Politie Mercenaries

Buro Jansen & Janssen

Observant 69, januari 2017

Inhoudsopgave Observant #69, januari 2017

Deze Observant draagt de titel politie mercenaries, politie huurlingen, een verwijzing naar huurlingen die in conflictgebieden worden ingehuurd. Het thema is het gebruik van digitale wapens door de Nederlandse politie. In de Engelstalige media wordt gebruik gemaakt van de term cyber weapons. Hier wordt de digitale wapens gebruikt. De term is niet geheel correct, maar offensieve software of spyware dekken niet de gehele lading. Het blijkt dat de digitale wapens namelijk vooral worden ingezet tegen oppositie bewegingen, journalisten, activisten vandaar dat het hier wordt gebruikt.

Centraal staan vier bedrijven, Hacking Team, Gamma Group, Providence en Kailax. Over Hacking Team En Gamma Group is al veel gepubliceerd vooral in de Engelstalig media op het internet waaronder de CitizenLab, Motherboard en Ars Technica. In deze Observant toch een uitgebreid profiel van beide bedrijven om vooral inzicht in te geven in het gebrek aan moraal bij deze bedrijven, de nauwe samenwerking met de overheden en het belang van historisch onderzoek naar achtergronden van bedrijven. Ook profielen van Providence en Kailax als mede de samenwerking tussen de Nationale Politie en deze bedrijven. De vier bedrijven belichten ieder een andere kant van het verhaal met betrekking tot digitale wapens, de geheimzinnige markt en de tussenhandel.

De focus lig op de Nederlandse politie. Dit wil niet zeggen dat andere bestuursorganen geen interesse tonen in digitale wapens. In door Wikileaks gepubliceerde gegevens van Hacking Team zitten de e-mail adressen van medewerkers van onder andere het Openbaar Ministerie, de belastingdienst, de inspectie SZW van het Nederlandse ministerie van Sociale Zaken en Werkgelegenheid (SZW), het ministerie van Defensie, het ministerie van Justitie (nu veiligheid en justitie) en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Verder in deze Observant een benadering van een Tor-beheerder, die van de AIVD eerst heel van alles kreeg aangeboden en vervolgens bedreigd omdat hij niet wilde meewerken. Het verhaal is opgesteld in het Engels en vertaald in het Nederlands. Tevens een gids van de Britse politie voor haar functionarissen over hoe zij hun veiligheid op het internet kunnen verbeteren met informatie over privacy instellingen voor sociale media, het veilig surfen op het internet en het gebruik van smartphones en tablets.

De artikelen staan ook op de website van Buro Jansen & Janssen

Boeven vangen met dubieuze software van dubieuze bedrijven

De Nederlandse politie breekt in op computers, smartphones en andere digitale hulpmiddelen van burgers, plaatst keyloggers en wil mensen digitaal kunnen volgen. Het maakt hierbij gebruik van digitale wapens. De branche van bedrijven die de Nederlandse politie digitale wapens te koop aanbiedt wordt gekenmerkt door een sfeer van geheimzinnigheid en ondoorzichtigheid. Deze wordt door de Nederlandse overheid in stand gehouden.

De afgelopen jaren zijn twee bedrijven die digitale wapens produceren gehackt. In 2014 publiceerde Wikileaks 40 GB aan documenten over Gamma Group en in 2015 400 GB over het Italiaanse computerbedrijf Hacking Team. Dit leverde een schat aan informatie op over deze bedrijven. In de Wikileaks documenten wordt duidelijk dat de Nederlandse politie contacten onderhoudt met de bedrijven Gamma Group, Hacking Team, Providence en waarschijnlijk Kailax.

Buro Jansen & Janssen heeft in 2016 diverse Wob (Wet Openbaarheid Bestuur) verzoeken ingediend, bij de Nationale Politie, het Ministerie van Veiligheid en Justitie, het Openbaar Ministerie en andere bestuursorganen. In een poging zicht te krijgen op de relatie tussen de Nederlandse overheid en deze ondoorzichtige markt. De Nederlandse overheid weigert echter om informatie openbaar te maken met welke bedrijven wordt samengewerkt en welke middelen zijn aangeschaft.

Het gebrek aan openbaarheid is zorgwekkend omdat er allerlei bezwaren kleven aan het gebruik van digitale wapens en de samenwerking met genoemde bedrijven. Er zijn allerlei veiligheidsrisico’s en risico’s voor de rechtspleging bij de inzet van digitale wapens. Er vallen vraagtekens te plaatsen bij de financiële integriteit van producerende bedrijven. De achtergronden van de producten, de onduidelijkheid over het ontwikkelingstraject van de producten en het gebruik van tussenhandelaren maakt de markt en de veiligheid van de digitale wapens nog ondoorzichtiger. Tevens leveren deze bedrijven aan repressieve regimes die digitale wapens inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten.

De Nederlandse politie hackt en niet alleen sinds de Wet computercriminaliteit III. De politie maakt voor dit hacken gebruik van digitale wapens. Hoe vaak dit gebeurt is niet duidelijk. In antwoord op Kamervragen antwoordde het Ministerie van Veiligheid en Justitie op 7 februari 2012 dat de politie beschikt over 'software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen'. Volgens het Ministerie was er op dat moment (2012) 'in een zeer beperkt aantal gevallen gebruik van gemaakt.'

Bredolab

Een eerste aanwijzing voor het gebruik van digitale wapens deed zich eind 2010 voor. Toen werd het zogenaamde Bredolab netwerk, met medewerking van de Nederlandse politie, uit de lucht gehaald. Het Bredolab botnet bestond vooral uit servers in Nederland en zou volgens de Nederlandse overheid miljoenen computers hebben besmet, waarna persoonsgegevens en gevoelige informatie werd gestolen. Het oprollen van het netwerk werd met veel bombarie in het nieuws gebracht. Het is echter onduidelijk of het netwerk daadwerkelijk is ontmanteld: besmette computers werden na de ontmanteling van het botnet na enkele dagen op een andere wijze aangestuurd.

Bij het oprollen van het botnet brak de politie in op computers van slachtoffers en waarschijnlijk ook verdachten. Op security.nl reageerde Peter Zinn (senior adviseur van het Team High Tech Crime van het Korps Landelijke Politiediensten) op 7 november 2011: *'Ondanks de ontstane commotie rond de legitimiteit van het optreden bij de Bredolab ontmanteling, zijn team niettemin op de ingeslagen weg voortgaat "al mag het misschien niet van de rechter"*.' De uitspraken van Zinn duiden op verdergaande interesse van de politie in digitale wapens.

Dat de politie digitale wapens is blijven gebruiken blijkt uit de antwoorden van de Minister van Veiligheid en Justitie van 7 oktober 2014 op vragen van het Kamerlid Sharon Gesthuizen van de SP: 'De politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte.' Als wettelijke grondslag voor het politie hacken wordt verwezen naar artikel 126l van het Wetboek van Strafvordering, 'het opnemen van vertrouwelijke communicatie.' Op de vraag of de politie experimenteert in de aanloop naar de Wet

Computercriminaliteit III stelt de minister dat ‘de politie niet experimenteert met het overnemen van computers van verdachten.’

BOB, Hacken bij wet

Inmiddels is de Wet Computercriminaliteit III in 2016 door de Tweede Kamer aangenomen en kan de vraag of de politie mag inbreken in smartphones, tablets en andere digitale hulpmiddelen van burgers positief worden beantwoord.

In deze wet wordt in artikel 126nba omschreven wanneer, onder welke omstandigheden en voorwaarden de politie mag inbreken op een smartphone. Volgens lid 1 kan 'de officier van justitie bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet.' Dit kan door middel van hacken of door fysiek in te breken in iemands huis en eventueel met behulp van een gegevensdrager (USB-stick of iets anders) een programma aan te brengen in de laptop, smartphone of iets anders om het gebruik van het digitale hulpmiddel te monitoren of af te kunnen luisteren.

De regering achtte de invoering van artikel 126nba noodzakelijk omdat het Wetboek van Strafvordering het inbreken op elektronica van burgers niet expliciet mogelijk zou maken. Al vóór de behandeling in de Tweede Kamer van de Wet Computercriminaliteit III werd echter al het digitale wapen FinFisher van Gamma Group gebruikt.

Het Openbaar Ministerie en de politie zullen zeggen dat zij hacken op grond van de BOB, de Bijzondere Opsporingsbevoegdheden. De BOB werd na de commissie Van Traa, de parlementaire commissie opsporingsmethoden, opgesteld en formaliseerde de opsporingsmethoden die tijdens de parlementaire enquête naar boven kwamen, zoals het doorlaten van drugstransporten en het runnen en inzetten van (burger)infiltranten. De effectiviteit van deze methoden werd door de Commissie Van Traa overigens in twijfel getrokken. De bijzondere opsporingsbevoegdheden zijn ondertussen opgenomen in het Wetboek van Strafvordering. Hiermee wordt eigenlijk onderstreept dat de overheid deze bevoegdheden niet meer als bijzonder beschouwd.

Artikel 126g tot en met 126ii (Wetboek van Strafvordering) waaronder

ook het artikel 126l valt, gaan over die 'bijzondere bevoegdheden' waarbij onderscheid is gemaakt tussen 'gewone bijzondere bevoegdheden' en 'bijzondere bevoegdheden' die ingezet kunnen worden bij misdrijven in georganiseerd verband en opsporing van terroristische misdrijven. Deze artikelen bieden voldoende aanknopingspunten voor politie en justitie om te beweren dat de inzet van 'technische hulpmiddelen' juridisch is afgedekt.

Toetsing door de rechtbank van deze 'bijzondere' middelen (en van middelen die in het verleden onder de BOB vielen) blijft echter een heikel punt. Er wordt niet altijd aan alle zorgvuldigheidseisen voldaan. Dit blijkt bijvoorbeeld bij de inzet en de precieze rol van informanten, die soms verborgen wordt gehouden voor de verdediging van de verdachte en de rechtbank. Technische hulpmiddelen om digitaal in te breken, zijn vergelijkbaar met de rol van de informant, de politie-infiltrant, de burgerinfiltrant, de gecontroleerde doorvoer en andere vergaande middelen die de overheid kan gebruiken.

De minister zegt dat er digitale wapens worden gebruikt, maar geeft niet aan welke. Tijdens rechtszaken wordt veelal niet expliciet vermeld of er is gehackt en welke digitale wapens zijn gebruikt. Dit roept de vraag op of het bewijs dat wordt verkregen met behulp van de inzet van digitale wapens rechtsgeldig is?

Uit de Wikileaks gegevens over Hacking Team blijkt dat de digitale wapens van dat bedrijf een *backdoor* hebben. Hacking Team, maar theoretisch ook anderen kunnen zich via die backdoor toegang verschaffen tot de systemen en ook tot computers van verdachten. Wie de daadwerkelijke ontwikkelaars van FinFisher zijn is niet duidelijk. Aan dit digitale wapen van Gamma Group hebben diverse bedrijven meegewerkt dit roept vragen op over de authenticiteit en integriteit van het product.

Of de Nationale Politie beschikt over de broncode van door haar gebruikte digitale wapens wil het ministerie van Veiligheid en Justitie niet zeggen. In de beantwoording van de Wob is een e-mail opgenomen van een ambtenaar die op 14 juli 2015, één dag nadat PvdA en D66 vragen hebben gesteld over Hacking Team, schrijft: 'Bij vraag 5 vraag ik mij af of je hier wel iets op moet zeggen, lijkt mij niet wenselijk om hier openbaar inzicht in te bieden.'

De politie heeft de broncode van digitale wapens waarschijnlijkheid niet.

Bij de afluisterapparatuur van Nice Systems heeft het ministerie begin 2016 aangegeven dat zij niet beschikt over de broncode en dus niet in staat is de werking van tapsystemen te doorgronden.

Doordat feitelijke gegevens over het al dan niet gebruiken van deze 'technische hulpmiddelen' geheim worden gehouden en openbare audit-rapporten over deze digitale wapens niet beschikbaar zijn, is controle op inzet en gebruik niet mogelijk. De vraag is of de politie zonder de broncode de authenticiteit en integriteit van de digitale wapens kan vaststellen. Dat maakt het bewijsmateriaal verkregen met behulp van digitale wapens discutabel. Er kan namelijk informatie worden binnen gehaald, documenten en data worden aangemaakt of geplaatst die de verdenking van de persoon rechtvaardigt.

Topje van de ijsberg

Met welke bedrijven gaat de Nederlandse politie in zee als het gaat om digitale wapens? Uit de Wikileaks documenten en de antwoorden op Wob verzoeken blijkt dat de Nationale Politie contacten heeft met Gamma Group, het Italiaanse computerbedrijf Hacking Team, Providence en waarschijnlijkheid Kailax. Het staat vast dat er van Gamma Group en Providence producten en/of diensten zijn afgenomen.

Wat deze bedrijven gemeen hebben is bovenal een gebrek aan openheid. Ze geven geen inzicht over de ontwikkelfase van hun digitale wapens zowel wat betreft ontwikkelaars als bedrijven die aan die ontwikkeling hebben meegewerkt of van wie de tussenhandelaren hun producten betrekken. Betreffende bedrijven publiceren op hun websites geen inhoudelijke of financiële jaarverslagen. Ook over hun financiële huishouding, bedrijfsstructuur, geschiedenis, achtergronden van ontwikkelaars, bedrijfsleiding, aan welke overheidsdiensten wordt geleverd en de klantenkring in het algemeen geven bedrijven nauwelijks inzicht in.

Met de publicatie van de Wikileaks documenten over Gamma Group en Hacking Team in 2014 en 2015 is een schat aan informatie over deze bedrijven naar boven gekomen, die daarvoor nog niet openbaar was. Waarschijnlijk betreft het hier nog maar het topje van de ijsberg.

Gamma Group, FinFisher, Louthean Nelson

Gamma Group is een van oorsprong Brits bedrijf met vertakkingen in Duitsland en de belastingparadijzen Britse Maagdeneilanden, Libanon, Cyprus en Singapore. Gamma Group houdt zich bezig met de productie en verkoop van digitale wapens. FinFisher/FinSpy dat sinds 2008 te koop wordt aangeboden is het meest gewilde product. Met FinFisher van Gamma Group kan worden ingebroken op computers, laptops, tablets en smartphones.

De herkomst van de FinFisher is een enigma. Het valt moeilijk te achterhalen welke bedrijven en individuen er betrokken zijn geweest bij de ontwikkeling. Als producenten van FinFisher worden de Duitse tak van Gamma International en het bedrijf Elaman genoemd. Het is echter de vraag of dit de makers zijn. Uit onderzoek is duidelijk geworden dat FinFisher waarschijnlijk in Duitsland is ontwikkeld met medewerking van een medewerker van het Amerikaanse bedrijf CloudShield en mogelijk de Amerikaanse inlichtingendienst (National Security Agency) en oud medewerkers van de NSA basis Bad Aibling bij München.

Grote man achter Gamma Group is Louthean Nelson. Hij begon zijn carrière in de jaren 80 en 90 bij PK Electronic van Peter Klüver. Dit Duitse bedrijf heeft een geschiedenis van wapenhandel met dubieuze regimes en is meerdere malen op de vingers getikt. Nelson zet met Gamma Group de traditie van de wapenhandel van PK Electronic voort, zowel wat betreft de digitale wapens die zowel civiel als militair worden gebruikt, als wat betreft de klantenkring.

Vanaf 2011 is duidelijk geworden dat Gamma Group FinFisher levert aan repressieve regimes die het digitale wapen inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten. In dat jaar ontdekken activisten tijdens de Arabische Lente dat dictator Moebarak voor ruim drie ton FinFisher had aangeschaft. In 2012 volgen onthullingen over de inzet van FinFisher in Bahrein tegen oppositieleden. Met de publicatie van de gehackte gegevens van Gamma Group door Wikileaks in 2014 en zijn er nog meer details over de klantenkring van Gamma Group bekend geworden. Deze klanten omvatten, naast Egypte en Bahrein, repressieve regimes zoals Saoedi-Arabië, Turkmenistan, Kazachstan, Venezuela en Marokko en ook landen als Nederland en België.

Hacking Team, Galileo RCS, David Vincenzetti

Het Italiaanse computerbedrijf Hacking Team heeft zich sinds haar oprichting in 2003 ontwikkeld van een handelaar in beveiligingssoftware waarmee bedrijven zich kunnen weren tegen digitale inbraak, tot een belangrijke producent van digitale wapens. In 2006 presenteerde Hacking Team de eerste versie van haar digitale wapen Remote Control System (RCS), dat eerst DaVinci werd genoemd en later Galileo. Hiermee kan worden ingebroken op telefoons en computers en toegang worden verkregen tot alle aanwezige programma's en accounts, zoals Skype of Facebook. RCS is het meest gewilde digitale wapen van Hacking Team.

Net als Gamma Group is ook Hacking Team niet kieskeurig in het bepalen van haar klantenkring. In 2013 en 2014 lekten al controversiële deals uit met Marokko, de Verenigde Arabische Emiraten, Egypte en - ondanks een VN embargo - ook Soedan. In 2015 werd de volle omvang van de handel met repressieve regimes duidelijk door de publicatie van 400GB aan gegevens van het bedrijf door de website Wikileaks. Volgens Hacking Team was er een ethische commissie die de verkoop van de digitale wapens evalueerde, maar hoeveel waarde aan die commissie moet worden gehecht is onduidelijk. Toen de commissie actief was werd er geëxporteerd naar Soedan.

De Wikileaks documenten leveren ook een unieke kijk op de tussenhandel van digitale wapens. Hacking Team leverde bijvoorbeeld ook aan Italiaanse bedrijven als SIO SpA en Area SpA, die afluistercentrales voor telefoon- en internetverkeer beheren voor het Italiaanse Openbaar Ministerie, maar ook actief zijn op de commerciële markt. Area SpA doet bijvoorbeeld zaken met het regime van Bashar al-Assad in Syrië en op dit moment loopt er een justitieel onderzoek naar illegale export naar Syrië door Area SpA. Een andere tussenhandelaar is het Israëlische Nice dat samen met Hacking Team leverde aan landen als Kazachstan en Oeganda. De Nederlandse politie toonde zich zeer geïnteresseerd in de RCS van Hacking Team.

De Wikileaks documenten over Hacking Team laten naast een dubieuze klantenkring ook de verwevenheid met en de ontbrekende controle en toezicht van de Italiaanse overheid zien. Het bedrijf wordt mede gefinancierd door een regionaal overheidsfonds en een privaat fonds dat ook geld van de nationale overheid ontvangt. De Italiaanse overheid was tevens een belangrijke klant van Hacking Team. Lange tijd verlangde de

Italiaanse overheid geen exportvergunningen voor de uitvoer naar conflictgebieden en repressieve regimes.

Centrale persoon in Hacking Team is David Vincenzetti. In de jaren 90 was hij werkzaam voor de Universiteit van Milaan en werd destijds door sommigen beschouwd als een van de voorvechters van internetvrijheid. Sinds eind jaren negentig is hij op zoek naar het grote geld, een van de hobby's die hij heeft is geld verdienen. Op zijn LinkedIn account schrijft hij: "My main non-professional interest is finance".

Providence, Turner, Holmes, Stolwerk

Providence is een in 2009 opgericht Brits bedrijf in security. Het biedt trainingen en apparatuur op het gebied van veiligheid en anti-terrorisme aan. Bij de trainingen gaat het bijvoorbeeld om observatie tactieken, inbreken en het installeren van afluisterapparatuur. Bij de apparatuur gaat het om zaken als toolkits voor het installeren van afluisterapparatuur, gespecialiseerd inbrekersgereedschap, nepstenen en boomstammen om camera's en microfoons in te verbergen. Providence produceert en ontwikkelt zelf geen digitale wapens.

Het bedrijf heeft hechte banden met het Britse leger. Oprichter Stephen Turner heeft een verleden bij de SAS, de Special Air Services. De SAS is veroordeeld voor mensenrechten schendingen in Noord-Ierland. Een ex-SAS commandant verklaarde in 2016: '*UK Special Forces were helping to run Latin American-style death squads*.' Turner staat in nauw contact met voormalig SAS generaal John Taylor Holmes. Holmes wordt gezien als de Britse super fixer, maar heeft een dubieuze reputatie.

Wikileaks documenten van Hacking Team geven een onthullend inzicht in Providence en de wereld van de tussenhandel. Zo speelt Providence gevoelige Australische overheidsinformatie door. Providence blijkt op de hoogte dat het Australische leger gebruik maakt van FinFisher van Gamma Group. Providence deelt deze gevoelige overheidsinformatie met Hacking Team en zegt dat de Australische Special Forces niet tevreden over FinFisher zijn. Providence probeert zich zo te ontwikkelen tot distributeur van digitale wapens van Hacking Team. Rond een potentiële klant van Hacking Team producten in Ecuador probeert Providence een Ecuadoraans bedrijf van twee van haar medewerkers naar voren te schuiven.

Er is weinig openbare informatie beschikbaar over Providence. Het bedrijf is opgebouwd uit een wirwar van Bv's, vooral in Groot-Brittannië, maar ook in Nederland en Panama. Over de financiële huishouding is weinig bekend, evenals over de klantenkring van het bedrijf. Deze zal echter niet veel afwijken van die van Hacking Team en Gamma Group. In de Wikileaks documenten over Hacking Team komt het bedrijf veelvuldig voor. Daardoor is er meer bekend over de tussenhandel. Providence blijkt te opereren als tussenhandelaar in digitale wapens, vooral de Kailax *Unlocker*.

De Nationale Politie doet inkopen

De Nationale Politie doet zaken met bovengenoemde dubieuze bedrijven. Het valt niet vast te stellen op welke wijze de politie precies in contact komt met deze bedrijven, maar beursbezoek behoort daar zeker bij. Bedrijven die digitale wapens aanbieden zoals Hacking Team en Gamma Group, en tussenhandelaren als Providence bieden hun producten of diensten aan op deze beurzen. Medewerkers van deze bedrijven komen elkaar en agenten van opsporings- en inlichtingendiensten tegen op deze beurzen en conferenties.

De bekendste beurzen zijn de Milipol beurs die jaarlijks afwisselend in Parijs en Doha (Qatar) plaatsvindt, en de Security & Policing in het Verenigd Koninkrijk. Daarnaast vinden er over de gehele wereld regelmatig conferenties/ontmoetingsbeurzen van ISS World plaats. ISS World (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering) is een bijeenkomst waar producenten als Gamma Group en Hacking Team, tussenhandelaren als Providence en vertegenwoordigers van opsporings- en inlichtingendiensten presentaties houden en informeel handel drijven.

'*ISS World Europe is the world's largest gathering of European Law Enforcement, Intelligence and Homeland Security Analysts as well as Telecom Operators responsible for Lawful Interception, Hi-Tech Electronic Investigations and Network Intelligence Gathering*', schrijft ISS in haar brochures. ISS World wordt gehouden in Praag, Dubai, Kuala Lumpur, Johannesburg, Mexico City en Washington DC.

Om vast te stellen of de Nederlandse politie deelneemt aan deze beurzen en conferenties heeft Buro Jansen & Janssen gevraagd om meer informatie. De Nationale Politie wil in haar beantwoording van Wob

verzoeken nog wel toegeven dat men op drie beurzen aanwezig is geweest en schrijft: 'Aan de conferentie Milipol Qatar 2014 hebben twee politieambtenaren deelgenomen, aan die van ISS World Europe 2015 vier en aan die van Security & Policing 2015 ook vier.'

'In het geval van de conferentie Milipol Qatar 2014 is een verslag opgesteld en er zijn respectievelijk 1 en 3 verslagen over die van Security & Policing 2015 en ISS World Europe 2015 opgesteld,' schrijft de Nationale Politie verder. Deze verslagen worden echter niet openbaar gemaakt. Wat de Nederlandse politie op die beurzen te zoeken heeft, wat men precies heeft gedaan, welke bedrijven zijn bezocht, wat men heeft aangeschaft, de Nationale Politie wil hier geen informatie over verstrekken.

'De verslagen die zijn aangetroffen, zijn doorspekt met informatie die is opgestoken vanuit de betreffende conferentie in samenhang en/of in vergelijking met hetgeen door de politie aan technieken, tactieken en werkwijzen (reeds) wordt gehanteerd/in de toekomst kan worden gehanteerd. Hierdoor kan ik u deze verslagen niet verstrekken. De (namen van) bedrijven — voor zover deze nog bij mij bekend zijn— die zich hebben gepresenteerd maak ik tevens niet openbaar.', aldus de Nationale Politie in antwoord op het Wob verzoek.

Geen openbaarheid

Buro Jansen & Janssen heeft via Wob verzoeken niet alleen verzocht om informatie over de beurzen maar ook om informatie over de relaties met Gamma Group, Hacking Team, Providence en Kailax. De antwoorden van de Nationale Politie zijn surrealistisch.

De Nationale Politie antwoordt in verband met de relatie met Hacking Team dat er geen documenten zijn. Uit de Wikileaks documenten van 2015 over Hacking Team blijkt echter dat de top van de Digitale Recherche van de Nederlandse politie sinds 2013 contacten met het Italiaanse computerbedrijf onderhoudt. Tientallen politiefunctionarissen zijn geabonneerd op een mailinglijst of nieuwsbrief van Hacking Team. Nederlandse politiefunctionarissen hebben op beurzen presentatie bijgewoond en tonen serieuze interesse in de aanschaf van het digitale wapen RCS Galileo. Op 6 juli 2015 stond er zelfs een presentatie gepland.

Zoveel contact maar daarover zou niets zijn vastgelegd? Betekent dit dat

politiemannen maar wat op eigen houtje doen en enig beleid, toezicht en controle ontbreekt?

Er zijn aparte Wob verzoeken ingediend ten aanzien van Gamma Group en FinFisher. De Nationale Politie antwoordt dat er geen documenten zijn ten aanzien van de Gamma Group. Uit de in 2014 gepubliceerde Wikileaks documenten over Gamma Group blijkt echter dat de Nederlandse politie sinds september 2012 zestien licenties voor het gebruik van het digitale wapen FinFisher van Gamma Group heeft aangeschaft. In antwoord op het Wob verzoek over FinFisher ontkent noch bevestigt de politie dit. De afwijzing wordt ook niet gemotiveerd.

Alleen het Wob verzoek over Providence levert iets concreets op. In antwoord op het Wob verzoek onderkent de Nationale Politie dat het zaken heeft gedaan met Providence, en zegt dat er 39 facturen van Providence bestaan. Verdere informatie wordt niet openbaar gemaakt. Hiermee blijft onduidelijk welke diensten of producten, wanneer de Nederlandse politie precies bij Providence heeft aangeschaft, en bij welke vestiging van Providence.

Het Wob verzoek over Kailax wordt afgedaan met het antwoord dat 'ten aanzien van de door u bevraagde bedrijven uit onderzoek op met name het internet blijkt dat deze bedrijven zich veelal bezig houden met de ontwikkeling van producten (technische hulpmiddelen) die haar toepassing kunnen vinden op het internet en bij telecommunicatie in al haar verschijningsvormen.' De politie weigert zelfs in haar eigen bestanden te kijken. Over Kailax is echter zeer weinig te vinden op het internet en zelfs de eigen website van het bedrijf vermeldt enkel dat het bedrijf iets doet met digitale veiligheid: 'We provide solutions in the cyber security domain.'

De overheid wil niets kwijt over haar contacten met bedrijven en verschuilt zich achter of het belang van de opsporing in het geval van Providence, of geen enkele reden in het geval van FinFisher en Kailax. De Nederlandse overheid houdt hiermee de geheimzinnigheid en de ondoorzichtigheid van de digitale wapenhandel branche in stand.

Unlocker, Max, Kailax, Mhyli, Nir Levy

De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De Kailax *Unlocker* is

een USB stick waarmee op Windows computers kan worden ingebroken, zonder dat de eigenaar dit in de gaten heeft. Het gaat hierbij om Windows Vista 7/8/8.1 Server 2008/Server 2012 − 32/64 bit.

De herkomst van digitale wapens is vaak onduidelijk, wat de vraag oplevert of overheden en veiligheidsdiensten wel weten wat voor product ze kopen en met welk bedrijf ze in zee gaan. De bemoeienis van tussenhandelaren als Providence draagt verder bij aan nog meer ondoorzichtigheid.

Over de *Unlocker* en het producerende bedrijf Kailax is nauwelijks openbare informatie beschikbaar. De website www.kailax.com bevat alleen de adresgegevens van het bedrijf (een adres in Singapore), maar geen verdere informatie. Uit openbare bronnen kan alleen worden opgemaakt dat het in Berlijn gevestigde bedrijf 2beuropa als tussenhandelaar voor Kailax fungeert.

Pas met de openbaarmaking van de Wikileaks documenten over Hacking Team in 2015 is er meer inzicht gekomen over het bestaan van de Kailax *Unlocker* en de handel in deze tool. De *Unlocker* blijkt een gewild digitaal wapen. Volgens de producent, die zich in e-mails afwisselend Max en Nir Levy noemt, levert Kailax de *Unlocker* aan zeventig landen.

Of dit waar is, valt niet te controleren, het bedrijf publiceert geen enkele gegevens. Wat wel duidelijk wordt uit de Wikileaks documenten is dat het Italiaanse computerbedrijf Hacking Team interesse heeft om de *Unlocker* aan haar assortiment toe te voegen. Het belandt hiervoor bij het Britse bedrijf Providence, dat als tussenhandelaar de *Unlocker* aanbiedt.

Buro Jansen & Janssen deed onderzoek naar de herkomst van de *Unlocker* en de personen Max en Nir Levy via een analyse van domeinnamen. Deze leidt naar Israël. De Kailax *Unlocker* blijkt van Israëlische afkomst te zijn. Nir (Max) Levy heeft een verleden bij de Israëlische geheime dienst en werkt nu voor het bedrijf Mhyli.

Buro Jansen & Janssen heeft het sterke vermoeden dat de Nationale Politie via Providence de Kailax *Unlocker* aanschaft. Dit zouden de 39 facturen voor diensten of producten van Providence zijn.

Het is aannemelijk dat de Nationale Politie de Kailax *Unlocker* heeft aangeschaft. Uit de communicatie van Hacking Team en Max/Nir Levy

blijkt dat de Israëlische ex-inlichtingendienst medewerker de Unlocker verkoopt als een soort zwarte doos. Gebruikers weten niet hoe het werkt en met welke servers in Israël het communiceert. Dit is vergelijkbaar met de afluistercentrales van Nice Systems die de Nationale Politie ook uit Israël betrekt.

Problemen voor de rechtspleging

Het probleem van de zogenaamde zwarte doos speelt al langer. De politie is niet in het bezit van de broncode, de precieze werking van bepaalde producten die zij gebruikt. Bij de afluistercentrales van Nice Systems concludeerde de Minister van Veiligheid en Justitie in februari 2016 dat er meer duidelijkheid over het functioneren van de apparatuur moet komen. Bij de vele telefoontaps die de politie uitvoert, is de leverancier van de afluisterapparatuur nauw betrokken. Maar essentiële informatie over de taps, wordt door diezelfde leverancier niet gedeeld. *'Er is geen garantie dat de politie volledig zicht heeft op alle storingen in het tapsysteem'* (NOS, 12-02-16).

De zwarte doos van de Kailax *Unlocker* is dus geen nieuw fenomeen. Het onderzoek met betrekking tot de afluisterapparatuur van het Israëlische Nice Systems, ondertussen overgenomen door Elbit, en de ondoorzichtige en geheimzinnige markt van digitale wapens roept allerlei vragen op.

Heeft de politie inzicht in wat voor producten zij aanschaft en gebruikt? Heeft de Nationale Politie de kennis en expertise in huis om te doorgronden hoe de software werkt en wat de veiligheidsrisico's zijn voor het gebruik, maar ook voor de rechtspleging? Weet de Nederlandse politie met welke bedrijven zij in zee gaat, zijn deze gescreend op hun financiële integriteit en mensenrechten beleid? De Nationale politie zegt geen documenten te bezitten als het gaat om Gamma Group en Hacking Team. Met betrekking tot Providence zijn er 39 facturen, over FinFisher kan men niets zeggen en een verzoek over Kailax wordt ook niet beantwoord. De politie wenst geen nadere informatie te verstrekken.

backdoors en diefstal

De veiligheidsrisico´s bij de inzet van digitale wapens door de Nederlandse politie zijn aanzienlijk. Per slot van rekening gaat het om

het verzamelen van bewijs en een eerlijke rechtsgang voor verdachten. De politie test zelf de authenticiteit en integriteit van de aangeschafte digitale wapens. Naar aanleiding van vragen van de Kamerleden Oosenburg (PvdA) en Verhoeven (D66) antwoordt staatssecretaris Dijkhoff op 28 augustus 2015: 'De beschikbare technische hulpmiddelen voor het opnemen van vertrouwelijke communicatie worden voorafgaand aan de inzet gekeurd door de onafhankelijke keuringsdienst van de politie. Deze keuring is voornamelijk gericht op de authenticiteit en integriteit van het middel.'

De staatssecretaris stelt dat er een 'onafhankelijk keuringsdienst van de politie' is. Dit is echter dezelfde afdeling die interesse toont in de digitale wapens van bedrijven, de aanschaf doet en betrokken is bij de inzet, zeker als het gaat om de bediening van de wapens. Het Nederlands Forensisch Instituut en TNO worden niet ingezet voor de vaststelling van de authenticiteit en integriteit.

De Nederlandse politie begeeft zich op een markt die gekenmerkt wordt door geheimzinnigheid en ondoorzichtigheid. De politie heeft FinFisher aangeschaft van Gamma Group en waarschijnlijkheid Kailax. Dit doet zij al dan niet met behulp van tussenhandelaren. Tevens toonde de politie interesse in Galileo van Hacking Team. De bedrijven bieden geen inzicht in de ontwikkeling van hun wapens. De ontwikkeling van RCS Galileo lijkt nog het meest duidelijk door naar alle waarschijnlijkheid ontwikkelaars van Hacking Team zelf. Bij Gamma Group en Kailax is het gissen naar de ontwikkelaars achter de producten.

Naast een onduidelijk ontwikkeltraject van de digitale wapens is er het probleem van de *backdoor.* De Wikileaks documenten over Hacking Team maken duidelijk dat Hacking Team software een *backdoor* heeft. Via die *backdoor* kan het bedrijf het wapen op afstand uitzetten, zonder dat de klant hier weet van heeft of hierover is geïnformeerd. De *backdoor* geeft echter niet alleen Hacking Team toegang tot de geïnfecteerde smartphones, laptops, computers. In theorie kunnen anderen zich daardoor ook toegang verschaffen en gegevens manipuleren.

