



Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware

2022/2077(INI)

28.11.2022

ENTWURF EINES BERICHTS

über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (2022/2077(INI))

Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware

Berichterstatlerin: Sophie in 't Veld

INHALT

	Seite
VORLÄUFIGE ERGEBNISSE.....	3
BEGRÜNDUNG.....	56

VORLÄUFIGE ERGEBNISSE

der Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (2022/2077(INI))¹

Das Europäische Parlament,

- gestützt auf Artikel 226 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV),
- gestützt auf seinen Beschluss vom 10. März 2022 über die Einsetzung, die Zuständigkeiten, die Mitgliederzahl und die Mandatszeit des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware und die Festlegung des Gegenstands der Untersuchung,
- gestützt auf den Bericht des Untersuchungsausschusses zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (A9-0000/2022).

I. Die Verwendung von Spähsoftware in der EU

I.A Polen

1. Der Einsatz von kommerzieller Spähsoftware in Polen wurde erstmals im Dezember 2021 einer breiten Öffentlichkeit bekannt. Die damit einhergehenden Gefahren sind nur im Gesamtzusammenhang vollends begreiflich. Bei kommerzielle Spähsoftware handelt es sich nicht nur um ein technisches Instrument, das isoliert und in zufällig gewählten Situationen eingesetzt wird. Sie ist vielmehr integraler und unabdingbarer Bestandteil eines Systems, das speziell für die ungehinderte Überwachung und Kontrolle der Bürger entwickelt wurde. Die rechtlichen, institutionellen und politischen Bausteine dieses Systems wurden zielgerichtet und methodisch zusammengestellt, um einen kohärenten und äußerst effektiven Rahmen zu schaffen. Es offenbart sich erst ein vollständiges Bild dieses sorgfältig geplanten Systems, wenn man sämtliche Punkte miteinander verbindet.
2. Die Möglichkeiten der legalen Überwachung wurden in Polen nahezu unbegrenzt ausgeweitet. Die Rechte der Opfer wurden auf ein Minimum beschnitten, und der Rechtsweg ist in der Praxis bedeutungslos geworden. Es ist so gut wie keine wirksame Ex-ante- und Ex-post-Kontrolle gegeben und jegliche unabhängige Aufsicht ist praktisch ausgeschaltet. Mitglieder der polnischen Regierung und Parteiloyalisten haben die direkte oder indirekte Kontrolle über die wichtigsten Positionen innerhalb des Systems. Die mit Spähsoftware gesammelten Informationen werden in Hetzkampagnen gegen Regierungskritiker und Oppositionelle über die Staatsmedien, die sich in der Kontrolle der Regierung befinden, verwendet. Es wurden sämtliche

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

Sicherheitsvorkehrungen beseitigt. Die Regierungsparteien haben die volle Kontrolle und die Opfer können sich an niemanden wenden.

Erwerb von Pegasus

3. Im November 2016 nahmen die ehemalige Ministerpräsidentin und heutige Europaabgeordnete Beata Szydło und der ehemalige Außenminister Witold Waszczykowski an einem Abendessen im Haus des damaligen israelischen Ministerpräsidenten Benjamin Netanjahu teil². Im darauffolgenden Jahr, im Juli, trafen sich Szydło und Netanjahu mit den Regierungschefs der Länder der Visegrád-Gruppe. Angeblich sprachen sie über die „Stärkung der Zusammenarbeit im Bereich der Innovation und der Hochtechnologien“ und über „Fragen im Zusammenhang mit der Sicherheit der Bürger im weiteren Sinne“³. Kurz nach diesem Treffen im Jahr 2017 wurde Pegasus nach einem Treffen zwischen Premierminister Mateusz Morawiecki, dem ungarischen Premierminister Viktor Orbán und Netanjahu von der polnischen Regierung erworben⁴. Trotz anfänglicher Dementis bestätigte PiS-Chef Jarosław Kaczyński im Januar 2022 den Erwerb der Spähsoftware durch die polnische Regierung^{5 6 7}.

Rechtlicher Rahmen

4. Im Jahr 2014 führte das Verfassungsgericht eine Überprüfung des Polizeigesetzes und anderer bestehender Gesetze zur Überwachung der Bürger durch, die als unvereinbar mit der polnischen Verfassung angesehen wurden⁸. Das Gericht veröffentlichte abschließend ein Urteil mit konkreten Empfehlungen und einem Zeitplan über 18 Monate, innerhalb deren die Gesetzesänderungen umgesetzt werden sollten⁹. Nach den Wahlen 2015 führte die neue Regierung Gesetzesänderungen ein. Das daraus resultierende Gesetz vom 15. Januar 2016 zur Änderung des Polizeigesetzes von 1990 und einiger anderer Gesetze (im Folgenden „das Polizeigesetz von 2016“) hat jedoch keine der vom Verfassungsgerichtshof geforderten Gesetzeslücken behoben¹⁰. Stattdessen hat das Polizeigesetz von 2016 die ohnehin schon schwachen Bestimmungen, die weder die Rechte der Bürger schützen noch eine angemessene Aufsicht schaffen, weiter abgeschwächt und die immer größer werdende Kluft zwischen dem polnischen Gesetzgeber und der Rechtsstaatlichkeit vergrößert.

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 Euoparlement 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>

Anti-Terror-Gesetz 2016

5. Neben dem Polizeigesetz von 2016 hat die polnische Regierung 2016 auch ein Gesetz zur Überwachung ausländischer Bürger verabschiedet, das sie als „Anti-Terror-Gesetz“ bezeichnet. Die Artikel des Gesetzes sehen vor, dass nicht-polnische Bürger ohne ihre Zustimmung für einen Zeitraum von drei Monaten – unter anderem durch das Abhören von Telefonen, die Erfassung von Fingerabdrücken, biometrischen Fotos und DNA sowie die Verpflichtung zur Registrierung von Prepaid-Telefonkarten – überwacht werden können, wenn ihre Identität als „zweifelhaft“ gilt¹¹. Der Generalstaatsanwalt ist für die Anordnung der Vernichtung von nicht relevantem Unterlagen zuständig – Zbigniew Ziobro, der Justizminister der PiS, hat dieses Amt derzeit inne^{12 13}.

Strafprozessordnung

6. Im Juli 2015 wurde in Polen das Gesetz zur Änderung der Strafprozessordnung eingeführt, um sicherzustellen, dass unrechtmäßig erlangte Beweise nicht in Strafverfahren verwendet werden können. Das Gesetz wurde jedoch später, im März 2016, umgeschrieben, um Artikel 168a aufzunehmen¹⁴. Dieser Zusatz stellt nun sicher, dass rechtswidrig erlangte Beweismittel bzw. „Früchte des vergifteten Baumes“, wie z. B. Informationen, die durch die Verwendung von Pegasus gewonnen wurden, vor Gericht eingebracht werden können¹⁵.

Telekommunikationsgesetz vom 16. Juli 2004

7. Das polnische Telekommunikationsgesetz sieht vor, dass die Polizei kostenlos und in bestimmten Fällen auch ohne das Zutun von Mitarbeitern der Telekommunikationsgesellschaften auf Telekommunikationsdaten zugreifen kann¹⁶. Dies kann unter dem vagen Vorwand der „Aufdeckung von Straftaten“ geschehen. Der Staatsanwalt entscheidet dann, wie er nach Erhalt dieser Daten weiter vorgehen will, und tatsächlich wird ihm in dem Gesetz eine beträchtliche Machtfülle eingeräumt – eine politische Entscheidung, wenn man bedenkt, dass Ziobro dieses Amt derzeit innehat^{17 18}.

Ex-ante-Kontrolle

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, p. 18 [hereinafter HFHR Report].

8. Obwohl die Überwachung in Polen grundsätzlich einer richterlichen Genehmigung bedarf, dient das Genehmigungsverfahren in der Praxis nicht mehr als Schutz vor Missbrauch, sondern eher als Mittel, um der Überwachung zu politischen Zwecken einen Anschein von Legalität zu verleihen. Es ist nicht ausdrücklich klargestellt worden, ob die Überwachung eines der bisher bekannten Opfer von Pegasus mit richterlicher Genehmigung erfolgte. Anträge auf richterliche Genehmigung einer Überwachungsmaßnahme werden von den Sonderdiensten gestellt¹⁹. Für die Beurteilung des Antrags stehen den Richtern nur die vom Antragsteller (d. h. den Sonderdiensten) eingereichten Informationen zur Verfügung, und der Staatsanwalt entscheidet, welche Unterlagen vorzulegen sind²⁰. Bei den Informationen handelt es sich oft nur um eine Zusammenfassung, die manchmal nicht einmal die grundlegendsten Details über die Zielperson (Name, Beruf, die Straftat, derer sie verdächtigt wird) und die anzuwendenden Überwachungsmethoden enthält.

Ex-post-Kontrolle

9. Die parlamentarische Kontrolle ist in Polen praktisch nicht vorhanden. Als die PiS 2015 an die Macht kam, wurde das traditionelle System, bei dem die Oppositionspartei den Vorsitz des parlamentarischen Überwachungsausschusses für die Sonderdienste (KSS) übernimmt, abgelehnt und die Regierungsparteien setzten die PiS-Mitglieder Waldemar Andzel als Vorsitzenden und Herrn Jarosław Krajewski als stellvertretenden Vorsitzenden ein²¹. Die Regierungsparteien haben die absolute Mehrheit im Ausschuss²². Darüber hinaus hat die regierungsfreundliche Mehrheit im Sejm die Forderung nach einer parlamentarischen Untersuchung der Vorwürfe des unrechtmäßigen Einsatzes von Spähsoftware abgelehnt^{23 24 25 26 27}. Der Senat hingegen, in dem die Regierungsparteien keine Mehrheit haben, hat zwar einen Untersuchungsausschuss eingesetzt, verfügt jedoch nicht über die Untersuchungsbefugnisse des Sejm²⁸.

Berichterstattung

10. Nach dem Polizeigesetz von 2016 ist die Polizei lediglich verpflichtet, den Gerichten halbjährliche Berichte über die Anzahl der Erhebungen von Telekommunikations-, Post- oder Internetdaten zusammen mit ihrer rechtlichen Begründung (in Bezug auf den

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, p. 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, p. 27, footnote 220.

Schutz von Menschenleben oder Gesundheit oder zur Unterstützung von Such- und Rettungsmaßnahmen) vorzulegen²⁹. Diese Berichte können nur im Nachhinein erstellt werden und werden nicht öffentlich gemacht. Wenn die Vorlage beanstandet wird, legt das Gericht innerhalb von 30 Tagen eine Antwort vor, kann aber nicht die Vernichtung der Daten anordnen, selbst wenn es Unvereinbarkeiten mit dem Gesetz feststellt. Kritisch anzumerken ist, dass dieses aufsichtliche Handeln nur fakultativ und nicht obligatorisch sind³⁰.

Rechtsbehelf

11. Bislang hat die polnische Staatsanwaltschaft noch keine Ermittlungen eingeleitet, obwohl es zahlreiche Beweise für schwere Straftaten gibt. Es scheint, dass nur der Fall der Staatsanwältin Ewa Wrzosek von den Gerichten aufgegriffen wurde. Wrzosek reichte ihren Fall zunächst bei der Staatsanwaltschaft ein. Als diese sich jedoch offiziell weigerte, den Fall zu übernehmen, legte sie bei den Gerichten Berufung ein. Ende September 2022 wies das Warschauer Bezirksgericht (Mokotów) die Staatsanwaltschaft an, eine Untersuchung einzuleiten³¹.

Öffentliche Kontrolle

12. Unabhängige Medien sind ein weiteres Element der demokratischen Kontrolle und üben eine öffentliche Kontrolle aus. Im Fall des Einsatzes von Spähsoftware hat sich der polnische öffentlich-rechtliche Rundfunk, der weitgehend von den Regierungsparteien kontrolliert wird, jedoch mit der Veröffentlichung von Material, das von den Smartphones mehrerer Zielpersonen, darunter Senator Brejza, stammt, zu einem Komplizen des illegalen Überwachungsskandals gemacht. Die Veröffentlichung von Informationen, die bei einer Überwachungsmaßnahme der Sonderdienste erlangt wurden, stellt an sich bereits eine strafbare Handlung dar. Dennoch wurden weder von der Polizei noch von der Staatsanwaltschaft Maßnahmen ergriffen.

Politische Kontrolle

13. Viele Schlüsselpositionen in der gesamten Kontrollkette werden von Mitgliedern oder Loyalisten der Regierungsparteien besetzt. Der Innenminister und Koordinator für Sonderdienste, Mariusz Kamiński, wurde 2015 wegen Machtmissbrauchs zu einer dreijährigen Haftstrafe verurteilt³². Unmittelbar nach den Parlamentswahlen 2015 begnadigte ihn Präsident Duda jedoch auf höchst irreguläre Weise, was unter anderem vom Obersten Gerichtshof Polens, dem EuGH, der Venedig-Kommission und dem US-Außenministerium verurteilt wurde. Dies lässt Zweifel an seiner Unabhängigkeit und Neutralität aufkommen. Herr Kaminski hat es abgelehnt, sich mit dem Sonderuntersuchungsausschuss des Europäischen Parlaments zum Einsatz von Pegasus

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, p. 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.

und ähnlicher Überwachungs- und Spähsoftware zu treffen oder mit ihm zusammenzuarbeiten³³.

Die Ziele

14. Im Rahmen von Untersuchungen von Associated Press und den Forschern von Citizen Lab an der Universität von Toronto wurde aufgedeckt, dass 2019 mindestens drei Personen in Polen ins Visier genommen wurden³⁴. Bei den Zielpersonen handelte es sich um den oppositionellen Senator Krzysztof Brejza, den Rechtsanwalt Roman Giertych und die Staatsanwältin Ewa Wrzosek. Sie wurden mit der Spähsoftware „Pegasus“, die die Regierung 2017 erworben hatte, gehackt³⁵. Die Regierung hat zwar den Erwerb der Software von der NSO-Gruppe bestätigt, aber nicht offiziell bestätigt, dass bestimmte Personen damit ausgespäht wurden. Keine der unten genannten Zielpersonen wurde formell eines Verbrechens angeklagt, noch wurden sie zur Befragung vorgeladen oder ein Antrag auf Aufhebung der Immunität der Zielpersonen, die politische Ämter bekleiden, gestellt.

Senator Krzysztof Brejza

15. Senator Krzysztof Brejza war als Wahlkampfleiter der Oppositionspartei Civic Platform tätig, als er Opfer eines Hackerangriffs mit Spähsoftware wurde³⁶. Es gab 33 Angriffe auf Brejzas Telefon in der Zeit, in der er die Kampagne der Civic Platform 2019 leitete. Die Angriffe begannen am 26. April 2019 und dauerten bis zum 23. Oktober 2019, nur wenige Tage nach dem Ende des Wahlzyklus, an³⁷.

Roman Giertych

16. Roman Giertych wurde in den letzten Wochen vor den Parlamentswahlen 2019 mit der Spähsoftware „Pegasus“ ausgespäht. Zwischen September und Dezember 2019 wurde Giertych ganze 18 Mal gehackt. Die meisten Angriffe fanden kurz vor dem Wahltermin am 13. Oktober 2019 statt. Zu dieser Zeit war er als Anwalt des Oppositionsführers Donald Tusk tätig. In dieser Zeit vertrat Giertych auch Radek Sikorski, den ehemaligen Außenminister und derzeitiges Mitglied des Europäischen Parlaments für die Europäische Volkspartei (PPE). Sikorski untersuchte die Verwicklung Kaczynskis und seiner Verbündeten in illegale Abhörmaßnahmen, bei denen Gespräche des Ministers aufgenommen und veröffentlicht wurden³⁸.

Ewa Wrzosek

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.

17. Die Staatsanwältin Ewa Wrzosek wurde zwischen dem 24. Juni und dem 19. August 2020 gleich sechs Mal Opfer eines Hackerangriffs mit der Spionagesoftware „Pegasus“³⁹. Wrzosek ist Mitglied der Lex Super Omnia, einer Gruppe von Staatsanwälten, die sich für die Unabhängigkeit der Staatsanwaltschaft einsetzen. Sie leitete zu dieser Zeit Untersuchungen zur Sicherheit der Durchführung von Präsidentschaftswahlen inmitten der weltweiten COVID-19-Pandemie. Dieser Fall wurde ihr entzogen und anschließend fallen gelassen, und sie wurde mit nur 48-stündiger Vorankündigung in die Stadt Srem transferiert. Der PiS-Generalstaatsanwalt Zbigniew Ziobro verfügt über eine wachsende Macht, die es ihm auch ermöglicht, zu entscheiden, dass bestimmte Fälle nicht verfolgt oder nachgeordnete Staatsanwälte von Fällen abgezogen werden⁴⁰. Als Wrzosek nach Warschau zurückkehrte, wurde sie Opfer eines Angriffs mit Spähsoftware. Die polnischen Behörden waren nicht dazu bereit, die Verantwortung für den Angriff zu übernehmen bzw. diese zu leugnen^{41 42}.

Andere mögliche Ziele

Oberster Rechnungshof

18. Als eine der ältesten Institutionen in Polen hat der Oberste Rechnungshof („NIK“) die Aufgabe, die öffentlichen Ausgaben und die Verwaltung der öffentlichen Dienste zu überwachen. Marian Banās leitet die Behörde zurzeit⁴³. Er hat sich wiederholt gegen die Aushöhlung der Rechtsstaatlichkeit im Land ausgesprochen und die PiS-Regierung in den erwähnten Hacking-Fällen zur Rechenschaft gezogen – und das obwohl er früher als Verbündeter der PiS-Partei galt⁴⁴.

Mitglieder der PiS-Partei

19. Es gibt die Vermutung, dass die Spähsoftware „Pegasus“ für das „präventive Abhören“ von Anführern und Organisatoren von Straßenprotesten eingesetzt wurde, die zum Protest gegen die von der PiS-Partei durchgeführten Reformen des Verfassungsgerichts stattfanden. Es wurden jedoch womöglich nicht nur Gegner der Regierungspartei mithilfe der Spähsoftware „Pegasus“ ausgespäht. Adam Hofman, ehemaliger Sprecher der PiS-Partei, beschuldigte ebenfalls seine eigenen Kollegen, ihn 2018 bespitzelt zu haben – nach dem Erwerb der Spähsoftware gehörte er zu den ersten Zielpersonen, die damit ausgespäht wurden. Hofman gründete nach seinem Ausschluss aus der PiS-Partei das PR-Unternehmen R4S^{45 46}. Berichten zufolge verärgerte diese Aktion die

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, p. 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.

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.

Regierungspartei und machte Hofman zur Zielscheibe von Überwachungsmaßnahmen. Ihm zufolge wurden die über ihn erhaltenen Informationen anschließend in einer Verleumdungskampagne gegen ihn verwendet.

Verbindung mit Verleumdungskampagnen

20. Wochenlang war Senator Brejza das Ziel einer Verleumdungskampagne, die sich auf Material stützte, das durch den Einsatz von Spähsoftware gewonnen wurde. Die Tatsache, dass dieses Material über das öffentliche Fernsehen veröffentlicht wurde, ist besonders alarmierend. Wie ist es zu erklären, dass ein öffentlich-rechtlicher Sender Zugang zu solchem Material erhält? Sollte es sich – wie die Regierung es halbherzig zu behaupten scheint – bei dem Hacking von Senator Brejza mit der Spähsoftware „Pegasus“ tatsächlich um eine Angelegenheit der nationalen Sicherheit gehandelt haben, würde die Weitergabe von Material, das im Rahmen einer geheimen Sicherheitsoperation erlangt wurde, ein sehr schweres Verbrechen darstellen. Die Tatsache, dass auch der öffentlich-rechtliche Rundfunk von der Regierungspartei beherrscht wird, lässt eher eine von den Regierungsparteien orchestrierte Verleumdungskampagne vermuten.

