Europees Parlement
2019-2024

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

2022/2077(INI)

28.11.2022

ONTWERPVERSLAG

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

van 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))[1]

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 het verslag van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken (A9-0000/2022),

I. Het gebruik van spyware in de EU

I.A. Polen

1. Het gebruik van commerciële spyware in Polen kwam voor het eerst onder de aandacht van het publiek in december 2021. De gevaren ervan kunnen alleen in de volledige context worden begrepen. Commerciële spyware is niet louter een technisch instrument dat in losstaande gevallen en toevallige situaties wordt gebruikt. Het is een integraal en vitaal onderdeel van een systeem dat specifiek is ontworpen voor de onbelemmerde surveillance en controle van burgers. De juridische, institutionele en politieke bouwstenen van dit systeem zijn doelgericht en methodisch samengesteld om een samenhangend en zeer doeltreffend kader tot stand te brengen. Het complete beeld van dit zorgvuldig geplande systeem wordt alleen zichtbaar door de punten met elkaar te verbinden.

2. De mogelijkheden voor wettelijke surveillance in Polen zijn vrijwel onbeperkt. De rechten van slachtoffers zijn tot een minimum beperkt en voorzieningen in rechte zijn in de praktijk van betekenis ontdaan. Doeltreffende toetsing vooraf en achteraf, alsook onafhankelijk toezicht, zijn vrijwel volledig afgeschaft. Leden van de Poolse regering en partijvertrouwelingen 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

[1] Het ontwerpverslag is gebaseerd op het document waarin de rapporteur haar bevindingen heeft uiteengezet. Elke in de loop van het onderzoek genoemde persoon aan wie dit onderzoek schade zou kunnen berokkenen, heeft het recht door de commissie te worden gehoord. Het secretariaat kan worden bereikt via pega-secretariat@europarl.europa.eu .

staatsmedia. Alle waarborgen zijn afgeschaft, de regeringspartijen beschikken over de volledige controle en de slachtoffers kunnen zich tot niemand wenden.

Aankoop van Pegasus

3. 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[2]. 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[3]. 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[4]. Ondanks aanvankelijke ontkenningen bevestigde PiS-leider Jarosław Kaczyński in januari 2022 de aankoop van spyware door de Poolse regering.[5] [6] [7].

Rechtskader

4. In 2014 heeft het Constitutioneel Hof een evaluatie uitgevoerd van de politiewet en andere bestaande wetten die betrekking hadden op de surveillance van burgers en die onverenigbaar met de Poolse grondwet geacht[8]. Het Hof sloot deze evaluatie af met een arrest dat specifieke aanbevelingen en een termijn van 18 maanden bevatte waarbinnen wetswijzigingen moesten worden doorgevoerd[9]. 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[10]. In plaats daarvan zijn de reeds gebrekkige bepalingen die de rechten van de burgers niet beschermen of geen behoorlijk toezicht creëren, in de Politiewet van 2016 verder verzwakt en is de groeiende afstand tussen de Poolse wetgever en de rechtsstaat verder toegenomen.

Antiterrorismewet 2016

---

[2] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, *29 januari 2022.*
[3] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, *29 januari 2022.*
[4] Financieele Dagblad, "De wereld deze week: het beste uit de internationale pers." *7 januari, 2022.*
[5] Financieele Dagblad, "Liberalen Europarlement eisen onderzoek naar spionagesoftware", *12 januari 2022.*
[6] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, *7 januari 2022.*
[7] Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e, *8 februari 2022.*
[8] Verslag van de Commissie van Venetië van juni 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e
[9] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani
[10] 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

5. Naast de Politiewet van 2016 heeft de Poolse regering in 2016 ook een wet aangenomen betreffende de surveillance van buitenlandse burgers, de zogenaamde “antiterrorismewet”. De artikelen van de wet bepalen dat niet-Poolse burgers gedurende drie maanden zonder hun toestemming kunnen worden gemonitord als hun identiteit "twijfelachtig" is, onder meer in de vorm van afluisteren van telefoons, het verzamelen van vingerafdrukken, biometrische foto's en DNA, en de verplichting om prepaid telefoonkaarten te registreren[11]. De procureur-generaal is verantwoordelijk voor het gelasten van de vernietiging van niet-relevant materiaal. Deze functie wordt momenteel uitgeoefend door Zbigniew Ziobro, de minister van Justitie van PiS[12].[13]

Wetboek van Strafvordering

6. 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 naderhand, in maart 2016, herschreven om daarin artikel 168a op te nemen[14]. Deze toevoeging zorgt er thans voor 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 ingebracht tijdens een rechtszaak[15].

Telecommunicatiewet van 16 juli 2004

7. De Poolse telecommunicatiewet bevat onder meer bepalingen op grond waarvan de politie gratis en in bepaalde gevallen zonder medewerking van werknemers, toegang krijgt tot telecommunicatiegegevens[16]. Hiertoe kan worden overgegaan op grond van de vage rechtvaardiging van “ontdekking van misdrijven”. De procureur besluit vervolgens hoe na ontvangst van deze gegevens te werk wordt gegaan, en beschikt door de wet over een aanzienlijke macht. Dat is een politiek besluit gezien het feit dat Ziobro die functie uitoefent[17][18].

Toetsing vooraf

8. Hoewel in Polen in beginsel rechterlijke toestemming vereist is voor surveillance, dient de machtigingsprocedure in de praktijk niet langer als waarborg tegen misbruik, maar

---

[11] Wet van 10 juni 2016 inzake terrorismebestrijdingsoperaties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf
[12] Wet van 10 juni 2016 inzake terrorismebestrijdingsoperaties, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf
[13] EDRi, https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/, *29 juni 2016.*
[14]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
[15] https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings
[16] Telecommunicatiewet van 16 juli 2004 https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004
[17] 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
[18] Helsinki Foundation for Human Rights, https://www.hfhr.pl/wp-content/uploads/2016/05/HFHR_hand_out_Venice_Commission_Act_on_Police_FNL.pdf, *28 april 2016*, blz. 18 [hierna” HFHR-verslag genoemd]

als middel 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 slachtoffers van Pegasus te bespioneren. Aanvragen voor rechterlijke machtiging voor een surveillance worden ingediend door de speciale diensten[19]. 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[20]. De informatie is vaak slechts een samenvatting, waarin soms zelfs de meest elementaire details over het doelwit (naam, beroep, het misdrijf waarvan hij/zij wordt verdacht) en de te gebruiken surveillancemethoden, niet worden vermeld.

Toetsing achteraf

9. In Polen bestaat er vrijwel geen parlementair toezicht. Toen PiS in 2015 aan de macht kwam, werd het traditionele systeem dat bepaalde dat de oppositiepartij het voorzitterschap van de parlementaire commissie voor toezicht op de speciale diensten (KSS) bekleedde, afgeschaft, en stelden de regeringspartijen de PiS-leden Waldemar Andzel als voorzitter en Jarosław Krajewski als ondervoorzitter aan[21]. De regeringspartijen hebben de absolute meerderheid in de commissie[22]. Bovendien werden verzoeken om een parlementair onderzoek naar de beschuldigingen van onrechtmatig gebruik van spyware door de regeringsmeerderheid in de Sejm afgewezen[23][24][25][26][27]. Daarentegen heeft de Senaat, waar de regeringspartijen geen meerderheid hebben, wel een enquêtecommissie ingesteld. De Senaat beschikt echter niet over de onderzoeksbevoegdheden van de Sejm[28].

Verslaglegging

10. Op grond van de Politiewet 2016 is de politie slechts verplicht halfjaarlijkse verslagen in te dienen bij de rechterlijke instanties over het aantal verzamelde telecommunicatie-, post- of internetgegevens, samen met de rechtsgronden daarvoor (die verband houden met de bescherming van het menselijk leven, de gezondheid of ondersteuning van opsporing en redding)[29]. Deze verslagen kunnen alleen *achteraf* worden opgesteld en

---

[19] 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
[20] 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
[21] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[22] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS
[23] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, *17 januari 2022*.
[24] Verslag van de Europese Commissie over de rechtsstaat 2022, hoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf blz. 27.
[25] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab *23 december 2021.*
[26] The Guardian, "Polish senators draft law to regulate spyware after anti-Pegasus testimony", *24 januari 2022.*
[27] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[28] Verslag van de Europese Commissie over de rechtsstaat 2022, hoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf at pg. 27, voetnoot 220.
[29] 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

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. Cruciaal is dat deze toezichtsmaatregelen slechts facultatief en niet verplicht zijn[30].

Verhaalsmogelijkheden

11. Tot dusver heeft de Poolse openbare aanklager geen onderzoek ingesteld, ondanks dat er overvloedig bewijs is dat er ernstige misdrijven zijn gepleegd. Het lijkt erop dat de rechter alleen de zaak van openbaar aanklager Ewa Wrzosek in behandeling heeft genomen. Wrzosek spande haar zaak aanvankelijk aan bij het Openbaar Ministerie, maar na de officiële weigering om de zaak in behandeling te nemen, kon zij beroep instellen bij de rechter. Eind september 2022 heeft de rechtbank van Warschau (Mokotów) de openbare aanklager gelast een onderzoek in te stellen[31].

Publieke controle

12. 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 Brejza. Het openbaar maken van in het kader van een surveillanceoperatie van de bijzondere diensten verkregen informatie is op zichzelf een strafbaar feit. Er is echter geen actie ondernomen, noch door de politie noch door het Openbaar Ministerie.

Politieke controle

13. 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[32]. 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 Hof van Justitie, 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. De heer Kaminski heeft geweigerd een ontmoeting te hebben of samen te werken met de Bijzondere Enquêtecommissie Pegasus van het Europees Parlement[33].

De doelwitten

---

[30] HFHR-rapport, blz. 4.
[31] Wyborcza, https://wyborcza.pl/7,75398,28963729,pegasus-w-telefonie-ewy-wrzosek-prokuratura-odmowila-sad-kaze.html, *28 september 2022.*
[32] Reuters, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, *17 november 2015.*
[33] EU Observer, https://euobserver.com/rule-of-law/156063, *15 september 2022.*

14. Uit onderzoek van de Associated Press en onderzoekers van het Citizen Lab aan de Universiteit van Toronto is gebleken dat in Polen in 2019 ten minste drie personen het doelwit van Pegasus zijn geweest[34]. Deze doelwitten betroffen de senator van de oppositie Krzysztof Brejza, advocaat Roman Giertych, en openbaar aanklager Ewa Wrzosek. Zij werden gehackt met door de regering in 2017 verkregen Pegasus spyware[35]. Hoewel de regering de aankoop van de software van de NSO-groep heeft bevestigd, heeft zij niet officieel erkend dat specifieke personen een doelwit zijn geweest. Geen van de hieronder genoemde 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 een politiek ambt bekleden.

Senator Krzysztof Brejza

15. Senator Krzysztof Brejza was campagneleider van de oppositiepartij Civic Platform toen hij het slachtoffer was van hacking met spyware[36]. In 2019, toen hij de campagne van het Burgerplatform leidde, werden er 33 pogingen gedaan om zijn telefoon te hacken. De aanvallen begonnen op 26 april 2019 en duurden tot 23 oktober 2019, enkele dagen na het einde van de verkiezingscyclus[37].

Roman Giertych

16. Tijdens de slotweken 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 verkiezingen op 13 oktober 2019. Destijds was hij de advocaat van oppositieleider 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[38].

Ewa Wrzosek

17. Aanklager Ewa Wrzosek was tussen 24 juni en 19 augustus 2020 wel zes keer het slachtoffer van hacking met Pegasus-spyware[39]. Wrzosek is lid van Lex Super Omnia, een groep van openbare aanklagers die zich inzetten voor de onafhankelijkheid van het Openbaar Ministerie. Ze deed onderzoek naar de veiligheid van het organiseren van presidentsverkiezingen midden tijdens de wereldwijde COVID-19-pandemie, toen zij

---

[34] 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.*
[35] Financieele Dagblad, 'De wereld deze week: het beste uit de internationale pers.' *7 januari, 2022.*
[36] Haaretz, https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000, *5 april 2022.*
[37] The Guardian, "More Polish opposition figures found to have been targeted by Pegasus spyware", *17 februari, 2022.*
[38] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, *21 december 2021.*
[39] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, *21 december 2021.*

van de naderhand ingetrokken zaak werd gehaald. Zij werd verplicht binnen 48 uur naar de stad Srem te vertrekken. De procureur-generaal van de PiS, Zbigniew Ziobro, beschikt over steeds meer macht om zelf te bepalen in welke zaken al dan niet tot vervolging wordt overgegaan of om ondergeschikte aanklagers van dossiers te halen[40]. Wrzosek werd het doelwit van spyware nadat zij naar Warschau teruggekeerd was. Steeds weer opnieuw weigeren de Poolse autoriteiten hun verantwoordelijkheid te bevestigen of te ontkennen[4142].

Andere mogelijke doelwitten

Hoge controle-instantie

18. De NIK, als een van de oudste instellingen in Polen, heeft tot taak te waken over de overheidsuitgaven en het beheer van overheidsdiensten. Marian Banās is momenteel hoofd van dat orgaan[43] en keert zich tegen de uitholling van de rechtsstaat. Hij vormt de voorhoede die erop aandringt dat de regering van PiS verantwoording aflegt voor deze gevallen van hacking, en dat terwijl hij voorheen een bondgenoot van de partij was[44].

PiS-leden

19. Volgens sommigen werd Pegasus gebruikt voor het “preventief afluisteren” van leiders en organisatoren van straatprotesten, die werden gehouden als reactie op de door de PiS-partij doorgevoerde hervormingen van het Constitutioneel Hof. Het zijn echter niet alleen opposanten van de regeringspartij die mogelijk het slachtoffer zijn geworden van Pegasus. Adam Hofman, voormalig woordvoerder van de PiS-partij, beweert dat zijn eigen collega’s hem in 2018 hebben bespioneerd, als een van de eerste doelwitten na de aankoop van de spyware. Hofman richtte R4S, een PR-bedrijf, op na uit de PiS-partij te zijn gezet[45] [46]. 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.