Regelmatig duiken er verhalen op dat producenten een *backdoor* in software hebben ingebouwd. *Backdoors*, geheime toegang tot software, wordt meestal ingebouwd omdat opsporingsdiensten zoals de Amerikaanse FBI dit eisen. Bij Hacking Team is onduidelijk waarom de *backdoor* is ingebouwd. Het heeft duidelijk niet te maken met het tegengaan van ongeoorloofd gebruik, want de digitale wapens van

Hacking Team zijn ingezet tegen oppositieleden, journalisten en activisten.

Over het bestaan van een backdoor in FinFisher van Gamma is niets bekend. Maar de in 2014 gepubliceerde Wikileaks documenten over Gamma Group duiden wel op andere veiligheidsproblemen. Enkele hulpvragen van de Nationale Politie gaan over '*non encrypted audio traffic between mobile target and server*' en '*non encrypted SMS traffic between mobile target and system*.' Dit kan betekenen dat een derde partij de gegevens kan onderscheppen.

Er is nog een ander probleem bij FinFisher, dat ook speelt bij de producten van Hacking Team. Kan het digitale wapen gestolen worden en gebruikt door derden? Martin J. Münch, die zichzelf de enige woordvoerder van Gamma Group noemt, reageert in 2012 op de beschuldiging van export naar Bahrein van het digitale wapen FinFisher. *'The company was investigating whether the product in the CitizenLab study was a demonstration copy of the product stolen from Gamma and used without permission' (Bloomberg* 27 juli 2012). Münch gaat zelfs nog een stap verder: *'It is unlikely that it was an installed system used by one of our clients but rather that a copy of an old FinSpy demo version was made during a presentation and that this copy was modified and then used elsewhere."*

***zero-days en* hacks**

Naast de *backdoors* is er het probleem van de *zero-days*. *Zero-days* (nul dagen) zijn veiligheidslekken in software, die nog niet bekend zijn bij de makers van die software en die nog niet zijn gedicht. Uit de Wikileaks documenten over Hacking Team wordt duidelijk dat dergelijke lekken door Hacking Team worden gebruikt om in te breken op smartphones, tablets, etc. Niet alleen Hacking Team maakt gebruik van zero-days, ook Gamma Group doet dat. De handel in *zero-days* is een zwarte markt waar veel geld in omgaat.

Op de zwarte markt bieden zowel bedrijven als individuen *zero-days* aan. De openbare gegevens over Hacking Team onthullen enkele facetten van die markt. Zo komen er drie bedrijven ter sprake in de stukken: Het Franse VUPEN security, Coseinc uit Singapore, het Amerikaanse Netragard and Vulnerabilities Brokerage International en een Rus met de naam 'Vitaliy Toropov'. De Italianen willen graag met hem afspreken,

maar hij houdt de boot af. Wie 'Vitaliy Toropov' precies is en of hij freelancer is of werkt voor een bedrijf of dienst is niet duidelijk.

Hacking Team heeft enkele Flash *zero-days* gekocht welke waarschijnlijk zijn gebruikt om in te breken op een smartphone, tablet of computer van burgers. Er is geen garantie dat Hacking Team de enige partij is die op de hoogte was van die veiligheidslekken in Flash en dat niemand anders dus bij de data van de verdachten heeft kunnen komen. 'Vitaliy Toropov' verkocht 'zijn' *zero-days* aan meerdere gegadigden. Hoe wijd verspreid de kennis van dit specifieke lek was, is vaak moeilijk te achterhalen omdat ook criminele organisaties en inlichtingendiensten deze *zero-days* aanschaffen.

Hacking Team heeft een digitaal wapen ontwikkeld waarmee de Nederlandse politie zou kunnen inbreken, maar kan nooit garanderen dat iemand anders ook al aan het inbreken is. De Nationale Politie heeft FinFisher aangeschaft, een digitaal wapen van Gamma Group waarvoor hetzelfde geldt. Wat betekent dit voor opsporing en voor het uitgangspunt van een eerlijk proces? Dat digitale wapens kwetsbaar zijn maken de digitale inbraken bij Gamma Group in 2014 en Hacking Team in 2015 duidelijk.

De technologiebedrijven hadden beide hun beveiliging niet op orde. Wat betekent dit voor de integriteit van hun digitale wapens? Uit de vorige vraag vloeit automatisch de vraag voort of het bewijs dat wordt verkregen met behulp van de inzet van digitale wapens wel rechtsgeldig is? Doordat feitelijke gegevens over het al dan niet gebruiken van deze 'technische hulpmiddelen', producenten en tussenhandelaren geheim blijft en openbare audit-rapporten over deze digitale wapens niet beschikbaar zijn, is controle op inzet en gebruik onmogelijk.

De korpsbeheerder van de Nationale Politie, het ministerie van Veiligheid en Justitie, voelt geen urgentie op dit terrein. De enige urgentie die bij ambtenaren van het ministerie leeft is het zo snel mogelijk beantwoorden van Kamervragen. In antwoord op Wob verzoeken over Hacking Team, Gamma Group, FinFisher en enkele andere bedrijven heeft het Ministerie een handvol e-mails openbaar gemaakt die slechts betrekking hebben op Kamervragen die in 2014 en 2015 zijn gesteld over het onderwerp.

Zo antwoordt een ambtenaar op 13 juli 2015: 'Nieuwe Kamervraag inzake het gebruik van software van het Hacking Team door de Nationale

Politie.' De volgende dagen is er overleg over de beantwoording. De vraag of de Nationale Politie over de broncode beschikt, wordt meteen al terzijde geschoven: 'Bij vraag 5 vraag ik mij af of je hier wel iets op moet zeggen, lijkt mij niet wenselijk om hier openbaar inzicht in te bieden', schrijft een ambtenaar op 14 juli 2015. De antwoorden zijn dan ook snel klaar: 'Ik heb wel al een voorzet voor beantwoording gedaan nav eerdere kamervragen, FinFisher.' De beantwoording van de Kamervragen levert dan ook niets op.

Veiligheidsrisico´s worden alleen maar groter

Het gebrek aan een serieuze benadering door het Ministerie van Veiligheid en Justitie is opmerkelijk, niet alleen in het licht van de discussie over digitale inbraken en de Amerikaanse verkiezingen. De ontwikkelingen op het gebied van digitale wapens gaan snel. Er komen steeds weer nieuwe bedrijven met nieuwe producten op de markt van digitale wapens. Dit bleek bijvoorbeeld in november 2016 toen Team Red Naga een onderzoek publiceerde over een nieuw digitaal wapen dat zich richt op Android Smartphones. Volgens *Motherboard* is de fabrikant van het wapen waarschijnlijk het Italiaanse Raxir. Raxir is niet het enige nieuwe bedrijf dat zich de laatste jaren roert op de markt van digitale wapens: Ook het Italiaanse RCS Lab met het product Mito3 en de Israëlische NSO Group dienen zich aan.

De kans dat digitale wapens op straat komen te liggen, wordt ook steeds groter. Recentelijk werd een medewerker van de Amerikaanse NSA (National Security Agency) aangehouden. Hij wordt verdacht van het lekken van spionagetools van de NSA. Een van de tools heet 'Extra Bacon', werd in de zomer van 2016 gepubliceerd door '*Shadowbrokers*'. De tool maakt het mogelijk om in te breken op firewalls, routers en switches van de bedrijven Cisco en Fortinet, en maakt hierbij gebruik van *zero-days*. In Nederland zou het om ruim duizend apparaten gaan, wereldwijd om tienduizenden die kwetsbaar zijn.

Het zal in de toekomst steeds makkelijker worden om digitale wapens aan te schaffen en deze zullen steeds geavanceerder worden. Een Duits voorbeeld laat echter zien dat complexe en ingewikkelde digitale inbraken met behulp van Quantuminsert van de NSA niet het enige gevaar zijn. In 2016 werd een Duitse hacker gearresteerd die wist in te breken op de computers van 150 Duitse jonge meiden. Hij bespiedde hen via hun webcam. Het lukte hem via het chatprogramma ICQ binnen

te dringen. Met behulp van een trojan, een programma waarmee je een computer infecteert en op afstand kan besturen, kon hij zo de webcam overnemen. De hack werd toevallig ontdekt door een man die lesgeeft over databeveiliging op middelbare scholen.

Financiële integriteit

De onduidelijkheid over het ontwikkelproces van digitale wapens, het bestaan van *backdoors* in de software, de suggestie dat gestolen digitale wapens zijn gebruikt, het gebruik en de geheimzinnige handel in *zero-days* en de digitale inbraken bij producenten van digitale wapens roepen vragen op over de veiligheid van de inzet van de 'technische hulpmiddelen.' Het zijn echter niet alleen de producten zelf die vragen over betrouwbaarheid en integriteit oproepen, ook bij de producenten en de tussenhandelaren zijn de nodige vraagtekens te zetten.

De Nationale Politie heeft zaken gedaan met de Gamma Group en Providence. Het heeft de FinFisher aangeschaft. Men zegt niet wat men bij Providence heeft aangeschaft, maar er zijn 36 facturen. Met Hacking Team is uitgebreid contact geweest en waarschijnlijk wordt de *Unlocker* van Kailax afgenomen via tussenhandelaar Providence.

Bij de financiële integriteit van zeker Gamma Group en Providence kunnen serieuze vraagtekens worden geplaatst. Beide bedrijven hebben een ondoorzichtige bedrijfsstructuur opgebouwd. Deze bestaat uit een wirwar van bedrijven en holdings, met steeds dezelfde directeuren die tegelijkertijd aandeelhouders zijn. Beide bedrijven hebben meerdere vestigingen in belastingparadijzen. De bedrijfsstructuur van Gamma en Providence zijn zeer geschikte constructies voor het wegsluizen van gelden en het ontduiken van belastingen.

Gamma Group International Limited is gevestigd op de Britse Maagdeneilanden buiten het zicht van financiële controleurs. Gamma Group heeft daarnaast vestigingen in andere belastingparadijzen: Gamma International Ltd. in Cyprus en vier bedrijven in Libanon (Gamma Group International SAL, Cyan Engineering Services SAL, Gamma Cyan SAL Offshore en Elaman - German Security Solutions SAL). Providence heeft een wat minder wijdvertakt netwerk, maar ook drie afdelingen in het belastingparadijs Panama waaronder Providence Global Corp. De twee andere bedrijven zijn Heva Intermediates Corp. en QP, S.A.

De Nationale Politie neemt digitale wapens af van bedrijven die gebruik maken van complexe bedrijfsstructuren, beperkte financiële gegevens publiceren en vestigingen hebben in belastingparadijzen. Dit lijkt geen issue te zijn voor de Nationale Politie. In antwoord op Wob verzoeken zegt de politie geen documenten te hebben over de financiële integriteit van deze bedrijven.

Freedom Online Coalition?

In het Nationaal Actieplan Bedrijfsleven en Mensenrechten van april 2014 schrijft het Ministerie van Buitenlandse Zaken dat 'Nederland de eerbiediging van mensenrechten door het bedrijfsleven bevordert.' Het actieplan stelt dat 'bedrijven een eigen maatschappelijke verantwoordelijkheid hebben om in het buitenland dezelfde mensenrechtennormen te hanteren als in Nederland.' Conform het Actieplan promoot de Nederlandse overheid dit beleid doordat zij 'transparantie en stakeholderdialoog' bevordert en dat zij 'het goede voorbeeld geeft, zoals via het duurzaam inkoopbeleid.'
Het gaat volgens het Actieplan om een beleid waarbij de overheid 'van de aan hen leverende bedrijven verlangt dat ze mensenrechten respecteren' (sinds 1 januari 2013).

Mooie woorden die hoopvol doen stemmen over de rol van ethiek bij de aanschaf van digitale wapens. Nog meer mooie woorden volgen in het antwoord op Kamervragen van 28 augustus 2015 door het Ministerie van Veiligheid en Justitie: *'Ook neemt Nederland wereldwijd een leidende rol in bij de beperking op uitvoer van ICT goederen en software naar regimes met een slechte staat van dienst op het gebied van mensenrechten via onder andere multilaterale fora als de Global Conference on Cyberspace 2015 en het statement over het gebruik en de export van surveillance technologie van de Freedom Online Coalition 4.'*

Nederland verlangt van bedrijven dat ze mensenrechten respecteren en bevordert de stakeholdersdialoog. Het is echter volstrekt onduidelijk hoe de Nationale Politie hier bij de aanschaf van digitale wapens invulling aan geeft. Nederland heeft FinFisher van Gamma gekocht in 2012. Op dat moment waren er al een aantal schandalen bekend. Vanaf 2013 onderhoudt de Nederlandse politie contact met Hacking Team en bezoekt presentaties het bedrijf, terwijl dan al bekend is dat Hacking Team aan

repressieve regimes haar digitale wapens verkoopt.

Naar aanleiding van het gebruik van digitale wapens tegen vijf activisten in de Verenigde Arabische Emiraten in 2012 vraagt *The Irish Times* commentaar over de kwestie aan Europarlementariër Marietje Schaake. '*With pressure group Privacy International urging nations around the continent to review export laws for 'offensive' software made by companies such as UK-based Gamma International and Italian company Hacking Team, Dutch MEP Marietje Schaake says the issue of the 'digital arms trade' needs to be acted upon 'urgently'*.' (09-05-13).

Na Egypte en Verenigde Arabische Emiraten volgen Marokko en Ethiopië, voordat de volle omvang van de export van digitale wapens naar repressieve regimes duidelijk wordt door de publicatie van gegevens over Gamma Group en Hacking Team door Wikileaks. In april 2014 vragen verschillende NGO's, waaronder Amnesty International en Human Rights Watch, aandacht voor de export van surveillance apparatuur of software.

De Nederlandse overheid doet niets mee. Op Wob verzoeken wordt afwijzend geantwoord. Er zijn geen documenten over Gamma Group en Hacking Team. Van Providence slechts 39 facturen en over FinFisher en Kailax wil men niets zeggen. Het zou de opsporing in gevaar brengen. De Nationale Politie maakt op geen enkele wijze aannemelijk dat het invulling geeft aan het Nationaal Actieplan Bedrijfsleven en Mensenrechten.

De Nederlandse politie en Hacking Team; Flirten met de tools van de dictator

Gamma Group en de politie; FinFisher trojan in de Nationale politie

Providence en de politie; Ketenaansprakelijkheid via een ex-agent

Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators

Gamma Group/Louthean Nelson; Wapenhandelaars pur sang

Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens

Kailax/Nir (Max) Levy; De magische hand van de Israëlische inlichtingendienst

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

De Nederlandse politie en Hacking Team; Flirten met de tools van de dictator (pdf)

Gamma Group en de politie: FinFisher trojan in de Nationale Politie (pdf)

Providence en de politie; Ketenaansprakelijkheid via een ex-agent (pdf)

Bedrijfsprofiel Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators (pdf)

Bedrijfsprofiel Gamma Group/Louthean Nelson; wapenhandelaars pur sang (pdf)

Bedrijfsprofiel Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens (pdf)

Bedrijfsprofiel Kailax/Nir (Max) Levy; De magische hand van de Israëlische inlichtingendienst (pdf)

Naar inhoudsopgave Observant #69

De Nederlandse politie en Hacking Team
Flirten met de tools van de dictator

Uit de in 2015 gepubliceerde Wikileaks documenten over Hacking Team blijkt dat de Nederlandse politie sinds 2012 contacten onderhoudt met het omstreden Italiaanse computerbedrijf Hacking Team. In antwoord op het WOB verzoek van Buro Jansen & Janssen antwoordt de Nationale Politie echter dat er geen documenten zijn die betrekking hebben op Hacking Team.

Het Italiaanse computerbedrijf Hacking Team verkoopt software aan politie- en veiligheidsdiensten, waarmee versleuteld digitaal dataverkeer kan worden ontcijferd en afgeluisterd. Het bekendste digitale wapen van Hacking Team is Remote Control System (RCS) - eerst onder de naam DaVinci later Galileo RCS. Hiermee kan worden ingebroken op telefoons en computers en toegang worden verkregen tot alle aanwezige programma's en accounts, zoals Skype of Facebook.

In 2015 werd Hacking Team zelf gehackt. De gepubliceerde Wikileaks documenten bevatten veel informatie over de contacten tussen de Nederlandse politie en Hacking Team. Het blijkt dat Nederlandse politiefunctionarissen sinds 2013 presentaties van Hacking Team hebben bijgewoond en verregaande interesse hadden in de aanschaf van de Galileo software.

Op grond van de Wet Openbaarheid van Bestuur (WOB) heeft Buro Jansen & Janssen bij de Nationale Politie documenten opgevraagd met betrekking tot contacten met (onder andere) Hacking Team. De politie antwoordt als volgt: 'Na onderzoek is gebleken dat met geen van de door u genoemde bedrijven de politie een contract heeft. Ook zijn bij de politie geen documenten aangetroffen betreffende de bedrijven Gamma Group en/of Gamma International en Hacking Team en/of vergelijkbare namen'.

Dat de politie geen contract heeft met Hacking Team, dat kan kloppen. Ook de Wikileaks documenten bevatten geen bewijs dat Nederland software van Hacking Team heeft aangeschaft. Dat de politie in het geheel geen documenten heeft betreffende Hacking Team, kan echter ten minste merkwaardig genoemd worden. Handelden de politiefunctionarissen die contact onderhielden met Hacking Team

dermate op eigen initiatief dat dit op geen enkele manier binnen de centrale politieorganisatie is vastgelegd?

Mailinglijst Hacking Team

Buro Jansen & Janssen heeft de politiefunctionarissen die op een of andere manier contact hadden met Hacking Team in kaart gebracht. En gereconstrueerd wanneer en op welke wijze verschillende functionarissen contact hadden met Hacking Team. Men zou verwachten dat hierover iets schriftelijk is vastgelegd.

In de Wikileaks documenten van Hacking Team komen diverse e-mail adressen en e-mails voor van Nederlandse politiefunctionarissen. Deze stonden allemaal of op een mailinglijst van het bedrijf, of hadden/hebben direct contact met een van de werknemers van de firma. Zo vraagt David Vincenzetti, baas van Hacking Team, op 15 januari 2015 aan Raymond van Bergem welk van de adressen hij moet verwijderen van de mailinglijst van het bedrijf.

Vincenzetti schijft dat er tien politie.nl adressen op de lijst staan namelijk: @rijnmond.politie.nl, @flevoland.politie.nl, @limburg-zuid.politie.nl, @klpd.politie.nl, @haaglanden.politie.nl, @rijnmond.politie.nl, @haaglanden.politie.nl, @klpd.politie.nl, @limburg-zuid.politie.nl, @ssc-noord.politie.nl. De documenten bevatten de namen van 22 politiefunctionarissen, mailadressen die verwijzen naar 'nl' of 'politie'.

Van de landelijke politie-eenheid stonden Henry Willering (Hoofd van de afdeling technologie en expertise ontwikkeling), Jan Noordam (Dienst Specialistische Recherche Toepassingen), Marco van Berkel (Hoofd product ontwikkeling), Felix Nijpels (Dienst Landelijke Operationele Samenwerking (DLOS) Afdeling Technologische Ontwikkeling & Expertise (ATOE)), Chris Oornick (Interceptie Specialist), Fred Wemeijer en Wilbert Paulissen (chef van de Nationale Recherche) op de mailinglijst.

Ook de naam van Joost van Slobbe (voorheen programmaleider Nationale Politie en nu Hoofd Opsporingsinformatie Inspectie Sociale Zaken en Werkgelegenheid) stond op de lijst toen hij in dienst was bij de politie, alsmede zijn toekomstige collega's digitale expertise bij de SIOD, thans Inspectie Sociale Zaken en Werkgelegenheid, Stefan Timmermans en Jelle Oorebeek.

Verdere bestudering van de WikiLeaks-documenten maakt duidelijk welke agenten zich nog meer hadden aangemeld voor de mailinglijst van Hacking Team. Van de Haagse eenheid komen Christophe Ruijs (IT-onderzoeker), Martin Beekink en Tim Mizee (Operationeel Specialist A, Contra Terrorisme en Radicalisering, Regionaal Informatie Knooppunt Den Haag) voor tussen de stukken. Van de Rotterdamse eenheid Frans Nab (Regionaal InformatieCentrum), Paul Spek en de al eerder genoemde Raymond van Bergem. De Amsterdamse eenheid was vertegenwoordigd door Manon den Dunnen (voorheen Team Digitale Expertise politie Amsterdam nu Nationale Politie).

Limburg is vertegenwoordigd door Jan Immeker en Hans Musters en Midden Nederland via Bert Aben (digitaal rechercheur). Van de eenheid Oost Nederland Jos van den Oetelaar (in de jaren '90 Regionale Criminele Inlichtingen Dienst (RCID) Noord- en Oost-Gelderland chef informatieverwerking, vervolgens Digitale Recherche van de Bovenregionale Recherche Zuid-Nederland, daarna Technische expert technische surveillance en ondersteuning Noord- en Oost-Gelderland Criminele Inlichtingen Eenheid en nu operationeel specialist A bij Digitale Opsporing Oost-Brabant) en Martijn Hekster (Eenheid Oost, Dienst Regionale Recherche, Digitale Expertise voorheen Politie Gelderland-Zuid, Divsie Centrale Operationele).

Noord Nederland (Friesland, Groningen en Drenthe) hebben Peter Silk (Shared Service Center Noord Nederland) op de lijst staan. Noord-Holland, Zeeland en West-Brabant zijn niet vertegenwoordigd maar wel de overzeese gebiedsdelen via Paul Wessels van de eenheid op de Nederlandse Antillen (Recherche SamenwerkingsTeam).

De mailinglijst waar de politiefunctionarissen op geabonneerd waren, voorziet in krantenartikelen uit bijvoorbeeld de Britse *Financial Times* en de Amerikaanse *Wall Street Journal*. Onderwerpen waren niet alleen spionage ('*Berlin Says U.S. May Be Spying on Merkel's Phone*') maar ook het geopolitieke machtsspel tussen verschillende grootmachten ('*Washington fears losing Greece to Moscow*') en de economische crisis ('*Greece asks eurozone for third bailout*').

De nieuwsservice lijkt op die van andere ondernemingen uit de private inlichtingenwereld zoals Stratfor en Global Info. Stratfor werd in 2011 gehackt door onder anderen Jeremy Hammond die daarvoor een celstraf van tien jaar uitzit. De documenten van Stratfor maken duidelijk dat

vooral actiegroepen en de oppositie in diverse landen in de gaten worden gehouden door dit soort bedrijven. Ditzelfde geldt voor Hacking Team dat zich niet alleen richt op het verspreiden van informatie, maar ook op het offensieve werk, zoals het inbreken in computers en telefoons van mensen.

Correspondentie HT met Nationale Politie

Het contact tussen Hacking Team en Nederlandse politiefunctionarissen betrof echter niet enkel aanmelding voor de mailinglijst of nieuwsbrief. Uit de Wikileaks documenten wordt duidelijk dat Nederlandse politiefunctionarissen serieuze interesse hadden in de aanschaf van digitale wapens van Hacking Team, met name de RCS Galileo.

Op 5 november 2014 beantwoordt Massimiliano Luppi van Hacking Team een e-mail van de Nederlandse politiefunctionaris Henry Willering, hoofd van de afdeling technologie en expertise ontwikkeling van de landelijke eenheid Nationale Politie. Willering bezocht samen met enkele collega's van 20 tot en met 22 oktober 2014 de Milipol Qatar. Op deze 'Homeland Security' beurs namen zij onder meer een kijkje bij de infokraam van Hacking Team en kregen hier een demonstratie voorgeschoteld.

Luppi stuurt Willering naar aanleiding van de show in Qatar een reclameboodschap via e-mail: '*Since you showed interest in our product, I take the occasion to send you some information related to the latest version of Remote Control System, codenamed Galileo. Galileo is designed to attack, infect and monitor target PCs and Smartphones, in a stealth way. It allows you to covertly collect data from the most common desktop operating systems*.'

Willering antwoordt op 5 november 2014: '*We of course do remember your demonstration and explanation of Galileo in Qatar very well!'*. Hij deelt zijn mail aan Luppi met Marco van Berkel, hoofd productontwikkeling bij de landelijke eenheid, en Jan Noordam van de Dienst Specialistische Recherche Toepassingen. De heren reageren enthousiast aan Hacking Team: '*We are discussing your 'product' and your offer to visit us with the people in our department responsible for the deployment of solutions like Galileo. We need a couple of days to do that and to respond to you. So I guess we will be in touch with you next week*.'

Luppi antwoordt Willering op 12 november 2014, en krijgt meteen antwoord: *'Ben afwezig tot vrijdag 14 november.'* De WikiLeaks documenten bevatten geen verdere mailwisselingen meer tussen Hacking Tea en Henry Willering.

Providence als tussenpersoon

In 2015 is er opnieuw contact tussen de politie en Hacking Team. Uit de Wikileaks documenten wordt duidelijk dat het bedrijf Providence hierbij als intermediair optreedt en een afspraak probeert te regelen tussen de Nationale Politie en Hacking Team.

Providence is een Brits security bedrijf dat trainingen aanbiedt en apparatuur verkoopt. Het is zelf geen producent van digitale wapens. Uit de Wikileaks documenten wordt duidelijk dat het bedrijf tevens als tussenhandelaar in digitale wapens actief is. Providence heeft ook een duidelijke Nederlandse connectie in de persoon van Peter Stolwerk, een voormalig politieman die sinds 2012 de Nederlandse vestiging van Providence (Providence BNLX) leidt. Stolwerk heeft al eerder geprobeerd om een samenwerking tussen Providence en Hacking Team tot stand te brengen in onder meer Australië en Ecuador.

Stolwerk probeert in 2015 een bijeenkomst te organiseren met Hacking Team en de Nationale Politie. Stolwerk heeft hiervoor zijn contacten binnen de politie- en inlichtingendienst aangeboord. Na afloop van de ISS World Europe beurs in Praag neemt Stolwerk op 8 juni 2015 contact op met Philippe Vinci van Hacking Team om een afspraak met de Nationale Politie te plannen.

Vinci wil zo snel mogelijk de data voor de afspraak weten, omdat hij een specialist moet meenemen voor de presentatie. Veel medewerkers van Hacking Team houden zich bezig met de acquisitie, slechts enkelen kunnen de software daadwerkelijk bedienen. '*Regarding the trip to the Netherlands and the presentation/demo to National Police (ex KLPD) and Netherland Intelligence, let me know which are the best dates/alternatives so that we can book the week and the presence of a Field Application Engineer.*', antwoordt Vinci nog op dezelfde dag.

Stolwerk beweert vervolgens dat de politie hem enkele uren later heeft geantwoord: '*The police just came back to us that they would like to have a demonstration in the first two weeks of july (that is when their*

main technician will be present)'. Vinci laat Stolwerk weten dat de voorkeur van Hacking Team uitgaat naar de tweede week van juli 2015. Vinci schrijft tevens dat hij de namen van de twee Nederlandse agenten zal opzoeken die eerder interesse voor de software van de Italianen toonden: '*I will also send you tomorrow the names of the 2 persons from KLPD that visited our booth in UK Security & Policy (Farnborough), so that you could check if they are in the same organization*.'

Stolwerk, Van de Oetelaar, Wemeijer

Het betreft hier de agenten Jos van den Oetelaar, in 2015 werkzaam bij de eenheid Oost Nederland en het jaar daarop operationeel specialist A bij Digitale Opsporing Oost-Brabant, en Fred Wemeijer van de landelijke eenheid. Van den Oetelaar en Wemeijer bezochten begin maart 2015 de Security & Policing beurs van het Britse Ministerie van Binnenlandse Zaken in Farnborough en kregen een presentatie over RCS Galileo.

Vinci schrijft op 16 juni 2015 aan Stolwerk: '*Jos visited our booth during the Security & Policing UK conference in Farnborough. He stayed quite long with us, almost 50 minutes, during which we did a very complete demonstration of Galileo. So he was able to see different infections (PC and mobiles) and have a look at the evidence that were collected*.'

Jos van den Oetelaar kent Hacking Team al geruime tijd. Uit de Wikileaks documenten blijkt dat hij al in 2013 tijdens een bezoek aan een beurs interesse had getoond in de software van Hacking Team. Van den Oetelaar en Hacking Team correspondeerden in deze periode al met elkaar. Zo tutoyeerde Van den Oetelaar op 2 september 2013 David Vincenzetti, de baas van Hacking Team: '*Hi David and a very good afternoon from The Netherlands. I temporary have another position within the National Police organisation. (…) When I'am back in my orginal job and office I let you know! Jos van den Oetelaar, Specialist Technical Surveillance and Support*.' Een maand later benaderde Emad Shehata van Hacking Team van den Oetelaar: '*I found that you visited our booth at Security & Policing 2013 and on behalf of Hacking Team I would like to thank you again*.'

Stolwerk kent Van de Oetelaar klaarblijkelijk ook. Stolwerk meldt op 15 juni 2015 dat Van den Oetelaar niet op de bijeenkomst van de Nederlandse politie met Hacking Team aanwezig zal zijn: '*Yes I know those Police Officers really well. Especially Jos van de Oetelaar. He is*

actually promoted as a chief of the National Technical Support unit. I don't believe they will be present at this meeting as you will meet the cyber and digital forensics department', aldus Stolwerk.

Stolwerk beweert in zijn e-mail van 15 juni 2015 een bijeenkomst te hebben georganiseerd met de landelijke politie-eenheid op 6 juli 2015: '*meeting confirmed on the 6th (after lunchtime) for the presentation. They arranged a secure facility with the necessary requirements*.' Volgens Stolwerk doen de agenten nogal geheimzinnig over de locatie: '*They are a bit secretive about it*.'

Geen openbaarheid

Uit de Wikileaks documenten wordt niet duidelijk of de op 6 juli 2015 geplande presentatie daadwerkelijk heeft plaatsgevonden. Hacking Team werd in deze periode zelf gehackt, waarna interne bedrijfsgegevens via Wikileaks op straat kwamen te liggen.

De Kamerleden Oosenburg (PvdA) en Verhoeven (D66) stellen in 2015 Kamervragen naar aanleiding van de hack van Hacking Team, onder meer over de presentatie: "Klopt het dat het bedrijf Hacking Team een productpresentatie zou houden voor de NP over hun producten? Is deze presentatie doorgegaan, na de ingrijpende inbraak bij het bedrijf?". Het Ministerie van Veiligheid en Justitie gaat in haar beantwoording echter niet in op deze vraag.

In antwoord op het WOB verzoek van Buro Jansen & Janssen geeft de Nationale Politie geen enkele informatie over de contacten met Hacking Team, ook niet over de presentatie van 6 juli 2015, de inhoud van deze presentatie, en welke personen hier aanwezig zouden zijn. Evenmin maakt de politie duidelijk of er sindsdien verdere contacten met Hacking Team hebben plaats gevonden en er wellicht een nieuwe presentatie is gepland.

Het gebrek aan openbaarheid roept vraagtekens op. Handelen de politiefunctionarissen die contact onderhielden met Hacking Team dermate op eigen initiatief dat dit op geen enkele manier binnen de centrale politieorganisatie is vastgelegd ?

En hoe zit het met het ethische aspect van zaken doen met Hacking Team? Onder de klanten van Hacking Team bevinden zich veel

repressieve staten die het niet zo nauw nemen met de naleving van de mensenrechten, en die de digitale wapens van Hacking Team onder meer inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten.

Dit is al enige jaren bekend. Zo werd in 2012 bekend dat de Marokkaanse geheime dienst digitale wapens van Hacking Team inzette tegen journalisten van *Mamfakinch*, en dat activisten in de Verenigde Arabische Emiraten slachtoffer van werden van overheidsspionage door middel van Hacking Team software. In 2014 publiceerde CitizenLab een onderzoek naar de digitale infiltratie van Ethiopische journalisten door het Ethiopische regime met behulp van software van Hacking Team. In april 2014 vroegen verschillende NGO's waaronder Amnesty International en Human Rights Watch, verenigd in de coalitie CAUSE(Coalition Against Unlawful Surveillance Exports) aandacht voor de export van surveillance apparatuur of software. Hacking Team werd in de documenten van CAUSE expliciet genoemd.

De Nationale Politie onderhoudt sinds 2013 uitvoerig contacten met Hacking Team. Uit niets blijkt dat de mensenrechtenreputatie een rol heeft gespeeld bij de overweging om met het bedrijf zaken te doen. Volgens het Nationaal Actieplan Beleidsleven en Mensenrechten verlangt de Nederlandse overheid van de aan hen leverende bedrijven dat ze de mensenrechten respecteren en dat de overheid de stakeholdersdialoog bevordert. Uit niets blijkt of en hoe de Nationale Politie hier in haar contacten met Hacking Team invulling aan heeft gegeven.

Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence

Boeven vangen met dubieuze software van dubieuze bedrijven

Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators

Bedrijfsprofiel Hacking Team/David Vincenzetti; Italiaanse staatsnerds in dienst van dictators (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Gehele Observant #69 Politie Mercenaries

Wikileaks Hacking Team documenten

CitizenLab onderzoek naar Hacking Team

CitizenLab diverse artikelen over Hacking Team

Enkele e-mails uit Hacking Team met de politie

Kamervragen Hacking Team

Adressen e-maillijst van Hacking Team

Naar inhoudsopgave Observant #69

Gamma Group en de politie
FinFisher trojan in de Nationale politie

Uit in 2014 gepubliceerde Wikileaks documenten over Gamma Group wordt duidelijk dat de Nederlandse politie sinds september 2012 zestien licenties heeft aangeschaft voor het digitale wapen FinSpy en FinMobile. De Nationale Politie maakt in antwoord op het WOB verzoek van Buro Jansen & Janssen echter geen verdere informatie openbaar.

Gamma Group is een van oorsprong Brits bedrijf met takken en dochterondernemingen over de gehele wereld. Sinds 2008 biedt Gamma Group het digitale wapen FinFisher aan. Met de software FinFisher of FinSpy kan via een USB of vanaf afstand via wifi of een netwerk inbreken op computers, laptops, tablets en smartphones.

Bevestigen noch ontkennen

Op grond van de Wet Openbaarheid van Bestuur (WOB) heeft Buro Jansen & Janssen bij de Nationale Politie documenten opgevraagd met betrekking tot contacten met Gamma Group. In antwoord op het WOB verzoek beweert de Nationale Politie over geen informatie te beschikken over de Gamma Group: 'Na onderzoek is gebleken dat met geen van de door u genoemde bedrijven de politie een contract heeft. Ook zijn bij de politie geen documenten aangetroffen betreffende de bedrijven Gamma Group en/of Gamma International en/of vergelijkbare namen.'