I. B. Ungarn

21. Ungarn war eines der ersten Länder, das in den europäischen Skandal um die Spähsoftware „Pegasus“ verwickelt war. Im Jahr 2021 enthüllte das Pegasus Project, dass sich unter den 50.000 Telefonnummern, die durch das Produkt von NSO möglicherweise gehackt wurden, auch eine Reihe ungarischer Telefonnummern befanden. Inzwischen wurde von Amnesty International bestätigt⁴⁷, dass über 300 Ungarn mithilfe der Spähsoftware „Pegasus“ bespitzelt worden sind, darunter politische Aktivisten, Journalisten, Anwälte, Unternehmer und ein ehemaliger Minister⁴⁸.

Erwerb von Pegasus

22. Das ungarische Innenministerium erwarb die Spähsoftware „Pegasus“ von der NSO Group im Jahr 2017, kurz nachdem Orbán sich mit dem polnischen Premierminister Mateusz Morawiecki und dem ehemaligen israelischen Premierminister Benjamin Netanjahu getroffen hatte⁴⁹ ⁵⁰. Das ungarische Innenministerium räumte dies erst am 8. April 2021 ein, als der Vorsitzende des parlamentarischen Ausschusses für Verteidigung und Strafverfolgung, Lajos Kósa, den Erwerb von Pegasus durch die Fidesz-Regierung bestätigte⁵¹. – Kósa beharrte jedoch weiterhin darauf, dass die Spähsoftware nie gegen ungarische Bürger eingesetzt wurde⁵².

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 Financieele 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.

⁵² DW, [Hungary admits to using NSO Group’s Pegasus spyware](#), 4 November 2021.

Rechtlicher Rahmen

23. Die rechtlichen Instrumente, die den Einsatz von Spähsoftware in Ungarn regeln, gehören zu den schwächsten Bestimmungen in Europa^{53 54}. Das System verstößt in eklatanter Weise gegen die europäischen Vorschriften und Grundsätze, die von der Europäischen Menschenrechtskonvention (EMRK) und den Urteilen des EGMR⁵⁵ für die Überwachung der Bürger festgelegt wurden, obwohl die Regierung versichert, in allen Fällen rechtmäßig gehandelt und sich vollständig an die Gesetze gehalten zu haben^{56 57}. Das *Gesetz CXXV von 1995 über die nationalen Sicherheitsdienste* (im Folgenden „das Gesetz“) regelt derzeit den Einsatz von Spähsoftware in Ungarn⁵⁸ und stellt eher ein Instrument zur Kontrolle und Machtausübung für die Regierung als ein Schutzschild für die Rechte und die Privatsphäre der Bürger dar. Es enthält nicht nur keine Verpflichtung zur Benachrichtigung der überwachten Personen, sondern schreibt ausdrücklich vor, dass die Zielpersonen von der autorisierenden Partei nicht darüber informiert werden dürfen, dass sie ausspioniert werden⁵⁹. Die Verpflichtung zur Benachrichtigung der Zielpersonen wurde in der Rechtssache *Klass and others/ Deutschland*⁶⁰ vor dem EGMR eindeutig festgestellt. Die ungarische Regierung hat es – ebenso wie Polen und viele andere Länder in der EU – versäumt, dieses Urteil umzusetzen.

Ex-ante-Kontrolle

24. Gemäß dem Gesetz ist die Überwachung durch den Sonderdienst für nationale Sicherheit (SNSS) unter Verwendung von Spähsoftware in den meisten Fällen von der Genehmigung des Justizministers und in einigen besonderen Fällen von dem vom Präsidenten des Landgerichts Budapest-Hauptstadt benannten Richter abhängig^{61 62}. Gegen diese Entscheidungen kann kein Rechtsbehelf eingelegt werden, und es findet praktisch keine Beaufsichtigung des Prozesses statt^{63 64}.

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, 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, p. 20.

⁶³ Act CXXV of 1995 on National Security Services, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, 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, p. 26.

Ex-post-Kontrolle

25. Im November 2021 führten zwei Ausschüsse des Senats auf Drängen der Opposition Anhörungen über den Einsatz von Spähsoftware in Ungarn und die angeblich politisch motivierte gezielte Überwachung von Bürgern durch die Regierung im Besonderen durch. Es wurde anschließend berichtet, dass die Regierungsvertreter darauf bestanden, dass alle Überwachungen über die entsprechenden Kanäle genehmigt wurden, sich aber weigerten, sich dazu zu äußern, ob Journalisten oder Politiker zur Zielscheibe geworden waren. Genauer zum Gesagten ist jedoch nicht bekannt, da die Regierungspartei das Protokoll der Anhörungen bis 2050 unter Verschluss hält.

Rechtsbehelf

26. Als die Pegasus-Abhöraffaire in Ungarn ans Licht kam, wurde klar, dass die Regierung vorrangig Journalisten ins Visier genommen hatten – auch wenn sie sich bis heute weigert, dies einzuräumen oder zu dementieren. Infolgedessen leitete eine Gruppe von sechs Journalisten und Aktivisten Anfang 2022 in Ungarn ein Gerichtsverfahren gegen den Staat und die Hungarian National Authority for Data Protection and Freedom of Information ein. Die Hungarian Civil Liberties Union (HCLU) wird die Journalisten Brigitta Csikász, Dávid Dercsényi, Dániel Németh und Szabolcs Panyi sowie Adrien Beauduin, einen belgisch-kanadischen Doktoranden und Aktivisten, vertreten. Der sechste Kläger möchte anonym bleiben. Die HCLU arbeitet auch mit Eitay Mack in Israel zusammen, um eine Klage beim Generalstaatsanwalt einzureichen, damit eine Untersuchung gegen die NSO Group eingeleitet wird⁶⁵.

Politische Kontrolle

27. Die politische Kontrolle über den Einsatz der Überwachung in Ungarn ist allumfassend und total. Das von Orbán geführte Fidesz-Regime hat ein Kontrollsystem eingerichtet, mit dem es Anwälte, Journalisten, politische Gegner und Organisationen der Zivilgesellschaft mit Leichtigkeit und ohne Angst vor Regressansprüchen ins Visier nehmen kann. Darüber hinaus können sie dank ihrer Kontrolle über fast alle ungarischen Medien weiterhin ihre eigene Version der Wahrheit verbreiten und verhindern, dass ein Großteil der von den Medien durchgeführten öffentlichen Untersuchungen die ungarischen Bürger erreicht.

Die Ziele

28. Es war von dem Moment an, als der Abhörskandal in Ungarn ans Licht kam, klar, dass das Vorgehen der Regierung politisch motiviert war. Berichten zufolge enthielten die Ergebnisse des Pegasus-Projekts die Telefonnummern von über 300 Personen⁶⁶. Darunter befanden sich mindestens fünf Journalisten, zehn Anwälte und ein Oppositionspolitiker sowie Aktivisten und Inhaber einflussreicher Unternehmen⁶⁷. Auch wenn nicht alle zu den auf der Liste aufgeführten Telefonnummern zugehörigen

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

⁶⁶ Washington 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.

Telefone mit an Sicherheit grenzender Wahrscheinlichkeit gehackt wurde, ist es doch ein aufschlussreicher Einblick in das methodische und systematische Vorgehen und die Haltung der Regierung Orbán gegenüber den Grundrechten und der Medienfreiheit. Seit diesem Zeitpunkt im Jahr 2021 wurde mittlerweile bestätigt, dass eine Reihe von Zielpersonen tatsächlich mit Spähsoftware bespitzelt wurde.

Szabolcs Panyi

29. Das Telefon des Journalisten und Redakteurs Szabolcs Panyi wurde im Rahmen seiner Tätigkeit bei Direkt36 gehackt. Als eine der wenigen verbliebenen unabhängigen Nachrichtenquellen in Ungarn stellt sie in den Augen der Regierungspartei ein Hauptziel für solche Angriffe dar. Panyi ist ein bekannter und geschätzter Journalist. Daraus folgt, dass nicht nur wichtige Informationen direkt über Panyi abgefangen werden können, sondern auch viele der Kontakte und Quellen auf seinem Telefon einen wertvollen Beifang für die Regierung darstellen könnten.

Zoltán Varga

30. Als CEO und Vorsitzender der Central Media Group ist Zoltán Varga der Eigentümer von Ungarns größter verbleibender unabhängiger Nachrichtenseite 24.hu. Nachdem die Orbán-Regierung im Jahr 2020 die Übernahme des Hauptkonkurrenten Index.hu eingeleitet hatte, blieb Varga als „letzter Mann“ übrig und bot der Regierungspartei weiterhin die Stirn.

Adrien Beauduin

31. Adrien Beauduin tauchte 2018 auf dem Radar des Orbán-Regimes auf, als er an der Central European University (CEU) in Gender Studies promovierte. Die Institution wurde von George Soros gegründet und die Regierung versuchte damals, sie aus Ungarn zu verbannen, ebenso wie das Fachgebiet der Gender Studies im Allgemeinen⁶⁸. Nach seiner Teilnahme an einer Demonstration in Budapest wurde Beauduin in einer als politisch motiviert angesehenen Aktion verhaftet und wegen Angriffs auf einen Polizeibeamten angeklagt. Er bestreitet den Sachverhalt vehement⁶⁹. Berichten zufolge lagen im Wesentlichen keine Beweise gegen Beauduin vor. Die vorgelegten Beweise sollen wortwörtlich von der Aussage eines Polizeibeamten in einem anderen Fall kopiert worden sein⁷⁰.

Ilona Patócs

32. Die Anwältin Ilona Patócs wurde im Sommer 2019 mutmaßlich mithilfe der Spätsoftware „Pegasus“ bespitzelt, als sie einen Mandanten in einem hochkarätigen, langwierigen Verfahren wegen Mordes vertrat⁷¹. Aufgrund der Art des von ihr

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.

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-celponnta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/>, 31 March 2022.

verwendeten Mobilgeräts konnte jedoch nicht ermittelt werden, ob der Hacking-Angriff erfolgreich war bzw. wann genau dieser stattfand. Ihr Mandant, István Hatvani, hatte bereits sieben Jahre wegen Mordes verbüßt – die Verurteilung war laut Patócs politisch motiviert⁷². Obwohl eine andere Person nach dem Prozess den Mord gestand, schickte das ungarische Berufungsgericht Hatvani zurück ins Gefängnis, um seine ursprüngliche Strafe fertig abzusitzen. Die Liste der Telefonnummern, die potenziell mit der Spähsoftware „Pegasus“ abgehört wurden, umfasst auch die einer Reihe von Anwälten, darunter auch die des Präsidenten der ungarischen Anwaltskammer János Bánáti⁷³. Dieses Vorgehen zeigt, dass die Regierung das Anwaltsgeheimnis zwischen Anwälten und ihren Mandanten eindeutig missachtet.

Weitere Ziele

33. Auch Personen aus dem Umfeld der Regierungspartei wurden mit Spähsoftware bespitzelt. Die unabhängige ungarische Zeitung Direkt36 berichtete im Dezember 2021, dass ein Leibwächter des Präsidenten und engen Verbündeten von Orbán János Áder Opfer eines Hackerangriffs mit der Spähsoftware „Pegasus“ geworden war. Der Direkt36-Journalist Szabolcs Panyi, der Opfer eines Angriffs mit Spähsoftware wurde, äußerte sich dahingehend, dass diese Art von Ausspähung vor allem auf die wachsende Paranoia des ungarischen Premierministers zurückzuführen sei.

Spähsoftware-Firmen

34. Die ungarische Regierung erwarb nicht nur die Spähsoftware „Pegasus“ und setzte diese gegen ihre Bürger ein. Ungarn diente auch als Brutstätte für andere Unternehmen der Geheimdienst-Branche. Bei der Firma Black Cube handelt es sich um einen privaten israelischen Nachrichtendienst, für den ehemalige Mitarbeiter des Mossad, des israelischen Militärs und der israelischen Geheimdienste tätig sind⁷⁴. Auf seiner eigenen Website bezeichnet sich das Unternehmen als kreativer Nachrichtendienst⁷⁵, der „maßgeschneiderte Lösungen für komplexe geschäftliche und rechtliche Herausforderungen findet⁷⁵. Black Cube war in eine Reihe von öffentlichen Kontroversen um Hackerangriffe verwickelt, unter anderem in den USA und Rumänien⁷⁶. Außerdem wurde aufgedeckt, dass das Unternehmen mit der NSO Group und Pegasus Spyware in Verbindung steht. Nach dem großen öffentlichen Druck in Bezug auf die Beauftragung von Black Cube durch NSO, um ihre Gegner ins Visier zu nehmen, räumte der ehemalige CEO von NSO Shalev Hulio ein, Black Cube in mindestens einem Fall in Zypern beauftragt zu haben.

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/>

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

35. In diesem Jahr wurde Griechenland von einer Reihe von Enthüllungen über den offensichtlich politisch motivierten Einsatz von Spähsoftware erschüttert. Am 26. Juli 2022 reichte Nikos Androulakis, Mitglied des Europäischen Parlaments und Vorsitzender der griechischen Oppositionspartei PASOK, bei der Staatsanwaltschaft des Obersten Gerichtshofs eine Beschwerde über den Versuch ein, sein Mobiltelefon mit der Spähsoftware „Predator“ zu infizieren⁷⁷. Der Versuch, sein Mobiltelefon mit einer Spähsoftware zu infizieren, wurde bei einer Überprüfung des Telefons von Androulakis durch den IT-Dienst des Europäischen Parlaments entdeckt⁷⁸. Die versuchten Hacking-Angriffe fanden in der Zeit statt, als Androulakis für den Vorsitz der Oppositionspartei kandidierte. Durch diese Enthüllung wurden die Beschwerden, die der Finanzjournalist Thanasis Koukakis im April und Mai 2022 eingereicht hatte, weil sein Telefon mit der Spähsoftware „Predator“ infiziert worden war, ins Rampenlicht gerückt. Im September wurde bekannt, dass das Mobiltelefon des ehemaligen Infrastrukturminister und Abgeordneten der Syriza-Partei, Christos Spirtzis⁷⁹, ebenfalls mit Spähsoftware infiziert worden war. Außerdem wurde später im selben Monat bekannt, dass der griechische Geheimdienst (EYP) angeblich zwei seiner eigenen Mitarbeiter mit Spähsoftware ausspioniert hatte⁸⁰. Am 5. und 6. November enthüllten die griechischen Medien eine Liste von 33 Zielpersonen, bei denen es sich allesamt um hochrangige Persönlichkeiten handelte⁸¹. Die Liste – deren Verifizierung noch aussteht – liest sich wie ein beeindruckendes Who is Who der Politik, Wirtschaft und Medienlandschaft in Griechenland. Die Auswirkungen dieses groß angelegten und politisch motivierten Einsatzes von Spähsoftware gehen weit über die Personen auf der Liste hinaus, da alle ihre jeweiligen Kontakte und Verbindungen indirekt ebenfalls von der Ausspähung betroffen sind, einschließlich ihrer Kontakte in EU-Gremien. Die weite Verbreitung von Spähsoftware wurde bereits im Meta-Bericht 2021 deutlich, in dessen Anhang 310 gefälschte Websites mit Links zur Spähsoftware „Cytrox“ aufführt wurden, von denen allein 42 eingerichtet wurden, um Zielpersonen in Griechenland in die Irre zu führen^{82 83}.
36. Die Enthüllungen über den Einsatz von Spähsoftware und die Überwachung von Journalisten durch EYP erzählen eine sehr beunruhigende Geschichte über ein kompliziertes und undurchsichtiges Netzwerk von Beziehungen, politischen und geschäftlichen Interessen, Gefälligkeiten und Vetternwirtschaft sowie politischem Einfluss. Dieses Labyrinth mag auf den ersten Anblick verwirrend erscheinen. Jedoch zeichnen sich darin auch ein paar Muster ab. Politische Mehrheiten werden eher für die Förderung von Partikularinteressen als für das Allgemeininteresse genutzt, insbesondere durch die Ernennung von Verbündeten und Loyalisten in Schlüsselpositionen wie dem EYP, EAD und Krikel. Spähsoftware hingegen wird – gegebenenfalls in Kombination mit der rechtmäßigen Überwachung des Telekommunikationsverkehrs – von der obersten politischen Führung des Landes als Instrument für politische Macht und Kontrolle eingesetzt. Die Mechanismen zur *ex ante*- und *ex post*-Kontrolle wurden

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?](#)

bewusst geschwächt und Transparenz und Rechenschaftspflicht werden umgangen. Kritische Journalisten oder Beamte, die sich gegen Korruption und Betrug engagieren, werden eingeschüchtert und behindert, und es gibt keinen Schutz für Hinweisgeber.

37. Die Ausspähung aus politischen Gründen ist in Griechenland nichts Neues, aber die neuen Spähsoftware-Technologien vereinfachen die illegale Überwachung um ein Vielfaches, insbesondere im Kontext stark geschwächter Schutzmaßnahmen. Im Gegensatz zu anderen Fällen, wie z. B. Polen, scheint der Missbrauch von Spähsoftware nicht Teil einer integralen autoritären Strategie zu sein, sondern eher ein Instrument, das ad hoc zum politischen und finanziellen Vorteil der Drahtzieher eingesetzt wird. Er untergräbt jedoch auch die Demokratie und die Rechtsstaatlichkeit und bietet reichlich Raum für Korruption, wo doch in diesen turbulenten Zeiten eine zuverlässige und verantwortungsvolle Führung gefragt ist.

Erwerb

38. Die Regierung bestreitet den Erwerb der Spähsoftware „Predator“⁸⁴. Wenn es jedoch nicht die griechische Regierung war, dann drängt sich der Schluss auf, dass ein nichtstaatlicher Akteur für die (versuchten) Hacking-Angriffe auf die Telefone von Koukakis und Androulakis verantwortlich gewesen sein muss. Dies würde nach griechischem Recht ein Verbrechen darstellen und es wäre zu erwarten, dass die griechischen Behörden angesichts eines derart schwerwiegenden Falles mit sofortiger Wirkung energische Ermittlungen einleiten würden. Bislang gibt es jedoch keine polizeilichen Ermittlungen, sondern nur staatsanwaltschaftliche Ermittlungen aufgrund von Beschwerden. Es wurden keine physischen Beweise beschlagnahmt. Die Hypothese, dass private Akteure hinter den Angriffen mit der Spähsoftware „Predator“ stecken, ist zudem höchst unplausibel, da sich dadurch die Auswahl der Zielpersonen nicht erklären ließe.
39. Eine andere Möglichkeit ist, dass Predator über Ketyak erworben wurde, eine vom ehemaligen EYP-Chef Kontoleon gegründete Sondereinheit. Sie unterhält nur noch entfernte Verbindungen zum EYP.
40. Da es in den Fällen in Griechenland keine Beweise für die Identität des Käufers und Nutzers von Predator gibt, lässt sich nicht mit Sicherheit feststellen, ob oder wie die Regierung oder ein anderer Akteur Predator erworben hat. Grundsätzlich ist es jedoch nicht unmöglich, Spähsoftware zu erwerben oder zu nutzen, ohne dass staatliche Stellen die Software direkt kaufen. Spyware kann – wie bereits aus anderen Fällen bekannt – über Proxys, Maklerfirmen oder Mittelsmänner gekauft werden, oder es können Vereinbarungen mit Spähsoftware-Anbietern getroffen werden, damit diese bestimmte Dienstleistungen im Bereich Spähsoftware und Überwachung erbringen. Es besteht kein Zweifel daran, dass es enge Verbindungen und Abhängigkeiten zwischen bestimmten Personen und Ereignissen im Zusammenhang mit der Regierung, dem EJP und den Anbietern von Spähsoftware gab, insbesondere Krikel, einem bevorzugten Lieferanten für Kommunikations- und Überwachungsausrüstung unter anderem für die Polizei und das EJP. Krikel unterhält enge Verbindungen zu Personen aus dem Umfeld von Premierminister Mitsotakis.

