Politie Black Box

Buro Jansen & Janssen

Observant # 81, december 2023

Inhoudsopgave Observant #81 / december 2023

Politie Black Box

Voor u ligt Observant #81. Eigenlijk is deze nog niet helemaal af. Een onderzoek naar een Israëlisch bedrijf is nog niet geheel afgerond. Toch sturen we het rond, omdat dat onderzoek misschien ook wordt opgenomen in een andere observant die zich niet alleen richt op dat bedrijf, maar de gehele spyware industrie in Israël en haar vertakkingen. Vandaar deze iets gemankeerde observant al zijn de conclusies van het onderzoek naar spyware wel afgerond.

Die zijn te vinden in twee kortere artikelen. Een over de inzet van spyware voor inlichtingendoelen en inkijkoperaties en niet voor het verzamelen van bewijs. De ander over de controversiële bedrijven die niet door de overheid worden gescreend. De meeste artikelen staan al enige tijd op de website van Buro Jansen & Janssen.

1. De digitale inkijkoperaties van de Politie Black Box (samenvatting I). Nederlandse politie gebruikt spyware voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen, niet voor het verzamelen van bewijs.

2. Nederlandse politie koopt spyware van controversiële bedrijven (samenvatting II). Overheid screent deze bedrijven in het geheel niet.

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

Buro Jansen & Janssen beweegt niet helemaal weg van de spyware, er volgt waarschijnlijk nog een Observant over het onderwerp. Net als bij deep packet inspection, het zogenaamd onderzoeken van dataverkeer omdat dit volgens de tech-industrie noodzakelijk is voor het goed functioneren van dat verkeer, is het bestaan van die tech tools genormaliseerd. Spyware lijkt ook steeds meer genormaliseerd, een fait accompli.

Een voldongen feit is ook dat we na de twee corona jaren even een pas op de plaats hebben gemaakt. Niet dat er niet meer onderzoek wordt gedaan, maar wel dat die corona jaren tot oude inzichten hebben geleid. Onze interesse, betrokkenheid en onderzoek naar corona demonstraties is door verschillende mensen die ons lange tijd steunden niet in dank afgenomen. Sommigen beweren zelfs dat Buro Jansen & Janssen extreemrechts steunt.

Buro Jansen & Janssen heeft veel geschreven over demonstraties tegen de coronamaatregelen, onderzoeken en analyses. Bij die demonstraties waren ook extreemrechtse individuen betrokken. Daar hebben we ook over geschreven. Bij al het onderzoek is niet geconstateerd dat extreemrechts de meerderheid vormde, ook niet bij demonstraties die door bepaalde groepen zijn georganiseerd. Het beeld van de deelnemers aan de demonstraties in die periode is dat het mensen zijn uit een zeer breed politiek spectrum, van extreemrechts tot radicaallinks.

Wat echter opvalt is de kritiek op het feit dat Buro Jansen & Janssen zich bezighoudt met onderzoek naar de repressie rond de coronademonstraties, de critici lijken te impliceren dat die demonstraties terecht onderdrukt zijn. De demonstranten zouden allemaal niet goed wijs zijn, om het simpel te zeggen. Nu lijkt dit een mening die in breed politiek links wordt gedeeld, niet alleen in parlementair links, maar ook het buitenparlementaire deel van de linkse gemeenschap.

10. Om de vrijheid te vieren moet je wel de kritiek op de vrijheidsbeperkingen accepteren

11. De Wijster Razzia, Volwassenen en kinderen geslachtofferd omdat de overheid een punt wilde maken

Buro Jansen & Janssen heeft haar wortels gelukkig niet in politiek, parlementair en buitenparlementair links, maar in de autonome beweging van de jaren tachtig. Daarbij past een algemeen kritische houding op elke politieke stroming en wie alle artikelen van Buro Janssen & Janssen rond de coronapandemie leest ziet daar een grote mate van verbazing over alle facetten van het overheidsbeleid, het gebrek aan verontwaardiging en kritiek op dat beleid, ook van links, niet direct steun voor de demonstranten, maar wel veel kritiek op de repressie en het geweld van de overheid bij de demonstraties. Dat links nu niet veel actiever vraagt om een parlementair onderzoek naar het coronabeleid roept nog meer vragen op en geeft te denken.

Vragen die Buro Jansen & Janssen ook stelt bij het onderzoek en de publicaties rond radicale moslims. In de tijd van de moord op Theo van Gogh en de diverse publicaties van Buro Jansen & Janssen in die tijd is het Buro ook veel mensen die het Buro jarenlang steunden kwijtgeraakt. Buro Jansen & Janssen zou opnieuw heulen met extreemrechts, nu in de gedaante van radicale moslims. En opnieuw antwoordde Jansen & Janssen toen, lees ons onderzoek, bekijk de publicaties en zie dat Buro Jansen & Janssen niet direct steun betuigt, maar wel onderzoek doet naar het repressie apparaat, net als het Buro doet bij preventief fouilleren, identificatieplicht en andere onderdrukkende wetgeving. En ook bij radicale moslims heeft het Buro moeten concluderen dat die repressie enorm is en veel vragen oproept.

Dit eerste post coronajaar was dus ook een soort bezinningsjaar. Met de coronapandemie moeten we zeker nog iets doen. De overheid lijkt het boek al te willen sluiten hoewel de rechtse Kamer het misschien wel wil, maar dan vast en zeker eerder als afrekening dan dat het serieus moet worden opgevat. De vraag moet namelijk zijn, wat doet de samenleving met alle de slachtoffers? Slachtoffers van falend beleid en slachtoffers van repressie en geweld van de overheid?

Het lijken dezelfde vragen als bij spyware industrie. Ook daar worden de slachtoffers en in dat geval zelfs de rechtstaat zelf vergeten en onder het ambtelijk tapijt geschoven. Andere onderwerpen roepen echter ook om aandacht.

5. Mindstone; De FinFisher boef die de gedachten en dromen van de ander leest en beheerst

7. DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (samenvatting)

8. DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)

Buro Jansen & Janssen bestaat in 2024 veertig jaar. Terugkijken en vooruit zien blijft het Buro altijd doen. Buro Jansen & Janssen, autonoom en gewoon inhoud.

Maak het werk van Buro Jansen & Janssen mogelijk, word donateur. Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan. Word donateur of vraag familie, vrienden en bekenden donateur te worden. Rekening NL43 ASNB 0856 9868 52 of NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

De digitale inkijkoperaties van de Politie Black Box (samenvatting I)

Nederlandse politie gebruikt spyware voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen, niet voor het verzamelen van bewijs

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 nauwelijks tot niet gebruikt als bewijs bij rechtszaken. Het lijkt erop dat de politie spyware tools gebruikt voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen.

Inzet hackbevoegdheid voor andere doeleinden

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.

Betrouwbaarheid verkregen bewijs in het geding

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, hoe gegevens worden verzameld en bewijs wordt verkregen en de aanwezigheid van backdoors kan niet worden uitgesloten.

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. Niet gekeurde of slecht gekeurde opsporingsmiddelen hebben gevolgen voor het gebruik van bewijsmateriaal in de rechtszaal.

Toezicht schiet tekort

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, hoewel de politie 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: er zijn sterke aanwijzingen dat spyware wordt ingezet voor andere doeleinden dan waarvoor zij wettelijk bedoeld is.

In het onderzoek ‘Een politie black box, het gebruik van spyware door de Nederlandse politie’ 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.

Naar inhoudsopgave Observant # 81

Nederlandse politie koopt spyware van controversiële bedrijven (samenvatting II)

Overheid screent deze bedrijven in het geheel niet

Commerciële spyware bedrijven leveren ook aan repressieve regimes die het inzetten tegen oppositieleden, activisten en journalisten. Volgens de overheid koopt Nederland geen spyware van bedrijven die ook leveren aan dubieuze regimes en vindt er een screening van bedrijven plaats. In de praktijk stelt deze screening echter niets voor. De politie vertrouwt volledig op verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes, maar doet geen eigen onderzoek.

Ook in andere opzichten is screening van leveranciers beperkt. Er vindt geen onderzoek plaatst naar de banden van bedrijven met nationale inlichtingdiensten, en hun belastingbeleid en exportbeleid. Ook vindt geen antecedentenonderzoek plaats naar mogelijke strafrechtelijke vervolging van functionarissen van bedrijven en tussenhandelaren.

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. De cybersurveillance industrie is controversieel, ondermeer vanwege de betrokkenheid van bedrijven bij mensenrechtenschendingen. In de loop der jaren zijn talloze voorbeelden bekend geworden van bedrijven die spyware leveren aan repressieve regimes die het inzetten tegen journalisten, activisten en oppositieleden. Het gaat daarbij ook om spyware van bedrijven die ook aan Nederland hebben geleverd, of waarin de Nederlandse overheid interesse had.

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. Nederland heeft spyware afgenomen van ondermeer Gamma Group en de Israëlische NSO Group. De FinFisher spyware van Gamma Group is aangeschaft door onder andere het Egypte van Moebarak, Oeganda, Ethiopië, Turkije en Saoedi-Arabië, waar het is ingezet tegen onder andere journalisten, mensenrechtenactivisten en oppositieleden. NSO leverde haar Pegasus spyware aan onder meer Bangladesh, Egypte, Mexico, Marokko, Polen en Saoedi-Arabië.

Screening stelt niets voor

In het regeerakkoord 2017-2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. In de praktijk is van een screening echter geen sprake. De politie doet geen eigen onderzoek en vraagt de bedrijven slechts om een verklaring dat zij niet leveren aan dubieuze regimes.

Het is echter niet duidelijk welke landen hiermee worden bedoeld. De Minister van Veiligheid en Justitie verklaarde meest recentelijk in december 2022 in antwoord op Kamervragen respectievelijk dat het ging om ‘landen waartegen EU of VN-sancties bestaan’ en ‘landen die mensenrechtenschendingen begaan’. Volgens de Minister wordt deze toets periodiek herhaald. Uit rapporten van de Inspectie Justitie en Veiligheid blijkt echter dat dit in de praktijk niet gebeurt.

De Inspectie constateert ook dat de screening van leveranciers van spyware slechts bestaat uit het vragen van een verklaringen aan bedrijven dat zij niet leveren aan dubieuze regimes. De Inspectie maakt echter niet duidelijk of ze deze verklaringen ook heeft ingezien, en plaatst geen kritische kanttekeningen bij de gebrekkige screening van de leveranciers.

Cyber surveillance industrie controversieel

De politie vertrouwt dus volledig op de verklaringen van bedrijven dat zij niet leveren aan dubieuze regimes. De screening van bedrijven is ook in andere opzichten beperkt. Veel controversiële aspecten van de cybersurveillance industrie blijven volledig buiten beschouwing.

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. Bij de screening van leveranciers van spyware wordt hier geen rekening mee gehouden. Hierdoor, en door de mogelijke aanwezigheid van backdoors in de spyware, is de nationale veiligheid in geding.

Er wordt ook geen onderzoek gedaan naar het belastingbeleid en exportbeleid van de bedrijven, hoewel dit wel op zijn plaats is. De meeste spyware bedrijven hebben namelijk ook vestigingen in belastingparadijzen en maken gebruik van offshore accounts, hetgeen belastingontduiking en mogelijk witwassen faciliteert. De bedrijven exporteren vaak ook via vestigingen in andere landen om exportbeperkingen te omzeilen.

Er vindt evenmin antecedentenonderzoek plaats naar mogelijke strafrechtelijke vervolging van functionarissen van bedrijven en tussenhandelaren. Functionarissen van spyware bedrijven zijn echter veroordeeld voor het betalen van steekpenningen, corruptie en zware georganiseerde criminaliteit of hiermee in verband gebracht.

In het onderzoek ‘Een Politie Black Box, het gebruik van spyware door de Nederlandse politie’ borduurt Buro Jansen & Janssen voort op eerdere onderzoeken van het Buro naar de cybersurveillance industrie en de 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 dat toezicht houdt op de uitvoering van de hackbevoegdheid door de Nederlandse politie.

Naar inhoudsopgave Observant # 81

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.

Naar inhoudsopgave Observant # 81

Documenten bij een Politie Black Box gebruik van spyware door de Nederlandse politie

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.

Artikelen

– De digitale inkijkoperaties van de Politie Black Box (samenvatting I). Nederlandse politie gebruikt spyware voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen, niet voor het verzamelen van bewijs.
– Nederlandse politie koopt spyware van controversiële bedrijven (samenvatting II). Overheid screent deze bedrijven in het geheel niet.
– Een Politie Black Box, gebruik van spyware door de Nederlandse politie (onderzoek)

– DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (samenvatting)
– DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)
– Documenten bij DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)

Boeven vangen met dubieuze software van dubieuze bedrijven (2017)

– Boeven vangen met dubieuze software van dubieuze bedrijven
– Inhoudsopgave Politie Mercenaries, Observant #69, januari 2017
– Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence
– Gamma Group/Louthean Nelson; Wapenhandelaars pur sang
– Door Wikileaks openbaar gemaakte stukken over Gamma Group/FinFisher
– CitizenLab over FinFisher
– CitizenLab diverse artikelen over FinFisher
– gebruik FinFisher Nederlandse politie
– gebruik FinFisher Nederlandse politie support
– Kamervragen FinFisher/Gamma Group
– Politie Mercenaries, Observant #69, januari 2017 (pdf)

Inspectie Justitie en Veiligheid

– Rapport toezicht Inspectie 2019
– Bijlage rapport toezicht Inspectie 2019
– Rapport toezicht Inspectie 2020
– Bijlage rapport toezicht Inspectie 2020
– Rapport toezicht Inspectie 2021
– Bijlage rapport toezicht Inspectie 2020

WODC

– WODC rapport samenvatting
– WODC rapport
– WODC rapport summary

Hoge Raad

– Onderzoek in een geautomatiseerd werk

Spyware algemeen documenten, Woo-verzoek van

– Spyware stukken 01
– Spyware stukken 02
– Spyware stukken 03

DigiTask documenten politie, Woo-verzoek van april 2019

– DigiTask stukken 01
– DigiTask stukken 02
– DigiTask stukken 03
– DigiTask stukken 04
– DigiTask stukken 05
– DigiTask stukken 06
– DigiTask stukken 07
– DigiTask stukken 08
– DigiTask stukken 09

Scriptie

– Hacken als opsporingsbevoegdheid in het licht van artikel 8 lid 2 EVRM: de zoektocht naar een 'fair balance' tussen opsporing en privacy

Naar inhoudsopgave Observant # 81

Mindstone

De FinFisher boef die de gedachten en dromen van de ander leest en beheerst

Als een schim beweegt hij zich in de wereld van de wapenhandel, Louthean Nelson. In 2017 schreef Buro Jansen & Janssen het artikel 'Gamma Group/Louthean Nelson; Wapenhandelaars pur sang' over de geschiedenis van het bedrijf achter de FinFisher spyware. Vijf jaar later heeft de schim zich verplaatst naar Singapore en is actief onder de naam Mindstone.

Nelson is uit de comic books van Marvel ontsnapt. Daar weet de marginale crimineel Turk Barrett de Mind Stone in handen te krijgen en een crimineel imperium op te bouwen. Een van de krachten die Turk aan de Mind Stone weet te ontlenen is om omstanders zelfmoord te laten plegen. De Mind Stone heeft in de Marvel wereld namelijk de kracht om gedachten en dromen van anderen te lezen en te beïnvloeden.

Die knipoog van Nelson naar Marvel is misschien niet toevallig. De FinFisher spyware, ook bekend onder de namen FinSpy en WingBird, wordt gebruikt om onder andere telefoons te hacken en daarmee het privéleven van personen te doorgronden. Daarnaast heeft Nelson in zijn carrière menig vervolging en data lek overleefd en het netwerk van bedrijven dat hij in de loop der jaren heeft opgezet uitgebreid en verplaatst.

Misschien het meest opvallendst aan Nelson is dat zijn bedrijven geen directe link met een nationale overheid lijken te hebben. Toen Hacking Team door een datalek in 2015 in de problemen kwam, werd het bedrijf door de Italiaanse overheid onder de loep genomen. Het bedrijf is voortgezet onder een andere vlag, Memento Labs, maar het moest toch een flinke dreun incasseren. Hetzelfde geldt voor de NSO-Group waar de Israëlische overheid heeft ingegrepen. Bij de Gamma Group en Louthean Nelson is van een dergelijke link met een nationale overheid geen sprake.

Als een kameleon kan Nelson zo zijn handel niet alleen van land naar land laten verhuizen, maar ook van bedrijf naar bedrijf. Van PK Electronic, naar Gamma Group, naar FinFisher, Vilicius, Raedarius en nu naar Mu Shun en Mindstone. Bijna organisch lijken de bedrijven in elkaar over te vloeien en als inktvlekken zich te verplaatsen. Altijd omringt door andere bedrijven die al dan niet een functie vervullen van administratieve afleiding, export hub of als (in)directe handel zoals Elaman en Trovicor. Ook de tussenhandel is gereguleerd in het imperium.

Eerste krasjes in het imperium

In de jaren tachtig als Nelson actief is voor het Duitse bedrijf PK Electronic van Peter Klüver, wordt hij niet geconfronteerd met enige vervolging. De tussenhandel in gevoelige elektronica van multinationals zoals Philips, Siemens, AEG-Telefunken en Zeiss is zeer lucratief. Het bedrijf wordt geen strobreed in de weg gelegd bij de export naar landen als Saoedi-Arabië, Libië, Syrië, Indonesië, Angola, Soedan, Nigeria, Jordanië, Irak en Taiwan soms zelfs zonder de vereiste exportvergunningen.

Begin jaren negentig van de vorige eeuw komen er scheuren in de onaantastbare positie van PK Electronic. Opiniebladen als Der Spiegel en Focus publiceren over de handel van het bedrijf en die aandacht wordt gevolgd door eerst enkele boetes, vervolgens in beslagnames van goederen en ten slotte exportbeperkingen. Zo is er in 1991 een boete voor de export van apparatuur naar Taiwan, in 1992 in beslagname van traangas en stroomstok wapens voor Angola en in 1994 wordt bekend dat het bedrijf als tussenhandelaar fungeert voor Irak om het embargo tegen dat land te ontlopen.

In diezelfde periode verwijdert Nelson zich langzaam van Klüver en bouwt vanaf eind jaren negentig zijn eigen netwerk op, vooral gevestigd in het Verenigd Koninkrijk. De wirwar van bedrijven die hij met zijn vader William Louthean Nelson opzet, zorgen de eerste jaren niet voor controverses. De indruk bestaat dat hij zelfs de wapenhandel heeft verlaten, maar vestigingen op Cyprus, in Beiroet en in Singapore geven aan dat Nelson niet de oude handelspraktijken gedag heeft gezegd. Zijn deelneming in maart 2006 in het bedrijf CBRN Team Ltd. van de Deen Niels Tobiasen is hier een stille getuige van.

CBRN Team in Oeganda

CBRN Team schrijft op haar website dat het Britse ministerie van Defensie, het ministerie van Binnenlandse, noodhulpdiensten, mediabedrijven zoals BBC, ITN, Sky and ABC en financiële instellingen in de City of London klanten van haar zijn.

Ook buitenlandse mogendheden behoren bij de klandizie van het bedrijf uit Salisbury. In 2004 is het bedrijf begonnen om Oeganda te voorzien van ‘CBRN (Chemical, biological, radiological and nuclear) threat detection equipment´. In totaal haalt CBRN team zes contracten binnen met een waarde van een half miljoen pond.

Een van die contracten ter waarde van 210.000 pond is een veiligheidspakket voor de Oegandese Presidentiele Garde voor de bijeenkomst van de regeringsleiders van de Gemenebest van Naties (Commonwealth of States) die in november 2007 in Kampala plaatsvindt.

In augustus 2008 verschijnt Tobiasen voor een Britse rechtbank. Hij is aangeklaagd voor corruptie, witwassen en het verdoezelen van crimineel vermogen. Tobiasen bekent schuld voor het betalen van steekpenningen en corruptie, maar ontkent de andere beschuldigingen.

De rechtbank seponeert de zaken rond het witwassen en het criminele vermogen. De 65-jarige Tobiasen wordt veroordeeld voor vijf maanden gevangenisstraf. In zijn schuldbekentenis verklaart dat hij tussen juni 2007 en februari 2008 twee Oegandezen via vijf overschrijvingen naar privérekeningen in totaal 83.000 pond betaalde.

Een van de Oegandezen, Ananias Gweinho Tumukunde, wetenschaps- en technologie adviseur van de Oegandese president Museveni, wordt in april 2008 op Heathrow gearresteerd en in september dat jaar veroordeeld tot twaalf maanden gevangenisstraf. Ook hij bekent schuld voor corruptie en het ontvangen van 50.000 pond aan steekpenningen.

De andere Oegandees, Rusoke Tagaswire, luitenant-kolonel van de Oegandese Presidentiele Garde, wordt niet uitgeleverd door de Oegandezen. Zij stellen dat Britten niet genoeg bewijs hebben om hem te vervolgen.

Nelson en het bedrijf ontlopen de dans

De corruptiezaak rond CBRN Team krijgt veel aandacht in de media omdat het een van de eerste rechtszaken van nieuwe wetgeving tegen corruptie is. De zaak is echter ook bevreemdend omdat de Britse overheid besluit om 40.000 pond van de steekpenningen die Tumukunde van CBRN Team ontving aan de Oegandese overheid te betalen.

Daarnaast verklaart de operationeel directeur van CBRN, Ian Day, dat Tobiasen, de financiële baas van het bedrijf, niets te maken had met de operaties of contracten. Volgens Day wist Tobiasen niet eens waar CBRN voor staat: “He has nothing to do with operations—he is a financial guy; he’s a money man… He couldn’t spell CBRN let alone do it. He’s not an expert in the field,” zegt Day tegen de website *The Black Star*.

Tobiasen is veroordeeld, maar hoeft zijn vijf maanden gevangenisstraf niet uit te zitten. Überhaupt wordt CRBN Team en haar directie als bedrijf niet onderzocht en vervolgd. Louthean Nelson, algemeen directeur van het bedrijf, wordt in geen van de rechtszaken rond de corruptie genoemd. Hetzelfde geldt voor de operationeel directeur Anthony Ian Day die betrokken is bij de trainingen.

Wat voor training CBRN Team aan de Oegandezen in Engeland en Oeganda heeft gegeven blijft onduidelijk. Day geeft zelfs aan dat van een gevaar voor biologische en chemische wapens op dat moment in Oeganda en op het Afrikaanse continent geen sprake is. Day suggereert in het interview in de *The Black Star* wel dat er sprake zou zijn van een terrorisme dreiging, maar waarom dan een private partij is ingeschakeld om de Oegandezen te training, blijft ook onduidelijk.

Klanten Gamma Group bekend door WikiLeaks

Dat CBRN Team apparatuur en training regelt voor de Oegandese Presidentiele Garde van dictator Museveni ligt in de lijn van de carrière van Louthean Nelson. Al decennia schurkt de Engelsman dicht tegen leiders van vooral repressieve regimes aan. In 1983 wordt de Saoedische kroonprins Prins Abdullah Ibn Nasir Ibn Abd al-Asis Al Saud door PK Electronic in een Duitse Leopard tank rondgereden.

Dat dezelfde leiders klanten zijn van zijn nieuwe netwerk van bedrijven rond Gamma Group verbaast daarom niet. Wel dat niet alleen repressieve regimes als Oeganda, Egypte, Ethiopië, Vietnam, Venezuela, Turkije, Turkmenistan en Bahrein klant zijn van Gamma Group, maar ook democratieën als Nederland, Groot-Brittannië en Duitsland.

Dat het klantenbestand van de Gamma Group openbaar is, is te danken aan WikiLeaks die in 2014 informatie over het bedrijf openbaar maakt. Een jaar later publiceert de Canadese interdisciplinaire laboratorium The Citizen Lab van de Munk School of Global Affairs van de University of Toronto een aanvullende lijst van 32 landen die producten van Gamma Group gebruiken.

Het gaat niet alleen om de spyware FinFisher, maar ook om IMSI Catchers (International Mobile Subscriber Identity Catchers) van Gamma Group. Met de IMSI Catchers kunnen binnen een bereik van ongeveer 2 kilometer telefoongesprekken en sms-verkeer worden afgeluisterd en opgenomen.

