Een Politie Black Box, gebruik van spyware door de Nederlandse politie (onderzoek)

De Nederlandse politie maakt de afgelopen jaren steeds vaker gebruik van spyware van commerciële bedrijven om laptops, computers, smartphones en andere gegevensdragers van verdachten binnen te dringen. Volgens de wet mag de politie alleen gebruik maken van haar hackbevoegdheid bij verdenkingen van terrorisme en ernstige criminaliteit. Door middel van spyware verkregen gegevens worden echter nauwelijks tot niet gebruikt als bewijs bij rechtszaken.

Volgens de overheid vindt een screening van de leveranciers van spyware plaats. In de praktijk is van een screening echter geen sprake. De politie vertrouwt volledig op de verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes, maar doet geen eigen onderzoek. Producenten van spyware leveren ook aan repressieve regimes waar spyware wordt ingezet tegen journalisten, mensenrechtenactivisten en oppositieleden. Ook bedrijven waarvan Nederland spyware heeft afgenomen, zoals Gamma Group en de NSO Group.

De betrouwbaarheid van met spyware verkregen bewijs is bij commerciële spyware in het geding. Spyware tools zijn een ‘black box’. De politie heeft weinig inzicht in de werking van de tools, de wijze waarop een computer of smartphone wordt binnengedrongen, en hoe gegevens worden verzameld en bewijs wordt verkregen. Leveranciers van de spyware, en mogelijk derden, kunnen toegang verkrijgen tot de gegevensdragers van de verdachte, de spyware en de servers waarop de gegevens worden bewaard. Manipulatie van de gegevens en bewijs is dan ook mogelijk: door de politie verzamelde bewijslast kan veranderd of vernietigd kan worden, en gegevens kunnen worden toegevoegd aan de bewijslast.

De keuring om de integriteit van spyware tools te waarborgen is zeer beperkt, omdat leveranciers van de spyware onvoldoende inzicht geven in de broncode en weigeren mee te werken aan een goede keuring. De politie neemt de keuringen nauwelijks serieus en spyware tools worden meestal ingezet zonder voorafgaand te zijn gekeurd. De inzet van niet gekeurde, of slecht gekeurde, opsporingsmiddelen heeft gevolgen voor de bruikbaarheid van bewijsmateriaal in de rechtszaal.

Volgens de overheid gebruikt de politie haar hackbevoegdheid bij onderzoeken naar terrorisme en ernstige criminaliteit. Vanwege het ontbreken van transparante cijfers over de inzet van spyware valt moeilijk te beoordelen in hoeverre dit daadwerkelijk het geval is. Met behulp van spyware verkregen gegevens worden nauwelijks tot niet als bewijs ingebracht in rechtszaken. De overheid geeft geen overzicht van het aantal en type onderzoeken waarbij spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf. Spyware kan ook worden ingezet bij onderzoeken naar minder zware vormen van criminaliteit, en ook tegen advocaten, journalisten en activisten.

Er zijn sterke aanwijzingen dat de politie voor andere doeleinden inzet dan het verkrijgen van bewijs in rechtszaken. Het lijkt erop dat de politie spyware tools gebruikt voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen, zonder dat een rechtercommissaris toezicht houdt op de rechtmatigheid van de inzet.

Binnen Europa, zoals in Hongarije, Griekenland, Polen en Spanje, is de afgelopen jaren steeds meer bekend geworden over de inzet van spyware tegen oppositieleden, journalisten en advocaten. Er is alle aanleiding tot zorg dat dit in Nederland ook het geval is. De Minister van Veiligheid en Justitie beantwoordde deze vraag in december 2022 bevestigend noch ontkennend.

Het toezicht op de toepassing van de hackbevoegdheid schiet tekort. De Inspectie Justitie en Veiligheid signaleert weliswaar problemen rond de betrouwbaarheid van door middel van de inzet van spyware verkregen bewijsmateriaal, de bewijslogging en keuring van de technische hulpmiddelen, maar op andere punten ontbreekt essentiële informatie in de verslagen van de Inspectie.

Zo publiceert de Inspectie niet het aantal bevelen van de inzet van spyware en het handmatig hacken. Hierdoor is niet duidelijk hoe vaak de politie daadwerkelijk gebruik maakt van de hackbevoegdheid, terwijl de politie wel steeds vaker hackt. De verslagen van de Inspectie bevatten ook geen overzicht van het aantal en type onderzoeken waarbij spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf.

Hierdoor is niet te beoordelen in hoeverre spyware alleen wordt ingezet bij onderzoeken naar terrorisme en georganiseerde ernstige criminaliteit. De proportionaliteit en subsidiariteit van de inzet kunnen hierdoor niet beoordeeld worden. Function creep ligt op de loer en er zijn sterke aanwijzingen dat spyware wordt ingezet voor andere doeleinden dan waarvoor zij wettelijk bedoeld is.

In dit onderzoek borduurt Buro Jansen & Janssen voort op eerdere onderzoeken van het Buro naar de cybersurveillance industrie en relatie tussen de Nederlandse politie en leveranciers van spyware. Er is gebruik gemaakt van openbare bronnen, Woo-verzoeken en rapporten van de Inspectie Justitie en Veiligheid.

De Nederlandse politie en spyware

In 2007 start het Korps Landelijke Politiediensten (KLPD), de voorloper van de nationale eenheid van de politie, een onderzoek naar de mogelijkheden om computersystemen te hacken, die systemen aan te vallen en Trojaanse paarden op die computers te installeren. Ook het Nederlands Forensisch Instituut (NFI) en de Nederlandse Organisatie

voor toegepast-natuurwetenschappelijk onderzoek (TNO) doen onderzoek in het kader van het programma cybercrime.

Medewerkers van de KLPD bezoeken vanaf 2008 de ISS World beurzen in Dubai en Praag. ISS-World (Intelligence Support Systems) is een handelsbeurs voor afluister- en surveillance-apparatuur. Naast bedrijven zijn medewerkers van legers, politie en inlichtingendiensten uit verschillende landen in het Midden-Oosten aanwezig.

De Nederlandse politie, en andere opsporings- en inlichtingendiensten en ondersteuningsorganisaties als het NFI geven weinig ruchtbaarheid aan hun bezoeken aan de ISS World Beurzen en andere beurzen. Een Woo-verzoek over het bezoek aan de ISS-beurs in Dubai in 2020 geeft een inkijkje in het opereren van de politie bij deze bezoeken.

Van 8 maart tot en met 12 maart 2020 bezoekt een agent van de Dienst Landelijke Operationele Samenwerking (DLOS) de ISS-beurs in Dubai. De agent schrijft dat hij werkt bij de afdeling Interceptie & Sensing: *"In het kader van ontwikkeling, innovatie en inrichting van de afdeling Interceptie & Sensing, en in mindere mate DLOS, is het van essentieel belang om op de hoogte te zijn van de laatste technologieën en technologische toepassingen… In mijn huidige functie is het belangrijk om van de laatste ontwikkelingen en innovaties op de hoogte te zijn, maar zeker ook om voor de DLOS de best mogelijke innovaties op de wereldmarkt te kunnen terugkoppelen."*

Bij de aanvraag voor de dienstreis voegt de politiefunctionaris de uitnodiging voor een training ("Invitation to Europe's Most Advanced Training on 4G/5G/Wi-Fi Signal Intercept and Electronic Surveillance") en het volledige programma van de beurs.

Op de lijst met bedrijven die hun hardware en software aanbieden staan veel bedrijven die al jaren de ISS World conferenties bezoeken zoals de Israëlische bedrijven Cellebrite en NSO Group, het Amerikaanse Verint, de Duits-Britse FinFisher en Gamma Group, het Britse Providence, de Italiaanse bedrijven AREA en RCS, het Nederlandse Group 2000, het Zuid-Afrikaanse VASTech en het Duitse Rohde & Schwarz.

Van welke bedrijven is gekocht?

De Nederlandse overheid geeft geen openheid van zaken over van welke bedrijven spyware is aangeschaft. In de loop der jaren is hierover echter het een en ander bekend geworden.

Toenmalig Minister van Veiligheid en Justitie Opstelten bevestigde in 2011 dat de Nederlandse politie spyware van het Duitse bedrijf DigiTask had aangeschaft. Het bedrijf had dit eerder zelf naar buiten gebracht.

DigiTask was begin deze eeuw een van de eerste bedrijven die software aanbood om computers en telefoons binnen te dringen. De hack software was betrekkelijk goedkoop en eenvoudig in gebruik, in vergelijking met andere tools die in die tijd werden aangeboden, zoals FinFisher van Gamma Group en de DaVinci of Galileo RCS (Remote Control System) van het Italiaanse bedrijf Hacking Team.