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

Grigoris Dimitriadis

41. Dimitriadis ist der Neffe von Premierminister Mitsotakis und war bis August 2022 Generalsekretär in dessen Büro. In dieser Funktion war er für die Kontakte der Regierung mit der EYP verantwortlich.

Felix Bitzios

42. Der Geschäftsmann Felix Bitzios war in den großen Skandal um die Verletzung von Kapitalkontrollen durch die Bank of Piraeus verwickelt. Bis zum Abschluss der Ermittlungen wurde das Vermögen von Bitzios eingefroren⁸⁵. Bitzios hatte von einer Gesetzesänderung profitiert, die Premierminister Mitsotakis kurz nach seinem Amtsantritt im Jahr 2019 eingeführt hatte. Die umstrittene Änderung legte eine zeitliche Begrenzung für das Einfrieren von Vermögenswerten fest und ermöglichte so die Freigabe eingefrorener Vermögenswerte nach maximal achtzehn Monaten⁸⁶. Dank der Änderung der Regierung Mitsotakis konnte das Vermögen von Bitzios freigegeben werden.
43. Bitzios besaß über seine Firma Santinomo 35 % der Aktien von Intellexa. Am 4. August 2022 ließ er jedoch die Übertragung all seiner Aktien auf Thalestris, die Muttergesellschaft von Intellexa, eintragen⁸⁷. Bemerkenswert ist nicht nur das Datum der Eintragung der Übertragung – nur wenige Tage nach den Enthüllungen des Hacking-Angriffs auf das Mobiltelefon von Androulakis – sondern auch die Tatsache, dass die Übertragung angeblich am 18. Dezember 2020, also mehr als 19 Monate zuvor, stattfand. Bitzios distanzierte sich damit rückwirkend von 1/3 der gesamten Intellexa-Anteile, die er bis dahin besaß. Nichtsdestotrotz war Bitzios von März 2020 bis Juni 2021 als stellvertretender Geschäftsführer für Intellexa tätig.

Giannis Lavranos

44. Giannis Lavranos war wegen Steuerhinterziehung angeklagt worden und der Journalist Koukakis hatte über Lavranos Fall berichtet.

Intellexa

45. Die Spähsoftware „Predator“ wird über Intellexa vertrieben, ein Konsortium von Spähsoftware-Anbietern mit Niederlassungen unter anderem in Zypern, Griechenland, Irland und Frankreich. Tal Dilian, der im Laufe seiner früheren Karriere bei den israelischen Streitkräften tätig war, gründete das Konsortium in Zypern. Seine zweite Ex-Frau, die polnische Staatsbürgerin Sara Hamou, ist eine zentrale Figur in diesem verschlungenen Netzwerk von Unternehmen. Tal Dilian hat zusätzlich auch die maltesische Staatsbürgerschaft angenommen. Das griechische Außenministerium, das für die Erteilung von Ausfuhrgenehmigungen zuständig ist, erklärte, dass der Intellexa-Unternehmensgruppe keine Ausfuhrgenehmigungen erteilt wurden⁸⁸. Die Intellexa-Unternehmen mit Sitz in Griechenland haben jedoch Berichten zufolge ihre Produkte

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.](#)

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

nach Bangladesch und in mindestens ein arabisches Land exportiert^{89 90}. Eine detaillierte Beschreibung von Intellexa finden Sie im Kapitel über die Spyware-Industrie.

Krikel

46. Krikel ist ein bevorzugter Lieferant von Ausrüstung für die griechischen Strafverfolgungs- und Sicherheitsbehörden. Es ist auch der griechische Vertreter von RCS Lab, einem italienischen Unternehmen, das Überwachungssoftware verkauft. Außerdem soll Giannis Lavranos über ein anderes Unternehmen namens Mexal zu 50 % Eigentümer von Krikel sein⁹¹. Es lässt sich wohl jedoch – trotz der zahlreichen Verträge mit staatlichen Behörden – nicht mit Sicherheit feststellen, wer letztlich der wirtschaftliche Eigentümer von Krikel ist.
47. Im Jahr 2014 wurde das Unternehmen Ioniki Techniki von Giannis Lavranos an Tetra Communications in London verkauft. Ioniki Techniki gehört zu den drei Unternehmen, die im selben Jahr TETRA-Kommunikationssysteme an das griechische Ministerium für Bürgerschutz gespendet haben⁹². Die Spende von TETRA-Kommunikationssystemen wurde von einem in Florida ansässigen Unternehmen vermittelt, so dass die üblichen Ausschreibungsverfahren umgangen werden konnten. Die Spende an die griechische Regierung wurde 2017 angenommen. Im Jahr 2018 unterzeichnete Krikel einen Vertrag über 10,8 Millionen Euro für Wartungsarbeiten und technischen Support. Der Verwalter von Krikel, Stanislaw Pelczar, unterzeichnete den Vertrag im Namen von Krikel, aber es ist davon auszugehen, dass Lavranos die ganze Zeit über informell an den Verhandlungen beteiligt war⁹³. Krikel wurde zu einem wichtigen Zulieferer des griechischen Ministeriums für Bürgerschutz. Seit 2018 hat das Unternehmen sieben Verträge mit der griechischen Regierung unterzeichnet, von denen sechs geheim sind⁹⁴.
48. Das Unternehmen Krikel wurde auch zum Vertreter des italienischen Unternehmens RCS Lab in Griechenland. Im Juni 2021 erwarb der griechische Nachrichtendienst (EYP) über Krikel⁹⁵ ein Abhörsystem von RCS Lab⁹⁶. Zu dieser Zeit war Dimitriadis für die Kontakte zwischen der Regierung und dem EYP verantwortlich. In einigen Quellen ist dokumentiert, dass während der Installation dieses neuen Systems Material mit Informationen über die Überwachung von Androulakis und Koukakis verloren gegangen ist – angeblich aufgrund eines technischen Problems⁹⁷. Andere Quellen

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](#).

⁹⁵ TVXS. [G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament](#).

⁹⁶ Hellas Posts English. [The EYP supplier contaminates smartphones in Greece as well](#).

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

hingegen behaupten, Kontoleon habe die Vernichtung der Akten am 29. Juli 2022 angeordnet⁹⁸.

49. Interessanterweise wurden Mitarbeiter von Krikel bei der Arbeit für Ketyak gesichtet, die sie angeblich unentgeltlich entrichteten. Ketyak hat offenbar im Rahmen eines vertraulichen Ausschreibungsverfahrens, das auf einer geheimen Entscheidung des Premierministers beruht, 40 Millionen Euro von der RRF erhalten.

Verwicklung von Bitzios und Lavranos

50. Bitzios und Lavranos waren beide aktiv an der Gründung von Krikel im Jahr 2017 beteiligt. Gemeinsam leiteten sie die Ernennung des polnischen Anwalts Stanislaw Pelczar zum Verwalter von Krikel im Oktober 2017 in die Wege⁹⁹. Bitzios Unternehmen Viniato Holdings Limited erhielt anschließend einen mit etwa 550 000 Euro Honorar dotierten Beratervertrag bei Krikel für den Zeitraum von Januar bis August 2018 (obwohl Krikel in diesem Jahr nur einen Umsatz von 840 000 Euro erzielte)¹⁰⁰.
51. Bitzios und Lavranos sind zwei Schlüsselfiguren bei der Lieferung von Kommunikations- und Überwachungsmaterial an staatliche Einrichtungen wie die Polizei und das EYP. Bitzios war eine Schlüsselfigur in dem Unternehmen, das Predator vertreibt. Beide standen Dimitriadis nahe und profitierten von lukrativen Regierungsverträgen. Ihnen spielte auch die Gesetzesänderung der neuen Regierung in die Karten, durch die ihre eingefrorenen Vermögenswerte freigegeben wurden. Sie hatten ein Motiv, Koykakis mithilfe von Spähsoftware zu bespitzeln. Diese Verflechtung von Geschäftsinteressen, persönlichen Beziehungen und politischen Verbindungen birgt ein sehr offensichtliches und hohes Risiko von Interessenkonflikten und Korruption. Diese beiden Männer wären des Weiteren in der Lage, entscheidende Informationen über den Erwerb und die Verwendung von Predator in Griechenland preiszugeben.

Rechtlicher Rahmen

52. Griechenland verfügt grundsätzlich über einen recht soliden Rechtsrahmen. Allerdings haben Gesetzesänderungen entscheidende Schutzmechanismen geschwächt und die politische Besetzung von Schlüsselpositionen behindert die Kontrolle und Rechenschaftspflicht.

Ex-ante-Kontrolle

53. In Griechenland stellt es gemäß mehrerer Artikel des griechischen Strafgesetzbuchs, darunter Artikel 292 über Straftaten gegen die Sicherheit des Telefonverkehrs, Artikel 292 B über die Beeinträchtigung des Betriebs von Informationssystemen sowie Artikel 370 über Verstöße gegen das Briefgeheimnis einen Straftatbestand dar, ein Gerät mit Spähsoftware zu infizieren. Darüber hinaus stellt die Herstellung, der Verkauf, die Lieferung, die Verwendung, die Einfuhr, der Besitz und die Verbreitung

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](#).

von Schadsoftware (einschließlich Spähsoftware) ebenfalls eine Straftat gemäß Artikel 292 C des griechischen Strafgesetzbuches dar¹⁰¹.

Gesetzgeberischer Akt

54. Nach den Enthüllungen über die Überwachung hat Premierminister Mitsotakis Änderungen am Betriebsrahmen des EYP vorgeschlagen. Eine dieser Änderungen war die Einführung des Gesetzgeberischen Akts durch die Regierung am 9. August 2022. Artikel 9 Absatz 2 des Gesetzes Nr. 3649/2008 wurde dahingehend aktualisiert, dass nun eine Stellungnahme des Ständigen Ausschusses für Institutionen und Transparenz zur Ernennung des Gouverneurs des EJP erforderlich ist¹⁰². Da die Regierungspartei jedoch im Ständigen Sonderausschuss für Institutionen und Transparenz des Parlaments derzeit über eine absolute Mehrheit verfügt, hat sie für die Ernennung von Herrn Demiris zum neuen Gouverneur des EJP gestimmt, während alle ebenfalls dort vertretenen Oppositionsparteien diese abgelehnt haben¹⁰³. Zweiter stellvertretender Kommandant des EYP ist übrigens Dionysis Melitsiotis¹⁰⁴, ein ehemaliges Mitglied des Kabinetts des Premierministers, und Anastasios Mitsialis, ein ehemaliger Nea Demokratia-Funktionär, ist als weiterer stellvertretender Direktor tätig¹⁰⁵.

Ex-post-Kontrolle

55. Seit 2019 unterstehen die Handlungen des EYP der direkten Kontrolle von Premierminister Kyriakos, nachdem das entsprechende Gesetz nach dem Sieg von New Democracy im Jahr 2019 geändert wurde¹⁰⁶.
56. Die im Gesetz Nr. 2225/1994 vorgesehenen Vorschriften zur Vertraulichkeit der Kommunikation besagen, dass eine Aufhebung dieser Vertraulichkeit nur in Fällen der nationalen Sicherheit und bei der Untersuchung schwerer Verbrechen möglich ist. Nach der Aufhebung der Vertraulichkeit sieht Artikel 5 dieses Gesetzes vor, dass die ADAE die Zielpersonen der Ermittlungen informieren kann, sofern der Zweck der Ermittlungen dadurch nicht beeinträchtigt wird¹⁰⁷. Das Recht einer Person auf Zugang zu Informationen darüber, ob sie Gegenstand einer Überwachung war, ist im Gesetz Nr. 2472/1997 verankert¹⁰⁸. Als jedoch im März 2021 die ADAE das EYP auf das Recht von Koukakis auf Information hinwies, legte die Regierung am 31. März 2021 sofort den Änderungsantrag Nr. 826/145 vor, der die Möglichkeit der ADAE abschafft, Bürger über die Aufhebung der Vertraulichkeit der Kommunikation zu informieren¹⁰⁹. Damit wird der Einzelne de facto seines Rechts auf Information beraubt. Die Änderung wurde auf höchst irreguläre Weise eingeführt. Sie wurde einem Gesetz hinzugefügt, das in keinem Zusammenhang mit dem Gesetz steht (einem Gesetzesentwurf zu Maßnahmen im Zusammenhang mit der COVID-19-Pandemie), und die von der

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](#).

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

Verfassung vorgeschriebenen Fristen wurden nicht eingehalten^{110 111 112}. Es fand also kein ordnungsgemäßer Konsultationsprozess statt.

57. Die Möglichkeiten für eine Ex-post-Kontrolle werden durch die Tatsache weiter geschwächt, dass Griechenland die Whistleblowing-Richtlinie der EU noch immer nicht vollständig umgesetzt hat¹¹³.

Öffentliche Kontrolle

58. Griechenland belegt im World Press Freedom Index 2022 den letzten Platz unter allen EU-Ländern: d. h. Platz 108 von 180¹¹⁴. Im Jahr 2021 wurde der Journalist Giorgos Karaivaz ermordet. Der Mord wurde bis heute nicht aufgeklärt. Journalisten sind Einschüchterungen und taktischen Klagen gegen die öffentliche Beteiligung (SLAPP-Klagen) ausgesetzt. Grigoris Dimitriadis¹¹⁵ hat SLAPP-Klagen gegen die Nachrichtenagenturen Reporters United und Efimerida ton Syntakton (EfSyn)¹¹⁶ eingereicht, nachdem er zum Rücktritt gezwungen wurde. Regierungsminister Oikonomou versuchte, die Politico-Reporterin Nektaria Stamouli zu diskreditieren, indem er ihr unterstellte, ihre Artikel über den Abhörskandal seien politisch motiviert¹¹⁷. In der Tat hatten zwei der Personen, die Opfer von Angriffen mit der Spähsoftware „Predator“ wurden, Koukakis und Malichoudis, kritisch über Korruptions- und Betrugsfälle und die Misshandlung von Migranten berichtet. Athanasios Telloglou und Eliza Triantafyllou berichteten über den Spähsoftware-Skandal und wurden angeblich überwacht¹¹⁸.

Rechtsbehelf

Nationale Transparenzbehörde

59. Am 22. Juli 2022 hat die nationale Transparenzbehörde (EAD) eine Untersuchung über den angeblichen Erwerb der Spähsoftware Predator durch das Ministerium für Bürgerschutz und das EYP eingeleitet. Bei der Prüfung wurden die griechische Polizei, das EYP und die Unternehmen Intellexa und Krikel überprüft. Die nationale Transparenzbehörde schloss ihren Bericht am 10. Juli 2022 ab, übergab ihn aber dem EYP zur vorherigen Genehmigung. Der offizielle Bericht, der Koukakis am 22. Juli zugesandt wurde, enthielt nur Bruchteile der vollständigen Prüfung, die von der nationalen Transparenzbehörde durchgeführt worden war. Unter dem Deckmantel des Schutzes personenbezogener Daten wurden mehrere Namen im Prüfbericht geschwärzt, darunter die Namen der Prüfer des EAD, des Staatsanwalts des EYP, der den

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](#).

ursprünglichen Bericht des EAD prüfte, sowie der Anwälte und Buchhalter der beteiligten juristischen Personen¹¹⁹.

60. Der Bericht der nationalen Transparenzbehörde kam zu dem Schluss, dass weder das EYP noch das Ministerium für Bürgerschutz Verträge mit Intellexa und anderen verbundenen nationalen Unternehmen abgeschlossen hatten. Sie hätten auch die Spähsoftware „Predator“ nie erworben oder verwendet¹²⁰. Die nationale Transparenzbehörde hat jedoch weder die Bankkonten von Intellexa und Krikel noch die angeschlossenen Offshore-Unternehmen untersucht. Außerdem besuchte die nationale Transparenzbehörde die Büros von Intellexa und Krikel erst nach 2 Monaten, als die Mitarbeiter aufgrund der COVID-19-Pandemie bereits von zu Hause aus arbeiteten. Die nationale Transparenzbehörde hat sich auch nicht mit den Rechtsvertretern der betreffenden Unternehmen getroffen¹²¹.
61. Es gibt Zweifel an der Unabhängigkeit der Führung der nationalen Transparenzbehörde. Kürzlich machte die nationale Transparenzbehörde Schlagzeilen mit Andeutungen einer regierungsfreundlichen Voreingenommenheit bei der Erstellung eines Berichts über die Zurückweisungen von Migranten¹²². Der Direktor der nationalen Transparenzbehörde, ein ehemaliger Mitarbeiter von Mitsotakis, hat sich während der Mission im November 2022 nicht mit dem Ausschuss zur Untersuchung des Einsatzes von Pegasus und ähnlicher Überwachungs- und Spähsoftware (PEGA) getroffen.

Griechische Behörde für Kommunikationssicherheit und Datenschutz (ADAE)

62. Im Juli 2022 bestätigte Nikos Androulakis, dass er bei der Staatsanwaltschaft des Obersten Gerichtshofs Anzeige erstattet hatte, weil er angeblich am 21. September 2021 mit der Spähsoftware „Predator“ ausgespäht worden war. Im Anschluss an Androulakis Beschwerde leitete die ADAE im August 2022 eine Untersuchung ein, in deren Rahmen zunächst Informationen von Androulakis Telekommunikationsanbieter eingeholt wurden.

Ausschuss für Institutionen und Transparenz

63. Im Juli 2022 lud der Ausschuss für Institutionen und Transparenz Kontoleon und den Präsidenten der ADAE Christos Rammos zu einer parlamentarischen Anhörung vor. Während dieser Anhörung räumte Kontoleon ein, dass das EYP Thanasis Koukakis aus Gründen der nationalen Sicherheit ausspioniert hatte, erklärte aber, dass er keine Kenntnis von dem versuchten Hacking-Angriff mit der Spähsoftware „Predator“ auf Androulakis Mobiltelefon hatte. Der Regierungssprecher Giannis Oikonomou ließ verlautbaren, die griechischen Behörden hätten die Spähsoftware Predator weder erworben noch jemals verwendet¹²³.

Parlamentarischer Untersuchungsausschuss

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. Einem Vorschlag der PASOK-KINAL-Partei zur Einsetzung eines Untersuchungsausschusses über den angeblichen Einsatz von Spähsoftware¹²⁴ stimmten 142 Abgeordnete der Opposition zu, während sich die 157 Abgeordneten der Nea Demokratia (ND) der Stimme enthielten¹²⁵. Allerdings hatte die ND eine absolute Mehrheit im Untersuchungsausschuss. Die Forderungen nach einem überparteilichen Präsidium wurden abgelehnt. Die ND legte das Arbeitsprogramm und die Liste der vorzuladenden Zeugen fest und lehnte mehrere der von den Oppositionsparteien vorgeschlagenen Zeugen ab. Der Ausschuss wurde am 29. August 2022 eingesetzt. Er nahm seine Arbeit am 7. September 2022 auf und schloss sie am 10. Oktober 2022 ab.
65. Die Regierungsmehrheit im Ausschuss weigerte sich, Bitzios und Lavranos vorzuladen. Stattdessen erfolgte die Vorladung von Stamatis Tribalís – dem derzeitigen Geschäftsführer von Krikel – und Sara Hamou. Am 22. September sagte Tribalís vor diesem parlamentarischen Ausschuss aus. Tribalís legte offenkundig falsche Informationen über die Beteiligung von Bitzios und Lavranos an Krikel vor und behauptete unter anderem, er selbst sei der Eigentümer von Krikel¹²⁶.
66. Eine Zeugin, Sarah Hamou, die für das Unternehmen Intelexa tätig ist, gab an, nicht persönlich erscheinen zu können (obwohl sie in Zypern lebt), und es wurde ihr gestattet, ihre Antworten schriftlich einzureichen. Da keine Einigung auf gemeinsame Schlussfolgerungen erzielt werden konnte, veröffentlichte jede Partei ihren eigenen Bericht. Etwa 5 500 Seiten an Dokumenten, einschließlich der Protokolle und der Aussage von Hamou, wurden als Verschlussache eingestuft, obwohl es in der Macht des Parlaments liegt, diese freizugeben. Paradoxerweise dient der Untersuchungsausschuss demzufolge dazu, Informationen unter Verschluss zu halten, anstatt sie zugänglich zu machen.