Surveillance schandaal in Noord Macedonië

Een van de landen die in ieder geval IMSI Catchers van Gamma Group aanschaft is Noord Macedonië (het land heette toen nog Macedonia). Macedonië wordt zowel in de data van WikiLeaks als het onderzoek van The Citizen Lab genoemd. Er blijkt sprake te zijn van massa surveillance in het land.

De Macedonische geheime dienst UBK (Administration for Security and Counterintelligence) heeft van 2008 tot en met 2015 670.000 telefoongesprekken van meer dan 20.000 individuen afgeluisterd. De dienst kon rond de 1.500 telefoons per minuut bespieden via vijf verschillende netwerken. Bij de afgeluisterde personen zou het gaan om ministers, politici, zakenmensen, wetenschappers en anderen.

De onthulling over het bespieden is speciaal omdat niet alleen de aantallen telefoongesprekken worden geopenbaard, mar ook een deel van de afgeluisterde gesprekken zelf. Vanaf februari 2015 publiceert de leider Macedonische sociaaldemocratische oppositie partij SDRM, Zoran Zaev, de opgenomen gesprekken die hij heeft ontvangen van drie voormalige medewerkers van de Macedonische geheime dienst UBK (Administration for Security and Counterintelligence), Gjorgi Lazarevski, Zvonko Krstevski en Saso Mijalkov.

De oppositie claimt dat de surveillance bewijst dat de lokale verkiezingen van 2013 en de landelijke en presidentiele verkiezingen van 2014 door de regering van de conservatieve partij VMRO-DPMNE zijn gemanipuleerd. Ook zouden de afgetapte gesprekken bewijzen dat de media wordt gecontroleerd door de regering en het justitiële apparaat wordt beïnvloed.

Als voorbeeld van het laatste stelt de oppositie dat overheid de moord van een jongeman door een politieagent zou hebben verdoezeld. De regering arresteert de drie UBK medewerkers op verdenking van het voorbereiden van een coup tegen de regering. Zij komen later vervroegd vrij en worden van alle blaam gezuiverd.

Vervolging van verdachten in Target-Fortress en Trezor

De Harde beschuldigingen aan het adres van de regering leiden in 2017 tot de val van het VMRO-DPMNE kabinet en onderzoeken door een speciale openbare aanklager. Naast onderzoek naar verkiezingsfraude en misbruik van macht openen de aanklagers het Target-Fortress onderzoek naar het afluisteren zelf en het Trezor (Vault) onderzoek naar corruptie bij de aanschaf van de afluisterapparatuur. Volgens de speciale aanklager is er bij de aanschaf 860.000 euro aan gemeenschapsgelden verduisterd.

In 2020 wordt voormalig directeur van de UBK, Sasho Mijalkov in de Target-Fortress onderzoek veroordeeld tot 12 jaar gevangenisstraf en krijgt in 2021 acht jaar voor corruptie. Naast Mijalkov worden ook nog Toni Jakimovsk, voormalig hoofd van het kantoor van Mijalkov, en oud onder minister van Binnenlandse Zaken, Nebojsha Stajkovik, tot vijf jaar veroordeeld en krijgt voormalig leidinggevende van het vijfde Directoraat van het Ministerie van Binnenlandse Zaken, Goran Grujevski, vijftien jaar voor corruptie. Eind 2022 wordt de uitspraak in de Target-Fortress in beroep verworpen en op 27 februari 2023 gaat een nieuw proces van start.

Geen Britse onderzoeken naar Gamma Group

Hoewel veel onderzoeken naar het handelen van de Macedonische regering op de lange baan zijn geschoven is er dus wel een veroordeling gekomen in de twee onderzoeken naar het afluisteren en

de corruptie rond de aanschaf. Dit is meer dan de Britse overheid heeft ondernomen tegen het bedrijf dat de spionage apparatuur heeft geleverd.

Zij heeft geen enkele juridische stappen gezet tegen Gamma Group. Dat is niet alleen opmerkelijk gezien het ontlopen van vervolging in de CBRN Team fraudezaak. Uit overheidsdocumenten die de Britse website Computer Weekly via de Freedom of Information Act (Britse Woo) heeft verkregen blijkt namelijk dat de Britse regering ook selectief is omgegaan met informatie om de export licentie te verlenen.

Bij het selectief omgaan met informatie gaat het om een voortgangsrapport van de Europese Unie uit 2011. Groot-Brittannië is op dat moment nog lid van de Unie. In deze toetredingsrapporten gaat het om mensenrechten, de rechtstaat en andere maatschappelijke aspecten van landen die willen toetreden tot de EU. Hoewel het EU-rapport uit 2011 positief is, uit het wel haar zorgen over onder andere de onafhankelijkheid van de politie en het toezicht op de inlichtingen en contra-inlichtingendiensten.

Juist de opsporings- en inlichtingendiensten zijn bij het afluisterschandaal over de scheef gegaan. Daarnaast heeft de Britse overheid geen onderzoek gedaan naar andere uitvoer van apparatuur van Gamma Group. Zo bericht de Britse krant The Guardian al in 2011, een jaar voor het verlenen van de Macedonische licentie, over de mogelijke verkoop van Gamma apparatuur aan het repressieve regime in Egypte.

Levering via Finzi DOOEL en een geraadpleegde Tory minister

Nu kenmerken export licenties voor dual use goederen als FinFisher en IMSI-Catchers zich meestal als hamerstukken en worden bedrijven geen strobreed in de weggelegd om repressieve regimes te helpen. Buro Jansen & Janssen heeft daartoe uitgebreid onderzoek gedaan naar Fox-IT en het Nederlandse exportbeleid.

Het Britse handelen ten aanzien het Macedonische afluisterschandaal is echter opvallend. Hoewel de Macedonische functionarissen beweren dat de apparatuur wordt aangeschaft voor de bestrijding van de georganiseerde criminaliteit wordt tijdens het onderzoek naar het afluisteren in Noord Macedonië duidelijk dat in 2010 functionarissen van de geheime dienst UBK op persoonlijke titel naar London reizen om de aanschaf van de Gamma apparatuur te bezegelen.

Voor de deal gebruiken de functionarissen niet de formele Macedonische overheidsinstanties, maar een netwerk van bedrijven in de Verenigde Staten en Cyprus met uiteindelijke afnemer het Macedonische bedrijf Finzi DOOEL Ltd. van Kosta Krpač. Kosta Krpač is in 2016 na het uitkomen van het afluisterschandaal dood gevonden. Hoewel er sprake is van verdachte omstandigheden is zijn dood als zelfmoord aangemerkt.

Of de Britse autoriteiten op de hoogte waren van de afnemer Finzi DOOEL Ltd. wordt niet duidelijk uit de openbaar gemaakte stukken. Wel is de toenmalige verantwoordelijke minister van Europa en latere staatssecretaris van justitie, de conservatief David Lidington, geraadpleegd over de uitvoer van onder andere zes IMSI-Catchers van Gamma Group in de periode van 2011 tot en met 2015.

Voor de export naar een land waar aan de onafhankelijkheid van het justitieapparaat wordt getwijfeld, kan het raadplegen van de verantwoordelijke minister een laatste check zijn. Tussen de openbaar gemaakte documenten zit echter geen aanvullend onderzoek naar de export licentie, dus waarom is de minister geraadpleegd. De Britten wilden blijkbaar de export van de Gamma Group niet tegenhouden, maar wel formeel afdekken. De export licentie voor de uitvoer van Gamma apparatuur naar Macedonië is op 3 oktober 2012 afgegeven.

De omvang van het Macedonische afluisterschandaal, de corruptie bij de aanschaf van de Gamma apparatuur, de vervolging van vier functionarissen door de Noord Macedonische justitie, het gebruik van onder andere Finzi DOOEL Ltd voor de aankoop, het persoonlijke bezoek van Macedonische functionarissen aan London, de gebrekkige

rechtstatelijk situatie in het land, de levering aan Egypte en het verleden van functionarissen van Gamma Group, lijken genoeg redenen om in ieder geval de omstandigheden van de export van Gamma apparatuur naar Macedonië nader te onderzoeken.

Het handelen van Gamma Group roept niet alleen vragen op over export licenties, maar ook over mogelijke corruptie en het betalen van steekpenningen door Gamma Group. Dit gebeurt niet. Gamma Group ontloopt de dans en daar waar Noord Macedonië in eerste instantie zeer voortvarend overgaat tot vervolging van verdachten van het afluisterschandaal en corruptie, gebeurt er in het Verenigd Koninkrijk niets.

Geen onderzoek naar export naar Bahrein en Ethiopië

Het Noord Macedonische export schandaal vindt plaats op hetzelfde moment dat Gamma Group door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) wordt beschuldigd van het schenden van mensenrechten richtlijnen bij de export van spyware naar het repressieve Bahrein in 2014. Dat oordeel van de OESO volgt op een procedure van Privacy International.

Privacy International probeert al sinds 2012 in eerste informatie openbaar te krijgen van de HMRC (Her Majesty's Revenue and Customs), de Britse douaneautoriteiten, over de export van spyware van Gamma Group naar Bahrein en Ethiopië. Het gaat dan vooral over de vraag of de HMRC onderzoek heeft gedaan naar de export van die apparatuur.

De verzoeken van Privacy International worden afgewezen en in mei 2013 tekent Privacy International beroep aan tegen de weigering van de HMRC. Dit beroep wordt gewonnen in 2014 omdat volgens de rechters er alle reden is voor de HMRC om de export van Gamma apparatuur te onderzoeken en openbaarmaking van die informatie niet zomaar geweigerd kan worden.

Het bedrijf exporteert bijvoorbeeld FinSpy, een van haar spyware producten, al vanaf 2006 zonder een export licentie. Pas in 2012 vraagt Gamma aan de HMRC of zij export licentie nodig heeft voor de verscheping van haar spyware producten naar het buitenland. Onduidelijk is of de HMRC de export van spyware naar Bahrein en Ethiopië überhaupt heeft onderzocht. Tot op heden is daarover geen informatie openbaar gemaakt.

Tijdens de beroepsprocedure tegen de HRMC getuigen Ala'a al-Shehabi van de organisatie Bahrain Watch en de gevluchte Ethiopische politicus Tadesse Kersmo dat zij slachtoffer zijn geworden van FinFisher. Shehabi en Kersmo vertellen de rechtbank over de spyware die op hun computers is geïnstalleerd om hun te bespioneren en data van hun computers te downloaden.

Volgens de Britse staatsburgers zijn respectievelijk de Bahreinse en de Ethiopische overheden verantwoordelijk voor die spionage met behulp van spyware van het Britse bedrijf Gamma International, onderdeel van de Gamma Group. Hoewel honderd procent zekerheid over de spionage zelf en de daders niet is vastgesteld tijdens de beroepsprocedure, blijkt in het jaar van de beroepsuitspraak uit gegevens van WikiLeaks en een jaar later van The Citizen Lab dat zowel Bahrein als Ethiopië ook klanten van de Gamma Group zijn.

Het argument dat beide repressieve regimes de spyware hebben aangeschaft voor de bestrijding van de georganiseerde criminaliteit gaat niet op als de apparatuur is ingezet tegen oppositieleden en mensenrechtenactivisten. Onderzoek naar de export van dual use goederen en het afgeven van onderbouwde licenties zou daarom noodzakelijk zijn.

Geen immuniteit voor Bahrein, wel voor Gamma

De rechtszaak rond de weigering van de HMRC om informatie vrij te geven gaat niet over de inzet van spyware zelf, maar om onderzoek naar de rechtmatigheid van de toegelaten export. Die inzet van de

spyware zelf staat jaren later wel centraal als Saeed Shehabi en Moosa Mohammed de Bahreinse staat voor de Britse rechter slepen.

Saeed al-Shehabi is de vader van Ala'a al-Shehabi en leider van de Bahrain Freedom Movement en de Bahreinse democatische organisatie Al Wefaq. Mohammed Moosa Abd-Ali Ali is net als al-Shehabi voorvechter van democratisering in Bahrein en het respecteren van de mensenrechten. Zij stapten in 2018 naar de rechter om een strafrechtelijk onderzoek naar het gebruik van spyware door de Bahreinse overheid tegen hen af te dwingen.

Veel hoop hebben de twee activisten niet hoewel zij Brits staatsburger zijn en het binnendringen van de spyware op hun gegevensdragers op Britse bodem plaatsvond. In het algemeen staat de immuniteit van een buitenlandse mogendheid vervolging in de weg. De Bahreinse staat betoogt dat dan ook tijdens de zitting, het Bahreinse optreden zou niet onder de jurisdictie van de Britse rechter vallen.

Het Hoog Gerechtshof oordeelt in februari 2023 echter dat de immuniteit in het geval van het gebruik van spyware tegen Saeed al-Shehabi en Mohammed Moosa Abd-Ali Ali wel vervalt omdat de Bahreinse staat daarmee persoonlijke schade toebrengt aan twee Britse staatsburgers.

Of een uiteindelijk strafzaak tegen de Bahreinse staat een veroordeling oplevert en iets zal veranderen valt te betwijfelen. Mohammed Moosa is na FinFisher namelijk ook slachtoffer geworden van Pegasus, spyware van het Israëlische bedrijf NSO. Het gaat de aanklagers echter niet zozeer om een veroordeling, maar vooral om het aan banden leggen van het gebruik van spyware.

Ook immuniteit van Saoedi-Arabië opgeheven

Het opheffen van de immuniteit van de Bahreinse staat bij het gebruik van spyware tegen Britse staatsburgers volgt op een vergelijkbaar vonnis tegen het Saoedische regime op 19 augustus 2022. In die zaak

klaagde mensenrechtenactivist Ghanem Al-Masarir de regering van Saoedi-Arabië aan voor het plaatsen van spyware op zijn telefoon.

Die spyware blijkt van de NSO Group te zijn, het Israëlische bedrijf dat Pegasus spyware aan de Saoediërs leverde om de Amerikaanse journalist Jamal Khashoggi te bespioneren en in Istanbul te vermoorden. Ook in de zaak van Ghanem Al-Masarir verwierp het Britse Hoog Gerechtshof de immuniteit van de Saoedische overheid.

Opvallend is echter wel dat in de beide zaken waarbij de immuniteit van staten is verworpen de commerciële bedrijven de strafrechtelijke dans ontspringen. In de zaak van Ghanem Al-Masarir gaat het om het Israëlisch bedrijf NSO Group, maar Gamma Group is lange tijd een Brits bedrijf zeker ten tijde van de verkoop van spyware aan Bahrein en Noord Macedonië.

In beide gevallen heeft de Britse overheid verzuimd burgers te beschermen en is export van spyware toegestaan in verband met de imaginaire bestrijding van de georganiseerde criminaliteit.

Schenden mensenrechten richtlijnen OECD door Gamma

Daar waar de Britse overheid verzuimt om export van de Gamma Group zelfs maar te onderzoeken veroordeeld de Britse afdeling van de OESO het bedrijf na een klacht. De OESO beter bekend onder haar Engelse naam de OECD (Organisation for Economic Co-operation and Development) is een internationaal orgaan van 38 landen.

De OECD propageert door middel van richtlijnen maatschappelijk ondernemen van internationaal opererende bedrijven. Bij die richtlijnen gaat het om aspecten van mensenrechten, kinderarbeid, milieu, corruptie, bij onder andere de productie en de export. De OECD bestaat uit veel landen van de EU, maar ook Japan, Mexico, Costa Rica, Australië, Zuid-Korea, Verenigde Staten.

Privacy International dient in 2013 een klacht in bij het OECD in het Verenigd Koninkrijk tegen Gamma International, de Britse tak van Gamma Group, in verband met de export van spyware naar Bahrein. Deze beschuldiging van het schenden van mensenrechten richtlijnen van de OECD wordt in eerste instantie in 2013 ontvankelijk verklaard en in 2014 omgezet in een veroordeling van Gamma Group voor die export naar Bahrein.

Uiteindelijk heeft de OECD-veroordeling geen grote gevolgen voor het bedrijf. Nelson heeft zijn handel dan al verhuisd naar Duitsland waar in 2013 de naam Gamma International GmbH wordt vervangen door FinFisher GmbH. Met de verhuizing ontloopt Gamma mogelijke sancties van de Britse overheid naar aanleiding van de OECD-veroordeling, hoewel de Britse overheid geen stappen tegen het bedrijf onderneemt.

Gamma partner Trovicor gaat vrijuit in Duitsland

In Duitsland is eind 2013 een vergelijkbare OECD klacht tegen het bedrijf Trovicor gestrand. In die klacht wordt Trovicor van hetzelfde beschuldigd als Gamma Group in het Verenigd Koninkrijk, namelijk het leveren van surveillance producten aan Bahrein die zijn ingezet tegen leden van de oppositie. Hoewel het bewijsmateriaal in de Duitse en Engelse zaak erg op elkaar lijkt wordt de Duitse klacht niet ontvankelijk verklaard.

Trovicor, ondertussen overgenomen door het Franse Boss Industries, moederbedrijf van Nexa Technologies (voorheen Amesys), een Franse spyware maker, onderhoudt een nauwe band met Gamma Group. De van origine joint venture van het Finse Nokia en het Duitse Siemens, Nokia Siemens Networks (NSN) is daarnaast ook nauw verbonden met het Duitse Elaman.

Elaman heeft vestigingen in Duitsland, Zwitserland, Libanon, de Emiraten, Singapore, Indonesië en Zuid-Afrika en presenteert zich als tussenhandelaar van vooral producten van Gamma Group, maar ook die van Trovicor, VASTech en Utimaco. Elaman is nauw verweven met Gamma Group en aanverwante bedrijven zoals Gamma TSE en G2 System.

Die verwevenheid is niet alleen als reseller, maar ook bestuurlijk en personeel technisch. Zo kennen de Zwitserse afdelingen van Elaman en Trovicor dezelfde bestuursleden en zijn er tevens personele wisselingen tussen de bedrijven.

De klachten tegen Gamma Group en Trovicor ten aanzien van de export naar het repressieve regime van Bahrein zijn dan ook niet los van elkaar te zien. Dat de Duitse klacht is afgewezen is wel opvallend, hoewel Gamma geen nadelige gevolgen heeft ondervonden van de veroordeling door de Britse OECD. Uiteindelijk ontspringt Louthean Nelson toch steeds de dans.

Immuniteit van Ethiopië in de VS wel veilig

De uitspraken van de Britse OECD en het Hoge Gerechtshof in het voordeel van individuele aanklagers over de export naar een land dat bekend staat om haar mensenrechtenschendingen en het gebrek aan controle op die export staan in schril contrast met een uitspraak in een vergelijkbare zaak in de Verenigde Staten in 2017.

Die uitspraak volgt op een procedure die een Ethiopische activist, aangeduid met de gefingeerde naam Kidane, in 2014 start. Naar aanleiding van de uitspraak over de export van spyware naar Bahrein en Ethiopië in de zaak die Privacy International heeft aangespannen tegen HRMC in het Verenigd Koninkrijk begint Kidane een procedure tegen de Ethiopische staat over het infecteren van zijn laptop.

Kidane is ook een slachtoffer van FinFisher. Al zijn digitale activiteiten en die van andere leden van zijn familie waaronder gesprekken via Skype zijn afgeluisterd. De Ethiopische Amerikaan verdenkt de Ethiopische staat van die spionage. De uitspraak in 2017 is teleurstellend en in tegenstelling tot het Hoge Gerechtshof in het Verenigd Koninkrijk oordeelt de Amerikaanse rechter dat Ethiopië immuun is voor strafvervolging in de VS.

Toepassing van spyware in de VS geen probleem

De uitspraak is opvallend niet omdat deze meteen tevergeefs wordt gebruikt door Saoedi-Arabië in de zaak van Ghanem Al-Masarir tegen de Saoedische staat in het Verenigd Koninkrijk. Het is opmerkelijk omdat een Amerikaanse rechter impliciet spionage van buitenlandse mogendheden op Amerikaanse bodem onder bepaalde omstandigheden toestaat.

En die omstandigheden zijn ruim, want volgens de rechter hebben de spionageactiviteiten, zoals de fabricage van de FinFisher spyware en de activiteiten van de Ethiopische geheime dienst tegen Kidane grotendeels buiten het Amerikaanse grondgebied plaatsgevonden. Slechts de installatie van de spyware op de gegevensdragers van Kidane en het onttrekken van data gebeurden volgens de rechter in de VS en dat is niet genoeg.

De rechter stelt dat de Foreign Sovereign Immunities Act (FSIA) in het kader van niet-commerciële spionageactiviteiten vereist dat de gehele operatie in de VS plaatsvindt. Het is voor het eerst dat een rechter de FSIA op deze wijze uitlegt. Geheel verrassend is de uitspraak niet. De bepaling over niet-commerciële spionageactiviteiten in de FSIA is waarschijnlijk juist met het oog op spionage van Amerikaanse staatsburgers aan de wet toegevoegd.

In de VS is er geregeld ophef over de spionage van haar eigen burgers door haar eigen opsporings- en inlichtingendiensten zoals de FBI, CIA en NSA. Er zijn veel geheime inlichtingenoperatie van de diensten die een schandaal zijn geworden zoals bijvoorbeeld COINTELPRO (Counter Intelligence Program) van de FBI tegen Amerikaanse politiek activisten.

Ook bij de onthullingen van Edward Snowden, maakten de Amerikanen zich vooral zorgen om het feit dat de NSA Amerikaanse burgers zou bespioneren. Staatsburgers in de rest van de wereld lijken er in dat debat niet toe te doen. Kidane versus Ethiopië maakt duidelijk dat de FSIA de mogelijkheid biedt aan een buitenlandse mogendheid om Amerikanen in de gaten te houden.

FSIA, Echelon, Snowden en spionage van Amerikaanse burgers

Snowden wijst met zijn openbaar gemaakte documenten op de nauwe samenwerking met onder andere de Britse GCHQ. Nauwe connecties met buitenlandse diensten zijn al in de jaren tachtig onthuld toen onder andere James Bamford uitgebreid het Echelon systeem beschreef. Echelon is een samenwerking tussen Australië, Canada, Nieuw-Zeeland, het Verenigde Koninkrijk en de Verenigde Staten, de zogenaamde Five Eyes.

Vraag is dus of FSIA een slimme zet van de Amerikaanse wetgever is geweest om spionage van bevriende staten op Amerikaanse bodem toe te staan? Bij de inwerkingtreding van de wet in de jaren tachtig is misschien gedacht dat de Amerikaanse digitale hegemonie en dat van haar directe bondgenoten van de Five Eyes blijvend zou zijn.

De 21st eeuw laat echter zien dat elk land spyware kan aanschaffen en daarmee iedere Amerikaanse staatsburgers kan afluisteren, zo ook Ethiopië met haar spyware van Britse bodem. Kidane versus Ethiopië, en de wijze waarop de Amerikanen nogal huiverig zijn om Saoedi-Arabië te vervolgen voor het bespioneren van de Saoedische Amerikaan Jamal Khashoggi zet de schijnwerper ook op een andere vraag.

Worden individuele rechten van Amerikaanse staatsburgers of burgers elders in de wereld wel als onderdeel van de nationale veiligheid gezien. Of zijn die rechten alleen maar ondergeschikt aan die nationale veiligheid. In die zin is het opheffen van de immuniteit van Bahrein en Saoedi-Arabië door het Britse Hooggerechtshof in een zaak van individuele klagers zeker een lichtend voorbeeld.

Burgers zijn niet geheel vogelvrij, maar ze moeten die rechten wel zelf bevechten dit in tegenstelling tot de bedrijven die hun producten aan iedereen kunnen verkopen zonder last te hebben van de consequenties.

Illegale export van FinFisher aan de Turkse geheime dienst MIT

Althans in bijna alle gevallen hebben bedrijven geen last van overheden bij de export van spyware. Dit gold lange tijd ook voor FinFisher dat zich lange tijd onaantastbaar achtte in het Duitse München totdat in september 2019 het Duitse openbaar ministerie een onderzoek naar de export van FinFisher naar Turkije begint.

Dit onderzoek start de Duitse overheid echter niet uit zichzelf. Het is een reactie op een aangifte van Reporters Without Borders, Netzpolitik.org, the Society for Civil Rights (Gesellschafft für Freiheitsrechte, GFF) en het European Center for Constitutional and Human Rights. In die aangifte worden Markus Meiler en Holger Rumscheidt van Elaman, Carlos Gandini van FinFisher en Lucian Hanga en Holger Tesche van Finfisher Labs aangeklaagd voor de export van spyware zonder vergunning naar Turkije.

