο του 2019 από ειδικό στη σύσταση εταιρειών, μόλις 12 ημέρες μετά τη δημόσια αποκάλυψη της ποινικής έρευνας για τον Dilian και την εταιρεία του WiSpear από τις κυπριακές αρχές. Ο ίδιος ο Tal Dilian, διευθύνων σύμβουλος της Intellexa, δεν εμφανίζεται στα έγγραφα της ιρλανδικής εταιρείας, αλλά, σύμφωνα με πληροφορίες, η δεύτερη πρώην σύζυγός του, Sarah Hamou αναφέρεται ως διευθύντρια τόσο της Thalestris όσο και της Intellexa²⁶⁷.

Λουξεμβούργο

137. Το Λουξεμβούργο φιλοξενεί εννέα οντότητες που συνδέονται άμεσα με τον όμιλο NSO, όπως αποκαλύφθηκε από τη Διεθνή Αμνηστία τον Ιούνιο του 2021²⁶⁸. Το γεγονός ότι ο υπουργός Εξωτερικών Jean Asselborn γνώριζε αρχικά μόνο δύο οντότητες της NSO που εδρεύουν στη χώρα²⁶⁹ και ότι οι επωνυμίες των εννέα εταιρειών (όπως η Triangle Holdings SA, η Square 2 SARL και η Q Cyber Technologies SARL) δεν αποκαλύπτουν αμέσως τη σύνδεση με τον όμιλο NSO, καταδεικνύει τον τρόπο με τον οποίο οι αδιαφανείς επιχειρηματικές δομές στο Λουξεμβούργο επιτρέπουν στις εταιρείες να λειτουργούν εντελώς εκτός δημόσιας θέας.

Ιταλία

138. Μέχρι στιγμής, δεν έχουν αναφερθεί πληροφορίες σχετικά με πιθανή αγορά κατασκοπευτικού λογισμικού από τις ιταλικές αρχές. Εκτός από τον πρώην πρωθυπουργό και Πρόεδρο της Επιτροπής Romano Prodi, ο οποίος κατασκοπεύτηκε με το Pegasus από τις μυστικές υπηρεσίες του Μαρόκου, δεν αναφέρθηκαν υποθέσεις κατασκοπείας υψηλού επιπέδου²⁷⁰. Ως πρώην ειδικός απεσταλμένος των Ηνωμένων Εθνών για το Σαχέλ, θα μπορούσε να αποτελέσει ενδιαφέρον στόχο για το Μαρόκο, δεδομένου του πιθανού δικτύου του με υψηλόβαθμες προσωπικότητες στη Δυτική Σαχάρα ή την Αλγερία.

Αυστρία

139. Απαντώντας σε γραπτές ερωτήσεις του Εθνικού Συμβουλίου της Αυστρίας (Κάτω Βουλή), ο πρώην υπουργός Εσωτερικών Karl Nehammer δήλωσε ότι η Αυστρία δεν

²⁶⁷ <https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/>

²⁶⁸ <https://www.amnesty.org/en/documents/doc10/4182/2021/en/>

²⁶⁹ <https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e>

²⁷⁰ <https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>

ήταν πελάτης της NSO²⁷¹. Ωστόσο, ο πρώην καγκελάριος Sebastian Kurz διατηρεί στενούς δεσμούς με τον ιδρυτή του ομίλου NSO, και η DSIRF, μεγάλη εταιρεία παροχής κατασκοπευτικού λογισμικού, έχει την έδρα της στην Αυστρία.

Εσθονία

140. Σύμφωνα με πληροφορίες, η Εσθονία ενδιαφέρθηκε επίσης να αγοράσει το κατασκοπευτικό λογισμικό Pegasus του ομίλου NSO. Το 2018 πραγματοποιήθηκαν αρχικές διαπραγματεύσεις μεταξύ της Εσθονίας και του ομίλου NSO, με αποτέλεσμα η Εσθονία να καταβάλει προκαταβολή για τη συμφωνία των 30 εκατομμυρίων δολαρίων για το λογισμικό παρακολούθησης²⁷².

Λιθουανία

141. Ο Anatoly Hurgin, ρωσό-ισραηλινής ιθαγένειας, πρώην ισραηλινός στρατιωτικός μηχανικός και συνυπεύθυνος ανάπτυξης του Pegasus μαζί με την NSO, φέρεται να είναι ιδιοκτήτης εταιρείας στη Λιθουανία, με την επωνυμία UAB «Communication technologies», στον τομέα των «υπηρεσιών σύνδεσης και τηλεπικοινωνιών»²⁷³. Το 2015 απέκτησε επίσης μαλτέζικο χρυσό διαβατήριο²⁷⁴.

Βουλγαρία

142. Στη Βουλγαρία, οι έλεγχοι των εξαγωγών και οι άδειες εξαγωγής για προϊόντα που χαρακτηρίζονται ως «είδη διπλής χρήσης» σύμφωνα με τον κανονισμό της ΕΕ για τη διπλή χρήση ελέγχονται από το Υπουργείο Οικονομίας, ειδικότερα από τη διυπουργική επιτροπή για τον έλεγχο των εξαγωγών και τη μη διάδοση των όπλων μαζικής καταστροφής²⁷⁵. Ο σημερινός υπουργός Οικονομίας και Βιομηχανίας είναι ο Nikola Stoyanov²⁷⁶. Μέχρι σήμερα, οι βουλγαρικές αρχές αρνούνται ότι έχουν χορηγήσει άδειες εξαγωγής στον όμιλο NSO²⁷⁷. Ωστόσο, η Novalpina Capital, πρώην ιδιοκτήτρια ιδιωτικών κεφαλαίων του ομίλου NSO τόνισε ότι τα προϊόντα NSO εξάγονται από την ΕΕ τόσο από την Κύπρο όσο και από τη Βουλγαρία²⁷⁸²⁷⁹²⁸⁰. Οι δύο αυτοί ισχυρισμοί είναι αντιφατικοί.

I.Z. Τα θεσμικά όργανα της ΕΕ

Στοχοποίηση της Ευρωπαϊκής Επιτροπής

²⁷¹ Responses by former Minister of Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 September 2021, Reference 2021-0.580.421

²⁷² The New York Times. [Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia](#)

²⁷³ https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/

²⁷⁴ <https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429>

²⁷⁵ Republic of Bulgaria. Ministry of Economy and Industry. [Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction.](#)

²⁷⁶ Council of Ministers of the Republic of Bulgaria.

²⁷⁷ POLITICO. [Pegasus makers face EU grilling. Here's what to ask them.](#)

²⁷⁸ Amnesty International. [Novalpina Capital's response to NGO coalition's open letter](#) (18 February 2019).

²⁷⁹ Access Now. [Is NSO Group's infamous Pegasus spyware being traded through the EU?](#)

²⁸⁰ <https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/>

143. Μετά τις αποκαλύψεις της Forbidden Stories και της Διεθνούς Αμνηστίας τον Ιούλιο του 2021, η Επιτροπή συγκρότησε «ειδική ομάδα εσωτερικών εμπειρογνομόνων», η οποία ξεκίνησε εσωτερική έρευνα στις 19 Ιουλίου 2021, με σκοπό «να εξακριβωθεί κατά πόσον το Pegasus είχε στοχεύσει συσκευές μελών του προσωπικού της Επιτροπής και του Σώματος των Επιτρόπων»²⁸¹. Στις 23 Νοεμβρίου 2021, η Apple απέστειλε επίσημες κοινοποιήσεις στις συσκευές του Επιτρόπου Reynders και σε «πρόσθετο προσωπικό της Επιτροπής», ότι «στοχοποιήθηκαν από κρατικούς επιτιθέμενους» και ότι οι συσκευές τους θα μπορούσαν να έχουν παραβιασθεί²⁸². Στις 11 Απριλίου 2022, το Reuters ανέφερε ότι ο Didier Reynders, Επίτροπος Δικαιοσύνης, και τουλάχιστον τέσσερις υπάλληλοι της Επιτροπής είχαν στοχοποιηθεί με το λογισμικό Pegasus τον Νοέμβριο του 2021²⁸³.
144. Σύμφωνα με την Επιτροπή, «είναι αδύνατο να αποδοθούν οι εν λόγω δείκτες σε συγκεκριμένο δράστη με απόλυτη βεβαιότητα». Η Επιτροπή θεωρεί ότι δεν μπορεί να επεκταθεί περαιτέρω όσον αφορά τα σημερινά πορίσματα της έρευνας, δεδομένου ότι «θα αποκάλυπταν στους αντιπάλους τις μεθόδους και τις δυνατότητες έρευνας της Επιτροπής, θέτοντας έτσι σε σοβαρό κίνδυνο την ασφάλεια του θεσμικού οργάνου». Το κοινό, πρωταρχικό θέμα με το οποίο ασχολούνται δύο από τους γνωστούς στοχευμένους υπαλλήλους της Επιτροπής, ο Επίτροπος Reynders και ένα μέλος του ιδιαίτερου γραφείου της Επιτρόπου Věra Jourová²⁸⁴, είναι το κράτος δικαίου. Απαντώντας στην ερώτηση της PEGA σχετικά με ενδεχόμενη συσχέτιση, η Επιτροπή αναφέρει ότι «δεν διαθέτει επαρκείς πληροφορίες που να μας επιτρέπουν να συνάγουμε οριστικά συμπεράσματα σχετικά με τη σχέση μεταξύ γεωεντοπισμού και πιθανής απόπειρας μόλυνσης από συσκευή μέσω του Pegasus»²⁸⁵.
145. Στο πλαίσιο της αλληλεπίδρασής της με την επιτροπή PEGA, η Επιτροπή εξήγησε επανειλημμένα ότι η παραβίαση της συσκευής του Επιτρόπου Reynders με το λογισμικό Pegasus δεν στέφθηκε με επιτυχία, γεγονός που φαίνεται να μειώνει τη σοβαρότητα της στόχευσης ενός Επιτρόπου. Ωστόσο, κάθε απόπειρα παραβίασης — επιτυχούς ή μη — (μέλους) της Επιτροπής αποτελεί πολύ σοβαρό πολιτικό γεγονός που επηρεάζει την ακεραιότητα της δημοκρατικής διαδικασίας λήψης αποφάσεων.