Verband met lastercampagnes

20. Wekenlang was Senator Brejza het doelwit van een lastercampagne waarbij gebruikgemaakt werd van met behulp van spyware verkregen materiaal. Het is opmerkelijk dat dit materiaal via de openbare televisie openbaar is gemaakt. Hoe kan

[40] Verslag van de Europese Commissie over de rechtsstaat 2022, hoofdstuk over Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, blz. 16.
[41] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, *21 december 2021.*
[42] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, *24 januari 2022.*
[43] https://www.nik.gov.pl/en/about-us/
[44] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[45] https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true
[46] Rzeczpospolita, https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana, *11 oktober 2014.*

worden verklaard dat 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 min of meer 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.

I.B. Hongarije

21. Hongarije was een van de eerste landen die verwikkeld waren in het Europese spywareschandaal. In 2021 bracht het Pegasusproject aan het licht dat in de lijst van 50 000 nummers die mogelijk gehackt waren met behulp van het NSO-product een aantal Hongaarse telefoonnummers waren opgenomen. Amnesty International[47] heeft naderhand bevestigd dat meer dan 300 Hongaren het slachtoffer zijn geworden van Pegasus, onder wie politieke activisten, journalisten, advocaten, ondernemers en een voormalige minister van de regering[48].

Aankoop van Pegasus

22. Het Hongaarse ministerie van Binnenlandse Zaken kocht Pegasus van de NSO-groep in 2017, kort nadat Orbán een ontmoeting had gehad met de Poolse premier Mateusz Morawiecki en de voormalige Israëlische premier Benjamin Netanyahu[4950]. Het Hongaarse ministerie van Binnenlandse Zaken heeft dit pas bevestigd op 8 april 2021, toen de voorzitter van de parlementaire commissie voor defensie en rechtshandhaving, Lajos Kósa, de aankoop van Pegasus door de Fidesz-regering erkende[51]. Kósa benadrukte echter nog altijd dat de spyware nooit tegen Hongaarse burgers is gebruikt[52].

Rechtskader

23. De rechtsinstrumenten met betrekking tot spyware in Hongarije behoren tot de zwakste regelingen in Europa[53] [54]. Het systeem is een flagrante schending van de Europese voorschriften en normen die door het EVRM en de uitspraken van het EHRM[55] zijn vastgesteld voor de surveillance van burgers. De regering daarentegen houdt vol dat zij

[47]Euractiv, "Hungary employed Pegasus spyware in hundreds of cases, says government agency", *1 februari 2022.*
[48] DW, "Pegasus scandal: In Hungary, journalists sue state over spyware", *29 januari 2022.*
[49] Financieele Dagblad, De wereld deze week: het beste uit de internationale pers, *7 januari 2022.*
[50] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[51] DW, "Hungary admits to using NSO Group's Pegasus spyware", *4 november 2021.*
[52] DW, Hungary admits to using NSO Group's Pegasus spyware', *4 november 2021.*
[53] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[54] DW, "Pegasus scandal: In Hungary, journalists sue state over spyware", *29 januari 2022.*
[55] Zie, onder meer, EHRM 4 december 2015, 47143/06 (Roman Zakharov v. Rusland); EHRM 6 september 1978, 5029/71 (Klass en anderen v. Duitsland), § 50, Series A no. 28. 40; EHRM 18 februari 2003 58496/00 (Prado Bugallo v. Spanje), § 30; EHRM 1 juli 2008, 58243/00 (Liberty en anderen v. Verenigd Koninkrijk) § 62.

in alle gevallen wettig heeft gehandeld en zich volledig aan de wet houdt[5657]. De *Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten* (hierna "de wet" genoemd) regelt thans het gebruik van spyware in Hongarije[58]. De wet is veel meer een instrument voor de regering om controle en macht uit te oefenen dan een schild voor de rechten en de privacy van de burgers. Niet alleen is er geen wettelijk voorschrift dat verplicht personen die onder surveillance staan daarvan in kennis te stellen, in de wet wordt specifiek bepaald dat de machtigende instantie de doelwitten niet mag inlichten van het feit dat zij worden bespioneerd[59]. Het Europees Hof voor de Rechten van de Mens (EHRM) heeft in de zaak *Klass en anderen v. Duitsland*[60] ondubbelzinnig vastgesteld dat slachtoffers in kennis moeten worden gesteld. De Hongaarse regering heeft nagelaten deze uitspraak op dezelfde wijze als Polen en vele andere landen in de EU ten uitvoer te leggen.

Toetsing vooraf

24. Volgens de wet is in de meeste gevallen van surveillance door de speciale diensten voor de nationale veiligheid (SNSS) met behulp van spyware de toestemming nodig van de minister van Justitie en in een aantal specifieke gevallen van de rechter die door de president van de regionale rechtbank van de hoofdstad Boedapest is aangewezen[6162]. Tegen deze besluiten kan geen beroep worden ingesteld en er is vrijwel geen toezicht op de procedure[6364].

Toetsing achteraf

25. In november 2021 hebben op aandringen van de oppositie twee senaatscommissies 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. Vervolgens werd bericht dat de regeringsvertegenwoordigers 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.

---

[56] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, *4 november 2021*.
[57] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 februari 2022*.
[58] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf
[59] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, sectie 58.
[60] EHRM 6 september 1978, Klass en anderen v. Duitsland, § 50, Series A no. 28. 40.
[61] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, secties 56-58.
[62] 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, p. 20.
[63] Wet CXXV van 1995 betreffende de nationale veiligheidsdiensten, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, secties 57 en 58.
[64] 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.

Het is echter niet mogelijk te weten wat er precies is gezegd, aangezien de regerende partij de notulen van de vergadering tot het jaar 2050 heeft geclassificeerd.

Verhaalsmogelijkheden

26. Toen het Pegasusschandaal in Hongarije uitbrak werd duidelijk dat journalisten tot een van de groepen behoorden die het vaakst het doelwit waren van de regering. De regering weigert dit noch te bevestigen, noch te ontkennen. Naar aanleiding hiervan heeft begin 2022 een groep van zes journalisten en activisten in Hongarije een gerechtelijke procedure ingeleid tegen zowel de staat als de NAIH. Het Hongaars verbond voor burgerlijke vrijheden (hierna "het verbond" genoemd) zal de journalisten Brigitta Csikász, Dávid Dercsényi, Dániel Németh en Szabolcs Panyi vertegenwoordigen, 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[65].

Politieke controle

27. In Hongarije staat het gebruik van surveillance onder volledige en totale politieke controle. Het Fidesz-regime onder leiding van Orbán heeft ervoor gezorgd dat advocaten, journalisten, politieke tegenstanders en maatschappelijke organisaties gemakkelijk en zonder angst voor vervolging als doelwit kunnen worden gekozen. Bovendien stelt hun controle over bijna alle Hongaarse media hen in staat hun eigen versie van de waarheid op te dringen, waardoor veel van de door de media uitgeoefende publieke controle de Hongaarse burger niet bereikt.

De doelwitten

28. Vanaf het moment dat het spywareschandaal in Hongarije uitbrak, was het overduidelijk dat het optreden van de regering politiek gemotiveerd was. De bevindingen van het Pegasus-project maakten melding van telefoonnummers van meer dan 300 personen [66]. Tot deze personen behoorden ten minste vijf journalisten, tien advocaten, een politicus van de oppositie, alsook activisten en prominente ondernemers[67]. Hoewel het voorkomen van telefoonnummers op deze lijst niet noodzakelijk betekent dat die telefoons 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.

Szabolcs Panyi

[65] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state, *28 januari 2022.*
[66]Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, *19 juli 2021*.
[67] 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*.

29. 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.

Zoltán Varga

30. 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.

Adrien Beauduin

31. Adrien Beauduin verscheen in 2018 op de radar van het regime van Orbán toen hij een doctoraat in genderstudies aan de Midden-Europese Universiteit (CEU) 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[68]. 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 geweldpleging jegens een politieambtenaar, iets wat hij ten stelligste ontkent[69]. 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[70].

Ilona Patócs

32. 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[71]. 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[72]. 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

[68] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[69] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[70] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18 juli 2021.*
[71] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.
[72] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.

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[73]. Met name deze keuze van doelwitten duidt op een kennelijke minachting van de regering voor het advocaat-cliënt-privilege.

Andere doelwitten

33. 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 een lijfwacht 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.

Spywarebedrijven

34. De Hongaarse regering heeft niet alleen Pegasus-spyware aangeschaft en tegen haar bevolking gebruikt, maar heeft ook andere bedrijven op de inlichtingenmarkt welkom geheten. Black Cube is een Israëlische privé-inlichtingendienst die bestaat uit voormalige werknemers van de Mossad, het Israëlische leger en de Israëlische inlichtingendiensten[74]. 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”[75]. Black Cube was betrokken bij een aantal hackingschandalen, onder meer in de VS en in Roemenië[76]. Het is ook gebleken dat zij banden hebben met de NSO Group 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.

I.C. Griekenland

35. Dit jaar is Griekenland opgeschrikt door een reeks onthullingen over het duidelijk politiek gemotiveerde gebruik van spyware. 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[77]. De poging tot infectie met spyware werd tijdens een controle van de telefoon van Androulakis door de IT-dienst van het Europees Parlement ontdekt[78]. De hackpogingen vonden plaats in de periode dat Androulakis kandidaat was voor het leiderschap van de oppositiepartij. Deze onthulling bracht de in april en mei 2022 door financieel journalist Thanasis Koukakis ingediende

[73] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31 maart 2022.
[74] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 okober 2019.
[75] https://www.blackcube.com/
[76] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[77] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader
[78] Tagesspiegel, Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not

klachten over de besmetting van zijn telefoon met Predator onder de aandacht. In september werd aan het licht gebracht dat Christos Spirtzis, voormalig minister van Infrastructuur en parlementslid voor de partij Syriza[79], ook het doelwit is geweest van spyware. Bovendien werd later die maand bekend dat de Griekse nationale inlichtingendienst (EYP) vermoedelijk spyware had ingezet tegen twee van zijn eigen werknemers[80]. Op 5 en 6 november onthulden de Griekse media een lijst van 33 doelwitten, allemaal hooggeplaatste personen[81]. De lijst – indien bevestigd – leest als een verbluffende "wie is wie" van de politiek, het bedrijfsleven en de media in Griekenland. Dit grootschalige politieke gebruik van spyware heeft een impact die verder verder gaat dan alleen de mensen die op de lijst vermeld staan, aangezien ook al hun respectieve contacten en connecties indirect in de spionageoperatie worden "afgetapt", met inbegrip van hun contacten in EU-organen. Dat spyware veel wordt gebruikt, was 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 alleen al 42 waren geplaatst met de bedoeling om doelwitten in Griekenland te misleiden[82][83].

36. De onthullingen over spywaregebruik en EYP-surveillance van journalisten schilderen een zeer verontrustend portret van een complex en ondoorzichtig netwerk van relaties, politieke en zakelijke belangen, gunsten en nepotisme, en politieke invloed. Het is gemakkelijk om in het labyrint te verdwalen. Er zijn echter enkele patronen te ontwaren. Een politieke meerderheid wordt 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 en Krikel te benoemen. Daarbij wordt Spyware, mogelijk in combinatie met legale onderschepping, gebruikt als instrument voor politieke macht en controle in de handen van het hoogste politieke leiderschap van het land. 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 en er wordt geen bescherming geboden aan klokkenluiders.

37. 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 integrale autoritaire strategie, maar veeleer een instrument dat op ad-hocbasis wordt gebruikt voor politiek en financieel gewin. Het leidt echter ook tot uitholling van de democratie en de rechtsstaat en biedt veel ruimte voor corruptie, terwijl deze turbulente tijden juist vragen om betrouwbaar en verantwoordelijk leiderschap.

Aankoop

38. De regering ontkent dat zij Predator-spyware heeft aangekocht[84]. Als het echter niet de Griekse regering was, moet worden geconcludeerd dat een niet-overheidsactor

[79] Reuters, One more Greek lawmaker files complaint over attempted phone hacking
[80] Efsyn, Targeting the disliked
[81] Documento, Apocalpyse: They Watched - This Sunday in Document.
[82] Meta, Threat Report on the Surveillance-for-Hire Industry
[83] InsideStory, Who was tracking the mobile phone of journalist Thanasis Koukakis?
[84] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader.

verantwoordelijk was voor de (pogingen tot) hacking van de telefoons van Koukakis en Androulakis. Dat zou een misdrijf naar Grieks recht zijn en men zou verwachten dat de Griekse autoriteiten een dergelijk ernstig geval onmiddellijk en grondig onderzoeken. Tot dusver heeft er echter nog geen politieonderzoek plaatsgevonden, slechts gerechtelijke onderzoeken naar aanleiding van klachten. Er is geen fysiek bewijsmateriaal in beslag genomen. De hypothese van particuliere actoren achter de Predator-aanvallen is bovendien zeer ongeloofwaardig, aangezien zij de keuze van de doelwitten niet zou verklaren.

39. Een andere mogelijkheid is dat Predator is verworven via Ketyak, een speciale entiteit die is opgericht door het voormalige hoofd van de EYP, Kontoleon. Het opereert op afstand van de EYP.

40. 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. 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 spionagesoftware, met name Krikel, een voorkeursleverancier van communicatie- en bewakingsapparatuur aan onder meer de politie en de EYP. Krikel is nauw verbonden met personen in de entourage van premier Mitsotakis.

Grigoris Dimitriadis

41. Dimitriadis is 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.

Felix Bitzios

42. 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 Bitzios bevroren[85]. 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[86]. Dankzij deze wijziging van de regering van Mitsotakis konden de activa van Bitzios worden vrijgegeven.

43. 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

[85] Lexology: Cyprus court offers directions to bank on ambit of freezing injunction
[86] Financial Times. Greek law change viewed as backtracking on money laundering

Thalestris, de moedermaatschappij van Intellexa, geregistreerd[87]. Opvallend is niet alleen de datum waarop deze overdracht werd geregistreerd — slechts enkele dagen na de onthullingen over de hacking van de telefoon van Androulakis — maar ook het feit dat de overdracht al zou hebben plaatsgevonden op 18 december 2020, meer dan 19 maanden eerder. Bitzios heeft zich dus met terugwerkende kracht gedistantieerd van zijn 1/3 eigenaarschap van Intellexa. Niettemin was Bitzios van maart 2020 tot juni 2021 als adjunct-administrateur verbonden aan Intellexa.