Uit de in 2015 openbaar gemaakte WikiLeaks documenten bleek dat Nederland sinds 2012 zestien licenties voor de tool FinFisher had aangeschaft van Gamma Group, een van oorsprong Brits bedrijf met dochterondernemingen over de gehele wereld. FinFisher kwam in 2008 op de markt en er kan mee worden ingebroken op computers, laptops en smartphones.

Ook werd in 2015 bekend dat de Nederlandse politie contact had met het Italiaanse bedrijf Hacking Team. Het is niet bekend of Nederland ook producten van het bedrijf heeft aangeschaft. Buro Jansen & Janssen heeft Woo-verzoeken ingediend over de contacten van de Nederlandse overheid met DigiTask, Gamma Group en Hacking Team. Er is nauwelijks informatie openbaar gemaakt, alle documenten zijn grotendeels zwart en onleesbaar gemaakt.

De Nederlandse politie heeft ook zaken gedaan met Providence, een Brits security bedrijf dat tevens als tussenhandelaar voor andere bedrijven opereert. In de cybersurveillance industrie zijn meer tussenhandelaren actief.

In antwoord op Woo-verzoeken erkende de politie in 2016 dat het 39 producten en diensten van het bedrijf had afgenomen, maar de politie maakte niet bekend welke. Uit nader onderzoek van Buro Jansen & Janssen is gebleken dat politie naar alle waarschijnlijkheid via Providence de Kailax Unlocker heeft gekocht, een USB-stick waarmee op Windows computers kan worden ingebroken. Kailax is een Israëlisch bedrijf. Providence, waar een voormalige Nederlandse politieman werkzaam was, speelde ook een bemiddelende rol bij de contacten tussen de Nederlandse overheid en Hacking Team.

In 2022 onthulde de *Volkskrant* dat de AIVD gebruik heeft gemaakt van de Pegasus spyware van NSO. De software kan telefoons op afstand overnemen zonder tussenkomst van de gebruiker. Het is op dit moment niet bekend of de Nederlandse politie gebruik maakt van de Pegasus spyware. De *Volkskrant* heeft via Woo verzoeken verzocht om nadere informatie openbaar te maken, maar deze lopen nog.

Woo-verzoeken van Buro Jansen & Janssen uit januari 2022 zijn tot op heden door de Nederlandse politie niet beantwoord. Het NFI, dat forensisch onderzoek voor de politie doet, heeft in antwoord op Woo-verzoeken toegegeven contact te hebben gehad met de NSO Group. De inhoud van die contacten is echter niet openbaar gemaakt, documenten zijn bijna volledig onleesbaar gemaakt.

Inzet spyware en gebruik in rechtszaken

Met behulp van spyware verkregen gegevens worden zelden als bewijs ingebracht in rechtszaken. Een van de weinige zaken waarin de inzet van spyware wel ter sprake kwam betrof de zaak tegen Aydin C. in 2014. Hij benaderde tientallen vrouwen en een man uit Nederland, Groot-Brittannië, Schotland, Noorwegen, Canada, Australië en de Verenigde Staten via chatprogramma's als Habbo, Chatroulette en Omegle. Hij gaf zich uit als vrouw en vroeg de vrouwen seksuele handelingen uitvoeren die hij opnam. Vervolgens chanteerde hij de vrouwen met die beelden ('sextortion'). Zijn zaak kreeg vooral bekendheid doordat hij de Canadese Amanda Todd tot zelfmoord zou hebben gedreven door middel van afpersing met naaktfoto's.

Volgens het proces-verbaal van terechtzitting van de rechtbank Amsterdam 6 november 2015 werd het technisch hulpmiddel in 2008 aangeschaft en ingezet van 22 december 2013 tot 13 januari 2014. Het hulpmiddel werd geïnstalleerd op de laptop en pc van de verdachte, waarmee de toetsaanslagen van de gebruiker en Skype sessie werden vastgelegd. In de processtukken wordt vooral gesproken over een 'keylogger' of 'technisch hulpmiddel'. Het Openbaar Ministerie maakte niet bekend welk middel werd ingezet, omdat dit de opsporing zou kunnen frustreren.

Gezien de eigenschappen van het hulpmiddel, het keuringsrapport van 24 maart 2009 (keuringsrapport OVC (Opname vertrouwelijke communicatie) van de DSTR Keuringsdienst (Dienst Specialistische Recherche Toepassingen) van technisch hulpmiddel 'THv030+102', gekeurd door teamleider J.G.J Kulker) en de tijd van inzet moet ervan uit gegaan worden dat het waarschijnlijk om de hacktool van DigiTask gaat, ook wel 0zapftis of R2-D2 genoemd.

Dat het gebruik van het 'technische hulpmiddel' in de zaak bekend is geworden is vooral te danken aan de advocaat van de verdachte. Hij trok het gebruik en het functioneren van de tool in twijfel en vroeg tijdens de rechtszitting om allerlei aanvullende documenten en onderzoek.

Wet Computercriminaliteit III

Toen de Nederlandse politie begin deze eeuw begon met de aankoop en inzet van spyware was hacken niet met zoveel woorden in het Wetboek van Strafvordering opgenomen. De politie experimenteerde met de inzet van deze opsporingsbevoegdheid.

Met de invoering van de Wet Computercriminaliteit III in 2019 is hackbevoegdheid van de Nederlandse politie wettelijk verankerd. Hacktools worden technische hulpmiddelen genoemd en zijn bedoeld om computers, laptops, smartphones en andere gegevensdragers/communicatiemiddelen binnen te dringen.

DIGIT (Digital Intrusion Team) is onderdeel van de Landelijke Eenheid van de politie en verantwoordelijk voor de uitvoering van de hackbevoegdheid. De Inspectie Justitie en Veiligheid houdt toezicht op zowel op de voorbereiding en de uitvoering van het hacken, als de keuring van de technische hulpmiddelen.

Sinds 2019 publiceert de Inspectie jaarlijks een rapport over de wettelijke hackbevoegdheid van de politie (*Verslag toezicht wettelijke hackbevoegdheid politie*). Ondertussen zijn er drie rapporten verschenen. Deze verslagen bestrijken de periode 1 maart 2019 tot en met 31 december 2021.

Screening van producenten spyware zeer beperkt

In het regeerakkoord 2017-2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes.

De controle hierop is verdeeld tussen de AIVD en de politie. De AIVD wordt door de politie gevraagd bedrijven te screenen. In de verslagen van de Inspectie Justitie en Veiligheid over 2019 en 2020 staat dezelfde passage over de screening: *"De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) ..."*

De screening periode bedraagt vier weken: *"In die procedure is opgenomen dat als de AIVD binnen vier weken geen bericht geeft, er vanuit gegaan wordt dat er geen nadelige gegevens zijn gevonden",* en dat er "*voor de AIVD geen belemmeringen bestaan voor deze leverancier".*

Het niet berichten door de AIVD hoeft niet te betekenen dat de AIVD daadwerkelijk onderzoek heeft verricht. De Inspectie gaat hier echter niet nader op in. Uit de verslagen wordt niet duidelijk hoeveel screeningsonderzoeken de AIVD verricht.

Het is niet duidelijk waaruit de onderzoeken van de AIVD bestaan en wat de screening behelst. De Inspectie gaat hier niet op in en merkt in haar verslag over 2021 alleen op dat "*in parlementaire stukken niet is uitgewerkt op welke aspecten de leverancier door de AIVD wordt gescreend. Deze screening is anders van inhoud dan de veiligheidsonderzoeken die de AIVD uitvoert voor personen die een vertrouwensfunctie (gaan) vervullen."*

Naast de onduidelijke screening door de AIVD vindt er tevens een toetsing door de politie plaats. Deze toetsing stelt in de praktijk weinig voor. In antwoord op Kamervragen geeft de Minister van Justitie en Veiligheid op 23 december 2022 (samen met de ministers van Binnenlandse Zaken en Koninkrijkrelaties en Defensie) aan: *"De leverancier wordt gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar het respecteren van mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning."*

Bij de toetsing door de politie ontbreekt het volledig aan een toetsingskader. Zo is niet duidelijk welke landen als dubieuze regimes worden beschouwd. De Minister heeft het in de beantwoording van de Kamervragen eerst over *"landen die zich schuldig maken aan ernstige schendingen van mensenrechten en internationaal recht"*, maar later over *"landen waartegen vanuit de EU of de VN sancties bestaan".*

De Minister, noch de politie en de Inspectie, verduidelijken om welke landen het precies gaat. Tegen tientallen landen zijn EU of VN-sancties afgekondigd. Er zijn talloze landen waar de mensenrechten worden geschonden. Ook bestaat er geen nadere uitwerking over de mensenrechtentoets in het exportcontrolebeleid in het land van vestiging van de producent van de spyware.