Μέτρα κυβερνοασφάλειας

146. Μετά την απόπειρα παραβίασης του τηλεφώνου του Επιτρόπου Reynders και τους δείκτες παραβίασης σε διάφορες συσκευές του προσωπικού της Επιτροπής, η Επιτροπή ανέπτυξε μια κινητή λύση «ανίχνευσης και αντίδρασης σε τελικά σημεία» (Endpoint Dedetection and Response — EDR) σε όλα τα εταιρικά τηλέφωνα τον Σεπτέμβριο του 2021.

Στόχευση πρώην Έλληνα Επιτρόπου και εκπροσώπων στο Συμβούλιο

²⁸¹ Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022

²⁸² Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022

Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

²⁸³ <https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/>

²⁸⁴ <https://pro.politico.eu/news/148627>

²⁸⁵ Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022,

147. Στις 6 Νοεμβρίου, η ελληνική εφημερίδα Documento δημοσίευσε εκτενή κατάλογο των ατόμων που φέρεται να έχουν ίχνη του Predator στις συσκευές τους, συμπεριλαμβανομένου του Δημήτρη Αβραμόπουλου, Ευρωπαϊού Επιτρόπου από το 2014 έως το 2019 και πολιτικού της Νέας Δημοκρατίας²⁸⁶. Δεν είναι σαφές αν είχε τεθεί στο στόχαστρο ενώ ήταν μέλος του Σώματος των Επιτρόπων και ποιος ήταν πίσω από τη στόχευση, αλλά λαμβάνοντας υπόψη τον μακρύ κατάλογο των στοχευόμενων ατόμων, συμπεριλαμβανομένων πολλών πολιτικών από τη Νέα Δημοκρατία και την αντιπολίτευση, η πιο εύλογη υπόθεση είναι ότι οι εντολές προήλθαν από το περιβάλλον του πρωθυπουργού.
148. Ως εκ τούτου, η παρούσα υπόθεση καταδεικνύει ότι (πρώην) Επίτροποι, καθώς και η επικοινωνίας του με συναδέλφους, μπορούν να στοχοποιηθούν για εγχώριους πολιτικούς λόγους ανά πάσα στιγμή από το εσωτερικό των κρατών μελών τους. Επιπλέον, μεταξύ του καταλόγου στόχων που δημοσίευσε το Documento, υπάρχουν αρκετοί σημερινοί υπουργοί της κυβέρνησης, συμπεριλαμβανομένων των υπουργών Εξωτερικών και Οικονομικών. Οι υπουργοί αυτοί είναι επίσης μέλη του Συμβουλίου, το οποίο αποφασίζει για την εξωτερική και δημοσιονομική πολιτική της ΕΕ. Ως εκ τούτου, ένα μόνο προσβεβλημένο τηλέφωνο θα μπορούσε επίσης να χρησιμεύσει για την υποκλοπή όλων των συνεδριάσεων της Επιτροπής και του Συμβουλίου σε πραγματικό χρόνο.

II. Ο κλάδος του κατασκοπευτικού λογισμικού

149. Η Ευρωπαϊκή Ένωση αποτελεί ελκυστικό τόπο για το εμπόριο τεχνολογιών και υπηρεσιών παρακολούθησης, συμπεριλαμβανομένων των εργαλείων κατασκοπευτικού λογισμικού. Αφενός, υπάρχουν οι κυβερνήσεις των κρατών μελών ως δυνητικοί πελάτες. Από την άλλη πλευρά, η έννοια του «ρυθμιζόμενου από την ΕΕ» χρησιμεύει ως σήμα ποιότητας, χρήσιμο για την παγκόσμια αγορά. Η εσωτερική αγορά της ΕΕ προσφέρει ελεύθερη κυκλοφορία και επωφελή εθνικά φορολογικά καθεστώτα. Οι κανόνες για τις δημόσιες συμβάσεις μπορούν να αποφευχθούν σε σχέση με την εθνική ασφάλεια, και οι κυβερνήσεις μπορούν να χρησιμοποιούν πληρεξούσιους ή μεσάζοντες, έτσι ώστε η αγορά κατασκοπευτικού λογισμικού από τις δημόσιες αρχές να είναι πολύ δύσκολο να εντοπιστεί και να αποδειχθεί. Η ΕΕ διαθέτει αυστηρούς κανόνες εξαγωγών, αλλά μπορούν εύκολα να καταστρατηγηθούν, καθώς τα κράτη μέλη επιδιώκουν να αποκτήσουν ανταγωνιστικό πλεονέκτημα με εσκεμμένα χαλαρή εθνική εφαρμογή, και η επιβολή από την Ευρωπαϊκή Επιτροπή είναι ανεπαρκής και επιφανειακή. Πράγματι, κάθε φορά που το καθεστώς για τις άδειες εξαγωγής έγινε αυστηρότερο στο Ισραήλ, αρκετές εταιρείες μετέφεραν τα τμήματα εξαγωγών τους στην Ευρώπη, ιδίως στην Κύπρο²⁸⁷²⁸⁸. Επιπλέον, αρκετές προσωπικότητες από τη βιομηχανία του κατασκοπευτικού λογισμικού έχουν αποκτήσει την ιθαγένεια της ΕΕ προκειμένου να είναι σε θέση να λειτουργούν ελεύθερα εντός και από την ΕΕ.
150. Σε πολλές περιπτώσεις, το ψευδώνυμο μισθοφορικό κατασκοπευτικό λογισμικό («mercenary spyware») φαίνεται να είναι ακριβές. Ο τομέας δεν διαθέτει ιδιαίτερα υψηλά δεοντολογικά πρότυπα, καθώς πωλεί στα πιο αιμοδιψή δικτατορικά καθεστώτα και σε εύπορους μη κρατικούς φορείς με μη φιλικές προθέσεις. Ο κατάλογος των

²⁸⁶ Documento, edition 6 November 2022.

²⁸⁷ Makarios Drousiotis. State Mafia. Chapter 6. Published 2022.

²⁸⁸ Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.

θυμάτων κατασκοπευτικού λογισμικού αφηγείται την πραγματική ιστορία και όχι οι κούφιες δεσμεύσεις για τα ανθρώπινα δικαιώματα στα φυλλάδια των προμηθευτών. Ακόμη και μετά τις αποκαλύψεις του «Pegasus Project»: το 2021 η Cellebrite ανακοίνωσε ότι θα σταματήσει τις πωλήσεις στη Ρωσία, όταν έγινε γνωστό ότι το κατασκοπευτικό της λογισμικό είχε χρησιμοποιηθεί σε ακτιβιστές κατά του Πούτιν. Ωστόσο, τον Οκτώβριο του 2022 υπάρχουν ενδείξεις ότι το Cellebrite εξακολουθεί να χρησιμοποιείται από τον Πούτιν²⁸⁹. Πρόκειται για μια επικερδή, ακμάζουσα και σκιώδη αγορά, η οποία προσελκύει πολλούς επιτήδειους. Ωστόσο, καταφέρνουν να πωλούν τα προϊόντα τους στις δημοκρατικές κυβερνήσεις των ΗΠΑ και της ΕΕ, γεγονός που τους προσδίδει μια επίφαση ευποληψίας. Παρ' όλα αυτά, παρά τους ισχυρισμούς ότι η χρήση κατασκοπευτικού λογισμικού είναι απολύτως νόμιμη και αναγκαία, οι κυβερνήσεις είναι αξιοσημείωτα διστακτικές να παραδεχθούν ότι κατέχουν κατασκοπευτικό λογισμικό. Μερικές φορές καταφεύγουν στη χρήση πληρεξουσίων, μεσαζόντων ή μεσιτών για την αγορά κατασκοπευτικού λογισμικού, ώστε να μην αφήνουν ίχνη. Η μεγάλη ετήσια εκδήλωση του κλάδου είναι η έκθεση «ISS World», γνωστή επίσης ως «The Wiretappers Ball». Η έδρα της ετήσιας ευρωπαϊκής εκδήλωσης είναι στην Πράγα. Υπάρχει σημαντική αλληλεπικάλυψη μεταξύ των εκθετών του ISS World και των εκθέσεων της βιομηχανίας όπλων.