Giannis Lavranos

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

Intellexa

45. De spyware Predator wordt verkocht via Intellexa, een consortium van spyware-verkopers, 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. Het Griekse Ministerie van Buitenlandse Zaken, dat verantwoordelijk is voor de distributie van uitvoervergunningen, heeft verklaard dat er geen uitvoervergunningen zijn afgegeven aan de groep Intellexa[88]. In Griekenland gevestigde ondernemingen uit deze groep zouden echter producten naar Bangladesh en ten minste één Arabisch land hebben uitgevoerd[89] [90]. Zie voor meer informatie over Intellexa het hoofdstuk over de spyware-industrie.

Krikel

46. 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[91]. 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.

---

[87] Inside Story. Predatorgate: The second shareholder of Intellexa SA.
[88] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[89] Haaretz. “As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.”
[90] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[91] 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 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. See: Inside Story. Predatorgate’s invisible privates. en TVXS. G.Lavranos behind KRIKEL - How the deception of the Parliament was attempted [Revealing documents].

47. In 2014 werd Ioniki Techniki, een bedrijf van Giannis Lavranos, verkocht aan Tetra Communications in Londen. In datzelfde jaar is Ioniki Techniki een van de drie ondernemingen die het communicatiesysteem Tetra schonken aan het Griekse ministerie van Burgerbescherming[92]. 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 getekend 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[93]. Krikel werd een belangrijke leverancier van het Griekse Ministerie van Burgerbescherming. Sinds 2018 heeft Krikel zeven overeenkomsten gesloten met de Griekse regering, waarvan er zes geheim zijn[94].

48. Het bedrijf Krikel werd ook de lokale vertegenwoordiger van het Italiaanse bedrijf RCS Lab. In juni 2021 kocht de EYP een afluistersysteem van RCS Lab[95], via Krikel[96]. 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[97]. Andere bronnen spreken dit tegen en voeren aan dat Kontoleon op 29 juli 2022 opdracht heeft gegeven tot de vernietiging van deze dossiers[98].

49. Interessant is dat er getuigen zijn die werknemers van Krikel hebben zien werken bij Ketyak, naar verluidt “pro bono”. Ketyak zou 40 miljoen EUR uit de herstel- en veerkrachtfaciliteit hebben ontvangen via een vertrouwelijke aanbestedingsprocedure op basis van een geheim besluit van de premier.

Betrokkenheid van Bitzios en Lavranos

50. 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[99]. 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)[100].

51. 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

[92] Inside Story. Predatorgate’s invisible privates.
[93] Inside Story. Predatorgate’s invisible privates.
[94] Inside Story. Predatorgate’s invisible privates.
[95] Hellas Posts English. The EYP supplier contaminates smartphones in Greece as well.
[96] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[97] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[98] Euractiv. Greek MEP spyware scandal takes new turn.
[99] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.
[100] Inside Story. From Koukakis to Androulakis: A new twist in the Predator spyware case.

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 Koykakis. 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.

Rechtskader

52. 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.

Toetsing vooraf

53. 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[101].

Wet inzake de inhoud van wetgeving

54. 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[102]. 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 nieuwe voorzitter van de EYP goedgekeurd, terwijl alle andere oppositiepartijen tegen waren[103]. Overigens is Dionysis Melitsiotis, voormalig lid van het kabinet van de premier, 2e plaatsvervangend voorzitter van de EYP[104], en een andere adjunct-directeur is Anastasios Mitsialis, een voormalig partijambtenaar van Nea Demokratia[105].

Controles achteraf

[101] ICLG. Cybersecurity Laws and Regulation Greece 2022.
[102] Efsyn. What (does not) change with the Act of Legislative Content for EYP.
[103] Kathemirini. Themistoklis Demiris: His appointment to the management of EYP was approved by a majority.
[104] Ekathimerini. National security takes center stage.
[105] Greek City Times. Greek PM appoints new security and intelligence chiefs.

55. Sinds 2019 staat de EYP onder rechtstreekste controle van premier Kyriakos, na een wetswijziging na de overwinning van Nea Demokratia in 2019[106].

56. In wet 2225/1994 is bepaald dat alleen van de vertrouwelijkheid van communicatie kan worden afgezien in gevallen van nationale veiligheid en voor het onderzoek 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[107]. Het recht van een persoon op toegang tot informatie over de vraag of de betrokkene onder surveillance staat, is vastgelegd in wet 2472/1997[108]. 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[109]. 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 hier volledig van losstond (een wetsvoorstel met betrekking tot COVID-19-maatregelen), en de in de grondwet voorgeschreven termijnen werden niet in acht genomen[110] [111] [112]. Er heeft dus geen behoorlijk raadplegingsproces plaatsgevonden.

57. De mogelijkheden voor controle achteraf worden verder verzwakt door het feit dat Griekenland de klokkenluidersrichtlijn van de EU nog steeds niet volledig ten uitvoer heeft gelegd[113].

Openbaar toezicht

58. 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)[114]. In 2021 werd journalist Giorgos Karaivaz vermoord. De moord is nog steeds niet opgelost. Journalisten krijgen te maken met intimidatie en strategische rechtszaken tegen publieke participatie (SLAPP's). Grigoris Dimitriadis[115] heeft SLAPP's aangespannen tegen nieuwskanalen Reporters United en Efimerida ton Syntakton (Efsyn)[116] 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 waren[117]. Twee van de slachtoffers van Predator, Koukakis en Malichoudis, hadden op kritische wijze bericht over gevallen van

[106] Euractiv. Another Greek opposition lawmaker victim of Predator.
[107] Constitutionalism. Contradiction of article 87 of Law 4790/2021 with the guarantees of the ECHR for safeguarding the confidentiality of communications.
[108] Dpa. Wet 2472/1997 inzake de bescherming van personen in verband met de verwerking van persoonsgegevens
[109] https://www.reportersunited.gr/8646/eyp-koukakis/
[110] Grieks parlement. Grondwet.
[111] Grieks parlement. Reglement
[112] Govwatch. Violation of the legislative process for amendments in law 4790/2021.
[113] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768
[114] https://rsf.org/en/index
[115] Tagesspiegel.
[116] EUobserver. Greece accused of undermining rule of law in wiretap scandal.
[117] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/

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[118].

Verhaalsmogelijkheden

De nationale autoriteit voor transparantie

59. Op 22 juli 2022 heeft de nationale autoriteit voor transparantie (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[119].

60. In het EAD-verslag werd geconcludeerd dat noch de EYP, noch het Ministerie van Burgerbescherming, een contract had gesloten met Intellexa of andere verbonden nationale bedrijven. Evenmin hadden zij de spyware Predator gekocht of gebruikt[120]. De EAD heeft echter geen onderzoek gedaan naar de bankrekeningen van Intellexa en Krikel of naar gelieerde offshore ondernemingen. Bovendien heeft de EAD pas na 2 maanden een bezoek gebracht aan de kantoren van Intellexa en Krikel, toen alle werknemers telewerkten als gevolg van COVID-19. Daarnaast heeft de EAD geen ontmoeting gehad met de wettelijke vertegenwoordigers van de betrokken ondernemingen[121].

61. Er zijn vragen over de onafhankelijkheid van het bestuur van de EAD. Onlangs baarde een verslag van de EAD over pushbacks van migranten opzien, en werd de autoriteit ervan beschuldigd in haar verslag een subjectief, regeringsgezind standpunt te hebben ingenomen[122]. De directeur van de EAD, een voormalig werknemer van Mitsotakis, heeft tijdens de missie in november 2022 geen ontmoeting gehad met PEGA.

De Griekse autoriteit voor communicatieveiligheid en privacy (ADAE)

62. 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

[118] Heinrich-Böll-Stiftung. In conditions of absolute loneliness.
[119] Inside Story. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[120] Inside Story. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[121] Inside Story. From Koukakis to Androulakis: A new twist in the Predator Spyware case.
[122] https://www.politico.eu/article/greek-transparency-agency-report-data-breach-migration-european-commission/

Androulakis startte de ADAE in augustus 2022 een onderzoek, en vroeg zij om te beginnen informatie op bij de telecomoperator van Androulakis.

De Commissie voor instellingen en transparantie

63. 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 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[123].

De parlementaire enquêtecommissie

64. Het voorstel van de partij PASOK-KINAL om een enquêtecommissie naar het vermeende gebruik van spyware in te stellen[124], werd door 142 parlementsleden van de oppositie gesteund. De 157 parlementsleden van Nea Demokratia onthielden zich van stemming[125]. 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.

65. De regeringsmeerderheid in de commissie weigerde 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. 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[126].

66. Eén getuige, Sarah Hamou van Intelexa, beweerde niet in persoon te kunnen verschijnen (hoewel zij op Cyprus woont), en mocht schriftelijk antwoorden geven. Aangezien geen gemeenschappelijke conclusies konden worden bereikt, publiceerde elke partij haar eigen verslag. Ongeveer 5 500 bladzijden documenten, waaronder de notulen en de verklaring van Hamou, zijn gerubriceerd, hoewel het Parlement volledig bevoegd is om deze te derubriceren. Paradoxaal genoeg dient de enquêtecommissie dus om informatie af te schermen in plaats van er toegang toe te verlenen.

De doelwitten

67. Op het moment dat dit verslag wordt geschreven, is een lijst met 33 namen van doelwitten gepubliceerd. Het is niet mogelijk een gedetailleerde analyse uit te voeren en

[123] Reuters. Greek intelligence service admits spying on journalist - sources.
[124] Tovina. Interceptions: Committee of Inquiry to monitor Androulakis - Pasok's proposal in detail.
[125] Tovina. Parliament: The examination for the attendances from 2016 was passed - With 142 'yes'.
[126] TVXS. G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.

er zijn nog geen formele onderzoeken gestart. De analyse van het handvol tot dusver bekende zaken geeft echter een vrij duidelijk beeld van de problemen in kwestie.

Thanasis Koukakis

68. 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 regering-Mitsotakis 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)[127]. Koukakis onderzocht ook de aanbesteding voor nieuwe identiteitskaarten, waarbij Lavranos en 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.

Nikos Androulakis

69. 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[128]. 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 Koukakis, heeft Androulakis niet geklikt op de link die hem was toegestuurd[129].

70. Surveillance van politici is zeer ongebruikelijk. De Griekse grondwet voorziet voor hen in 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. De peilingen voorspelden dat Nea Demokratia haar absolute meerderheid zou verliezen. 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 Androulakis werd gezegd dat hij openstond voor het idee, zolang het niet met 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. Manolis Othonas, de rechterhand van een andere kandidaat, zou ook behoren tot degenen die nauwere betrekkingen onderhielden met Nea Demokratia en Dimitriadis. De publicatie van de lijst van andere vermeende doelwitten door Documento versterkt het vermoeden dat er politieke redenen waren voor de

[127] Inside Story. Who was tracking the mobile phone of journalist Thanasis Koukakis?
[128] Inside Story. From Koukakis to Androulakis: A new twist in the Predator spyware case.
[129] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.

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.

Stavros Malichoudis

71. 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[130] [131]. Malichoudis schreef over een 12-jarig Syrisch kind dat maandenlang in een detentiekamp op het Griekse eiland Kos moest blijven[132].

Christos Spirtzis

72. Op 15 november 2021 werd de telefoon van voormalig minister van Infrastructuur en wetgever voor de partij Syriza Christos Spirtzis het doelwit van een poging tot hacking met de spyware Predator[133].

Tasos Telloglou, Eliza Triantafyllou en Thodoris Chondrogiannos

73. Ten tijde van hun onderzoekswerkzaamheden voor Inside Story zouden Tasos Telloglou en Eliza Triantafyllou zijn bespioneerd.

Andere doelwitten

74. 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[134]. De heer Oikonomou, woordvoerder van de regering, heeft verklaard dat het artikel geen concrete bewijzen bevatte[135].

75. 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[136]. Op de lijst stonden onder andere 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. Deze onthullingen zijn zeer verontrustend, niet alleen vanwege de prominente namen op de lijst, maar ook omdat dit

[130] Efsyn. Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.
[131] Solomon. Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'.
[132] BalkanInsight. Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.
[133] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.
[134] Ta Nea. Four illegal manipulations by suspicious center.
[135] Politico. Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.
[136] Documento, 6 november 2022.

lijkt te suggereren dat het gebruik van spyware systematisch en op grote schaal plaatsvindt en deel uitmaakt van een politieke strategie.

I.D. Cyprus

76. Cyprus is een belangrijk Europees exportknooppunt voor de surveillancesector. 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. Naar verwachting zal in 2023 een reeks nieuwe wetgevingsinitiatieven worden voltooid om het rechtskader voor de uitvoer te verstrengen en de naleving te verbeteren.

77. 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.

78. Cyprus lijkt zeer nauw samen te werken met Israël op het gebied van surveillancetechnologie. Cyprus heeft met Israël en de VS overleg gepleegd over de hervorming van zijn rechtskader. Het land is een populaire bestemming voor tal van Israëlische spywarebedrijven.

Rechtskader

Verordening inzake producten voor tweeërlei gebruik

79. In tegenstelling tot wat zijn rechtskader doet vermoeden, is Cyprus naar verluidt vrij soepel bij het verstrekken van uitvoervergunningen aan spywarebedrijven[137]. Bedrijven gebruiken bepaalde werkwijzen om de regels te omzeilen: zo wordt bijvoorbeeld de fysieke hardware van een product, zonder software erop, naar een ontvangend land verzonden[138]. Vervolgens wordt de activeringssoftware (ook wel de “licentiesleutel” genoemd) apart op een usb-stick naar het land van bestemming gestuurd[139]. Een andere werkwijze is om aan te geven dat het product alleen voor demonstratiedoeleinden wordt uitgevoerd, hoewel een gedetailleerde beschrijving van het product wordt toegevoegd[140].

