Europees Parlement
2019-2024

Zittingsdocument

A9-0189/2023

22.5.2023

VERSLAG

over het onderzoek naar vermeende inbreuken op en gevallen van wanbeheer bij het toepassen van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance
(2022/2077(INI))

Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken

Rapporteur: Sophie in ’t Veld

INHOUD

Blz.

ONTWERP VAN DE RESULTATEN

over het onderzoek naar vermeende inbreuken op en gevallen van wanbeheer bij het toepassen van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance
(2022/2077(INI))

Het Europees Parlement,

– gezien artikel 226 van het Verdrag betreffende de werking van de Europese Unie (VWEU),

– gezien zijn besluit van 10 maart 2022 tot instelling van een enquêtecommissie om het gebruik van Pegasus- en soortgelijke spyware voor surveillance te onderzoeken, en houdende de vaststelling van het onderwerp van de enquête, alsook van de bevoegdheden, het aantal leden en de duur van het mandaat van de commissie,

– gezien de artikelen 54 en 208 van zijn Reglement,

– gezien het verslag van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken (A9-0189/2023),

Algemene inleiding

1. In juli 2021 publiceerde een collectief van onderzoeksjournalisten, ngo's en onderzoekers – het Pegasusproject – een verslag op basis van een in hun bezit zijnde lijst van ongeveer 50 000 telefoonnummers die mogelijk met Pegasus-spyware zijn benaderd. Dergelijke spyware is op grote schaal gebruikt door zowel autoritaire als democratische regeringen over de hele wereld, zowel met als zonder gerechtelijk toezicht, om journalisten, advocaten, rechters, activisten, politici en staatsambtenaren te bespioneren. Ook in de Europese Unie zijn mensen het doelwit geweest van spyware: sommige door actoren buiten de EU, en andere door actoren binnen de EU, waaronder regeringsinstanties. De meeste, zo niet alle, regeringen van de lidstaten hebben spyware gekocht, in principe voor wetshandhavings- en veiligheidsdoeleinden. Er zijn echter voldoende aanwijzingen dat spyware in verschillende lidstaten is misbruikt voor zuiver politieke doeleinden, waarbij critici en tegenstanders van de regeringspartijen het doelwit waren, of in verband met corruptie. Onderzoeksresultaten brengen Pegasus en andere surveillancesoftware in verband met diverse mensenrechtenschendingen door regeringen, waaronder monitoring, chantage, lastercampagnes, intimidatie en pesterijen. Dit geeft aanleiding tot bezorgdheid op verschillende niveaus van de EU-rechtsorde met betrekking tot gegevensbescherming en privacy, vrijheid van meningsuiting, persvrijheid, vrijheid van vereniging, verhaalmechanismen, rechtsmiddelen en een eerlijk proces, en democratische processen en instellingen. Hoewel het gebruik van spyware de noodzakelijkheids- en evenredigheidstoets kan doorstaan in geval van ernstige bedreigingen van de nationale veiligheid, is het misbruik van spyware voor politieke doeleinden uiterst verontrustend en geeft het aanleiding tot zeer ernstige bezorgdheid over de procedurele en materiële rechtmatigheid van surveillancepraktijken en het niveau van bescherming dat door het Europese en nationale recht wordt geboden.

Dergelijk misbruik van spyware ondermijnt rechtstreeks de grondrechten en de democratie, de kernwaarden waarop de EU is gegrondvest. Uit latere onderzoeksverslagen in de media en andere bronnen is gebleken dat spyware uit EU-landen wordt uitgevoerd naar derde landen met ondemocratische regimes en een hoog risico op mensenrechtenschendingen, wat een flagrante schending van de EU-uitvoerregels inhoudt. De spyware-industrie is stevig gevestigd in de EU en profiteert van zeer gunstige voorwaarden voor bedrijven.

2. In reactie op dit groeiende schandaal heeft het Europees Parlement op 10 maart 2022 besloten om overeenkomstig artikel 226 VWEU een enquêtecommissie in te stellen om vermeende inbreuken op, of wanbeheer bij de toepassing van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken ("PEGA"). Terwijl een overtreding het bestaan inhoudt van onwettig gedrag, in de zin van handelingen of nalatigheden die in strijd zijn met de wet, van de instellingen of organen van de EU of van de autoriteiten van de lidstaten bij de uitvoering en handhaving van de EU-wetgeving, betekent wanbeheer slechte of ontbrekende administratieve handelingen, waarvan bijvoorbeeld sprake is indien de beginselen van goed beheer niet in acht worden genomen. Voorbeelden van wanbeheer omvatten onregelmatigheden en nalatigheden, machtsmisbruik, onredelijkheid, ondeugdelijk functioneren of incompetentie, discriminatie, maar ook vermijdbare vertragingen, weigering om informatie te verstrekken, nalatigheid en andere tekortkomingen die gebrekkige toepassing van het Unierecht inhouden.

3. In het kader van dit onderzoek heeft PEGA een brede benadering gehanteerd van wat spyware is, namelijk spyware voor surveillance die op mobiele apparaten wordt geïnstalleerd door misbruik te maken van IT-kwetsbaarheden. Tijdens het onderzoek is ook gebruikgemaakt van de definitie "producten voor cybersurveillance" van de verordening inzake producten voor tweeërlei gebruik: in deze definitie worden dergelijke producten omschreven als "producten voor tweeërlei gebruik die speciaal zijn ontworpen om het heimelijk surveilleren van natuurlijke personen mogelijk te maken door gegevens uit informatie- en telecommunicatiesystemen te monitoren, te extraheren, te verzamelen of te analyseren". In september 2022 stelde de Commissie een definitie van spyware voor in haar voorstel voor een verordening mediavrijheid, en beschreef zij spyware als "een product met digitale elementen dat speciaal is ontworpen om te profiteren van kwetsbaarheden in andere producten met digitale elementen, en dat de heimelijke surveillance van natuurlijke of rechtspersonen mogelijk maakt door het monitoren, extraheren, verzamelen of analyseren van gegevens van dergelijke producten of van de natuurlijke of rechtspersonen die dergelijke producten gebruiken, met name door het heimelijk opnemen van gesprekken of het anderszins gebruiken van de microfoon van een eindgebruikersapparaat, het filmen van natuurlijke personen, machines of hun omgeving, het kopiëren van berichten, het fotograferen, het volgen van surfactiviteiten, het traceren van de geolocatie, het verzamelen van andere sensorgegevens of het traceren van activiteiten op meerdere eindgebruikersapparaten, zonder dat de betrokken natuurlijke of rechtspersoon daarvan op specifieke wijze in kennis is gesteld en daarvoor zijn uitdrukkelijke specifieke toestemming heeft gegeven".

4. Op 19 april 2022 begon PEGA haar werkzaamheden door informatie te verzamelen via openbare zittingen, missies, raadpleging van deskundigen, verzoeken om gegevens,

bewijs, en onderzoek.

5. Tijdens verschillende openbare zittingen werd in het onderzoek de werking van spyware onderzocht. Spyware is een soort malware die de activiteiten van een gebruiker bespioneert zonder diens medeweten of toestemming. Deze spionageactiviteiten kunnen bestaan uit keystroke logging, monitoring van activiteiten, gegevensverzameling en andere vormen van gegevensdiefstal. Spyware wordt meestal verspreid als een Trojaans paard of door misbruik te maken van kwetsbaarheden in de software[1]. Spyware kan op afstand worden geïnstalleerd op de mobiele telefoons van vooraf bepaalde personen, zelfs over de grenzen heen. In sommige gevallen worden telecomnetwerken gebruikt voor de overdracht van de spyware naar het doelapparaat. Zodra de spyware het systeem geïnfiltreerd heeft, schakelt hij de beschermingsmechanismen en beveiligingsupdates uit. Het geïnfecteerde apparaat stuurt vervolgens de verzamelde gegevens van het apparaat door en stelt exploitanten in staat realtime te surveilleren door inkomende tekstberichten te lezen, gesprekken en locaties te volgen en via de microfoon en camera van het apparaat audio en video op te nemen.

6. In tegenstelling tot conventionele afluisterapparatuur, die alleen de realtime monitoring van communicatie mogelijk maakt, biedt spyware volledige en retroactieve toegang tot oudere bestanden en berichten, wachtwoorden en metagegevens over eerdere communicatie. Bijgevolg biedt een rechterlijke beslissing over een begindatum en duur voor een surveillanceoperatie geen doeltreffende waarborgen wanneer spyware volledige en retroactieve toegang tot gegevens biedt. Ook is het technisch mogelijk zich uit te geven voor het doelwit door toegang tot hun digitale inloggegevens en identiteit te verkrijgen. Het is uiterst moeilijk voor het doelwit om te ontdekken of er een inbraak met spyware heeft plaatsgevonden. Spyware laat weinig tot geen sporen achter op het toestel van het doelwit, en zelfs als de software wordt ontdekt, is het zeer moeilijk te achterhalen wie achter de aanval zit.

7. PEGA heeft weinig tot geen antwoorden gekregen van de nationale autoriteiten over de aankoop en het gebruik van spyware in hun lidstaten, noch over de budgettaire aspecten. Verkopers en landen die uitvoervergunningen afgeven (meestal Israël) delen geen informatie over hun klanten. Veel autoriteiten van de lidstaten hebben PEGA geen nuttige informatie verstrekt over de juridische kaders voor het gebruik van spyware of over het gebruik van spyware in hun lidstaten, naast hetgeen reeds publiekelijk bekend was, voornamelijk vanwege nationale wettelijke voorschriften inzake geheimhouding en vertrouwelijkheid.

8. Sommige lidstaten hebben spyware gebruikt en weigerden hier commentaar op te geven door zich te beroepen op de nationale veiligheid, die volgens artikel 4, lid 2, van het Verdrag betreffende de Europese Unie (VEU) “uitsluitend de verantwoordelijkheid van elke lidstaat” blijft. Volgens de rechtspraak van het Hof van Justitie van de Europese Unie (HvJ-EU) en het Europees Hof voor de rechten van de mens (EHRM) moeten nationale veiligheidsoverwegingen echter worden verzoend met de grondrechten en democratische normen die sterk in het EU-recht zijn verankerd. Hoewel het aan de lidstaten is om hun wezenlijke nationale veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te

[1] https://www.enisa.europa.eu/topics/incident-response/glossary/malware

verzekeren, heeft het HvJ-EU verklaard dat “het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, niet ertoe [kan] leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen[2]”, en heeft zij de criteria verduidelijkt die de lidstaten moeten volgen bij het bepalen van zaken die onder de nationale veiligheid vallen. Verschillende lidstaten hebben beweerd dat het gebruik van spyware onder de nationale veiligheid valt en dat dit de toepasselijkheid van het EU-recht uitsluit. Wanneer de lidstaten echter alleen maar verwijzen naar de nationale veiligheid als zodanig, kan de beperking van de grondrechten niet worden gerechtvaardigd als vallend onder de nationale veiligheid. Het EU-recht moet van toepassing zijn, met alle waarborgen die het biedt. Er is voldoende bewijs van misbruik van spyware om redenen die niets te maken hebben met nationale veiligheid. De lidstaten zouden niet aan hun verantwoordelijkheid voor dergelijke ernstige misbruiken van spyware mogen ontsnappen met een loutere verwijzing naar de nationale veiligheid. Door deze dubbelzinnigheid was het moeilijk om voldoende informatie te verkrijgen tijdens hoorzittingen en missies en naar aanleiding van verzoeken om informatie. Het gebrek aan duidelijkheid over de definitie van nationale veiligheid en de te ruime interpretatie van het toepassingsgebied ervan door de nationale autoriteiten vormen een uitdaging bij het begrijpen van de rechtvaardiging voor het gebruik van spyware.

9. Door informatie uit verschillende bronnen samen te voegen, kon PEGA echter een gedeeltelijk maar duidelijk beeld reconstrueren, en kon het zaken identificeren die zorgwekkend zijn en nader onderzoek verdienen.

10. Er kan met zekerheid van worden uitgegaan dat de autoriteiten in alle lidstaten op de een of andere manier gebruikmaken van spyware, sommige legitiem, sommige niet. Spyware kan rechtstreeks worden aangekocht, of via een gevolmachtigde, een makelaar of een tussenpersoon. Er kunnen ook afspraken worden gemaakt over specifieke diensten, in plaats van de software zelf aan te schaffen. Er kunnen aanvullende diensten worden aangeboden, zoals de opleiding van personeel of de levering van servers. Spyware moet niet op zichzelf worden gezien, maar als onderdeel van een breed scala aan producten en diensten die worden aangeboden op een groeiende en lucratieve wereldmarkt. Het is belangrijk te beseffen dat de aanschaf en het gebruik van spyware zeer duur is en in de miljoenen euro’s loopt. Maar in veel lidstaten zijn deze uitgaven niet opgenomen in de reguliere begroting, waardoor ze aan het toezicht kunnen ontsnappen.

11. Uit door de NSO-groep verstrekte informatie is bekend dat Pegasus in ten minste 14 EU-landen werd verkocht totdat de contracten met twee landen werden beëindigd. Het is niet bekend welke landen, maar algemeen wordt aangenomen dat het om Polen en Hongarije gaat. Zolang de NSO-groep of de Israëlische regering echter geen officiële verklaring over contractbeëindiging aflegt, kan dit niet worden nagegaan.

12. Een bijkomend gegeven is de deelnemerslijst van de editie 2013 van de beurs ISS World (waarbij ISS staat voor Intelligence Support Systems, oftewel systemen voor inlichtingenondersteuning). Met uitzondering van Portugal en Luxemburg waren alle huidige EU-lidstaten vertegenwoordigd door een breed scala aan organisaties,

[2] Arrest van 6 oktober 2020, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.*, C-623/17, EU:C:2020:790.

waaronder lokale politiediensten[3]. De laatste jaren is de NSO-groep de hoofdsponsor van het evenement geworden, maar ook Intellexa, Candiru, RCS en vele andere staan op de lijst van sponsoren[4].

13. Als het gaat om de handel in spyware zijn de lidstaten zijn niet alleen koper, maar spelen zij ook andere, uiteenlopende rollen. Sommige zijn gastheer voor spywareverkopers, andere zijn de favoriete bestemming voor financiële en bankdiensten, en weer andere bieden burgerschap en een verblijfplaats aan de hoofdrolspelers van de industrie.

14. In de overgrote meerderheid van de lidstaten worden de inlichtingendiensten gereguleerd door een wettelijk kader – vaak met bepalingen over de organisatie en de werking van deze diensten, alsmede over hun mandaten en bevoegdheden, met inbegrip van hun actiemiddelen en de voorwaarden voor het gebruik ervan – en toezichtsmechanismen die uitvoerende controle, parlementair toezicht, deskundigenorganen en rechterlijke toetsing omvatten. Toch is er bezorgdheid geuit over de permissieve inlichtingenkaders van bepaalde landen, de ondoeltreffende controles, de lakse toezichtpraktijken en de politieke inmenging**.**

15. Spyware wordt duidelijk ook gebruikt door rechtshandhavingsinstanties, niet alleen door inlichtingendiensten. Er bestaat ernstige bezorgdheid over de toelaatbaarheid in rechte van dergelijk materiaal als bewijsmateriaal in het kader van de politiële en justitiële samenwerking in de EU, ook binnen Europol en Eurojust, indien dergelijke informatie afkomstig zou zijn van de toegepaste onderzoeksmethoden zonder behoorlijk gerechtelijk toezicht. Afhankelijk van de nationale wetgeving is het gebruik van spyware legitiem bij onderzoeken onder gerechtelijk toezicht.

16. Het misbruik van spyware brengt de democratie en de grondrechten in gevaar. Sinds de onthullingen van het Pegasusproject hebben de Verenigde Staten verschillende stappen ondernomen om het te onderzoeken en te reguleren. Binnen de EU is er tot nu toe zeer weinig actie ondernomen. Er moeten duidelijke regels komen voor het gebruik van en de handel in spyware, bij voorkeur samen met andere landen, zoals de VS.

I. Het gebruik van spyware in de EU

I.A Polen

17. De vertegenwoordigers van de ministeries weigerden de delegatie van de commissie te ontmoeten. In antwoord op de door PEGA op 15 juli 2022 verzonden vragenlijst hebben de Poolse autoriteiten niet alle vragen beantwoord en volgehouden dat de bestaande bepalingen toereikend waren en dat zij strikt binnen de wet opereerden[5]. Ook de minister van Binnenlandse Zaken, Mariusz Kaminski, weigerde in te gaan op een uitnodiging van PEGA om standpunten uit te wisselen[6].

[3] https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf
[4] https://www.issworldtraining.com/iss_europe/sponsors.html
[5] Antwoord van de permanente vertegenwoordiger van Polen bij de EU, Andrzej Sadós, aan de commissie PEGA, 7 september 2022.
[6] Antwoord van minister van Binnenlandse Zaken, Mariusz Kaminski, per brief aan de commissie PEGA, 12 juli 2022.

18. De onderzoeksmissie van PEGA naar Polen in september 2022 was voor de commissie van het allergrootste belang, omdat zij op die manier informatie en feiten kon verzamelen over het gebruik van Pegasus-spyware. De vergaderingen in Warschau hebben nieuw licht geworpen op het illegale gebruik van intrusieve surveillancesoftware tegen democratische actoren in Polen. De leden kwamen te weten hoe het systeem van wettelijke en institutionele controles is ontmanteld om personen die als politieke tegenstanders worden beschouwd te kunnen viseren met cyberwapens van militaire kwaliteit. Als gevolg daarvan zijn cruciale democratische normen en burgerrechten die in de EU en de Poolse wetgeving zijn vastgelegd, op grove wijze geschonden. Dit is opnieuw een andere dimensie van de crisis van de rechtsstaat in Polen.

AANKOOP VAN PEGASUS

19. In november 2016 waren voormalig premier en huidig EP-lid Beata Szydło en voormalig minister van Buitenlandse Zaken Witold Waszczykowski aanwezig bij een diner ten huize van de toenmalige Israëlische premier Benjamin Netanyahu[7]. Het daaropvolgende jaar in juli hadden Szydło en Netanyahu een ontmoeting met de regeringsleiders van de landen van de Visegrad-groep. Naar verluidt bespraken zij de versterking van de samenwerking op het gebied van innovatie en geavanceerde technologieën en kwesties in verband met de veiligheid van burgers in brede zin[8]. Niet lang na deze bijeenkomst in 2017 werd Pegasus door de Poolse regering verworven na een ontmoeting tussen premier Mateusz Morawiecki, de Hongaarse premier Viktor Orbán en Netanyahu[9].

20. Aanvankelijk ontkenden de Poolse regering en PiS-leider Jarosław Kaczyński de aankoop van Pegasus[10]. Begin januari 2022 bevestigden ze echter de aankoop van spyware door de Poolse regering[11] [12] [13]. In dezelfde maand werd bekend dat de hoge controle-instantie in 2018 belangrijk bewijsmateriaal in verband met de aankoop van Pegasus had verzameld tijdens een controle van het Fonds voor Justitie dat door het ministerie van Justitie wordt beheerd en is opgezet om slachtoffers van misdrijven te ondersteunen. Op 18 januari 2022 hebben het voormalig hoofd van de hoge controle-instantie van Polen (NIK) en nadien de onafhankelijke senator Krzysztof Kwiatkowski voor de speciale commissie van de Senaat inzake gevallen van surveillance met gebruikmaking van het Pegasus-systeem getuigd over de aankoop van Pegasus[14]. Nadat hij was ontslagen van de geheimhoudingsplicht die aan zijn functie was verbonden, legde hij de commissie twee facturen voor waarin de aankoop van spyware voor het

[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 januari 2022.
[8] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 januari 2022.
[9] Financieele Dagblad, "De wereld deze week: het beste uit de internationale pers", 7 januari 2022.
[10] https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/
[11] Financieele Dagblad, "Liberalen Europarlement eisen onderzoek naar spionagesoftware", 12 januari 2022.
[12] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/
[13] January 2022, Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e, 8 februari 2022.
[14] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.

centraal bureau voor corruptiebestrijding (CBA) werd bevestigd, met 25 miljoen PLN uit het door het ministerie van Justitie beheerde Fonds voor Justitie[15]. Kwiatkowski getuigde dat de NIK rekeningen van de Nationale Bank van Polen had ontdekt waarin de overschrijving werd gecertificeerd[16].

21. De facturen werden uitgereikt door Matic Sp. z o.o., dat optrad als tussenpersoon via welke het CBA deze aankoop uitvoerde[17]. Matic Sp. z o.o. is een in Warschau gevestigd IT- en beveiligingsbedrijf dat eigendom is van en geleid wordt door personen die tijdens de communistische periode actief waren in de inlichtingen- en veiligheidsdiensten[18].

22. Matic werd volgens Wyborcza onmiddellijk na de aankoop van Pegasus in november 2017 een vennootschap op aandelen en werkt met een licentie van het ministerie van Binnenlandse Zaken voor de handel in technologieën met de veiligheidsdiensten en de politie, en in de wapenhandel[19]. De onderneming is tevens in het bezit van een speciaal licentiecertificaat van de binnenlandse veiligheidsdienst, waarvan de meest recente in 2019 werd afgegeven, op grond waarvan zij bepaalde vertrouwelijke informatie geheim kan houden tot het einde van het decennium[20]. Vertegenwoordigers van Matic hebben geweigerd de onderzoekscommissie te ontmoeten en informatie te verstrekken.

23. Volgens de Poolse wet kunnen de activiteiten van het CBA alleen uit de staatsbegroting worden gefinancierd. De aankoop van Pegasus werd echter gefinancierd uit het Fonds voor Justitie, dat geen deel uitmaakt van de staatsbegroting maar een overheidsfonds is dat bestemd is voor slachtoffers van misdrijven[21]. De aankoop was derhalve in strijd met het Poolse recht. Bovendien staan de oorspronkelijke reglementen die dit fonds beheren niet toe dat het wordt gebruikt om activiteiten van de speciale diensten te financieren[22]. In september 2017 werd echter bij de commissie overheidsfinanciën van de Sejm (lagerhuis van het Poolse parlement) een motie om het financiële plan van het Fonds voor Justitie te veranderen ingediend door Michał Woś, de plaatsvervangend

---

[15] ONET, https://wiadomosci.onet.pl/kraj/wiceminister-michal-wos-nie-wiem-co-to-jest-pegasus/e9fbrvh, 3 januari 2022; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 2022.

[16] The Wire, https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation, 4 januari 2022; Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.

[17] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 januari 2022.

[18] https://ipn.gov.pl/en/about-the-institute

[19] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 januari 2022.

[20] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 januari 2022.

[21] The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", 17 februari 2022; The Guardian, "Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24 januari 2022; Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, blz. 26; Gazeta Wyborcza, https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba, 3 januari 2022.

[22] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.

minister van Justitie[23] en een naaste medewerker van de minister van Justitie, Zbigniew Ziobro[24]. De parlementsleden hebben deze verandering goedgekeurd. Toen later werd onthuld dat het Fonds voor Justitie werd gebruikt om Pegasus te financieren voor het CBA, zeiden parlementsleden dat "hier tijdens de commissievergadering met geen woord over was gerept"[25]. Het lijkt er dus op dat zij door de regering zijn misleid. Hoewel de NIK een officiële kennisgeving heeft ingediend bij het openbaar ministerie in verband met een wetsovertreding betreffende het gebruik van middelen uit het Fonds voor Justitie voor de aankoop van Pegasus in 2017, wordt niet verwacht dat het openbaar ministerie in een dergelijke zaak actie zal ondernemen, gezien het huidige institutionele en politieke klimaat.

24. Woś heeft het ministerie van Financiën ook om toestemming verzocht om de 25 miljoen PLN die uit het Fonds voor Justitie aan Pegasus was besteed opnieuw toe te wijzen aan "andere activiteiten" die gericht zijn op het "bestrijden van de gevolgen van criminaliteit". De plaatsvervangend minister gaf vervolgens zijn goedkeuring voor de overdrachten uit het Fonds voor Justitie naar het CBA. Toen hij ernaar werd gevraagd in januari 2022, ontkende Woś in eerste instantie echter dat hij iets wist over het instrument zelf, laat staan over de aankoop ervan door de staat, maar inmiddels heeft hij de aankoop bevestigd. Het is onduidelijk hoe de exploitatiekosten voor het gebruik van Pegasus gefinancierd zijn.

25. Naar verluidt heeft de NSO-groep Pegasus tot dusver aan 14 landen in Europa verkocht. De NSO-groep heeft echter ook toegegeven dat zij de licenties van twee van die landen heeft ingetrokken[26]. Tijdens haar getuigenis in de commissie PEGA verklaarde de NSO-groep dat zij alleen "kwesties" in verband met het gebruik van Pegasus onderzoekt wanneer zij informatie ontvangt van klokkenluiders of via de media. Wanneer de NSO-groep klachten ontvangt, onderzoekt en beoordeelt zij deze, en vervolgens kan zij Pegasus afsluiten voor actoren die er misbruik van hebben gemaakt[27]. Op basis van het grote aantal mediaberichten over het gebruik van Pegasus in Polen is het zeer waarschijnlijk dat Polen een van die twee landen was die de gebruiksvoorwaarden van NSO hebben geschonden; dit is evenwel niet bevestigd.

26. Sinds de eerste tekenen van gebruik van Pegasus door de Poolse autoriteiten heeft de Poolse ombudsman getracht bij de autoriteiten te informeren of dit het geval was en heeft hij gepleit voor de verbetering van waarborgen inzake democratische en mensenrechten om misbruik van surveillance te voorkomen, onder andere door middel van jaarlijkse rapportage aan het Poolse Parlement. In januari 2023 stuurde de Poolse ombudsman een brief naar de minister van Binnenlandse Zaken waarin staat dat er geen rechtsgrondslag was voor het gebruik van Pegasus of gelijksoortige spyware in Polen, onder verwijzing naar de rechtspraak van het Poolse Grondwettelijk Hof alsook de

[23] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 2022; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html, 3 januari 2022.
[24] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 2022.
[25] https://polishnews.co.uk/pegasus-reports-of-surveillance-and-backstage-of-the-purchase-themis-judges-association-on-a-possible-breach-of-the-law-appeal-to-appoint-a-commission-of-inquiry/, 4 januari 2022.
[26] Discussie met de NSO-groep, missie van de enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken naar Israël, juli 2022.
[27] Getuigenis van Chaim Gelfand, General Counsel en Chief Compliance Officer, NSO, in PEGA, 21 juni 2022.

rechtspraak van het EHRM[28].

RECHTSKADER

27. In 2014 heeft het Grondwettelijk Hof een evaluatie uitgevoerd van de Politiewet van 1990 en andere bestaande wetten die betrekking hadden op de surveillance van burgers en die onverenigbaar met de grondwet van Polen geacht[29]. Het Hof sloot deze evaluatie af met een arrest dat specifieke aanbevelingen en een termijn van 18 maanden bevatte waarbinnen wetswijzigingen moesten worden doorgevoerd[30]. Na de verkiezingen van 2015 heeft de nieuwe regering wetswijzigingen ingevoerd. Die wet van 15 januari 2016 tot wijziging van de Politiewet van 1990 en enkele andere wetten (hierna "Politiewet van 2016" genoemd) heeft echter geen van de tekortkomingen van de wet verholpen, zoals het Grondwettelijk Hof had geëist[31]. In plaats daarvan zijn de bestaande bepalingen die, op zich beschouwd, de rechten van de burgers niet voldoende hadden beschermd en evenmin behoorlijk toezicht creëerden, in de Politiewet van 2016 verder verzwakt.

28. In haar advies over de Politiewet van 2016 stelt de Commissie van Venetië dat "... de procedurewaarborgen en materiële voorwaarden waarin de Politiewet voorziet voor het uitvoeren van geheime surveillance, nog steeds ontoereikend zijn om een excessieve toepassing van de wet en een ongerechtvaardigde bemoeienis met de private levenssfeer van personen te voorkomen"[32]. Bovendien maken het ontbreken van bijzonderheden met betrekking tot toezicht, garanties tegen misbruik, en de categorieën personen en misdrijven die doelwit kunnen worden, ook inbreuk op de uitspraken van het EHRM[33]. Met name in de uitspraak in de zaak *Roman Zakharov* v. *Rusland* in 2015, onderzocht het Hof de noodzaak van duidelijkheid over het gebruik van spyware. Er werd geoordeeld dat er met betrekking tot de geheime surveillance van burgers strengere criteria, goed gerechtelijk toezicht, de onmiddellijke vernietiging van irrelevante gegevens, gerechtelijke controle op noodprocedures en een vereiste om slachtoffers in kennis te stellen nodig zijn[34]. Bovendien stelde het Hof uitdrukkelijk dat het "in strijd met de rechtsstaat" zou zijn als de bevoegdheid ten aanzien van geheime surveillance volledig bij de uitvoerende macht van het gerechtelijke apparaat zou zijn geconcentreerd[35]. De Politiewet van 2016 die in Polen van kracht blijft, weerspiegelt in geen geval deze uitspraak van het Hof. De bepalingen ervan vormen namelijk een

[28] Hoorzitting van de commissie PEGA, 19 januari 2023.
[29] Advies nr. 839/2016 over de wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten, zoals aangenomen door de Commissie van Venetië en haar 107e plenaire vergadering, 10-11 juni 2016.
[30] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani
[31] Wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten bij art. 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf
[32] Advies nr. 839/2016 over de wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten, zoals aangenomen door de Commissie van Venetië en haar 107e plenaire vergadering, 10-11 juni 2016.
[33] Zie onder meer *Roman Zakharov* v. *Rusland* [GK], nr. 47143/06, EHRM, arrest van 4 december 2015; *Klass en anderen* v. *Duitsland*, nr. 5029/71, EHRM, arrest van 6 september 1978, § 40; *Prado Bugallo* v. *Spanje*, nr. 58496/00, EHRM, arrest van 18 februari 2003, § 30; *Liberty en anderen* v. *Verenigd Koninkrijk*, nr. 58243/00, arrest van 1 juli 2008, § 62.
[34] *Roman Zakharov* v. *Rusland* [GK], nr. 47143/06, EHRM, arrest van 4 december 2015.
[35] *Roman Zakharov* v. *Rusland* [GK], nr. 47143/06, EHRM, arrest van 4 december 2015, § 229 en 230. Zie ook Advies nr. 839/2016 van de Commissie van Venetië, juni 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, blz. 11.

rechtstreekse schending van een groot deel van de uitspraak.

29. Het EHRM was ook ondubbelzinnig in zijn standpunt over de noodzakelijkheidstest, dat wil zeggen dat het toezicht van voldoende belang moet zijn om een inbreuk op de privacy als noodzakelijk aan te merken. In zijn arrest in de zaak *Klass en anderen* v. *Duitsland* in 1978 werd dit standpunt duidelijk uiteengezet, en werd gesteld dat het Hof, ongeacht het surveillancesysteem, tevreden moet zijn dat er "passende en doeltreffende garanties tegen misbruik"[36] zijn. De zorgvuldig georkestreerde vernietiging van controles en waarborgen in Polen maakt duidelijk dat de regeringspartij zich overduidelijk niets aantrekt van de rechters. Desondanks houdt de door PiS geleide regering vol dat de bestaande bepalingen toereikend zijn, en dat zij strikt binnen de grenzen van de wet handelen[37]. Tegelijkertijd heeft de regering alle verzoeken om dialoog en opheldering over het gebruik van surveillance in Polen afgewezen.

ANTITERRORISMEWET VAN 2016

30. Naast de Politiewet van 2016 heeft de Sejm in 2016 ook een wet aangenomen betreffende de surveillance van buitenlandse burgers, de zogenaamde "antiterrorismewet". Deze wet bepaalt dat niet-Poolse burgers gedurende drie maanden zonder toestemming van het Hof kunnen worden gemonitord als hun identiteit "twijfelachtig" is, onder meer in de vorm van het afluisteren van telefoons, het verzamelen van vingerafdrukken, biometrische foto's en DNA, en de verplichting om prepaid telefoonkaarten te registreren[38]. Volgens artikel 9.8 van de wet heeft de procureur-generaal de bevoegdheid de vernietiging van niet-relevant materiaal te gelasten. Gezien het feit dat de huidige procureur-generaal, Zbigniew Ziobro, tevens minister van Justitie is, bestaat er ernstige bezorgdheid over de vraag of hij in staat is onafhankelijke en onpartijdige beslissingen te nemen zonder te worden beïnvloed door de politieke belangen van de regering die hij vertegenwoordigt[39] [40].

WETBOEK VAN STRAFVORDERING

31. In juli 2015 werd in Polen de Wet tot wijziging van het Wetboek van Strafvordering ingevoerd om ervoor te zorgen dat onrechtmatig verkregen bewijsmateriaal niet in de strafprocedure kan worden opgenomen. De wet werd echter, nadat PiS aan de macht kwam, in maart 2016 herzien om daarin artikel 168a op te nemen[41]. Deze toevoeging zorgt ervoor dat bewijsmateriaal dat in strijd met de wet is verzameld, oftewel "fruit of the poisonous tree", zoals informatie die met behulp van Pegasus is verkregen, eventueel kan worden gebruikt in strafprocedures[42]. Er moet echter aan worden

[36] *Klass en anderen* v. *Duitsland*, 6 september 1978, punt 50, Serie A nr. 28. 40.
[37] Brief van Mariusz Kaminski, minister van Binnenlandse Zaken en Bestuurszaken van Polen, aan de commissie PEGA, 8 september 2022.
[38] Wet van 10 juni 2016 inzake terrorismebestrijdingsoperaties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf
[39] Wet van 10 juni 2016 inzake terrorismebestrijdingsoperaties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf
[40] EDRi, https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/, 29 juni 2016.
[41] Wet van 11 maart 2016 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf
[42] 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

toegevoegd dat het Hooggerechtshof van Polen in een vonnis heeft aangegeven dat dit artikel niet in strijd met de bepalingen van het Europees Verdrag voor de rechten van de mens en van de grondwet van Polen kan worden toegepast, dat in bepaalde gevallen de daadwerkelijke toepassing ervan beperkt[43]. Er zijn ook vonnissen waarin artikel 168a gedeeltelijk ongrondwettig is bevonden[44]. Niettemin leidt de aanwezigheid van deze bepaling in het rechtsstelsel tot onzekerheid met betrekking tot de inachtneming van de grondrechten.

TELECOMMUNICATIEWET

32. Na de wijziging in 2016 van de telecommunicatiewet van 2004, bevat de Poolse telecommunicatiewet onder meer bepalingen op grond waarvan de politie onbeperkte toegang kan krijgen tot metagegevens, en in bepaalde gevallen zonder betrokkenheid van de telecommunicatiebedrijven[45]. Die toegang kan worden verkregen op grond van een zeer brede rechtvaardiging van "preventie of opsporing van misdrijven". De procureur besluit vervolgens hoe na ontvangst van deze gegevens te werk wordt gegaan. Dit kan echter niet als een waarborg worden beschouwd, aangezien het Openbaar Ministerie door de samenvoeging van de functie van minister van Justitie en die van procureur-generaal niet als onafhankelijk van de uitvoerende macht kan worden beschouwd[46].

33. De bovenstaande wijziging van het Wetboek van Strafvordering om "fruit of the poisonous tree" mogelijk te maken, heeft een aanzienlijk effect gehad op het belang van telecommunicatie-exploitanten en de gegevens die deze bedrijven bewaren. In Polen zijn de grootste telecomaanbieders effectief verplicht om over een speciaal team te beschikken dat reageert op de talrijke afluisterverzoeken van de autoriteiten. Zij hebben echter meestal niet veel inzicht in de inhoud van het afluisteren of de operationele details van individuele gevallen[47].

DE WET TER UITVOERING VAN DE RICHTLIJN RECHTSHANDHAVING

34. Polen heeft de richtlijn wetshandhaving (Richtlijn (EU) 2016/680)[48], op grond waarvan specifieke normen voor de verzameling en verwerking van persoonsgegevens door de politie en andere diensten zijn vereist, niet naar behoren uitgevoerd. De richtlijn rechtshandhaving werd in het Poolse recht omgezet bij de wet van 2018 inzake de

[43] Bijvoorbeeld het vonnis van het Hooggerechtshof van Polen van 26 juni 2019, IV KK 328/18.
[44] Bijvoorbeeld het vonnis van het Hooggerechtshof van Polen van 26 juni 2019, IV KK 328/18.
[45] Telecommunicatiewet van 16 juli 2004, https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004
[46] Wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten bij art. 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf
[47] https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_NL.pdf; The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17 februari 2022; 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; https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, blz. 16-17.
[48] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

bescherming van persoonsgegevens die worden verwerkt in verband met de preventie en bestrijding van criminaliteit. De wet voorziet in een aanmerkelijke uitbreiding van de gronden van de richtlijn om te weigeren personen in kennis te stellen van de verwerking van hun gegevens en gaat voorbij aan het mechanisme van artikel 17 van de richtlijn, waarmee personen de mogelijkheid wordt geboden hun bevoegdheid uit te oefenen via de relevante toezichthoudende autoriteit – in Polen, de voorzitter van het bureau voor de bescherming van persoonsgegevens. Voorts voorziet de wet in een aanzienlijke uitzondering voor de nationale veiligheid, met inbegrip van de uitvoering van wettelijk verplichte taken door verschillende agentschappen van de veiligheidsdiensten[49].

35. Polen heeft ook de klokkenluidersrichtlijn van de EU nog niet ten uitvoer gelegd. Het land heeft de uiterste termijn van december 2021 niet gehaald nadat zijn eerste ontwerpwetgeving was mislukt. In april 2022 werd een tweede ontwerp gepubliceerd, maar er is verder geen vooruitgang geboekt en de voorgestelde wetgeving bevat aanzienlijk zwakkere bepalingen. In januari 2022 heeft de Commissie een inbreukprocedure tegen Polen ingeleid wegens de gebrekkige uitvoering van de richtlijn en in februari 2023 heeft de Commissie besloten Polen voor het HvJ-EU te dagen[50].

36. De Sejm, met name leden van PiS, is momenteel bezig met het opstellen van een wet inzake elektronische communicatie. Deze wet maakt het voor de autoriteiten gemakkelijker om toegang te verkrijgen tot de e-mails en berichten op sociale media van Poolse burgers. Aanbieders moeten e-mails en berichten opslaan op hun servers zodat de bevoegde rechterlijke instanties bevelen zouden kunnen geven om toegang te krijgen tot de gegevens, IP-adressen en de inhoud van de berichten[51].

TOETSING VOORAF

37. Hoewel in Polen in de regel rechterlijke toestemming vereist is voor surveillance, dient de bestaande machtigingsprocedure niet als waarborg tegen misbruik, maar veeleer als een manier om aan surveillance voor politieke doeleinden een schijn van wettigheid te verlenen. Het is niet expliciet duidelijk geworden of er een rechterlijke machtiging voorhanden was om de doelwitten van Pegasus te bespioneren. Aanvragen voor rechterlijke machtiging voor een surveillance worden ingediend door de speciale diensten[52]. Voor de beoordeling van het verzoek beschikken rechters alleen over de informatie die door de verzoeker (d.w.z. de speciale diensten) wordt verstrekt, en het is de openbaar aanklager die beslist welk materiaal relevant is om te worden voorgelegd[53]. De informatie is vaak slechts een samenvatting, waarin soms zelfs de meest elementaire details over het doelwit (naam, beroep, het misdrijf waarvan het doelwit wordt verdacht) en een beschrijving van de te gebruiken surveillancemethoden, niet worden

[49] Adam Bodnar et al., "How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform", september 2019, https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf
[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_703
[51] Euractiv, "Polish government working on controversial surveillance bill", https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/
[52] Wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten bij art. 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf
[53] Wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten bij art. 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf

vermeld.

38. Als rechters een verzoek weigeren, moeten zij de redenen voor een dergelijk besluit geven, en kan er tegen het besluit beroep worden ingesteld[54]. In noodgevallen kan de aanklager aanvankelijk het gebruik van onderscheppingsmethoden toestaan zonder toestemming van een rechter, op voorwaarde dat de rechter vervolgens binnen vijf dagen toestemming geeft[55]. Dit is een grote en welbewuste maas in de Poolse wet.

39. Verzoeken om toestemming voor surveillance door de belangrijke diensten, d.w.z. het CBA, de politie (Policja KGP), en de inlichtingendiensten (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro Nadzoru Wewnętrznego MSWiA, en het onlangs toegevoegde Inspektorat Służby Więziennej) worden bijna uitsluitend ingediend bij de rechtbank in Warschau (Sad Okręgowy), waar de meerderheid van deze diensten is gevestigd.

40. Dagelijks worden tientallen surveillancetoepassingen ingediend, waardoor de capaciteit van de rechter om elk verzoek grondig te onderzoeken op de proef wordt gesteld[56]. Het systeem dat zaken willekeurig toewijst aan de rechters van de rechtbanken wordt technisch gezien nog steeds gebruikt in Polen, maar werkt alleen tijdens kantooruren. Aangezien rechters 24 uur per dag toestemming voor surveillance geven, zijn er echter ruimschoots mogelijkheden om het systeem te omzeilen. Door een verzoek in het weekend of buiten de normale kantooruren in te dienen, wordt de zaak automatisch toegewezen aan de dienstdoende rechter[57]. De informatie over wie op welk moment dienst heeft, is bekend bij de geheime diensten, die dan in wezen een “welwillende rechter” kunnen kiezen bij wie zij hun verzoek om surveillance kunnen indienen[58]. Bovendien kan willekeurige toewijzing ook worden omzeild door alle IT-medewerkers die toegang hebben tot het systeem en verzoeken om surveillance aan “welwillende rechters” kunnen toewijzen[59]. Dit alles ondermijnt in ernstige mate het vermogen van de rechtbank om doeltreffend rechterlijk toezicht uit te oefenen.

TOETSING ACHTERAF

41. In Polen bestaat er vrijwel geen parlementair toezicht. Vóór 2016 werd de parlementaire commissie van toezicht op de speciale diensten (KSS) geleid door het voorzitterschap te laten rouleren tussen de regerings- en oppositiepartijen. PiS heeft deze parlementaire

[54] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef
[55] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef
[56] Getuigenverklaring van Ewa Wroszek, landspecifieke hoorzitting over Polen, vergadering van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, 15 september 2022.
[57] Getuigenverklaring van Ewa Wroszek, landspecifieke hoorzitting over Polen, vergadering van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, 15 september 2022.
[58] Getuigenverklaring van Ewa Wroszek, landspecifieke hoorzitting over Polen, vergadering van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, 15 september 2022.
[59] Getuigenverklaring van Ewa Wroszek, landspecifieke hoorzitting over Polen, vergadering van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, 15 september 2022.

regel echter gewijzigd en PiS-leden Waldemar Andzel en Jarosław Krajewski geïnstalleerd als respectievelijk permanente voorzitter en ondervoorzitter van deze commissie[60]. De regeringspartijen hebben de absolute meerderheid in de commissie[61]. Dit maakt de toezichtsfunctie van de commissie zinledig. Bovendien werden verzoeken om een parlementair onderzoek naar de beschuldigingen van onrechtmatig gebruik van spyware door de regeringsmeerderheid in de Sejm afgewezen[62] [63] [64] [65] [66]. Anderzijds heeft de Senaat, waar de regeringspartijen geen meerderheid hebben, begin 2022 een onderzoekscommissie ingesteld. De senaatscommissie heeft echter niet de onderzoeksbevoegdheden van de Sejm[67], waarvan de onderzoekscommissie getuigen kan oproepen en beëdigde verklaringen kan horen. De commissie is bij elke gelegenheid tegengewerkt door de regeringspartij in de Sejm[68], regeringsfunctionarissen en veiligheidsdiensten, die allemaal hebben geweigerd mee te werken of hun eigen onderzoek in te stellen[69].

42. De controle en oplossingen die worden geboden door andere onafhankelijke organen zijn ook aanmerkelijk verzwakt. De hoge controle-instantie heeft werkelijke bevoegdheden op het gebied van toezicht; niettemin krijgen haar leden en personeel voortdurend te maken met belemmering, pesterijen en intimidatie, hetgeen ernstige gevolgen heeft voor hun operationele capaciteit[70]. De Sejm is er tot dusver niet in geslaagd 10 van de 19 leden van de NIK-raad[71] te benoemen. Het vereiste doorlichten van raadsleden door de speciale diensten, onder leiding van minister Kaminski, verloopt

[60] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[61] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[62] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 januari 2022.
[63] Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, blz. 27.
[64] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 december 2021.
[65] The Guardian, "Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24 januari 2022.
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[67] Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, blz. 27, voetnoot 220.
[68] Bloomberg, https://www.bloomberg.com/news/articles/2022-01-03/polish-government-urged-to-probe-spyware-use-as-scandal-grows?leadSource=uverify%20wall#xj4y7vzkg, 3 januari 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 januari 2022; Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, blz. 27; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 december 2021; The Guardian, "Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24 januari 2022; Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4 februari 2022; discussie met de hoge controle-instantie, missie van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken naar Polen, september 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; discussie met het personeel van de hoge controle-instantie, missie van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken naar Polen, september 2022.

zeer traag[72].

43. Wanneer een overtreding van de wet wordt ontdekt door de NIK, heeft zij de bevoegdheid het Openbaar Ministerie in te lichten[73]. Het is echter aan het Openbaar Ministerie om op basis van deze melding een zaak in te leiden. In situaties waarin het Openbaar Ministerie geen maatregelen neemt, kan de NIK weinig doen. Wanneer een gemelde overtreding betrekking heeft op het functioneren van het Openbaar Ministerie zelf, ontstaat er een vicieuze cirkel van niet-aansprakelijkheid. Bovendien moeten alle door de NIK bij het Openbaar Ministerie gemelde zaken worden gemeld bij de procureur-generaal, die ook de minister van Justitie is en aan het hoofd staat van het ministerie dat de spyware zelf heeft aangekocht. De procureur-generaal is bevoegd om onderzoeken die door het Openbaar Ministerie zijn beëindigd, stop te zetten of te hervatten. Hij kan ook tuchtprocedures inleiden tegen aanklagers die hij ervan verdenkt verkeerde beslissingen te hebben genomen.

44. De huidige ombudsman, Marcin Wiącek, werd in 2021 benoemd toen de Sejm en de Senaat na een langdurige krachtmeting overeenstemming bereikten over een politiek neutrale compromiskandidaat[74]. Met betrekking tot de zaak van senator Brejza voerde Wiącek aan dat de ombudsman niet mag worden betrokken in vroege stadia van een zaak. Desondanks heeft zowel de vorige als de huidige ombudsman de situatie gemonitord en een bepaalde hoeveelheid druk uitgeoefend op de noodzaak om een onafhankelijk toezichtorgaan in te stellen om democratisch toezicht op de activiteiten van de geheime diensten te houden[75].

VERSLAGLEGGING

45. Op grond van de Politiewet van 2016 is de politie slechts verplicht tweemaal per jaar verslagen in te dienen bij de bevoegde rechterlijke instanties over het aantal verzamelde telecommunicatie-, post- of internetgegevens, samen met de rechtsgronden daarvoor (die verband houden met de preventie of opsporing van misdaden, de bescherming van het menselijk leven, de gezondheid of ondersteuning van opsporings- en reddingsoperaties)[76]. Deze verslagen kunnen alleen achteraf worden opgesteld en worden niet openbaar gemaakt. Mocht er een probleem zijn met de indiening, dan zal de rechtbank binnen 30 dagen haar bevindingen voorleggen, maar kan zij niet de vernietiging van gegevens bevelen, zelfs niet als zij strijdigheden met de wet vaststelt. Zeer belangrijk is dat deze toezichtsmaatregelen slechts facultatief en niet verplicht zijn.

---

[72] Discussie met het personeel van de hoge controle-instantie, missie van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken naar Polen, september 2022.
[73] Wet van 23 december 1994 betreffende de hoge controle-instantie, https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html, artikel 63.
[74] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22 juli 2021.

[75]Europees Parlement. Directoraat-generaal Parlementaire Onderzoeksdiensten, “Europe’s PegasusGate: Countering spyware abuse”-studie, 6 juli 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, blz. 22.
[76] Wet van 15 januari 2016 tot wijziging van de Politiewet en enkele andere wetten bij art. 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf

VERHAALSMOGELIJKHEDEN

46. Ondanks dat er overvloedig bewijs is dat er ernstige misdrijven zijn gepleegd, heeft de Poolse openbare aanklager zich tot dusver zeer afwachtend opgesteld. Het lijkt erop dat de rechter alleen de zaak van openbaar aanklager Ewa Wrzosek en Krzysztof Brejza in behandeling heeft genomen. Wrzosek diende haar zaak aanvankelijk in bij het Openbaar Ministerie. Na de officiële weigering om de zaak in behandeling te nemen, kon zij echter in beroep gaan bij de rechter. Eind september 2022 heeft de rechtbank van Warschau (Mokotów) de openbare aanklager gelast een onderzoek in te stellen. Tot dusver heeft de openbare aanklager echter geen enkele zinvolle procedure ingeleid die noodzakelijk is voor de voortgang van de zaken, zoals het verzamelen van getuigenissen van het doelwit.

47. Het is belangrijk om op te merken dat Wrzosek dit beroep alleen bij de rechter kon instellen na een officiële weigering van het Openbaar Ministerie te hebben ontvangen. In veel andere gevallen rekt de openbaar aanklager zijn onderzoek om te voorkomen dat hij ooit een officieel antwoord moet geven, aangezien hij zich ervan bewust is dat als hij dat doet, hij zal worden blootgesteld aan de beroepsprocedures voor de gerechtelijke instanties.

48. Burgers die het doelwit zijn geweest kunnen een civiele procedure aanhangig maken bij de rechter, maar de bewijslast dat zij het voorwerp van surveillance waren ligt bij hen en het is zonder medewerking van de autoriteiten vrijwel onmogelijk om het onrechtmatige gebruik van spyware aan te tonen. De tekortkomende nakoming van de mededelingsplicht in Polen, zoals uiteengezet in het arrest *Klass*, houdt in dat veel personen mogelijk nooit te weten komen dat zij doelwit zijn geweest.

49. Momenteel zijn de zaken *Pietrzak* v. *Polen* en *Bychawska-Siniarska en anderen* v. *Polen* aanhangig voor het EHRM, waarbij bezwaar wordt gemaakt tegen het gebrek aan transparantie, toezicht, kennisgeving en rechtsmiddelen als het gaat om surveillance in Polen. Belangrijk is dat het Hof besloot een ongebruikelijke hoorzitting voor deze zaken te houden, die plaatsvond op 27 september 2022. De zaken waren aanhangig gemaakt door vijf burgers[77] die in respectievelijk september 2017 en februari 2018 klachten hadden ingediend bij het EHRM. In deze zaak dienden elf entiteiten stellingnamen als *amicus curiae* in, met inbegrip van de Europese vereniging van strafrechtadvocaten[78], de Poolse ombudsman, en de speciale VN-rapporteur voor de bevordering en bescherming van mensenrechten en fundamentele vrijheden bij de bestrijding van terrorisme[79].

50. Hoewel deze rechtsgang voor klachten naar het EHRM openstaat voor burgers, valt het te betwijfelen of dit als een doeltreffend rechtsmiddel kan worden beschouwd, gezien de

---

[77] Mikołaj Pietrzak, advocaat, deken van de orde van Warschau; Dominika Bychawska-Siniarska, lid en medewerkster van de Helsinki Foundation for Human Rights; Barbara Grabowska-Moroz, universitair docent/onderzoeker en extern deskundige bij de Helsinki Foundation for Human Rights; Wojciech Klicki en Katarzyna Szymielewicz, leden van de in Warschau gevestigde Panoptykon Foundation.

[78] https://www.ecba.org/content/index.php/working-groups/human-rights/857-ecba-hr-office-at-the-echr-hearing-in-the-case-pietrzak-v-poland-and-bychawska-siniarska-and-others-v-poland-hearing-29-09-2022.

[79] https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/AmicusBrief_Poland_SRCT_ECHR.pdf.

lengte van de procedure. Vijf jaar na de eerste klacht is er nog steeds geen rechterlijke beslissing genomen in deze zaak.

51. Op basis van artikel 227 van het wetboek bestuursprocesrecht werden eerder in 2017 klachten ingediend bij de minister-president en de respectieve hoofden van de verschillende politie- en inlichtingendiensten. Deze inlichtingendiensten omvatten het CBA, de binnenlandse veiligheidsdienst, de nationale belastingdienst, de militaire contraspionagedienst, de nationale politie, de grenspolitie en de nationale gendarmerie. Hun klachten hadden betrekking op het feit dat de wet leden van deze politie- en inlichtingendiensten toestond hun telecommunicatie en digitale communicatie te monitoren zonder hun medeweten. Aangezien de leden van de desbetreffende diensten niet verplicht waren hen over mogelijke surveillance te informeren, was het voor de verzoekers bijgevolg niet mogelijk de wettigheid van die activiteit te laten beoordelen door een rechter, hetgeen volgens hen in strijd was met de Poolse grondwet.

52. Tussen juni en september 2017 stuurden de hoofden van de bovengenoemde politie- en inlichtingendiensten hun antwoorden op de klachten van de verzoekers. De verzoekers beriepen zich op artikel 8 (recht op eerbiediging van het privéleven en van het familie- en gezinsleven) van het Europees Verdrag voor de rechten van de mens en klaagden dat de geheime systemen voor het monitoren van telecommunicatie, post- en digitale communicatie en het verzamelen van metagegevens, die zijn opgenomen in de toepassing van de Politiewet en de terrorismebestrijdingswet, hun recht op eerbiediging van het privéleven aantasten. De verzoekers beroepen zich op artikel 8 en artikel 13 (recht op een doeltreffende voorziening in rechte) en voeren aan dat zij niet beschikten over een doeltreffende voorziening in rechte die hen in staat stelde vast te stellen of zij zelf het doelwit van geheime surveillance waren geweest en, indien nodig, de wettigheid van die surveillance te laten beoordelen door een rechter.

OPENBAAR TOEZICHT

53. De onafhankelijke media vormen een ander element van democratische “checks-and-balances”, waarbij publieke controle wordt uitgeoefend. In het geval van het gebruik van spyware werd de Poolse publieke omroep, die grotendeels wordt gecontroleerd door de regeringspartijen, echter in feite medeplichtig aan het onwettige surveillanceschandaal door materiaal openbaar te maken dat afkomstig was van de smartphones van verschillende doelwitten, waaronder senator van de oppositie Krzysztof Brejza. Het openbaar maken van de in het kader van een surveillanceoperatie van de bijzondere diensten verkregen informatie is op zichzelf een strafbaar feit; toch is er geen actie ondernomen, noch door de politie, noch door het Openbaar Ministerie.

POLITIEKE CONTROLE

54. Veel sleutelposities in de hele keten worden bezet door leden of vertrouwelingen van de regeringspartijen. Minister van Binnenlandse Zaken en coördinator van de speciale diensten Kaminski werd in 2015 veroordeeld tot drie jaar gevangenisstraf wegens

machtsmisbruik[80]. Onmiddellijk na de parlementsverkiezingen van 2015 heeft president Duda hem echter op zeer onregelmatige wijze gratie verleend, een handelswijze die onder meer door het Poolse Hooggerechtshof, het HvJ-EU, de Commissie van Venetië en het Amerikaanse ministerie van Buitenlandse Zaken werd veroordeeld. Een en ander geeft aanleiding tot bezorgdheid over zijn onafhankelijkheid en neutraliteit. Kaminski heeft geweigerd de commissie PEGA te ontmoeten of met haar samen te werken[81].

55. Het CBA wordt volledig gecontroleerd door de regerende meerderheid en is niet onafhankelijk, ondanks zijn titel en zijn mandaat, dat is vastgesteld bij de wet van 9 juni 2006 betreffende het centraal bureau voor corruptiebestrijding[82], waarvan artikel 1, lid 1, bepaalt dat het centraal bureau voor corruptiebestrijding is opgericht als een speciale dienst ter bestrijding van corruptie in het openbare en economische leven, met name in openbare en lokale overheidsinstellingen, en ter bestrijding van activiteiten die schadelijk zijn voor het economische belang van de Staat[83]. In het verslag over de rechtsstaat van 2022 stelt de Commissie vast dat "[d]e onafhankelijkheid van de belangrijkste instellingen voor corruptiebestrijding nog altijd een probleem [is], met name gezien de ondergeschiktheid van het centraal bureau voor corruptiebestrijding aan de uitvoerende macht en de minister van Justitie die tegelijkertijd de procureur-generaal is"[84].

56. De inspanningen van de regering om controle te krijgen over de rechterlijke macht zijn uitvoerig gedocumenteerd en bevestigd door een groot aantal instanties, waaronder de Commissie, het HvJ-EU en het EHRM.

57. Niet alleen zijn er juridische en institutionele omstandigheden gecreëerd om bijna onbeperkte surveillance met spyware mogelijk te maken, maar worden vrijwel alle onderdelen van het proces ook grondig gecontroleerd door de regeringspartijen. Bijgevolg hebben waarborgen die op papier bestaan, in de praktijk geen of weinig betekenis.

DE DOELWITTEN

58. De eerste gedocumenteerde gevallen van het gebruik van Pegasus in Polen dateren van 2018. Een daarvan betrof de voormalige onderminister van Financiën, Paweł Tamborski, wiens telefoon in februari 2018 met behulp van Pegasus werd gehackt, zoals Amnesty International en Wyborcza in juli 2022 onthulden. Op dezelfde dag stelde het CBA hem in bewaring, evenals vijf voormalige functionarissen van het ministerie, en marktanalisten, die ervan werden beschuldigd de marktwaarde van het chemiebedrijf CIECH te laag te hebben geschat in ruil voor steekpenningen. De rechter was het niet eens met hun aanhouding en eiste hun invrijheidstelling. De CEO en eigenaar van het pr-bureau Cross Media, Andrzej Długosz, was ook een doelwit en werd uiteindelijk tussen maart 2018 en november 2019 minstens 61 keer gehackt. Vervolgens verzocht de Ombudsman de autoriteiten om aanvullende informatie, maar

[80] *Reuters*, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, 17 november 2015.
[81] EU Observer, https://euobserver.com/rule-of-law/156063, 15 september 2022.
[82] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf
[83] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf, artikel 1.1.
[84] Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, blz. 1.

daaraan werd geen gehoor gegeven. Toentertijd bleef de regering ontkennen de spyware te hebben aangekocht.

59. Naar aanleiding van de onderzoeken van de Associated Press en onderzoekers van het Citizen Lab aan de Universiteit van Toronto werd onthuld dat er in Polen in 2019 nog drie personen het doelwit van Pegasus zijn geweest[85], namelijk de senator van de oppositie Krzysztof Brejza, advocaat Roman Giertych en openbaar aanklager Ewa Wrzosek. Hoewel sommige leden van de regerende meerderheid de aankoop van de software van de NSO-groep hebben bevestigd, heeft de regering niet officieel erkend dat specifieke personen een doelwit zijn geweest. Geen van de drie doelwitten is formeel beschuldigd van enig misdrijf of is opgeroepen voor verhoor, noch is er een verzoek ingediend voor opheffing van de immuniteit van de doelwitten die in verband met deze zaak een openbaar ambt bekleden.

60. Het Citizen Lab had in Polen eind 2017 een aantal infecties opgespoord; zij konden de doelwitten toen echter niet identificeren[86].

61. Het gebruik van spyware en inspanningen om burgers te controleren, moeten in nauw verband met het kiesstelsel worden gezien. Verschillende doelwitten van Pegasus waren op enigerlei wijze verbonden met verkiezingen: senator Krzysztof Brejza (hoofd van de verkiezingscampagne van de grootste oppositiepartij), Roman Giertych (advocaat van oppositieleider en voormalig voorzitter van de Europese Raad, Donald Tusk), Ewa Wrzosek (de openbaar aanklager die het stemmen per brief voor de presidentsverkiezingen onderzoekt), de hoge controle-instantie (NIK) (dat verslagen heeft gepubliceerd over het stemmen per brief voor de presidentsverkiezingen), en Michael Kolodziejczak (oprichter van een agrarische politieke partij die strijdt om dezelfde kiezers als de regeringspartijen).

62. Tegelijkertijd is de onafhankelijkheid van de nationale kiescommissie in twijfel getrokken door het feit dat deze bestaat uit rechters die zijn aangeduid door het parlement en de rechtbanken die de regeringspartij onder haar controle heeft gebracht. Bovendien is de rechtbank van Warschau die verantwoordelijk is voor de registratie van nieuwe politieke partijen[87] gevuld met regeringsgetrouwe “neorechters” wier onafhankelijkheid in twijfel kan worden getrokken.

KRZYSZTOF BREJZA

63. Senator Krzysztof Brejza was hoofd van de verkiezingscampagne van de oppositiepartij Burgerplatform voor de Europese en lokale verkiezingen toen hij het doelwit werd van hacking met spyware[88]. In 2019, toen hij de campagne van het Burgerplatform voor de parlementsverkiezingen leidde, werden er 33 pogingen gedaan om zijn telefoon te hacken. De aanvallen begonnen op 26 april 2019 en duurden tot 23 oktober 2019,

[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, *17 februari 2022.*
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[87] Wet van 27 juni 1997 betreffende politieke partijen, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, artikel 11.
[88] 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.

enkele dagen na het einde van de verkiezingscyclus[89].

64. Als rechtstreeks gevolg van het hacken van de telefoon van Brejza, werden naar verluidt sms-berichten gestolen, bewerkt en vervolgens op het door de staat gecontroleerde televisienetwerk (TVP)[90] uitgezonden tijdens de verkiezingen van 2019 in een naar verluidt georkestreerde lastercampagne[91]. Dit heeft ertoe geleid dat senator Brejza vraagtekens heeft geplaatst bij de legitimiteit van de verkiezing van 2019, die nipt werd gewonnen door de regerende PiS-partij[92].

65. Hoewel de PiS-regering toegeeft Pegasus te hebben aangekocht, ontkent zij krachtig dat dit voor politieke doeleinden is gebruikt[93]. Kaczynski heeft niet bevestigd noch ontkend Brejza in het vizier te hebben gehad, maar beweert dat de senator in verband werd gebracht met "vermeende misdrijven", iets wat Brejza vurig ontkent[94]. Er is nooit een aanklacht tegen Brejza ingediend en hij is nooit opgeroepen om te getuigen. Dit wijst erop dat het gebruik van spyware geen enkel onderzoeksdoel diende. Door de suggestie dat Brejza met criminele activiteiten te maken had, probeerde de regering het gebruik van spyware formeel te legitimeren door omstandigheden te creëren waarin de Poolse regering Pegasus-spyware kon gebruiken voor een van de gronden die de NSO-groep "legitiem" achtte toen zij overwoog haar software te verkopen aan een regering, namelijk het onderzoeken van ernstige criminele activiteiten[95].

66. Wekenlang was senator Brejza het doelwit van een lastercampagne waarbij gebruikgemaakt werd van met behulp van Pegasus-spyware verkregen materiaal. Het is opmerkelijk dat dit materiaal via de openbare televisie openbaar is gemaakt. Er kan niet worden verklaard hoe een publieke omroep toegang krijgt tot dergelijk materiaal. Indien de Pegasus-hack van Senator Brejza inderdaad een kwestie van nationale veiligheid was geweest, zoals de regering lijkt te suggereren, zou het een zeer ernstig misdrijf zijn om het bij een geheime veiligheidsoperatie verkregen materiaal te lekken. Het feit dat de regeringspartij de publieke omroep in zijn greep heeft, wijst eerder in de richting van een door de regeringspartijen georkestreerde lastercampagne.

67. Op dat moment werd echter een strafrechtelijk onderzoek ingesteld naar de vader van senator Brejza, Ryszard Brejza. In zijn tijd als burgemeester van Inowroclaw, een centraal in Polen gelegen stad, werd Brejza sr. opgeroepen voor verhoor in verband met

---

[89] The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", 17 februari 2022.
[90] Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, blz. 20-23; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab23 december 2021.
[91] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 december 2021.
[92] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware, 12 januari 2022.
[93] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 januari 2022.
[94] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 januari 2022.
[95] BBC, https://www.bbc.com/news/technology-57881364, 19 juli 2021.

vermeend wanbeheer van overheidsmiddelen en het niet-uitvoeren van zijn taken[96]. Dit verhoor vond plaats vlak nadat Brejza jr. een juridische procedure tegen Kaczynski wegens smaad had ingeleid. Krzysztof en Ryszard Brejza hebben beiden beweerd dat de aanklacht tegen Brejza sr. een vergelding voor de rechtszaak was.