Τρωτά σημεία

151. Αν δεν υπήρχαν τρωτά σημεία σε διάφορα λογισμικά, θα ήταν αδύνατο να εγκατασταθεί και να αναπτυχθεί κατασκοπευτικό λογισμικό. Ως εκ τούτου, προκειμένου να ρυθμιστεί η χρήση του κατασκοπευτικού λογισμικού, πρέπει επίσης να ρυθμιστεί η ανακάλυψη, η γνωστοποίηση και η εκμετάλλευση τρωτών σημείων²⁹⁰. Παρά την ενίσχυση της άμυνας των ψηφιακών συστημάτων που απαιτείται και ενθαρρύνεται από την οδηγία NIS 2 και την πρόταση πράξης για την κυβερνοανθεκτικότητα, είναι σχεδόν αδύνατο να αναπτυχθούν συστήματα χωρίς τρωτά σημεία.

Δίκτυα τηλεπικοινωνιών

152. Οι πάροχοι τηλεπικοινωνιακών υπηρεσιών διαδραματίζουν σημαντικό ρόλο στη διαδικασία κατασκοπείας τόσο της νόμιμης όσο και της παράνομης. Ζούμε σε μια σύγχρονη εποχή τεχνητής νοημοσύνης, μαζικών δεδομένων, κβαντικής υπολογιστικής, αλλά ταυτόχρονα χρησιμοποιούμε και βασιζόμαστε σε μεγάλο βαθμό σε ένα διεθνές πρωτόκολλο τηλεπικοινωνιών που ονομάζεται SS7. Το πρωτόκολλο αυτό αναπτύχθηκε το 1975 και εξακολουθεί να χρησιμοποιείται σήμερα. Το σύστημα αυτό ελέγχει τον τρόπο δρομολόγησης και τιμολόγησης των τηλεφωνικών κλήσεων και καθιστά δυνατές προηγμένες λειτουργίες κλήσεων και την υπηρεσία σύντομων μηνυμάτων (SMS)²⁹¹. Μέσω του δικτύου SS7 υπάρχει η δυνατότητα υποκλοπής τηλεφωνικών κλήσεων,

²⁸⁹ <https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000>

²⁹⁰ Ot van Daalen, intervention in PEGA 27 October 2022;

EDRi Paper: Breaking encryption will doom our freedoms and rights <https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdf>

<https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu>

²⁹¹ <https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as,up to and including 5G.>

μηνυμάτων SMS και γεωεντοπισμού, καθώς και μόλυνσης ενός θύματος με κατασκοπευτικό λογισμικό, όπως το Pegasus, το Predator κ.λπ.²⁹².

Όμιλος NSO

153. Το κατασκοπευτικό λογισμικό Pegasus παράγεται από τον όμιλο NSO. Ο όμιλος NSO ιδρύθηκε το 2010 από τους Shalev Hulio, Omri Lavie και Niv Karmi, αναπτύσσοντας τεχνολογία για να βοηθήσει αδειοδοτημένες κυβερνητικές υπηρεσίες και υπηρεσίες επιβολής του νόμου στον εντοπισμό και την πρόληψη της τρομοκρατίας και του εγκλήματος²⁹³. Το κατασκοπευτικό λογισμικό Pegasus είναι το πιο γνωστό προϊόν του ομίλου NSO. Εισήχθη στην παγκόσμια αγορά το 2011²⁹⁴²⁹⁵.

Εταιρική δομή, διαφάνεια και δέουσα επιμέλεια

154. Στις 25 Ιανουαρίου 2010, ο όμιλος NSO εγκαινίασε την πρώτη εταιρεία του στο Ισραήλ. Η εταιρεία αυτή ήταν καταχωρισμένη με την επωνυμία NSO Group Technologies Limited. Ο όμιλος NSO είναι τόσο η επωνυμία της πρώτης καταχωρισμένης εταιρείας, όσο και ο γενικός όρος για τις διάφορες εταιρείες που έχουν εγκατασταθεί σε άλλες περιοχές δικαιοδοσίας. Αυτή η πρώτη εταιρεία είναι κάτοχος του εμπορικού σήματος του ομίλου NSO²⁹⁶.

Έλεγχοι των εξαγωγών

155. Δεδομένου ότι το κατασκοπευτικό λογισμικό Pegasus χαρακτηρίζεται τεχνολογία διπλής χρήσης, πρέπει να λάβει άδεια εξαγωγής. Οι εταιρείες του ομίλου NSO αποκτούν τις άδειες εξαγωγής τους στο Ισραήλ, τη Βουλγαρία και την Κύπρο²⁹⁷. Οι περισσότερες από αυτές τις άδειες χορηγούνται από τις ισραηλινές αρχές²⁹⁸. Το Ισραήλ δεν αποτελεί μέρος του Διακανονισμού του Wassenaar, αλλά δηλώνει ότι έχει ενσωματώσει ορισμένα από τα στοιχεία του στον εθνικό νόμο 5766 για τον έλεγχο των εξαγωγών στον τομέα της άμυνας, του 2007.²⁹⁹ Ο Οργανισμός Ελέγχου των Εξαγωγών (DECA) του Υπουργείου Άμυνας είναι αρμόδιος για την έκδοση αδειών εμπορίας και εξαγωγών³⁰⁰. Μετά τις αποκαλύψεις του «Pegasus Project» και την ένταξη της NSO σε μαύρη λίστα, ο κατάλογος των επιλέξιμων χωρών μειώθηκε από 102 σε 37, οι οποίες πρέπει να υπογράψουν πιστοποιητικό τελικής χρήσης/χρήστη³⁰¹. Στο πλαίσιο της διαδικασίας δέουσας επιμέλειας, το Ισραήλ θεωρεί αυτομάτως ότι όλα τα κράτη μέλη της ΕΕ συμμορφώνονται με τα πρότυπα της ΕΕ και, ως εκ τούτου, δεν θα διενεργεί πρόσθετες αξιολογήσεις για μεμονωμένες χώρες. Ωστόσο, η απόφαση καταγγελίας των συμβάσεων με δύο κράτη μέλη της ΕΕ φαίνεται να υποδηλώνει ότι η ΕΕ δεν θεωρείται πλέον ενιαία οντότητα για τους σκοπούς της δέουσας επιμέλειας.

²⁹² <https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/>

²⁹³ NSO Group. [About us.](#)

²⁹⁴ NYTimes. [The Battle for the World's Most Powerful Cyberweapon.](#)

²⁹⁵ Hulio S., NSO Never Engaged in Illegal Mass Surveillance, The Wall Street Journal, 24 February 2022

²⁹⁶ Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

²⁹⁷ Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure. P. 62.

²⁹⁸ Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

²⁹⁹ European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.

³⁰⁰ Amnesty International. [Noalpin Capital's reply to NGO coalition letter \(15 April 2019\) and Citizen Lab letter \(06 March 2019\)](#)

³⁰¹ European Parliamentary Research Service. Europe's PegasusGate. Countering spyware abuse.

Αντιδεοντολογική συμπεριφορά που πυροδοτεί αγωγές, καταχώριση σε μαύρη λίστα και συγκρούσεις μεταξύ επενδυτών

156. Τον Ιούλιο του 2021, μια σύγκρουση μεταξύ των τριών συνιδρυτών της Novalpina Capital άρχισε να επηρεάζει τις δραστηριότητες του ομίλου NSO, οδηγώντας τελικά τους επενδυτές στην απόφαση να αφαιρέσουν την εταιρεία ιδιωτικών επενδυτικών κεφαλαίων από τον έλεγχο του³⁰². Στις 27 Αυγούστου 2021, η αμερικανική εταιρεία συμβούλων Berkeley Research Group (BRG) εξαγόρασε το ιδιωτικό επενδυτικό κεφάλαιο και κίνησε έρευνες σχετικά με τη νομιμότητα των δραστηριοτήτων του ομίλου NSO και τη συμμόρφωσή τους με τη μαύρη λίστα των ΗΠΑ. Η διευθυντική ομάδα του ομίλου NSO εμπόδισε τις έρευνες της BRG τον Μάιο του 2022³⁰³. Ένα στέλεχος της BRG δήλωσε ότι η συνεργασία με τον όμιλο NSO έχει καταστεί «σχεδόν ανύπαρκτη» λόγω της πίεσης που ασκεί ο όμιλος NSO για τη συνέχιση των πωλήσεων σε χώρες με αμφιλεγόμενες επιδόσεις στον τομέα των ανθρωπίνων δικαιωμάτων³⁰⁴. Στις 25 Απριλίου 2022, δύο πρώην ομόρρυθμοι εταίροι της Novalpina άσκησαν αγωγή ενώπιον λουξεμβουργιανού δικαστηρίου κατά της BRG, ζητώντας την επαναφορά της Novalpina Capital ως ομόρρυθμοι εταίρου και την αναστολή όλων των αποφάσεων που έχουν ληφθεί από την BRG³⁰⁵. Το λουξεμβουργιανό δικαστήριο απέρριψε τα αιτήματα αυτά και η BRG παραμένει υπεύθυνη για το κεφάλαιο που ελέγχει τον όμιλο NSO³⁰⁶.