80. Veel Israëlische bedrijven gaan naar Cyprus om hun activiteiten in Europa op te starten[141]. Uit verschillende bronnen blijkt dat ongeveer 29 Israëlische bedrijven in het land gevestigd zijn[142]. De handel in spyware hangt nauw samen met de diplomatieke betrekkingen. In ruil voor de facilitering van vergunningen voor Israëlische bedrijven

[137] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[138] Inside Story. Who signs the exports of spyware from Greece and Cyprus?
[139] Philenews. This is how interception patents are exported from Cyprus.
[140] Philenews. Export of monitoring software confirmed.
[141] Philenews. Revelations in Greece: Predator came from Cyprus.
[142] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.

zou Cyprus producten hebben ontvangen die deze ondernemingen ontwikkelen en uitvoeren, zoals de spyware Pegasus van NSO[143] evenals spyware van WiSpear[144].

Toetsing vooraf

81. In Wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie is bepaald dat het verzoek om toestemming voor toezicht op privécommunicatie bij het Hof moet worden ingediend[145].

Controles achteraf

82. Op papier is het schenden van de bescherming van privécommunicatie de jure een strafbaar feit. De facto wordt dit vaak omzeild door zich te beroepen op de nationale veiligheid[146]. 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 zijn deze bepalingen niet ingevoerd[147].

Verhaalsmogelijkheden

83. 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 in te stellen. Bovendien worden de jaarverslagen met de bevindingen van dit comité eerst naar de president gestuurd[148].

Sleutelfiguren in de spyware-industrie

84. Tal Dilian heeft een sleutelrol gespeeld in veel van de ontwikkelingen in Cyprus en Griekenland. In 2017 verwierf hij de Maltese nationaliteit[149]. Hij bekleedde gedurende 25 jaar verschillende leidinggevende functies bij de Israëlische defensiemacht, voordat hij in 2002 uit dienst trad[150]. Dilian startte vervolgens een carrière als "inlichtingendeskundige, gemeenschapsbouwer en serieel ondernemer" in Cyprus en

[143] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.
[144] Inside Story. Predator: The 'spy' who came from Cyprus.
[145] CyLaw. Wet 92(I)/1996 betreffende de bescherming van de vertrouwelijkheid van privécommunicatie (onderschepping van en toegang tot opgenomen privécommunicatie)
[146] Makarios Drousiotis. Κράτος Μαφία.. Hoofdstuk 6. Gepubliceerd in 2022.
[147] Philenews. Legal but uncontrolled interceptions.
[148] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[149] 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
[150] https://taldilian.com/about/

lanceerde Aveledo Ltd., later bekend als WiSpear Systems ltd. en daarna Passitora Ltd[151].

85. In Cyprus ontwikkelde Dilian nauwe banden met Abraham Sahak Avni. Avni was voorheen als rechercheur actief bij de speciale eenheden van de Israëlische politie[152]. In november 2015 werd hij Cypriotisch staatsburger en kreeg hij een gouden paspoort in verband met een investering van 2,9 miljoen euro in onroerend goed[153]. Avni richtte het Cypriotische bedrijf NCIS Intelligence Services ltd.[154] op, dat naar verluidt banden had met de machtigste technologiebedrijven wereldwijd[155]. NCIS Intelligence and Security Services leverde tussen 2014 en 2015 beveiligingssoftware aan het hoofdkwartier van de politie en gaf tussen 2015 en 2016 opleidingen aan de medewerkers van het Bureau voor misdaadanalyse en -statistiek[156]. Ook regeringspartij DISY (Dimokratikós Sinagermós) behoorde tot de klanten van de onderneming. Avni had naar verluidt beveiligingsapparatuur geïnstalleerd in de kantoren van de partij[157]. Naast de beveiligingsapparatuur van Avni werd het materiaal van Dilian ook verkocht aan het Cypriotische Agentschap voor drugshandhaving en de Cypriotische politie[158].

86. Er zijn talloze banden tussen Dilian en Avni. WiSpear, de onderneming van Dilian, deelde een gebouw in Lacarna en aantal personeelsleden met Avni[159]. In 2018 begonnen zij samen het bedrijf Poltrex, dat later is omgedoopt tot Alchemycorp Ltd. Poltrex is ondergebracht in de Novel Tower, een locatie het bedrijf deelt met Avni[160], en maakt 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[161].

De spywarebestelwagen van Dilian

87. Na de verkoop van Circles technologies en de oprichting van WiSpear richtte Tal Dilian in 2019 ook Intellexa Alliance op, dat op haar eigen website wordt beschreven als “een in de EU gevestigd en gereguleerd bedrijf dat ernaar streeft technologieën te ontwikkelen en te integreren om inlichtingendiensten meer zeggenschap te geven”[162]. Onder de koepel van Intellexa Alliance bestaan er verschillende aanbieders van surveillancetechnologieën, zoals Cytrox, WiSpear — later omgedoopt tot Passitora Ltd. — Nexa technologies en Poltrex ltd. Deze verschillende aanbieders binnen de alliantie van Dilian maken een breed assortiment surveillancesoftware en -diensten mogelijk dat Intellexa kan combineren en aan haar klanten kan aanbieden[163]. Meer gedetailleerde

[151] Opencorporates. Passitora ltd.
[152] Shahak Avni. About Shahak Avni.
[153] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[154] Philenews. FILE: The state insulted Avni and Dilian.
[155] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[156] Philenews. FILE: The state insulted Avni and Dilian.
[157] Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.
[158] Inside Story. Predator: The “spy” who came from Cyprus.
[159] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[160] CyprusMail. Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal.
[161] Inside Story. Predator: The “spy” who came from Cyprus.
[162] https://intellexa.com/
[163] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

informatie over de bedrijfsstructuur is terug te vinden in het hoofdstuk over de spyware-industrie.

88. Naar aanleiding van de klachten tegen Dilian werd duidelijk dat het Israëlische Go Networks naar verluidt banden had met Intellexa, omdat zij gezamenlijk eigenaar waren van ondernemingen in Ierland. Voormalige hooggeplaatste vertegenwoordigers zouden bij Intellexa topfuncties hebben gekregen[164]. 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"[165][166].

89. In 2011 richtte 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[167] en is met de hulp van het voormalige advocatenkantoor van Savvas Angelides geregistreerd[168]. Hun partnerschap is echter in 2012 ontbonden. Savvas Angelides was echter wél verantwoordelijk voor de controle van Avni en Dilian in de zaak rond de spywarebestelwagen[169].

90. 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[170]. 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[171]. Door de buitenvervolgingstelling blijft de informatie over de banden tussen de onderneming van Dilian en de Cypriotische regering beschermd[172]. Uit dit voorbeeld blijkt dat de bescherming van personen tegen schending van hun gegevensbeschermingsrechten door het gebruik van apparatuur voor grootschalige surveillance niet volledig is gewaarborgd. Hoewel er op papier rechtsmiddelen bestaan, worden de gerechtelijke resultaten beïnvloed door overheidsingrijpen, waardoor de individuele slachtoffers weerloos achterblijven.

De verhuizing naar Griekenland

91. Na de heisa rond de bestelwagen en de rechtszaak heeft Dilian de activiteiten van Intellexa naar Griekenland verplaatst, hoewel hij Cyprus nooit heeft verlaten en er nog steeds woont. Uit indirecte banden tussen meerdere natuurlijke en rechtspersonen die in

[164] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[165] Makarios Drousiotis. Κράτος Μαφία. Hoofdstuk 6. Gepubliceerd in 2022.
[166] Philenews. Export of tracking software from Cyprus.
[167] Politis. "Interceptions" file: Classified Police Report (2016) shows he knew everything about Avni.
[168] Persbericht van de adjunct-procureur-generaal van 10.08.2022, zoals verkregen tijdens de PEGA-missie naar Cyprus op 2.11.2022.
[169] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[170] Financial Times. Anger after 'spy van' charges dropped.Le
[171] Makarios Drousiotis. Κράτος Μαφία.. Hoofdstuk 6. Gepubliceerd in 2022.
[172] Makarios Drousiotis. Κράτος Μαφία.. Hoofdstuk 6. Gepubliceerd in 2022.

Cyprus en Griekenland zijn geregistreerd, blijkt dat de activiteiten van Dilian in Athene zijn gefaciliteerd[173].

92. Volgens recente getuigenissen in het licht van het gerechtelijk onderzoek in de zaak van de bestelwagen, heeft advocaat Aleksandros Sinka een grote rol gespeeld bij de verhuizing naar Griekenland. Sinka — die voorheen een centrale rol speelde in de centrumrechtse partij DISY — had blijkbaar goede betrekkingen met zowel Dilian als Avni[174]. Het lijkt erop dat Sinka ook een kennis was van voormalig secretaris-generaal van de Griekse regering Dimitriadis. Beide mannen bekleedden functies in het bureau van de European Democrat Students (EDS), de studentenorganisatie van de Europese Volkspartij (EVP). Tussen 2003 en 2004 was Sinka voorzitter en Dimitriadis ondervoorzitter[175]. Dimitriadis zou zijn vriend en Grieks zakenman Felix Bitzios aan Sinka hebben voorgesteld, in verband met diens reeds lang aanslepende geschil in de Cypriotische rechtbank. Sinka suggereerde op zijn beurt om Harris Kyriakidis als advocaat in te schakelen om Bitzios bij zijn geschil te helpen. Kyriakidis had eveneens goede betrekkingen met de DISY[176].

NSO-groep en Cyprus

93. 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[177]. Zes jaar later werd Circles Technologies verkocht aan Francisco Partners voor iets minder dan 130 miljoen dollar, waarvan 21,5 miljoen dollar naar 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[178].

94. De ontkenning van de Cypriotische regering dat Pegasus in het land zou zijn ontwikkeld en daarvandaan zou zijn geëxporteerd lijkt echter onjuist. Op 21 juni 2022 verklaarde NSO-medewerker Chaim Gelfad dat NSO-bedrijven in Cyprus en Bulgarije zich bezighouden met software voor het leveren van inlichtingendiensten[179]. 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 schijnt een factuur van 7 miljoen dollar te hebben opgesteld voor diensten aan de betrokken onderneming[180].

95. 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

[173] Haaretz. “As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.”
[174] Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.
[175] EDS. 2003/2004 Bureau.
[176] Tovima. The unknown “bridge” between Greece and Cyprus for the eavesdropping system.
[177] Amnesty International. Operating from the Shadows.
[178] Amnesty International. Operating from the Shadows.
[179] Verslag van Fanis Makridis. Werkbezoek PEGA aan Cyprus op 1 november 2022.
[180] AKEL-verslag. Werkbezoek van PEGA aan Cyprus.

Limassol een bijeenkomst plaats tussen NSO-medewerkers en Saoedi-Arabische 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 een bedrag van 55 miljoen EUR[181] [182]. Hierbij 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 hij en zijn naasten met Pegasus werden bespioneerd.

Black Cube

96. 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[183].

Aanschaf en gebruik van spyware door Cyprus

97. De Cypriotische regering biedt niet alleen een gunstig exportklimaat voor spywarebedrijven, maar heeft in het verleden zelf 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.

Slachtoffer Makarios Drousiotis

98. Vanaf februari 2018 zou onderzoeksjournalist Makarios Drousiotis zijn bespioneerd door de Cypriotische regering. Deze spionagezaak begon tijdens Drousiotis' voormalige functie als assistent 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 Drousiotis was het deze laatste functie die de aanzet gaf tot de eerste surveillancepoging[184].

Aanvullende opmerkingen

99. Cyprus lijkt te beschikken over een solide rechtskader voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer, voor het verlenen van toestemming voor surveillance en voor uitvoer. In de praktijk lijken de regels echter gemakkelijk te omzeilen en bestaan er nauwe banden tussen de politiek, de veiligheidsdiensten en de

[181] Makarios Drousiotis. Κράτος Μαφία.. Hoofdstuk 6. Gepubliceerd in 2022.

[182] Haaretz. Israëlisch cyberbedrijf onderhandelde met Saoedi's over verkoop geavanceerde aanvalscapaciteiten, onthult Haaretz

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

[184] Makarios Drousiotis. Κράτος Μαφία, Chapter 5. Gepubliceerd in 2022.

surveillance-industrie. Het lijkt de lakse toepassing van de regels te zijn die Cyprus zo aantrekkelijk maakt voor de handel in spyware. Cyprus is ook van aanzienlijk strategisch belang voor Rusland, Turkije en de VS. Bovendien lijken de nauwe betrekkingen met Israël bijzonder gunstig voor de handel in spyware. Uitvoervergunningen voor spyware zijn een valuta geworden in de diplomatieke betrekkingen.

Spanje

100. Uit de onthullingen van het Pegasus-project van juli 2021 bleek dat er sprake was van een groot aantal doelwitten in Spanje. Deze lijken echter het doelwit te zijn geweest van verschillende actoren en om verschillende redenen. Over het algemeen wordt aangenomen dat de Marokkaanse autoriteiten premier Pedro Sánchez, minister van Defensie Margarita Robles en minister van Binnenlandse Zaken Fernando Grande-Marlaska als doelwit hadden, net als in het geval van de Franse president en ministers[185]. Het geval van een tweede groep slachtoffers wordt "CatalanGate" genoemd[186]. Hiertoe behoren Catalaanse parlementsleden, leden van het Europees Parlement, advocaten, leden van maatschappelijke organisaties en enkele familie- en personeelsleden die banden hebben met deze slachtoffers[187]. Over het "CatalanGate"-surveillanceschandaal werd voor het eerst bericht in 2020, 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[188]. In mei 2020 gaven de Spaanse autoriteiten toe dat zij 18 van die 65 slachtoffers met toestemming van de rechter hadden gesurveilleerd[189].

Aanschaf van spyware

101. De eerdere aanschaf van verschillende spywareproducten, zoals SITEL in 2001 en de spyware van Hacking Team in 2010, door het ministerie van Binnenlandse Zaken, de Spaanse nationale inlichtingendienst (CNI) en de politie is breed uitgemeten in de pers[190]. Ook maakte CitizenLab eerder bekend dat Spanje een vermoedelijke klant van Finfisher was[191]. 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[192]. De Spaanse regering zou de spyware in de eerste helft van de jaren 2010 hebben

---

[185] Le Monde, https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-phone-hacking_5982990_4.html, *10 mei 2022.*
[186]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*.
[187]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 1.
[188]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 1.
[189] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, *5 mei 2022.*
[190]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 4-5.
[191]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 5.
[192]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 5.

gekocht voor een bedrag van naar schatting 6 miljoen EUR[193] [194]. Bovendien heeft een voormalige werknemer van NSO bevestigd dat Spanje een rekening heeft bij het bedrijf, hoewel de Spaanse autoriteiten dit niet willen toelichten of bevestigen[195].