Die Ziele

67. Zum Zeitpunkt der Erstellung dieses Berichts war eine Liste mit 33 Namen von Zielpersonen veröffentlicht worden. Eine detaillierte Analyse ist nicht möglich, und es wurde noch kein förmliches Untersuchungsverfahren eingeleitet. Die Analyse der wenigen bisher bekannten Fälle genügt jedoch, um ein recht klares Bild der vorliegenden Probleme zu zeichnen.

Thanasis Koukakis

68. Im Sommer 2020 wurde der Journalist Thanasis Koukakis von der EYP abgehört. Zu dieser Zeit berichtete er über Finanzthemen, einschließlich des Piräus/Libra-Skandals, in den Felix Bitzios verwickelt war, über die angebliche Steuerhinterziehung durch den griechischen Geschäftsmann Yiannis Lavranos sowie über die umstrittenen Bankengesetze, die von der Regierung Mitsotakis eingeführt wurden und die die Verfolgung von Geldwäsche und anderen Finanzdelikten behinderten (tatsächlich hatten die neuen Vorschriften rückwirkend die Einstellung von zwölf anhängigen Verfahren zur Folge)¹²⁷. Koukakis untersuchte auch die Beschaffung neuer Personalausweise, an denen Lavranos und Bitzios ein geschäftliches Interesse hatten. Etwa zu der Zeit, als

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](#).

Koukakis zum ersten Mal vor dem PEGA erschien, wurde die Ausschreibung plötzlich zurückgezogen und der zuständige Generalsekretär trat zurück.

Nikos Androulakis

69. Am 21. September 2021 wurde Nikos Androulakis, Vorsitzender der Mitte-Links-Partei PASOK-KINAL und Mitglied des Europäischen Parlaments, mit der Spähsoftware „Predator“ angegriffen, als er einen bösartigen Link auf seinem Telefon zugeschickt bekam¹²⁸. Androulakis erhielt eine Textnachricht mit dem Wortlaut „Machen Sie mal ein bisschen Ernst, wir haben viel zu gewinnen“. Außerdem enthielt die Nachricht einen Link zur Installation der Spähsoftware „Predator“ auf seinem Telefon. Im Gegensatz zu Koukakis klickte Androulakis jedoch nicht auf den Link, der ihm zugesandt wurde¹²⁹.
70. Die Überwachung eines Politikers ist höchst ungewöhnlich, und die griechische Verfassung sieht einen besonderen Schutz für Politiker vor. Das EYP bestreitet jede Beteiligung an der Überwachung mit der Spähsoftware „Predator“. Die Regierung hat zunächst Vermutungen über die Involvierung ausländischer Mächte geäußert, die angeblich die Überwachung von Androulakis beantragt hätten, oder stellte in den Raum, seine Mitgliedschaft in einem Ausschuss des Europäischen Parlaments, der für die Beziehungen zu China zuständig ist, könnte ihn zur Zielscheibe gemacht haben. Keine dieser Hypothesen war besonders glaubwürdig. Die Überwachung fand in einem politischen Kontext statt, kurz vor den Wahlen. Umfragen sagten voraus, dass die Néa Demokratía ihre absolute Mehrheit verlieren würde. Die PASOK würde bei den Wahlen als der bevorzugte Koalitionspartner hervorgehen. Im Herbst 2021 traten vier Kandidaten für die Führung der PASOK an, die jeweils unterschiedliche Ansichten über eine solche Koalition hatten. Von Androulakis hieß es, er sei offen für die Idee, aber nicht unter der Premierministerschaft von Mitsotakis. Ein anderer Kandidat, Andreas Loverdos, hatte zuvor als Minister in einer Koalition aus Néa Demokratía und PASOK gedient und galt eher als Befürworter der Idee. Er war mit Dimitriadis bekannt. Manolis Othonas, die rechte Hand eines anderen Kandidaten, soll ebenfalls engere Beziehungen zu Néa Demokratía und Dimitriadis unterhalten. Angesichts der Liste weiterer angeblicher Zielpersonen, die durch Documento veröffentlicht wurde, erhärtet sich der Verdacht, dass die Überwachung politisch motiviert war. Es gibt keine Beweise für eine dieser Hypothesen, aber es ist wichtig, dass diese untersucht und nach Möglichkeit aus der Welt geräumt werden.

Stavros Malichoudis

71. Am 13. November 2021 enthüllte die Zeitung EFSYN, dass mehrere Journalisten, die über Flüchtlingsfälle berichteten, angeblich von der EYP abgehört wurden. Ein internes Dokument des EYP zeigte, dass die EYP die Überwachung und Sammlung von Daten des griechischen Journalisten Stavros Malichoudis angeordnet hatte^{130 131}. Malichoudis schrieb über ein 12-jähriges syrisches Kind, das gezwungen wurde, mehrere Monate lang in einem Internierungslager auf der griechischen Insel Kos zu leben¹³².

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 Malichoudis under surveillance for 'national security reasons'.](#)

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

Christos Spirtzis

72. Am 15. November 2021 wurde der ehemalige Minister für Infrastruktur und Abgeordnete der Syriza-Partei Christos Spirtzis mit der Spionagesoftware Predator auf seinem Mobiltelefon angegriffen¹³³.

Tasos Telloglou, Eliza Triantafyllou und Thodoris Chondrogiannos

73. Tasos Telloglou und Eliza Triantafyllou wurden angeblich bespitzelt, während sie investigativ für „Inside Story“ tätig waren.

Sonstige Zielpersonen

74. Am 29. Oktober 2022 wurde berichtet, dass auch andere Politiker mit der Spähsoftware „Predator“ ausspioniert wurden, darunter ein Minister der Regierung, der in keinem guten Verhältnis zum Premierminister stand. Darüber hinaus soll ein weiteres Mitglied der Néa Demokratía einen Link für die Installation der Spähsoftware „Predator“ erhalten haben¹³⁴. Der Regierungssprecher, Giannis Oikonomou, ließ verlautbaren, dass sich der Artikel auf keinerlei konkreten Beweisen stütze¹³⁵.
75. Am 5. und 6. November 2022 veröffentlichte Documento eine Liste mit 33 Namen von Personen, die mithilfe der Spähsoftware „Predator“ ausgespäht wurden¹³⁶. Darunter viele hochrangige Politiker, unter anderem auch Mitglieder der aktuellen Regierung, der ehemalige Premierminister Samaras, der ehemalige EU-Kommissar Avramopoulos, der Chefredakteur einer regierungsfreundlichen nationalen Zeitung und Personen aus dem Umfeld von Vangelis Marinakis, Reeder, Medienmogul und Besitzer der Fußballclubs Olympiakos und Nottingham Forest. Die Enthüllungen der Liste sind höchst beunruhigend, nicht nur wegen der hochkarätigen Namen, sondern auch, weil sie darauf hindeuten, dass der Missbrauch von Spähsoftware systematisch und in großem Umfang erfolgt und Teil einer politischen Strategie ist.

I. D. Zypern

76. Zypern ist ein wichtiges europäisches Ausfuhrzentrum für die Überwachungsindustrie. Auf dem Papier bietet das Land, indem auch die EU-Gesetze Anwendung finden, einen soliden Rechtsrahmen. In der Praxis jedoch ist Zypern ein attraktiver Standort für Unternehmen, die Überwachungstechnologien verkaufen. Die jüngsten Skandale haben dem Ruf des Landes jedoch geschadet. Eine Reihe neuer Gesetzesinitiativen zur Verschärfung des Rechtsrahmens für Ausfuhren und zur Verbesserung der Einhaltung der Vorschriften wird voraussichtlich 2023 abgeschlossen sein.
77. Auf dem Papier ist ein rechtlicher Rahmen gegeben, in dem der Schutz der privaten Kommunikation, die Verarbeitung personenbezogener Daten und das Recht des Einzelnen auf Information geregelt sind. In der Praxis gibt es jedoch keine eindeutigen

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.

Regeln für den Einsatz von Abhörgeräten und den Schutz der verfassungsmäßigen Rechte der Bürger, sobald die nationale Sicherheit geltend gemacht wird.

78. Zypern scheint eine sehr enge Zusammenarbeit mit Israel im Bereich der Überwachungstechnologien zu pflegen. Zypern hat sich mit Israel und den USA über die Reform seines Rechtsrahmens beraten. Zypern ist ein beliebter Standort für zahlreiche israelische Spähsoftware-Firmen.

Rechtlicher Rahmen

Dual-Use-Verordnung

79. Verglichen mit dem geltenden Rechtsrahmen ist Zypern Berichten zufolge recht großzügig, wenn es um die Erteilung von Ausfuhrlizenzen für Spähsoftware geht¹³⁷. Die Unternehmen wenden Tricks an, um die Vorschriften zu umgehen. Die physische Hardware des Produkts wird in ein Empfängerland geschickt, ohne dass die Software darauf hochgeladen wurde¹³⁸. Im Anschluss wird die Aktivierungssoftware (auch als „Lizenzschlüssel“ bezeichnet) separat über einen USB-Stick in das Zielland geschickt¹³⁹. Eine andere Möglichkeit besteht darin, anzugeben, dass das Produkt nur zu Demonstrationszwecken ausgefahren wird – selbst wenn eine detaillierte Beschreibung des Produkts beigefügt ist¹⁴⁰.
80. Viele israelische Unternehmen entscheiden sich für Zypern als Standort, um mit ihren Tätigkeiten am europäischen Markt zu beginnen¹⁴¹. Verschiedene Quellen berichten außerdem, dass im Land circa 29 israelische Unternehmen ansässig sind¹⁴². Der Handel mit Spähsoftware und die diplomatischen Beziehungen des Landes sind eng miteinander verbunden. Als Gegenleistung für die Erteilung von Lizenzen für israelische Unternehmen hat Zypern angeblich einige der Produkte erhalten, die diese Unternehmen entwickeln und exportieren, wie z. B. die Spähsoftware „Pegasus“ von NSO¹⁴³ sowie Spähsoftware-Material von WiSpear¹⁴⁴.

Ex-ante-Kontrolle

81. Das Gesetz über den Schutz der Vertraulichkeit privater Kommunikation 92(I)/1996 sieht vor, dass der Antrag auf Genehmigung zur Überwachung privater Kommunikation bei Gericht eingereicht werden muss¹⁴⁵.

Ex-post-Kontrolle

82. Auf dem Papier stellt die Verletzung des Schutzes der privaten Kommunikation de jure eine Straftat dar. De facto wird die Illegalität einer solchen Handlung häufig durch die

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.](#)

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

Berufung auf die nationale Sicherheit verdeckt¹⁴⁶. Es gibt kein Gesetz, das regelt, unter welchen Umständen die Polizei oder andere Nachrichtendienste Abhörgeräte einsetzen können, wer die Verfahren für Abhörungen regelt und wie der Schutz der verfassungsmäßigen Rechte der Bürger gewährleistet wird. Die entsprechenden Vorschriften und Protokolle liegen derzeit im Repräsentantenhaus zur Diskussion und Genehmigung vor. Bis auf Weiteres sehen diese Bestimmungen keine Kontrollmechanismen vor¹⁴⁷.

Rechtsbehelf

83. Der zypriotische Staatspräsident hat ein erhebliches Mitspracherecht bei der Bildung des Ausschusses, dem die Befugnis zuteilwird, kritische Untersuchungen zu den Handlungen der KYP einzuleiten. Darüber hinaus werden die Jahresberichte mit den Ergebnissen des Ausschusses in einem ersten Schritt zunächst dem Präsidenten übermittelt¹⁴⁸.

Schlüsselfiguren in der Spyware-Industrie

84. Tal Dilian hat bei vielen der Entwicklungen in Zypern und Griechenland eine Schlüsselrolle gespielt. 2017 erhielt er die maltesische Staatsbürgerschaft¹⁴⁹. Tal Dilian hatte 25 Jahre lang verschiedene Führungspositionen in den israelischen Verteidigungskräften inne, bevor er 2002 aus dem Militär ausschied¹⁵⁰. Zu Beginn seiner Karriere als „Geheimdienstexperte, Community Builder und Serial Entrepreneur“ in Zypern gründete Dilian die Aveledo Ltd, die später in die Ws WiSpear Systems Ltd. umbenannt wurde, sowie zu einem späteren Zeitpunkt auch die Passitora Ltd¹⁵¹.
85. In Zypern stand Dilian in enger Verbindung zu Abraham Sahak Avni. Avni war früher bei den Spezialeinheiten der israelischen Polizei als Sonderermittler tätig¹⁵². Im November 2015 konnte er dank einer Investition in Immobilien im Wert von 2,9 Millionen Euro die zypriotische Staatsbürgerschaft und einen „goldenen Pass“ erwerben¹⁵³. Avni gründete die zypriotische NCIS Intelligence Services Ltd¹⁵⁴, ein Unternehmen, das Berichten zufolge mit den mächtigsten Technologie-Unternehmen der Welt zusammenarbeitet¹⁵⁵. NCIS Intelligence and Security Services lieferte zwischen 2014 und 2015 Sicherheitssoftware an das Polizeipräsidium und waren zwischen 2015 und 2016 für die Schulung von Mitarbeitern des Amtes für Kriminalitätsanalyse und Statistik zuständig¹⁵⁶. Zu den Kunden des Unternehmens zählt auch die Regierungspartei Dimokratikós Sinagermós (DISY). Berichten zufolge war

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.

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

¹⁵⁶ Philenews. FILE: The state insulted Avni and Dilian.

Avni für die Installation von Sicherheitsanlagen in den Büros der Partei zuständig¹⁵⁷. Neben der Sicherheitsausrüstung von Avni wurden die Materialien von Dilian auch an die zypriotische Drogenbekämpfungsbehörde und die zypriotische Polizei verkauft¹⁵⁸.

86. Zwischen Dilian und Avni bestehen zahlreiche Verbindungen. Dilians Unternehmen WiSpear teilte sich in Larnaca ein Gebäude und einige Beschäftigte mit Avni¹⁵⁹. 2018 gründeten die beiden Männer das Unternehmen Poltrex, das später zu Alchemycorp Ltd. umbenannt wurde. Seinen Sitz im Novel Tower teilte Poltrex mit Avni¹⁶⁰, und das Unternehmen gehört auch dem Firmenverbund Intellexa Alliance an. Berichten zufolge war mit Avnis Beziehungen zur DISY-Partei der Boden für die Erprobung von Dilians Produkten bestellt¹⁶¹.

Dilians Spähsoftware im Transporter

87. Nach dem Verkauf von Circles Technologies und der Gründung von WiSpear gründete Tal Dilian 2019 auch noch die Intellexa Alliance, die auf der Website als ein EU-gestütztes und reguliertes Unternehmen beschrieben wird, das dem Zweck dient, Technologien zur Stärkung von Nachrichtendiensten zu entwickeln und zu integrieren¹⁶². Mehrere Überwachungsanbieter sind unter die Marketingbezeichnung Intellexa Alliance versammelt, z. B. Cytrox, WiSpear – später umbenannt zu Passitora Ltd. – Nexa Technologies und Poltrex Ltd. Diese verschiedenen dem Firmenverbund von Dilian angehörenden Anbieter machen ein breites Sortiment von Überwachungssoftware und -dienstleistungen möglich, die Intellexa Kunden einzeln oder in Kombination anbieten kann¹⁶³. Weitere Einzelheiten zur Firmenstruktur finden sich im Kapitel über die Spähsoftwarebrachen.
88. Nach Beschwerden gegen Dilian stellte sich heraus, dass die israelischen Go Networks mutmaßlich über verteilte Eigentumsstrukturen des Unternehmens in Irland mit Intellexa verbunden waren. Ehemaligen hohen Vertretern wurden angeblich Spitzenfunktionen bei Intellexa besorgt¹⁶⁴. Ferner ergaben die polizeilichen Ermittlungen, dass WiSpear Ausfuhrgenehmigungen erteilt wurden für „Abhörausrüstung, konstruiert für die Extraktion von über die Luftschnittstelle übermittelten Sprachinformationen oder Daten“^{165 166}.
89. 2011 gründete Avni zusammen mit Michael Angelides, dem Bruder des ehemaligen Ministers und stellvertretenden Generalstaatsanwalts Savvas Angelides, ein Unternehmen. Dieses Unternehmen namens S9S wurde am 10. November 2011¹⁶⁷ beim Registergericht und mit Unterstützung der ehemaligen Anwaltskanzlei von Savvas

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 [tps://intellexa.com/](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.](#)

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.](#)

Angelides angemeldet¹⁶⁸. Die Partnerschaft wurde jedoch 2012 aufgelöst. Trotz alledem wurde gerade Savvas Angelides im Fall des Transporters mit Spähsoftware mit der Kontrolle von Avni und Dilian beauftragt¹⁶⁹.

90. Die Oppositionspartei AKEL brachte ihre Empörung darüber zum Ausdruck, dass das Verfahren gegen Dilian und seine Mitarbeiter eingestellt wurde, und prangerte die juristische Entscheidung als Vertuschungsmaßnahme des Generalstaatsanwalts an¹⁷⁰. Denn die zyprische Regierung hatte angeblich Ausrüstung von Dilians Unternehmen gekauft, und einer der angeklagten Beschäftigten war mutmaßlich für NSO tätig und lieferte dem zyprischen Nachrichtendienst KYP Bedienungsanweisungen für die Pegasus-Spähsoftware¹⁷¹. Durch die Einstellung des Verfahrens war der fortwährende Schutz der Verbindungen zwischen Dilians Unternehmen und der zyprischen Regierung sichergestellt¹⁷². Dieses Beispiel belegt, dass die Datenschutzrechte natürlicher Personen nicht in vollem Umfang gewährleistet und gegen Verletzungen durch Massenüberwachungs-ausrüstung resistent sind. Zwar sind auf Papier Rechtsmittel festgeschrieben, doch wirken sich staatliche Eingriff auf den Ausgang von Gerichtsverfahren aus und lassen Einzelpersonen, die Opfer solcher Rechtsverstöße werden, wehrlos zurück.

Umzug nach Griechenland

91. Nach der Episode mit dem Transporter und dem Gerichtsverfahren verlagerte Dilian die Geschäftstätigkeit von Intellexa nach Griechenland, obwohl er Zypern nie verließ und weiterhin dort wohnhaft ist. Indirekte Verbindungen zwischen einigen in Zypern und Griechenland gemeldeten natürlichen und juristischen Personen machen offenbar, wie der Umzug von Dilians Unternehmen nach Athen ermöglicht wurde¹⁷³.
92. Laut jüngsten Aussagen, die im Rahmen der gerichtlichen Untersuchungen der Angelegenheit mit dem Spähtransporter erfasst wurden, übte der Rechtsanwalt Alexandros Sinka in Bezug auf den Umzug nach Griechenland erheblichen Einfluss aus. Sinka, der vormals in der Mitte-Rechts-Partei DISY eine zentrale Rolle spielte, unterhielt augenscheinlich gute Beziehungen zu Dilian und Avni¹⁷⁴. Allem Anschein nach war Sinka auch ein Bekannter des ehemaligen Generalsekretärs der griechischen Regierung Dimitriadis. Beide Männer bekleideten Positionen beim Bureau of European Democrat Students (EDS), der Studentenorganisation der Europäischen Volkspartei (PPE). Zwischen 2003 und 2004 dienten Sinka als dessen Vorsitzender und Dimitriadis als Vizevorsitzender¹⁷⁵. Angeblich machte Dimitriadis seinen Freund, den griechischen Geschäftsmann Felix Bitzios, in Verbindung mit dessen langjähriger gerichtlicher Auseinandersetzung in Zypern, mit Sinka bekannt. Sinka seinerseits empfahl Bitzios,

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.](#)

¹⁷⁵ EDS. [2003/2004 Bureau.](#)

für seinen Rechtsstreit die Hilfe des Anwalts Harris Kyriakidis in Anspruch zu nehmen. Auch Kyriakidis unterhielt gute Beziehungen zu DISY¹⁷⁶.