Black Cube

157. Η Black Cube είναι μια ισραηλινή ιδιωτική υπηρεσία πληροφοριών που αποτελείται από πρώην υπαλλήλους της Mossad, του ισραηλινού στρατού και των ισραηλινών υπηρεσιών πληροφοριών³⁰⁷. Ο ίδιος ο δικτυακός τόπος της εταιρείας τους περιγράφει ως «δημιουργική υπηρεσία πληροφοριών» που βρίσκει «προσαρμοσμένες λύσεις σε σύνθετες επιχειρηματικές και δικαστικές προκλήσεις»³⁰⁸. Η Black Cube έχει εμπλακεί σε μια σειρά δημόσιων αντιπαραθέσεων σε σχέση με υποθέσεις χάκινγκ, μεταξύ άλλων στις ΗΠΑ και τη Ρουμανία³⁰⁹. Ειδικότερα, οι επικεφαλής της Black Cube παραδέχτηκαν ότι κατασκόπευαν την πρώην γενική εισαγγελέα της Εθνικής Διεύθυνσης Καταπολέμησης της Διαφθοράς της Ρουμανίας, Laura Kovesi³¹⁰. Η Kovesi είναι σήμερα η πρώτη Ευρωπαϊά Γενική Εισαγγελέας που διευθύνει την Ευρωπαϊκή Εισαγγελία (EPPO). Ο Daniel Dragomir, πρώην Ρουμάνος μυστικός πράκτορας, φέρεται ότι ήταν το πρόσωπο που ανέθεσε το έργο στη Black Cube³¹¹.

Intellexa Alliance

³⁰² Financial Times. [Private equity owner of spyware group NSO stripped of control of €1bn fund.](#)

³⁰³ Financial Times. [NSO Group keeping owners 'in the dark', manager says.](#)

³⁰⁴ The New Yorker. [How democracies spy on their citizens.](#)

³⁰⁵ Letter to Mr Jeroen Lenaers and his Vice Chairs.

³⁰⁶ Luxembourg Times. [Top five stories you may have missed.](#)

³⁰⁷ The New Yorker, <https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators>, 7 October 2019.

³⁰⁸ <https://www.blackcube.com/>

³⁰⁹ The New Yorker, <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>, 18 April 2022.

³¹⁰ Balkan Insight. [Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case.](#)

³¹¹ Haaretz. [Black Cube CEO Suspected of Running Crime Organisation. Revealed: The Romania Interrogation.](#)

158. Η Intellexa ιδρύθηκε το 2019 στην Κύπρο από τον Tal Dilian. Ο Dilian κατείχε διάφορες ηγετικές θέσεις στην Ισραηλινή Αμυντική Δύναμη προτού ξεκινήσει τη σταδιοδρομία του ως «εμπειρογνώμονας στον τομέα των πληροφοριών, δημιουργός κοινοτήτων και κατά συρροήν επιχειρηματίας»³¹². Στον ιστότοπό της, η Intellexa Alliance περιγράφεται ως «εταιρεία με έδρα στην ΕΕ και ρυθμιζόμενη από το δίκαιο της με σκοπό την ανάπτυξη και την ενσωμάτωση τεχνολογιών για την ενδυνάμωση των υπηρεσιών πληροφοριών.» Αρκετοί προμηθευτές εξοπλισμού παρακολούθησης που αποτελούν μέρος της εμπορικής επωνυμίας της Intellexa Alliance είναι οι εξής:

- Cytrox, WiSpear (που αργότερα μετονομάστηκε σε Passitora Ltd)
- Nexa technologies (υπό τη διαχείριση πρώην διευθυντικών στελεχών της Amesys)
- Poltrex

WiSpear και Cytrox

159. Το 2013, η Tal Dilian ίδρυσε κυπριακή καταχωρισμένη εταιρεία με την επωνυμία Aveledo Ltd., αργότερα γνωστή ως Ws WiSpear Systems Ltd. και μετά ως Passitora Ltd³¹³. Με έδρα τη Λεμεσό στην Κύπρο, η Wispear πωλεί κυρίως εξοπλισμό και λογισμικό για τον εντοπισμό και την παρακολούθηση ατόμων μέσω του κινητού τους τηλεφώνου. Σε συνέντευξη με το περιοδικό Forbes, ο Dilian εξήγησε τις δυνατότητες του λογισμικού WiSpear παρουσιάζοντας το αξίας 9 εκατομμυρίων δολαρίων μαύρο βαν του, ικανό να παραβιάζει συσκευές σε ακτίνα 500 μέτρων. Επιπλέον, το WiSpear διαθέτει εξοπλισμό που μπορεί να υποκλέπτει δεδομένα από δίκτυα Wi-Fi³¹⁴. Τα δημόσια σκάνδαλα σχετικά με τα προϊόντα αυτά πυροδότησαν τη μεταφορά των κύριων επιχειρηματικών δραστηριοτήτων της Intellexa από την Κύπρο στην Ελλάδα.

Amesys και Nexa Technologies

160. Η Amesys και η Nexa Technologies αποτελούν επίσης μέρος της Intellexa Alliance και δεν είναι απαλλαγμένες από αντιπαραθέσεις, όπως αναφέρεται στο κεφάλαιο για τη Γαλλία.

Poltrex

161. Η Poltrex ιδρύθηκε τον Οκτώβριο του 2018 και μοναδικός μέτοχος της εταιρείας ήταν η Intellexa Ltd, καταχωρισμένη στις Βρετανικές Παρθένες Νήσους. Ο ισραηλινός Shahak Avni — ιδρυτής της κυπριακής NCIS Intelligence Services Ltd³¹⁵ και συνεργάτης του Tal Dilian — καταχωρίστηκε ως διευθυντής της Poltrex τον Σεπτέμβριο του 2019. Τον Οκτώβριο του 2019, τόσο ο Avni όσο και ο Dilian έγιναν συνδιευθυντές και η Poltrex μετονομάστηκε σε Alchemycorp Ltd. Παρά τη

³¹² Tal Dilian. [About.](#)

³¹³ Open Corporates. Passitora Ltd. <https://opencorporates.com/companies/cy/HE318328>

³¹⁴ Haaretz. [As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.](#)

³¹⁵ Philenews. [FILE: The state insulted Avni and Dilian.](#)

μετονομασία της Poltrex, η εταιρεία εξακολουθούσε να φιλοξενείται στον Novel Tower —την ίδια τοποθεσία με τη διεύθυνση της WiSpear³¹⁶.

Candiru

162. Η Candiru είναι μια άλλη εταιρεία καταχωρισμένη στο Ισραήλ που παράγει προϊόντα κατασκοπευτικού λογισμικού. Η εταιρεία ιδρύθηκε το 2014 από τους Ya'acov Weitzman και Eran Shorer. Και οι δύο ιδρυτές έχουν ιστορικό στη Στρατιωτική Μονάδα Πληροφοριών 8200 της Ισραηλινής Αμυντικής Δύναμης (IDF) και αμφότεροι ήταν πρώην υπάλληλοι του ομίλου NSO³¹⁷. Ο πρώην επενδυτής στον όμιλο NSO, Isaac Zack έγινε ο μεγαλύτερος μέτοχος της Candiru. Η εταιρεία πωλεί κατασκοπευτικό λογισμικό για το χάκινγκ ηλεκτρονικών υπολογιστών και εξυπηρετητών³¹⁸. Οι δημοσιοποιημένες πληροφορίες μιας πρότασης έργου υπογραμμίζουν ότι η Candiru πωλεί τον εξοπλισμό του ανά αριθμό ταυτόχρονων λοιμώξεων. Δηλαδή, τον αριθμό των στόχων που μπορούν να στοχοποιηθούν με το κατασκοπευτικό λογισμικό σε μια δεδομένη χρονική στιγμή. Για παράδειγμα, για 16 εκατομμύρια δολάρια, ένας πελάτης λαμβάνει απεριόριστο αριθμό προσπαθειών κατασκοπευτικού λογισμικού, αλλά μπορεί να στοχεύσει μόνο 10 συσκευές ταυτόχρονα. Ένας πελάτης μπορεί να αγοράσει 15 επιπλέον συσκευές για επιπλέον 1,5 εκατ. δολάρια³¹⁹.

Tykelab και RCS Lab

163. Τον Αύγουστο του 2022, η έκθεση Lighthouse ανέφερε ότι η Tykelab, εταιρεία που εδρεύει στη Ρώμη και ανήκει στο RCS lab, χρησιμοποιεί δεκάδες τηλεφωνικά δίκτυα, συχνά σε νησιά του Νότιου Ειρηνικού, για την αποστολή δεκάδων χιλιάδων μυστικών «πακέτων παρακολούθησης» σε ολόκληρο τον κόσμο, με στόχο ανθρώπους σε χώρες όπως η ίδια η Ιταλία, η Ελλάδα, η Βόρεια Μακεδονία, η Πορτογαλία, η Λιβύη, η Κόστα Ρίκα, η Νικαράγουα, το Πακιστάν, η Μαλαισία, το Ιράκ και το Μάλι. Η Tykelab εκμεταλλεύεται τα τρωτά σημεία των παγκόσμιων τηλεφωνικών δικτύων, τα οποία επιτρέπουν σε τρίτους να βλέπουν τις τοποθεσίες των χρηστών των τηλεφώνων και ενδεχομένως να υποκλέπτουν τις κλήσεις τους, χωρίς να αφήνονται ίχνη της παραβίασης στις συσκευές³²⁰. Μόλις σε δύο ημέρες τον Ιούνιο του 2022, η εταιρεία διείσδυσε σε δίκτυα σε όλες σχεδόν τις χώρες του κόσμου³²¹. Στον ιστότοπό της, η Tykelab αναφέρει ότι «συνδυάζει εικοσαετή πείρα στον σχεδιασμό, την εφαρμογή και τη συντήρηση λύσεων κεντρικού δικτύου Telco, μια ισχυρή εμπειρογνώσια στην παροχή διαχειριστικών υπηρεσιών, στην ενοποίηση συστημάτων με βάση τον πελάτη και στην ανάπτυξη εφαρμογών κινητής τηλεφωνίας»³²².