De Nationale Politie zegt dus geen contract te hebben met Gamma Group of een bedrijf met een vergelijkbare naam. Dit kan zijn. Gamma Group bestaat uit een netwerk van verschillende bedrijven. De FinFisher software wordt te koop aangeboden door een aantal Duitse bedrijven die tot het netwerk behoren namelijk Elaman GmbH de Duitse dochterondernemingen van Gamma Group die sinds 2013 de naam FinFisher in de naamvoering hanteren (FinFisher GmbH, FinFisher Labs, FinFisher Holding).

Buro Jansen & Janssen heeft ook een WOB verzoek ingediend naar de contacten met FinFisher. De Nationale Politie antwoordt hierop dat het niet kan bevestigen noch ontkennen dat zij informatie bezit over

FinFisher: 'Indien zoals in het onderhavige geval, uw verzoek om informatie ziet op het openbaar maken c.q. verstrekken van informatie over met name genoemde bedrijven waarmee de politie overeenkomsten c.a. zou kunnen hebben, vormt dit een onaanvaardbaar risico voor die overeenkomsten c.a..'

De politie hanteert hier een moeilijk te doorgronden formulering ('bedrijven waarmee de politie overeenkomsten zou kunnen hebben'). Dit roept vraagtekens op. Indien de politie geen overeenkomst heeft met een FinFisher bedrijf, dan zou men dat kunnen zeggen. Zo antwoordt de politie in antwoord op het WOB verzoek inzake de relaties met Hacking Team ook dat er geen contract is met Hacking Team. In de beantwoording van het WOB verzoek ontkent noch bevestigt de Nationale Politie dus dat er een contract is met FinFisher.

Het valt ook moeilijk te ontkennen. Uit de in 2014 gepubliceerde Wikileaks documenten over Gamma Group wordt immers duidelijk dat de politie de FinFisher heeft aangeschaft.

Jochem van der Wal

De Wikileaks documenten over Gamma Group bevatten een overzicht van de klantgegevens van het bedrijf, en een overzicht van hulpvragen die door gebruikers van Gamma software aan het bedrijf zijn gesteld. Uit de documenten blijkt dat het Korps Landelijke Politiediensten (KLPD), tegenwoordig de landelijke eenheid van de Nationale Politie, sinds 2012 een klant is van Gamma Group. De Wikileaks documenten bevatten een overzicht van zestien licenties die het KLPD heeft aangeschaft.

Het KLPD wordt aangemerkt als klant '20FEC907'. Dit is een code, die is gekoppeld aan een naam: het KLPD uit Nederland. Nader onderzoek toont aan dat een Nederlandse politiefunctionaris de contactpersoon is met het bedrijf: Jochem van der Wal. Deze persoon werd aan zijn PGP-Key identiteit herkend door Twitter persoonlijkheid '@DrWhax', Jurre van Bergen.

Wie is Jochem van der Wal? Van der Wal wordt in 2007 en 2008 regelmatig in de media aangehaald. Emerce.nl noemt van der Wal in relatie tot een congres op 14 juni 2007 over de politie en SPSS (Data collectie, voorspellende analyses en netwerken met collegae − De politie als getuige). Hij zal als KLPD politiefunctionaris op het congres spreken

over 'digitaal forensische analyse onder handbereik van het tactische onderzoekstraject door toepassing van de Digitale Wasstraat.' *Predictive policing*, een net woord voor *profiling*, is toch iets anders dan digitaal inbreken, maar Van der Wal werkt dan al voor het KLPD.

Techzine wijdt in september 2008 een artikel aan SPSS (Statistical Package for the Social Science). SPSS is software die in de sociale wetenschappen voor statistieken wordt gebruikt, en wordt ontwikkeld door het gelijknamige bedrijf. In het artikel (SPSS helpt politie bij voorspellen van misdaad) wordt Van der Wal aangehaald als ICT-specialist bij het KLPD.

Ook in het buitenland wordt het werk van Van der Wal opgemerkt. *Hendon Publishing* publiceert in december 2008 een artikel '*Police departments fighting crime with predictive analytics software.'*, waarin van der Wal wordt omschreven als '*technical engineer at KLPD*.' In een interview met *Hendon Publishing* zegt Van der Wal: '*After implementing text-mining software and deploying it to a crime case, we found an essential connection within just five minutes—which we couldn't have found in the past three months of investigations*.' Hij heeft het over de digitale wasstraat die is ontwikkeld door het KLPD. Hij noemt het 'Open Computer Forensic Architecture (OCFA), the '*digital washing machine', which creates an automated index out of the unstructured contents of a PC's hard drive, enabling investigators to perform keyword searches for evidence.*'

Copyright op OFCA zou liggen bij het KLPD met als contactadres ocfa@dnpa.nl. Dnpa.nl werd 4 april 2005 geregistreerd door het KLPD. DNPA staat voor Dutch National Police Agency en de afkorting wordt bijvoorbeeld gebruikt op github.com en andere websites. Van der Wal hanteert het al in 2002 voor een artikel in de bundel '*Dealing with the data flood, mining data, tekst and multimedia*.' Hij is dan al werkzaam voor het KLPD: '*J. van der Wal, Msc. Duch National Police, Criminal Investigation Department. Research and Development, Driebergen – Rijsenburg, the Netherlands.*'

Van der Wal is anno 2016 nog steeds werkzaam bij de landelijke eenheid (voorheen KLPD). Dit blijkt uit de *acknowledgement*-pagina van Tim Cocx, die in 2016 zijn Phd afrondde aan de Universiteit van Leiden. Cocx bedankt enkele medewerkers van de landelijke eenheid van de Nationale politie voor hun steun aan zijn onderzoek, waaronder Jochem van der Wal.

Daarnaast worden ook Ton Holslag (Dienst Specialistische Recherche Toepassingen), Wil van Tilburg (Coördinator informatieverzoeken), Leen Prins (adviseur expertise bij de Dienst Internationale Politie Informatie (IPOL) van het KLPD) en Henry Willering genoemd. Deze laatste komt ook naar voren in de in 2015 openbaar gemaakte Wikileaks documenten over Hacking Team. Willering is hoofd van de afdeling technologie en expertise ontwikkeling (Research and Development) van de nationale eenheid en de baas van Jochem van der Wal.

Inzet van FinSpy en FinSpy Mobile

Uit de Wikileaks documenten blijkt dat de Nederlandse politie, gedurende de vier jaar dat het met Gamma Group heeft samengewerkt, zestien licenties voor het gebruik van FinSpy / Fin Mobile heeft afgenomen. Sommige licenties eindigen na 2014 (het jaar waarin Gamma Group is gehackt). In totaal zou het gaan om 58 doelen, waarmee naar alle waarschijnlijkheid wordt gedoeld op computers, smartphones en andere digitale hulpmiddelen (en niet op individuen).

De Nationale Politie geeft, in antwoord op het WOB verzoek van Buro Jansen & Janssen, geen enkele informatie over de inzet van FinFisher. Er zijn echter aanwijzingen die wijzen op het gebruik van FinFisher door de Nederlandse politie.

Computerworld meldt op 8 augustus 2014 (naar aanleiding van de publicatie van de Wikileaks documenten over Gamma Group) dat het al eerder duidelijk was dat de politie digitale wapens inzette: *'Dat de Nederlandse politie wel dergelijke software gebruikt, werd duidelijk in het begin van dit jaar, bij de geslaagde operatie om een zedenverdachte op te pakken. Op diens PC in een vakantiebungalow werd spionagesoftware geplaatst. Welke software is verder nooit bekend gemaakt en ook nu doen politie en justitie geen mededelingen over welke type software zij gebruiken voor opsporingsdoeleinden.'*
Het is overigens niet duidelijk of deze operatie is geslaagd, de rechtszaak tegen de verdachte loopt nog.

Volgens de politie werden bij deze zaak van begin december 2013 tot en met half januari 2014 keyloggers ingezet. Het ging om zogenaamde doelen (digitale hulpmiddelen) die werden besmet, waarvan er één mislukte. Er zouden twee computers als doelwit zijn uitgekozen.

Dit kan overeenkomen met een van de hulpvragen die door de Nederlandse politie aan Gamma Group/FinFisher zijn gesteld en die gaan over het feit dat het digitale wapen FinSpy door het anti-virus programma AVG werd ontdekt. Een hulpvraag meldt: '*Some functionality of the agent/system do not work when the AVG AV tool is active. For example the keylogger module.*' In een andere hulpvraag wordt gewag gemaakt van dezelfde foutmelding: '*AVG anti virus tool detects generated infection on agent.*'

De Wikileaks documenten bevatten in totaal negen hulpvragen van de Nederlandse politie aan Gamma Group. Enkele hulpvragen gaan over '*non encrypted audio traffic between mobile target and server*' en '*non encrypted SMS traffic between mobile target and system*.' Dit kan betekenen dat een derde partij de gegevens kan onderscheppen.

Een andere hulpvraag gaat over een '*Android bug easy to reverse engineer and easy to find in target.*' Dit kan betekenen dat het doel waartegen de politie het digitale wapen inzet, door het slachtoffer zelf of door anderen gemakkelijk kan worden opgespoord.

Uit de Wikileaks documenten wordt niet duidelijk of de geconstateerde gebreken aan de software zijn verholpen. Evenmin is duidelijk of de politie naar aanleiding van de ondervonden problemen heeft besloten om het verkregen bewijsmateriaal voor de inbraken niet te gebruiken. Ook in de beantwoording van het WOB verzoek verstrekt de Nationale Politie hier geen informatie over.

Andere vraagtekens

Er kunnen ook andere vraagtekens gezet worden bij de aanschaf van FinFisher en bij de handel met Gamma Group.

Nederland bevindt zich als FinFisher gebruiker in een dubieus gezelschap. Gamma Group heeft het digitale wapen ook verkocht aan een reeks repressieve regimes die het hebben ingezet tegen onder meer oppositieleden, journalisten en mensenrechtenactivisten. Met de publicatie van de Wikileaks documenten in 2014 en de gehackte gegevens van Gamma Group zijn de details over de klantenkring van Gamma Group in de volle openbaarheid gekomen. Maar ook daarvoor was er al het nodige bekend. In 2011 ontdekten activisten tijdens de

Arabische Lente dat dictator Moebarak voor meer dan drie ton aan FinFisher spyware had aangeschaft. In 2012 volgden onthullingen over de inzet van FinFisher in Bahrein.

Ook bij de financiële integriteit van het bedrijf kunnen vraagtekens geplaatst worden. De wijze waarop de Gamma Group is georganiseerd, maakt het tot een perfecte constructie om gelden weg te sluizen naar belastingparadijzen, al dan niet via andere bedrijven. Verschillende bedrijven van de Gamma Group zijn nooit veel geld waard geweest. Gamma Group, zoals het bedrijf zich presenteert op beurzen, is gevestigd in het belastingparadijs Britse Maagdeneilanden, op naam van Gamma Group International Ltd. Daarnaast heeft Gamma Group vestigingen in Libanon (Gamma Group International Sal), Cyprus en Singapore, landen die bekend staan als belastingparadijzen.

Politie nog geheimzinniger dan AIVD

De Nationale Politie heeft de beschikking over de FinFisher, maar wenst geen verder informatie te geven. Geheimzinnigheid is troef. Een grondige bestudering van de beantwoording van het WOB verzoek leert dat de Nationale Politie ten aanzien van FinFisher nog geheimzinniger doet dan het normaliter doet bij de beantwoording van WOB verzoeken.

De beantwoording is nog ondoorgrondelijker dan de gebruikelijke beantwoording van inlichtingendiensten in het kader van de WIV (Wet op de Inlichtingen- en Veiligheidsdiensten). Bij inzageverzoeken in het kader van de WIV wordt vaak gesteld dat 'met betrekking tot aangelegenheden die voor de taakuitvoering van de AIVD nog wel actueel zijn, uitdrukkelijk geen mededeling worden gedaan, ook niet ten aanzien van de vraag of dergelijke gegevens wel of niet aanwezig zijn.'

De Nationale Politie antwoordt ten aanzien van FinFisher: 'Indien zoals in het onderhavige geval, uw verzoek om informatie ziet op het openbaar maken c.q. verstrekken van informatie over met name genoemde bedrijven waarmee de politie overeenkomsten c.a. zou kunnen hebben, vormt dit een onaanvaardbaar risico voor die overeenkomsten c.a..'

Het is opmerkelijk dat hier gesproken wordt over onaanvaardbaar risico voor de overeenkomst. In 2014 weigerde het Ministerie van Veiligheid en Justitie namelijk nog om informatie te verstrekken vanwege de risico’s ten aanzien van de inzetbaarheid van het middel. Op 8 augustus 2014

stelde woordvoerster Sentina van der Meer van het ministerie in *Computerworld*: *'Het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken een onaanvaardbaar risico vormt voor de inzetbaarheid van die middelen. Mede om die reden hebben de verwervingstrajecten van deze middelen onder geheimhoudingsverklaring plaatsgevonden.'*

Plaatsvervangend Politiechef/Hoofd Operatie Landelijke Eenheid Theo van der Plas struikelt in de beantwoording van het WOB verzoek dan ook bijna over zijn woorden: 'Onder meer dit gegeven c.q. deze omstandigheid verhindert dat wordt meegedeeld dat er geen gegevens bij een bestuursorgaan berusten die op uw verzoek om informatie zien en eveneens moet worden geheimgehouden dat er wel gegevens bij een bestuursorgaan berusten. Daarom kan ik geen mededeling doen of de gevraagde informatie in documenten is vastgelegd, dan wel al dan niet bij een bestuursorgaan berusten.'

In gewoon Nederland: de politie kan geen mededeling doen of dergelijke gegevens wel of niet aanwezig zijn. In de beantwoording van het WOB verzoek ontbreekt zelfs een motivering: 'Een nadere motivering van dit oordeel is uit de aard van de aangelegenheid dan wel de aard en/of inhoud van de gevraagde informatie niet te geven, zonder zicht te bieden op de al dan niet aanwezigheid van de door u gevraagde informatie.'

De Nationale Politie is hiermee nog ondoorgrondelijker dan de AIVD normaliter is in reactie op verzoeken op grond van de WIV. Hoewel inlichtingendiensten in het kader van de geheimhouding vaak ook gebruik maken van onnavolgbare redeneringen, verwijzen inlichtingendiensten meestal naar wetsartikelen die in ieder geval de wettelijke basis voor de weigering verduidelijken. Bij de AIVD gaat het dan om niet verstrekking in verband met 'het actueel kennisniveau van de AIVD (WIV artikel 53, lid 1); bronnen van de AIVD en/of zijn rechtsvoorgangers (WIV artikel 55, lid 1 onder b, in samenhang met artikel 15, aanhef en onder b); werkwijze van de AIVD en/of zijn rechtsvoorgangers (WIV artikel 55, lid 1 onder b).'

De Nationale Politie bedient zich van een vergelijkbaar ondoorgrondelijk jargon als Louthean Nelson en zijn bedrijf Gamma Group. Bij het bedrijf zelf is nauwelijks te doorgronden wie de ontwikkelaars van FinFisher en wie de partners en/of tussenhandelaren van Gamma Group zijn. De Nationale politie is onderdeel geworden van het spiegelpaleis van Louthean Nelson.

Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence

Boeven vangen met dubieuze software van dubieuze bedrijven

Gamma Group/Louthean Nelson; Wapenhandelaars pur sang

Bedrijfsprofiel Gamma Group/Louthean Nelson; wapenhandelaars pur sang (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Gehele Observant #69 Politie Mercenaries

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

Naar inhoudsopgave Observant #69

Providence en de Nationale Politie
Ketenaansprakelijkheid via een ex-agent

In antwoord op het WOB verzoek van Buro Jansen en Janssen onderkent de Nationale Politie dat het zaken heeft gedaan met het Britse bedrijf Providence. Er zijn 39 facturen, maar de politie wil verder niet duidelijk maken welke producten of diensten het heeft afgenomen.

Providence is een Brits security bedrijf dat trainingen en apparatuur aanbiedt. Providence produceert – voor zover bekend – zelf geen digitale wapens. De in 2015 gepubliceerde Wikileaks documenten over Hacking Team maken echter duidelijk dat Providence als tussenhandelaar in digitale wapens fungeert.

In antwoord op het WOB verzoek van Buro Jansen en Janssen onderkent de Nationale Politie dat zij zaken heeft gedaan met Providence: 'Voor de bedrijven Providence (...) zijn wel documenten aangetroffen.' (...) 'De producten en/of diensten en/of middelen van Providence worden op individuele basis afgenomen. Dit betekent dat zij worden afgenomen op het moment dat de desbetreffende afdeling een bepaald middel nodig heeft voor de politie- en/of opsporingswerkzaamheden'.

De Nationale Politie onderkent dus er dat documenten over Providence zijn aangetroffen. Daar blijft het bij: verdere informatie wordt er niet gegeven. De door de politie openbaar gemaakte documenten leveren nauwelijks informatie op. Volgens de politie zijn er 39 facturen, maar hiervan wordt alleen de naam 'factuur Providence' openbaar gemaakt. De openbaar gemaakte facturen bevatten geen verdere informatie, zelfs geen datum, logo of adressering. Er wordt zelfs geen zwart gemaakte kopie van de factuur openbaar gemaakt.

De vraag blijft: wat heeft de Nationale Politie van Providence gekocht?

Alles wijst er echter op dat de Nationale Politie, met bemiddeling van de voormalige Nederlandse politieman Peter Stolwerk, naar alle waarschijnlijkheid de *Unlocker* van het Israëlische bedrijf Kailax heeft aangeschaft. Dit blijkt uit een analyse van de in 2015 gepubliceerde Wikileaks documenten over Hacking Team, een analyse van het aanbod van Providence en een digitale zoektocht naar de domeinnamen die door

de producent van de *Unlocker* worden gebruikt.

Peter Stolwerk

Het is aannemelijk dat Peter Stolwerk een belangrijke rol heeft gespeeld in het tot stand brengen van een handelsrelatie tussen de Nationale Politie en Providence. Stolwerk is een voormalig politieman die sinds 2012 managing director is van Providence BNLX, de Providence vestiging in Haarlem.

Uit de in 2015 gepubliceerde Wikileaks documenten over Hacking Team wordt duidelijk dat Stolwerk de nodige contacten heeft binnen de Nederlandse politie. Zo organiseerde Stolwerk in 2015 een bijeenkomst tussen het Italiaanse computerbedrijf Hacking Team en de Nederlandse politie, waar de Italianen een presentatie over hun software zouden geven. (De bijeenkomst stond gepland op 6 juli 2015, maar het is niet duidelijk of deze doorgang heeft gevonden).

Uit de email correspondentie tussen Stolwerk en Hacking Team wordt duidelijk dat hij bekend is met diverse mensen van de digitale recherche in Nederland. Op 15 juni 2015 schrijft Stolwerk aan Hacking Team: '*Yes I know those Police Officers really well. Especially Jos van de Oetelaar. He is actually promoted as a chief of the National Technical Support unit. I don't believe they will be present at this meeting as you will meet the cyber and digital forensics department*.'

Het is niet bekend of de contacten van Stolwerk binnen de Nederlandse politie doorslaggevend zijn geweest voor de totstandkoming van de handelsrelatie tussen de Nationale Politie en Providence, maar het is wel aannemelijk. De beantwoording van het WOB verzoek geeft hierover geen nader inzicht.

Het aanbod van Providence

De Nationale Politie onderkent dat er 39 facturen Providence bestaan, maar ze maakt niet duidelijk wat het heeft aangeschaft bij Providence. Het is opmerkelijk dat de politie zaken heeft gedaan met Providence, want het reguliere aanbod van Providence lijkt op het eerste gezicht niet aan te sluiten bij de behoeften van de Nederlands politie.

Providence biedt volgens haar website trainingen en apparatuur aan op het gebied van veiligheid en anti-terrorisme. Het gaat hierbij om trainingen in bijvoorbeeld observatie en het installeren van afluisterapparatuur, een cursus over verschillende tracking methoden, hoe apparatuur te verhullen is, trainingen in inbreken en een black catalogus met waarschijnlijk militaire trainingen. Tot de aangeboden apparatuur behoren een special toolkit voor het installeren van afluisterapparatuur voor zowel audio- als video-opnames en los gespecialiseerd inbrekersgereedschap. Ook complete inbrekerskits behoren tot het assortiment, alsmede het verbergen van camera's en microfoons in nepstenen, boomstammen, dakpannen en andere manieren om apparatuur te verhullen.

Het ligt niet voor de hand dat de Nederlandse politie trainingen, in bijvoorbeeld observatie of het gebruik van afluisterapparatuur, van Providence heeft afgenomen. De politie kan hiervoor gebruik maken van diverse Nederlandse trainers en trainingscentra.

Het is ook weinig aannemelijk dat de politie iets heeft gekocht uit het reguliere aanbod van apparatuur dat door Providence wordt aangeboden. Vergelijkbare producten worden al jaren door reguliere leveranciers zoals Cellebrite, Nice Systems en andere bedrijven aangeboden, en door de Nederlandse politie bij deze leveranciers afgenomen.

Providence is een jonge speler op de markt van trainingen en digitale wapens. Medewerkers van Hacking Team zijn niet overtuigd van de kwaliteiten van Providence en merken begin 2015 op dat de brochures van Providence niet erg oud zijn en geen up-to-date contact gegevens bevatten. '*Still have to read all documents carefully, but all of them have been written on January 2015 (versions 1.0), so it seems they're recently organizing contents. P.S. All their e-mail addresses on the last pages are wrong*'.

De Nationale Politie verklaart in antwoord op het WOB verzoek dat het belang van opsporing geschaad zou worden door meer informatie over Providence openbaar te maken. Deze redenering is moeilijk toepasbaar op het reguliere Providence aanbod aan trainingen en apparatuur, omdat deze niet zozeer voor opsporingsdoeleinden zijn bedoeld. Het argument over het schaden van het belang van de opsporing is wel van toepassing op digitale wapens.

Ook anderszins vormt de formulering van het antwoord op het WOB

verzoek een aanwijzing dat de politie een digitaal wapen van Providence heeft gekocht: 'De producten en/of diensten en/of middelen van Providence worden op individuele basis afgenomen. Dit betekent dat zij worden afgenomen op het moment dat de desbetreffende afdeling een bepaald middel nodig heeft voor de politie- en/of opsporingswerkzaamheden'. Dit lijkt op geen enkele manier van toepassing op de trainingen en apparatuur uit het Providence aanbod.

Veel wijst er dan ook op dat de Nationale Politie via Providence een digitaal wapen heeft aangeschaft. Alles wijst er dan op dat de politie de Kailax *Unlocker* heeft aangeschaft.

Kailax *Unlocker*

Providence profileert zich niet in de openbaarheid als tussenhandelaar voor de Kailax *Unlocker*. Maar uit de Wikileaks documenten over Hacking Team wordt duidelijk dat Peter Stolwerk namens Providence als tussenhandelaar voor de Kailax *Unlocker* opereert.

Met de Kailax *Unlocker* kan een inbreker zich toegang tot een Windows computer verschaffen, zonder in te loggen en zonder dat de eigenaar dit in de gaten heeft. Het gaat hierbij om Windows Vista/7/8/8.1 Server 2008/Server 2012- 32/64 bit. De *Unlocker* van Kailax kan worden gebruikt in samenhang met een keylogger of digitaal wapen als Galileo RCS of FinFisher. Met de *Unlocker* kan een computer worden ontgrendeld waarna ongezien spionagesoftware wordt geïnstalleerd. Vervolgens kan op afstand de verdachte worden geobserveerd.

Er is weinig openbare informatie bekend over de *Unlocker* en het producerende bedrijf. Volgens de producent wordt de Kailax *Unlocker* aan zeventig landen geleverd. Of dit waar is, valt niet te controleren. Maar het feit dat Hacking Team het in 2015 aan haar assortiment wil toevoegen duidt erop dat het inderdaad een zeer gewild digitaal wapen is.

Zwarte doos

Het is aannemelijk dat de Nationale Politie via Providence de Kailax *Unlocker* heeft aangeschaft. Het is sterk de vraag of de politie zich hierbij bewust is van de achtergronden van de tool en het producerende bedrijf.

Providence is tussenhandelaar en geen producent. Het is de vraag of de politie dit weet. Uit de e-mail correspondentie tussen Stolwerk en Hacking Team blijkt dat hij wel de *Unlocker* aanbiedt, maar niets bekend maakt over de herkomst.

Wanneer de politie wel op de hoogte is van de bedrijfsnaam Kailax, is het sterk de vraag of men inzicht heeft in de achtergrond van het bedrijf. De website www.kailax.com bevat alleen de adresgegevens van het bedrijf (een adres in Singapore), maar geen verdere informatie.

Kailax is echter een Israëlisch bedrijf. Uit de Wikileaks documenten wordt duidelijk dat Max / Nir Levy het runt. Via openbare bronnen en op de Kailax website is verder geen informatie over hem aanwezig. Uit een digitale zoektocht naar domeinnamen blijkt dat Max/Nir Levy 25 jaar voor de Israëlische inlichtingendienst heeft gewerkt.

Wanneer de Nederlandse politie de Kailax *Unlocker* heeft aangeschaft, heeft het een zwarte doos in huis gehaald. Met de Kailax *Unlocker* kunnen computers ontgrendeld worden waarbij gebruik wordt gemaakt van een internet verbinding. Max / Nir Levy geeft in de correspondentie met Hacking Team aan dat hij ze een zwarte doos aanbiedt waarbij de techniek en het IP adres van de server van de *Unlocker* worden verhuld. *'Option 1 is feasible only if you are prepared to supply to customers as a sub distributer black box technology which you do not own, have no deal understanding of the IP or maintain.'*

Als de Nederlandse politie de Kailax *Unlocker* gebruikt zou Nederland dus een tweede Israëlische zwarte doos in huis hebben gehaald. Die nog ondoorzichtiger is dan de afluistercentrales van Nice Systems die Nederland eerder heeft aangekocht. En waarvan de minister van Veiligheid en Justitie in februari 2016 heeft aangegeven dat er meer duidelijkheid over het functioneren van de apparatuur moet komen. 'Bij de vele telefoontaps die de politie uitvoert, is de leverancier van de afluisterapparatuur nauw betrokken. Maar essentiële informatie over de taps, wordt door diezelfde leverancier niet gedeeld. ‘Er is geen garantie dat de politie volledig zicht heeft op alle storingen in het tapsysteem’ (NOS, 12 februari 2016).'

Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence

Boeven vangen met dubieuze software van dubieuze bedrijven

Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens

Kailax/Nir (Max) Levy; De magische hand van de Israëlische inlichtingendienst

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Bedrijfsprofiel Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens (pdf)

Bedrijfsprofiel Kailax/Nir (Max) Levy; De magische hand van de Israëlische inlichtingendienst (pdf)

Providence Group power point presentatie

Providence bedrijfsschema

Enkele emails Hacking Team providence 2010 - juni 2015

Enkele emails Hacking Team providence juni 2015 deel twee

Enkele emails Hacking Team providence juli 2015

Invitation to Workshops Exhibition and BBQ van Providence

Map and Directions van Providence

Registration form signed Hacking Team voor Providence event

Naar inhoudsopgave Observant #69

Hacking Team/David Vincenzetti
Italiaanse staatsnerds in dienst van dictators

Het in 2003 opgerichte Italiaanse computerbedrijf Hacking Team heeft zich in dertien jaar tijd ontwikkeld van een handelaar in beveiligingssoftware waarmee bedrijven zich kunnen weren tegen digitale inbraak, tot aan een specialist in offensieve wapens om documenten op internet aangesloten apparatuur in te zien en af te luisteren.

In 2006 presenteerde Hacking Team de eerste versie van haar digitale wapen Remote Control System (RCS) onder de naam DaVinci uit. Later verandert de naam in Galileo RCS. Hiermee kan worden ingebroken op telefoons en computers en toegang worden verkregen tot alle aanwezige programma's en accounts, zoals Skype of Facebook.

De digitale wapens van Hacking Team zijn gewild. Het bedrijf heeft een bedenkelijke reputatie. Onder meer vanwege het leveren van offensieve software aan autoritaire regeringen die ze hebben ingezet tegen oppositieleden, journalisten en mensenrechtenactivisten. De volle omvang werd duidelijk met de hack van Hacking Team in juli 2015 waarmee 400 GB aan interne data van het bedrijf (waaronder klantgegevens en emailcorrespondentie) in de openbaarheid kwamen.

Terug in de tijd

De Italianen David Vincenzetti en Valeriano Bedeschi richten in 2003 Hacking Team op. Beiden zijn nog altijd werkzaam bij het bedrijf: Bedeschi op de achtergrond, Vincenzetti altijd op de voorgrond.

David Vincenzetti is technisch onderlegd. Hij werkt van 1989 tot 1992 voor Hewlett Packard Italia als training course instructor. Vervolgens is hij tot 1996 werkzaam bij de Universiteit van Milaan als medewerker op de afdeling '*Dipartimento di Scienze dell'Informazione*'. Als '*Assunto ex. Art. 26*' is hij verantwoordelijk voor '*network & security laboratori siLAB*'.

Vincenzetti houdt zich in het begin van de jaren '90 vooral bezig met de beveiliging van computersystemen en de inzet van defensieve digitale wapens op het internet. In mei 1995 geeft hij bijvoorbeeld samen met

Stefano Taino, collega op de universiteit, twee lezingen tijdens een Italiaanse Unix bijeenkomst. Unix is een open source besturingsprogramma waar een gemeenschap gezamenlijk aan werkt om die te ontwikkelen. De lezingen gaan over Unix system & Network security en internet Firewall.

Een maand later spreken Vincenzetti, Taino en Fabio Bolognesi (eveneens werkzaam op de Universiteit van Milaan) op een bijeenkomst over computerbeveiliging in Salt Lake City in de Verenigde Staten. De drie Italianen presenteren zich hier als het 'Computer Emergency Resource Team Italy (CERT-IT)' van de informatie technologie faculteit van de Universiteit van Milaan. Ter introductie van hun presentatie schrijven zij: '*Eavesdropping is becoming rampant on the Internet. We, as CERT_IT, have recorded a great number of sniffing attacks in the Italian community. In fact, sniffing is the most popular hacker's attack technique all over the Internet (juni 1995)*.'

In hun presentatie stellen zij dat er vooral door overheden veel wordt afgeluisterd op het internet. Zij omschrijven dit als een soort sniffen, het rondneuzen in computersystemen. In hun presentatie claimen zij een beveiligd systeem hebben ontwikkeld om dat sniffen te verhinderen: '*This paper presents a secure telnet implementation which has been designed by the Italian CERT, to make eavesdropping ineffective to remote terminal sessions. It is not to be considered as a definitive solution but rather as a 'bandaid' solution, to deal with one of the most serious security threats of the moment.*'

Tijdens zijn werkzaamheden voor de Universiteit van Milaan is Vincenzetti tevens betrokken bij twee bedrijven. Van 1992 tot 1995 is hij voor de helft eigenaar van het bedrijf ISAC Snc (Information Security And Cryptography) en heeft hij in dit bedrijf ook een management functie. Ook neemt Vincenzetti van 1995 tot 1997 voor 33 procent deel aan CryptoNet Spa. Beide bedrijven, maar vooral CryptoNet, houden zich bezig met defensieve middelen op het internet. CryptoNet levert oplossingen voor antimalware, anti-DDos en anti-defacement, antimalvertising en security awareness. Vincenzetti's voormalige collega op de universiteit Stefano Taino is momenteel nog steeds werkzaam voor CryptoNet als directeur en informaticus.

Interesse voor offensieve strategieën

Vincenzetti houdt zich in de jaren 90 hoofdzakelijk bezig met defensieve

software, maar hij is in het begin van de jaren 90 al wel geïnteresseerd in offensieve software. Kennis die hij later te gelde zal maken voor Hacking Team.

De website *Ars Technica* publiceert op 8 juli 2015 enkele oude bijdragen van Vincenzetti op internetfora. In november 1991 schreef hij bijvoorbeeld over het stelen van wachtwoorden als methode om computersystemen over te nemen: '(…) *written a program that spies pseudo terminals when they are first used by rlogin or telnet or similar programs. I can steal the root password on most unixes in hours, or even minutes. The bug lies on the fact that the idle unallocated ptys are by default mode 666, and so readable and writeable by everyone. The login phase is virtually simulated, the user cannot get aware of what is happening, unless it effectively enters the password, and at that time it is too late. The bug is simple and evident: it's a just a matter of programming skill*.'

In 1992 schreef Vincenzetti op een Usenet forum: '*I have written ATP (Anti Tampering Program), a program that system administrators and `paranoia-users' will find useful. It is a program to make file tampering and nasty-hacking ineffective. ATP snapshots the critical files and you can examine them later, to discover if SOMETHING has changed. There are many options and the program is quite flexible. I cannot explain it here. Just get a copy at ftp site ghost.dsi.unimi.it, under the pub/crypt directory.*' Hij stelde computer beveiligingsprogramma's beschikbaar via de servers van de universiteit. Het is ook de tijd dat hij PGP gaat gebruiken, versleutelde email berichten.

Stefano Zanero, voormalig klasgenoot en momenteel professor op de Universiteit van Milaan, zegt over Vincenzetti: '*He was one [of the] geeks that were beginning to understand how the Internet worked (Foreign Policy 26 april 2016).*' Volgens Zanero dacht Vincenzetti tijdens zijn studietijd al na over de ontwikkeling van digitale wapens: '*The security industry was dominated by companies focused on defending businesses and governments against hackers. But, he wondered, what would happen if hackers were instead unleashed as a mode of security?*'

Keerpunt in Vincenzetti's carrière

Het jaar 1997 vormt een keerpunt in de carrière van Vincenzetti. Hij verlaat de Universiteit van Milaan en stapt in het bedrijf Intesis SpA In minder dan drie jaar tijd werkt het bedrijf zich op tot een bedrijf

gespecialiseerd in oplossingen voor digitale infrastructuur, netwerken en computerbeveiliging. Intesis SpA wordt in 2000 verkocht aan Finmatica Spa, een Italiaanse software onderneming van de succesvolle zakenman Pierluigi Cruel. Vincenzetti bezat 14 procent van Intesis SpA en maakt voor de eerste keer in zijn loopbaan een flinke winst. Hij zal het geld investeren in de oprichting van Hacking Team.

Vincenzetti gaat de commerciële markt op, net als veel van zijn vroegere universitaire collega's van de Universiteit van Milaan. Zo wordt Fabio Bolognesi, met wie Vincenzetti en Taino samenwerkte op de Universiteit van Milaan, Network Security Manager bij het Italiaanse I.Net, een Italiaanse provider. I.Net wordt in 2001 overgenomen door BT, het voormalige British Telecom.