68. Ryszard Brejza ontving tussen juli en augustus 2019 zelf tien sms-berichten die door het veiligheidslab van Amnesty International als verdacht werden aangemerkt en overeenkwamen met de bijzonderheden van Pegasus[97]. Bovendien ontving senator Brejza's voormalige assistente Magdalena Losko tijdens de campagne voor het Europees Parlement in april 2019 vier verdachte sms-berichten die volgens forensische onderzoekers van Amnesty International technisch gezien overeenkwamen met de spyware Pegasus van de NSO-groep[98].

ROMAN GIERTYCH

69. Tijdens de laatste weken van de parlementsverkiezingen van 2019 was Roman Giertych het doelwit met Pegasus-spyware. Tussen september en december 2019 werd Giertych wel 18 keer gehackt. Het merendeel van de hacks vond plaats vlak voor de datum van de verkiezingen, 13 oktober 2019. Op dat moment was hij de advocaat van de leider van de oppositiepartij Burgerplatform en voormalig minister-president Donald Tusk. In die periode vertegenwoordigde Giertych ook Radek Sikorski, voormalig minister van Buitenlandse Zaken en huidig lid van het Europees Parlement namens de Europese Volkspartij (EVP). Toen Sikorski een zaak in behandeling nam om de betrokkenheid te onderzoeken van Kaczynski en zijn bondgenoten bij illegale afluisterpraktijken, werden zijn gesprekken opgenomen en gepubliceerd[99].

70. Net als bij de zaak van senator Brejza wilde de regering niet bevestigen noch ontkennen of zij verantwoorden was voor deze aanvallen. De Associated Press heeft gemeld dat een openbaar aanklager een motie had ingediend om Giertych aan te houden met betrekking tot een onderzoek naar vermeende financiële misdrijven, slechts enkele uren voordat de woordvoerder voor staatsveiligheid Stanislaw Zaryn vragen van de AP over het hacken van de telefoon van Giertych zou beantwoorden. Giertych ontkent dit met klem. Zaryn weigerde commentaar te geven op het mogelijke verband tussen deze incidenten. Bij een vergelijkbaar incident in 2020 werd het huis van Giertych binnengevallen en doorzocht door functionarissen van het centrale corruptiebestrijdingsbureau[100].

71. In deze periode in 2019 vertegenwoordigde Giertych tevens Gerald Birgfellner, een Oostenrijkse ontwikkelaar. Birgfellner was betrokken bij een bouwproject voor PiS-

[96] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f, 10 januari 2022.
[97] The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", 17 februari 2022; Le Monde, https://www.lemonde.fr/pixels/article/2022/07/18/affaire-pegasus-un-an-apres-le-crepuscule-de-nso-group_6135168_4408996.html, 18 juli 2022.
[98] The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", 17 februari 2022.
[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[100] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.

leider Jarosław Kaczynski, met wie hij familiebanden heeft, toen de deal werd afgeblazen. Na het vrijgeven van opgenomen gesprekken tussen de twee barstte een politiek schandaal los voor Kaczynski, die het project vervolgens annuleerde. Birgfellner voert aan dat nooit betaald was voor zijn diensten en daarom Giertych in de arm nam[101]. De minister van Justitie en procureur-generaal Zbigniew Ziobro merkte in 2021 ook op dat hij probeerde een aanklacht in te dienen tegen Giertych "die ervan wordt verdacht misdrijven te hebben gepleegd"[102].

EWA WRZOSEK

72. Aanklager Ewa Wrzosek was tussen 24 juni en 19 augustus 2020 wel zes keer het slachtoffer van hacking met Pegasus-spyware[103]. Wrzosek is lid van Lex Super Omnia, een vereniging van openbare aanklagers die zich inzetten voor de onafhankelijkheid van het Openbaar Ministerie. Ze deed onderzoek naar de beslissing om de Poolse presidentsverkiezingen van 2020 te houden midden tijdens de wereldwijde COVID-19-pandemie, toen zij van de naderhand ingetrokken zaak werd gehaald. De procureur-generaal, Zbigniew Ziobro, en zijn rechterhand, nationaal procureur Bogdan Święczkowski, kunnen beslissen bepaalde zaken niet te vervolgen of ondergeschikte procureurs van bepaalde zaken af te halen[104]. Naderhand werd procureur Wrzosek weggestuurd, waarvan zij slechts 48 uur van tevoren in kennis werd gesteld, naar het bureau van een andere procureur in een stad op enkele uren van haar huis. Wrzosek werd het doelwit van Pegasus-spyware nadat zij naar Warschau teruggekeerd was. Steeds weer weigeren de Poolse autoriteiten hun verantwoordelijkheid te bevestigen of te ontkennen[105] [106].

73. Wrzosek heeft ook een juridische klacht ingediend over de infectie met Pegasus van haar mobiele telefoon. De rechter heeft gevraagd om een expertiserapport van het Citizen Lab over de Pegasus-infectie en Wrzosek heeft zelf verzocht om haar telefoon te laten nakijken door de deskundigen van het Citizen Lab. De aanklager heeft dit verzoek echter geweigerd en een andere deskundige uitgekozen die geen enkele infectie in verband kon brengen met Pegasus. De aanklager heeft de telecomoperator bovendien verzocht alle metagegevens met betrekking tot Wrzosek te overhandigen, voor een periode die irrelevant is voor de gerechtelijke onderzoeken. Wrzosek is van mening dat zij nog steeds onder surveillance staat en dat de procedure van de aanklager gericht is op het verstrekken van aanvullend bewijs dat in andere zaken tegen haar zou kunnen worden gebruikt[107].

---

[101] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2, 16 februari 2019; TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator, 11 februari 2019.
[102] TVP Info, https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrole-operacyjna-do-gry-politycznej, 23 december 2021.
[103] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[104] Verslag van de Commissie over de rechtsstaat 2022, Landenhoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, blz. 16.
[105] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw--8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[106] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, 24 januari 2022.
[107] Hoorzitting van de commissie PEGA, 19 januari 2023.

74. Zoals benadrukt door Wrzosek tijdens de vergadering van de commissie PEGA van 19 januari 2023, wordt zij momenteel door het Openbaar Ministerie aangeklaagd voor het onthullen van informatie over een zaak die geen verband houdt met Pegasus, en voor betrokkenheid bij politieke activiteiten. Wrzosek kan haar verdediging niet opbouwen omdat het Openbaar Ministerie geen toegang tot documenten verleent[108]. Dit lijkt een duidelijke schending te zijn van het recht op een eerlijk proces en wekt de indruk dat de zaak alleen bedoeld is om Wrzosek in diskrediet te brengen.

ANDERE MOGELIJKE DOELWITTEN

HOGE CONTROLE-INSTANTIE

75. Hoewel geen doelwit van Pegasus, werd de NIK – de hoge controle-instantie –, die belast is met de bescherming van de overheidsuitgaven en het beheer van overheidsdiensten en die de facturen voor de "aankoop van speciale technologische middelen voor het opsporen en voorkomen van criminaliteit" voor een totaalbedrag van 25 miljoen PLN openbaar maakte, door de Poolse autoriteiten aangevallen en lastiggevallen. De timing van de aanvallen is met name relevant gezien de aard van het onderzoek dat de NIK uitvoerde. De woordvoerder van de NIK bevestigde dat zij onderzoek deed naar het annuleren van de presidentsverkiezingen in 2020. Uit dit onderzoek bleek dat met betrekking tot de minister-president, leden van zijn regering, en een fonds van het ministerie van Justitie meldingen van misdrijven waren gedaan. Dit lijkt het vermoeden te versterken dat Pegasus in Polen voornamelijk voor politieke doeleinden is gebruikt[109].

PIS-LEDEN

76. Blijkbaar werd Pegasus gebruikt voor het "preventief afluisteren" van leiders en organisatoren van straatprotesten tegen de door PiS doorgevoerde hervormingen van het Grondwettelijk Hof. Het zijn echter niet alleen opposanten van de regeringspartij die mogelijk het slachtoffer zijn geworden van Pegasus. Volgens door Wyborcza geciteerde bronnen werd de voormalige PiS-partijwoordvoerder Adam Hofman in 2018 bespioneerd, waardoor hij een van de eersten was die het doelwit werd na de aankoop van de spyware. Hofman richtte R4S, een pr-bedrijf, op na uit PiS te zijn gezet[110] [111]. Naar verluidt is was de regerende partij alles behalve ingenomen met deze actie en heeft Hofman als surveillancedoelwit gekozen. Hij beweert dat de over hem verkregen informatie vervolgens gebruikt is in een tegen hem gerichte lastercampagne.

77. Bovendien zouden, volgens Wiadomości, voormalig PiS-parlementslid Mariusz Antoni Kaminski en voormalig PiS-minister van Overheidsfinanciën Dawid Jackiewicz het doelwit zijn geweest van aanvallen door de regering met Pegasus[112]. Mariusz A.

---

[108] Hoorzitting van de commissie PEGA, 19 januari 2023.
[109] Notes from Poland, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/, 7 februari 2022.
[110] https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true
[111] Rzeczpospolita, https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana, 11 oktober 2014.
[112] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym

Kaminski werd uit PiS gezet nadat hij tegelijk met Hofman in een schandaal verwikkeld was geraakt, Jackiewicz is echter nog steeds lid van de regeringspartij, ondanks zijn plotselinge terugtreding als minister[113].

78. In februari 2018 voerde de regeringspartij ook een vergelijkbare lastercampagne tegen de voormalige voorzitter van de werkgevers van de Republiek Polen, Andrzej Malinowski. In april 2022 legde hij tijdens een speciale zitting van een commissie van de Senaat een verklaring af over het feit dat zijn telefoon met Pegasus was gehackt om de informatie voor zijn publieke vernedering te verkrijgen[114]. Hij wees erop dat er met Pegasus WhatsApp- en sms-berichten van zijn telefoon waren gehaald en strategisch waren gebruikt om online haat tegen hem te verspreiden. Deze aanval was een wraakactie omdat hij het niet eens was met de regeringspartij en om alternatieve economische beleidsmaatregelen had verzocht.

SLOTOPMERKINGEN

79. Het misbruik van Pegasus in Polen moet worden gezien in de volledige context van de crisis van de rechtsstaat in het land, die begon in 2015 toen de regering, geleid door PiS, begon met de ontmanteling van het gerechtelijk apparaat en sindsdien systematisch de belangrijkste instellingen in het land heeft overgenomen, waarbij partijgetrouwen in alle strategische functies werden geïnstalleerd. De regeringspartij heeft doelbewust en systematisch de juridische, institutionele en politieke bouwstenen van dit systeem samengevoegd tot een coherent en zeer effectief kader, waarin het gebruik van Pegasus een integraal en vitaal onderdeel is van een systeem voor het controleren van de oppositie en critici van de regering voor politiek gewin. Het was bedoeld om de regerende meerderheid en de regering aan de macht te houden.

80. De ruimte voor surveillance in Polen is de afgelopen jaren enorm uitgebreid, waardoor waarborgen en toezichtsbepalingen zijn verzwakt of geschrapt. In de loop van de systematische en gerichte wetswijzigingen die door de regerende meerderheid tot stand zijn gebracht, zijn de rechten van slachtoffers tot een minimum beperkt en zijn rechts- en verhaalmiddelen in de praktijk zinledig gemaakt. Doeltreffende toetsing vooraf en achteraf, alsook onafhankelijk toezicht, zijn feitelijk afgeschaft. Leden van de Poolse regering en partijgetrouwen controleren direct of indirect de belangrijkste posities binnen het systeem. De met spyware geoogste informatie wordt gebruikt in lastercampagnes tegen critici en opposanten van de regering, via de door de overheid gecontroleerde staatsmedia. Het feit dat de Poolse regering de statuten op deze systematische en doelgerichte manier heeft uitgebreid in het kader van het nationale recht, blijft de rechtsgrondslag voor surveillance overtuigend in strijd met het Unierecht, de uitspraak van het Poolse Grondwettelijk Hof van 2014, en de grondrechten van de Poolse burgers. Op die manier werd onwettige surveillance die duidelijk in strijd is met het EU- en het nationale recht, in wezen gelegaliseerd.

I.B. Hongarije

[113] https://nextvame.com/dawid-jackiewicz-is-back-jaroslaw-kaczynski-confirms-the-reports/
[114] https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9668,1.html

81. Hongarije was een van de eerste landen die verwikkeld waren in het Europese spywareschandaal. In 2021 heeft het Pegasusproject aan het licht gebracht dat meer dan 300 Hongaren mogelijk het slachtoffer zijn geworden van het misbruik van Pegasus, onder wie politieke activisten, onderzoeksjournalisten, advocaten, ondernemers, een politicus van de oppositie, en een voormalige minister van de regering. Dit werd door Amnesty International bevestigd[115].

82. In februari 2023 heeft een delegatie van de commissie PEGA een bezoek gebracht aan Hongarije. Zij kwam tot de conclusie dat alles erop wijst dat er in Hongarije op grove wijze misbruik is gemaakt van spyware en dat de verklaring van de autoriteiten met betrekking tot de nationale veiligheid weinig overtuigend was. Er zijn sterke aanwijzingen dat mensen zijn bespioneerd met het doel om nog meer politieke en financiële controle te krijgen over de publieke sfeer en de media.

83. De commissie was ervan overtuigd dat de rechtsstaat en de fundamentele democratische normen in Hongarije ernstig zijn geschonden en dat de situatie in dit land tot de ergste in de EU behoort. Als gevolg van jaren van democratische achteruitgang lijken staatsinstellingen niet gericht op het dienen van burgers en het beschermen van hun rechten en vrijheden, maar op het nastreven van de politieke doelstellingen van de regering. De commissie riep de autoriteiten op een zinvol onderzoek naar misbruik toe te staan.

AANKOOP VAN PEGASUS

84. In 2017 heeft de nationale veiligheidscommissie van het Hongaarse parlement gestemd over de mogelijkheid voor de inlichtingendiensten van het land om bepaalde apparatuur aan te schaffen via de reguliere openbare aanbestedingsprocedure. Op verzoek van de speciale dienst voor de nationale veiligheid (Nemzetbiztonsági Szakszolgálat, NBSZ) heeft het Hongaarse parlement de aanschaf van geavanceerde spyware gesteund[116]. De procedure was echter geheim en in de verzoeken om goedkeuring werden het specifieke merk en type technologie niet vermeld[117].

85. Het Hongaarse ministerie van Binnenlandse Zaken kocht Pegasus voor 6 miljoen EUR via Communication Technologies Ltd. indirect van een onderneming van de NSO-groep in Luxemburg in 2017, kort nadat premier Viktor Orbán een ontmoeting had gehad met zijn Poolse ambtsgenoot Mateusz Morawiecki en de voormalige Israëlische premier Benjamin Netanyahu[118] [119]. Het Hongaarse ministerie van Binnenlandse Zaken heeft dit

[115] Euractiv, "Hungary employed Pegasus spyware in hundreds of cases, says government agency", *1 februari 2022*.
[116] Studie – "The use of Pegasus and equivalent spyware – The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware", Europees Parlement, directoraat-generaal Intern Beleid van de Unie, beleidsondersteunende afdeling C – Rechten van de burger en Constitutionele Zaken, 5 december 2022, beschikbaar op: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf
Direkt36, The inside story of how Pegasus was brought to Hungary, https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/
[117] PEGA-missie naar Hongarije, ontmoeting met leden van de nationale veiligheidscommissie van het Hongaarse parlement, 20-21 februari 2023.
[118] Financieele Dagblad, De wereld deze week: het beste uit de internationale pers. 7 januari 2022.
[119] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 Juli 2021.

pas bevestigd in november 2021, toen de voorzitter van de parlementaire commissie voor defensie en rechtshandhaving, Lajos Kósa, de aankoop van Pegasus door de Fidesz-regering erkende[120]. Kósa benadrukte echter nog altijd dat de spyware nooit tegen Hongaarse burgers was gebruikt[121].

86. De Hongaarse nationale autoriteit voor gegevensbescherming en vrijheid van informatie (NAIH) deed navraag naar de aanbestedingsprocedure voor de aankoop van de spyware en kreeg toegang tot het geheime contract met NSO. Tijdens de PEGA-missie naar Boedapest in februari 2023 verklaarde de voorzitter van de NAIH, Attila Péterfalvi, aanvankelijk dat het niet waar was dat de verstrekking van Pegasus aan de Hongaarse autoriteiten was beëindigd, wat zou betekenen dat Hongarije niet een van de twee EU-lidstaten was die waren geschrapt van de lijst van 14 waaraan NSO Pegasus verstrekt. Péterfalvi trok zijn verklaring later in en hield vol dat hij niet wist of NSO het gebruik van Pegasus in Hongarije al dan niet had beëindigd.

RECHTSKADER

87. In Hongarije is het kader voor de legale onderschepping van communicatie in het kader van een strafrechtelijk onderzoek vastgelegd in de Politiewet. Volgens de Politiewet kan de surveillance van particuliere burgers in een strafrechtelijk onderzoek alleen plaatsvinden met toestemming van de rechter. In zaken die verband houden met terrorisme verwijst de Politiewet echter naar de in de Wet Nationale Veiligheid genoemde onderzoekssurveillance[122]. Volgens deze bepaling hoeft voor het gebruik van deze technieken geen rechterlijke toestemming te worden gevraagd, maar is de minister van Justitie wel verantwoordelijk voor het verlenen van de toestemming[123]. In verzoeken om toestemming voor surveillance wordt niet vermeld welk type technologie zal worden gebruikt[124].

88. Overeenkomstig Wet CXXV van 1995 wordt het belang van de nationale veiligheid gedefinieerd als “het waarborgen van de soevereiniteit en de bescherming van de rechtsorde van Hongarije, en binnen dit kader”, wat een vrij ruime definitie is.

89. In een baanbrekende zaak (*Szabó en Vissy* v. *Hongarije*[125]) oordeelde het Europees Hof voor de Rechten van de Mens (EHRM) dat de nationale veiligheidswet niet voorzag in waarborgen die voldoende nauwkeurig, doeltreffend en volledig zijn voor het gelasten, uitvoeren en eventueel herstellen van surveillancemaatregelen. De Wet Nationale Veiligheid bevat geen wettelijk voorschrift dat verplicht personen die onder surveillance staan daarvan in kennis te stellen, en er wordt specifiek in bepaald dat de machtigende instantie de doelwitten niet mag inlichten van het feit dat zij worden bespioneerd[126]. Het

[120] DW, Hungary admits to using NSO Group’s Pegasus spyware”, 4 november 2021.
[121] DW, Hungary admits to using NSO Group’s Pegasus spyware”, 4 november 2021.
[122] Bureau van de Europese Unie voor de grondrechten (FRA), “National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary”, 26 september 2014.
[123] FRA, “National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary”, juridische update, 23 oktober 2017.
[124] PEGA-missie naar Hongarije, 20-21 februari 2023.
[125] Szabó en Vissy v. Hongarije, verzoekschrift nr. 37138/14, arrest van 12 januari 2016, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}
[126] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf

Europees Hof voor de Rechten van de Mens (EHRM) heeft in de zaak *Klass en anderen* v. *Duitsland*[127] ondubbelzinnig vastgesteld dat slachtoffers in kennis moeten worden gesteld. Bovendien zijn er geen doeltreffende rechts- en verhaalmiddelen in geval van misbruik en is er geen behoorlijk toezicht. De Hongaarse regering heeft tot nu toe geen van beide vonnissen uitgevoerd.

TOETSING VOORAF

90. Volgens de Wet Nationale Veiligheid is voor surveillance door de speciale diensten voor de nationale veiligheid (SNSS) met behulp van spyware in de meeste gevallen de toestemming nodig van de minister van Justitie en in een aantal specifieke gevallen van de rechter die door de president van de stedelijke rechtbank van Boedapest is aangewezen[128] [129]. Tegen deze besluiten kan geen beroep worden ingesteld en er is vrijwel geen toezicht op de procedure[130] [131].

91. Ondanks de ernst van een dergelijk besluit laat de huidige minister van Justitie, Judit Varga, wanneer zij niet beschikbaar is, de verantwoordelijkheid voor de toestemming voor spywaregebruik tegen burgers over aan de staatssecretaris van het ministerie van Justitie, een functie die momenteel wordt bekleed door Robert Repassy[132]. Dit werd door Repassy zelf bevestigd in een reactie die hij schreef op schriftelijke vragen over de kwestie[133]. Uit talrijke berichten blijkt dat Varga regelmatig de verantwoordelijkheid heeft overgedragen aan Repassy's voorganger Pál Völner, die in december 2021 gedwongen werd af te treden als gevolg van een groot corruptieschandaal[134]. Volgens berichten aanvaardde hij miljoenen Hongaarse forint in steekpenningen van een aantal prominente belanghebbenden in ruil voor gunstige beslissingen en benoemingen op belangrijke posten door Völner in zijn hoedanigheid van staatssecretaris[135].

92. Hoewel de minister van Binnenlandse Zaken Sándor Pintér erop aandringt dat deze machtigingsprocedure via de minister of de rechtbanken altijd en zonder uitzondering wordt gevolgd[136], maken de zwakke wettelijke bepalingen van de Wet Nationale Veiligheid het ook mogelijk dat de directeuren-generaal van de SNSS voorlopige toestemming verlenen voor het uitvoeren van surveillance zonder toestemming totdat

---

[127] Klass en anderen v. Duitsland, 6 september 1978, § 50, Series A, nr. 28.
[128] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, secties 56-58.
[129] Europa's PegasusGate: Countering Spyware Abuse – EPRS-verslag, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, juli 2022, blz. 20.
[130] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf secties 57 en 58.
[131] Verslag van de Europese Commissie over de rechtsstaat 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf , blz. 26.
[132] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium; Europa's PegasusGate: Countering Spyware Abuse, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, juli 2022, blz. 20.
[133] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese.
[134] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/.
[135] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye
[136] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.

officiële toestemming kan worden verleend. Hierdoor kunnen de SNSS zonder enige passende rechterlijke machtiging opereren zolang zij beweren dat de vertraging bij het verkrijgen van toestemming hun werking zou aantasten. In dergelijke gevallen kan de ongeoorloofde surveillance doorgaan[137].

93. De bij de wet vastgestelde wettelijke maximumduur van 90 dagen voor surveillance kan met nog eens 90 dagen worden verlengd op eenvoudig verzoek van een directeur-generaal aan de ambtenaar die toestemming geeft[138], die slechts is voorzien om de schijn van een wettelijke waarborg te wekken.

94. Bovendien bestaat de rol van de NAIH erin om toezicht te houden op alle surveillance door de geheime diensten. De voorzitter van de NAIH, Attila Péterfalvi, heeft altijd beweerd dat Pegasus alleen gebruikt was met het oog op de nationale veiligheid, wat onder de exclusieve bevoegdheid van nationale regeringen valt[139]. De NAIH controleerde de machtigingsprocedure echter alleen op technische gronden, om na te gaan of de gegevensverwerking rechtmatig was, maar ging niet in op de inhoud van het gebruik van Pegasus. De NAIH zag geen noodzaak om de doelwitten op te roepen om te getuigen, aangezien de NAIH toegang had tot alle relevante documenten. Alleen de door de minister van Justitie gemachtigde zaken zijn onderzocht, aangezien de NAIH geen onderzoek kan instellen naar machtigingen die door een rechter zijn verleend[140].Volgens Péterfalvi heeft het onderzoek van de NAIH geen illegale activiteiten of zaken in strijd met de verkoopvoorwaarden van de NSO-groep aan het licht gebracht[141].

95. Het hoofd van de NAIH wordt benoemd door de premier; hun onafhankelijkheid kan dus in twijfel worden getrokken[142]. Het EHRM oordeelde hierover in september 2022 in een zaak *Hüttl* v. *Hongarije*[143] die was aangespannen door de advocaat Tivadar Hüttl van het Hongaars verbond voor burgerlijke vrijheden toen de nationale veiligheidscommissie, nadat hij zou zijn afgeluisterd, besloot geen verder onderzoek in te stellen en er geen rechtsmiddelen meer beschikbaar waren[144]. Het EHRM verklaarde in zijn arrest duidelijk dat de NAIH, hoewel die bevoegd was om de acties van de geheime diensten te onderzoeken, niet in staat was onafhankelijk toezicht uit te oefenen op het gebruik van surveillance. Het Hof oordeelde dat de NAIH niet daartoe bevoegd was, aangezien de geheime diensten de toegang tot bepaalde documenten op basis van geheimhouding kunnen weigeren[145]. In een dergelijk geval is het aan de minister die verantwoordelijk is voor de geheime diensten om een audit uit te voeren, die op generlei

[137] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, sectie 59.
[138] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, sectie 58.
[139] HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21 november 2011.
[140] PEGA-missie naar Hongarije, 20 februari 2023.
[141] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 februari 2022.
[142] https://hclu.hu/en/pegasus-whats-new
[143] https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-219501%22]}
[144] https://tasz.hu/cikkek/valoszinusithetoen-lehallgattak-pert-nyert-strasbourgban-a-tasz-ugyvedje; https://hudoc.echr.coe.int/fre?i=001-219501
[145] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere

wijze als onafhankelijk toezicht kan worden beschouwd[146].

TOETSING ACHTERAF

96. In november 2021 hebben, op aandringen van de oppositie, de nationale veiligheidscommissie en de commissie voor defensie en veiligheid, in het parlement hoorzittingen gehouden over het gebruik van spyware in Hongarije en met name de vermeende praktijk van de regering om zich politiek gemotiveerd op burgerdoelwitten te richten. De regeringspartij had 4 van de 6 zetels in de nationale veiligheidscommissie en verhinderde elke zinvolle en democratische controle op het gebruik van Pegasus**.** De vertegenwoordigers van de regeringspartij bleven volhouden dat alle surveillance door de juiste instanties was toegestaan, en dat zij weigerden de vraag te beantwoorden of journalisten dan wel politici het doelwit waren geweest. Zij weigerden ook commentaar te geven op het feit dat de machtigingen door de minister van Justitie werden gedelegeerd aan de staatssecretaris, Pál Völner, tegen wie momenteel een onderzoek loopt inzake beschuldigingen van corruptie en machtsmisbruik. Zij wezen ook verzoeken van oppositieleden af om een diepgaand onderzoek in te stellen en de veiligheidsdiensten te bezoeken om individuele agenten te ondervragen. Belangrijke doelwitten, zoals Zoltán Varga en Szabolcs Panyi, werden door de commissie niet gehoord. In augustus 2021 werd alleen een algemeen pro-formaonderzoek uitgevoerd, omdat dit de enige formule was die steun kreeg van de meerderheid[147]. Het is echter niet mogelijk te weten wat er precies is gezegd, aangezien de regerende partij de notulen van de vergadering tot 2050 heeft geclassificeerd[148].

97. Een NAIH-onderzoek werd gestart naar aanleiding van beschuldigingen door ten minste tien advocaten, de voorzitter van de Hongaarse orde van advocaten, en ten minste vijf journalisten die waren bespioneerd[149]. Het resulterende verslag werd op 31 januari 2022 gepubliceerd en hierin werd geconcludeerd dat het gebruik van Pegasus om strikte redenen van nationale veiligheid was.

98. Evenzo heeft het Hongaarse openbaar ministerie op 15 juni 2022 zijn onderzoek naar de spionage afgerond en geconcludeerd dat geen ongeoorloofde surveillance had plaatsgevonden.

99. Gezien het feit dat de machtigingsbevoegdheid bij het ministerie van Justitie berust en de door Fidesz gesteunde procureur-generaal, Péter Polt, in 2019 voor nog eens negen jaar werd herkozen (terwijl hij tot op dat moment al voor een totale periode van 15 jaar over twee verschillende ambtstermijnen had gediend), kan echt toezicht op de regering in twijfel worden getrokken.

100. Er is geen steun in het Hongaarse kader voor corruptiebestrijding in reactie hierop, aangezien het ministerie van Binnenlandse Zaken – dat oorspronkelijk Pegasus van de

[146] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere

[147] PEGA-missie naar Hongarije, ontmoeting met leden van de nationale veiligheidscommissie van het Hongaarse parlement, 20 februari 2023.

[148] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.

[149] Verslag van de Commissie over de rechtsstaat 2022, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, blz. 26.

NSO-groep kocht – verantwoordelijk is voor de coördinatie van alle beleid en toezicht voor corruptiebestrijding[150].

VERHAALSMOGELIJKHEDEN

101. Toen het Pegasusschandaal in Hongarije uitbrak, behoorden journalisten tot een van de groepen die het vaakst het doelwit waren van de regering. Naar aanleiding hiervan heeft begin 2022 een groep van zes journalisten en activisten in Hongarije gerechtelijke procedures ingeleid bij de Hongaarse autoriteiten, de Commissie en het EHRM. Het Hongaars verbond voor burgerlijke vrijheden (hierna "het verbond" genoemd) vertegenwoordigt de journalisten Brigitta Csikász, Dávid Dercsényi, Dániel Németh en Szabolcs Panyi, naast Adrien Beauduin, een Belgisch-Canadese PhD-student en activist. De zesde eiser heeft ervoor gekozen anoniem te blijven. Het verbond werkt ook samen met Eitay Mack in Israël die een verzoek zal indienen bij de procureur-generaal om een onderzoek in te stellen naar de NSO-groep[151].

102. Deze zaak wordt belemmerd door tal van technische aspecten in de Hongaarse rechtbanken. Aangezien er op dit gebied niet veel jurisprudentie bestaat, zijn de procedures onduidelijk. Zo zijn er bijvoorbeeld problemen met betrekking tot de rechtsbevoegdheid gerezen. Zulke acties en enorme vertragingen worden voornamelijk beschouwd als pogingen om de zaak op grond van een technische of procedurele fout af te voeren.

103. Ook de toegang tot informatie is een ernstig probleem. Om toegang te vragen tot de bestanden met alle gegevens die over één burger zijn verzameld, moet men de exacte naam weten van het bestand waarop het verzoek betrekking heeft, informatie die bijna onmogelijk te verkrijgen is. Nu de verzoeken van de zes door het verbond vertegenwoordigde partijen onvermijdelijk door het Hooggerechtshof zijn afgewezen, heeft het verbond het Grondwettelijk Hof verzocht deze praktijk en de uitspraak van het Hongaarse Hooggerechtshof ongrondwettig te verklaren. In 2021 verwierp het Grondwettelijk Hof echter het verzoek van het verbond.

104. Naast zijn rechtszaken voor de rechtbanken heeft het verbond ook andere wegen bewandeld om toegang te krijgen tot de gegevens van zijn zes cliënten. Er werd een administratieve procedure ingeleid en aanvaard uit hoofde van de wet gerubriceerde gegevens en de wet bescherming persoonsgegevens. Er zal echter in elk afzonderlijk geval een evaluatie van een jaar door het bureau voor de bescherming van de grondwet plaatsvinden, voordat resultaten bekend zullen worden gemaakt[152]. Daarnaast zijn de spywareaanvallen aan de commissaris voor grondrechten (ombudsman) gemeld. Het Grondwettelijk Hof heeft bepaald dat het de verantwoordelijkheid van de ombudsman is om misbruiken door de geheime diensten te onderzoeken[153].

105. In een andere poging om enige transparantie te bewerkstelligen, heeft het verbond om

[150] Verslag van de Commissie over de rechtsstaat 2022, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, blz. 10.
[151] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state, *28 januari 2022*.
[152] https://hclu.hu/en/pegasus-case-hungarian-procedures
[153] https://hclu.hu/en/pegasus-whats-new

toegang gevraagd tot de gegevens die worden verzameld en verwerkt als gevolg van het hacken van de zes doelwitten in een proces dat buiten het gerechtelijk systeem wordt uitgevoerd. Het recht op deze informatie bestaat echter slechts zolang het verstrekken van de gegevens aan de betrokkenen geen afbreuk doet aan de nationale veiligheid[154]. Dit vormt weer een ander voorwendsel voor de Hongaarse autoriteiten om weer terug te vallen op redenen van nationale veiligheid[155]. Tot dusver heeft het bureau voor de bescherming van de grondwet 270 verzoeken om vrijheid van informatie, die het verbond tussen 2018 en mei 2022 heeft ingediend, afgewezen[156].

POLITIEKE CONTROLE

106. In Hongarije staat het gebruik van surveillance onder volledige politieke controle. Het Fidesz-regime onder leiding van Orbán heeft een systeem gecreëerd waarin advocaten, journalisten, politieke tegenstanders en maatschappelijke organisaties als doelwit kunnen worden gekozen.

107. De minister van Binnenlandse Zaken was in eerste instantie verantwoordelijk voor de aankoop van Pegasus-spyware en de minister van Justitie blijft belast met het toestaan van het gebruik ervan. Het Hongaarse wetgevingskader inzake de surveillance van zijn burgers is herhaaldelijk ontoereikend bevonden. De regeringspartij zal echter geen stappen ondernemen om het te veranderen, omdat het hun eigen agenda uitkomt.

108. De premier kiest het hoofd van de NAIH, het orgaan dat verantwoordelijk is voor het onafhankelijke toezicht op het gebruik van Pegasus door de geheime diensten. Aangezien hij een politiek benoemde persoon is, is onafhankelijk toezicht afwezig. Dit soort politieke benoemingen zijn Hongarije en de regering-Fidesz niet vreemd. De regering heeft partijgetrouwen systematisch in bestuursfuncties aangesteld in organen zoals het Grondwettelijk Hof, het Hooggerechtshof, de Rekenkamer, het openbaar ministerie, de Nationale Bank van Hongarije en de Nationale Verkiezingscommissie[157]. Dit zorgt ervoor dat elke instelling die wordt opgericht met de bedoeling toezicht op de uitvoerende macht uit te oefenen, haar rol niet onafhankelijk kan vervullen[158].

109. Wat het praktische aspect van surveillance met behulp van spyware betreft, spelen telecommunicatiebedrijven een belangrijke rol. Er zijn meerdere gevallen van toestellen van doelwitten die werden besmet via links die per sms werden verzonden, en de schat aan gegevens waartoe telecommunicatiebedrijven toegang hebben, is zeer aantrekkelijk voor wie wil spioneren. In het geval van Hongarije is de situatie gevaarlijker geworden omdat de Hongaarse regering Vodafone Hongarije onlangs heeft overgenomen[159]. Met steun van de Hongaarse regering heeft het bedrijf 4iG 51 % van Vodafone via een

---

[154] https://hclu.hu/en/pegasus-case-hungarian-procedures
[155] https://hclu.hu/en/pegasus-whats-new
[156] https://hclu.hu/en/pegasus-whats-new
[157] Martin, J en Ligeti, M., "Hungary. Lobbying, State Capture and Crony Capitalism", Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. en Harris, P. (eds.), Springer, 2017, blz. 177-193, op blz. 178.
[158] Martin, J. en Ligeti, M., "Hungary. Lobbying, State Capture and Crony Capitalism", Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. en Harris, P. (eds.), Springer 2017, blz. 177-193 op blz. 178.
[159] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 augustus 2022.

dochteronderneming overgenomen. Daarnaast heeft de Hongaarse regering 49 % van de aandelen van Vodafone via een ander bedrijf overgenomen. De banden tussen 4iG en de regering zijn duidelijk. De huidige directeur van het bedrijf was een vertrouweling van de Hongaarse oligarch Lőrinc Mészáros, een jeugdvriend van Viktor Orbán. Dankzij de totale overname ter waarde van 1,7 miljard EUR krijgt de regering gemakkelijke en directe toegang tot de gegevens van meer dan 3 miljoen klanten[160]. Bovendien zal de staat dankzij deze overname een toegangspunt hebben tot het decennia oude wereldwijde berichtensysteem dat SS7 heet[161]. Dit systeem stelt mobiele operators in staat om gebruikers over de hele wereld met elkaar te verbinden. De Hongaarse staat zal ook in staat zijn een dergelijk toegangspunt verder te leasen, zoals het geval was voor Rayzone[162].

DE DOELWITTEN

110. De bevindingen van het Pegasusproject maakten melding van telefoonnummers van meer dan 300 personen[163]. Tot deze personen behoorden ten minste vijf journalisten, tien advocaten, de tot de oppositie behorende burgemeester van Gödöllő, een werknemer van de oppositiepartij, alsook activisten en prominente ondernemers[164]. Niemand van hen was echter het voorwerp van een strafrechtelijk onderzoek of was in beschuldiging gesteld. Hoewel het voorkomen van telefoonnummers op deze lijst niet noodzakelijk betekent dat die telefoons daadwerkelijk zijn gehackt, biedt het een onthullend inzicht in de methodische en systematische acties en houding van Orbáns regering tegenover grondrechten en mediavrijheid. Na die periode in 2021 is gebleken dat een aantal doelwitten inderdaad met behulp van spyware zijn gehackt. Zodra het spywareschandaal in Hongarije uitbrak, was het overduidelijk dat het optreden van de regering politiek gemotiveerd was.

SZABOLCS PANYI

111. Het hacken van de telefoon van journalist en redacteur Szabolcs Panyi vond plaats in de periode dat hij werkte voor Direkt36. Aangezien het een van de weinige resterende onafhankelijke nieuwsbronnen in Hongarije is, vormt Direkt36 een belangrijk doelwit van de regerende partij. Panyi is een bekende, goed aangeschreven journalist, waaruit volgt dat, afgezien van het verzamelen van belangrijke informatie rechtstreeks van Panyi zelf, veel van de contacten en bronnen op zijn telefoon waardevolle bijvangst zouden zijn voor de regering.

112. Amnesty International bevestigde dat Panyi's telefoon in 2019 over een periode van

---

[160] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 augustus 2022; Volkskrant, Orbán verstevigt met overname Vodafone Hongarije grip op telecommunicatie, critici uiten zorgen.
[161] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands, 16 december 2020.
[162] https://www.haaretz.com/israel-news/tech-news/2020-12-17/ty-article/israeli-spy-tech-firm-tracked-mobile-users-around-the-world-investigation-suggests/0000017f-e76b-da9b-a1ff-ef6f847c0000
[163]Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[164] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021 en Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.

zeven maanden consequent werd gehackt[165]. Deze aanvallen waren doelgericht en kwamen vaak voor in een tijd waarin Panyi de regering had gevraagd commentaar te geven op bepaalde kwesties. Een specifiek en zorgwekkend voorbeeld hiervan vond plaats op 3 april 2019. Panyi nam contact op met de regering met het verzoek om commentaar op het artikel dat hij had geschreven over de verhuizing van een Russische bank naar de Hongaarse hoofdstad, wat een spraakmakend verhaal was, aangezien er vragen rezen of de bank niet in feite een dekmantel was voor de Russische inlichtingendiensten[166]. Amnesty International bevestigde dat Panyi's telefoon de dag nadien werd gehackt en stelde bovendien dat er elf andere soortgelijke gevallen van hacking in de onmiddellijke periode na een verzoek om commentaar van Orbáns regering hadden plaatsgevonden[167]. Dat komt erop neer dat meer dan de helft van Panyi's verzoeken het doelwit waren binnen die periode van zeven maanden[168].

113. De autoriteiten hebben geveinsd niet op de hoogte te zijn van de spionage van Panyi en zullen bevestigen noch ontkennen dat zij verantwoordelijk waren. De regering heeft Panyi echter eerder al publiekelijk aangevallen, waarbij Orbáns woordvoerder beweerde dat hij een fanatieke politieke activist was en hem beschuldigde van "Orbánofobie" en "Hongarofobie"[169]. Dit is een flagrante poging om Panyi in diskrediet te brengen en zowel zijn bronnen als hemzelf af te schilderen als de "vijand" via de eigen door de staat gecontroleerde media van de regering.

114. Na een onderzoek van Panyi naar het Hongaarse makelaarsbedrijf Communication Technologies Ltd., via hetwelk Pegasus werd gekocht, klaagde het bedrijf hem aan[170].

ZOLTÁN VARGA

115. Als CEO en voorzitter van Central Media Group is Zoltán Varga eigenaar van de grootste resterende onafhankelijke nieuwssite van Hongarije, 24.hu. Nadat de regering van Orbán in 2020 het initiatief had genomen voor de overname van de belangrijkste concurrent, Index.hu, bleef Varga over als laatste luis in de pels van de regerende partij[171].

116. Fidesz voert al geruime tijd een lastercampagne tegen Varga via de door de regering gecontroleerde media om zowel zijn persoonlijke publieke figuur als de uitgeverij – ondanks haar populariteit met een publiek van meer dan 7,5 miljoen per maand – in diskrediet te brengen[172]. Varga beweert meermaals te zijn gelokt en bedreigd om tot verkoop over te gaan, ook door middel van aanbiedingen van royale subsidies voor

[165] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[166] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[167] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[168] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[169] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[170] PEGA-missie naar Boedapest, 20-21 februari 2023.
[171] https://www.mapmf.org/alert/25319
[172] Politico, https://www.politico.eu/article/viktor-orban-bent-on-muzzling-independent-press-hungarian-media-mogul-warns-index-24-hu-news-sites/, 25 juli 2020.

staatsreclame in ruil voor het aanstellen van door de regering gekozen redactiemedewerkers[173]. Varga vermoedde voor het eerst dat zijn telefoon met Pegasus was besmet toen de oproep werd afgespeeld terwijl hij nog midden in het gesprek zat. Varga vermoedde voor het eerst dat zijn telefoon met Pegasus was besmet toen de oproep werd afgespeeld terwijl hij nog midden in het gesprek zat. Vervolgens werd in 2021 door Amnesty International ontdekt dat Varga inderdaad hoogstwaarschijnlijk door Pegasus was gehackt, maar het kon niet worden bevestigd omdat de telefoon sindsdien was vervangen[174].

117. Kort na de verkiezingen van 2018 probeerde de herkozen Orbán indirect tot bij Varga te komen. Na een door Varga in het voorjaar van 2018 georganiseerd diner om te praten over de overname van de media door de regering – waar ook Attila Chikán, een voormalige Fidesz-minister die nu een Orbán-criticus is, aanwezig was – werd vastgesteld dat alle aanwezigen te boek stonden als kandidaten voor surveillance[175]. Vervolgens werd bevestigd dat één gast ten tijde van het diner was gehackt, terwijl andere telefoons sporen van potentiële Pegasus-hacks vertoonden, maar geen bewijs van succesvolle besmetting[176]. De hacking werd terdege bevestigd door een aan de regering verbonden kennis van Varga die in het gesprek direct naar het diner verwees en waarschuwde voor de sociale omgang met mensen die “gevaarlijk” zouden kunnen zijn[177].

118. Varga is ook het voorwerp van traditionele surveillance geweest. Afluisterpraktijken in de zakelijke omgeving, auto’s die langzaam rond zijn huis rijden, helikopters die boven zijn huis hangen en indringers in zijn tuin hebben hem ertoe gebracht fulltime beveiliging in te zetten.

119. In oktober 2022 werd een strafrechtelijke aanklacht tegen Varga ingediend. Hij werd opgeroepen voor verhoor door de politie en slechts enkele minuten later berichtten de regeringsgezinde media er al over[178].

ADRIEN BEAUDUIN

120. Adrien Beauduin verscheen in 2018 op de radar van het regime van Orbán toen hij een doctoraat in genderstudies aan de Midden-Europese Universiteit aan het afronden was. De regering probeerde destijds deze door George Soros opgerichte instelling uit Hongarije te doen vertrekken, en daarmee het volledige vakgebied genderstudies[179]. Na het bijwonen van een manifestatie in Boedapest werd Beauduin gearresteerd in wat wordt gezien als een politiek gemotiveerde actie, en werd hij aangeklaagd wegens

[173] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[174] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[175] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[176] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[178] PEGA-missie naar Boedapest, 20-21 februari 2023.
[179] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.

geweldpleging jegens een politieambtenaar, iets wat hij ten stelligste ontkent[180]. Bericht werd dat er in wezen geen bewijs tegen Beauduin was en dat het overgelegde bewijsmateriaal letterlijk was overgenomen van een getuigenverklaring van de politie in een andere zaak[181]. In 2020 werd de strafzaak tegen Adrien Beauduin, die in de zaak door het verbond werd vertegenwoordigd, beëindigd.

121. Het zogenaamde pro-immigratie-Soros-netwerk werd door regeringsvertegenwoordigers publiekelijk veroordeeld voor het organiseren van "gewelddadige demonstraties in Boedapest"[182]. Vervolgens werden sporen van Pegasus gevonden op de telefoon van Beauduin, maar het was niet mogelijk te bevestigen of er een succesvolle besmetting was geweest.

122. Aangezien Beauduin een Belgisch staatsburger was die ten tijde van deze incidenten in Hongarije woonde, kan het belang van de grensoverschrijdende dimensie in dit geval niet voldoende worden benadrukt. Het is van cruciaal belang omdat het van invloed is op de soevereine rechten van EU-burgers, zoals het vrije verkeer en het recht om te werken. De Commissie beschikt over een klachtenprocedure waarop eenieder beroep kan doen als zijn rechten uit hoofde van het Handvest zijn geschonden. Adrien Beauduin diende een dergelijke klacht in op 24 januari 2022, maar zeven maanden later, in een aan zijn advocaat gerichte brief van 17 augustus 2022, beweerde de Commissie niet te beschikken over de bevoegdheid om tussen te komen[183].

ILONA PATÓCS

123. Advocaat Ilona Patócs was in de zomer van 2019 een vermeend slachtoffer van Pegasus-surveillance, in de tijd dat zij een cliënt vertegenwoordigde in een belangrijke, langdurige moordzaak[184]. Vanwege het type mobiele toestel dat zij gebruikte, was het echter niet mogelijk om te bevestigen of de hack geheel geslaagd was en wanneer deze precies heeft plaatsgevonden. Haar cliënt, István Hatvani, had al zeven jaar vastgezeten in verband met een moordzaak, waarin, volgens Patócs, sprake was van een "politiek gemotiveerde" veroordeling[185]. Hoewel een andere partij naderhand de verantwoordelijkheid voor de moord op zich heeft genomen, is Hatvani door het Hongaarse Hof van Beroep naar de gevangenis teruggezonden om zijn oorspronkelijke straf uit te zitten. In de lijst van mogelijke doelwitten van Pegasus zijn de telefoonnummers van veel andere advocaten opgenomen, waaronder de voorzitter van de Hongaarse orde van advocaten, János Bánáti[186]. Met name deze keuze van doelwitten duidt op een kennelijke minachting van de regering voor het advocaat-cliënt-

[180] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[181] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[182] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[183] https://tasz.hu/a/files/220816-Complaint-unlawful-surveillance.pdf
[184] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.
[185] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.
[186] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.

privilege.

GYÖRGY GÉMESI

124. György Gémesi, de burgemeester van Gödöllő, werd eind 2018 ook het doelwit van de Pegasus-spyware, net toen hij onder zware druk van de regering stond en onbekende personen in zowel zijn huis als in de huizen van zijn kinderen inbraken. Tegelijkertijd met de tot de oppositie behorende burgemeester werd eind 2018 ook een aan de regering verbonden kennis van Gémesi als doelwit van de spyware gekozen. Daarnaast stonden ook twee telefoonnummers die waren verbonden aan zijn partijgenoten en voormalig burgemeester van Gémesi op de lijst.

BRIGITTA CSIKÁSZ

125. Tijdens haar surveillance deed Brigitta Csikász, een van de meest ervaren misdaadverslaggevers van Hongarije, onder meer onderzoek naar het misbruik van fondsen van de Europese Unie. Uit het onderzoek van Csikász bleek dat de Hongaarse autoriteiten, ondanks dat het Europees Bureau voor fraudebestrijding (OLAF) de alarmklok luidde, niet de wil of het vermogen hadden om de verdachte besteding van EU-geld te vervolgen. Dit bewijst eens te meer dat het openbaar ministerie de jure onafhankelijk en zeer hiërarchisch is, maar dat de hoofdaanklager de facto nauw verbonden is met de regeringspartij en de premier.

126. De voorzitter van de Hongaarse orde van advocaten, János Bánáti, strafrechtadvocaten en verschillende andere advocaten werden ook het doelwit van Pegasus.

ANDERE DOELWITTEN

127. Ook personen in de kring van de regerende partij zijn het doelwit geweest van spyware. Het onafhankelijke Hongaarse kanaal Direkt36 meldde in december 2021 dat het hoofd van de beveiligingsdienst en de persoonlijke bodyguard van János Áder, de president en nauw verbonden met Orbán, werd gehackt met Pegasus-spyware. Volgens Direkt36-journalist en slachtoffer van spyware Szabolcs Panyi is dit soort spionage voornamelijk het gevolg van de groeiende paranoia van de Hongaarse premier. Cecília Szilas, voormalig ambassadeur van Hongarije in China, werd het doelwit van Pegasus, kort voordat zij senior adviseur werd van Viktor Orbán. Attila Aszódi, staatssecretaris van de regering-Orbán, verantwoordelijk voor de bouw en ontwikkeling van de door Roszatom te bouwen Paks II-kerncentrale, was ook het doelwit van de Pegasus-spyware. Hij werd een doelwit in 2018, toen hij deel uitmaakte van de regering, maar was in een conflict verwikkeld met zijn meerdere, minister János Süli.

128. Daarnaast werden zowel de zoon als de advocaat van een van Orbáns oudste vrienden, Lajos Simicska, met Pegasus gehackt[187]. Simicska, die eerst een goede vriend van Orbán was, was nu zijn tegenstander. Hij was bezig met de verkoop van zijn mediaconsortium, hetgeen de vete grotendeels had aangewakkerd na de

[187] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.

verkiezingsoverwinning van Orbán in 2018 toen deze surveillance via naasten plaatsvond[188]. Simicska zelf was geen doelwit om de eenvoudige reden dat hij geen smartphone gebruikt, waardoor besmetting door spyware zoals Pegasus onmogelijk is[189]. Ajtony Csaba Nagy, de advocaat van Simicska, vermoedde een besmetting toen zijn gesprek met Simicska tijdens een telefoontje werd afgespeeld. Later werden die vermoedens ogenschijnlijk bevestigd toen informatie die alleen tijdens die oproepen was besproken, in de Hongaarse media verscheen[190]. Aangezien de meeste nieuwskanalen in Hongarije staatseigendom zijn, is het waarschijnlijk dat de regering de informatie rechtstreeks aan de media zelf heeft verstrekt.

SPYWAREBEDRIJVEN

129. De Hongaarse regering heeft niet alleen Pegasus-spyware aangeschaft en tegen haar bevolking gebruikt, maar heeft ook andere bedrijven op de inlichtingenmarkt, zoals Black Cube en Cytrox, welkom geheten. Black Cube is een Israëlische privé-inlichtingendienst die bestaat uit voormalige werknemers van de Mossad, het Israëlische leger en de Israëlische inlichtingendiensten[191]. Op de website van het bedrijf wordt Black Cube beschreven als een "creatieve inlichtingendienst" die "oplossingen op maat" aanbiedt voor "complexe zakelijke uitdagingen en geschillen"[192]. Black Cube was betrokken bij een aantal hackingschandalen, onder meer in de VS en in Roemenië[193]. Criticallylinks zijn ook ontdekt met de NSO-groep en Pegasus-spyware. Wat betreft het inhuren van Black Cube door NSO om tegenstanders te observeren, heeft, na veel publieke druk op NSO, de voormalige directeur van NSO, Shalev Hulio, toegegeven dat Black Cube voor ten minste één situatie op Cyprus is ingehuurd.

130. Black Cube werd tijdens de verkiezingen van 2018 actief in Hongarije, toen het diverse ngo's en personen bespioneerde die mogelijke banden hadden met George Soros. Zij deden hiervan verslag aan Orbán, zodat hij hun activiteiten met een lastercampagne in een kwaad daglicht kon stellen[194]. Tot de doelwitten behoorden onder meer advocate en lid van het Hongaarse Helsinki-comité, de vooraanstaande ngo op het gebied van de mensenrechten, Marta Pardavi[195]. De informatie die de surveillance van deze personen en ngo's opleverde, verscheen niet alleen in de door de Hongaarse staat gecontroleerde

[188] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[189] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[190] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[191] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 oktober 2019.
[192] https://www.blackcube.com/
[193] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[194] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[195] *Reuters*, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC, 16 december 2021.

media, maar ook in de Jerusalem Post[196].

131. Nog een band met Hongarije wordt gevormd door Cytrox Holdings Zrt., dat op een adres in Boedapest staat ingeschreven. Cytrox, de maker van Predator-spyware, werd oorspronkelijk opgericht in Noord-Macedonië, voordat het werd overgenomen door WiSpear, dat nu deel uitmaakt van de door Tal Dilian gerunde Intellexa-alliantie.

SLOTOPMERKINGEN

132. Het gebruik van Pegasus in Hongarije lijkt onderdeel te zijn van een berekende en strategische campagne om de persvrijheid en de vrijheid van meningsuiting door de regering lam te leggen[197]. De regering heeft deze spyware gebruikt om gemakkelijk en zonder vrees voor verhaal een regime van pesterijen, chantage, bedreigingen en druk tegen onafhankelijke journalisten, media, politieke tegenstanders en maatschappelijke organisaties in te voeren. De controle van de regering over bijna alle Hongaarse offlinemedia en omroepen stelt haar in staat haar eigen versie van de waarheid op te dringen, waardoor veel van de door onafhankelijke media uitgeoefende publieke controle de Hongaarse burgers niet bereikt.

133. De wet die het gebruik van onderschepping toestaat is veel meer een controle- en machtsinstrument voor de regering dan een schild voor de rechten en de privacy van de burgers, en is een van de zwakste in Europa[198] [199]. Het systeem is een flagrante schending van de Europese voorschriften en normen die door het Europees Verdrag tot bescherming van de rechten van de mens en de uitspraken van het EHRM zijn vastgesteld voor de surveillance van burgers[200]. De regering daarentegen houdt vol dat zij in alle gevallen wettig heeft gehandeld en zich volledig aan de wet houdt[201] [202]. Hoewel de regering constant terugvalt op redenen van "nationale veiligheid"[203], zijn haar beweringen dat de doelwitten een bedreiging vormen voor de nationale veiligheid niet geloofwaardig.

I.C. Griekenland

134. De commissie PEGA heeft Griekenland in november 2022 bezocht in het kader van een gezamenlijke missie Griekenland-Cyprus. De leden ontmoetten minister van Buitenlandse Zaken Giorgos Gerapetritis en bespraken spraakmakende

---

[196] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[197] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[198] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[199] DW, "Pegasus scandal: In Hungary, journalists sue state over spyware", 29 januari 2022.
[200] Zie onder meer Roman Zakharov v. Rusland [GK], nr. 47143/06, ECHR 2015 39; Klass en anderen v. Duitsland, 6 september 1978, § 50, Series A nr. 28. 40; Prado Bugallo v. Spanje, nr. 58496/00, § 30, 18 februari 2003; Liberty en anderen v. Verenigd Koninkrijk, nr. 58243/00, § 62, 1 juli 2008.
[201] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.
[202] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 februari 2022.
[203] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1 februari 2022.

surveillancezaken en de bredere context van pluralisme in de media en de rechtsstaat in Griekenland. Ze hebben er ook onderzoeksjournalisten, leden van het Griekse parlement, de voorzitter van de Griekse gegevensbeschermingsautoriteit (APDPX), vertegenwoordigers van de ADAE en ngo's, en mensenrechtenverdedigers ontmoet.

135. Het bezoek bracht aan het licht dat er meer inspanningen moeten worden geleverd om de transparantie te waarborgen. De beschuldigingen van misbruik van surveillance en het gebruik van spyware moeten grondig worden onderzocht en waar nodig bestraft. Alle nodige waarborgen moeten worden ingebouwd en de hervormingen moeten de transparantie verbeteren en zorgen voor een passend rechterlijk toezicht op het gebruik van surveillance. Het bezoek bevestigde ook dat er duidelijke regels nodig zijn om het gebruik van de nationale veiligheid als reden voor surveillance te beperken, te zorgen voor behoorlijk rechterlijk toezicht en een gezonde, pluralistische mediaomgeving te waarborgen.

136. In 2022 werd Griekenland opgeschrikt door een reeks berichten over het gebruik van spyware, wat volgens de Griekse wet illegaal is. Op 26 juli 2022 diende het lid van het Europees Parlement en leider van de Griekse oppositiepartij PASOK Nikos Androulakis een klacht in bij het parket van het Hooggerechtshof over pogingen om zijn mobiele telefoon met Predator-spyware te infecteren[204]. De poging tot infectie met spyware werd tijdens een controle van de telefoon van de heer Androulakis door de IT-dienst van het Europees Parlement ontdekt[205]. Volgens de forensische analyse van de IT-dienst vonden de hackpogingen plaats in de periode dat de heer Androulakis kandidaat was voor het leiderschap van de oppositiepartij. Deze onthulling bracht de in april en mei 2022 door financieel journalist Thanasis Koukakis ingediende klachten over de besmetting van zijn telefoon met Predator onder de aandacht. Zijn besmetting werd bevestigd door Citizen Lab. In september beweerde Christos Spirtzis, voormalig minister van Infrastructuur en parlementslid voor de partij Syriza[206], ook het doelwit te zijn geweest van de Predator-spyware. Hoewel zijn mobiele telefoon niet officieel werd gecontroleerd, deelde de heer Spirtzis de ontvangen links met twee technici die mondeling bevestigden dat hij een doelwit was geweest[207]. Bovendien werd later die maand bekend dat de Griekse nationale inlichtingendienst (EYP) vermoedelijk spyware had ingezet tegen twee van zijn eigen werknemers[208]. Op 5 en 6 november onthulden de Griekse media een lijst van 33 doelwitten van Predator, allemaal hooggeplaatste personen[209]. De lijst – noch bevestigd noch ontkend door de regering of door de doelwitten – bevat namen van mensen die werkzaam zijn in de politiek, het bedrijfsleven en de media in Griekenland. De gevolgen van de vermeende surveillance van personen die op de lijst staan, zouden veel groter kunnen zijn, aangezien al hun respectieve contacten en connecties indirect ook in de spionageoperatie kunnen worden "betrapt", met inbegrip van hun contacten in EU-organen. Dat spyware veel wordt gebruikt, was naar verluidt al te lezen in het Meta-verslag van 2021, dat in de bijlage melding maakt van 310 links naar nepwebsites van het spywarebedrijf Cytrox, waarvan

[204] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader.
[205] Tagesspiegel, Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.
[206] *Reuters*, One more Greek lawmaker files complaint over attempted phone hacking.
[207] https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias
[208] EfSyn, Targeting the disliked.
[209] Documento, Apocalypse: They Watched – This Sunday in Document.

alleen al 42 waren geplaatst met de bedoeling om doelwitten in Griekenland te misleiden[210] [211]. Eind november 2022 publiceerde de Griekse krant *Documento* een lijst van 498 URL's die waren gebruikt om te spioneren met behulp van Predator-spyware. Sommige URL's waren identiek aan die in het Meta-verslag van 2021[212]. Op 28 februari 2023 bevestigde de voorzitter van de APDPX dat 300 tekstberichten in verband met Predator-spyware naar ongeveer honderd apparaten waren verzonden. De voorzitter van de ADAE verklaarde bovendien dat de ADAE verschillende klachten in behandeling heeft genomen, twee gevallen van het gebruik van Predator heeft vastgesteld en een bankrekeningnummer van een persoon achter de valse tekstberichten heeft geïdentificeerd. Het ADAE-onderzoek naar nieuwe klachten loopt[213].

137. In augustus 2022 gaf de Griekse regering toe dat de EYP de heren Androulakis en Koukakis inderdaad had gemonitord, maar ontkende dat het ooit Predator-spyware had gebruikt of aangekocht. Daarnaast kwamen in deze periode andere gevallen van surveillance door de EYP aan het licht, zoals die van journalist Stavros Malichoudis[214]. Tot op heden zijn de officiële redenen voor de surveillance niet bekendgemaakt.

138. Op 8 augustus 2022 gaf premier Mitsotakis een videoboodschap uit waarin hij dubbelzinnig stelde dat de surveillance van de heer Androulakis "legaal" maar "politiek onaanvaardbaar" was. Hierbij vermeldde hij noch de surveillance van de heer Koukakis noch de andere vermeende gevallen. Ook verklaarde hij niet op de hoogte te zijn geweest van de surveillance en dat hij, als hij het had geweten, het niet zou hebben toegestaan[215]. Volgens de officiële verklaring van de regeringswoordvoerder Yiannis Oikonomou heeft minister van Buitenlandse Zaken Giorgos Gerapetritis, zodra de premier op de hoogte was van de "legale onderschepping" van de heer Androulakis, getracht de heer Androulakis onder vier ogen volledig te informeren over de redenen voor zijn surveillance[216]. De heer Androulakis wees het aanbod om geïnformeerd te worden af, met de opmerking dat een dergelijke particuliere briefing onwettig zou zijn en dat de enige wettige weg via het Griekse parlement loopt. Later, toen minister Gerapetritis voor het parlement getuigde, verklaarde hij nooit op de hoogte te zijn geweest van de redenen, en vroeg hij om alle relevante informatie strikt geheim te houden. De EYP staat onder directe controle van premier Kyriakos Mitsotakis als gevolg van een wetswijziging die kort nadat zijn partij Néa Dimokratía aan de macht kwam in 2019 werd goedgekeurd[217].

139. Na de onthullingen traden Grigoris Dimitriadis, de secretaris-generaal van de regering die verantwoordelijk was voor de samenwerking tussen de Griekse regering en de EYP,

---

[210] Meta, Threat Report on the Surveillance-for-Hire Industry.
[211] Inside Story, Who was tracking the mobile phone of journalist Thanasis Koukakis?.
[212] Documento, 27 november 2022.
[213] Gedachtewisseling van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos, 28 februari 2023.
[214] Solomon, Solomon's reporter Stavros Malichudis under surveillance for "national security reasons"; Ekathimerini, Wiretapping case: The phone data that triggered developments; EPRS. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?.
[215] Greek PM says he was unaware of phone tapping of opposition party leader.
[216] 1b LIFO, Androulakis denied information in private upon his surveillance https://www.lifo.gr/now/politics/o-androylakis-arnithike-idiotiki-enimerosi-apo-ton-gerapetriti-kai-zita-na-toy
[217] Euractiv, Another Greek opposition lawmaker victim of Predator.

en de directeur van de EYP, Panagiotis Kontoleon, af[218].

AANKOOP

140. Eind 2019 had secretaris-generaal Dimitriadis contact met de NSO-groep om Pegasus-spyware aan te kopen. In januari 2020 had een officieel voorstel van de NSO-groep betrekking op een overeenkomst tussen regeringen ter waarde van 50 miljoen EUR. Na de ondertekening van de overeenkomst zou het individu zich terugtrekken en zou de EYP het overnemen. De EYP zou samenwerken met de Mossad voor de installatie van het systeem. De regeling werd uiteindelijk afgeblazen[219].

141. Zowel de EYP als de regering ontkennen ten stelligste dat Predator ooit door de Griekse autoriteiten is gekocht of gebruikt[220].142. Bij gebrek aan enig bewijs in de Griekse zaken betreffende de identiteit van de koper en gebruiker van Predator, kan niet met zekerheid worden vastgesteld of en hoe de overheid of een andere actor Predator heeft verworven. Als het niet de Griekse regering was, moet worden geconcludeerd dat een niet-overheidsactor verantwoordelijk was voor de (pogingen tot) hacking van de telefoons van de heren Koukakis en Androulakis. Dat zou volgens de Griekse wet een misdaad zijn, die onderzocht zou moeten worden. De hypothese dat particuliere actoren achter de Predator-aanvallen zaten is bovendien zeer ongeloofwaardig, aangezien zij de keuze van de doelwitten niet zou verklaren. In beginsel is het echter niet onmogelijk voor overheidsorganen om spyware te verwerven of te gebruiken zonder de software daadwerkelijk rechtstreeks aan te kopen. Spyware kan worden gekocht via gelieerden, tussenpersonen of bemiddelaars, zoals in andere gevallen is gebleken. Ook kunnen regelingen worden getroffen met spyware-verkopers om bepaalde spyware-gerelateerde diensten te verlenen. Het lijdt geen twijfel dat er nauwe banden en onderlinge afhankelijkheden bestonden tussen bepaalde personen en gebeurtenissen in verband met de regering, de EYP en de leveranciers van spyware, met name Krikel, een voorkeursleverancier van communicatie- en surveillanceapparatuur aan onder meer de politie en de EYP. Krikel is nauw verbonden met personen in de entourage van premier Mitsotakis. Er zijn steeds meer bewijzen voor nauwe betrekkingen tussen Intellexa, het bedrijf dat eigenaar is van Predator-spyware, en de Griekse staat. Op 16 januari 2023 legde de Griekse gegevensbeschermingsautoriteit Intellexa een geldboete van 50 000 EUR op wegens het niet meewerken en het weigeren om informatie over haar klantenkring over te dragen, in het kader van haar onderzoek dat in juli 2020 naar aanleiding van de klacht van de heer Androulakis is gestart. Dit onderzoek loopt nog[221].