Κατασκοπευτικό λογισμικό Hermit

164. Το RCS Lab έχει αναπτύξει το Hermit, κατασκοπευτικό λογισμικό που μπορεί να χρησιμοποιηθεί για την εξ αποστάσεως ενεργοποίηση του μικροφώνου του τηλεφώνου,

³¹⁶ CyprusMail. [Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.](#)

³¹⁷ Haaretz. ['We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers](#)

³¹⁸ Haaretz. [Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.](#)

³¹⁹ CitizenLab. [Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.](#)

³²⁰ <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

³²¹ <https://euobserver.com/digital/155849>

³²² <http://www.tykelab.it/wp/about/>

καθώς και για την καταγραφή κλήσεων, και την προσπέλαση μηνυμάτων, αρχείων καταγραφής κλήσεων, επαφών και φωτογραφιών³²³. Τον Ιούνιο του 2022, η ομάδα ανάλυσης απειλών της Google αποκάλυψε ότι φορείς υποστηριζόμενοι από κυβερνήσεις που χρησιμοποιούν το κατασκοπευτικό λογισμικό του RCS Lab συνεργάζονται με τους παρόχους υπηρεσιών διαδικτύου του στόχου για να απενεργοποιήσουν τη συνδεσιμότητα δεδομένων κινητής τηλεφωνίας του στόχου. Μετά την απενεργοποίηση, ο επιτιθέμενος έστειλε κακόβουλη σύνδεση μέσω SMS ζητώντας από τον στόχο να εγκαταστήσει μια εφαρμογή για την ανάκτηση της συνδεσιμότητας των δεδομένων. Η Google θεωρεί ότι αυτός είναι ο λόγος για τον οποίο οι περισσότερες εφαρμογές «μεταμφιέζονται» σε εφαρμογές παρόχων κινητής τηλεφωνίας. Όταν δεν είναι δυνατή η συμμετοχή των παρόχων υπηρεσιών διαδικτύου, οι εφαρμογές παρουσιάζονται ψευδώς ως εφαρμογές ανταλλαγής μηνυμάτων. Τα θύματα που στοχοποιήθηκαν με το κατασκοπευτικό λογισμικό του RCS Lab βρίσκονταν στην Ιταλία και το Καζακστάν³²⁴, καθώς και στη Ρουμανία³²⁵.

DSIRF - Decision Supporting Information Research and Forensic

165. Το υπουργείο Δικαιοσύνης της Αυστρίας ξεκίνησε πρόσφατα ποινική διαδικασία ενάντια στην DSIRF GmbH (LLC)³²⁶, αυστριακή εταιρεία με έδρα τη Βιέννη και μητρική εταιρεία στο Λιχτενστάιν που ιδρύθηκε το 2016, και η οποία ισχυρίζεται ότι παρέχει «εξατομικευμένες υπηρεσίες στους τομείς της έρευνας πληροφοριών, της εγκληματολογικής έρευνας, καθώς και της παροχής πληροφοριών που βασίζονται σε δεδομένα σε πολυεθνικές εταιρείες στον τομέα της τεχνολογίας, του λιανικού εμπορίου, της ενέργειας και του χρηματοπιστωτικού τομέα».³²⁷ Η DSIRF προφανώς πραγματοποιεί πωλήσεις σε μη κρατικούς φορείς.

FinFisher

166. Είναι σημαντικό να αναφερθεί στην παρούσα έκθεση η ποινική έρευνα για τη FinFisher, μια πρώην εταιρεία κατασκοπευτικού λογισμικού με έδρα το Μόναχο της Γερμανίας, και η πτώχευσή της. Η FinFisher είναι ένα δίκτυο εταιρειών, που ιδρύθηκε το 2008, και αρχικά είχε ισχυρούς δεσμούς με το βρετανικό δίκτυο εταιρειών υπό την επωνυμία «Gamma». Η FinFisher προώθησε το κατασκοπευτικό λογισμικό της ως «πλήρες χαρτοφυλάκιο εισβολής ΤΠ», με το λογισμικό της να χρησιμοποιείται από δεκάδες χώρες σε ολόκληρο τον κόσμο³²⁸, συμπεριλαμβανομένων 11 κρατών μελών της ΕΕ³²⁹ και 13 «μη ελεύθερων» χωρών³³⁰.

³²³ <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

³²⁴ <https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/>

³²⁵ <https://www.lighthousereports.nl/investigation/revealing-europes-nso/>

³²⁶ DSIRF is an abbreviation for “Decision Supporting Information Research and Forensic”

³²⁷ <https://dsirf.eu/about/>

³²⁸ <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/> -

<https://wikileaks.org/spyfiles4/customers.html>

³²⁹ Belgium, Czech Republic, Estonia, Germany, Hungary, Italy, Netherlands, Romania, Slovakia, Slovenia, Spain

³³⁰ Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Myanmar, Oman, Qatar, Saudi Arabia, Turkey

III. Η ικανότητα αντίδρασης της Ευρωπαϊκής Ένωσης

167. Ορισμένες κυβερνήσεις έχουν στοχεύσει πολίτες της ΕΕ με ισχυρό κατασκοπευτικό λογισμικό. Αυτό απειλεί τη δημοκρατία και τα ατομικά δικαιώματα των πολιτών. Η ΕΕ έχει την εξουσία να αναλάβει δράση για την αντιμετώπιση αυτών των απειλών, αν και πολύ περιορισμένη. Όταν, ωστόσο, τα κράτη μέλη επικαλούνται την «εθνική ασφάλεια», η ΕΕ βρίσκεται ουσιαστικά εκτός του παιχνιδιού. Τα κράτη μέλη καθορίζουν μονομερώς την εθνική ασφάλεια και μπορούν ανά πάσα στιγμή να κλείσουν την πόρτα. Εκτός από αυτούς τους νομικούς περιορισμούς, υπάρχουν και πολιτικοί λόγοι που συνεπάγονται την παθητικότητα της ΕΕ. Η Ευρωπαϊκή Επιτροπή, ως θεματοφύλακας των Συνθηκών της ΕΕ, έχει γίνει επιφυλακτική όσον αφορά την επιβολή του δικαίου της ΕΕ³³¹. Αυτό δεν οφείλεται στο γεγονός ότι υπάρχουν νομικοί περιορισμοί, αλλά πρόκειται περισσότερο για πολιτική επιλογή. Η Επιτροπή τείνει να ερμηνεύει τις εξουσίες της κατά τον στενότερο δυνατό τρόπο. Αντιμέτωπη με κατάφωρες παραβιάσεις του κράτους δικαίου και των θεμελιωδών δικαιωμάτων, η στάση αυτή καθίσταται ιδιαίτερα προβληματική. Υπάρχει ο κίνδυνος η επικουρικότητα και ο σεβασμός των αποκλειστικών εθνικών αρμοδιοτήτων να εξελιχθούν σε ατιμωρησία. Στη συνέχεια θα εξετάσουμε τις εξουσίες που έχουν στη διάθεσή τους τα θεσμικά όργανα της ΕΕ. Το Κοινοβούλιο, η Επιτροπή και το Συμβούλιο έχουν την εξουσία και το καθήκον να νομοθετούν, να ρυθμίζουν και να επιβάλλουν, και πρέπει να το πράττουν με αποφασιστικότητα και φιλοδοξία, προτάσσοντας την υπεράσπιση της δημοκρατίας μας έναντι βραχυπρόθεσμων πολιτικών πτυχών.