Een andere medestudent en ontwikkelaar van software van de Universiteit van Milaan is Massimo Cotrozzi. Hij bezocht samen met Vincenzetti in oktober 1993 het vierde Unix security Symposium om een voordracht te geven over een door hen ontwikkeld programma, het ATP - Anti-Tampering Program. Ook Cotrozzi maakt na de universiteit carrière in de commerciële sector en werkt twee jaar als adjunct-directeur bij Ernst & Young (EY) in Londen en drie jaar bij KCS Group (Knightsbridge Company Services). KCS Group wordt geleid door een voormalig medewerker van MI6 en is een private inlichtingendienst die ook aan risico management doet. Te vergelijken met Stratfor, Global Info, The Inkerman Group en andere private inlichtingendiensten. Op dit moment is Cotrozzi Director Cyber Security - Cyber Engineering bij Deloitte UK.

Cotrozzi kent de wereld van de private inlichtingendienst en onderhoudt contact met Vincenzetti. In 2012, als Massimo Cotrozzi bij KCS Group werkzaam is, regelt hij een ontmoeting tussen zijn oude vriend Vincenzetti en de baas van KCS. Cotrozzi en Vincenzetti delen sinds 2012 geregeld informatie uit over potentiële klanten.

Zo mailt Cotrozzi op 3 juni 2015, hij werkt dan voor EY in London, dat het hoofd van het Amerikaanse National Cyber Security Program van de FBI, Peter Trahon, en de commandant van Special Investigations van de Amerikaanse luchtmacht, Kevin J. Jacobsen, in Rome zijn. Het gaat om 'classified' informatie die door de Italianen wordt gedeeld: '*I due individui saranno a roma dal 22 al 25 :)*.' De Amerikanen reageren niet.

De beginjaren van Hacking Team

In 2003 richt Vincenzetti, samen met Valeriano Bedeschi, Hacking Team (HT) op. Vincenzetti wordt voor twee derde eigenaar van Hacking Team en Bedeschi voor een derde.

Bedeschi en Vincenzetti kennen elkaar al heel lang. Bedeschi werkte in het verleden (net als Vincenzetti) voor CryptoNet, ISAC en (als technisch directeur) voor Intesis SpA Bedeschi leidt bij Hacking Team de afdelingen voor defensieve software en digitale wapens. In 2004 treedt een andere oude bekende van CryptoNet in dienst bij Hacking Team. Marco Bettini, voormalig collega op de universiteit van Milaan, wordt sales manager van het jonge IT bedrijf.

In de beginjaren van Hacking Team vormen digitale wapens zeker niet het belangrijkste product van het bedrijf. Volgens Alberto Pelliccione, die van 2007 tot 2014 in dienst was bij het bedrijf, was Hacking Team in 2007 een klein bedrijf, waar slechts vier mensen actief werkten aan het produceren van digitale wapens: *"At the time (2007), the company was a small brand that dealt with consulting for other companies, such as large banks who wanted to protect themselves. The year before, the company had begun to work on some offensive hacking solutions, such as the application which is then known as DaVinci, the first version of RCS*'', aldus Pelliccione in een interview met Motherboard (2 november 2015).

Volgens Pelliccione had het bedrijf in 2007 een beperkte ontwikkelafdeling met weinig financiële middelen. In *Ars Technica* van 20 juli 2015 zegt hij: ,,*[When I joined], they were only doing [penetration testing], they were only a defensive unit—the offensive unit had only existed for three months, it was brand new*.''

Remote Control System RCS

De komst van Marco Valleri naar Hacking Team in 2004 speelt een belangrijke rol in de ontwikkeling van digitale wapens door het bedrijf. Valleri werkte eerder voor Intesis SpA (het bedrijf waar Vincenzetti in 2001 vertrok). Valleri vertrekt ook begin deze eeuw bij Intesis en ontwikkelt daarna samen met Alberto Ornaghi (ALoR) de software Ettercap (Ettercap-Graphical).

Ettercap is een van de eerste '*man in the middle*' (MITM) software

applicaties. '*Man in the middle*' is een programma waarmee ingebroken kan worden op datastromen om zo digitale communicatie af te kunnen luisteren, wachtwoorden te stelen en iemands computer van afstand te manipuleren. Inbreken op dataverbindingen behelst een geheel andere techniek dan inbreken in een programma op een computer. In korte tijd werd Ettercap zeer veel gebruikt, zowel door mensen die de veiligheid van hun netwerken wilden controleren als door hackers om op systemen in te breken. Ook de Italiaanse politie bleek al snel geïnteresseerd in Ettercap. *The Verge* schrijft in een artikel van 13 september 2013 dat de Milanese politie rond 2001 al geïnteresseerd bleek in Ettercap en Valleri benaderde met de vraag of zij Ettercap konden aanpassen voor het afluisteren van Skype gesprekken op Windows computers.

In 2006 brengt Hacking Team de eerste versie van het digitale wapen Remote Controle System (RCS) onder de naam DaVinci uit. DaVinci en de opvolger Galileo RCS worden de pronkstukken van Hacking Team en het bedrijf gaat zich uiteindelijk volledig richten op digitale wapens. In 2007 wordt Alberto Pelliccione aangetrokken om de toepasbaarheid van het digitale wapen verder te ontwikkelen. Hij ontwikkelde in het verleden Ettercap en deed onderzoek naar robots en kunstmatige intelligentie. In 2008 trekt Hacking Team ook de andere ontwikkelaar van Ettercap, Alberto Ornaghi ('ALoR'), aan. Zo breidt het bedrijf langzamerhand zijn ontwikkelafdeling uit.

Vincenzetti beschrijft de allereerste versie van RCS in *Foreign Policy* als volgt: '*Think of it as a criminal dossier: A tab marked 'Targets' calls up a profile photo, which a spy must snap surreptitiously using the camera inside the subject's hacked device. Beside the picture, a menu of technologies (laptop, phone, tablet, etc.) offers an agent the ability to scroll through the person's data, including email, Facebook, Skype, online aliases, contacts, favorite websites, and geographical location. Over time, the software enables government spooks to build a deep, sprawling portfolio of intelligence.*'

Na het inbreken, neemt het programma de telefoon of de computer van de verdachte over en heeft zo toegang tot alle programma's en accounts, bijvoorbeeld Skype en Facebook, van de betreffende persoon. Dat inbreken is in het begin nog niet zo eenvoudig. '*Spies must get it into technology quickly and secretly — say, in the seconds a phone passes through security at a border checkpoint. Moreover, each device a target uses must be infected separately. Yet there are myriad options for delivery: a USB, DVD, public Wi-Fi network, or even a QR code disguised*

as something enticing (such as an ad for an escort service)', aldus Vincenzetti.

Eigenlijk is er in de loop der jaren niet veel veranderd aan de tool, al is deze natuurlijk wel verbeterd. Het inbreken, blijft echter een probleem. Dit moet ofwel fysiek met een USB stick of DVD, maar kan ook online via wifi of een netwerk.

De Italiaanse overheid als klant

Hacking Team groeit na de oprichting in 2003 gestaag. Het jaar 2007 is financieel een belangrijk jaar. Het bedrijf haalt twee miljoen euro aan investeringen binnen van twee grote Italiaanse fondsen: 'Next' van Finlombarda SGR S.p.a. en 'Innogest Capital' van Innogest SGR SpA. Het bedrijf groeit gestaag verder. In 2008 werken er 24 mensen voor het bedrijf en dit stijgt naar 26 in 2009, 30 in 2010, en 33 in 2011.

Tot de eerste afnemers van de digitale wapens van Hacking Team in 2004 behoort de Milanese Polizia postale e delle comunicazioni, de Italiaanse digitale recherche die regionaal is georganiseerd. Vincenzetti verklaart in een artikel in Foreign Policy van 26 april 2016 dat de Milanese recherche al in 2003 een eerste prototype van RCS gebruikte. De Spaanse geheime dienst (Centro Nacional de Inteligencia) wordt in 2006 overtuigd door Hacking Team dat met de RCS de Spanjaarden terroristen kunnen vangen.

Het duurt tot 2009 voordat Hacking Team andere Italiaanse klanten werft. In 2009 kan Vincenzetti de Italiaanse Presidenza del Consiglio dei Ministri (PCM, president van de ministerraad) bijschrijven. De PCM is een coördinatie orgaan voor de Italiaanse inlichtingendiensten.

Daarnaast verkoopt Hacking Team haar digitale wapens aan SIO SpA, een privaat bedrijf dat afluistercentrales voor telefoon- en internetverkeer beheert voor bijvoorbeeld het Italiaanse Openbaar Ministerie. Het is een private onderneming die grotendeels afhankelijk is van de Italiaanse staat, maar ook de commerciële markt op mag. SIO SpA heeft samen met Area SpA en Research Control Systems de Italiaanse markt voor afluistercentrales in handen. Er is niet veel openbare informatie bekend over de commerciële klanten van deze drie bedrijven.

In de jaren die volgden sleept Vincenzetti nog een aantal andere belangrijke Italiaanse spelers de opsporings- en inlichtingenwereld binnen. In 2010 bestelt de ROS (Raggruppamiento Operativo Speciale), een speciale eenheid van de Italiaanse politie, voor een half miljoen digitale wapens bij Hacking Team. In 2012 bestelt SIO S.p.a. opnieuw en werd door Vincenzetti bestempeld als een 'vaste' klant. De Italiaanse FIOD, de Guardia di Finanza, sluit zich in 2013 zich bij de andere diensten aan en betaalt Hacking Team vier ton.

Als laatste bekende Italiaanse klant koopt de concurrent van SIO SpA, Area SpA, in 2014 voor ruim vier ton digitale wapens in. Sinds eind 2016 loopt er een justitieel onderzoek in Italië naar illegale export naar Syrië door Area SpA. Het was echter al eerder bekend dat Area SpA samen werkte met het regime van Bashar al-Assad in Syrië.

De Italiaanse overheid als financier

Vincenzetti heeft zich binnen enkele jaren tijd genesteld in de top van de Italiaanse opsporings- en inlichtingenwereld. Met zijn contacten binnen zit hij aan tafel met de hoogste bazen van de inlichtingendiensten.

De verwevenheid tussen Hacking Team en de Italiaanse staat neemt verder toe door de financiële injectie in 2007 door het regionale overheidsfonds 'Next' van Finlombarda SGR SpA en het private fonds 'Innogest Capital' van Innogest SGR SpA dat ook geld van de Italiaanse overheid ontvangt. Beide fondsen hebben een kwart van Hacking Team in handen. 'Next' is een fonds van de regionale overheid waar de regio's Milaan en Lombardije onder vallen. 'Innogest Capital' is een privaat investeringsfonds, maar uitsluitend geïnteresseerd in het Italiaanse bedrijfsleven, vooral startups in de zorg en de digitale sector. Tien procent van het 'Innogest Capital' is in handen van een voormalig Amerikaanse ambassadeur in Italië: Ronald Spogli. Hij is tevens een van de oprichters van het fonds.

De Amerikaanse betrokkenheid bij dit investeringsfonds, en bij de ontwikkeling van Hacking Team, lijkt zelfs verder te gaan. In een interview met het Italiaanse *Panorama* noemt Fernando Napolitano, partner van Innogest SGR, nog een andere Amerikaan die betrokken is bij het fonds: "*Mike McCollough, a Booz&Co. partner and former head of the National Security Agency*".

Waarschijnlijk betreft het hier Michael McCullough die al twee decennia werkt voor Booz Allen & Hamilton, het bedrijf waarvoor ook Edward Snowden werkzaam was. Booz Allen & Hamilton is een bedrijf dat onder andere voor de NSA werkt.

Volgens Napolitano heeft McCullough een rol gespeeld bij het verkrijgen van toegang tot de Amerikaanse markt voor Hacking Team. ,,*It was McCollough himself who met with the young members of the Milan-based Hacking Team, specialists in eavesdropping software used by police forces, the purpose of the meeting being to help them break into the tough US market*", noteert *Panorama* op 8 november 2011. In 2011 en 2012 mocht Hacking Team de FBI (Federal Bureau of Investigation), Department of Defense (Amerikaanse Ministerie van Defensie) en Drug Enforcement Administration (DEA) bijschrijven als klant voor ruim een miljoen euro.

Klanten stromen binnen

Hacking Team groeit vanaf 2007. Het digitale wapen RCS blijkt een zeer gewild product dat kennelijk in behoeften voldoet.

De klantenkring van Hacking Team breidt zich snel uit. Onder de klanten bevinden zich dus Italiaanse overheidsdiensten, veel diensten uit Europese landen (Albanië, Cyprus, Hongarije, Luxemburg, Polen, Spanje, Tsjechië, Zwitserland), maar ook veel repressieve staten die het niet zo nauw nemen met de naleving van de mensenrechten, en die de digitale wapens van Hacking Team onder meer inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten.

De omvang van, en de details over, de klantenkring worden pas in juli 2015 in volle omvang duidelijk met de publicatie van de Wikileaks documenten.

Tot de eerste klanten van Hacking Team behoren in 2008 de inlichtingendiensten Infocomm Development Authority of Singapore en Information Office uit Hongarije en in 2009 de Malaysian Anti Corruption Commission. In 2009 wordt ook een andere Hongaarse inlichtingendienst, de Special Service of National Security (SSNS), klant van Hacking Team. Hongarije wordt onder de autoritaire leiding van Viktor Orbán een vaste klant en zal uiteindelijk miljoenen besteden aan digitale wapens. Vanaf 2010 is ook Mexico een grote klant.

Nog voor de Wikileaks in 2015 vinden er echter verschillende onthullingen plaats over controversiële klanten van Hacking Team. Onder meer door onderzoek van het Canadese Citizen Lab (Universiteit van Toronto).

In 2012 gebruikt de Marokkaanse geheime dienst de CSDN digitale wapens van Hacking Team tegen journalisten van *Mamfakinch*. Dit komt in oktober 2012 in de openbaarheid in een onderzoek van Citizen Lab over de inzet van DaVinci van Hacking Team tegen het Marokkaanse journalistencollectief.

Op 10 oktober 2012 publiceert Citizen Lab een rapport over een activist uit de Verenigde Arabische Emiraten: dhr. Mansoor. Hij werd het slachtoffer van overheidsspionage en vervolgens gearresteerd vanwege zijn politieke activiteiten. Mansoor en vier van zijn mede-activisten (de UAE5) werden in 2011 tot drie jaar gevangenisstraf veroordeeld. De president verleende Mansoor gratie, maar zijn veroordeling blijft staan, en zijn toekomst lijkt onzeker. Onderzoek van Citizen Lab toont aan dat Hacking Team achter de spionage van de activisten zat: "Some of the *backdoor* programming code in the *Mamfakinch* infection alluded to a user named "Guido" and the software has been identified as a variant of a commercial spyware marketed by Hacking Team, a Milan company, the report says."

Citizen Lab komt op 12 februari 2014 met een nieuw onderzoek, naar de digitale infiltratie van Ethiopische journalisten door het Ethiopische regime met behulp van software van Hacking Team. Citizen Lab schrijft: "In this report, we identified three instances where Ethiopian journalist group ESAT was targeted with spyware in the space of two hours by a single attacker. In each case the spyware appeared to be RCS (Remote Control System), programmed and sold exclusively to governments by Milan-based Hacking Team."

Begin april 2014 vragen verschillende ngo's waaronder Amnesty International en Human Rights Watch, verenigd in de coalitie CAUSE (Coalition Against Unlawful Surveillance Exports) aandacht voor de export van surveillance apparatuur of software. Hacking Team wordt in de documenten van CAUSE expliciet genoemd.

Ondanks de negatieve publiciteit over de controversiële leveranties van Hacking Team, blijft het aantal klanten van het bedrijf stijgen. Het lijkt

welhaast of de negatieve publiciteit als gratis reclame voor het digitale wapen RCS DaVinci en haar opvolger Galileo RCS werkt. In 2009 en 2010 had Hacking Team nog maar vijf klanten per jaar in 2011 stijgt dit tot acht en in 2012 tot vijftien, en in 2013 ook (getallen zijn een benadering van de gegevens van Hacking Team).

Tussenhandel

De lijst van leveranties van digitale wapens door Hacking Team aan repressieve regimes is lang, en wordt in de loop der jaren steeds langer. Soms vindt de handel plaats met behulp van een tussenhandelaar.

Nice Systems (Nice Intelligence Solutions of Nice Ltd), een Israëlisch bedrijf dat handelt in tapcentrales, is een belangrijke tussenhandelaar voor Hacking Team. Privacy International maakt in een onderzoek van november 2014 al duidelijk dat Israëlische bedrijven in Centraal-Azië surveillance software leveren aan repressieve regimes. De tussenhandel van digitale wapens past daar mooi bij: Hacking Team en Nice Systems hebben elkaar iets te bieden. Het onderzoek maakt duidelijk dat Nice Systems Italiaanse digitale wapens levert aan Azerbeidzjan, een land met een bedenkelijke reputatie op het gebied van de mensenrechten. Of de software van Hacking Team tegen journalisten, ngo's of de oppositie werd ingezet, is niet vastgesteld. Ook bemiddelt Nice Systems tussen het repressieve regime in Oezbekistan en Hacking Team over de aanschaf van digitale wapens. Ook andere landen in Centraal-Azië, waaronder Kazachstan, staan op het lijstje van beide bedrijven.

De Italianen en de Israëliërs zijn erg close. Marco Bettini van Hacking Team geeft in een mail toe dat zij de Russische inlichtingendienst als klant hebben. '*Dear Adam. Thank you very much for this opportunity! Please let me be very open to you with regard to FBS. We got in touch with FSB in September 2010 through a Russian Governmental R&D Institution which is acting as a local partner. They visited us last week and they confirmed their interest in our solution. We have provided them with a demo version of our product and they are presently testing it. They are looking forward to setting up a large pilot project in order to test our product in real-life investigation scenarios with multiple targets*', aldus Bettini in een mail aan Adam Weinberg van Nice Systems.

Nice Systems en Hacking Team hebben ook samengewerkt in de leverantie van digitale wapens naar Oeganda. Dit wordt blootgelegd in

een artikel van *Buzzfeed* op 24 augustus 2015: 'Emails Reveal Israeli and Italian Companies Role In Government Spying'. Uit de openbaar gemaakte Wikileaks documenten blijkt dat het Nice Systems als tussenhandelaar voor Hacking Team aan de Oegandese politie heeft geleverd. De Israëliërs en Italianen hebben de Oegandezen geen belemmeringen opgelegd ten aanzien van het gebruik van de geleverde digitale wapens. De digitale wapens zijn ingezet in 2014 tegen LHBT-activisten (lesbisch, homo, bi en trans).

De Oegandese LHBT-activisten zijn het slachtoffer geworden van de zogenoemde Zeus malware, die al eerder door Hacking Team is gebruikt in haar digitale wapens. Een medewerker van Hacking Team, Alberto Ornaghi, grapt over Zeus en het feit dat de activisten niet hebben ontdekt dat Hacking Team erachter zat: '*They think we are a new Zeus*.'

Robotec fungeert als tussenhandelaar voor Hacking Team in Latijns Amerika. Robotec is een privaat Colombiaans bedrijf onder leiding van Hugo Fernando Ardila en Jamie Caicedo. Het bedrijf heeft verschillende deals voor Hacking Team afgesloten, onder meer met de anti-drugs en inlichtingendienst in Colombia, en met Panama, waar de digitale wapens zijn ingezet tegen de oppositie.

In 2013 schaft de Ecuadoraanse inlichtingendienst Senain met bemiddeling van Robotec software van Hacking Team. De Senain heeft een dubieuze reputatie. In 2015 publiceerde de website Ecuador Transparente een rapportage over de Senain die tussen 2012 en 2014 de oppositie, de media en mensenrechtenactivisten systematisch had bespioneerd. Amnesty International en Human Rights Watch schreven in dezelfde periode over de schendingen van de rechten van de inheemse volken in dat land door de Ecuadoraanse overheid en haar veiligheidsapparaat. Ook rapporteerden de mensenrechtenorganisaties over bedreigingen en de moord op mensenrechtenactivisten, de straffeloosheid van de politie en zorgen over de vrijheid van meningsuiting.

Uittocht van ontevreden medewerkers

Niet iedereen bij Hacking Team is gelukkig met de klantenkring van het bedrijf. Binnen het bedrijf zijn verschillende ontwikkelaars ongelukkig met de verkoop van digitale wapens aan repressieve regimes.

Al na de onthulling van Citizen Lab in 2012 over de inzet van de digitale wapens door de Marokkaanse overheid tegen journalisten, breekt er een discussie uit binnen het bedrijf. In 2014, na de onthullingen over de inzet van Hacking Team's digitale wapens tegen Ethiopische journalisten, wordt de onvrede nog duidelijker. Alberto Pelliccione neemt ontslag, en in de maanden die volgen houden meerdere werknemers het voor gezien.

Het antwoord van Vincenzetti op de interne discussie was de verschillende afdelingen van elkaar te scheiden zodat de ontwikkelafdeling geen zicht had op de verkoop, maar ook niet op de 'exploit afdeling', de afdeling die de documenten bewerkt om de apparatuur van mensen te infecteren. Deze documenten kunnen Word-documenten, pdf's of andere digitale bestanden zijn.

De technici van het bedrijf stellen dan ook dat zij niet wisten wie de klanten waren. De mensen van de 'exploit afdeling' zijn echter wel op de hoogte van de afnemers. Als Hacking Team zijn digitale wapens verkoopt aan Marokko, Ethiopië of Soedan, zijn deze landen immers van deze afdeling afhankelijk om documenten te prepareren waarmee het slachtoffer kan worden geïnfecteerd. De inhoud van die documenten verraadt allerlei aspecten van het doelwit.

De onthullingen van Citizen Lab toonden aan dat de digitale wapens van Hacking Team niet meer onzichtbaar zijn. Vincenzetti en zijn managers willen dat de ontwikkelaars zich inspannen om de software meer te verhullen, zodat ze niet meer te herleiden zijn tot Hacking Team. Na het vertrek van Pelliccione in 2014 vertrekken ook andere ontwikkelaars. Vincenzetti spreekt de vrees uit dat het onmogelijk zal zijn om het digitale wapen in de toekomst onzichtbaar en *up to date* te houden. Er lijkt sprake van een lichte vorm van paranoia binnen het bedrijf. De baas van Hacking Team is bang dat alle werknemers naar de concurrentie overlopen en hun kennis meenemen.

Vincenzetti is 'not amused' over de ontstane commotie over zijn bedrijf en over het vertrek van zijn medewerkers. Als Guido Landi krijgt hij de woede van de grote baas over zich heen. Landi is de voormalige rechterhand van de CTO (Chief Technology Officier). Landi is een van de belangrijkste ontwikkelaars die Hacking Team in 2014 verlaten.

Vincenzetti is woedend over het vertrek van de ontwikkelaar. Landi zal in de maanden die volgen ontdekken dat Vincenzetti goed is ingevoerd in de top van de Italiaanse opsporings- en inlichtingenwereld. De baas van

Hacking Team schrijft na het vertrek van Landi dat hij dit op het hoogste niveau bij de Italiaanse overheid zal aankaarten. Vervolgens krijgt Landi bezoek van twee hooggeplaatste functionarissen van de Italiaanse geheime dienst: kolonel Riccardo Russi en generaal Antonello Vitale. Later wordt Landi flink aangepakt door de openbare aanklager, die de hack van Hacking Team in 2015 onderzoekt. Landi is niet aangeklaagd, maar het onderzoek naar de hack loopt nog.

Vincenzetti en ethiek

Hacking Team ligt de afgelopen jaren regelmatig onder vuur vanwege de dubieuze leveranties van digitale wapens aan repressieve regimes. De reactie van Vincenzetti hierop is niet overtuigend. Eerst ontkende Vincenzetti de handel met omstreden regimes. Vervolgens claimde hij dat zijn bedrijf geen invloed had op de wijze waarop de wapens door haar klanten werden gebruikt. Vincenzetti beweerde ook regelmatig dat Hacking Team normaliter zorgvuldig naar de achtergrond van haar klanten kijkt, maar wat hier mee bedoelde maakte hij niet duidelijk.

Het overtuigt niet. Hacking Team heeft namelijk vanaf het begin geen problemen gehad om digitale wapens te verkopen aan klanten die een twijfelachtige reputatie hebben. Zo was Mexico vanaf het begin een van de grootste klanten van Hacking Team. Een land waar veel twijfels zijn over relaties tussen opsporings- en inlichtingendiensten en criminele organisaties, en waarbij men zich dus kan afvragen in welke handen de digitale wapens van Hacking Team terecht komen. Voor Mexico kochten Singapore, Marokko, Saoedi-Arabië digitale wapens bij de Italianen.

Uiteindelijk stelde Vincenzetti een ethische commissie, onder leiding van het advocatenkantoor Bird & Bird, in die moest toezien of de afnemers van Hacking Team wel door de beugel konden. Het is niet duidelijk met hoeveel zaken de commissie zich heeft bezig gehouden en hoe ze deze heeft beoordeeld.

Het werk van de ethische commissie kan echter weinig om het lijf hebben gehad en er lijkt eerder sprake te zijn van window dressing. Illustratief is dat in 2014, toen de ethische commissie al werkzaam was, Hacking Team digitale wapens leverde aan Soedan en hiervoor door de Verenigde Naties werd getikt vanwege het schenden van een embargo.

Hacking Team en Vincenzetti hebben ethiek niet hoog in het vaandel

staan. In maart 2013 velt Reporters Without Borders in haar jaarlijkse rapport *Enemies of the Internet* een hard oordeel over het bedrijf. Vincenzetti en zijn oude vrienden die allen een geschiedenis hadden in defensief beveiligingswerk op het internet waren in een periode van twintig jaar van vrienden tot vijanden van het internet verworden. Hun woorden uit de tijd van CryptoNet, toen het nog over het beschermen van de vrijheid van meningsuiting ging, blijken leeg. Zij zijn uiteindelijk voornamelijk geïnteresseerd in geld verdienen door middel van digitale offensieve wapens.

Het is dan ook een schok voor Hacking Team als twintig actievoerders in 2013 de voorruit van het kantoor van het bedrijf kapot slaan en binnenstormen. Vincenzetti is daar drie jaar later nog verontwaardigd over. Als *Foreign Policy* naar de bestorming vraagt, zegt hij: "*It was a full assault*." Bij het protest namen de actievoerders documenten, notities, zo'n beetje alles wat er te pakken viel, mee.

Een voormalig collega van Vincenzetti, Salvatore Sanfilippo die met hem samenwerkte bij Intesis SpA, wordt door *Ars Technica* geïnterviewd. Hij zegt niet verbaasd te zijn dat Vincenzetti de commerciële weg is ingeslagen en digitale wapens is gaan produceren, maar wel over de gebrekkige beveiliging van Hacking Team als gevolg waarvan het bedrijf in 2015 werd gehackt: "*I don't have the details, but if this is the case, it's a big mismatch to the experience I had with Vincenzetti and [Hacking Team Managing Director Valeriano] Bedeschi. They are both top-class hackers, and when I used to work with them in 1998, security was a top concern.*''

Volgens Sanfilippo was Vincenzetti wel een groot voorstander van de vrijheid van meningsuiting en encryptie. Toch vindt Sanfilippo het logisch dat Vincenzetti de markt van digitale wapens en de verkoop aan repressieve regimes is opgegaan: "*I'm not surprised about Hacking Team creation since probably this was seen as an effective way to monetize on security products.*''

Financiële motieven zullen dan ook een belangrijke reden voor het opzetten van Hacking Team zijn geweest. De *Daily Dot* stelt op 7 juli 2015 dat Vincenzetti zijn collega's uit de jaren 90, zoals Massimo Cotrozzi en Fabio Bolognesi, zag vertrekken naar de commerciële sector en daar veel geld gingen verdienen: '*In his 20s, Vincenzetti watched from afar as security colleagues became big-time businessmen who traded with the world's top banks, a path he'd eventually follow.*'

Financiële motieven lijken doorslaggevend voor Vincenzetti. Dit komt misschien wel het beste tot uitdrukking op zijn LinkedIn account waarin hij verklaart: '*My main non-professional interest is finance*.'

Exportvergunning

In 2014, twee jaar na de ontdekking van de inzet van digitale wapens van Hacking Team tegen Marokkaanse journalisten, wordt de Italiaanse overheid wakker. Vanwege de export van digitale wapens naar landen als Marokko, Ethiopië en Soedan vergelijkt de Italiaanse overheid de digitale wapens van Hacking Team met oorlogstuig. Dit betekent dat er in principe tevens een exportvergunning voor moeten worden aangevraagd bij het Italiaanse Ministerie van Economische Zaken.

Hacking Team had dit in het verleden nooit eerder gedaan uit angst voor het 'dual use' argument tegen de export: de digitale wapens kunnen voor opsporing worden gebruikt, maar ook om dissidenten, journalisten en politieke oppositieleden mee aan te vallen. Deze mogelijkheid kan na de onthullingen over onder meer Marokko in 2012 en Ethiopië in 2013 echter niet meer worden genegeerd.

Het Italiaanse Ministerie van Economische Zaken komt inmiddels tot een zelfde conclusie. Het ministerie stelt dat zij informatie heeft dat de digitale wapens van Hacking Team worden ingezet voor repressieve doeleinden waarbij de mensenrechten worden geschonden, en schrijft op 30 oktober 2014: '*Questa amministrazione è in possesso di elementi di informazione relativamente ad operazioni di esportazione da parte della Società in oggetto, che potrebbero configurarsi come connesse con possibili utilizzazioni attinenti alla repressione interna ed alla violazione dei diritti umani.*'

Het ministerie eist van klanten van Hacking Team dat zij een zwart-op-wit verklaring overhandigen waarin gesteld wordt dat de digitale wapens niet tegen de eigen bevolking worden ingezet.

Vincenzetti ziet meteen in dat dit misschien het einde van de lucratieve export voor Hacking Team betekent. Van de vijf landen die het meest besteden aan digitale wapens zijn er in ieder geval al twee (Marokko en Saoedi-Arabië) die de wapens niet gebruiken voor opsporingsdoeleinden. Ook met betrekking tot Mexico leven er grote twijfels, en kunnen de

wapens bovendien in handen komen van criminele kartels. Wanneer alleen de Europese Unie overblijft als handelsgebied, is het de vraag of Hacking Team financieel zal kunnen overleven.

Vincenzetti ziet het gevaar in en schrijft al zijn Italiaanse klanten aan met de mededeling dat het bedrijf mogelijk zijn handel moet opgeven. Via een van die klanten, de PCM, is Vincenzetti in staat om de president en de ministerraad van Italië te bereiken. Dit heeft resultaat. Er volgt een gesprek op het Ministerie van Economische Zaken waarbij ook enkele topambtenaren aanwezig zijn.

Het Ministerie van Economische Zaken zit zelf namelijk ook met een probleem. Zij is niet alleen controleur van Hacking Team, maar ook een klant van het bedrijf. Sinds 2013 gebruikt ook de Italiaanse FIOD (Guarda di Finanza) immers de digitale wapens van het bedrijf.

Vincenzetti wint deze slag, Hacking Team mag blijven exporteren. Begin 2015 wordt er een oplossing gevonden. Hacking Team vraagt een exportlicentie aan voor de gehele wereld om de uitvoer van spionagesystemen die niets met wapens of oorlog te maken hebben mogelijk te maken.

Een paar maanden later, in juli 2015, ligt de administratie van het Italiaanse bedrijf op straat en blijkt op welke schaal Hacking Team heeft samengewerkt met repressieve regimes. Dit heeft nog niet direct gevolgen voor de wereldwijde exportlicentie. De Italiaanse overheid wacht met het intrekken van die exportvergunning tot april 2016. In april 2016 trekt de Italiaanse overheid de vergunning voor de export naar landen buiten de Europese Unie in. Voor export naar landen buiten de EU moet Hacking Team per klant elke keer een aparte vergunning aanvragen. Hacking Team verliest daardoor in eerste instantie het grootste deel van zijn klanten. Slechts Zeven van de ongeveer 46 klanten van het bedrijf komen uit de Europese Unie.

De *backdoor* lekt uit

Voor de Italiaanse overheid dient zich naast de export vraagstukken vervolgens nog een ander probleem aan.

In hoeverre is het bewijs dat wordt verkregen met behulp van de inzet van digitale wapens van Hacking Team rechtsgeldig? Vincenzetti heeft

regelmatig gezegd dat zijn digitale wapens door Italiaanse opsporingsdiensten worden gebruikt om grote misdrijven mee op te lossen, zoals rond maffiabazen en moordenaars. Concreet bewijs hiervoor is echter nooit geleverd door Hacking Team noch door de Italiaanse overheid. Net als in Nederland is in Italië het inbreken op smartphones, laptops en andere digitale hulpmiddelen een grijs gebied waar binnen veel mogelijk is.

Er is echter nog een groter probleem. Informatie over de werking van de software die Hacking Team voor zijn digitale wapens gebruikt, is ook openbaar geworden. Verschillende publicisten, zoals internet veiligheidsdeskundige Bruce Schneier, verwijst naar openbaar gemaakte documenten waarin een *backdoor* (achterdeur) in de digitale wapens van Hacking Team wordt beschreven. Middels die *backdoor* kan het bedrijf het wapen in ieder geval op afstand uitzetten zonder dat de klant daar weet van heeft.

De klanten van Hacking Team zijn niet geïnformeerd over die achterdeur. De *backdoor* geeft echter niet alleen Hacking Team toegang tot de geïnfecteerde smartphones, laptops, computers. In theorie kunnen anderen zich daardoor ook toegang verschaffen en gegevens manipuleren. Dat maakt de bruikbaarheid van het bewijs dat verkregen is met behulp van digitale wapens minder aannemelijk.

Naast vragen ten aanzien van de afwezigheid van exportvergunningen, zelfs naar landen waar een VN embargo voor geldt en repressieve regimes, en de mogelijke aanwezigheid van een *backdoor* is er ook nog de handel in *zero-days* van Hacking Team. *Zero-days* (nul dagen) zijn veiligheidslekken in software die nog niet bekend zijn bij de makers van de software waarbij dei lekken zijn vastgesteld. Die *onbekende* veiligheidslekken worden door Hacking Team gebruikt om met hun digitale wapens in te breken op smartphones, tablets, etc. De handel in *zero-days* is een zwarte markt waar veel geld in omgaat.

De mensen die *zero-days* verkopen, kunnen werkzaam zijn bij een bedrijf als het Franse VUPEN security, Coseinc uit Singapore, het Amerikaanse Netragard and Vulnerabilities Brokerage International, maar individuen kunnen veiligheidslekken aanbieden. De bedrijven die beweren dat ze alleen overheden veiligheidslekken aanbieden dus niet aan de producenten van de software die lek is. De openbare data van Hacking Team maakt echter duidelijk dat het voor private partijen niet al te moeilijk is om *zero-days* aan te schaffen, zowel van bedrijven als

Vupen en Coseinc als van individuen.