De politie verricht geen enkel eigen onderzoek vertrouwt volledig op de verklaringen van de leverancier van de spyware zelf. *"De toets aangaande het niet leveren aan dubieuze regimes wordt door de politie uitgevoerd door een verklaring hierover op te vragen bij de leverancier",* aldus de Inspectie.

De Inspectie maakt in haar verslagen niet duidelijk of zij inzage heeft gekregen in de door de politie opgevraagde verklaringen. Uit de verslagen van de Inspectie wordt evenmin duidelijk of de politie het bedrijf tevens vraagt naar de uitwerking van de mensenrechtentoets in het exportcontrolebeleid in het land van vestiging.

De Minister van Veiligheid en Justitie voegt hier in de beantwoording van de Kamervragen in december 2022 nog aan toe dat de controle door de politie periodiek wordt herhaald: *"De politie past dit beleid toe en eist van leveranciers dat niet aan zulke dubieuze regimes wordt geleverd en deze toets wordt door de politie periodiek herhaald."*

Het lijkt er echter op dat de politie deze toets in de praktijk niet daadwerkelijk herhaalt. De Inspectie merkt in haar verslag over 2021 op dat screeningsaanvraag en toets eenmalig heeft plaatsgevonden in 2019, maar in latere jaren niet is herhaald.

Cybersurveillance industrie is controversieel

De screening van bedrijven is dus zeer beperkt. De politie verricht zelf geen onderzoek en vertrouwt volledig op de verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes. Dit beleid is bevreemdend, zeker in het licht van de vele controversiële aspecten die kenmerkend zijn voor de cybersurveillance industrie.

Spyware wordt wereldwijd regelmatig ingezet tegen politici, oppositieleden, journalisten en mensenrechtenactivisten, ook in landen waartegen geen EU of VN-sancties gelden. In de loop der jaren zijn talloze gevallen bekend geworden van een dergelijke inzet door repressieve regimes. Het gaat daarbij ook om spyware van bedrijven die ook aan Nederland hebben geleverd, of waarin de Nederlandse overheid interesse had.

Zo is de FinFisher spyware van Gamma Group aangeschaft door onder andere het Egypte van Moebarak, Oeganda, Ethiopië, Vietnam, Venezuela, Turkije, Turkmenistan, Bahrein en Saoedi-Arabië, waar het is ingezet tegen onder andere journalisten, mensenrechtenactivisten en oppositieleden. Hacking Team leverde onder andere aan Panama, Mexico, Ecuador, Colombia, Oeganda, Ethiopië, Soedan, Oezbekistan en de Verenigde Arabische Emiraten. NSO leverde haar Pegasus spyware aan onder meer Azerbaijan, Bangladesh, Egypte, Duitsland, El

Salvador, India, Mexico, Hongarije, Marokko, Polen, Saoedi-Arabië en Spanje.

Bij de screening van bedrijven onderzoekt de politie niet of de leverancier haar spyware ook heeft verkocht aan regimes die het hebben ingezet bij mensenrechtenschendingen.

Nationale veiligheid en spyware

Commerciële leveranciers van spyware hebben vaak nauwe banden met de nationale inlichtingendiensten in de landen waar zij zijn gevestigd. De belangen van deze buitenlandse inlichtingendiensten komen vanzelfsprekend vaak niet overeen met Nederlandse belangen. Sprekend voorbeeld is natuurlijk het afluisterschandaal rond de Amerikaanse inlichtingendienst NSA in Europese landen. Met het gebruik van spyware van controversiële bedrijven zetten Nederlandse opsporings- en inlichtingendiensten echter de deur zelf open voor spionage door buitenlandse mogendheden.

Een recent voorbeeld is de Israëlische NSO Group, die de afgelopen jaren regelmatig in opspraak is geweest. NSO heeft connecties met de militaire inlichtingendienst van het Israëlische leger en andere Israëlische inlichtingendiensten. Veel werknemers van het bedrijf zijn voormalig werknemers van geheime diensten van het land, zoals de bekende eenheid 8200 van de IDF (Israëli Defense Force). De Israëlische overheid lijkt de spyware Pegasus van de NSO ook zelf bij haar diplomatieke betrekkingen in de wereld te gebruiken. In november 2021 plaatste de Amerikaanse regering NSO op een zwarte lijst vanwege ‘het uitvoeren van activiteiten die in strijd zijn met de nationale veiligheid of de belangen van het buitenlandse beleid’.

Bij de screening van bedrijven worden eventuele banden van de leverancier met buitenlandse inlichtingendiensten en potentiële gevaren voor de nationale veiligheid echter niet meegewogen. Ditzelfde geldt de veiligheid van bondgenoten en de NAVO (Noord-Atlantische Verdragsorganisatie). Niet alleen de aanschaf van spyware door bijvoorbeeld Nederland is een veiligheidsprobleem, ook de algehele export van spyware van deze bedrijven.

In 2017 faciliteerde de Nederlandse overheid bijvoorbeeld de vestiging van het Zuid-Afrikaanse VASTech in Nederland. Niet alleen heeft dit bedrijf nauwe banden met de Zuid-Afrikaanse inlichtingendiensten, haar exportbeleid staat haaks op Nederlandse belangen. Het bedrijf werd in een rapport van de Amerikaanse denktank *Atlantic Council* uit 2021 genoemd als een van de bedrijven die haar producten levert aan vijanden van de Verenigde Staten en de NAVO. Het rapport '*Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets'* presenteert een lijst van spyware bedrijven die hun tools ook verkopen aan landen die niet Nederlands of Europees gezind zijn.

De Atlantic Council schrijft: *"75 percent of companies likely selling interception/intrusion technologies have marketed these capabilities to governments outside their home continent. Five irresponsible proliferators—BTT, Cellebrite, Micro Systemation AB, Verint, and Vastech— have marketed their capabilities to US/NATO adversaries in the last ten years"*.

De Nederlandse politie heeft lange tijd afluisterapparatuur van Verint afgenomen. Nog steeds houden medewerkers van het bedrijf afluistercentrales met Verint programmatuur draaiende. Het bedrijf, tegenwoordig opererend onder de naam Cognyte, heeft ook een Nederlandse vestiging.

VASTech handelt niet alleen niet in overeenstemming met de Nederlandse nationale veiligheid, het bedrijf leverde in het verleden ook aan bijvoorbeeld Zimbabwe, Syrië en Libië, waar haar producten werden gebruikt bij mensenrechtenschendingen. Het is niet bekend of de Nederlandse overheid producten van VASTech heeft afgenomen. In antwoord op Woo-verzoeken van Buro Jansen & Janssen hebben verschillende Nederlandse overheidsinstanties hierover tot op heden geen informatie openbaar gemaakt.

Spyware industrie en strafbare feiten

Bij de screening van leveranciers van spyware wordt dus niet gekeken naar hun betrokkenheid bij mensenrechtenschendingen en de impact van de bedrijfsactiviteiten op de nationale veiligheid. Ook wordt geen onderzoek gedaan naar het belastingbeleid en exportbeleid van bedrijven, en vindt geen antecedentenonderzoek plaats naar mogelijke strafrechtelijke vervolging van functionarissen van bedrijven en tussenhandelaren.

Hoewel de wet dit niet voorschrijft behoren politie en justitie in een rechtstaat met betrouwbare bedrijven samen te werken, helemaal met het oog op een zuiver openbaar bestuur en een eerlijke rechtspleging.

Bij producenten van spyware is waakzaamheid ten aanzien van de overtreding van exportregels, corruptie, witwassen, belastingfraude echter op zijn plaats, aangezien zij vaak een netwerk van vestigingen en bedrijven hebben opgericht. Hiermee kunnen exportbeperkingen omzeild worden en kan bijvoorbeeld de mensenrechtentoets in het exportcontrolebeleid van het land worden genegeerd. Daarnaast hebben veel spyware bedrijven ook vestigingen in belastingparadijzen en maken gebruik van offshore accounts, hetgeen belastingontduiking en mogelijk witwassen faciliteert.