Ευρωπαϊκή Επιτροπή

168. Η Ευρωπαϊκή Επιτροπή, αντιδρώντας στο σκάνδαλο του κατασκοπευτικού λογισμικού, έχει μέχρι στιγμής περιοριστεί στη σύνταξη επιστολών με τις οποίες ζητεί διευκρινίσεις από τις κυβερνήσεις της Πολωνίας, της Ουγγαρίας, της Ισπανίας και της Ελλάδας. Ωστόσο, φαίνεται ότι αυτή η διστακτική επίπληξη της Επιτροπής δεν θα ακολουθηθεί από περαιτέρω ενέργειες. Είναι αλήθεια ότι, υπό στενή έννοια, η Επιτροπή δεν έχει την εξουσία να ενεργήσει στον τομέα της εθνικής ασφάλειας. Ωστόσο, όπως επισημαίνει η ίδια η Επιτροπή στις εν λόγω επιστολές, η «εθνική ασφάλεια» δεν πρέπει να ερμηνεύεται ως απεριόριστη εξαίρεση από τους ευρωπαϊκούς νόμους και τις ευρωπαϊκές Συνθήκες και να μετατρέπεται σε τομέα ανομίας.
169. Σε αντίθεση με τις ΗΠΑ, η Επιτροπή δεν έχει προβεί μέχρι στιγμής σε ανάλυση της κατάστασης ούτε σε αξιολόγηση των εταιρειών που δραστηριοποιούνται στην ευρωπαϊκή αγορά. Δεν υπάρχει προφανής νομική αντίρρηση κατά της διενέργειας μιας τέτοιας ανάλυσης.
170. Η ΕΕ διαθέτει διάφορους νόμους που θα μπορούσαν να χρησιμεύσουν ως ρυθμιστικά εργαλεία όσον αφορά το κατασκοπευτικό λογισμικό. Εκτός από τη νομοθεσία για την προστασία των δικαιωμάτων των πολιτών, όπως η νομοθεσία για την προστασία των δεδομένων και της ιδιωτικότητας των επικοινωνιών (ΓΚΠΔ, ψηφιακή ιδιωτικότητα), υπάρχουν νόμοι για τις εξαγωγές (κανονισμός για τα είδη διπλής χρήσης) και τις δημόσιες συμβάσεις. Ωστόσο, η επιβολή από την Επιτροπή είναι ανεπαρκής. Τείνει να περιορίζεται στην επαλήθευση του κατά πόσον ένα κράτος μέλος έχει μεταφέρει ορθά τη νομοθεσία της ΕΕ στο εθνικό του δίκαιο. Ωστόσο, τούτο υποδηλώνει ελάχιστα

³³¹ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

πράγματα για την πραγματική επί τόπου κατάσταση. Κατά συνέπεια, η έκθεση³³² της Επιτροπής σχετικά με την εφαρμογή του κανονισμού για τα είδη διπλής χρήσης φαίνεται να καταλήγει στο συμπέρασμα ότι η εφαρμογή βρίσκεται σε καλό δρόμο, ενώ υπάρχουν πολλά στοιχεία που αποδεικνύουν ότι στην πράξη είναι ανεπαρκής και αποσπασματική, και σε ορισμένες χώρες μάλιστα σκοπίμως. Παρά τους κανόνες που ορίζονται στον κανονισμό για τα είδη διπλής χρήσης, η Κύπρος φαίνεται να έχει καταστεί ελκυστικός εξαγωγικός κόμβος για πωλητές κατασκοπευτικού λογισμικού. Χωρίς κατάλληλη και ουσιαστική επιβολή, οι νόμοι της ΕΕ είναι απλώς «χάρτινες τίγρεις» που δημιουργούν άφθονο χώρο για την παράνομη χρήση κατασκοπευτικού λογισμικού.

Ευρωπαϊκό Κοινοβούλιο

171. Το Ευρωπαϊκό Κοινοβούλιο έχει συστήσει την εξεταστική επιτροπή PEGA, η οποία εργάζεται επιμελώς και αποτελεσματικά στο πλαίσιο των εξουσιών και της εντολής της. Ωστόσο, δεν έχει την εξουσία να κλητεύει μάρτυρες ή να τους εξετάζει ενόρκως, και δεν έχει πρόσβαση σε διαβαθμισμένες πληροφορίες. Δεν διαθέτει τις πλήρεις εξουσίες έρευνας που διαθέτουν τα περισσότερα εθνικά κοινοβούλια. Επιπλέον, η επιρροή των εθνικών κυβερνήσεων είναι συχνά παρούσα στις διαβουλεύσεις της PEGA, πράγμα που ενίοτε αποτελεί εμπόδιο για διεξοδικές, πλήρως ανεξάρτητες και αντικειμενικές έρευνες. Είναι μάλλον κυνικό το γεγονός ότι το Ευρωπαϊκό Κοινοβούλιο δεν διαθέτει πλήρεις εξουσίες διερεύνησης, όταν ορισμένα από τα μέλη του είναι θύματα παράνομης παρακολούθησης.

Ευρωπαϊκό Συμβούλιο και Συμβούλιο Υπουργών

172. Μολονότι οι εθνικές κυβερνήσεις ισχυρίζονται ότι το σκάνδαλο του κατασκοπευτικού λογισμικού είναι αμιγώς εθνικό ζήτημα, στην πραγματικότητα συζητήθηκε στο Συμβούλιο της Ευρωπαϊκής Ένωσης και οι εθνικές κυβερνήσεις αποφάσισαν να απαντήσουν συλλογικά στο ερωτηματολόγιο του Ευρωπαϊκού Κοινοβουλίου³³³. Με τον τρόπο αυτό, αναγνώρισαν πλήρως ότι στην πραγματικότητα εμπίπτει στην αρμοδιότητα του Συμβουλίου. Ωστόσο, η ευθύνη δεν είναι μενού από το οποίο μπορείτε να επιλέξετε: δεν μπορείτε να ασχοληθείτε μόνο επιλεκτικά με διαδικαστικά ζητήματα, αλλά όχι με την ουσία.
173. Μέχρι σήμερα, το Ευρωπαϊκό Συμβούλιο δεν έχει απαντήσει δημοσίως ή ουσιαστικά στο σκάνδαλο. Ορισμένα από τα μέλη του έχουν συμμετοχή στο θέμα αυτό, καθώς τα ίδια μπορεί να είναι συνεργοί στις παράνομες παραβιάσεις ή απλώς επιθυμούν να διατηρήσουν την ΕΕ αδύναμη και ανίσχυρη σε αυτόν τον τομέα. Η ομερτά και η έλλειψη συνεργασίας του Συμβουλίου δεν συνιστά καλό οίονο για τυχόν μελλοντικές ρυθμιστικές πρωτοβουλίες. Το Συμβούλιο είναι νομοθέτης, αλλά μπορεί κάλλιστα να είναι απρόθυμο να ρυθμίσει τα μέλη του.
174. Ακόμη και αν αποδεικνυόταν τελικά παράνομη ή εγκληματική συμπεριφορά, τα μέλη των εθνικών κυβερνήσεων δεν μπορούν να παραπεμφθούν ούτε να υποχρεωθούν να παραιτηθούν από τις θέσεις τους στην ΕΕ. Αυτό σημαίνει ότι τα άτομα που είναι ένοχα για τέτοιες πράξεις μπορούν κάλλιστα να συνεχίσουν με ατιμωρησία να συμμετέχουν

³³² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223>

³³³ Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

στα όργανα της ΕΕ και να λαμβάνουν αποφάσεις που επηρεάζουν όλους τους Ευρωπαίους πολίτες.

Ευρωπόλ

175. Ζητήθηκε από την Ευρωπόλ να συνδράμει την κυπριακή αστυνομία και έναν ακαδημαϊκό εμπειρογνώμονα στη διενέργεια εγκληματολογικής εξέτασης σε τρία επίπεδα του εξοπλισμού που βρέθηκε στο μαύρο βαν του Tal Dilian το 2019. Κατά τη διάρκεια της ακρόασης PEGA στις 30 Αυγούστου 2022, η Ευρωπόλ δεν έκανε καμία αναφορά σε αυτό, παρά τις ερωτήσεις των βουλευτών σχετικά με τον ρόλο της Ευρωπόλ στη διερεύνηση κατασκοπευτικού λογισμικού στην ΕΕ. Έκτοτε δεν έχει γίνει αναφορά στο θέμα.
176. Η Ευρωπόλ δεν διαθέτει αυτόνομες επιχειρησιακές εξουσίες και δεν μπορεί να ενεργεί χωρίς τη συγκατάθεση και τη συνεργασία των ενδιαφερόμενων κρατών μελών. Αυτό αποτελεί πρόβλημα όταν υπάρχουν σαφή αποδεικτικά στοιχεία για εγκληματικές πράξεις —όπως κυβερνοέγκλημα, διαφθορά και εκβίαση— αλλά οι εθνικές αρχές δεν διερευνούν το ζήτημα. Το πρόβλημα επιδεινώνεται όταν οι αρχές των κρατών μελών είναι οι ίδιες συνεργοί στα εγκλήματα.
177. Ωστόσο, η Ευρωπόλ απέκτησε πρόσφατα νέες εξουσίες που της επιτρέπουν να προτείνει προορατικά μια έρευνα, ακόμη και όταν αφορά έγκλημα που διαπράχθηκε μόνο σε ένα κράτος μέλος³³⁴, αλλά μέχρι στιγμής έχει φανεί απρόθυμη να κάνει χρήση των εξουσιών αυτών. Η Ευρωπόλ επιθυμεί να απολαμβάνει καλές σχέσεις με τις κυβερνήσεις, καθώς φοβάται ότι μια τέτοια πρωτοβουλία θα οδηγούσε σε κατάρρευση της συνεργασίας σε άλλους τομείς.
178. Στις 28 Σεπτεμβρίου 2022, η επιτροπή PEGA απέστειλε επιστολή στην Ευρωπόλ³³⁵, καλώντας την να κάνει χρήση των νέων εξουσιών της σύμφωνα με το άρθρο 6 του κανονισμού για την Ευρωπόλ³³⁶. Σε απαντητική επιστολή της με ημερομηνία 13 Οκτωβρίου 2022³³⁷, η Ευρωπόλ δήλωσε ότι «επικοινωνήσε με πέντε κράτη μέλη για να εξακριβώσει αν υπάρχουν διαθέσιμες σχετικές πληροφορίες σε εθνικό επίπεδο για την Ευρωπόλ και αν υπάρχει εν εξελίξει ή προβλεπόμενη ποινική έρευνα (ή, αντ' αυτού, άλλη έρευνα βάσει των εφαρμοστέων διατάξεων του εθνικού δικαίου). Εν τω μεταξύ, ένα από τα πέντε κράτη μέλη επιβεβαίωσε στην Ευρωπόλ την έναρξη ποινικών ερευνών υπό την εποπτεία των αρμόδιων δικαστικών αρχών, κάτι που έχει επίσης επαληθευτεί από την Eurojust». Δεν είναι γνωστό σε ποιες χώρες αναφέρεται η επιστολή, ούτε αν η προαναφερθείσα ποινική έρευνα από ένα κράτος μέλος αφορά την κατάχρηση κατασκοπευτικού λογισμικού από κυβερνήσεις κρατών μελών της ΕΕ ή από τρίτες χώρες.