Rechtskader

102. Het recht op privacy wordt beschermd door artikel 18 van de Spaanse grondwet van 1978, evenals het recht op geheimhouding in "post-, telegraaf- en telefoonverkeer"[196]. Het gebruik van spyware zoals Pegasus en Candiru vormt een schending van artikel 18; op deze rechten mag echter een uitzondering worden gemaakt wanneer een rechtbank daarvoor toestemming verleent[197]. De grondwet voorziet ook in verdere uitzonderingen op deze rechten in deel I, sectie 55, door te bepalen dat sommige vrijheden kunnen worden opgeschort met "medewerking van de rechter en passende parlementaire controle" in het geval van personen tegen wie een onderzoek loopt wegens activiteiten die verband houden met gewapende groepen of terroristische organisaties[198].

103. De Spaanse inlichtingendienst bestaat uit drie hoofdorganen. Ten eerste het Nationale Inlichtingencentrum (CNI), dat onder toezicht staat van het ministerie van Defensie. 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[199]. Het tweede orgaan is de binnenlandse inlichtingendienst, het Inlichtingencentrum voor Terrorismebestrijding en Georganiseerde Misdaad (CITCO). Het derde en laatste orgaan is het Inlichtingencentrum van de Spaanse strijdkrachten (CIFAS). Het CIFAS staat eveneens onder direct toezicht van het ministerie van Defensie[200] [201].

Toetsing vooraf

104. De surveillance in Spanje is grotendeels uitgevoerd door het CNI, een orgaan dat in het verleden betrokken is geweest bij een aantal surveillanceschandalen[202]. Het CNI is opgericht bij wet 11/2002 van 6 mei, die het CNI machtigt "veiligheidsonderzoeken" te

---

[193] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/, *20 april 2022.*
[194] 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.*
[195] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , *18 april 2022.*
[196] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, sectie 18.
[197] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, sectie 18.
[198] Spaanse grondwet 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx , sectie 55.
[199] https://www.cni.es/en/intelligence
[200] https://emad.defensa.gob.es/en/?__locale=en
[201] Centrum voor governance van de veiligheidssector Genève, Verslag 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf, blz. 40.
[202] CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 2.

verrichten[203]. Er is echter weinig duidelijkheid over de middelen of grenzen van dergelijke activiteiten[204]. Wet 11/2002 voorziet ook in parlementair, uitvoerend en wetgevend toezicht op het CNI[205]. Het parlementaire toezicht wordt uitgeoefend door de Commissie staatsgeheimen van het Spaanse Congres, die in 1995 is opgericht[206]. De Gedelegeerde Commissie voor inlichtingenzaken heeft de uitvoerende macht en coördineert de inlichtingenactiviteiten van het CNI[207]. Ten slotte oefent de Defensiecommissie van het Congres van Afgevaardigden wetgevend toezicht uit op het CNI[208]. De jaarlijkse inlichtingenrichtlijn bepaalt de prioriteiten van het CNI voor dat jaar[209].

Toetsing achteraf

105. Bij de wetten tot oprichting van het CNI is ook de Defensiecommissie van het Congres van Afgevaardigden ingesteld, die verantwoordelijk is voor de toewijzing van de vertrouwelijke middelen voor het CNI en de opstelling van een jaarverslag over het CNI. In de Spaanse grondwet is echter niet bepaald dat toegang wordt verleend tot documenten of informatie over de werkzaamheden van de inlichtingendiensten en ook in het rechtskader van de wet inzake transparantie is geen sprake van deze verplichting. Daarom worden de werkzaamheden van het CNI grotendeels geheimgehouden en ontbreekt het aan transparantie[210].

106. De Commissie staatsgeheimen moet jaarlijks een verslag indienen over de activiteiten van de inlichtingendiensten, maar toen zij naar aanleiding van de surveillance door het CNI bijeen werd geroepen, was het de eerste vergadering van het orgaan in meer dan twee jaar. Hoofd van het CNI Paz Esteban verscheen op 5 mei 2022 voor de commissie om de gerechtelijke machtigingen te presenteren voor de 18 slachtoffers van wie de autoriteiten hebben toegegeven dat zij doelwit waren[211]. De hoorzitting was niet openbaar en de aanwezigen mochten geen elektronische apparaten mee naar binnen nemen[212].

---

[203] 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, lid 5.
[204] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, *4 mei 2022*.
[205] 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.
[206] Wet 11/1995 van 11 mei 1995, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[207] 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.
[208] 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.
[209]On Balance: Intelligence Democratization in Post-Franco Spain, https://www.tandfonline.com/doi/full/10.1080/08850607.2018.1466588?scroll=top&needAccess=true , *International Journal of Intelligence and Counter intelligence* [2018], jaargang 31, nummer 4, 769-804, blz. 776.
[210]CatalanGate-verslag Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 2.
[211] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, *5 mei 2022*.
[212] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, *5 mei 2022*.

Openbaar toezicht

107. Sinds het "CatalanGate"-schandaal in april 2022 aan het licht kwam, is er veel publieke aandacht aan besteed. De Spaanse media en mediakanalen over de hele wereld hebben samen met maatschappelijke organisaties het surveillancesysteem in Spanje uitgebreid onder de loep genomen en gepleit voor de grondrechten van de slachtoffers. 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. Een medewerker van CitizensLab, zelf van Catalaanse afkomst, was een van de doelwitten, samen met zijn ouders, die helemaal niet politiek actief zijn[213].

Verhaalsmogelijkheden

108. Het Openbaar Ministerie heeft in Madrid bij de Audienca Nacional, de Spaanse nationale rechtbank, een rechtszaak aangespannen naar aanleiding van de surveillance van minister-president Sánchez en minister van Defensie Robles[214]. Rechter José Luis Calama, hoofd van de centrale rechtbank van instructie nummer 4, is verantwoordelijk voor deze lopende zaak[215]. Op 13 oktober 2022 bezorgde rechter Calama een vragenlijst aan zowel Robles als Grande-Marlaska, met daarin een vraag over hoe de Pegasusinfecties 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[216].

109. In tegenstelling tot de zaak van Sánchez et. al. in Madrid, verlopen de zaken die in Barcelona zijn aangespannen door Catalaanse slachtoffers van spyware traag[217] [218]. De eerste zaak voor onderzoeksrechtbank nummer 32 in Barcelona werd in 2020 aangespannen door twee Pegasus-slachtoffers: voormalig voorzitter van het Catalaanse parlement en huidig minister van Handel en Werk, Roger Torrent, en voormalig minister van Buitenlands Optreden, Institutionele Betrekkingen en Transparantie van Catalonië en huidig ERC-voorzitter in de gemeenteraad van Barcelona, Ernest Maragall[219]. Andreu Van Den Eynde is een van de advocaten die Torrent en Maragall in deze zaak vertegenwoordigen, en is zelf slachtoffer van Pegasus. Van Den Eynde heeft kritiek geuit op het feit dat de rechtbanken de procedure consequent vertragen en de zaak vrijwel "verlammen"[220]. Ook Omnium Cultural en de partij Candidatura d'Unitat Popular (CUP) hebben een zaak aangespannen bij dezelfde rechtbank in Barcelona.

---

[213] Dit Kan Geen Toeval Zijn, podcastserie van de Volkskrant door Huib Modderkolk en Simone Eleveld, 2022.
[214] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[215] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[216] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[217] El Diario, https://www.eldiario.es/catalunya/juez-barcelona-no-ve-base-imputar-empresa-pegasus-espionaje_1_9068271.html, *9 juni 2022*.
[218] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, *30 mei 2022*.
[219] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[220] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, *30 mei 2022*.

Advocaat Benet Salellas, die bij beide zaken betrokken is, beweert dat de Spaanse regering achter de surveillance zit[221].

110. Aangezien de Spaanse nationale rechtbank bevoegd is voor zaken in verband met de zwaarste misdrijven op alle grondgebieden, zou het Openbaar Ministerie kunnen verzoeken alle Pegasus-zaken samen te voegen[222]. Met andere woorden, de zaken van de slachtoffers van de Spaanse regering en de "CatalanGate"-slachtoffers zouden allemaal in de Spaanse nationale rechtbank in Madrid worden behandeld. De advocaten van de Catalaanse slachtoffers beweren dat er geen verband is tussen de zaken, tenzij bewezen wordt dat de dader in alle gevallen dezelfde is[223].

111. Er loopt nog een aantal andere rechtszaken in verband met de 65 Catalaanse slachtoffers. Eén daarvan is door advocaat en Pegasus-slachtoffer Gonzalo Boye namens ten minste 19 slachtoffers aangespannen tegen NSO, haar drie oprichters Niv Karmi, Shalev Hulio en Omri Lavie, Q Cyber Technologies en OSY, een dochteronderneming in Luxemburg[224] [225]. Ook in een aantal andere EU-lidstaten, waaronder Frankrijk, België, Zwitserland, Duitsland en Luxemburg, lopen juridische procedures naar aanleiding van de surveillance van de Catalaanse separatisten in ballingschap[226].

Doelwitten

112. Het volgen van Catalaanse burgers met spyware begon naar verluidt al in 2015 en wordt sinds 2017 op grote schaal uitgevoerd[227]. Na de eerste media-aandacht in 2020 brak het volledige schandaal in april 2022 in heel Europa los met de publicatie van het CitizenLab-verslag van de Universiteit van Toronto. 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[228].

113. De Spaanse premier Pedro Sánchez, minister van Defensie Margarita Robles en minister van Binnenlandse Zaken Fernando Grande-Marlaska werden tussen mei en juni 2021 gesurveilleerd met Pegasus[229]. Er is tot dusver weinig informatie beschikbaar over de details van deze hack, aangezien deze door de regering werden onthuld en niet het

---

[221] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[222] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[223] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.
[224] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, *3 mei 2022*.
[225] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, *19 april 2022*.
[226] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, *19 april 2022*.
[227] https://catalonia.citizenlab.ca/#targeting-puigdemont
[228]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 5.
[229] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, *2 mei 2022*.

resultaat waren van een onderzoek van CitizenLab of een andere onderzoeksdienst of onderzoeksjournalisten. 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[230]. Grande-Marlaska werd geïnfecteerd op zijn persoonlijke toestel[231]. Minister van Landbouw Luis Planas, die voorheen als diplomaat in Marokko werkte, 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, maar die informatie is niet bevestigd[232].

114. In totaal werd bevestigd dat 65 Catalanen het doelwit waren van huurlingspyware, 63 van Pegasus, vier van Candiru en ten minste twee personen van allebei[233]. Ten minste 51 personen werden met succes geïnfecteerd[234]. De Spaanse regering heeft geweigerd commentaar te geven op de vraag of zij al dan niet verantwoordelijk was voor de surveillance van andere slachtoffers dan de 18 waarvan zij toegeeft dat ze doelwit waren[235]. De meeste van die 18 personen zijn nooit beschuldigd van een misdrijf, maar zijn toch op deze lijst geplaatst. Minister van Defensie Robles heeft zich sterk beroepen op de wet op staatsgeheimen in plaats van uit te leggen wat de redenen waren voor de observatie van die specifieke doelwitten[236]. Alle 65 Catalaanse doelwitten hebben op enig moment contact gehad met de Catalaanse separatisten die buiten Spanje wonen.

Leden van het Europees Parlement

115. Een van de belangrijkste groepen die doelwit bleken te zijn, zijn de naar onafhankelijkheid strevende Catalaanse leden van het Europees Parlement. Zij werden ieder direct of indirect gehackt met spyware via wat CitizenLab “relational targeting” noemt, oftewel surveillance via naasten[237]: Diana Riba i Giner, Antoni Comín i Oliveres, Jordi Solé, Carles Puigdemont en Clara Ponsati.

Catalaanse politici

116. Voormalig voorzitter van het Catalaanse parlement en huidig minister van Handel en Werk Roger Torrent was een van de eerste personen die zich meldde als slachtoffer van

---

[230] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, *7 mei 2022*.
[231] La Razón.
[232] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, *7 mei 2022*.
[233]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 1.
[234]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 5.
[235] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, *5 mei 2022*.
[236] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, *5 mei 2022*.
[237]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 6.

de WhatsApp Pegasus-infecties van 2019[238]. Kort daarna kwamen ook Ernest Maragall, leider van de onafhankelijkheidsgezinde partij ECR (Catalaans Repubikeins links), en Anna Gabriel, die eerder regionaal parlementslid was voor de partij CUP, naar voren als slachtoffers van Pegasus[239]. Sinds 2010 zijn alle presidenten van Catalonië tijdens of na hun ambtstermijn het doelwit geweest van surveillance met spyware[240]. Tot de 65 doelwitten behoorden maar liefst twaalf ERC-leden, onder wie de secretaris-generaal van de partij Marta Rovira. die volgens CitizenLab in juni 2020 minstens twee keer werd gehackt. Het is veelzeggend dat zowel Gabriel als Rovira in Zwitserland woonden toen zij na de breuk die volgde op het referendum van 2017 werden gesurveilleerd.

Maatschappelijke organisaties

117. Jordi Domingo was een van de eerste Catalaanse activisten die in 2020 doelwit zouden zijn geweest. Hoewel hij aanhanger is van de Catalaanse onafhankelijkheid, geloofde Domingo volgens de Guardian dat hij per abuis 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 grondwet van Catalonië[241].

Advocaten

118. Gonzalo Boye heeft vele hooggeplaatste Catalanen vertegenwoordigd, onder wie de voormalige presidenten Puigdemont en Torras[242]. Gedurende vijf maanden, tussen januari en mei 2020, was hij zelf slachtoffer van Pegasus[243]. Boye was in die periode maar liefst 18 keer doelwit via tekstberichten die overkwamen als tweets van maatschappelijke organisaties of prominente nieuwskanalen[244]. 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[245]. De aanval op Boye heeft vragen opgeroepen over de rechtmatigheid van het schenden van de vertrouwelijkheid van de communicatie tussen advocaat en cliënt.