143. Een mogelijkheid is dat Predator is verworven via Ketyak, het centrum voor technologische ondersteuning, ontwikkeling en innovatie dat is opgericht door de voormalige directeur-generaal van de EYP Kontoleon. Het opereert onafhankelijk van de EYP[222] en neemt deel aan projecten rond onderzoek, innovatie en technologische ontwikkeling[223].

---

[218] POLITICO, PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal.
[219] https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all
[220] EPRS. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?.
[221] https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-stin-intellexa-ae-gia-mi-synergasia-me-tin-arhi
[222] https://www.tovima.gr/print/politics/to-trigono-lfpou-egkatestise-lfto-predator-crstin-ypiresia-crpliroforion-crkai-i-lista-crton-xeiriston-tou/
[223] https://www.nis.gr/en/ketyak

DE DOELWITTEN

GRIGORIS DIMITRIADIS

144. Dimitriadis is de neef van premier Mitsotakis en was tot augustus 2022 secretaris-generaal van diens kabinet. In die hoedanigheid was hij verantwoordelijk voor de contacten van de regering met de EYP. Hij moest gedwongen ontslag nemen op 5 augustus 2022 na de onthulling dat de EYP de telefoon van de heer Androulakis had afgeluisterd. Oorspronkelijk werd zijn ontslag toegeschreven aan de toxische politieke omgeving, maar later heeft de premier hem de politieke verantwoordelijkheid toegeschoven voor het afluisteren van de heer Androulakis en andere politici[224].

145. Het voormalig hoofd van de EYP, Panagiotis Kontoleon, gaf zijn "sociale relatie" met de heer Dimitriadis aan de Griekse parlementaire enquêtecommissie toe. Hoewel de heer Kontoleon door de regering-Mitsotakis werd benoemd, moesten een aantal wettelijke bepalingen worden aangepast om zijn benoeming mogelijk te maken[225].

146. De heer Dimitriadis is ook op verschillende manieren nauw verbonden met Felix Bitzios en Giannis Lavranos. De drie heren zijn persoonlijke kennissen van elkaar. De heren Dimitriadis en Lavranos waren elkaars getuige ("Koumbaroi")[226] en de heer Dimitriadis is de peetvader van het tweede kind van de heer Lavranos[227]. De heer Dimitriadis was ook indirect verbonden met de heer Bitzios via zakelijke transacties met diens broer[228].

147. Hierdoor vormt hij de kern van een netwerk dat hem zowel professioneel als persoonlijk verbindt met sleutelfiguren bij Intellexa, Krikel en de EYP.

148. Naar verluidt is de heer Dimitriadis ook een bekende van Andreas Loverdos, die kandidaat was voor het PASOK-KINAL-leiderschap in 2021.

FELIX BITZIOS

149. Zakenman Felix Bitzios was betrokken bij het enorme schandaal rond de schending van de controle op kapitaalverkeer door Piraeus Bank. In afwachting van het onderzoek werden de tegoeden van de heer Bitzios bevroren[229]. De heer Bitzios profiteerde van een wetswijziging die door premier Mitsotakis werd ingevoerd kort nadat hij in 2019 aan de macht was gekomen. Het omstreden amendement voorzag in een uiterste termijn voor het bevriezen van tegoeden, zodat deze na maximaal achttien maanden moeten worden vrijgegeven[230]. Dankzij deze wijziging van de regering van Mitsotakis konden de activa van de heer Bitzios worden vrijgegeven.

150. De heer Bitzios is gelieerd aan Cyprus via zijn bedrijf Santinomo, dat in Cyprus staat

---

[224] https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp, https://primeminister.gr/2022/08/08/29961
[225] *Ieidiseis*, SYRIZA – PASOK findings on wiretapping: Both scandal and cover-up.
[226] TVXS, Giannis Lavranos: The koumbarias with Tsouvala and Dimitriadis.
[227] Ieidiseis, SYRIZA - PASOK findings on wiretapping: Both scandal and cover-up.
[228] Reporters United, The Great Nephew and Big Brother.
[229] Lexocology, Cyprus court offers directions to bank on ambit of freezing injunction.
[230] Financial Times, Greek law change viewed as backtracking on money laundering.

ingeschreven, en zijn connectie met Tal Dilian. Het lijkt erop dat de heer Bitzios een belangrijke rol heeft gespeeld bij de overdracht van Intellexa aan Griekenland[231].

151. De heer Bitzios had, via zijn onderneming Santinomo, 35 % van de aandelen van Intellexa in handen. Op 4 augustus 2022 heeft hij echter de overdracht van al zijn aandelen aan Thalestris, de moedermaatschappij van Intellexa, geregistreerd[232]. De registratiedatum van de overdracht was enkele dagen na de onthullingen van de Androulakis-hack. De overdracht zelf zou echter hebben plaatsgevonden op 28 december 2020, meer dan 19 maanden eerder. De heer Bitzios heeft zich dus met terugwerkende kracht gedistantieerd van zijn eenderde-eigenaarschap van Intellexa. Niettemin was de heer Bitzios van maart 2020 tot juni 2021 als adjunct-administrateur verbonden aan Intellexa[233].

GIANNIS LAVRANOS

152. Giannis Lavranos was beschuldigd van belastingontduiking, en de heer Koukakis had als journalist verslag uitgebracht over deze zaak.

INTELLEXA

153. De spyware Predator wordt verkocht via Intellexa, een consortium van spywareverkopers, dat aanwezig is in onder meer Cyprus, Griekenland, Ierland en Frankrijk. Tal Dilian, die eerder al actief was bij de Israëlische inlichtingendienst, heeft het consortium op Cyprus opgericht. Zijn tweede ex-vrouw, de Poolse Sara Hamou, is een centrale figuur in het complexe netwerk van bedrijven. Tal Dilian heeft ook de Maltese nationaliteit verworven. De Griekse regering heeft verklaard dat twee uitvoervergunningen zijn afgegeven aan Intellexa, waarvan één de uitvoer naar Madagaskar toestond. Bovendien heeft de Griekse regering een uitvoervergunning voor Predator naar Sudan afgegeven. Het is niet bevestigd aan wie de vergunning is afgegeven, of het nu aan Intellexa of een andere entiteit is. Naar verluidt heeft Intellexa zijn producten ook naar Bangladesh uitgevoerd.

154. Op 30 november 2022 bleek uit een onderzoeksrapport van Lighthouse Reports, in samenwerking met de Israëlische krant *Haaretz* en het Griekse kanaal Inside Story, dat de Predator-operaties van Tal Dilian in Griekenland verband zouden houden met een Cessna-jet die tussen april en augustus 2022 van Griekenland en Cyprus naar Sudan vloog. Naar verluidt werd met dit vliegtuig in het geheim en illegaal geavanceerde surveillancetechnologie aan de Janjaweed geleverd[234]. Aan de hand van de vluchtgegevens werd de privéjet die van en naar Cyprus vloog in verband gebracht met Tal Dilian, een voormalige hoge officier van de Israëlische krijgsmacht die Intellexa Alliance in 2019 opzette, met vestigingen in Cyprus en Griekenland. Op 18 februari 2023 heeft de Commissie bevestigd dat zij contact heeft opgenomen met de nationale autoriteiten van Griekenland en Cyprus om opheldering over deze kwestie te

[231] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[232] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[233] https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae.
[234] https://www.lighthousereports.nl/investigation/flight-of-the-predator/; https://www.haaretz.com/israel-news/security-aviation/2022-11-30/ty-article-magazine/.premium/jet-linked-to-israeli-spyware-tycoon-brings-spy-tech-from-eu-to-notorious-sudanese-militia/00000184-a9f4-dd96-ad8c-ebfcd8330000; https://insidestory.gr/article/flight-predator.

vragen. De Commissie heeft echter geen antwoord ontvangen[235]. Op 19 april 2023 heeft de Griekse plaatsvervangende minister van Buitenlandse Zaken Miltiadis Varvitsiotis bevestigd dat de Griekse regering de vergunning voor de uitvoer van Predator-spyware naar Sudan heeft goedgekeurd. De minister ontkent echter elke rol van Predator bij de recente gevechten tussen de Sudanese strijdkrachten en de RSF-milities in Sudan[236].

155. In december 2022 maakte de Griekse regering bekend dat zij Intellexa op 15 november 2021 twee uitvoervergunningen had verleend. Volgens de woordvoerder van het Griekse ministerie van Buitenlandse Zaken, Alexandros Papaioannou, werd aan de hand van een van deze vergunningen toestemming verleend voor de verkoop van Predator aan Madagaskar[237]. De vergunning werd afgegeven ondanks de slechte reputatie van het land op het gebied van mensenrechten[238] en mogelijk in strijd met EU-verordening inzake producten voor tweeërlei gebruik[239]. De secretaris-generaal van Internationale Economische Betrekkingen, Ioannis Smyrlis – die toestemming gaf voor de verkoop van Predator aan Madagaskar – diende zijn ontslag in nadat deze onthullingen aan het licht kwamen[240] om de functie te bekleden van adjunct-directeur-generaal van de regerende partij Néa Dimokratía, die verantwoordelijk is voor de komende verkiezingen.

156. Naast de uitvoer van spyware zou Griekenland ook opleidingsreizen voor het gebruik van spyware hebben georganiseerd. In juni 2021 kocht Bangladesh een spywarevoertuig van de Cypriotische firma Passitora. Volgens documenten van het ministerie van Binnenlandse Zaken van Bangladesh werd het personeel van het National Telecommunication Monitoring Centre (NTMS) tussen 2021 en 2022 in Griekenland opgeleid om het spionagevoertuig te gebruiken. Het voertuig arriveerde uiteindelijk in Bangladesh in juni 2022[241].

KRIKEL

157. Krikel is een voorkeursleverancier voor apparatuur aan de Griekse rechtshandhavings- en veiligheidsautoriteiten. Krikel is ook de Griekse vertegenwoordiger van RCS Lab, een Italiaans bedrijf dat surveillancesoftware verkoopt. Bovendien zou Giannis Lavranos via een ander bedrijf, Mexal genaamd, voor 50 % eigenaar zijn van Krikel[242].

---

[235] https://www.europarl.europa.eu/doceo/document/E-9-2022-003990-ASW_NL.html; Vergadering van de PEGA-commissie, 28 maart 2023.
[236] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/; https://www.aa.com.tr/en/africa/greek-government-admits-opposition-s-claim-of-spyware-export-to-sudan/2876824
[237] *The New York Times*, 8 december 2022, "How the Global Spyware Industry Spiraled Out of Control", https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html
[238] *The New York Times*, 8 december 2022, "How the Global Spyware Industry Spiraled Out of Control", https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html
[239]Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (PB L 206 van 11.6.2021, blz. 1).
[240] *The National Herald*, "Top Greek Official Who Authorized Predator Spyware Sale Resigns".
[241] *Haaretz*, "Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record".
[242] Er zijn in deze zaak verschillende verbanden van belang. Lavranos verkocht zijn gezinswoning in Athene in april 2021 onder de marktwaarde aan Albitrum Properties. De vertegenwoordiger van Albitrum Properties tijdens de verkoop was de halfbroer van Felix Bitzios, Theodoros Zervos. Albitrum is een Cypriotische

Het lijkt echter onmogelijk om met zekerheid vast te stellen wie de uiteindelijke begunstigde van Krikel is, ondanks de vele contracten van Krikel met overheidsinstanties.

158. In 2014 werd Ioniki Technologiki, een bedrijf van Giannis Lavranos, verkocht aan Tetra Communications in Londen. In datzelfde jaar was Ioniki Technologiki een van de drie ondernemingen die het communicatiesysteem Tetra schonken aan het Griekse ministerie van Burgerbescherming[243]. In 2014 had de Griekse regering ook interesse getoond in het Italiaanse spywaremerk RCS Galileo van het bedrijf Hacking Team, zoals onthuld door WikiLeaks, maar deze software werd nooit aangekocht[244]. De schenking van Tetra werd mogelijk gemaakt door een in Florida gevestigd bedrijf, waardoor de reguliere aanbestedingsprocedures konden worden omzeild. De Griekse regering heeft de schenking in 2017 aanvaard. In 2018 ondertekende Krikel een contract voor onderhoud en technische ondersteuning ter waarde van 10,8 miljoen EUR. Stanislaw Pelczar ondertekende als bestuurder van Krikel, maar het lijkt erop dat Lavranos de hele tijd informeel betrokken was bij de onderhandelingen[245]. Krikel werd een belangrijke leverancier van het Griekse Ministerie van Burgerbescherming. Sinds 2018 heeft Krikel zeven contracten gesloten met de Griekse regering, waarvan er zes geheim zijn[246].

159. Het bedrijf Krikel werd ook de lokale vertegenwoordiger van het Italiaanse bedrijf RCS Lab. In juni 2021 kocht de EYP naar verluidt een afluistersysteem van RCS Lab[247], via Krikel[248]. Op dat moment was Dimitriadis verantwoordelijk voor de contacten tussen de regering en de EYP. Sommige bronnen beweren dat tijdens de installatie van dit nieuwe systeem materiaal met informatie over het toezicht op Androulakis en Koukakis verloren is gegaan, naar verluidt als gevolg van een technisch probleem[249]. Andere bronnen spreken dit echter tegen en voeren aan dat Kontoleon op 29 juli 2022 opdracht had gegeven tot de vernietiging van deze dossiers[250].

160. Interessant is dat er getuigen zijn die werknemers van Krikel hebben zien werken bij Ketyak, naar verluidt “pro bono”. Ketyak zou naar verluidt 40 miljoen EUR uit de herstel- en veerkrachtfaciliteit van de EU hebben ontvangen via een vertrouwelijke aanbestedingsprocedure op basis van een geheim besluit van de premier[251]. Onrechtmatig gebruik van EU-middelen voor de financiering van illegale spyware zou een ernstige schending van het Unierecht uitmaken en zou vallen onder de

---

onderneming waarvan Mexal Services Ltd. aandeelhouder is. Mexal Services bezit 100 % van Eneross Holdings Ltd. Eneross Holdings is bovendien eigenaar van Krikel. Het kantoor van Giannis Lavranos is geregistreerd op hetzelfde adres als Eneross Holdings en Mexal Services op Cyprus. Zie: Inside Story, “Predatorgate’s invisible privates”, and TVXS, “G. Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]”.

[243] Inside Story, “Predatorgate’s invisible privates”.

[244] Inside Story, “The timeless interest of the Greek authorities in spyware”.

[245] Inside Story, “Predatorgate’s invisible privates”.

[246] Inside Story, “Predatorgate’s invisible privates”.

[247] *Hellas Posts English*, “The EYP supplier contaminates smartphones in Greece as well”.

[248] TVXS, “G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]”.

[249] TVXS, “G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]”.

[250] Euractiv, “Greek MEP spyware scandal takes new turn”.

[251] https://www.flash.gr/politiki/1988373/predator-apokalypseis-gia-to-ketyak-tis-eyp-me-xrimatodotisi-kai-apo-to-tameio-anakampsis

bevoegdheden van tal van Europese organen, waaronder het Europees Openbaar Ministerie.

161. Naar verluidt hebben Krikel-medewerkers in december 2021 en januari 2022 ook EYP-faciliteiten in Agia Paraskevi bezocht in hun rol als "trainer". Deze faciliteiten worden gecontroleerd door de Griekse regering en zouden de plaats zijn waar de Predator-spyware werd geïnstalleerd[252].

BETROKKENHEID VAN BITZIOS EN LAVRANOS

162. Bitzios en Lavranos waren allebei actief betrokken bij de oprichting van Krikel in 2017. Samen hebben zij ervoor gezorgd dat de Poolse advocaat Stanislaw Pelczar in oktober 2017 tot bestuurder van Krikel werd benoemd[253]. Viniato Holdings Limited, een bedrijf van Bitzios, werd vervolgens tussen januari en augustus 2018 voor consultancydiensten door Krikel aangetrokken, voor een vergoeding van ongeveer 550 000 EUR (hoewel de omzet van Krikel dat jaar slechts 840 000 EUR bedroeg)[254].

163. Bitzios en Pelczar hebben ook andere wederzijdse zakelijke connecties. Uit de Paradise Papers blijkt dat zij een bedrijf delen dat in Malta is geregistreerd onder de naam Baywest Business[255]. Daarnaast heeft Tal Dilian, de oprichter van Intellexa, een Maltees (gouden) paspoort[256] en heeft hij ook een brievenbusbedrijf MNT Investments LTD in de eilandstaat[257].

164. Bitzios en Lavranos zijn twee sleutelfiguren in de levering van communicatie- en surveillancemateriaal aan overheidsinstanties zoals de politie en de EYP. Bitzios was een spilfiguur in de onderneming die Predator verkoopt. Zij stonden dicht bij Dimitriadis en profiteerden allebei van lucratieve overheidscontracten. Zij hebben ook voordeel gehaald uit de wetswijziging van de nieuwe regering waardoor hun bevroren tegoeden werden vrijgegeven. Zij hadden een motief voor het gebruik van spyware tegen Koukakis. Er bestaat een zeer duidelijk en groot risico op belangenconflicten en corruptie wanneer zakelijke belangen, persoonlijke betrekkingen en politieke banden verstrengeld raken. Bitzios en Lavranos zouden daarnaast goed geplaatst zijn om cruciale informatie over de aankoop en het gebruik van Predator in Griekenland te verstrekken.

165. Ondanks de duidelijke relevantie om Bitzios en Lavranos voor de enquêtecommissie van het Griekse parlement te laten getuigen, verwierp de meerderheid van Néa Dimokratía in de commissie de verzoeken van de oppositie om deze mannen op te

---

[252] Inside Story, "Greek State and spyware vendor Intellexa: they are acquainted after all".
[253] TVXS, "G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament [Revealing documents]".
[254] Inside Story, "From Koukakis to Androulakis: A new twist in the Predator spyware case".
[255] International Consortium of Investigative Journalists, Offshore Leaks Database, Paradise Papers – Malta Corporate Registry.
[256] Government of Malta, Persons Naturalised Registered as Citizens of Malta, 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
[257] https://mlt.databasesets.com/company-all/company/73006 https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/

roepen voor een hoorzitting.

TOETSING VOORAF

166. In Griekenland is infectie van een apparaat met spyware een strafbaar feit, zoals bepaald in verschillende artikelen van het Griekse wetboek van strafrecht, waaronder artikel 292 over misdrijven tegen de beveiliging van telefoongesprekken, artikel 292B over het belemmeren van de werking van informatiesystemen en artikel 370 over schendingen van het briefgeheim. Bovendien is de productie, de verkoop, de levering, het gebruik, de invoer, het bezit en de distributie van malware (met inbegrip van spyware) ook een strafbaar feit, zoals omschreven in artikel 292C van het Griekse wetboek van strafrecht[258]. Dit artikel is op 9 december 2022 door de Griekse regering gewijzigd.

167. Het aantal toegestane aftapoperaties is in de loop der jaren aanzienlijk toegenomen. van 4 871 in 2015 tot 11 680 in 2019 en 15 475 in 2021[259]. Tegenwoordig moeten dagelijks ongeveer zestig verzoeken worden behandeld, tot voor kort door één enkele aanklager. Bovendien wordt in de bepalingen van de EYP die de vertrouwelijkheid van de communicatie van burgers om redenen van nationale veiligheid opheffen, geen melding gemaakt van de naam van de betrokkene noch de reden voor de opheffing van de vertrouwelijkheid. Ze zijn beperkt tot het telefoonnummer en het inroepen van de nationale veiligheid[260].

168. De gerechtelijke toestemming om toezicht te houden op privécommunicatie, alsmede de verlenging en beëindiging van een dergelijke toestemming moeten worden goedgekeurd door de bevoegde openbare aanklager. Zoals bepaald in Wet 3649/2008, is de aanklager die bevoegd is geheimhouding en vertrouwelijkheid op te heffen, de interne aanklager van de EYP. Een wetswijziging van 2018 onder de tweede regering-Tsipras heeft het aantal aanklagers dat nodig is voor de toestemming voor een afluisteroperatie teruggebracht van twee naar één. De aanklager die verantwoordelijk is voor de betrokken zaken is Vasiliki Vlachou[261]. Vlachou heeft geen ontmoeting gehad met de PEGA-missie naar Griekenland.

WET INZAKE DE INHOUD VAN WETGEVING

169. Naar aanleiding van de onthullingen over door hen uitgeoefende surveillance, heeft premier Mitsotakis voorgesteld het operationele kader van de EYP te wijzigen. Een van de aanpassingen is de invoering van de wet inzake de inhoud van wetgeving door de regering op 9 augustus 2022. Artikel 9, lid 2, van Wet 3649/2008 werd gewijzigd, waardoor nu een advies van de Permanente Commissie voor instellingen en transparantie vereist is met betrekking tot de benoeming van de voorzitter van de EYP[262]. Aangezien de regeringspartij momenteel echter een absolute meerderheid heeft in de Bijzondere Permanente Commissie voor instellingen en transparantie van het Parlement, heeft zij de benoeming van de heer Demiris als de nieuwe voorzitter van de

[258] International Comparative Legal Guide, *Cybersecurity Laws and Regulation Greece 2022.*
[259] Ekathimerini, "Wiretapping and 'national security'".
[260] Reporters United, "Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis".
[261] Reporters United, "Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis".
[262] EfSyn, "What (does not) change with the Act of Legislative Content for EYP?".

EYP goedgekeurd, terwijl alle andere oppositiepartijen tegen waren[263]. Overigens is Dionysis Melitsiotis[264], voormalig lid van het kabinet van de premier, tweede plaatsvervangend voorzitter van de EYP, en een andere adjunct-directeur is Anastasios Mitsialis, een voormalig partijambtenaar van Néa Dimokratía[265].

170. Bovendien is met deze wet de toestemming van twee aanklagers voor monitoringverzoeken opnieuw ingevoerd[266]. Artikel 5 van Wet 3649/2008 betreffende de opheffing van de vertrouwelijkheid van communicatie door de EYP wordt aangevuld met een indiening ter goedkeuring aan de bevoegde procureur van beroep, die daarna dient te worden goedgekeurd door de openbaar aanklager van het hof van beroep[267].

TOETSING ACHTERAF

171. Sinds 2019 staat de EYP onder rechtstreekste controle van premier Kyriakos Mitsotakis, na een wetswijziging na de overwinning van Néa Dimokratía in 2019[268].

172. De Permanente Commissie voor instellingen en transparantie oefent parlementaire controle uit. Zij houdt toezicht op de acties van de EYP en heeft de bevoegdheid documenten te verzamelen, personen te onderzoeken en de directeur-generaal voor een hoorzitting uit te nodigen[269]. De regeringspartij heeft absolute meerderheid in de huidige samenstelling van de commissie.

173. De Griekse autoriteit voor communicatieveiligheid en privacy (ADAE) zorgt voor de bescherming van de vertrouwelijkheid van e-mails en alle andere vormen van communicatie[270]. Het statuut van de ADAE verleent haar administratieve autonomie[271]. De ADAE kan onderzoeken uitvoeren ten aanzien van faciliteiten, databanken en archieven, en van de technische apparatuur en documenten van de EYP[272].

174. In Wet 2225/1994 is bepaald dat alleen van de vertrouwelijkheid van communicatie kan worden afgezien in gevallen van nationale veiligheid en voor onderzoeken naar ernstige misdrijven. Als de vertrouwelijkheid is opgeheven, is in artikel 5 van deze wet bepaald dat de ADAE de betrokkenen mag informeren, mits het doel van het onderzoek niet in het gedrang komt[273]. Het recht van een persoon op toegang tot informatie over de vraag

---

[263] Ekathemirini, "Themistoklis Demiris: His appointment to the management of EYP was approved by a majority".
[264] Ekathimerini, "National security takes center stage".
[265] Greek City Times, "Greek PM appoints new security and intelligence chiefs".
[266] At a Glance, "Greece's Predatorgate: The latest chapter in Europe's spyware scandal?", Europees Parlement, directoraat-generaal Parlementaire Onderzoeksdiensten, 8 september 2022.
[267] EfSyn, "What (does not) change with the Act of Legislative Content for EYP?".
[268] Euractiv, "Another Greek opposition lawmaker victim of Predator".
[269] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*.
[270] Presentatie van ADAE
[271] Het ADAE-regelgevingskader:
[272] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*.
[273] Constitutionalism, "Contradiction of Article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications".

of de betrokkene onder surveillance staat, is vastgelegd in wet 2472/1997[274]. Toen de ADAE echter in maart 2021 aan de EYP meedeelde dat Koukakis het recht had om te worden geïnformeerd, diende de regering onmiddellijk daarna, op 31 maart 2021, amendement 826/145 in, waardoor de ADAE niet langer burgers mocht informeren wanneer de vertrouwelijkheid van communicatie werd opgeheven[275]. Hierdoor wordt het individu de facto zijn recht op informatie ontnomen. De wijziging werd op zeer onregelmatige wijze ingevoerd. Het amendement werd toegevoegd aan een wet die hiervan losstond (een wetsvoorstel met betrekking tot COVID-19-maatregelen), en de in de grondwet voorgeschreven termijnen werden niet in acht genomen[276] [277] [278]. Er heeft dus geen behoorlijk raadplegingsproces plaatsgevonden.

175. Met de wet inzake de inhoud van wetgeving beoogde Mitsotakis de transparantie en verantwoordingsplicht te versterken. Amendement 826/145 wordt hiermee echter niet ingetrokken.

176. Op 9 december 2022 heeft de Griekse regering Wet 5002/2022 aangenomen met het oog op de actualisering en de totstandbrenging van een doeltreffend juridisch kader voor de bescherming van persoonsgegevens en het communicatiegeheim en de versterking van de cyberveiligheid. De wet voert echter verschillende bepalingen in die de waarborgen, het toezicht en de verantwoordingsplicht verzwakken. Zoals bepaald in artikel 4, lid 7[279], wordt elk verzoek van personen om informatie over de vraag of zij om redenen van nationale veiligheid onder toezicht zijn geplaatst, onderzocht door een comité van drie leden, bestaande uit de directeur van de EYP, de aan de EYP verbonden aanklager en het hoofd van de ADAE. Dit betekent dat de meerderheid ligt bij degenen die de opdracht (directeur van de EYP) en de toestemming (aanklager) voor de surveillance hebben gegeven. Bovendien wordt het voor personen die om redenen van nationale veiligheid onder surveillance staan praktisch onmogelijk om achteraf naar behoren te worden geïnformeerd, aangezien de wet bepaalt dat zij pas drie jaar na de beëindiging van hun surveillance een desbetreffend verzoek kunnen indienen. Dit is onverenigbaar met de relevante jurisprudentie van het Europees Hof en het Europees Handvest van de rechten van de mens[280] en de wet voorziet niet in institutionele checks-and-balances om de goede werking van de staatsbevoegdheden te waarborgen. De ADAE heeft laten weten het niet eens te zijn met het driekoppige orgaan. Tot op heden

---

[274] Griekse gegevensbeschermingsautoriteit (APDPX), Wet 2472/1997 inzake de bescherming van personen in verband met de verwerking van persoonsgegevens.
[275] https://www.reportersunited.gr/8646/eyp-koukakis/
[276] Grieks parlement, Grondwet.
[277] Grieks parlement, Reglement.
[278] Govwatch, "Violation of the legislative process for amendments in law 4790/2021".
[279] https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022
[280] https://www.dsa.gr/%CE%B4%CE%B5%CE%BB%CF%84%CE%AF%CE%B1-%CF%84%CF%8D%CF%80%CE%BF%CF%85/%CE%B1%CF%80%CE%BF%CF%86%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%B4%CF%83/%CE%B1%CF%80%CF%8C%CF%86%CE%B1%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%BF%CE%B9%CE%BA%CE%B7%CF%84%CE%B9%CE%BA%CE%BF%CF%8D-%CF%83%CF%85%CE%BC%CE%B2%CE%BF%CF%85%CE%BB%CE%AF%CE%BF%CF%85-%CF%84%CE%BF%CF%85-%CE%B4%CF%83%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7-%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B5%CE%B9%CF%83%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB

bestaat er geen operationeel kader voor het tripartiete comité, waardoor het de facto niet functioneert[281]. Bovendien stelt de nieuwe wet het gebruik van spyware door particulieren of particuliere bedrijven strafbaar, en legaliseert zij voor het eerst de aankoop van spyware door overheidsinstanties, waarbij de regering wordt gemachtigd de procedure in te stellen via een presidentieel besluit. Er zijn geen bepalingen voor gerechtelijk toezicht op het gebruik van spyware of voor het uitbesteden van afluisteractiviteiten aan particuliere entiteiten.

177. De levering door particuliere actoren van spyware is enkel illegaal als dergelijke software is opgenomen in een indicatieve lijst van "verboden spyware" die elke zes maanden door het hoofd van de EYP wordt bijgewerkt. Hierdoor wordt de EYP gemachtigd om spyware legaal te verwerven, aangezien kritieke relevante kwesties uitsluitend zullen worden behandeld via secundaire wetgeving (namelijk een presidentieel besluit). Daarom wordt een bijgewerkte versie van bestaande spyware als legaal beschouwd totdat deze in de bovengenoemde lijst is opgenomen. De definitie van "nationale veiligheid" in de wet is uiterst breed en vaag, en dus in strijd met artikel 19, lid 1, van de grondwet, dat een enge interpretatie vereist. De ADAE is verder belemmerd in zijn inspanningen om zijn grondwettelijk aangewezen rol uit te oefenen bij het controleren van het derubriceringsproces. De rol van de onafhankelijke autoriteit die cruciaal was bij het blootleggen van het surveillanceschandaal wordt in de nieuwe wet gebagatelliseerd, ondanks de relevante grondwettelijke garanties.

178. De mogelijkheden voor controle achteraf werden verzwakt door het feit dat Griekenland er lang over heeft gedaan om de EU-klokkenluidersrichtlijn volledig uit te voeren[282]. Op 27 januari 2022 heeft de Commissie een inbreukprocedure ingeleid door Griekenland een ingebrekestelling te sturen. Op 15 juli 2022[283] heeft de Commissie een met redenen omkleed advies gestuurd, met een termijn van twee maanden om te antwoorden. Het Griekse parlement stemde uiteindelijk op 11 november 2022 over Wet 4990/2022, waarmee de EU-klokkenluidersrichtlijn in Griekse wetgeving werd omgezet.

OPENBAAR TOEZICHT

179. Griekenland staat in de wereldindex voor persvrijheid 2022 op de laagste plaats van alle EU-landen, namelijk de 108e (op een totaal van 180 landen)[284]. In 2021 werd journalist Giorgos Karaivaz vermoord. De moord is nog steeds niet opgelost. Journalisten worden geconfronteerd met intimidatie en strategische rechtszaken tegen publieke participatie (Strategic Lawsuits against Public Participation – SLAPP's). Grigoris Dimitriadis[285] heeft SLAPP's aangespannen tegen nieuwskanalen Reporters United en *Efimerida ton Syntakton* (EfSyn)[286] nadat hij gedwongen was ontslag te nemen. Minister Oikonomou trachtte een verslaggever van Politico, Nektaria Stamouli, in diskrediet te brengen door te suggereren dat haar artikelen over het spywareschandaal politiek gemotiveerd

[281] Gedachtewisseling van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos, 28 februari 2023.
[282] https://ec.europa.eu/commission/presscorner/detail/nl/inf_22_3768
[283] https://ec.europa.eu/commission/presscorner/detail/nl/inf_22_3768
[284] https://rsf.org/en/index
[285] Tagesspiegel.
[286] EUobserver, "Greece accused of undermining rule of law in wiretap scandal".

waren[287]. Twee van de doelwitten van surveillance, Koukakis en Malichoudis, hadden op kritische wijze bericht over gevallen van corruptie en fraude, en over de slechte behandeling van migranten. Athanasios Telloglou en Eliza Triantafillou brachten verslag uit over het spywareschandaal, en werden vervolgens naar verluidt onder surveillance geplaatst[288]. Bovendien heeft de Griekse aanklager van het hooggerechtshof Isidoros Dogiakos mediakanalen in diskrediet gebracht die de Griekse gerechtelijke autoriteiten bekritiseerden omdat ze het Griekse afluisterschandaal niet goed hadden afgehandeld. Hij probeerde zelfs de media die het schandaal onderzochten te intimideren door selectieve belastingcontroles te vragen voor hun eigenaars[289].

VERHAALSMOGELIJKHEDEN

DE NATIONALE AUTORITEIT VOOR TRANSPARANTIE

180. Zoals bepaald in artikel 82 van Wet 4622/2019 heeft de nationale autoriteit voor transparantie (EAD) de verantwoordelijkheid om de verantwoordingsplicht, transparantie en integriteit van acties van regeringsinstanties, overheidsinstanties, administratieve autoriteiten en openbare organisaties te versterken. Daarnaast moet de EAD fraude en corruptie door openbare en particuliere instanties voorkomen, opsporen en aanpakken. Volgens deze wet heeft de EAD alle verantwoordelijkheden, rechten en plichten van de volgende overheidsinstanties overgenomen: het secretariaat-generaal voor de bestrijding van corruptie; het orgaan van auditors-inspecteurs van het openbaar bestuur; het bureau van de inspecteur-generaal van het openbaar bestuur; het orgaan van inspecteurs van gezondheids- en welzijnsdiensten; het orgaan van inspecteurs van openbare werken; en het orgaan van auditors-inspecteurs van vervoer[290]. Terwijl de onafhankelijkheid van de ADAE in de grondwet is vastgelegd, is de EAD geen onafhankelijke autoriteit.

181. Op 22 juli 2022 heeft de EAD een onderzoek ingesteld naar de vermeende aankoop van de spyware Predator door het ministerie van Burgerbescherming en de EYP. Bij de audit werden de Griekse politie, de EYP en de ondernemingen Intellexa en Krikel gecontroleerd. De EAD heeft haar verslag op 10 juli 2022 afgerond, maar legde het vervolgens ter voorafgaande goedkeuring aan de EYP voor. Het officiële rapport dat op 22 juli aan Koukakis is toegezonden, omvatte niet de volledige audit zoals uitgevoerd door de EAD: het bevatte slechts delen daarvan. Onder het mom van de bescherming van persoonsgegevens werden verschillende namen uit het verslag onleesbaar gemaakt, waaronder de namen van de controleurs van de EAD, de aanklager van de EYP die het eerste verslag van de EAD had gecontroleerd, en de advocaten en accountants van de betrokken rechtspersonen[291].

182. Uiteindelijk werd in het EAD-verslag geconcludeerd dat noch de EYP, noch het Ministerie van Burgerbescherming, een contract had gesloten met Intellexa of andere

[287] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/.
[288] Heinrich-Böll-Stiftung, "In conditions of absolute loneliness".
[289] ESIEA Journalists Unions condemn threats from Supreme Court Prosecutor, https://www.esiea.gr/oi-dimosiografikes-enoseis-gia-tis-di/.
[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019
[291] Inside Story, "From Koukakis to Androulakis: A new twist in the Predator Spyware case".

verbonden nationale bedrijven. Evenmin hadden zij de spyware Predator gekocht of gebruikt[292]. De EAD heeft echter geen onderzoek gedaan naar de bankrekeningen van Intellexa en Krikel, of die van gelieerde offshore ondernemingen. Bovendien bezocht de EAD de kantoren van Intellexa en Krikel pas twee maanden na de eerste publicatie over het gebruik van Predator in Griekenland. Op dat moment werkten de werknemers thuis naar aanleiding van COVID-19. Daarnaast heeft de EAD geen ontmoeting gehad met de wettelijke vertegenwoordigers van de betrokken ondernemingen[293].

183. Er zijn vragen over de onafhankelijkheid van het bestuur van de EAD. De huidige directeur, een voormalige werknemer van Mitsotakis, vervult sinds de zomer van 2022 de functie ad interim. Het is onduidelijk waarom de aanwervingsprocedure niet is gestart. De directeur van de EAD heeft tijdens de missie in november 2022 geen ontmoeting gehad met PEGA. De directeur heeft op 7 maart 2023 een ontmoeting gehad met de delegatie van de commissie LIBE, waar vragen over spyware in Griekenland werden gesteld.

DE GRIEKSE AUTORITEIT VOOR COMMUNICATIEVEILIGHEID EN PRIVACY (ADAE)

184. In juli 2022 bevestigde Nikos Androulakis dat hij op 21 september 2021 een klacht had ingediend bij het openbaar ministerie bij het Hooggerechtshof, omdat hij naar verluidt het doelwit was van de spyware Predator. Naar aanleiding van de klacht van Androulakis startte de ADAE in augustus 2022 een onderzoek, en vroeg zij om te beginnen informatie op bij de telecomoperator van Androulakis.

185. Predator-spyware laat weinig sporen van besmetting achter bij telecommunicatieaanbieders. De ADAE constateerde echter dat de mobiele telefoon van Androulakis werd gemonitord door de EYP[294], en dat de interne aanklager Vasiliki Vlachou toestemming had verleend voor de monitoring en het opheffen van vertrouwelijkheid in september 2021, hetgeen in de tijd samenviel met de vermeende Predator-aanval.

186. Naar aanleiding van de bevindingen van het ADAE-onderzoek namen Grigoris Dimitriadis en Panagiotis Kontoleon ontslag uit hun overheidsfuncties[295]. Kontoleon verklaarde dat de monitoring van Androulakis in gang werd gezet op verzoek van buitenlandse autoriteiten – meer bepaald de inlichtingendiensten van Armenië en Oekraïne – in het licht van zijn deelname aan de Commissie internationale handel van het Europees Parlement, die zich bezighoudt met de handelsbetrekkingen tussen de EU en China[296]. Zowel Oekraïne als Armenië hebben deze beweringen verworpen[297].

187. Op 15 december 2022 heeft de autoriteit gevolg gegeven aan verzoeken van journalisten Tasos Telloglou en EP-lid Giorgos Kyrtsos over de vraag of zij het doelwit van de EYP zijn geweest. Uit een audit van de ADAE bij het telecommunicatiebedrijf Cosmote

[292] Inside Story, "From Koukakis to Androulakis: A new twist in the Predator Spyware case".
[293] Inside Story, "From Koukakis to Androulakis: A new twist in the Predator Spyware case".
[294] https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf
[295] Politico, "PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal".
[296] https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/
[297] At a Glance, "Greece's Predatorsgate: The latest chapter in Europe's spyware scandal?", Europees Parlement, directoraat-generaal Parlementaire Onderzoeksdiensten, 8 september 2022.

bleek dat zowel Telloglou als Kyrtsos inderdaad onder surveillance stonden[298]. Cosmote stelde het hooggerechtshof in kennis en trok de wettigheid van het onderzoek van de ADAE in twijfel[299]. De ADAE richtte een speciaal team op om de telecommunicatieaanbieders te controleren, waarbij met name werd gezocht naar andere verzoeken van de EYP om de vertrouwelijkheid op te heffen[300].

188. De regering heeft getracht de leden van de raad van bestuur van de ADAE te vervangen. Bovendien heeft de Griekse hoofdaanklager Dogiakos op 10 januari 2023 officieel een advies uitgebracht, waarin werd bepaald dat de ADAE geen onderzoek mag instellen naar de gegevens van telecommunicatieaanbieders om de opheffing van de vertrouwelijkheid van communicatie te onderzoeken. Volgens het advies kunnen strafrechtelijke sancties van toepassing zijn zodra de ADAE met dergelijke audits aanvangt[301]. Dit advies, dat in tegenspraak is met eerdere adviezen van de procureur-generaal, is een duidelijke inbreuk op de onafhankelijkheid van de ADAE[302] en probeert haar te verhinderen onderzoeken uit te voeren. Tijdens een vergadering van de commissie PEGA op 28 februari 2023 verklaarde Rammos dat het advies van Dogiakos niet bindend is en dat de taken van de ADAE gewoon door kunnen gaan[303].

189. De ADAE heeft bevestigd dat de EYP ook het hoofd van het Griekse leger Konstantinos Floros, een zittende minister, diverse ambtenaren die zich bezighielden met zaken met betrekking tot wapens en een voormalige nationale-veiligheidsadviseur heeft bespioneerd. Vanwege het huidige onvermogen van de ADAE om de betrokken personen te informeren, wilde de ADAE de bevindingen voorleggen aan de commissie transparantie van het Griekse parlement en de instellingen van het Griekse parlement[304]. Christos Rammos deed een brief het Griekse parlement toekomen met het verzoek om deze presentatie. Aanvankelijk stelde de voorzitter de kwestie niet aan de orde door te beweren geen tijd te hebben gevonden om de brief van Rammos te lezen tijdens zijn naamdag. Uiteindelijk heeft de meerderheid van de Nea Dimokratía in de commissie voor instellingen en transparantie zijn verzoek afgewezen. Op 24 januari 2023 viel de woordvoerder van de regering de ADAE en haar voorzitter aan naar aanleiding van haar onderzoeken[305], met het argument dat Rammos aan “activisme” deed en zijn mandaat “te buiten ging”, wat het onderzoek van de ADAE niet ten goede kwam. Op 25 januari 2023 noemde Syriza-leider Alexis Tsipras in het Griekse parlement publiekelijk de in het rapport genoemde personen en bevestigde hij dat het hoofd van de strijdkrachten, het voormalige hoofd van het Griekse leger, de minister van Werk, de voormalige nationale veiligheidsadviseur van de premier en twee adviseurs van het directoraat

[298] Euractiv, “Exclusive: Another MEP and journalist the latest victims of “Greek Watergate””.
[299] International Press Institute, “Greece: MFRR alarmed by latest revelations of spying on journalists”.
[300] Euractiv, “Exclusive: Another MEP and journalist the latest victims of “Greek Watergate””.
[301] Euractiv, “Chief prosecutor puts Greece’s rule of law to the test”.
[302] http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/
[303] Gedachtewisseling van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos, 28 februari 2023.
[304]https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/
[305] https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/

Apparatuur van de strijdkrachten door het EYP in de gaten werden gehouden. Gezien de ernst van de bevindingen komen de weigering om de ADAE toe te staan verslag uit te brengen aan het Griekse parlement en het in diskrediet brengen van de autoriteit neer op het belemmeren van verantwoordingsplicht en transparantie[306].

190. Bovendien verklaarde Rammos dat de wijzigingen in het wettelijke kader van de ADAE voor onzekerheid hebben gezorgd, hetgeen heeft geleid tot een briefwisseling met de ministeries om het operationele kader van de autoriteit voor klachten en onderzoeken te verduidelijken. Rammos merkte op dat de ADAE ongeveer tien klachten per dag ontvangt[307].

COMMISSIE VOOR INSTELLINGEN EN TRANSPARANTIE

191. In juli 2022 heeft de commissie voor instellingen en transparantie Kontoleon en de voorzitter van de ADAE, Christos Rammos, opgeroepen voor een parlementaire hoorzitting. Tijdens deze hoorzitting gaf Kontoleon naar verluidt toe dat de EYP om redenen van nationale veiligheid Thanasis Koukakis had bespioneerd, maar verklaarde hij niet op de hoogte te zijn van de poging tot hacking van de telefoon van Androulakis met Predator. Giannis Oikonomou – woordvoerder van de regering – verklaarde dat de Griekse autoriteiten de spyware Predator niet hebben aangekocht noch gebruikt[308].

192. Hoewel de vergaderingen achter gesloten deuren plaatsvinden[309], waren naar verluidt noch Kontoleon noch Dimitriadis bereid substantieel bewijs te leveren, waarbij zij redenen van nationale geheimhouding inriepen[310]. Het nieuwe hoofd van de EYP, Demiris, ontzegde de commissie toegang tot een verslag met informatie over de vermeende vernietiging van surveillancegegevens[311]. Dit betekent feitelijk dat de EYP de verantwoordingsplicht weigert en het Grieks parlement zijn mandaat van parlementair toezicht niet kan uitvoeren.

193. Op 30 augustus 2022 riep de commissie negen personen bijeen voor een hoorzitting achter gesloten deuren, waaronder openbaar aanklager Vasiliki Vlachou, voormalig secretaris-generaal Grigoris Dimitriadis en voormalig hoofd van de EYP, Kontoleon. Ze deden allemaal een beroep op de vertrouwelijkheid en wilden geen vragen beantwoorden tijdens deze hoorzitting[312].

PARLEMENTAIRE ENQUÊTECOMMISSIE

194. Het voorstel van de partij PASOK-KINAL om een enquêtecommissie naar het vermeende gebruik van spyware in te stellen[313], werd door 142 parlementsleden van de

[306]Newsbomb, "SYRIZA: Maximos circles" through ADAE – What he sees behind the "blockade" of ND in Rammos".
[307] Discussie van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos, 28 februari 2023.
[308] Reuters. Greek intelligence service admits spying on journalist – sources.
[309] Ekathimerini, "Transparency committee to hold closed-door meeting on phone hacking allegation".
[310] Tovima, "In combat positions for eavesdropping".
[311] Tovima, "In combat positions for eavesdropping".
[312] Ieidiseis, "SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up", https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi
[313] Tovina. Interceptions: Committee of Inquiry to monitor Androulakis – Pasok's proposal in detail.

oppositie gesteund. De 157 parlementsleden van Nea Demokratia onthielden zich van stemming[314]. Nea Demokratia had echter wel een absolute meerderheid in de enquêtecommissie. De oproepen voor een tweepartijenbureau werden afgewezen. Nea Demokratia legde het werkprogramma en de lijst van uit te nodigen getuigen vast, en verwierp verschillende van de door de oppositiepartijen voorgestelde getuigen. Op 29 augustus 2022 werd de commissie opgericht. Zij is op 7 september 2022 met haar werkzaamheden begonnen en heeft haar taak op 10 oktober 2022 afgerond.

195. De regeringsmeerderheid in de commissie weigerde de heren Bitzios en Lavranos uit te nodigen, maar nodigde wel Stamatis Tribalis – de huidige directeur van Krikel – en Sara Hamou uit. Op 22 september heeft Tribalis voor deze parlementaire commissie een getuigenis afgelegd. De heer. Tribalis gaf flagrant onjuiste informatie over de betrokkenheid van Bitzios en Lavranos bij Krikel, waarbij hij onder meer beweerde dat hij zelf de eigenaar van Krikel was[315].

196. Eén getuige, Sarah Hamou van Intellexa, beweerde niet in persoon te kunnen verschijnen (hoewel zij op Cyprus woont), en mocht schriftelijk antwoorden geven. Door de sterke polarisatie van het politieke landschap konden geen gemeenschappelijke conclusies worden bereikt. Een door de regering geleide meerderheid besloot zo'n 5 500 bladzijden aan documenten te classificeren, waaronder de notulen en de verklaring van Hamou en de belangrijkste bevindingen van de partijen, hoewel het volledig binnen de bevoegdheid van het Parlement valt om deze informatie te derubriceren en toegang te verlenen tot deze informatie. Om die reden is er geen openbare samenvatting opgesteld. Alleen het slotdebat in de plenaire vergadering van het Griekse parlement was openbaar en de bevindingen van zowel PASOK als Syriza werden door de partijen zelf gepubliceerd.

197. De oppositie stelde andere getuigen voor, zoals Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos en Bitzios, maar de commissie weigerde uiteindelijk hen uit te nodigen. Op 10 oktober 2022 heeft de commissie haar onderzoeken afgesloten en hebben alle politieke partijen hun eindverslagen ingediend[316].

DE GRIEKSE GEGEVENSBESCHERMINGSAUTORITEIT

198. De Griekse gegevensbeschermingsautoriteit (HDPA) is een onafhankelijke autoriteit en heeft de taak toezicht te houden op de toepassing van de algemene verordening gegevensbescherming[317] (AVG), andere verordeningen en nationale wetten met betrekking tot gegevensbescherming van personen in Griekenland[318]. De wet 4624/2019 sloot de nationale veiligheid uit van het toepassingsgebied van de HDPA, terwijl deze sinds de wet van 1997[319]wel was opgenomen. Naar aanleiding van de klacht van Nikos Androulakis in juli 2022 is de autoriteit in juli 2022 een onderzoek gestart naar de

[314] Tovina. *Parliament: The 2016 inquiry into surveillance was passed – with 142 votes in favour.*
[315] TVXS. *G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament.*
[316] Ieidiseis. *SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up*.
[317] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (PB L 119 van 4.5.2016, blz. 1).
[318] De Griekse gegevensbeschermingsautoriteit. *Persoonlijke gegevens*.
[319] Staatsblad van de Helleense Republiek.

installatie van spyware op mobiele telefoons en de daarop volgende verzameling van persoonsgegevens en gegevensverwerking. De autoriteit voerde een audit uit bij het Intellexa-kantoor in Chalandri en een Intellexa-vestiging in Elliniko. Intellexa verstrekte echter geen cruciale informatie en beantwoordde de vragenlijsten met een aanzienlijke vertraging, waarmee zij dus de audit van de autoriteit belemmerde[320].

199. Op 16 januari 2023 legde de HDPA Intellexa S.A. een geldboete van 50 000 EUR[321] op wegens deze belemmering en het niet willen meewerken tijdens de audit op grond van artikel 31 van de AVG.

200. Na de actie van de HDPA heeft Intellexa documenten overhandigd, maar de autoriteit onderzoekt deze nog. Volgens de voorzitter van de HDPA, de heer Menoudakos, heeft de autoriteit domeinnamen ontdekt die mogelijk toebehoren aan bedrijven die binnen en buiten de EU samenwerken met Intellexa. Dit onderzoek is nog steeds lopende[322].

201. Tijdens een vergadering van de commissie PEGA op 28 februari 2023 vermeldde de voorzitter van de HDPA dat een onderzoek van de HDPA betrekking had op internettoepassingen voor het verzenden van tekstberichten. Volgens de heer Menoudakos hebben bedrijven gebruik gemaakt van deze internettoepassingen om tekstberichten te versturen die verband houden met de Predator-spyware. De HDPA probeert momenteel de doelwitten te identificeren, maar heeft tot nu toe bevestigd dat driehonderd tekstberichten met deze methode naar ongeveer honderd ontvangers zijn gestuurd. De HDPA heeft de bedrijven opgedragen deze gegevens te bewaren en benadrukt dat als deze bedrijven geen wettelijke vertegenwoordiger in de EU hebben, zij de AVG schenden[323].

DE DOELWITTEN

THANASIS KOUKAKIS

202. In de zomer van 2020 werden de telefoongesprekken van journalist Thanasis Koukakis afgeluisterd door de EYP. In die periode bracht hij verslag uit over financiële onderwerpen, waaronder het schandaal Piraeus/Libra, waarbij Felix Bitzios betrokken was, en over vermeende belastingontduiking door de Griekse zakenman Yiannis Lavranos, en over controversiële bankwetten die door de Griekse regering waren ingevoerd en die de vervolging van witwaspraktijken en andere financiële wanpraktijken belemmerden (de terugwerkende kracht leidde er inderdaad toe dat twaalf hangende zaken werden geseponeerd)[324]. De heer Koukakis onderzocht ook de aanbesteding voor nieuwe identiteitskaarten, waarbij de heer Lavranos en de heer Bitzios zakelijke belangen hadden. Rond de tijd dat Koukakis voor het eerst verschijnt voor PEGA, werd de aanbesteding plots ingetrokken en trad de verantwoordelijke secretaris-generaal af.

[320] De Griekse gegevensbeschermingsautoriteit. Boete opgelegd aan Intellexa S.A. wegens niet-medewerking aan de HDPA.
[321] De Griekse gegevensbeschermingsautoriteit. Boete opgelegd aan Intellexa S.A. wegens niet-medewerking aan de HDPA.
[322] Discussie van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos. 28.02.2023.
[323] Discussie van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos. 28.02.2023.
[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis*?.

203. Op 29 juli 2022 verklaarde het hoofd van de EYP, Panagiotis Kontoleon, dat de EYP de telefoon van de heer Koukakis vanwege “nationale veiligheidsredenen” had gemonitord.

204. Op 1 juni 2020 diende de EYP een eerste verzoek in om de vertrouwelijkheid van het telefoonnummer van de heer Koukakis voor twee maanden op te heffen, tot 1 augustus 2020. De EYP diende vervolgens een verzoek in om verlenging met nog eens twee maanden[325], d.w.z. tot 1 oktober 2020. De aanklager van het hof van beroep, Vasiliki Vlachou, keurde al deze verzoeken goed op grond van de nationale veiligheid[326].

205. Twaalf dagen later, op 12 augustus 2020, verzocht de EYP echter plotseling om de beëindiging van de opheffing van de vertrouwelijkheid van het telefoonnummer van de heer Koukakis, anderhalve maand eerder dan in het oorspronkelijke verzoek was voorzien. Dit gebeurde op dezelfde dag dat Koukakis de ADAE benaderde met het verzoek om te worden ingelicht over een mogelijke surveillance van zijn twee mobiele telefoons en een vaste lijn.

206. Op 10 maart 2021 meldde de ADAE bij de procureur van de EYP dat Koukakis op de hoogte kon worden gebracht van de surveillance van zijn mobiele telefoon. Op 31 maart keurde de Griekse regering echter Amendement 826/145 goed, op grond waarvan de bevoegdheid van de ADAE om burgers op de hoogte te brengen wanneer de vertrouwelijkheid van hun communicatie wordt opgeheven, met terugwerkende kracht werd ingetrokken[327]. De voorzitter van de ADAE, Christos Rammos, en twee andere leden van de ADAE hebben tegen dit amendement gepleit en wezen er in een opiniestuk op dat het amendement het recht op eerbiediging van het privéleven en het familie- en gezinsleven dat is verankerd in het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) en de bescherming van de vertrouwelijkheid van communicatie uit hoofde van de grondwet schendt[328].

207. Tussen 12 juli 2021 en 14 september 2021 was de telefoon van de heer Koukakis geïnfecteerd met Predator-spyware[329]. De heer Koukakis beweert een tekstbericht te hebben ontvangen met een koppeling naar een webpagina met financieel nieuws[330]. Op 28 maart 2022 heeft CitizenLab de besmetting officieel onthuld[331].

208. De heer Koukakis heeft meerdere pogingen gedaan om genoegdoening te verkrijgen voor het surveillance-incident. Hij heeft twee klachten ingediend bij de ADAE: de eerste op 6 april 2022 waar hij verzocht om een grondig onderzoek naar de Predator-

---

[325] Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*.
[326] Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*; Inside Story. *Who was tracking journalist Thanasis Koukakis’ cell phone?*.
[327] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis: https://www.reportersunited.gr/8646/eyp-koukakis/ Inside Story Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.
[328] Constitutionalisme. In strijd met artikel 87 van wet 4790/2021 met de waarborgen van het EHRM voor de bescherming van de vertrouwelijkheid van communicatie: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/
[329] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.
[330] Europees Parlement. Hoorzitting van 8 september 2022.
[331] Inside Story. *Who was tracking journalist Thanasis Koukakis’ cell phone?*.

infectie van zijn mobiele telefoon; de tweede op 13 mei 2022 in het licht van de nieuwe onthullingen van InsideStory en Reporters United. Daarnaast diende Koukakis op 4 mei 2022 een klacht in bij de EAD, waarin hij verzocht om een onderzoek naar de context waarin de onderscheppingen door de EYP en de aanval met Predator plaatsvonden[332].

209. Het onderzoek dat de nationale autoriteit voor transparantie (de EAD) op 21 juli 2022 uitvoerde in de kantoren van Intellexa − het bedrijf dat Predator-spyware verkoopt − in Athene, was beperkt en oppervlakkig, ondanks het feit dat er cruciale informatie over de Predator-aanvallen – een strafbaar feit – kon worden gevonden. Er werden geen servers, IT-hardware en administratieve documenten in beslag genomen en bemachtigd. De controle van de financiële administratie was beperkt tot het jaar 2020[333]. De dochterondernemingen van Intellexa op Cyprus en in Ierland werden helemaal niet onderzocht[334]. Voorts maakte informatie over de bankrekeningen en dochterondernemingen van Intellexa geen deel uit van de onderzoeken[335]. Koukakis ging op 27 juli 2022 in beroep bij het Europees Hof voor de Rechten van de Mens[336].

210. Op 5 oktober 2022 diende de heer Koukakis bij het parket van Athene een klacht in tegen Intellexa Alliance, en in het bijzonder tegen Tal Dilian en Sara Hamou[337], wegens schending van de vertrouwelijkheid van zijn communicatie[338].

NIKOS ANDROULAKIS

211. Op 21 september 2021 werd Nikos Androulakis, leider van de centrumlinkse partij PASOK-KINAL en lid van het Europees Parlement, het doelwit van de spyware Predator, toen een malafide link naar zijn telefoon werd gestuurd[339]. De heer Androulakis ontving een tekstbericht met de volgende tekst: “Laat ons de ernst van de zaak inzien, man, we hebben er veel bij te winnen”. Het bericht bevatte een link om Predator op zijn telefoon te installeren, maar, in tegenstelling tot de heer Koukakis, heeft de heer Androulakis niet geklikt op de link die hem was toegestuurd[340]. Tijdens een vergadering van de commissie PEGA op 28 februari 2023 heeft de heer Androulakis verklaard dat de HDPA de kredietkaartrekening heeft geïdentificeerd waarmee de naar hem gestuurde tekstberichten zijn betaald. Deze informatie werd gedeeld met de bevoegde aanklager[341].

212. In juli 2021 kondigde de heer Androulakis aan dat hij zich kandidaat stelde voor het leiderschap van zijn partij[342]. Volgens het onderzoek van de ADAE werd de mobiele telefoon van de heer Androulakis op dat moment afgetapt door de EYP via aanbieders van telecomdiensten[343]. EYP-procureur Vasiliki Vlachou autoriseerde de opheffing van

---

[332] Avgi. *Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him*.
[333] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[334] Inside Story. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[335] Inside Story. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[336] BBC. *Greece wiretap and spyware claims circle around PM Mitsotakis.*
[337] News 24 7. Wiretapping scandal: Lawsuit against Intellexa by Thanasis Koukakis.
[338] Heinrich Boll Stiftung. *A State of Absolute Solitude*.
[339] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case.*
[340] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader.*
[341] Discussie van de commissie PEGA met Konstantinos Menoudakos en Christos Rammos. 28.02.2023.
[342] Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped.
[343] Kathimerini. *Surveillance case: the data that triggered the developments*.

de vertrouwelijkheid van de telefoon van de heer Androulakis op gronden van "nationale veiligheid". Deze goedkeuring viel samen met zowel de aanval met Predator als de kandidatuur van de heer Androulakis.

213. Toen de heer Androulakis in december 2021 werd verkozen tot partijleider, werd de "officiële" surveillance door de EYP onmiddellijk stopgezet[344], ondanks dat toestemming was gegeven voor een surveillance van twee maanden en deze termijn nog niet was verstreken.

214. Op 28 juni 2022 controleerde DG ITEC van het Europees Parlement de telefoon van de heer Androulakis en vond het bewijs van de aanvalspoging met Predator in september 2021. Het bracht de heer Androulakis hiervan dienovereenkomstig op de hoogte[345]. De heer Androulakis deed op 26 juli 2022 aangifte bij de procureur van het Hooggerechtshof[346].

215. Een paar dagen later, op 29 juli, presenteerde de heer Androulakis de informatie over de Predator-aanval aan de ADAE. Op diezelfde dag hoorde het Permanent Comité voor instellingen en transparantie EYP-directeur Panagiotis Kontoleon en ADAE-directeur Christos Rammos, in aanwezigheid van de minister van Digitaal Bestuur en de staatssecretaris. De bijeenkomst vond achter gesloten deuren plaats[347].

216. Op 8 september 2022 verzocht de heer Androulakis de ADAE hem zijn aftapdossier te overhandigen[348]. Op diezelfde dag rapporteerde Ta Nea echter over een officiële briefing van de ADAE waarin stond dat de dossiers van zowel de heer Androulakis als de heer Koukakis door het EYP waren vernietigd[349]. Dat de dossiers vernietigd zijn, is een feit. Het verhaal achter de vernietiging is nog steeds onduidelijk. Sommige bronnen beweren dat de vernietiging van de dossiers te wijten is aan een wijziging in de elektronische systemen van de EYP in 2021[350]. Deze wijziging in het nieuwe wettelijke assemblagesysteem zou hebben geleid tot technische problemen die de vernietiging zouden hebben veroorzaakt. Maar andere bronnen stellen dat de heer Kontoleon op 29 juli 2022, dezelfde dag dat Androulakis de ADAE op de hoogte bracht van de surveillancepogingen, de opdracht zou hebben gegeven om deze dossiers te vernietigen[351]. Tijdens een hoorzitting van de commissie PEGA heeft de voorzitter van de ADAE, de heer Rammos, de vernietiging van dossiers niet bevestigd noch ontkend[352].

217. Op 5 augustus dienden de heer Kontoleon en de heer Dimitriadis hun ontslag in. Op 8 augustus erkende de heer Mitsotakis op televisie dat de heer Androulakis werd afgeluisterd, maar beweerde hij wederom daar niet van op de hoogte te zijn geweest[353].

---

344 Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader.*
345 Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
346 News 247. Nikos Androulakis: Near-Victim of Predator Software – Filed a Lawsuit.
347 Avgi. *Predator scandal / EYP dragged to Parliament over surveillance.*
348 Ekathimerini. Androulakis asks ADAE for his wiretapping file.
349 TaNea*. The archive of the surveillance of Nikos Androulakis destroyed.*
350 TVXS. *G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament.*
351 Ieidiseis. *SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.*
352Europees Parlement. Hoorzitting van 8 september 2022.
353 Reuters*. Greek PM says he was unaware of phone tapping of opposition party leader.*

218. Tot nu toe heeft de EYP niet bekend willen maken op welke gronden Androulakis werd bespioneerd. De dienst heeft wel aangeboden de heer Androulakis persoonlijk van de gronden op de hoogte te brengen. Dit zou echter onrechtmatig zijn. De heer Androulakis heeft verzocht om overlegging van zijn surveillancedossier aan het Comité voor instellingen en transparantie, maar zijn verzoek werd geweigerd.

219. Op 7 december 2022 diende de heer Androulakis een klacht in bij het Europees Hof voor de Rechten van de Mens naar aanleiding van de aftapactiviteiten van de EYP en het gebrek aan officiële informatie over zijn zaak[354].

220. Surveillance van politici is zeer ongebruikelijk. De Griekse grondwet verstrekt hun speciale bescherming. De EYP ontkent elke betrokkenheid bij de surveillance met Predator. De regering opperde aanvankelijk dat buitenlandse mogendheden misschien hadden gevraagd om Androulakis af te luisteren, en suggereerde dat hij misschien werd afgeluisterd omdat hij lid was van een EP-commissie die belast was met de betrekkingen met China. Geen van deze hypothesen was erg geloofwaardig. De surveillance vond plaats in de politieke context van nakende verkiezingen. PASOK zou de voorkeurscoalitiepartner worden. In het najaar van 2021 waren er vier kandidaten voor het voorzitterschap van PASOK, elk met verschillende standpunten over een dergelijke coalitie. Van de heer Androulakis werd gezegd dat hij openstond voor het idee, zolang het niet met de heer Mitsotakis als premier was. Een andere kandidaat, Andreas Loverdos, was eerder al minister geweest in een coalitie tussen Nea Demokratia en PASOK, en werd geacht een dergelijke coalitie meer genegen te zijn. Hij was een kennis van Dimitriadis. De publicatie van de lijst van andere vermeende doelwitten door Documento versterkt het vermoeden dat er politieke redenen waren voor de surveillance. Voor geen enkele van deze hypothesen bestaat er bewijs, maar het is van essentieel belang dat deze mogelijkheden worden onderzocht en waar mogelijk uitgesloten.

GIORGOS KYRTSOS

221. Op 15 december 2022 werd bij een controle van ADAE bij telecombedrijf Cosmote bevestigd dat Europees parlementslid Giorgos Kyrtsos door de EYP werd bespioneerd[355]. Zowel zijn mobiele telefoons als zijn vaste lijn werden afgetapt. De surveillanceperiode zou negen keer zijn verlengd[356] gedurende een periode van 18 maanden.