Wie die individuele handelaren zijn blijft duister. Zo schaft Hacking Team veiligheidslekken aan van een Rus met de naam 'Vitaliy Toropov'. Hij biedt lekken aan in de browser Safari van Apple, in Flash van Adobe en Silverlight browser plug-in van Microsoft. De Italianen kopen uiteindelijk de lekken in Flash van de Rus maar hebben geen exclusiviteit. De Rus kan ze ook aan andere bieders aanbieden, zowel overheden, bedrijven als individuen. De Italiaanse overheid gebruikt dus digitale wapens die gebruik maken van veiligheidslekken die verhandeld worden op een zwarte markt waarbij onduidelijk is wie ze allemaal in handen krijgen.

Hacking Team heeft enkele Flash *zero-days* gekocht welke waarschijnlijk zijn gebruikt om in te breken op een smartphone, tablet, computer van een verdachte. Er is geen garantie dat Hacking Team de enige partij is die op de hoogte was van die veiligheidslekken in Flash en dat niemand anders dus bij de data van verdachten heeft kunnen komen. Hoe wijd verspreid de kennis van dit specifieke lek was, is moeilijk te achterhalen omdat ook criminele organisaties en inlichtingendiensten deze *zero-days* aanschaffen.

Hacking Team heeft dan wel een digitaal wapen ontwikkeld om mee in te breken, maar kan nooit garanderen dat iemand anders ook al aan het inbreken is. Het feit dat het Italiaanse technologiebedrijf zelf het slachtoffer is geworden van een digitale inbraak, maakt duidelijk dat digitale wapens misschien eerder digitale boemerangs zijn dan technische hulpmiddelen voor opsporings- en inlichtingeninstanties.

Besluit Nationale politie op Wob verzoek over Hacking Team, Gamma Group en Providence

Boeven vangen met dubieuze software van dubieuze bedrijven

De Nederlandse politie en Hacking Team; Flirten met de tools van de dictator

De Nederlandse politie en Hacking Team; Flirten met de tools van de dictator (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Gehele Observant #69 Politie Mercenaries

Wikileaks Hacking Team documenten

CitizenLab onderzoek naar Hacking Team

CitizenLab diverse artikelen over Hacking Team

Enkele e-mails uit Hacking Team met de politie

Kamervragen Hacking Team

Adressen e-maillijst van Hacking Team

Presentatie van Hacking Team RCS

Presentatie Man in the Middle hack uit 2003

Despite Hacking Team's poor opsec, CEO came from early days of PGP

Fear This Man; To spies, David Vincenzetti is a salesman. To tyrants, he is a savior. How the Italian mogul built a hacking empire.

The Hacking Team Defectors

Hacking Team goes to war against former employees, suspects some helped hackers

Let me show you the America that counts

Bruce Schneier over de Hacking Team *backdoor*

Hacker 'Phineas Fisher' Speaks on Camera for the First Time—Through a Puppet

Naar inhoudsopgave Observant #69

Gamma Group/Louthean Nelson
Wapenhandelaars pur sang

Met de software FinFisher of FinSpy van Gamma Group kan via een USB stick of van afstand worden ingebroken op computers, laptops, tablets en smartphones.

De FinFisher is een gewild digitaal wapen. Onder de klanten bevindt zich ook Nederland dat sinds 2012 zestien licenties voor FinFisher heeft aangeschaft. Nederland bevindt zich als FinFisher gebruiker in dubieus gezelschap. Het wapen is ook aangeschaft door een reeks repressieve regimes die het inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten. De volle omvang hiervan werd duidelijk in 2014 toen Gamma Group gehackt werd en via Wikileaks 40 GB aan interne data werd gepubliceerd.

De activiteiten van Gamma Group spelen zich veelal buiten de openbaarheid af. Er vallen veel vragen te stellen over he bedrijf. Vragen over de financiële integriteit van het bedrijf, over de vestigingen in belastingparadijzen zoals de Maagdeneilanden, Cyprus en Libanon. De herkomst van FinFisher, waarbij niet duidelijk is wie betrokken zijn geweest bij de ontwikkeling van het digitale wapen. Dit brengt ook aanzienlijke veiligheidsrisico's met zich mee.

De centrale figuur in de Gamma Group is Louthean Nelson. Hij begon zijn carrière in de jaren 80 bij PK Electronic, een Duits bedrijf dat groot werd als tussenhandelaar in de internationale wapenhandel. Louthean Nelson lijkt in die periode een aantal lessen te hebben geleerd, die hij bij Gamma Group toepast in de internationale handel in digitale wapens.

Peter Klüver wapenhandel

Louthean Nelson begint zijn carrière in Duitsland in de jaren tachtig bij het bedrijf PK Electronic of PK Electronic International. PK Electronic is het bedrijf van Peter Klüver, die in de jaren 80 een bedenkelijke reputatie heeft opgebouwd in de internationale wapenhandel.

Klüver is van oorsprong een handelaar in elektronica. In de openbaar

gemaakte *Cables* van de Amerikaanse ambassades kwam hij al in 1973 voor. *Cable '1973HAMBUR01517'* ('*Request for P.L. export transaction check on proposed shipment to: PK Electronic, Peter Kluver, Blumenstr. 52, 2 Hamburg 39, West Germany'*) geeft een korte beschrijving van het bedrijf en omschrijft PKE als een '*fairly young firm, with good reputation in its field, but with limited financial resources*.'

Het nieuwe bedrijf wil chips gaan produceren en voor de benodigde apparatuur uit de VS heeft PKE een exportvergunning nodig: '*PK Electronic has found a gap in the market in Germany for integrated circuits and therefore intends to begin the manufacture of IC-chips next spring.*' De *Cable* beschrijft een financier voor het Hamburgse bedrijf en een mr. Mueller die tot het bedrijf zal toetreden en de Department of State al heeft bezocht. De Amerikanen zijn ook al uitgenodigd om de machines te komen controleren zodra die uit de VS in Hamburg zijn opgesteld voor productie.

Dat het Peter Klüver voor de wind ging, bleek tien jaar later in 1985. Het Duitse weekblad *Der Spiegel* wijdde een groot artikel aan Klüver en zijn bedrijf PK Electronic: '*Wie im Familienclan, Spiegel-Report über den Handel mit deutscher Kriegs-Elektronik*' (5 augustus 1985). Het artikel behandelt het bezoek van de Saoedische kroonprins Prins Abdullah Ibn Nasir Ibn Abd al-Asis Al Saud in 1983 aan Hamburg. Abdullah werd hierbij gefêteerd met ritjes in een Leopard-tank en een banket, waarbij de hoogste baas van het West-Duitse leger aanschuift en liters champagne vloeien. Het uitje van de prins werd georganiseerd en betaald door Klüver. Hij hield er een order voor elektronische apparatuur van 65 miljoen Mark aan over. Het ging om een partij afluisterapparatuur, infrarood en laser instrumenten en nachtzicht apparaten, bestemd voor de Saoedische inlichtingendienst.

PK Electronic en een aantal andere vergelijkbare Duitse bedrijven waren in de jaren 80 in een niche markt gestapt door als tussenhandelaar op te treden en producten van multinationals zoals Philips, Siemens, AEG-Telefunken, Zeiss door te verkopen. Volgens *Der Spiegel* kon soms direct worden geëxporteerd wegens gebrekkige controle, soms via een omweg, meestal door te verhullen wat er daadwerkelijk werd uitgevoerd. PK Electronic kocht bijvoorbeeld een partij nachtzicht apparatuur van Philips-dochter Philips Elektro-Spezial, en verkocht die door aan Saoedi-Arabië zonder de daarvoor vereiste exportvergunningen.

Klüver handelde niet alleen met de Saoedi's, maar ook met de Libische

dictator Muammar al-Qaddafi, de familie Assad in Syrië en het Indonesië van Suharto. PK Electronic verkocht bijvoorbeeld een partij automatische radioscanners of peilapparaten waar radiosignalen mee kunnen worden opgespoord aan Syrië. Vanwege de in de Verenigde Staten geldende exportbeperkingen mocht het Amerikaanse bedrijf Ocean Applied Research Corporation deze niet zelf verkopen aan het Midden-Oosten; daarom werd de apparatuur via Klüver naar Syrië verscheept.

Volgens het *Der Spiegel*-artikel deden Peter Klüver en zijn PK Electronic deden goede zaken tijdens de Koude Oorlog. Het artikel citeert een defenspecialist volgens wie Klüver actief was in de wapenhandel in met name landen in Afrika en het Midden Oosten. Volgens het artikel kochten verschillende landen minder geavanceerde Russische tanks. Deze waren voor veel landen betaalbaarder dan bijvoorbeeld Duitse tanks, al waren ze dan niet voorzien van de modernste elektronica. Deze electronica konden landen vervolgens te zijner tijd voor een veel lager bedrag bij PK Electronic aanschaffen.

Naar aanleiding van het artikel klaagde Klüver *Der Spiegel* aan. De rechtbank van Hamburg dwong het weekblad een weerwoord van hem af te drukken. Dit gebeurde een maand na publicatie, waarbij *Der Spiegel* vermeldde dat de rechtbank de juistheid van de beweringen uit het artikel niet had onderzocht en dat het weekblad achter de inhoud van het artikel bleef staan. Klüver ontkende in zijn weerwoord alle handel van PK Electronic met het Midden-Oosten.

Halverwege de jaren tachtig breidde Peter Klüver zijn netwerk uit in Groot-Brittannië en de Verenigde Staten. Mede ingegeven door de ontstane problemen rond de uitbreiding in Hamburg en de groeiende Duitse media interesse voor zijn bedrijf.

Louthean Nelson & PK Electronic International

Louthean Nelson is al langer actief voor Peter Klüver en als blijk van vertrouwen wordt hij in 1985 onderdeel van de bedrijfsstructuur van PK Electronic. *Intelligence Online* schrijft op 18 december 2013 dat Louthean Nelson werkzaam was als '*the sales representative of the German security products firm PK Electronic International, he prospected the Chinese market back in the early 1980s*.'

Op 14 november 1985, twee maanden na het artikel in *Der Spiegel*,

wordt de Britse tak van het bedrijf PK Electronic International Limited opgezet. Louthean Nelson is een van de oprichters en wordt sales director. Derek Alan Myers, een zakenpartner van Louthean, wordt managing director. Een half jaar eerder was ook al een Amerikaanse tak van PK Electronic opgezet: PK Electronic International Corporation in New York.

De verhouding tussen Nelson en Klüver is zo goed dat Nelson tevens deelnemer wordt van het Duitse bedrijf PK Electronic International. Als correspondentie-adres gebruikt Nelson in deze periode zowel het adres van PK Electronic International (Marschnerstieg 5-7) als de privé-adressen Juthornstrasse 84 en Southerstrasse 84 in Hamburg.

Het laatste adres keert terug bij het tweede bedrijf dat Nelson in de jaren '80 opzet. Op 13 januari 1987 richt hij, samen met Myers, Personal Protection Products Limited op. De bedrijfsnaam is aanvankelijk Mardenmanor Ltd., maar wordt na twee weken gewijzigd. Als reden voor het opzetten van Personal Protection Products Ltd. geeft *Intelligence Online* aan dat de behoefte aan persoonsbeveiliging in de jaren 80 en 90 zou zijn toegenomen: '*In the wake of the IRA car bomb death of British MP Ian Gow at his home in Sussex, it (PK Electronic) tried to flog bomb detection technology to other British Mps*.'

Opkomst en ondergang van PK Electronic International

In de jaren '80 groeide PK Electronic langzaam uit zijn voegen. Rond 1986 verhuisde het bedrijf van de Heidenkampsweg via de Grasweg naar de Marschnerstieg in Hamburg-Noord. Deze verhuizing ging bijna niet door, omdat het Hamburgse gemeentebestuur de vestiging aan de Marschnerstieg dwarsboomde. Klüver dreigde zijn bedrijf te verplaatsen naar Londen waardoor 65 arbeidsplaatsen, en 150 arbeidsplaatsen bij toeleveranciers, op de tocht zouden komen te staan. Op 26 april 1988 ging de Hamburgse gemeenteraad alsnog akkoord met de verhuizing naar Marschnerstieg.

De groei van PK Electronic zette eind jaren '80 en begin jaren '90 door. De klantenkring bestond niet alleen meer uit Saoedi-Arabië, Syrië, Libië en Indonesië, maar ook uit Angola, Soedan, Nigeria, Jordanië, Irak en Taiwan.

Het Duitse weekblad *Focus* berichtte in 1995 onder de titel '*Knüppel für*

Folterknechte' (knuppel voor de martelknecht) over PK Electronic. Eerst somt het weekblad een lijst met klanten van het bedrijf op, die niet bekend staan vanwege het respecteren van de mensenrechten. Daarnaast gaat het artikel in op aantal tegenslagen die PK Electronic heeft ondervonden. *Focus* schrijft dat het bedrijf in 1991 een boete kreeg voor de export van apparatuur naar Taiwan. In 1992 werd een lading traangas en stroomstok wapens met bestemming Angola in België onderschept en in beslag genomen. In 1994 leverde PK Electronic aan een bedrijf in Jordanië dat bekend stond als tussenhandelaar aan Irak, om het embargo tegen Irak kunnen ontlopen.

PK Electronic is voor succesvolle handel gebaat bij onzichtbaarheid. Er komen echter steeds meer details over de handel van het bedrijf in de openbaarheid. Het zal PK Electronic in de komende jaren dan ook steeds minder voor de wind gaan. Zo wordt PK Elektronic door de Nederlandse overheid als leverancier van conventionele wapens geregistreerd, hetgeen tevens betekende dat het bedrijf binnen de radars van het wapenexportbeleid (inclusief de daarbijhorende exportbeperkingen) kwam te vallen.

Het lijkt erop dat Klüver pogingen heeft ondernomen om in de 21ste eeuw een nieuwe weg in te slaan. In 2005/2006 wijzigt Klüver de naam van PK Electronic International in PKI Electronic Intelligence. Het bedrijf verhuist naar Lütjensee aan de Großenseer Strasse 18, net buiten Hamburg. Op hetzelfde adres is het Motoren-Museum SchleswigHolstein gevestigd, waar Klüver directeur van is. Het is een online winkel voor allerlei electronica die zowel voor civiele als militaire doeleinden kunnen worden gebruikt. Voor zover bekend speelt Klüver geen rol in de productie en handel in digitale wapens.

Louthean Nelson blijft tot het einde van de jaren ‘90 verbonden aan PK Electronic International. Op 5 februari 1997 wordt hij uitgeschreven als zaakwaarnemer van PK Electronic. Op 22 september 1998 wordt de Engelse tak ontbonden. De Amerikaanse tak blijft bestaan tot 12 april 2005.

De opbouw van het Gamma Group imperium

Louthean Nelson begint in de jaren 90 met de opbouw van zijn bedrijfsimperium, dat later bekend zal komen te staan als de Gamma Group. Gamma Group, zoals het bedrijf zich presenteert op beurzen is

gevestigd in het belastingparadijs Britse Maagdeneilanden, op naam van Gamma Group International Ltd. Volgens haar website is Gamma Group een *'international manufacturer of surveillance & monitoring systems with technical and sales offices in Europe, Asia, the Middle East and Africa. We provide advanced technical surveillance, monitoring solutions and advanced government training as well as international consultancy to National and State Intelligence Departments and Law Enforcement Agencies'.*

Gamma Group bestaat uit een omvangrijk aantal bedrijven, waarvan vooral de bedrijven Gamma International (UK) en Gamma TSE bekend zijn. Gamma International UK houdt zich volgens de Gamma website bezig met 'communications monitoring solutions, tactical communications monitoring data recovery and forensic lab.

Gamma TSE *'has been supplying government agencies worldwide with turnkey surveillance projects since the 1990s. Gamma TSE manufactures highly specialized surveillance vehicles and integrated surveillance systems, helping government agencies collect data and communicate it to key decision-makers for timely decisions to be made.'* Volgens de website werkt Gamma TSE sinds de jaren '90 samen met de Britse overheid in het kader van surveillanceprojecten. Verdere details worden niet vermeld. Gamma TSE presenteert zich op beurzen in het Verenigd Koninkrijk, Frankrijk en het Midden-Oosten bijvoorbeeld bij de Security & Policing beurzen in het Engelse Farnborough.

De Gamma Group bestaat uit een grote aantal bedrijven. Louthean Nelson vervult samen met zijn vader, William Louthean Nelson, de centrale rol binnen Gamma Group. William Louthean Nelson (geboren in 1932) werd in de jaren 90 directeur en eigenaar van een aantal bedrijven die door zijn zoon waren opgezet. Het enige bedrijf dat op naam van William Nelson staat en van voor zijn Gamma-periode dateert, heet Compass Military Services Limited (opgericht op 1 januari 1970), een tussenhandelaar in militaire middelen. William is woonachtig in Wintersbourne Earls in de buurt van Salisbury in het zuiden van Engeland. Volgens de bedrijfsinschrijvingen van het Verenigd Koninkrijk is zijn vestigingsadres Parsonage Mead. Louthean Nelson is woonachtig in Beiroet Libanon, waar ook enkele van de Gamma bedrijven (Gamma International Sal) gevestigd zijn.

Gamma Group omschrijft zichzelf als een netwerk of een alliantie. Maar het is een schimmige wirwar. Zo blijkt in een poging om de

chronologische ontwikkeling van de Gamma Group te ontrafelen.

Chronologie Gamma Group

In 1998 richt Louthean Nelson Trophy Investments Limited op. Trophy Investments verandert in mei 1999 van naam. In juni 1999 wordt Nelson directeur van het bedrijf en gaat het bedrijf door onder de naam Gamma 2000.

Op 6 augustus 1999 wordt Computplus Limited opgezet, met Louthean Nelson als directeur. Op dezelfde dag wordt ook Technical Surveillance Equipment Ltd. opgericht. De naam van dit bedrijf wordt in 2005 veranderd in Gamma TSE. Louthean Nelson is sinds 22 mei 2001 directeur.

In het begin van zijn carrière gebruikt Louthean voor het opzetten van een bedrijf gevestigde bedrijven zoals Instant Companies en Swift Incorporations.

In 2000 wordt Louthean Nelson directeur van het in dat jaar opgezette Gamma Cyan Limited. Het bedrijf is inmiddels weer opgeheven.

In 2000 zet Nelson ook nog een ander bedrijf op onder zijn eigen naam BN Management Security Systems Ltd. Het bedrijf wijzigt een jaar later van naam in Axcition Europe, weer twee jaar later in Gamma Tema Consultants, om uiteindelijk augustus 2005 de huidige bedrijfsnaam G2 Systems te krijgen.

Het blijft vervolgens enige jaren stil met het opzetten van nieuwe bedrijven. Wel stapt Nelson in maart 2006 in het bedrijf CBRN Team van Niels Tobiasen en wordt directeur van het bedrijf. Tobiasen was dit bedrijf in 2004 begonnen om Oeganda te voorzien van '*CBRN (Chemical, biological, radiological and nuclear) threat detection equipment´* . Deze handel liep voor Tobiasen niet goed af: hij werd veroordeeld wegens corruptie en verdween voor een jaar in de gevangenis. Het is niet duidelijk of Louthean een rol bij de corruptie heeft gespeeld, maar hij werd als directeur van het bedrijf niet vervolgd. In 2011 wordt CBRN Team opgeheven.

Of Louthean Nelson zelf ook een bedrijf in CBRN heeft opgezet is niet vastgesteld. In een openbaar geworden nieuwsbrief van Gamma Group

uit het eerste kwartaal van 2011 staat dat "Gamma opened a company in the UK specializing in CBRN and VIP security." Dit zou in 2005 hebben plaatsgevonden. Het bedrijf staat niet op naam van vader of zoon Nelson.

In 2006 gaat Nelson verder met de uitbouw van de Gamma Group. In 2006 richt Louthean Nelson TS Comms ltd. op. Hij wordt tevens directeur van dit bedrijf. Een jaar later wijzigt de bedrijfsnaam in Gamma International (UK) Ltd.

In 2006 richt Nelson tevens (op 18 september) Gamma International Ltd. op onder nummer HE184042. Het bedrijf is gevestigd in Cyprus.

In 2006 wordt Singapore Global Surveillance Systems opgericht.

In november 2007 vestigt Gamma Group International Limited zich op de Britse Maagdeneilanden, welbekend als belastingparadijs. Ook vestigt Nelson een Gamma Group International SAL in Beiroet, Libanon. Beiroet is tevens de woonplaats van Louthean Nelson.

Gamma Group GmbH/FinFisher GmbH, de Duitse tak

In 2008 begint de uitbreiding van de Gamma Group in Duitsland. In Duitsland is ook het digitale wapen FinFisher ontwikkeld.

Op 25 november 2008 wordt de Duitse tak van Group, Gamma International GmbH, geregistreerd bij de Industrie- und Handelskammer (Kamer van Koophandel) in München. Het bedrijf staat aanvankelijk ingeschreven op het adres Tiepolostrasse 33 in Hamburg, maar zal later naar München verhuizen. Louthean Nelson heeft een belang in Gamma International GmbH, de Duitse tak van de Group. Er worden ook verschillende Duitse dochterondernemingen opgericht: Gamma International Sales GmbH, Gamma International GmbH en Gamma International Holding GmbH).

In mei 2013 wordt de naam Gamma International GmbH vervangen door FinFisher GmbH. Alle andere Duitse dochterondernemingen van het bedrijf ondergaan een zelfde naamsverandering. De Duitse bedrijven heten in het vervolg: FinFisher GmbH (voorheen Gamma International Sales GmbH), FinFisher Labs (voorheen Gamma International GmbH) FinFisher Holding (voorheen Gamma International Holding GmbH). Al deze bedrijven zijn gevestigd in München.

Anno 2016 behoren ook de volgende bedrijven tot de Duitse tak van de Gamma Group: Raedarius m8 GmbH en So m8 GmbH, allen gevestigd in München.

Naast Duitsland breidt Louthean nelson ook zijn imperium uit in Libanon. Naast de Gamma Group International SAL in Beiroet zet hij ook nog Elaman - German Security Solutions SAL (duidelijk onderdeel van Gamma Group), Gamma Cyan SAL Offshore (zelfde adres en telefoonnummer als Elaman) en Cyan Engineering Services SAL (zelfde adres, ander telefoonnummer) op.

Het laatste adres is direct gekoppeld aan een digitaal wapen om op de oude Nokia Symbian in te kunnen breken. In de Hacking Team-documenten van WikiLeaks komt een e-mail voor van Alberto Pelliccione (op dat moment Senior Software Developer van Hacking Team) die over het Symbian wapen schrijft. Pelliccione denkt dat het bedrijf Cyan Engineering Services een offshore vestiging is van het moederbedrijf en de website slechts een front. '*A giudicare dal sito sembra giusto una societa' di facciata*', schrijft hij op 1 augustus 2012. Volgens Pellicione is het bedrijf Cyan Engineering Services SAL gevestigd is in de wijk Hamra, Beiroet in Libanon. Het is dus heel goed mogelijk dat Gamma Group via bedrijven in Libanon of elders ook zijn digitale wapens verhandelt, buiten het zicht van controlerende instanties.

Financiële integriteit

Hoe al deze bedrijven in elkaar grijpen, valt nauwelijks te doorgronden. Zowel de openbaar gemaakte documenten van Gamma Group als de oude websites van het bedrijf en onthullingen over klanten van Gamma Group schetsen een beeld van een spiegelpaleis. In die zin heeft Gamma Group alle kenmerken van een inlichtingen frontorganisatie.

Louthean Nelson treedt zelden in de openbaarheid, maar heeft − samen met zijn vader − duidelijk de controle over Gamma Group. Nelson is directeur en aandeelhouder van Gamma Group International Ltd. Bestudering van de aan Gamma Group gelieerde bedrijven levert een duidelijk patroon op. Zodra Louthean Nelson uit de directie van een bedrijf stapt, neemt zijn vader de rol van directeur over. Zo houden de Nelsons de controle over hun imperium. Naast Louthean en zijn vader zijn er slechts een handjevol familieleden en vrienden die of

aandeelhouder of directeur zijn.

De wijze waarop de Gamma Group georganiseerd, lijkt te wijzen op een slimme constructie om gelden weg te sluizen naar belastingparadijzen, al dan niet via andere bedrijven. Gamma Group, zoals het bedrijf zich presenteert op beurzen, is gevestigd in het belastingparadijs Britse Maagdeneilanden, op naam van Gamma Group International Ltd. Daarnaast heeft Gamma Group vestigingen in Libanon (Gamma Group International Sal) en Cyprus. Landen die bekend staan als belastingparadijzen.

Wanneer men zich verdiept in de bedrijven van Louthean Nelson, valt op dat verschillende van zijn bedrijven nooit veel geld waard zijn geweest. De cijfers die gebruikt zijn voor onderzoek naar de cijfers van Gamma Group zijn afkomstig van de Britse Kamer van Koophandel. Engelse bedrijven met aandeelhouders moeten in principe jaarlijks een beperkt aantal financiële gegevens openbaar maken. Het gaat hierbij om een balans met het startkapitaal aan het begin van het jaar, de uitstaande rekeningen, de waarde van de bezittingen en het eind kapitaal van het lopende boekjaar.

Zo heeft het in 1999 opgerichte Gamma 2000 nooit winst gemaakt en is ook nooit iets waard geweest. Het in 1999 opgerichte Computplus was enige tijd 7.000 pond waard, maar recente cijfers duiden erop dat het bedrijf niets meer waard is.

Gamma TSE zou op 30 november 2015 rond de één miljoen waard zijn geweest, een verlies van ruim één miljoen in vergelijking met 2013.
In 2015 had het Engelse bedrijf een negatief vermogen van 250 duizend pond. Geld lijkt te verdampen bij de Engelse takken, terwijl dat de bedrijven zijn die zich presenteren als verkopers van FinFisher zowel op beurzen als op de website van Gamma Group.

Louthean Nelson en zijn vader William Nelson hebben daarnaast ook nog belangen in bedrijven, die formeel geen deel uitmaken van de Gamma Group, maar er wel nauw mee samenwerken. Zo neemt vader William Nelson neemt deel aan de bedrijven Elaman GmbH, TS Comms, en Fink Secure Communications. Deze bedrijven lijken op het eerste gezicht geen formele relatie te hebben met Gamma Group.

Niets is echter wat het lijkt in de Gamma Group. Dat wordt ondermeer duidelijk in de relatie met het bedrijf Elaman. Het Duitse Elaman wordt

door de Gamma Group soms gepresenteerd als retailer van Gamma Group. De website van de Gamma Group vermeldt dat de alliantie met Elaman zijn vruchten heeft afgeworpen: 'The successful Gamma-Elaman partnership has successfully been involved over the past five years in multi-million Euro projects. Gamma and Elaman operate (sales, manufacturing, development, and technical support) out of offices located in Europe, Africa, the Middle East, and Far East.'

Elaman maakt formeel dus geen onderdeel deel uit van de Gamma Group. Maar vader William heeft een aandeel in Elaman GmbH. En Louthean Nelson heeft een belang in de Zwitserse tak: Elaman AG, de Zwitserse tak van Elaman.

De ontwikkeling van FinFisher, Bad Aibling Station en de NSA

Louthean Nelson begeeft zich op de markt van digitale wapens. In 2008 wordt de FinFisher voor het eerst op de website van de Gamma Group te koop aangeboden. Begin 2009 wordt FinFisher eveneens vermeld (16 februari 2009) op de website: '*Leading IT experts from the Intrusion field are part of Gamma International's team. They are constantly developing and enhancing solutions to gather information from a variety of IT systems*', luidt het bijschrift van FinFisher. Tevens worden FinUSB Suite, FinSpy, FinFly en FinIntrusion Kit te koop aangeboden.

Het valt moeilijk te achterhalen welke bedrijven en individuen er betrokken zijn geweest bij de ontwikkeling van FinFisher. Als Duitse producenten van FinFisher worden steeds Gamma International GmnH (sinds 2013 van naam veranderd in FinFisher GmbH) en Elaman genoemd. Het is echter de vraag of dit ook de makers zijn van het digitale wapen. Wat uit onderzoek wel duidelijk is geworden: FinFisher is in Duitsland ontwikkeld, met medewerking van het bedrijf Elaman, maar ook met een ontwikkelaar van het Amerikaanse bedrijf CloudShields, en mogelijk de NSA.

In het artikel '*Reborn in the U.S.A.: The long, winding story of Gamma Group'* van *Insider Surveillance* (24 december 15) wordt gesuggereerd dat er een relatie bestaat tussen de Gamma Group en het Bad Aibling Station (BAS) van het Amerikaanse leger.

Het in in 1947 opgezette Bad Aibling Station, gelegen op zestig kilometer van München, werd tot 2004 gerund door de National Security Agency

(NSA). Het was een afluisterstation dat onderdeel uitmaakte van het Echelon netwerk, een afluister- en analyse-netwerk van Australië, Canada, New Zealand, het Verenigd Koninkrijk en de Verenigde Staten. Op 30 september 2004 werd BAS overgedragen aan de Duitsers en sindsdien in principe gerund door Bundesnachrichtendienst (BND), de Duitse inlichtingendienst.

In 2013 onthulde het weekblad *Der Spiegel* al op grond van openbaar gemaakte documenten van Edward Snowden dat de NSA nog steeds actief is in Bad Aibling en samenwerkt met de BND in de zogeheten Operation Eikonal.

In het artikel van *Insider Surveillance* wordt een relatie getrokken met de ontwikkelingen van digitale wapens die door de Amerikanen, vooral de NSA, worden geproduceerd. De door Snowden openbaar gemaakte documenten maken duidelijk dat de NSA bezig was met de ontwikkeling van digitale wapens waarbij niet hoeft te worden gewacht op de handelingen van het doelwit, zoals het openen van een attachment of het bezoeken van een website, om in te kunnen breken op de computer of de smartphone. De techniek/het programma van de inlichtingendienst wordt 'Quantuminsert' genoemd. De NSA was ook op zoek naar dergelijke digitale wapens die door andere partijen ontwikkeld werden.

CloudShield

Betrokkenheid van de NSA bij de ontwikkeling van FinFisher is nooit bewezen. Wel staat vast dat het Amerikaanse bedrijf Cloud Shields betrokken was bij de ontwikkeling van FinFisher.

CloudShield ontwikkelde defensieve digitale wapens voor het Amerikaanse leger. *The Washington Post* beschrijft op 15 augustus 2014 in het artikel '*U.S. firm helped the spyware industry build a potent digital weapon for sale overseas'* een ontmoeting in het najaar van 2009 tussen een senior ontwikkelaar van CloudShield Technologies, Eddy Deegan, en een Duitse contactpersoon, Martin J. Münch.

Deehan werkte enige tijd voor Gamma, maar had geen contract. Münch had zich in november 2008 aangesloten bij Gamma International GMBH, in dezelfde periode dat FinFisher voor het eerst te koop werd aangeboden. Hij is dan al langer betrokken bij Gamma, waarschijnlijk via Elaman of andere bedrijven waar de Group mee samenwerkt. Binnen de

IT-wereld staat Münch vooral bekend als ontwikkelaar van BackTrack Linux, een besturingsprogramma dat speciaal werd ontwikkeld voor beveiligingstesten.

Het is opmerkelijk dat CloudShield Technologies, een bedrijf dat voor het Amerikaanse leger hardware en software ontwikkelt, een medewerker zonder contract en rapportage naar Duitsland stuurt om met Münch van Gamma Group te gaan samenwerken. Als CloudShield ontwikkelaar Deegan in 2009 naar München afreist, ontmoet hij iemand van een bedrijf dat al bezig is met de ontwikkeling van digitale wapens. *The Washington Post* schrijft: '*Over several months, the engineer adapted Gamma's digital weapons to run on his company's specialized, high-speed network hardware. Until then CloudShield had sold its CS-2000 device, a multipurpose network and content processing product, primarily to the Air Force and other Pentagon customers, who used it to manage and defend their networks, not to attack others*.'

De ontwikkeling van digitale wapens is op dat moment (2008-2010) op het punt beland dat het afspelen van een YouTube film of het bezoeken van een Microsoft Live pagina genoeg is om de digitale wapens te activeren en in te breken op computers van slachtoffers. '*Merely by playing a YouTube video or visiting a Microsoft Live service page, for instance, an unknown number of computers around the world have been implanted with Trojan horses by government security services that siphon their communications and files.*' (*The Washington Post*, 15-09-14).

De door Edward Snowden openbaar gemaakte documenten maken duidelijk dat de NSA in deze periode dergelijke digitale wapens ontwikkelt door middel van het programma 'Quantuminsert'. YouTube wordt geïnfecteerd met een schadelijk computervirus. De gebruiker klikt de video aan en via een fout in een programma zoals bijvoorbeeld Adobe Flash kan de controle over de computer worden overgenomen. Hetzelfde geldt voor gaten in Oracle Java technologie of lekken in browsers.

De digitale wapens maken gebruik van zogenaamde *zero days*, fouten of lekken in software die nog niet ontdekt zijn door de fabrikanten en dus nog niet zijn gedicht. Grote internetbedrijven als Google en Microsoft maken zich volgens *The Washington Post* zorgen over deze manier van inbreken bij internetgebruikers. Het raakt namelijk niet alleen verdachten van strafbare feiten, maar iedereen die gebruik maakt van het internet.

FinFisher, maar ook Hacking Team's digitale wapen Galileo RCS, maken gebruik van de een vergelijkbare techniek van injectie. Het is aannemelijk dat deze technologie via CloudShield en de NSA bij Gamma terecht is gekomen. Het valt echter niet met zekerheid vast te stellen in hoeverre de Amerikaanse overheid daar een actieve rol bij heeft gespeeld.

Wel is aannemelijk dat diverse specialisten hebben gewerkt aan de ontwikkeling van digitale wapens waar de NSA al mee bezig was. Dit kan gebeurd zijn in commercieel verband. Mogelijk onder de vleugels van de Gamma Group, mogelijk onder de hoede van Elaman of Trovicor, twee van de bedrijven die in München in digitale wapens handelen.

Elaman

Elaman was betrokken bij de ontwikkeling van FinFisher. Dit blijkt onder meer op de website, waarop Eleman in 2010 schrijft: 'Leading IT experts from the Intrusion field are part of Elaman's team. They are constantly developing and enhancing solutions to gather information from a variety of IT systems. FinUSB Suite: The FinUSB Suite is a tactical USB device, which extracts predefined information from a target PC.'

Gamma Group meldt op haar website weer: 'The Remote Monitoring and Infection Solutions are used to access target systems. They give full access to stored information, the ability to take control of the target systems' functions, and even capturing encrypted data and communications.'