Het is dan al twee jaar bekend dat de Turkse overheid FinFisher gebruikt tegen vooral de oppositie. Ook dit feitenonderzoek is niet uitgevoerd door de Duitse overheid, maar door onder andere de organisatie Access Now. Twee jaar lang zet de Duitse staat dus geen stappen en zelfs na het openen van een strafrechtelijk onderzoek in september 2019 duurt het nog tot oktober 2020 voordat de kantoren van de bedrijven op vijftien locaties in Duitsland en Roemenië worden doorzocht.

In Duitsland gaat het om een scala adressen van de verschillende FinFisher bedrijven rondom Munchen. In Roemenië om een adres van bedrijven die gelieerd zijn aan FinFisher, SIS Eastern Europe GmbH en SIS Romania GmbH. Daarnaast zijn er rechtshulpverzoeken verstuurd aan de autoriteiten in Zweden, Cyprus, Maleisië, Bulgarije en Roemenië.

Uiteindelijk worden in mei 2023 vier voormalig directeuren van de bedrijven, aangeduid als 'G', 'H.', 'T.' en 'D.' door het openbaar ministerie aangeklaagd. Zij zouden in januari 2015 een contract ter waarde van 5 miljoen euro voor de levering van spyware met de Turkse geheime dienst MIT (Milli Istihbarat Teskilati) hebben ondertekend.

De directe levering wordt door Duitsland geblokkeerd. Er is geen exportvergunning afgegeven. Het bedrijf heeft vervolgens de export doorgezet via een zusterbedrijf in Bulgarije, Raedarius M8 EOOD. Op de overtreding van de export naar Turkije staat een straf van tussen de drie maanden en vijf jaar en bij levering aan de Turkse geheime dienst van minimaal een jaar.

FinFisher spyware en bedrijf gaan ondergronds

Terwijl de Duitse justitieonderzoek aan het doen is naar de export van FinFisher naar Turkije gaat de tool zelf ondergronds volgens antivirussoftware bedrijf Kaspersky. Kaspersky volgt de FinFisher

spyware (FinSpy of Wingbird) al sinds 2011 en constateert in september 2021 dat de makers van de spyware evenveel werk stoppen in de tool zelf als in het verbergen van de spyware voor zowel de slachtoffers als antivirussoftware makers.

"It seems like the developers put at least as much work into obfuscation and anti-analysis measures as in the Trojan itself. As a result, its capabilities to evade any detection and analysis make this spyware particularly hard to track and detect," zegt Igor Kuznetsov, onderzoeker bij het Kaspersky's Global Research and Analysis Team (GReAT) op de website van het bedrijf.

Vijf maanden na het rapport van Kaspersky lijkt het bedrijf zelf ook te verdwijnen. In februari 2022 wordt faillissement aangevraagd voor FinFisher GmbH, FinFisher Labs GmbH en Raedarius M8 GmbH in Duitsland. Het faillissement heeft geen gevolgen voor de vervolging van de vier voormalig directeuren, maar het onderzoek van Kaspersky roept wel de vraag op of de bedrijfsactiviteiten van de Gamma Group daadwerkelijk zijn gestopt.

Gamma Group heeft zich na de verhuizing naar Duitsland namelijk ook deels al verplaatst naar Oost-Europa, het Midden-Oosten en Zuidoost-Azië. De FinFisher Holding die eerst Gamma International Holding heette en nu Vilicius Holding staat nog op het adres van FinFisher ingeschreven, maar net als bij de verhuizing van Engeland naar Duitsland is er slechts een oude huid van lege BV's achtergelaten.

Het bedrijf zelf is verplaatst, maar heeft geleerd van het datalek, de aanklachten in het Verenigd Koninkrijk en Duitsland en vervolging in het laatste land, want van een kantoor met adres voor FinSpy of Wingbird is geen sprake meer.

De nieuwe decentrale Gamma Group?

Twee van de directeuren van de FinFisher bedrijven waartegen door de vier organisaties aangifte is gedaan, Lucian Hanga en Holger Tesche, lijken van het Gamma toneel verdwenen. De derde aangeklaagde directeur Carlos Hugo Gandini is zijn eigen bedrijf AdSum UG begonnen, maar zijn carrière binnen het Gamma netwerk lijkt beëindigd met de overstap naar het cyber intelligence bedrijf CPX in de Emiraten. Lijkt, want misschien is de relatie tussen Gamma Group en CPX een stuk complexer.

CPX is de nieuwe naam van het çybersecurity' bedrijf dat zich eerder Digital 14 (2021) en DarkMatter (2014) noemde. DarkMatter wordt in verschillende media als The Intercept en Ars Technica genoemd als een bedrijf dat surveillance uitvoerd voor de Verenigde Arabische Emiraten. Die surveillance is ook onderdeel van onderzoek van de Amerikaanse FBI naar betrokkenheid van DarkMatter bij de moord op de Amerikaanse journalist Jamal Khashoggi.

Hoewel niet in de aangifte genoemd, maar voor de export naar Turkije wel belangrijk is de directeur van Raedarius M8 GmbH, Christoph Diekhöfer. De export naar Turkije zou namelijk zijn gefaciliteerd door het Bulgaarse bedrijf Raedarius M8 EOOD dat niet alleen verbonden is aan de Duitse Raedarius, maar ook Raedarius Ltd. op Cyprus, een bedrijf waar naar Diekhöfer ook Louthean Nelson aan verbonden is.

Behalve het faillissement van Raedarius in Duitsland zijn de andere vestigingen van het Raedarius netwerk in Bulgarije, Cyprus, Maleisië en de Verenigde Arabische Emiraten nog actief. Parallel aan dit netwerk heeft een voormalig directeur van FinFisher Martin Johannes Münch het bedrijf MuShun GmbH opgezet met ook afdelingen in Maleisië en de Verenigde Arabische Emiraten

Martin Johannes Münch (Martin J. Münch of MJM) wordt soms aangeduid als de 'brains behind Finfisher's Trojan Horse' (Intelligence Online). Hij zou op dit moment FinFisher runnen vanuit de Emiraten. Dit laatste zou kunnen omdat Dubai en Abu Dhabi vrijplaatsen voor veel spyware makers zijn geworden. Of Münch echter de leiding over het netwerk heeft is niet duidelijk.

Buro Jansen & Janssen omschrijft Münch in 'Gamma Group/Louthean Nelson; Wapenhandelaars pur sang' vooral als woordvoerder van Gamma Group die wartaal uitkraamt. Erg overtuigend zijn de zeer beperkte mediaoptredens van Münch namelijk niet. In Britse krant The Guardian struikelt hij in 2012 over het meerderheidsaandeel van Louthean Nelson in het bedrijf.

En in een interview met het Amerikaanse Bloomberg in hetzelfde jaar portretteert Münch zichzelf als slachtoffer omdat hij geen sociaal leven meer heeft door de publiciteit rond FinFisher: "Muench says he's given up on a social life for now. "If I meet a girl and she Googles my name, she'll never call back," he says."

Natuurlijk wast hij zijn handen in onschuld in Bloomberg want Gamma Group is slechts de maker van spyware. Wat de landen ermee doen is niet de verantwoordelijkheid van het bedrijf. Maar als het over Bahrein gaat, gooit hij het plots over een andere boeg. De gevonden FinSpy zou een gestolen demoversie zijn en zonder toestemming gebruikt.

Wat Münch precies bedoeld wordt niet duidelijk in het interview want gestolen betekent in principe altijd gebruik zonder toestemming, maar de 'brains behind FinFisher' spreekt zelfs over een gemodificeerde gestolen demoversie die ergens anders is gebruikt. Het is een nogal gekunsteld verhaal, misschien bedoeld om de eventuele juridische

gevolgen van de verkoop van spyware aan Bahrein te vermijden, maar overtuigend is het niet.

Het Gamma netwerk bestrijkt landen in de Europese Unie (Duitsland, Bulgarije, Cyprus, Roemenië), daar net buiten (Zwitserland, Verenigd Koninkrijk, Britse Maagdeneilanden), het Midden-Oosten (Libanon, de Verenigde Arabische Emiraten) en Zuidoost-Azië (Singapore, Maleisië). Of Mu Shun Fze in de Emiraten en Mu Shun Sdn. Bhd. in Maleisië daaraan direct verbonden is, is door de losse structuur niet meer vast te stellen.

Wel opvallend is dat Louthean Nelson naast zijn hoofdvestiging Mindstone International Pte. Ltd. in Singapore ook een Mindstone International Ltd. op de British Maagdeneilanden (Virgin Islands) heeft geregistreerd, dezelfde constructie die Nelson met zijn Gamma Group in het Verenigd Koninkrijk en Duitsland heeft gehanteerd. De Britse krant The Guardian schaart Nelson in het lijst van grote wapenleveranciers als BAE systems dat in het verleden ook brievenbusfirma's in belastingparadijzen gebruikte voor handels deals.

De olifant in de kamer

Al decennialang beweegt Louthean Nelson zich met zijn wapenhandel in de coulissen van de macht. Hij schudt net zo makkelijk een Saoedische prins de hand als een Egyptische, Libische, Ethiopische of andere repressieve alleenheerser. Dit alles zonder het diplomatieke korps van een invloedrijk land zoals de NSO Group meereist met de Israëlische premier.

Hij is een schim, er zijn weinig beelden van de man, laat staan van een ontmoeting met een regeringsleider. Als een ware kosmopoliet is hij verhuisd van Duitsland naar het Verenigd Koninkrijk, terug naar Duitsland, en via Libanon naar Singapore. De man lijkt onschendbaar. Hij is nooit door overheden aangeklaagd en vervolgd, slechts door individuen en belangenorganisaties, maar niet bij naam. Zelfs de forse tegenslagen bij PK Electronic, CBRN, FinFisher GmbH hebben niet voor

meer dan een rimpeling gezorgd in de voortzetting van zijn bedrijfsvoering.

Die ongrijpbaarheid roept vragen op over de relatie van Nelson met diezelfde overheden. In die context moet de vermelding van PK Electronic als een bedrijf dat nauw samenwerkt met de Amerikaanse inlichtingendienst de CIA worden gezien. Die opmerking komt van Wayne Madsen in zijn boek 'The Almost Classified Guide to CIA Front Companies, Proprietaries & Contractors'.

PK Electronic wordt in het boek omschreven als een bedrijf dat slechte encryptie levert om het afluisteren van diplomatiek verkeer te vergemakkelijken: "Delivering flawed encryption equipment to countries like Sudan to make interception of diplomatic communications easier". Die omschrijving is wat overtrokken, maar hier gaat het om de vraag of PK Electronic een CIA front was.

Omstreden Madsen

Hoewel Madsen een lange staat van dienst heeft bij de Amerikaanse marine en hij ook heeft gewerkt voor de NSA, National Security Agency, en de State Department, het Amerikaanse ministerie van Buitenlandse Zaken, wordt hij in zijn latere jaren als schrijver voor pubicaties als CounterPunch en CovertAction Quarterly, vooral na de Irak oorlog van 2003 meer en meer bevangen door samenzweringstheorieën.

Zo was hij lange tijd gast van The Alex Jones Show, de man die na 11 september 2001 in eerste instantie een kritisch geluid laat horen in de VS, maar langzamerhand ontspoort. Zeker vanaf 2012 toen Jones de schietpartij op de basisschool van Sandy Hook omschreef als een toneelstuk met acteurs, een operatie van inlichtingendiensten en andere beschrijvingen om de gebeurtenis en het leed van mensen volledig te ontkennen.

In 2013 breekt Madsen met Jones, maar verspreidt zelf lange tijd geruchten over de vermeende homoseksualiteit van President Obama en zijn Keniaanse nationaliteit. Al met al een schrijver waarvan uitspraken en beweringen niet zomaar moeten worden overgenomen, maar dat geldt natuurlijk voor alle bronnen ook die van gevestigde media.

Het ingetrokken Observer verhaal blijkt toch juist

Als de Britse krant The Observer, de zondag editie van The Guardian, op 29 juni 2013 een verhaal publiceert over de samenwerking tussen Amerikaanse en Europese inlichtingendiensten bij het verzamelen van persoonsgegevens van burgers voor de Amerikanen steekt er een storm van kritiek op. De krant en vooral de schrijver van het artikel, Jamie Doward, en zijn bron, Wayne Madsen, krijgen veel kritiek te verduren.

Doward lijkt niet te hebben geverifieerd wie Madsen is en het verhaal wordt door The Guardian ingetrokken. Hoewel Madsen misschien samenzweringstheorieën aanhangt, is zijn informatie volledig afwijzen niet de juiste weg, want op dezelfde dag dat The Observer het verhaal van Madsen publiceert en intrekt, brengt Reuters hetzelfde verhaal.

Reuters schrijft op basis van gegevens die openbaar zijn gemaakt door Edward Snowden over de spionage programma's Tempora en Prism, waarmee respectievelijk de Britse inlichtingendienst GCHQ en de Amerikaanse inlichtingendienst NSA in samenwerking met onder andere Denemarken, Duitsland, Frankrijk, Italië, Nederland en Spanje op grote schaal burgers over de gehele wereld afluisteren.

PK Electronic (PKE), een CIA bedrijf?

Al met al is Madsen een schrijver met een wat fluïde pen. Het noemen van PK Electronic (PKE) als een CIA front company kan dus niet

zomaar als waar worden aangenomen, maar aan de andere kant verklaard het wel allerlei aspecten van het Duitse bedrijf die opvallend zijn.

In het artikel 'Wie im Familienclan, Spiegel-Report über den Handel mit deutscher Kriegs-Elektronik' (5 augustus 1985) van het Duitse magazine Der Spiegel wordt PK Electronic omschreven als wapenhandelaar voor met name Afrika en het Midden-Oosten. Veel landen kochten goedkope wapens in Rusland en verbeterden die met duurdere elektronica van PKE die als tussenhandelaar fungeerde voor bedrijven als Philips en dochter Philips Elektro-Spezial, Siemens, AEG-Telefunken, Zeiss, maar ook het Amerikaanse Ocean Applied Research Corp.

Zo belandt afluisterapparatuur, automatische radioscanners of peilapparaten, infrarood en laser instrumenten en nachtzicht apparaten in Saoedi-Arabië, Syrië, Libië, Angola, Soedan, Nigeria, Jordanië, Irak, Taiwan en Indonesië.

In verband met exportbeperkingen is directe verkoop aan die landen in de Koude Oorlog niet mogelijk, maar PK Electronic zorgt voor het ideale kanaal om die export wel mogelijk te maken. Vanuit het perspectief van de Koude Oorlog, het behouden van invloedsferen, het in het zadel houden van repressieve regimes, afluisteroperaties en andere strategische overwegingen zijn de export van bepaalde goederen, hoewel verboden, lucratief om landen uit de invloedsferen van Rusland te houden, regering in die landen af te luisteren of te destabiliseren.

De omvang van de handel van PK Electronic is in de jaren zeventig en tachtig dusdanig dat die niet onopvallend is gebleven voor welke autoriteit dan ook, zeker als PK Electronic de Saoedische kroonprins Prins Abdullah Ibn Nasir Ibn Abd al-Asis Al Saud in 1983 een ritje laat maken in een Duitse Leopard-tank. Die zichtbaarheid voor nationale overheden en de landen waar PK Electronic aan leverde zijn aanwijzingen dat het bedrijf de hand boven het hoofd is gehouden tijdens de Koude Oorlog. Veel van de landen die door het bedrijf zijn bediend, zijn uiteindelijk ook niet volledig toegetreden tot de Russische invloedsferen.

Einde Koude Oorlog en PK Electronic, opkomst Gamma

Met de val de Muur, het uiteenvallen van de Sovjet-Unie en het vermeende einde van de Koude Oorlog verdwijnt het belang van PK Electronic als tussenhandelaar. Het bedrijft struikelt steeds meer over openbaar geworden informatie over export naar Taiwan, Angola en Jordanië/Irak. Exportbeperkingen stapelen zich op zoals door de registratie als leverancier van conventionele wapens door Nederland. Peter Klüver verhuist het bedrijf naar een dorp in de buurt van Hamburg, maar de provincie biedt geen cover. PK Electronic verdwijnt van het geopolitiek toneel.

Louthean Nelson heeft dan allang het zinkende schip verlaten en in het Verenigd Koninkrijk een nieuw imperium gebouwd van digitale wapens. De klanten van weleer zijn in de nieuwe constellatie opnieuw klanten van Gamma Group. Hoewel de Sovjet-Unie is veranderd in Rusland is de conventionele oorlog geëvolueerd in een cyber- en proxy-oorlog.

Naast een informatieoorlog zijn er ook de onzichtbare oorlogen in onder andere Syrië, Libië, de Centraal Afrikaanse Republiek, Soedan, Mali en deels ook economische oorlogen in bijvoorbeeld Kenia, Madagascar en Burkina Faso. Rusland probeert net als China en het Westen haar invloedsferen te bestendigen of uit te breiden. Veel van die landen kenmerken zich door repressieve regimes of instabiele regeringen. Veel van die landen zijn klanten van spyware makers zo ook van Gamma Group.

Mindstone, een CIA front?

En daar komt de link met de inlichtingendiensten weer om de hoek kijken. Veel van de landen die klant zijn van de Gamma Group naast de Europese spelen een rol in het geopolitieke steekspel. Het feit dat leden van oppositie, journalisten en mensenrechtenactivisten, maar ook zoals uit het Noord Macedonische afluisterschandaal blijkt ministers van de eigen regering, zakenmensen, wetenschappers en anderen worden bespied zegt iets over de informatie die de spyware tools verzamelen. Informatie die van onschatbare waarde is voor buitenlandse diensten.

Het verbaast dan ook niet dat in 2022 een engineer van het Franse spyware maker Nexa Technologies (voorheen Amesys) verklaarde, dat het bedrijf een backdoor in haar tool heeft gebouwd. Deze backdoor zou in Libië actief gebruikt worden door de Franse inlichtingendienst DGSE (Direction générale de la Sécurité extérieure). En de geruchten over backdoors zijn niet nieuw. Ook bij de RCS Vinci en Galileo van Hacking Team waren er vragen over een backdoor of kill switch, toegang tot de verzamelde data om die te vernietigen.

Dat Gamma Group niet expliciet verbonden is aan een nationale overheid zoals de NSO Group in Israël kan voor bepaalde landen van belang zijn. Die onafhankelijkheid heeft nadelen als het gaat om het gebrek aan diplomatieke bescherming, maar levert ook in zekere zin onafhankelijkheid op. Deze onafhankelijkheid vertaalt zich bij Gamma Group op een vreemde wijze.

Gamma Group, 'Black Oasis', 'Neodymium', 'Promethium', …

Sinds 2015 berichten verschillende cybersecurity onderzoekers over het gebruik van FinSpy of een tool die erg op FinSpy lijkt, door 'hackersgroepen'. Een van die groepen is door het virus softwarebedrijf Kaspersky 'Black Oasis' genoemd. De groep was plotseling in 2015 actief maar sinds 2017 zijn er volgens onderzoekers geen activiteiten van de groep waargenomen.

Het online magazine Cyberscoop dat veel over digitale veiligheid schrijft, omschrijft in oktober 2017 de groep als een zeer actieve welvarende hackergroep uit het Midden-Oosten die FinFisher gebruiken: "A well-funded, highly active group of Middle Eastern hackers was caught, yet again, using a lucrative zero-day exploit in the wild to break into computers and infect them with powerful spyware developed by an infamous cyberweapons dealer named Gamma Group."

Het verhaal over 'Black Oasis' doet denken aan de verdediging van Münch in het Bahrein afluisterschandaal. Martin Johannes Münch zegt dan niet expliciet dat Gamma Group geen spyware heeft verkocht aan Bahrein, maar dat de gebruikte spyware bij de oppositieleden een gemodificeerde gestolen demoversie is. Geen enkele vertegenwoordiger van FinFisher heeft ooit publiekelijk iets over het gebruik van FinSpy door 'Black Oasis' gezegd, maar het bedrijf zal zeker ontkennen dat het spyware aan hackers heeft verkocht.

En ‘Black Oasis’ is niet de enige die FinFisher gebruikt. Ook de door Microsoft genoemde ‘hackersgroep’ van Turkse origine ‘Neodymium’ ontdekt in 2016 lijkt een FinSpy achtige tool te gebruiken. De relatie met het Midden-Oosten, kapitaalkrachtig en Gamma Group werpt ook een nieuw licht op het toetreden van voormalig topman van FinFisher Carlos Hugo Gandini tot CPX, de nieuwe naam van het mysterieuze bedrijf DarkMatter uit de Emiraten.

Is Mindstone uit Marvel’s comic book ontsnapt?

Het eventuele gebruik van FinFisher door ‘Black Oasis’ en ‘Neodymium’ kan drie dingen betekenen. Of spyware is de grote aanjager van een toekomstige cybercrime golf waarbij spyware veel persoonsgegevens en geld van burgers gaat stelen omdat spyware straks voor veel meer mensen beschikbaar wordt. Of de decentrale opzet van Gamma Group heeft zich vertaald in het ondergronds opereren van het bedrijf verhuld als ‘hackersgroep’. Het kan echter ook betekenen dat Gamma Group een nieuwe lucratieve klant heeft gevonden.

Van een criminele hackersgroep lijkt bij ‘Black Oasis’ geen sprake als naar de slachtoffers wordt gekeken. Het zou gaan om journalisten, denktanks, activisten en de Verenigde Naties en gaan om landen in het Midden-Oosten (Bahrein, Iran, Irak, Jordanië, Saoedi-Arabië), Afrika (Angola, Libië, Nigeria, Tunesië), maar ook Rusland, Afghanistan en Europese landen als het Verenigd Koninkrijk en Nederland.

De landen lijken willekeurig, maar wie zegt dat ‘Black Oasis’ niet voor meerdere overheidsklanten werkt. Dan is plots het profiel van de slachtoffers hetzelfde als wat zichtbaar is bij standaard spyware makers. Van het opereren van ‘Black Oasis’ is iets meer bekend dan van ‘Neodymium’ dat zich vooral op Europa zou richten.

Nederland is dus gebruiker en slachtoffer van spyware van Gamma Group als de gegevens over 'Black Oasis' juist zijn. Erg onlogisch is die gedachte zeker niet. Uiteindelijk gaat het gebruik van spyware waarschijnlijk volledig uit de hand lopen, eigenlijk vergelijkbaar met de wijze waarop sociale media nu meer als een last dan als een lust wordt gezien. Bij spyware zijn de gevolgen echter iets groter dan alleen online haat, belediging of sextortion.

Gamma Group zou dus heel goed kunnen opereren als een front voor de CIA zoals PK Electronic. Het bespieden van 'bevriende' landen in Europa is de Amerikanen niet vreemd zoals de NSA leaks, Snowden, maar ook Madsen hebben aangegeven. Wie er het slachtoffer wordt van spyware is namelijk niet het belangrijkste, wel de klanten van de spyware bedrijven. Meekijken bij die klanten is dan het hoofddoel, de slachtoffers slechts collateral damage.

Met de oogkleppen van de strijd tegen de georganiseerde misdaad lijkt alles geoorloofd, alleen bijt straks die misdaad de rechtstaat in haar staart met dezelfde spyware waarmee ze bestreden wordt. Mindstone leest nu de gedachten en dromen van criminelen, maar straks van crime fighters zeker als niet actief strafrechtelijk onderzoek wordt gedaan naar de handel en wandel van bedrijven die spyware op de markt brengen.

De Mindstone is dan ook crimineler dan georganiseerde misdaad die het zou moeten bestrijden. De gevolgen zijn namelijk veel groter dan het gebruik bij criminaliteitsbestrijding nu. Heel slim is die bestrijding van de georganiseerde misdaad daarom niet. Louthean Nelson zal dat allemaal zeker overleven. Hij is de schim die misschien geen diplomatieke bescherming heeft, maar wel een machtige broodheer.

Naar inhoudsopgave Observant # 81

FinFisher Spyware overview

In the course of several years we collected data on the use of FinFisher spyware. This overview is not at all complete. It could be that some countries did not use the spyware from FinFisher, but we listed these countries nevertheless because their names came up in research from WikiLeaks, Citizen Lab, Privacy International or other organizations/media because for example 'control servers' were located in these countries but also demonstrations were given. This does not necessarily mean anything but the lack of formal denial, formal and open investigation into the existence of these servers and other reluctance to give openness and transparency about the use or existence of spyware in these countries forces Buro Jansen & Janssen to list them.