NSO Group und Zypern

93. Neben Intellexa Alliance war angeblich auch die NSO Group in Zypern ansässig. 2010 gründete Tal Dilian zusammen mit Boaz Goldman und Eric Banoun das Unternehmen Circles Technologies, dessen Spezialität der Verkauf von Systemen war, die die SS7-Schwachstelle ausnutzen¹⁷⁷. Sechs Jahre später wurde Circles Technologies für knapp 130 Mio. USD an Francisco Partners verkauft, wovon Dilian 21,5 Mio. USD erhielt. Diese Private-Equity-Gesellschaft mit Sitz in Kalifornien erwarb auf ähnliche Weise 90 % der NSO Group, wodurch Circles Technologies und NSO Group unter dem Namen L.E.G.D Company Ltd. zusammengeführt wurden; dieses Unternehmen wurde am 29. März 2016 in Q Cyber Technologies Ltd. umbenannt¹⁷⁸.
94. Die Leugnung der Ausfuhr und Entwicklung von Pegasus im Land durch die zyprischen Regierung scheint allerdings falsch zu sein. Am 21. Juni 2022 stellte der NSO-Bedienstete Chaim Gelfad fest, dass die Unternehmen der NSO Group in Zypern und Bulgarien an Software zur Bereitstellung von Nachrichtendiensten beteiligt sind¹⁷⁹. Laut einem Dokument, das von der Oppositionspartei AKEL dem Europäischen Parlament vorgelegt wurde, hat die NSO Group die Pegasus-Spähsoftware mutmaßlich über eine ihrer Tochterunternehmen in Zypern an ein Unternehmen in den Vereinigten Arabischen Emiraten exportiert. Eines der Tochterunternehmen hat dem fraglichen Unternehmen offensichtlich 7 Mio. USD in Rechnung gestellt¹⁸⁰.
95. Berichten zufolge besaß die NSO Group auch in Zypern ein aktives Unternehmen, das angeblich ein Kundenservicecenter unterhielt. Im Jahr 2017 fand im Four Seasons Hotel in Limassol ein Treffen zwischen NSO-Bediensteten und saudi-arabischen Kunden zur Vorführung der neuesten Funktionen der Version 3 der Pegasus-Spähsoftware statt. Diese Version enthielt die neuartige Zero-Click-Funktion, die es ermöglichte, ein Gerät zu infizieren, ohne dass ein Link angeklickt werden musste, beispielsweise auf dem Wege eines verpassten WhatsApp-Anrufs. Die saudi-arabischen Kunden kauften die Technologie umgehend für einen Betrag in Höhe von 55 Mio. EUR^{181 182}. In diesem Zusammenhang muss erwähnt werden, dass das saudische Regime ein Jahr später, am 2. Oktober 2018, Jamal Khashoggi im saudi-arabischen Konsulat in der Türkei tötete, nachdem er und ihm nahestehende Personen mit der Pegasus-Software überwacht worden waren.

Black Cube

96. Black Cube ist ein Unternehmen, das ehemalige Offiziere israelischer Nachrichtendienste wie Mossad engagiert. Das Unternehmen beschäftigt Einsatzkräfte mit gefälschten Identitäten. Laut The New Yorker verpflichtete der ehemalige CEO der

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.](#)

NSO Group Shalev Hulio Black Cube, nachdem drei Rechtsanwälte – Mazen Masri, Alaa Mahajna und Christiana Markou – in Israel und Zypern gegen NSO und ein angeschlossenes Tochterunternehmen klagten¹⁸³.

Kauf und Einsatz von Spähsoftware durch Zypern

97. Die zyprische Regierung hat nicht nur den Ruf, ein gefälliges Klima für die Ausfuhr von Spähsoftware zu fördern, sondern hat in der Vergangenheit selbst Spähsoftware gekauft. Angeblich hat sie sogar selbst Überwachungssysteme benutzt. Zum Zeitpunkt der Berichtverfassung war weiterhin unklar, wann Zypern herkömmliche Überwachungsmethoden und wann Spähsoftware benutzt hat.

Opfer Makarios Drousiotis

98. Ab Februar 2018 wurde der Investigativjournalist Makarios Drousiotis angeblich von der zyprischen Regierung ausgespäht. In diesem Fall begann die Bespitzelung, während Drousiotis seine ehemalige Position als Assistent des zyprischen EU-Kommissars für Humanitäre Hilfe und Krisenmanagement, Christos Stylianides, bekleidete und während seiner Recherchen zu den finanziellen Verbindungen zwischen Präsident Anastasiades und russischen Subjekten wie dem Oligarchen Dmitri Rybolowlew. Laut Drousiotis wurde der Überwachungsversuch durch seine letztere Tätigkeit ausgelöst¹⁸⁴.

Sonstige Bemerkungen

99. Zypern verfügt scheinbar über einen stabilen Rechtsrahmen für den Schutz personenbezogener Daten und der Privatsphäre, die Genehmigung von Überwachung und für Ausfuhren. In der Praxis lassen sich diese Regelungen jedoch offenbar leicht umgehen, und Politik, Sicherheitskräfte und die Überwachungsbranche unterhalten enge Verbindungen zueinander. Augenscheinlich ist die laxe Anwendung der Regeln der Grund, der Zypern für den Handel mit Spähsoftware so attraktiv macht. Zudem ist Zypern von erheblichem strategischem Interesse für Russland, die Türkei und die USA. Mit Blick auf den Handel mit Spähsoftware erscheinen enge Beziehungen zu Israel des Weiteren von besonderem gegenseitigem Nutzen. In diplomatischen Beziehungen sind Ausfuhrgenehmigungen für Spähsoftware zu einer Währung geworden.

Beispiel Spanien

100. Die Enthüllungen vom Juli 2021 im Zuge der Pegasus-Recherchen brachten zahlreiche Ziele von Bespitzelungen in Spanien ans Licht. Allerdings scheint es, dass unterschiedliche Akteure aus unterschiedlichen Gründen an diesen Aktivitäten beteiligt waren. Allgemein wird davon ausgegangen, dass die marokkanischen Behörden den Ministerpräsidenten Pedro Sanchez, die Verteidigungsministerin Margarita Robles und den Innenminister Fernando Grande-Marlaska, ebenso wie den französischen Präsidenten und französische Regierungsminister ins Visier nahmen¹⁸⁵. Die Ausspähung einer

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

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

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.

zweiten Gruppe von Opfern wird als „CatalanGate“ bezeichnet¹⁸⁶. Betroffen waren in diesem Fall katalanische Parlamentarier, Mitglieder des Europäischen Parlaments, Angehörige zivilgesellschaftlicher Organisationen und einige Familienangehörige und Beschäftigte, die mit diesen Opfern in Verbindung stehen¹⁸⁷. Erste Berichte über den „CatalanGate“-Überwachungsskandal erschienen im Jahr 2020, aber erst nach Abschluss eingehender Untersuchungen durch Citizen Lab im April 2022 wurde das Ausmaß des Skandals offenbart. Die Untersuchungen ergaben, dass mindestens 65 Personen zu Zielscheiben der Ausspähaktion wurden¹⁸⁸. Im Mai 2020 räumten die spanischen Behörden ein, dass sie 18 dieser 65 Opfer mit gerichtlicher Genehmigung ins Visier genommen hatten¹⁸⁹.

Kauf von Spähsoftware

101. In der Vergangenheit wurde der Kauf diverser Spähsoftwareprogramme, etwa von SITEL im Jahr 2001 und der Spähsoftware von Hacking Team im Jahr 2010, durch das Innenministerium, den spanischen Geheimdienst (CNI) und die Polizei allgemein bekannt gemacht¹⁹⁰. Früheren Berichten von Citizen Lab zufolge wird Spanien außerdem verdächtigt, Kunde von Finfisher zu sein¹⁹¹. Die spanische Tageszeitung *El Pais* berichtete 2020, dass Spanien mit der NSO Group Geschäfte geschlossen hat und dass der spanische Geheimdienst CNI Pegasus routinemäßig nutzt¹⁹². Angeblich kaufte die spanische Regierung die Spähsoftware in der ersten Hälfte der 2010er Jahre für einen geschätzten Betrag von 6 Mio. EUR¹⁹³ ¹⁹⁴. Außerdem hat ein ehemaliger NSO-Mitarbeiter bestätigt, dass Spanien ein Kundenkonto bei dem Unternehmen unterhält, auch wenn die spanischen Behörden nicht geneigt war, dies zu bestätigen oder zu kommentieren¹⁹⁵.

Rechtlicher Rahmen

102. Nach Artikel 18 der spanischen Verfassung von 1978 ist das Recht auf Privatsphäre, das das Post- und Fernmeldegeheimnis einschließt, geschützt¹⁹⁶. Der Einsatz von

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, p. 1.

¹⁸⁸ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022, p. 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, p. 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, p. 5.

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

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

Spähsoftware wie Pegasus und Candiru stellt einen Verstoß gegen Artikel 18 dar; allerdings gilt im Falle einer gerichtlichen Genehmigung eine Ausnahme von diesem Recht¹⁹⁷. Weitere Ausnahmen hiervon sieht die Verfassung in Teil I Abschnitt 55 vor, wo es heißt, dass bei Personen, gegen die Ermittlungen zu Aktivitäten in Verbindung mit bewaffneten Gruppen oder terroristischen Organisationen laufen, einige Freiheiten unter Beteiligung der Gerichte und ordnungsgemäßer parlamentarischer Kontrolle ausgesetzt werden können¹⁹⁸.

103. Der spanische Nachrichtendienst besteht im Wesentlichen aus drei Stellen. Erstens der nationale Geheimdienst CNI, der dem Verteidigungsministerium untersteht. Der Direktor des CNI wird vom Verteidigungsminister ernannt und dient dem Ministerpräsidenten als leitender Berater in Fragen der nachrichtendienstlichen Aufklärung und Spionageabwehr¹⁹⁹. Die zweite Stelle ist das Amt für Verfassungsschutz, das Zentrum für den Kampf gegen Terrorismus und organisierte Kriminalität (CITCO). Die dritte und letzte Stelle ist der spanische Militärgeheimdienst (CIFAS). Auch CIFAS untersteht der direkten Aufsicht des Verteidigungsministeriums^{200 201}.

Ex-ante-Kontrolle

104. Die Überwachungsaktionen in Spanien wurden großteils vom CNI durchgeführt, einer Stelle, die in der Vergangenheit bereits in mehrere Bespitzelungsskandale verwickelt war²⁰². Der CNI wurde gemäß Gesetz 11/2002 vom 6. Mai eingerichtet, das dem CNI die Befugnis erteilt, „sicherheitsrelevante Ermittlungen“ durchzuführen²⁰³. Allerdings gibt es kaum Erläuterungen zu den Mitteln oder Beschränkungen entsprechender Tätigkeiten²⁰⁴. Zudem sieht das Gesetz 11/2002 ein Instrument für die parlamentarische, exekutive und legislative Aufsicht und Kontrolle des CNI²⁰⁵ vor, wobei die parlamentarische Kontrolle vom Ausschuss für Staatsgeheimnisse des Spanischen Kongresses ausgeübt wird, der 1995 eingerichtet wurde²⁰⁶. Dem Delegierten Ausschuss für nachrichtendienstliche Angelegenheiten obliegt die exekutive Kontrolle dieser Stelle, und er koordiniert die nachrichtendienstlichen Tätigkeiten des CNI²⁰⁷. Der Verteidigungsausschuss des spanischen Abgeordnetenhauses schließlich übt die

¹⁹⁷ Constitution of Spain 1978,

https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primerero.aspx , Section 18.

¹⁹⁸ Constitution of Spain 1978,

https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primerero.aspx , 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, p. 40.

²⁰² Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022, p. 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>, 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>, Article 11.

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>, Article 6.

legislative Aufsicht über den CNI aus²⁰⁸. In der jährlichen nachrichtendienstlichen Direktive werden die Prioritäten des CNI für das Jahr festgelegt²⁰⁹.

Ex-post-Kontrolle

105. Mit den Gesetzen zur Einrichtung des CNI wurde auch der Verteidigungsausschuss des Abgeordnetenhauses eingerichtet, der für die Zuweisung vertraulicher Mittel an den CNI und die Erstellung eines Jahresberichts über den CNI verantwortlich ist. Allerdings ist in der spanischen Verfassung nicht festgelegt, Zugang zu Dokumente oder Informationen in Bezug auf die Arbeit der Nachrichtendienste zu gewähren, und eine solche Vorgabe fehlt vor allem auch im rechtlichen Rahmen des Gesetzes über Transparenz. Daher bleibt die Tätigkeit des CNI größtenteils im Verborgenen und es mangelt an Transparenz²¹⁰.
106. Der Ausschuss für Staatsgeheimnisse ist verpflichtet, einen jährlichen Bericht zu den Tätigkeiten der Geheimdienste einzureichen; als dieser jedoch in der Folge der Überwachung durch den CNI zusammengekommen ist, war dies die erste Sitzung der Einrichtung seit mehr als zwei Jahren. Die Leiterin des CNI, Paz Esteban, erschien am 5. Mai 2022 vor dem Ausschuss, um die gerichtlichen Genehmigungen für die 18 Opfer vorzulegen, für deren Überwachung die Behörden die Verantwortung übernommen haben²¹¹. Die Anhörung war nicht öffentlich und den Anwesenden war es nicht gestattet, den Raum mit jeglicher Art von Elektronik zu betreten²¹².

Öffentliche Kontrolle

107. Seitdem der „CatalanGate“-Skandal im April 2022 ans Licht kam, hat sich die Öffentlichkeit eingehend damit befasst. Die spanischen Medien und Medienunternehmen weltweit haben in Zusammenarbeit mit Organisationen der Zivilgesellschaft intensiv daran gearbeitet, das Überwachungssystem in Spanien zu untersuchen und sich für die Grundrechte der Opfer einzusetzen. Umgekehrt haben manche spanische Politiker versucht, CitizenLab zu diskreditieren, indem sie behaupteten, ihre Methoden seien unseriös oder dass sie politisch motiviert seien. Ein Mitarbeiter von CitizenLab, der selbst katalanischer Herkunft ist, gehörte zu den Zielpersonen, ebenso wie seine Eltern, die überhaupt nicht politisch aktiv sind²¹³.

Rechtsbehelf

108. Die Staatsanwaltschaft hat bei der Audiencia Nacional, dem spanischen nationalen Gericht, in Madrid eine Klage in Bezug auf die Überwachung von Premierminister

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>, 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, p. 776.

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

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

Sanchez und Verteidigungsministerin Robles eingereicht²¹⁴. Der Richter Jose Luis Calama, Leiter des zentralen Ermittlungsgerichts Nummer 4 ist für diesen laufenden Fall verantwortlich²¹⁵. Am 13. Oktober 2022 übermittelte Richter Calama einen Fragebogen an Robles und Grande-Marlaska, der eine Anfrage einer Bestätigung durch Rechtsquellen enthielt, wie die Infizierung mit Pegasus ermittelt wurden. Die Staatsanwaltschaft und das Büro des Staatsanwalts übermittelten ebenfalls Fragen an die Minister²¹⁶.

109. Im Gegensatz zu dem schnell vorankommenden von Sanchez u. a. eingereichten Fall in Madrid kommen die Fälle, die in Barcelona von katalanischen Opfern der Spähsoftware eingereicht wurden, nur langsam voran^{217 218}. Die erste Klage wurde im Untersuchungsgericht Nummer 32 in Barcelona von zwei Opfern von Pegasus im Jahr 2020 eingereicht: dem ehemaligen Präsidenten des katalanischen Parlaments und derzeitigen Minister für Wirtschaft und Arbeit Roger Torrent und dem früheren Minister für auswärtige Angelegenheiten, institutionelle Beziehungen und Transparenz von Katalonien und derzeitigen Präsident der ERC im Stadtrat von Barcelona, Ernest Maragall²¹⁹. Andreu Van Den Eynde ist einer der Anwälte, die Torrent und Maragall in diesem Fall vertreten, und selbst ein Opfer von Pegasus. Van Den Eynde hat die Gerichte immer wieder kritisiert, dass sie die Verfahren verzögern und den Fall geradezu „lähmen“²²⁰. Omnium Cultural und die Partei Candidatura d’Unitat Popular (Kandidatur der Volkseinheit, CUP) haben ebenfalls Klage in demselben Gericht in Barcelona eingereicht. Der Anwalt Benet Salellas, der in beiden Fällen betroffen ist, behauptet, dass die spanische Regierung hinter den Angriffen steht²²¹.
110. Da das spanische nationale Gericht für die schwersten Straftaten in allen Gebieten rechtlich zuständig ist, ist es möglich, dass die Staatsanwaltschaft die Zusammenlegung aller Pegasus-Fälle beantragen könnte²²². Mit anderen Worten: Die Fälle der Opfer der spanischen Regierung und der „CatalanGate“-Opfer würden alle vor dem spanischen nationalen Gericht in Madrid verhandelt werden. Die Anwälte der katalanischen Opfer

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.

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

machen geltend, dass es keinen Zusammenhang zwischen den Fällen gibt, solange nicht bewiesen ist, dass der Täter in allen Fällen der Überwachung derselbe ist²²³.

111. Es gibt eine Reihe anderer anhängiger Rechtssachen im Zusammenhang mit den 65 katalanischen Opfern. Eine solche Klage wurde von Rechtsanwalt und Pegasus-Opfer Gonzalo Boye im Namen von mindestens 19 Opfern gegen NSO, seine drei Gründer Niv Karmi, Shalev Hulio und Omri Lavie, Q Cyber Technologies und OSY, eine Tochtergesellschaft mit Sitz in Luxemburg, eingereicht^{224 225}. Auch in einer Reihe anderer EU-Mitgliedstaaten, darunter Frankreich, Belgien, die Schweiz, Deutschland und Luxemburg, sind aufgrund der Überwachung der katalanischen Separatisten im Exil rechtliche Schritte eingeleitet worden²²⁶.