Elaman maakt geen formeel onderdeel uit van de Gamma Group. Maar Louthean Nelson heeft een belang in Elaman AG, de Zwitserse tak van Elaman.

Volgens de Elaman website kunnen klanten voor FinFisher contact opnemen met het kantoor aan de Baierbrunner Straße 15 in München. De Gamma-website en brochures verwijzen voor hulpvragen naar hetzelfde adres (Baierbrunner Strasse 15 in München) met name naar de persoon van Stephen Oelker.

Oelkers is betrokken bij de Duitse bedrijven van het Gamma netwerk: FinFisher GmbH, FinFisher Labs GmbH, FinFisher Holding GmbH, Raedarius m8 GmbH en So m8 GmbH. (FinFisher GmbH, FinFisher Labs

GmbH en FinFisher Holding droegen tot 2013 de naam van Gamma International GmbH) Naast Oelkers zijn bij de Duitse tak van Gamma Louthean Nelson en Martin Johannes Münch betrokken. Gamma International GmbH was gevestigd op hetzelfde adres als Elaman in München, alle aan FinFisher gerelateerde bedrijven zijn daar ook gebleven.

Andere betrokkenen zijn Thomas Fisher en Carlos Gandini. In een kwartaal-nieuwsbrief van Gamma Group uit 2011 schrijft de onderneming: 'Thomas Fisher joined Gamma International GmbH as the IP Monitoring Specialist. Gamma Group was fortunate to add Mr. Carlos Gandini to its growing team of experts in 2010. Carlos joined Gamma International GmbH in October, and is based in Munich, where he heads the Sales Department for our exclusive FinFisher lt Intrusion Portfolio.'

Wat hier ook allemaal van zij. Of Gamma Group nu haar kennis voor de ontwikkeling van FinSpy heeft gekregen van voormalig NSA medewerkers, de NSA zelf, Cloud Shields, of van een aantal andere Zwitserse of Duitse computerdeskundigen. De FinFisher zal uitgroeien tot een gewild artikel.

De klantenkring van Gamma

Wie zijn de klanten van Gamma Group? De website van Gamma Group, Elaman en FinFisher maken dit niet inzichtelijk. De bedrijven publiceren ook geen jaarverlslagen die meer inzicht zouden kunnen geven in de samenstelling van de klantenkring.

In de loop der jaren is echter duidelijk geworden dat FinFisher ook is aangeschaft wordt door repressieve regimes die het digitale wapen inzetten tegen oppositieleden, journalisten en mensenrechtenactivisten. Vanaf 2011 komen hiervan verschillende voorbeelden in de media.

In 2011 ontdekken activisten tijdens de Arabische Lente dat dictator Moebarak voor meer dan drie ton aan FinFisher spyware had aangeschaft. In 2012 volgen onthullingen over de inzet van FinFisher in Bahrein. Met de publicatie van de Wikileaks documenten in 2014 en de gehackte gegevens van Gamma Group zijn er nog meer details over de klantenkring van Gamma Group bekend geworden.

Nederland behoort ook tot de clientele. Sinds 2012 heeft de Nationale

Politie zestien licensies aangeschaft voor het gebruik van FinFisher. Nederland voegde zich aan in de rij Europese landen die eveneens hadden besloten digitale wapens van Gamma Group aan te schaffen. Die groep bestaat vooral uit Centraal- en Oost-Europese staten, 'Oostenrijk, Bulgarije, de Republiek Tsjechië, Estonië, Finland, Hongarije, Letland, Litouwen, Macedonië, Roemenië, Servië' en Nederland, Groot-Brittannië en Duitsland.

Uit de Wikileaks documenten blijkt dat ook de volgende landen tot de klantenkring van Gamma Group behoren. Onder de klanten bevinden zich veel landen met een repressief regime, waaronder 'Egypte, Oeganda, Ethiopië, Vietnam, Venezuela, Turkije, Turkmenistan, Bahrein.'

Wikileaks documenten maken tevens duidelijk dat Gamma handelde in Turkmenistan. In samenwerking met het Zwitserse bedrijf Dreamlab Technologies. Thomas Fisher van Gamma International uit München verbleef in 2010 samen met Nicolas Mayencourt, de CEO van Dreamlab, in Turkmenistan. Beide bedrijven hebben daar voor de Turkmeense overheid '*an Infection Proxy Infrastructure and Solution applicable nationwide for all international traffic the Turkmentel and TMCell networks*' opgezet. Dreamlab Technologies en Gamma Group hebben het repressieve regime geholpen om een infrastructuur te ontwikkelen om het gehele mobiele telefoonverkeer mee in de gaten te houden. In Oman werkten Gamma en Dreamlab op een vergelijkbare wijze samen. Gamma Group heeft Dreamlab Technologies voor deze projecten rond de een miljoen dollar betaald.

Martin J. Münch, woordvoerder Gamma, spreekt wartaal

Gamma Group doet niet veel moeite om zich publiekelijk te verantwoorden of verdedigen over haar leveranties van digitale wapens aan repressieve regimes. Louthean Nelson treedt sowieso zelden in de openbaarheid.

De enige woordvoerder van het bedrijf, Martin Münch, communiceert bijnan surrealistisch met de media over de betrokkenheid van Louthean Nelson bij de Gamma Group.

Martin J. Münch (Muench) stelt in *the Guardian* van 28 november 2012 dat Louthean Nelson niets met Gamma Group te maken heeft en dat hij de enige woordvoerder is van de Group: *'He initially denied to us that*

Nelson was linked to Gamma, and denied that Nelson owned the anonymous BVI affiliate. Martin Muench, who has a 15% share in the company's German subsidiary, said he was the group's sole press spokesman, and told us: "Louthean Nelson is not associated with any company by the name of Gamma Group International Ltd. If by chance you are referring to any other Gamma company, then the explanation is the same for each and every one of them".'

Als *The Guardian* bewijs op tafel legt dat Louthean nelson wel degelijk betrokken is, draait Münch, maar toch ook weer niet helemaal. '*After he was confronted with evidence obtained by the Guardian/ICIJ investigation, Muench changed his position. He told us: "You are absolutely right, apparently there is a Gamma Group International Ltd. So in effect I was wrong - sorry. However I did not say that Louthean Nelson was not associated with any Gamma company, only the one that I thought did not exist".'*

Naar aanleiding van de onthullingen rond de verkoop van Gamma Group producten aan Egypte in 2011 Bahrein in 2012 communiceert het bedrijf ook op opmerkelijke wijze met de buitenwereld.

Advocaten van Gamma International GmbH ontkennen in de *Frankfurter Rundschau* van 11 maart 2011 dat de Duitsers zaken hebben gedaan met het Egypte van dictator Moebarak: '*Das Angebot, auf das Sie sich möglicherweise beziehen, stammt nicht von unserer Mandantschaft, sondern von der rechtlich unabhängigen Firma Gamma International UK Ltd. mit Geschäftssitz in Großbritannien.*' Volgens de Duitse advocaten hebben beide Gamma-onderdelen Gamma International GmbH en Gamma International UK dus niets met elkaar te maken.

Toch beantwoordt Martin J. Münch een jaar later vragen van *Bloomberg.* Münch wordt gepresenteerd als de '*managing director of Gamma International GmbH*.' In deze hoedanigheid ontkent de directeur dat FinFisher aan Bahrein was verkocht.

Münch gaat vervolgens echter in de verdediging. Hij stelt op 27 juli 2012 tegen *Bloomberg*: *'The company was investigating whether the product in the CitizenLab study was a demonstration copy of the product stolen from Gamma and used without permission.'*

Münch gaat zelfs nog een stap verder: *'It is unlikely that it was an installed system used by one of our clients but rather that a copy of an*

old FinSpy demo version was made during a presentation and that this copy was modified and then used elsewhere."

Volgens *Bloomberg* suggereert Münch zelfs dat de demoversie gestolen is: *"He went further to suggest that the demonstration version may have been stolen using a flash drive while conceding.'*

De verklaring van Münch, dat een demonstratieversie van FinFisher mogelijk gestolen is, is niet heel aannemelijk. De WikiLeaks documenten over Gamma Group van 15 september 2014 maken namelijk ondubbelzinnig duidelijk dat Gamma Group wel degelijk met Bahrein heeft samengewerkt. De verkoop van een FinFly USB licentie begon in oktober 2010 en de economische relatie duurde tot februari 2013.

Münch spreekt in dit specifieke geval dus niet de waarheid. De uitspraken van Münch zijn echter ook om een andere reden zeer opmerkelijk, en zorgwekkend. Münch houdt het klaarblijkelijk voor mogelijk dat de FinFisher op relatief eenvoudige wijze gestolen kunnen worden. Dit levert serieuze vraagtekens op over de veiligheid. Digitale wapens kunnen, net als fysieke wapens, in handen van derden vallen. Of dit nu wederrechtelijk is of door het nabouwen aan de hand van een voorbeeld.

Naast diefstal zijn er nog een aantal andere zaken ten aanzien van het gebruik van FinFisher die veiligheidsvraagstukken op roepen. In de openbare helpdesk vragen van klanten van FinFisher staan vragen over de ontdekking van het digitale wapen door virusscanners op computers of laptops. Dit duidt erop dat verschillende inbraken met FinFisher niet zullen lukken, maar ook dat het wapen ontdekt en geneutraliseerd kan worden. Welke gevolgen dit heeft voor de verzamelde bewijslast, de bruikbaarheid van het wapen is onduidelijk.

De ondoorzichtige ontstaansgeschiedenis van FinFisher roept daarnaast andere veiligheidsvraagstukken op. Bij het digitale wapen Galileo RCS van Hacking Team is gewezen op het bestaan van een *backdoor.* De openbare documenten van Gamma Group bevatten weinig specifieke informatie over het programma, wel de werking, maar niet het specifiek functioneren van de tool. De onduidelijke ontstaansgeschiedenis en de betrokkenheid van verschillende partijen bij de ontwikkeling van het wapen geeft genoeg aanleiding om te twijfelen aan de integriteit van de tool, iets dat Münch met zijn optreden in de media lijkt te bevestigen. Van enige onduidelijkheid over de ontwikkeling van Galileo RCS van

Hacking Team is geen sprake, het bedrijf heeft de tool zelf ontwikkeld. En de Italianen hebben daarbij ook bedacht om een *backdoor* in de software in te bouwen zodat zij er zelf nog bij kunnen zonder dat hun klanten dat weten. Het lijkt logisch te veronderstellen dat dit bij FinFisher ook het geval is.

Business as usual

Gamma Group lijkt weinig last te hebben van de controverses van de afgelopen jaren. FinFisher is nog steeds een gewild digitaal wapen en het bedrijf lijkt het economisch voor de wind te gaan.

Louthean Nelson is in die zin een succesvol ondernemer. Die goed heeft geleerd van de ervaring die hij in de jaren 80 en 90 als tussenhandelaar in de internationale wapenhandel bij PK Electronic heeft opgedaan. Vanuit het perspectief van Louthean Nelson heeft hij het werk van PK Electronic voortgezet, inclusief de klandizie die daarbij hoort. De analogie tussen PK Electronic in de jaren 80 en 90 en Gamma Group van na de eeuwwisseling is sprekend. PK Electronic betrok wapens van Philips Elektro-Spezial, Siemens, AEG-Telefunken en Zeiss en verkocht die door aan repressieve regimes in Azië, het Midden-Oosten en Afrika. PK Electronic probeerde eerst zelf chips te produceren, maar het bleek later lucratiever om als tussenhandelaar op te treden. Gamma Group betrekt digitale wapens van producenten in Duitsland en verkoopt ze aan vergelijkbare klanten. Als Duitse producenten worden steeds Gamma International GmbH/FinFisher en Elaman genoemd. Maar zijn dat ook echt de makers van de wapens?

Boeven vangen met dubieuze software van dubieuze bedrijven

Gamma Group en de politie; FinFisher trojan in de Nationale politie

Gamma Group en de politie: FinFisher trojan in de Nationale Politie (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Gehele Observant #69 Politie Mercenaries

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

Cable '1973HAMBUR01517'

Wie im Familienclan, Spiegel-Report über den Handel mit deutscher Kriegs-Elektronik

PK Electronic International

Knüppel für Folterknechte

PKI Electronic Intelligence

U.S. firm helped the spyware industry build a potent digital weapon for sale overseas

Offshore company directors' links to military and intelligence revealed

Elaman folder FinFisher

Gamma folder FinFisher

Gamma Group presentatie FinFly

FinFisher - Internal Newsletter Aug 2010

gamma-group_newsletter_gamma-newsletter-2011q1

FinFisher - Internal Newsletter Mar 2011

FinFisher - Internal Newsletter Jul 2011

Gamma Group Oeganda

GAMMA Dreamlab Turkmenistan

Contract DREAMLAB en GAMMA 2011

FinFlyISP on the CloudShield CS-2000

Fintraining

Een van de folders van PKI Electronic Intelligence

PK ELECTRONIC gegevens Kamer van Koophandel

Kamervragen FinFisher/Gamma Group

Gamma bedrijfsschema

Naar inhoudsopgave Observant #69

Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens

Providence is een relatief nieuwe speler in de internationale handel in digitale wapens. Het bedrijf produceert en ontwikkelt zelf geen digitale wapens, maar manifesteert zich als tussenhandelaar.

Providence is een in 2009 opgericht Brits bedrijf in security. Het biedt trainingen en apparatuur op het gebied van veiligheid en anti-terrorisme aan. Het gaat hierbij om trainingen in bijvoorbeeld observatie en het installeren van afluisterapparatuur, een cursus over verschillende tracking methoden, hoe apparatuur te verhullen is, trainingen in inbreken en een black catalogus met waarschijnlijk militaire trainingen. Het bedrijf biedt een special toolkit voor het installeren van afluisterapparatuur voor zowel audio- als video-opnames en los gespecialiseerd inbrekersgereedschap aan. Ook een complete inbrekerskits behoren tot het assortiment, evenals het verbergen van camera's en microfoons in nepstenen, boomstammen, dakpannen en andere manieren om apparatuur te verhullen.

Providence produceert en ontwikkelt – voor zover bekend - zelf geen digitale wapens. Met de publicatie van de Wikileaks documenten over Hacking Team in 2015 is echter duidelijk geworden dat Providence een tussenhandelaar is in digitale wapens. De Wikileaks documenten geven een onthullende inkijk in het optreden van Providence en de wereld van de tussenhandel, waarin opportunisme en financiële belangen de boventoon voeren.

Er is weinig openbare informatie over Providence beschikbaar. Het bedrijf heeft echter een breed netwerk in veiligheids- en defensiekringen, met opmerkelijke connecties met de SAS, vooral met de controversiële voormalige SAS generaal John Taylor Holmes.

Providence SA

Providence is in 2009 opgericht door Stephen Turner. Turner zat van 1988 tot 2005 bij het Britse leger, met name bij de SAS.

De SAS is een speciale eenheid van het Britse leger en heeft in Hereford een van haar grootste militaire bases. Er is regelmatig controversie over de rol die Special Air Services (SAS) speelt. De eenheid is zelfs veroordeeld voor mensenrechtenschendingen in de jaren '70 tijdens The Troubles in Noord-Ierland. In de zomer van 2016 in het kader van het Chilcot onderzoek (the Iraq Inquiry) naar de Britse betrokkenheid bij de Irak-oorlog, rezen er vragen over de wijze van optreden in dat land. Een ex-SAS commandant verklaarde: '*UK Special Forces were helping to run Latin American-style death squads*.'

Na zijn tijd bij de SAS werkte Turner in 2005-2006 korte tijd voor AKE, een bedrijf dat de beveiliging doet voor verschillende mediaorganisaties. In 2006-2007 werkte hij enkele maanden voor ArmourGroup Ltd., ook wel bekend onder de naam ArmorGroup. Dit bedrijf opereerde in opdracht van het Amerikaanse leger in Irak en Afghanistan en werd geplaagd door schandalen over onder meer misbruik en mishandeling van Afghaanse werknemers, het inhuren van mensen met een crimineel strafblad en het inhuren van de Taliban voor hun eigen bescherming. Turner hield zich (volgens zijn LinkedIn account) voor ArmorGroup bezig met "training US military, intelligence gathering techniques to combat terrorism by the use of irregular warfare". Van 2007 tot 2009 werkt Turner nog twee jaar bij het beveiligingsbedrijf Anubis Associates.

Stephen Turner zet op 24 juni 2009 Providence SA Ltd. op, samen met zijn zakenpartners Hugh Richard Macdougall en Michael William Davies. Davies was van 1997 tot 2007 werkzaam op het Britse Ministerie van Defensie als telecommunicatie engineer. Op 18 juli 2014 zal de naam van het bedrijf worden veranderd in Providence Global Itf Ltd. ITF staat voor Intelligence Through Foresight.

Providence krijgt al snel na haar oprichting de beschikking over een klein complex op het Harewood Park Estate, onder andere bestaande uit the Gatehouse en de Upper Barn Grange Farm bij Harewood End, Hereford. Hereford is de belangrijkste basis van de SAS. Over het complex meldt Providence in 2010 op haar website: *'Providence operates at a discreet location in Herefordshire, England. Our state of the art facilities provide the very best operational training environment.*'

Bij de lancering van haar eerste website in 2010 (providenceltd.com) presenteert het bedrijf zich nog als Providence Consultants, eigenlijk een soort netwerk van freelancers in de beveiligingswereld.

Turner zet hoog in op de website. Hij presenteert Providence als een omvangrijke organisatie: '*We are market leaders in technical surveillance products, training and specialist consultancy.*' '*Providence Consultants are world class subject matter experts in the Field of Defence; they possess Global Operational experience which is academically underpinned.*'

De website vervolgt: '*Backed by subject matter experts in the technical and engineering fields, as well as a robust and inquisitive approach to R and D*.' Ook hiermee lijkt Providence te willen suggereren dat het een omvangrijk bedrijf is, met allerlei afdelingen zoals onderzoek en ontwikkeling (R&D, Research & Development), maar in werkelijkheid is het van bescheiden omvang.

De website vervolgt: '*Our operational experts have worldwide experience in both permissive and non-permissive intelligence gathering environments and have a highly attuned sensitivity to the nuances of tactics and techniques that can be employed in any given situation*'. Bij deze laatste omschrijving lijkt Turner te willen verwijzen naar zijn ervaringen bij de SAS en de militaire aannemers waar hij vervolgens voor heeft gewerkt.

Providence probeert zich op allerlei plekken te verkopen. Het huurt regelmatig een stand en presenteert zich op de ISS World beurzen, de Duitse General Police Equipment Exhibition & Conference (GPEC), de Security and Policing beurs in Farnborough van het Britse ministerie van Binnenlandse Zaken, de Emirates Security Exhibition and Conference (Emsec) en Milipol in Parijs en Dubai.

In 2010 breidt Providence zijn organisatie verder uit. Providence opent een kantoor in Singapore. Matt Jamieson is hier de centrale figuur.

John Taylor Holmes

Providence oprichter Stephen Turner heeft een verleden bij de SAS.
De SAS connectie van het bedrijf gaat echter verder. Providence werkt vanaf 2011 nauw samen met de voormalig SAS generaal John Taylor Holmes, die in het verleden onder meer in Noord Ierland heeft gevochten. In 2012 richten Turner en Holmes ook samen een bedrijf op, Quintel Intelligence Limited.

Providence werkt hiermee samen met een controversiële figuur, wiens carrière een aaneenschakeling is van dubieuze praktijken. Na zijn vertrek bij de SAS in 2001 is Holmes verbonden aan verschillende private militaire bedrijven voor huurlingen die voor de Britse overheid werkten in Irak, Afghanistan, maar ook in Engeland zelf.

Na zijn vertrek bij de SAS in 2001 werkt Holmes voor The Inkerman Group, dat zich bezighoudt met het in de gaten houden van demonstranten en activisten, in opdracht van bedrijven, regeringen en individuen. Een van de protestgroepen waar The Inkerman Group het vizier op richtte was het Britse Plain Stupid, een anti-luchtvaart collectief waarvan de activisten door het bedrijf werden omschreven als 'ecoterroristen'.

Hierna is Holmes directielid van het bedrijf Erinys, een private militaire aannemer, dat onder meer in opdracht van de Amerikaanse en Britse overheid werkte voor de beveiliging van olie-installaties in Irak. Het bedrijf is ook actief in de mijn en olie industrie in onder andere Colombia, Nigeria, Angola en Ghana.

De lijst van controverses rond Erinys is lang. De arbeidsomstandigheden van Iraakse werknemers in dat land tijdens de oorlog na de Amerikaanse invasie van 2003 waren slecht. Het bedrijf is door Amnesty International beschuldigd van mishandeling van een zestienjarige jongen in Kirkuk, Irak. Medewerkers van het bedrijf schoten op een menigte waarbij drie gewonden vielen. Erinys leunt ook sterk op militairen uit Zuid-Afrika die tijdens de Apartheid lid waren geweest van de paramilitaire politie-eenheid Koevoet die bekend stond om haar gewelddadigheden, martelen en moorden. Zelfs enkele bestuurders van het bedrijf zijn tijdens de apartheid in Zuid-Afrika actief geweest voor de militaire inlichtingendienst en netwerken van extreemrechtse groeperingen.

In 2004/2005 richt Holmes het bedrijf Titon International Limited op. Dit bedrijf levert vooral dienstverlening op het grensvlak tussen politie, leger en inlichtingendiensten. Denk aan '*business intelligence, recovering stolen assets, covert anti-fraud operations, protecting intellectual property and electronic counter-espionage.*'

In 2011 duikt Holmes op in Libië. Hij verblijft hier uit naam van zijn eigen bedrijf, dat in dienst van de Britse oliemaatschappij Heritage Oil opereert. Wat Heritage Oil precies in Libië deed blijft schimmig, maar in de grondstofrijke Noord-Afrikaanse staat zal het om het herstel van olie-

installaties of hernieuwde productie zijn gegaan. Holmes wordt in een artikel van persbureau Reuters omschreven als de '*super-fixer*' van Engeland.

Holmes lijkt de afgelopen jaren minder actief te zijn voor Titon International. Het bedrijf is eigenlijk afgeschreven, hetgeen alles te maken heeft met het voormalige adres van het bedrijf: 25 Grosvenor Street in Londen. Titon huurde hier kantoorruimte van de Russische miljardair en oligarch Boris Berezovsky, de in het Verenigd Koninkrijk woonachtige Russische vluchteling en bekend als criticus van Poetin.

Na de moord op Alexander Litvinenko (voormalig medewerker van de Russische geheime dienst FSB) in november 2006, werden tijdens het politieonderzoek in de percelen van 25 Grosvenor Street sporen van Polonium 210 aangetroffen. Litvinenko was overleden aan vergiftiging door het middel Polonium 210. Titon International ontkende elke betrokkenheid bij de moord op Litvinenko. Het was echter bekend dat Litvinenko contact had met een andere huurder in het gebouw: Erinys International, het bedrijf waar Holmes in het verleden werkzaam voor was geweest.

Providence en Titon/Quintel

Vanaf 2011 groeien de twee ex-SAS'ers Stephen Turner van Providence, en John Taylor Holmes, van Titon International, naar elkaar toe.

Holmes is op leeftijd. Zijn eigen bedrijf Titon International heeft duidelijk reputatieschade opgelopen. De aandacht voor 25 Grosvenor Street en de bedrijven die op het adres gevestigd waren - Holmes moest ook verschijnen voor de onderzoekscommissie - is voor bedrijven die het liefst in het duister opereren niet welkom.

Turner maakt deel uit van een jongere generatie SAS-soldaten. Hij is duidelijk de protegé van Holmes en staat met Providence nog aan het begin van zijn zakelijke carrière. Het is evident dat de samenwerking met Holmes Providence geen windeieren zal leggen. De ervaring van Holmes bij de SAS en het bedrijfsleven, evenals zijn netwerk bij het Britse Ministerie van Defensie, het Britse leger en de wereld van de private inlichtingenbedrijven, zijn vanzelfsprekend zeer bruikbaar voor het nog jonge bedrijf Providence.

Turner en Holmes richten in 2012 het bedrijf Titon Systems Limited op, dat na een maand van naam verandert in Quintel Intelligence Limited. Waarschijnlijk omdat de bedrijfsnaam Titon als gevolg van het onderzoek naar de moord op Litvinenko besmet is geraakt. Holmes en zijn bedrijf Titon International Limited zijn mede-eigenaar van Quintel Intelligence, dat is gevestigd is op hetzelfde adres als Titon: 57 Grosvenor Street in Londen.

Holmes is Providence SA zijn bij de oprichting aandeelhouders van Quintel Intelligence Limited. Later worden Turner en HMS Harewood Ltd. (onderdeel van de Providence Group) toegevoegd als aandeelhouders van het bedrijf. In 2015 worden bovendien nog de bedrijven Quintel (Overseas) voor onderzoeksactiviteiten, en Quintel Asset Recovery voor financieel onderzoek, opgericht. Dit laatste bedrijf zal later van naam veranderen in Quintel Financial, en vervolgens in Quintel Consultants.

Uitbreiding Providence

Providence breidt zijn organisatie vanaf 2012 verder uit.

In juli 2012 richt Stephen Turner, samen met Michael William Davies en Neil Macdougall, DMT Holdings (Harewood) op, dat een jaar later van naam verandert in Providence Global Ltd. Deze tak moet de defensieactiviteiten gaan ontplooien, terwijl Providence Global Itf Ltd. de beveiligingsactiviteiten voor haar rekening neemt. Ook wordt nog een bedrijf opgericht voor het beheer van het trainingscomplex bij Harewood End: HMS Harewood.

Ten slotte wordt in juni 2013 Counter Threat Solutions Ltd. opgezet, en in oktober 2013 Providence Itf UK Ltd.

Providence krijgt ook een Nederlandse connectie. De Nederlander Peter Stolwerk gaat onderdeel uitmaken van het Providence netwerk. Stolwerk was van 1993 tot 2006 werkzaam bij achtereenvolgens de KMar, de politie Zeeland en Amsterdam. In 2012 wordt Stolwerk directeur van Providence BNLX, een Providence kantoor in Haarlem, Nederland.

Anno 2016 heeft Providence – volgens haar website - kantoren in het Verenigd Koninkrijk (Providence Global, Providence UK en Counter Threat Solutions), de Verenigde Staten (Providence US), Nederland (Providence Europe en Tac-up), Singapore (Providence Global) en Maleisië

(Providence Global). En daarnaast − al vermeldt de bedrijfswebsite dit niet − een brievenbusfirma in Panama, Providence Global Corp. Het Executive Team van Providence Global ITF bestaat uit de oprichters Stephen Turner en Michael Davies en, sinds 2014, Peter Stolwerk.

Financiële integriteit

De website van Providence geeft weinig informatie over de omvang van het bedrijf, het aantal werknemers, de omzet, en haar klantenkring. Het is echter duidelijk dat Providence een breed netwerk heeft, gezien de achtergrond van Turner en Davies bij onder meer het Britse Ministerie van Defensie, het Britse leger, de SAS, en verschillende private beveiligingsbedrijven. De ervaring van Holmes bij de SAS, evenals zijn werkzaamheden na zijn vertrek bij de SAS, zullen zeker geholpen hebben bij de verdere uitbreiding van het netwerk. Het is evident dat dit netwerk Providence zal helpen geholpen bij de opbouw van haar klantenkring.

Er vallen echter vraagtekens te plaatsen bij de financiële integriteit van Providence. De constructie is dusdanig dat het geschikt is voor het wegsluizen van gelden en het onttrekken financiële controle.

Providence heeft een vestiging in een belastingparadijs: Panama.
Bij de meeste bedrijven die tot de Providence Group behoren is de directeur tevens aandeelhouder. Turner gaf de Nederlander Peter Stolwerk een plek in zowel Providence Itf UK als Providence Global en HMS Harewood. Hij verbond daarmee Providence Europe BV aan Providence Group. Stolwerk is geen directeur of aandeelhouder van het centrale bedrijf van Providence Group, Providence Global Itf.

Het is niet duidelijk hoeveel geld er in het bedrijf omgaat. Providence biedt op haar website geen inzicht hierin. De Europese Providence bedrijven lijken nauwelijks omzet te maken. De financiële cijfers van de Panama vestiging vallen niet in te zien.

In 2010, toen het bedrijf nog over Providence Consultants sprak, zou er ongeveer een half miljoen in het bedrijf zitten. Volgens de jaarcijfers heeft het bedrijf Providence Global ITF Ltd. in 2011 een negatief eigen vermogen van een half miljoen. Providence Global Ltd. zou in 2013 nog ongeveer 120.000 pond waard zijn geweest, maar dat geld was in 2014 grotendeels verdampt. Inhoudelijke en financiële jaarverslagen

ontbreken op de website.

De cijfers die gebruikt zijn voor onderzoek naar de cijfers van Providence zijn afkomstig van de Britse Kamer van Koophandel. Engelse bedrijven met aandeelhouders moeten in principe jaarlijks een beperkt aantal financiële gegevens openbaar maken. Het gaat hierbij om het startkapitaal aan het begin van het jaar, de uitstaande rekeningen, de waarde van de bezittingen en het eind kapitaal van het lopende boekjaar. Van Providence zijn niet veel gegevens beschikbaar.

Tussenhandelaar Providence en staatsgeheimen

Providence produceert zelf geen digitale wapens. Het bedrijf profileert zich op haar website ook niet als een producent van digitale wapens.

De in 2015 gepubliceerde Wikileaks documenten over Hacking Team maken echter duidelijk dat Providence als tussenhandelaar in digitale wapens opereert. De Wikileaks documenten bevatten veel informatie en (email) correspondentie van Providence, onder meer over de pogingen om samen te werken het Italiaanse computerbedrijf. De Wikileaks documenten geven een onthullende kijk in de wereld van de tussenhandel.

In 2012 probeert Providence een zakenrelatie aan te gaan met Hacking Team. Eind 2012 schrijft Matt Jamieson (van Providence Australasia) David Vincenzetti en Valeriano Bedeschi van Hacking Team aan. Jamieson introduceert Providence als een wereldspeler: '*Providence Group deliver intelligence consultancy services to government, law enforcement and defence agencies worldwide. We currently have offices in UK, USA, Benelux and Australia.*'

Daniel Maglietta van het Hacking Team kantoor in Singapore neemt vervolgens op 3 december 2012 via Skype contact op met Jamieson. Tijdens dat onderhoud gaat Jamieson verder in op het werk van Providence: '*We provide intelligence consultancy to government departments, using very operationally experienced operators and technicians who are able to provide not only the technical solution, but also the context of how to use the technique. We must develop a pattern of life of the target through surveillance.*'

Volgens Jamieson is Providence beter in staat is om producten te

promoten dan fabrikanten dat kunnen, en heeft Providence contacten op hoog niveau: '*We currently have R&D contracts for DSTL (Defence Science and Technology Laboratory - UK) and also for US DoD - these R&D projects are to deliver new technologies to governments and involve our technicians adapting commercial products for 'other uses'*.'

Maglietta licht nog dezelfde dag zijn bazen in Milaan in over het gesprek: '*Hi guys, This company is formed by ex SAS people from the UK and Australia. I had a 1 hour skype conf and they seem pretty professional. They are mainly focused on training and consultancy on security.*' Maglietta en Jamieson sturen elkaar vervolgens een geheimhoudingsverklaring toe.

Hacking Team wordt een wortel voorgehouden door Providence. Jamieson claimt dat Providence samenwerkt met '*numerous agencies which are looking for alternative technologies to the products which they are currently using.*' Tijdens het Skype-gesprek geeft Jamieson aan dat het hierbij gaat om het Australische leger, met name de Australian Special Forces.

Hacking Team ziet haar kans schoon: '*Hi guys, FYI the client Providence is representing in Australia is the Special Forces from Defence*', schrijft Maglietta. '*Apparently this client is already using Gamma's solution but he is not happy at all with it and asked Providence to contact us. Time for us to defeat competition!*' De baas van Hacking Team antwoordt direct: '*So there! Let's kick their ass!*'

Providence en Hacking Team hebben beiden ambities om de Australische markt te betreden. In de eerste twee weken van december 2012 wordt er dan ook flink over en weer gemaild. Het is duidelijk dat Providence dealer van Hacking Team software wil worden. De Italianen lijken begin januari 2013 overtuigd. Dat komt waarschijnlijk ook omdat Jamieson openhartig is geweest over de Australische Special Forces die volgens hem niet zo tevreden zijn over Finfisher.

Danielle Milan, Operations Manager van Hacking Team, schrijft: '*The training they provide is unconventional, focusing on military intelligence and surveillance. Anyway, for clients that make use of physical infections, it may prove to be a high-value complementary formation.*' De Italianen denken dat ze hun klanten nog wat extra geld uit de zak kunnen kloppen door omgekeerd als bemiddelaar op te treden voor Providence. '*Well worth a try proposing it to some selected clients. Premium price here is*

mandatory! :)', vervolgt Milan.

De Wikileaks documenten bevatten geen verdere correspondentie tussen Hacking Team en Providence. Uiteindelijk gaat deze deal tussen Hacking Team en Providence niet door. De Australische Special Forces komt niet voor op de openbaar gemaakte klantenlijst van Hacking Team.

De pogingen van Hacking Team en Providence om de Australische markt te betreden staan niet op zichzelf, maar zijn illustratief voor de handel in digitale wapens. De markt is klein en, vanwege het beperkte aantal producenten, competitief. Hacking Team en Gamma Group behoorden enkele jaren geleden tot de eerste bedrijven die digitale wapens aanboden. Het lijkt bij de onderlinge concurrentiestrijd te horen om te proberen elkaars klanten af te pakken.

De gang van zaken geeft ook onthullende inkijk in het optreden van de tussenhandelaar Providence. Providence beschikt over relevante en gevoelige informatie, namelijk dat het Australische leger gebruik maakt van de Gamma tool Finfisher, en hier niet tevreden over is. Providence deelt deze gevoelige overheidsinformatie met een andere partij. Het realiseren van de eigen (financiële) belangen van Providence lijkt hiermee voorop te staan, terwijl er vraagtekens geplaatst kunnen worden bij het zo vrijpostig vrijgeven van gevoelige overheidsinformatie.

Marchanderen in Ecuador

Providence probeert Hacking Team ook te interesseren in een samenwerking in Europa. Matt Jamieson vraagt Daniel Maglietta daarom of hij kan zorgen voor een contactpersoon voor zijn collega Peter Stolwerk van het Benelux kantoor van Providence. Stolwerk is eveneens geïnteresseerd in de software van Hacking Team.

Jamieson introduceert zijn collega Stolwerk per email aan Marco Bettini en Massimiliano Luppi. 'P*eter is extremely well connected in Europe and manages a very large area (everywhere other than Poland and Sweden I believe)*', aldus Jamieson.