119. Andreu van den Eynde i Adroer, werd op 14 mei 2020 met Pegasus besmet[246]. De hack vond plaats terwijl hij optrad als advocaat van zowel Raul Romeva als Oriol Junqueras in hun zaak voor het Hooggerechtshof.

---

[238] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, *13 juli 2020.*
[239]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz. 5.
[240] Artur Mas (na zijn ambtstermijn), Carles Puigdemont (surveillance via naasten), Joaquim Torra (tijdens zijn ambstermijn), Pere Aragonès (geïnfecteerd tijdens zijn ambtstermijn als vice-president van Torra). https://catalonia.citizenlab.ca/
[241] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, *13 juli 2020.*
[242] https://catalonia.citizenlab.ca/
[243] https://catalonia.citizenlab.ca/
[244] https://catalonia.citizenlab.ca/
[245] https://catalonia.citizenlab.ca/
[246]CatalanGate-verslag CitizenLab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022*, blz.10.

120. Ook de vooraanstaande advocaat Jaume Alonso-Cuevillas werd besmet toen hij belangrijke Catalaanse figuren zoals Carles Puigdemont vertegenwoordigde. CitizenLab kon de precieze datum van de succesvolle besmetting echter niet vaststellen.

Andere lidstaten

121. De nationale autoriteiten hebben tot dusver zeer weinig officiële informatie gedeeld over de aanschaf en het gebruik van spyware in hun land, noch over de budgettaire aspecten of het rechtskader daarvoor. Verkopers en landen die uitvoervergunningen afgeven (met name Israël) delen geen informatie over de klanten. Alleen Oostenrijk, Polen en Cyprus hebben geantwoord op de op 15 juli 2022 door PEGA toegezonden vragenlijst, maar eerder op een zeer algemene, zelfs ontwijkende manier.

122. Door informatie uit verschillende bronnen te combineren, kan echter een gedeeltelijk beeld worden gereconstrueerd en kunnen zaken worden vastgesteld die zorgen baren en nader onderzoek verdienen.

123. Er kan met zekerheid van worden uitgegaan dat de autoriteiten in alle lidstaten op de een of andere manier gebruikmaken van spyware. 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. 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.

124. Uit informatie van de NSO-groep weten we dat Pegasus in ten minste veertien EU-landen werd verkocht, totdat de contracten met twee landen werden beëindigd. Het is niet bekend welke, 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 niet worden nagegaan of dit waar is.

125. 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). Deze beurs staat ook wel bekend als "The Wiretappers' Ball" (het bal van afluisteraars). Met uitzondering van Portugal en Luxemburg waren alle huidige EU-lidstaten vertegenwoordigd door een breed scala aan organisaties, waaronder lokale politiediensten[247]. De laatste jaren is de NSO-groep de hoofdsponsor van het evenement geworden, maar ook Intellexa, Candiru, RCS en vele anderen staan op de lijst van sponsoren[248].

126. 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, sommige zijn de favoriete bestemming voor financiële en

[247] https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf
[248] https://www.issworldtraining.com/iss_europe/sponsors.html

bankdiensten, andere bieden burgerschap en een verblijfplaats aan de hoofdrolspelers van de industrie.

127. Spyware wordt duidelijk ook gebruikt door rechtshandhavingsinstanties, niet alleen door inlichtingendiensten. Er is geen informatie over het met spyware verkregen materiaal, en over hoe dat kan worden en is gebruikt om criminaliteit op te sporen, te onderzoeken en te vervolgen in het kader van de politiële en justitiële samenwerking in de EU. Er zijn grote vraagtekens bij 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.

Nederland

128. 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 gebruikt de politie sinds 2019 hacksoftware, al vermelden de autoriteiten niet welk type[249]. 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[250]. Er wordt geen inzicht gegeven in de uitgaven van zowel politie- als inlichtingendiensten voor de aanschaf en het gebruik van het spywaresysteem.

129. 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[251]. Het is niet duidelijk of het contract uiteindelijk is getekend en of er spyware is geleverd aan het Nederlandse ministerie van Defensie.

België

130. In een interview met The New Yorker onthulde een voormalige Israëlische inlichtingenambtenaar dat de Belgische politie Pegasus gebruikt bij haar operaties[252]. In reactie daarop verklaarde de Belgische politie geen uitspraken te 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

[249] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland
[250] https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021
[251] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[252] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

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[253].

Duitsland

131. 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[254]: toegang tot alle informatie (Online-Durchsuchung[255]) en toegang tot alleen live communicatie (Quellen-TKÜ[256]). 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 in strijd zijn met de wet. Het BKA vroeg NSO daarom een broncode te schrijven, zodat Pegasus alleen toegang zou hebben tot wat wettelijk is toegestaan. Aanvankelijk weigerde NSO dit te doen[257]. Pas na nieuwe onderhandelingen ging NSO akkoord, en kocht het BKA een aangepaste versie aan[258]. 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 dat in de praktijk werkt. Het BKA heeft over deze aangepaste versie een rapport geschreven, dat vertrouwelijk blijft[259].

Gebruik van Finfisher

132. In 2012 en 2013 kochten zowel het BKA als de Berlijnse politie (LKA) onafhankelijk van elkaar FinFisher-spyware (meer over deze spyware in het hoofdstuk over de spyware-industrie). 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.

Malta

133. Verschillende sleutelfiguren uit de spywarehandel hebben een bedrijf op Malta geregistreerd of hebben 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: Tal Dilian, Anatoly Hurgin, Felix Bitzios, Stanislaw Szymon Pelczar en Peter Thiel.

[253] https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html
[254]https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html
[255]https://www.gesetze-im-internet.de/stpo/__100b.html
[256]https://www.gesetze-im-internet.de/stpo/__100a.html
[257]https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html
[258]https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-103.html
[259] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/

Frankrijk

Slachtoffers in Frankrijk

134. In de zomer van 2021 werden in het kader van het Pegasusproject verschillende gevallen onthuld van pogingen tot hacks door de Pegasus-spyware in Frankrijk[260]. De gelekte dataset bevatte het telefoonnummer van president Emmanuel Macron, evenals de telefoonnummers van 14 leden van zijn kabinet[261] [262]. Aan de hand van forensische analyses kan worden bevestigd dat de telefoons van verschillende ministers besmet waren met de Pegasus-spyware[263].

Spywarebedrijven in Frankrijk

135. De spyware-industrie is ook gevestigd in Frankrijk. Nexa technologies, onderdeel van Tal Dilian's Intellexa Alliance, is een Frans cyberdefensie- en inlichtingenbedrijf dat is opgericht in 2000[264]. Nexa Technologies wordt geleid door voormalige managers van Amesys. Amesys werd opgericht in 1979[265] en staat bekend als de verkoper van een programma genaamd Cerebro, dat in staat is elektronische communicatie van zijn slachtoffers, zoals e-mailadressen en telefoonnummers, te traceren[266].

Ierland

136. 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 naar verluidt tweede vrouw Sara Hamou wordt genoemd als directeur van zowel Thalestris als Intellexa[267].

Luxemburg

137. In juni 2021 onthulde Amnesty International dat er in Luxemburg negen entiteiten gevestigd zijn die rechtstreeks in verband staan met de NSO-groep[268]. Jean Asselborn,

---

[260] The Guardian. Pegasus spyware found on journalists' phones, French intelligence confirms.
[261] The Guardian. Spyware 'found on phones of five French cabinet members'.
[262] Euractiv. France's Macron targeted in project Pegasus spyware case.
[263] The Guardian. Spyware 'found on phones of five French cabinet members'.
[264] Bloomberg. Nexa Technologies Inc.
[265] PitchBook. Amesys.
[266] Le Monde. Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen.
[267] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/
[268] https://www.amnesty.org/en/documents/doc10/4182/2021/en/

de Luxemburgse minister van Buitenlandse Zaken, gaf aan slechts weet te hebben van de aanwezigheid in het land van twee zulke entiteiten[269]. Uit de namen van de negen ondernemingen (bijvoorbeeld Triangle Holdings SA, Square 2 SARL en Q Cyber Technologies SARL) kan bovendien niet meteen een band met de NSO-groep worden afgeleid. Hieruit blijkt hoe bedrijven in Luxemburg dankzij ondoorzichtige ondernemingsstructuren geheel buiten het weten van het publiek om actief kunnen zijn.

Italië

138. Tot dusver zijn er geen meldingen gedaan over de mogelijke aankoop van spyware door de Italiaanse autoriteiten. Voormalig premier en Commissievoorzitter Romano Prodi werd door de Marokkaanse geheime diensten bespioneerd aan de hand van Pegasus, maar afgezien daarvan zijn er geen gevallen van spionage op hoog niveau bekend[270]. Als voormalig speciaal gezant van de VN voor de Sahel is het mogelijk dat de heer Prodi in contact stond met hooggeplaatste personen in de Westelijke Sahara of Algerije, wat hem in de ogen van Marokko tot een interessant doelwit kan hebben gemaakt.

Oostenrijk

139. In antwoord op schriftelijke vragen van de Oostenrijkse Nationale Raad heeft voormalig minister van Binnenlandse Zaken Karl Nehammer verklaard dat Oostenrijk nooit klant is geweest bij de NSO-groep[271]. 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.

Estland

140. Ook Estland heeft naar verluidt interesse getoond in de aankoop van de Pegasus-spyware van de NSO-groep. In 2018 vonden eerste onderhandelingen plaats tussen Estland en de NSO-groep. Hierop deed Estland een aanbetaling voor een aankoopcontract voor de NSO-surveillancesoftware ter hoogte van 30 miljoen dollar[272].

Litouwen

141. Anatoly Hurgin, een Russisch-Israëlisch staatsburger die vroeger als ingenieur bij het Israëlische leger werkte en samen met NSO Pegasus heeft ontwikkeld, bezit naar verluidt een bedrijf in Litouwen, UAB Communication Technologies genaamd, dat werkzaam is op het gebied van 'connectiviteits- en telecommunicatiediensten'[273]. In 2015 verkreeg hij overigens een zogeheten gouden paspoort van Malta[274].

---

[269] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e
[270] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/
[271] 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.
[272] The New York Times. Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia
[273] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/
[274] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429

Bulgarije

142. In Bulgarije worden uitvoercontroles en uitvoervergunningen voor producten voor tweeërlei gebruik (conform de definitie hiervan in de desbetreffende EU-verordening), gecontroleerd door het ministerie van Economische Zaken, meer bepaald door de Interministeriële Commissie voor uitvoercontrole en non-proliferatie van massavernietigingswapens[275]. De huidige minister van Economische Zaken en Industrie is Nikola Stoyanov[276]. Tot op heden ontkennen de Bulgaarse autoriteiten dat zij uitvoervergunningen hebben verleend aan de NSO-groep[277]. Novalpina Capital, het private-equityfonds dat de voornaamste eigenaar is van de NSO-groep, heeft echter uitdrukkelijk aangegeven dat de producten van NSO vanuit zowel Cyprus als Bulgarije uit de EU worden uitgevoerd[278] [279] [280]. Beide stellingen spreken elkaar tegen.

EU-instellingen

Doelwit: de Europese Commissie

143. Naar aanleiding van de onthullingen van Forbidden Stories en Amnesty International in juli 2021 heeft de Commissie een "speciaal team van interne deskundigen" opgericht, dat op 19 juli 2021 een intern onderzoek heeft geopend om na te gaan of met Pegasus elektronische toestellen van medewerkers van de Commissie en leden van het college zijn geïnfiltreerd[281]. Op 23 november 2021 ontvingen Didier Reynders, commissaris voor Justitie, en andere medewerkers van de Commissie een officiële kennisgeving van Apple. Hierin stond dat zij het doelwit waren geworden van "door een staat gesteunde aanvallers" en dat hun toestellen mogelijk niet meer veilig waren[282]. Op 11 april 2022 meldde Reuters dat Didier Reynders en ten minste vier andere personeelsleden van de Commissie in november 2021 het doelwit waren geweest van de Pegasus-software[283].

144. Volgens de Commissie is het "onmogelijk om deze feiten met volledige zekerheid aan een bepaalde dader toe te schrijven". De Commissie is van mening dat zij niet kan ingaan op de bevindingen van het onderzoek tot dusver, aangezien "tegenstanders zo kennis zouden verkrijgen van de onderzoeksmethoden en -capaciteiten van de Commissie en de veiligheid van de instelling hierdoor ernstig in gevaar zou worden gebracht". Het gemeenschappelijke onderwerp waarmee twee van de in het vizier genomen ambtenaren van de Commissie, namelijk commissaris Reynders en een kabinetsmedewerker van commissaris Věra Jourová[284], zich beroepshalve bezighouden,

[275] De Republiek Bulgarije. Ministerie van Economische Zaken en Industrie. Interministeriële Commissie voor uitvoercontrole en non-proliferatie van massavernietigingswapens.
[276] Ministerraad van de Republiek Bulgarije.
[277] POLITICO. Pegasus makers face EU grilling. Here's what to ask them.
[278] Amnesty International. Novalpina Capital's response to NGO coalition's open letter (18 February 2019).
[279] Access Now. Is NSO Group's infamous Pegasus spyware being traded through the EU?
[280] https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/
[281] Antwoordbrief van commissarissen Hahn en Reynders aan de rapporteur - 25 juli 2022.
[282] Antwoordbrief van commissarissen Hahn en Reynders aan de rapporteur - 25 juli 2022.
Antwoordbrief van commissarissen Hahn en Reynders aan de Commissie PEGA - 9 september 2022.
[283] https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/
[284] https://pro.politico.eu/news/148627

is de rechtsstaat. Op de vraag van PEGA over een mogelijke correlatie heeft de Commissie verklaard dat zij “niet over voldoende informatie beschikt om definitieve conclusies te kunnen trekken over een verband tussen geolocatie en een mogelijke poging tot het verkrijgen van toegang tot toestellen aan de hand van Pegasus-spyware”[285].