Then there are three other aspects of the listing which are important to mention. Some countries, for example Cyprus, but also Germany, Italy, and Israel are known for harboring the firms which produce the spyware or export or facilitate the export. This is not separately mentioned but only a reason for their listing. Then as already is said there are of course the meetings, negotiations and demonstration which might not have resulted in the purchase of FinFisher. This might be the case, but because transparency is lacking and countries do not give any accountability to why they meet up with companies which have relations with repressive regimes and could be labelled as criminal organization, these countries appear on the list. Finally there is the case of 'Black Oasis'.

This name is assigned to an unspecified mysterious group which can be a hackers group whether or not related to a company, a state or a governmental body apparently using FinFisher tools in relation to several countries. Mostly it is assigned to some Russian hackers group. The problem is that in a world of spyware which is entangled with secrecy and secret services it is also possible that the targets do not tell the whole story of the group or organization behind the name. It is difficult to tell.

So the countries connected to Black Oasis are also added to the list, especially because no specific investigation into the usage of FinFisher by this group is officially and openly reported or announced. All in all the countries on this list can be labeled as in one way or another connected to FinFisher using the way the authorities always explain their actions towards presumed suspects of terrorism or organized crime, 'when there's smoke, there's fire'.

Then lastly there is the amount of publishing about FinFisher in a country. About FinFisher in some countries a lot is published also because there were some specific cases or other reasons. About other countries much less is published. Some only related to 'Black Oasis'. These countries are still added like Cyprus, Iran, Iraq, Kuwait, Madagascar, Myanmar, Russia, Sweden, Switzerland, Syria, Thailand and Yemen.

The same accounts for the numerous companies and persons involved in FinFisher. What started with one company spiraled into a web of companies from the UK to Germany, Cyprus, Virgin Island, Lebanon, Bulgaria, Malaysia, Singapore and other countries. The web consists of dismantled, sleeping, silent, active and other registries. All creating a web which has all the whole marks of a money Laundering and organized crime operation. Question remains why all these companies amongst which are a lot registered in so-called democratic states were able to sell their goods to these Western countries which paid for spyware to a company about which not only ethical questions could be asked but also tax avoidance, money laundering questions and in relation to that organized crime questions.

Therefor the list of companies is long. Some companies might only be related to property ownership of one or more of the employees or institutional related persons involved in one of the companies which provide spyware, but this is impossible to say because of the nature of the web. Unless persons involved are clear (supported with documents) about their position towards Gamma Group, the trade to repressive regimes, the tax policy of the companies and other aspects of professional and legitimate business operations nothing conclusive can be said about their involvement. So again, 'when there's smoke, there's fire'.

Gamma Group/ FinFisher is regularly related to two other set of companies which are formally nog connected. These are Elaman and Trovicor. Elaman looks the typical reseller which has its own network of companies in Germany, Switzerland, Lebanon, the Emirates and probably Singapore, Indonesia and South Africa. Although it looks like an intermediary, Elaman seems much more connected to the Gamma Group network. It presents itself as closely connected to Gamma TSE, Gamma Group and G2 Systems. As a Technical Sales and Consultancy specialist Elaman seems much more as a covered Gamma Group sales department, less connected then fr example the Raedarius network.

And then there is the Trovicor network which was known as Nokia Siemens Networks or NSN, a joint venture between the Finnish Nokia and the German Siemens. Trovicor looks like a competitor of Gamma Group but the world of spyware companies show similarities of the world of spies, a world or mirrors. Gamma Group worked in the past closely together with Siemens Pte. Elaman sells not only products from Gamma Group, but also Trovicor and Nokia Siemens Networks, VASTech and Utimaco. The Swiss branch of Trovicor is closely connected to the Swiss branch of Elaman. Personnel has been switching from Nokia Siemens Networks to Elaman. Although there are no formal connections between Gamma Group and Trovicor, definitely there are very close relations. If that is still the case remains unclear since the acquisition of Trovicor by the French Boss Industries. Boss Industries also owns Nexa Technologies, formerly known as Amesys.

Then what about the people involved. Starting with father and son Nelson only a few people have come in the limelight over the years, these are mainly Stefan of Stephen Oelker of Stephan Ölkers, who died in 2016, and Martin Johannes Münch (Muench). For the rest the listed persons are connected to one or more companies related to the network of Gamma Group and FinFisher. Interesting example is for example Christoph Diekhöfer. A person who is vaguely related to the network although he pops up in relation to a company in Cyprus, connected to Louthean Nelson and connected to export of FinFisher. So again, are these people involved in providing spyware to repressive regimes, tax avoidance, money laundering, criminal activities? Question mark yes, but also no, because if you define the Gamma Group as an organized crime group providing repressive regimes and other criminal activities with tools to violate human rights then every person in that group could be a suspect in an investigation. So definitely smoke, and 'when there's smoke, there's fire'.

Related companies (dismantled, sleeping, silent, active and other registries):

In the United Kingdom: Gamma International (UK) Ltd, Gamma TSE Limited, Gamma 2000 Limited, Gamma 2000 Waste Management Limited, G2 Systems Limited, The CBRN Team Limited, Computplus Limited, Finfisher Limited, T.S. Comms Limited, Gamma Cyan Limited, Personal Protection Products Limited, Compass Military Services Limited
In Germany: PK Electronic International Limited, Gamma International GmbH, Gamma International Sales GmbH, Gamma International Holding GmbH, FinFisher GmbH, FinFisher Labs GmbH, FinFisher Holding GmbH, Raedarius m8 GmbH, So m8 GmbH, Lench IT Solutions Plc, SIS Eastern Europe GmbH, SIS Romania GmbH, Vilicius Holding GmbH, Martin J. Muench GmbH, MuShun GmbH
In Germany, probably not directly related to the production of spyware, although not conclusive but might be related to trade and/or trade relations: Villa Deta GmbH, SO Verwaltungsgesellschaft mbH, VGL Verwaltungsgesellschaft mbH, hph Immobilienberatung GmbH, hph consulting GmbH, Objekt 5001 GmbH, Quaestus Alp47 GmbH, Quaestus alpha GmbH, AK Invest Gmbh, SIS Solar Installation Service, AdSum UG, H & D Holding GmbH, GM Vermögensverwaltung GmbH, IQbyte GmbH, NTT Security (Germany) Services GmbH,
In Switzerland: Gamma Sales AG, FinFisher AG, Amador AG, Raedarius AG, Gamma Global Holding AG, Global Environnement Capital SA
In Bulgaria: Raedarius M8 EOOD (РАЕДАРИУС М8 ЕООД)
In Singapore: Mindstone International Pte. Ltd., Global Surveillance Systems, BizCorp Management Pte Ltd.,
In Malaysia: Raedarius M8 Sdn. Bhd., Mu Shun (Malaysia) Sdn. Bhd.
In Lebanon: Gamma Group International SAL, Alaman – German Security Solutions SAL, Gamma Cyan SAL Offshore, Cyan Engineering Services SAL, Mtrac?
In the British Virgin Islands: Gamma Group International Limited, Mindstone International LTD
In Cyprus: GTSC LTD, Gamma International Ltd, Gamma 2000 (Cyprus) Limited, Raedarius Limited
In the United Arab Emirates: Mu Shun Fze (?), Raedarius (Media, IT & Telecommunication)

The several branches of Elaman: Elaman GmbH (Germany), Alaman - German Security Solutions Sal Offshore (Lebanon), Elaman ME FZE (UAE/Dubai), Elaman AG (Switzerland)(probably also companies in Singapore, Indonesia and South Africa)

The several branches of Trovicor: Trovicor gmbh (Germany), Trovicor holding GmbH, Datafusion Systems GmbH (Germany), Datafusion Holding GmbH (Germany), Intelligence Solutions Holding GmbH (Germany), Blitz 08-500 GmbH (Germany), Trovicor AG (Switzerland), Trovicor (Smc Pvt.) Ltd. (Pakistan), Trovicor SOLUTIONS FZ LLC (UAE/Dubai), Trovicor Fz-Llc (UAE/Dubai), Trovicor Technology Sdn. Bhd. (Malaysia), TROVICOR SDN. BHD. (Malaysia), Eirene - Trovicor Solutions India Pvt.Ltd (India), Trovicor s.r.o. (Czech Republic), Trovicor LLC (Oman), Trovicor solutions asia limited (Hong Kong), Trovicor (full name?, Lebanon)

Related persons:

Peter Klüver (PKI Electronic Intelligence GmbH)
William Louthean Nelson (Gamma TSE Limited, FinFisher Limited, Gamma 2000 Waste Management Limited, Gamma International (UK) Limited, Gamma 2000 Limited, Gamma Cyan, Limited, G2 Systems Limited, Computplus Limited, Compass Military Services Limited)
Louthean John Alexander Nelson (PKI Electronic Intelligence GmbH, PK Electronic International Limited, PK Electronic International Corporation, Gamma TSE Limited, FinFisher Limited, Gamma 2000 Waste Management Limited, Computplus Limited, Gamma International (UK) Limited, the CBRN Team Limited, Gamma 2000 Limited, Gamma Cyan, Limited, G2 Systems Limited, BN Management Security Systems Ltd, Axcition Europe, Gamma Tema Consultants, Gamma International Ltd, Gamma International GmbH, Gamma Group International SAL, GTSC LTD, Gamma International Ltd, Gamma 2000 (Cyprus) Limited, Raedarius Limited, Mindstone International Pte. Ltd., Global Surveillance Systems, BizCorp Management Pte Ltd, Gamma Group International Limited, Mindstone International Ltd)
Brydon Stewart Deas Nelson (Gamma Cyan, Limited, G2 Systems Limited)
Pauline Louise Nelson (G2 Systems Limited, Computplus Limited, Gamma 2000 Waste Management Limited, Gamma 2000 Limited)
Jacob Perch Nelson (the CBRN Team Limited)
Derek Alan Myers (Gamma TSE Limited, PK Electronic International Limited)
Martyn Russell Myers (Gamma TSE Limited)
Christine-Ann Myers (Gamma TSE Limited)
Thomas Fisher (Gamma International)
Mohamed Farid Matar (Gamma Group International SAL)
Edgar Bucheli (Gamma International Asia)
Johnny Debs (Cyan Engineering Services Sal)
Emmanuel Chagot
David John Wood (Gamma Cyan Limited)
Julian Oliver Snell (Gamma Cyan Limited)
Karen Jean Seymour (G2 Systems Limited)

Stefan of Stephen Oelker of Stephan Ölkers (died in 2016): (Vilicius Holding GmbH (FinFisher Holding GmbH, Gamma International Holding GmbH), so m8 GmbH, raedarius m8 GmbH, FinFisher GmbH, FinFisher Labs GmbH, Mtrac? (Libanon)
Sascha Markus Kampf (Vilicius Holding GmbH, so m8 GmbH, FinFisher Holding GmbH, Villa Deta GmbH, SO Verwaltungsgesellschaft mbH, VGL Verwaltungsgesellschaft mbH, hph Immobilienberatung GmbH, hph consulting GmbH, Objekt 5001 GmbH, raedarius m8 GmbH, Quaestus Alp47 GmbH)
Andreas Knab (Villa Deta GmbH, SIS Eastern Europe GmbH, AK Invest Gmbh, SIS Solar Installation Service)
Georg Glatzeder (VGL Verwaltungsgesellschaft mbH)
Katja Gogalla (VGL Verwaltungsgesellschaft mbH)
Martin Johannes Münch (Muench) (raedarius m8 GmbH, FinFisher GmbH, Vilicius Holding GmbH, Martin J. Muench GmbH, MuShun GmbH, FinFisher GmbH, FinFisher Labs GmbH, FinFisher Labs GmbH)
Carlos Hugo Gandini (Trovicor, AdSum UG, H & D HOLDING GMBH, FinFisher GmbH, Gamma Group, Gamma International)
Holger Tesche (GM Vermögensverwaltung GmbH, FinFisher Labs GmbH, Gamma International GmbH)
Lucian of Lucien Hanga (FinFisher Labs GmbH, Gamma International GmbH)
Daniel Maly (FinFisher GmbH)
Christoph Diekhöfer (raedarius m8 GmbH, Raedarius Limited)
Georg Johann Magg (FinFisher Labs GmbH, Raedarius m8 GmbH, IQbyte GmbH, NTT Security (Germany) Services GmbH, Integralis Deutschland GmbH, Integralis Services GmbH, Activis Ismaning GmbH, Activis GmbH, NTT Com Security (Deutschland) Services GmbH, NTT Com Security (Germany) Services GmbH), Integralis AG, Nocitra Limited (voorheen Articon-Integralis Limited, Integralis Limited, Intercede 601 Limited), NTT Security UK Limited (voorheen NTT Com Security (UK) Limited, Integralis Limited, Integralis Network Systems Limited, Coleslaw 355 Limited, Silversky EU GmbH)
Harald Heid (IQbyte GmbH, MTI Technology GmbH)
Michael Marr (IQbyte GmbH)
Nicolas Mayencourt (Dreamlab)
Peter Habertheuer (Vastech AG, Nokia Siemens Networks, Elaman GmbH)

Monika Frech-Hänggi (Vastech AG, Elaman AG, FAI AG, Famoex AG, Kialo AG, S.A. de la Communication Sécurisée SCS, SBI Consulting- und Verwaltungs- AG, Priparop S.A., Falcontec SA, Marphil AG)
Henning Möller (Elaman AG, Trovicor AG, Falcontec SA, FAI AG, Kialo AG (Ciphire Labs GmbH/ Kialo GmbH))
Markus Michael Meiler (Elaman AG, Elaman GmbH, inseen UG)
Holger Günther Rumscheidt (Elaman GmbH, Elaman AG, MAELU Franchise Gmb, Toleo GmbH)
Eugen Fissl (Elaman GmbH)
Wolfgang Sandow (Famoex AG, Falcontec SA, WKW AG)
Georg Johann Magg (FinFisher Labs GmbH, raedarius m8 GmbH, IQbyte GmbH, NTT Security (Germany) Services GmbH (Integralis Deutschland GmbH, Integralis Services GmbH, Activis Ismaning GmbH, Activis GmbH, NTT Com Security (Deutschland) Services GmbH, NTT Com Security (Germany) Services GmbH), Integralis AG, Nocitra Limited (voorheen Articon-Integralis Limited, Integralis Limited, Intercede 601 Limited), NTT Security UK Limited (voorheen NTT Com Security (UK) Limited, Integralis Limited, Integralis Network Systems Limited, Coleslaw 355 Limited))

Disclaimer

Buro Jansen & Janssen does not claim that this research is fully satisfactory, but it is an attempt to protect the rule of law by which suspects have insight in the way evidence is gathered and by which the legitimacy of evidence can be proven beyond a reasonable doubt. Spyware, and in this case FinFisher, has all the whole marks of a black box by which evidence is collected which cannot be verified beyond a reasonable doubt that it is truly evidence and not fabricated proof of guilt by a state or even a non-state actor. This doubt is enlarged because of the secrecy and the lack of transparency by both states and companies of the usages, inner workings, limitations, security entity breaches and other aspects of the used spyware. In the case of FinFisher the use by a non-identified, for now named 'Black Oasis', questions also the fact if law enforcement agencies are the only actors targeting the suspects. It opens Pandora's Box of possibilities to fabricate evidence of wrongdoing. And in the case of FinFisher there is not only the possibility of violation of export regulations, but also the questions about tax evasion, money laundering, espionage and other criminal activities in relation to the export and usage of spyware by repressive regimes. Because isn't there a possibility that 'Black Oasis' is part of the FinFisher network. This is not an unreasonable conclusion. No official investigation has been started in relation to 'Black Oasis', no official publication and statement has been issued in relation to 'Black Oasis', so everything is possible.

In the case that you or your company is listed here and this is not correct, Buro Jansen & Janssen will correct this if beyond a reasonable doubt the claim of not being connected to the Gamma Group network is made public.

The countries

Angola

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

https://advox.globalvoices.org/2014/02/26/digital-surveillance-in-angola-and-other-less-important-african-countries/

https://www.computerworld.com/article/2497737/new-mac-spyware-found-on-angolan-activist-s-computer.html

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Australia

https://www.itnews.com.au/news/nsw-police-named-as-finfisher-spyware-user-392090

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Austria
https://citizenlab.ca/2013/04/for-their-eyes-only-2/

https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf

https://www.schneier.com/blog/archives/2013/05/more_on_finspyf.html

https://www.helpnetsecurity.com/2013/05/02/finfisher-spy-kits-cc-servers-are-popping-up-around-the-world/
https://feathersproject.wordpress.com/tag/finfisher/

Bahrain
https://privacyinternational.org/blog/1231/bahraini-government-help-finfisher-tracks-activists-living-united-kingdom

https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://globalvoices.org/2014/08/10/evidence-suggests-bahrains-government-hacked-its-own-fact-finding-commission/

https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

https://web.archive.org/web/20140815233325/https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

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

Bangladesh
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

https://www.ecoi.net/en/document/2060896.html

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Belgium
https://www.datapanik.org/2014/09/18/finfisher-spyware-in-belgie/

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

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

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

Bosnia and Herzegovina
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Brazil
https://www.br.de/nachrichten/bayern/razzia-bei-muenchner-spionage-firma,SDJtroG

https://web.archive.org/web/20201026065537/https://www.tagesschau.de/investigativ/ndr/spaehsoftware-finfisher-101.html

http://www.transparencia.mg.gov.br/component/transparenciamg/despesa-orgaos/2019/01-01-2019/31-12-2019/3888/1868/546/21/40

http://transparencia.mpmg.mp.br/arquivo/licitacoes_contratos_e_convenios/contratos/contratos/2020/CONTRATOS_2020-07.xls

https://www.mpmg.mp.br/files/diariooficial/DO-20191219.PDF#page=140

https://www.mpmg.mp.br/files/diariooficial/DO-20191221.PDF#page=461

Brunei
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf

Bulgaria
https://bivol.bg/en/finspy-bulgaria-mtitc-english.html

https://bivol.bg/finspy-bulgaria.html#english

https://www.helpnetsecurity.com/2013/05/02/finfisher-spy-kits-cc-servers-are-popping-up-around-the-world/

https://www.security.nl/posting/402911/EFF+hekelt+vermeende+aanschaf+Finfisher+door+Nederland

Canada
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.huffpost.com/archive/ca/entry/finfisher-spyware-canada-among-25-countries-hosting-servers-for_n_2876724

https://www.cbc.ca/news/politics/servers-in-canada-linked-to-finfisher-spyware-program-1.1351993

https://openmedia.org/article/item/spying-software-linked-canadian-servers

Cyprus
https://www.propublica.org/article/leaked-docs-show-spyware-used-to-snoop-on-u.s.-computers

Czech Republic
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.rapid7.com/blog/post/2012/08/08/finfisher/

https://buggedplanet.info/index.php?title=CZ

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Egypt
https://buggedplanet.info/images/a/a2/EG-2011-Finfisher-Gamma-DE.PDF

https://archive.f-secure.com/weblog/archives/00002114.html

https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

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

https://www.dandc.eu/en/article/egyptian-regime-uses-spyware-against-critics-some-it-bought-european-companies

https://www.israeldefense.co.il/en/node/45584

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

Estonia
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://news.err.ee/113620/wikileaks-estonia-spent-over-1-million-on-spyware

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

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Ethiopia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.vice.com/en/article/j5d8ng/ethiopia-allegedly-spied-on-security-researcher-with-israel-made-spyware

https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk

https://nakedsecurity.sophos.com/2017/03/16/court-blocks-american-from-suing-ethiopia-over-alleged-hacking/

http://america.aljazeera.com/articles/2015/7/13/foreign-cyber-spying-on-us-citizens.html

https://ethiounite.blogspot.com/2015/07/lawsuit-alleges-that-addis-ababa-used.html

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Gabon

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

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Germany

https://www.itnews.com.au/news/german-police-building-malware-329254

https://netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisher-finspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

Hungary
https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

India
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://cis-india.org/internet-governance/blog/fin-fisher-in-india-and-myth-of-harmless-metadata

Indonesia
https://www.abc.net.au/news/2016-01-26/notorious-spyware-used-to-take-over-computers-found-in-sydney/7114734

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

https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

https://www.abc.net.au/news/2016-01-26/notorious-spyware-used-to-take-over-computers-found-in-sydney/7114734

https://privacyinternational.org/blog/1540/elaman-and-gamma-whats-selling-and-whos-buying-indonesia

Iran
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

Iraq
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

Italy
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

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

Japan
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

Jordan
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://ammannet.net/sites/default/files/2022-04/Jordan%20report-final_0.pdf

https://daraj.com/en/89117/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Kazakhstan
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Kenya
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

Kuwait
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://advox.globalvoices.org/2014/09/05/exclusive-german-companies-are-selling-unlicensed-surveillance-technologies-to-human-rights-violators-and-making-millions/

https://www.spiegel.de/politik/deutschland/deutsche-spaehtechnik-gabriels-ausfuhrkontrollen-bleiben-wirkungslos-a-987555.html

https://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf

Latvia
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

https://www.wikileaks.org/spyfiles/docs/GAMMA-2011-LoutNels-en.pdf

Lebanon
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

https://middle-east-online.com/en/lebanon%E2%80%99s-operation-%E2%80%98dark-caracal%E2%80%99-and-shia-link

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

Libya
https://netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_Technical-Appendix_ENG.pdf

https://bahrainileaks.com/en/2021/03/01/espionage/

Lithuania
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/04/for-their-eyes-only-2/

https://cyberwar.nl/d/fortheireyesonly.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

Madagascar
https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

https://buggedplanet.info/index.php?title=MG

Malaysia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.digitalnewsasia.com/digital-economy/malaysian-govt-spyware-use-may-be-unconstitutional-call-for-action

https://www.theedgemarkets.com/article/minister-no-proof-surveillance-software-server-used-malaysia

https://publications.parliament.uk/pa/cm201415/cmselect/cmquad/608/608iii.pdf

https://www.theedgemarkets.com/article/minister-no-proof-surveillance-software-server-used-malaysia

Mexico
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Mongolia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://wiki.piratenpartei.de/FinFisher

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

Morocco
https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/

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

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Myanmar
https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Netherlands
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

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

Nigeria
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

https://www.arise.tv/report-nigerias-military-acquired-equipment-to-spy-on-citizens-calls-active-since-2015/

North Macedonia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/

Oman
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.theregister.com/2015/05/20/omani_intel_docs/

https://www.corpwatch.org/article/turkmenistan-and-oman-negotiated-buy-spy-software-wikileaks

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Pakistan
https://bolobhi.org/faq-what-is-finfisher-what-is-it-doing-in-pakistan/

https://upload.wikimedia.org/wikipedia/commons/7/77/GISwatch_2014_PDF.pdf

https://www.dawn.com/news/1127405

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Panama
https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

https://www.aies.at/download/2020/AIES-Studies-Colonial-Cables.pdf

Paraguay
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

Qatar
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://dohanews.co/wikileaks-qatar-spent-qr3-2-million-computer-snooping-software/

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

Romania
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Russia
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

Saudi Arabia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Serbia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.cigionline.org/articles/in-the-former-soviet-bloc-the-democratic-dreams-of-1989-continue-to-fade/

Singapore
https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Slovakia
https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://wikileaks.org/spyfiles4/database.html

Slovenia
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

South Africa
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://mybroadband.co.za/news/security/110288-did-sa-government-blow-e2-million-on-spyware.html

https://advox.globalvoices.org/2014/02/26/digital-surveillance-in-angola-and-other-less-important-african-countries/

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

https://theconversation.com/leaked-emails-ramaphosas-hypocrisy-on-spying-by-the-south-african-state-83605

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

Spain
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://duo.com/decipher/pegasus-spyware-operations-targeted-uk-gov-officials-catalans-in-spain

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

Sweden
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://www.securityweek.com/windows-zero-day-exploited-fruityarmor-sandcat-threat-groups/

Switzerland
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://www.wikileaks.org/spyfiles/docs/GAMMA-2011-LoutNels-en.pdf

Taiwan
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

Thailand
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://www.vice.com/en/article/aemeae/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers

Tunisia
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1749&context=auilr Trovicor

https://www.eff.org/nl/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa Trovicor

https://web.archive.org/web/20150330102727/http://database.statewatch.org/article.asp?aid=32351 German authorities

https://info.publicintelligence.net/EU-MassSurveillance-1-Annex1.pdf

Turkey
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf

https://www.reuters.com/article/germany-turkey-spyware-idUSL5N25W29M

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

https://thearabweekly.com/erdogans-vast-espionage-apparatus-helps-him-crack-down-opponents

https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Turkmenistan
https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

https://www.corpwatch.org/article/turkmenistan-and-oman-negotiated-buy-spy-software-wikileaks

https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

UAE
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

Uganda
https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

https://www.monitor.co.ug/uganda/news/national/police-buys-israeli-phone-hacking-tool-3928802

Ukraine

https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf

United Kingdom

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

United States

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Venezuela

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

https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf

https://cdn.netzpolitik.org/wp-upload/2019/09/2019-07-05_FinFisher_Criminal-Complaint_ENG.pdf

Vietnam

https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ control servers for FinSpy

https://www.silicon.co.uk/workspace/british-surveillance-kit-used-in-somalia-vietnam-110302

https://www.theguardian.com/technology/2014/sep/16/wikileaks-finfisher-files-malware-surveillance

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

Yemen
https://arstechnica.com/tech-policy/2014/08/leaked-docs-show-spyware-used-to-snoop-on-us-computers/

https://www.eff.org/nl/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa Trovicor

https://leonievanbreeschoten.nl/wp-content/uploads/2018/02/Leonie-van-Breeschoten-Dealing-in-Deadly-Software.pdf Trovicor

Additional

'Black Oasis'
https://www.infosecuritymagazine.nl/nieuws/kaspersky-lab-ontdekt-adobe-flash-zero-day-met-nederlandse-slachtoffers

https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

https://www.scmagazine.com/news/content/did-israel-deliver-spyware-using-adobe-flash-0-day-in-word-document

https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-discovers-adobe-flash-zero-day

StrongPity
https://ahvalnews.com/turkey/uncontrollable-mess-proliferation-state-spyware

https://www.bleepingcomputer.com/news/security/strongpity-hackers-target-android-users-via-trojanized-telegram-app/

https://www.zdnet.com/article/this-is-how-promethium-malware-operators-used-security-research-bulletins-in-their-favor/

extra
https://anti-interception.com/spyware-en/

Trovicor
https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1749&context=auilr

https://www.privacyinternational.org/blog/our-oecd-complaint-against-gamma-international-and-trovicor

Hacking Team
https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/CITIZEN_LAB.pdf

Naar inhoudsopgave Observant # 81

DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (samenvatting)

Het Duitse bedrijf DigiTask was een van de eerste bedrijven die software ontwikkelde om computers en telefoons te hacken en te doorzoeken. De Duitse overheid gebruikte sinds 2007 de spyware van DigiTask. Het bedrijf leverde haar spyware ook aan Nederland.