Op 5 december 2012 hebben Luppi en Stolwerk een telefonische afspraak en wisselen een geheimhoudingsverklaring uit. Binnen Hacking Team wordt gekeken of verdere samenwerking met Providence zinvol is. De Italianen vragen zich af wat Providence, naast de Special Forces in

Australië als potentiële klant, nog meer te bieden hebben.

Stolwerk blijkt niet op de hoogte te zijn van de contacten die Hacking Team al in Nederland heeft. Een daadwerkelijke samenwerking tussen Hacking Team en Providence in Nederland komt daarom in dit stadium niet van de grond.

Stolwerk krijgt begin 2013 wat documentatie van de Italianen. Eind januari 2013 neemt Stolwerk contact op met Hacking Team, want hij ziet naast Europa mogelijkheden in Latijns Amerika. Hij stelt dat er vooruitgang wordt geboekt ten aanzien van marketing voor Hacking Team in Europa, hoewel er nog geen klanten zijn. Hij heeft een deal met Hacking Team voor een klant in Ecuador voor ogen. Hierbij probeert hij een bevriend bedrijf uit het eigen Providence netwerk naar voren te schuiven, en een andere tussenhandelaar van Hacking Team te passeren.

Stolwerk geeft aan als tussenhandelaar op te willen treden voor de verkoop van digitale wapens van Hacking Team aan het Ecuadoraanse leger. '*I just had a skypecall with our office in Equador (Ecuador red.). They are approached by the Equadorian military. They requested a quote from our office for a license for the RMI and Da Vinci (big potential)*', aldus Stolwerk.

Stolwerk noemt in februari 2013 de naam van het bedrijf waarmee Providence in Ecuador samenwerkt: Quimipac SA. '*The company we will use to close the deal with the military is Quimipac.com.ec (but our local people will be involved). This all because of obvious reasons*', aldus Stolwerk (het juiste internetadres van het bedrijf is http://www.grupoquimipac.com.ec).

Met 'our local people' doelt Stolwerk op de broers Hugh Richard en Neil Roderick MacDougall. Zij zijn respectievelijk manager en president van Quimipac.

De broers zijn nauw verbonden aan Providence. Hugh MacDougall is directeur bij zowel Providence Global ITF, Providence Global, Providence UK ITF en HMS Harewood Limited. Neil Macdougall was in de periode 2011-2012 korte tijd directeur van Providence Global ITF Ltd. Hugh en Neil zitten samen met een andere directeur van Providence (Michael William Davis) in het Panamese bedrijf Providence Global Corp., en in Heva Intermediates Corp. en QP, S.A.

Er is echter een probleem. Hacking Team heeft al een tussenhandelaar in Ecuador, namelijk Robotec. Dit private Colombiaanse bedrijf, van Hugo Fernando Ardila en Jamie Cacedo, heeft in het verleden al diverse deals voor de Italianen afgesloten. Zo heeft Hacking Team eerder spyware aan de anti-drugs en de inlichtingen afdeling van de Colombiaanse politie geleverd. Hugo Fernando Ardila zorgde ook voor een grote order in Panama, waar de digitale wapens van Hacking Team werden ingezet tegen de oppositie.

Robotec staat op redelijke voet met Hacking Team. Zo schreef Marco Bettini in augustus 2012 dat Robotec geen prijslijst nodig heeft: '*They know how build the prices*.' Er is echter ook sprake van wrijvingen, want collega Massimiliano Luppi wilde eind 2012 graag meer inzicht in het handelen van de Colombianen: '*I'd like to know exactly from them what they do expect from all these contacts (1½ years ago they said: "we expect to close 2 deals in Colombia by end of 2011").*'

Dit speelde eind 2012. Korte tijd later, begin 2013, komt Stolwerk met een klant bij Hacking Team: het Ecuadoraanse leger. Volgens Stolwerk wil het Ecuadoraanse leger niet met Robotec samenwerken, en hij zegt te weten dat Hacking Team in Ecuador gebruik maakt van Robotec als distribiteur. Robotec heeft in Ecuador echter net (in december 2012) ook al een klant geworven voor Hacking Team: Senain, de in 2009 opgerichte Ecuadoraanse inlichtingendienst.

Providence wacht op een beslissing van Hacking Team. Op 11 februari 2013 laat Stolwerk van Providence merken dat de Britten haast hebben: '*Dear Massimiliano, Sorry for bothering you again. This is normally not my style. I really want to move forward with our customer/project. Please let me know how to proceed.*'

Een dag later antwoordt Luppi of Stolwerk diezelfde dag om drie uur tijd heeft om te bellen. De Wikileaks documenten bevatten geen verdere e-mail correspondentie meer tussen Stolwerk en Hacking Team. De zakenrelatie is door de Italianen afgebroken. Hacking Team benadert Robotec op 23 februari 2013: '*Did the guy from providence contact you about the army counterpart?*' Hugo Ardila antwoordt een dag later: '*We were never been contacted about the Army Intelligence Opportunity.*' Ardila zal naar Ecuador gaan om direct met de klant te gaan praten.

Ook in dit geval lukt het Providence dus niet om een succesvolle samenwerking met Hacking Team aan te gaan. Het Ecuadoraanse

avontuur van Providence geeft echter wederom een inzicht in de wereld van de tussenhandel in digitale wapens. Providence schrikt er niet voor terug om te proberen een tussenhandelaar van Hacking Team af te pakken. En Providence maakt van de mogelijkheid gebruik om een bevriend bedrijf te betrekken en hiermee haar eigen mensen te verrijken.

Het roept vragen over de bedrijfsethiek van Providence. En het stemt nieuwsgierig naar de klantenkring van het bedrijf.

Providence treedt niet in de openbaarheid over haar klantenkring. Volgens haar website wil Providence vooral een bijdrage leveren aan de internationale strijd tegen terrorisme: *"The company's offerings are intended to serve government, defence and law enforcement agencies internationally in the global war on terrorism."*

Het is de vraag hoe een zakenrelatie met het Ecuadoraanse leger hierin past. In 2013, toen Providence bezig was met haar pogingen om zaken te doen met Ecuador, Verschenen rapporten van Amnesty International en Human Rights Watch over de mensenrechtenschendingen jegens inheemse volkeren door de Ecuadoraanse overheid en haar veiligheidsapparaat.

Providence en de Nederlandse politie

Bovenstaande twee pogingen van Providence om te infiltreren in Australische en Ecuadoraanse markt vormen geen succesvolle business case. In andere landen en op enkele andere terreinen heeft Providence wel geluk.

Uit de Wikileaks documenten blijkt dat Providence distribiteur is van de Kailax Unlocker. Met deze tool kunnen computers worden ontgrendeld met een USB-stick, zonder dat er veel sporen worden achtergelaten. Kailax is van een Israëlisch bedrijf dat helemaal geen informatie geeft over haar economische integriteit en haar klanten op haar website. Het bedrijf doet het zelfs voorkomen dat het een Singaporees bedrijf is.

Over de klantenkring van Providence is weinig bekend. De website van Providence geeft hierin geen nader inzicht. Wel is bekend dat Nederland zaken doet met Providence. In antwoord op het WOB verzoek van Buro Jansen & Janssen antwoordt de Nationale Politie dat het 39 diensten / producten van Providence heeft afgenomen, al maakt men niet openbaar

op welke data deze diensten zijn afgenomen en wat men precies heeft aangeschaft. Tevens geeft de Nederlandse politie niet aan met wie van de Providence groep wordt samengewerkt. De Nederlandse tak, een van de Britse bedrijven of de vestiging in Panama.

Boeven vangen met dubieuze software van dubieuze bedrijven

Providence en de politie; Ketenaansprakelijkheid via een ex-agent

Kailax/Nir (Max) Levy; De magische hand van de Israëlische inlichtingendienst

Providence en de politie; Ketenaansprakelijkheid via een ex-agent (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Providence Group power point presentatie

Providence bedrijfsschema

Enkele emails Hacking Team providence 2010 - juni 2015

Enkele emails Hacking Team providence juni 2015 deel twee

Enkele emails Hacking Team providence juli 2015

Invitation to Workshops Exhibition and BBQ van Providence

Map and Directions van Providence

Registration form signed Hacking Team voor Providence event

Naar inhoudsopgave Observant #69

Kailax / Nir (Max) Levy
De magische hand van de Israëlische inlichtingendienst

De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De *Unlocker* is een tool waarmee een inbreker zich toegang kan verschaffen tot een Windows computer, zonder dat de eigenaar dit in de gaten heeft.

Over de *Unlocker* en het producerende bedrijf Kailax is nauwelijks openbare informatie beschikbaar. De website www.kailax.com bevat alleen de adresgegevens van het bedrijf (een adres in Singapore), maar geen verdere informatie. Uit openbare bronnen kan alleen worden opgemaakt dat het in Berlijn gevestigde bedrijf 2beuropa als tussenhandelaar voor Kailax fungeert.

Pas met de openbaar making van de Wikileaks documenten over Hacking Team in 2015 is er meer inzicht gekomen over het bestaan van de Kailax *Unlocker* en de handel in deze tool. De Kailax *Unlocker*, soms aangeduid als *Unlocker/U-cap* blijkt een gewild digitaal wapen. Volgens de producent, die zich in e-mails afwisselend Max en Nir Levy noemt, levert Kailax de *Unlocker* aan zeventig landen.

Of dit waar is, valt niet te controleren. Wat wel duidelijk wordt uit de Wikileaks documenten is dat het Italiaanse computerbedrijf Hacking Team interesse heeft om de *Unlocker* aan haar assortiment toe te voegen. Het belandt hiervoor bij het Britse bedrijf Providence, dat als tussenhandelaar de *Unlocker* blijkt aan te bieden.

De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De herkomst van digitale wapens is vaak onduidelijk, hetgeen de vraag oplevert of overheden en veiligheidsdiensten wel weten wat voor product ze kopen en met welk bedrijf ze in zee gaan. De bemoeienis van een tussenhandelaar als Providence draagt bij aan de ondoorzichtigheid en onveiligheid.

Buro Jansen & Janssen deed een digitale zoektocht naar de herkomst van de *Unlocker*. Deze leidt naar Israël. De Kailax *Unlocker* blijkt van

Israëlische afkomst te zijn, voormalig leden van de Israëlische veiligheidsdienst zijn betrokken.

Hacking Team en Kailax

Uit de in 2015 gepubliceerde Wikileaks documenten wordt duidelijk dat het Italiaanse bedrijf Hacking Team begin 2015 interesse heeft om de Kailax *Unlocker* aan te schaffen. Met deze *Unlocker* verschaft een inbreker zich toegang tot een Windows computer zonder in te loggen en zonder dat de eigenaar dit in de gaten heeft. Het gaat hierbij om Windows Vista/7/8/8.1 Server 2008/Server 2012- 32/64 bit.

Hacking Team gebruikt eenzelfde soort techniek voor zijn Tactical Network Injector (TNI) voor Firewire. In een 'Statement of Work' schrijft Nir Levy (Max) van het producerende bedrijf Kailax dat het product '*a handheld unit is that once plugged into any USB port of locked windows PC, will automatically execute at system rights a propriety payload on the target PC.*' Het laat volgens Kailax weinig sporen achter op de computer van het slachtoffer.

De Italianen beschouwen de *Unlocker* als een aanwinst voor hun digitale inbrekerskit. Het is misschien een optie om de tool zelf te ontwikkelen, maar zonder een prototype lijkt dit voor de Italianen een stap te ver. Hacking Team probeert de tool eerst te verkrijgen via het kantoor van Kailax in Singapore, maar er volgt geen antwoord op het verzoek.

Op 23 januari 2015 vraagt Walter Furlan in een interne mail aan enkele werknemers van Hacking Team of zij de Kailax *Unlocker* kennen. Een Zwitserse klant van de Italianen, de Kantonspolizei Zürich heeft de *Unlocker* gekocht van 2beuropa. Ook een andere klant, de Raggruppamento Operativo Speciale (ROS, Special Operations Group) van de Italiaanse militaire politie, heeft de *Unlocker* aangeschaft bij 2beuropa.

Giancarlo Russo van Hacking Team neemt hierop contact op met Rami Zoltak van 2beuropa. Dit in Berlijn gevestigde bedrijf opereert als distribiteur van Kailax. Zoltak antwoordt echter dat 2beuropa alleen met overheden handelt: '*We are working only with governmental offices, we are unfortunately unable to assist.*'

De Italianen blijven echter aanhouden. Russo bluft dat een 'LEA client' (Law Enforcement Agency) interesse heeft in de *Unlocker*.

Uiteindelijk reageert Max, die in de eerste mails nog ondertekent met Kailax Sales. Max zegt dat de klant van Hacking Team enkel een USB *Unlocker* kan aanschaffen via de officiële dealer van Kailax. Hij vermeldt er echter niet bij wie deze dealer is.

Russo probeert Max nog een keer te overtuigen maar Kailax blijft weigeren. Er komt wel steeds meer informative over de tool vrij: '*The Unlocker is a self-contained sealed and secure hand held unit that does one thing and one thing only, bypasses windows passwords and gives system rights on the locked live PC.*' Volgens Max is de *Unlocker* aan ruim zeventig landen verkocht.

Max geeft Hacking Team één optie, namelijk dat Hacking Team de *Unlocker* op haar systeem installeert voor waarmee de tool onbeperkt kan worden gebruikt. Hij vraagt Russo om de garantie dat niemand anders toegang krijgt tot het IP-adres van Kailax: '*you also have to convince and assure us that no one else but you will have access to our IP.*' Max ondertekent nu als Nir Levy (Max)

De Italiaan en Max mailen nog een tijdje met elkaar, maar veel schot lijkt er niet te komen in de zaak. Max houdt de boot af: '*We are both manufacturer suppliers of technology we are in essence competitors*', schrijft hij. '*As you must know we are in same niche market that is usually based on trust*.'

Max stelt nog wel een tussenoplossing voor. Hacking Team kan als een soort onderaannemer fungeren, die uitsluitend een zwarte doos aan haar klanten kan verkopen: '*Option 1 is feasible only if you are prepared to supply to customers as a sub distributer black box technology which you do not own, have no deal understanding of the IP or maintain.*'

De Italianen zien het niet zitten en besluiten om enkele van hun eigen klanten te vragen een Kailax *Unlocker* voor Hacking Team aan te schaffen. Russo benadert daarvoor probeert het nu via de Zwitserse politie, de Kantonspolizei Zürich. De Zwitsers reageren niet dus proberen de Italianen het bij een Italiaanse klant, de Raggruppamento Operativo Speciale (ROS, Special Operations Group) van de Italiaanse militaire politie. Hacking Team vraagt de ROS om twee *Unlockers* te bestellen,

maar de militaire politie lijkt niet al te happig om zich voor het karretje van Hacking Team te laten spannen.

Providence komt in beeld

Begin maart 2015 loopt het contact tussen Hacking Team en Kailax spaak. Hierop zoeken de Italianen toenadering tot het Britse bedrijf Providence. Beide bedrijven kennen elkaar, en probeerden in de voorafgaande jaren een samenwerking in Australië en Ecuador tot stand te brengen waarbij Providence als tussenhandelaar voor producten van Hacking Team wilde fungeren

Providence claimt een eigen tool, 'de *'Windows Unlocker* en *U-Cap*', in haar assortiment te hebben. Deze voorziet in eenzelfde behoefte als de Kailax *Unlocker*. De Kailax *Unlocker* wordt soms ook aangeduid als *Unlocker*/*U-Cap*. Op 18 maart 2015 geeft Providence tijdens de ISS World MEA in Dubai een presentatie onder de titel 'Tactical Bypass of IT Security', die door medewerkers van Hacking Team wordt bijgewoond.

Een week later schrijft Giancarlo Russo van Hacking Team aan Steve Minto van Providence dat de Italianen geïnteresseerd zijn in het bespreken van een zakenrelatie. Russo mailt op 8 april 2015: '*My colleagues visited your booth in Dubai last week and they reported me positive impression about your USB tool for launching payloads on PCs*. *As you might know, we are active in more than 30 countries providing IT Offensive technology exclusively to many LEA/Intelligence agencies and we think that your USB might be useful for many of our countries*.'

Nog dezelfde dag antwoordt Peter Stolwerk van Providence dat hij zeer geïnteresseerd is in een mogelijke samenwerking met Hacking Team ten aanzien van de *'Windows Unlocker and U-Cap* (the special add-on for the *Unlocker*).' Providence maakt in dit stadium van de onderhandelingen nog niet duidelijk dat het de *'Windows Unlocker en U-Cap'* niet zelf heeft ontwikkeld.

Stolwerk reist af naar Milaan voor een presentatie. Deze verloopt echter niet vlekkeloos. De Italianen merken op dat de *Unlocker* sporen achter laat: '*Regarding the product I would like to have a feedback regarding the behavior we experienced during the demo (pop-ups on unlocked PC)*.'

Russo een schrijft verslag van de bijeenkomst en stuurt dit Stolwerk op. Russo en Stolwerk hebben het tijdens hun overleg gehad over '*Partnership on Training programs for HT Clients. Social Engineering and how to get increasing benefit from HT technologies in real case operations.*'

Uit het verslag blijkt dat Hacking Team Providence een deal wil aanbieden. Het accepteert Providence als een soort distribiteur, in ruil voor de USB *Unlocker*: '*The U-cap + Unlocker product to be added to Hacking Team's solution for its customers needing an additional tool to deliver payload during Physical infection.*'

Providence mag als tussenhandelaar producten van Hacking Team verkopen en klanten trainen het beste uit de cyberwapens te halen: '*Providence Group can offer and provide training, workshops and assistance to Hacking Team's end-users in order to help them maximize the efficiency of their attacks, to be either physical (covert installation, intrusion), tactical through WIFI (close to target training, mimicry) or remote (Social Engineering)*.' Ook mag Providence softwareproducten van Hacking Team aan haar klanten aanbieden: '*Providence would play more the role of an agent/consultant, rather than a distributor*'.

Bij de '*Unlocker + U-cap*' willen de Italianen echter Providence omzeilen en het liefst alle mogelijkheden in handen hebben om het product aan hun assortiment toe te kunnen voegen. '*Regarding the cooperation we feel that the first, easiest and fastest, way to cooperate is to include the USB Unlocker into our portfolio*', laat Russo aan Stolwerk weten.

Tijdens de bijeenkomst in Milaan wordt echter langzamerhand duidelijk dat Providence niets te zeggen heeft over de USB *Unlocker*. Stolwerk moet steeds terug keren naar de producent die hij slechts één keer bij naam noemt: 'Max'. Russo van Hacking Team schrijft na de bijeenkomst in Milaan, waar Max blijkbaar ter sprake is gekomen: '*I expect you and Max to elaborate more on which cooperation options you consider viable*'. Stolwerk zegt dat hij Max gesproken heeft: '*Agreed, I spoke to Max and he is positive that we will together find a solution on this.*'

Hacking Team heeft begin 2015 ook al direct contact gehad met Max over de mogelijke aanschaf van de *Unlocker*. Opvallend genoeg blijkt uit

de correspondentie in de Wikileaks documenten niet of de Italianen zich dit beseffen, of dat zij Providence hiervan op de hoogte stellen.

Werving nieuwe klanten

Hacking Team wordt uitgenodigd om het kantoor van Providence in Hereford in mei 2015 te bezoeken en de samenwerking verder te bespreken. Het Engelse bedrijf is gretig en vraagt Hacking Team onder meer of het bereid is om een defensieve cyberoorlog training te geven aan twintig mensen uit het Midden-Oosten. Het lijkt erop dat Providence nog niet helemaal door heeft wat de Italianen nu eigenlijk doen. Een telefonisch onderhoud moet de Engelsen vervolgens duidelijk maken dat Hacking Team uitsluitend digitale wapens verkoopt.

De Italianen zijn, naast de acquisitie van de 'U-cap + *Unlocker*', ook geïnteresseerd om via Providence nieuwe klanten te werven: '*We should go to Hereford and take advantage to visit them and also perform a demo for their sales team*', schrijft Vinci van Hacking Team.

Vinci suggereert ook een bijeenkomst te organiseren met het Britse Ministerie van Defensie: '*There is a big MOD field camp in Hereford. We can try to organize a meeting with MOD (Ministry of Defence)*'. Hacking Team hoopt dat Providence iets kan betekenen richting het Britse Ministerie. Er zijn echter ook andere potentiële tussenhandelaren zoals Bob Quick van BlueLight Global Solutions. Naast het Ministry of Defence zijn er ook andere potentiële klanten zoals de National Crime Agency en BAE Systems, een grote militaire wapenproducent.

Het cursus- en trainingsaanbod van Providence is voor de Italianen minder interessant. Vinci mailt: '*a training on how to enter into a home and defeat an alarm :-), can be certainly useful for our customers to do physical infections, (…) but we won't put this training in our catalogue.*'

De Italianen houden erg de boot af en Providence als tussenhandelaar lijkt nog een lange weg: '*I suggest that you provide us with 1 or 2 'low hanging fruit' we could start the collaboration on and add more accounts as we progress. Benelux would be a nice test for our cooperation in addition to the MOD intelligence in the UK for example.*'

De Italianen stellen Providence voor dat, wanneer zij distributeur willen worden voor Hacking Team, zij om te beginnen een aantal gemakkelijke

klanten moeten aanleveren. Wanneer Providence echter zelf op jacht wil gaan naar klanten dient zij de gegevens door te geven aan Hacking Team, dat vervolgens bepaalt of de Engelsen mogen handelen. De ervaring leert namelijk dat sommige klanten al bezet zijn door een andere tussenhandelaar. Dit was bijvoorbeeld het geval in Ecuador, waar Providence met een bedrijf kwam, terwijl Hacking Team al via een ander bedrijf (Robotec) zaken deed in het land.

Beet of toch niet

Op 8 mei 2015 wordt de verhouding tussen Max en Providence duidelijk. Stolwerk: '*The manufacture will only allow you to purchase the Unlocker & u-cap via his regional distributors. We cover a large part of the world but for parts that we don't cover you have to make arrangements with the regional distributor that covers that area.*'

Providence heeft Max kennelijk weten te overtuigen. Volgens Stolwerk is Providence de distributeur van *Unlocker* voor een groot deel van de wereld. Hij maakt echter niet duidelijk voor welke van de zeventig landen, waarvan Max beweert dat de Kailax USB stick aan wordt geleverd, Providence als tussenhandelaar opereert. Het andere deel verloopt via lokale distributeurs zoals 2beuropa.

Kailax is bereid om voor Hacking Team een speciale versie van de '*Unlocker*/*U-cap* combination' te maken. De ontwikkeling hiervan komt voor rekening van de Italianen. Eigenlijk kan een succesvolle bijeenkomst in Hereford niets meer in de weg staan. De Italianen presenteren daar hun pronkstuk de Galileo RCS (Remote Controle System) en willen graag het volledige repertoire van de Engelsen zien, '*in particular the training and workshop around cyber, covert entry, installation, surveillance, getting close to the targets, etc*.'

De communicatie tussen Hacking Team en Providence, met name Peter Stolwerk, gaat de hierop volgende maanden vooral over de *Unlocker*. De Italianen zeggen een klant te hebben voor de Kailax USB stick en willen weten hoe zij die tevreden kunnen stellen. Giancarlo Russo van Hacking Team zegt dat het om een Italiaanse opsporingsdienst gaat en dat Max de dienst al kent.

Stolwerk wil de Italianen ook graag behouden als mogelijke partner en schrijft dat er in Nederland interesse bestaat voor de producten van

Hacking Team: '*I will speak to the guys here as I have some good news about the Netherlands for your products.*'

De Italianen lijken echter nog niet volledig overtuigd van de kwaliteiten van Providence. Eind mei 2015 schrijft een Hacking Team medewerker, na het bestuderen van de presentaties van de Engelsen: '*Still have to read all documents carefully, but all of them have been written on January 2015 (versions 1.0), so it seems they're recently organizing contents. P.S. All their e-mail addresses on the last pages are wrong*.' Bij Providence zijn ze kennelijk begin 2015 begonnen met het opstellen van hun trainingen, bestaan dus net en hun e-mail adressen kloppen niet.

Providence en Hacking Team zijn dichtbij een overeenkomst. De Italianen worden zelfs uitgenodigd voor een exclusieve bijeenkomst van Providence op 26 augustus 2015. Op het terrein in Hereford is een kleine markt met workshops en een barbecue georganiseerd. Naast Hacking Team zijn Tac Up (van Providence), Claresys Covert Video Surveillance (van het Britse Ministerie van Defensie), en nog twintig andere bedrijven, uitgenodigd waaronder Cobham, Eomax, Sentinor. Allemaal 'vrienden' van Providence.

Uit de Wikileaks documenten wordt niet duidelijk of Hacking Team de *Unlocker* uiteindelijk aan haar assortiment heeft toegevoegd. In juli 2015 wordt Hacking Team getroffen door een hack en worden interne documenten over het bedrijf gepubliceerd door WikiLeaks. Ook komt het Italiaanse bedrijf onder vuur te liggen vanwege de levering van digitale wapens aan repressieve regimes en verliest het haar exportvergunningen voor handel buiten de Europese Unie.

Kailax - Mhyli

De correspondentie tussen Hacking Team en Providence geeft een onthullend inzicht in de wereld van de tussenhandel in digitale wapens. De Kailax *Unlocker* is illustratief voor de geheimzinnigheid en ondoorzichtigheid van de handel in digitale wapens. De herkomst van digitale wapens is vaak onduidelijk, hetgeen de vraag oplevert of overheden en veiligheidsdiensten wel weten wat voor product ze kopen en met welk bedrijf ze in zee gaan. De bemoeienis van een tussenhandelaar als Providence draagt bij aan de ondoorzichtigheid.

Over het bedrijf Kailax is nauwelijks openbare informatie bekend. Het

bedrijf heeft een website (www.kailax.com). Volgens welke het bedrijf is gevestigd onder de naam Kailax in Singapore: Kailax PTE LTD op 129 Lower Delta Rd. #09-03 Cendex Center. Op de website zijn twee zinnen te lezen, 'We provide solutions in the cyber security domain' en 'For details please contact us at info@kailax.com'. Verder staat er op de website geen informatie over producten, expertise, omzet, investeerders, klanten, etc.

Kailax is zelf nooit aanwezig op de verschillende beurzen voor digitale wapens of ISS World. Het verkoopt via het bedrijf 2beuropa. Het bedrijf 2beuropa wordt gerund door Rami Zoltak en is gevestigd in Berlijn aan de Mittenwalder Strasse. Zoltak komt uit de vastgoedwereld en handelt in allerlei producten waaronder digitale wapens zoals ook van Kailax.

Op de website van 2beuropa staat dat het bedrijf handelt in 'taktischen Überwachung beste High-End-Hardware- und Softwareprodukte.' Het gaat om surveillance, tactische surveillance en hoogwaardige hardware en software producten. Bij producten gaat het echter ook om een veiligheidskoffer voor een VIP, drugs testen, stinkende spray als openbare orde middel, containers voor de vervoer van explosieven

Op de website van 2beuropa wordt Kailax als partner genoemd sinds de nieuwe website in 2014 online is gegaan.

De website maakt echter niet duidelijk wat voor producten Kailax te bieden heeft. Wat opvalt is dat de winkel van Rami Zoltak uitsluitend Israëlische producten aanbiedt. Alle partners zijn Israëlische bedrijven die verbonden zijn aan de IDF, het Israëlische leger. 2beuropa geeft op haar website aan dat haar partners de volgende bedrijven zijn: Towersec, Karil International, Touch&Know, iDenta, Septier, ITP Novex, Memtex, Prosecs, ODF Optronics, ODI-X en Pro4tech. Kailax staat daar tussen en het is aannemelijk dat het een Israëlisch bedrijf is.

Max – Nir Levy - Mhyli

Namens Kailax wordt gecorrespondeerd door Max. Ook gebruikt Max in de correspondentie met Hacking Team de naam Nir Levy, maar het is niet bekend of dit zijn echte naam is. De Kailax website bevat geen verdere informatie over Max en/of Nir Levy. Uit de Wikileaks documenten ontstaat de indruk dat Max / Nir Levy de belangrijkste persoon is binnen Kailax.

Buro Jansen & Janssen heeft getracht informatie te achterhalen over Max / Nir Levy. Het lijkt hier om één persoon te gaan. Hij gebruikt het e-mailadres max@kailax.com.

Aan dit adres is nog een aantal domeinen gekoppeld. Het gaat hierbij om: s-mic.com, k-mic.info, *Unlocker*-u.com en toplucktrading.com. Deze sites werken allemaal niet, behalve de *Unlocker*-u.com die verwijst naar kailax.com. Toplucktrading houdt geen kantoor in Singapore, maar in Hong Kong, op het adres: Unit 1203 12F CEO Tower, Admin Street: 77 Wing Hong St Cheung Sha Wan, Kowloon.

Een digitale zoektocht naar Max en Nir Levy levert niet veel informatie op. Een uitdraai van de domeinnamen op naam van Nir Levy levert wel een interessant pallet op. Er zijn meerdere vele Nir Levy's: de meesten zijn Israëli, een enkeling woont in de Verenigde Staten. Bij de bovenstaande domeinen, zoals *Unlocker*-u.com, wordt Nir Levy als onderdeel vermeld van Kailax, met het e-mail adres max@kailax.com. Er bestaan echter andere domeinnamen op naam van deze Nir Levy, die gelinkt zijn aan een voormalig medewerker van de Israëlische geheime dienst.

Domeinnamen

Van alle Nir Levy's die domeinen hebben geregistreerd, zijn er maar twee die (net als max@kailax.com) de naam Max gebruiken. Het betreft een Nir Levy met het e-mail adres max@mknowlegde.com, en een Nir Levy met het adres max@mhyli.com.

Beide Maxen blijken betrekking te hebben op dezelfde Nir Levy, die als als adres opgeeft: 7 shamir, hod hasharon in Israel, telefoonnummer +972.97480608. Deze gegevens hebben betrekking op de volgende websites: mknowledge-demo.com en mknowledge.com (gekoppeld aan het e-mail adres max@mknowledge.com) en mknowledge.info, smthid.com en mhyli.com (gekoppeld aan het e-mail adres max@mhyli.com).

Max van Kailax en de Max van 'mknowlegde' en 'mhyli' zijn dus dezelfde persoon. Er zijn geen andere Nir Levy's die de naam Max gebruiken. Daarnaast zijn de mknowlegde-websites even ontoegankelijk als de websites van Kailax.

Opvallend is de kleine presentatie van Max op de website van Mhyli. Hij vermeldt hier dat hij tevens directeur is van Pro4Tech, een producent van tactische video-observatie oplossingen. (Pro4Tech is ook aangesloten bij het bedrijf 2beuropa, dat ook als tussenhandelaar voor Kailax optreedt) Ook schrijft Max op de Mhyli website dat hij CEO is van EDM, een bedrijf dat informatie van het internet geautomatiseerd vergaart. Volgens de Mhyli website: '*Nir also holds the position of Director at Pro4Tech, a company manufacturing innovative Tactical Surveillance Video solutions. Nir is also founder and C.E.O. in EDM, a company dealing in automation of internet information gathering*.'

De reden waarom Nir Levy (Max) zo geheimzinnig doet over zijn achtergrond, heeft te maken met zijn carrière voordat hij in het bedrijfsleven stapte. Max heeft namelijk 25 jaar voor de Israëlische inlichtingendienst gewerkt. De Mhyli website vermeldt: *'Before founding Mhyli, Nir served for 25 years in the Israeli Intelligence Community. During his time there, Nir commanded a variety of teams and projects, in his last post Nir headed a division specializing in computing and communications.'*

Dit is zeer opvallend. Op de website van Kailax ontbreekt enige achtergrondinformatie over Max of Nir, maar op de Mhyli website is hij een stuk openhartiger over zijn achtergrond: *'He also completed various managerial technical and command courses in the Prime Ministers Office, including the Senior Commander course.*'

Ook zijn collega bij Mhyli, Daniel Kario, blijkt een verleden te hebben bij het Israelische leger. Volgens de website heeft hij gewerkt als '*group leader in a leading technological unit of IDF.*' (Israëlische Defense Forces)

Het valt niet vast te stellen of Kailax een zelfstandig bedrijf is en alleen door Nir Levy wordt gerund. De website van Kailax bevat hierover geen enkele informatie. De website maakt evenmin duidelijk of Nir Levy en Daniel Kario gespecialiseerde IT-ontwikkelaars zijn en die de tool zelf in elkaar hebben gezet.

Dat de Max van Kailax en de Max van Mhyli dezelfde persoon zijn, is met het oog op de geheimzinnigheid rond Kailax meer dan logisch. Wie wil er nu een digitaal wapen kopen van een voormalig medewerker van de Israëlische inlichtingendienst? In sommige landen zal er grote twijfel ontstaan bij het in zee gaan met Kailax, zodra bekend is dat het hier een

Israëlisch bedrijf betreft, en al helemaal als daarbij contacten met de Israëlische inlichtingenwereld een rol spelen.

Geen zicht op afkomst *Unlocker*

Buro Jansen & Janssen concludeerde in 2011 in een onderzoek naar de relatie van Nederland met de Israëlische veiligheidsindustrie dat de Israëliërs op allerlei manieren proberen voet aan de grond te krijgen in Nederland en Europa. Hierbij gebruiken zij de oorlog in de bezette gebieden als ervaringsbewijs in de reclame voor hun producten. Tegelijkertijd proberen zij hun relatie met Israël te verdoezelen door het opzetten van buitenlandse zuster- of dochterondernemingen die de handel met bepaalde landen op zich nemen.

Het bedrijf Kailax past in dit profiel. Het is aannemelijk dat Kailax aan aan vergelijkbare landen / klanten levert als Hacking Team en Gamma Group/Finfisher, al dan niet met Providence als tussenhandelaar. Het is sterk de vraag of de afnemers van de Kailax *Unlocker* de achtergrond van het bedrijf, haar werknemers, investeerders en klanten kennen.

Deze vraag is ook relevant met betrekking tot Nederland. In antwoord op het WOB verzoek van Buro Jansen & Janssen maakt de Nationale Politie bekend dat het 39 producten of diensten van Providence heeft afgenomen. De politie maakt echter niet openbaar wat het precies van Providence heeft gekocht. Het is aannemelijk dat de Kailax *Unlocker* is aangeschaft.

Providence is een jonge speler op de veiligheidsmarkt. Het Britse bedrijf biedt trainingen, accommodatie en apparatuur aan. De Nederlandse politie kan voor trainingen gebruik maken van eigen trainers en trainingscentra. Veel apparatuur wordt door de politie ingekocht bij reguliere leveranciers als Cellebrite, Nice-Systems en andere bedrijven, vraag is of Providence met haar aanbod iets beters in handen heeft.