145. In haar interactie met de Commissie PEGA heeft de Commissie meermaals te kennen gegeven dat het kraken van het toestel van commissaris Reynders met de Pegasus-software niet is gelukt. Hiermee lijkt zij de ernst van het feit dat een commissaris in het vizier is genomen, te willen afzwakken. Nochtans is elke poging, geslaagd of niet, om een toestel van (een lid van) de Commissie te kraken, een uitermate ernstig politiek feit dat de integriteit van het democratische besluitvormingsproces op de helling zet.

Maatregelen op het gebied van cyberbeveiliging

146. Naar aanleiding van de poging tot kraken van de telefoon van commissaris Reynders en de aanwijzingen van indringing op verschillende toestellen van medewerkers van de Commissie heeft de Commissie in september 2021 op alle zakelijke telefoons van haar personeel een mobiel systeem voor “Endpoint Detection and Response” (EDR) geïnstalleerd.

Doelwitten: voormalig Grieks Commissielid en leden van de Raad

147. Op 6 november 2022 publiceerde de Griekse krant Documento een lange lijst van mensen die naar verluidt sporen van Predator op hun apparaten hebben aangetroffen. Eén van hen is Dimitris Avramopoulos, Europees commissaris van 2014 tot 2019 en Néa Dimokratía-politicus[286]. Het is niet duidelijk of hij werd geviseerd terwijl hij lid was van het college noch door wie. De lijst is evenwel lang en telt heel wat politici vanuit zowel Néa Dimokratía als de oppositie. De meest waarschijnlijke hypothese is dan ook dat het bevel om deze personen te bespioneren, is gegeven door de entourage van de eerste minister.

148. Dit geval toont met andere woorden aan dat (voormalige) commissarissen op gelijk welk moment om binnenlandse politieke redenen kunnen worden bespioneerd door personen uit hun eigen lidstaat - hetgeen ook hun uitwisselingen met collega’s behelst. Op de door Documento gepubliceerde lijst van doelwitten staan bovendien meerdere ministers van de huidige regering, onder meer de ministers van Buitenlandse Zaken en van Financiën. Deze ministers zijn ook lid van de Raad, die beslist over het buitenlands en financieel beleid van de EU. Eén enkele gekraakte telefoon kan hebben volstaan om in realtime alle vergaderingen van de Commissie en de Raad af te luisteren.

II. De spyware-industrie

149. De Europese Unie is een aantrekkelijke plek voor de handel in bewakingstechnologieën en -diensten, inclusief spyware-tools. Ten eerste zijn er de regeringen van de lidstaten, die potentieel interesse hebben in dergelijke technologieën en diensten. Ten tweede doet

[285] Antwoordbrief van commissarissen Hahn en Reynders aan de Commissie PEGA - 9 september 2022.
[286] Documento, uitgave van 6 november 2022.

het begrip “door de EU gereguleerd” dienst als een kwaliteitskeurmerk, dat 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 hanteert strenge uitvoerregels, maar ook deze kunnen gemakkelijk worden omzeild. De lidstaten proberen elkaar immers te beconcurreren door deze regels opzettelijk minder strikt uit te voeren, en de Europese Commissie kan de naleving van de regels slechts beperkt en oppervlakkig controleren. Telkens wanneer de regeling voor uitvoervergunningen in Israël werd aangescherpt, verlegden verschillende bedrijven zo hun uitvoeractiviteiten naar Europa, en met name Cyprus[287] [288]. Bovendien hebben verschillende belangrijke figuren uit de spyware-industrie het EU-burgerschap verkregen en kunnen zij aldus vrij binnen en vanuit de EU opereren.

150. In veel gevallen lijkt de bijnaam ‘huurlingspyware’ terecht te zijn. De sector kent geen bijster hoge ethische normen en verkoopt zelfs aan de bloedigste dictaturen en aan rijke privé-actoren met slechte bedoelingen. De waarheid zien we op de lijst van slachtoffers van spyware, niet in de brochures van de verkopers ervan, met hun holle beloften inzake mensenrechten. Na de onthullingen van het Pegasusproject, toen bekend werd dat de spyware van Cellebrite was ingezet tegen tegenstanders van Poetin, kondigde het bedrijf in 2021 aan dat het Rusland uit zijn klantenbestand zou schrappen. In oktober 2022 schijnt Poetin echter nog altijd gebruik te maken van de diensten van Cellebrite[289]. De spywaremarkt boomt, brengt veel geld op en wordt bevolkt door talrijke malafide personages zonder scrupules. Het feit dat zij hun producten verkopen aan democratische regeringen in de VS en de EU verleent hen evenwel een schijn van eerbaarheid. Niettemin geven regeringen opvallend ongraag toe dat zij gebruikmaken van spyware, ondanks hun beweringen dat dit gebruik geheel 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. Elk jaar organiseert de sector een groot evenement: “ISS World” (ISS: Intelligence Support Systems), een beurs die ironisch ook wel “The Wiretappers’ Ball” (het spionnengala) 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.

Zwakke plekken

151. Software heeft altijd zwakke plekken. Anders zou spyware niet kunnen worden geïnstalleerd en geactiveerd. 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[290]. De NIS 2-richtlijn (herziene richtlijn inzake beveiliging van

[287] Makarios Drousiotis. State Mafia (Overheidsmaffia). Hoofdstuk 6. Gepubliceerd in 2022.
[288] Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.
[289] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000
[290] 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

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.

Telecomnetwerken

152. 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. Tegelijkertijd berust de moderne telecommunicatie in grote mate op een internationaal protocol: SS7 (Signalling System nr. 7). Dit protocol dateert uit 1975 en is nog altijd in gebruik. SS7 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[291]. Via het SS7-netwerk kunnen telefoongesprekken en tekstberichten worden onderschept en kunnen toestellen worden gelokaliseerd en worden besmet met spyware, zoals Pegasus of Predator[292].

De NSO-groep

153. Pegasus wordt geproduceerd door de NSO-groep. Deze groep werd opgericht in 2010 door Shalev Hulio, Omri Lavie and Niv Karmi. Ze ontwikkelt technologie die gemachtigde overheidsagentschappen en rechtshandhavingsinstanties helpt om terrorisme en misdaad op het spoor te komen en te verhinderen[293]. Pegasus is het bekendste product van de NSO-groep. De spyware werd in 2011 op de internationale markt gebracht[294] [295].

Bedrijfsstructuur, transparantie en zorgvuldigheid (due diligence)

154. 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 deze eerste geregistreerde onderneming 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'[296].

Exportcontroles

155. Aangezien de Pegasus-spyware wordt beschouwd als een technologie voor tweeërlei gebruik, moet er een vergunning worden toegekend voor de uitvoer ervan. Ondernemingen van de NSO-groep verkrijgen hun uitvoervergunningen in Israël, Bulgarije en Cyprus[297]. De meeste van deze vergunningen worden verleend door de

[291] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7.
[292] https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/
[293] NSO Group. About us.
[294] NYTimes. The Battle for the World's Most Powerful Cyberweapon.
[295] Hulio S., NSO Never Engaged in Illegal Mass Surveillance, The Wall Street Journal, 24 februari 2022.
[296] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[297] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure, blz. 62.

Israëlische autoriteiten[298]. Israël is geen partij bij het Akkoord van Wassenaar maar beweert dat het een deel van de inhoud van dit akkoord heeft overgenomen in zijn wet inzake de controle op de uitvoer van defensiegoederen (wet nr. 5766, uit 2007)[299]. Het agentschap voor de controle op defensie-uitvoer van het ministerie van Defensie staat in voor de uitgifte van vergunningen voor verkoop en uitvoer[300]. Na de onthullingen van het Pegasusproject en het opstellen van een zwarte lijst door NSO is het aantal landen waar Pegasus kan worden verkocht, herleid van 102 tot 37. Al deze landen moeten een getuigschrift inzake eindgebruik/eindgebruiker ondertekenen[301]. In het kader 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

156. In juli 2021 begon een conflict tussen de drie oprichters van Novalpina Capital gevolgen te hebben voor de activiteiten van de NSO-groep. De investeerders in de groep besloten uiteindelijk om Novalpina Capital het zeggenschap over de groep te ontnemen[302]. 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[303]. Een leidinggevende bij BRG verklaarde dat de samenwerking met de 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[304]. Op 25 april 2022 spanden twee voormalige beherende vennoten van Novalpina bij de Luxemburgse rechtbank een rechtszaak aan tegen BRG, waarin zij eisten dat Novalpina Capital zijn onafhankelijkheid zou terugkrijgen en alle door BRG genomen beslissingen zouden worden teruggedraaid[305]. 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[306].

Black Cube

157. Black Cube is een Israëlische privé-inlichtingendienst die bestaat uit voormalige werknemers van de Mossad, het Israëlische leger en de Israëlische

---

[298] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.
[299] Onderzoeksdienst van het Europees Parlement (EPRS). Europe's PegasusGate. Countering spyware abuse.
[300] Amnesty International. Antwoord van Novalpina Capital op de brief van de NGO-coalitie (15 april 2019) en brief van het Citizen Lab (6 maart 2019)
[301] Onderzoeksdienst van het Europees Parlement (EPRS). Europe's PegasusGate. Countering spyware abuse.
[302] Financial Times. Private equity owner of spyware group NSO stripped of control of €1bn fund.
[303] Financial Times. NSO Group keeping owners 'in the dark', manager says.
[304] The New Yorker. How democracies spy on their citizens.
[305] Brief aan de heer Jeroen Lenaers en zijn ondervoorzitters.
[306] Luxembourg Times. Top five stories you may have missed.

inlichtingendiensten[307]. 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”[308]. Black Cube was betrokken bij een aantal hackingschandalen, onder meer in de VS en in Roemenië[309]. 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[310]. Kovesi is momenteel het eerste hoofd van het Europees Openbaar Ministerie (EOM). Black Cube zou de opdracht voor het bespioneren van Kovesi hebben gekregen van Daniel Dragomir, een voormalig Roemeens geheim agent[311].

Intellexa Alliance

158. Intellexa werd opgericht in 2019 in Cyprus door Tal Dilian. Dilian bekleedde meerdere leidinggevende functies bij de Israëlische defensiemacht voordat hij een carrière begon als “inlichtingendeskundige, community builder en veelvoudig ondernemer”[312]. Op de website van Intellexa Alliance wordt het bedrijf beschreven als een “in de EU gevestigde en gereguleerde onderneming die technologieën ontwikkelt en toepast waarmee inlichtingendiensten autonomer kunnen worden”. Tot het marketinglabel van Intellexa Alliance behoren verscheidene surveillance-aanbieders, zoals:

- Cytrox, WiSpear (inmiddels omgedoopt tot Passitora Ltd),
- Nexa Technologies (beheerd door voormalige managers van Amesys),en
- Poltrex.

WiSpear en Cytrox

159. In 2013 richtte Tal Dilian een in Cyprus geregistreerde onderneming, Aveledo Ltd, waarvan de naam later werd veranderd in Ws WiSpear Systems Ltd en vervolgens Passitora Ltd[313]. De onderneming is gevestigd in Limassol (Cyprus) en verkoopt apparatuur en software waarmee individuen via hun gsm kunnen worden gelokaliseerd en gevolgd. In een interview met het tijdschrift Forbes legde Dilian uit waartoe de software van WiSpear in staat is en had hij het over de zwarte bestelwagen van het bedrijf, met een waarde van 9 miljoen dollar, waarmee toestellen binnen een straal van 500 meter kunnen worden gehackt. Daarnaast bezit WiSpear apparatuur die gegevens van wifi-netwerken kan onderscheppen[314]. Wegens een aantal publieke schandalen rond

[307] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators , 7 oktober 2019.
[308] https://www.blackcube.com/
[309] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens , 18 april 2022.
[310] Balkan Insight. Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case.
[311] Haaretz. Black Cube CEO Suspected of Running Crime Organisation. Revealed: The Romania Interrogation.
[312] Tal Dilian. About.
[313] Open Corporates. Passitora Ltd. https://opencorporates.com/companies/cy/HE318328
[314] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

deze producten heeft Intellexa zijn voornaamste bedrijfsactiviteiten overgebracht van Cyprus naar Griekenland.

Amesys en Nexa Technologies

160. Ook Amesys en Nexa Technologies maken deel uit van Intellexa Alliance. Beide ondernemingen hebben een omstreden reputatie; zie hiervoor het hoofdstuk over Frankrijk.

Poltrex

161. Poltrex werd opgericht in oktober 2018. De enige aandeelhouder van Poltrex is Intellexa Ltd, die geregistreerd staat op de Britse Maagdeneilanden. Israeli Shahak Avni, oprichter van NCIS Intelligence Services Ltd[315] en vennoot 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. Het bedrijf behield evenwel zijn plaats van vestiging in de Novel Tower - hetzelfde adres als dat van WiSpear[316].

Candiru

162. Candiru is nog een in Israël geregistreerde onderneming die spyware produceert. Candiru werd opgericht in 2014 door Ya'acov Weitzman en Eran Shorer. Beide mannen hebben deel uitgemaakt van Eenheid 8200 van het Israëlische defensieleger en beide hebben voor de NSO-groep gewerkt[317]. Isaac Zack, die eerder al investeerde in de NSO-groep, werd de voornaamste aandeelhouder van Candiru. Het bedrijf verkoopt spyware voor het hacken van computers en servers[318]. Uit publiek geworden informatie over een ontwerpproject blijkt dat de apparatuur van Candiru in prijscategorieën is ingedeeld volgens het aantal toestellen dat er gelijktijdig mee kan worden geïnfecteerd, dat wil zeggen het aantal doelwitten dat de spyware op eenzelfde moment kan viseren. Voor 16 miljoen dollar kunnen klanten bijvoorbeeld apparatuur kopen die een onbeperkt aantal pogingen tot binnendringing mogelijk maken maar slechts tien toestellen tegelijk kan viseren. Voor 1,5 miljoen dollar meer komen daar nog eens vijftien toestellen bij[319].