222. Giorgios Kyrtsos is een voormalig lid van Nea Demokratia en de Europese Volkspartij. In februari 2022 zette Nea Demokratia Kyrtsos uit de partij, die Griekenland op dat moment regeerde, wegens zijn afkeuring van de maatregelen van de regering op het gebied van de COVID-19-pandemie, de beperking van de mediavrijheid en de aanpak van het Novartis-schandaal[357]. De heer Kyrtsos werd hierna lid van Renew Europe.

STAVROS MALICHOUDIS

[354] Ekathimerini. *Socialist leader appeals to European Court over tapping.*
[355] Euractiv. *Another MEP and journalist the latest victims of "Greek Watergate".*
[356] Politico. *Greek prosecutor slams unflattering comparisons to Belgium's Qatargate probe.*
[357] Euractiv. *Renew Europe welcomes first Greek MEP who left EPP.*

223. Op 13 november 2021 onthulde de krant Efsyn dat de telefoons van verschillende journalisten die berichtten over de vluchtelingenproblematiek naar verluidt door de EYP werden afgeluisterd. Uit een intern document bleek dat de EYP opdracht had gegeven tot het monitoren en verzamelen van gegevens over de Griekse journalist Stavros Malichoudis[358][359]. Malichoudis schreef over een 12-jarig Syrisch kind dat maandenlang in een detentiekamp op het Griekse eiland Kos moest blijven[360].

224. Op 15 november 2021 bevestigde Giannis Oikonomou, woordvoerder van de regering, de aantijgingen indirect. Hij stelde dat de EYP personen kan afluisteren als "interne of externe bedreigingen" de nationale veiligheid in gevaar brengen[361]. Op 24 november en 17 december 2021 ontkende staatssecretaris George Gerapetritis echter dat er in Griekenland journalisten (waaronder Malichoudis) zouden zijn bespioneerd. Volgens het mediakanaal Solomon echter bevestigde noch ontkende hij de echtheid van de interne documenten van de EYP[362].

225. Tijdens de PEGA-hoorzitting in Griekenland op 8 september 2022 stelde de heer Malichoudis dat de EYP door zijn telefoon af te tappen, ook informatie kon verzamelen over collega's en journalisten met wie hij in die tijd contacten onderhield[363]. De EYP zou hebben meegeluisterd met gesprekken die de heer Malichoudis had met de Internationale Organisatie voor Migratie (IOM)[364], en Malichoudis wijst op het gevaar dat daardoor kan zijn ontstaan voor andere mensen van de zogenaamde "bijvangsten" van de aftapactiviteiten. Voorts presenteerde de heer Malichoudis tijdens de hoorzitting bewijs dat de EYP belangstelling had voor zijn werk en bronnen, maar dat de redenen voor de surveillance niet bekend worden gemaakt omwille van de "nationale veiligheid"[365].

CHRISTOS SPIRTZIS

226. Op 9 september 2022 beweerde de voormalig minister van Infrastructuur en wetgever voor de partij Syriza Christos Spirtzis het doelwit te zijn geworden van een poging tot hacking met de Predator-spyware[366]. Parlementslid Spirtzis had op 15 november 2021 kritische parlementaire vragen bij de regering ingediend over de surveillancebevoegdheden van de EYP. Op diezelfde dag ontving hij een bericht dat vergelijkbaar was met het bericht dat Europarlementslid Androulakis had ontvangen[367]. Op 19 november werd een tweede bericht, met een koppeling naar een artikel in Efimerida ton Syntakton, naar parlementslid Spirtzis verzonden[368]. Hoewel CitizenLab deze berichten niet heeft gecontroleerd, heeft Spirtzis de links die hij heeft ontvangen wel gedeeld met twee technici die mondeling bevestigden dat hij het doelwit was[369]. Op

---

[358] Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.*
[359] Solomon. *Solomon's reporter Stavros Malichudis under surveillance for "national security reasons"*.
[360] BalkanInsight. *Greek Intelligence Service Accused of "Alarming'"Surveillance Activity.*
[361] BalkanInsight. *Greek Intelligence Service Accused of "Alarming" Surveillance Activity.*
[362] Solomon, Solomon*'s* reporter *Malichudos* under surveillance for national security reasons.
[363]Europees Parlement. Hoorzitting van 8 september 2022.
[364] BalkanInsight. *Greek Intelligence Service Accused of "Alarming" Surveillance Activity.*
[365]Europees Parlement. Hoorzitting van 8 september 2022.
[366] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.
[367] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware*.
[368] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware*.
[369] Inside story, *Predator: More than 20 targets in Greece according to the Data Protection Authority*.

9 september 2022 diende Spirtzis een klacht in bij de openbare aanklager van het Hooggerechtshof[370]. Spirtzis is een vertrouwenspersoon van partijleider Alexis Tsipras en is regelmatig aanwezig bij bijeenkomsten op hoog niveau van het partijleiderschap.

TASOS TELLOGLOU, ELIZA TRIANTAFYLLOU EN THODORIS CHONDROGIANNOS

227. Ten tijde van hun onderzoekswerkzaamheden voor de nieuwe nieuwsdienst Inside Story zouden journalisten Tasos Telloglou en Eliza Triantafyllou zijn bespioneerd. In een artikel voor de Heinrich-Böll-Stiftung van 24 oktober 2022 vertelde Telloglou over hoe hij werd bespioneerd en geïntimideerd toen hij onderzoek deed naar de surveillanceschandalen in Griekenland. Hij denkt op basis van zijn waarnemingen dat hij tussen mei en augustus 2022 werd bespioneerd[371].

228. Daarnaast had een bron bij de veiligheidsdienst Telloglou in juni 2022 medegedeeld dat zijn bewegingen en die van zijn collega's Eliza Triantafyllou (InsideStory) en Thodoris Chondrogiannos (Reporters United) door de autoriteiten werden gevolgd om te zien met welke bronnen zij contacten onderhielden[372]. De Griekse regering heeft op het moment van schrijven nog niet op de aantijgingen gereageerd.

229. Op 15 december 2022 werd bij een controle van ADAE bij telecombedrijf Cosmote bevestigd dat Telloglou door de EYP werd bespioneerd. Vanwege "nationale veiligheid" kon de reden voor de surveillance niet worden onthuld[373].

ANDERE DOELWITTEN

230. Op 29 oktober 2022 werd gemeld dat ook andere politici het doelwit waren geweest van de spyware Predator, waaronder een minister die niet op goede voet stond met de premier. Bovendien had een ander lid van Nea Demokratia naar verluidt een link hebben ontvangen om Predator te installeren[374]. De heer Oikonomou, een woordvoerder van de regering, heeft verklaard dat het artikel geen concrete bewijzen bevatte[375].

231. Op 5 en 6 november 2022 bracht Documento verslag uit over een lijst met 33 namen van personen die het doelwit waren geweest van de spyware Predator[376]. Op de lijst stonden veel prominente politici, waaronder leden van de huidige regering, voormalig premier Samaras, voormalig EU-commissaris Avramopoulos, hoofdredacteur van een nationale regeringsgezinde krant, en personen in de entourage van Vangelis Marinakis, eigenaar van een rederij, mediamagnaat en eigenaar van voetbalclubs Olympiakos en Nottingham Forest. De ADAE bevestigde dat sommige namen op de lijst door het EYP werden gecontroleerd door middel van conventionele afluisterapparatuur. Tot deze

[370] Reuters. *One more Greek lawmaker files complaint over attempted phone hacking; Euractiv. Another Greek opposition lawmaker victim of Predator.*
[371] Heinrich-Böll-Stiftung. *A State of Absolute Solitude*.
[372] MapMF, *Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.*
[373] Euractiv, Another MEP and journalist the latest victims of "Greek Watergate".
[374] Ta Nea, *Four illegal manipulations by suspicious center.*
[375] Politico, *Brussels Playbook: Lula wins in Brazil – Trick or trade – Grain deal woes.*
[376] Documento, 6 november 2022.

namen behoren Europarlementslid Giorgos Kyrtsos[377], hoofd van de gezamenlijke stafchefs Konstantinos Floros[378], hoofd van het Griekse leger Haralambos Lalousis[379], minister van Arbeid en Sociale Zaken Kostis Hatzidakis[380], de voormalige directeuren-generaal voor defensiematerieel en investeringen Theodoros Lagios en Aristides Alexopoulos[381], voormalig veiligheidsadviseur Alexandros Diakopoulos[382] en de Griekse onderzoeksjournalist Tasos Telloglou[383].

232. Daarnaast stond ook Meta's voormalige Cybersecurity Policy Manager Artemis Seaford op de lijst van 33 namen en werd bevestigd dat zij tegelijkertijd werd afgeluisterd door het EYP en bespioneerd met Predator. Seaford werd door het EYP afgeluisterd van juli 2021 tot de zomer van 2022, wat betekent dat de toestemming voor het afluisteren van het toestel van mevrouw Seaford zes keer werd verlengd, waarvoor in principe allemaal toestemming nodig is van de interne aanklager van het EYP, Vasiliki Vlachou. CitizenLab bevestigde dat ook haar mobiele telefoon vanaf september 2021 minstens twee maanden lang besmet was met Predator. De Predator-besmetting vond dus ongeveer één tot twee maanden na het begin van de conventionele afluisterpraktijken plaats. Mevrouw Seaford verklaarde dat informatie over haar COVID-19 vaccinafspraak via conventionele afluisterapparatuur uit haar sms-berichten werd verkregen. Deze informatie werd vervolgens gebruikt om een geavanceerde geautomatiseerde SMS te maken, met dezelfde opzet als de officiële afspraak, met het verzoek de afspraak via een link te bevestigen. Door op deze link te klikken werd het apparaat geïnfecteerd met de spyware Predator. De SMS-berichten bevatten nauwkeurige en gedetailleerde informatie over haar vaccinatiedossier, en het werd slechts enkele minuten na de echte, officiële, berichten verzonden, hetgeen erop wijst dat degene die de berichten verzond, toegang had tot de inhoud en de timing van de SMS-berichten, die EYP via de conventionele afluisterprocedure zou hebben gehad.

233. Het afluisteren en/of surveilleren van een particulier is ongebruikelijk, vooral wanneer de nationale veiligheid in een dergelijk geval niet legitiem kan worden ingeroepen. Dit roept de vraag op welke andere motieven een rol kunnen hebben gespeeld bij de targeting. De surveillance vond plaats terwijl mevrouw Seaford bij Meta werkte, een bedrijf dat een dreigingsrapport over de "surveillance-for-hire"-industrie heeft gepubliceerd en meerdere spywarebedrijven, waaronder Cytrox, van zijn platform heeft verbannen. Het is echter hoogst onwaarschijnlijk dat haar rol bij Meta de reden was voor de surveillance. Het dreigingsrapport van Meta werd pas in december 2021 gepubliceerd, enkele maanden later dan het tijdstip waarop het toestel van mevrouw Seaford werd aangevallen, en geen van de andere personen die bij het schrijven van het rapport betrokken waren, was zelf een doelwit. Bovendien verklaarde

[377] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*
[378] https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotakiAvgi,
[379] *https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotaki*
[380] https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/
[381] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/*
[382] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/*
[383] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*

mevrouw Seaford[384] dat zij slechts gedeeltelijk bij deze activiteiten betrokken was en dat Meta zeer discreet is over het vermelden van de namen van haar werknemers.

234. In maart 2021 publiceerde het tijdschrift Marie-Claire een artikel met een passage uit een boekenreeks geschreven door mevrouw Seaford. In het artikel worden Seafords ervaringen vermeld met alledaags seksisme en intimidatie in Griekenland en beschrijft met name een geval van seksuele intimidatie door "een politicus"[385]. De surveillance begon een paar maanden later. Een verklaring kan zijn dat de politicus in kwestie het artikel heeft gelezen en bang was dat zijn naam openbaar zou worden gemaakt. Een andere verklaring zou kunnen zijn dat iemand anders de politicus herkende uit de beschrijving in het artikel, en om politieke redenen meer informatie over die persoon wilde vergaren. Hoe dan ook, slechts zeer weinig personen zouden de macht hebben om zowel een officieel verzoek tot afluistering bij het EYP in te dienen, als om ervoor te zorgen dat Predator spyware wordt gebruikt. De combinatie van surveillance door het EYP en Predator spyware is ook in andere gevallen bevestigd.

235. Het is van belang dat deze mogelijkheden verder worden onderzocht, met name de vraag wie om de surveillance door het EYP heeft verzocht. Mevrouw Seaford heeft een verzoek ingediend bij de ADAE en een klacht ingediend bij de rechtbank in Griekenland. Het onderzoek loopt echter nog steeds. Zij is de eerste bekende Amerikaanse burger die het doelwit is binnen de EU[386][387].

236. Andere namen op de lijst die niet officieel zijn bevestigd, zijn voormalig minister van Onderwijs en Religieuze Zaken Andreas Loverdos, voormalig premier Antonis Samaras, minister van Staat George Gerapetritis, voormalig commissaris Dimitris Avramopoulos, minister Nikos Dendias, minister van Onderwijs Niki Kerameus, minister Akis Skertsos, minister van Investeringen Nikos Papathanasis, voormalig minister van Burgerbescherming Mihalis Chrysochoidis, Vice-minister van Defensie van de Helleense Republiek Nikos Hardalias, Aristotelia Peloni, parlementslid Christos Spirtzis, voormalig minister van Burgerbescherming Olga Gerovasili, hoofd van de Griekse politie Michalis Karamalakis, hoofd van het bureau van de economische aanklager Christos Barkadis, intern aanklager van het EYP Eleni Vlachou, regeringswoordvoerder Giannis Oikonomou, plaatsvervangend hoofd van het EYP Vassilis Grizis; deze onthullingen zijn zeer verontrustend, niet alleen vanwege de prominente namen op de lijst, maar ook omdat het gebruik van spyware systematisch en grootschalig is.

237. In 2023 meldde de ADAE dat de EYP ook een zittende minister, diverse ambtenaren die zich bezighielden met zaken met betrekking tot wapens en een voormalige nationale-veiligheidsadviseur heeft afgeluisterd[388].

---

[384] Bijeenkomst van de commissie PEGA, 20 april 2023.

[385] https://www.marieclaire.gr/art-lifestyle/artemis-seaford-i-chiroteri-morfi-katapiesis-ine-afti-pou-den-katalavenis-oti-ifistase/

[386] *https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html#:~:text=Artemis%20Seaford%2C%20a%20dual%20U.S.,of%20illicit%20snooping%20in%20Europe*

[387] Bijeenkomst van de commissie PEGA, 20 april 2023.

[388] Politico. *Brussels Playbook: Globalization's sanatorium – Vestager rings alarm – S(upended & D(dumped).*

238. Er zijn patronen die erop wijzen dat de Griekse regering het gebruik van spyware tegen journalisten, politici en zakenlieden mogelijk maakt. Het maakt ook de uitvoer van spyware naar landen met een slechte reputatie op het gebied van mensenrechten mogelijk en voorziet in een opleidingscentrum voor agenten uit niet-EU-landen die willen leren over spyware. Hoewel het gebruik van spyware in Griekenland illegaal is, kwam het onderzoek naar de oorsprong van de spyware-aanvallen pas in de zomer van 2022 in een stroomversnelling. Naar verluidt wordt een politieke meerderheid gebruikt voor de bevordering van specifieke belangen in plaats van het algemeen belang, met name door partners en vertrouwelingen in sleutelfuncties binnen onder meer de EYP, EAD (nationale autoriteit voor transparantie) en Krikel (een bedrijf gespecialiseerd in systemen voor elektronische beveiliging) te benoemen. De hoogste politieke leiders van het land gebruiken spyware als instrument voor politieke macht en controle, in sommige gevallen parallel aan of na legale interceptie. Griekenland beschikt in beginsel over een vrij solide rechtskader. Door wetswijzigingen zijn echter cruciale waarborgen afgezwakt, en de politieke benoemingen op sleutelposities belemmeren controle en verantwoordingsplicht. De mechanismen voor controle vooraf en achteraf zijn opzettelijk verzwakt en transparantie en verantwoordingsplicht worden omzeild. Kritische journalisten of functionarissen die corruptie en fraude bestrijden, krijgen te maken met intimidatie en obstructie. In het algemeen is het systeem van waarborgen en toezicht op de surveillance ontoereikend om de burgers te beschermen tegen misbruik door overheidsinstanties en particuliere actoren. Er moet meer worden gedaan om dit probleem aan te pakken. Bovendien wordt het voorwendsel van “nationale veiligheid” aangevoerd als rechtvaardiging voor het afluisteren van personen.

239. Spionage om politieke redenen is niet nieuw in Griekenland, maar de nieuwe spywaretechnologieën maken illegale surveillance veel gemakkelijker, met name in een context van sterk verzwakte waarborgen. In tegenstelling tot andere gevallen, zoals in Polen, lijkt het misbruik van spyware geen deel uit te maken van een geïntegreerde autoritaire strategie, maar veeleer een instrument dat op ad-hocbasis wordt gebruikt voor politiek en financieel gewin. Het leidt echter tot uitholling van de democratie en de rechtsstaat net zo veel en laat veel ruimte voor corruptie, hoewel deze turbulente tijden juist vragen om betrouwbaar en verantwoordelijk leiderschap.

I.D. Cyprus

240. De commissie heeft Cyprus in november 2022 bezocht in het kader van een gezamenlijke missie naar Griekenland en Cyprus. De leden hadden een ontmoeting met de minister van Energie, Handel en Industrie, andere overheidsfunctionarissen en leden van het Huis van Afgevaardigden die zitting hebben in relevante commissies om het huidige rechtskader voor spyware te bespreken. Zij hebben ook geluisterd naar juridische deskundigen, vertegenwoordigers van ngo’s en journalisten die de commissie documentatie over surveillance en corruptie hebben verstrekt. De commissie benadrukte dat er meer moet worden gedaan aan registers van uiteindelijke begunstigden. Deze zijn onvoldoende transparant, hoewel ze werden aangelegd om dergelijke kwesties aan de kaak te stellen.

241. In tegenstelling tot andere lidstaten is er niet veel informatie over het gebruik van

spyware door Cyprus. Er zijn geen officieel bevestigde gevallen van personen die illegaal met spyware worden of werden geviseerd. De journalist Makarios Drousiotis zou echter in februari 2018 door de Cypriotische regering zijn afgeluisterd met zowel afluistertechnieken als spyware[389]. Op papier is er een robuust rechtskader, dat EU-regels omvat, maar in de praktijk blijkt Cyprus een aantrekkelijke plek te zijn voor bedrijven die surveillancetechnologie verkopen. Recente schandalen hebben echter de reputatie van het land geschaad. De regering ontkent dit echter en wijst op een daling van het aantal geregistreerde spywarebedrijven in het land. Naar verwachting zal in 2023 een reeks nieuwe wetgevingsinitiatieven worden voltooid om het rechtskader voor de uitvoer te verstrengen en de naleving te verbeteren.

242. Er zijn nauwe banden tussen Cyprus en Griekenland wat inzake spyware. Intellexa van Tal Dilian is in Griekenland gevestigd en zijn Predator-spyware is gebruikt in Griekse hackingschandalen. Beide landen waren betrokken bij de illegale uitvoer van Predator-spyware naar milities van de Sudanese Rapid Support Forces (RSF)[390]. Griekenland gaf een uitvoervergunning af, terwijl het materiaal vanaf de luchthaven van Larnaca naar Sudan werd verscheept[391].

243. Bovenop de export van spyware naar landen buiten de EU, faciliteert Cyprus ook de handel in subsystemen en spywaretechnologie naar de lidstaten. De naam van UTX Technologies – geregistreerd op Cyprus en gekocht door de Israëlische technologiegigant Verint – is verschenen op facturen van Duitse, Franse en Poolse bedrijven die Gi2-technologie en surveillancesystemen hebben verzonden[392].

244. Op papier is er een wettelijk kader voor de bescherming van particuliere communicatie, de verwerking van persoonsgegevens en het recht op informatie van het individu. In de praktijk zijn er echter, zodra men zich beroept op de nationale veiligheid, geen duidelijke regels voor het gebruik van onderscheppingsapparatuur en de bescherming van de grondwettelijke rechten van de burgers.

RECHTSKADER

DE EU-VERORDENING INZAKE PRODUCTEN VOOR TWEEËRLEI GEBRUIK

245. Cyprus lijkt zeer nauw samen te werken met Israël inzake surveillancetechnologie. Cyprus heeft Israël en de VS geraadpleegd over de hervorming van zijn juridisch kader en het controlesysteem voor de uitvoer van producten voor tweeërlei gebruik. Het land is een populaire bestemming voor tal van Israëlische spywarebedrijven.

246. De afdeling Vergunningen voor de export van strategische producten van het ministerie van Energie, Handel en Industrie reguleert de export van producten voor tweeërlei gebruik[393]. In de PEGA-vragenlijst die naar alle lidstaten werd verstuurd, gaf Cyprus aan alle aanvragen voor exportvergunningen voor producten van tweeërlei gebruik individueel te monitoren en te beoordelen, volledig in overeenstemming met de

[389] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
[390] LightHouse Reports. Flight of the Predator.
[391] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/
[392] Philenews. Cyprus is a pioneer in software exports (documents).
[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument

relevante sanctieregelingen. Het gaat hierbij om de wereldwijde EU-sanctieregeling voor de mensenrechten en de Verordening inzake producten voor tweeërlei gebruik, waarbij de criteria van het relevante gemeenschappelijke standpunt van de Raad (2008/944/CFSP) worden toegepast[394]. De commissie PEGA neemt kennis van het feit dat Cyprus deelnemer is bij de Overeenkomst van Wassenaar betreffende exportcontrole voor conventionele wapens en goederen en technologieën voor tweeërlei gebruik. Tijdens de missie van de commissie PEGA werd aangegeven dat Turkije de deelname van Cyprus aan deze overeenkomst had geblokkeerd. De regering verklaart echter dat zij zich aan dezelfde normen houdt.

247. Het ministerie van Energie, Handel en Industrie kan het zogeheten adviescomité raadplegen over de toekenning van exportvergunningen. Dit comité bestaat uit vertegenwoordigers van het ministerie van Defensie, het ministerie van Justitie en Openbare Orde, het ministerie van Buitenlandse Zaken, het departement Douane en Accijns en andere departementen[395]. Volgens de Cypriotische regering wordt dit comité regelmatig geraadpleegd bij de evaluatie van aanvragen voor exportvergunningen. Er is meerdere malen een vergunning voor de export van producten voor tweeërlei gebruik naar derde landen afgewezen naar aanleiding van een negatief advies van dit comité[396]. De kamer van koophandel geeft gewoonlijk geen informatie over het aantal goedgekeurde en afgewezen licenties voor het in de handel brengen van software[397].

248. Tijdens de missie van de commissie PEGA naar Cyprus op 1 en 2 november 2022 hadden de deelnemers een bijeenkomst met het ministerie van Energie, Handel en Industrie en de viceminister van Onderzoek, Innovatie en Digitaal Beleid. Ministers Natasa Pilides en staatssecretaris Kyriacos Kokkinos stelden dat het aantal in spyware actieve bedrijven in Cyprus sterk was gedaald. Er waren 32 bedrijven geregistreerd, maar volgens de minister waren er ten tijde van het bezoek slechts 8 tot 10 actief, waarvan er drie of vier spyware produceren[398]. Zij erkenden echter ook dat het technisch moeilijk is om toezicht te houden en controle uit te oefenen op in Cyprus gevestigde bedrijven die zelfstandig afzonderlijke spywarecomponenten verkopen.

249. In de praktijk is Cyprus naar verluidt vrij soepel bij het verstrekken van uitvoervergunningen aan spywarebedrijven[399]. Bedrijven gebruiken bepaalde technieken om de regels te omzeilen: de fysieke producthardware, zonder software erop, wordt naar een ontvangend land verzonden[400]. Vervolgens wordt de activeringssoftware (ook wel de “licentiesleutel” genoemd) apart op een USB-stick naar het land van bestemming gestuurd[401]. Een andere werkwijze is om aan te geven dat het product alleen voor demonstratiedoeleinden wordt uitgevoerd, hoewel een gedetailleerde beschrijving van het product is inbegrepen[402]. Bovendien worden onduidelijke beschrijvingen van de spyware ingevuld op het uitvoerformulier voor uitvoervergunningen, hetgeen passende

[394] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[395] Lelaw, “Export Controls for dual-use products”.
[396] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[397] Inside Story, “Who signs the exports of spyware from Greece and Cyprus?”.
[398] Bijeenkomst met Natasa Pilides, minister van Energie, Handel en Industrie, en Kyriacos Kokkinos, staatssecretaris van Onderzoek, Innovatie en Digitaal Beleid, tijdens de PEGA-missie op 2 februari 2022.
[399] InsideStory, “Who signs the exports of spyware from Greece and Cyprus?”.
[400] InsideStory, “Who signs the exports of spyware from Greece and Cyprus?”.
[401] Philenews, “This is how interception patents are exported from Cyprus”.
[402] Philenews, “Export of monitoring software confirmed”.

douanecontroles heeft belemmerd.

250. Er zijn naar verluidt exportvergunningen voor de verkoop van “producten voor tweeërlei gebruik” aan derde landen verleend aan diverse Cypriotische bedrijven. Het zou gaan om UTX Technologies, Coralco Tech, Prelysis en Passitora[403].

251. UTX Technologies is betrokken geweest bij de verkoop van spyware aan EU-lidstaten en derde landen. Tussen 2013 en 2014 werd UTX genoemd op facturen van Duitse (Syborg Informationsysteme), Franse (COFREXPORT) en Poolse (Verint) bedrijven in verband met de handel in surveillancesystemen en Gi2-technologie[404].

252. Het Cypriotische handelsagentschap heeft tijdelijke exportvergunningen verleend aan Cognyte-dochteronderneming UTX Technologies voor de verkoop van surveillancesoftware aan Mexico, de Verenigde Arabische Emiraten, Nigeria, Israël, Peru, Colombia, Brazilië en Zuid-Korea[405]. UTX Technologies heeft naar verluidt ook een contract ter waarde van 3 miljoen USD ondertekend met Thailand voor de verkoop van surveillancesubsystemen. In de beschrijving van deze subsystemen werd verwezen naar een type “tweeledig gebruik” met “algoritmen voor spraakanalyse” en “metadata en spraak”. In de overeenkomst werd ook specifiek verwezen naar een bedrijf uit Litouwen. Aangezien de Cypriotische autoriteiten de exportvergunning weigerden, werd het ministerie van Energie, Handel en Industrie omzeild door de export via het in Litouwen geregistreerde UAB Communication Technologies te laten lopen[406]. De Russisch-Israëlische Anatoly Hurgin is de eigenaar van dit bedrijf. Hij heeft ook een Maltees paspoort[407]. Daarnaast ondertekende UTX een overeenkomst met Bangladesh voor een online inlichtingensysteem ter waarde van 2 miljoen USD in 2019 en een monitoringsysteem voor mobiele telefoons ter waarde van 500 000 USD in 2021[408].

253. Uit de exportoverzichten van Cyprus blijkt ook dat Coralco Tech – oorspronkelijk opgericht in Singapore maar ook geregistreerd in Israël en Nicosia – na een aanbestedingsprocedure in 2018 surveillanceapparatuur met een waarde van 1,6 miljoen USD leverde aan het leger van Bangladesh. De eigenaar van Coralco Tech is de Israëliër Eyal Almog[409].

254. In 2019 kocht de nationale inlichtingendienst van Bangladesh (de NSI) software voor wifi-onderschepping voor een totaalbedrag van 3 miljoen USD van het (in Cyprus geregistreerde) bedrijf Prelysis. Kobi Naveh – de oprichter van Prelysis – werkte tot 2014 voor het Israëlische bedrijf Verint. Verint is ook het bedrijf dat het in Cyprus geregistreerde UTX Technologies overnam[410].

255. In de zomer van 2021 kocht Bangladesh daarnaast een spionagevoertuig van de firma Passitora (voorheen “WiSpear”) van Tal Dilian. Het Zwitserse bedrijf Toru Group

---

[403] Philenews, “Cyprus is a pioneer in software exports (documents)”; Haaretz, “Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record”.
[404] Philenews, “Cyprus is a pioneer in software exports (documents)”.
[405] Philenews, “Cyprus is a pioneer in software exports (documents)”.
[406] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[407] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[408] Haaretz, “Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record”.
[409] Haaretz, “Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record”.
[410] Haaretz, “Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record”.

Limited, geregistreerd op de Britse Maagdeneilanden, fungeerde als intermediair voor de overeenkomsten met Passitora[411].

256. Op 4 oktober 2022 werd bekend dat het Nederlandse ministerie van Defensie in november 2019 op het punt heeft gestaan een overeenkomst te tekenen met WiSpear, het bedrijf van Tal Dilian, dat eerder Cytrox, de fabrikant van Predator-spyware, had overgenomen[412]. Volgens berichten in de media en verklaringen van de voorzitter van DISY (Dimokratikós Sinagermós) heeft WiSpear een e-mail aan regeringspartij DISY en het ministerie van Energie, Handel en Industrie met het verzoek om bijstand bij de uitvoering van de overeenkomst met het Nederlandse ministerie van Defensie[413]. Het is niet duidelijk of het contract uiteindelijk is getekend en of er spyware is geleverd aan het Nederlandse ministerie van Defensie.

257. Uit deze voorbeelden blijkt dat er veel activiteit is in de surveillancesector in Cyprus en dat hierbij dezelfde spelers zijn betrokken als bij het spywareschandaal dat PEGA onderzoekt.

258. Veel Israëlische bedrijven gaan naar Cyprus om hun activiteiten in Europa op te starten[414]. Bovendien blijkt uit verschillende bronnen dat ongeveer 29 Israëlische bedrijven in het land gevestigd zijn[415]. Sommige bronnen wijzen op een nauw verband tussen de handel in spyware en de diplomatieke betrekkingen. In ruil voor de facilitering van vergunningen voor Israëlische bedrijven zou Cyprus producten hebben ontvangen die deze ondernemingen ontwikkelen en uitvoeren, zoals de spyware Pegasus van NSO[416] evenals spyware van WiSpear[417]. Cyprus fungeert als uitvalsbasis voor de commercialisering van Israëlische spyware op de interne EU-markt en de export van spyware naar derde landen.

TOETSING VOORAF

259. In wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie is bepaald dat de procureur-generaal bij het Hof een verzoek in kan dienen om uitgifte van een gerechtelijk bevelschrift waarin de onderschepping van privécommunicatie door een gemachtigde persoon wordt geautoriseerd of verlengd. Dit verzoek van de procureur-generaal aan het Hof vereist een schriftelijk verzoek van de korpschef, de commandant van de Cypriotische inlichtingendienst of een onderzoeksrechter. De bepalingen inzake de toestemming of goedkeuring kunnen echter nietig worden verklaard in gevallen waarin de onderschepping van privécommunicatie het nationale belang dient of om delicten te voorkomen, te onderzoeken of te vervolgen[418].

---

411 Haaretz, “Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record”.
412 https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
413 https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
414 Philenews. Revelations in Greece: Predator came from Cyprus.
415 Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.
416 Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.
417 Inside Story, “Predator: the “spy” who came from Cyprus”.
418 CyLaw, wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie (onderschepping van en toegang tot opgenomen privécommunicatie).

260. Nadat de aanvraag is ingediend, geeft het hoofd van de politie – in overleg met het adjunct-hoofd van de politie en de commandant van de Cypriotische inlichtingendienst – medewerkers van zijn dienst of medewerkers die opdrachten uitvoeren voor zijn dienst schriftelijk toestemming om privécommunicatie te onderscheppen en/of toegang te krijgen tot de surveillanceapparatuur om technische werkzaamheden uit te voeren[419].

261. Voorts wordt in artikel 4, lid 2, van wet 92(I)/1996, zoals gewijzigd in 2020[420], bepaald dat geen enkele persoon apparaten of toestellen die primair zijn ontworpen, geproduceerd, aangepast of vervaardigd om de onderschepping of surveillance van privécommunicatie mogelijk te maken of te faciliteren, mag invoeren, vervaardigen, verkopen of anderszins mag distribueren of er reclame voor mag maken. Bij schending van dit artikel kan een boete van 50 000 EUR en/of een gevangenisstraf van maximaal vijf jaar worden opgelegd[421]. Deze bepalingen zijn niet van toepassing als de leverancier de centrale inlichtingendienst (KYP), de politie en de commissaris op het hoogte heeft gebracht en van hen goedkeuring heeft gekregen. Deze bepalingen zijn niet van toepassing op de surveillancesystemen die worden gebruikt door het hoofd van de politie en de commandant van de KYP[422].

TOETSING ACHTERAF

262. In Cyprus bepaalt de wet die voorziet in de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en voor het vrije verkeer van dergelijke gegevens van 2018 dat wanneer persoonsgegevens van iemand worden gebruikt of verwerkt, deze persoon het recht heeft hiervan op de hoogte te worden gebracht[423]. Er kan een uitzondering op dit recht worden gemaakt wanneer de commissaris gegevensbescherming op gronden van nationale veiligheid beslist dat dat gerechtvaardigd is[424].

263. Voorts wordt in de wet inzake de bescherming van de vertrouwelijkheid van privécommunicatie uit 1996 specificeert dat de procureur-generaal bij onderschepping van privécommunicatie door wetshandhavingsinstanties, verplicht is de betrokken persoon in te lichten. De betrokkene moet worden geïnformeerd binnen een termijn van maximaal negentig dagen vanaf de startdatum van het rechterlijke bevelschrift[425] of binnen een termijn van maximaal dertig dagen vanaf de uitvoering van dit rechterlijke bevelschrift. De procureur-generaal moet de betrokken persoon schriftelijk informeren dat een rechterlijk bevelschrift is uitgegeven en op welke datum, en dat tijdens een zekere periode sprake is geweest van onderschepping van of toegang tot privécommunicatie. Deze verplichting kan tijdelijk worden geschorst als de procureur-

[419] CyLaw, wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie (onderschepping van en toegang tot opgenomen privécommunicatie).
[420] CyLaw. E.U. Par. J VAN WET 13(J)/2020.
[421] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[422] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[423] Wet 125(I) van 2018.
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf
[424] Bureau van de Europese Unie voor de grondrechten, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.
[425] CyLaw, wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie (onderschepping van en toegang tot opgenomen privécommunicatie).

generaal beslist dat het onder meer in het belang van de nationale veiligheid is om deze informatie achter te houden[426]. Het Hof kan ook oordelen dat de informatie niet mag worden bekendgemaakt met het oog op de veiligheidsbelangen van Cyprus[427].

264. Het schenden van de bescherming van privécommunicatie is de jure een strafbaar feit. De facto wordt dit vaak omzeild door zich te beroepen op de nationale veiligheid[428]. Het is niet in de wetgeving vastgelegd hoe de politie of andere inlichtingendiensten de onderscheppingsmiddelen mogen gebruiken; evenmin is bepaald wie de procedures voor onderschepping reguleert of hoe de bescherming van de grondwettelijke rechten van burgers wordt gewaarborgd. De desbetreffende regelingen en protocollen liggen momenteel ter bespreking en goedkeuring voor in het Huis van Afgevaardigden. Vooralsnog blijft deze activiteit ongecontroleerd[429].

VERHAALSMOGELIJKHEDEN

265. De rechtmatigheid van de acties van de Cypriotische inlichtingendienst wordt geëvalueerd door een comité met drie leden, zoals beschreven in de wet inzake de Cypriotische inlichtingendienst (74(I)/2016). Het tripartiete comité wordt benoemd door de ministerraad, op basis van de aanbeveling van de president van de Republiek[430].

266. Wet 92(I)/1996 werd in 2020 gewijzigd om het toezichtkader van de Republiek te versterken, met name de bepalingen over het tripartiete comité. Als onderdeel van zijn mandaat kan het comité ambtshalve een onderzoek inleiden en kan het de voorzieningen, de technische apparatuur en het gearchiveerde materiaal van de KYP aan een onderzoek onderwerpen. Zoals bepaald in artikel 17 A, lid 1, van wet 92(I)/1996, zoals gewijzigd bij wet 13(I)/2020, kan het comité ook de voorzieningen, de technische apparatuur en het gearchiveerde materiaal van de politie aan een onderzoek onderwerpen. In het licht van dergelijke onderzoeken, kan het comité de zaak voorleggen aan de procureur-generaal, de commissaris voor de bescherming van persoonsgegevens of de commissaris voor de reglementering van elektronische communicatie en postdiensten om verdere actie te ondernemen. Het comité dient een jaarverslag in bij de president van de Republiek waarin het zijn activiteiten omschrijft, waarnemingen en aanbevelingen formuleert en omissies aankaart[431].

267. De president van Cyprus heeft een belangrijke stem in de samenstelling van het comité dat bevoegd is om een kritisch onderzoek naar het optreden van de KYP te starten. Bovendien worden de jaarverslagen met de bevindingen van dit comité eerst naar de president gestuurd[432]. Op het moment van schrijven is er geen informatie beschikbaar over de exacte samenstelling van het comité, zijn werkzaamheden of het toezicht op zijn

[426] Bureau van de Europese Unie voor de grondrechten, “Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update”.
[427] CyLaw, wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie (onderschepping van en toegang tot opgenomen privécommunicatie).
[428] Makarios Drousiotis, “ΚράτοςΜαφία”, hoofdstuk 6, 2022.
[429] Philenews. “Legal but uncontrolled interceptions”.
[430] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[431] Antwoord van Cyprus op vragenlijst van het Europees Parlement; CyLaw. E.U. Par. J VAN WET 13(J)/2020.
[432] Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.

functioneren[433].

SLEUTELFIGUREN IN DE SPYWARE-INDUSTRIE

268. Tal Dilian heeft een sleutelrol gespeeld in veel van de ontwikkelingen in Cyprus en Griekenland. In 2017 verwierf hij de Maltese nationaliteit[434]. Hij bekleedde gedurende 25 jaar verschillende leidinggevende functies bij de Israëlische defensiemacht, voordat hij in 2002 uit dienst trad[435]. Dilian startte vervolgens een carrière als "inlichtingendeskundige, gemeenschapsbouwer en serieel ondernemer" in Cyprus en lanceerde Aveledo Ltd., later bekend als WiSpear Systems ltd. en daarna Passitora Ltd[436].

269. In Cyprus ontwikkelde Dilian nauwe banden met Abraham Sahak Avni. Avni was voorheen als rechercheur actief bij de speciale eenheden van de Israëlische politie[437]. In november 2015 werd hij Cypriotisch staatsburger en kreeg hij een gouden paspoort door middel van een investering van 2,9 miljoen EUR in onroerend goed[438]. Avni richtte het Cypriotische bedrijf NCIS Intelligence Services ltd. op[439], dat naar verluidt banden had met de machtigste technologiebedrijven wereldwijd[440]. NCIS Intelligence and Security Services leverde tussen 2014 en 2015 beveiligingssoftware aan het hoofdkwartier van de politie en verstrekte tussen 2015 en 2016 opleidingen aan de medewerkers van het Bureau voor misdaadanalyse en -statistiek[441]. Ook regeringspartij DISY behoorde tot de klanten van de onderneming. Avni installeerde naar verluidt beveiligingsapparatuur in de kantoren van de partij[442]. Naast de beveiligingsapparatuur van Avni werd het materiaal van Dilian ook verkocht aan het Cypriotische Agentschap voor drugshandhaving en de Cypriotische politie[443].

270. Het departement misdaadonderzoek van de politie detecteerde schendingen van de vertrouwelijkheid van privécommunicatie met betrekking tot het bedrijf van Avni. De politie besloot de zaak af te sluiten[444].

271. Er zijn talloze banden tussen Dilian en Avni. WiSpear, de onderneming van Dilian, deelde een gebouw in Lacarna en aantal personeelsleden met Avni[445]. In 2018 lanceerden de twee mannen het bedrijf Poltrex, dat later werd omgedoopt tot Alchemycorp Ltd. Poltrex heeft kantoren in de Novel Tower, net als Avni[446], en maakt

---

433 Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
434 Maltese overheid. Register van genaturaliseerde personen, d.d. 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
435 https://taldilian.com/about/
436 Opencorporates, Passitora ltd.
437 Shahak Avni. Over Shahak Avni.
438 Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
439 Philenews, "FILE: The state insulted Avni and Dilian".
440 Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
441 Philenews, "FILE: The state insulted Avni and Dilian".
442 Tovima, "The unknown "bridge" between Greece and Cyprus for the eavesdropping system".
443 Inside Story, "Predator: The 'spy' who came from Cyprus'.
444 Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
445 Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
446 CyprusMail, "Akel says found "smoking gun" linking Cyprus to Greek spying scandal".

ook deel uit van Intellexa Alliance. Naar verluidt hebben de betrekkingen van Avni met de partij DISY als test voor de producten van Dilian gediend[447].

DE SPYWAREBESTELWAGEN VAN DILIAN

272. Na de verkoop van Circles technologies en de oprichting van WiSpear richtte Tal Dilian in 2019 ook Intellexa Alliance op, dat volgens haar eigen website "een in de EU gevestigd en gereguleerd bedrijf is dat ernaar streeft technologieën te ontwikkelen en te integreren om inlichtingendiensten meer zeggenschap te geven"[448]. Er zijn verschillende surveillanceleveranciers die onder het marketinglabel van Intellexa Alliance vallen, zoals Cytrox, WiSpear (later omgedoopt tot Passitora Ltd.), Nexa technologies en Poltrex Ltd. Deze verschillende verkopers in de groep van Dilian s'bedrijven stellen Intellexa in staat een breed assortiment surveillancesoftware en -diensten aan haar klanten te leveren en te combineren[449]. Meer gedetailleerde informatie over deze bedrijfsstructuur is te vinden in het hoofdstuk over de spyware-industrie.

273. Op 5 augustus 2019 gaf Dilian een interview aan het tijdschrift Forbes over zijn zwarte WiSpear-bestelbus, waarin hij opschepte over de verschillende spywarediensten die zijn alliantie levert. Met de bestelbus ter waarde van 9 miljoen EUR konden apparaten op een afstand van 500 meter worden gehackt[450]. De publieke belangstelling die het interview in Forbes[451] wekte, had tot gevolg dat de Cypriotische autoriteiten een onderzoek startten. De advocaat Elias Stefanou werd benoemd als onafhankelijke strafrechtelijke onderzoeker voor de zaak. Tijdens het onderzoek ontdekten de autoriteiten dat Dilian ook actief was geweest op de internationale luchthaven van Larnaca[452].

274. Op 16 juni 2019 zou Tal Dilian een niet-contractuele relatie zijn aangegaan met Hermes Airports voor gebruik van zijn WiSpear-apparatuur, zogenaamd om het wifi-signaal voor passagiers op de internationale luchthaven van Larnaca te versterken, waarna drie wifi-antennes werden geïnstalleerd[453]. Het Israëlische bedrijf Go Networks, dat niet op Cyprus geregistreerd is, was ook betrokken bij de onderhandelingen die tot de overeenkomst leidden[454]. De echte reden achter de overeenkomst was echter om de aftaptechnologie van WiSpear te gebruiken. De onderschepte gegevens van passagiers werden opgeslagen op de servers in de serverruimte van de luchthaven, nabij het kantoor in Larnaca dat WiSpear met Avni deelde[455]. In de periode dat de antennes werden gebruikt, werden gegevens van 9 507 429 mobiele apparaten onderschept[456].

275. Naar aanleiding van de klachten tegen Dilian, had het Israëlische Go Networks naar verluidt banden had met Intellexa, omdat zij gezamenlijk eigenaar waren van

[447] Inside Story, "Predator: The 'spy' who came from Cyprus'.
[448] https://intellexa.com/
[449] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[450] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[451] Forbes, "A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van".
[452] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[453] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[454] Makarios Drousiotis, "ΚράτοςΜαφία", hoofdstuk 6, 2022.
[455] Makarios Drousiotis, "ΚράτοςΜαφία", hoofdstuk 6, 2022.
[456] Makarios Drousiotis, "ΚράτοςΜαφία", hoofdstuk 6, 2022.

ondernemingen in Ierland. Voormalige hooggeplaatste vertegenwoordigers van het Israëlische Go Networks zouden bij Intellexa toppositities hebben gekregen[457]. Bovendien bleek uit het politieonderzoek dat aan WiSpear uitvoervergunningen waren verleend voor "systemen voor interceptie ontworpen voor het extraheren van stemgeluid of gegevens, overgebracht over de etherinterface"[458] [459]. De bedrijven van Dilian hebben volgens de kamer van koophandel in de afgelopen twee jaar geen exportvergunningen verkregen. Op het moment van schrijven is het nog onduidelijk wie deze exportvergunningen heeft geautoriseerd[460].

276. De elektronische gegevens die in het kader van het onderzoek uit de in beslag genomen apparatuur werden gehaald, werden onderworpen aan een forensische analyse op drie niveaus: door de politie, een academische deskundige en Europol[461]. De bestelwagen wordt door de politie in bewaring gehouden, maar het is niet duidelijk wat er is gebeurd met de surveillanceapparatuur. Naar verluidt is deze apparatuur aan Dilian teruggegeven, maar dit is niet bevestigd.

277. Op 15 november 2021 werd een zaak aanhangig gemaakt bij het strafhof, met WS WiSpear Systems Ltd, Tal Dilian en twee andere medewerkers van WiSpear in de beklaagdenbank. Procureur-generaal George Savvides besloot bijgevolg de zaak tegen het bedrijf WiSpear voort te zetten, maar de strafrechtelijke aanklachten tegen Dilian en de medewerkers werden geseponeerd[462]. De redenen achter dit besluit zijn gerubriceerd. De procureur-generaal kan echter op elk willekeurig moment beslissen de zaak tegen de drie personen opnieuw te openen.

278. Op 22 februari 2022 pleitte WiSpear in het hof van assisen schuldig ten aanzien van 42 beschuldigingen. Het bedrijf kreeg boetes voor een bedrag van 76 000 EUR opgelegd[463]. WiSpear bekende schuld ten aanzien van de beschuldigingen van illegale onderschepping van privécommunicatie en schendingen van de voorschriften inzake gegevensbescherming[464]. Het hof maakte zijn eindoordeel bekend en stelde hierin het volgende: "het hof van assisen heeft vastgesteld dat bij de schending waaraan het bedrijf schuldig is bevonden, op geen enkel moment sprake was van intentie, hacken [of] aftappen, en dat geen poging daartoe is gedaan en het niet de bedoeling was data te personaliseren. Het hof benadrukte dat er geen schade is berokkend aan individuen"[465]. In aanvulling op de door het hof van assisen opgelegde boete, legde de commissaris voor de bescherming van persoonsgegevens Irini Loizidou Nicolaidou WiSpear ook een boete van 925 000 EUR op voor schendingen van de AVG[466]. Hoewel werd beweerd dat het voorval met de zwarte bestelwagen betrekking had op zaken van nationaal

[457] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[458] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.
[459] Philenews. Export of tracking software from Cyprus.
[460] Inside Story, "Who signs the exports of spyware from Greece and Cyprus?".
[461] Persbericht van de adjunct-procureur-generaal van 10 augustus 2022, zoals verkregen tijdens de PEGA-missie naar Cyprus op 2 november 2022.
[462] Financial Mirror, "Anger after "spy van" charges dropped".
[463] Makarios Drousiotis, "Κράτος Μαφία", Hoofdstuk 6, 2022; Persbericht van de adjunct-procureur-generaal van 10 augustus 2022, zoals verkregen tijdens de PEGA-missie naar Cyprus op 2 november 2022.
[464] Financial Mirror, "Spy van company fined €76,000".
[465] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[466] CyprusMail. Israeli company that deployed "spy van" fined €925,000 for data violations; Financial Mirror, "Anger after "spy van" charges dropped".

belang en kritieke infrastructuur, waren de sancties voor de daders zeer licht. Deze incidenten kunnen politieke implicaties hebben die verder gaan dan de schending van de privacy van passagiers. Aangezien Cyprus zich in veel opzichten op een kruispunt bevindt, zijn er diverse derde landen die mogelijk belangstelling hebben voor informatie over het verkeer van passagiers op de luchthaven Larnaca: zoals Turkije, Israël, Rusland en de VS.

279. De oppositiepartij AKEL uitte haar verontwaardiging over het feit dat Dilian en sommige van zijn personeelsleden buiten vervolging werden gesteld, en hekelde het juridische besluit als een doofpotactie van de procureur-generaal[467]. De Cypriotische regering had immers naar verluidt apparatuur gekocht van het bedrijf van Dilian, en een van de beschuldigde werknemers zou voor NSO hebben gewerkt en de KYP instructies hebben gegeven voor het gebruik van Pegasus[468]. Door de buitenvervolgingstelling blijft de informatie over de banden tussen de onderneming van Dilian en de Cypriotische regering beschermd[469]. De procureur-generaal weigerde de conclusies van het onderzoek te overleggen, ook al had de commissie PEGA hierom verzocht tijdens haar officiële missie in Cyprus. Dit voorbeeld toont aan dat er geen volledige wettelijke garanties zijn voor de rechten op gegevensbescherming van personen door apparatuur voor massale surveillance. Hoewel er op papier rechtsmiddelen bestaan, kunnen de gerechtelijke resultaten worden beïnvloed door de overheid, waardoor de individuele slachtoffers weerloos achterblijven. Uit het onderzoek bleek voorts dat Cyprus een voedingsbodem is geworden voor in Cyprus gevestigde bedrijven om zelf te experimenteren met surveillance-apparatuur.

VERHUIZING NAAR GRIEKENLAND

280. Na de heisa rond de bestelwagen en de rechtszaak heeft de heer Dilian de activiteiten van Intellexa naar Griekenland verplaatst, hoewel hij Cyprus nooit heeft verlaten. Hij is naar verluidt zijn terugkeer naar Tel Aviv aan het plannen[470]. Uit indirecte banden tussen meerdere natuurlijke en rechtspersonen die in Cyprus en Griekenland zijn geregistreerd, blijkt dat de activiteiten van Dilian in Athene zijn overgeheveld[471]. Vervolgens wordt een aantal van de namen genoemd die deel uitmaken van de connecties tussen Cyprus en Griekenland. De hoofdrol van Intellexa SA wordt echter verder toegelicht in het hoofdstuk over Griekenland.

281. De gerechtelijke onderzoeken hadden tot gevolg dat de activiteiten van de heer Avni en de heer Dilian in Poltrex werden overgedragen aan Yaron Levgoren. De heer Levgoren is een permanente ingezetene van Canada. Hij werd aandeelhouder, directeur en secretaris van Poltrex. Levgoren heeft ook banden met Intellexa in Griekenland[472]. Volgens zijn LinkedIn-profiel vertegenwoordigt hij momenteel het in Griekenland gebaseerde Intellexa-bedrijf Apollo Technologies.

[467] Financial Times. Anger after “spy van” charges dropped.
[468] Makarios Drousiotis. ΚράτοςΜαφία. Hoofdstuk 6. Gepubliceerd in 2022.
[469] Makarios Drousiotis. ΚράτοςΜαφία. Hoofdstuk 6. Gepubliceerd in 2022.
[470] Intelligence Online, Israeli cyber tsar Tal Dilian plans Tel Aviv return.
[471] *Haaretz*, As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[472] Philenews, How the spyware scandal in Greece is related to Cyprus.

282. Naast Intellexa Alliance zou ook de NSO-Groep in Cyprus gevestigd zijn. In 2010 zette Tal Dilian samen met Boaz Goldman en Eric Banoun het bedrijf Circles Technologies op, dat gespecialiseerd was in de verkoop van systemen die zwakke plekken in SS7 uitbuiten[473]. Zes jaar later werd Circles Technologies verkocht aan Francisco Partners voor iets minder dan 130 miljoen USD, waarvan 21,5 miljoen USD naar de heer Dilian ging. Deze in Californië gevestigde private-equityfirma verwierf eveneens 90 % van de NSO-groep, wat resulteerde in de fusie van Circles Technologies en de NSO-groep onder de naam L.E.G.D Company Ltd., sinds 29 maart 2016 bekend als Q Cyber Technologies Ltd[474].

283. Volgens het antwoord van de Cypriotische regering aan de commissie PEGA staat er geen juridische entiteit van NSO Group in het Register van bedrijven en intellectueel eigendom. NSO Group heeft geen aandelen in op Cyprus geregistreerde juridische entiteiten. Individuele directieleden van NSO Group hebben echter zes bedrijven opgericht en gekocht. Voorts is er geen register van de ontwikkeling van Pegasus-spyware op Cyprus of de officiële export van de spyware vanuit Cyprus[475].

284. Bij de uitbreiding van Francisco Partners tussen 2014 en 2019 waren zes Cypriotische bedrijven betrokken. ITOA Holdings Ltd., geregistreerd op Cyprus en moedermaatschappij van CS-Circles Solutions Ltd., Global Hubcom Ltd. en MS Magnet Solutions werden aan Francisco Partners toegevoegd. Ms Magnet Solutions is eigenaar van Mi Compass Ltd. CS-Circles Solutions Ltd. is voorts eigenaar van CI-Compass Ltd. CS-Circles Solutions Ltd. bezit naast de Cypriotische entiteiten ook Bulgaarse entiteiten. NSO Group heeft verklaard dat “de Bulgaarse bedrijven op contractbasis onderzoeks- en ontwikkelingsdiensten uitvoeren voor hun respectieve verwante Cypriotische ondernemingen en de producten van het netwerk exporteren voor gebruik door de overheid”[476].

285. De Cypriotische regering ontkent de export en ontwikkeling van Pegasus. Op 21 juni 2022 verklaarde NSO-medewerker Chaim Gelfad echter dat NSO-bedrijven in Cyprus en Bulgarije zich bezighielden met software voor het leveren van inlichtingendiensten[477]. Volgens een document dat door oppositiepartij AKEL met het Europees Parlement is gedeeld, zou de NSO-groep de Pegasus-spyware via een van haar dochterondernemingen in Cyprus hebben uitgevoerd naar een bedrijf in de Verenigde Arabische Emiraten. Een van de dochterondernemingen stelde naar verluidt een factuur van 7 miljoen USD op voor diensten aan de betrokken onderneming[478]. Deze informatie kan echter niet worden bevestigd.

286. Naar verluidt had de NSO-groep ook een actief bedrijf in Cyprus dat een klantenservicecentrum zou huisvesten. In 2017 vond in het Four Seasons Hotel in Limassol een bijeenkomst plaats tussen NSO-medewerkers en Saoedi-Arabische

[473] Amnesty International, Operating from the Shadows.
[474] Amnesty International, Operating from the Shadows.
[475] Antwoord van Cyprus op vragenlijst van het Europees Parlement.
[476] Amnesty International, Operating from the Shadows.
[477] Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.
[478] Akel-verslag, werkbezoek van PEGA aan Cyprus.

klanten om hun de nieuwste mogelijkheden van de Pegasus 3-versie spyware te presenteren. Deze versie bood de nieuwe klikvrije mogelijkheid, waarmee een apparaat kon worden besmet zonder dat er op een link hoefde te worden geklikt, bijvoorbeeld via een gemiste WhatsApp-oproep. De Saoedi-Arabische klanten kochten de technologie onmiddellijk voor 55 miljoen USD[479] [480]. Er moet worden opgemerkt dat het Saoedische regime een jaar later, op 2 oktober 2018, Jamal Kashoggi om het leven bracht in het Saoedische consulaat in Turkije, nadat zijn naasten met Pegasus werden bespioneerd. Dit wordt door de NSO betwist.

287. Volgens CitizenLab waren in 2020 25 overheidsactoren klant van Circles Technologies. Tot deze overheidsactoren behoorden België, Denemarken, Estland en Servië[481]. In 2020 sloot NSO Group zijn Circles-kantoren op Cyprus. Op het moment van schrijven is het nog onduidelijk welke Circles-bedrijven actief zijn op Cyprus[482].

288. Het Israëlische QuaDream is een ander bedrijf dat naar verluidt in verband wordt gebracht met de export van zijn spywareproduct "Reign" vanuit Cyprus. In april 2023 meldden de media dat QuaDream haar Israëlische kantoren zou sluiten[483]. Via InReach, een bedrijf dat sinds 2017 in Cyprus is geregistreerd, werden QuaDream-producten indirect aan klanten verkocht. Zo werden de Israëlische exportcontroles omzeild. De twee bedrijven zijn verwikkeld in een juridisch geschil[484].

289. De huidige directeur en secretaris van InReach is A.I.L. Nominee Services Ltd. Deze onderneming was reeds in 2010 in Cyprus geregistreerd en haar oprichtende aandeelhouder was de huidige plaatsvervangend procureur-generaal Savvas Angelides[485]. De heer Angelides heeft zijn aandelen in A.I.L. Nominee Services verkocht aan Christos Ioannides op 16 februari 2018, enkele weken voordat hij minister van Defensie werd[486]. A.I.L. Nominee Services blijft echter directeur en secretaris van InReach[487] en doet dus zaken met een onderneming die QuaDream-producten uitvoert naar derde landen.

290. In 2011 richtte Abraham Sahak Avni een bedrijf op met Michael Angelides, de broer van de voormalige minister en huidige adjunct-procureur-generaal Savvas Angelides. Hun onderneming S9S is op 10 november 2011 ingeschreven in het handelsregister[488] met de hulp van het voormalige advocatenkantoor van Savvas Angelides[489]. Bovendien werd vastgesteld dat A.I.L. Nominee Services Ltd. de secretaris van S9S is. Gedurende

---

[479] Makarios Drousiotis, ΚράτοςΜαφία, hoofdstuk 6, gepubliceerd in 2022.
[480] Haaretz, Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.
[481] CitizenLab. Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles.
[482] Amnesty International, Operating from the Shadows.
[483] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000
[484] Amnesty International, Operating from the Shadows.
[485] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/ https://opencorporates.com/companies/cy/HE373827
[486] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.
[487] https://opencorporates.com/companies/cy/HE373827
[488] Politis, dossier "Onderscheppingen": Gerubriceerd politierapport (2016) toont aan dat hij alles wist over Avni.
[489] Persbericht van de adjunct-procureur-generaal van 10 augustus 2022 zoals verkregen tijdens de PEGA-missie naar Cyprus op 2 november 2022.

die tijd was Savvas Angelides nog steeds de hoofdaandeelhouder van A.I.L. Nominee Services[490]. Het partnerschap tussen Michael Angelides en de heer Avni werd echter in 2012 ontbonden. Savvas Angelides werd in 2020 plaatsvervangend procureur-generaal en was belast met het onderzoek naar de heer Avni en de heer Dilian in de zaak van het surveillancebusje[491]. In een persverklaring van 10 augustus 2022 verklaarde de plaatsvervangend procureur-generaal dat noch hij, noch zijn familieleden enige band hadden met Tal Dilian. Over het partnerschap tussen Michael Angelides en de heer Avni zei hij dat de "professionele samenwerking vanaf het begin spaak liep, in combinatie met het feit dat de door mijn voormalige advocatenkantoor in opdracht van mijn familielid geregistreerde vennootschap nooit werd geactiveerd" en dus nooit een "belemmering vormde voor mijn betrokkenheid bij de beslissing over de zaak van de "zwarte bestelwagen"[492]. In de persverklaring wordt echter niet verwezen naar de onderneming A.I.L Nominee Services Ltd. van Savvas Angelides, die in juli 2010 werd geactiveerd[493], noch naar de rol van de onderneming als secretaris in het partnerschap tussen zijn familielid en de heer Avni in S9S.

BLACK CUBE

291. Black Cube is een bedrijf dat voormalige werknemers van Israëlische inlichtingendiensten, zoals de Mossad, in dienst heeft. Het bedrijf gebruikt agenten met valse identiteiten. Volgens de New Yorker huurde voormalig CEO van de NSO-groep Shalev Hulio Black Cube in nadat drie advocaten – Mazen Masri, Alaa Mahajna en Christiana Markou – NSO en een gelieerde dochteronderneming in Israël en Cyprus hadden aangeklaagd[494]. In 2018 ontvingen de drie advocaten diverse berichten van zogenaamde bekenden van bepaalde bedrijven en personen die een bijeenkomst in Londen voorstelden. Hulio zei hierover: "In het kader van de rechtszaak op Cyprus heb ik één keer contact gehad met Black Cube", aangezien de rechtszaak "uit het niets kwam en ik wilde begrijpen wat er gaande was"[495]. Black Cube is ook in verband gebracht met spionageschandalen in Hongarije en Roemenië.

AANSCHAF EN GEBRUIK VAN SPYWARE DOOR CYPRUS

292. De Cypriotische regering biedt niet alleen een gunstig exportklimaat voor spywarebedrijven, maar heeft zelf in het verleden ook spyware aangeschaft. Zij zou zelf ook surveillancesystemen hebben gebruikt. Op het moment van schrijven blijft het onduidelijk in welke gevallen Cyprus gebruik heeft gemaakt van conventionele surveillancemethoden of spyware.

---

[490] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://b2bhint.com/en/company/cy/s9s-ltd--%CE%97%CE%95%20296578; https://i-cyprus.com/company/433750

[491] Verslag van Fanis Makridis, PEGA-missie naar Cyprus op 1 november 2022.

[492] Persbericht van de adjunct-procureur-generaal van 10 augustus 2022, zoals verkregen tijdens de PEGA-missie naar Cyprus op 2 november 2022.

[493] https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=271194&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1

[494] The New Yorker, How Democracies Spy on their Citizens.

[495] The New Yorker, How Democracies Spy on their Citizens.

293. Na de verkiezingen van 2013 werd Andreas Pentaras benoemd tot hoofd van de Cypriotische inlichtingendienst en werd surveillance-expert Andreas Mikellis verantwoordelijk voor de bescherming van de communicatie van president Anastasiades. In datzelfde jaar bezocht de heer Mikellis naar verluidt de ISS-beurs voor surveillancetechnologie in Praag, waar hij met Hacking Team zou hebben onderhandeld over de aanschaf van een software met de naam DaVinci[496]. Met de DaVinci-software kunnen applicaties op een mobiele telefoon worden besmet, en de software voldeed daarom niet aan de officiële vereisten voor de opheffing van privacy[497].

294. De door WikiLeaks bekendgemaakte informatie over de contacten tussen de heer Mikellis en Hacking Team duidden erop dat er geen aanbestedingsprocedures werden gevolgd en dat het aangeschafte surveillancesysteem niet naar behoren kon worden geëvalueerd. Aan het begin van 2014 werd de software naar verluidt geïnstalleerd en werden vier medewerkers van KYP, met inbegrip van de heer Mikellis, opgeleid in het gebruik ervan[498].

295. Toen WikiLeaks de aanschaf van de surveillancesoftware van Hacking Teams onthulde, stelde de KYP dat dit systeem alleen werd gebruikt voor nationale doeleinden[499]. Ondanks dat de contacten met Hacking Team via de heer Mikellis liepen[500], was het KYP-hoofd Andreas Pentaras die zijn ontslag indiende toen deze onthullingen aan het licht kwamen[501]. Hij werd opgevolgd door de heer Kyriakos Kouros.

296. Volgens WikiLeaks heeft een andere politieafdeling naar verluidt ook belangstelling getoond voor de aanschaf van een communicatiesurveillancesysteem van Hacking Team. Deze afdeling probeerde het systeem te bemachtigen via Sahak Avni[5021 bis]. Het is echter niet duidelijk om welke politieafdeling het gaat.

DOELWIT MAKARIOS DROUSIOTIS

297. Vanaf februari 2018 zou onderzoeksjournalist Makarios Drousiotis zijn bespioneerd door de Cypriotische regering met behulp van zowel afluistertechnieken als spyware[503]. Deze spionagezaak begon toen de heer Drousiotis assistent was van de Cypriotische EU-commissaris voor Humanitaire Hulp en crisisbeheersing Christos Stylianides en tijdens zijn onderzoek naar de financiële banden tussen president Anastasiades en Russische figuren zoals oligarch Dmitri Rybolovlev. Volgens de heer Drousiotis was het deze laatste functie die de aanzet gaf tot de eerste surveillancepoging[504].

298. Tijdens het onderzoek dat de heer Drousiotis deed naar de Russische connecties verschenen er onthullingen in internationale media over activiteiten van NSO Group op

---

[496] Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 6, gepubliceerd in 2022.
[497] Inside Story, Predator: The "spy" who came from Cyprus.
[498] Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 6, gepubliceerd in 2022.
[499] Inside Story, Predator: The "spy" who came from Cyprus.
[500] Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 6, gepubliceerd in 2022.
[501] CyprusMail, Intelligence chief resigns after spy tech revelations. https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/
[502] Inside Story, Predator: The "spy" who came from Cyprus.
[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 5, gepubliceerd in 2022.
[504] Makarios Drousiotis, ΚράτοςΜαφία, hoofdstuk 5, gepubliceerd in 2022.