In 2011 werd de spyware onderzocht door het hackerscollectief CCC en de Duitse landelijke databeschermingsautoriteiten en die van verschillende deelstaten, waaronder Beieren. Het is een van de weinige keren dat spyware uitgebreid is onderzocht door derden en niet door de leverancier of de overheid die de spyware gebruikt.

Uit deze onderzoeken blijkt dat de politie weinig inzicht heeft in de werking van de tools van DigiTask en de wijze waarop gegevens verkregen worden. De leverancier, en mogelijk derden, kunnen toegang krijgen tot de spyware, gegevensdragers van verdachten en servers en kunnen gegevens, toevoegen of wijzigen. De onderzoeken leggen de tekortkomingen bloot die inherent zijn aan alle commerciële spyware. De betrouwbaarheid van het verkregen bewijsmateriaal is bij alle commerciële spyware in het geding.

Volgens de Duitse overheid wordt spyware, waaronder die van DigiTask, ingezet bij de bestrijding van terrorisme en zware georganiseerde criminaliteit. Het is echter moeilijk om deze claim te beoordelen. De Duitse overheid publiceert, net als andere landen, nauwelijks gegevens over de inzet van spyware, zoals het aantal en het type zaken waarin spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf.

Mediaberichtgeving, rapporten van databeschermingsautoriteiten en andere openbare bronnen duiden erop dat de spyware van DigiTask nauwelijks is ingezet in onderzoek naar verdachten van terrorisme, maar vooral bij onderzoeken naar minder zware vergrijpen. Het is onduidelijk in hoeveel zaken dit daadwerkelijk tot een veroordeling heeft geleid.

Ook andere landen, waaronder Zwitserland, België en Nederland, hebben de tools van het Duitse bedrijf aangeschaft. Toenmalig Minister van Veiligheid en Justitie Opstelten verklaarde in 2011 dat de Nederlandse politie de spyware van DigiTask had aangekocht, nadat dit eerder door het Duitse bedrijf zelf naar buiten was gebracht. Het lijkt erop dat de Nederlandse politie de spyware in ieder geval tot 2014 is blijven gebruiken.

In de loop der jaren heeft DigiTask miljoenen euro verdiend aan de verkoop van spyware aan niet alleen de Duitse overheid, maar ook aan buitenlandse overheden. Dit valt ten minste opmerkelijk te noemen. Het bedrijf leverde onveilige en onbetrouwbare apparatuur. Bovendien heeft het bedrijf een verleden van corruptie en een veroordeling vanwege het betalen van steekpenningen. DigiTask is in 2018 overgenomen door Rohde & Schwarz.

De Nederlandse overheid heeft tot nu toe geen openheid van zaken gegeven over de inzet van DigiTask. Woo-verzoeken van Buro Jansen & Janssen blijven deels onbeantwoord, openbaar gemaakte documenten zijn grotendeels onleesbaar gemaakt.

Naar inhoudsopgave Observant # 81

DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)

Het Duitse bedrijf DigiTask was een van de eerste bedrijven die software ontwikkelde om computers en telefoons te hacken en te doorzoeken. De Duitse overheid gebruikte sinds 2007 de spyware van DigiTask. Het bedrijf leverde haar spyware ook aan Nederland.

In 2011 werd de spyware onderzocht door het hackerscollectief CCC en de Duitse landelijke databeschermingsautoriteiten en die van verschillende deelstaten, waaronder Beieren. Het is een van de weinige keren dat spyware uitgebreid is onderzocht door derden en niet door de leverancier of de overheid die de spyware gebruikt.

Uit deze onderzoeken blijkt dat de politie weinig inzicht heeft in de werking van de tools van DigiTask en de wijze waarop gegevens verkregen worden. De leverancier, en mogelijk derden, kunnen toegang krijgen tot de spyware, gegevensdragers van verdachten en servers en kunnen gegevens, toevoegen of wijzigen. De onderzoeken leggen de tekortkomingen bloot die inherent zijn aan alle commerciële spyware. De betrouwbaarheid van het verkregen bewijsmateriaal is bij alle commerciële spyware in het geding.

Volgens de Duitse overheid wordt spyware, waaronder die van DigiTask, ingezet bij de bestrijding van terrorisme en zware georganiseerde criminaliteit. Het is echter moeilijk om deze claim te beoordelen. De Duitse overheid publiceert, net als andere landen, nauwelijks gegevens over de inzet van spyware, zoals het aantal en het type zaken waarin spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf.

Mediaberichtgeving, rapporten van databeschermingsautoriteiten en andere openbare bronnen duiden erop dat de spyware van DigiTask nauwelijks is ingezet in onderzoek naar verdachten van terrorisme, maar vooral bij onderzoeken naar minder zware vergrijpen. Het is onduidelijk in hoeveel zaken dit daadwerkelijk tot een veroordeling heeft geleid.
Ook andere landen, waaronder Zwitserland, België en Nederland, hebben de tools van het Duitse bedrijf aangeschaft. Toenmalig Minister van Veiligheid en Justitie Opstelten verklaarde in 2011 dat de Nederlandse politie de spyware van DigiTask had aangekocht, nadat dit eerder door het Duitse bedrijf zelf naar buiten was gebracht. Het lijkt erop dat de Nederlandse politie de spyware in ieder geval tot 2014 is blijven gebruiken.

In de loop der jaren heeft DigiTask miljoenen euro verdiend aan de verkoop van spyware aan niet alleen de Duitse overheid, maar ook buitenlandse overheden. Dit valt ten minste opmerkelijk te noemen. Het bedrijf leverde onveilige en onbetrouwbare apparatuur. Bovendien heeft het bedrijf een verleden van corruptie en een veroordeling vanwege het betalen van steekpenningen.

Van Reuter Leiterplatten naar DigiTask

Digi Task GmbH Gesellschaft für besondere Telekommunikationssysteme wordt in 2000 opgericht in Haiger in de deelstaat Hessen. De voorloper van het bedrijf is Reuter Leiterplatten GmbH, dat vanaf 1986 samen met Reuter Electronic afluisterapparatuur voor de Duitse opsporings- en inlichtingendiensten ontwikkelde. DigiTask is zeer nauw verbonden met het bedrijf Reuter Electronic GmbH van eigenaar Hans-Hermann Reuter.

DigiTask is een van de eerste bedrijven die software aanbiedt om computers en telefoons te hacken en binnen te dringen. De software is betrekkelijk goedkoop en eenvoudig te gebruiken, in vergelijking met bijvoorbeeld FinFisher van Gamma Group en DaVinci (Da Vinci) en Galileo RCS (Remote Control System) van Hacking Team.

DigiTask begeeft zich op de internationale markt. Zo presenteert het bedrijf zich op de ISS World beurzen. 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. Ook het Nederlandse Fox-IT is op de beurzen te vinden, net als ambtenaren van Nederlandse ministeries, het Nederlands Forensisch Instituut en politiefunctionarissen van de toenmalige KLPD (Korps landelijke politiediensten, nu de landelijke eenheid).

DigiTask presenteert haar producten op de ISS World beurzen in 2008 en 2009 in Dubai en van 2008 tot en met 2010 en 2012 in Praag. In presentaties uit oktober 2008 en juni 2009 stelt Dr. Michael Thomas dat DigiTask al jaren actief is op de surveillance markt en speciale oplossingen voor afluisteroperaties ontwikkelt.

Het bedrijf beweert dat het marktleider is in Duitsland. "*Digitask has overall experience of many years in LI systems, is market leader for LI in Germany and is privately owned and independent (LI Lawful Interception)*", aldus zijn presentatie op ISS World in 2008 over 'Remote Forensic Software'.

Dat DigiTask marktleider in Duitsland is wordt opnieuw onderstreept op de ISS World beurs in Praag in juni 2009 door twee andere medewerkers van het bedrijf: Tobias Hain tijdens de presentatie "Challenges in Intercepting WiFi" en Thomas Kröckel bij "Future Challenges in the Lawful Interception of IP based Telecommunication."

DigiTask in Beieren

In 2008 wordt bekend dat de Beierse overheid gebruik maakt van de spyware van DigiTask. De Duitse Piratenpartij maakt via WikiLeaks twee documenten openbaar die wijzen op de ontwikkeling/aanschaf van interceptie programmatuur door de Beierse overheid.

Een document is een brief van het Beierse Ministerie van Justitie aan het Openbaar Ministerie in München over de kosten van de aanschaf en welke instantie de rekening gaat betalen.

In de brief wordt gesproken over de aanschaf van software van de firma DigiTask waarmee VoIP-gesprekken (Voice over IP) kunnen worden afgetapt. De spyware wordt direct of via een e-mail geïnstalleerd op de computers van verdachten om programma's zoals het destijds populaire Skype af te luisteren en beveiligde communicatie van verdachten te ontsleutelen. Dit gebeurt bijvoorbeeld met een 'Skype Capture Unit', die gesprekken real time kan streamen naar de Duitse autoriteiten. De ontsleutelde bestanden worden verstuurd naar een server die tegelijkertijd tien gesprekken via Skype kan opnemen. Het Skype-gesprek zelf wordt niet onderbroken. Het gaat om een zogenaamd 'man in the middle' aanval die moeilijk te ontdekken is voor de persoon waarbij de tool wordt gebruikt.

Het andere document betreft een aanbod van DigiTask van 4 september 2007 om software te leveren waarmee Skype-gesprekken van verdachten kunnen worden afgeluisterd. Het bedrijf rekent 3.500,00 euro per maand voor het huren van de software. Eenmalig wordt 2500 euro in rekening gebracht voor installatie en verwijderingskosten van de computer van de verdachte. Voor datzelfde bedrag decodeert DigiTask de communicatie van de verdachte met zijn bank, online winkels, web-mail, e-mail, chatprogramma's, andere internetactiviteiten en programma's op de verdachte computer. Volgens het document kost een abonnement voor de tool 200.000 euro per jaar.

Het is een gevoelig onderwerp voor de Duitse autoriteiten. Op 11 september 2008 doet de politie een inval op het privéadres van een van de woordvoerders van de Piratenpartij en neemt computers in beslag. De overheid is op zoek naar de anonieme bron die de twee documenten aan de Piratenpartij heeft gelekt. De Duitse overheid wil niet dat openbaar wordt dat de politie spyware of - zoals de tools in Duitsland worden genoemd - Staatstrojaner (overheidsmalware) gebruikt.

De Duitse wetgeving biedt op dat moment wel enige ruimte voor het gebruik van spyware door de overheid. Het Duitse verleden en de sterk ontwikkelde privacy cultuur in het land zorgen echter voor een stevige oppositie. Door de spyware als Staatstrojaner te labelen en te spreken over 'Stasi 2.0' domineren de tegenstanders van de inzet van spyware lange tijd het publieke debat in Duitsland.

Daarnaast is het zeer opmerkelijk dat de Duitse overheid producten van DigiTask koopt, vanwege het dubieuze verleden van het bedrijf.

Steekpenningen

De voorganger van DigiTask was Reuter Leiterplatten. Eind vorige eeuw werd de directeur van dit bedrijf, Hans-Hermann Reuter, tevens bedrijfsleider van Reuter Electronic, gearresteerd in verband met het (gedurende een periode van tien jaar) betalen van steekpenningen aan ambtenaren van de douane. In 2002 werd Reuter wegens corruptie veroordeeld tot 21 maanden gevangenisstraf en een boete van 1,5 miljoen euro. Volgens het tijdschrift *Focus* heeft Reuter door het betalen van steekpenningen 50 miljoen Duitse Mark aan opdrachten voor het bedrijf binnengehaald.

Reuter Leiterplatten was volgens ZDF en het tijdschrift *Wirtschaftswoche* in de jaren negentig ook bereid om illegaal afluisterapparatuur te leveren aan Deutsche Telekom voor het afluisteren van medewerkers van het bedrijf. Uit interne documenten van Deutsche Telecom blijkt dat 120 gesprekken van vier telefoonnummers werden afgeluisterd. De drie afgeluisterde personen werden in december 1996 verdacht van een mogelijke hackaanval op de systemen van Deutsche Telecom. Het bedrijf luisterde de medewerkers af zonder gerechtelijk bevel. Toen het toenmalige Bundesministerium für Post und Telekommunikation hiervan op de hoogte werd gesteld bestempelde het de operatie als illegaal.

Na de arrestatie van Reuter in 1999 en de naamsverandering van Reuter Leiterplatten in DigiTask in 2000 werd – in overleg met het Ministerie van Justitie - Deloitte Deutschland formeel verantwoordelijk voor het bedrijf, hetgeen het tot 2006 zou blijven. Deloitte zegt niet actief betrokken te zijn geweest bij de bedrijfsvoering. Het heeft naar alle waarschijnlijkheid alleen het bedrijf draaiende gehouden in verband met lopende opdrachten van de Duitse overheid. Voor de Duitse overheid was het van belang dat DigiTask niet kon omvallen.

Wanneer in 2008 bekend wordt dat de Duitse overheid spyware van DigiTask heeft aangekocht claimen de autoriteiten dat Hans-Hermann Reuter na zijn straf te hebben uitgezeten geen betrokkenheid meer heeft met het bedrijf. Het is echter de vraag of dit daadwerkelijk zo is. In 2006 kwam het bedrijf namelijk in handen van Reuter en kwamen de bedrijfseigendommen op zijn naam.

Ook is Reuter in 2008 nog steeds eigenaar van Reuter Electronic, dat nauw samenwerkt met DigiTask. Daarnaast bevestigt de advocaat van DigiTask in *Frankfurter Rundschau* dat de bedrijfsleiding van DigiTask in handen is van de echtgenote van Reuter. Reuter zelf zou volgens zijn advocaat echter niets met het bedrijf te maken hebben. De dagelijkse leiding van het bedrijf zou in handen zijn van Achim Pulverich. Hoe de verhouding tussen Hans-Hermann Reuter, Reuter Electronic en DigiTask precies is geregeld maakt het bedrijf niet openbaar.

Spyware ter discussie in rechtszaak

In 2011 laait het debat over het gebruik van spyware in opsporingsonderzoeken in Duitsland op. Aanleiding is een rechtszaak tegen een verdachte van de handel in farmaceutische producten. Tijdens de rechtszaak blijkt dat op de computer van de verdachte spyware is geïnstalleerd. Later zal blijken dat het gaat om spyware van DigiTask.

De Duitse rechter beoordeelt de inzet van de spyware deels als rechtmatig. Volgens de rechter is de monitoring van de Skype-gesprekken geoorloofd en in overeenstemming met de op dat moment geldende Duitse wetgeving. In de toestemming voor het gebruik van de spyware was in april 2009 toestemming gegeven voor het drie maanden afluisteren van audio en geschreven communicatie.

Het constant nemen van screenshots wordt door de rechter echter als onrechtmatig beoordeeld. De spyware op de computer van de cliënt van advocaat Patrick Schladt stuurde elke dertig seconden een screenshot naar een server van de politie. De screenshots waren afbeeldingen van alle handelingen op de computer van de verdachte zoals het gebruik van e-mail, internet browsen en andere handelingen. Voor deze laatste inbreuk is volgens de Duitse rechter geen rechtsgrond.

Volgens advocaat Schladt is de spyware waarschijnlijk in de lente van 2009 op de luchthaven van München bij de douanecontrole op de computer van zijn cliënt geïnstalleerd. Nadat de verdachte is aangeklaagd bestuderen Schladt en zijn cliënt het dossier en vermoeden dat het digitale bewijs is verkregen door de inzet van spyware. Spyware die misschien nog steeds op de laptop van de verdachte aanwezig is.

Volgens de Duitse wetgeving is inzet van spyware alleen toegestaan bij verdenking van terrorisme of ernstige misdrijven. Hiervan is in deze zaak echter geen sprake. De cliënt van Schladt wordt verdacht van de handel in farmaceutische producten. Hij werkt voor een bedrijf dat handelt in producten die in Duitsland legaal zijn, maar buiten Duitsland deels niet.

Voor advocaat Schladt is daarmee de kous niet af. Het gaat hem niet alleen om de rechtmatigheid van de inzet van de spyware, maar zeker om de vraag hoe de spyware precies functioneert. Hij benadert daarom de Duits Chaos Computer Club (CCC), een collectief van ethische hackers, om nader onderzoek te doen naar het functioneren van de spyware.

Vernietigend CCC-rapport

De spyware die de CCC onderzoekt wordt door de Duitse overheid in het algemeen aangeduid als Quellen-TKÜ: bron telecommunicatie surveillance. In Duitsland worden twee andere namen veelvuldig gebruikt voor de door de CCC onderzochte spyware: Ozapftis en R2D2. Ozapftis is een verwijzing naar O'zapft is!, de traditie van het aanbreken van het eerste biervat door de burgemeester van München tijdens het Oktoberfeest. R2D2 is een verwijzing naar een digitale code van de spyware die de onderzoekers bij de analyse hebben gevonden, maar ook een verwijzing naar de 'robot' R2-D2 in Star Wars.

De CCC publiceert haar analyse op 8 oktober 2011. De onderzoekers concluderen veel tekortkomingen in de tool. Zij bevestigen de uitspraak van de Beierse rechter dat de tool op de computer van de verdachte veel meer kan dan wettelijk is toegestaan in Duitsland. Met de spyware kunnen niet alleen Skypegesprekken worden afgeluisterd en screenshots worden gemaakt, hetgeen volgens de rechtbank is toegestaan. Er kunnen ook bestanden en programma's op de computer van de verdachte worden gemanipuleerd, vernietigd of toegevoegd.

De tool is dus niet alleen gericht op het afluisteren van de communicatie via een gegevensdrager, maar kan de computer of laptop in zijn geheel overnemen. Dit maakt manipulatie mogelijk, zoals het verwijderen en toevoegen van data op de computer van de verdachte, en – omdat de spyware ook toetsaanslagen registreert - het wijzigen van wachtwoorden. Dit is mogelijk omdat de tool op afstand bestuurd kan worden. Deze zogenaamde 'remote control' is mogelijk door een ingebouwde 'backdoor': een mogelijkheid die veel spyware heeft om een bepaalde functionaliteit van de tool te veranderen en uit te breiden.

Niet alleen de politie en de producent kunnen de spyware op afstand besturen. De CCC toont aan dat ook derden de computer van de verdachte kunnen overnemen, omdat de beveiliging van de backdoor niet op orde is en de verzamelde data niet versleuteld over het internet worden verzonden. Iedereen kan deze data dus in principe inzien.

Veel spyware communiceren met een server elders om zo direct de afgeluisterde data te verzamelen. Door de slechte beveiliging kan de tool door derden worden overgenomen en kunnen derden zelfs vervalste informatie naar de server van de autoriteiten sturen. Dit wordt veroorzaakt door het ontbreken van een authenticatiemechanisme in de tool: door de tool wordt niet vastgesteld met wie met de tool communiceert en door de tool verstuurde gegevens worden ook niet op echtheid gecontroleerd.

Tot slot stelt de CCC vast dat de server waarmee de spyware op de laptop van de verdachte mee communiceert, waarschijnlijk niet in Duitsland maar in de Verenigde Staten staat. De CCC baseert zich hierbij op het IP-adres van de server. De politie heeft dit waarschijnlijk zo ingericht om ontdekking van de tool te voorkomen. Communicatie van het besturingssysteem op de laptop, in dit geval Windows, of andere software met de Verenigde Staten wordt door de afgeluisterde persoon als minder verdacht beschouwd dan communicatie met een server in Duitsland. Het bewaren van informatie over een verdachte op een buitenlandse server roept echter juridische vragen en vragen met betrekking tot de beveiligingsvragen, zoals in welk datacentrum de server staat en wie daar fysieke toegang toe heeft.

De CCC concludeert in haar onderzoek dat de tool die het heeft onderzocht afkomstig is van DigiTask. DigiTask verdedigt zich tegen de kritiek door te stellen dat de CCC een oude versie van de spyware heeft onderzocht: het zou gaan om een testversie of een prototype. De claim van DigiTask is bevreemdend, omdat de CCC stelt meerdere versies van de DigiTask tool te hebben onderzocht. En omdat het zou betekenen dat een onveilige testversie is gebruikt bij een opsporingsonderzoek.

De CCC heeft de herkomst van de andere onderzochte versies niet bekend gemaakt. Het gaat mogelijk om websites als VirusTotal en de databases van antivirus bedrijven, aangezien de spyware van DigiTask ook door verschillende antivirusprogramma's is ontdekt en geneutraliseerd. Delen van de spyware zijn zo in handen gekomen van deze bedrijven.

Het onderzoek van de CCC roept vragen op over de veiligheid van de inzet en de betrouwbaarheid van de verkregen informatie. Het belang van het CCC-onderzoek is niet alleen groot voor de situatie rond DigiTask, maar ook voor andere spyware. Het is namelijk de eerste keer dat spyware, of een deel van spyware, uitgebreid is onderzocht door derden en niet door de overheid of de bedrijven zelf.

Het onderzoek legt de vinger op de zere plek die bij alle spyware speelt. De politie heeft weinig inzicht in de werking van de tool en wijze waarop gegevens verkregen worden. De leverancier, en mogelijk, derden kunnen toegang krijgen en gegevens toevoegen of wijzigen. De betrouwbaarheid van door middel van spyware verkregen bewijsmateriaal is dus in het geding.

Een paar jaar later laat het Canadese Citizen Lab zien dat zij de communicatie tussen spyware en een server kan traceren en zo ontdekken welke computers en smartphones door overheidsinstanties zijn gehackt met tools als FinFisher (Gamma Group), Pegasus (NSO Group) of RCS (Hacking Team). Deze communicatie is natuurlijk de eerste stap bij de mogelijke onderschepping en manipulatie van die communicatie en daarmee bewijsmateriaal.