³³⁴ Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

³³⁵ https://twitter.com/EP_PegaInquiry/status/1576855144574377984

³³⁶ “where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation.”

³³⁷ File no 1260379.

179. Η ΕΕ αποδεικνύεται σε απόλυτη αδυναμία έναντι ενδεχόμενης εγκληματικής δραστηριότητας εθνικών αρχών, ακόμη και αν αυτή επηρεάζει την ΕΕ.
180. Παραδόξως, σε αντίθεση με την Ευρώπη, οι ΗΠΑ διερευνούν ενεργά τη χρήση κατασκοπευτικού λογισμικού στην ΕΕ. Στις 5 Νοεμβρίου 2022, αναφέρθηκε ότι το FBI επισκέφθηκε την Αθήνα για να διερευνήσει «πόσο έχει διασπαρεί το παράνομο λογισμικό παρακολούθησης και ποιοι το διακίνησαν»³³⁸.

Ευρωπαϊκό δικαστικό σώμα

181. Το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) και το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΑΔ) διαδραματίζουν σημαντικό ρόλο στην προάσπιση της δημοκρατίας, του κράτους δικαίου και των θεμελιωδών δικαιωμάτων. Ωστόσο, μπορούν να ενεργήσουν μόνο κατόπιν καταγγελίας ή προδικαστικού ερωτήματος. Οι διαδικασίες είναι ιδιαίτερα χρονοβόρες και παρέχουν ελάχιστα συγκεκριμένα ένδικα μέσα σε μεμονωμένες υποθέσεις. Με την πάροδο των ετών, τα δικαστήρια έχουν δημιουργήσει έναν τεράστιο όγκο σχετικής νομολογίας, για παράδειγμα θεσπίζοντας πρότυπα για την παρακολούθηση. Ωστόσο, τα εν λόγω δικαστήρια δεν διαθέτουν μέσα για να διασφαλίσουν την εκτέλεση της απόφασής τους. Μέχρι στιγμής, έχει υποβληθεί στο ΕΔΑΔ μία καταγγελία σχετικά με την παράνομη χρήση κατασκοπευτικού λογισμικού³³⁹. Ωστόσο, ο δρόμος προς τα δικαστήρια του Στρασβούργου ή του Λουξεμβούργου είναι συχνά μακρύς, δαπανηρός και επαχθής, καθώς πρέπει πρώτα να εξαντληθούν όλες οι επιλογές που αφορούν εθνικές δικαστικές διαδικασίες. Αυτό ισχύει ιδίως σε περίπτωση που οι εθνικοί εισαγγελείς ή δικαστές δεν αναλάβουν ή αρνηθούν να αναλάβουν μια υπόθεση, οπότε τα κριτήρια για να χαρακτηριστεί παραδεκτή μια υπόθεση είναι άυστηρα.

Άλλα όργανα της ΕΕ

182. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, ο Ευρωπαίος Διαμεσολαβητής, το Ευρωπαϊκό Ελεγκτικό Συνέδριο και η Eurojust έχουν ελάχιστες αρμοδιότητες να ελέγχουν ή να παρεμβαίνουν σε περίπτωση παράνομης χρήσης ή εμπορίας κατασκοπευτικού λογισμικού από κυβερνήσεις κρατών μελών. Ορισμένα από τα μέλη τους ενδέχεται πράγματι να εμπλέκονται στα σκάνδαλα στο κράτος μέλος καταγωγής τους και στη συγκάλυσή τους. Επιπλέον, αυτό μπορεί να έχει αντίκτυπο στη λειτουργία και την ακεραιότητα των εν λόγω οργάνων της ΕΕ. Η Ευρωπαϊκή Εισαγγελία θα μπορούσε ενδεχομένως να παρέμβει όταν εμπλέκονται χρήματα της ΕΕ με οποιονδήποτε τρόπο.

³³⁸ <https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ>

³³⁹ Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

Europe's Watergate

In summer 2021, the Pegasus Project, a collective of investigative journalists, NGOs and researchers, revealed a list of 50,000 persons who had been targeted with mercenary spyware. Among them, journalists, lawyers, prosecutors, activists politicians, and even heads of state. The most dramatic case may well be that of Jamal Khashoggi, the Saudi journalist, who was savagely murdered in 2018 for his criticism of the Saudi regime. However, there were also many European targets on the list. Some had been targeted by actors outside the EU, but others were targeted by their own national governments. The revelations met with outrage around the world.

The scandal was quickly labelled "Europe's Watergate". However, rather than the political thriller "All the President's Men" about the burglary into the Watergate building in 1972, today's spyware scandal is reminiscent of the chilling movie "Das Leben der Anderen" (The Life of Others) depicting the surveillance of citizens by the totalitarian communist regime. Today's digital burglary with spyware is far more sophisticated and invasive, and hardly leaves any trace. The use of spyware goes far beyond the conventional surveillance of a person. It gives total access and control to the spying actors. Contrary to classic wiretapping, spyware does not only allow for real-time surveillance, but full, retroactive access to files and messages created in the past, as well as metadata about past communications. The surveillance can even be done at a distance, in countries anywhere in the world. Spyware can be used to essentially take over a smart-phone and extract all its contents, including documents, images and messages. Material thus obtained can be used not only to observe actions, but also to blackmail, discredit, manipulate and intimidate the victims. Access to the victim's system can be manipulated and fabricated content can be planted. The microphone and camera can be activated remotely and turn the device into a spy in the room. All the while, the victim is not aware of anything. Spyware leaves few traces on the victim's device, and even if it is detected it is nearly impossible to prove who was responsible for the attack.

The abuse of spyware does not just violate the right to privacy of individuals. It undermines democracy and democratic institutions by stealth. It silences opposition and critics, eliminates scrutiny and has a chilling effect on free press and civil society. It further serves to manipulate elections. The term "mercenary spyware" reflects very well the nature of the product and of the industry. Even failed attempts to infect a smart phone with spyware have political ramifications, and can harm the individual as well as democracy. Participation in public life becomes impossible without the certainty of being free and unobserved.

The spyware scandal is not a series of isolated national cases of abuse, but a full-blown European affair. EU Member State governments have been using spyware on their citizens for political purposes and to cover up corruption and criminal activity. Some went even further and embedded spyware in a system deliberately designed for authoritarian rule. Other Member State governments may not have engaged in abuse of spyware, but they have facilitated the obscure trade in spyware. Europe has become an attractive place for mercenary spyware. Europe has been the hub for exports to dictatorships and oppressive regimes, such as Libya, Egypt and Bangladesh, where the spyware has been used against human rights activists, journalists and government critics.

The abuse of spyware is a severe violation of all the values of the European Union, and it is testing the resilience of the democratic rule of law in Europe. In the past years, the EU has very rapidly built up its capacity to respond to external threats to our democracy, be it war, disinformation campaigns or political interference. By contrast, the capacity to respond to internal threats to democracy remain woefully underdeveloped. Anti-democratic tendencies can freely spread like gangrene throughout the EU as there is impunity for transgressions by national governments. The EU is ill equipped to deal with such an attack on democracy from within. On the one hand the EU is very much a political entity, governed by supranational laws and supranational institutions, with a single market, open borders, passportless travel, EU citizenship and a single Area of Security, Freedom and Justice. However, despite solemn pledges to European values, in practice those values are still considered very much a national matter. The spyware scandal mercilessly exposes the immaturity and weakness of the EU as a *democratic* entity. With regard to democratic values, the EU is built on the "presumption of compliance" by national governments, but in practice, it has turned into "pretence of compliance". The scenario of national governments deliberately ignoring and violating the EU laws, is simply not foreseen in the EU governance structures. The EU has not been equipped with instruments for such cases. The EU bodies have few powers, and even less appetite, to confront national authorities in case of transgressions, and certainly not in the delicate area of "national security". By intergovernmental logic, the EU institutions are subordinate to the national governments. However, without effective, meaningful supranational enforcement mechanisms, new legislation will be futile. Fixing the problem will require both regulatory measures and governance reforms.

The US is not spared from attacks on democracy from the inside, for example Watergate, and the siege of Congress on January 6th 2021, but it is equipped to respond forcefully. It has the powers to confront even the highest political leaders when they do not respect the law and the Constitution.

Indeed, following the 2021 revelations on spyware, the United States responded rapidly and with determination to the revelations of the Pegasus Project. The US Trade Department swiftly blacklisted NSO Group, the Department of Justice launched an inquiry, and strict regulation for the trade in spyware is in the pipeline. The FBI even came to Europe to investigate a spyware attack against a dual US-European citizen. Tech giants like Apple and Microsoft have launched legal challenges against spyware companies. Victims have filed legal complaints, prosecutors are investigating and parliamentary inquiries have been launched.