Einzelziele

112. Die gezielte Ausspähung katalanischer Bürger mit Spähsoftware begann Berichten zufolge bereits 2015 und wurde seit 2017 in großem Umfang durchgeführt²²⁷. Nach einer ersten Medienberichterstattung im Jahr 2020 wurde der gesamte Skandal im April 2022 mit der Veröffentlichung des CitizenLab-Berichts der Universität Toronto in ganz Europa bekannt. Da seit dem Beginn des Hackings und diesen Enthüllungen viel Zeit verstrichen ist, konnte eine Reihe von Zielpersonen aufgrund verschiedener Faktoren nicht identifiziert oder weiter untersucht werden, darunter eine Reihe von Zielpersonen, die das betreffende Telefon entsorgt haben²²⁸.
113. Der spanische Premierminister Pedro Sánchez, die Verteidigungsministerin Margarita Robles und der Innenminister Fernando Grande-Marlaska wurden zwischen Mai und Juni 2021 mit Pegasus angegriffen²²⁹. Bisher liegen nur wenige Informationen über die Einzelheiten dieses Hackings vor, da sie von der Regierung angekündigt wurden und nicht das Ergebnis einer Untersuchung von CitizenLab oder eines anderen Recherchedienstes oder investigativen Journalisten waren. Sánchez und Robles sind die Leiter der beiden Regierungsabteilungen, die den CNI, das für die Überwachung in Spanien zuständige Organ, beaufsichtigen. Die infizierten Geräte von Sánchez und Robles waren Regierungsgeräte und wurden gelegentlich auf Spähsoftware gescannt²³⁰. Grande-Marlaska wurde über sein privates Gerät infiziert²³¹. Landwirtschaftsminister Luis Planas, der früher als Diplomat in Marokko tätig war, wurde ebenfalls mit Spähsoftware angegriffen, allerdings ohne Erfolg. Es wurde berichtet, dass die

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, p. 5.

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

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.

marokkanische Regierung möglicherweise für diese Angriffe verantwortlich sein könnte, diese Information wurde jedoch nicht bestätigt²³².

114. Insgesamt wurde bestätigt, dass 65 Katalanen mit Söldner-Spähsoftware angegriffen wurden, 63 mit Pegasus, vier mit Candiru und mindestens zwei Personen mit beiden Programmen²³³. Mindestens 51 Personen wurden erfolgreich infiziert²³⁴. Die spanische Regierung hat sich geweigert, sich dazu zu äußern, ob sie für die Überwachung anderer Opfer als der 18, die sie zugegeben hat, verantwortlich war oder nicht²³⁵. Die meisten dieser 18 Personen wurden nie eines Verbrechens angeklagt und stehen dennoch auf dieser Liste. Verteidigungsministerin Robles hat sich in hohem Maße auf das Gesetz über die Wahrung von Staatsgeheimnissen berufen, anstatt die Gründe für die Überwachung dieser speziellen Zielpersonen zu erläutern²³⁶. Alle 65 katalanischen Zielpersonen standen zu irgendeinem Zeitpunkt in Kontakt mit den katalanischen Separatisten, die außerhalb Spaniens leben.

Mitglieder des Europäischen Parlaments

115. Eine der Schlüsselgruppen, die – wie enthüllt wurde – zur Zielscheibe geworden ist, sind die unabhängigkeitsbefürwortenden katalanischen Mitglieder des Europäischen Parlaments. Jede und jeder von ihnen wurde entweder direkt oder indirekt anhand einer Methode, die von CitizenLab als relationale Zielbestimmung (relational targeting) bezeichnet wird, mit einer Spähsoftware gehackt²³⁷: Diana Riba i Giner, Antoni Comín i Oliveres, Jordi Solé, Carles Puigdemont, und Clara Ponsati.

Katalanische Politiker

116. Der ehemalige Präsident des Parlaments von Katalonien und derzeitige Handels- und Arbeitsminister Roger Torrent gehörte zu den ersten Personen, die als Opfer der WhatsApp-Infektion mit Pegasus im Jahr 2019 an die Öffentlichkeit getreten sind²³⁸. Kurz darauf traten auch der Vorsitzende der unabhängigkeitsbefürwortenden Republikanischen Linken Kataloniens, Ernest Maragall, und Anna Gabriel, ein ehemaliges regionales Mitglied des Parlaments der Candidatura d'Unitat Popular, ebenfalls als Opfer von Pegasus an die Öffentlichkeit²³⁹. Seit 2010 waren alle Ministerpräsidenten Kataloniens Angriffen mit Spähsoftware ausgesetzt, entweder

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, p. 1.

²³⁴ Citizen Lab CatalanGate Report, <https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>, 18 April 2022, p. 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, p. 6.

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, p. 5.

während oder nach ihrer Amtszeit²⁴⁰. Unter den 65 Zielpersonen waren nicht weniger als 12 Mitglieder der Republikanischen Linken Kataloniens, einschließlich der Generalsekretärin der Partei, Marta Rovira, die laut CitizenLab im Juni 2020 mindestens zwei Mal gehackt wurde. Äußerst wichtig ist, dass sowohl Frau Gabriel als auch Frau Rovira zum Zeitpunkt ihrer Überwachung im Anschluss an die Unabhängigkeitserklärung Kataloniens nach dem Referendum im Jahr 2017 in der Schweiz lebten.

Zivilgesellschaftliche Organisationen

117. Jordi Domingo war einer der ersten katalanischen Aktivisten, der Berichten zufolge im Jahr 2020 zur Zielscheibe wurde. Obwohl er die Unabhängigkeit Kataloniens unterstützte, wurde im Guardian berichtet, dass Domingo überzeugt war, irrtümlicherweise zur Zielperson geworden zu sein. Da er bei den Ereignissen von 2017 keine wesentliche Rolle gespielt hatte, war die eigentliche Zielperson seiner Ansicht nach ein Anwalt mit demselben Namen, der an der Abfassung der Verfassung Kataloniens mitgewirkt hatte²⁴¹.

Anwälte

118. Gonzalo Boye hat viele hochrangige katalanische Mandanten vertreten, wie zum Beispiel die ehemaligen Ministerpräsidenten Puigdemont und Torra²⁴². Fünf Monate lang, zwischen Januar und Mai 2020, war er selbst Opfer von Pegasus²⁴³. Boye wurde in diesem Zeitraum ganze 18 Mal zur Zielperson und zwar anhand von Textnachrichten, die Tweets von zivilgesellschaftlichen Organisationen oder bekannten Nachrichtenmedien zu sein schienen²⁴⁴. CitizenLab bestätigte mindestens eine erfolgreiche Infektion am 30. Oktober 2020. Die Infektion erfolgte nur 48 Stunden nach der Festnahme einer seiner Mandanten²⁴⁵. Dadurch, dass Boye zur Zielperson wurde, wurde die Rechtmäßigkeit eines Angriffs auf das Privileg der Angehörigen von Rechtsberufen in Frage gestellt.
119. Andreu van den Eynde i Adroer wurde am 14. Mai 2020 erfolgreich mit Pegasus infiziert²⁴⁶. Er wurde gehackt, während er als Anwalt seine Mandanten Raul Romeva und Oriol Junqueras in ihrem Verfahren vor dem Obersten Gerichtshof vertrat.
120. Auch der bekannte Anwalt Jaume Alonso-Cuevillas wurde infiziert, während er katalanische Schlüsselfiguren wie Carles Puigdemont vertrat. CitizenLab war jedoch nicht in der Lage, das genaue Datum der erfolgreichen Infektion festzustellen.

²⁴⁰ Artur Mas (after leaving office), Carles Puigdemont (relational targeting), Joaquim Torra (while in office), Pere Aragonès (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/>

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

I.F. Andere Mitgliedstaaten

121. Einzelstaatliche Behörden haben bisher nur sehr wenige offizielle Informationen über den Erwerb und die Nutzung von Spähsoftware in ihren Ländern herausgegeben, sowohl hinsichtlich der finanziellen Aspekte als auch bezüglich des zugrunde liegenden Rechtsrahmens. Anbieter und Länder, die Exportlizenzen herausgeben (insbesondere Israel), geben keinerlei Informationen über ihre Kunden heraus. Lediglich Österreich, Polen und Zypern haben den Fragebogen beantwortet, den der Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (PEGA) am 15. Juli 2022 verschickt hatte, zumeist allerdings in sehr allgemeiner, geradezu ausweichender Art und Weise.
122. Wenn man die einzelnen Informationen aus den unterschiedlichen Quellen jedoch zusammensetzt, kann ein Teilbild rekonstruiert werden. Dadurch lassen sich Aspekte ermitteln, die Anlass zur Besorgnis geben und eine eingehendere Untersuchung erfordern.
123. Es kann mit Sicherheit angenommen werden, dass die Behörden aller Mitgliedstaaten auf die eine oder andere Art und Weise Spähsoftware nutzen. Spähsoftware kann direkt oder über einen Stellvertreter, ein Maklerunternehmen oder einen Mittelsmann erworben werden. Möglicherweise werden auch Vereinbarungen über bestimmte Dienstleistungen geschlossen, statt die Software tatsächlich zu erwerben. Zusätzliche Dienstleistungen können angeboten werden, wie die Schulung von Personal oder die Bereitstellung von Servern. Wichtig ist, sich zu vergegenwärtigen, dass der Erwerb und die Nutzung von Spähsoftware sehr kostspielig ist und sich auf Millionen von Euro beläuft. In vielen Mitgliedstaaten wird diese Ausgabe jedoch nicht im regulären Haushalt ausgewiesen, wodurch Kontrollen umgangen werden können.
124. Durch Informationen, die von der NSO Group bereitgestellt wurden, wissen wir, dass Pegasus in mindestens 14 EU-Länder verkauft wurde, bis die Verträge mit zwei Ländern beendet wurden. Welche Länder das sind, ist nicht bekannt, aber es besteht die allgemeine Annahme, dass es sich um Polen und Ungarn handelt. Solange die NSO Group oder die israelische Regierung keine offizielle Stellungnahme zur Beendigung eines Vertrages herausgibt, kann jedoch nicht überprüft werden, ob dies der Wahrheit entspricht.
125. Eine weitere Teilinformation bildet die Teilnehmerliste der Messe „ISS World“ (Intelligence Support Systems), auch bekannt als „The Wiretappers Ball“ (der Ball der Abhörwanzen), aus dem Jahr 2013. Mit Ausnahme von Portugal und Luxemburg waren alle derzeitigen EU-Mitgliedstaaten von einem breiten Spektrum von Organisationen vertreten, einschließlich der lokalen Polizeikräfte²⁴⁷. In den vergangenen Jahren ist die NSO Group zum Hauptsponsor der Veranstaltung aufgestiegen, während auch Intellexa, Candiru, RCS und viele weitere Organisationen zu den Sponsoren zählen²⁴⁸.
126. Die Mitgliedstaaten sind nicht nur Kunden der gewerblichen Anbieter von Spähsoftware, sondern spielen auch andere, unterschiedliche Rollen im Handel mit Spähsoftware. Einige dienen den Anbietern von Spähsoftware als Gastgeberländer,

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

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

andere sind das favorisierte Ziel für Finanz- und Bankdienstleistungen, andere wiederum bieten den Akteuren dieser Sparte Staatsangehörigkeit und Wohnsitz an.

127. Spähsoftware wird eindeutig auch von den Vollzugsbehörden verwendet, nicht nur von Nachrichtendiensten. Es gibt keinerlei Informationen über das Material, das mithilfe der Spähsoftware erbeutet wird, wie es erbeutet wird und wie es genutzt wird, um Verbrechen im Rahmen der europäischen polizeilichen und justiziellen Zusammenarbeit zu ermitteln, zu untersuchen und strafrechtlich zu verfolgen. Ob dieses Material im Rahmen der europäischen polizeilichen und justiziellen Zusammenarbeit als Beweismaterial vor Gericht verwendet werden darf, auch von Europol und Eurojust, ist durchaus fraglich.

Die Niederlande

128. In der Koalitionsvereinbarung der niederländischen Regierung aus dem Jahr 2017 wurde festgehalten, dass es der niederländischen Polizei untersagt ist, Spähsoftware von Anbietern zu erwerben, die ihre Produkte „dubiosen Regimen“ zur Verfügung stellen, die später als „Länder, die sich schweren Verletzungen gegen die Menschenrechte oder humanitäres Völkerrecht schuldig gemacht haben“ bezeichnet werden. Vor jeglicher Anschaffung von Spähsoftware ist die niederländische Polizei gehalten, den Anbieter zu fragen, ob er an Länder Produkte geliefert hat, die von der EU oder von den VN sanktioniert wurden, und zu prüfen, ob das Land, in dem der Anbieter ansässig ist, über ein Ausfuhrkontrollregime verfügt, in dessen Rahmen die Menschenrechte bei der Vergabe der Ausfuhrgenehmigung kontrolliert werden. Diese Prüfung wird regelmäßig wiederholt. Es sei darauf hingewiesen, dass diese Einschränkung lediglich für den Erwerb von Spähsoftware durch die Polizei zu gelten scheint. Die Nachrichtendienste werden nicht explizit erwähnt. Nach Regierungsinformationen nutzt die Polizei seit 2019 Hacking-Software, obgleich nicht erwähnt wird, welche Art von Software genutzt wird²⁴⁹. Die NSO Group und ihre Spähsoftware Pegasus würden die oben genannten Standards anscheinend nicht erfüllen, jedenfalls nicht vor der Verschärfung des israelischen Exportregimes im Dezember 2021²⁵⁰. In die Ausgaben für den Erwerb und die Nutzung des Spähsoftware-Systems wird sowohl von der Polizei als auch von den Nachrichtendiensten keine Einsicht gewährt.
129. Am 4. Oktober 2022 wurde enthüllt, dass das niederländische Verteidigungsministerium im November 2019 einen Vertrag mit WiSpear unterzeichnen wollte, dem Unternehmen von Tal Dilian, der zuvor Cytrox erworben hatte, dem Hersteller der Spähsoftware Predator²⁵¹. Es ist unklar, ob dieser Vertrag unterzeichnet wurde und ob dem niederländischen Verteidigungsministerium eine Spähsoftware zur Verfügung gestellt wurde.

Belgien

130. In einem Interview mit The New Yorker enthüllte ein ehemaliger israelischer Geheimdienstmitarbeiter, dass die belgische Polizei Pegasus bei ihren Operationen

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>

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

einsetzt²⁵². Daraufhin erklärte die belgische Polizei, „nicht über technische und/oder taktische Mittel zu kommunizieren, die für Ermittlungen und Einsätze verwendet werden“. Im September 2021 erwähnte Justizminister Vincent Van Quickenborne, dass Pegasus von den Geheimdiensten „auf legale Weise verwendet werden kann“, wollte aber nicht bestätigen, ob der belgische Geheimdienst ein Kunde von NSO ist oder Spähsoftware gegen Kriminelle einsetzt²⁵³.

Deutschland

131. Im September 2021 wurde berichtet, dass das deutsche Bundeskriminalamt (BKA) Ende 2020 Pegasus erworben hatte. Es ist wichtig, an dieser Stelle darauf hinzuweisen, dass das deutsche Recht zwei Formen des Einsatzes von Spähsoftware unterscheidet²⁵⁴: Zugriff auf alle Informationen (Online-Durchsuchung²⁵⁵) und Zugriff nur auf die Live-Kommunikation (Quellen-TKÜ²⁵⁶). Da die ursprüngliche Pegasus-Software auf alle Informationen auf einem Gerät zugreifen konnte und nicht nur auf die Live-Kommunikation, würde ihre Verwendung durch das BKA gegen das Gesetz verstoßen. Das BKA ersuchte daher NSO darum, einen Quellcode zu schreiben, damit Pegasus nur auf die gesetzlich erlaubten Daten zugreifen kann. Zunächst weigerte sich NSO, dies zu tun²⁵⁷. Erst nach neuen Verhandlungen willigte NSO ein, sodass das BKA eine modifizierte Version erwarb²⁵⁸. Sie soll seit März 2021 im Einsatz sein. Bei der vom BKA gekauften Version waren bestimmte Funktionen gesperrt, um Missbrauch zu verhindern, obwohl unklar ist, wie das in der Praxis funktioniert. Das BKA hat einen Bericht über diese modifizierte Version verfasst, der jedoch als Verschlussache eingestuft bleibt²⁵⁹.

Verwendung von FinFisher

132. In den Jahren 2012 und 2013 kauften sowohl das BKA als auch das LKA Berlin unabhängig voneinander die Spähsoftware FinFisher (mehr zu dieser Spähsoftware im Kapitel über die Spähsoftware-Industrie). Auch hier, genau wie im Fall von Pegasus, wies das BKA das Unternehmen an, die Spähsoftware FinFisher so zu entwickeln, dass sie nicht auf alle Daten auf einem Gerät zugreifen kann, sondern nur auf die Live-Kommunikation, damit sie mit den deutschen Gesetzen konform ist.

Malta

133. Mehrere Schlüsselfiguren des Handels mit Spähsoftware haben ein Unternehmen auf Malta angemeldet oder einen maltesischen Pass erhalten, aber sie sind offenbar weder dort ansässig noch scheinen ihre Unternehmen dort aktiv zu sein. Bisher wurden einige

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-spionagetool-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/spaeh-software-pegasus-deutschland-101.html>

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

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

wichtige Persönlichkeiten im Handel mit Spähsoftware identifiziert: Tal Dilian, Anatoly Hurgin, Felix Bitzios, Stanislaw Szymon Pelczar und Peter Thiel.

Frankreich

Opfer in Frankreich

134. Im Sommer 2021 deckte das Pegasus-Projekt mehrere Fälle von versuchten Hacks durch die Pegasus-Spähsoftware in Frankreich auf²⁶⁰. Dieser durchgesickerte Datensatz enthielt die Telefonnummer von Präsident Emmanuel Macron sowie die Telefonnummern von 14 Mitgliedern seines Kabinetts²⁶¹ ²⁶². Die Ergebnisse forensischer Analysen haben bestätigt, dass die Telefone mehrerer Minister mit der Pegasus-Spähsoftware infiziert waren²⁶³.

Spähsoftware-Firmen in Frankreich

135. Frankreich ist auch die Heimat der Spähsoftware-Industrie. Nexa Technologies, Teil der Intellexa-Allianz von Tal Dilian, ist ein französisches Cyberverteidigungs- und Cyberinformationsunternehmen, das im Jahr 2000 gegründet wurde²⁶⁴. Nexa Technologies wird von ehemaligen Managern von Amesys geleitet. Amesys wurde 1979 gegründet²⁶⁵ und ist bekannt für den Verkauf eines Programms namens Cerebro, das in der Lage ist, die elektronische Kommunikation seiner Opfer, wie E-Mail-Adressen und Telefonnummern, zu verfolgen²⁶⁶.

Irland

136. Irland ist aufgrund seiner Steuergesetze zu dem Mitgliedstaat geworden, in dem einige der wichtigsten in Skandale verwickelten Spähsoftware-Firmen registriert sind. Am 20. September 2022 enthüllte *The Currency*, ein irischer Verlag für investigativen Journalismus, dass sowohl Thalestris Limited, das Mutterunternehmen von Intellexa, als auch Intellexa selbst ihren Hauptsitz in Irland haben und bei einer Anwaltskanzlei in der Stadt Balbriggan registriert sind. Es ist bemerkenswert, dass der Antrag auf Eintragung von Thalestris Limited in Irland im November 2019 von einem Spezialisten für Unternehmensgründungen eingereicht wurde, nur 12 Tage nachdem die strafrechtliche Ermittlung der zyprischen Behörden gegen Dilian und sein Unternehmen WiSpear öffentlich bekannt wurden. Tal Dilian selbst, der Vorstandsvorsitzende von Intellexa, taucht in den irischen Unternehmensunterlagen nicht auf, aber seine Berichten zufolge zweite Ehefrau Sara Hamou wird als Direktorin sowohl von Thalestris als auch von Intellexa genannt²⁶⁷.

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'Egypte : la société Nexa Technologies mise en examen.](#)

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

Luxemburg

137. Luxemburg beherbergt neun Unternehmen, die direkt mit der NSO-Gruppe verbunden sind, wie Amnesty International im Juni 2021 aufdeckte²⁶⁸. Die Tatsache, dass Außenminister Jean Asselborn zunächst nur von zwei im Land ansässigen NSO-Unternehmen wusste²⁶⁹ und dass die Namen der neun Unternehmen (wie Triangle Holdings SA, Square 2 SARL und Q Cyber Technologies SARL) die Verbindung zur NSO-Gruppe nicht sofort erkennen lassen, zeigt, wie undurchsichtige Geschäftsstrukturen in Luxemburg es den Unternehmen ermöglichen, völlig unbemerkt von der Öffentlichkeit zu operieren.