Onderzoek door Duitse databeschermingsautoriteiten

Het Duitse Ministerie van Binnenlandse Zaken en de politiediensten geven geen gedetailleerd commentaar op de bevindingen van de CCC en stellen geen nader onderzoek in. Verschillende databeschermingsautoriteiten, waaronder de landelijke en die van de deelstaat Beieren, doen wel onderzoek en zijn kritisch over het functioneren van de DigiTask spyware. Ze

stellen fundamentele vragen bij de betrouwbaarheid van verkregen gegevens en bewijsmateriaal.

Het Beierse onderzoek is even kritisch als dat van de CCC, hoewel de databeschermingsautoriteit geen toegang krijgt tot de broncode van de DigiTask tool. Toegang tot de broncode is noodzakelijk om inzicht te krijgen in de precieze werking en mogelijkheden van een tool. DigiTask eist een aanvullende geheimhoudingsverklaring boven op de al door de databeschermer wettelijk vastgelegde geheimhouding.

De Beierse databeschermingsautoriteit voegt een extra element toe aan de vaststelling van de CCC dat derden de DigiTask tool kunnen overnemen door gebrekkige beveiliging van de tool. Uit het Beierse onderzoek blijkt namelijk dat de Beierse politie onzorgvuldig is omgegaan met het gebruik van de spyware.

De gehuurde Amerikaanse server die gebruikt is om de data van de computers van de afgeluisterde verdachten te bewaren, was steeds dezelfde server met hetzelfde IP-adres. De databeschermingsautoriteit acht het niet onwaarschijnlijk dat – wanneer de surveillance door de politie is afgebouwd - een derde de server kan overnemen en de surveillance met dezelfde server en IP-adres kan voorzetten. Door de publiciteit rondom de DigiTask tool en het rapport van de CCC, waarin het IP-adres wordt genoemd, was het voor iedereen mogelijk het IP-adres te bemachtigen en de specifieke server te huren.

Ook de landelijke databeschermingsautoriteit van Duitsland doet onderzoek. Opnieuw werkt DigiTask tegen en krijgt de databeschermingsautoriteit geen toegang tot de broncode van het bedrijf. Naast een separate geheimhoudingsverklaring wil het bedrijf zelfs 1.200 euro in rekening brengen voor iedere dag en elke werknemer die toegang zou krijgen tot de broncode.

De landelijke databeschermingsautoriteit stelt dat het gebruik van de spyware niet in overeenstemming is met Duitse wetgeving ten aanzien van de integriteit van het persoonlijk leven. Volgens de databeschermingsautoriteit is alle communicatie van verdachten afgeluisterd en opgenomen, waaronder bijvoorbeeld ook momenten van telefoonseks.

Ook is onduidelijk hoe de spyware precies functioneert door gebrek aan documentatie en inzicht in de broncode, functioneert het afluisteren soms niet terwijl de spyware niet is verwijderd van de gegevensdragers, en is het soms niet mogelijk de programmatuur na de afluister operatie te verwijderen. Daarnaast vraagt de landelijke databeschermingsautoriteit zich af waarom spyware is gebruikt en geen contact is opgenomen met de producent van Skype om te assisteren bij de afluisteroperatie.

Hoe vaak wordt spyware ingezet?

De onderzoeken van de CCC en de databeschermingsautoriteiten leiden tot debat in Duitsland over het gebruik van de spyware van DigiTask. En verontwaardiging vanwege de schending van privacywetgeving en de onbetrouwbaarheid van door middel van de inzet van spyware verkregen bewijs. Desalniettemin lijkt het erop dat de Duitse overheid de spyware van DigiTask blijft gebruiken.

Tot ongeveer 2013 hebben maar liefst negen van de zestien Duitse deelstaten (Brandenburg, Beieren, Baden-Württemberg, Hessen, Nedersaksen, Noordrijn-Westfalen, Rijnland-Palts, Saksen-Anhalt en Sleeswijk-Holstein) de spyware van DigiTask gebruikt. Ook de steden Hamburg en Bremen, de landelijke politie, de opsporingsdienst van de Duitse Douane en onder andere de Bundesnetzagentur (de Duitse netwerkbeheerder voor het elektriciteits-, gas, telecommunicatienetwerk) hebben de spyware gebruikt.

Volgens de Duitse overheid wordt spyware alleen ingezet bij de bestrijding van terrorisme en zware georganiseerde criminaliteit. Andere Europese landen claimen hetzelfde. Bij repressieve regimes die hetzelfde beweren blijkt echter keer op keer dat spyware, van bedrijven als Gamma Group (FinFisher), Hacking Team (RCS Galileo en DaVinci) en NSO Group (Pegasus), wordt ingezet tegen oppositieleden, mensenrechtenactivisten, journalisten en andere tegenstanders van de regimes.

Over de inzet van spyware in democratische landen komt meestal weinig naar buiten. De laatste jaren is echter wel van de inzet van de spyware Pegasus van het Israëlische bedrijf NSO in Spanje, Hongarije en Griekenland duidelijk geworden dat het er ook op lijkt dat oppositieleden, journalisten en mensenrechtenactivisten slachtoffer zijn geworden van spyware. De vraag is dus gerechtvaardigd of in hoeverre spyware alleen wordt gebruikt voor de bestrijding van terrorisme en zware georganiseerde criminaliteit.

Het is echter moeilijk om deze claim te onderzoeken. Overheden publiceren over het algemeen nauwelijks gegevens over de inzet van spyware, zoals het aantal en type zaken waarbij spyware is ingezet, het aantal zaken waarbij de inzet tot een veroordeling heeft geleid, en met welke straf. Ook de Duitse overheid publiceert dergelijke gegevens niet.

Zo verklaart de Duitse regering in 2011 dat er sinds 2009 ongeveer 35 keer per jaar spyware werd ingezet. Het gaat hierbij niet alleen om de spyware van DigiTask, de Duitse overheid gebruikt ook spyware van andere bedrijven. Het is niet duidelijk of dit cijfer betrekking heeft op het aantal opsporingsonderzoeken waarbij spyware is ingezet, of het aantal personen of het aantal gegevensdragers die zijn gehackt.

Vanwege het ontbreken van openbare gegevens valt niet vast te stellen hoe betrouwbaar het genoemde aantal van 35 inzetten per jaar is. Verzamelde gegevens uit de media, rapportages van de databeschermingsautoriteiten en andere bronnen over de inzet van DigiTask en andere spyware in Duitsland duiden erop dat spyware in de periode 2007-2013 in ongeveer honderd gevallen is ingezet.

Alleen al in de deelstaat Beieren gaat het om ongeveer 25 verschillende onderzoeken en in Sleeswijk-Holstein om 5 onderzoeken. In de deelstaten Noordrijn-Westfalen, Hessen, Brandenburg en Neder-Sachsen is spyware in twee onderzoeken ingezet. In Bremen, Hamburg, Rijnland-Palts, Baden-Württemberg en Saksen-Anhalt een keer. Ook is spyware in negentien zaken ingezet door de Duitse douane en heeft de landelijke aangegeven dat in 41 zaken computers te hebben geïnfecteerd met spyware.

Wanneer wordt spyware van DigiTask ingezet?

Het is niet duidelijk of in alle bovengenoemde zaken de tools van DigiTask, of andere spyware, is ingezet. Het is evenmin duidelijk of het in alle gevallen ging om onderzoeken naar terrorisme of zware georganiseerde criminaliteit. Het lijkt er echter op dat spyware slechts in een klein aantal gevallen werd ingezet in zaken waarin sprake was van verdenking van terrorisme.

Zo is in Beieren bekend gemaakt dat de regionale Beierse inlichtingendienst (Landesamt für Verfassungsschutz) tot 2011 drie keer gebruik heeft gemaakt van de DigiTask tool bij het afluisteren van mensen die verdacht werden van het voorbereiden van een bomaanslag. Het is niet duidelijk of de inzet tot veroordelingen heeft geleid.

De landelijke politie (BKA) verklaart tussen 2007 en 2011 in 41 gevallen spyware te hebben gebruikt in onderzoeken naar terreurverdachten. In zeven gevallen keer werd niet alleen passief afgeluisterd, maar werd ook de computer op afstand onderzocht met behulp van spyware van bedrijven als DigiTask, Gamma Group en Era IT Solutions AG.

Het is echter moeilijk om de betrouwbaarheid van deze cijfers te duiden en het is de vraag of in het al deze gevallen daadwerkelijk om verdenking van terrorisme ging. Het Duitse landelijk Openbaar Ministerie, dat belast is met de bestrijding van terrorisme in geheel Duitsland, zegt in deze periode namelijk geen gebruik gemaakt te hebben van spyware.

Over negen opsporingsonderzoeken uit de deelstaten Brandenburg, Neder-Saksen en Beieren tot 2012 waarbij spyware is ingezet is meer informatie openbaar geworden en in de media te vinden. Het geeft een indruk van het type opsporingsonderzoeken waarbij de Duitse politie spyware heeft ingezet. Het gaat vooral om drugshandel en andere vormen van smokkel. Uit de openbare informatie wordt niet altijd duidelijk of het in deze zaken tot een veroordeling is gekomen.

Zo werd in Brandenburg spyware ingezet bij een opsporingsonderzoek naar sigarettensmokkel en bij een onderzoek naar de handel in nagemaakte medicijnen, volgens de autoriteiten een vorm van georganiseerde criminaliteit. Bij een van de onderzoeken beschadigde de spyware van DigiTask de harde schijf van de computer van de verdachte dusdanig dat die kapotging. Het is onduidelijk of dit gevolgen had voor het vervolg van het onderzoek, de uiteindelijke vervolging en de strafmaat.

In Neder-Saksen werd de spyware van DigiTask bij twee drugsonderzoeken ingezet. Volgens de autoriteiten ging het wederom om georganiseerde criminaliteit. Het is onduidelijk of het tot vervolging is gekomen.

De Duitse krant *Süddeutsche Zeitung* zet in 2011 vijf opsporingsonderzoeken in 2008, 2009 en 2010 waarbij de Beierse politie spyware van DigiTask heeft ingezet op een rijtje. De krant stelt dat, hoewel het om ernstige vergrijpen gaat, het allemaal niet heel groots (“Auch nichts wirklich ganz Großes”) en ‘geen zware criminaliteit’.

Een van de onderzoeken betreft de verdachte van handel in farmaceutische producten die samen met zijn advocaat Schladt de spyware op zijn laptop ontdekte. Bij de andere onderzoeken gaat het volgens de krant om vergelijkbare criminaliteit zoals handel in verdovende middelen, dopingproducten, gestolen goederen en oplichting. Een van die onderzoeken betreft een groep van vijftien oplichters die honderden elektrische apparaten op internet aanboden en niet leverden. In totaal werden er ruim honderdduizend slachtoffers gemaakt en verdiende de bende zeven miljoen euro.

De derde en vierde inzet van DigiTask in Beieren draait om een groep helers die gestolen kleding en parfumerie naar het buitenland smokkelden en daar verkochten. Een van de verdachten werd veroordeeld tot twee jaar gevangenisstraf. De andere verdachten kregen lichtere straffen, zoals taakstraffen en geldboetes.

De vijfde inzet betreft een onderzoek naar handel in dopingproducten. De verdachte werd veroordeeld tot vier en een half jaar gevangenisstraf, maar niet zozeer vanwege de handel in doping, maar vooral voor geweldsdelicten in combinatie met diefstal en oplichting. Onduidelijk is bij welk deel van het opsporingsonderzoek de spyware is ingezet.

Tot slot schrijft de krant dat, los van de vijf bovenstaande onderzoeken, de gegevensdragers van drie cannabis handelaren zijn geïnfecteerd met de spyware van DigiTask. Of het hierbij ging om aparte opsporingsonderzoeken of een geheel onderzoek wordt niet vermeld.

De beschikbare informatie duidt er dus op dat de spyware van DigiTask niet alleen is ingezet bij onderzoeken naar terrorisme en zware georganiseerde criminaliteit, maar zeker ook bij minder zware misdrijven.

In latere jaren heeft de Duitse overheid iets meer cijfers gepubliceerd over de inzet van spyware. Zo maakte het Bundesamt für Justiz cijfers bekend over 2019, die een vergelijkbaar beeld opleveren als de beschikbare gegevens over de periode tot 2013. Volgens deze cijfers werd in 2019 in 35 zaken de inzet van spyware gelast. Het ging in 13 zaken om roof met geweld (Rauberische Erpressung) en 12 keer om drugs gerelateerde onderzoeken. De overheid maakt niet duidelijk in hoeveel zaken het tot veroordeling is gekomen en met welke straf. Terrorisme wordt dus niet genoemd in het overzicht. Wel werd de inzet van spyware twee keer gelast bij verdenking op lidmaatschap van een criminele organisatie, en een keer bij landsverraad.

Hoewel het aan uitgebreid onderzoek naar de inzet van spyware in Duitsland ontbreekt, laten de beperkte gegevens zien dat de nadruk bij de inzet niet op terrorisme en zware georganiseerde criminaliteit ligt, maar op minder zware misdrijven.

DigiTask verdient miljoenen euro

Al vanaf de eerste onthulling over het gebruik van DigiTask door de Duitse overheid in 2008 zijn er in de Duitse media bedragen gepubliceerd die door de overheid aan DigiTask, en andere spyware bedrijven, zijn betaald. Er is geen duidelijk overzicht van alle betalingen aan het bedrijf.

Uit mediaberichtgeving en andere onderzoeken wordt echter duidelijk dat DigiTask tussen 2008 en 2013 miljoenen euro van de Duitse overheid heeft ontvangen. Hierbij moet wel aangetekend worden dat het hierbij niet per se om spyware hoeft te gaan, omdat het bedrijf ook andere surveillance middelen, zoals klassieke afluisterapparatuur, videobewaking en data-analyse software, produceert.

De opsporingsdienst van de Duitse douane is een van de grote afnemers van DigiTask. In maart 2008 betaalt het resp. 511.112 en 208.750 euro voor de evaluatie van spyware en hardware en software licenties. Het gaat waarschijnlijk om DigiTask, aangezien later bekend is geworden dat de douane de tools van DigiTask heeft gebruikt. In 2009 ontvangt DigiTask 2.075.256 miljoen euro van de douane voor de levering van haar eigen tool. In oktober 2009 ontvangt het bedrijf 693.672 euro voor het verder in bedrijf houden van de tool, en in 2011 bijna 3,5 miljoen euro.

De Bundeskrimalamt BKA betaalt DigiTask in 2011 200.000 euro. In 2012 moet het bedrijf 423.000 euro delen met Gamma Group en het Zwitserse Era IT Solutions. In 2013 betaalt het Bundesnetzagentur 660.987 aan DigiTask. Hoewel het hierbij om spyware zou kunnen gaan (het Bundesnetzagentur heeft dit namelijk niet ontkend) zou het ook om bewakingsapparatuur van DigiTask kunnen gaan (“TKÜ-TMC, Funk- und Fernsprechüberwachungssystem”).

Deelstaten hebben een flink budget aan de spyware tools van DigiTask besteed. Ook van deze betalingen bestaat geen volledig overzicht, omdat veel deelstaten geen of onvolledige gegevens openbaar hebben gemaakt. Er zijn echter wel indicaties. Zo lijkt de deelstaat Beieren een voorname afnemer te zijn van DigiTask.

In 2006 betaalt de Beierse politie 409.035 euro aan het bedrijf, in 2008 247.773 euro en 614.984 euro. De omschrijvingen bij de betalingen suggereren dat de deelstaat Beieren heeft meebetaald aan de ontwikkelkosten van de spyware. De betaling in november 2008 staat vermeld dat deze is bedoeld voor de "Erweiterung des TKÜ-Systems um ein Archivsystem", de uitbreiding van de spyware tool met een archiveringssysteem.

In totaal betaalt de deelstaat Beieren tot 2013 dertien miljoen euro aan DigiTask. Het is niet bekend of dit bedrag alleen betrekking heeft op de aankoop van spyware, of ook voor andere producten zoals bewakingsapparatuur.

Drie andere deelstaten steken ook miljoenen de aankoop van spyware van DigiTask en andere bedrijven. Niet alleen DigiTask profiteert van die miljoen. Zo betaalt de deelstaat Hessen in 2010 5,3 miljoen euro voor spyware van het bedrijf Syborg onderdeel van het Amerikaanse Verint Systems Inc., nu Cognyte Software Ltd.

Rijnland-Palts betaalde 2,5 miljoen euro ("Lieferung eines TKÜ-Systems") aan een onbekende leverancier. Baden-Württemberg betaalde 1,2 miljoen euro (1.218.225,35) aan de spyware van DigiTask ("TKÜ-System, Lieferung einer TKÜ-Anwendung und Dienstleistung zur Erstellung eines kompletten TKÜ-Systems für die Polizei des Landes Baden-Württemberg").

Andere deelstaten lijken minder aan DigiTask te hebben betaald. In 2012 huurt Noordrijn-Westfalen DigiTask in voor 19.000 euro voor spyware. Een jaar eerder betaalde de deelstaat voor het gebruik van spyware bij twee verdachten 397.714 euro aan concurrent Syborg ("Wartungsvertrag GEMINI ("ist das TKÜ System in NRW").

In 2012 besteedt Noordrijn-Westfalen 400.000 euro aan een nieuwe opdracht voor spyware, maar het is onbekend of DigiTask het enige bedrijf was dat hiervan profiteerde.

Al met al is dus duidelijk dat DigiTask in de loop der jaren miljoenen euro heeft ontvangen van de Duitse overheid. Dit valt ten minste opmerkelijk te noemen, gezien het verleden van corruptie en steekpenningen van het bedrijf.

De miljoenen die de Duitse overheid aan spyware van DigiTask heeft besteed staan in schril contrast met het half miljoen (682.581 euro) dat is uitgetrokken voor de ontwikkeling van een niet-commerciële spyware tool, ontwikkeld door de overheid. Uiteindelijk is die spyware van de overheid nooit operationeel geworden.

DigiTask ook in Nederland gebruikt

DigiTask is in 2018 overgenomen door Rohde & Schwarz. Dit bedrijf uit München maakt elektronica voor test- en meetapparatuur, de ruimtevaart, defensie, mediabedrijven en cybersecurity. In de loop der jaren heeft Rohde & Schwarz ook diverse andere bedrijven overgenomen zoals het in radio monitoring gespecialiseerde Franse Arpège SAS in 2007, het Duitse Ipoque GmbH in 2011 en Sirrix AG in 2015.

De Duitse overheid is de spyware van DigiTask tot waarschijnlijk tot 2014 blijven gebruiken. Ook andere landen waaronder Zwitserland, België en Nederland hebben de tools van het Duitse bedrijf aangeschaft.

Toenmalig Minister van Veiligheid en Justitie Opstelten verklaarde in 2011 dat de Nederlandse politie de spyware van DigiTask heeft aangekocht, nadat dit eerder door het Duitse bedrijf zelf naar buiten was gebracht. Het lijkt erop dat de Nederlandse politie de spyware in ieder geval tot 2014 is blijven gebruiken. De Nederlandse overheid heeft tot nu toe geen openheid van zaken gegeven over de inzet van DigiTask. Woo-verzoeken van Buro Jansen & Janssen blijven deels onbeantwoord, openbaar gemaakte documenten zijn grotendeels onleesbaar gemaakt.

Naar inhoudsopgave Observant # 81

Documenten bij DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware

Voor dit profiel zijn mediaberichtgeving, rapporten van databeschermingsautoriteiten en andere openbare bronnen geraadpleegd. Ook zijn er informatieverzoeken gedaan bij de Nederlandse overheid.

De Nederlandse overheid heeft tot nu toe geen openheid van zaken gegeven over de inzet van DigiTask. Woo-verzoeken van Buro Jansen & Janssen blijven deels onbeantwoord, openbaar gemaakte documenten zijn grotendeels onleesbaar gemaakt.

Artikelen

– DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (samenvatting)
– DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)

– De digitale inkijkoperaties van de Politie Black Box (samenvatting I). Nederlandse politie gebruikt spyware voor inlichtingenoperaties, inkijkoperaties en andere opsporingsdoelen, niet voor het verzamelen van bewijs.
– Nederlandse politie koopt spyware van controversiële bedrijven (samenvatting II). Overheid screent deze bedrijven in het geheel niet.
– Een Politie Black Box, gebruik van spyware door de Nederlandse politie (onderzoek)
– Documenten bij een Politie Black Box gebruik van spyware door de Nederlandse politie

– Boeven vangen met dubieuze software van dubieuze bedrijven (2017)
– Inhoudsopgave Politie Mercenaries, Observant #69, januari 2017
– Politie Mercenaries, Observant #69, januari 2017 (pdf)

Enkele CCC-rapportages

– staatstrojaner-report23
– staatstrojaner-report42

Enkele DigiTask stukken

– 24_remote-forensic-software
– 25_future-challenges-in-the-lawful-interception-fo-ip-based
– 45_challenges-in-intercepting-wifi
– 46_remote-forensic-software
– Stellungnahme_DigiTask
– DIGITASK-20070731
– DIGITASK-20080731
– DIGITASK-20090731

Enkele stukken Duitse overheid

– Bayern-skype-tkue
– AG_Landhut_Anordnung-TKUe
– LG_Landshut_4_Qs_346-101
– Schaar-Staatstrojaner
– 4364782314
– Uebersicht_TKUE_2010
– Uebersicht_TKUE_2019
– Uebersicht_Online_Durchsuchung_2019
– Uebersicht_Verkehrsdaten_2019

ISS World

ISS World EMEA Dubai 2008
– issworldemeafeb2008programfromwebsite
– issworldemeafeb2008sponsorsfromwebsite
– issworldemea2008visitors

ISS World MEA Dubai 2009
– ISSWorldMEA2009
– issworldmea2009programfromwebsite
– issworldmeafeb2009sponsorsfromwebsite

ISS World Europe Prague 2008
– ISSWorldEuropebrochure2008
– issworldeurope2008programfromwebsite
– issworldeurope2008sponsorsfromwebsite
– issworldeuropeoktober2008visitors

ISS World Europe Prague 2009
– issworldeurope2009programfromwebsite
– issworldeurope2009sponsorsfromwebsite

ISS World Europe Prague 2010
– issworldeuropeagenda2010
– ISSWorldeurope2010programfromwebsite
– ISSWorldeurope2010sponsorsfromwebsite

ISS World Europe Prague 2012
– ISSworldeurope2012brochure
– ISSWorldeurope2012programfromwebsite
– ISSWorldeurope2012sponsorsfromwebsite

– Surveillance attendees and exhibitors – Surveillance Who's Who data
– Training-Agenda-AGT_Sep2007

DigiTask documenten politie, Woo-verzoek van april 2019

– DigiTask stukken 01
– DigiTask stukken 02
– DigiTask stukken 03
– DigiTask stukken 04
– DigiTask stukken 05
– DigiTask stukken 06
– DigiTask stukken 07
– DigiTask stukken 08
– DigiTask stukken 09

Enkele Ipoque, ook onderdeel van Rohde & Schwarz, stukken

– IPOQUE-DPXNetwProb-en
– IPOQUE-PACEProtAppl-en
– 191_supported-protocols-and-applications

Aanverwante discussie DPI en surveillance

– the-privacy-security-research-paper-series

Naar inhoudsopgave Observant # 81

Om de vrijheid te vieren moet je wel de kritiek op de vrijheidsbeperkingen accepteren

Het politieoptreden bij de verboden demonstratie op 5 mei 2020 was niets bijzonders, zo wordt er meestal opgetreden bij het niet aanmelden van een demonstratie. Wegwezen! Erg in lijn met grondwettelijke rechten is die houding van politie en bestuur niet, maar het is de regel. Op 5 mei 2020 hard optreden toont echter vooral aan dat de overheid enig contact met de werkelijkheid kwijt is. Corona of niet voor een weerbare rechtstaat is het noodzakelijk dat de vrijheid van meningsuiting en het recht op betoging niet met knuppel en paard de gevangenis of de trein naar huis in wordt gemept. Dan is er echt niets meer te vieren.