Gamma Group heeft een groot netwerk van bedrijven die soms op naam staan van oprichter Louthean Nelson en soms op naam van anderen. Het netwerk omvat bedrijven in ten minste negen landen (Engeland, Duitsland, Zwitserland, Bulgarije, Singapore, Maleisië en de

drie bekende belastingparadijzen Cyprus, Maagdeneilanden en Libanon). De Nederlandse politie heeft FinFisher spyware gekocht van Gamma Group, maar het is niet bekend aan welk bedrijf Nederland heeft betaald. Mogelijk aan FinFisher GmbH in Duitsland. In antwoord op Woo-verzoeken van Buro Jansen & Janssen wordt hierover geen informatie openbaar gemaakt.

Ook de NSO Group bestaat uit een groot netwerk van bedrijven, met vestigingen in onder andere Israël, Bulgarije, Verenigd Koninkrijk, Verenigde Staten, Nederland, Luxemburg en de belastingparadijzen Cyprus en Maagdeneilanden.

De netwerkstructuur maakt handel via criminele tussenhandelaren mogelijk. Dit was bijvoorbeeld het geval bij de levering van spyware aan Bangladesh door de Israëlische spyware producent PicSix. *Al Jazeera* onthulde in 2022 overheidsdocumenten die aantonen dat het bedrijf spyware via Hongarije en Thailand aan een voor moord veroordeeld lid van een criminele organisatie in Bangladesh leverde. De persoon trad als tussenpersoon op voor de Directorate General of Forces Intelligence (DGFI), de militaire inlichtingendienst van Bangladesh.

Bij de screening van leveranciers van spyware wordt door de Nederlandse overheid echter niet gekeken naar mogelijke veroordelingen van personen die actief zijn in de industrie.

Dit is bevreemdend, zeker daar Nederland in het verleden spyware heeft gekocht van DigiTask, een bedrijf met een verleden van corruptie. De voormalig directeur van het bedrijf Hans-Hermann Reuter werd begin deze eeuw in Duitsland veroordeeld tot een gevangenisstraf voor het betalen van steekpenningen. Voor de Nederlandse politie vormde dit geen enkel beletsel voor het aanschaffen van de spyware van DigiTask.

Ook de oprichter van Gamma Group Louthean Nelson is betrokken bij een bedrijf dat vervolgd is voor corruptie. Het Engelse bedrijf CBRN Team (CBRN staat voor Chemical, biological, radiological and nuclear) van Niels Tobiasen begon in 2004 met de levering van CBRN threat

detection equipment aan Oeganda. In 2008 werd Tobiasen veroordeeld tot een jaar gevangenisstraf voor het betalen van steekpenningen aan Oegandese overheidsfunctionarissen. Nelson was destijds directeur van het bedrijf. Welke rol hij speelde is niet duidelijk ook omdat hijzelf zegt dat Gamma Group in 2005 een bedrijf heeft opgezet gespecialiseerd in *'CBRN and VIP security'*. Nelson is niet vervolgd in de corruptiezaak rond Tobiasen.

Slachtoffers van de FinFisher spyware en Ngo's zijn verschillende rechtszaken gestart over de handelswijze van het bedrijf, zowel tegen het bedrijf zelf als tegen overheden die de spyware hebben gebruikt. Deze zijn tot op heden niet succesvol geweest. In 2019 deed een aantal Ngo's aangifte tegen onder andere FinFisher GmbH van het Gamma Group netwerk en directieleden van de diverse bedrijven vanwege de illegale export van spyware naar Turkije. De Duitse politie deed vervolgens invallen in bedrijfspanden van het netwerk. In februari 2022 werd FinFisher failliet verklaard en is er een curator aangesteld. Het valt moeilijk vast te stellen of de bedrijfsactiviteiten daadwerkelijk zijn gestopt, omdat het netwerk van Gamma Group bestaat uit ondernemingen over de gehele wereld.

Ook tegen de NSO Group en overheden zijn rechtszaken gestart door slachtoffers van onder andere de spyware Pegasus van het bedrijf. Twee procedures in de Verenigde Staten springen in het oog. Het technologiebedrijf Apple eiste in 2021 dat NSO een permanent verbod krijgt op het gebruik van haar hardware, software en services. Meta, eigenaar van WhatsApp en Facebook, beschuldigde de afgelopen jaren in verschillende rechtszaken sinds 2019 NSO van onder meer het sturen van spyware naar meer dan duizend smartphones en andere apparatuur en hiermee het overtreden van de *'Computer Fraud and Abuse Act'* en de *'California Comprehensive Data Access and Fraud Act'.* Het gaat hierbij niet alleen om het verhalen van schade op de NSO, maar ook om strafbare feiten.

Al met al de is het duidelijk dat screening van de bedrijven, waarvan door de Nederlandse overheid spyware wordt aangekocht, zeer beperkt is. Veel relevante aspecten van de cybersurveillance industrie blijven buiten beschouwing. De AIVD en de politie verrichten

nauwelijks onderzoek en er wordt volledig vertrouwd op de verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes. De Inspectie Justitie en Veiligheid plaatst in haar toezichthoudende rol geen kritische kanttekeningen bij de screening.

'Black box' en de betrouwbaarheid van verkregen bewijs

De betrouwbaarheid van het verkregen bewijs staat op het spel bij de inzet van spyware. De politie heeft namelijk weinig inzicht in de werking van de tools, de wijze waarop een computer of smartphone wordt binnengedrongen, en hoe gegevens worden verzameld en bewijs wordt verkregen. Leveranciers van de spyware, en mogelijk derden, kunnen toegang verkrijgen tot de gegevensdragers van de verdachte, de spyware en de servers waarop de gegevens worden bewaard.

De Inspectie Justitie en Veiligheid onderkent dit en noemt, net als de politie, de commerciële software daarom een 'black box'. De Inspectie schrijft in het verslag over 2021: *"Net als in 2020 heeft de politie in het merendeel van de zaken gebruik gemaakt van commerciële software. Voor zowel de politie als de Inspectie is deze software een 'black box'. (...) Het kenmerk van een 'black-box' is dat de resultaten zichtbaar zijn maar voor de gebruiker niet bekend is hoe de software precies werkt."*

De leverancier heeft toegang tot de servers en kan in principe gegevens wijzigen, verwijderen en toevoegen. De Inspectie schrijft dan ook: *"De leverancier van het technisch hulpmiddel heeft de servers die de politie hiervoor gebruikt in technisch beheer en kan hier op afstand op inloggen om beheer- en supportwerkzaamheden uit te voeren. Werkzaamheden die de leverancier uitvoert, kunnen, mogelijk zelfs tijdens uitvoering van een bevel, gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel."*

De producenten van spyware hebben onbeperkt toegang tot de spyware en de servers om die te onderhouden, updates te draaien en andere handelingen te verrichten. Ook tijdens het doorzoeken van de

smartphones of laptop van een verdachte en het verzamelen van bewijs door de politie. De Inspectie constateert dat de producent het verzamelde bewijsmateriaal kan inzien: *"De leverancier kan daarbij mogelijk ook toegang verkrijgen tot de tijdens een inzet met deze software verkregen gegevens."*

De toegang van leveranciers is voor de politie niet te controleren, ondanks een aanvulling aan het contract met het bedrijf: *"Ondanks een addendum bij de contracten met de softwareleveranciers, kan de politie niet "technisch en controleerbaar afdwingen wat de leverancier van deze software precies op welk moment doet."*

De politie werkt dus samen met een bedrijf dat haar spyware levert voor het binnendringen van gegevensdragers en het verzamelen van bewijs over strafbare feiten van een verdachte. Tegelijkertijd heeft dat bedrijf zelf ook de mogelijkheid om die spyware voor dezelfde doeleinden te gebruiken. Dit is voor de politie niet te controleren.

De politie kan niet garanderen dat alleen zij toegang heeft tot de gegevensdragers van de verdachte. Volgens de Inspectie kan de politie *"door het 'black box' karakter van het technisch hulpmiddel (...) de toegang door de leverancier (...) niet technisch controleren of beperken"* en kan *"hierdoor niet gegarandeerd worden dat bij het gebruik van het technisch hulpmiddel uitsluitend verbindingen tot stand gebracht worden tussen het geautomatiseerde werk en de servers van de politie."*

Mogelijke manipulatie betreft niet alleen de toegang van de producent tot de servers, maar ook de opslag van bewijsmateriaal op die servers. De politie bewaart bewijsmateriaal namelijk op de servers van de spyware, waartoe dus ook de leveranciers toegang hebben. De Inspectie constateert *"dat de door de politie verzamelde gegevens geruime tijd zijn opgeslagen in het technisch hulpmiddel waar ook de leverancier op afstand toegang toe heeft."*

Het betekent dat de door de politie verzamelde bewijslast veranderd of vernietigd kan worden, en gegevens kunnen worden toegevoegd aan de bewijslast. De Inspectie signaleert deze problemen rond de 'black

box’ en de betrouwbaarheid van verkregen bewijsmateriaal niet alleen in haar verslag over 2021, maar ook al in haar eerdere verslagen van over 2019 en 2020.