Italien

138. Bislang gibt es keine Berichte über den möglichen Kauf von Spähsoftware durch die italienischen Behörden. Abgesehen vom ehemaligen Ministerpräsidenten und Kommissionspräsidenten Romano Prodi, der von den marokkanischen Geheimdiensten mit Pegasus ausspioniert wurde, sind keine hochrangigen Fälle von Spionage bekannt geworden²⁷⁰. Als ehemaliger UN-Sonderbeauftragter für die Sahelzone hätte er ein interessantes Ziel für Marokko sein können, da er möglicherweise mit hochrangigen Persönlichkeiten in der Westsahara oder Algerien vernetzt ist.

Österreich

139. In der Antwort auf schriftliche Anfragen des österreichischen Nationalrats (Nationalrat) erklärte der ehemalige Innenminister Karl Nehammer, dass Österreich kein Kunde von NSO gewesen sei²⁷¹. Der ehemalige Bundeskanzler Sebastian Kurz hat jedoch enge Beziehungen zum Gründer der NSO-Gruppe, und DSIRF, ein großer Spähsoftware-Anbieter, hat seinen Sitz in Österreich.

Estland

140. Berichten zufolge war Estland ebenfalls am Kauf der Spähsoftware Pegasus der NSO-Gruppe interessiert. Im Jahr 2018 fanden erste Verhandlungen zwischen Estland und der NSO-Gruppe statt, die Estland dazu veranlassten, eine Anzahlung auf das 30-Millionen-Dollar-Geschäft für die Überwachungssoftware zu leisten²⁷².

Litauen

141. Anatoly Hurgin, ein russisch-israelischer Staatsbürger, ehemaliger israelischer Militäringenieur und Mitentwickler von Pegasus zusammen mit NSO, ist Berichten zufolge Eigentümer eines Unternehmens in Litauen mit dem Namen UAB „Communication technologies“, das im Bereich „Verbindungs- und

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/>

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](#)

Telekommunikationsdienste“ tätig ist²⁷³. Außerdem erwarb er 2015 einen maltesischen goldenen Pass²⁷⁴.

Bulgarien

142. In Bulgarien werden Ausfuhrkontrollen und Ausfuhrgenehmigungen für Produkte, die gemäß der EU-Verordnung über Güter mit doppeltem Verwendungszweck als „mit doppeltem Verwendungszweck“ eingestuft sind, vom Wirtschaftsministerium und insbesondere von der Interministeriellen Kommission für Ausfuhrkontrolle und Nichtverbreitung von Massenvernichtungswaffen kontrolliert²⁷⁵. Der derzeitige Minister für Wirtschaft und Industrie ist Nikola Stoyanov²⁷⁶. Bis heute bestreiten die bulgarischen Behörden, der NSO-Gruppe Ausfuhrgenehmigungen erteilt zu haben²⁷⁷. Der frühere Private-Equity-Eigentümer der NSO-Gruppe, Novalpina Capital, betonte jedoch, dass NSO-Produkte sowohl von Zypern als auch von Bulgarien aus in die EU exportiert werden^{278 279 280}. Diese beiden Behauptungen sind widersprüchlich.

I.G. Organe der Union

Die Kommission als Ziel

143. Infolge der Enthüllungen von Forbidden Stories und Amnesty International im Juli 2021 richtete die Kommission ein „Spezialteam mit internen Experten“ ein, das am 19. Juli 2021 eine interne Untersuchung einleitete, um zu „überprüfen, ob Geräte von Kommissionsbediensteten und Mitgliedern des Kollegiums von Pegasus angegriffen wurden“²⁸¹. Am 23. November 2021 übermittelte Apple offizielle Benachrichtigungen an die Geräte von Kommissar Reynders und „weiteren Kommissionsbediensteten“, in denen es hieß, sie seien „Ziel von staatlich geförderten Angreifern“ geworden und ihre Geräte seien möglicherweise kompromittiert²⁸². Am 11. April 2022 berichtete Reuters, dass Didier Reynders, Kommissar für Justiz, und mindestens vier weitere Kommissionsbedienstete im November 2021 Ziel von Pegasus-Software gewesen seien²⁸³.
144. Laut Kommission ist es „unmöglich, diese Indikatoren mit absoluter Gewissheit einem bestimmten Täter zuzuordnen“. Die Kommission ist der Auffassung, dass sie die

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/>

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/>

aktuellen Ergebnisse der Untersuchung nicht weiter ausführen kann, da sie damit „den Gegnern die Untersuchungsmethoden und -fähigkeiten der Kommission offenbaren und somit die Sicherheit der Institution ernsthaft gefährden würde“. Das gemeinsame übergeordnete Thema, mit dem sich die beiden bekannten angegriffenen Beamten der Kommission, Kommissar Reynders und ein Kabinettsmitglied von Kommissarin Věra Jourová²⁸⁴, beschäftigen, ist die Rechtsstaatlichkeit. Auf die Frage von PEGA nach einem möglichen Zusammenhang erklärte die Kommission, dass ihr „nicht genügend Informationen zur Verfügung stehen, um endgültige Schlussfolgerungen über einen Zusammenhang zwischen der Geolokalisierung und einem möglichen Versuch, Geräte über Pegasus zu infizieren, zu ziehen“²⁸⁵.

145. Im Rahmen ihrer Interaktion mit dem PEGA-Ausschuss erklärte die Kommission wiederholt, dass der Versuch, Kommissar Reynders' Gerät mit Pegasus-Software zu hacken, nicht erfolgreich gewesen sei, womit allem Anschein heruntergespielt wurde, wie schwerwiegend ein derartiger Angriff auf einen Kommissar ist. Ein Hacking-Versuch, ob erfolgreich oder nicht, auf die Kommission bzw. auf ein Mitglied der Kommission ist jedoch eine sehr ernst zu nehmende politische Tatsache, die Auswirkungen auf die Integrität der demokratischen Entscheidungsprozesse hat.

Cybersicherheitsmaßnahmen

146. Nach dem versuchten Hacken des Telefons von Kommissar Reynders und den Gefährdungsindikatoren für mehrere Geräte von Kommissionsbediensteten hat die Kommission im September 2021 eine mobile „Endpoint Detection and Response“-Lösung (EDR) für alle Diensttelefone eingeführt.

Angriffe auf früheren griechischen Kommissar und auf Ratsvertreter

147. Am 6. November veröffentlichte die griechische Zeitung „Documento“ eine umfangreiche Liste mit Personen, auf deren Geräten angeblich Spuren von Predator gefunden wurden, darunter Dimitris Avramopoulos, EU-Kommissar von 2014–2019 und Néa-Dimokratía-Politiker²⁸⁶. Es ist unklar, ob der Angriff erfolgte, als er Mitglied des Kollegiums war, und wer dahintersteckte, angesichts der langen Liste von angegriffenen Personen, darunter viele Politiker und Politikerinnen sowohl von Néa Dimokratía als auch von der Opposition ist die plausibelste Hypothese jedoch, dass die Anordnung aus dem Umfeld des Ministerpräsidenten kam.
148. Dieser Fall zeigt somit, dass (frühere) Kommissarinnen und Kommissare, einschließlich ihrer Kommunikation mit Kollegen, jederzeit aus innenpolitischen Gründen aus ihrem jeweiligen Mitgliedstaat angegriffen werden können. Darüber hinaus befinden sich auf der von „Documento“ veröffentlichten Liste mehrere Minister der aktuellen Regierung, darunter der Außen- und der Finanzminister. Diese Minister sind auch Mitglieder des Rates und entscheiden über die Außen- und Finanzpolitik der Union. Daher könnte ein einziges infiziertes Telefon auch dazu dienen, alle Sitzungen der Kommission und des Rates in Echtzeit abzuhören.

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

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

²⁸⁶ Documento, edition 6 November 2022.

II. Die Spyware-Industrie

149. Die Europäische Union ist ein attraktiver Ort für den Handel mit Überwachungstechnologien und -dienstleistungen, einschließlich Spyware-Tools. Zum einen gibt es die Regierungen der Mitgliedstaaten als potenzielle Kunden. Zum anderen dient die Wahrnehmung als „EU-reguliert“ als Qualitätsmerkmal, das auf dem Weltmarkt von Nutzen ist. Der EU-Binnenmarkt bietet Freizügigkeit und vorteilhafte nationale Steuerregelungen. Vorschriften in Bezug auf die Beschaffung können mit Hinweis auf die nationale Sicherheit umgangen werden, und die Regierungen können auf Vertreter oder Mittelsmänner zurückgreifen, sodass der Kauf von Spyware durch öffentliche Stellen sehr schwer festzustellen und zu beweisen ist. In der EU gelten strenge Ausfuhrvorschriften, die allerdings leicht umgangen werden können, da die Mitgliedstaaten sich durch eine bewusst laxen nationalen Umsetzung einen Wettbewerbsvorteil verschaffen wollen. Die Durchsetzung seitens der Europäischen Kommission ist schwach und oberflächlich. Tatsächlich verlegten mehrere Unternehmen immer wenn die Regelungen für Ausfuhrlicenzen in Israel verschärft wurden ihre Exportabteilungen nach Europa, insbesondere nach Zypern^{287 288}. Darüber hinaus haben mehrere Personen aus der Spyware-Industrie eine EU-Staatsbürgerschaft erlangt, um frei innerhalb der EU und aus der EU heraus agieren zu können.
150. In vielen Fällen scheint die Bezeichnung „Söldner-Spyware“ angebracht. Der Sektor verfügt über keine sehr hohen ethischen Standards und verkauft an die blutrünstigsten Diktaturen und an reiche nicht staatliche Akteure mit feindseligen Absichten. Die wahre Geschichte wird von der Liste der Spyware Opfer erzählt, nicht von den hohlen Menschenrechtsbekenntnissen in den Broschüren der Verkäufer. Nach den Enthüllungen des Pegasus-Projekts kündigte Celebrité 2021 an, man wolle den Verkauf an Russland stoppen, wenn sich herausstellen sollte, dass Spyware gegen Anti-Putin-Aktivisten eingesetzt wird. Im Oktober 2022 gibt es jedoch Anzeichen dafür, dass Celebrité noch immer von Putin genutzt wird²⁸⁹. Es handelt sich um einen lukrativen, boomenden und zwielichtigen Markt, der eine Menge Cowboys anzieht. Trotzdem schaffen sie es, ihre Produkte an demokratische Regierungen in den USA und in der EU zu verkaufen, was ihnen einen Anschein von Seriosität verleiht. Trotz der Beteuerungen, dass die Nutzung von Spyware vollkommen rechtmäßig und notwendig sei, sind die Regierungen auffallend zurückhaltend, wenn es darum geht zuzugeben, dass sie Spyware besitzen. Manchmal greifen sie für den Kauf von Spyware auf Vertreter, Mittelsmänner oder Makler zurück, um keine Spuren zu hinterlassen. Die größte jährliche Veranstaltung der Branche ist die Messe „ISS World“, auch bekannt als „The Wiretappers‘ Ball“. Die europäische Version findet jedes Jahr in Prag statt. Zwischen den Ausstellern bei der ISS World und Messen der Waffenindustrie gibt es erhebliche Überschneidungen.

Schwachstellen

151. Ohne Schwachstellen in der Software wäre es unmöglich, Spyware zu installieren und einzusetzen. Um die Verwendung von Spyware zu regulieren, müssen deshalb die

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

²⁸⁸ Haaretz. [Cyprus, Cyberspies and the Dark Side of Israeli Intel.](#)

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>

Aufdeckung, die Offenlegung und die Ausnutzung von Schwachstellen ebenfalls reguliert werden²⁹⁰. Trotz der Stärkung der Abwehr digitaler Systeme, die durch die NIS2-Richtlinie und das vorgeschlagene Cyberresilienzgesetz vorgeschrieben und gefördert wurde, ist es nahezu unmöglich, Systeme ohne Schwachstellen zu entwickeln.

Telekommunikationsnetze

152. Telekommunikationsanbieter spielen eine wichtige Rolle bei der legalen und illegalen Spionage. Wir leben in einem modernen Zeitalter mit KI, Big Data und Quantencomputern, aber gleichzeitig nutzen wir ein internationales Telekommunikationsprotokoll mit der Bezeichnung SS7, auf das wir in hohem Maße angewiesen sind. Dieses Protokoll wurde 1975 entwickelt und wird heute noch immer verwendet. Mit diesem System wird gesteuert, wie Anrufe geroutet und abgerechnet werden, und es ermöglicht fortschrittliche Anruf-Features und Kurznachrichtendienste (SMS)²⁹¹. Über das SS7-Netz ist es möglich, Anrufe und SMS abzufangen und Standorte zu identifizieren sowie ein Opfer mit Spyware wie Pegasus, Predator usw. zu infizieren²⁹².

NSO Group

153. Die Pegasus-Spyware wird von der NSO Group hergestellt. Die NSO Group wurde 2010 von Shalev Hulio, Omri Lavie und Niv Karmi gegründet, um Technologien zu entwickeln, die lizenzierten Regierungsagenturen und Strafverfolgungsbehörden dabei helfen, Terrorismus und Kriminalität aufzudecken und zu verhindern²⁹³. Die Pegasus-Spyware ist das bekannteste Produkt der NSO Group. Sie wurde 2011 auf den Weltmarkt gebracht^{294 295}.

Unternehmensstruktur, Transparenz und Sorgfaltspflicht

154. Am 25. Januar 2010 gründete die NSO Group ihr erstes Unternehmen in Israel. Dieses Unternehmen wurde unter dem Namen NSO Group Technologies Limited registriert. NSO Group ist sowohl der Name des ersten registrierten Unternehmens als auch der Überbegriff für verschiedene in anderen Ländern gegründete Unternehmen. Das zuerst gegründete Unternehmen ist Eigentümer der Marke „NSO Group“²⁹⁶.

Ausfuhrkontrollen

155. Da die Pegasus-Spyware als Technologie mit doppeltem Verwendungszweck gilt, wird dafür eine Ausfuhrgenehmigung benötigt. Die Unternehmen der NSO Group erhalten

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.

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.

ihre Ausfuhrgenehmigungen in Israel, Bulgarien und Zypern²⁹⁷. Die meisten dieser Genehmigungen werden von den israelischen Behörden erteilt²⁹⁸. Israel ist nicht Teil des Wassenaar-Abkommens, erklärt aber, einige Elemente daraus in sein nationales Gesetz über die Kontrolle von Ausfuhren im Verteidigungsbereich (5766) von 2007 übernommen zu haben²⁹⁹. Die Agentur für die Kontrolle von Ausfuhren im Verteidigungsbereich (DECA) des Verteidigungsministeriums ist für die Erteilung von Vermarktungs- und Ausfuhrgenehmigungen zuständig³⁰⁰. Nach den Enthüllungen des Pegasus-Projekts und dem Blacklisting von NSO wurde die Liste der in Betracht kommenden Länder von 102 auf 37 gekürzt, die alle eine Endverbleibserklärung unterzeichnen müssen³⁰¹. In den Verfahren zur Erfüllung der Sorgfaltspflicht geht Israel automatisch davon aus, dass alle EU-Mitgliedstaaten die EU-Normen erfüllen, und führt deshalb keine zusätzlichen Überprüfungen einzelner Länder durch. Die Entscheidung, die Verträge mit zwei EU-Mitgliedstaaten zu kündigen, scheint jedoch darauf hinzudeuten, dass die EU im Hinblick auf die Sorgfaltspflicht nicht mehr als eine zentrale Stelle betrachtet wird.

Gerichtsverfahren, Blacklisting und Investorenkonflikte aufgrund unethischen Verhaltens

156. Im Juli 2021 begann sich ein Konflikt zwischen den drei Gründern von Novalpina Capital auf die Geschäftstätigkeit der NSO Group auszuwirken, was schließlich dazu führte, dass die Investoren entschieden, der Private-Equity-Gesellschaft die Kontrolle zu entziehen³⁰². Am 27. August 2021 übernahm das US-Beratungsunternehmen Berkeley Research Group (BRG) den Private-Equity-Fonds und leitete kritische Untersuchungen in Bezug auf die Gesetzmäßigkeit der Aktivitäten der NSO Group und ihre Erfüllung der US-Blacklisting-Vorschriften ein. Die Untersuchungen von BRG vom Mai 2022 wurden vom Führungsteam der NSO Group behindert³⁰³. Ein leitender BRG-Mitarbeiter erklärte, die Zusammenarbeit mit der NSO Group sei aufgrund des Drucks der NSO Group, weiter in Länder mit umstrittener Menschenrechtslage zu verkaufen, „so gut wie nicht vorhanden“³⁰⁴. Am 25. April 2022 reichten zwei der ehemaligen Komplementäre von Novalpina bei einem Luxemburger Gericht eine Klage gegen BRG ein, in der sie die Wiedereinsetzung von Novalpina Capital als Komplementär und die Rücknahme aller von BRG getroffenen Entscheidungen forderten³⁰⁵. Das Luxemburger Gericht hat diese Forderungen abgewiesen, und BRG bleibt für den Fonds, der die NSO Group kontrolliert, verantwortlich³⁰⁶.

Black Cube

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. Novalpina 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.

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.

157. Bei der Firma Black Cube handelt es sich um einen privaten israelischen Nachrichtendienst, für den ehemalige Mitarbeiter des Mossad, des israelischen Militärs und der israelischen Geheimdienste tätig sind³⁰⁷. Auf seiner eigenen Website bezeichnet sich das Unternehmen als kreativen Nachrichtendienst, der maßgeschneiderte Lösungen für komplexe geschäftliche und rechtliche Herausforderungen findet³⁰⁸. Black Cube war in eine Reihe von öffentlichen Kontroversen um Hackerangriffe verwickelt, unter anderem in den USA und Rumänien³⁰⁹. Insbesondere räumte die Black-Cube-Führung ein, die frühere leitende Staatsanwältin der rumänischen nationalen Antikorruptionsdirektion, Laura Kövesi, ausspioniert zu haben³¹⁰. Laura Kövesi ist derzeit die erste Europäische Generalstaatsanwältin und leitet die Europäische Staatsanwaltschaft (EUSTa). Angeblich war der frühere rumänische Geheimagent Daniel Dragomir derjenige, der Black Cube mit diesem Job beauftragt hat³¹¹.

Intellexa Alliance

158. Intellexa wurde 2019 von Tal Dilian in Zypern gegründet. Dilian bekleidete verschiedene Führungspositionen bei den israelischen Streitkräften, bevor er eine Laufbahn als „Geheimdienstexperte, Community Builder und Serienunternehmer“ begann³¹². Intellexa Alliance wird auf seiner Website als ein in der EU ansässiges und von der EU reguliertes Unternehmen mit dem Zweck der Entwicklung und Integration von Technologien zur Stärkung der Geheimdienste beschrieben. Zu den Überwachungsanbietern, die Teil des Marketing-Labels von Intellexa Alliance sind, gehören:

- Cytrox, WiSpear (später umbenannt in Passitora Ltd)
- Nexa Technologies (unter der Leitung früherer Amesys-Manager)
- Poltrex

WiSpear und Cytrox

159. Tal Dilian gründete 2013 ein in Zypern registriertes Unternehmen mit dem Namen Aveledo Ltd., das später in WS WiSpear Systems Ltd. und danach in Passitora Ltd. umbenannt wurde³¹³. WiSpear hat seinen Sitz in Limassol, Zypern, und verkauft hauptsächlich Ausrüstung und Software für die Lokalisierung und Verfolgung von Personen über ihre Mobiltelefone. In einem Interview mit dem Forbes-Magazin erklärte Dilian die Fähigkeiten der WiSpear-Software, indem er seinen schwarzen Van im Wert von 9 Millionen Dollar zeigte, der in der Lage ist, Geräte in einem Umkreis von 500 Metern zu hacken. Darüber hinaus verfügt WiSpear über Ausrüstung, mit der Daten

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.](#)

³¹² Tal Dilian. [About.](#)

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

aus WLAN-Netzen abgefangen werden können³¹⁴. Nach dem Bekanntwerden der Skandale im Zusammenhang mit diesen Produkten wurden die Hauptgeschäftstätigkeiten von Intellexa von Zypern nach Griechenland verlegt.