De vraag is natuurlijk waar gaat het dan fout. Is het de basishouding van oprotten, ga toch werken, of is er aanvankelijk een open houding naar grondrechten, maar ontspoort de repressie door allerlei omstandigheden. Openbaar gemaakte documenten, hoewel voor een groot deel gecensureerd, openbare bronnen, sociale en gewone mediaberichten en verhalen van deelnemers leveren een interessante inkijk op een overheid die geen raad weet met protesten tegen coronamaatregelen. Dit onvermogen duurt tot het eind van de coronacrisis zoals optreden in 2021 in Amsterdam laat zien.

Op 5 mei 2020 is er echter iets bijzonders aan de hand. De demonstratie is niet aangemeld en dat betekent eigenlijk maar een ding: “Demonstratie 5 mei wordt door burgermeester niet toegestaan, indien er demonstranten verschijnen worden zij aangehouden op basis van de WOM.” Zo staat het dan ook in een van de vier “presentatie t.b.v. Operationele kaderbriefing Demonstratie tegen Covid 19 maatregelen”. Een dergelijke operationele briefing wordt gehouden voor de aanvang van de festiviteiten van de dag, in dit geval 5 mei 2020. Het vreemde is dat er in de andere drie presentaties verschillende beleidsuitgangspunten worden verwoord.

De standaard is dus, niet aangemeld, niet toegestaan, maar in de andere presentaties staan ook mildere uitgangspunten zoals "demonstratie alleen op het Malieveld" en "het voorkomen dat een demonstratie ontstaat op een andere locatie in het centrum van Den Haag dan op het Malieveld." Welke presentatie(s) de politiemanschappen voorafgaande aan de inzet hebben gezien is van belang om te weten waarom er zo fors is opgetreden.

Ook ten aanzien van de coronamaatregelen tonen de presentaties grote verschillen. Bij een presentatie is het meteen afgelopen met de grondrechten pret: "Indien demonstranten zich niet aan Coronavoorschriften, houden dan demo direct beëindigen (na contact BM (burgemeester red.)." Volgens de presentaties is beëindiging mogelijk op grond van "artikel 5 WOM (bescherming van de gezondheid)." Om welke voorschriften het hier gaat wordt niet in deze specifieke presentatie vermeld. Mondkapjes waren in mei 2020 niet verplicht, anderhalve meter afstand houden wel. Hoe die afstand te controleren bij een groep demonstrerende mensen lijkt enigszins willekeurig en wordt niet gespecificeerd. Een andere presentatie is dan ook iets milder: "Een Eventuele demonstratie/manifestatie op het Malieveld in goede orde te doen verlopen en in lijn met de maatregelen in verband met COVID-19 (1,5m afstand)."

De 5 mei 2020 demonstratie heeft geen lange voorgeschiedenis. Het protest us niet aangemeld en er is geen communicatie met de organisatoren. Na een eerder protest, op 28 april 2020, wordt op social media aangekondigd op 5 mei 2020 opnieuw te protesteren en niet alleen in Den Haag. In de oproepen worden naast Den Haag diverse andere steden genoemd zoals Amsterdam en Utrecht. Uiteindelijk vindt niet alleen in Den Haag een wat groter protest plaats, maar ook in Utrecht waar een colonne auto's in de stad rondrijdt met ongeveer honderdvijftig deelnemers.

De oproepen om een stem te laten horen worden voor 5 mei verspreid door de 'gele hesjes', 'Nederland in opstand', 'Burger Bond Nederland', 'Nederland slaap lekker verder', 'volk word wakker', 'StopDeLockdown' en enkele andere initiatieven. Hoewel in de media en ook in de

documenten van de politie de indruk wordt gewekt dat het een demonstratie is tegen van alles, van 5G tot 'Break the system' en de anderhalve meter maatregel is er duidelijk een gemene deler bij de demonstranten, zij roepen om 'vrijheid'.

Demonstreren voor het abstracte begrip 'vrijheid' op de dag van de vrijheid, klinkt bijna historisch. De deelnemers aan de demonstratie lijken zich daar volstrekt niet van bewust. Het protest heeft geen centrale organisatie, het lijkt alle kanten op te gaan, sprekers zijn er niet echt, iedereen is spreker. De demonstratie is duidelijk een herhaling van 28 april 2020. Dat protest was ook een roep om het ongenoegen te laten horen. Uit de stukken blijkt dat de politie niet te spreken is over deze demonstratie van 28 april die volgens de autoriteiten door de 'Burgerbond Nederland' is georganiseerd.

In de politiedocumenten wordt gesteld dat die "demonstratie niet is aangemeld, dat het contact met de organisatie zeer moeizaam is en dat de demonstranten de noodverordening overtreden." Het protest op 28 april trekt tussen de 100 tot 200 deelnemers en begint op het Binnenhof, wordt door de politie verplaatst naar het Plein en later ingesloten en naar het Malieveld gepusht, om vervolgens met zachte hand te worden beëindigd. Directe aanleiding van de demonstratie op 28 april is een nieuwe persconferentie waarin Mark Rutte verlenging van de coronamaatregelen aankondigt.

Nederland is dan al ruim een maand in 'intelligente lockdown' zoals de regering het bestempelt, de onzekerheid is groot. Vaak wordt de indruk gewekt alsof het voor de wetenschap allemaal glashelder is, maar zeker in hinsight is dat allerminst zeker. Dit betekent niet dat er van de demonstranten enige compassie gevraagd kan worden met de kwetsbaren in de samenleving. Als echter de overheid dat zelf ook niet doet, gezien de houding van de autoriteiten naar verzorgings- en verpleegtehuizen, is het de vraag of het wegzetten van deze demonstranten als niet-intelligent, als wappies, wel correct is, helemaal op een symbolische dag als 5 mei.

Terug naar 28 april 2020. Wat een kleine groep demonstranten allemaal niet teweeg kan brengen. De politie is niet alleen niet te

spreken over de demonstranten, ze bestempelt de sfeer ook als ‘grimmig’. Dat die grimmige sfeer misschien met het politieoptreden zelf te maken heeft, verplaatsing van het Binnenhof naar het Plein daarna insluiting en pushen naar het Malieveld om met ‘zachte hand’te worden beëindigd, wordt niet opgemerkt. De politie vindt namelijk dat haar uitgangspunt is de “inzet … om binnenhof vrij te houden en groep in te boxen.” Een deel van de tekst is gecensureerd, maar duidelijk is dat de politie niet wil dat mensen demonstreren bij de plek waar de persconferentie wordt gehouden. Dat dit tot verontwaardiging bij de demonstranten leidt is natuurlijk logisch. De politie is daar altijd verbolgen over, terwijl het fundament van het grondrecht om de mening te laten horen juist bedoeld is om dat te doen op de plaats-delict.

De typering van ‘grimmig’ is naast het al dan niet toelaten van de demonstratie op 5 mei 2020 het startpunt van de dag van de vrijheid. Het bestuur heeft ook besloten dat het Binnenhof, het Plein en een geheime gecensureerde locatie ook no-go zones zijn. Blijft over het Malieveld, daar is echter Staatsbosbeheer verbolgen over. Staatsbosbeheer is beheerder van het Malieveld. Zij wil “geen medewerking verlenen aan een (niet aangemelde) demonstratie op het Malieveld.” Ook het gras wil geen grondrechten toelaten: “De potentiële schade is te groot voor het jonge gras, de net herstelde en ingezaaide delen inclusief de nu zachte toplaag. Dat geldt ook voor de bermen.” Demonstreren op 5 mei voor de vrijheid is niet toegestaan. Een gesubsidieerd vrijheidsvuur wel: “Daarnaast faciliteren wij het Vrijheidsvuur op het Malieveld, op de enige plek die op dit moment in goede staat is,” schrijft Staatsbosbeheer aan politie-eenheid Den Haag.

Zie hier de voorbode van de arrestatie van tachtig mensen die van hun grondrechten gebruik maken op 5 mei. Op de dag zelf komen rond de 300 mensen protesteren, ze bewegen zich een beetje tussen Den Haag Centraal en het Malieveld, wat dus niet betreden kan worden, in het Prinsessepark. De onduidelijke inzet, verboden of toch toegestaan en al dan niet optreden bij overtreding van de coronamaatregelen, zorgen voor een grimmige houding van de politie. Deze is versterkt door alle verzamelde inlichtingen.

In totaal zijn er zes inlichtingenrapportages over de demonstratie van 5 mei 2020 gemaakt: Drie TOOI-informatierapporten openbare orde (TOOI is Team Openbare Orde Inlichtingen) 6612-2020, 6613-2020 en 6621-2020 d.d. 1 mei 2020, een Signaalrapport DRIO (Dienst Regionale Informatie Organisatie Den Haag), d.d. 2 mei 2020, een OSINT (Open Source Intelligence) Rapportage d.d. 4 mei 2020 en Informatierapport demonstratie 5 mei, Den Haag, DRIO, RIK (regionaal informatieknooppunt), d.d. 4 mei 2020.

Al deze inlichtingenrapportages zijn geheim en volledig gecensureerd. Het spreekt echter voor zich wat er in die rapportages staat. Gezien de vele oproepen op social media zullen al deze oproepen, de deelnemers van de pagina's en groepen waarin de aankondigen worden verspreid door de politie wasstraat zijn gehaald. Komen zij voor in de politie systemen en zo ja met wie hebben zij contacten. Op radicaal linkse websites wordt vermeld dat enkele van de demonstranten extreemrechts zijn en/of extreemrechtse connecties hebben. Dit zal de politie ook niet ontgaan zijn. Uit onderzoek naar andere demonstraties is duidelijk geworden dat de politie extreemrechtse of vermeende extreemrechtse sympathisanten vanaf hun huisdeur tot aankomst bij een demonstratie in de gaten houden. Naast extreemrechts en voetbalsupporters kijkt de politie ook naar krakers en radicaal linkse activisten. Van al die groepen waren enkelen aanwezig op zowel 28 april als op 5 mei 2020.

Al die inlichtingen zorgen niet voor een verlaging van de gespannen houding op Bevrijdingsdag, maar werken eerder spanning verhogend. De usual suspects zijn er weer, denkt de politie, het gaat weer uit de hand lopen. Onderzoek naar andere demonstraties toont die grondhouding van de overheid aan. Als bepaalde groepen deelnemen aan een protest is de kans op escalatie vanuit de politie groter. De 'sfeer' is dan al vanaf het begin van de demonstratie grimmig. Twee andere elementen zorgen ervoor dat vanaf het begin duidelijk is dat de politie fors gaat optreden of althans haar gezag zal tonen in tegenstelling tot 28 april 2020.

Het eerste element lijkt niet relevant, maar in de begintijd van de coronacrisis echter uiterst gevoelig. Na de demonstratie op 28 april is er geklaagd over het optreden van de politie. De klacht wordt door de politie in de stukken als volgt weergegeven: "Klacht richting politie over niet optreden tegen overtreden noodverordening." Meestal hebben komen klachten over de politie niet terug in politiedocumenten, ze lijken niet te bestaan, maar deze klacht wordt zelfs in de briefingspresentatie vermeld. Natuurlijk is het nieuw, de pandemie en de coronamaatregelen. Wat te doen bij een protest tegen deze maatregelen? Op het 'eerste vooroverleg SGBO DEMO 5 mei 2020 (overleg 1-5-20)' wordt echter al een voorzet gegeven voor een antwoord op die vraag: "Juridisch kader: WOM (uitzonderingsgrond Volksgezondheid), demo's vallen niet onder noodverordening." Aan de andere kant kun je zeggen, de volksgezondheid is een belangrijk geod, daar moet de overheid voor staan, optreden dus zoals de klager eist.

De aandacht voor de klacht in de briefings moet ook gezien worden in het licht van de opmerking over de demonstratie van 28 april dat er "veel pers aanwezig" is. De politie lijkt een oorzakelijk verband te leggen tussen de klacht en de aanwezigheid van de media die naast de beelden van een saaie persconferentie gelukkig wat actie kunnen tonen. "Veel media aanwezig, beeld dat werd geschetst dat demonstranten veel ruimte kregen en niet gehandhaafd werd," staat in het verslag van 'overleg 1-5-20'. Over de demonstratie van 5 mei 2020 schrijft de politie dat de aandacht nog veel groter is: "De Wereld kijkt mee!!!!" De empowerment die dan volgt is bijna eng en komt nogal sektarisch over: "Wij gebruiken op professionele wijze geweld, Wij gebruiken correcte taal, Wij hebben de uitstraling van een krachtige ME, Wij maken het verschil !!!!" Het komt over als het geschreeuw voor aanvang van een wedstrijd die gewonnen moet worden.

Er is echter geen wedstrijd, er is gewoon een demonstratie van mensen die tegen bepaald beleid zijn, dat kun je verstandig, slecht, leuk etc. vinden of niet, maar het belangrijkste is dat deze mensen hun grondrechten moeten kunnen uitoefenen, helemaal in crisistijd. Het vreemde is dat in alle stukken natuurlijk 5 mei steeds terugkomt, als datum waarop een demonstratie plaatsvindt, maar niet wat de dag

nu betekent en waarom het misschien van belang is om het recht op vrijheid van meningsuiting en het recht op betoging op die specifieke dag extra te respecteren, corona of niet. Geen enkel woord over de herinnering aan het eind van de Nazi-bezetting, waar 4/5 mei toch voor staan, toch vreemd.

De demonstratie eindigt waar die is begonnen. Voor Den Haag Centraal worden mensen gearresteerd. Waarom is niet geheel duidelijk, tuurlijk het niet opvolgen van de coronavoorschriften, maar een deel van de demonstratie is wel degelijk breed opgezet, misschien niet precies 1,5 meter afstand, maar toch gepaste afstand. Opdracht van de politie is echter voor het optreden zo snel mogelijk het protest te smoren: ”In vroeg stadium voorkomen dat demo groter wordt. Dus snel ingrijpen al bij 2 of meer demonstranten. Moet nog formeel met Burgemeester worden kortgesloten” (overleg 1-5-20). De autoriteiten willen koste was het kost voorkomen dat het protest groeit. Vandaar de grove inzet met arrestatie-eenheden, paarden, gevechtstenue en lange latten, ‘oprotten wappies’ hoor je de staat bij monde van waarnemend burgemeester Remkes roepen. De oogst, tachtig demonstranten aangehouden voor het overtreden van coronamaatregelen, opeengepakt in bussen met enkele centimeters tussen hun hoofden, allemaal voor de bescherming van de volksgezondheid, zie hier waar de staat echt voor staat in een crisis, zeker op Bevrijdingsdag 5 mei.

Politie stukken demonstratie 5 mei 2020 deel 1

Politie stukken demonstratie 5 mei 2020 deel 2

Politie stukken demonstratie 5 mei 2020 deel 3

Politie stukken demonstratie 5 mei 2020 deel 4

Naar inhoudsopgave Observant # 81

De Wijster Razzia

Volwassenen en kinderen geslachtofferd omdat de overheid een punt wilde maken.

Tijdens de politieactie heeft de media geen oog voor het verhaal van de slachtoffers, pas een half jaar later volgt een reconstructie. Rechters vinden dat burgers niet mogen demonstreren als overheden dat stellen. Burgemeesters stellen zich afzijdig op en gaan niet pal voor grondwettelijke rechten staan. Zie hier in een notendop het afglijden van de Nederlandse rechtstaat. Het optreden rond de blokkade van Attero op 8 juli 2020 is exemplarisch voor het demonstratierecht in Nederland.

Naar aanleiding van de boerenprotesten dit jaar is door verschillende activisten gesuggereerd dat de boeren door de politie met fluwelen handschoenen zijn aangepakt. Dit in vergelijking met klimaatactivisten, mensen die protesteren tegen het woonbeleid en meer vermeende 'linkse' thema's. Buro Jansen & Janssen is altijd voorzichtig in zeer stellige beweringen, deels omdat de waarheid altijd in de nuances zit, maar ook omdat de bovenstaande suggestie op een aansporing aan de politie lijkt om maar eens flink te gaan optreden tegen de boeren.

Die aansporing is niet alleen kortzichtig, maar ook gevaarlijk, uiteindelijk kan iedere stellingname ten aanzien van demonstraties of meningsuitingen van anderen tegen je eigen actiegroep gebruikt worden. Zo wordt er vaak gejuicht als extreemrechtse demonstraties door burgemeesters worden verboden of verplaatst naar afgelegen, uitgestorven industrieterreinen. Buro Jansen & Janssen juicht niet want kijkt vooral vooruit, wat gaat dit betekenen in de toekomst voor anderen. Tegenwoordig komt het dan ook regelmatig voor dat

demonstraties worden verbannen naar locaties die volstrekt niet relevant zijn of van publiek verstoken. Dat heeft dus een historie.

Bij het toejuichen van de belemmering van grondwettelijke rechten aan bepaalde groepen, moet je jezelf altijd de vraag stellen, zijn wij de volgende, want als bestuur en rechterlijke macht kans zien om bepaalde uitingen te verbieden, kunnen andere uitingen daar ook het slachtoffer van worden. Dat wil niet zeggen dat je tegen bepaalde demonstraties kunt zijn, maar het steunen van overheidsbeleid ten aanzien van grondwettelijke rechten is niet zonder gevolgen.

Bij de boerenprotesten speelt daarnaast nog een ander aspect. De boeren gebruiken groot materieel. In het algemeen is de politie daar niet dusdanig op voorbereid om adequaat tegen op te treden. Wat ook speelt is dat de macht van het getal zijn tol eist bij de ordehandhaving. De boeren komen vaak in dusdanige aantallen opdraven dat van handhaving geen sprake meer is.

Wijster 8 juli 2020

Dat wil niet zeggen dat de politie de wens niet heeft om hard op te treden. Veel politieoptreden blijft echter onzichtbaar. Toch laat optreden van de politie na een protest in Wijster op 8 juli 2021 zien dat de politie even hard optreedt bij boeren als bij andere actievoerders als zij daartoe de kans krijgen. De politie spreekt in een SGBO-verslag en in een Power Point Presentatie van 63 arrestanten en respectievelijk 27 en 7 minderjarigen, waarvan er een vijftien jaar is. Alle actievoerders worden niet tijdens de blokkade van afvalverwerker Attero gearresteerd, maar op het terrein van het loonwerkersbedrijf Fikkert, aan de Vamweg in Wijster, waar zij na de demonstratie verzamelden.

De actie start in alle vroegte. “Sinds 4.30 uur actie in Wijster. Auto's en landbouwvoertuigen,” schrijft de politie. In het eerste SGBO-vergadering op 8 juli 2020 om 06.45 uur staat dat “in de loop van de nacht de boeren in actie zijn gekomen in Wijster.” Volgens de politie

zou het gaan om “60 a 70 voertuigen (landbouwvoertuigen en personenauto's)” en is de politie al ter plaatse. “Terrein is afgezet door politie eenheden,” staat in het verslag. In een uitzending van Hart van Nederland zegt een van de demonstranten dat bij afvalverwerker Attero om halfvijf begon. “We pakken de grootste stikstof uitstoter van Drenthe aan,” voegt hij toe.

WOM-brief

In alle overheidscommunicatie wordt verwezen naar een zogenoemde WOM-brief (WOM Wet Openbare Manifestaties). Deze brief van de voorzitter van de veiligheidsraad zou alleen het demonstreren met landbouwvoertuigen verbieden. Dat is ook de aanhef van WOM-beschikking ‘aan protesterende boeren en sympathisanten die van plan zijn met trekkers en andere (zware) voertuigen de weg te gebruiken’. In de beschikking wordt verwezen naar acties op 4 en 5 juli 2020 bij Jumbo te Beilen, GAE, knooppunt Hoogeveen, Coop te Gieten.

De brief bevat echter ook een verwijzing naar de COVID-maatregelen die toen van kracht waren en die de mogelijkheid geven om demonstraties verder te beperken zoals tijdens de coronapandemie zichtbaar is geworden. “Ik wijs er verder op dat in de afgelopen dagen is gebleken dat bij de demonstraties, de daarmee gepaard gaande wanordelijkheden en de bestrijding daarvan, ook de COVID-regels niet in acht (kunnen) worden genomen,” schrijft de plaatsvervangend voorzitter van de Veiligheidsregio Drenthe H.F. van Oosterhout.

Is het politieoptreden juridisch afgedicht?

Uit die eerste SGBO-vergadering van 06.45 uur wordt dan ook duidelijk dat de politie gaat optreden in Wijster en niet alleen met boetes. De plaatsvervangend districtscommandant Drenthe somt nog even de bekeuringen van de vorige dag op: “Sinds 07-07-2020 geldt WOM brief in alle drie de districten (Friesland, Groningen en Drenthe

red.). Geldt alleen voor landbouwvoertuigen. Gisteravond actie in Leeuwarden. 60-70 personenauto's… Er zijn bekeuringen uitgeschreven. 30 personen zijn gebleven … in Heerenveen. Vier bekeuringen uitgedeeld.”

Het Hoofd Bewaken en Beveiligen (HBB) vraagt of het politieoptreden juridisch is afgedicht. “HOPS (Hoofd Opsporing) loopt het juridisch kader door en geeft aan dat het juridisch dicht is. Collega's zijn gebriefd en zijn bekend met de kaders. Collega's ter plaatse wordt gevraagd bij een aanhouding foto's te maken en bij de foto's de naam van de collega die aanhoud te vermelden.” Hoewel er altijd rekening wordt gehouden met mogelijke arrestaties bij demonstraties is bij Wijster duidelijk dat de politie van zins is iedereen aan te houden. “Aan de Balkengracht wordt een arrestantenstraat ingericht,” staat al in het eerste SGBO-verslag.

Onderaan het eerste verslag van 8 juli 2020 staat dat het volgende overleg over een uur zal plaatsvinden: “Volgend overleg 08-07-2020 08.00 uur.” Het verslag van dit overleg is niet openbaar gemaakt. Dat is opvallend omdat bij het volgende overleg al gesproken wordt over het aanhouden van verdachten. Hoofd Handhaving: “Richten op … Boeren zijn dit terrein opgegaan. Terrein is van … Verwachting is dat er 50 tot 60 verdachten worden aangehouden. Situatie ter plekke is rustig. Voertuigen staan op het terrein van …”

Boeren beëindigen blokkade in overleg met politie

Tijdens de blokkade van vuilverwerker Attero heeft de politie niet alleen het terrein van Attero afgezet zoals zij zelf schrijft, maar ook de toegangswegen. Er kan niemand meer door. In de rapportage van de politie wordt niet aangegeven wanneer dit was, maar dit is zeker voor halfnegen gebeurd. In Dagblad van het Noorden wordt een vrouw aangehaald die om halfnegen met haar dochter van twee jaar probeert weg te rijden en teruggestuurd door de politie. Naar alle waarschijnlijkheid heeft de politie al voor 06.45 uur de toegangswegen afgezet omdat Attero zelf de poort heeft gesloten. Dit is te zien op

foto’s van de demonstratie. RTV Drenthe meldt om 07.15 uur dat de politie al verschillende wegen heeft afgesloten. Pottenkijkers zijn niet welkom.

Van 06.45 tot 08.10 uur hebben de actievoerders uit zichzelf de blokkade beëindigd en zijn vertrokken naar het terrein van een bevriende ondernemer. Dit wordt zowel door de politie als door een uitgebreid verslag in Dagblad van het Noorden van 19 december 2020 bevestigd. De politie meldt in de Sitrap (situatie rapportage red.) nr. 8 van 8 juli 2020 om 20.40 uur: “8.10 uur: De ingang van … is weer vrij, stoet verplaatst zich in noordelijke richting; via Vamweg. Van de demonstranten staat nog er 1 tractor, 1 auto en 1 vrachtwagen bij … boeren zouden vanaf … rechtsomkeert hebben gemaakt en weer richting Spier zijn gaan rijden. De demonstratie zou nog niet zijn afgelopen (bron: RTV Drenthe).” De politie heeft de Sitrap’s nummer 1 tot en met 3 niet openbaar gemaakt.

Wat de politie en RTV Drenthe bedoelen met het laatste bericht is niet duidelijk. Uiteindelijk eindigde de blokkade van de boeren met een ochtend barbecue of het terrein van Fikkert. Ook de aanhoudingen van de Wijster demonstratie vinden allemaal plaats op het terrein van het loonwerkersbedrijf. Van een demonstratie na acht uur wordt nergens melding gemaakt. In Dagblad van het Noorden artikel ‘Klopjacht op het erf’ zeggen de boeren zelf dat zij om acht uur de blokkade hebben beëindigd: “In alle rust en redelijkheid, zo zullen meerdere boeren het zich herinneren, is de demonstratie die ochtend om 8 uur beëindigd.”