De kritiek is echter niet nieuw. Bij de DigiTask tool is deze al eerder benoemd. In 2011 analyseerde maakte het Duitse hackerscollectief Chaos Computer Club (CCC) een uitgebreide analyse van de spyware van DigiTask. De CCC constateerde dat de producent toegang had tot de gegevensdragers van de verdachte en tot servers waarop het bewijs werd verzameld, en gegevens konden veranderen, verwijderen en toevoegen. De conclusies van de CCC werden bevestigd door onderzoeken van de Duitse databeschermingsautoriteiten.

Bij de onderzochte DigiTask tool ging het zelfs nog verder. Omdat de communicatie met de gegevensdragers en de servers niet beveiligd was konden - buiten de producent en de opsporingsdiensten die de spyware gebruiken - ook anderen toegang verkrijgen.

De Inspectie gaat in haar verslagen niet in op de mogelijke toegang van derden bij door de Nederlandse politie gebruikte spyware.

Geen inzicht in broncode en backdoor

Om inzicht te krijgen in de precieze werking van spyware en het functioneren van een tool is toegang tot de broncode noodzakelijk. Zonder toegang tot die broncode valt niet vast te stellen of er bijvoorbeeld sprake is van zwakheden in de programmatuur, welke mogelijkheden de spyware biedt en of die wel wettelijk zijn toegestaan, en of er bewust manieren zijn ingebouwd in de spyware om ongezien toegang te krijgen tot het programma, haar gebruikers en haar target (zogenaamde backdoors).

Een backdoor in de programmatuur geeft de leverancier van de spyware dus de mogelijkheid mee te kijken wanneer de spyware bij een verdachte op een computer, laptop of smartphone is geplaatst. Uit het onderzoek van de CCC naar DigiTask bleek dat als gevolg van de onbeveiligde communicatie van het programma zelfs derden gebruik kunnen maken van de spyware en toegang kunnen krijgen tot de programmatuur. Niet alleen bij de spyware van DigiTask kunnen echter vraagtekens worden gezet bij de veiligheid en betrouwbaarheid van de tool.

Nadat het Italiaanse Hacking Team in 2015 werd gehackt werd een deel van de broncode openbaar. Het bedrijf kreeg vervolgens vragen over het bestaan van een backdoor in haar tools RCS Vinci en Galileo, maar ontkende dit. De Engelse onderzoeker Joseph Greenwood, verbonden aan het Cloud beveiligingsbedrijf 4armed, oordeelde na bestudering van het openbare deel van de broncode dat de spyware van Hacking Team misschien geen backdoor heeft, maar wel een soort kill switch. De gehele broncode was niet openbaar, dus Greenwood kon geen definitief uitsluitsel geven over het al dan niet bestaan van een backdoor.

De kill switch geeft het Italiaanse bedrijf de mogelijkheid om zich toegang te verschaffen tot de verzamelde gegevens en deze te vernietigen. Hiermee kan het bedrijf sporen wissen die kunnen wijzen op misbruik van de spyware door klanten van Hacking Team.

Een backdoor en een kill switch maken het ook mogelijk om op afstand een gegevensdrager van een verdachte binnen te dringen, programmatuur aan te passen, gegevens te verwijderen en toe te voegen. De betrouwbaarheid van door middel van de inzet van spyware verkregen bewijs is hiermee in het geding.

Een backdoor en een kill switch kunnen niet alleen door de leverancier van de spyware worden gebruikt. Ook derden kunnen gebruik maken van een backdoor, bijvoorbeeld buitenlandse inlichtingendiensten. Dit is een reëel risico, aangezien producten van spyware vaak nauwe banden onderhouden met de inlichtingendiensten in het land van vestiging.

In 2022 verklaarde een engineer van het Franse bedrijf Nexa Technologies (voorheen Amesys), dat ook nauwe contacten onderhoudt met de Franse inlichtingendiensten, tegenover de website *Intelligence Online* dat Nexa spyware verkoopt aan Libië, waarbij een backdoor is ingebouwd. Deze backdoor zou gebruikt worden door de Franse inlichtingendienst DGSE. In Frankrijk loopt een justitieel onderzoek naar Nexa Technologies in verband met de verkoop van spyware aan Libië en Egypte en daaraan gekoppelde martelingen en verdwijningen. In het kader van het justitiële onderzoek zijn volgens *Intelligence Online* drie functionarissen van de inlichtingendienst door de Franse justitie gehoord over de backdoor en het gebruik ervan door de DGSE.

Ook bestaan er veel geruchten over het bestaan van een backdoor in de Pegasus spyware van de Israëlische NSO Group. Het is op dit moment echter niet bekend of er een backdoor in de programmatuur is ingebouwd.

Backdoors in software zijn echter niet alleen voorbehouden aan spyware. Ook bij veel andere programmatuur kan er sprake zijn van een ingebouwde verhulde toegang. Zo waarschuwde de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in 2020, tijdens de ontwikkeling van de Nederlandse corona-app, voor samenwerking met een Israëlisch bedrijf in verband met het bestaan van een mogelijke backdoor. De NCTV heeft ten aanzien van de aankoop van spyware nimmer een dergelijke waarschuwing afgegeven. Het is onduidelijk waarom niet.

De Inspectie Justitie en Veiligheid gaat in haar rapporten niet in op de mogelijke aanwezigheid van backdoors in door de Nederlandse politie gebruikte spyware. De Inspectie besteedt evenmin aandacht aan de relatie tussen leveranciers van spyware en buitenlandse inlichtingendiensten, hoewel het handelen van buitenlandse inlichtingendiensten en buitenlandse commerciële spyware producenten niet altijd in overeenstemming is met de Nederlandse belangen.

Technische infrastructuur en bewijslogging

Hoewel de Inspectie Justitie en Veiligheid niet ingaat op de mogelijke aanwezigheid van backdoors en de relatie van spyware leveranciers met inlichtingendiensten, signaleert het dus wel problemen rond het 'black box' karakter van de spyware en de betrouwbaarheid van de met spyware verkregen gegevens en bewijsmateriaal. Tevens trekt de Inspectie in twijfel of de verkregen gegevens op een beveiligde plek worden opgeslagen, omdat de gegevens in de spyware en/of op de servers van de producent worden opgeslagen.

De Inspectie vraagt zich af of de politie haar technische infrastructuur op orde heeft en schrijft in het verslag over 2021 dat de politie de reikwijdte van de 'technische infrastructuur' nog niet had bepaald: *"De Inspectie heeft in 2020 geconstateerd dat de politie nog niet bepaald had wat de reikwijdte van de technische infrastructuur is, waardoor de Inspectie niet met zekerheid kon vaststellen of alle bewijslogging wel op de juiste plek en op betrouwbare wijze is vastgelegd. … Dit proces was in 2021 nog niet afgerond."*

Bewijslogging is van belang om te bepalen of bewijs op correcte wijze is verkregen. De technische infrastructuur is echter nauw verbonden met de leverancier van de spyware: *"De Inspectie stelt echter vast dat een gedeelte van de bewijslogging daarnaast ook is opgeslagen op locaties die door DIGIT niet tot de technische infrastructuur gerekend worden. … Deze tijdelijke opslag van een deel van de bewijslogging vond plaats op servers die technisch worden beheerd door een externe leverancier."*

De Inspectie schrijft over 2020 daarom: *"De leverancier kan daarmee mogelijk ook toegang verkrijgen tot de bewijslogging die met dit middel is verkregen."* Ook zet de Inspectie vraagtekens bij het forensisch vastleggen van het bewijsmateriaal, van belang om de rechtmatigheid van het bewijs te waarborgen. De Inspectie constateert dat een "*uitwerking van hoe het technisch team gegevens kan selecteren op basis van een forensische kopie niet voorhanden is."*

Het is dus de vraag is of het hacken formeel belastend bewijs kan leveren in een strafzaak. In haar verslag over 2021 schrijft de Inspectie zelfs dat *"het voor de Inspectie niet is vast te stellen welke gegevens precies zijn overgedragen aan de tactische teams omdat hier niet altijd logging en verslaglegging van is."* En voegt hieraan toe dat een *"deel van deze selecties is gemaakt op basis van een forensische kopie uit de technische infrastructuur, zodat de integriteit van de brongegevens maximaal is gewaarborgd. Enkele malen is bij het maken van tussentijdse selecties echter geen gebruik gemaakt van een forensische kopie uit de technische infrastructuur."*

Maximale waarborging lijkt echter niet te betekenen dat de politie kan vaststellen of er niet met het bewijsmateriaal is geknoeid. Soms is er namelijk niet gebruik gemaakt van een forensische kopie. De Inspectie concludeert over 2020 dan ook dat *"risico's niet kunnen worden uitgesloten voor wat betreft de betrouwbaarheid van met de hackbevoegdheid verkregen bewijs en de privacy van de betrokkenen."*

De Inspectie werpt dus met zoveel woorden de vraag op of de met behulp van spyware verkregen gegevens zijn te gebruiken als bewijs in een rechtszaak.