Cyprus, waaronder een presentatie van Pegasus 3 in het hotel Four Seasons. CitizenLab verdacht Cyprus er bovendien van een van de landen te zijn die NSO-technologieën gebruiken om communicatie in de computersystemen van het Britse ministerie van Buitenlandse Zaken te onderscheppen[505]. De heer Drousiotis herinnert dat er vanaf dat moment diverse signalen waren dat zijn telefoon was besmet met Pegasus-spyware, waaronder een gemist WhatsApp-gesprek en het feit dat zijn batterij snel leeg raakte en de telefoon warm werd, zelfs als hij niet werd gebruikt[506]. In het licht van deze voorvallen denkt de heer Drousiotis dat de Cypriotische regering – en meer in het bijzonder de Cypriotische inlichtingendienst – achter de besmetting van zijn telefoon zit.

299. In mei 2019 verzond de heer Drousiotis een brief naar president Anastasiades waarin hij zijn bezorgdheid uitte over de surveillance van zijn telefoon, de mogelijke redenen hierachter uiteenzette en de president persoonlijk aansprakelijk stelde mocht er na de spionage iets met hem gebeuren. De heer Anastasiades stuurde de brief door naar het huidige hoofd van de Cypriotische inlichtingendienst, Kyriakos Kouros. De heer Anastasiades en de heer Kouros ontkenden de vermeende surveillance met Pegasus-software beiden en blijven herhalen dat NSO Group niet eens geregistreerd stond op Cyprus[507].

300. In de daarop volgende maanden vonden diverse intimidatiepogingen plaats. Zo verdween er onder meer bewijsmateriaal van de computer van de heer Drousiotis, werden zijn beveiligingscamera's uitgeschakeld en werd hij gevolgd door vreemden. Na het verhaal openbaar te hebben gemaakt en een klacht te hebben ingediend bij de Cypriotische politie, contacteerde de heer Drousiotis Lambros Katsonis, hoofd van de afdeling technische ondersteuning van Panda Security, een Cypriotisch bedrijf gespecialiseerd in antivirusapparatuur. De heer Drousiotis wist echter niet dat de Cypriotische regering deze antivirussoftware ook gebruikte voor haar eigen apparaten. Tegen deze achtergrond lijkt het erop dat Katsonis onder valse voorwendselen naar het huis van Drousiotis werd gestuurd, mogelijk zodat deze de apparaten van Drousiotis in opdracht van de KYP kon besmetten[508].

301. In 2019 werd de heer Drousiotis zich bewust van de verdachte toegang tot zijn Android-telefoon en contacteerde hij Google One Support om te vragen om wat voor toegangspogingen het ging. Google reageert echter in het algemeen niet op zaken die verband houden met surveillance en verwees de klant in kwestie door naar de nationale rechtshandhavingsinstanties[1 bis].Hoewel de heer Drousiotis geen vertrouwen had in de politie, stemde hij er toch mee in zijn apparaten te overhandigen voor forensisch onderzoek[509].

SLOTOPMERKINGEN

302. Cyprus beschikt over een solide rechtskader voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer, voor het verlenen van toestemming

[505] BBC, No 10 network targeted with spyware, says group.
[506] Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 5, gepubliceerd in 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, hoofdstuk 5, gepubliceerd in 2022.
[508] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 5. Gepubliceerd in 2022.
[509] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 5. Gepubliceerd in 2022.

voor surveillance en voor export. In de praktijk lijken de regels echter gemakkelijk te omzeilen en bestaan er nauwe banden tussen de politici, de veiligheidsdiensten en de surveillance-industrie. Het lijkt de lakse toepassing van de regels te zijn die Cyprus zo aantrekkelijk maakt voor handel in spyware. De bestaande regels moeten beter worden uitgevoerd. Cyprus is ook van aanzienlijk strategisch belang voor Rusland, Turkije en de VS. Bovendien lijken de nauwe betrekkingen met Israël bijzonder gunstig voor handel in spyware. Uitvoervergunningen voor spyware zijn een valuta geworden in de diplomatieke betrekkingen.

I.E. Spanje

303. Naar aanleiding van de uitnodiging van de commissie PEGA zijn de Spaanse autoriteiten uitgenodigd voor een hoorzitting op 29 november 2022 om verantwoording af te leggen over het gebruik van spywaresurveillance in Spanje, voor zover mogelijk binnen hun wettelijke verplichtingen. Vanwege deze verklaarde "wettelijke beperkingen" waren de antwoorden aan het commissie beperkt en bleven de meeste vragen onbeantwoord.

304. De commissie PEGA heeft in maart 2023 een bezoek gebracht aan Madrid. De delegatie had een ontmoeting met de staatssecretaris voor Europese Zaken en mensen die volgens CitizenLab het doelwit waren van spyware, namelijk de voorzitter van de regionale regering van Catalonië, de Catalaanse regionale minister van Buitenlandse Zaken en een gemeenteraadslid van de stad Barcelona. Zij hadden ook ontmoetingen met leden van de Enquêtecommissie Pegasus van het Catalaanse parlement, een vertegenwoordiger van het bureau van de ombudsman, ngo's die actief zijn op het gebied van de grondrechten, en journalisten.

305. Uit de onthullingen van het Pegasus-project van juli 2021 bleek dat er sprake was van een groot aantal vermeende doelwitten in Spanje. Deze lijken echter het doelwit te zijn geweest van verschillende actoren en om verschillende redenen. In mei 2022 werd in een rapport in de krant *The Guardian* vermeld dat Marokko mogelijk meer dan 200 Spaanse mobiele telefoons heeft bespioneerd. De Spaanse regering bevestigde dat premier Pedro Sánchez, minister van Defensie Margarita Robles en minister van Binnenlandse Zaken Fernando Grande-Marlaska zijn besmet met Pegasus-spyware. Minister van Landbouw Luis Planas was wel doelwit, maar werd niet besmet[510]. Zij suggereerde eveneens dat ook de mobiele telefoon van de toenmalige minister van Buitenlandse Zaken, Arancha González Laya, is bespioneerd, ook al kon in dit geval de herkomst van de cyberaanval niet worden vastgesteld en niet worden bevestigd of het gebruikte systeem Pegasus was. Het geval van een tweede groep doelwitten wordt "CatalanGate" genoemd[511]. Hiertoe behoren Catalaanse parlementsleden, leden van het Europees Parlement, advocaten, journalisten, leden van maatschappelijke organisaties, academici en enkele familie- en personeelsleden die banden hebben met deze doelwitten,[512] die kunnen worden gecategoriseerd als doelwitten van "indirecte"

[510] 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 mei 2022.
[511] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022.
[512] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 1.

surveillance of van “surveillance via naasten”. Over het “CatalanGate”-surveillanceschandaal werd voor het eerst bericht in 2020, na een gezamenlijk onderzoek door *The Guardian* en *El País*[513], maar de omvang van het schandaal werd pas duidelijk toen CitizenLab in april 2022 zijn diepgaande onderzoek voltooide. Uit de resultaten van dat onderzoek bleek dat ten minste 65 personen doelwit waren[514]. Er moet worden opgemerkt dat CitizenLab vanaf december 2022 heeft erkend dat één besmetting ten onrechte is toegeschreven aan de gevolgen van een fout in de etikettering van de initialen[515], hoewel het totale aantal Catalaanse doelwitten ongewijzigd is gebleven. In mei 2022 hebben de Spaanse autoriteiten toegegeven dat zij 18 personen surveilleren met toestemming van de rechter[516], hoewel de bevelen voor die zaken niet openbaar zijn gemaakt. De voormalige directeur van het Spaanse nationale inlichtingencentrum (CNI) Paz Esteban verscheen voor de commissie staatsgeheimen van het Parlement tijdens een vergadering achter gesloten deuren om de surveillance van deze 18 personen te rechtvaardigen.

306. De Spaanse regering heeft tot nu toe beperkte informatie gegeven over haar rol in deze surveillance en beklemtoont de noodzaak van vertrouwelijkheid vanwege juridische en nationale veiligheidsredenen. Op basis van een reeks indicatoren[517], waarvan sommige zijn erkend door de bovengenoemde commissie staatsgeheimen, wordt echter aangenomen dat de surveillance van de Catalaanse doelen door de Spaanse autoriteiten is uitgevoerd.

307. Uit een grondige analyse van de surveillance komt een duidelijk patroon naar voren. De meeste onderscheppingen van CatalanGate vallen samen met en hebben betrekking op belangrijke politieke gebeurtenissen, kwesties of figuren, zoals de ontvankelijkheid van de afscheidingswetten door het Catalaanse parlement, de rechtszaken tegen Catalaanse separatisten, door Tsunami Democràtic georganiseerde openbare bijeenkomsten en communicatie met Catalaanse separatisten die buiten Spanje wonen[518]. Dergelijke surveillance heeft bijvoorbeeld betrekking op communicatie tussen een gedetineerde separatist en zijn advocaat in de aanloop naar diens rechtszaak, contacten tussen echtgenoten of communicatie over de bezetting van zetels in het Europees Parlement. Met betrekking tot de overige 47 gevallen van spyware kon niet worden beoordeeld hoe de doelwitten een onmiddellijke impact op de nationale veiligheid of de integriteit van de staat zouden hebben gehad of hoe zij een onmiddellijke bedreiging daarvoor vormden, en hierover werd geen informatie verstrekt[519]. Hoewel tegen sommige personen die het doelwit waren, strafrechtelijke vervolging was ingesteld voordat zij het

[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware

[514] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 1.

[515] Citizen Lab, *Correcting a case,* verslag CatalanGate https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/, 22 december 2022.

[516] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.

[517] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 1+3.

[518] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022.

[519] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022.

doelwit waren, is tegen geen van de 18 personen die het doelwit waren van spywaresurveillance een strafrechtelijke vervolging ingesteld[520].

AANSCHAF VAN SPYWARE

308. De Spaanse autoriteiten hebben eerder de aanschaf van instrumenten voor de onderschepping van telecommunicatie en de aankoop van SITEL (Systemen voor de legale interceptie van telecommunicatie) in 2001 erkend. Zij erkenden ook dat het ministerie van Binnenlandse Zaken, het CNI en de Spaanse nationale politie in 2010 bij Hacking Team een contract hadden gesloten voor spywarediensten in het kader van de uitvoering van het geïntegreerde telecommunicatie-onderscheppingssysteem, waarbij het de operationele eenheden van de wetshandhavingsdienst (FCSE) de middelen verschafte om elektronische communicatie te onderscheppen en op te nemen als een rechter hiervoor toestemming heeft gegeven[521]. Sinds de aanschaf is SITEL door de Spaanse autoriteiten onder meer gebruikt bij drugsbestrijdinginitiatieven, om de leden van de jihadistische cel die achter de aanslagen in Madrid van 11 maart 2004 zat te lokaliseren en om gevallen van politieke corruptie te bestrijden. Ook maakte CitizenLab eerder bekend dat Spanje een vermoedelijke klant van Finfisher was[522]. In 2020 meldde de Spaanse krant El País dat Spanje zaken heeft gedaan met de NSO-groep en dat het CNI routinematig gebruikmaakt van Pegasus[523]. De Spaanse regering zou de spyware in de eerste helft van de jaren 2010 hebben gekocht voor een bedrag van naar schatting 6 miljoen EUR[524] [525]. Vicepresident de la Vega bevestigde de aanschaf van SITEL in 2009[526] en het CNI gaf in een commentaar in de krant El Confidencial in 2015 toe dat een beroep is gedaan op de diensten van Hacking Team[527]. Bovendien heeft een voormalige werknemer van NSO bevestigd dat Spanje een rekening heeft bij het bedrijf[528], hoewel de Spaanse autoriteiten dit niet willen toelichten of bevestigen[529].

309. Volgens de Threat Analysis Group (TAG) van Google zou het in Barcelona gevestigde Variston IT in verband kunnen worden gebracht met een structuur die misbruik maakt van zero-day-kwetsbaarheden in Microsoft Defender, Chrome en Firefox door spyware te installeren op bepaalde apparaten. Deze kwetsbaarheden werden in 2021 en aan het

[520] Missie naar Spanje.
[521] Ministerio del Interior, Secretaría de Estado de Seguridad, Centro Tecnológico de Seguridad, Homeland Security Project, scetse.ses.mir.es/publico/cetse/nl/proyectosEuropeos/fondoISF/marcoFinanciero-2021-2027/proyectosEuISF
[522] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 5.
[523] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 5.
[524] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 20 april 2022.
[525] El País, https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html, 20 april 2022.
[526] Newtral, https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/, 9 mei 2022.
[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/, 6 juli 2015.
[528] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 April 2022.

begin van 2022 gecorrigeerd[530]. Volgens zijn website biedt Variston "op maat gemaakte oplossingen voor de beveiliging van informatie" aan[531].

RECHTSKADER

310. Het recht op privacy wordt beschermd door artikel 18 van de Spaanse grondwet van 1978, evenals het recht op geheimhouding van communicatie, en in het bijzonder garanties inzake "post-, telegraaf- en telefoonverkeer[532]". Het gebruik van spyware zoals Pegasus en Candiru zou een schending van artikel 18 vormen zonder rechterlijk bevel, een mogelijkheid waarin de Spaanse wetgeving voorziet[533]. De grondwet voorziet ook in verdere uitzonderingen op deze rechten in deel I, sectie 55, door te bepalen dat sommige rechten kunnen worden opgeschort onder voorbehoud van "medewerking van de rechter en passende parlementaire controle" indien is overeengekomen een noodtoestand of beleg af te kondigen overeenkomstig de bepalingen van de grondwet of in het geval van personen tegen wie een onderzoek loopt wegens activiteiten die verband houden met gewapende groepen of terroristische organisaties[534]. Artikel 55 bevat eveneens democratische waarborgen die garanderen dat een ongerechtvaardigde of onrechtmatige uitoefening van dergelijke bevoegdheden tot strafrechtelijke aansprakelijkheid leidt.

311. Voor activiteiten die de onschendbaarheid van de woning en het communicatiegeheim kunnen aantasten, vereist artikel 18 van de Spaanse grondwet een rechterlijk bevel. Artikel 8 van het EVRM vereist voorts dat elke inmenging in de uitoefening van dit recht door een overheidsinstantie in overeenstemming moet zijn met dit recht het maatregelen betreft die, in een democratische samenleving, noodzakelijk zijn met het oog op de nationale veiligheid, openbare veiligheid, het economische belang van het land, de bescherming van de openbare orde of het voorkomen van misdrijven, de bescherming van de volksgezondheid of zedelijkheid, of de bescherming van de rechten en vrijheden van anderen.

312. Op de uitzonderingen op het recht op privacy uit hoofde van artikel 18 wordt uitgebreider ingegaan in het Wetboek van Strafvordering.[535] [536]. Artikel 588 van deze wet beperkt het gebruik van onderzoeksmaatregelen uitdrukkelijk tot het onderzoek van feiten die wegens hun bijzondere ernst een beperking van de grondrechten rechtvaardigen. Desalniettemin worden de volgende instrumenten in de gevallen waarin wordt voorzien van deze bepalingen uitgesloten: a) Organieke wet 2/2002 van 6 mei

---

[530] Threat Analysis Group. *New details on commercial spyware vendor Variston.; Techcrunch. Spyware vendor Variston exploited Chrome, Firefox and Windows zero-days, says Google.*

[531] *https://variston.net/*

[532] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, sectie 18.

[533] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx**,** sectie 18.

[534] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, sectie 55.

[535] Wet strafvordering 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.

[536] Koninklijk besluit van 14 september 1882 tot goedkeuring van de wet op de strafvordering, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907.

2002 tot regeling van de voorafgaande rechterlijke controle op de nationale inlichtingendienst; b) Organieke wet 4/1981 van 1 juni 1981 inzake noodtoestanden, uitzonderingstoestanden en staat van beleg; en c) Organieke wet 2/1989 van 13 april inzake de militaire procedure, die aanvullende bepalingen bevat die van toepassing zijn op de wet inzake de strafvordering. Artikel 588 van de wet vereist dat een rechter toestemming moet geven voor de onderschepping van telefoon- en telematische communicatie wanneer onderzoek wordt gedaan naar ernstige misdrijven, zoals terrorisme of misdaden die worden gepleegd met computerondersteunde instrumenten of elke andere informatie- of communicatietechnologie of een communicatiedienst. Voorts moeten beperkingen worden goedgekeurd door een rechterlijke instantie. Voor vergunningen gelden vier specifieke beginselen: ten eerste, specialisatie (de surveillance heeft betrekking op een specifiek misdrijf); ten tweede, adequaatheid (afbakening van de duur, de objectieve en de subjectieve reikwijdte); ten derde, evenredigheid (sterkte van het beschikbare bewijsmateriaal, ernst van de zaak en nagestreefde resultaat), en ten slotte het uitzonderlijke karakter en de noodzaak (er zijn geen andere maatregelen beschikbaar en zonder die maatregelen wordt het onderzoek verstoord)[537]. Artikel 588 septies (a, b en c) bepaalt specifiek de voorwaarden voor het doorzoeken van computers op afstand. De bevoegde rechter kan op grond van artikel 588 septies de installatie autoriseren van software om een computer op afstand en telematisch te onderzoeken zonder dat de eigenaar of gebruiker hier weet van heeft, mits dit gebeurt met betrekking tot een onderzoek naar bepaalde strafbare feiten. Hiertoe is de maatregel strikt beperkt tot een strikte looptijd van één maand, die met perioden van één maand kan worden verlengd tot maximaal drie maanden.

313. Artikel 197 van het strafwetboek voorziet in straffen van twaalf maanden tot vier jaar gevangenisstraf en een boete van 12 tot 24 maanden voor personen die zonder correcte toestemming onder meer elektronische post en telecommunicatie in beslag nemen of onderscheppen[538]. Daarnaast regelt artikel 264 van het strafwetboek verder de strafbare handeling van het wissen of verwijderen van gegevens en geeft het toegang tot de gegevens in situaties waarin de vereiste toestemming is verleend door een bevoegde autoriteit[539].

314. De vereisten voor gerechtelijk toezicht zijn: a) de gerechtelijke politie moet de onderzoeksrechter op de hoogte houden van de uitvoering en resultaten van de maatregel; b) de rechter moet in de onderliggende rechterlijke uitspraak specificeren met welke frequentie en in welke vorm de gerechtelijke politie hen op de hoogte moet houden van de uitvoering van de maatregel; c) de gerechtelijke politie moet binnen de vastgestelde termijnen de rechter twee verschillende digitale dossiers ter beschikking stellen, een met de transcriptie van de passages die worden verondersteld van belang te zijn en een met de volledige opnamen; d) de opnames moeten de oorsprong en

---

[537] . Wet strafvordering 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf

[538] Wetboek van Strafrecht 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, artikel 197.

[539] Wetboek van Strafrecht 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, artikel 264.

bestemming van elke communicatie aangeven; e) de gerechtelijke politie moet een geavanceerd elektronisch verzegelings- of ondertekeningssysteem gebruiken of een voldoende betrouwbaar waarschuwingssysteem hanteren om de echtheid en integriteit te garanderen van de informatie die wordt overgebracht van de centrale computer naar de digitale media waarop de communicatie wordt opgenomen; en f) de gerechtelijke politie moet na afloop van de uitvoering van de maatregel verslag uitbrengen met de resultaten ervan.

315. De Spaanse inlichtingendienst bestaat uit drie hoofdorganen. In de eerste plaats de Nationale Inlichtingendienst (CNI)die zijn opdrachten vervult door het verzamelen van informatie in Spanje en overzee en handelt onder toezicht en controle van de uitvoerende, wetgevende en rechterlijke macht en aanhet ministerie van Defensie verbonden is[540]. De directeur van het CNI wordt benoemd door de minister van Defensie en is de belangrijkste adviseur van de premier op het gebied van inlichtingen en contra-inlichtingen[541]. Het tweede orgaan is de binnenlandse inlichtingendienst, het Inlichtingencentrum voor Terrorismebestrijding en Georganiseerde Misdaad (CITCO). Het derde orgaan is het Inlichtingencentrum van de Spaanse strijdkrachten (CIFAS). Het CIFAS staat eveneens onder direct toezicht van het ministerie van Defensie[542] [543]. Het CNI is opgericht bij wet 11/2002 van 6 mei 2002, die het CNI machtigt "veiligheidsonderzoeken" te verrichten[544]. Het orde- en wetshandhavingsagentschap van het land, de "Guardia Civil", heeft een "militair karakter" en legt ook verantwoording af aan het ministerie van Defensie[545].

316. De wet op staatsgeheimen, die dateert van 1968, heeft betrekking op gerubriceerde documenten in Spanje en bevat geen termijn voor derubricering waarna een staatsgeheim vervalt[546]. Tenzij de regering uitdrukkelijk de vrijgave van documenten beveelt, d.w.z. de uitdrukkelijke derubricering van een document door een ministerie of een andere officiële instantie, blijven deze documenten geheim. Deze wet wordt momenteel herzien door de Spaanse regering, en hoewel er geen termijn is vastgesteld voor de aanneming ervan, is op 1 augustus 2022 een voorontwerp van wet inzake gerubriceerde informatie goedgekeurd. Zij bepaalt dat gerubriceerde informatie binnen een periode van vier tot vijftig jaar openbaar moet worden gemaakt, hoewel deze periode kan worden verlengd.

TOETSING VOORAF

317. De missie van het CNI is de Spaanse regering de informatie en inlichtingen te verschaffen die noodzakelijk zijn om risico's en gevaren te voorkomen en te vermijden die afbreuk doen aan de onafhankelijkheid en integriteit van de staat, nationale belangen

[540] Nationaal Inlichtingencentrum (CNI), https://www.cni.es/
[541] https://www.cni.es/en/intelligence
[542] https://emad.defensa.gob.es/en/?__locale=en.
[543]Centrum voor governance van de veiligheidssector – Genève, Verslag 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf blz. 40.
[544] Wet 11/2002 van 6 mei 2002, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, artikel 5.5.
[545] https://www.guardiacivil.es/es/institucional/Conocenos/index.html.
[546] El Pais, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html, 5 april 2021; Wet op staatsgeheimen uit 1968.

en de stabiliteit van de rechtsstaat en zijn instellingen. De surveillance in Spanje is grotendeels uitgevoerd door het CNI. Het CNI is opgericht bij wet 11/2002 van 6 mei, die het CNI bevoegdheden verleent om "veiligheidsonderzoeken" naar personen of entiteiten te verrichten[547]. Er is echter weinig duidelijkheid over de middelen die worden gebruikt voor of beperkingen aan dergelijke activiteiten[548], aangezien de activiteiten van het CNI, zijn organisatie en interne structuur, middelen en procedures, personeel, voorzieningen, databanken en datacentra, informatiebronnen en informatie of data die kunnen leiden tot kennis van de eerder genoemde kwesties, van vertrouwelijke aard zijn en in de relevante categorie "geheime informatie" vallen[549]. Wet 11/2002 voorziet ook in parlementair, uitvoerend en wetgevend toezicht op het CNI[550]. Het parlementaire toezicht wordt uitgeoefend door de commissie voor het gebruik van en de controle op aan vertrouwelijke middelen toegewezen kredieten (de commissie staatsgeheimen) van het Spaanse Parlement, die in 1995 is opgericht[551]. Door de vertraagde oprichting van de commissie tijdens de 14e zittingsperiode van het Spaanse parlement (verkozen in december 2019) heeft de commissie staatsgeheimen haar jaarverslag over de activiteiten van het CNI niet ingediend, zoals de wet voorschrijft. In april 2023 is tijdens deze zittingsperiode geen jaarverslag ingediend. De door de regering gedelegeerde commissie voor inlichtingenzaken coördineert de inlichtingenactiviteiten van alle Spaanse inlichtingen- en informatiediensten[552]. Ten slotte oefent de Defensiecommissie van het Congres van Afgevaardigden wetgevend toezicht uit op het CNI[553]. De jaarlijkse inlichtingenrichtlijn formuleert de prioriteiten van het CNI.

318. Organieke wet 2/2002 van 6 mei 2002[554] [555] voorziet in rechterlijke controle op de activiteiten van het CNI, die wet 11/2002 van 7 mei tot regeling van het CNI aanvult. In het bijzonder vereist deze verordening dat wanneer het CNI toezicht tracht uit te voeren, de staatssecretaris en de directeur van het CNI de verplichting heeft om toestemming te vragen aan een bevoegde magistraat van het Hooggerechtshof overeenkomstig de organieke wet van de rechterlijke macht, om de vaststelling van maatregelen die de onschendbaarheid van de woning en de geheimhouding van de communicatie beïnvloeden[556], toe te staan, op voorwaarde dat dergelijke handelingen noodzakelijk zijn voor de uitoefening van de taken van het CNI. Voorts wordt in de wet bepaald dat surveillance-activiteiten niet langer dan drie maanden mogen duren en dat verlengingen

[547] Wet 11/2002 van 6 mei 2002, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 mei 2022.
[549] Wet 11/2002 van 6 mei 2022 tot regeling van de nationale inlichtingendienst, artikel 5.1.
[550] Wet 11/2002 van 6 mei 2002, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 11.
[551] Wet 11/1995 van 11 mei 1995, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[552] Wet 11/2002 van 6 mei 2002, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 6.
[553] Wet 11/2002 van 6 mei 2002, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 11.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 mei 2022.
[555] Wet 2/2002 van 6 mei 1995, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html
[556] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 mei 2022.

van deze periode naar behoren gemotiveerd moeten worden. Deze bepalingen werden echter vastgesteld op een moment dat surveillancetechnologie nog veel minder geavanceerd was en spyware als Pegasus en Candiru nog niet bestond. Derhalve bestaat het risico dat de juridische waarborgen verouderd zijn en burgers onvoldoende bescherming bieden. Daarom kondigde de uitvoerende macht aan dat zij het juridische kader van het CNI zou hervormen, maar er zijn nog geen voorstellen ingediend.

TOETSING ACHTERAF

319. Bij de wetten tot oprichting van het CNI werd ook de Defensiecommissie van het Congres van Afgevaardigden opgericht, dat verantwoordelijk is voor de toewijzing van de geheime fondsen voor het CNI en voor het opstellen van een jaarverslag over het CNI. De bedragen die aan geheime fondsen worden toegewezen, zijn vastgesteld in de Spaanse algemene begrotingswet voor elk boekjaar[557]. Alle organen die belast zijn met het toezicht op het CNI, zoals de Defensiecommissie, de commissie staatsgeheimen of de ombudsman, hebben toegang tot de noodzakelijke informatie om te beoordelen of de operaties rechtmatig en correct zijn uitgevoerd. De regering formuleert in de inlichtingenrichtlijn, die vertrouwelijk is, jaarlijks de doelstellingen van het CNI en keurt deze goed[558] [559]. De directeur van het CNI heeft de exclusieve bevoegdheid om te beslissen over het doel en de bestemming van de toegewezen middelen en moet periodiek verslag uitbrengen aan de premier over het gebruik ervan. De commissie staatsgeheimen wordt op de hoogte gebracht van de doelstellingen van de inlichtingendiensten en heeft het voorrecht om jaarlijks een verslag in te dienen over de activiteiten van de inlichtingendiensten[560]. Zij heeft ook toegang tot het jaarverslag van de directeur van het CNI over de evaluatie van de activiteiten en de situatie van het CNI en de mate waarin het zijn doelstellingen heeft bereikt. De Spaanse wet bepaalt echter niet dat het publiek toegang krijgt tot documenten of informatie over de werkzaamheden van de inlichtingendiensten. Deze eis ontbreekt ook opvallend in het rechtskader van de wet op de transparantie[561]. Gezien deze geheimhouding kan niet met zekerheid worden vastgesteld of de Spaanse regering contracten met de NSO-groep heeft gesloten en of zij Pegasus heeft aangeschaft en gebruikt. De personen die doelwit waren kennen de redenen, de omvang en de gevolgen van de onderschepping van hun communicatie niet[562].

320. Naar aanleiding van de onthulling dat het CNI Pegasus en Candiru zou hebben gebruikt, kondigde de Spaanse ombudsman een ambtshalve onderzoek[563]. In de officiële verklaring van de Spaanse ombudsman van 18 mei 2022 werd erkend dat de ministerraad de ombudsman volledige toegang tot gerubriceerde documenten had

[557] Wet 11/1995 van 11 mei 1995 tot regeling van het gebruik van en de controle op aan vertrouwelijke middelen toegewezen kredieten, artikel 2, https://www.boe.es/eli/es/l/1995/05/11/11/con
[558] Wet 11/2002 van 6 mei 2002 tot regeling van de nationale inlichtingendienst (CNI), artikel 3.
[559] CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 2.
[560] Wet 11/1995 van 11 mei 1995 tot regeling van het gebruik van en de controle op aan vertrouwelijke middelen toegewezen kredieten, artikel 7, lid 4.
[561] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022. 2.
[562] Amnesty International – 10 medidas que garanticen la no repeticion de violaciones des Derechose Humanos.
[563] https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6, 24 april 2022

verleend, zonder gebruik te maken van zijn voorrecht als bedoeld in artikel 22 van organieke wet 3/1981 inzake de ombudsman. Dit onderzoek had echter alleen betrekking op de 18 personen waarvan de Spaanse autoriteiten hebben bevestigd dat zij, met toestemming van de rechter, werden gesurveilleerd[564] [565]. Het onderzoek concludeerde dat de onderscheppingen binnen de wet waren uitgevoerd omdat was vastgesteld dat een rechtbank deze had goedgekeurd en de toestemming vergezeld ging van de vereiste rechtvaardiging[566]. De ombudsman is echter niet bevoegd om de evenredigheid te beoordelen, die alleen door een rechter kan worden bepaald[567]. Hij heeft ook geen contact opgenomen of gesprekken gevoerd met de betrokkenen of hun advocaten. De ombudsman beval, waar nodig, een herziening aan van de huidige wettelijke bepalingen en hervormingen om de modernisering van de surveillancesystemen weer te geven[568]. Als gevolg hiervan kondigde de Spaanse regering in mei 2022 een herziening aan van de wet op staatsgeheimen uit 1968 en de Organieke wet 2/2002[569] [570], al is er geen tijdsbestek vastgesteld voor de goedkeuring van deze herziening.

321. De Commissie staatsgeheimen moet jaarlijks een verslag indienen over de activiteiten van de inlichtingendiensten. Zij werd op 5 mei 2022 bijeengeroepen in het licht van de surveillance-activiteiten van het CNI, maar dit was de eerste vergadering van het orgaan in meer dan drie jaar wegens de onderbreking van de parlementaire activiteiten als gevolg van de COVID-19-pandemie. Het hoofd van de CNI, Paz Esteban, verscheen voor de commissie en gaf toe 18 leiders van de afscheidingsbeweging te surveilleren. Zij heeft ook de gerechtelijke uitspraken voor die 18 zaken aan de commissie voorgelegd[571] [572]. Overeenkomstig artikel 5, lid 5, van wet 11/2002 vond de hoorzitting echter achter gesloten deuren plaats en mochten de aanwezigen geen elektronische apparaten meenemen[573]. Er werd geen officiële informatie verstrekt, met uitzondering van het aantal zaken. Volgens de woordvoerders die bij de hoorzitting aanwezig waren, ging de sessie bijna uitsluitend over de Catalaanse doelwitten en niet over Pedro Sánchez, Margarita Robles en de 3 GB aan data die van hun apparaten zou zijn afgetapt

[564] The Guardian, https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking, 5 mei 2022.
[565] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/
[566] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 mei 2022.

[567] Informatie over de missie naar Spanje.
[568] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/
[569] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 mei 2022.
[571] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.
[572] El País, https://elpais.com/espana/2022-05-05/la-directora-del-cni-da-explicaciones-sobre-el-espionaje-de-pegasus-ante-el-escepticismo-de-los-partidos.html, 21 mei 2022.
[573] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.

met behulp van spionagesoftware[574]. Robles heeft herhaaldelijk volgehouden dat het surveilleren van de 18 Catalaanse doelwitten gerechtvaardigd was.

322. Sánchez heeft ook over de kwestie gesproken in het Spaanse Parlement waar hij wederom benadrukte dat op elk moment binnen de grenzen van de wet is gehandeld en dat het Spaans Parlement en andere overheidsorganen toezicht houden op de nationale veiligheid[575]. Ook de voormalige CEO Shalev Hulio van NSO Group stelt dat het gebruik van Pegasus door het CNI volledig legaal was. Hij vertelde The New Yorker dat het gebruik van Pegasus door Spanje rechtmatig was gezien de grote eerbied voor de rechtsstaat in Spanje en de vereiste toestemming van het hooggerechtshof[576].

323. Op 3 mei 2022 stemde het Spaanse Congres tegen een voorstel om een onderzoekscommissie in te stellen naar het gebruik van Pegasus. Op 21 september 2022 heeft het Catalaanse parlement een onderzoekscommissie ingesteld naar de spionage van politieke vertegenwoordigers, activisten, journalisten en hun gezinnen door het Koninkrijk Spanje met de programma's Pegasus en Candiru.

OPENBAAR TOEZICHT

324. Sinds de onthullingen in april 2022 aan het licht kwamen, is het gebruik van spyware tegen leden van de Spaanse regering en voorstanders van de Catalaanse onafhankelijkheid veelvuldig in het openbaar onderzocht. De Spaanse media en mediakanalen over de hele wereld hebben intens samengewerkt met maatschappelijke organisaties om het surveillancesysteem in Spanje onder de loep te nemen en hebben gepleit voor de grondrechten van de gesurveilleerde personen. Omgekeerd hebben sommige Spaanse politici geprobeerd CitizensLab in diskrediet te brengen door te suggereren dat hun methoden ondeugdelijk zijn of dat ze politiek gemotiveerd zijn.

VERHAALSMOGELIJKHEDEN

325. Het Openbaar Ministerie heeft bij de Spaanse nationale rechtbank (SNC) te Madrid, de Audienca Nacional, een rechtszaak aangespannen naar aanleiding van de surveillance door middel van spyware van minister-president Pedro Sánchez en minister van Defensie Margarita Robles[577]. De bevoegdheid van de SNC is vastgelegd in artikel 65, lid 1 bis, van de Organieke wet 6/1985 betreffende de rechterlijke macht. Volgens dit artikel vallen de vermeende feiten onder de bevoegdheid van de SNC aangezien zij betrekking hebben op personen in hoge nationale organen, zoals de premier en de minister van Defensie. Rechter José Luis Calama, hoofd van de centrale rechtbank van instructie nummer 4, is verantwoordelijk voor deze lopende zaak[578]. Op 13 oktober 2022 diende rechter Calama een vragenlijst in bij Robles en Grande-Marlaska, met

[574] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.
[575] . La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26 mei 2022.
[576] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[577] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.
[578] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.

daarin een vraag over hoe de Pegasusbesmettingen werden ontdekt. Het antwoord moest worden gestaafd met juridische bronnen. Ook het Openbaar Ministerie en het bureau van de openbare aanklager verzonden vragen aan de ministers[579].

326. Bij de onderzoeksrechtbank in Barcelona zijn gerechtelijke klachten naar aanleiding van spywaresurveillance aangespannen door personen die directe of indirecte banden hebben met de Catalaanse onafhankelijkheidsbeweging, en onderzoeken zijn lopende, zij het in een traag tempo. De eerste klacht werd in 2020 ingediend door Roger Torrent, voormalig voorzitter van het Catalaanse parlement en huidig minister van Handel en Werk, van Catalonië, en Ernest Maragall, voormalig minister van Buitenlands Optreden, Institutionele Betrekkingen en Transparantie van Catalonië en huidig ERC-voorzitter in de gemeenteraad van Barcelona[580] [581]. De zaak werd toegewezen aan onderzoeksrechtbank nummer 32 in Barcelona, die de zaak voorlopig sloot. Andreu Van Den Eynde is een van de advocaten die Torrent en Maragall in deze zaak vertegenwoordigen, en werd zelf gesurveilleerd met Pegasus. Van Den Eynde heeft kritiek geuit op het feit dat de rechtbanken de procedure consequent vertragen en de zaak vrijwel "verlammen"[582]. Omnium Cultural, de Assemblea Nacional Catalana (ANC) en de partij Candidatura d'Unitat Popular (CUP) hebben verschillende strafrechtelijke klachten ingediend bij dezelfde rechtbank in Barcelona, maar er is nog geen onderzoek ingesteld. Onderzoeksrechtbank nummer 32 in Barcelona heeft het verzoek om gezamenlijke rechtszaken afgewezen, zodat deze nu door verschillende rechtbanken en rechters worden behandeld. De klachten van Òmnium Cultural en CUP zijn toegewezen aan onderzoeksrechtbank nummer 21 in april 2022, en die van de ANC aan rechtbank 23 op 26 juli 2022. De klachten zijn nog niet volledig in behandeling genomen en er is ook nog geen overeenstemming bereikt over het instellen van een onderzoek. De meeste zaken zijn door de rechters geseponeerd totdat meer bewijsmateriaal is verzameld, aangezien het belangrijkste bewijsmateriaal – de vermeende besmette mobiele telefoons – niet in het bezit van de eisers was[583]. Rechters kunnen besluiten de rapporten van CitizenLab te aanvaarden als deskundig bewijs in de zaak. Als de rechters dit echter niet toestaan, wordt het voor de betrokkenen moeilijk om hun zaak te hard te maken[584].

327. Aangezien de SNC in heel Spanje bevoegd is voor de ernstigste strafzaken, zou het openbaar ministerie kunnen verzoeken dat alle Pegasus-zaken worden samengevoegd[585]. Met andere woorden, de zaken van diegenen die werden gesurveilleerd door de Spaanse regering en de "CatalanGate"-doelwitten zouden allemaal in de Spaanse nationale rechtbank in Madrid worden behandeld. De advocaten

[579] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.
[580] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.
[581] El Diario, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30 mei 2020.
[582] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 mei 2022.
[583] El Pais, https://elpais.com/espana/catalunya/2022-05-30/el-juez-de-barcelona-archiva-de-forma-provisional-la-causa-por-el-espionaje-con-pegasus-a-torrent-y-maragall.html, 30 mei 2022.
[584] Missie naar Spanje.
[585] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.

van de Catalaanse doelwitten beweren dat er geen verband is tussen de zaken, tenzij bewezen wordt dat de dader in alle gevallen dezelfde is[586].

328. Er loopt nog een aantal andere rechtszaken in verband met de 65 Catalaanse doelwitten. Eén daarvan is door advocaat en Pegasus-doelwit Gonzalo Boye namens ten minste 19 doelwitten aangespannen tegen NSO, haar drie oprichters Niv Karmi, Shalev Hulio en Omri Lavie, Q Cyber Technologies en OSY, een dochteronderneming in Luxemburg[587] [588]. Voormalig Catalaans president Quim Torra en voormalig vicevoorzitter van het Catalaanse parlement, Josep Costa, hebben een klacht ingediend bij het Hooggerechtshof, maar een jaar later moet nog steeds worden beslist door de rechterlijke macht of de zaak voor het Hooggerechtshof of het SNC moet worden behandeld. Er heeft inmiddels nog geen onderzoek plaatsgevonden. Ook in Frankrijk, België, Zwitserland, Duitsland en Luxemburg lopen rechtszaken over het toezicht op Catalaanse separatisten in ballingschap[589].

DE DOELWITTEN

329. Het met spyware surveilleren van leden van de Catalaanse onafhankelijkheidsbeweging en hun familie en personeel begon naar verluidt al in 2015, toen de toenmalige voorzitter van de Assemblea Nacional Catalana (ANC), Jordi Sánchez, kort na een grote demonstratie in Barcelona het doelwit werd. Volgens het CitizenLab-verslag van april 2022 werden ten minste 65 personen tussen 2017 en 2020 het slachtoffer van spyware: 63 van Pegasus, vier van Candiru en ten minste twee personen van allebei[590]. De toestellen van ten minste 51 personen werden met succes besmet[591]. Onder degenen die direct of indirect gesurveilleerd zouden zijn, bevonden zich politieke figuren die voorstander zijn van de onafhankelijkheid van Catalonië, zoals de minister van Handel en Werk en voormalig voorzitter van het Catalaanse parlement, Roger Torrent; de huidige voorzitter van de Esquerra Republicana de Catalunya (ERC) in de gemeenteraad van Barcelona en voormalig minister van Buitenlands Optreden, Institutionele Betrekkingen en Transparantie van Catalonië, Ernest Maragall; en vier leden van het Europees Parlement. Gezien het aanzienlijke tijdsverloop sinds het begin van de hack en deze onthullingen, kon een aantal doelwitten vanwege verschillende factoren niet worden geïdentificeerd of verder onderzocht; zo waren enkele doelwitten niet meer in het bezit van de telefoon in kwestie[592].

330. De Spaanse premier Pedro Sánchez, minister van Defensie Margarita Robles en

---

[586] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.
[587] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, 3 mei 2022.
[588] Catalaans nieuws, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19 april 2022.
[589] Catalaans nieuws, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19 april 2022.
[590] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022. 5.
[591] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 April 2022. 5.
[592] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz. 5.

minister van Binnenlandse Zaken Fernando Grande-Marlaska werden tussen mei en juni 2021 gesurveilleerd met Pegasus[593]. Er is tot dusver weinig informatie beschikbaar over de details van deze hack, aangezien deze door de regering werden onthuld en niet het resultaat waren van een onderzoek van Citizen Lab of een andere onderzoeksdienst of door onderzoeksjournalisten, en zijn nog steeds onderdeel van een lopend onderzoek. Sánchez en Robles zijn de hoofden van de twee regeringstakken die toezicht houden op het CNI, het orgaan dat verantwoordelijk is voor de surveillance in Spanje. De besmette apparaten van Sánchez en Robles waren verstrekt door de overheid en werden af en toe gescand op spyware[594]. Grande-Marlaska werd geïnfecteerd op zijn persoonlijke toestel[595]. Minister van Landbouw Luis Planas, die voorheen als diplomaat in Marokko had gewerkt, was ook het doelwit van spyware maar er vond geen succesvolle infectie plaats. Er is gemeld dat de Marokkaanse regering mogelijk verantwoordelijk is voor deze poging tot surveillance. Die informatie is evenwel niet bevestigd[596].

331. Van de 65 gevallen is bevestigd dat 18 gevallen door de Spaanse autoriteiten werden gesurveilleerd, maar de regering heeft geen commentaar gegeven op de 47 overige personen[597]. Het blijft onduidelijk of de andere personen al dan niet met een gerechtelijk bevel door de CNI werden gesurveilleerd of dat een andere instantie gerechtelijke bevelen had gekregen om hen wettelijk te surveilleren. Ondanks de gerechtelijke bevelen voor het gebruik van spyware op 18 personen, werden zij vervolgens niet beschuldigd van een misdrijf in verband met het bevel tot gebruik van spyware. Onder de doelwitten voor wie de surveillance werd goedgekeurd, behoren huidig Catalaans president Pere Aragonès, voormalig president en huidig parlementslid Carles Puigdemont, en andere Catalaanse onafhankelijkheidsgezinde politici en medestanders[598]. Met inachtneming van de in de wet vervatte vereisten inzake geheimhouding en vertrouwelijkheid heeft minister van Defensie Robles verwezen naar de wet op staatsgeheimen om niet nader in te gaan op de redenen voor de surveillance van deze specifieke doelwitten[599]. De meeste van de 65 Catalaanse doelen zijn op enig moment in contact geweest met de leden van de pro-Catalaanse onafhankelijkheidsbeweging die buiten Spanje wonen. Sommige van de personen die werden gesurveilleerd, bevonden zich buiten Spanje toen de besmetting plaatsvond, onder andere in België, Zwitserland, Duitsland en Frankrijk. Dergelijke digitale surveillance zou in Duitsland illegaal zijn, tenzij de federale overheid uitdrukkelijk toestemming geeft.

332. Een van de belangrijkste groepen die doelwit bleken te zijn, zijn de naar onafhankelijkheid strevende Catalaanse leden van het Europees Parlement. Zij werden

---

[593] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 mei 2022.
[594] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7 mei 2022.
[595] La Razon, https://www.larazon.es/espana/20220510/gwxedc4drzhali5bqi4vbhk7kq.html
[596] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7 mei 2022.
[597] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.
[598] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.
[599] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 mei 2022.

ieder direct of indirect gehackt met spyware via wat Citizen Lab "surveillance via naasten" noemt, oftewel surveillance via naasten[600]: Diana Riba i Giner, Jordi Solé, Carles Puigdemont en Clara Ponsatí. De mobiele telefoon van een voormalig geaccrediteerd medewerker van mevrouw Ponsatí werd met succes met Pegasus besmet. In het geval van Antoni Comín, die tijdens een hoorzitting van de commissie PEGA de Spaanse staat ervan beschuldigde hem te hebben bespioneerd, erkende Citizen Lab dat de besmetting verkeerd was toegeschreven als gevolg van een fout in de etikettering van initialen.

333. De telefoon van Diana Riba i Giner, EP-lid van Esquerra Republicana de Catalunya (ERC), werd op 28 oktober 2019, slechts drie maanden nadat ze zitting neemt in het Parlement, direct geïnfecteerd met Pegasus-spyware. Tijdens een telefoongesprek met haar assistente werd de communicatie onderbroken en hoorde haar staflid een opname van het gesprek dat zij zojuist met Riba i Giner had gevoerd. De timing van deze besmetting viel direct samen met een cruciale rechterlijke uitspraak over de Catalaanse separatisten, waaronder Raül Romeva, echtgenoot van Riba i Giner, die uiteindelijk een straf van twaalf jaar kreeg[601]. Riba i Giner verklaarde tijdens een hoorzitting van de commissie PEGA in het Parlement dat in die tijd het merendeel van haar telefoongesprekken betrekking had op de rechtszaak en dat ze talloze vergaderingen en bezoeken aan de rechtbanken aflegde. Als zodanig was de bijvangst in dit geval ongelooflijk groot, onder wie Romeva en degenen die bij de baanbrekende zaak betrokken waren[602].

334. Volgens het onderzoek van Citizen Lab[603] zou Jordi Solé, lid van het Europees Parlement, ook van de ERC, zowel op 11 als op 27 juni 2020 zijn gehackt. Later kwamen echter nog vijf aanvallen in dezelfde periode aan het licht[604]. Solé ontdekte slechts bij toeval dat hij met Pegasus werd gesurveilleerd toen hij, nadat hij enkele mogelijk verdachte berichten had ontvangen, zijn telefoon inleverde om te laten controleren als onderdeel van een documentaire[605]. Net als bij zijn collega is de timing van deze surveillance opmerkelijk. Dit gebeurde tijdens kritische politieke discussies over de vacante zetel van Oriol Junqueras, die geen toestemming kreeg om zijn functie als lid van het Europees Parlement op te nemen terwijl hij in Spanje[606] gevangen zat, en slechts één maand voordat Solé werd benoemd om desbetreffende zetel in juli 2020 over te nemen. Bovendien waren er toen besprekingen gaande over de partijstrategie en

---

[600] CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz.6.
[601] Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, hoorzitting getuigenis van mevrouw Diana Riba i Giner, lid van het Europees Parlement, Straatsburg, 6 oktober 2022.
[602] Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, hoorzitting getuigenis van mevrouw Diana Riba i Giner, lid van het Europees Parlement, Straatsburg, 6 oktober 2022.
[603] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022. 7.
[604] Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, hoorzitting getuigenis van de heer Jordi Sole, lid van het Europees Parlement, Straatsburg, 6 oktober 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[606] Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken, hoorzitting getuigenis van de heer Jordi Sole, lid van het Europees Parlement, Straatsburg, 6 oktober 2022.

internationale geschillen betreffende hun gevangengenomen en verbannen collega's ten tijde van de infecties[607].

335. Europees Parlementslid Carles Puigdemont voor JUNTS en voormalig president van Catalonië was een doelwit via zijn echtgenote Marcela Topor, personeelsleden en een aantal van zijn medestanders[608]. In totaal meldt Citizen Lab dat tot elf personen in nauw contact met Puigdemont het doelwit waren, waaronder ten minste twee bevestigde infecties op het toestel van Topor op 7 oktober 2019 en 4 juli 2020[609].

336. Clara Ponsatí, lid van het Europees Parlement voor JUNTS en voormalig minister van Onderwijs van Catalonië, was een doelwit via naasten. Pol Cruz, staflid aan het Europees Parlement, werd op 7 juli 2020 geïnfecteerd[610].

337. Sinds 2010 zijn alle presidenten van Catalonië tijdens of na hun ambtstermijn het doelwit geweest van surveillance met spyware[611]. Tot de 65 doelwitten behoorden maar liefst twaalf ERC-leden, onder wie de secretaris-generaal van de partij Marta Rovira. die volgens Citizen Lab in juni 2020 minstens twee keer werd gehackt. Het is veelzeggend dat zowel Gabriel als Rovira in Zwitserland woonden toen zij na de breuk in de nasleep van het referendum van 2017 werden gesurveilleerd.

BURGERDOELWITTEN, MET INBEGRIP VAN JOURNALISTEN, ADVOCATEN EN VERTEGENWOORDIGERS VAN MAATSCHAPPELIJKE ORGANISATIES

338. Jordi Domingo was een van de eerste Catalaanse activisten die in 2020 doelwit zouden zijn geweest. Hoewel hij aanhanger is van de Catalaanse onafhankelijkheid en lid van de Assemblea Nacional Catalana (ANC), geloofde Domingo volgens *The Guardian* dat hij per vergissing tot doelwit was gemaakt. Aangezien hij geen belangrijke rol heeft gespeeld in de gebeurtenissen van 2017, denkt hij dat het beoogde doelwit een gelijknamige advocaat was die heeft bijgedragen aan het opstellen van de potentiële grondwet van een onafhankelijk Catalonië[612].

339. De ANC, een Catalaanse maatschappelijke organisatie die de Catalaanse onafhankelijkheid steunt, was een van de eerste organisaties die voorafgaand aan het Catalaanse referendum het doelwit waren, en is sindsdien het onderworpen aan uitgebreide surveillance[613]. Tot de zes doelwitten van het ANC behoren twee van zijn voormalige voorzitters, Jordi Sanchez (2015-2017) en Elisenda Paluzie (2018-2022),

---

[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9 januari 2020.

[608] CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz.7.

[609] CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz.8.

[610] CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz.7.

[611] Artur Mas (na zijn ambtstermijn), Carles Puigdemont (surveillance via naasten), Joaquim Torra (tijdens zijn ambtstermijn), Pere Aragonès (geïnfecteerd tijdens zijn ambtstermijn als vicepresident van Torra). https://catalonia.citizenlab.ca/

[612] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, 13 juli 2020.

[613] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

wier spywaresurveillance op gerechtelijk bevel werd toegestaan, evenals die van de deskundige op het gebied van digitaal stemmen en decentralisatie, Jordi Baylina, twee leden van zijn nationale raad (Arià Bayè en Sònia Urpí) en een lid van een lokale afdeling (Jordi Domingo).

340. De apparaten van personen uit de omgeving van Jordi Cuixart, voorzitter van Òmnium Cultural (tot februari 2022), werden besmet, omdat hij toen in de gevangenis zat. Onder hen was Marcel Mauri, vicevoorzitter van de ngo, wiens surveillancespyware op gerechtelijk bevel werd toegestaan.

341. Citizen Lab ontdekte in februari 2021 een actieve Candiru-infectie op de laptop van Joan Matamala, een zakenman en activist met nauwe banden met Catalaanse onafhankelijkheidsgezinde politici[614]. Matamala's surveillancespyware werd toegestaan op gerechtelijk bevel. Candiru is aanzienlijk moeilijker te traceren dan Pegasus, en deze ontdekking van een actieve infectie stelde de onderzoekers van Citizen Lab in staat de patronen ervan beter te begrijpen. Hierop werden zestien andere infecties op Matamala's toestel aangetroffen[615]. Microsoft heeft de kwetsbaarheden vervolgens via updates verholpen, maar het is niet bekend hoeveel Candiru-infecties onopgemerkt zijn gebleven[616].

342. Ten minste drie bekende open-sourceontwikkelaars en ondernemers waren het doelwit van Pegasus. Xavier Vives en Pau Escrich, medeoprichters van Vocdoni, een op Ethereum-blockchain gebaseerd open-sourceprotocol voor veilig, censuurbestendig digitaal stemmen, waren beiden het doelwit. Vives werd specifiek in het vizier genomen met Candiru-malware, terwijl tegen Escrich zowel Pegasus als Candiru werden ingezet[617]. Vives en Escrich's surveillancespyware werd toegestaan op rechterlijk bevel.

343. Gonzalo Boye is de advocaat van de voormalige presidenten Puigdemont en Torras[618]. In de vijf maanden tussen januari en mei 2020 was Boye maar liefst 18 keer het doelwit van tekstberichten die als tweets van maatschappelijke organisaties of prominente nieuwsfeiten verschenen[619]. CitizenLab bevestigde ten minste één succesvolle infectie op 30 oktober 2020. De infectie kwam slechts 48 uur na de arrestatie van een van zijn cliënten[620]. De aanval op Boye heeft vragen opgeroepen over de rechtmatigheid van het schenden van de vertrouwelijkheid van de communicatie tussen advocaat en cliënt.

344. Elena Jimenez, internationaal vertegenwoordiger van Omnium Cultural, en Jordi Bosch, advocaat belast met institutionele betrekkingen van Omnium Cultural, waren beiden het doelwit van Pegasus toen zij deel uitmaakten van het juridisch team van Jordi Cuixart. Jimenez stond voortdurend in contact met het volledige juridische team van Cuixart,

---

[614] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[615] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[616] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[617] https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#finding-catalans-targeted-with-candiru
[618] https://catalonia.citizenlab.ca/
[619] https://catalonia.citizenlab.ca/
[620] https://catalonia.citizenlab.ca/

met inbegrip van het internationale team dat een klacht bij het EHRM voorbereidde. Tot nu toe heeft Citizen Lab alleen Jimenez' meest recent aangekochte mobiele telefoon onderzocht, maar ze hebben een succesvolle klikvrije infectie in februari 2020 bevestigd. Bosch, een minder openbaar gezicht van het juridische team, was het doelwit in juli 2020, minder dan een week voordat Cuixart een mildere vorm van detentie kreeg en op dezelfde dag dat hij namens Omnium voor het eerst op de Catalaanse televisie verscheen.

345. Andreu van den Eynde i Adroer, werd op 14 mei 2020 met Pegasus besmet[621]. De hack vond plaats terwijl hij optrad als advocaat van zowel Raul Romeva als Oriol Junqueras in hun zaak voor het Hooggerechtshof.

346. Ook het toestel van advocaat Jaume Alonso-Cuevillas werd besmet toen hij belangrijke Catalaanse figuren zoals Carles Puigdemont vertegenwoordigde. Citizen Lab kon de precieze datum van de succesvolle besmetting echter niet vaststellen.

ONDERZOEKEN EN JURIDISCHE HERVORMINGEN

347. Nadat de beschuldigingen in de zaak "CatalanGate" op 22 april 2022 aan het licht waren gekomen, leidden de Spaanse instellingen een procedure tot toetsing in om ervoor te zorgen dat de richtsnoeren inzake surveillance correct waren toegepast. Deze maatregelen betroffen de oproeping van Paz Esteban, directeur van het CNI, voor commissie staatsgeheimen op 5 mei, aangekondigd door de minister van het voorzitterschap Felix Bolaños; de zitting voor parlementaire toetsing van de regering en de minister van Defensie op 26 en 27 april; en de onafhankelijke beoordeling door de ombudsman, die van start ging op 26 april en op 18 mei werd afgerond. Minister van Defensie Margarita Robles, hoewel gebonden aan geheimhouding in overeenstemming met de wet inzake staatsgeheimen, wees erop dat de maatregelen waren genomen als reactie op de actie van degenen die "de grondwet schenden, publieke infrastructuur overnemen, de openbare orde verstoren en banden hebben met de politieke leiders van een land dat Oekraïne binnenvalt"[622]. De regeringspartij (PSOE) en de drie belangrijkste oppositiepartijen (PP, Vox en Ciudadanos) meldden dat de directeur bevredigende uitleg had verstrekt over de noodzaak en de wettigheid van de surveillancespywaremaatregelen[623] [624].

348. De Spaanse ombudsman concludeerde dat een groot deel van de in Spanje uitgevoerde surveillance door het CNI gebeurde in volledige naleving van de wettelijke procedures. Naar aanleiding van zijn aanbevelingen over de toereikendheid van de parlementaire en gerechtelijke controles, en om de wetgeving te actualiseren, de garanties van gerechtelijke controle te versterken en een maximale eerbiediging van de grondrechten van personen te garanderen, heeft de Spaanse uitvoerende macht zich er niettemin toe

[621] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, blz.10.
[622] El País, https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html, 27 april 2022.
[623] La Vanguardia, https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html, 5 mei 2022.
[624] El Periodico de Espana, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5 mei 2022.

verbonden:

1. binnen het CNI een intern onderzoek in te stellen;

2. een onderzoek in te stellen binnen de commissie omtrent het gebruik en de controle van kredieten voor geheime fondsen van het Spaanse Congres, en een hoorzitting te organiseren waarbij de directeur van het CNI zou verschijnen; alsmede

3. de openbaarmaking aan de commissie over het gebruik en de controle van kredieten die zijn toegewezen aan geheime fondsen van het Spaanse Congres van het Hooggerechtshof; 18 bevelen uit te geven die de inbraken toestaan; en de derubricering van CNI-documenten met betrekking tot de beoogde leden van de pro-Catalaanse onafhankelijkheidsbeweging, op verzoek van een rechter;

4. de Spaanse wet op staatsgeheimen van 1968 te hervormen[625];

5. het rechtskader van het CNI te hervormen[626];

6. een nieuwe inlichtingenrichtlijn, waarin de doelstellingen van het CNI op het gebied van inlichtingen worden vastgesteld, goed te keuren; alsmede

7. de nationale veiligheidsstrategie van 2021 en het cyberbeveiligingsplan bij te werken.

349. Het Hooggerechtshof van Spanje[627] opende een eigen onderzoek nadat de regering stelde dat Pegasus-software werd gebruikt om ministers, waaronder premier Sánchez, te bespioneren. Als onderdeel van een zogeheten onderzoekscommissie om de spionage te onderzoeken, riep het Hof de CEO van het Israëlische bedrijf NSO Group voor Pegasus-spyware en minister Felix Bolaños, op om als getuigen op te treden. De onderzoeksrechter ondervroeg ook de voormalige directeur van het nationale inlichtingencentrum, Paz Esteban[628] [629], en de ministers van Defensie en Binnenlandse Zaken, wier apparaten werden gehackt. Het Hof[630] stuurde de Israëlische regering een formeel verzoek om internationale rechtshulp, waarin het om informatie vroeg over “verschillende aspecten van de softwaretool”. Het Hooggerechtshof heeft ook de geheimhouding van de documenten in verband met de zaak opgeheven en een verbod op onderzoek naar het afluisteren van mobiele telefoons van premier Pedro Sánchez en minister van Defensie Margarita Robles ongedaan gemaakt.

SLOTOPMERKINGEN

350. Spanje heeft een onafhankelijk rechtsstelsel met voldoende waarborgen. Na de

[625] El País, “El Gobierno inicia la reforma de la ley franquista de secretos oficiales”, 5 april 2021.
[626] La Moncloa, “Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías”, 26 mei 2022.
[627] https://www.reuters.com/world/spanish-court-calls-ceo-israels-nso-group-testify-case-spying-with-pegasus-2022-06-07
[628] https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html
[629] https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations
[630] https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations

ontdekking van de twee categorieën doelstellingen in Spanje blijven er echter nog enkele vragen over, die kunnen worden beantwoord door snelle en grondige hervormingen en de daadwerkelijke uitvoering daarvan. De Spaanse regering werkt aan wijzigingen om de tekortkomingen aan te pakken. Wat de hervorming van de CNI betreft, heeft de Spaanse regering op 26 mei 2022 haar voornemen aangekondigd om het rechtskader van de CNI te hervormen, maar er is nog geen voorstel ingediend. Op 1 augustus 2022[631] heeft de regering wetswijzigingen op de wet op staatsgeheimen ingediend. De regering wacht momenteel op het advies van de Raad van State.

351. De 47 personen die in het verslag van het Citizen Lab worden genoemd, voor wie het nog onduidelijk is of zij al dan niet het doelwit waren van het CNI met een rechterlijk bevel, dan wel of een andere autoriteit al dan niet rechterlijke bevelen had ontvangen om hen legaal als doelwit te nemen, zijn niet op de hoogte van de redenen, reikwijdte of actoren die achter de surveillance met Pegasus zitten. Deze personen moeten toegang hebben tot justitie en er moet een onderzoek worden ingesteld om deze zaken op te helderen.

352. Met betrekking tot de 18 gevallen waarvoor een rechterlijk bevel was uitgevaardigd, is de wettigheid ervan gecontroleerd en bevestigd door de ombudsman, maar hun bijzondere aard, adequaatheid, uitzonderlijk karakter, proportionaliteit en noodzaak[632] kunnen alleen door een rechtbank worden gecontroleerd.

353. Meer in het algemeen gaan gerechtelijke procedures door de betrokken personen niet zo snel als gehoopt, met als doel transparantie en toegang tot zinvolle rechtsmiddelen te bieden. Samenwerking door de autoriteiten is hierbij van cruciaal belang. Om meer duidelijkheid te verschaffen en bij te dragen met technische expertise, zou Europol kunnen worden uitgenodigd en steun kunnen verlenen om ervoor te zorgen dat een goed forensisch proces wordt gevolgd.

I.F. Andere lidstaten

NEDERLAND

354. In het regeerakkoord van 2017 staat dat de Nederlandse politie geen hacksoftware mag aanschaffen bij leveranciers die hun producten verkopen aan “dubieuze regimes”, later gespecificeerd als “landen die zich schuldig maken aan ernstige schendingen van de mensenrechten of het internationaal humanitair recht”. Voordat de Nederlandse politie spyware aanschaft, moet zij de leverancier vragen of deze geleverd heeft aan landen waartegen sancties lopen van de EU of de VN, en nagaan of het land waar de leverancier is gevestigd een uitvoercontroleregeling heeft waarbij de mensenrechten in de uitvoervergunningsprocedure worden beoordeeld. Deze beoordeling wordt periodiek herhaald. Daarbij moet worden opgemerkt dat deze beperking alleen lijkt te gelden voor spyware die door de politie wordt aangeschaft. De inlichtingendiensten worden niet uitdrukkelijk genoemd. Volgens de overheid heeft de politie sinds 2019 hacksoftware

631 https://www.mpr.gob.es/servicios/participacion/Documents/MAIN%20APL%20Informaci%C3%B3n%20Clasificada.pdf

632 Artikel 588 bis. i., hoofdstuk IV, wet op de strafvordering.

gebruikt, al vermelden de autoriteiten niet welk type[633]. De NSO-groep lijkt met haar spywareproduct Pegasus niet aan de genoemde normen te voldoen, in ieder geval niet voordat de uitvoerregeling van Israël in december 2021 werd aangescherpt[634]. Er werd geen inzicht gegeven in de uitgaven van zowel politie- als inlichtingendiensten voor de aanschaf en het gebruik van het spywaresysteem.

355. In Nederland is in 2018 een nieuwe instantie (Toetsingscommissie Inzet Bevoegdheden – TIB) opgericht om vooraf te toetsen of de toestemming van de regering aan de inlichtingendiensten om surveillancetechnieken in te zetten rechtmatig was. De surveillance kan niet plaatsvinden als de TIB de toestemming onrechtmatig acht. De TIB is een aanvulling op het belangrijkste toezichtsorgaan, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De CTIVD houdt, nadat de toestemming werd gegeven, toezicht op de lopende surveillance-activiteiten van de inlichtingendiensten en behandelt klachten.

356. Er wordt op gewezen dat de NSO-groep van november 2014 tot december 2016 kon opereren dankzij twee in Nederland gevestigde vennootschappen, Shapes 1 BV en Shapes 2 BV, die werkzaam zijn in de sectoren “financiële holdings” en “ingenieurs en ander technisch ontwerp en advies”. Beide werden na twee jaar operationeel te zijn weer geliquideerd[635].