In contrast, with the exception of the European Parliament, the other EU institutions have remained largely silent and passive, claiming it is an exclusively national matter.

The European Council and the national governments are practising omertà. There has not been any official response to the scandal by the European Council. Member State governments have largely declined the invitation to cooperate with the PEGA committee. Some governments downright refused to cooperate, others were friendly and polite but did not really share meaningful information. Even a simple questionnaire sent to all Member States about the details of their national legal framework for the use of spyware, has hardly received any substantial answers. Literally on the eve of the publication of this draft report, the PEGA committee received a joint reply from the Member States via the Council, also without any substance.

The European Commission has expressed concern and asked a few Member State governments for clarifications, but only those cases where a scandal had already erupted at national level. The Commission has shared - reluctantly and piecemeal - information concerning the spyware attacks on its own Commission officials.

Europol has so far declined to make use of its new powers to initiate an investigation. Only after being pressed by the European Parliament, it addressed a letter to five Member States, asking if a police inquiry had started, and if they could be of assistance.

Europe's business

The abuse of spyware is mostly seen through the keyhole of national politics. That narrow national view obscures the full picture. Only by connecting all the dots, it becomes clear that the matter is profoundly European in all its aspects.

Although it is not officially confirmed, we can safely assume that all EU Member States have purchased one or more commercial spyware products. One company alone, NSO Group, has sold its products to twenty-two end-users in no fewer than fourteen Member States, among which are Poland, Hungary, Spain, The Netherlands and Belgium. In at least four Member States, Poland, Hungary, Greece, and Spain, there has been illegitimate use of spyware, and there are suspicions about its use in Cyprus. Two Member States, Cyprus and Bulgaria, serve as the export hub for spyware. One Member State, Ireland, offers favourable fiscal arrangements to a large spyware vendor, and one Member State, Luxemburg, is a banking hub for many players in the spyware industry. The home of the annual European fair of the spyware industry, the ISS World "Wiretappers Ball", is Prague in The Czech Republic. Malta seems to be a popular destination for some protagonists of the trade. A few random examples of the industry making use of Europe without borders: Intellexa has a presence in Greece, Cyprus, Ireland, France and Hungary, and its CEO has a Maltese passport and (letterbox) company. NSO has a presence in Cyprus and Bulgaria and it conducts its financial business via Luxemburg. DSIRF is selling its products from Austria, Tykelab from Italy, FinFisher from Germany (before it closed down).

The trade in spyware benefits from the EU internal market and free movement. Certain EU countries are attractive as an export hub, as - despite the EU's reputation of being a tough regulator - enforcement of export regulations is weak. Indeed, when export rules from Israel were tightened, the EU became more attractive for vendors. They advertise their business as being "EU regulated", using, as it were, their EU presence as a quality label. "EU" grants respectability. EU membership is also beneficial for governments who want to buy spyware: EU Member States are exempt from the individual human rights assessment required for an export license from the Israeli authorities, as EU membership is considered sufficient guarantee for compliance with the highest standards.

The sales side of the trade in spyware is opaque and elusive, but lucrative and booming. Company structures are conveniently, if not deliberately, complex to hide from sight undesirable activities and connections, including with EU governments. On paper the sector is regulated, but in practice it manages to circumvent many rules, not least because spyware is a product that may serve as political currency in international relations. Spyware companies are established in several countries, but many have been set up by former Israeli army and intelligence officers. Most vendors claim they sell only to state actors, although backstage,

some also sell to non-state actors. It is virtually impossible to get any information about those customers, or about the contractual terms and compliance.

Trade in, and use of spyware fall squarely within the scope of EU law and case law. The purchase and sale of spyware is governed by i.a. procurement rules and export rules such as the Dual Use Regulation. The use of spyware has to comply with the standards of the GDPR, EUDPR, LED and e-Privacy Directive. The rights of targeted persons are laid down in the Charter on Fundamental Rights and international conventions, notably the right to privacy and the right to a fair trial, and in EU rules on the rights of suspects and accused. The abuse of spyware will in many cases constitute cybercrime, and it may entail the crimes of corruption and extortion, all of which fall within the remit of Europol. If European funds are involved, the European Public Prosecutor has the mandate to act. The abuse of spyware may also affect police and justice cooperation, notably the sharing of information and implementation of the European arrest warrant and the Evidence Warrant.

The abuse of spyware affects the EU and its institutions directly and indirectly. Amongst those targeted with spyware, there were members of the EU Parliament, of the European Commission and of the (European) Council. Others were affected as "by-catch", indirect targets. Inversely, some of the "perpetrators" also sit on the (European) Council. In addition, manipulation of national elections with the use of spyware, directly affects the composition of EU institutions and the political balance in the EU governance bodies. The four or five governments accused of abusing spyware, represent almost a quarter of the EU population, so they carry considerable weight in the Council.

Spyware as part of a system

Spyware is not a mere technical tool, used ad hoc and in isolation. It is used as integral part of a system. In principle its use is embedded in a legal framework, accompanied by the necessary safeguards, oversight and scrutiny mechanisms, and means of redress. The inquiry shows that these safeguards are often weak and inadequate. That is mostly unintentional, but in some cases, the system has - in part or in whole - been bent or designed purposefully to serve as a tool for political power and control. In those cases, the illegitimate use of spyware is not an incident, but part of a deliberate strategy. The rule of law turns into the law of the ruler. The legal basis for surveillance can be drafted in in vague and imprecise terms, so as to legalise broad and unfettered use of spyware. *Ex-ante* scrutiny in the form of judicial authorisation of surveillance can easily be manipulated and gutted of any meaning, in particular in the case of politicisation, or state capture of the judiciary. Oversight mechanisms can be kept weak and ineffective, and brought under control of the governing parties. Legal remedy and civil rights may exist on paper, but they become void in the face of obstruction by government bodies. Complainants are refused access to information, even regarding the charges against them that supposedly justified their surveillance. Prosecutors, magistrates and police refuse to investigate and often put the burden of proof on the victims, expecting them to prove they have been targeted with spyware. This leaves the victims in a Catch-22 situation, as they are denied access to information. Government parties can tighten their grip on public institutions and the media, so as to smother meaningful scrutiny. Public or commercial media close to the government can serve as the channel for smear campaigns using the material obtained with spyware. "National security" is frequently invoked as a pretext for eliminating transparency and accountability. All these elements combined form a system, designed for control and oppression. This not only leaves individual victims

completely exposed and defenceless against an all-powerful government, it also means all vital checks and balances of a democratic society have been disabled.

Some governments have already reached this point, others are halfway there. Fortunately, most European governments will not go down this road. However, when they do, the EU in its current institutional and political set up, is not equipped to prevent or counter it. Spyware is the canary in the coal mine: exposing the dangerous constitutional weaknesses in the EU.

Secrecy

A major obstacle in detecting and investigating the illegitimate use of spyware is secrecy.

For most victims it is not possible to get any information about their case from the authorities. In many cases the authorities refer to national security grounds as justification for secrecy, in other cases they simply deny the existence of a file, or the files are destroyed. At the same time, prosecutors frequently refuse to investigate these cases, arguing that the victims do not have sufficient evidence. This is a vicious circle that leaves victims without recourse.

Governments most often refuse to disclose whether they have bought spyware and what type. Spyware vendors equally refuse to disclose who their customers are. Governments often resort to middlemen, proxies or personal connections, to purchase commercial spyware or spyware-related services, so as to conceal their involvement. They circumvent procurement rules and budget procedures, so as to not leave any government fingerprints.

Israel is an important hub of spyware companies, and responsible for issuing marketing and export licenses. Although Israel and Europe are close allies, Israel does not give out any information about the issuance (or repeal) of licenses for spyware to EU countries, despite the fact that it is being used to violate the rights of European citizens and to undermine our democracy.

Freedom of information requests by journalists yield little to no information. Dedicated scrutiny and oversight bodies, like the data protection authorities or the court of auditors, are struggling as well to get information. Independent oversight over secret services is notoriously weak and often non-existent. Parliamentary inquiry committees are often stonewalled by the government parties. Judicial inquiries focus on hacks by third countries, not on illegitimate use by EU governments. Journalists reporting on the issue are facing strategic lawsuits against public participation (SLAPPs), verbal attacks by politicians or smear campaigns. The courageous and diligent journalists who are unearthing the facts of the scandal deserve our respect and gratitude. They are Europe's Woodwards and Bernsteins. Furthermore, adequate whistleblower protection is still not in place in all Member States. In some cases victims of a spyware attack themselves wish to remain silent, as they do not wish to expose the parties behind the attack, for fear of retaliatory actions, or of the consequences of compromising material coming to the surface.

Next steps

At a time when European values are under attack from an external aggressor, it is all the more important to bolster our democratic rule of law against attacks from the inside. The findings of the PEGA inquiry are shocking and they should alarm every European citizen. It is evident that the trade in, and use of spyware should be strictly regulated. The PEGA committee will

make a series of recommendations to that effect. However, there should equally be initiatives for institutional and political reforms enabling the EU to actually enforce and uphold those rules and standards, even when they are violated by Member States themselves. The EU has to rapidly develop its defence lines against attacks on democracy from within.