Keuring van technische hulpmiddelen

Om de integriteit van de technische hulpmiddelen te waarborgen worden de hacktools van de fabrikanten gekeurd. Keuring van opsporingshulpmiddelen is onderdeel van de rechtspleging. Zonder keuring en certificering kan in de rechtszaal de waarde van verkregen bewijs niet worden vastgesteld. De keuring van spyware is echter zeer beperkt, mede daar leveranciers van de spyware onvoldoende meewerken.

Van 11 maart 2019 tot eind 2020 werden de keuringen uitgevoerd door de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO). Sinds 2021 wordt de keuring uitgevoerd door de landelijke eenheid van de Nationale Politie, hetgeen voor 2019 ook het geval was.

Volgens de cijfers van de Inspectie is in 2019 een technisch hulpmiddel gekeurd, zijn er in 2020 zes keuringen uitgevoerd (op drie hulpmiddelen), en in 2021 zeven keuringen (waarbij niet wordt vermeld om hoeveel hulpmiddelen het gaat). Er worden soms meerdere keuringen op een technisch hulpmiddel uitgevoerd, wanneer er sprake is van verschillende versies van het middel.

Volgens de Inspectie worden de technische hulpmiddelen regelmatig aangepast en zijn er dus vele versies van in omloop. De Inspectie geeft niet aan hoe vaak dit het geval is, de politie en de producent van de spyware vermelden deze informatie ook niet. Het hulpmiddel uit 2019 is afgekeurd, in 2020 en 2021 zijn twee hulpmiddelen afgekeurd. Uit de rapporten van de Inspectie valt echter niet op te maken hoeveel hulpmiddelen er uiteindelijk zijn goedgekeurd en of het hier om versies gaat hulpmiddel die eerder zijn afgekeurd.

De keuring vindt plaats volgens een geheim keuringsprotocol. De Inspectie oordeelt dat de keuringen conform het protocol zijn uitgevoerd, maar tekent wel aan dat keuringsdienst slechts uit een persoon bestaat. Uit de rapporten van de Inspectie wordt niet duidelijk wat de keuring precies omvat. De Inspectie geeft geen uitgebreide omschrijving van de keuring, maar merkt wel op dat *"commerciële binnendringsoftware doorgaans wordt geleverd met een eigen technisch hulpmiddel dat onlosmakelijk is verbonden met de binnendringsoftware."*

De politie neemt dus zowel de tool voor het binnendringen in een computer, laptop of een smartphone, als de tool voor het verrichten van onderzoekshandelingen aan die gegevensdragers, van dezelfde leverancier af. De Inspectie licht niet toe wat voor consequenties dit heeft voor de keuring van beide.

Volgens de Inspectie is in 2021 in 23 van de 28 onderzoeken commerciële binnendringingssoftware gebruikt voor het binnendringen. Daarnaast zijn in 15 van de 28 zaken onderzoekshandelingen verricht met een technisch hulpmiddel. Zowel de werking van binnendringingssoftware als de programmatuur voor het doorzoeken van de gegevensdragers zijn voor de politie onduidelijk, maar de binnendringingssoftware wordt niet aangemerkt als technisch hulpmiddel. Alleen als het over onderzoekshandelingen gaat spreekt de Inspectie over "een 'black box' voor de politie."

In een e-mail aan Buro Jansen & Janssen verduidelijkt de Inspectie het onderscheid: *"Er kan op basis van het verslag en de deductie naar aanleiding van de genoemde aantallen niet geconcludeerd worden dat in 8 zaken commerciële binnendringsoftware is gebruikt waar geen sprake is van een 'black box'."* De Inspectie verwijst met de acht zaken naar de zaken die overblijven van de 23 zaken waarbij binnendringingssoftware is gebruikt (23 min 15).

Volgens de Inspectie is er dus alleen sprake van een technisch hulpmiddel wanneer de politie onderzoekshandelingen verricht. Het laat per mail weten: *"Wanneer gesproken wordt over een technisch hulpmiddel dan heeft dat alleen betrekking op het verrichten van*

onderzoekshandelingen." Dit zou betekenen dat in de acht overgebleven zaken alleen op de gegevensdragers is binnengedrongen, zonder dat er onderzoekshandelingen zijn verricht. Wat er in deze situaties is gebeurd laat de Inspectie onbesproken.

Het antwoord van de Inspectie is niet erg verhelderend. Veel spyware tools zijn namelijk binnendringingssoftware en onderzoeker in een. Dit geldt bijvoorbeeld voor de tools van de NSO Group. Anderzijds is het vreemd waarom bijvoorbeeld een tool om binnen te dringen in een computer of laptop zoals bijvoorbeeld het Israëlische Kailax niet gezien wordt als technisch hulpmiddel en daarmee als mogelijke 'black box'.

Kailax Unlocker ontgrendelt Windows computers via connectie met servers van het bedrijf. Het lijkt erop dat de politie, die de Unlocker waarschijnlijk heeft aangeschaft, geen kennis heeft van de werking van de tool en de rol die Kailax servers spelen bij het binnendringen zodat er wel degelijk sprake is van een 'black box' al zou er geen sprake zijn van onderzoekshandelingen. Dit laatste kan de Inspectie niet vaststellen, want of het wordt niet gezien als technisch hulpmiddelen en niet gecontroleerd of het is een 'black box' en kan niet worden gecontroleerd. In haar rapportage verwijst de Inspectie daar dan ook indirect naar.

Het kan daarom worden betwijfeld in hoeverre technische hulpmiddelen afdoende gekeurd worden. De integriteit van de apparatuur en software kan niet volledig worden onderzocht wanneer de keuringscommissie geen toegang heeft tot de broncode en de producent geen inzicht geeft in het functioneren van de spyware.

De Inspectie is dan ook kritisch over de reikwijdte van de keuring: *"De Inspectie voorziet dat keuring wordt bemoeilijkt doordat de leveranciers waarschijnlijk geen (volledige) inzage geven in de werking van deze software."*

Daarnaast worden niet alle aspecten van het functioneren van de software gekeurd, omdat een deel bedrijfsgeheimen zijn. Zo maakt *"de wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van*

het omzeilen van de beveiliging van een geautomatiseerd werk, geen deel uit van het keuringsproces."

De keuring lijkt vooral gericht om vast te stellen of het technische hulpmiddel doet wat het doet in een testomgeving. De vergelijking met het emissieschandaal in de auto-industrie dringt zich op. Onder ideale omstandigheden, gecontroleerd door de producenten is alles volgens de regels. Daarbuiten niet.

Justitie en politie vinden keuring niet nodig

De keuring beoogt de integriteit van spyware vast te stellen, maar kent dus allerlei tekortkomingen. Het blijkt bovendien dat de politie, Openbaar Ministerie en het Ministerie van Justitie en Veiligheid weinig belang hechten aan de keuringen. Technische hulpmiddelen worden namelijk vaak ingezet zonder keuring vooraf te zijn gekeurd.

De wet schrijft voor dat technische hulpmiddelen vooraf gekeurd worden, maar dat hier vanaf kan worden geweken wanneer een aantal waarborgen zijn getroffen. *"In dat geval vermeldt de officier van justitie in de processtukken dat is afgezien van keuring en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen,"* aldus de Inspectie Justitie en Veiligheid.

De Inspectie verduidelijkt niet op grond van welke overwegingen technische hulpmiddelen niet voorafgaand aan de inzet gekeurd worden, en welke waarborgen er zijn getroffen. Uit de cijfers van de Inspectie wordt duidelijk dat er nauwelijks vooraf goedgekeurde technische hulpmiddelen worden ingezet, en hulpmiddelen vaak ook niet achteraf worden gekeurd.