De boeren zeggen in het artikel zelfs gebeurd dat dit in overleg met aanwezige agenten is gebeurd. “In overleg met de politie bovendien, zeggen twee boeren die twee dienders spraken van wie zich in ieder geval een voordeed als leidinggevende. Ze hoorden het de politieman nog twee keer navragen. ‘Dus jullie houden er echt mee op nu?’” Omdat de toegangswegen zijn afgesloten, verhuizen de actievoerders van de poort van Attero naar de andere kant van de Vamweg: “Een club van bijna zeventig mensen is vervolgens naar de andere kant van de Vamweg, het erf van Fikkert gegaan. Ze konden ook eigenlijk nergens anders heen, de politie heeft alles afgesloten.”

Het verhaal van de boeren in Dagblad van het Noorden wordt bevestigd door een HHN bericht (Hoofd Handhaven Netwerken): "07.53 uur contact met woordvoerder … Woont in … Gaat contact leggen met … 08.05 uur contact met … Hij gaf aan dat het op de locatie opgelost lijkt te zijn. Boeren zijn weg. … Ze laten weer mensen door. … 08.30 uur contact met … De boeren zijn inmiddels weg. De meeste medewerkers van … konden via een andere ingang naar binnen" (berichten knophoofd HHN 8 juli 2020). Om half negen was de blokkade volledig opgeheven, maar al eerder konden de werknemers van Attero gewoon het bedrijf bereiken omdat niet alle ingangen zijn geblokkeerd. De demonstratie is dus vooral symbolisch.

De zienswijze van de boeren in december 2020 dat de blokkade in goed overleg met de politie is opgebroken bereikt die dag de media niet. In het SGBO-verslag van 09.00 uur staat dan ook dat de media de lijn van de politie volgen: "Media communiceert wat wij weten." Of journalisten hebben gepoogd om dichterbij de demonstratie te komen, komt in de media niet voor. De opmerking dat de media communiceert wat de politie weet of beter gezegd communiceert heeft ook betrekking op het aantal voertuigen dat aanwezig is bij de actie.

Fakenieuws van de politie

In de eerste berichten over de demonstratie van Wijster spreekt de politie van "60 a 70 voertuigen (landbouwvoertuigen en personenauto's)." Dit staat in het eerste SGBO-verslag van die dag. Opvallend is dat dit precies het aantal is dat ook in Leeuwarden is vastgesteld. Daar gaat het echter alleen om personenauto's: "Gisteravond actie in Leeuwarden. 60-70 personenauto's…" De boeren zelf stellen dat het door de politie genoemde aantal onzin is. "Op luchtfoto's van de blokkade die ochtend zijn niet meer dan 25 trekkers zichtbaar." Ook hiervan is onduidelijk of de media geprobeerd heeft de informatie van de politie te verifiëren.

Het genoemde aantal van de boeren wordt bevestigd door beelden van het omsingelde terrein van het loonwerkersbedrijf. In de discussie over

de actie gaat het dan allang niet meer over de blokkade, maar over de vraag of de aanhoudingen rustig zullen verlopen en of het tot een kloppartij met de Mobiele Eenheid. In het SGBO-verslag van 10.00 uur constateert de politie tevreden: “Pers is aanwezig. Berichtgeving is feitelijk.” Vraag is echter of de aanwezige journalisten pogingen hebben gedaan om een of meerdere actievoerders te spreken.

Daar lijkt het niet op. De reconstructie van Dagblad van het Noorden vertelt het verhaal van de eigenaren van het loonwerkersbedrijf, Henk en Wilma Fikkert. Terwijl zij niet hebben deelgenomen aan de demonstratie worden ook zij aangehouden, maar twee van de drie dochters kunnen zich schuilhouden in de boerderij. “Hun twee dochters zijn met hun jonge kinderen via de keuken de slaapkamer ingevlucht, bovenin de bij het huis betrokken schuur, boven het café. Ze zullen zich daar meer dan twee uur lang angstig schuilhouden.”

Wat er in die twee uur gebeurd is voor de politie dan al duidelijk. Iedereen op het terrein is, wordt gearresteerd en meegenomen naar het arrestantencomplex Balkengracht in Assen. Dat corona maatregelen er wel voor de politiefunctionarissen zijn, maar niet voor de demonstranten is dan ook al duidelijk. Niet de demonstranten respecteren niet de corona regels, maar de overheid: “Indien er zo'n grote groep wordt aangehouden geeft dit problemen m.b.t. de COVID-maatregelen bij het arrestantencomplex aan de Balkengracht. Ruimten zijn te klein. Voorgesteld wordt om de parkeergarage aan de Balkengracht te gebruiken voor het ophouden van de verdachten,” staat in de derde SGBO-vergadering van 8 juli 2020 om 9.00 uur. In dezelfde vergadering blijkt dat er wel over de overheidsfunctionarissen wordt gezorgd: “COVID beschermingsmiddelen voor de collega's ter plekke zijn geregeld.”

Om 8.28 uur wordt er door de ME nog gemeld dat mensen zouden proberen te ontsnappen door met tractoren over de velden te rijden: “Tractoren zouden over de landerijen rijden (bron: ME).” Dit zijn geen tractoren van de demonstranten, maar medewerkers van het loonwerkersbedrijf die horen van de massale arrestatie. Vanaf negen uur gaat het snel. De politie betreedt het terrein van het loonwerkersbedrijf en drijft iedereen bijeen. In Sitrap nr. 4 8 juli 2020

09.30 uur van de SGBO ENN Boerendemonstratie staat de eerste demonstranten zijn gearresteerd: “9.10 uur: Eerste aanhouding gedaan, rustig verlopen. Bron GMS (Geïntegreerd Meldkamer Systeem red.), tenzij anders aangegeven.” Uiteindelijk worden er 63 mensen aangehouden waaronder zeven minderjarigen. De arrestanten staan boven op elkaar in een cirkel met de ME om hen heen. Ze worden in volle bussen vervoerd en vastgehouden. Coronaregels gelden niet voor de aangehouden demonstranten.

Ontsnappen door een maïsveld

Sommigen ontspringen de dans. Twee boeren vertellen Dagblad van het Noorden hun verhaal van een ontsnapping: “Als de politiebusjes het erf opkomen lopen twee boeren de andere kant het erf af, een paar honderd meter in de richting van de sloot en het spoor. Acht of tien ME’ers staan daar met honden te wachten. Dat ze er gloeiend bij zijn, horen ze. Ze mogen teruglopen naar voren, maar schieten halverwege gauw het maïsveld in, samen met een vrouw met twee kinderen die ze niet kennen, in een ultieme poging aan de politie te ontkomen.” De politie schrijft in Sitrap 4:”9.10 uur: 10 demonstranten zijn het maisveld in gelopen.”

Een vrouw die met haar gezin ook door het maisveld deelt haar verhaal: “Mijn vriend rende voorop met de twee jongens en ik er achteraan. Totaal liepen er zo een 15 man met ons op. De een na de ander dook het mais veld in en een paar rende gebukt door een sloot of greppel een heel eind verder het land in. Mijn vriend rende daar ook met de kinderen en ik er dus achter aan. Er stond blubber in de sloot en ik verloor al snel mijn schoenen. Ik pakte ze nog op en op blote voeten ging ik verder. Ik zakte steeds door mijn benen voelde mij verlamd door angst. Het enige wat er door mijn hoofd ging was de kinderen, de kinderen oh de kinderen. Ik zakte steeds in elkaar en mijn vriend en kinderen stond op het einde op mij te wachten en moedigde mij aan om op te schieten. Ik zei ga maar breng de kinderen in veiligheid ik kon niet ik was verlamd van angst. Ze gingen de greppel uit en doken het maisveld in en weg waren ze.”

Nu zijn er mensen die zullen zeggen, dit is wel erg dramatisch, de vrouw heeft het in haar verhaal zelfs over de Tweede Wereldoorlog. In de reconstructie van Dagblad van het Noorden vertellen demonstranten in dezelfde bewoordingen over het politieoptreden: "Het erf van Fikkert wordt grondig schoongeveegd door politiemannen, meerdere met bivakmuts, beenbeschermers om en een helm aan de gordel. Sommige mensen blijven verstijfd en verbijsterd staan. Wat gebeurt hier? Ongeloof klinkt ook maanden later nog door in hun verhalen." Klimaatactivisten, mensen die protesteren voor dierenrechten, tegen het opsluiten van vluchtelingen, voor kraken of het recht op wonen, zullen aangeven dat dit echter 'gewoon' politieoptreden is. 'Gewoon' alsof het 'de normaalste zaak van de wereld is'. Dat is het echter niet en dat vinden die boeren blijkbaar ook niet als het hen overkomt.

Alle arrestanten vrij

De politie heeft in Assen een zogenaamde arrestanten straat ingericht. Daar rijden de politiebussen naartoe en zetten de demonstranten af. Boeren uit de omgeving komen naar het politiebureau om de arrestanten te steunen. Het is bijna alsof er een ouderwetse krakers demo 'alle arrestanten vrij' plaatsvindt. In Sitrap nr. 6 8 juli 2020 15.00 uur wordt de ondersteuningsdemo beschreven: "De collega's hebben de wegen rond de Balkengracht afgezet. Demonstranten verzamelen zich hier (ongeveer 150 demonstranten om 14.12 en neemt voortdurend toe, sfeer is nu goed)."

In dezelfde Sitrap 6 staat dat de eerste arrestanten vrij worden gelaten: "De eerste arrestanten zijn met een beschikking weer vrijgelaten." Iedereen komt die middag vrij. Sitrap nr. 7 8 juli 2020 17.20 uur meldt dat alle arrestanten vrij zijn: "17.01 uur: Laatste arrestanten zijn vertrokken (bron: HOPS)." Dat na de arrestaties, de vrijlating met een beschikking er uiteindelijk geen vervolging plaatsvindt is bij demonstraties vaak ook niets nieuws.

Bij de blokkade van Attero in Wijster zijn volgens de politie 63 demonstranten opgepakt. Het openbaar ministerie spreekt in de rechtszaal over 54 arrestanten. Volgens de politie zijn 27 demonstranten minderjarig, in de media wordt gesproken over zeven of vijf minderjarigen. De politie zegt dat de jongste vijftien jaar is, de boeren negen jaar. De minderjarigen zijn meteen doorverwezen naar Halt voor een straf. Onduidelijk is of de politie heeft vastgesteld of de jongeren ook deelnamen aan de demonstratie.

Onterecht gearresteerd

Het Openbaar Ministerie oordeelt begin november 2020 dat 35 arrestanten niet verder worden vervolgd. Volgens het Openbaar ministerie zijn zes verdachten onterecht gearresteerd, is bij 28 arrestanten onvoldoende bewijs voor deelname aan de blokkade van Attero en in een geval acht het openbaar ministerie zich om onduidelijke redenen niet-ontvankelijk. Dat betekent dat meer dan de helft van de arrestanten vier maanden na hun arrestatie te horen krijgen dat ze onterecht zijn gearresteerd, niet voor de rechter hoeven te verschijnen en geen boete hoeven te betalen. Ze zijn dus onterecht van hun vrijheid beroofd.

Na de detentie op het politiebureau in Assen krijgen alle demonstranten een brief mee dat zij op 19 november 2020 voor de rechter moeten verschijnen en in ieder geval een boete van 390 euro. Vier betogers accepteren die boete op 8 juli 2020 meteen om strafvervolging af te kopen. Vier maanden later blijkt dus dat ze te snel schuld bekenden, want de politie heeft gewoon allerlei mensen willekeurig aangehouden. Uiteindelijk krijgen naast die vier demonstranten nog eens vijftien in november een strafbeschikking van 390 euro. Acht van de vijftien zijn het er niet mee eens en stappen naar de rechter. Wat vooral opvalt is dat een van hen, de eigenaar van het loonwerkersbedrijf, alsnog wordt vrijgesproken. Hij heeft niet deelgenomen aan de demonstratie. Zeven anderen krijgen een voorwaardelijke boete, ze hoeven geen 390 euro te betalen, maar

krijgen wel een standje. Een kleine overwinning voor de overheid, terwijl het optreden uiterst bizar is.

De rechter stelde bij de uitspraak dat er geen sprake van willekeur door politie en justitie, pas later zou zijn beoordeeld wie een boete kreeg, terwijl wel iedereen inclusief minderjarigen zijn aangehouden. Ook oordeelde de rechter dat het niet uitmaakte of je deelnam met een landbouwvoertuig of personenauto (het demonstratieverbod "geldt alleen voor landbouwvoertuigen," volgens de politie), fiets of anderszins, volgens haar was de WOM-beschikking van de veiligheidsregio Noord-Nederland een totaal verbod om te demonstreren, de demonstranten hoorden er niet te zijn. Dat in hoger beroep vier van de zeven voorwaardelijk veroordeelden zijn vrijgesproken doet niets af aan de implicaties van de rechter, blijkbaar is het simpelweg mogelijk om demonstraties te verbieden en gaat de rechterlijke macht daar akkoord mee. Het hoger beroep eind november 2021 is dan ook niet gewonnen op principiële gronden, maar omdat de WOM-beschikking in Drenthe niet officieel is gepubliceerd, dat geeft te denken.

Politiechef legt het de media uit

Het geeft vooral te denken in het licht van de verharding van de boerenacties in 2022. Frustraties over vooral bestuurders die niet direct communiceren met hun burgers, iets dat in Wijster op 8 juli 2020 erg zichtbaar is. De overheid is present via de lange warm van de macht, de ordehandhavers. Om 10.00 uur tijdens de 4e Vergadering SGBO-vergadering met HCOM (Hoofd Communicatie) dat de politiechef van de eenheid Noord-Nederland naar plaats delict afreist, niet om arrestaties te voorkomen, maar om de media te woord te staan: "Politiechef gaat naar locatie in Wijster om duiding te geven aan de media." De demonstratie is dan allang geen lokaal nieuws meer: "Niet alleen regionaal maar ook nationaal nieuws" (HCOM). Waarom korpschef Gery Veldhuis naar Wijster afreist als de demonstratie is beëindigd en iedereen op het terrein van het Loonwerkersbedrijf is aangehouden is niet openbaar gemaakt.

Veldhuis blijft tot in de middag aanspreekpunt voor de regionale en nationale media en kan daarmee de berichtgeving sturen. Tijdens de SGBO-vergadering van 14.00 uur meldt HCOM dat Wijster ondertussen groot nieuws is: "Acties zijn groot nationaal nieuws." Veldhuis wordt duidelijk naar voren geschoven als het bevoegd gezag dat de orde hersteld, de overheid wil stevig optreden uitstralen: "Politiechef is het boegbeeld" (HCOM). In de situatie rapportage van 15.00 uur wordt ook nog melding gemaakt dat de korpschef zelfs op de locatie van de arrestantenstraat de media te woord staat: "Gery Veldhuis ontvangt verslaggevers aan de Balkengracht" (Sitrap nr. 6 8 juli 2020 15.00 uur).

Er lijkt een soort parallelle werkelijkheid te zijn ontstaan. De reguliere media en de sociale media. Volgens de politie is het allemaal fake nieuws. "Veel fake nieuws momenteel," meldt HCOM om 15.30 uur tijde een SGBO-stafvergadering. Dat terwijl er wel vanuit de arrestantenlocatie live wordt gestreamd door twee mensen die zeggen dat ze journalisten zijn: "Twee dames zijn aan de Balkengracht bezig met een liveverslag. Uitgezocht wordt wie dit zijn." (HCOM 14.00 uur). Ook de komst van rond de 150 demonstranten naar het politiebureau in Assen om de vrijheid van de arrestanten te eisen is geen fakenieuws, de politie meldt zelf die aantallen. Sommigen zijn naar de stad gekomen met de tractor.

Media communiceert het beeld van de politiechef

Veldhuis is zelf tevreden over zijn werk als woordvoerder. De media communiceert blijkbaar het beeld dat de politie wil laten zien: "PC geeft aan dat het beeld van buiten tevreden is. Bestuurlijk wordt het goed opgepakt" (Politiechef tijdens de zesde SGBO-vergadering). De mediastrategie is geslaagd. Medewerker veiligheidszaken Synthia Jakobs appt nog even drie emoji's van gespierde armen. De overheid maakt weer eens duidelijk hoe zij met burgers communiceert, via de gespierde arm. Of dit nationaal is ingestoken blijft is niet openbaar gemaakt door de politie. Wel is duidelijk dat de minister de

ontwikkelingen in Wijster op de voet volgt. Ook hij, toentertijd Ferdinand Grapperhaus, overtreder van de coronaregels, staat in direct contact met het SGBO: “Actie heeft warme belangstelling van de Minister van Veiligheid en Justitie” (hoofd bestuursondersteuning (HBO)).

Het feit dat de bestuursondersteuning dit meldt is opvallend aangezien in de stukken er weinig verwijzingen zijn naar de burgemeester Mieke F.V. Damsma van Midden-Drenthe, waar Wijster onder valt, maar ook niet de voorzitter van de veiligheidsregio Drenthe of Noord-Nederland. Het is dan ook logisch dat de eigenaar van het loonwerkersbedrijf de indruk heeft dat de overheid hard wilde optreden: “Ik heb meer het idee dat er een signaal afgegeven moet worden door een aantal burgemeesters” (Hart van Nederland 8 juli 2020). Dit terwijl hij eraan toevoegt dat er geen gekke dingen zijn gebeurd. Dit wordt bevestigd door de documenten van de politie. Of de burgemeesters de aanzet hebben gegeven tot harder optreden of dat dit meer vanuit Den Haag komt, is niet openbaar gemaakt.

Wel blijkt dat politieagenten tijdens de demonstratie en de arrestatie enigszins gefrustreerd zijn. Of dit de agenten zijn die met de demonstranten bij Attero spreken over het opheffen van de blokkade en de boeren laten vertrekken naar het terrein van Fikkert is ook niet openbaar gemaakt. In de laatste SGBO-vergadering van 8 juli 2020 meldt de bestuursondersteuning dat er blijkbaar een bestuurlijk verschil is geweest. Dit kan duiden op onenigheid tussen het lokale gezag, de burgemeester, en het regionale/nationale gezag, de veiligheidsregio en het ministerie. “Bestuurlijk verschil van inzicht is voor collega's erg lastig. Wie is er verantwoordelijk voor? Politie blijft lokale gezag informeren. Openbare orde is altijd verantwoordelijkheid van de BM (Burgemeester red.)” (HBO).

Volgende keer precies hetzelfde

In de reconstructie van Dagblad van het Noorden in december 2020 wordt geschreven dat bij de politie ook twijfels zijn bij het optreden:

“Een signaal waarvan de politie later zal zeggen: het had absoluut anders gekund.” Deze opmerking lijkt niet erg waarachtig. Uit de openbaar gemaakte stukken van politie en veiligheidsregio blijkt niet dat het de volgende keer anders zal verlopen. Dit wordt ook bevestigd door telefonische vragen van Buro Jansen & Janssen aan de behandelend jurist van de politie-eenheid Noord-Nederland over een Wob-verzoek over de demonstratie.

De behandelend jurist heeft bij de SGBO-leiding nagevraagd of er een evaluatie heeft plaatsgevonden naar aanleiding van het politieoptreden in Wijster. Een dergelijke evaluatie zit niet bij de stukken. De SGBO-leiding van de eenheid Noord-Nederland bevestigt dat er geen evaluatie is. Op de vraag van Jansen & Janssen of de volgende keer op precies dezelfde wijze zal worden opgetreden, wordt bevestigend geantwoord, alsof er niets is gebeurd.

Politie stukken Wijster

Extra stukken bij wijster

Wijster demo 8 juli 2020 veiligheidsregio stukken na bezwaar

Wijster demo 8 juli 2020 veiligheidsregio stukken

app over optreden politie bij boeren protesten te Wijster

Naar inhoudsopgave Observant # 81

Maak het werk van Buro Jansen & Janssen mogelijk: Word donateur

Wilt u dat Buro Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, overheidsoptreden in het algemeen, bedrijven die meewerken aan repressief overheidsbeleid en/of zelf ook repressief of diep ingrijpen in het leven van burgers in Nederland en Europa steun ons dan.

Word donateur of vraag familie, vrienden en bekenden donateur te worden. Rekening NL43 ASNB 0856 9868 52 of NL56 INGB 0000 6039 04 ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam.

Stichting Res Publica is aangemerkt als ANBI (Algemeen Nut Beogende Instellingen) instelling. Dit betekent voor mensen die ons willen steunen het volgende:

– Als een instelling door de Belastingdienst is aangewezen als een ANBI, kan een donateur giften van de inkomsten- of vennootschapsbelasting aftrekken (uiteraard binnen de daarvoor geldende regels).

De werkvelden worden onderverdeeld in grondrechten, directe actie en vrije meningsuiting, radicale transparantie en fundamentele kritiek.

De werkvelden worden onderverdeeld in grondrechten, directe actie en vrije meningsuiting, radicale transparantie en fundamentele kritiek.

Grondrechten

– Centraal staan bij Buro Jansen & Janssen grondrechten in de breedste zin van het woord

Onderzoek van Buro Jansen & Janssen richt zich op politie, inlichtingendiensten, justitie, migratie en de overheid in het algemeen vooral in Nederland, een beetje Europa, maar de laatste jaren meer en meer ook buiten Europa zoals het Midden-Oosten en Centraal-Amerika. Onderwerpen in Nederland zijn in het kader van beperking van grondrechten; geweldsgebruik (onder andere politiewapen, pepperspray, stroomstootwapen, aanhoudingseenheden, mobiele eenheid), profilering/discriminatie (onder andere etnisch profileren, ochtendgloren, mobiel banditisme), overheid in de publieke ruimte (onder andere preventief fouilleren, identificatieplicht, gebiedsverboden), opsporingsmiddelen in het algemeen, digitale opsporingsmiddelen (onder andere politie spyware/malware, Social Media surveillance), inlichtingen operaties en privacy (inlichtingendiensten) en nog veel meer. Over veel zaken zijn in de afgelopen jaren diverse publicaties verschenen.

Directe actie en vrije meningsuiting

– Wij blijven op de achtergrond radicaal activisme steunen

Deels door publicaties zoals recentelijk de arrestantenhandleiding, een totaal vernieuwde update van het oude Tips tegen Tralies waarvan nu een tweede druk komt, maar ook door mensen te ondersteunen bij benaderingen, onderzoek naar mogelijke informanten, steun bij klachten, beschikbaar stellen van de digitale infrastructuur voor publicaties als de kraakhandleiding en andere wijzen. Alle publicaties en informatie zijn op de websites van Buro Jansen & Janssen te vinden.

Radicale transparantie

– Wij ondersteuning onderzoek en verbeteren van informatiepositie van individuen en groepen

Naast informatieverzoeken voor het eigen onderzoek ondersteunt Buro Jansen & Janssen individuen en groepen bij hun onderzoek en het verbeteren van hun informatiepositie en kennis. Het gaat hierbij om milieubeleid, drugsbeleid, sociale zekerheid, vrouwenrechten en andere terreinen. Al geruime tijd worden openbaarheid punt nl alle openbaar gemaakte documenten door Buro Jansen & Janssen online gezet. Ook door anderen verkregen Wob documenten worden daar nu aan toegevoegd. Rond de inlichtingendiensten is het nationaal veiligheidsarchief opgezet dat langzaam wordt uitgebouwd.

Fundamentele kritiek

– Impliciet heeft Buro Jansen & Janssen al sinds de jaren tachtig kritiek geuit op beleid en praktijk. Actieve lobby doet het Buro niet, maar het onderzoek, de artikelen en de documenten worden door veel mensen gebruikt. De laatste jaren wordt in artikelen van Buro Jansen & Janssen wel explicieter fundamentele kritiek geuit als onderdeel van een onderzoek. Voorbeelden zijn het magazine over de WIV2017, de observant over Social Media Surveillance in Nederland, een reeks artikelen en onderzoek naar de relatie tussen de wetenschap en de politie, over het duurzaamheidsbeleid van Nederlandse overheid en het gebruik van spyware/malware door de Nederlandse overheid en de bedrijven die die digitale wapens ontwikkelen.

Naar inhoudsopgave Observant # 81