Amesys und Nexa Technologies

160. Amesys und Nexa Technologies gehören ebenfalls zu Intellexa Alliance und sorgen ihrerseits, wie im Kapitel über Frankreich beschrieben, für Kontroversen.

Poltrex

161. Poltrex wurde im Oktober gegründet, mit Intellexa Ltd., registriert auf den Britischen Jungferninseln, als einzigem Aktionär der Gesellschaft Shahak Avni aus Israel, Gründer der zypriotischen NCIS Intelligence Services Ltd.³¹⁵ und Geschäftspartner von Tal Dilian, wurde im September 2019 als Geschäftsführer von Poltrex eingetragen. Im Oktober 2019 wurden Avni und Dilian Co-Geschäftsführer und der Firmenname wurde von Poltrex in Alchemycorp Ltd. geändert. Ungeachtet der Umbenennung befand sich der Firmensitz weiterhin im Novel Tower, genau wie die Geschäftsräume von WiSpear³¹⁶.

Candiru

162. Candiru ist ein weiteres in Israel registriertes Unternehmen, das Spyware-Produkte herstellt. Es wurde 2014 von Ya'acov Weitzman und Eran Shorer gegründet. Die beiden Gründer haben eine Vergangenheit in der Einheit 8200 des israelischen militärischen Geheimdienstes und beide waren früher bei der NSO Group beschäftigt³¹⁷. Isaac Zack, ein früherer Investor der NSO Group, wurde Hauptaktionär von Candiru. Das Unternehmen verkauft Spyware, um Computer und Server zu hacken³¹⁸. Offengelegte Informationen zu einem Projektvorschlag zeigen, dass Candiru seine Ausrüstung nach der Anzahl gleichzeitiger Infektionen verkauft, also der Anzahl der Ziele, die mit der Spyware zu einem bestimmten Zeitpunkt angegriffen werden können. Beispielsweise erhalten Kunden für 16 Millionen Dollar eine unbegrenzte Anzahl von Spyware-Versuchen, können aber nur zehn Zielgeräte gleichzeitig angreifen. 15 zusätzliche Geräte sind für weitere 1,5 Millionen Dollar erhältlich³¹⁹.

Tykelab und RCS Lab

163. Im August 2022 berichtete Lighthouse Report, dass Tykelab, ein Unternehmen mit Sitz in Rom, das zu RCS Lab gehört, Dutzende von Telefonnetzen, oft auf Inseln im Südpazifik, genutzt hat, um Zehntausende von geheimen „Tracking-Paketen“ in die ganze Welt zu senden, wobei es Menschen in Ländern wie Italien selbst, Griechenland, Mazedonien, Portugal, Libyen, Costa Rica, Nicaragua, Pakistan, Malaysia, Irak und

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.](#)

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.](#)

Mali ins Visier nahm. Tykelab nutzt Schwachstellen in globalen Telefonnetzen aus, die es Dritten ermöglichen, den Standort von Telefonnutzern einzusehen und möglicherweise deren Anrufe abzuhören, ohne dass auf den Geräten irgendwelche Hinweise auf eine Sicherheitsverletzung hinterlassen werden³²⁰. In nur zwei Tagen im Juni 2022 sondierte das Unternehmen Netze in fast allen Ländern der Welt³²¹. Laut seiner Webseite vereint Tykelab zwanzig Jahre Erfahrung in der Gestaltung, Implementierung und Wartung von Kernnetz-Telekommunikationslösungen mit umfangreichem Fachwissen in der Bereitstellung von Managed Services, kundenbasierter Systemintegration und der Entwicklung mobiler Apps³²².

Die Spähsoftware Hermit

164. RCS Lab hat Hermit entwickelt, eine Spähsoftware, mit der das Mikrofon des Telefons aus der Ferne aktiviert werden kann und mit der Anrufe aufgezeichnet und auf Nachrichten, Anrufprotokolle, Kontakte und Fotos zugegriffen werden kann³²³. Im Juni 2022 deckte die Threat Analysis Group von Google auf, dass von der Regierung unterstützte Akteure, die die Spähsoftware von RCS Lab verwenden, mit den Internetdiensteanbietern der Zielpersonen zusammenarbeiten, um die mobile Datenverbindung der Zielpersonen zu deaktivieren. Nach der Deaktivierung schickte der Angreifer einen schädlichen Link per SMS, in der die Zielperson aufgefordert wird, eine Anwendung zu installieren, um ihre Datenverbindung wiederherzustellen. Google geht davon aus, dass dies der Grund ist, warum sich die meisten Anwendungen als Anwendungen von Mobilfunkanbietern getarnt haben. Wenn eine Beteiligung des Internetanbieters nicht möglich ist, werden die Anwendungen als Nachrichten-Anwendungen getarnt. Die Opfer, auf die die Spähsoftware von RCS Lab abzielte, befanden sich in Italien und Kasachstan³²⁴, und sie wurde auch in Rumänien gefunden³²⁵.

DSIRF – Decision Supporting Information Research and Forensic

165. Ein Unternehmen, gegen das das österreichische Justizministerium kürzlich ein Strafverfahren eingeleitet hat, ist die DSIRF GmbH³²⁶, ein 2016 gegründetes österreichisches Unternehmen mit Sitz in Wien und einem Mutterunternehmen in Liechtenstein, das nach eigenen Angaben „maßgeschneiderte Dienstleistungen in den Bereichen Informationsrecherche, Forensik sowie datengestützte Aufklärung für multinationale Unternehmen in den Bereichen Technologie, Einzelhandel, Energie und Finanzen“ anbietet³²⁷. DSIRF verkauft offensichtlich an nichtstaatliche Akteure.

FinFisher

166. Ein wichtiger Punkt in diesem Bericht ist die strafrechtliche Untersuchung und der Konkurs von FinFisher, einem ehemaligen Spähsoftware-Unternehmen mit Sitz in

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

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

³²² <http://www.tykelab.it/wp/about/>

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/>

München, Deutschland. FinFisher ist ein im Jahr 2008 gegründetes Unternehmensnetz, das ursprünglich starke Verbindungen zum britischen Unternehmensnetz unter der Marke „Gamma“ hatte. FinFisher warb für seine Spähsoftware als „komplettes IT-Eingriffs-Portfolio“, wobei seine Software in Dutzenden von Ländern auf der ganzen Welt³²⁸ eingesetzt wurde, darunter 11 EU-Mitgliedstaaten³²⁹ und 13 „nicht-freie“ Länder³³⁰.

III. Kapazität der Europäischen Union für Reaktionen

167. Die Regierungen haben EU-Bürger mit leistungsfähiger Spähsoftware ins Visier genommen. Dies stellt eine Bedrohung für die Demokratie und die Rechte der einzelnen Bürger dar. Die EU verfügt über Befugnisse, auf diese Bedrohungen zu reagieren, wenn auch nur über sehr wenige. Wenn sich die Mitgliedstaaten jedoch auf die „nationale Sicherheit“ berufen, ist die EU im Grunde aus dem Spiel. Die Mitgliedstaaten definieren die nationale Sicherheit einseitig und können die Tür jederzeit schließen. Neben diesen rechtlichen Einschränkungen gibt es auch politische Gründe, die auf eine Passivität der EU hinauslaufen. Die Kommission ist als Hüterin der EU-Verträge zurückhaltend geworden, wenn es um die Durchsetzung von EU-Recht geht³³¹. Dies liegt nicht an rechtlichen Einschränkungen, sondern vielmehr an einer politischen Entscheidung. Die Kommission neigt dazu, ihre Befugnisse so eng wie möglich auszulegen. Angesichts schwerwiegender Verstöße gegen die Rechtsstaatlichkeit und die Grundrechte wird diese Haltung sehr problematisch. Die Subsidiarität und die Achtung der ausschließlichen nationalen Zuständigkeiten drohen in Straßlosigkeit umzuschlagen. Im Folgenden werden die Befugnisse untersucht, über die die Organe der EU verfügen. Das Parlament, die Kommission und der Rat haben die Befugnis und die Pflicht, Gesetze zu erlassen und Regelungen vorzunehmen sowie diese durchzusetzen, und sie müssen dies mit Nachdruck und Ehrgeiz tun und dabei die Verteidigung unserer Demokratie über kurzfristige politische Überlegungen stellen.

Europäische Kommission

168. Die Kommission hat sich in ihrer Reaktion auf den Spähsoftware-Skandal bisher darauf beschränkt, die Regierungen Polens, Ungarns, Spaniens und Griechenlands schriftlich um Klarstellung zu bitten. Es scheint jedoch, dass dieser zaghafte Ermahnung der Kommission keine weiteren Maßnahmen folgen werden. Es stimmt, dass die Kommission streng genommen keine Befugnisse hat, im Bereich der nationalen Sicherheit tätig zu werden. Wie die Kommission in diesen Schreiben jedoch selbst betont, sollte der Begriff „nationale Sicherheit“ nicht als unbegrenzte Ausnahmeregelung von den europäischen Gesetzen und Verträgen interpretiert werden und zu einem Bereich der Gesetzlosigkeit werden.
169. Anders als in den USA hat die Kommission bisher weder eine Analyse der Situation noch eine Bewertung der auf dem europäischen Markt tätigen Unternehmen

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.

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

vorgenommen. Es gibt keine offensichtlichen rechtlichen Einwände gegen die Durchführung einer solchen Analyse.

170. Die EU verfügt über mehrere Gesetze, die als Regulierungsinstrumente in Bezug auf Spähsoftware dienen können. Neben Gesetzen zum Schutz der Rechte der Bürger, wie den Gesetzen zum Datenschutz und zum Schutz der Privatsphäre in der Kommunikation (DSGVO, Datenschutzrichtlinie für elektronische Kommunikation), gibt es Gesetze zur Ausfuhr (Verordnung über Güter mit doppeltem Verwendungszweck) und zur Vergabe öffentlicher Aufträge. Die Durchsetzung durch die Kommission ist jedoch schwach. Sie beschränkt sich in der Regel darauf, zu überprüfen, ob ein Mitgliedstaat die EU-Gesetze korrekt in nationale Rechtsvorschriften umgesetzt hat. Dies sagt jedoch sehr wenig über die tatsächliche Situation vor Ort aus. So scheint der Bericht der Kommission über die Durchführung³³² der Verordnung über Güter mit doppeltem Verwendungszweck zu dem Schluss zu kommen, dass die Umsetzung gut vorankommt, während es zahlreiche Belege dafür gibt, dass sie in der Praxis schwach und lückenhaft ist und in einigen Ländern sogar absichtlich so erfolgt. Trotz der in der Verordnung über Güter mit doppeltem Verwendungszweck festgelegten Regeln scheint Zypern ein attraktives Exportzentrum für Spähsoftware-Anbieter geworden zu sein. Ohne eine ordnungsgemäße und sinnvolle Durchsetzung sind die EU-Gesetze nur Papiertiger, die viel Raum für die illegale Nutzung von Spähsoftware schaffen.

Europäisches Parlament

171. Das Europäische Parlament hat den Untersuchungsausschuss PEGA eingesetzt, der im Rahmen seiner Befugnisse und seines Mandats gewissenhaft und effizient arbeitet. Er ist jedoch nicht befugt, Zeugen vorzuladen oder unter Eid zu vernehmen, und er hat keinen Zugang zu Verschlusssachen. Ihm fehlen die vollen Ermittlungsbefugnisse, über die die meisten nationalen Parlamente verfügen. Darüber hinaus ist der Einfluss der nationalen Regierungen bei den Beratungen des PEGA-Ausschusses häufig präsent, was gelegentlich ein Hindernis für gründliche, völlig unabhängige und objektive Untersuchungen darstellt. Es ist ziemlich zynisch, dass das Europäische Parlament nicht über die vollen Ermittlungsbefugnisse verfügt, wenn einige seiner eigenen Mitglieder Opfer illegaler Überwachung sind.

Europäischer Rat und Rat der Europäischen Union

172. Obwohl die nationalen Regierungen behaupten, der Spähsoftware-Skandal sei eine rein nationale Angelegenheit, wurde er tatsächlich im Rat der Europäischen Union erörtert, und die nationalen Regierungen haben beschlossen, den Fragebogen des Europäischen Parlaments gemeinsam zu beantworten³³³. Damit haben sie voll und ganz anerkannt, dass es sich in der Tat um eine Angelegenheit des Rates handelt. Verantwortung ist jedoch kein Menü, aus dem man sich etwas aussuchen kann: Man kann sich nicht nur selektiv mit Verfahrensfragen, aber nicht mit dem Inhalt befassen.
173. Bislang hat der Europäische Rat weder öffentlich noch substantiell auf den Skandal reagiert. Einige seiner Mitglieder haben ein Interesse an der Angelegenheit, da sie möglicherweise selbst in die illegalen Hacks verwickelt sind, oder sie möchten einfach,

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.

dass die EU in diesem Gebiet schwach und machtlos bleibt. Die Omertà und die mangelnde Kooperation des Rates verheißen nichts Gutes für künftige Regulierungsinitiativen. Der Rat ist ein Gesetzgeber, aber er könnte durchaus zögern, seine eigenen Mitglieder zu regulieren.

174. Selbst wenn ein rechtswidriges oder kriminelles Verhalten nachgewiesen werden sollte, können Mitglieder nationaler Regierungen nicht angeklagt oder zum Rücktritt von ihren EU-Posten gezwungen werden. Dies bedeutet, dass Personen, die sich solcher Handlungen schuldig gemacht haben, weiterhin ungestraft in Einrichtungen der EU sitzen und Entscheidungen treffen können, die alle europäischen Bürger betreffen.

Europol

175. Europol wurde aufgefordert, die zyprische Polizei und einen akademischen Sachverständigen bei der Durchführung einer dreistufigen forensischen Untersuchung der Geräte zu unterstützen, die 2019 in dem schwarzen Lieferwagen von Tal Dilian gefunden wurden. Während der PEGA-Anhörung am 30. August 2022 erwähnte Europol dies nicht, obwohl die Mitglieder Fragen zur Rolle von Europol bei der Untersuchung von Spähsoftware in der EU stellten. Seitdem wurde es nicht erwähnt.
176. Europol verfügt über keine autonomen operativen Befugnisse und kann nicht ohne die Zustimmung und die Zusammenarbeit des betroffenen Mitgliedstaats bzw. der betroffenen Mitgliedstaaten handeln. Dies stellt ein Problem dar, wenn es eindeutige Beweise für kriminelle Handlungen – wie Cyberkriminalität, Korruption und Erpressung – gibt, die nationalen Behörden aber nicht ermitteln. Dieses Problem wird noch verschärft, wenn die Behörden der Mitgliedstaaten selbst in die Straftaten verwickelt sind.
177. Allerdings hat Europol vor kurzem neue Befugnisse erhalten, die es ihm erlauben, proaktiv eine Ermittlung vorzuschlagen, auch wenn es sich um eine Straftat handelt, die nur in einem Mitgliedstaat begangen wurde³³⁴, aber bisher zögerte es, von diesen Befugnissen Gebrauch zu machen. Europol möchte die guten Beziehungen zu den Regierungen pflegen, da es befürchtet, dass eine solche Initiative zum Scheitern der Zusammenarbeit in anderen Bereichen führen würde.
178. Am 28. September 2022 richtete PEGA ein Schreiben an Europol³³⁵, in dem er Europol nachdrücklich auffordert, von seinen neuen Befugnissen gemäß Artikel 6 der Europol-Verordnung³³⁶ Gebrauch zu machen. In einem Antwortschreiben vom 13. Oktober 2022³³⁷ teilte Europol mit, dass es sich *mit fünf Mitgliedstaaten in Verbindung gesetzt hat, um festzustellen, ob auf nationaler Ebene relevante Informationen für Europol zur Verfügung stehen und ob eine strafrechtliche Ermittlung (oder stattdessen eine andere Untersuchung nach den geltenden Bestimmungen des nationalen Rechts) läuft oder*

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.

geplant ist. Einer der fünf Mitgliedstaaten hat Europol inzwischen bestätigt, dass strafrechtliche Ermittlungen unter der Aufsicht der zuständigen Justizbehörden eingeleitet wurden, was auch von Eurojust überprüft wurde. Es ist weder bekannt, auf welche Länder sich das Schreiben bezieht, noch ob die zuvor erwähnte strafrechtliche Untersuchung durch einen Mitgliedstaat den Missbrauch von Spähsoftware durch die Regierungen von EU-Mitgliedstaaten oder durch Drittländer betrifft.

179. Die EU erweist sich als ziemlich machtlos gegenüber möglichen kriminellen Handlungen der nationalen Behörden, selbst wenn diese die EU betreffen.
180. Paradoxerweise untersuchen die USA im Gegensatz zu Europol aktiv den Einsatz von Spähsoftware in der EU. Am 5. November 2022 wurde berichtet, dass das FBI Athen besuchte, um zu untersuchen, „wie weit sich die illegale Überwachung ausgebreitet hat und wer mit ihr gehandelt hat.“³³⁸

Europäische Justiz

181. Der Gerichtshof der Europäischen Union (EuGH) und der Europäische Gerichtshof für Menschenrechte (EGMR) spielen eine wichtige Rolle bei der Verteidigung von Demokratie, Rechtsstaatlichkeit und Grundrechten. Sie können jedoch nur auf eine Beschwerde oder eine vorgerichtliche Frage hin tätig werden. Die Verfahren sind sehr langwierig und bieten in Einzelfällen kaum konkrete Abhilfe. Im Laufe der Jahre haben die Gerichte eine umfangreiche einschlägige Rechtsprechung geschaffen und beispielsweise Standards für die Überwachung festgelegt. Die Gerichte verfügen jedoch nicht über die Mittel, um für die Durchsetzung ihrer Urteile zu sorgen. Bislang wurde dem EGMR eine Beschwerde über den unrechtmäßigen Einsatz von Spähsoftware vorgelegt³³⁹. Der Weg zu den Gerichten in Straßburg oder Luxemburg ist jedoch oft lang, kostspielig und umständlich, da zunächst alle Möglichkeiten der nationalen Gerichtsverfahren ausgeschöpft werden müssen. Dies gilt insbesondere dann, wenn nationale Staatsanwälte oder Richter einen Fall nicht annehmen oder ablehnen, denn die Hürde für die Zulässigkeitsprüfung ist hoch.

Andere EU-Einrichtungen

182. Der Europäische Datenschutzausschuss, der Europäische Datenschutzbeauftragte, die EU-Bürgerbeauftragte, der Europäische Rechnungshof und Eurojust verfügen nur über wenige Befugnisse, um im Falle der unrechtmäßigen Verwendung von oder des Handels mit Spähsoftware durch die Regierungen von Mitgliedstaaten Untersuchungen vorzunehmen oder einzugreifen. Einige ihrer Mitglieder könnten in der Tat in die Skandale in ihrem Herkunftsmitgliedstaat und in deren Vertuschung verwickelt sein. Darüber hinaus kann dies Auswirkungen auf die Funktionsweise und die Integrität dieser Einrichtungen der EU haben. Die Europäische Staatsanwaltschaft könnte möglicherweise eingreifen, wenn EU-Gelder in irgendeiner Weise involviert sind.

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

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

BEGRÜNDUNG

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, Luxembourg, 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 Luxembourg. 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.