In 2019 zijn technische hulpmiddelen altijd (11 keer in het kader van 8 onderzoeken) ingezet zonder vooraf te zijn gekeurd. Het middel dat achteraf werd gekeurd, is afgekeurd. In 2020 is in het kader van 14 onderzoeken tien keer commerciële spyware ingezet, elf keer een niet

gekeurd technisch hulpmiddel en een keer een gekeurd hulpmiddel (een hulpmiddel kan meerdere keren worden ingezet). Twee hulpmiddelen zijn goedgekeurd. Onduidelijk is of dit aantal inclusief het vooraf gekeurde hulpmiddel is.

In 2021 is in het kader van 28 onderzoeken 23 keer commerciële spyware ingezet, 24 keer een niet gekeurd technisch hulpmiddel en twee keer een gekeurd hulpmiddel. De Inspectie schrijft dat *"in 23 zaken door de officier van justitie is bepaald dat het onderzoeksbelang dringend vordert dat een niet vooraf gekeurd technisch hulpmiddel wordt ingezet."* Vijf hulpmiddelen zijn goedgekeurd. Onduidelijk is of dit aantal inclusief of exclusief de twee vooraf goedgekeurde hulpmiddelen is.

Spyware vaker ingezet, bewijs niet ingebracht in rechtszaken

De politie maakt de afgelopen jaren steeds vaker gebruik van de hackbevoegdheid.

Uit de cijfers van de Inspectie is over de periode van drie inspectieverslagen van 1 maart 2019 tot en met 31 december 2021 blijkt er in 50 zaken spyware is ingezet, jaarlijks gaat het om een verdubbeling: in 2019 werd in 8 onderzoeken spyware ingezet, in 2020 in 14 onderzoeken en in 2021 in 28 onderzoeken.

Per onderzoek kunnen echter meerdere bevelen worden afgegeven, veelal voor het hacken van verschillende gegevensdragers van mogelijk meerdere personen. Volgens de Inspectie werden in 2019 17 bevelen afgegeven in 8 onderzoeken, zowel initiële als aanvullende bevelen. De Inspectie vermeldt in haar verslagen niet hoeveel bevelen er in 2020 en 2021 zijn afgegeven.

Het ontbreken van recente cijfers over het aantal bevelen belemmert een volledig inzicht in de toename van het gebruik van de hackbevoegdheid. Uitgaande van het afgeven van twee bevelen per onderzoek in 2019, gaat het in 2020 om dertig bevelen en in 2021

mogelijk om zestig afgegeven bevelen. In een tijdspanne van drie jaar gaat het dus mogelijk om een totaal van rond de honderd bevelen.

Het is bovendien de vraag of de door de Inspectie genoemde cijfers volledig zijn. De politie maakt namelijk ook gebruik van handmatig hacken, met behulp van zowel commerciële als niet-commerciële spyware. Tussen de politie en de Inspectie bestaat een meningsverschil over handmatig hacken: volgens de politie valt het niet onder de inzet van technische hulpmiddelen, maar volgens de Inspectie wel. Uit de rapporten van de Inspectie wordt echter niet duidelijk of de genoemde aantallen inzetten van technische hulpmiddelen ook het aantal gevallen omvat waarin handmatig is gehackt.

Hoewel de politie de afgelopen jaren steeds vaker gebruik maakt van spyware, blijkt dat door middel van spyware verkregen gegevens niet of nauwelijks als bewijs worden gebruikt in rechtszaken. Over 2019 schrijft de Inspectie dat het aantal *"zaken waarin met de bevoegdheid verkregen gegevens als bewijs zijn ingebracht in een strafzaak"* nul is.

In de verslagen over 2020 en 2021 geeft de Inspectie niet meer aan in hoeveel gevallen met spyware verkregen gegevens als bewijs is gebruikt in rechtszaken. De Inspectie licht niet toe waarom zij deze gegevens niet meer in haar rapporten opneemt.

Het is logisch om te veronderstellen dat ook in 2020 en 2021 door middel van spyware verkregen gegevens niet of nauwelijks als bewijs is ingebracht in rechtszaken. Alle relevante aspecten van de hackbevoegdheid, zoals bijvoorbeeld de bewijslogging, zijn in drie jaar niet wezenlijk veranderd.

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) publiceerde in 2022 het onderzoek *'De hackbevoegdheid in de praktijk'* naar de uitvoering van de hackbevoegdheid. Dit onderzoek bevestigt de veronderstelling over het niet inbrengen van gehackte gegevens in rechtszaken. Het WODC heeft in het kader van haar onderzoek 26 onderzoeken uit de periode 2019-2022 bestudeerd en constateert dat

de zittingsrechter het met de hackbevoegdheid verkregen bewijs in geen enkel geval inhoudelijk heeft behandeld.

Het WODC concludeert dat de vraag of door hack verkregen gegevens bijdragen aan bewijsvoering niet beantwoord kan worden. Er kunnen "*geen uitspraken worden gedaan over de waardering van de nieuwe bevoegdheid als bewijsmiddel: dragen de middels de hackbevoegdheid gegevens bij aan de bewijsvoering in een strafzaak?"*

Ook de vaststellingen van de Inspectie over de bewijslogging duiden erop dat door middel van spyware verkregen gegevens niet of nauwelijks als bewijs worden gebruikt in rechtszaken. Bewijslogging is van belang voor gebruik van de verkregen gegevens in strafzaken, het bewijs moet forensisch worden vastgelegd door het DIGIT-team.

De bewijslogging lijkt op veel punten niet volgens de regels te verlopen. De Inspectie constateert: *"In 2021 zijn in 15 zaken onderzoekshandelingen verricht door medewerkers van DIGIT die niet vooraf formeel aangewezen zijn als lid of deelnemer van het technisch team"*.

Ook in haar verslag over 2020 concludeerde de Inspectie al dat de bewijslogging niet voldeed en dat de Inspectie *"niet met zekerheid (kan) vaststellen of al deze bewijslogging wel op de juiste plek en op betrouwbare wijze is vastgelegd."*

De Inspectie constateert met zoveel woorden dat het met behulp van spyware verkregen bewijs niet rechtmatig is verkregen. En dus niet als bewijsmateriaal bij een rechtszaak kan worden ingebracht.

Hackbevoegdheid ingezet bij ernstige criminaliteit?

Volgens de Wet Computercriminaliteit III mag de hackbevoegdheid alleen worden ingezet bij onderzoeken naar terrorisme en ernstige criminaliteit. De Inspectie Justitie en Veiligheid schrijft in 2020 dan ook: *"De bevoegdheid mag uitsluitend worden ingezet in geval van*

verdenking van een ernstig of specifiek aangewezen misdrijf, georganiseerde criminaliteit of aanwijzingen van een terroristisch misdrijf."

Volgens de Minister van Veiligheid en Justitie gebeurt dit in de praktijk. De Minister stelt in beantwoording van Kamervragen in december 2022: *"In opsporingsonderzoeken waarin binnendringingssoftware is ingezet, was hoofdzakelijk sprake van een verdenking van een combinatie van strafbare feiten. Het betrof een combinatie van (...) artikelen uit het wetboek van strafrecht, de Opiumwet (Ow), de Wet Wapens en Munitie (Wwm), de wet op het financieel toezicht (Wft) en de Wet economische delicten (WED)."*

De Inspectie Justitie en Veiligheid schrijft in haar verslag over 2019 dat *"de inzet van de bevoegdheid is beperkt tot de limitatief omschreven doelen"* en over 2020 dat *"van een ongecontroleerde inzet op grote schaal geen sprake (is)."*

De beweringen van de Inspectie vallen echter moeilijk te beoordelen. De vraag in hoeverre spyware alleen wordt ingezet bij onderzoeken naar terrorisme en ernstige criminaliteit kan namelijk alleen beantwoord worden met openbare informatie over het aantal en type onderzoeken waarbij spyware is ingezet, de aard van de strafbare feiten, informatie over rechtszaken, het aantal zaken waarin dit tot een veroordeling heeft geleid, en de straf. In de verslagen van de Inspectie ontbreekt echter een dergelijk overzicht. Sterker nog, met spyware verkregen gegevens worden nauwelijks tot niet als bewijs gebruikt in rechtszaken.

Ook het WODC gaat slechts beperkt in op het type onderzoeken waarin de politie gebruik maakt van de hackbevoegdheid. De onderzoekers hebben 26 onderzoeken bekeken waarbij de hackbevoegdheid is gebruikt. Op basis hiervan schrijft het WODC dat de bevoegdheid *"vooral ingezet is in opsporingsonderzoeken naar zwaardere vormen van traditionele criminaliteit, zoals (poging tot) moord, zaken rondom verdovende middelen, valsheid in geschrifte, zeden, terrorisme en lidmaatschap van criminele organisatie."*

Ook het WODC laat dus veel onduidelijk. De formulering 'vooral bij zwaardere vormen van traditionele criminaliteit' betekent dat spyware ook bij minder zware vormen van criminaliteit kan worden ingezet. De term 'zwaardere vormen van traditionele criminaliteit' geeft bovendien geen goed inzicht in de ernst van de criminaliteit.

