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