357. Op 4 oktober 2022 werd bekend dat het Nederlandse ministerie van Defensie in november 2019 op het punt stond een overeenkomst te tekenen met WiSpear, het bedrijf van Tal Dilian, dat eerder Cytrox, de fabrikant van Predator-spyware, had overgenomen[636]. WiSpear had een aanbesteding van het Nederlandse ministerie gewonnen. Uit de e-mailcorrespondentie is niet duidelijk of het Predator of een ander product betreft. Uit openbaar gemaakte e-mails die zijn uitgewisseld tussen het Cypriotische ministerie van Energie, Handel en Industrie en WiSpear, blijkt dat een vertegenwoordiger van het Nederlandse ministerie van Defensie op 13-15 november 2019, slechts enkele dagen voordat het “spionagebusje”-verhaal van Dilian uitkwam, contact had opgenomen met het Cypriotische ministerie van Handel om garanties te krijgen over WiSpear. Dilian deelde de vertegenwoordiger van het Cypriotische ministerie van Handel mee dat hij haar onmiddellijke bijstand in deze zaak op prijs zou stellen, aangezien de termijn voor de ondertekening van de contracten bijna zou verstrijken[637]. Het is niet duidelijk of het contract uiteindelijk is getekend en of er spyware is geleverd aan het Nederlandse ministerie van Defensie.

358. In Nederland bevindt zich ook een dochteronderneming van Cognyte die geregistreerd staat als Cognyte Netherlands B.V. Zoals blijkt uit een uittreksel van de Nederlandse Kamer van Koophandel is de enige aandeelhouder van de Nederlandse dochteronderneming het in Cyprus gevestigde UTX Technologies. Zoals beschreven in het hoofdstuk over Cyprus en de spyware-industrie, heeft UTX Technologies een

[633] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland
[634] https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021
[635] Amnesty International, “Operating from the Shadows: Inside NSO Group’s corporate structure”, https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[636] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[637] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.

geschiedenis van export van inlichtingen- en volgsystemen naar Bangladesh en verzending van surveillancesystemen naar EU-lidstaten. Bovendien was het Israëlische bedrijf Verint – dat tevens eigenaar was van Cognyte vóór de afsplitsing ervan in 2021 – de belangrijkste leverancier van het surveillancesysteem aan de Nederlandse politie[638]. De banden tussen de politie en deze Israëlische leverancier worden nog duidelijker, als we constateren dat de voormalige politieman Robert van Bosbeek sinds 2014 de rol van bestuurder van Cognyte Netherlands B.V. op zich heeft genomen[639]. Een andere bestuurder van deze Nederlandse dochteronderneming, David Abadi, is ook de CFO van het Israëlische Cognyte Software Ltd dat in verband is gebracht met de verkoop van onderscheppingsspyware aan Myanmar[640].

359. Op 2 juni 2022 meldden de media dat de Nederlandse inlichtingendienst Algemene Inlichtingen- en Veiligheidsdienst (AIVD) Pegasus heeft gebruikt toen deze de politie bijstond bij het opsporen van een verdachte van een ernstig misdrijf, Ridouan T., die hoofdverdachte werd van meerdere moorden in verband met georganiseerde criminaliteit, drugshandel en het leiden van een criminele organisatie, en op 16 december 2022 in Dubai werd gearresteerd[641]. De Nederlandse overheid weigerde te reageren. Dit is een opmerkelijk geval dat nadere aandacht verdient. De lekken vonden plaats toen Pegasus en de NSO-groep onder veel publieke kritiek stonden, en de zwarte lijst van het Amerikaanse ministerie van Handel de NSO-groep financieel pijn deed. Het Nederlandse succesverhaal van de vangst van een persoon die een van de meest gezochte criminelen in jaren was, was een welkom positief bericht voor het bedrijf. Het mediabericht is gebaseerd op verklaringen van vier bronnen binnen de AIVD. Hun motief voor het lek wordt er niet in vermeld. Ook lijkt er geen onderzoek te zijn gedaan naar het lekken, wat de vraag oproept of het lek de goedkeuring had van de AIVD-directie. Het is echter hoogst onwaarschijnlijk dat de AIVD zou toestaan dat een dergelijk verhaal naar buiten komt, zonder medeweten en goedkeuring van de Israëlische autoriteiten.

BELGIË

360. In een interview met The New Yorker onthulde een voormalige Israëlische inlichtingenambtenaar dat de Belgische politie Pegasus gebruikt bij haar operaties[642]. In reactie daarop verklaarde de Belgische politie dat zij geen uitspraken zou doen over eventuele technische en/of technische middelen die voor onderzoeken en missies worden gebruikt. In september 2021 verklaarde minister van Justitie Vincent Van Quickenborne dat Pegasus op een legale manier door de inlichtingendiensten kan worden gebruikt, maar wilde hij niet bevestigen of de Belgische inlichtingendienst klant is van NSO of spyware inzet tegen criminelen[643].

361. El Mahjoub Maliha, mensenrechtenactivist uit de Westelijke Sahara, die in België woont, en Carine Kanimba, dochter van de Rwandese politieke activist Paul

[638] Volkskrant: “Achterdeur in het nationale aftapsysteem van de politie, Israëli’s konden meeluisteren”.
[639] Kamer van Koophandel: Bedrijfsprofiel – Cognyte Netherlands B.V. (34139430).
[640] Reuters: “Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show”.
[641] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/
[642] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
[643] https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html

Rusesabagina, zijn ook bespioneerd via Pegasus-software terwijl zij in België waren, en zelfs tijdens ontmoetingen met Belgische regeringsambtenaren. De spyware-aanvallen werden naar alle waarschijnlijkheid uitgevoerd door, of namens, respectievelijk de Marokkaanse en de Rwandese autoriteiten. Rwanda wordt er ook van beschuldigd Pegasus-spionagesoftware te gebruiken tegen critici die in Belgische ballingschap leven, waaronder prominente oppositieleden Placide Kayumba en David Batenga[644]. De Belgische militaire inlichtingendienst ADIV ontdekte verder dat Pegasus zeer waarschijnlijk door Rwanda was geïnstalleerd op de smartphone van de Kagame-kritische Belgische journalist Peter Verlinden en zijn vrouw Marie Bamutese[645]. Andere Belgische doelwitten van het gebruik van spyware zijn voormalig premier Charles Michel en zijn vader Louis Michel (toen lid van het Europees Parlement, voormalig commissaris en minister van Buitenlandse Zaken). Volgens Belgische media zou de Marokkaanse regering achter de aanvallen zitten[646].

DUITSLAND

362. Duitse entiteiten die gebruikmaken en hebben gebruikgemaakt van hacking zijn de Bundesnachrichtendienst, de Federale Inlichtingendienst of BND, het leger en de douane- en politiediensten. De BND is het agentschap dat het meest gebruikmaakt van hacking. In 2009 hadden ze al 2 500 toestellen gevolgd[647].

363. Duitsland heeft een rechtskader dat het gebruik van spyware regelt. Sinds 2008 verleent de Duitse federale wetgeving aan de politie hackbevoegdheden in gevallen van internationaal terrorisme en ter voorkoming van terroristische aanslagen[648]. In 2017 is een nieuwe wet in werking getreden, waardoor elke rechtshandhavingsinstantie bij 42 strafbare feiten mag gebruikmaken van overheidshacking. Deze delicten omvatten onder meer het indienen van frauduleuze asielaanvragen, belastingontduiking en drugsdelicten[649]. In 2021 heeft de Bondsdag het wetsontwerp van de Bondsregering "houdende aanpassing van de wetgeving inzake de bescherming van de grondwet" aangenomen. Hiermee wordt hacken door de staat gelegaliseerd voor alle 19 Duitse inlichtingendiensten[650] en worden aanbieders van communicatiediensten verplicht om bij hackactiviteiten samen te werken met de staat[651].

364. Hackwetten in Duitsland worden vaak gerechtvaardigd in het licht van misdrijven tegen seksuele zelfbeschikking, kinderpornografie, de vorming van criminele organisaties en moord. De meeste onderzoeken waarbij de politie hebben gebruikgemaakt van hackingtools hielden echter geen verband met bovengenoemde misdrijven[652]. Uit de

[644] https://www.ft.com/join/licence/88bec95c-78fd-4030-9526-a95fbdeb9da8/details?ft-content-uuid=d9127eae-f99d-11e9-98fd-4d6c20050229
[645] https://www.vrt.be/vrtnws/nl/2021/09/17/pegasus-spionageware-op-de-telefoon-van-journalist-peter-verlind/
[646] https://www.knack.be/nieuws/wereld/belgisch-slachtoffer-van-pegasus-spyware-mijn-leven-is-in-gevaar/; https://www.knack.be/nieuws/pegasus-project-macron-en-michel-in-het-vizier-van-marokko/
[647]Europees Parlement. Duitsland hoorzitting; https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html.
[648] https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/__20k.html
[649] https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528
[650] https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408
[651] https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/.
[652] Europees Parlement, Duitsland Hoorzitting.

meest recente cijfers van 2020 blijkt dat de Duitse politie toestemming kreeg voor 48 hacks. Ze gebruikten slechts 22 hacks waarvan geen enkele verband hield met terrorismebestrijding en moord[653].

365. In september 2021 werd gemeld dat de Duitse federale recherche (Bundeskriminalamt – BKA) Pegasus eind 2020 had aangeschaft. Hierbij moet worden opgemerkt dat de Duitse wet twee vormen van spywaregebruik onderscheidt[654]: toegang tot alle informatie (Online-Durchsuchung[655]) en toegang tot alleen live communicatie (Quellen-TKÜ[656]). Aangezien de oorspronkelijke Pegasus-software toegang had tot alle informatie op een apparaat, en niet alleen tot live communicatie, zou het gebruik ervan door het BKA een inbreuk zijn op de wet. Sinds een belangrijke uitspraak van het Duitse Federale Grondwettelijk Hof in 2008 moet alle door de politie gebruikte spyware voldoen aan de voor het BKA opgestelde normen voor telecommunicatie- en onlinesurveillance [657] [658]. Het BKA vroeg NSO daarom een broncode te schrijven, zodat Pegasus toegang zou hebben tot wat wettelijk is toegestaan. Aanvankelijk weigerde NSO dit te doen[659]. Pas na nieuwe onderhandelingen is NSO akkoord gegaan, en kocht het BKA een aangepaste versie aan[660]. Hoewel dit niet publiekelijk is erkend, bevestigde Martina Link, destijds vice-voorzitter van het BKA, de aankoop van een gewijzigde versie tijdens een vergadering achter gesloten deuren van de Innenausschuss in de Bondsdag[661]. Deze zou sinds maart 2021 worden ingezet. In de door het BKA aangeschafte versie waren bepaalde functies geblokkeerd om misbruik te voorkomen, al is onduidelijk hoe dit in de praktijk werkt. Het BKA heeft over deze aangepaste versie een rapport geschreven, dat vertrouwelijk blijft[662]. Het BKA heeft maatschappelijke organisaties de toegang tot contracten met spywarebedrijven ontzegd totdat ze daartoe door de rechter werd gedwongen. Maar zelfs toen werden de overeenkomsten slechts vrijgegeven in sterk bewerkte versies[663]. Ondanks twee uitnodigingen voor de commissie PEGA heeft het BKA wegens planningsproblemen geen hoorzittingen

---

[653] De Quellen-TKÜ (§ 100a StPO) werd 25 keer goedgekeurd en 14 keer uitgevoerd, en de Online-Durchsuchung (§ 100b StPO) werd 23 keer goedgekeurd en 8 keer uitgevoerd. Bron: https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_TKUE_2020.pdf?__blob=publicationFile

[654]https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

[655]https://www.gesetze-im-internet.de/stpo/__100b.html

[656]https://www.gesetze-im-internet.de/stpo/__100a.html

[657] "The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware", https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.

[658] Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile

[659] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

[660] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

[661] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

[662] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/

[663] Getuigenis van Andre Meister, landspecifieke hoorzitting inzake Duitsland, bijeenkomst van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken met betrekking tot Polen, 14 november 2022. https://netzpolitik.org/2022/finfisher-vertrag-wir-haben-das-bka-verklagt-und-gewonnen/

kunnen bijwonen.

366. In oktober 2021 werd ook bekend dat de Duitse buitenlandse inlichtingendienst (Bundesnachrichtendienst – BND) een aangepaste versie van Pegasus had gekocht, hoewel de aankoop geheim was[664]. In antwoord op een parlementaire vraag deelde de Bondsregering mee dat het gebruik van Pegasus alleen is toegestaan in individuele gevallen en moet voldoen aan strikte wettelijke voorwaarden die zijn vastgelegd in het Duitse wetboek van strafvordering (Strafprozessordnung – StPO), de wet inzake beperkingen van het brief-, post- en telecommunicatiegeheim (Artikel 10-Gesetz – G-10) en de wet betreffende de federale gerechtelijke politie (Bundeskriminalamtgesetz – BKAG), maar dat zij om redenen van geheimhouding (Geheimhaltungsbedürftigkeit) geen verder commentaar kon geven op het gebruik ervan[665].

GEBRUIK VAN SPYWARE

367. In 2012 en 2013 kochten zowel het BKA als de Berlijnse politie (LKA) onafhankelijk van elkaar FinSpy van FinFisher. Net als in het geval van Pegasus verzocht het BKA ook FinFisher zijn spyware zo aan te passen dat het niet alle gegevens op een apparaat kon inzien, maar alleen de live communicatie, om te voldoen aan de Duitse wet. Het BKA bleef nieuwe versies van de door FinFisher geleverde spyware testen om deze uitsluitend op een "wettelijk veilige en technisch zuivere" manier te gebruiken, en pas na vijf jaar, in 2018, heeft het Bondsministerie van Binnenlandse Zaken het gebruik ervan goedgekeurd. Dit was in hetzelfde jaar waarin het gebruik van FinFisher-software tegen oppositiepartijen in Turkije werd ontdekt, terwijl Duitsland sinds 2015 geen exportvergunning meer had afgegeven voor de export van surveillancesoftware naar derde landen[666]. Het contract tussen FinFisher en de Berlijnse politie was toen echter al afgelopen, zodat de politie in de hoofdstad het nooit heeft gebruikt. Het BKA gaf verder geen commentaar op een eventueel gebruik van FinFisher bij zijn activiteiten en of het contract nog steeds geldig is[667].

368. In 2017 heeft de bondsminister van Binnenlandse Zaken het centraal bureau voor Informatietechnologie in de veiligheidssector (Zentrale Stelle für Informationstechnik im Sicherheitsbereich – ZITiS) opgericht om onderzoek en ontwikkeling voor hackingtools door de overheid en de aankoop van hackingtools bij bedrijven die desbetreffende producten aanbieden te vergemakkelijken[668]. Op 6 april 2022 werd gemeld dat ZITiS op zoek was naar andere beschikbare technologieën na de faillissementsaanvraag van het in ongenade gevallen spywarebedrijf FinFisher[669]. Er werd onder meer gemeld dat het sinds 2019 vijf keer[670] was samengekomen met het Italiaanse surveillancebedrijf RCS Lab, maar er was geen bewijs dat een tool van RCS

---

664 https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974
665 https://dserver.bundestag.de/btd/19/322/1932246.pdf
666 "The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware", https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.
667 https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/
668 https://www.zitis.bund.de/DE/Home/home_node.html.
669 https://www.intelligenceonline.com/surveillance--interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art.
670 Antwoord op een parlementaire vraag van Martina Renner, lid van de fractie The Left https://dserver.bundestag.de/btd/20/038/2003840.pdf.

Lab werd aangekocht[671]. Bovendien kwam ZITiS samen met het Oostenrijkse bedrijf DSIRF[672], alsmede met het Israëlische Quadream[673] en Candiru[674], en evalueerde het hun spywareproducten.

369. In januari 2023 meldde Tagesschau dat ZITiS ook in contact stond met Intellexa of dochteronderneming Cytrox, hoewel het onduidelijk is of de Predator-spyware uiteindelijk is gekocht. Voormalig coördinator van de geheime dienst Bernd Schmidbauer trad naar verluidt op als vertegenwoordiger voor de producten van Intellexa. Volgens e-mails van november 2021 had de heer Schmidbauer contact met Arne Schönbohm, de voormalige voorzitter van de federale dienst voor informatiebeveiliging (Bundesamt für Sicherheit in der Informationstechnik – BSI), met als doel een afspraak met Intellexa te regelen. In februari 2022 nam de heer Schmidbauer ook contact op met de voorzitter van ZITiS voor een presentatie van Intellexa. Bovendien had de heer Schmidbauer contact met de vicevoorzitter van de federale dienst voor de bescherming van de grondwet (Bundesamt für Verfassungsschutz – BfV), wat naar verluidt begin juli 2022 resulteerde in een presentatie van Intellexa aan BfV-personeel. De regering heeft geen commentaar gegeven op deze afspraken die voortvloeien uit de controversiële lobbyactiviteiten van de heer Schmidbauer[675]. In 2021 kwam de heer Schmidbauer ook een ontmoeting met Jan Marsalek, die verbonden is aan DSIRF[676].

MALTA

370. Verschillende sleutelfiguren uit de spywarehandel hebben ofwel een bedrijf op Malta geregistreerd ofwel een Maltees paspoort gekregen, maar ze lijken er niet echt te wonen, noch lijken hun bedrijven actief te zijn. Tot dusver zijn enkele belangrijke personen uit de spywarehandel geïdentificeerd.

371. Tal Dilian is een Israëlisch staatsburger, voormalig lid van het Israëlische leger. Hij is oprichter van Intellexa en woont op Cyprus. In 2017 verkreeg hij een paspoort van Malta[677]. Hij is ook mede-eigenaar van een bedrijf op Malta, MNT Investments LTD genaamd[678].

372. Anatoly Hurgin is een Russisch-Israëlisch staatsburger en voormalig Israëlisch militair ingenieur. In 2015 verkreeg hij een paspoort van Malta[679]. Hij is de oprichter van Ability Ltd, een bedrijf dat met de NSO-groep samenwerkte aan Pegasus en de

---

671 https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/
672 https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12.
673 https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29.
674 https://dserver.bundestag.de/btd/20/003/2000327.pdf.
675 https://www.tagesschau.de/investigativ/swr/predator-spionage-software-101.html. https://dserver.bundestag.de/btd/20/050/2005061.pdf.
676 https://www.tagesschau.de/investigativ/swr/wirecard-marsalek-schmidbauer-101.html
677 Personen die in 2017 zijn genaturaliseerd tot/geregistreerd als burgers van Malta, gepubliceerd op 21 december 2018. https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf
678 https://mlt.databasesets.com/company-all/company/73006; https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/
679 https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429

netwerkkant van de activiteiten van NSO beheerde[680]. Op het moment dat hij een Maltees paspoort aanvroeg, werd hij al door zowel de Amerikaanse als de Israëlische autoriteiten onderzocht wegens verschillende strafbare feiten[681]. Onderzoeksjournalist Daphne Caruana Galizia, die later in oktober 2017 werd vermoord, schreef over hem in augustus 2016[682]. In 2017 werd Ability Ltd onderzocht door de Amerikaanse Commissie van toezicht op het effecten- en beurswezen (Securities and Exchange Commission – SEC) omdat het bedrijf zou hebben gelogen over de staat van zijn financiën, en het werd ook bijna van de beurs gehaald door NASDAQ[683]. Naar verluidt bezit de heer Hurgin ook een bedrijf in Litouwen, UAB "Communication Technologies" genaamd, dat "connectiviteits- en telecommunicatiediensten" verleent[684].

373. Felix Bitzios is bestuurder van het in Malta gevestigde bedrijf Baywest Business Europe Ltd[685], was vroeger eigenaar en werknemer van Intellexa en was betrokken bij de Piraeus/Libra-fraudezaak[686].

374. Stanislaw Szymon Pelczar is wettelijk vertegenwoordiger van Baywest Business Europe Ltd, geregistreerd in Malta, en was voormalig bewindvoerder bij Krikel. Hij wordt genoemd in de Paradise Papers[687].

375. Peter Thiel is een in Duitsland geboren Amerikaans staatsburger, die in 2011 het Nieuw-Zeelandse staatsburgerschap verwierf ondanks dat hij er niet woont. In 2022 vroeg hij een Maltees gouden paspoort aan (kort na de aankondiging van de gezamenlijke start-up van de heren Kurz en Hulio)[688]. Hij is een oprichter van PayPal en van het controversiële bedrijf Palantir (betrokken bij het Cambridge Analytica-schandaal). Hij is een sponsor van Donald Trump en de eerste externe investeerder van Facebook. Hij heeft Sebastian Kurz (die onlangs een bedrijf heeft opgericht met Shalev Hulio, ex-NSO) ingehuurd als strateeg[689].

FRANKRIJK

DOELWITTEN IN FRANKRIJK

376. In 2021 werden in het kader van het Pegasusproject verschillende gevallen onthuld van

---

[680] https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=543a981a3997; https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/

[681] https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/

[682] https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passporteu-citizenship/

[683] https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/

[684] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/

[685] https://offshoreleaks.icij.org/nodes/55071906.

[686] https://www.haaretz.com/israel-news/tech-news/2022-04-19/ty-article/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter/00000180-6565-dc5d-a1cd-757f069c0000

[687] https://offshoreleaks.icij.org/nodes/55071906

[688] https://www.nytimes.com/2022/10/15/technology/peter-thiel-malta-citizenship.html.

[689] https://www.politico.eu/article/austria-former-chancellor-sebastian-kurz-palantir-technologies-silicon-valley-peter-thiel/

pogingen tot hacks door de Pegasus-spyware in Frankrijk[690]. De gelekte dataset bevatte het telefoonnummer van president Emmanuel Macron, alsmede de telefoonnummers van 14 leden van zijn kabinet[691] [692]. De uitkomsten van forensische analyses door de Franse inlichtingendienst hebben bevestigd dat de telefoons van minister van Onderwijs Jean-Michel Blanquer, minister van Territoriale Samenhang Jacqueline Gourault, minister van Landbouw Julien Denormandie, minister van Huisvesting Emmanuelle Wargon en minister van Overzeese Gebieden Sebastien Lecornu besmet waren met de Pegasus-spyware[693]. De telefoon van parlementslid Adrien Quatennens was ook besmet[694].

377. Het register dat in het kader van het Pegasusproject werd ingezien, bevatte naar verluidt ook de telefoonnummers van andere Franse burgers, waaronder journalisten, voormalige politici en hun familieleden. Het Franse agentschap voor computerbeveiliging (Agence nationale de la sécurité des systèmes d'information) heeft bevestigd dat de mobiele toestellen van de directeur van het Parijse radiostation TSF Jazz Bruno Delport, voormalig minister Arnaud Montebourg en onderzoeksjournalisten Edwy Plenel, Lénaïg Bredoux en een naamloze journalist van France 24 met Pegasus waren besmet[695]. Daarnaast was ook Claude Mangin – de vrouw van Naâma Asfari, die als Saharawi politiek gevangene vastzit in Marokko – het doelwit van Pegasus[696]. Voorts was Joseph Breham, de in Parijs gevestigde advocaat van verschillende activisten van het Polisario-Front voor de Sahara-zaak, eveneens het doelwit van Pegasus[697].

378. Marokko lijkt achter veel van de aanvallen op zowel journalisten als politici in Frankrijk te zitten[698], waaronder Marokkaanse journalisten die in Franse ballingschap leven, te weten onderzoeksjournalist Hicham Mansouri, die in 2016 de voortdurende intimidatie van de Marokkaanse autoriteiten ontvluchtte, en de onafhankelijke journalist Aboubakr Jamai, die Marokko in 2007 verliet[699].

379. Naar verluidt stond Frankrijk in 2021 zelf op het punt Pegasus-spyware aan te schaffen. Ten tijde van de slotonderhandelingen met de NSO-groep leidden onthullingen over het vermeende gebruik van spyware tegen Franse regeringsambtenaren tot de abrupte opschorting van de verkoop[700]. Het Franse Ministerie van Buitenlandse Zaken heeft

---

690 The Guardian, "Pegasus spyware found on journalists' phones, French intelligence confirms".
691 The Guardian, "Spyware found on phones of five French cabinet members".
692 Euractiv, "France's Macron targeted in project Pegasus spyware case."
693 The Guardian, "Spyware found on phones of five French cabinet members".
694 https://www.google.com/url?q=https://www.bfmtv.com/politique/cible-par-le-logiciel-espion-pegasus-le-depute-insoumis-adrien-quatennens-annonce-deposer-plainte_AV-202107210122.html&sa=D&source=docs&ust=1674591349575339&usg=AOvVaw2rgujnaWzoVapS7ZbiH4-r
695 Haaretz, "The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware".
696 Haaretz, "The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware".
697 https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-breham-avocat-mangin-algerie
698 Radio France, "Projet Pegasus: le gouvernement et toute la classe politique française dans le viseur du Maroc".
699 https://forbiddenstories.org/journaliste/hicham-mansouri/; https://forbiddenstories.org/journaliste/aboubakr-jamai/
700 MIT Technology Review, "NSO was about to sell hacking tools to France. Now it's in crisis".

ontkend dat het gesprekken met de NSO-groep heeft gehouden[701].

380. In een vergadering van de commissie PEGA op 9 januari 2023 verklaarde Serge Lasvignes, voorzitter van de nationale commissie voor toezicht op inlichtingentechnieken, dat het besluit om het gebruik van Pegasus in Frankrijk niet toe te staan was genomen vóór de onthullingen van het Pegasusproject. Volgens Lasvignes maken de Franse inlichtingendiensten alleen gebruik van surveillanceproducten die in Frankrijk zijn gemaakt om te voorkomen dat buitenlandse producenten van spyware toegang krijgen tot informatie. Lasvignes preciseerde echter dat het technisch directoraat dat de Franse spyware bouwt wel degelijk bepaalde onderdelen van niet-Franse bedrijven importeert[702].

381. In Frankrijk moeten verzoeken om toestemming voor surveillance van een persoon eerst worden goedgekeurd door de directeur-generaal van de dienst en vervolgens door de minister van Binnenlandse Zaken. Uiteindelijk moeten alle verzoeken door de eerste minister worden goedgekeurd. Momenteel worden in Frankrijk 23 000 personen gesurveilleerd, en iedere operatie is goedgekeurd door de eerste minister. Indien een doelwit wenst te weten of hij of zij onder surveillance staat of heeft gestaan, wordt de toegang tot zijn of haar dossier geweigerd onder verwijzing naar de nationale veiligheid. De persoon kan om verificatie door een rechter verzoeken. De rechter kan echter alleen beslissen of de surveillance al dan niet legaal was, maar kan het doelwit niet inlichten, aangezien dit onder het vertrouwelijke karakter van nationale veiligheid valt[703]. Dit betekent dat het recht op verhaal in de praktijk zinledig is, aangezien de bewijslast bij het individu ligt en het vrijwel onmogelijk is om van de autoriteiten enig bewijs te krijgen.

382. Volgens een ISS World-brochure uit 2013 waren het Franse Ministerie van Binnenlandse Zaken, het Ministerie van Defensie, Interpol en de ambassade van Togo in Frankrijk als deelnemers aanwezig op de beurs ISS World 2012, ook bekend als “The Wiretappers Ball” (het spionagegala). Bovendien blijkt uit een lijst van verkopers en technologie-integratoren van ISS dat de volgende Franse spywarebedrijven aanwezig waren op dit evenement: Advantech, Amesys-Bull, AQSACOM France, Bertin Technologies, BreakingPoint, BULL, COFREXPORT, DataDirect Networks, Ercom, EXFO NetHawk, HALY3, Intersec, IP Solutions, OLEA Partners France, Scan & Target, Thales Communications & Security, Utimaco, VUPEN Security en WAHOUE AND PARTNERS[704].

SPYWAREBEDRIJVEN IN FRANKRIJK

383. Verschillende spywarebedrijven, waarvan Nexa Technologies en Amesys de belangrijkste zijn, zijn gevestigd in Frankrijk. Nexa technologies, onderdeel van Tal Dilian’s Intellexa Alliance, is een Frans cyberdefensie- en inlichtingenbedrijf dat is opgericht in 2000[705]. Nexa Technologies wordt geleid door voormalige managers van

[701] MIT Technology Review, “NSO was about to sell hacking tools to France. Now it’s in crisis”.
[702] Hoorzitting van de commissie PEGA, 9 januari 2022.
[703] Hoorzitting van de commissie PEGA, 9 januari 2022.
[704] ISS World, “Programme schedule for year 2013”.
[705] Bloomberg, “Nexa Technologies Inc.”

Amesys. Amesys is opgericht in 1979[706] en staat bekend als de verkoper van een programma genaamd Cerebro, dat in staat is de elektronische communicatie van zijn doelwitten, zoals e-mailadressen en telefoonnummers, te traceren[707].

384. Naar verluidt verkocht Amesys deze telecommunicatiesurveillancetechnologie in 2007 aan Libië, waar het regime van Kadhafi haar gebruikte om critici van het regime te arresteren en te martelen. Volgens Telerama is Nexa opgericht om de surveillancesoftware een nieuwe naam te geven en de verkoop van Amesys aan het Egyptische regime voort te zetten[708]. In 2014 zou Nexa Technologies een onderscheppingssysteem aan het Egyptische regime hebben verkocht onder de naam Eagle. Dit systeem werd gebruikt met het oog op opsluiting en marteling van politieke tegenstanders van het regime van Al-Sissi[709]. Eagle werd van 2007 tot en met 2011 door Amesys uitgerold en onderhouden[710].

385. Er zijn verschillende klachten ingediend tegen zowel Amesys als Nexa Technologies. In oktober 2011 hebben de Internationale federatie voor de mensenrechten (FIDH) en de Human Rights League (LDH) bij het Hooggerechtshof van Parijs een rechtszaak tegen Amesys aangespannen wegens hun vermeende verkoop aan Libië[711]. In de zomer van 2013 zijn vijf Libische doelwitten gehoord en één Libisch doelwit is gehoord in december 2015. Als resultaat van nieuw bewijsmateriaal dat het gebruik van de surveillancetechnologie van Amesys door het regime van Kadhafi onderstreept, is Amesys officieel de status van "témoin assisté" toegekend wegens medeplichtigheid aan foltering tussen 2007 en 2011[712].

386. In 2010 werd Amesys overgenomen door het Franse computerbedrijf Bull. In 2014 nam Atos, dat destijds werd geleid door Thierry Breton, Bull over en verwierf daarmee ook Amesys[713]. Ten tijde van de overname waren de dubieuze activiteiten van Amesys op het gebied van handel met autoritaire regimes reeds algemeen bekend. Er was namelijk al een klacht ingediend.

387. In 2017 bracht een onderzoeksverslag in de media aan het licht dat Nexa Technologies in 2014 surveillancesystemen aan Egypte had verkocht, wat leidde tot een klacht van de FIDH, LDH en het Cairo Institute for Human Rights Studies (CIHRS) tegen het bedrijf[714] [715].

388. In juni 2021 heeft de arrondissementsrechtbank van Parijs na verschillende klachten van mensenrechtenorganisaties vier leidinggevenden van Amesys en Nexa Technologies in verdenking gesteld voor de verkoop van surveillancetechnologie aan de regeringen van

[706] PitchBook, "Amesys".
[707] Le Monde, "Vente de matériel de cybersurveillance à l'Egypte: la société Nexa Technologies mise en examen".
[708] ZDNet, "Amesys and Nexa Technologies executives indicted".
[709] Trial International, "Amesys (Nexa Technologies)".
[710] ZDNet, "Amesys and Nexa Technologies executives indicted".
[711] Trial International, "Amesys (Nexa Technologies)".
[712] Trial International, "Amesys (Nexa Technologies)".
[713] L'Obs, "Amesys file un coup de main à l'agence en charge du fichier monstre".
[714] Le Monde, "Vente de matériel de cybersurveillance à l'Egypte: la société Nexa Technologies mise en examen".
[715] ZDNet, "Amesys and Nexa Technologies executives indicted".

Libië en Egypte[716]. Het is zorgwekkend dat er tien volle jaren zijn verstreken tussen de eerste klacht en de aanvang van de rechtszaak. Intussen kon Amesys zijn activiteiten ongehinderd voortzetten, met inbegrip van de bovengenoemde verkoop van surveillancetechnologie aan Egypte.

389. Ondanks deze controverses ondertekende het nationaal agentschap voor beveiligde titels (Agence Nationale des Titres Sécurisés – ANTS) in oktober 2016 een contract met Amesys ter waarde van ruim 5 miljoen EUR voor het technisch beheer van de TES-databank (met persoons- en biometrische gegevens van alle Franse burgers). Dit besluit van de Franse autoriteiten om Amesys, toen al bekend om zijn praktijken, bij een dergelijk project te betrekken, werd bekritiseerd. Hoewel Amesys geen volledige controle zou hebben over de systemen die voor het controversiële TES-gegevensbestand worden gebruikt, zou het de projectbeheerders van het agentschap die met het TES-bestand werken bijstaan, zodat niet kan worden uitgesloten dat Amesys toegang heeft tot persoonsgegevens. De directeur van ANTS was echter van mening dat er geen juridisch bezwaar bestond tegen het zakendoen met Amesys[717].

390. In Frankrijk wordt de afgifte van uitvoervergunningen gecontroleerd door de dienst voor goederen voor tweeërlei gebruik (Service des biens à double usage – SBDU) van het Ministerie van Economie, Industrie en Digitale Zaken. Bovendien inspecteert de Interministeriële Commissie goederen voor tweeërlei gebruik, onder voorzitterschap van het Ministerie van Europa en Buitenlandse Zaken, de meer gevoelige goederen voor tweeërlei gebruik. Op het moment van schrijven was er geen informatie beschikbaar over de toekenning van uitvoervergunningen door de Franse regering aan Nexa Technologies.

IERLAND

391. Vanwege zijn fiscale wetgeving is Ierland de lidstaat geworden waar enkele van de belangrijkste bij schandalen betrokken spywarebedrijven zich hebben geregistreerd. Op 20 september 2022 onthulde The Currency, een Ierse uitgever van onderzoeksjournalistiek, dat zowel Thalestris Limited, het moederbedrijf van Intellexa, als Intellexa zelf hun hoofdkantoor hebben in Ierland, en geregistreerd staan bij een advocatenkantoor in de stad Balbriggan. Het is opmerkelijk dat de aanvraag om Thalestris Limited in Ierland op te richten in november 2019 werd ingediend door een specialist in bedrijfsvorming, slechts twaalf dagen nadat het strafrechtelijk onderzoek naar Dilian en zijn bedrijf WiSpear door de Cypriotische autoriteiten openbaar werd gemaakt. Tal Dilian zelf, CEO van Intellexa, komt niet voor in de Ierse bedrijfsdocumenten, maar zijn tweede vrouw, Sara Hamou, wordt naar verluidt genoemd als directeur van zowel Thalestris als Intellexa[718].

392. Uit gepubliceerde rekeningen van Thalestris voor de periode eindigend op 31 december 2020 blijkt dat er tien andere dochterondernemingen bestaan in Griekenland, Cyprus, Zwitserland en de Britse Maagdeneilanden, en dat Thalestris niet aan

[716] Amnesty, “Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture”.
[717] L’Obs, “Amesys file un coup de main à l’agence en charge du fichier monstre”.
[718] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/

vennootschapsbelasting was onderworpen. Thalestris maakte gebruik van een aantal fiscale bepalingen die ook door in Ierland werkzame multinationals worden gebruikt, en was derhalve technisch verliesgevend[719].

393. De Ierse regering weigerde te antwoorden op de vraag of zijzelf/haar wetshandhavingsinstanties was/waren benaderd door Thalestris of Intellexa, of dat zij ooit gebruik had/hadden gemaakt van hun diensten, met het argument: “het zou om gezonde operationele en nationale veiligheidsredenen niet gepast zijn om commentaar te leveren op de details van nationale veiligheidsregelingen, noch zou het gepast zijn om de cyberbeveiligingsregelingen van het departement of die van staatsbureaus, agentschappen en organen die onder de bevoegdheid van het departement vallen, bekend te maken”. De Ierse regering weigerde ook commentaar te geven op eventuele Ierse banden met de door Thalestris en Intellexa geproduceerde spyware[720]. Er is geen openbaar bekend bewijs van misbruik van spyware in Ierland.

394. GoNet Systems was betrokken bij de levering van wifi-infrastructuurdiensten op de luchthaven van Larnaca, werd in verband gebracht met Dilians WiSpear en werd in 2022 stopgezet[721].

395. In januari 2023 werd gemeld dat naar aanleiding van een brief van EP-lid Barry Andrews de Oireachtas-commissie voor Justitie het bestaan zou onderzoeken van bedrijven in Ierland die betrokken zijn bij de productie van spyware. De commissie verklaarde dat zij zich tijdens een besloten vergadering op 18 januari over deze kwestie had gebogen en was overeengekomen het onderwerp toe te voegen aan haar werkprogramma voor 2023[722].

396. Er zij op gewezen dat het Ierse vennootschapsrecht voortdurend wordt getoetst en regelmatig wordt bijgewerkt teneinde de transparantie van bedrijfsstructuren te vergroten. Voorbeelden daarvan zijn de Companies Act (wet inzake de handhavingsautoriteit voor bedrijven) in 2021, waarbij het handhavingsregime werd geactualiseerd, en een komende actualisering daarvan die in 2023 wordt verwacht, en de Miscellaneous Provisions Bill (wetsvoorstel met verschillende bepalingen betreffende transparantie en registratie van commanditaire vennootschappen en bedrijfsnamen) in 2023. Voorts heeft de Ierse regering verdere investeringen in het nationale centrum voor cyberbeveiliging (National Cyber Security Centre – NCSC) aangekondigd om het NCSC beter in staat te stellen cyberdreigingen die gericht zijn op kritieke infrastructuur en kritieke netwerken actief op te sporen en te verslaan. Het NCSC zal steeds beter in staat zijn incidenten te volgen en erop te reageren door de voortdurende evolutie van het gezamenlijke centrum voor beveiligingsoperaties (Joint Security Operations Centre – JSOC) en de uitbreiding van de analyse- en rapportagecapaciteit. Er wordt ook gewerkt

[719] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/

[720] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/

[721] https://www.haaretz.com/israel-news/security-aviation/2022-09-20/ty-article-magazine/.highlight/as-israel-reins-in-its-cyberarms-industry-an-ex-intel-officer-is-building-a-new-empire/00000183-5a07-dd63-adb3-da173af40000?lts=1667755247674

[722] https://www.irishtimes.com/politics/oireachtas/2023/01/29/justice-committee-to-investigate-controversial-spyware-technology-group-with-links-to-ireland/

aan de ontwikkeling van een technologiestrategie voor het NCSC met externe consultants[723].

LUXEMBURG

397. In Luxemburg zijn negen entiteiten gevestigd die rechtstreeks in verband staan met de NSO-groep. Dit werd in juni 2021 onthuld door Amnesty International en bevestigd door Jean Asselborn, de Luxemburgse minister van Buitenlandse Zaken[724]. Het feit dat de namen van de negen ondernemingen (zoals Triangle Holdings SA, Square 2 SARL en Q Cyber Technologies SARL), die alle onder de paraplu van management- en participatiemaatschappij Novalpina Capital vallen, niet onmiddellijk het verband met NSO Group onthullen, toont aan hoe ondoorzichtige bedrijfsstructuren in Luxemburg bedrijven in staat stellen om in Luxemburg volledig buiten het publieke zicht te opereren.

398. Na Amnesty's onthullingen over de negen NSO-entiteiten in Luxemburg in juni 2021 stuurde minister van Buitenlandse Zaken Jean Asselborn elk van hen een brief, waarin hij hen opriep zich te onthouden van elke besluitvorming die zou kunnen leiden tot onrechtmatig gebruik van de goederen en technologieën die zij aan hun klanten ter beschikking stellen. Volgens LuxTimes antwoordde NSO-groep dat het zijn spyware alleen met toestemming van de Israëlische regering uit Israël uitvoert, maar Asselborn verklaarde in oktober 2021 dat hij dit niet kon verifiëren[725]. In ieder geval mocht volgens de minister geen van de negen entiteiten cybersurveillanceproducten uit Luxemburg uitvoeren, aangezien Luxemburg geen uitvoervergunningen heeft verleend[726]. "Luxemburg zal in geen geval tolereren dat uitvoeroperaties vanuit Luxemburg bijdragen tot schendingen van mensenrechten in derde landen en zal, indien van toepassing, de benodigde maatregelen nemen om elke schending van mensenrechten te verhelpen en toekomstige schendingen te voorkomen", aldus Asselborn[727]. De NSO-groep kan echter nog steeds opereren dankzij de in Luxemburg gevestigde entiteiten, zoals Q Cyber Technologies, dat verantwoordelijk is voor de afhandeling van facturen, contracten en betalingen van zijn softwareklanten[728]. Op 24 augustus 2022 werd bekend dat de NSO-groep meer dan de helft van haar omzet over de twee voorgaande jaren in Luxemburg heeft geboekt, wat duidelijk maakt dat Luxemburg als belangrijk zakelijk centrum voor de NSO-groep fungeert[729].

399. In oktober 2021 heeft eerste minister Xavier Bettel bevestigd dat Luxemburg Pegasus heeft gekocht en gebruikt "om redenen van staatsveiligheid"[730].

---

[723] https://www.kildarestreet.com/wrans/?id=2022-12-15a.199&s=cyber+security#g201.r
[724] https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[725] https://www.luxtimes.lu/en/luxembourg/government-cannot-verify-pegasus-export-claims-616eead9de135b9236b1efcc.
[726] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e.
[727] https://delano.lu/article/nine-nso-entities-in-luxembour.
[728] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e.
[729] https://www.luxtimes.lu/en/business-finance/pegasus-firm-nso-booked-most-sales-through-luxembourg-6303754ade135b9236e0870b
[730] https://www.luxtimes.lu/en/luxembourg/tax-voting-rights-housing-watch-bettel-video-highlights-6176e835de135b923682378d

ITALIË

400. Tot dusver zijn er geen meldingen gedaan over de mogelijke aankoop van spyware door de Italiaanse autoriteiten. Er zijn geen gevallen van spionage op hoog niveau bekend, hoewel het telefoonnummer van voormalig premier en Commissievoorzitter Romano Prodi is aangetroffen op de in het kader van het Pegasusproject gepubliceerde lijst[731]. Als voormalig speciaal gezant van de VN voor de Sahel zou hij een interessant doelwit voor Marokko hebben kunnen zijn, gezien zijn mogelijke netwerken met hooggeplaatste personen in de Westelijke Sahara en Algerije.

401. De spywarebedrijven, Tykelab en RCS Lab hebben Italië als vestigingsplaats gekozen.

402. Een ander bedrijf dat al zeker sinds 2012 vanuit Italië offensieve inbraakprogrammatuur ("intrusion software") aanbiedt, was Hacking Team, dat nu Memento Labs heet. Het bedrijf kreeg bekendheid na een hack waarbij de verkoop aan verschillende autoritaire landen werd onthuld, die de RCS-spyware vervolgens gebruikten om politieke dissidenten, journalisten en mensenrechtenactivisten aan te vallen. Een door ngo's en VN-onderzoekers ingesteld onderzoek naar de uitvoer van RCS-spyware naar Soedan bracht de Italiaanse autoriteiten er uiteindelijk toe krachtens de Italiaanse uitvoerwetgeving een "vangnet"-bepaling op te leggen wegens mensenrechtenkwesties, en dus moest het bedrijf voor elke uitvoer een individuele vergunning aanvragen. Hacking Team weigerde niet alleen om mee te werken tijdens het onderzoek, maar maakte ook gebruik van zijn nauwe relaties met hooggeplaatste ambtenaren in de regering, de inlichtingendienst en de rechtshandhaving in Italië om zich te positioneren als een aanwinst voor de nationale veiligheid, en zette uiteindelijk het Ministerie van Economische Ontwikkeling onder druk om het bedrijf opnieuw een algemene uitvoervergunning te verlenen[732].

OOSTENRIJK

403. In antwoord op schriftelijke vragen van het Oostenrijkse parlement heeft de Oostenrijkse federale regering verklaard dat Oostenrijk nooit klant is geweest van NSO[733]. De voormalige bondskanselier van Oostenrijk, Sebastian Kurz, heeft echter nauwe banden met de oprichter van de NSO-groep, en DSIRF, een belangrijke aanbieder van spyware, is in Oostenrijk gevestigd.

404. Na zijn aftreden werd de heer Kurz ingehuurd als mondiaal strateeg voor Thiel Capital, dat eigendom is van miljardair Peter Thiel[734]. In oktober 2022 lanceerden de heer Kurz en Shalev Hulio (oprichter van de NSO-groep) een cyberbeveiligingsbedrijf, genaamd

---

[731] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

[732] **1 bis** https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/;
https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/

[733] Antwoorden van Karl Nehammer, voormalig minister van Binnenlandse Zaken, aan Nikolaus Scherak, lid van de Nationale Raad; 22 september 2021, referentie 2021-0.580.421.

[734] https://www.bloomberg.com/news/articles/2021-12-30/billionaire-thiel-gives-austria-s-former-wunderkind-a-job.

Dream Security[735]. Hoewel de heer Hulio in augustus 2022 was afgetreden als CEO van de NSO-groep, hebben Dream Security en NSO nauwe banden via verschillende persoonlijke en zakelijke relaties. Een van de investeerders ervan, Adi Shalev, was ook een vroege investeerder in NSO. Een ander stichtend lid van Dream Security is Gil Dolev. De zuster van Dolev, Shiri Dolev, is voorzitter van de NSO-groep. Shalev Hulio heeft eerder een van de bedrijven van Gil Dolev overgenomen[736].

405. In juli 2022 gebruikten exploitanten spyware van het in Oostenrijk gevestigde bedrijf DSIRF om advocatenkantoren, banken en adviesbureaus in Oostenrijk, Panama en het VK te hacken. Volgens onderzoekers van Microsoft maakte de tool "Subzero" van DSIRF gebruik van onbeschermde zwakke plekken om toegang te krijgen tot vertrouwelijke informatie, zoals wachtwoorden en andere gegevens[737]. In oktober 2022 zei het federale Ministerie van Arbeid en Economische Zaken dat het niet op de hoogte was van aanvragen voor uitvoervergunningen door DSIRF, en dat er de afgelopen tien jaar geen uitvoeraanvragen voor "inbraaksoftware" waren ingediend[738]. Bij gebreke van een uitvoervergunning voor de uitvoer van software door DSIRF heeft het parket van Wenen een vooronderzoek ingesteld op verdenking van onrechtmatige toegang tot een computersysteem naar Oostenrijks recht.

ESTLAND

406. Ook Estland heeft naar verluidt interesse getoond in de aankoop van de Pegasus-spyware van de NSO-groep. De eerste onderhandelingen tussen Estland en de NSO-groep vonden plaats in 2018, waarna Estland een aanbetaling deed voor een aankoopcontract voor de NSO-surveillancesoftware ter hoogte van 30 miljoen USD[739].

407. Een jaar later bracht een Russische defensiefunctionaris Israël er echter van op de hoogte dat Estland voornemens was de Pegasus-spyware te gebruiken voor Russische telefoonnummers. Deze informatie bracht het Israëlische Ministerie van Defensie ertoe Estland te verhinderen wereldwijd Russische toestellen te bespioneren, omdat de deal schadelijk zou zijn voor de Israëlisch-Russische betrekkingen[740]. Het geval van Estland onderstreept dat de Pegasus-spyware niet alleen een surveillancewapen is, maar ook dient als politieke munt in diplomatieke betrekkingen.

LITOUWEN

408. Een Litouws bedrijf, UAB Communication Technologies, dat actief is op het gebied van verbindings- en telecommunicatiediensten, is eigendom van Anatoly Hurgin, een

[735] https://www.spiegel.de/netzwelt/web/sebastian-kurz-und-ex-nso-chef-gruenden-it-sicherheitsfirma-dream-security-a-4482132c-9faf-4be3-927a-86560ba28670.
[736] https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/
[737] Studie getiteld "Pegasus and the EU's external relations", Europees Parlement, directoraat-generaal Intern Beleid, beleidsondersteunende afdeling C – Rechten van de burger en Constitutionele Zaken, 25 januari 2023, blz. 52; Microsoft (2022), "Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits".
[738] https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf
[739] The New York Times, "Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia", 23 maart 2022.
[740] The New York Times, "Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia", 23 maart 2022.

Russisch-Israëlisch staatsburger, voormalig Israëlisch militair ingenieur en, samen met NSO, medeontwikkelaar van Pegasus[741]. In 2015 verkreeg ook Hurgin een gouden paspoort van Malta[742].

BULGARIJE

409. In Bulgarije worden uitvoercontroles en uitvoervergunningen voor producten voor tweeërlei gebruik krachtens de EU-verordening inzake producten voor tweeërlei gebruik gecontroleerd door het Ministerie van Economische Zaken, en meer bepaald door de Interministeriële Commissie voor uitvoercontrole en non-proliferatie van massavernietigingswapens[743]. De huidige minister van Economische Zaken en Industrie is Nikola Stoyanov[744]. De Bulgaarse autoriteiten ontkennen dat zij uitvoervergunningen hebben verleend aan de NSO-groep of haar dochterondernemingen[745]. Novalpina Capital, het private-equityfonds dat de voormalige eigenaar van de NSO-groep is, heeft echter uitdrukkelijk aangegeven dat de producten van NSO vanuit zowel Cyprus als Bulgarije uit de EU worden uitgevoerd[746] [747] [748]. Beide stellingen spreken elkaar tegen. Voorts wordt in mediapublicaties beweerd dat sommige servers van de netwerkinfrastructuur via hetwelk de Pegasus-aanvallen worden uitgevoerd, zich bevinden in een Bulgaars datacentrum dat eigendom is van een Bulgaars bedrijf. Dit bedrijf is eigendom van de NSO Group, Circles Bulgaria en Magnet Bulgaria, die van de autoriteiten exportvergunningen hebben gekregen. Vanuit Bulgarije verleent deze dochteronderneming van de NSO-groep de Cypriotische dochterondernemingen onderzoeks- en ontwikkelingsdiensten en voert netwerkproducten uit naar regeringen[749]. Magnet is momenteel slapend, maar Circles is momenteel actief en heeft een uitvoervergunning verkregen die geldig is tot 25 april 2023[750].

410. In februari 2022 startte het parket van Sofia een onderzoek om vast te stellen of overheidsdiensten illegaal Pegasus-spyware hadden gebruikt om Bulgaarse burgers tot doelwit te maken. Dit onderzoek momenteel loopt nog[751]. In januari 2022 oordeelde het EHRM in de zaak Ekimdzhiev e.a./Bulgarije dat de bestaande wetten in Bulgarije inzake geheime surveillance en het inhouden van en toegang tot communicatie niet voldeden aan de kwaliteitseisen van het Verdrag en verzocht het de regering de noodzakelijke wijzigingen in de nationale wetgeving aan te brengen om een einde te

---

[741] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[742] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration
[743] Republiek Bulgarije. Ministerie van Economische Zaken en Industrie, Interministeriële Commissie voor uitvoercontrole en non-proliferatie van massavernietigingswapens.
[744] Ministerraad van de Republiek Bulgarije.
[745] Politico, "Pegasus makers face EU grilling. Here's what to ask them", 21 juni 2022.
[746] Amnesty International, "Novalpina Capital's response to NGO coalition's open letter", 18 februari 2019.
[747] Access Now, "Is NSO Group's infamous Pegasus spyware being traded through the EU?", 12 september 2019.
[748] https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/
[749] Amnesty International, "Operating From the Shadows: Inside NSO Group's Corporate Structure".
[750] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuser uploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK
[751] https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria

maken aan de schending[752].

I.G. De EU-instellingen

DOELWIT: DE EUROPESE COMMISSIE

411. Op 11 april 2022 meldde Reuters dat commissaris voor Justitie Didier Reynders en ten minste vier personeelsleden van de Commissie in november 2021 waren gehackt met Pegasus-software[753]. Op 23 november 2021 stuurde Apple officiële meldingen naar de toestellen van commissaris Reynders en "andere medewerkers van de Commissie" met de mededeling dat zij "het doelwit waren geweest van door een staat gesteunde aanvallers" en dat hun toestellen mogelijk waren besmet[754].

412. Na deze onthullingen is commissaris Reynders uitgenodigd om op 30 mei 2022 te spreken voor de commissie PEGA en heeft hij ook schriftelijk geantwoord op de vragen van de commissie. Al op 19 juli 2021, na de onthullingen van Forbidden Stories en Amnesty International, heeft de Commissie een "speciaal team van interne deskundigen dat is belast met een intern onderzoek" opgericht om "na te gaan of Pegasus toestellen van medewerkers van de Commissie en leden van het college had gehackt"[755]. De Commissie heeft in september 2021 op alle bedrijfstelefoons ook een mobiele endpointdetectie en -respons (EDR)-oplossing ingezet, die de diensten van de Commissie helpt bij het identificeren van mogelijk geïnfecteerde mobiele bedrijfstoestellen.

413. In de loop van het onderzoek deelde de Commissie mee dat "noch ... voor noch na deze datum [23 november 2021]" deze controles hadden bevestigd dat de persoonlijke of professionele toestellen van commissaris Reynders waren besmet. De bevoegde diensten van de Commissie hebben ook de toestellen van andere personeelsleden geïnspecteerd die op dezelfde dag vergelijkbare kennisgevingen van Apple kregen, maar "bij geen van de geïnspecteerde toestellen konden de vermoedens van Apple worden bevestigd"[756].

414. In haar brief van 9 september 2022 erkende de Commissie echter dat tijdens het lopende onderzoek naar het hacken van de Commissie met Pegasus "verschillende controles van toestellen hebben geleid tot de ontdekking van aanwijzingen dat ze waren besmet". De Commissie is tot dusver noch in het openbaar noch in de commissie PEGA nader op de bevindingen van haar onderzoek ingegaan, omdat "zij de onderzoeksmethoden en -capaciteiten van de Commissie aan tegenstanders zouden onthullen, waardoor de veiligheid van de instelling ernstig in gevaar zou komen"[757]. Inofficiële meldingen van meer dan vijftig gedetecteerde infecties zijn door de Commissie niet bevestigd.

---

[752] Ekimdzhiev e.a. tegen Bulgarije, verzoekschrift nr. 70078/12, arrest van 11 januari 2022, beschikbaar op: https://hudoc.echr.coe.int/fre?i=001-214673

[753] https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/

[754] Antwoordbrief van de commissarissen Hahn en Reynders aan de rapporteur, 25 juli 2022; antwoordbrief van de commissarissen Hahn en Reynders aan de commissie PEGA, 9 september 2022.

[755] Antwoordbrief van de commissarissen Hahn en Reynders aan de rapporteur, 25 juli 2022.

[756] Antwoordbrief van de commissarissen Hahn en Reynders aan de commissie PEGA, 9 september 2022.

[757] https://pro.politico.eu/news/148627

415. Op de vraag van de commissie PEGA welke actor of actoren achter deze aanvallen zouden kunnen zitten, antwoordde de Commissie dat “het onmogelijk is deze indicatoren met volledige zekerheid aan een specifieke dader toe te schrijven”. Het gemeenschappelijke overkoepelende onderwerp waarmee twee van de gehackte ambtenaren van de Commissie, namelijk commissaris Reynders en een kabinetsmedewerker van commissaris Věra Jourová[758], zich beroepshalve bezighouden, is de rechtsstaat. In antwoord op de vraag van PEGA over een mogelijk verband heeft de Commissie geweigerd nadere informatie te verstrekken over het aantal afdelingen dat mogelijk is besmet, over de beroepen van het getroffen personeel of enige andere informatie die van belang zou zijn voor de werkzaamheden van de commissie PEGA en die de oorsprong van de aanval zou kunnen bepalen, en heeft zij verklaard dat zij “niet over voldoende informatie beschikt om definitieve conclusies te trekken over een verband tussen geolocatie en een mogelijke poging tot besmetting van toestellen via Pegasus”[759].

416. In het licht van het bovenstaande kunnen verschillende problemen worden vastgesteld. Ten eerste is de Commissie zich duidelijk onvoldoende bewust en heeft zij te weinig begrip van de enorme politieke risico’s die verbonden zijn aan het doelwit zijn van spyware. Elke poging, geslaagd of niet, om de Commissie of een of meer van haar leden te hacken, is een uitermate ernstig politiek feit dat de integriteit van het democratische besluitvormingsproces aantast. In haar interactie met de commissie PEGA heeft de Commissie meermaals te kennen gegeven dat het hacken van het toestel van commissaris Reynders met Pegasus-software niet is gelukt. Zoals de Commissie echter zelf vermeldde, hebben “verschillende controles van toestellen [van het personeel] hebben geleid tot de ontdekking van aanwijzingen dat ze waren besmet”, waarover geen verdere mededelingen zijn gedaan. Dit lijkt erop te wijzen dat de Commissie de ernst bagatelliseert van het feit dat een EU-instelling wordt gehackt.

417. Ten tweede lijkt er onvoldoende IT-capaciteit en -vermogen te zijn geweest om commissarissen en het personeel te beschermen tegen aanvallen of om hun cyberveiligheid te bewaken en te verifiëren. Hoewel de Commissie nieuwe maatregelen heeft getroffen, zoals de EDR-oplossing, op alle telefoons van de Commissie, en voortdurend samenwerkt met CERT-EU[760], is het door het gebrek aan informatie die PEGA van de Commissie heeft ontvangen onduidelijk in hoeverre de maatregelen van de Commissie om eerdere spyware-aanvallen te analyseren succesvol zijn geweest en in hoeverre de getroffen maatregelen in de toekomst afdoende zullen zijn.

418. Ten derde heeft de Commissie de meldingen of de aanwijzingen van besmetting niet officieel voor nader onderzoek aan de Belgische politie gemeld, maar heeft zij in het kader van haar “regelmatige samenwerking” alleen contact gehad met de Belgische politie over “technische details”. De Commissie heeft verklaard dat “de relevante IT-afdelingen van de Commissie iedere dag meerdere keren dit soort meldingen krijgen” en dat het daarom niet nodig was hiervan officieel aangifte te doen bij de politie. Aangezien de melding van Apple volgens de Commissie geen aanwijzingen bevatte van een “definitieve infectie, maar een mogelijke poging van de malware om het betreffende apparaat te hacken”, heeft de Commissie geen verdere stappen ondernomen met de

[758] https://pro.politico.eu/news/148627
[759] Antwoordbrief van de commissarissen Hahn en Reynders aan de commissie PEGA, 9 september 2022.
[760] Antwoordbrief van de commissarissen Hahn en Reynders aan de commissie PEGA, 9 september 2022.

rechtshandhavingsinstanties[761].In andere gevallen, bijvoorbeeld in Spanje en Frankrijk, is er evenwel een strafrechtelijk onderzoek ingesteld naar het gebruik van spyware tegen ministers en het staatshoofd. Spyware wordt doorgaans gebruikt door overheidsactoren die zich beroepen op redenen van nationale veiligheid. De Commissie voert aan dat "bepaalde aspecten van nationale veiligheid buiten de bevoegdheid van de Commissie vallen"[762], maar legt niet uit hoe commissarissen en personeel van de Commissie redelijkerwijs een risico voor de nationale veiligheid zouden kunnen vormen.

419. Ten vierde betekent het feit dat de Commissie noch achter gesloten deuren zinvolle informatie aan PEGA heeft verstrekt over het hacken van de Commissie, noch meer in het algemeen enige basisinformatie heeft gegeven met betrekking tot het onderzoek, dat het Parlement niet in staat was zijn democratische controle naar behoren uit te oefenen. De Commissie moet opnieuw beoordelen welke informatie zij openbaar kan maken om zinvol parlementair toezicht mogelijk te maken.

DOELWIT: LEDEN VAN HET EUROPEES PARLEMENT, DE RAAD EN DE COMMISSIE

420. Niet alleen een huidig lid van de Commissie en ander personeel van de Commissie waren het doelwit, maar ook regeringsleiders, ministers en een voormalig commissaris zouden het doelwit van spyware van buiten en binnen de Unie zijn geweest.

421. Het telefoonnummer van de Franse president Macron stond op de lijst van potentiële doelwitten van het Pegasus-project en de Spaanse regering bevestigde dat de telefoons van de Spaanse premier Pedro Sanchez, minister van Defensie Margarita Robles en minister van Binnenlandse Zaken Fernando Grande-Marlaska besmet waren met Pegasus-spionagesoftware, naar verluidt van buiten de Unie.

422. Volgens de Griekse krant Documento, die een uitgebreide lijst heeft gepubliceerd van mensen bij wie sporen van Predator op hun toestellen zouden zijn aangetroffen[763], waren Dimitris Avramopoulos, die van 2014 tot 2019 Europees commissaris was, en verschillende huidige ministers, waaronder de minister van Buitenlandse Zaken en de minister van Financiën, het doelwit van spyware. Het is niet duidelijk of de vermeende hackpogingen tegen Avramopoulos plaatsvonden terwijl hij lid was van de Commissie, noch is het duidelijk wie erachter zat. De lange lijst van personen die in het visier zijn genomen omvat echter vele Griekse politici van zowel de regeringspartij als de oppositie. Deze bevestigde en vermeende besmettingen en hackpogingen tonen aan dat het mogelijk is dat huidige regeringsleiders en ministers, en huidige of voormalige leden van de Commissie, met inbegrip van hun communicatie met collega's, van buiten of binnen de Unie het doelwit zijn geweest terwijl zij lid waren van de Europese Raad, de Raad en de Commissie. Daarom zou één besmette telefoon ook de informatie van de instellingen, met inbegrip van informatie die tijdens vergaderingen van de Commissie en de Raad in real time wordt uitgewisseld, ernstig in gevaar kunnen brengen.

[761] Antwoordbrief van de commissarissen Hahn en Reynders aan de commissie PEGA, 9 september 2022.
[762] Antwoordbrief van de commissarissen Hahn en Reynders aan de rapporteur, 25 juli 2022.
[763] Documento, uitgave van 6 november 2022.

I.H. Derde landen

423. In dit hoofdstuk wordt belicht in hoeverre het gebruik van Pegasus of soortgelijke surveillancespyware voor surveillancedoeleinden, waarbij direct of indirect met de EU verbonden entiteiten betrokken waren, heeft bijgedragen aan de illegale bespionering van journalisten, politici, wetshandhavers, diplomaten, advocaten, zakenmensen, actoren van het maatschappelijk middenveld, mensenrechtenverdedigers of andere actoren in derde landen. Daarbij wordt ook bekeken in hoeverre het gebruik van spyware heeft geleid tot mensenrechtenschendingen die van grote zorg zijn in verband met de doelstellingen van het gemeenschappelijk buitenlands- en veiligheidsbeleid van de EU, en of het gebruik van die spyware in strijd was met de waarden die zijn vastgelegd in artikel 21 VEU en het Handvest, mede gelet op de leidende beginselen inzake bedrijfsleven en mensenrechten van de Verenigde Naties en andere rechten die zijn vastgelegd in internationale mensenrechtenwetgeving.

424. Van de derde landen die betrokken zijn bij het gebruik van spyware hebben Israël en Marokko bijzondere aandacht gekregen van de commissie PEGA, met een hoorzitting en een bezoek aan Israël in juli 2022, en in februari 2023 een sessie van de hoorzitting over geopolitieke aspecten van spyware die aan Marokko was gewijd. Daarnaast was een hoorzitting in augustus 2022 gedeeltelijk gewijd aan Rwanda, met opmerkingen van Carine Kanimba, die een doelwit van Pegasus was.

ISRAËL

425. De commissie PEGA bracht in juli 2022 een bezoek aan Israël. Het hoofddoel van de reis was een ontmoeting met de producent van Pegasus-spyware, het in Israël gevestigde bedrijf NSO-groep. De PEGA-delegatie vernam dat de NSO-groep spyware heeft verkocht aan 14 EU-regeringen, met gebruikmaking van exportvergunningen van de Israëlische regering. Zij bespraken het misbruik van commerciële surveillanceinstrumenten en de gevolgen daarvan voor de democratie, de rechtsstaat en de grondrechten in de EU. De commissie heeft ook ontmoetingen gehad met vertegenwoordigers van de regering, de Knesset, deskundigen en het maatschappelijk middenveld. Dit bezoek onderstreepte de doeltreffendheid van de bestaande beschermingsmaatregelen tegen misbruik van spyware en de noodzaak van een veel strengere regelgeving van de Europese Unie voor de verkoop, de aankoop en het gebruik van spyware. Het gebied van cyberinlichtingen moet doeltreffend worden gereguleerd om misbruik van spyware in de toekomst te voorkomen.