Het is dan ook niet opmerkelijk dat de politie zelden tot nooit ruchtbaarheid geeft aan de inzet van spyware en eventuele behaalde successen met de hackbevoegdheid. Door middel van hacken verkregen bewijs wordt toch niet voorgelegd aan de rechter. Wanneer dit mogelijk wel gebeurt is de kans aanzienlijk dat het niet gebruikt kan worden, omdat de bewijslogging niet in orde is en het bewijs niet op de juiste wijze is vastgelegd.

Als de Nationale Politie in juli 2022 een persbericht rondstuurt, waarin het vermeldt gebruik te hebben gemaakt van de hackbevoegdheid bij een onderzoek naar een verdachte van kindermisbruik, is het zaak op de hoede te zijn. Het persbericht lijkt bedoeld als legitimatie van de inzet van spyware, terrorisme en kindermisbruik worden vaker gebruikt voor de legitimatie van controversiële opsporingsmiddelen.

Het feit dat het zeldzaam is dat de politie persberichten uitbrengt over met behulp van spyware behaalde successen werpt, net als het niet voorleggen van door middel van de inzet van hacken verkregen bewijs aan de rechter, dan ook de vraag op in hoeverre de politie spyware alleen inzet bij verdenkingen van terrorisme en ernstige criminaliteit. En of het gebruik van de hackbevoegdheid een meerwaarde had ten opzichte van andere politiebevoegdheden en iets heeft opgeleverd.

De inzet van spyware is een zwaar middel. De proportionaliteit van de inzet van spyware valt met het ontbreken van transparante cijfers niet te beoordelen. Ook de subsidiariteit kan niet beoordeeld worden: kan het bewijs dat verkregen is of waarnaar gezocht wordt ook worden verkregen met minder ingrijpende middelen dan het gebruik van de hackbevoegdheid, bijvoorbeeld door middel van het plaatsen van een telefoontap, een huiszoeking, een verhoor, of het opvragen van gegevens bij bedrijven zoals Meta, eigenaar van Facebook en WhatsApp.

De Inspectie besteedt in haar rapporten zeer weinig aandacht aan de proportionaliteit, en geen enkele aandacht aan de subsidiariteit van de inzet van de hackbevoegdheid.

Dat is zorgwekkend. In een rechtsstaat moeten de proportionaliteit en subsidiariteit van de inzet van opsporingsmethodes en politiebevoegdheden uiteindelijk worden getoetst door de rechter. Hiervan is bij de toepassing van de hackbevoegdheid echter geen sprake. Met behulp van spyware verkregen gegevens worden immers nauwelijks tot niet als bewijs in rechtszaken ingebracht.

Welk doel dient de inzet van spyware dan?

Door middel van spyware verkregen gegevens blijken nauwelijks tot niet te worden gebruikt als bewijs in rechtszaken. Tegelijkertijd maakt de Nederlandse politie de afgelopen jaren steeds vaker gebruik van de hackbevoegdheid. De vraag is simpel: Waarom maakt de Nederlandse politie steeds meer gebruik van spyware, terwijl het niet tot bewijs in rechtszaken leidt?

Men zou verwachten dat deze vraag een belangrijk aandachtspunt is voor het toezicht op de uitvoering van de hackbevoegdheid. De vraag wordt door de Inspectie Justitie en Veiligheid in het geheel niet geadresseerd.

Het WODC maakt hier in haar evaluatierapport enige opmerkingen in 2022 over: Het *"blijkt dat bevoegdheid (..) tot nu toe vooral sturingsinformatie oplevert. De verzamelde gegevens leveren, in tegenstelling tot sommige verwachtingen, tot nog toe niet het bewijs op binnen een opsporingsonderzoek. Verder heeft een zittingsrechter, voor zover bekend, nog geen enkele inzet inhoudelijk behandeld."*

De passage is enigszins cryptisch geformuleerd. De term 'sturingsinformatie' is een gangbare term in de managementinformatie, maar is geen juridische term. Het roept echter

associaties op met andere onderdelen van de politiepraktijk, zoals het doen van een huiszoeking zonder huiszoekingsbevel, telefoontaps die niet in procesdossier terecht komen, informatie van informanten die niet aan de rechter wordt voorgelegd en de inzet van infiltranten. Het niet vermelden van het gebruik van dergelijke opsporingsmethoden staat een eerlijk proces in de weg.

Het heeft er alle schijn van dat de politie door middel van de inzet van spyware digitaal wil meekijken met verdachten, een soort digitale huiszoeking of observatie op last van een officier van justitie, maar zonder betrokkenheid van een rechtercommissaris en zonder waarborgen.

Dit beeld wordt bevestigd door de slordige omgang van het DIGIT-team van de politie met bewijslogging. Onzorgvuldige omgang met bewijslogging betekent dat bewijs niet rechtmatig is verkregen en dat verkregen gegevens niet kunnen worden gebruikt in rechtszaken. Het niet conform de procedures omgaan met bewijslogging kan simpelweg duiden op slordigheid van individuele politieambtenaren. Er is echter sprake van aanhoudende structurele slordigheid. Het bevestigt de indruk dat het de politie bij inzet van spyware niet per se gaat om het verkrijgen van bewijsmateriaal dat bij de rechtbank standhoudt. De politie is niet geïnteresseerd in het verkrijgen van bewijs maar alleen inlichtingen en daarom wordt er niet correct gelogd.

Gebruik voor oneigenlijke doeleinden?

Het is de wettelijke bedoeling van de inzet van spyware om bewijs te verkrijgen in onderzoek naar terrorisme en zware georganiseerde criminaliteit. Uit de rapporten van de Inspectie Justitie en Veiligheid wordt duidelijk dat hiervan in de praktijk weinig tot niets terecht komt. Door middel van spyware verkregen gegevens worden niet of nauwelijks gebruikt als bewijs in rechtszaken.

Er lijkt dus sprake van ‘function creep’: de politie gebruikt de hackbevoegdheid voor andere doeleinden dan waarvoor deze bedoeld

is. Het gaat niet om het rechtmatig verkrijgen van bewijs maar, om inkijkoperaties en het verzamelen van inlichtingen. Het gaat niet alleen om onderzoeken op verdenking van terrorisme en zware georganiseerde criminaliteit, maar het kan ook gaan om een verdenking van minder ernstige vormen van criminaliteit. En mogelijk om het hacken van advocaten, journalisten en activisten.

In het Europees Parlement is toenemende zorg over het gebruik van spyware voor andere doeleinden dan de bestrijding van terrorisme en ernstige criminaliteit. Het Europees Parlement bracht in november 2022 een voorlopig rapport uit over het gebruik van spyware in de landen van de Europese unie. In Spanje, Polen, Hongarije en Cyprus hebben overheden spyware ingezet voor het bespioneren van journalisten, politici, oppositieleden en leden van burgerrechtenbewegingen. Ook in Frankrijk en Griekenland waren er de afgelopen jaren vergelijkbare berichten.

De Minister van Veiligheid en Justitie werd in 2022 bevraagd of dergelijke praktijken, de inzet van hacksoftware tegen advocaten, protestgroepen zonder terroristisch oogmerk en/of politieke groepen, ook in Nederland plaatsvinden.

De Minister beantwoordt de Kamervragen in december 2022 noch ontkennend noch bevestigend en stelt dat er *"geen inzage (kan) worden gegeven tegen welke specifieke verdachten in opsporingsonderzoeken de bevoegdheid ex art. 126nba Sv is ingezet", dat "in het kader van opsporingsonderzoeken die door de politie worden uitgevoerd inzake een (mogelijke) strafrechtelijke vervolging door het openbaar ministerie kent de bijzondere opsporingsbevoegdheid van 126nba, 126uba en 126zpa geen uitzonderingen voor advocaten, protestgroepen, zonder terroristisch oogmerk en/of politieke groepen"* en vermeldt dat *"voor de inzet van bijzondere opsprongsbevoegdheden ten aanzien van journalisten en advocaten aanvullende waarborgen" gelden.*

De ontwikkelingen in Europa geven aanleiding tot zorg of spyware ook in Nederland wordt ingezet tegen journalisten en activisten. Met deze beantwoording neemt de Minister deze zorgen niet weg.