Tykelab en RCS Lab

163. In augustus 2022 meldde Lighthouse Reports dat Tykelab, een in Rome gevestigd bedrijf dat eigendom is van RCS Lab, tientallen telefoonnetwerken 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 zoals Italië zelf, Griekenland, Macedonië, Portugal, Libië, Costa Rica, Nicaragua, Pakistan, Maleisië, Irak en Mali. Tykelab maakt gebruik van zwakke plekken in mondiale

[315] Philenews. DOSSIER: Avni en Dilian beledigd door de staat (in het Grieks).
[316] CyprusMail. Akel says found 'smoking gun' linking Cyprus to Greek spying scandal.
[317] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers
[318] Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.
[319] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

telefoonnetwerken die derden in staat stellen de locatie van telefoongebruikers te bekijken en hun oproepen eventueel te onderscheppen, zonder dat dit op hun toestel wordt geregistreerd[320]. Gedurende slechts iets meer dan twee dagen in juni 2022 is het bedrijf erin geslaagd netwerken in nagenoeg alle landen ter wereld binnen te dringen[321]. Op zijn website beroept Tykelab zich op "twintig jaar ervaring in het ontwerpen, toepassen en onderhouden van Core Network Telco-oplossingen en grote deskundigheid op het gebied van managed services, klantgebaseerde systeemintegratie en het ontwikkelen van mobiele apps"[322].

Hermit-spyware

164. Hermit is een door RCS Lab ontwikkelde spyware die kan worden gebruikt om de microfoon van gsm's vanop afstand te activeren en om gesprekken, inlogberichten, oproeplijsten, contactbestanden en foto's te kopiëren[323]. In juni 2022 bracht de Threat Analysis Group van Google aan het licht dat door de overheid gesteunde actoren die gebruikmaken van de spyware van RCS Lab, de internetprovider van het doelwit gebruiken om de mobieledataconnectiviteit van het doelwit te desactiveren. Na deze desactivatie stuurt de aanvaller het doelwit een sms met het verzoek een app te installeren om de mobieledataconnectiviteit te herstellen, via een malafide link. Volgens Google is dit de reden waarom de meeste apps de vorm hebben van mobiele apps. 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 Kazakhstan[324] en is ook aangetroffen in Roemenië[325].

DSIRF - Decision Supporting Information Research and Forensic

165. Het Oostenrijkse ministerie van Justitie heeft onlangs een strafzaak aangespannen tegen DSIRF GmbH (LLC)[326], een in Wenen gevestigde Oostenrijkse onderneming met een in 2016 in Liechtenstein opgerichte moedermaatschappij. Volgens eigen zeggen biedt het bedrijf "diensten op maat op het gebied van informatieresearch, forensisch onderzoek en gegevensgestuurde inlichtingen aan voor multinationals in de sectoren technologie, detailhandel, energie en financiën"[327]. DSIRF verkoopt duidelijk aan niet-overheidsactoren.

FinFisher

166. In dit verslag is het belangrijk te wijzen op het faillissement van en het strafrechtelijk onderzoek naar FinFisher. Dit in 2008 opgerichte en in de Duitse stad München gevestigde netwerk van bedrijven produceerde en verkocht spyware. Oorspronkelijk

[320] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[321] https://euobserver.com/digital/155849
[322] http://www.tykelab.it/wp/about/
[323] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[324] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[325] https://www.lighthousereports.nl/investigation/revealing-europes-nso/
[326] DSIRF is een afkorting voor "Decision Supporting Information Research and Forensic" (informatieresearch en forensisch onderzoek ter ondersteuning van besluitvorming).
[327] https://dsirf.eu/about/

had FinFisher nauwe banden met de Brits-Duitse onderneming Gamma Group. FinFisher promootte zijn spyware als “een compleet gamma voor IT-hacking”. Tientallen landen over de hele wereld[328] gebruikten de software, waaronder elf EU-lidstaten[329] en dertien “niet-vrije” landen[330].

III. Reactievermogen van de Europese Unie

167. EU-burgers zijn het slachtoffer geworden van hacking door regeringen met krachtige spyware. Dit brengt de democratie en de individuele burgerrechten in gevaar. De bevoegdheden van de EU om tegen deze bedreigingen op te treden, zijn uitermate beperkt. Zodra een lidstaat zich evenwel beroept op “de nationale veiligheid”, heeft de EU in wezen niets meer te zeggen. De lidstaten beslissen geheel autonoom wat hun nationale veiligheid inhoudt en kunnen dit argument op gelijk welk moment inroepen. De passieve houding van de EU is niet alleen terug te voeren op deze juridische beperkingen maar heeft ook politieke oorzaken. De Europese Commissie, nochtans de hoedster van de EU-verdragen, is in de loop der tijd terughoudender geworden als het gaat om de handhaving van het EU-recht[331], niet zozeer op grond van juridische beperkingen maar veeleer als gevolg van een politieke keuze. De Commissie heeft de neiging om haar bevoegdheden zo minimalistisch mogelijk te interpreteren. Bij flagrante schendingen van de rechtsstaat en de grondrechten wordt deze houding evenwel hoogst problematisch. De beginselen van subsidiariteit en eerbiediging van de exclusieve bevoegdheden van de lidstaten kunnen zo uitmonden in straffeloosheid. 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

168. De Europese Commissie heeft zich in haar reactie op het spywareschandaal tot dusver beperkt tot het schrijven van brieven aan de regeringen van Polen, Hongarije, Spanje en Griekenland waarin zij om opheldering verzoekt. Het lijkt er evenwel op dat zij na deze schuchtere vermaning geen andere stappen zal zetten. 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.

---

[328] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ - https://wikileaks.org/spyfiles4/customers.html

[329] België, Duitsland, Estland, Hongarije, Italië, Nederland, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië.

[330] Angola, Bahrein, Bangladesh, Egypte, Ethiopië, Gabon, Jordanië, Kazachstan, Myanmar, Oman, Qatar, Saudi-Arabië, Turkije.

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

169. Anders dan de VS heeft de Commissie nog geen analyse uitgevoerd van de situatie of van de ondernemingen die actief zijn op de Europese markt. Er bestaat nochtans geen duidelijk juridisch bezwaar tegen een dergelijke analyse.

170. 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), maar ook wetten inzake uitvoer (verordening tweeërlei gebruik) en overheidsopdrachten. De handhaving van deze wetgeving door de Commissie is echter zwak. Zij gaat doorgaans alleen na of de lidstaten de EU-wetgeving correct hebben omgezet in nationale wetgeving. 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[332] te besluiten 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. Ondanks de voorschriften van de verordening tweeërlei gebruik lijkt Cyprus zelfs te zijn uitgegroeid tot een aantrekkelijk uitvoerknooppunt voor verkopers van spyware. Zonder gepaste, reële handhaving is de EU-wetgeving niet meer dan een papieren tijger en laat zij meer dan genoeg ruimte voor een onrechtmatig gebruik van spyware.

Europees Parlement

171. Het Europees Parlement heeft de Enquêtecommissie PEGA 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. Soms staat dit de grondigheid, volledige onafhankelijkheid en objectiviteit van de werkzaamheden van de commissie in de weg. Het is nogal cynisch dat het Europees Parlement niet over onbegrensde onderzoeksbevoegdheden beschikt terwijl sommige van zijn eigen leden illegaal werden of worden bespioneerd.

Europese Raad en Raad van Ministers

172. Hoewel het spywareschandaal volgens de regeringen van de lidstaten een louter nationale aangelegenheid vormt, is de zaak in de Raad van de Europese besproken en hebben de nationale regeringen besloten samen op de vragenlijst van het Europees Parlement te antwoorden[333]. Daarmee hebben zij onmiskenbaar toegegeven dat het wel degelijk gaat om een kwestie voor de Raad. Verantwoordelijkheid is echter niet zoals een menukaart waaruit men naar believen kan kiezen: en het is niet mogelijk alleen bepaalde procedurele kwesties te behandelen en de inhoud buiten beschouwing te laten.

173. 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

[332] https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1662029750223&uri=COM%3A2022%3A434%3AFIN
[333] Ontwerpbrief van het secretariaat-generaal van de Raad aan de delegaties, 26 september 2022.

ze zelf medeplichtig zijn aan de onwettige hacks, of eenvoudigweg omdat ze willen dat de EU op dit gebied zwak en machteloos blijft. Het zwijgen van de Raad en zijn gebrek aan medewerking beloven niet veel goeds voor eventuele regelgevingsinitiatieven in de toekomst. De Raad is weliswaar een wetgevende instantie, maar controleert misschien niet graag zijn eigen leden.

174. Zelfs als uiteindelijk zou worden bewezen dat er sprake is 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

175. De Cypriotische politie en een academische deskundige hebben de opdracht gekregen een meerlagig forensisch onderzoek uit te voeren van de uitrusting die in 2019 in de zwarte bestelwagen van Tal Dilian werd aangetroffen. Europol werd hierbij om assistentie verzocht. Tijdens de PEGA-hoorzitting van 30 augustus 2022 heeft Europol hier evenwel niets over gezegd, ondanks de vragen van leden van PEGA over de rol van Europol bij het onderzoek naar spyware in de EU. Ook daarna is niets meer gezegd over de assistentie van Europol bij het eerder genoemde onderzoek.

176. Europol beschikt niet over autonome operationele bevoegdheden en kan niet handelen zonder toestemming en medewerking van de betrokken lidstaat of lidstaten. Dit vormt een probleem als er duidelijk sprake is van strafbare feiten - zoals cybercriminaliteit, corruptie en afpersing - maar de nationale autoriteiten deze niet onderzoeken. Nog problematischer wordt het wanneer de autoriteiten van de lidstaten zelf medeplichtig zijn aan de misdrijven.

177. Europol heeft echter onlangs nieuwe bevoegdheden gekregen waarmee het op eigen initiatief een onderzoek kan voorstellen, zelfs als het gaat om een misdrijf dat slechts in één lidstaat is gepleegd[334]. Tot nog toe heeft het agentschap evenwel nog geen gebruik willen maken van die bevoegdheden. Het wil immers Europol goede betrekkingen onderhouden met de regeringen van de lidstaten en vreest dat een dergelijk initiatief een negatieve impact zou hebben op de samenwerking op andere gebieden.

178. Op 28 september 2022 heeft PEGA Europol schriftelijk verzocht[335] gebruik te maken van zijn nieuwe bevoegdheden uit hoofde van artikel 6 van de Europol-verordening[336].

---

[334] 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 persoonsgegevens door Europol in strafrechtelijke onderzoeken en de rol van Europol op het gebied van onderzoek en innovatie.

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

[336] "[... D]e 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."

Op 13 oktober 2022 verklaarde Europol in een antwoordbrief[337] 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). Een van de vijf lidstaten heeft inmiddels aan Europol bevestigd dat er onder toezicht van de bevoegde justitiële autoriteiten een strafrechtelijk onderzoek is ingesteld. Deze informatie is ook bevestigd door Eurojust."* Het is niet bekend om welke lidstaten het gaat, noch of het genoemde strafrechtelijk onderzoek door een van die vijf landen betrekking heeft op het misbruik van spyware door regeringen van EU-lidstaten of door derde landen.

179. De EU blijkt eerder machteloos te staan tegen mogelijke criminele activiteiten van nationale autoriteiten, zelfs als deze handelingen gevolgen hebben voor de EU.

180. 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"[338].

Europese rechterlijke macht

181. Het Hof van Justitie van de Europese Unie (HvJ-EU) en het Europees Hof voor de Rechten van de Mens (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 in Europa een uitgebreide relevante jurisprudentie gecreëerd en onder meer normen voor surveillance vastgelegd. 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[339]. 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. Met name als nationale aanklagers of rechters verzuimen of weigeren een zaak in behandeling te nemen, is het moeilijk om de zaak voor een EU-rechtbank te kunnen brengen.

Andere EU-organen

182. Het Europees Comité voor gegevensbescherming, de Europese Toezichthouder voor gegevensbescherming, de Europese Ombudsman, de Europese Rekenkamer en Eurojust hebben slechts beperkte bevoegdheden om toezicht te houden op onrechtmatig gebruik van of onrechtmatige handel in spyware door de regeringen van de lidstaten, of om in dergelijke situaties in te grijpen. Sommige van hun medewerkers kunnen zelfs betrokken zijn bij schandalen in hun lidstaat van herkomst of bij de toedekking ervan. Dit kan ook gevolgen hebben voor de werking en de integriteit van deze EU-organen.

[337] Dossier nr. 1260379.
[338] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ
[339] Beroep van Koukakis bij het Europees Hof voor de Rechten van de Mens, 27 juli 2022.

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 Watergatecomplex in 1972, doet dit spywareschandaal eerder denken aan de ijzingwekkende film "Das Leben der Anderen", over de controle en het bespioneren van de burgerbevolking door het totalitaire communistische regime. Een digitale inbraak met spyware is totaal anders dan een gewone inbraak: veel geavanceerder en invasiever, en nauwelijks te achterhalen. 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 in wezen een smartphone overnemen en alles wat de smartphone bevat, inclusief documenten, afbeeldingen en berichten, 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 de smartphone en op het toestel kan fake content 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 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 "huurlingspyware" vertaalt de aard van het product en van de sector uiterst treffend. 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 in de hele EU uitbreiden. 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, gaat de EU uit van de “veronderstelling van naleving” door de nationale regeringen. In werkelijkheid is deze veronderstelling evenwel niet meer dan een schijnnaleving. 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 Luxemburg, een andere lidstaat, is een financieel centrum voor veel spelers in de spywaresector. De Europese jaarbeurs van de sector, "ISS World", ook wel "The Wiretappers' Ball" (het spionnengala) 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 bezit vestigingen in Cyprus en Bulgarije en verricht zijn 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. Hoewel de EU de reputatie heeft een strenge regelgever te zijn, schiet de handhaving van de Europese uitvoervoorschriften tekort. Dit vergroot de aantrekkelijkheid van bepaalde EU-landen als exportknooppunt, Zo is de EU sinds de aanscherping van de regels voor uitvoer vanuit Israël aantrekkelijker geworden voor verkopers van spyware. Zij promoten hun bedrijf als “door de EU gereguleerd” en gebruiken hun aanwezigheid in de EU als een kwaliteitskeurmerk. De term “EU” verleent hun een imago van respectabiliteit. 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. Andere EU-medewerkers zijn onrechtstreeks, als bijvangst, het slachtoffer geworden van spyware. Omgekeerd telt de

(Europese) Raad ook een aantal “daders” in zijn rangen. 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 vaak 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.