426. De geopolitieke en veiligheidssituatie van Israël heeft de regering en de particuliere sector ertoe aangezet instrumenten voor het verzamelen van inlichtingen te ontwikkelen waarmee de cyberbeveiligingscapaciteit van het land kan worden uitgebreid, vooral met het oog op de verdediging ervan. In de loop der jaren is Israël een van ’s werelds belangrijkste producenten van geavanceerde surveillancetechnologieën en spyware geworden, aangezien het land een aanzienlijke expertise heeft in het ontwikkelen van instrumenten voor het verzamelen van inlichtingen. De sector exporteert zijn producten wereldwijd. In een studie in opdracht van het Europees Parlement die in 2023 werd gepubliceerd onder de titel “Pegasus en de externe betrekkingen van de EU” wordt opgemerkt dat “voor de exporterende landen de spywaresector een lucratieve bron van

inkomsten kan zijn en een middel om diplomatieke invloed uit te oefenen”[764]. Dit wordt ook bevestigd door nieuwsberichten, waarin experts het nut van Pegasus bevestigen om diplomatieke betrekkingen tot stand te brengen, zoals met de Golfstaten[765].

427. Behalve om te voldoen aan deze strategische binnenlandse redenen heeft Israël zichzelf daarnaast met succes gepromoot als innovatieve start-supinatie, met bedrijven met de meest geavanceerde technologie op dit gebied, zoals NSO, Cellebrite, Candiru, QuaDream en Intellexa. De totale omzet van de sector wordt geschat op ten minste 1 miljard USD per jaar[766], wat neerkomt op ongeveer 0,6 % van de Israëlische uitvoer[767]. De Israëlische strijdkrachten en inlichtingendienst, en met name de cyberbeveiligingsafdeling Eenheid 8200, hebben een centrale rol gespeeld in Israëls succesvolle spywaresector, en bedrijven onderhouden nauwe banden met de entiteit. Volgens een studie uit 2018 was 80 % van de 2 300 personen die de 700 cyberbeveiligingsbedrijven in Israël hebben opgezet voormalige personeelsleden van de inlichtingeneenheden van de Israëlische strijdkrachten. Een van de meest prominente figuren binnen de sector is de eigenaar en oprichter van Intellexa, Tal Dilian (zie het hoofdstuk over Intellexa en Tal Dilian)[768].

428. Spywarebedrijven uit Israël hebben overal ter wereld surveillancetechnologie verkocht, waaronder aan EU-lidstaten en aan autoritaire Golfstaten. Volgens de krant Haaretz werd de verkoop van Pegasus gebruikt als diplomatiek ruilmiddel en vergemakkelijkte het de onderhandelingen voor het aanknopen van formele diplomatieke banden met Marokko, Bahrein en, formeel, de Verenigde Arabische Emiraten in het kader van de Abraham-akkoorden[769]. De verkoop van spyware aan autoritaire regimes is bekritiseerd, vooral in de nasleep van het Pegasus-project. Als gevolg daarvan heeft de Israëlische regering in december 2021 de exportregels voor apparatuur voor cyberoorlogsvoering aangescherpt. In het licht van Israëls geplande justitiële hervorming krijgen veel Israëlische technologiebedrijven naar verluidt van Griekenland, Cyprus en Portugal stimulerende aanbiedingen om hun bedrijven naar deze landen te verplaatsen. Volgens berichten in de media zouden de drie landen Israëlische technologiebedrijven belastingvoordelen bieden, terwijl Griekenland naar verluidt versneld staatsburgerschap verleent[770].

429. Volgens deskundigen creëert de bereidheid van Israël om nieuwe surveillancesystemen te testen op Palestijnen in de bezette gebieden stimulansen voor een bedrijfsmodel in de

---

[764] “Pegasus and the EU’s external relations”, Europees Parlement, directoraat-generaal Intern Beleid, beleidsondersteunende afdeling C – Rechten van de burger en Constitutionele Zaken, 25 januari 2023.
[765] https://www.france24.com/en/livenews/20210719-pegasus-scandal-showsrisk-of-israel-s-spy-tech-diplomacyexperts
[766] https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000
[767] https://en.globes.co.il/en/article-israels-exports-rise-sharply-in-2022-1001433699#:~:text=According%20to%20a%20conservative%20estimate,a%20then%20record%20%24144%20billion
[768] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106
[769] Haaretz (2022) “Netanyahu gebruikte NSO’s Pegasus voor diplomatie”, https://www.haaretz.com/israelnews/2022-02-05/tyarticle/.premium/netanyahu-used-nsospegasus-for-diplomacy-now-he-blames-itfor-his-downfall/0000017f-e941-dc91- a17f-fdcd55c80000
[770] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106

surveillancesector, waarvan ook NSO heeft geprofiteerd[771]. Als resultaat hiervan dragen landen die de "praktisch geteste" spyware uit Israël kopen bij aan de mensenrechtenschendingen in de bovengenoemde regio's. Het gedrag van EU-lidstaten, evenals dat van NSO's meest prestigieuze klanten, staat dan ook haaks op de EU-agenda inzake het buitenlands en veiligheidsbeleid ten aanzien van het steunen van de mensenrechten en de democratie[772].

430. De Pegasus-spyware van NSO is ingezet tegen het Palestijnse maatschappelijk middenveld, waaronder zes Palestijnse mensenrechtenverdedigers[773]. In het geval van Ubai Al-Aboudi, uitvoerend directeur van het Bisan Center for Research and Development, en Salah Hammouri, met dubbele Franse-Palestijnse nationaliteit, advocaat en veldonderzoeker bij Addameer Prisoner Support and Human Rights Association, lijkt het gebruik van surveillancespyware te hebben geleid tot hun administratieve inhechtenisneming. De surveillance van alle zes betrokken personen valt samen met de uiterst omstreden aanwijzing van zes Palestijnse mensenrechtenorganisaties als "terroristisch", die heeft geleid tot internationale protesten waarbij het besluit van de Israëlische regering werd veroordeeld. Deze surveillance van Palestijnse mensenrechtenverdedigers eens te meer een bewijs van het gebrek aan handhaving van het mensenrechtenbeleid van NSO[774], dat het bedrijf heeft gebruikt om zijn legitimiteit en geloofwaardigheid kracht bij te zetten bij de verkoop aan EU-lidstaten.

431. Opgemerkt moet worden dat de Commissie contact heeft opgenomen met de Israëlische autoriteiten over de meldingen van misbruik van de Pegasus-spyware van NSO, in strijd met de mensenrechten. In een brief aan de commissie PEGA van 9 september 2022 antwoordde de Commissie dat zij haar zorgen over het mogelijke misbruik kenbaar had gemaakt aan de Israëlische uitvoerautoriteiten en "had verzocht om informatie over eventuele passende risicobeperkende maatregelen die de bevoegde Israëlische instanties voor uitvoercontrole in de toekomst zouden kunnen overwegen". Ten tijde van de brief had de Commissie deze informatie nog niet van de bevoegde Israëlische instanties voor uitvoercontrole ontvangen, maar zij was van plan "het thema van de mogelijke risicobeperkende maatregelen opnieuw aan te kaarten tijdens de volgende vergadering van de subcommissie EU-Israël inzake industrie, handel en diensten in het kader van de associatieovereenkomst".

MAROKKO

432. Talrijke nieuwsberichten hebben beschuldigingen gedocumenteerd dat Marokko op grote schaal gebruik maakt van spyware. Met een licentie voor circa 100 000 telefoonnummers kan Marokko als een van de grootste Pegasus-klanten van NSO

[771] PEGA-missie naar Israël, 18 tot 20 juli 2022.
[772] In overeenstemming met de meeste bevindingen in het jaarverslag van de Commissie over de toepassing van het EU-Handvest van de grondrechten 2021, getiteld "Bescherming van de grondrechten in het digitale tijdperk", is de EU gehouden de onlinewerkzaamheden van mensenrechtenverdedigers te faciliteren.
[773] https://www.frontlinedefenders.org/en/statement-report/statement-targetingpalestinian-hrds-pegasus; https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/
[774] https://www.amnesty.org/en/latest/researc h/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/

worden beschouwd[775]. Marokko heeft de aantijgingen naar aanleiding van het Pegasusproject afgedaan als “onjuist”. In december 2020 bleek uit een rapport van Citizen Lab dat Marokko een van de 25 klanten is van Circles, een dochteronderneming van de NSO-groep[776].

433. Het onderzoek liet ook zien dat naar verluidt surveillance samen met spyware in het land is gebruikt om journalisten en activisten te hacken en hen vervolgens te intimideren[777]. In een recente resolutie over de surveillance en gevangenneming van onderzoeksjournalist Omar Radi heeft het Europees Parlement het feit veroordeeld dat de Marokkaanse regering journalisten aanhoudend met juridische aanklachten bestookt, en er bij de Marokkaanse autoriteiten op aangedrongen “een einde te maken aan hun surveillance van journalisten, onder meer via de Pegasus-spyware van NSO”[778]. Een van de doelwitten, Ignacio Cembrero, een onderzoeksjournalist die werkt voor de Spaanse krant El Confidencial, verscheen op 29 november 2022 voor de commissie PEGA. Hij ontdekte dat zijn telefoon was gehackt nadat tekstberichten tussen hem en de Spaanse overheid in een Marokkaanse krant werden gepubliceerd. Toen een Spaanse rechtbank om hun medewerking verzocht, weigerden de Israëlische autoriteiten verdere informatie ter ondersteuning van de zaak te verstrekken.

434. Marokko heeft ook Hicham Mansouri en Aboubakr Jamaim vervolgd[779], twee Marokkaanse journalisten die in ballingschap in Frankrijk verblijven, alsmede voorvechters van de Westelijke Sahara, onder wie de in Parijs gevestigde advocaat Joseph Breham en de in België gevestigde Sahraoui-mensenrechtenverdediger El Mahjoub Maliha[780].

435. Marokko heeft diverse rechtszaken aangespannen in reactie op aantijgingen over de betrokkenheid van het land bij het gebruik van Pegasus in Frankrijk, Spanje en Duitsland. In Frankrijk hebben de Marokkaanse autoriteiten rechtszaken aangespannen wegens laster tegen verschillende mediakanalen en maatschappelijke organisaties, waaronder Le Monde, Forbidden Stories, Radio France, Mediapart, L’Humanité en Amnesty International. Op 25 maart 2022 verklaarde het strafhof van Parijs de zaken niet-ontvankelijk, waarop de Marokkaanse autoriteiten beroep aantekenden. In Spanje spanden de Marokkaanse autoriteiten een zaak aan tegen journalist Ignacio Cembrero op basis van een uit de middeleeuwen stammende bepaling in het Wetboek van Strafrecht, waarbij zij hem beschuldigden van “opschepperij”. Deze zaak loopt nog en wordt bekritiseerd omdat hij bedoeld zou zijn als een poging om Cembrero en anderen te weerhouden over het gebruik van de spyware door Marokko te berichten[781].

436. Volgens een nieuwsbericht was Marokko ook voordat het op grote schaal gebruik

---

[775] https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara
[776] https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
[777] https://daraj.media/en/76202/
[778] Resolutie van het Europees Parlement van 19 januari 2023 over de situatie van journalisten in Marokko, met name de zaak Omar Radi, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_NL.html
[779] Forbidden Stories. https://forbiddenstories.org/journaliste/hicham-mansouri/, https://forbiddenstories.org/journaliste/aboubakr-jamai/
[780] https://www.middleeasteye.net/fr/entretien s/pegasus-espionnage-maroc-francemacron-sahara-occidental-brehamavocat-mangin-algerie
[781] https://www.middleeastmonitor.com/20220705-morocco-files-lawsuit-against-spain-journalist-who-reported-use-of-pegasus-spyware/

maakte van Pegasus ook al klant bij ten minste drie Europese leveranciers van spyware, te weten de Franse bedrijven Amesys en Vupen[782] en het Italiaanse bedrijf Hacking Team. Volgens vertrouwelijke documenten was Marokko de twee na grootste klant van het Italiaanse bedrijf en betaalde het in de loop van zes jaar meer dan 3 miljoen EUR voor de aankoop van Hacking Team's RCS-software voor de Marokkaanse Hoge Nationale Raad voor Defensie (CSDN) en het Directoraat voor Territoriale Surveillance (DST)[783]. Diverse VN-afdelingen en -diensten op hoog niveau zijn met behulp van deze spyware gesurveilleerd.

437. Marokko heeft niet alleen spyware in de EU gekocht, maar heeft ook technologische en financiële steun van de Europese Commissie ontvangen. Volgens Der Spiegel ontving Marokko twee spywaresystemen om personen te bespioneren voor grensbewakingsdoeleinden (de Frans-Libanese spyware XRY van het Frans-Libanese MSAB en spyware van het in de VS gevestigde Oxygen Forensics genaamd Detective)[784]. Daarnaast werden medewerkers van het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol) naar Marokko gestuurd om persoonlijk trainingen te geven over het gebruik van spyware, alsook om de politie te leren hoe zij informatie van profielen op sociale media kunnen halen door middel van sociale hacking[785]. In tegenstelling tot Pegasus kan de genoemde spyware alleen fysiek op toestellen worden aangebracht en laten zij geen sporen achter van het gebruik daarvan. In het bericht worden diverse gevallen geschetst waarin smartphones werden afgenomen van doelwitten, onder wie journalisten en activisten, en teruggegeven met hints over hun mogelijke besmetting. Hoewel het niet mogelijk is om te verifiëren of de spyware door derden op correcte wijze is gebruikt, zijn er geen aanwijzingen dat de Commissie het correcte gebruik van de geleverde technologieën heeft gecontroleerd. Analoog aan de situatie zoals beschreven in een klacht bij de EU-ombudsman over de financiering van surveillancetechnologieën in het kader van het EU-TFA-programma (zie het desbetreffende hoofdstuk hieronder), heeft de Commissie geen effectbeoordeling uitgevoerd om mogelijk misbruik van de geleverde technologieën in kaart te brengen. De Commissie heeft verklaard dat het aan de gebruiker, Marokko, is om de spyware op verantwoorde wijze en in overeenstemming met de contractuele overeenkomst (d.w.z. uitsluitend voor de in de overeenkomst genoemde doeleinden) in te zetten[786].

OVERIGE DERDE LANDEN

438. Wereldwijd hebben ten minste 75 landen, waaronder repressieve regimes, spyware gekocht en/of gebruikt[787]. Mensenrechtenorganisaties hebben talloze incidenten gedocumenteerd waarbij spyware werd misbruikt voor het hacken van politici,

[782] https://moroccomail.fr/2022/09/21/morocco-used-hacking-team-to-spy-on-the-un/
[783] https://privacyinternational.org/blog/1394 /facing-truth-hacking-team-leak-confirms-moroccan-government-use-spyware; https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
[784] https://www.spiegel.de/ausland/marokkowie-die-eu-rabatsueberwachungsapparat-aufruestet-ad3f4c00e-4d39-41ba-be6c-e4f4ba65035; https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware
[785] https://privacyinternational.org/longread/4289/revealed-eu-training-regimeteaching-neighbours-how-spy
[786] https://disclose.ngo/en/article/how-theeu-supplied-morocco-with-phonehacking-spyware
[787] Carnegie Endowment for International Peace, "Global Inventory of Commercial Spyware & Digital Forensics", 11 januari 2023, https://carnegieendowment.org/programs/democracy/commercialspyware.

journalisten, advocaten, mensenrechtenverdedigers en andere activisten uit het maatschappelijk middenveld die zich inzetten voor de mensenrechten, de rechten van vrouwen en milieubescherming[788].

DE MEDEPLICHTIGHEID VAN EU-LIDSTATEN ALS KLANTEN VAN DE NSO-GROEP VOOR HET MISBRUIK VAN PEGASUS IN DERDE LANDEN

439. De autoriteiten van 14 niet-EU-landen zijn waarschijnlijk verantwoordelijk voor veel gevallen waarbij de tot doelwit genomen personen zijn geïdentificeerd en de infectie technisch bewezen is. De betreffende landen zijn El Salvador, Mexico, Thailand, Marokko, India, Rwanda, Saudi-Arabië, Bahrein, Jordanië, Kazachstan, Togo, de Verenigde Arabische Emiraten, Israël en Azerbeidzjan[789].

440. Het Pegasusproject, een samenwerkingsverband van meer dan tachtig journalisten van 17 mediakanalen, heeft gedocumenteerd hoe Pegasus door repressieve regeringen is gebruikt om journalisten het zwijgen op te leggen, activisten aan te vallen en dissidenten te onderdrukken. Onderzoek door het Pegasusproject heeft uitgewezen dat familieleden van de Saoedische journalist Jamal Khashoggi het doelwit van Pegasus-spyware waren, zowel voordat als nadat hij op 2 oktober 2018 in Istanbul door Saoedische agenten werd vermoord, ook al heeft de NSO-groep dit herhaaldelijk ontkend. Het Security Lab van Amnesty International stelde vast dat de Pegasus-spyware nog maar vier dagen na de moord met succes op de telefoon van Khashoggi's verloofde, Hatice Cengiz, werd geïnstalleerd. Zijn vrouw, Hanan Elatr, was tussen september 2017 en april 2018 ook herhaaldelijk het doelwit van de spyware, evenals zijn zoon Abdullah, die ook als doelwit werd gekozen, samen met andere familieleden in Saoedi-Arabië en de Verenigde Arabische Emiraten[790].

441. Bovendien heeft het Pegasusproject aangetoond dat journalisten regelmatig het doelwit van Pegasus-software zijn geweest. in Mexico werd de telefoon van journalist Cecilio Pineda een paar weken voordat hij in 2017 werd vermoord als doelwit gekozen. Pegasus is ook gebruikt in Azerbeidzjan, een land waar nog maar een paar onafhankelijke mediakanalen over zijn. Volgens het onderzoek zijn meer dan veertig Azerbeidzjaanse journalisten geselecteerd als mogelijke doelwitten. Het Security Lab van Amnesty International ontdekte dat de telefoon van Sevinc Vaqifqizi, een freelance journalist die voor het onafhankelijke mediakanaal Meydan TV werkte, gedurende meer dan twee jaar was geïnfecteerd, tot mei 2021. In India werden ten minste veertig journalisten van vrijwel alle grote mediakanalen in het land tussen 2017 en 2021 als mogelijke doelwitten geselecteerd. Forensische tests hebben uitgewezen dat de telefoons van Siddharth Varadarajan en MK Venu, medeoprichters van het onafhankelijke onlinekanaal The Wire, nog tot juni 2021 met Pegasus-software waren geïnfecteerd[791].

---

[788] Forensic Architecture, Amnesty International en The Citizen Lab, "Digital Violence", https://www.digitalviolence.org/#/

[789] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[790] Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 19 juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/

[791] Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 19 juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/

442. Mensenrechtenverdedigers worden nog steeds regelmatig als doelwit gekozen, onder meer door de autoriteiten van de volgende landen: Mexico, El Salvador, Marokko, Rwanda, Israël, Jordanië, Saoedi-Arabië, Bahrein, Verenigde Arabische Emiraten, India, Kazachstan, Indonesië en Belarus[792]. In 2021 publiceerde Frontline Defenders een rapport waarin de gerichte surveillance van mensenrechtenverdedigers werd gedocumenteerd in landen waaronder India. In juli 2018 werden 16 mensenrechtenverdedigers op grond van de Indiase antiterreurwetgeving gevangen genomen in wat bekend staat als de Bhima Koregaon-zaak, die betrekking heeft op het geweld dat plaatsvond in Bhima Koregaon. Een van de mensenrechtenverdedigers, de 84-jarige jezuïet Stan Swamy, stierf in juli 2021 tijdens zijn hechtenis[793]. Uit digitaal forensisch onderzoek bleek dat het "bewijs" waarop de aanklagers tegen de groep zich baseerden door middel van Pegasus-spyware op de toestellen van de mensenrechtenverdedigers Rona Wilson en Surendra Gadling was geplant en dat er geen bewijs was dat de mensenrechtenverdedigers contact met elkaar hadden gehad[794].

II. De spywaresector

443. De Europese Unie is een aantrekkelijke plek voor de handel in bewakingstechnologieën en -diensten, inclusief spyware-tools. Aan de ene kant zijn de regeringen van de lidstaten potentiële klanten. Aan de andere kant doet het begrip "door de EU gereguleerd" dienst als een benchmark, die goed van pas komt op de wereldmarkt. De interne markt van de EU biedt vrijheid van verkeer en gunstige nationale belastingregelingen. Aanbestedingsregels kunnen worden omzeild middels het inroepen van redenen van nationale veiligheid, en regeringen kunnen gebruikmaken van gevolmachtigden of tussenpersonen, zodat het heel moeilijk is om de aankoop van spyware door overheidsinstanties op het spoor te komen of te bewijzen. De EU heeft strenge uitvoerregels, maar de laatste tijd is er een tendens dat de lidstaten deze omzeilen en een concurrentievoordeel proberen te behalen door een onjuiste nationale tenuitvoerlegging ervan. Bovendien is de handhaving door de Europese Commissie vaak ontoereikend geweest. Erger nog, telkens wanneer de regeling voor uitvoervergunningen in Israël werd aangescherpt, verlegden verschillende bedrijven hun uitvoeractiviteiten naar Europa, met name Cyprus[795] [796]. Bovendien hebben verschillende belangrijke figuren uit de spyware-industrie het EU-burgerschap verkregen en kunnen zij aldus vrij binnen en vanuit de EU opereren.

444. Daarnaast waren het, zoals het hoofd van Amnesty Tech, Claudio Guarniery, tegen de commissie PEGA verklaarde, Europese bedrijven als het Duitse FinFisher en het Italiaanse Hacking Team die vooropliepen in de industrie voor commerciële spyware. De eerste berichten over de rol van deze bedrijven bij het monitoren van journalisten en het onderdrukken van dissidenten kwamen tien jaar geleden naar buiten, toen bij de als

[792] https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/; https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/

[793] Frontline Defenders (2 december 2021): "Action needed to address targeted surveillance of human rights defenders" https://www.frontlinedefenders.org/en/statement-report/action-needed-addresstargeted-surveillance-human-rightsdefenders

[794] The Wire, "Rona Wilson's iPhone Infected With Pegasus Spyware, Says New Forensic Report", 17 december 2021, https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal

[795] Makarios Drousiotis, "State Mafia", 2022, hoofdstuk 6.

[796] Haaretz. "Cyprus, Cyberspies and the Dark Side of Israeli Intel".

de Arabische Lente bekend staande protestbewegingen contracten met deze bedrijven opdoken uit de kantoren van de geheime politie[797].

445. De spywaresector heeft een ondoordringbare structuur, opgebouwd uit een doolhof van personen, vestigingen, dwarsverbanden, eigendomsstructuren, brievenbusfirma's, constant veranderende bedrijfsnamen, geldstromen, gevolmachtigden en tussenpersonen van overheden, magnaten en regeringen.

446. In veel gevallen lijkt de bijnaam "huurlingspyware" terecht te zijn. Zoals blijkt uit het aantal illegaal als doelwit gekozen personen, lopen veel bedrijven achter met betrekking tot ethische normen, verkopen zij vaak aan dictaturen en rijke niet-overheidsactoren, en blijven zij dit doen, zelfs na de onthullingen van het Pegasus-project. In 2021, toen bekend werd dat haar spyware was gebruikt tegen anti-Poetin activisten, kondigde Cellebrite aan te stoppen met de verkoop aan de Russische overheid. In oktober 2022 waren er echter aanwijzingen dat Cellebrite nog door de Russische autoriteiten wordt gebruikt[798]. Het is een lucratieve en schimmige markt. Het feit dat veel spywarebedrijven hun producten kunnen verkopen aan democratische regeringen in de VS en de EU verleent hen evenwel een schijn van eerbaarheid. Desalniettemin zijn overheden terughoudend als het erop aankomt toe te geven dat ze spyware bezitten, ondanks beweringen dat het gebruik van spyware volkomen legitiem en noodzakelijk is. Soms doen zij een beroep op gevolmachtigden, tussenpersonen of bemiddelaars om bij de aankoop van spyware geen sporen achter te laten. Het grote jaarlijkse evenement voor de sector is de "ISS World"-beurs, die ook wel "The Wiretappers' Ball" (het spionagegala) wordt genoemd. De jaarlijkse Europese editie vindt plaats in Praag. Veel van de exposanten op ISS World zijn ook terug te vinden op beurzen van de wapenindustrie.

447. Naast de "officiële kanalen" bestaat er ook een zwarte markt voor deze producten. Hoewel veel aanbieders beweren dat zij alleen aan overheden verkopen, lijkt het erop dat zij ook proberen zaken te doen met niet-overheidsactoren. Het is heel moeilijk daarvan waterdicht bewijs te vinden, aangezien deze sector nauwelijks sporen achterlaat. De Griekse krant Documento beweert over bewijs te beschikken dat de software op de zwarte markt wordt verkocht – voor bedragen die oplopen tot 50 miljoen USD – niet alleen aan overheden en agentschappen voor terrorismebestrijding, maar ook aan particulieren[799]. Een andere Griekse krant, To Vima, meldde dat Predator was verkocht aan 34 klanten uit Griekenland[800]. Gelekte documenten tonen aan dat een illegale versie van het product die officieel alleen aan overheden werd verkocht, voor de prijs van 8 miljoen USD beschikbaar was, een bedrag dat ook de training van de agenten die het programma gaan gebruiken omvat, alsmede 24-uurs technische ondersteuning en monitoring van de sociale media-accounts van het doelwit[801].

448. De sector biedt een grote verscheidenheid aan surveillance- en inlichtingenproducten en

[797] PEGA-hoorzitting van 30 augustus 2022 over de gevolgen van spyware voor EU-burgers, https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/
[798] 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
[799] Documento, "Documento's 'Predator' revelations on Euractiv – Europol's intervention calls for Dutch MEP".
[800] To Vima, Interceptions "Spy software has 34 customers".
[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/

-diensten, niet alleen spyware als op zichzelf staand product. Spyware is slechts één hulpmiddel uit het assortiment van “hack-for-hire”-bedrijven.

Zwakke plekken

449. Als software geen zwakke plekken had, zou het onmogelijk zijn om spyware te installeren en te activeren. Om het gebruik van spyware te reguleren, moeten er daarom ook regels komen voor de opsporing, het delen en het benutten van deze zwakke plekken[802]. De NIS 2-richtlijn (herziene richtlijn inzake beveiliging van netwerk- en informatiesystemen) en het Europese wetsvoorstel inzake cyberweerbaarheid omvatten vereisten en aanbevelingen ter versterking van de weerbaarheid van digitale systemen. Desondanks is het nagenoeg onmogelijk systemen zonder zwakke plekken te ontwikkelen.

450. Zwakke plekken moeten daarom zo snel mogelijk worden bekendgemaakt en verholpen. De huidige EU-wetgeving stimuleert bekendmaking echter niet, integendeel. Uit hoofde van de richtlijn inzake cybercriminaliteit en de auteursrechtenrichtlijn kunnen onderzoekers op het gebied van informatiebeveiliging strafrechtelijk en civielrechtelijk aansprakelijk worden gesteld wanneer zij onderzoek doen naar zwakke plekken en de resultaten daarvan delen. Bovendien is het voor onderzoekers niet verplicht om informatie over kwetsbaarheden te delen. Onderzoekers kunnen er daarom voor kiezen hun kennis over zwakke plekken te verkopen aan een particuliere tussenpersoon, in ruil voor een hoge vergoeding.

451. Deze praktijk heeft geleid tot een levendige en lucratieve handel in kwetsbaarheden. Het zijn echter niet alleen handelaren in onbeschermde zwakke plekken die op zoek zijn naar kwetsbaarheden: ook veiligheidsdiensten en rechtshandhavingsinstanties verzamelen zwakke plekken, die soms door hun eigen experts worden gevonden en soms van tussenpersonen worden gekocht. Als zwakke plekken niet worden gemeld, worden ze ook niet verholpen, waardoor IT-systemen verzwakken en gebruikers niet beschermd worden. Dit maakt het mogelijk om spyware te blijven gebruiken.

Telecomnetwerken

452. Telecomaanbieders spelen een belangrijke rol in het spionageproces, zowel bij legale als illegale spionage. Ons moderne tijdperk wordt gekenmerkt door artificiële intelligentie, big data en kwantumcomputing, maar tegelijkertijd berust de moderne telecommunicatie in grote mate op een internationaal protocol genaamd Signalling System nr. 7 (SS7). Dit protocol is ontwikkeld in 1975 en is nog altijd in gebruik. Dit systeem regelt de route die telefoongesprekken volgen en de manier waarop ze worden gefactureerd, biedt geavanceerde belopties en maakt het mogelijk om tekstberichten (sms: Short Message Service) te versturen[803]. Via het SS7-netwerk kunnen telefoongesprekken en tekstberichten worden onderschept, geolocaties worden

[802] Interventie van Ot van Daalen voor de commissie PEGA, 27 oktober 2022;

Nota van EDRi: “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

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

geïdentificeerd en kan een doelwit worden besmet met spyware, zoals Pegasus of Predator[804].

453. Het risico van misbruik door telecombedrijven die toegang bieden tot deze netwerken is hoog. Er bestaan verschillende gedocumenteerde gevallen van misbruik, waarbij toegangspunten ("global titles") werden verhuurd aan bedrijven die de communicatie van doelwitten controleerden en onderschepten met behulp van "man-in-the-middle"-aanvallen. Zij verzamelden ook geolocatiegegevens en metadata voor hun eigen economische doeleinden. Een "global title" is een adres dat wordt gebruikt voor het routeren van berichten binnen SS7. Het valt te vergelijken met een IP-adres, in de zin dat de global title verwijst naar een adres in het telecommunicatiesysteem[805]. Volgens een klokkenluider is dit de reden dat NSO zó geïnteresseerd was in toegang tot het SS7-netwerk in de VS dat het probeerde toegang te kopen van hun bedrijf[806]. Telecomaanbieders houden de normen in de sector bewust laag om lokale rechtshandhavingsinstanties gemakkelijker toegang te bieden.

De NSO-groep

454. Pegasus-spyware wordt geproduceerd door de NSO-groep. Deze groep is in 2010 opgericht door Shalev Hulio, Omri Lavie and Niv Karmi en ontwikkelt technologie om gemachtigde overheidsagentschappen en rechtshandhavingsinstanties te helpen terrorisme en misdaad op te sporen en te voorkomen[807]. Pegasus-spyware is het bekendste product van de NSO-groep. De spyware werd in 2011 op de internationale markt gebracht[808] [809].

455. Sinds het bedrijf in 2010 werd opgericht, heeft de NSO-groep vestigingen gehad in Israël, het VK, Luxemburg, de Kaaimaneilanden, Cyprus, de VS, Nederland, Bulgarije en de Britse Maagdeneilanden. Veel informatie over de rol van deze verschillende vestigingen ontbreekt nog en sommige bedrijven zijn inmiddels al opgeheven. De NSO-groep heeft in haar transparantie- en verantwoordelijkheidsrapport 2021 verklaard dat Bulgarije en Cyprus beide uitvoerknooppunten zijn[810]. Volgens Amnesty International fungeerden de Nederlandse entiteiten (opgeheven per 22 december 2016) als financiële holdings en was het in Luxemburg gevestigde Q Cyber Technologies actief als commerciële distributeur die verantwoordelijk was voor de afgifte van facturen, de ondertekening van contracten en de incasso van betalingen door klanten. Daarnaast ondersteunde het in de VS geregistreerde Westbridge Technologies vermoedelijk de verkopen van het bedrijf in de VS[811].

456. NSO zou in 2020 een omzet hebben gehad van 243 miljoen USD[812]. Na de onthullingen door het Pegasusproject kampte het bedrijf echter met diverse problemen. De

---

[804] https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/
[805] https://www.gms-worldwide.com/glossary/global-title/
[806] https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims
[807] NSO-groep. "About us".
[808] The New York Times, "The Battle for the World's Most Powerful Cyberweapon".
[809] Shalev Hulio, "NSO Never Engaged in Illegal Mass Surveillance", The Wall Street Journal, 24 februari 2022.
[810] NSO-groep, "Transparency and Responsibility Report 2021".
[811] Amnesty International, "Operating from the shadows – inside NSO Group's corporate structure".
[812] Haaretz, "NSO Is Having a Bad Year – and It's Showing".

rechtszaken die Apple[813] en Meta[814] tegen het bedrijf hebben aangespannen, het Amerikaanse Ministerie van Handel dat NSO op de zwarte lijst zette, de aanscherping van de Israëlische uitvoerregelingen, kritische onderzoeken in verschillende landen en interne spanningen binnen het private-equityfonds achter de NSO-groep hebben geleid tot een forse daling van de winst. Op een bepaald moment liep de schuld van de NSO-groep naar verluidt zelfs op tot 6,5 maal de normale jaarlijkse inkomsten[815].

457. De commissie PEGA heeft twee vergaderingen gehad met de NSO-Groep, waarvan één in Brussel en één in Israël. De Pegasus-spyware werd aanvankelijk aan 22 eindgebruikers in 14 EU-lidstaten verkocht op basis van door Israël afgegeven handels- en uitvoervergunningen. De contracten met eindgebruikers in twee lidstaten werden vervolgens beëindigd[816]. Welke lidstaten tot de genoemde 14 lidstaten behoren, noch welke twee zijn gestaakt, is niet bevestigd. Er kan echter worden aangenomen dat het bij die twee om Polen en Hongarije gaat.

BEDRIJFSSTRUCTUUR, TRANSPARANTIE EN ZORGVULDIGHEID (DUE DILIGENCE)

458. Op 25 januari 2010 richtte de NSO-groep in Israël haar eerste bedrijf op. Dit bedrijf werd geregistreerd onder de naam "NSO Group Technologies Limited". "NSO Group" is zowel de naam van dit als eerste geregistreerde bedrijf als de overkoepelende term voor de diverse ondernemingen die in andere rechtsgebieden zijn gevestigd. Het eerst opgerichte bedrijf is eigenaar van het handelsmerk "NSO Group"[817].

459. In maart 2014 verwierf het private-equityfonds Francisco Partners een belang van 70 % in de NSO-groep. Onder Francisco Partners breidde het bedrijf zijn aanwezigheid uit naar verschillende rechtsgebieden, waaronder Cyprus, Bulgarije, de VS, Nederland en Luxemburg. Tijdens de jaren met Francisco Partners (2014 tot 2019) beoordeelde het fonds stelselmatig de verkoop van de producten van de NSO-groep door middel van de Business Ethics Committee (BEC – de commissie bedrijfsethiek). Volgens Francisco Partners heeft de BEC tientallen miljoenen dollars aan verkopen afgewezen die anders, zuiver op wettelijke gronden, zouden zijn goedgekeurd[818].

460. Francisco Partners verkocht zijn volledige belang, waaronder dat in de dochterondernemingen, op 14 februari 2019 aan Novalpina Capital. Na deze management buy-out veranderden de governancenormen en werd de BEC vervangen door de Governance, Risk and Compliance Committee (GRCC – de commissie governance, risico en naleving), die de staat van dienst op het gebied van de mensenrechten van potentiële klanten moest beoordelen[819].

461. In overeenstemming met de verklaring inzake eindgebruik/eindgebruiker na aanscherping van de Israëlische uitvoerregelingen heeft de NSO-groep een mensenrechtenbeleid en een zorgvuldigheidsprocedure voor mensenrechten ingevoerd. Zoals wordt beschreven in het transparantie- en verantwoordelijkheidsrapport 2021 van

[813] Apple, "Apple sues NSO Group to curb the abuse of state-sponsored spyware".
[814] Bloomberg Law, "NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware".
[815] Bloomberg, "Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop".
[816] Antwoorden verstrekt door de NSO-groep aan het PEGA-secretariaat na de hoorzitting op 20 juli 2022.
[817] Amnesty International, "Operating from the shadows – inside NSO Group's corporate structure".
[818] Amnesty International, "Operating from the shadows – inside NSO Group's corporate structure".
[819] Hoorzitting van de commissie PEGA met NSO, 21 juni 2022.

de NSO-groep, vereist de NSO-groep dat alle contracten met klanten clausules over de naleving van de mensenrechten bevatten, alsook clausules waarin de opschorting of beëindiging van het gebruik van de producten van de NSO-groep wordt bedongen in geval van misbruik dat verband houdt met de mensenrechten. In een schriftelijke verklaring aan PEGA heeft de NSO-groep bevestigd dat zij de contracten heeft opgezegd met EU-lidstaten[820] die de clausules inzake de mensenrechten zouden hebben geschonden. De NSO-groep heeft niet verduidelijkt of zij de auditverslagen heeft onderzocht en of de klanten in kwestie met een dergelijk onderzoek hadden ingestemd. Het is dan ook niet bekend of er nog enig bewijs van het misbruik bestaat, of de NSO-groep dat bewijs kan bewaren en of de Israëlische autoriteiten over enig bewijs beschikken.

462. Volgens Amnesty International ontbreekt in het transparantierapport van de NSO-groep een behoorlijk herstelbeleid voor personen die het doelwit zijn geworden van onrechtmatige surveillance, en bevat het ook geen informatie over de rechtszaken die tegen de NSO-groep lopen[821]. Er blijft spyware van NSO worden ontdekt op de toestellen van journalisten en critici van autoritaire regimes, in strijd met het mensenrechtenbeleid en de zorgvuldigheidsprocedure van NSO[822].

EXPORTCONTROLES

463. Aangezien Pegasus-spyware wordt geclassificeerd als een technologie voor tweeërlei gebruik, moet er een vergunning worden toegekend voor de uitvoer ervan. De ondernemingen van de NSO-groep verkrijgen hun uitvoervergunningen in Israël, Bulgarije en Cyprus[823]. De NSO-groep zelf heeft dit bevestigd, maar ontkent dat Pegasus-spyware wordt uitgevoerd vanuit Cyprus en Bulgarije[824]. De regeringen van Cyprus en Bulgarije hebben ontkend dat zij uitvoervergunningen hebben verleend aan NSO-bedrijven in het algemeen. Andere bronnen hebben dit in twijfel getrokken en beweren dat de dochterondernemingen van NSO zich in de nationale handelsregisters vaak achter een andere naam verschuilen. Maar een van de dochterondernemingen van NSO in Cyprus, die opereerde onder de naam Circles, heeft haar kantoor in 2020 gesloten[825]. Er zijn ook vergunningen verleend door de Israëlische autoriteiten[826]. Israël maakt geen deel uit van het Wassenaar Arrangement, maar verklaart dat het een aantal elementen ervan heeft opgenomen in de Israëlische nationale wet betreffende de controle op de defensie-uitvoer nr. 5766-2007[827]. Het Agentschap voor de controle op defensie-uitvoer van het Ministerie van Defensie is verantwoordelijk voor de afgifte van verkoop- en uitvoervergunningen[828]. Na de onthullingen van het Pegasusproject en nadat NSO op de zwarte lijst is gezet, is lijst van landen waar Pegasus kan worden verkocht teruggebracht van 102 naar 37. Al deze landen moeten een verklaring inzake

[820] Hoorzitting van de commissie PEGA met NSO, 21 juni 2022.
[821] Amnesty International, "NSO Group's new transparency report is 'another missed opportunity'", persbericht, 1 juli 2021.
[822] The New York Times, "U.S. Blacklists Israeli Firm NSO Group Over Spyware".
[823] Amnesty International, "Operating from the shadows - inside NSO Group's corporate structure", blz. 62.
[824] Amnesty International, "Operating from the shadows - inside NSO Group's corporate structure".
[825] VICE, "NSO Group Closes Cyprus Office of Spy Firm".
[826] Amnesty International, "Operating from the shadows - inside NSO Group's corporate structure".
[827] Onderzoeksdienst van het Europees Parlement, "Europe's PegasusGate – countering spyware abuse".
[828] Amnesty International, "Novalpina Capital's reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (6 March 2019)".

eindgebruik/eindgebruiker ondertekenen[829]. Op grond van zijn zorgvuldigheidsprocedure gaat Israël er automatisch vanuit dat alle EU-lidstaten aan de EU-normen voldoen. Het voert dan ook geen aanvullende beoordelingen voor afzonderlijke landen uit. Het feit dat Israël heeft besloten om de contracten met twee EU-lidstaten stop te zetten, lijkt er evenwel op te wijzen dat de EU in het kader van de zorgvuldigheidsprocedures niet langer als één enkele entiteit wordt beschouwd.

ONETHISCH GEDRAG DAT AANLEIDING GEEFT TOT RECHTSZAKEN, PLAATSING OP EEN ZWARTE LIJST EN CONFLICTEN TUSSEN INVESTEERDERS

464. In juli 2021 begon een conflict tussen de drie oprichters van Novalpina Capital gevolgen te hebben voor de activiteiten van de NSO-groep, wat de grootste investeerders uiteindelijk tot de beslissing bracht het private-equitybedrijf de zeggenschap over de groep te ontnemen[830]. Op 27 augustus 2021 nam het Amerikaanse adviesbureau Berkeley Research Group (BRG) het private-equityfonds over en startte het een kritisch onderzoek naar de rechtmatigheid van de activiteiten van de NSO-groep en naar de naleving door de groep van de Amerikaanse zwarte lijst. In mei 2022 werd BRG in zijn onderzoek gehinderd door het managementteam van de NSO-groep[831]. Een leidinggevende bij BRG verklaarde dat de samenwerking met de NSO-groep "vrijwel was stilgevallen" doordat de groep tot elke prijs zijn producten wilde blijven verkopen aan landen met een omstreden reputatie voor wat de mensenrechten betreft[832]. Op 25 april 2022 spanden twee voormalige beherende partners van Novalpina bij de Luxemburgse rechtbank een rechtszaak aan tegen BRG, waarin zij eisten dat Novalpina Capital opnieuw zou worden aangesteld als beherend partner en dat alle door BRG genomen beslissingen zouden worden opgeschort[833]. De Luxemburgse rechtbank heeft deze eisen afgewezen en BRG is nog altijd verantwoordelijk voor het fonds dat de grootste eigenaar is van de NSO-groep[834].

465. Naast de ruzie over de eigendom werd de NSO-groep op 3 november 2021 door het Amerikaanse Ministerie van Handel op een zwarte lijst gezet vanwege de onverenigbaarheid van haar activiteiten met het buitenlandse beleid en de nationale-veiligheidsbelangen van de VS. De Amerikaanse overheid verbiedt de uitvoer van technologie naar de NSO-groep en haar dochterondernemingen, wat feitelijk betekent dat geen enkel Amerikaans bedrijf met de NSO-groep kan samenwerken[835].

466. Naar aanleiding van de opname op een zwarte lijst in de VS zou Credit Suisse, een van de schuldeisers van de NSO-groep, het bedrijf onder druk hebben gezet om door te gaan met de verkoop van Pegasus-software aan nieuwe klanten. In een brief aan BRG, gestuurd door Willkie Farr & Gallagher, stelden verschillende schuldeisers dat zij bezorgd waren dat BRG de NSO-groep belette om "nieuwe klanten te zoeken en binnen te halen". Hoewel dit niet uitdrukkelijk in de brief wordt gesteld, hebben twee deskundigen ter zake verklaard dat een van de schuldeisers Credit Suisse was. BRG

[829] Onderzoeksdienst van het Europees Parlement, "Europe's PegasusGate – countering spyware abuse".
[830] Financial Times, "Private equity owner of spyware group NSO stripped of control of €1bn fund".
[831] Financial Times, "NSO Group keeping owners "in the dark", manager says".
[832] The New York, "How democracies spy on their citizens".
[833] Brief aan de heer Jeroen Lenaers en zijn vicevoorzitters.
[834] Luxembourg Times, "Top five stories you may have missed".
[835] The New York Times, "U.S. Blacklists Israeli Firm NSO Group Over Spyware".

antwoordde de kredietverstrekkers dat het haar ernstig zorgen baarde dat zij de NSO-groep onder druk zetten om meer omzet te behalen[836].

467. Een paar dagen nadat NSO door de VS op een zwarte lijst was gezet, bevestigde het Amerikaanse Hof van Beroep dat de behandeling van de rechtszaak die door Meta tegen NSO was aangespannen door kon gaan. Onmiddellijk daarna diende Apple bij de federale rechtbank een klacht in tegen NSO[837]. In juni 2022 verwierp de Amerikaanse rechtbank het beroep van de NSO-groep op immuniteit in de door Apple aangespannen procedure[838]. Op het moment van schrijven is de rechtszaak van Apple tegen de NSO-groep nog aanhangig.

468. Ondanks de opname op de zwarte lijst zou de regering Biden in oktober 2022 een voormalig adviseur van NSO, Jeremy Bash, hebben benoemd tot lid van een inlichtingenadviesraad. Bash zou namens Beacon Global Strategies door Francisco Partners zijn ingehuurd om de NSO-groep te adviseren. Volgens The Guardian was hij een van de acht leden van NSO's commissie voor bedrijfsethiek, waardoor hij een stem zou hebben gehad in voorgestelde verkopen van NSO. Beacon Global Strategies beëindigde haar werk voor NSO na de beoogde verkopen van de groep aan Saoedi-Arabië[839].

469. De NSO-groep heeft ook te lijden gehad onder het vertrek van personeel. Sinds de moord op Jamal Kashoggi en de toenemende verontrusting over de rol van Pegasus daarbij, hebben veel medewerkers de NSO-groep verlaten. Diezelfde maand trad medeoprichter Shalev Hulio af als CEO van de NSO-groep en werd hij vervangen door Yaron Shohat[840]. De NSO-groep wijzigde vervolgens haar beleid en richt zich nu alleen op NAVO-leden[841]. In maart 2023 werd gemeld dat de aandelen van NSO waren overgedragen aan Dufresne Holding, de investeringsmaatschappij van medeoprichter Omri Lavie[842].

470. Door de druk op de NSO-groep is er vraag ontstaan naar andere spywarebedrijven. De Financial Times berichtte op 31 maart 2023 dat de Indiase regering op zoek zou zijn naar een mogelijkheid om alternatieve commerciële spyware te kopen met soortgelijke functies als de nu omstreden Pegasus-spyware, en dat zij ook de Predator-spyware van Intellexa zou overwegen[843].

471. In oktober 2022 richtten Shalev Hulio en de voormalige bondskanselier van Oostenrijk, Sebastian Kurz, een nieuw cyberbeveiligingsbedrijf op, genaamd Dream Security. Kurz trad in oktober 2021 na een corruptieschandaal af als bondskanselier en ging twee maanden later aan de slag voor de beleggingsfirma van Peter Thiel. Het bedrijf zal oplossingen creëren op het gebied van cyberincidenten, waarbij de nadruk zal liggen op

---

[836] Financial Times, "Credit Suisse pushed for spyware sales at NSO despite US blacklisting".
[837] The New York Times, "Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones".
[838] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/
[839] The Guardian, "Biden intelligence advisor previously vetted deals for Israeli NSO Group".
[840] The Washington Post, "CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup"; Calcalist, "After cutbacks and CEO departure, what's next for the controversial NSO?".
[841] The Guardian, "CEO of Israeli Pegasus spyware firm NSO to step down".
[842] The Guardian, "NSO Group co-founder emerges as new majority owner".
[843] https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9

kunstmatige intelligentie, en zich commercieel richten op de Europese markt.[844] De samenwerking tussen Kurz en Hulio vormt een indirecte, maar verontrustende connectie tussen de spyware-industrie en Peter Thiel en zijn bedrijf Palantir.

472. Dream Security haalde 20 miljoen USD op bij verschillende investeerders, zoals Adi Shalev, die ook betrokken was bij investeringen in NSO. Een andere investeerder is Yevgeny Dibrov[845], die de "nieuwe Russische stem" vertegenwoordigt in wat hij "het Russisch-Israëlisch technologisch ecosysteem" noemt[846]. Hieruit blijkt dat, ondanks de turbulentie en de economische uitdagingen waarmee de NSO-groep wordt geconfronteerd, dezelfde namen steeds weer nieuwe spywarebedrijven binnen en buiten de EU opzetten.

BLACK CUBE

473. Black Cube is een Israëlische particuliere inlichtingendienst die bestaat uit voormalige werknemers van het Israëlische leger en de Israëlische inlichtingendiensten[847]. Op zijn eigen website wordt het bedrijf beschreven als een "creatieve inlichtingendienst" die "oplossingen op maat" aanbiedt voor "complexe zakelijke uitdagingen en geschillen"[848]. Black Cube was betrokken bij een aantal hackingschandalen in verschillende landen, onder meer in de VS en in Roemenië[849]. De directie van Black Cube heeft met name toegegeven dat het bedrijf Laura Kovesi heeft bespioneerd, de voormalige hoofdaanklager van het Roemeense nationale directoraat voor corruptiebestrijding[850]. Kovesi is momenteel de eerste Europese hoofdaanklager, d.w.z. het hoofd van het Europees Openbaar Ministerie (EOM). Black Cube zou de opdracht hiervoor hebben gekregen van Daniel Dragomir, een voormalig Roemeens geheim agent[851].

474. Ernstig genoeg is ook ontdekt dat Black Cube banden heeft met de NSO-groep en Pegasus-spyware. Na veel publieke druk met betrekking tot het inhuren van Black Cube door NSO om hun tegenstanders te observeren, heeft Shalev Hulio, de voormalige directeur van NSO, toegegeven dat hij Black Cube voor ten minste één situatie op Cyprus had ingehuurd.

475. Black Cube was tijdens de verkiezingen van 2018 actief in Hongarije, waar het diverse ngo's en personen bespioneerde die mogelijke banden hadden met George Soros, en deed hiervan verslag aan Orbán, zodat hij hun activiteiten met een lastercampagne in een kwaad daglicht kon stellen[852]. De informatie die de surveillance van deze personen

[844] Organised Crime and Corruption Reporting Project, "Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm"; The Times, "Former NSO CEO and ex-Austrian Chancellor found startup".
[845] The Times, "Former NSO CEO and ex-Austrian Chancellor found startup".
[846] Calcalist, "From Russia, With Coding Skills".
[847] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 okober 2019.
[848] https://www.blackcube.com/
[849] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[850] Balkan Insight, "Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case".
[851] Haaretz, "Black Cube CEO Suspected of Running Crime Organisation – Revealed: The Romania Interrogation".
[852] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.

en ngo's opleverde, verscheen niet alleen in de door de Hongaarse staat gecontroleerde media, maar ook in de Jerusalem Post[853].

INTELLEXA ALLIANCE

476. Intellexa werd opgericht in 2019 in Cyprus door Tal Dilian. Dilian bekleedde verschillende leidinggevende functies bij de Israëlische krijgsmacht voordat hij een carrière begon als "inlichtingendeskundige, community builder en veelvoudig ondernemer"[854]. Op de website van Intellexa Alliance wordt het bedrijf beschreven als een in de EU gevestigde en gereguleerde onderneming die ten doel heeft technologieën te ontwikkelen en toe te passen waarmee inlichtingendiensten autonomer kunnen worden. De aanbieders van surveillancesoftware die deel uitmaken van het marketinglabel van Intellexa Alliance zijn Cytrox, WiSpear (later omgedoopt tot Passitora Ltd), Nexa Technologies (geleid door voormalige managers van Amesys) en Poltrex.

477. Al deze aanbieders leveren verschillende systemen. Terwijl Cytrox gespecialiseerd is in het kopiëren van gegevens uit mobiele telefoons, biedt Nexa Technologies gebruikmaking van mondiale mobiele-communicatiesystemen. WiSpear kan daarnaast gegevens uit wifi-netwerken kopiëren. De verschillende aanbieders binnen de alliantie van Dilian bieden derhalve een breed assortiment aan software en diensten die Intellexa apart of gecombineerd kan aanbieden aan haar klanten binnen en buiten de EU[855].

478. De moedermaatschappij van Intellexa Alliance, Thalestris Limited, heeft verschillende dochterondernemingen met vestigingen in Ierland, Griekenland, de Britse Maagdeneilanden, Zwitserland en Cyprus. Sara Aleksandra Hamou, naar verluidt de tweede ex-vrouw van Tal Dilian, was de directeur van Thalestris Limited en algemeen directeur van een dochteronderneming in Griekenland[856]. Hamou, die in Polen is geboren, heeft een Cypriotisch paspoort dat is afgegeven door de Poolse ambassade op Cyprus[857].

WISPEAR EN CYTROX

479. In 2013 richtte Tal Dilian Aveledo Ltd op, een op Cyprus geregistreerde onderneming waarvan de naam later werd veranderd in Ws WiSpear Systems Ltd en vervolgens in Passitora Ltd[858]. De onderneming is gevestigd in Limassol (Cyprus) en verkoopt voornamelijk apparatuur en software waarmee individuen via hun mobiele telefoon kunnen worden gelokaliseerd en gevolgd. In een interview met het tijdschrift Forbes legde Dilian de mogelijkheden van de WiSpear-software uit aan de hand van een demonstratie met zijn zwarte busje van 9 miljoen USD waarmee toestellen binnen een bereik van 500 meter kunnen worden gehackt. WiSpear bezit ook apparatuur die

[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[854] Tal Dilian. About.
[855] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[856] Thalestris Limited, jaarverslag en geconsolideerde jaarrekening voor de periode van 28 november 2019 tot en met 31 december 2020.
[857] ReportersUnited, "The Great Nephew and Big Brother".
[858] Open Corporates, "Passitora Ltd", https://opencorporates.com/companies/cy/HE318328

gegevens van wifi-netwerken kan onderscheppen[859]. Wegens een aantal publieke schandalen rond deze producten heeft Intellexa zijn voornaamste bedrijfsactiviteiten overgebracht van Cyprus naar Griekenland.

480. Cytrox Holdings Zrt. werd in 2017 in Noord-Macedonië opgericht door Ivo Malinkovski. In werkelijkheid is Cytrox echter afkomstig uit Tel Aviv en was Malinkovski alleen maar een dekmantel. Na de onthullingen van het Pegasusproject heeft Malinkovski geprobeerd alle sporen die hem met Cytrox verbonden uit te wissen.

481. Cytrox was het bedrijf dat de Predator-spyware ontwikkelde. In tegenstelling tot de Pegasus-spyware moet het doelwit bij Predator op een link klikken om de software te installeren[860]. Toen Cytrox op het punt stond failliet te gaan, werd het gered door Tal Dilian, via een overname die minder dan 5 miljoen USD kostte[861]. Cytrox werd vervolgens samengevoegd met Dilians bedrijf WiSpear[862]. Door deze overname werd de Predator-spyware toegevoegd aan het arsenaal technologieën van Intellexa. Zoals gemeld door Lighthouse Reports, in samenwerking met Haaretz en Inside Story, leverde Intellexa in het geheim en illegaal Predator-spyware aan de Soedanese militie Rapid Support Force met behulp van een privévliegtuig van het merk Cessna[863].

482. Volgens Citizen Lab zijn er twee Cytrox-bedrijven geregistreerd in Israël (Cytrox EMEA Ltd en Cytrox Software Ltd) en één in Hongarije (Cytrox Holdings Zrt.)[864]. Alle aandelen van Cytrox Holdings Zrt. en Cytrox EMEA Ltd – later omgedoopt tot Balinese Ltd – werden overgedragen aan Aliada Group Inc., dat geregistreerd staat op de Britse Maagdeneilanden. Aliada Group is ook de eigenaar van WiSpear. De voornaamste aandeelhouders van Aliada Group zijn Dilian zelf, Meir Shamir en Avi Rubinstein. In december 2020 diende Rubinstein een klacht in tegen zijn medeaandeelhouders van Aliada Group wegens de onrechtmatige verwatering van zijn aandelen. Volgens deze vordering werd met de overschrijving van de aandelen naar de Britse Maagdeneilanden en later naar Ierland de wetgeving inzake uitvoercontroles van Israël en andere landen omzeild[865].

483. Op 16 december 2021 bracht Citizen Lab een rapport naar buiten waarin werd gesteld dat er vermoedelijke klanten van Predator waren gevonden in Armenië, Egypte, Griekenland, Indonesië, Madagaskar, Oman, Saoedi-Arabië en Servië[866].

AMESYS EN NEXA TECHNOLOGIES

484. Ook Amesys en Nexa Technologies maken deel uit van Intellexa Alliance en hebben

---

[859] Haaretz, "As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire".
[860] Onderzoeksdienst van het Europees Parlement, "Greece's Predatorgate. The latest chapter in Europe's spyware scandal?".
[861] BalkanInsight, "Wine, Weapons and Whatsapp: A Skopje Spyware Scandal".
[862] Pitchbook, overzicht van Cytrox.
[863] https://www.lighthousereports.nl/investigation/flight-of-the-predator/
[864] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware".
[865] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware".
[866] Citizen Lab, "Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

een omstreden reputatie, zoals beschreven in het hoofdstuk over Frankrijk.

POLTREX

485. Poltrex werd opgericht in oktober 2018 en haar enige aandeelhouder was Intellexa Ltd, die geregistreerd staat op de Britse Maagdeneilanden. Shahak Avni, de Israëlische oprichter van het Cypriotische bedrijf NCIS Intelligence Services Ltd[867] en medewerker van Tal Dilian, werd in september 2019 geregistreerd als directeur van Poltrex. In oktober 2019 werden Avni en Dilian allebei directeur van Poltrex en werd de naam van het bedrijf gewijzigd in Alchemycorp Ltd. Maar hoewel het bedrijf een andere naam had gekregen, zaten de kantoren nog steeds in de Novel Tower, dezelfde locatie als de kantoren van WiSpear[868].

486. Toen het onderzoek naar de spywarebestelwagen van Dilian aan e gang was, werd de eigendom van Alchemycorp Ltd overgedragen aan Yaron Levgoren, een werknemer van Cytrox Holdings[869]. Volgens zijn LinkedIn-pagina vertegenwoordigt Levgoren momenteel de Intellexa-dochter Apollo Technologies, die in Griekenland is gevestigd[870].

VERINT/COGNYTE

487. Verint is een Israëlisch-Amerikaans cyberbedrijf met een groot aantal dochterondernemingen in de hele wereld. Alleen al in Europa is Verint geregistreerd in Bulgarije, Nederland, Cyprus, Duitsland en Frankrijk (toestand in 2021). Verint had ook dochterondernemingen die actief waren onder de naam Cognyte. Deze dochterondernemingen opereren zelfstandig sinds 2021, nadat Verint de overdracht van haar inlichtingen- en cyberactiviteiten aan Cognyte had voltooid[871]. De Europese dochterondernemingen van Cognyte's staan geregistreerd in Cyprus (UTX Technologies), Bulgarije (Cognyte Bulgaria EOOD), Nederland (Cognyte Netherlands B.V.), Duitsland (Syborg GmbH, Syborg Grundbesitz GmbH en Syborg Informationsysteme b.h. OHG) en Roemenië (Cognyte Romania S.R.L.)[872].

488. Verint heeft surveillance-instrumenten verkocht aan diverse repressieve regeringen, waaronder die van Azerbeidzjan, Indonesië en Zuid-Soedan. In het laatste geval gebruikte de Zuid-Soedanese nationale veiligheidsdienst (National Security Service – NSS) de interceptie-apparatuur van Verint tussen maart 2015 en februari 2017 tegen mensenrechtenactivisten en journalisten. Volgens een onderzoek van Amnesty International stelde Vivacell Network of the World, een lokale exploitant van mobiele telecommunicatie, de NSS in staat om alle telecommunicatie in het land af te luisteren[873]. Verint reageerde niet op vragen van Amnesty, maar bracht wel een verklaring naar buiten waarin werd uitgelegd dat Verints zelfstandig opererende onderdeel Cognyte in feite de defensiedivisie vormt en dat Verint uitsluitend het

[867] Philenews, "FILE: The state insulted Avni and Dilian".
[868] CyprusMail, "Akel says found "smoking gun" linking Cyprus to Greek spying scandal".
[869] Philenews, "How the spyware scandal in Greece is related to Cyprus".
[870] https://ca.linkedin.com/in/yaron-levgoren-116948101
[871] Calcalistech, "Verint completes spin-off of its defense activities into new company Cognyte Software".
[872] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm
[873] Haaretz, "Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds"; Amnesty International, "South Sudan: rampant abusive surveillance by NSS instils climate of fear".

klantenbeheer verzorgt. Verint beweert dat de afscheiding van Cognyte al jaren een feit was voordat het in 2021 officieel werd afgesplitst en distantieert zich daarmee van de vermeende uitvoer van surveillanceapparatuur aan landen met een slechte reputatie op het gebied van de mensenrechten[874].

489. Cognyte heeft in het verleden ook vaak producten uitgevoerd naar landen met een slechte reputatie op het gebied van de mensenrechten. In 2021 werden bij een onderzoek van Meta klanten gevonden in Israël, Servië, Colombia, Kenia, Marokko, Mexico, Jordanië, Thailand en Indonesië[875]. Cognyte-dochteronderneming UTX Technologies, die op Cyprus geregistreerd staat, zou tussen september 2014 en maart 2015 ook vergunningen hebben gekregen voor de uitvoer van monitoringsoftware naar Mexico, de Verenigde Arabische Emiraten, Nigeria, Israël, Peru, Colombia, Brazilië, Zuid-Korea en Thailand[876]. Vier van deze landen werden ook geïdentificeerd als klanten Cognyte in het Meta-rapport van 2021. Daarnaast sloot UTX Technologies in 2019 een overeenkomst met Bangladesh voor een inlichtingensysteem voor het internet ter waarde van 2 miljoen USD en in 2021 voor een volgsysteem voor mobiele telefoons ter waarde van 500 000 USD[877].

490. Op 15 januari 2023 berichtten de media dat het Israëlische Cognyte Software Ltd een aanbesteding had gewonnen voor de levering van zijn interceptie-spyware aan Myanmar, één maand voor de militaire staatsgreep in februari 2021. De aankoop van de Cognyte-spyware door Myanmar vond officieel plaats op 30 december 2020[878].

491. Cognyte exporteert niet alleen naar derde landen, maar heeft ook het vervoer van volgapparatuur naar lidstaten gefaciliteerd. Via het in Cyprus geregistreerde bedrijf UTX Technologies werd Gi2-technologie verstuurd naar Syborg Informationsysteme, een andere dochteronderneming van Cognyte in Duitsland[879]. Deze Gi2-technologie zou ook naar een dochteronderneming van Verint in Polen zijn gestuurd, voor "demonstratiedoeleinden". Gi2-technologie biedt de mogelijkheid toegang te krijgen tot een specifiek toestel en zelfs om zich voor te doen als de eigenaar ervan en valse berichten te sturen met datzelfde toestel[880]. Deze zendingen vonden plaats in 2013 en 2014. Op dat moment maakten Verint en Cognyte nog deel uit van dezelfde bedrijfsstructuur.

492. UTX Technologies verkocht in 2013 ook monitoringsystemen aan een Frans exportbedrijf genaamd COFREXPORT[881]. Dit bedrijf is niet langer actief en was op het moment van schrijven opgeheven.

493. Zoals veel andere aanbieders van spyware heeft Cognyte een uiterst complexe bedrijfsstructuur ten gevolge van de naamswijzigingen en de op- en afsplitsingen die in de loop der tijd hebben plaatsgevonden. De dochterondernemingen van Cognyte laten echter zien dat de EU-lidstaten niet alleen worden gebruikt als basis om

[874] Haaretz, "Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds".
[875] Meta, Threat Report on the Surveillance-for-Hire Industry.
[876] Philenews, "Cyprus is a pioneer in software exports" (documenten).
[877] Haaretz, "Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records".
[878] Reuters, "Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup" (documenten).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm.
[880] Philenews, "Cyprus is a pioneer in software exports" (documenten).
[881] Philenews, "Cyprus is a pioneer in software exports" (documenten).

surveillanceapparatuur uit te voeren, maar ook als uitvalsbasis voor de verkoop en verzending van surveillanceapparatuur binnen Europa. Israëlische spywarebedrijven profiteren dus van de interne markt van de EU doordat deze het vervoer van hun apparatuur naar hun eigen dochterondernemingen, alsook naar nieuwe, in de EU-lidstaten geregistreerde bedrijven mogelijk maakt.

QUADREAM

494. QuaDream is een Israëlisch bedrijf dat werd opgericht door Ilan Dabelstein, een voormalige hoge ambtenaar van de Israëlische militaire inlichtingendienst, en de voormalige NSO-medewerkers Guy Geva en Nimrod Rinsky. Het bedrijf is vooral bekend om zijn spywareproduct Reign, dat naar verluidt gebruik maakt van zero-click exploits en een zelfvernietigingsfunctie bevat die alle sporen van de infectie uitwist. Dit type spyware heeft verschillende functionaliteiten, zoals het opnemen van audio, het volgen van locaties, het zoeken naar bestanden en het maken van foto's via beide camera's.[882]

495. Volgens Citizen Lab en een analyse van Microsoft Threat Intelligence opereren QuaDream-systemen vanuit Bulgarije, Tsjechië, Hongarije, Roemenië, Ghana, Israël, Mexico, Singapore, de Verenigde Arabische Emiraten en Oezbekistan. Daarnaast zijn er ten minste vijf maatschappelijke doelwitten vastgesteld in Noord-Amerika, Centraal-Azië, Zuidoost-Azië, Europa en het Midden-Oosten.[883]

496. In 2017 werd op Cyprus een bedrijf geregistreerd onder de naam InReach. Dit bedrijf is uitsluitend opgericht voor de promotie buiten Israël van producten van QuaDream, zoals Reign. Naar verluidt gebruikte QuaDream InReach om haar producten aan klanten te verkopen en zo de Israëlische uitvoercontroles te omzeilen. Veel van de belangrijkste werknemers van beide ondernemingen hebben gewerkt voor de NSO-groep, Verint en UTX Technologies[884].

497. Na de rapportage van Citizen Lab en de analyse van Microsoft Threat Intelligence werd op 16 april 2023 bekendgemaakt dat QuaDream zijn activiteiten in Israël had stopgezet. Volgens Haaretz had het bedrijf de voorafgaande maanden te kampen gehad met dalende verkoopcijfers en vertrek van werknemers[885].

---

[882] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066

[883] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

[884] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066

[885] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000

CANDIRU

498. Candiru is nog een in Israël geregistreerd bedrijf dat spywareproducten produceert. Candiru werd opgericht in 2014 door Ya'acov Weitzman en Eran Shorer. Beide oprichters hebben deel uitgemaakt van de Militaire Inlichtingeneenheid 8200 van de Israëlische strijdkrachten en beiden hebben voor de NSO-groep gewerkt[886]. Isaac Zack, voormalig investeerder in de NSO-groep, werd de voornaamste aandeelhouder van Candiru. Het bedrijf verkoopt spyware voor het hacken van computers en servers[887]. Uit openbaar gemaakte informatie over een projectvoorstel blijkt dat Candiru haar apparatuur verkoopt op basis van het aantal gelijktijdige infecties, d.w.z. het aantal apparaten dat tegelijkertijd met de spyware kan worden gehackt. Voor 16 miljoen USD krijgt een klant bijvoorbeeld een onbeperkt aantal spyware-pogingen, maar kan hij slechts tien apparaten tegelijk hacken. Voor 1,5 miljoen USD meer kan een klant daar nog eens de capaciteit om 15 extra apparaten te hacken bij kopen[888].

499. Volgens een onderzoek van TheMarker biedt Candiru nu ook spyware aan om in te breken in mobiele apparaten[889]. Het bedrijf verkoopt zijn spyware alleen aan overheden en heeft klanten in Europa, de voormalige Sovjet-Unie, de Perzische Golf, Azië en Latijns-Amerika[890]. In het hoofdstuk over Spanje wordt vermeldt dat 65 mensen het doelwit waren van spyware: vier van hen werden gehackt met Candiru en ten minste twee van hen met zowel Candiru als Pegasus[891].

500. Net als bij de andere aanbieders van spyware is bedrijfsmatige versluiering typerend voor dit bedrijf, dat in de afgelopen paar jaar diverse naamswijzigingen heeft ondergaan. In 2017 veranderde het bedrijf zijn naam in DF Associates Ltd, in 2018 in Grindavik Solutions Ltd, in 2019 in Taveta Ltd en meest recentelijk, in 2020, in Saito Tech Ltd[892]. Voor de duidelijkheid wordt het bedrijf in dit verslag aangeduid als Candiru.

501. Net als de NSO-groep werd Candiru in november 2021 door het Amerikaanse Ministerie van Handel op de zwarte lijst gezet. Er is wel gesuggereerd dat Candiru op de zwarte lijst werd gezet omdat de CEO van de NSO-groep, Shalev Hulio, een geheime partner van Candiru zou zijn en het bedrijf bij belangrijke tussenpersonen in de inlichtingenwereld zou hebben geïntroduceerd. Naar verluidt zou Hulio zelfs hebben beweerd dat het product van Candiru in feite een herverpakte versie van Pegasus zou zijn[893]. Op 1 juli 2022 ontdekten beveiligingsonderzoekers een nieuwe onbeschermde zwakke plek in Chrome die door Candiru werd gebruikt om personen in Libanon,

---

[886] Haaretz, "'We're on the U.S. Blacklist Because of You':The Dirty Clash Between Israeli Cyberarms Makers".
[887] Haaretz, "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed".
[888] Citizen Lab, "Hooking Candiru:Another Mercenary Spyware Vendor Comes into Focus".
[889] Haaretz, "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed".
[890] Citizen Lab, "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus".
[891] Citizen Lab, "CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru".
[892] Citizen Lab, "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus".
[893] Haaretz, ""We're on the U.S. Blacklist Because of You": The Dirty Clash Between Israeli Cyberarms Makers".

Palestina, Jemen en Turkije te hacken[894]. De zwakke plek werd doorgegeven aan Google en is sindsdien ook verholpen door Microsoft en Apple[895].

TYKELAB EN RCS LAB

502. In augustus 2022 meldde Lighthouse Reports dat Tykelab, een in Rome gevestigd bedrijf dat eigendom is van RCS Lab, tientallen telefoonnetwerken had gebruikt, vaak op eilanden in het zuidelijke deel van de Stille Oceaan, om wereldwijd tienduizenden geheime "volgpakketten" te verzenden. Doelwit hiervan waren personen in landen waaronder Italië zelf, Griekenland, Macedonië, Portugal, Libië, Costa Rica, Nicaragua, Pakistan, Maleisië, Irak en Mali. Tykelab maakt gebruik van zwakke plekken in mondiale telefoonnetwerken die derden in staat stellen de locatie van telefoongebruikers te bekijken en hun oproepen eventueel te onderscheppen, zonder dat deze besmetting op hun toestel wordt geregistreerd[896]. In slechts twee dagen in juni 2022 is het bedrijf erin geslaagd netwerken in nagenoeg alle landen ter wereld binnen te dringen[897]. Op zijn website beweert Tykelab dat het bedrijf "twintig jaar ervaring in het ontwerpen, toepassen en onderhouden van telecommunicatie-oplossingen voor het kernnetwerk combineert met grote deskundigheid op het gebied van beheerde diensten, klantgebaseerde systeemintegratie en het ontwikkelen van mobiele apps"[898].

503. In het onderzoek van Lighthouse Reports werd ook gewezen op de rol van de telecomindustrie, waar het huren van toegangspunten tot telefoonnetwerken of "global titles" het mogelijk maakt om door te gaan met dit soort misbruik. Volgens GSM Association, de brancheorganisatie die exploitanten van mobiele netwerken wereldwijd vertegenwoordigt, kunnen telefoonmaatschappijen de bron en het doel van het verkeer op hun netwerken niet altijd vaststellen, wat het moeilijk maakt om een einde te maken aan deze praktijken.[899]

504. Tykelab maakt deel uit van RCS Lab, een Italiaans bedrijf dat bekend staat om zijn afluisteractiviteiten in Italië en daarbuiten. Dit kwam aan het licht door een aankondiging van een derde bedrijf, Cy4Gate, dat RCS Lab heeft overgenomen. RCS Lab heeft vestigingen in Frankrijk, Duitsland en Spanje[900], en ook nog een verborgen dochteronderneming, Azienda Informatica Italiana, die onderscheppingssoftware bouwt voor Android-toestellen en iPhones[901].

HERMIT SPYWARE

505. RCS Lab heeft Hermit ontwikkeld, een spyware die kan worden gebruikt om de microfoon van de beoogde telefoon op afstand te activeren, gesprekken op te nemen en toegang te krijgen tot berichten, gesprekslogboeken, contactlijsten en foto's[902]. In juni 2022 bracht de Threat Analysis Group van Google aan het licht dat door de overheid

---

[894] TechCrunch, "Spyware maker Candiru linked to Chrome zero-day targeting journalists".
[895] The HackerNews, "Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists".
[896] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[897] https://euobserver.com/digital/155849
[898] http://www.tykelab.it/wp/about/
[899] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[900] https://euobserver.com/digital/155849
[901] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[902] https://www.lighthousereports.nl/investigation/revealing-europes-nso/

gesteunde actoren die gebruikmaken van de spyware van RCS Lab, de internetprovider van het doelwit gebruikten om de mobieledataconnectiviteit van het doelwit te deactiveren. Zodra deze was gedeactiveerd, stuurde de aanvaller het doelwit een sms met het verzoek om, via de meegezonden malafide link, een app te installeren om de mobieledataconnectiviteit te herstellen. Volgens Google is dit de reden waarom de meeste apps eruit zagen als apps voor mobiele apparaten. Wanneer het niet mogelijk is gebruik te maken van een internetprovider, worden de apps vermomd als een berichtenapp. De spyware van RCS Lab is ingezet tegen personen in Italië en Kazachstan[903], en is ook aangetroffen in Roemenië[904].

506. Justin Albracht, een dreigingsinformatieonderzoeker van het cyberbeveiligingsbedrijf Lookout, heeft gezegd dat de installatiemethode van Hermit weliswaar minder geavanceerd was dan die van Pegasus, maar dat de gebruiksmogelijkheden vergelijkbaar waren. Om Hermit de mogelijkheid te bieden een toestel binnen te dringen, moet de gebruiker van een telefoon eerst op een besmette link klikken[905].

507. Volgens RCS Lab "wordt elke verkoop of toepassing van producten slechts uitgevoerd na ontvangst van een officiële vergunning van de bevoegde nationale autoriteiten. De geleverde producten worden in de gebouwen van de klant geïnstalleerd en medewerkers van RCS Lab mogen in geen geval operationele activiteiten verrichten om de klant te ondersteunen of toegang krijgen tot de verwerkte gegevens. Vanwege bindende geheimhoudingsovereenkomsten kan RCS Lab geen details over zijn klanten bekendmaken. De Cy4gate Group, waarvan RCS Lab deel uitmaakt, onderschrijft het Global Compact van de VN en veroordeelt derhalve alle vormen van mensenrechtenschendingen. De producten van RCS Lab hebben een duidelijk, specifiek en exclusief doel: rechtshandhavingsinstanties te ondersteunen bij het voorkomen en bestrijden van gruwelijke misdrijven"[906]. Het is echter niet mogelijk om na te gaan of de Cy4gate Group, met inbegrip van RCS Lab, zich houdt aan de door haar zelf aangegeven normen.

508. Volgens een onderzoek van Lighthouse Reports dat in augustus 2022 werd gepubliceerd, werd Tykelabs surveillancesoftware Hermit gebruikt om personen in de hele wereld te observeren, waaronder in Libië, Nicaragua, Maleisië, Costa Rica, Irak, Mali, Griekenland en Portugal, en ook in Italië zelf[907].

DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC" (DSIRF – INFORMATIE- EN FORENSISCH ONDERZOEK TER ONDERSTEUNING VAN BESLUITVORMING)

509. Een onderneming waartegen het Oostenrijkse Ministerie van Justitie onlangs een

[903] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[904] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[905] https://euobserver.com/digital/155849
[906] https://euobserver.com/digital/155849
[907] Lighthouse Reports, "Revealing Europe's NSO", https://www.lighthousereports.nl/investigation/revealing-europes-nso/

strafrechtelijke procedure heeft ingeleid, is DSIRF GmbH (LLC)[908]. DSIRF, opgericht in 2016, is een Oostenrijkse onderneming die gevestigd is in Wenen, met een moedermaatschappij in Liechtenstein. Zij beweert "op maat gesneden diensten op het gebied van informatieonderzoek, forensisch onderzoek en datagestuurde inlichtingen" te leveren "aan multinationale ondernemingen in de technologie-, detailhandel-, energie- en financiële sector"[909]. DSIRF verkoopt duidelijk aan niet-overheidsactoren.

510. DSIRF heeft een spyware ontwikkeld genaamd Subzero/KNOTWEED, die gebruik maakt van onbeschermde zwakke plekken in Windows en Adobe Reader en die – volgens hun eigen reclame – heimelijk op de beoogde apparaten kan worden geïnstalleerd. Eenmaal geïnstalleerd neemt Subzero "de volledige controle over de beoogde computer over" en biedt het "volledige toegang tot alle gegevens en wachtwoorden". Klanten van Subzero kunnen wachtwoorden kopiëren, screenshots maken, huidige en eerdere locaties zien en "bestanden op de doelcomputer inzien, downloaden, wijzigen en uploaden" via een webinterface. DSIRF prijst Subzero aan als geschikt voor "de volgende generatie cyberoorlogvoering", en stelt dat de software "is toegesneden op het cybertijdperk"[910]. In 2020 schatte DSIRF de waarde van Subzero op 245 miljoen EUR.

511. De link met Rusland werd duidelijk door de relaties van diverse leidinggevenden bij SDRIF. De eigenaar van DSIRF is Peter Dietenberger, een "man met uitstekende connecties in het Kremlin" en iemand "die deuren opent voor Westerse bedrijven in het rijk van Poetin"[911]. Dietenberger woonde een aantal jaren in Rusland en had een Russisch bedrijf en diverse Russische zakenpartners. Een van zijn Russische zakenpartners, Boris Vasilyev, zat ook in de raad van bestuur van DSIRF. DSIRF geeft diverse referenties voor het bedrijf en zijn producten: Michael Harms (CEO van de Duitse ondernemersvereniging voor Oost-Europa), Stephan Fanderl (voorzitter van de raad van bestuur van Galeria Karstadt Kaufhof, die Walmart in Rusland wilde introduceren), Christian Kremer (voormalig voorzitter van BMW in Rusland en CEO van Russian Machines, dat sinds 2018 onderworpen is aan sancties in de VS) en Florian Schneider (partner bij het grote zakelijke advocatenkantoor Dentons in Moskou)[912]. Russian Machines, een bedrijf dat eigendom is van de oligarch Oleg Deripaska, maakt naar verluidt gebruik van de diensten van DSIRF. De machtige lokale ondernemer Siegfried "Sigi" Wolf, die voormalig bondskanselier Sebastian Kurz adviseerde over economische kwesties, wordt beschouwd als een vertrouweling van Deripaska[913]. Ook Jan Marsalek, een vermeende crimineel die door Interpol wordt gezocht wegens vermoedelijke handelsfraude ter waarde van miljoenen dollars, naast andere financiële en economische delicten, is hierbij betrokken. In augustus 2018 kreeg hij een e-mail van Florian Stermann (secretaris-generaal van de Russisch-Oostenrijkse Vriendschapsvereniging, die door het openbaar ministerie wordt beschouwd als een

---

[908] DSIRF is een afkorting voor "Decision Supporting Information Research and Forensic" (informatie- en forensisch onderzoek ter ondersteuning van besluitvorming).
[909] https://dsirf.eu/about/
[910] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[911] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
[912] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/
[913] https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf

"vertrouweling" van de FPÖ)[914] met een bedrijfspresentatie van DSIRF. In 2013 zou Marsalek geprobeerd hebben spyware van het Italiaanse bedrijf Hacking Team te verkopen aan Grenada. Naar verluidt houdt hij zich op dit moment schuil in Moskou, beschermd door de FSB, de Russische geheime dienst[915].

512. In juli 2022 ontdekte Microsoft dat Subzero was gebruikt tijdens niet-geautoriseerde, kwaadwillige activiteiten om advocatenkantoren, banken en strategische adviesbureaus in Oostenrijk, het Verenigd Koninkrijk en Panama aan te vallen[916]. Oostenrijk beschikt momenteel niet over een wettelijke grondslag voor de niet-geautoriseerde toepassing van spyware zoals Subzero door overheidsinstanties, en als een particulier bedrijf het tegen een ander bedrijf gebruikt zou dat ook illegaal zijn. Na de publicatie van Microsoft op 28 juli 2022 diende Epicenter.works, de Oostenrijkse ngo voor digitale rechten, bij het openbaar ministerie in Wenen een strafklacht in tegen DSIRF wegens onrechtmatige toegang tot een computersysteem, gegevensbeschadiging, verstoring van de werking van computersystemen, frauduleus gebruik van gegevensverwerking, deelneming aan een criminele organisatie en schending van de Wet op de buitenlandse handel en betalingen met betrekking tot goederen voor tweeërlei gebruik[917]. Op 7 oktober 2022 verklaarde het Oostenrijks federaal Ministerie van Sociale en Economische Zaken dat het geen uitvoervergunning had afgegeven aan DSIRF[918], en volgens het Oostenrijks federaal Ministerie van Justitie had het openbaar ministerie in Wenen een strafrechtelijk onderzoek ingesteld naar DSIRF[919]. Het gebruik van Subzero-spyware tegen doelwitten in Oostenrijk betekent dat een particuliere of publieke entiteit in Oostenrijk de software op illegale wijze heeft toegepast, dat de software werd gebruikt door een buitenlandse actor en er uitvoerbeperkingen door DSIRF werden geschonden, of dat de software illegaal werd uitgevoerd naar een andere lidstaat en van daaruit op wettige of onwettige wijze werd gebruikt tegen een Oostenrijks doelwit. Dit onderzoek loopt nog.

FINFISHER

513. Ook het strafrechtelijk onderzoek naar en het faillissement van FinFisher, een voormalig spywarebedrijf uit München, Duitsland, is het waard om in dit te worden vermeld. FinFisher is een in 2008 opgericht bedrijfsnetwerk dat oorspronkelijk sterke banden had met het Britse netwerk van bedrijven die onder het merk Gamma opereren. FinFisher prees zijn spyware aan als "een compleet gamma voor IT-hacking". Tientallen landen over de hele wereld gebruikten de software[920], waaronder elf EU-

[914] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
[915] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/; https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213
[916] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
[917] https://en.epicenter.works/document/4236
[918] Antwoord van Martin Kocher, federaal minister van Digitale en Economische Zaken van Oostenrijk, op schriftelijke parlementaire vragen van Stephanie Krisper, 7 oktober 2022, kenmerk 2022-0.575.143, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml
[919] Antwoord van Alma Zadić, federaal minister van Justitie, op schriftelijke parlementaire vragen van Stephanie Krisper, 7 oktober 2022, kenmerk 2022-0.575.216, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml
[920] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; https://wikileaks.org/spyfiles4/customers.html

lidstaten[921] en 13 “niet-vrije” landen[922].

514. In 2017 werd FinFishers product FinSpy in Turkije ontdekt op een valse versie van een mobilisatiewebsite voor de Turkse oppositie. De software was vermomd als een downloadbare app die werd aanbevolen aan deelnemers aan demonstraties tegen de regering[923]. FinFisher had in zijn reclame zelf altijd gesteld dat zijn producten alleen voor de bestrijding van criminaliteit werden gebruikt. In 2019 werd er een strafklacht tegen FinFisher ingediend door de Gesellschaft für Freiheitsrechte (GFF), Reporter ohne Grenzen, het blog netzpolitik.org en het European Center for Constitutional and Human Rights (ECCHR) wegens het uitvoeren van spyware zonder de noodzakelijke uitvoervergunning van het Duitse Federale Bureau voor Economische Zaken en Uitvoercontrole. Hiermee had het bedrijf de EU-verordening inzake producten voor tweeërlei gebruik en de overeenkomstige Duitse nationale wetgeving geschonden. Naar aanleiding van de klacht deed het parket van München onderzoek naar FinFisher, en in oktober 2020 doorzocht het 15 bedrijfsgebouwen van de FinFisher-groep in Duitsland en Roemenië, en ook particuliere woningen. In 2021 gaf de arrondissementsrechtbank van München toestemming voor de inbeslagname van de bankrekeningen van FinFisher, teneinde ervoor te zorgen dat onrechtmatig verkregen winsten in beslag zouden worden genomen als FinFisher zou worden veroordeeld. In februari 2022 werd FinFisher echter failliet verklaard. De bedrijfsactiviteiten zijn gestaakt, het kantoor is gesloten en alle 22 werknemers zijn ontslagen[924]. Het strafrechtelijk onderzoek naar de personen die verantwoordelijk waren voor de activiteiten van FinFisher loopt nog.

III. Reactievermogen van de Europese Unie

515. Sommige regeringen hebben EU-burgers gehackt met krachtige en zeer invasieve en opdringerige spyware, waarbij ze misbruik maken van hun recht om toezicht te houden als de nationale veiligheid in gevaar is. Dit brengt de democratie, de rechtsstaat en de grondrechten van individuele burgers in gevaar. De EU heeft weinig bevoegdheden om op te treden tegen deze bedreigingen en blijkt slecht toegerust tegen mogelijke criminele activiteiten van nationale autoriteiten, zelfs als deze de EU zelf treffen. Krachtens de Verdragen blijft de nationale veiligheid de exclusieve bevoegdheid van de lidstaten, maar hun optreden moet wel in overeenstemming zijn met de grondrechten en de democratische normen die in het EU-recht zijn verankerd. Ook politieke factoren beperken de slagkracht van de EU. De Europese Commissie, als hoedster van de EU-verdragen, heeft haar inspanningen om het EU-recht te handhaven door gebruik te maken van de rechtsinstrumenten die zij tot haar beschikking heeft, niet zo groot mogelijk gemaakt. De Commissie heeft de neiging haar bevoegdheden zeer eng te interpreteren, aangezien het vrijwel uitsluitend gaat om de correcte omzetting van EU-wetgeving in nationale wetgeving. De Commissie is van mening dat het aanpakken van inbreuken op de EU-wetgeving uitsluitend de verantwoordelijkheid is van de nationale

[921]België, Tsjechië, Estland, Duitsland, Hongarije, Italië, Nederland, Roemenië, Slovenië, Slowakije en Spanje.
[922]Angola, Bahrein, Bangladesh, Egypte, Ethiopië, Gabon, Jordanië, Kazachstan, Myanmar, Oman, Qatar, Saudi-Arabië en Turkije.
[923] https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/
[924] https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/; https://edri.org/our-work/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact-the-finfisher-group-of-companies-ceases-business-operations-after-its-accounts-are-seized-by-public-prosecutor/; https://netzpolitik.org/wp-upload/2022/03/2022-02-08_AG-Muenchen_Insolvenzbekanntmachung_FinFisher-Labs-GmbH.txt

autoriteiten. Bij flagrante schendingen van de rechtsstaat en de grondrechten wordt deze houding – waarvoor geen grondslag is in de EU-Verdragen – evenwel hoogst problematisch. Hoewel subsidiariteit en verdeling van bevoegdheden een pijler van het EU-recht zijn, mogen deze niet leiden tot straffeloosheid voor regeringen die voor politieke doeleinden spyware richten op EU-burgers. Hieronder gaan we in op de bevoegdheden waarover de EU-instellingen beschikken. Het Parlement, de Commissie en de Raad zijn bevoegd en verplicht om wetgeving en regelgeving vast te stellen en deze te handhaven, en zij moeten dit met overtuiging en ambitie doen en hierbij voorrang geven aan de verdediging van onze democratie boven politieke kortetermijnoverwegingen.

Europese Commissie

516. Naar aanleiding van persberichten over het gebruik van spyware in de lidstaten en vragen van PEGA heeft de Commissie in haar reactie op het spywareschandaal aanvankelijk alleen brieven geschreven waarin zij de regeringen van Polen, Hongarije, Spanje, Griekenland, Cyprus en Frankrijk om opheldering vroeg. Het lijkt er evenwel op dat er na deze schuchtere vermaning geen verdere stappen zijn gezet. Strikt genomen klopt het dat de Commissie niet kan optreden op het gebied van de nationale veiligheid van de lidstaten. Nochtans mag het concept van nationale veiligheid niet worden uitgelegd als een reden tot onbegrensde vrijstelling van de Europese wetten en verdragen, noch mag de nationale veiligheid uitgroeien tot een zone van wetteloosheid. Zo formuleert de Commissie het zelf in de hierboven genoemde brieven. Het is evenwel aan de lidstaten om "aan te tonen dat de nationale veiligheid in het concrete geval zou worden bedreigd". In antwoord op de vraag welke maatregelen de Commissie zal nemen als de nationale autoriteiten beschuldigingen van illegale spionage niet grondig onderzoeken, verwijst de Commissie enkel naar het Europees Hof van Justitie en artikel 47 van het Handvest, dat voorziet in het recht op een doeltreffende voorziening in rechte voor een rechtbank. Er lijkt geen sprake te zijn van een politieke wil om op te treden.

517. Daarnaast heeft de Commissie op 21 december 2022 een algemene brief aan alle lidstaten gestuurd met een verzoek om informatie over het gebruik van spyware door de nationale autoriteiten en het rechtskader voor dat gebruik, teneinde "de situatie in de lidstaten in kaart te brengen" en "de wisselwerking met het EU-recht" te onderzoeken[925]. De Commissie heeft specifieke vragen gesteld over onder meer het doel van het gebruik van spyware, de autoriteiten die bevoegd zijn om spyware in te zetten, de nationale definitie van nationale veiligheid, relevante wetgeving die de verwerking van gegevens voor nationale veiligheidsdoeleinden regelt, waarborgen, voorafgaande toestemming van een rechtbank of een onafhankelijke bestuurlijke instantie, toezicht en kennisgeving, met 31 januari 2023 als uiterste datum om te antwoorden. Op 28 maart 2023 verklaarde Commissaris Reynders aan PEGA dat een grote meerderheid van de lidstaten had geantwoord, maar dat de Commissie nog bezig was met het verzamelen van de antwoorden van de lidstaten op deze inventarisatie en dat zij de antwoorden "zorgvuldig zou beoordelen". Op basis van deze inventarisatie zal de Commissie nadenken over haar opties met betrekking tot het gebruik van spyware in de lidstaten. "Gezien de zich ontwikkelende en gevoelige aard van de beoordeling" is er echter geen

[925] Brief van DG JUST aan de lidstaten, Ref. Ares(2022)8885417, van 21 december 2022.

specifieke einddatum voorzien voor de beoordeling door de Commissie. De Commissie verklaarde ook dat zij de bevindingen van PEGA op de voet zal volgen.

518. In tegenstelling tot de VS, die op de onthullingen hebben gereageerd door bedrijven op een zwarte lijst te plaatsen, onderzoeken uit te voeren, ook op het grondgebied van de EU, en een uitvoerend bevel uit te vaardigen dat de aankoop van commerciële spyware door federale instanties in de VS verbiedt, heeft de Commissie nog geen analyse uitgevoerd van de situatie of van de bedrijven die actief zijn op de markt voor spyware binnen de EU. Er bestaat nochtans geen duidelijk juridisch bezwaar tegen een dergelijke analyse. Het is opmerkelijk dat de grote hoeveelheid bewijzen de Commissie er nog niet toe hebben bewogen enige zinvolle actie te ondernemen. Deze passiviteit komt neer op medeplichtigheid aan mensenrechtenschendingen en plichtsverzuim.

519. De EU beschikt daarentegen over verscheidene wetten die kunnen dienstdoen als regelgevingsinstrumenten met betrekking tot spyware. Er bestaan niet alleen Europese wetten ter bescherming van de burgerrechten, zoals de wetgeving inzake gegevensbescherming (AVG) en de privacy van communicatie (e-privacy)[926], maar ook wetten inzake uitvoer (verordening tweeërlei gebruik) en overheidsopdrachten. De handhaving door de Commissie als hoedster van de Verdragen wordt echter niet optimaal uitgevoerd. Zij gaat doorgaans alleen na of de lidstaten EU-recht correct hebben omgezet in nationaal recht. hetgeen eigenlijk niets zegt over de werkelijke situatie ter plaatse. Zo lijkt de Commissie in haar verslag over de tenuitvoerlegging van de verordening tweeërlei gebruik[927] te concluderen dat alles probleemloos verloopt, hoewel er talrijke aanwijzingen zijn dat deze tenuitvoerlegging in de praktijk ontoereikend is en lacunes vertoont – in sommige landen gebeurt dit trouwens met opzet. De tenuitvoerlegging van de e-privacyrichtlijn en de daaruit voortvloeiende jurisprudentie laat te wensen over. De Commissie stelt dat de lidstaten verantwoordelijk zijn voor de tenuitvoerlegging en handhaving, maar neemt geen actie wanneer de lidstaten dit verzuimen. Zonder juiste en zinvolle handhaving is de EU-wetgeving niet doeltreffend en laat zij meer dan genoeg ruimte voor onrechtmatig gebruik van spyware.

520. De richtlijn gegevensbescherming bij rechtshandhaving was bedoeld om strikte normen van gegevensbescherming te bieden en het vrije verkeer van data tussen rechtshandhavings- en strafrechtelijke instanties te waarborgen. De richtlijn moest in het nationaal recht worden omgezet, waarbij aan de lidstaten ruime discretionaire bevoegdheden werden gegeven. Op dit moment is het duidelijk dat de tenuitvoerlegging per lidstaat verschilt, met name wat betreft de rechten van betrokkenen op het gebied van gegevens. De Commissie moet de tenuitvoerlegging in alle lidstaten dringend evalueren en de ernstigste tekortkomingen in kaart brengen. De Commissie moet concrete richtsnoeren voor de lidstaten opstellen voor de tenuitvoerlegging van de richtlijn teneinde ervoor te zorgen dat de EU-normen in heel de Unie worden geëerbiedigd. Daarnaast moet de Commissie in voorkomend geval inbreukprocedures inleiden wanneer de richtlijn niet correct is omgezet en de lidstaten zich niet bereid

[926] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (PB L 201 van 31.7.2002, blz. 37).
[927] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

tonen dit te corrigeren.

Europees Parlement

521. Het Europees Parlement heeft de PEGA-enquêtecommissie opgericht, die binnen de grenzen van haar bevoegdheden en mandaat grondig en doeltreffend te werk gaat. Zij kan echter geen getuigen oproepen of onder ede horen, en heeft evenmin toegang tot gerubriceerde informatie. PEGA beschikt niet over de uitgebreide onderzoeksbevoegdheden van de meeste nationale parlementen. Bovendien wordt het overleg binnen PEGA geregeld beïnvloed door de regeringen van de lidstaten, wat soms een belemmering vormt voor grondige, volledig onafhankelijke en objectieve onderzoeken. Het is nogal verontrustend dat het Europees Parlement niet over onbegrensde onderzoeksbevoegdheden beschikt terwijl sommige van zijn eigen leden het doelwit zijn geweest van spyware.

Europese Raad en Raad van Ministers

522. Hoewel het spywareschandaal volgens de regeringen van de lidstaten een zuiver nationale aangelegenheid is, is de zaak in de Raad van de Europese Unie besproken en hebben de nationale regeringen besloten gezamenlijk op de vragenlijst van het Europees Parlement te antwoorden[928]. Daarmee hebben zij onmiskenbaar toegegeven dat het wel degelijk gaat om een kwestie voor de Raad.

523. Tot dusver heeft de Europese Raad niet publiekelijk of inhoudelijk op het schandaal gereageerd. Sommige van zijn leden hebben een belang in de kwestie: misschien omdat ze zelf medeplichtig zijn aan de onwettige hacks, of eenvoudigweg omdat ze willen dat de EU op dit gebied zwak en machteloos blijft.

524. Zelfs als uiteindelijk zou worden bewezen dat er sprake was van illegale of criminele handelingen, kunnen leden van nationale regeringen niet in staat van beschuldiging worden gesteld of uit hun functie bij de EU worden ontzet. Het is met andere woorden goed mogelijk dat personen die zich schuldig hebben gemaakt aan dergelijke handelingen, ongestraft blijven deel uitmaken van EU-organen en besluiten blijven nemen die gevolgen hebben voor alle Europese burgers.

Europol

525. Europol beschikt niet over autonome operationele bevoegdheden en kan niet handelen zonder toestemming en medewerking van de betrokken lidstaat of lidstaten overeenkomstig artikel 88, lid 3, VWEU, terwijl de toepassing van dwangmaatregelen onder de exclusieve verantwoordelijkheid van de bevoegde nationale autoriteiten valt. Dit vormt een probleem als er duidelijk sprake is van strafbare feiten – zoals cybercriminaliteit, corruptie en afpersing – maar de nationale autoriteiten deze niet onderzoeken. Europol heeft onlangs nieuwe bevoegdheden gekregen die het in staat stellen proactief een onderzoek voor te stellen, zelfs als het gaat om een misdrijf dat slechts in één lidstaat is gepleegd[929], maar tot nog toe heeft het geen gebruik gemaakt

[928] Ontwerpbrief van het secretariaat-generaal van de Raad aan de delegaties, 26 september 2022.
[929] Verordening (EU) 2022/991 van het Europees Parlement en de Raad van 8 juni 2022 tot wijziging van Verordening (EU) 2016/794, wat betreft de samenwerking van Europol met particuliere partijen, de verwerking

van die bevoegdheden.

526. Op 28 september 2022 heeft PEGA Europol schriftelijk verzocht [930]gebruik te maken van zijn nieuwe bevoegdheden uit hoofde van artikel 6 van de Europol-verordening[931]. Op 13 oktober 2022 verklaarde Europol in een antwoordbrief[932] dat het "contact [had] opgenomen met vijf lidstaten om na te gaan of er op nationaal niveau relevante informatie beschikbaar is voor Europol en of er een strafrechtelijk onderzoek loopt of wordt overwogen (of eventueel een ander onderzoek op grond van het toepasselijke nationale recht)". Op 11 april 2023 verklaarde Europol in een brief aan PEGA dat de brieven waren verzonden aan Griekenland, Hongarije, Bulgarije, Spanje en Polen. Na het antwoord van de vijf lidstaten op de brieven van Europol, meldde Europol dat geen van hen beschikte over "relevante informatie die voor Europol beschikbaar is". In oktober 2022 had een van de vijf lidstaten aan Europol bevestigd dat er "onder toezicht van de bevoegde justitiële autoriteiten een strafrechtelijk onderzoek is ingesteld, en dit ook is geverifieerd door Eurojust." In december 2022 had een tweede lidstaat Europol meegedeeld "dat er een strafrechtelijke procedure was ingeleid in verband met het vermoedelijke onrechtmatige gebruik van Pegasus-software, die inmiddels door de verantwoordelijke justitiële autoriteiten in dat land was afgesloten". Een derde lidstaat stelde Europol ervan in kennis dat "in één geval op regionaal niveau een gerechtelijk vooronderzoek is ingesteld", en vroeg of "Europol beschikt over informatie over het gebruik van Pegasus-software in het betrokken land die relevant is voor het gerechtelijk vooronderzoek". Een vierde lidstaat deelde Europol mee "dat er geen strafrechtelijk onderzoek loopt of wordt overwogen", maar dat er "gerechtelijke onderzoeken zijn ingeleid". In april 2023 had de vijfde lidstaat aan Europol uitgelegd dat "er na raadpleging van de bevoegde autoriteiten in dat land, onder verwijzing naar het vooronderzoek van het openbaar ministerie, voor Europol geen relevante informatie beschikbaar is over het onrechtmatige gebruik van opdringerige surveillance- en onderscheppingssoftware". Het is niet bekend of de bovengenoemde strafrechtelijke procedures door twee lidstaten, gerechtelijke vooronderzoeken door één lidstaat en prejudiciële procedures van het openbaar ministerie in een andere lidstaat betrekking hebben op het misbruik van spyware door de regeringen van EU-lidstaten of door derde landen.

527. De EU blijkt eerder machteloos te staan tegen mogelijke criminele activiteiten van nationale autoriteiten, zelfs als deze handelingen gevolgen hebben voor de EU.

528. Paradoxaal genoeg voeren de VS, in tegenstelling tot Europol, actief onderzoek naar het gebruik van spyware in de EU. Op 5 november 2022 werd gemeld dat de FBI een bezoek aan Athene had gebracht om "na te gaan welke omvang de illegale surveillance heeft aangenomen en wie hierbij betrokken is"[933]. Bovendien heeft president Biden van

---

van persoonsgegevens door Europol ter ondersteuning van strafrechtelijke onderzoeken, en de rol van Europol bij onderzoek en innovatie (PB L 169 van 27.6.2022, blz. 1).

[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984

[931] "De uitvoerend directeur kan, indien hij oordeelt dat een strafrechtelijk onderzoek moet worden ingesteld naar een specifiek strafbaar feit dat slechts betrekking heeft op één lidstaat maar een schending inhoudt van een gemeenschappelijk belang dat voorwerp is van Uniebeleid, aan de bevoegde autoriteiten van de betrokken lidstaat via zijn nationale eenheid voorstellen om een dergelijk strafrechtelijk onderzoek in te stellen, te voeren of te coördineren.".

[932] Dossier nr. 1260379.

[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ

de VS in maart 2023 een uitvoeringsbesluit uitgevaardigd dat het gebruik van spyware door federale instanties in de VS grotendeels verbiedt. Enkele dagen later gaven andere landen, waaronder Frankrijk en Denemarken, te kennen dat zij zich inzetten voor internationale samenwerking op dit gebied.

Europese rechterlijke macht

529. Het HvJ-EU en het EHRM spelen een belangrijke rol bij de verdediging van de democratie, de rechtsstaat en de grondrechten. Zij kunnen echter alleen optreden naar aanleiding van een klacht of een precontentieuze vraag. De procedures hiervoor duren heel lang en leveren in individuele gevallen weinig concrete oplossingen op. In de loop der jaren hebben de rechtbanken een uitgebreide relevante jurisprudentie gecreëerd, onder meer door normen voor surveillance vast te leggen. Zij beschikken evenwel niet over de nodige middelen om te garanderen dat hun uitspraken daadwerkelijk worden uitgevoerd. Tot nog toe heeft het EHRM één klacht ontvangen over het onrechtmatige gebruik van spyware[934]. De weg naar de rechtbanken van de EU in Straatsburg of Luxemburg is vaak lang, duur en complex, en kan pas worden ingeslagen als alle mogelijkheden voor nationale gerechtelijke procedures zijn uitgeput. Dit is met name het geval als nationale aanklagers of rechters verzuimen of weigeren een zaak in behandeling te nemen. De lat voor de ontvankelijkheidstest ligt hoog.

De Ombudsman

530. Op 28 november 2022 concludeerde de Europese Ombudsman dat de Commissie de risico's voor de mensenrechten onvoldoende had beoordeeld voordat er steun werd verstrekt aan Afrikaanse landen om surveillancecapaciteit te ontwikkelen, met name in het kader van het EU-noodtrustfonds voor Afrika (EU-TFA). De conclusies kwamen tot stand naar aanleiding van een klacht van diverse maatschappelijke organisaties. In Niger kende het Fonds, ondanks de repressie tegen activisten in het land, 11,5 miljoen EUR toe voor de levering van surveillanceapparatuur, waaronder surveillancesoftware, een afluistercentrum en apparatuur die in staat is de identiteit van een internationale mobiele abonnee te achterhalen[935]. Om de door haar vastgestelde tekortkomingen aan te pakken, stelde de Ombudsman verbeteringen voor om ervoor te zorgen dat er voorafgaand aan toekomstige EU-TFA-projecten een effectbeoordeling op het gebied van de mensenrechten zou plaatsvinden.

Andere EU-organen

531. Het Europees Comité voor gegevensbescherming, de Europese Toezichthouder voor gegevensbescherming, de Europese Rekenkamer en Eurojust hebben weinig bevoegdheden om gevallen van onwettig gebruik van of handel in spyware door de regeringen van de lidstaten te onderzoeken of daarin in te grijpen. Sommige van hun leden kunnen zelfs betrokken zijn bij schandalen in hun lidstaat van herkomst. Dit kan

[934] Beroep van Koukakis bij het Europees Hof voor de Rechten van de Mens, 27 juli 2022.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf

ook gevolgen hebben voor de werking en de integriteit van deze EU-organen. Het Europees Openbaar Ministerie zou kunnen ingrijpen wanneer er EU-middelen in het spel zijn.

TOELICHTING

Europa's Watergate

Tijdens de zomer van 2021 maakte het Pegasusproject, een collectief van onderzoeksjournalisten, ngo's en onderzoekers, een lijst bekend van 50 000 personen die het doelwit waren geworden van huurlingspyware. Onder hen waren journalisten, advocaten, openbare aanklagers, activisten, politici en zelfs staatshoofden. Het meest dramatische geval is ongetwijfeld dat van Jamal Khashoggi, de Saudi-Arabische journalist die in 2018 op brutale wijze werd vermoord wegens zijn kritiek op het Saudische regime. Op de lijst stonden echter ook heel wat personen uit Europa. Sommigen waren het doelwit van actoren buiten de EU, maar anderen werden bespioneerd door hun eigen nationale regeringen. De onthullingen ontketenden over de hele wereld een storm van verontwaardiging.

Al snel kreeg het schandaal de bijnaam "Europa's Watergate". Maar waar het in de politieke thriller "All the President's Men" gaat om de inbraak in het Watergategebouw in 1972, doet het huidige spywareschandaal eerder denken aan de ijzingwekkende film "Das Leben der Anderen", waarin het bewaken van de burgerbevolking door het totalitaire communistische regime wordt uitgebeeld. Een hedendaagse digitale inbraak met spyware is veel geavanceerder en indringender en laat nauwelijks sporen na. Het gebruik van spyware houdt veel meer in dan de klassieke observatie van een persoon: het verleent spionnen onbeperkte toegang tot en controle over die persoon. In tegenstelling tot conventionele afluisterapparatuur maakt spyware niet alleen realtime-surveillance mogelijk maar ook volledige en retroactieve toegang tot oudere bestanden en berichten en tot metagegevens over eerdere communicatie. Dit toezicht kan zelfs op afstand plaatsvinden, in gelijk welk land ter wereld. Spyware kan worden gebruikt om een smartphone feitelijk over te nemen en alles wat erin zit, met inbegrip van documenten, afbeeldingen en berichten, te kopiëren. Het aldus verkregen materiaal kan niet alleen worden gebruikt om handelingen te observeren, maar ook om slachtoffers te chanteren, in diskrediet te brengen, te manipuleren en te intimideren. Er kan worden geknoeid met de toegang tot het systeem van het slachtoffer en er kan valse inhoud worden geplaatst. Microfoon en camera kunnen op afstand worden geactiveerd, zodat het toestel een heuse spion ter plaatse wordt. Dit alles gebeurt zonder dat het slachtoffer iets merkt. Spyware laat weinig sporen achter op het toestel van het slachtoffer, en zelfs als de software wordt ontdekt, is het nagenoeg onmogelijk om te achterhalen wie achter de aanval zit.

Het misbruik van spyware is niet alleen in strijd met het recht op privacy van personen. Het vormt ook een sluikse ondermijning van de democratie en van democratische instellingen. Met spyware wordt oppositie en critici het zwijgen opgelegd, toezicht onmogelijk gemaakt en de vrije pers en het maatschappelijk middenveld op beangstigende wijze beïnvloed. Bovendien kan spyware ook worden ingezet om verkiezingen te manipuleren. De term "commerciële spyware" geeft de aard van het product en van de sector uiterst treffend weer. Zelfs mislukte pogingen om een smartphone met spyware te besmetten, hebben politieke gevolgen en kunnen nefast zijn, zowel op individueel niveau als voor de democratie. Deelname aan het openbare leven wordt onmogelijk als we er niet kunnen van uitgaan vrij te zijn en niet te worden geobserveerd.

Het gaat hier niet om een reeks afzonderlijke gevallen van spywaremisbruik op nationaal vlak maar om een heus Europees schandaal. EU-regeringen gebruiken spyware tegen hun burgers

voor politieke doeleinden en om corruptie en criminele activiteiten te verdoezelen. In sommige lidstaten zijn regeringen zelfs zo ver gegaan om spyware te integreren in een speciaal met autoritaire doeleinden ontworpen systeem. De regeringen van andere lidstaten mogen dan wel niet actief spyware hebben gebruikt, maar hebben de dubieuze handel van spyware vergemakkelijkt. Europa is uitgegroeid tot een aantrekkelijke plek voor huurlingspyware. We hebben als knooppunt gediend voor de uitvoer ervan naar dictaturen en repressieve regimes zoals Libië, Egypte en Bangladesh, waar de spyware is gebruikt tegen mensenrechtenactivisten, journalisten en regeringsoppositieleden.

Het misbruik van spyware komt neer op een ernstige schending van alle waarden die de Europese Unie verdedigt en stelt de weerbaarheid van de democratische rechtsstaat in Europa op de proef. De afgelopen jaren heeft de EU haar capaciteit om te reageren op externe bedreigingen voor onze democratie, zoals oorlog, desinformatiecampagnes en politieke inmenging, in snel tempo vergroot. Haar vermogen om te reageren op interne bedreigingen voor de democratie blijft daarentegen jammerlijk onderontwikkeld. Aangezien overtredingen door nationale regeringen ongestraft blijven, kunnen antidemocratische bewegingen zich ongehinderd als gangreen door de hele EU verspreiden. De EU is slecht toegerust om het hoofd te bieden aan aanvallen op de democratie van binnenuit. De EU is onbetwistbaar een politieke entiteit, met supranationale wetten en supranationale instellingen, en biedt een interne markt, open grenzen, de mogelijkheid om zonder paspoort te reizen, EU-burgerschap en een eengemaakte ruimte van vrijheid, veiligheid en recht. Ondanks plechtige toezeggingen ten aanzien van de Europese waarden worden deze waarden in de praktijk echter nog altijd vooral als een nationale aangelegenheid beschouwd. Het Pegasus-spywareschandaal legt ongenadig de onrijpheid en zwakke plekken van de EU als democratische entiteit bloot. Wat democratische waarden betreft, is de EU gebouwd op de “veronderstelling van naleving” door de nationale regeringen, maar in werkelijkheid is die veronderstelling veranderd in de “schijn van naleving”. Een scenario waarin nationale regeringen de EU-wetgeving opzettelijk negeren en met de voeten treden, is eenvoudigweg niet voorzien in de bestuursstructuur van de EU, en de Unie is niet voorbereid dergelijke gevallen. De EU-instanties hebben slechts weinig bevoegdheden, en nog minder zin, om nationale autoriteiten bij overtredingen op het matje te roepen, al helemaal niet als het om de delicate kwestie van “nationale veiligheid” gaat. Volgens de intergouvernementele logica zijn de EU-instellingen onderworpen aan de nationale regeringen. Zonder doeltreffende en zinvolle supranationale handhavingsmechanismen is nieuwe wetgeving evenwel zinloos. Om het probleem te kunnen oplossen, zijn zowel regelgevende maatregelen als bestuurshervormingen nodig.

Ook in de VS wordt de democratie van binnenuit aangevallen - denken we maar aan Watergate of aan de belegering van het Congres op 6 januari 2021 -, maar zij beschikken wel over middelen om hier kordaat tegen op te treden. De VS kunnen zelfs aan de meest hooggeplaatste politieke leiders het hoofd bieden wanneer die de wet of de grondwet niet naleven.

Zo hebben de VS na de onthullingen van het Pegasusproject in 2021 snel en vastberaden gereageerd. Het Amerikaanse ministerie van Handel heeft de NSO-groep meteen op een zwarte lijst geplaatst, het ministerie van Justitie is een onderzoek begonnen, en er wordt gewerkt aan een strenge regelgeving voor de handel in spyware. De FBI kwam zelfs naar Europa om een spyware-aanval op een persoon met een dubbele Amerikaanse en Europese nationaliteit te onderzoeken. Technologiereuzen zoals Apple en Microsoft hebben juridische

stappen ondernomen tegen spyware-bedrijven. Slachtoffers dienden juridische klachten in, openbare aanklagers zijn bezig met onderzoeken en er zijn parlementaire onderzoeken gestart.

De Europese instellingen, met uitzondering van het Europees Parlement, zijn daarentegen grotendeels stilzwijgend en passief gebleven, en gaven hiervoor als argument dat het om een uitsluitend nationale aangelegenheid gaat.

De houding van de Europese Raad en de nationale regeringen kan zelfs worden bestempeld als een omerta. De Europese Raad heeft geen enkele officiële reactie gegeven op het schandaal. De regeringen van de lidstaten hebben het verzoek van de PEGA-commissie om medewerking bijna allemaal afgeslagen. Sommige regeringen weigerden ronduit, andere waren vriendelijk en beleefd maar verstrekten informatie die niet echt nuttig was. Zelfs op de eenvoudige vragenlijst die PEGA aan alle lidstaten heeft toegezonden, over de details van hun nationale rechtskader voor het gebruik van spyware, zijn nauwelijks betekenisvolle antwoorden gekomen. Letterlijk de dag voor de publicatie van dit ontwerpverslag ontving de PEGA-commissie via de Raad een gezamenlijk antwoord van de lidstaten, evenwel ook zonder enige betekenis.

De Europese Commissie heeft zich bezorgd getoond en de regeringen van een paar lidstaten om opheldering gevraagd, maar alleen in die gevallen waarin reeds een schandaal op nationaal niveau was uitgebroken. Zij heeft - terughoudend en slechts met mondjesmaat - informatie gedeeld over de spyware-aanvallen op haar eigen medewerkers.

Europol heeft tot dusver geen gebruik willen maken van zijn nieuwe bevoegdheden om een onderzoek in te stellen. Pas nadat het Europees Parlement Europol onder druk heeft gezet, heeft het agentschap schriftelijk contact opgenomen met vijf lidstaten en gevraagd of er een politieonderzoek was gestart en of Europol hierbij van nut kon zijn.

Europa's zaak

De problematiek van het misbruik van spyware wordt vooral bekeken vanuit het perspectief van de nationale politiek. Deze tunnelvisie staat een totaalbeeld in de weg. Pas door alle elementen met elkaar te verbinden, wordt duidelijk dat het probleem in al zijn veelzijdigheid een werkelijk Europese zaak is.

We mogen ervan uitgaan dat alle EU-lidstaten een of meer commerciële spywareproducten hebben gekocht, ook al bestaat hiervoor geen officiële bevestiging. Alleen al één enkele onderneming, de NSO-groep, heeft zijn producten verkocht aan 22 eindgebruikers in niet minder dan veertien lidstaten, waaronder Polen, Hongarije, Spanje, Nederland en België. In ten minste vier lidstaten, namelijk Polen, Hongarije, Griekenland en Spanje, is spyware op illegale wijze ingezet, en dat is waarschijnlijk ook gebeurd in Cyprus. Cyprus en Bulgarije, fungeren als knooppunt voor de uitvoer van spyware. Eén lidstaat, Ierland, biedt gunstige fiscale regelingen aan een belangrijke spyware-verkoper en een andere lidstaat ,Luxemburg, is een financieel centrum voor veel spelers in de spywaresector. De Europese jaarbeurs van de sector, ISS World, ook wel "The Wiretappers' Ball" (het spionagegala) genoemd, vindt plaats in de Tsjechische hoofdstad Praag. Een aantal belangrijke figuren uit het milieu lijken graag in Malta te verblijven. Heel wat spywarebedrijven profiteren van de afwezigheid van grenzen in Europa. Zo heeft Intellexa vestigingen in Griekenland, Cyprus, Ierland, Frankrijk en Hongarije, en beschikt de CEO van Intellexa over een Maltees paspoort en een

(brievenbus)bedrijf in Malta. De NSO-groep heeft vestigingen op Cyprus en in Bulgarije en verricht haar financiële activiteiten via Luxemburg. DSIRF verkoopt zijn producten vanuit Oostenrijk, Tykelab vanuit Italië en FinFisher (voor het bedrijf de deuren sloot) vanuit Duitsland.

De handel in spyware haalt voordeel uit de eengemaakte Europese markt en het beginsel van vrij verkeer in de EU. Bepaalde EU-landen zijn aantrekkelijk als uitvoerknooppunt, omdat de handhaving van de uitvoerregels zwak is – de reputatie van de EU als strenge regelgever ten spijt. Zo is de EU sinds de aanscherping van de regels voor uitvoer vanuit Israël aantrekkelijker geworden voor verkopers van spyware. Zij prijzen hun bedrijf aan als "door de EU gereguleerd" en gebruiken hun aanwezigheid in de EU als een kwaliteitskeurmerk. De term "EU" verleent hun een imago van eerbaarheid. Het EU-lidmaatschap is ook een goede zaak voor regeringen die spyware willen kopen: de EU-lidstaten zijn immers vrijgesteld van de afzonderlijke mensenrechtenbeoordeling die vereist is voor een uitvoervergunning van de Israëlische autoriteiten. Het feit dat een land deel uitmaakt van de EU, volstaat als garantie dat het land aan de hoogste normen op dit gebied voldoet.

De verkoop van spyware is ondoorzichtig en ongrijpbaar, maar brengt veel op en is in volle bloei. Ingewikkelde bedrijfsstructuren komen goed van pas - of worden opzettelijk zo complex gemaakt - om ongepaste activiteiten en banden - bijvoorbeeld met EU-regeringen - aan het zicht te onttrekken. Op papier is de sector gereguleerd, maar in de praktijk kunnen talloze regels worden omzeild. Een van de redenen hiervoor is dat spyware in internationale betrekkingen als politieke munt kan dienen. Talrijke landen dienen als plaats van vestiging voor spywarebedrijven, maar deze bedrijven zijn vaak opgericht door personen die vroeger voor het Israëlische leger en de Israëlische inlichtingendiensten werkten. De meeste verkopers beweren dat zij alleen aan overheidsactoren verkopen, maar achter de schermen doen sommigen ook zaken met niet-overheidsspelers. Het is vrijwel onmogelijk informatie te verkrijgen over deze klanten of over de voorwaarden en de naleving van klantencontracten.

De handel in en het gebruik van spyware vallen volledig binnen het toepassingsgebied van het EU-recht en de EU-jurisprudentie. Voor de aankoop en verkoop van spyware gelden onder meer aanbestedings- en uitvoervoorschriften zoals die van de verordening inzake producten voor tweeërlei gebruik. Het gebruik van spyware moet voldoen aan de bepalingen van de AVG (algemene verordening gegevensbescherming), de EUVG (Europese verordening gegevensbescherming), de richtlijn gegevensbescherming bij rechtshandhaving en de e-privacyrichtlijn. De rechten van de betrokken personen, met name het recht op privacy en het recht op een eerlijk proces, zijn vastgelegd in het Handvest van de grondrechten, internationale verdragen en de EU-regels inzake de rechten van verdachten en beklaagden. Misbruik van spyware is in veel gevallen een vorm van cybercriminaliteit en kan de strafbare feiten corruptie en afpersing omvatten. Al deze misdrijven vallen onder de bevoegdheid van Europol. Als er Europese middelen in het spel zijn, kan de Europese openbare aanklager in actie komen. Het misbruik van spyware kan ook de aanzet geven tot politiële en justitiële samenwerking, met name de uitwisseling van informatie en de uitvaardiging van een Europees aanhoudingsbevel of bewijsverkrijgingsbevel.

Misbruik van spyware heeft zowel rechtstreeks als onrechtstreeks gevolgen voor de EU en haar instellingen. Onder de doelwitten van spyware bevonden zich leden van het Europees Parlement, de Europese Commissie en de (Europese) Raad. Anderen werden getroffen als "bijvangst", omdat zij indirecte doelwitten waren. Omgekeerd zit een aantal "daders" ook in

de (Europese) Raad. Daarnaast heeft de manipulatie van nationale verkiezingen aan de hand van spyware een rechtstreekse impact op de samenstelling van de EU-instellingen en op het politieke evenwicht in de bestuursorganen van de EU. De landen van de vier of vijf regeringen die worden beschuldigd van spywaremisbruik, omvatten bijna een kwart van de Eu-bevolking: het gewicht van deze landen in de Raad is met andere woorden aanzienlijk.

Spyware als onderdeel van een systeem

Spyware is niet alleen een technisch instrument dat punctueel en op zichzelf wordt gebruikt. Het maakt integraal deel uit van een systeem. In beginsel is het gebruik ervan ingebed in een rechtskader, dat vergezeld gaat van de nodige waarborgen, toezicht- en controlemechanismen en rechtsmiddelen. Uit het PEGA-onderzoek blijkt evenwel dat deze waarborgen vaak zwak en ontoereikend zijn. Ook al is dit doorgaans niet bedoeld, soms worden het hele regelgevingssysteem of delen ervan opzettelijk verbogen of zelfs ontworpen om te kunnen worden gebruikt als een instrument voor politieke macht en controle. Dan is het onrechtmatige gebruik van spyware geen onvoorzien voorval maar maakt het deel uit van een bewuste strategie. De rechtsstaat wordt in dat geval omgevormd tot het recht van de regeerder. De rechtsgrondslag voor surveillance wordt soms in vage en onnauwkeurige bewoordingen geformuleerd om een breed en ongehinderd gebruik van spyware te legaliseren. Controle vooraf in de vorm van rechterlijke toestemming voor surveillance is gemakkelijk te manipuleren en betekenisloos te maken, met name in het geval van politisering van of overheidsinmenging in de rechterlijke macht. Toezichtmechanismen kunnen zwak en ondoeltreffend worden gehouden en worden onderworpen aan de controle van regerende partijen. Rechtsmiddelen en burgerrechten kunnen wel bestaan op papier maar verliezen elke inhoud als overheidsinstanties de toepassing ervan verhinderen. Klagers krijgen geen toegang tot informatie en kunnen zelfs niet achterhalen op welke zogezegde gronden ze zijn bespioneerd. Aanklagers, magistraten en politieambtenaren weigeren onderzoeken in te stellen en verschuiven de bewijslast vaak naar de slachtoffers door van hen te eisen dat ze bewijzen het slachtoffer te zijn geworden van spyware. De slachtoffers bevinden zich zo in een paradoxale, uitzichtloze situatie, aangezien hun de toegang tot informatie wordt ontzegd. Regeringspartijen kunnen hun greep op overheidsinstellingen en op de media verstevigen om betekenisvol toezicht te onderdrukken. Openbare en commerciële media die banden hebben met regeringen, kunnen dienstdoen als kanaal voor lastercampagnes op basis van met spyware verkregen materiaal. De “nationale veiligheid” wordt regelmatig als voorwendsel aangehaald om transparantie en verantwoordingsplicht terzijde te schuiven. Al deze elementen samen vormen een heus systeem dat is ontworpen met het oog op controle en onderdrukking. Zo worden individuele slachtoffers hulpeloos overgeleverd aan een almachtige regering en wordt bovendien alle essentiële democratische controle tenietgedaan.

Sommige regeringen zijn al op dit punt beland, andere zijn ernaar op weg. Gelukkig slaan de meeste regeringen in Europa deze richting niet in. Maar als ze dat wel zouden doen, is de EU in haar huidige institutionele en politieke vorm niet in staat om hier iets tegen te doen. Spyware is de kanarie in de kolenmijn: de problematiek brengt gevaarlijke constitutionele zwakheden in de EU aan het licht.

Geheimhouding

Geheimhouding vormt een belangrijke hindernis voor het opsporen en onderzoeken van onrechtmatig gebruik van spyware.

De meeste slachtoffers slagen er niet in informatie over hun geval los te krijgen van de autoriteiten. Vaak verwijzen de autoriteiten naar redenen van nationale veiligheid om deze geheimhouding te rechtvaardigen; in andere gevallen ontkennen ze eenvoudigweg het bestaan van een dossier of worden dossiers vernietigd. Tegelijkertijd weigeren openbare aanklagers vaak om gevallen van illegitiem spywaregebruik te onderzoeken, met als argument dat de slachtoffers niet over voldoende bewijs beschikken. In deze vicieuze cirkel staan slachtoffers machteloos.

Overheden weigeren meestal mee te delen of zij spyware hebben gekocht, en welk type. Spywareverkopers weigeren eveneens mee te delen wie hun klanten zijn. Om hun betrokkenheid te verhullen, doen overheden voor de aankoop van commerciële spyware of spywaregerelateerde diensten vaak een beroep op tussenpersonen, gevolmachtigden of persoonlijke kennissen. Om als overheid geen sporen na te laten, omzeilen ze aanbestedingsregels en begrotingsprocedures.

Israël is een belangrijk centrum voor spywarebedrijven en is verantwoordelijk voor de afgifte van vergunningen voor verkoop en uitvoer. Hoewel Israël en Europa nauwe bondgenoten zijn, verstrekt Israël geen informatie over de afgifte van vergunningen voor spyware aan Eu-landen (of de intrekking ervan), ondanks het feit dat deze wordt gebruikt op een manier die de rechten van Europese burgers schendt en onze democratie ondergraaft.

Verzoeken van journalisten op basis van het beginsel van de vrijheid van informatie leveren weinig tot geen informatie op. Ook specifieke controle- en toezichtsorganen, zoals gegevensbeschermingsautoriteiten of rekenkamers, verkrijgen slechts met moeite inlichtingen. Onafhankelijk toezicht op geheime diensten, als dat er überhaupt is, is notoir zwak. Parlementaire enquêtecommissies worden vaak gehinderd door de regeringspartijen. Gerechtelijke onderzoeken zijn gericht op hacking door derde landen en niet op onrechtmatig gebruik van spyware door EU-regeringen. Journalisten die over de problematiek verslag uitbrengen, worden geconfronteerd met strategische rechtszaken tegen publieke participatie (SLAPP's), verbale aanvallen door politici of lastercampagnes. De moedige journalisten die de feiten rond het schandaal zorgvuldig hebben blootgelegd, verdienen ons respect en onze dank. Zij zijn de Woodwards en Bernsteins van Europa. Daarenboven is een adequate bescherming voor klokkenluiders nog altijd niet in alle lidstaten voorhanden. In sommige gevallen zijn het de slachtoffers van een spyware-aanval zelf die zwijgen: ze willen de partijen achter de aanval niet blootstellen uit angst voor vergeldingsacties of voor de gevolgen van het eventuele opduiken van compromitterend materiaal.

Volgende stappen

Momenteel nemen buitenlandse vijandige partijen de Europese waarden onder vuur. In deze context is het des te belangrijker om de Europese rechtsstaat te wapenen tegen aanvallen van binnenuit. De schokkende bevindingen van het PEGA-onderzoek moeten alle Europese burger doen opschrikken. Het is duidelijk dat de handel in en het gebruik van spyware streng moeten worden gereguleerd. De PEGA-commissie zal daartoe een reeks aanbevelingen doen. Er moeten echter ook initiatieven worden genomen voor institutionele en politieke hervormingen die de EU in staat stellen dergelijke regels en normen effectief te handhaven, zelfs wanneer zij door de lidstaten zelf worden geschonden. De EU moet haar verdedigingslinies tegen aanvallen op de democratie van binnenuit onverwijld versterken.

INFORMATIE OVER DE GOEDKEURING IN DE BEVOEGDE COMMISSIE

Datum goedkeuring	8.5.2023
Uitslag eindstemming	+: 30 –: 3 0: 4
Bij de eindstemming aanwezige leden	Bartosz Arłukowicz, Vladimír Bilčík, Karolin Braunsberger-Reinhold, Saskia Bricmont, Anna Júlia Donáth, Cornelia Ernst, Giorgos Georgiou, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Sophia in ‘t Veld, Assita Kanko, Beata Kempa, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Hannah Neumann, Carles Puigdemont i Casamajó, Diana Riba i Giner, Sándor Rónai, Ernő Schaller-Baross, Birgit Sippel, Dominik Tarczyński, Róża Thun und Hohenstein, Dragoş Tudorache, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Bij de eindstemming aanwezige vaste plaatsvervangers	Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom
Bij de eindstemming aanwezige plaatsvervangers (art. 209, lid 7)	Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder

HOOFDELIJKE EINDSTEMMING IN DE BEVOEGDE COMMISSIE

30	+
PPE	Bartosz Arłukowicz, Vladimír Bilčík, Franc Bogovič, Karolin Braunsberger-Reinhold, Andrzej Halicki, Jeroen Lenaers, Gabriel Mato, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Renew	Anna Júlia Donáth, Sophia in 't Veld, Moritz Körner, Róża Thun und Hohenstein, Yana Toom, Dragoş Tudorache
S&D	Theresa Bielowski, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Juan Fernando López Aguilar, Thijs Reuten, Sándor Rónai, Andreas Schieder
The Left	Cornelia Ernst, Giorgos Georgiou
Verts/ALE	Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé

3	-
ECR	Beata Kempa, Dominik Tarczyński
NI	Ernő Schaller-Baross

4	0
ECR	Assita Kanko
ID	Aurélia Beigneux, Catherine Griset
NI	Carles Puigdemont i Casamajó

Verklaring van de gebruikte tekens:
+ : voor
- : tegen
0 : onthouding