De Nationale Politie verklaart in antwoord op het WOB verzoek dat het belang van opsporing geschaad zou worden door meer informatie over Providence openbaar te maken. Deze redenering is moeilijk toepasbaar op het reguliere Providence aanbod aan trainingen en apparatuur, omdat deze niet zozeer voor opsporingsdoeleinden zijn bedoeld. Het argument over het schaden van het belang van de opsporing is wel van toepassing op digitale wapens.

In de afwijzing van het verzoek staat expliciet vermeld dat het bij Providence op individuele basis iets wordt afgenomen. ‘Dit betekent dat zij worden afgenomen op het moment dat de desbetreffende afdeling een bepaald middel nodig heeft voor de politie- en/of opsporingswerkzaamheden,’ staat in het antwoord van de politie. Dit lijkt op geen enkele manier van toepassing op de trainingen en apparatuur uit het Providence aanbod, maar wel op de Kailax Unlocker.

Met de Kailax *Unlocker* kunnen computers ontgrendeld worden waarbij gebruik wordt gemaakt van een internet verbinding. Max / Nir Levy geeft in de correspondentie met Hacking Team aan dat hij ze een zwarte doos aanbiedt waarbij de techniek en het IP adres van de server van de *Unlocker* worden verhuld. '*Option 1 is feasible only if you are prepared to supply to customers as a sub distributer black box technology which you do not own, have no deal understanding of the IP or maintain.*'

Als de Nederlandse politie de Kailax *Unlocker* gebruikt zou Nederland wel eens een tweede Israëlische zwarte doos in huis hebben gehaald. Die nog ondoorzichtiger is dan de afluistercentrales van Nice Systems die Nederland eerder heeft aangekocht. En waarvan de minister van Veiligheid en Justitie in februari 2016 heeft aangegeven dat er meer duidelijkheid over het functioneren van de apparatuur moet komen. 'Bij de vele telefoontaps die de politie uitvoert, is de leverancier van de afluisterapparatuur nauw betrokken. Maar essentiële informatie over de taps, wordt door diezelfde leverancier niet gedeeld. ‘Er is geen garantie dat de politie volledig zicht heeft op alle storingen in het tapsysteem’ (NOS, 12 februari 2016).'

Besluit Nationale politie op Wob verzoek over onder andere Kailax

Boeven vangen met dubieuze software van dubieuze bedrijven

Providence en de politie; Ketenaansprakelijkheid via een ex-agent

Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens

Providence en de politie; Ketenaansprakelijkheid via een ex-agent (pdf)

Bedrijfsprofiel Providence/Turner, Holmes, Stolwerk; SAS tussenhandelaar van inbrekers-kits tot digitale wapens (pdf)

Inleiding Boeven vangen met dubieuze software van dubieuze bedrijven (pdf)

Security Industry: links between Israel and the Netherlands? an inventory

Wikileaks Hacking Team documenten

Enkele e-mails uit HackingTeam gegevens over 2beuropa

Enkele e-mails uit Hacking Team over Kailax

Statement of Work Hacking Team en Kailax

Naar inhoudsopgave Observant #69

‘Je weet maar nooit’
Na privacy en de onschuld, is nu ook de veiligheid dood

De Nederlandse overheid propageert geheimzinnigheid rond digitale wapens en 'zero-days', een zorgelijke ontwikkeling die als een boemerang de Nederlandse economie en veiligheidsdiensten zal treffen. Want als de laatste decennia iets hebben duidelijk gemaakt, is dat overheden de digitale revolutie niet in de hand hebben.

Elke zomer is het raak. De politie breekt in bij burgers en laat 'witte voetjes' achter indien blijkt dat de woningen niet goed zijn afgesloten. De actie vond in 2015 plaats in Wassenaar, dit jaar, 2016, in Leiden en Noordwijk. De politie zegt dat het goed bedoeld is, want mensen moeten opletten. Sluit deuren en ramen voor het gevaar, de inbrekers. Of deze acties zin hebben, effectief zijn, mensen eerder de stuipen op het lijf jagen dan een gevoel van veiligheid geven, het is onduidelijk. De politie wil dienstverlenend zijn en breekt daarom in om aan te tonen dat mensen hun veiligheid niet op orde hebben.

De 'witte voetjes' acties hebben veel weg van de voorlichting eind vorige eeuw over beter hang- en sluitwerk, ze gaan alleen een stap verder. Gebrekkige regelgeving zorgde er destijds voor dat inbrekers hang- en sluitwerk tegenkwamen dat al open gingen als je er maar naar keek. De overheid had verzuimd strengere regelgeving in te voeren waarmee uitsluitend deugdelijk sluitwerk op de markt toe wordt gelaten. De politie werd voorlichter van beter hang- en sluitwerk. Inbrekers oppakken was onbegonnen werk, bewoners moesten voortaan voor hun eigen veiligheid gaan zorgen.

Handhaving digitale kwetsbaarheid

De situatie van destijds in relatie tot fysieke beveiliging herhaalt zich nu in de digitale wereld. De overheid verzuimt duidelijke regelgeving in te voeren en te handhaven aan de hand waarvan de veiligheid van burgers serieus wordt genomen. Daarentegen propageert zij maatregelen en werkt nauw samen met bedrijven die de veiligheid van het internet ondermijnen. Het is niet zozeer dat de politie achter de feiten aanloopt bij cybercriminaliteit. Politie, OM en het Ministerie van Veiligheid en

Justitie propageren geen serieuze veiligheid van het internetgebruik, zij houden de digitale kwetsbaarheid in stand.

Argument hiervoor is dat boeven en terroristen moeten worden gevangen. Die zouden via beveiligde netwerken communiceren over hun snode plannen. Of het afluisteren van die informatie uiteindelijk een belangrijke bijdrage levert aan de veiligheid in Nederland is allang geen vraag meer. De overheid wil zo zicht houden op de kwaadwillenden. Dat het beleid daarmee onveiligheid stimuleert lijkt geen punt. Lapwerk als het 'witte voetjes' programma moet de burger gerust stellen.

De analogie met het slechte hang- en sluitwerk uit de vorige eeuw gaat nog verder. De overheid wil namelijk te allen tijde zicht houden op de boefjes. Wie dat zijn is allang geen vraag meer. Om schurken en terroristen te vangen moet er namelijk soms ingebroken worden via het internet. Zodra woningen en bedrijfspanden onneembare vestingen zijn geworden, kost het opsporings- en inlichtingendiensten ook meer tijd om de percelen binnen te komen om verborgen camera's op te hangen, afluisterapparatuur en andere technische middelen te installeren. Dat slechte sloten iedereen treft, is niet van belang. Politie- en inlichtingendiensten willen zicht houden op de inwoners van dit land.

Fysiek inbreken in woningen is echter een stuk arbeidsintensiever dan digitaal inbreken op smartphones. Voor criminelen en politie zou het onbegonnen werk zijn om miljoenen deuren open te breken en de ruimten te scannen op waardevolle goederen of interessante informatie om mensen af te persen. Digitaal is dat allemaal minder arbeidsintensief. Vanachter het bureau in Driebergen of Katwijk kan zo in korte tijd een schat aan informatie worden verzameld uit slecht beveiligde communicatie of opslag van digitale hulpmiddelen.

Dood van de veiligheid

De dood van de veiligheid is de derde stap in de ontmanteling van de rechtsstaat en volgt daarmee privacy en onschuld. In maart 2008 publiceerde Buro Jansen & Janssen (J&J) het artikel 'Niet de privacy maar (...) de onschuld is dood'. In de eerste alinea werd verwezen naar de ranking van Nederland op de privacyladder van Privacy International:

'In het jaarrapport van de NGO Privacy International wordt Nederland afgeschilderd als een staat waar het met de privacy slecht is gesteld.

Nederland staat onderaan hun ranglijst van privacy schendende staten. De plaats op de lijst is een gevolg van de stortvloed van genomen maatregelen die het niet zo nauw nemen met de bescherming van persoonlijke levenssfeer van Nederlandse burgers. Politici en opsporings- en inlichtingendienstambtenaren zeggen dat het inleveren van onze privacy de prijs is die wij voor een veilige samenleving moeten betalen. Maar is dat wel zo?'

Eind jaren '80, begin jaren '90 veranderde het denken over criminaliteit. Eenduidige oorzaken van die verandering zijn niet direct aan te wijzen. Vaak wordt verwezen naar de val van de Muur, de opkomst van criminele organisaties uit het Oosten en migratie. De drugssmokkel was toentertijd echter niet in handen van Oost-Europese criminele organisaties en in de jaren '70 en '80 vond er ook georganiseerde criminaliteit plaats. Wel nam de migratie toe door meer en goedkopere vliegroutes en, mede als gevolg daarvan, ruimere mogelijkheden om conflicten te ontvluchten.

De Sovjet-Unie viel uiteen en de tweedeling in goed en kwaad uit de tijd van de Koude Oorlog was ten einde. Het veiligheidsapparaat leek in een soort vacuüm beland zonder een duidelijk 'vijandbeeld'. De aanpak van de georganiseerde criminaliteit ontspoorde in de eerste helft van de jaren '90, maar die criminaliteit staat niet voor een bepaalde groep in de samenleving. De georganiseerde criminaliteit is complexer en laat juist de verwevenheid tussen de boven- en onderwereld zien, maar ook tussen criminelen en rechtshandhavers. Opsporings- en inlichtingendiensten gingen zich in die jaren explicieter richten op bepaalde bevolkingsgroepen.

In een periode van enkele jaren werd een nieuw vijandsbeeld gecreëerd en nieuwe potentiële bedreigingen voor de rechtsstaat aangewezen. Allereerst waren daar de vluchtelingen die in de jaren '80 naar Europa waren gekomen en organisaties die die vluchtelingen ondersteunden. Ook illegalen maakten deel uit van de vermeende dreiging van migranten. Daarnaast waren er de dak- en thuislozen en drugsgebruikers en tot slot krakers en actievoerders.

Opschorting van het onschuld-adagium

In de jaren '90 liet J&J zien dat voor die groepen in de samenleving de privacy al dood was. Zeker voor vluchtelingen en illegale migranten die probeerden te overleven was privacy volledig uit het zicht verdwenen.

Een reeks wetten maakte tevens een eind aan de solidariteit onder de bevolking: invoering van de Wet op de Identificatieplicht op het werk, Koppelingswet, toepassing van het Sociaal-Fiscaal nummer (SoFi, thans Burger Service Nummer geheten) als controlemiddel, nieuwe controlediensten als het Mobiel Toezicht Vreemdelingen (MTV). In de brochure *Administratieve Apartheid* van het Autonoom Centrum werd die tweedeling in de samenleving onderbouwd.

Naast de privacy werd in de jaren '90 ook langzaamaan het onschuld-adagium voor bepaalde bevolkingsgroepen in de rechtsstaat opgeschort. Tijdens de Eurotop in Amsterdam in juni 1997 gingen 50.000 mensen de straat op om te protesteren tegen de Europese Unie. Ook werden tijdens die Europese top honderden demonstranten preventief opgepakt en enkele dagen vastgezet. Zowel rechters als de Ombudsman veroordeelden deze preventieve hechtenis, maar politiek, politie en justitie oordeelden dat zij in de toekomst op dezelfde wijze zouden handelen.

Protest tegen de Europese Unie, zeker op straat, is steeds spaarzamer geworden. De overheid zet vaker grove middelen in als noodverordeningen en noodbevelen, een soort noodtoestand die politie en justitie verregaande bevoegdheden geeft. Het is steeds 'normaler' geworden dat mensen die protesteren preventief worden gearresteerd.

Niet alleen demonstranten worden geconfronteerd met het einde van het onschuld-adagium in de loop van de jaren '90, ook vluchtelingen en illegalen. Zij moeten aantonen dat zij 'echte' vluchtelingen zijn en kunnen preventief, maanden soms jaren, worden opgesloten, alleen omdat zij zonder geldige papieren in Nederland verblijven.

Andere groepen die in de loop der jaren hun privacy en hun recht op onschuld verloren zijn de dak- en thuislozen en drugsgebruikers. In de schaduw van de bestrijding van de georganiseerde criminaliteit en de doorgeschoten opsporingsmethoden (commissie Van Traa) werd gewerkt aan een kaartenbak van daklozen en drugsgebruikers. Die ontwikkeling is in de 21ste eeuw mede dankzij voortschrijdende digitale technieken verder uitgekristalliseerd.

De intensieve samenwerking tussen hulpverleningsorganisaties, opsporingsdiensten en gemeenten met de toenemende automatisering zorgde voor een digitaal overzicht van daklozen en drugsgebruikers. Controle in binnensteden verscherpte eind jaren '90 en het begin van

deze eeuw. Onder de noemer openbare orde werden ‘bekende’ gebruikers en daklozen gecontroleerd. Blijkt iemand ‘gebruikers benodigdheden’ op zak te hebben dan kan een gebiedsverbod worden opgelegd.

In de loop der jaren is de termijn en omvang van die verboden in diverse gemeenten toegenomen. Gebiedsverboden lijken veel op de stadionverboden die bij de bestrijding van supportersgeweld wordt gebruikt. Voetbalsupporters zijn ook een groep die in de afgelopen drie decennia hun privacy en onschuld hebben moeten inleveren.

Je was erbij dus je bent erbij

Gebiedsverboden, stadionverboden en noodverordeningen worden gebruikt als openbare orde maatregelen om demonstraties, manifestaties, uitingen van vrijheid van meningsuiting en andere grondwettelijke rechten op te schorten. Uitgangspunt bij deze maatregelen is niet meer het onschuld-adagium, maar het principe dat iedereen schuldig is tenzij hij of zij het tegendeel kan bewijzen.

De strafmaatregel wordt niet opgelegd voor de eigenlijke overtreding, maar een mogelijke overtreding die eventueel zal worden begaan. In het strafrecht doet daarnaast ook de groepsveroordeling zijn intrede. Het principe 'je was erbij dus je bent erbij', zonder dat de individuele bijdrage aan een strafbaar feit door de overheid hoeft te worden aangetoond.

Daar waar in het eerste decennium na de val van de Muur ‘randgroepen’ gericht werden aangepakt, verschoof de aandacht na de eeuwwisseling naar een groter segment van de bevolking. De invoering van de uitgebreide Identificatieplicht (WUID) (eigenlijk gewoon een plicht voor iedereen om zich te legitimeren), preventief fouilleren, grote gecombineerde verkeerscontroles en andere maatregelen richten zich op de gehele bevolking vanwege het principe 'je was erbij dus je bent erbij'.

Van de identificatieplicht kan nog worden gezegd dat het alleen mensen treft die in overtreding zijn of een strafbaar feit begaan, maar in werkelijkheid is daarvan geen sprake. Wie onwetend met een kapot achterlicht rondfietst, kan worden aangehouden en beboet. Indien er geen legitimatiebewijs kan worden getoond, volgt in sommige gevallen de politiecel. De overheid treedt steeds meer op vanuit een onredelijk

repressieve opstelling, de burger is strafbaar.

Bij een grote verkeerscontrole wordt de automobilist gedwongen om een gevaarlijke parkeerplaats op te rijden waar allerlei opsporingsdiensten op hem wachten. Vervolgens worden hem alle gegevens ontfutseld en wordt hij door een wasstraat geleid op zoek naar strafbare feiten en overtredingen. Elke vondst van een vergrijp wordt breeduit gemeten in de media. Meestal gaan die verkeerscontroles gepaard met preventief fouilleren.

De burger moet ook betast worden door de overheid, want iedereen die zich op die parkeerplaats, of het centrum van een stad of achterstandsbuurt begeeft, is potentieel een wapendrager. Los van het stigmatiserende karakter van preventief fouilleren - alleen bepaalde wijken worden aangewezen op basis van discutabele cijfers en analyses – betekent de maatregel ook dat wie weigert nog verder van huis is. De publieke ruimte is niet van de argeloze burger, nee, de overheid is daarin heer en meester.

WUID levert dubbele boetes op

Onderzoek van Buro Jansen & Janssen naar de werking van de Wet op de Uitgebreide Identificatieplicht (WUID) toont aan dat veel mensen dubbel beboet worden. Dit zijn vaak dezelfde dak- en thuislozen en drugsgebruikers die al bekend zijn bij de overheid, maar die toch hard moeten worden aangepakt. Dubbele boetes voor het door rood licht oversteken op een zebrapad of ergens staan waar een politieagent van vindt dat dat niet mag.

De WUID is ook een extra controlemiddel om te jagen op vluchtelingen, illegalen, bewoners van Nederland die geen standaard witte huid hebben. Een groot deel van de boetes voor overtreding van de identificatieplicht wordt al jaren opgelegd zonder daadwerkelijke overtreding of vergrijp. Etnisch profileren is in die zin geen nieuwe maatregel, maar vloeit voort uit bovenstaande maatregelen waarbij de overheid bepaalt wat er gebeurt in de openbare ruimte.

Hebben al die maatregelen een veiliger samenleving opgeleverd? Volgens de politiestatistieken daalt de criminaliteit al jaren, maar in hoeverre die cijfers waarheidsgetrouw zijn blijft onduidelijk. De aangiftebereidheid onder bewoners van Nederland is laag, rond de 27

procent. Dit verschilt wel enigszins per regio en per delict, maar het lage percentage geeft wel aan hoeveel vertrouwen er is in politie en justitie.

Naast de geringe aangiftebereidheid is de oplossingsgraad van strafbare feiten door politie en justitie al jaren bedroevend laag. Nu blijkt zelfs dat er getwijfeld wordt aan het lage aantal moorden. OM iets te doen nemen bedrijven en burgers zelf actie. Fysieke beveiliging van huizen en winkels blijken de afgelopen dertig jaar meer effect te hebben gehad, dan enig optreden van de politie of maatregelen van de overheid.

Onderzoek van J&J naar grote verkeerscontroles maakt duidelijk dat woninginbraken in de dorpen rondom die operaties niet zijn afgenomen. De overheid communiceert nog wel met veel bombarie de vangst bij dergelijke grote controles, opgezet om insluipers met inbrekerssetjes te vangen, maar in de evaluaties gaat het vooral om de ‘leuke’ samenwerking tussen allerlei opsporingsgroepen in Nederland.

'Je weet maar nooit' argumenten

Redenen voor invoering van wetgeving die zowel de privacy als de onschuld inperken, blijken fluïde en verschuiven regelmatig. Politieke verschillen zijn er niet echt als het gaat om het veiligheidsbeleid. De invoering van de identificatieplicht werd door D66-bewindslieden gepromoot vanuit het oogpunt van terrorismebestrijding. Toen de wet eenmaal in de maak was en besproken werd in het parlement kwam dat facet niet meer ter sprake. Een rechter van PvdA-huize vond de wet noodzakelijk om hangjongeren aan te pakken. Daarbij ging het niet om jongeren die een strafbaar feit of overtreding hadden begaan, maar om bestrijding van het onschuld-adagium. Het ‘je weet maar nooit’ argument voor invoering van veel repressieve wetgeving.

Dat ‘je weet maar nooit’ argument is ook een van de argumenten geweest voor het invoeren van preventief fouilleren. De bevoegdheden worden opgerekt, want de overheid moet genoeg instrumenten hebben om op te kunnen optreden. Onderzoek van J&J toonde aan dat preventief fouilleren vaak ineffectief is en soms zelfs contraproductief. Er zijn indicaties dat geweldscriminaliteit toeneemt in die gebieden die door de overheid worden aangewezen als onveilig, als risicogebieden. De overheid bestempelt een buurt als veiligheidsrisicogebied en burgers gaan deze straten mijden. Anderen die zich er wel in begeven bewapenen zich, want ‘je weet maar nooit.’

Niet alleen in de openbare ruimte wil de overheid burgers disciplineren. Zowel in de fysieke als in de digitale wereld rukt zij op. Werkplicht, voorschriften over kleding en uiterlijk voor mensen met een uitkering, druk op dak- en thuislozen en drugsgebruikers om aan allerlei programma's deel te nemen, inkomens gestuurde huisvesting, controle van bewoning door woningbouwverenigingen samen met bestuur en politie, etc. Langzaam wordt er een arsenaal aan maatregelen uitgerold om ook direct in het leven van burgers in te kunnen grijpen.

Bij dat arsenaal hoort ook het 'toezicht' door de overheid op het internet, sociale media en webfora. Deels laat de techniek dit toe, maar er ontbreekt tevens duidelijke wetgeving omtrent bevoegdheden van politiefunctionarissen op het internet en is patrouilleren, het verzamelen van persoonsgegevens en het opstellen van profielen op en met behulp van sociale media zeer eenvoudig. Mensen zijn zich vaak niet bewust van wat zij allemaal aan informatie en sporen op het internet achterlaten en met wie zij die informatie delen. Dit gebeurt meestal op sociale media, maar ook op andere plaatsen op het internet.

Smartphone als alter ego voor de burger

Fysieke en digitale werkelijkheid convergeren steeds vaker. Door plaatsbepaling, toegenomen kennis van bedrijven over interesses, wensen, verlangens, voorkeuren (zowel seksueel, politiek of anderszins) van burgers; sociale media spelen daarbij een belangrijke rol. Gerichte reclames, aanbiedingen bij het passeren van winkels en horecagelegenheden; het is onderdeel geworden van de interactie tussen de fysieke en digitale werkelijkheid.

Het algemene gebruik van de smartphone maakt in combinatie met de plaatsbepaling het allemaal veel gemakkelijker om te profileren en gericht individuen te benaderen. Berichten, foto's, contacten, cv's, identiteitsgegevens en bankgegevens komen allemaal voort vanuit een digitaal apparaat. De smartphone is vandaag de dag dé keuzebepaler voor films, eten, restaurants, boeken, relaties maar ook voor huishoudelijke doeleinden, zoals aansluitingen voor gas, licht en water, betalingen, bankzaken, contact met de overheid, identiteit, reizen, boardingpas voor vliegreizen, etc.

De smartphone heeft zich als digitale en fysieke alter ego van burgers

ontwikkeld. Het verbindt beide werelden en is sterk geïndividualiseerd, al is dat aan het apparaat zelf nog niet af te lezen. Niet alleen bedrijven azen op dat alter ego. Naast commerciële interesses zijn vooral de overheid en opsporings- en inlichtingendiensten geïnteresseerd in al die gegevens en sporen die burgers achterlaten.

Het begon met invoering van de Wet bewaarplicht van telecommunicatiegegevens in 2009, Nederlandse wetgeving gebaseerd op een Europese richtlijn. De bewaarplicht (dataretentie) werd ingevoerd onder druk van aanslagen in de Verenigde Staten, Spanje en het Verenigd Koninkrijk. Bedrijven worden door de bewaarplicht voorgeschreven communicatiegegevens voor een bepaalde tijd bewaren. Het gaat vooral om gegevens als wanneer en met wie er wordt gecommuniceerd en de metadata van een bericht. De inhoud werd buiten beschouwing gelaten in verband met het briefgeheim en 'privacy' issues.

De bewaarplicht raakt iedereen en niet alleen specifieke verdachten van strafbare feiten. Of de maatregelen terrorisme-aanslagen voorkomen, de samenleving veiliger maken... het antwoord blijft uit. De effectiviteit is nooit onderzocht. Dat is ook onmogelijk bij zo'n algemene weg. De argumentatie voor invoering was 'je weet maar nooit' en nieuwe repressieve maatregelen staan alweer op de rol.

IP-tap

Op het internet waren tot aan de invoering van de bewaarplicht nog geen specifieke maatregelen getroffen ten aanzien van bepaalde groepen. Sommige webfora en nieuwspagina's van radicaal-linkse en extreem-rechtse groepen werden al wel in de gaten gehouden, maar van specifieke *targeting* van groepen zoals in de fysieke wereld bleek nog geen sprake.

De internettap (IP-tap) werd wel uitgebreid zoals de telefoontap. Niet meer alleen de verdachten werden gericht afgeluisterd, ook familie, vrienden, kennissen. Dit was voortgekomen uit de ontspoorde opsporingsmethoden in de jaren '80/'90 en de commissie Van Traa. De Bijzondere Opsporingsbevoegdheden formaliseerden echter die methoden en in de nieuwe eeuw werden zij aan de gewone strafvordering toegevoegd.

Toch is de IP-tap niet te vergelijken met databanken van vluchtelingen, illegalen, activisten, dak- en thuislozen en andere randgroepen. Aan de andere kant heeft de bewaarplicht echter wel de poorten opengezet om verder binnen te dringen in het digitale leven van burgers, en daarmee ook in het fysieke leven.

De laatste jaren monitort de overheid steeds meer sociale media. Daarbij gaat het niet langer alleen om wie met wie communiceert en wanneer, nee, het gaat steeds vaker om de inhoud en om facetten zoals plaatsbepaling. De schroom wat betreft persoonsgegevens, privécommunicatie; het lijkt allemaal niet meer relevant. De politie volgt berichten op Twitter die niet per se voor publieke doeleinden zijn bedoeld, Facebook berichten die niet exclusief aan vrienden zijn gericht. De overheid wil op FB ook 'bevriend' raken met burgers zodat zij zicht kan houden op de communicatie binnen afgesloten groepen.

Bij politiepatrouilles in de fysieke werkelijkheid kan aan de hand van gegevens van de GBA (Gemeentelijke Basisadministratie) en de RDW (Rijksdienst voor het Wegverkeer) worden gecheckt wie welk huis bewoont en wat voor auto hij bezit. Met de identificatieplicht en preventief fouilleren kunnen opsporingsdiensten al grote stappen vooruit maken in het binnendringen van de persoonlijke levenssfeer. U moet zich legitimeren en aantonen dat u geen gevaarlijke wapendrager bent.

Patrouilleren in de digitale wereld, op sociale media, onthult echter allerlei persoonlijke opvattingen waaronder politieke meningen, met wie die worden gedeeld en wanneer, en wie het met die meningen eens is. Het algemene gebruik van de smartphone als digitaal hulpmiddel om ons op het internet of sociale media te begeven, maakt het ook mogelijk plaatsbepaling en andere gegevens aan die dataset toe te voegen.

Nog een bredere toegang gewenst

De overheid wil desondanks nog bredere toegang. Dat uit zich bijvoorbeeld in het pleidooi tegen encryptie van opsporings- en inlichtingendiensten. Het zou het werk van die diensten bemoeilijken en de veiligheid in gevaar brengen. Afscherming, privacy en anonimiteit zijn volgens de overheid schuilplaatsen van het kwaad. De veiligheidsdiensten moeten toegang hebben, want 'je weet maar nooit'.

De overheid gaat echter nog een stap verder. Zij wil graag inbreken op

digitale hulpmiddelen van de slechteriken. Nu is dat te vergelijken met een gerichte telefoon- of internettap, de verdachte is het doel. Voor dat gericht inbreken is het echter noodzakelijk dat besturingssystemen van smartphones, tablets, laptops, etc. veiligheidslekken hebben, anders kan er niet worden ingebroken. Die veiligheidslekken worden regelmatig ontdekt, de zogenoemde *zero-days*, beveiligingslekken die net bekend zijn (nul dagen) en door bedrijven die software hebben ontwikkeld nog niet zijn gedicht.

Die *zero-days* en de digitale wapens om in te breken kopen Nederlandse opsporings- en inlichtingendiensten van individuen en bedrijven of via bedrijven zoals Hacking Team en Gamma Group. De beveiligingslekken gelden echter niet alleen voor de smartphone van een verdachte, maar voor iedereen met een vergelijkbare telefoon of hetzelfde besturingssysteem. Opsporings- en inlichtingendiensten willen die lekken onder de pet houden, want dan zijn ze vaker te misbruiken om in te breken. *Die zero-days* zijn echter niet exclusief voor de Nederlandse politie. Meestal zijn veel meer partijen op de hoogte van dezelfde lekken. Dat zijn overheden, opsporings- en inlichtingendiensten, maar ook bedrijven en criminele organisaties. De Nederlandse overheid ontwikkelt zelf niet de digitale wapens en ontdekt ook niet zelf de *zero-days*.

Nederlandse diensten lopen dus constant achter de feiten aan en laten burgers bewust rondlopen met onveilige smartphones, laptops en tablets. Het zou echter essentieel zijn voor de opsporing, hoewel dat argument niet met feiten wordt onderbouwd. Wat wel duidelijk is en door feiten wordt gestaafd, is dat bedrijven als Hacking Team en Gamma Group het niet zo nauw nemen met burger- en mensenrechten. Zij verkopen hun waar aan repressieve regimes als Soedan, Ethiopië, Egypte, Rusland en lijken er geen bezwaar tegen te hebben dat hun wapens worden ingezet tegen oppositiegroepen en journalisten.

Aan die bedrijven kleven weer allerlei andere bezwaren zoals het gebrek aan duidelijkheid over de rol van investeerders en de relaties die deze bedrijven hebben met bepaalde overheden, militaire eenheden, inlichtingendiensten en investeerders. Ook is de geschiedenis van de technologie waar hun digitale wapens op gebaseerd is niet te controleren en kunnen overheden, diensten en bedrijven daar een rol in hebben gespeeld bijvoorbeeld door de aanwezigheid van *backdoors* die de veiligheid van verdachten, en dus van de gehele bevolking, in gevaar kan brengen. En tot slot is er zelfs sprake van onduidelijke bedrijfsstructuren en twijfels over de economische integriteit door het gebruik van BV's in

belastingparadijzen als Cyprus, Libanon, Panama en de Britse Maagdeneilanden.

Wit voetje halen

In de zomer breekt de politie fysiek in om een 'wit voetje' bij de burger te halen. Als dienstverlener wil ze waarschuwen voor het kwaad. Het gehele jaar laat diezelfde politie de deuren van smartphones en andere digitale middelen wagenwijd open staan. Die veiligheidslekken moeten gebruikt kunnen worden voor de enkele keer dat de diensten inbreken bij een verdachte, want 'je weet maar nooit'. Hoewel fysieke goederen nog steeds gewild zijn bij inbrekers, zijn digitale goederen veel meer waard. De smartphone, het alter ego van veel burgers, omvat veel gegevens en sporen, data die voor een cybercrimineel interessanter en waardevoller zijn dan de nieuwste gekromde UHDTV.

Hoe makkelijk het is om digitaal in te kunnen breken, laat de constante stroom hack-incidenten ons zien. In de zomer van 2016 werd bijvoorbeeld een Duitse hacker gearresteerd die wist in te breken op de computers van 150 Duitse schoolmeiden. Hij bespiedde hen via hun webcam en slaagde erin via het chatprogramma ICQ binnen te dringen. Met behulp van een trojan, een programma waarmee je een computer infecteert en op afstand kan besturen, kon hij zo de webcam overnemen. De hack werd niet ontdekt door de politie maar door een man die lesgeeft over databeveiliging op middelbare scholen. Het voorbeeld laat zien dat databescherming essentieel is en eigenlijk een grondwettelijk recht moet zijn.

De Nederlandse overheid propageert echter geen databescherming en veilige communicatie. Zij wil op de hoogte gehouden worden van datalekken, maar wat dat bijdraagt aan een grotere veiligheid op het internet is onduidelijk. Opsporings- en inlichtingendiensten willen geen encryptie, willen inbreken op digitale hulpmiddelen van burgers en *zero-days* onder de pet houden. Meerdere datalekken zullen het gevolg zullen daarvan zijn en minder digitale veiligheid. Voeg dit bij een lage aangiftebereidheid en een zeer lage oplossingsgraad van politie en justitie, en zie daar de onveilige samenleving die zich verder ontwikkelt.

Strenge regelgeving ten aanzien van software en hardware die op de markt komen is essentieel, zeker nu veel apparatuur bijna standaard aan het internet is gekoppeld. Controle ten aanzien van het updaten van die

software en hardware in het licht van de snelle ontwikkelingen. Een verbod op de handel in *zero-days,* met zware straffen als die niet wordt gemeld, en een verbod op het maken van digitale wapens.

Boemerang

De kans dat de Nederlandse overheid deze stappen zal gaan zetten, is nihil. Zij propageert geheimzinnigheid rond digitale wapens en *zero-days,* een zorgelijke ontwikkeling die als een boemerang de Nederlandse economie en veiligheidsdiensten zal treffen. Want als de laatste decennia iets hebben duidelijk gemaakt, is dat overheden de digitale revolutie niet in de hand hebben.

Na de privacy en het onschuld-adagium is nu ook de veiligheid geofferd. Langzaamaan wordt de rechtsstaat ontmanteld. De argumenten daarvoor zijn veelal niet gebaseerd op feiten. Terrorismebestrijding, criminaliteitsbestrijding, openbare orde; de eventueel controleerbare argumenten voor de invoering van maatregelen zijn naar de achtergrond verschoven. Noodzakelijk onderzoek of die maatregelen wel het juiste effect hebben gesorteerd, wordt vermeden of uitgevoerd op een manier waardoor opsporings- en inlichtingendiensten altijd in het gelijk worden gesteld zonder feitelijke onderbouwing. Wat overblijft is het enge argument dat de overheid en de diensten keer op keer herhalen: ‘je weet maar nooit’.

‘Je weet maar nooit’; Na privacy en de onschuld, is nu ook de veiligheid dood (pdf)

Naar inhoudsopgave Observant #69

Dutch secret service tries to recruit Tor-admin

Recently a Dutch man with an MSc (Master of Science) at the Delft University of Technology and admin of Tor-exit nodes was approached by two agents of the Dutch intelligence service, the AIVD. They wanted to recruit the man as an informant or undercover agent, who would also infiltrate foreign hacker communities. The person tells his story.

We received this story from a person who wants to remain anonymous. We conducted an investigation to the existence of this person and confirmed their existence. The person did not want to answer additional questions about the conversation held with the Dutch secret service (AIVD for its initials in Dutch) and wanted to remain anonymous. We respect this. We publish this account because we think the story is important both for the hackers community and beyond. The person has written the story in English, which we have edited without changing the contents. We have also translated it into Dutch with some slight clarification in relation to some comments, again without changing the contents.

Stories about recruitments are complex because they take place between the authorities and a civilian. The authorities will never reveal any information about these encounters. The effects of an attempt to recruit someone or recruitments can be severe. This is the experience of Buro Jansen & Janssen in dealing 35 years with the practices of the secret service and recruitments.

People who are recruited are mostly selected by the secret service, generally because they can easily be influenced, are vulnerable and/or unstable. This can be part of someone’s personality, as a result of events in someone’s life just before the recruitment, or in other moments in his or her life. These effects in some cases have resulted in moments of vulnerability and/or instability or

tendencies to be easily influenced. Secret services abuse these weaknesses of people, surprise people, show people that they know a lot about their lives, threaten them with that knowledge and threaten people not to share their experiences with others.

The agents Rob de Vries and Fatma threatened the person who wrote this account not to make it public. This threat has no moral or legal basis. If the secret service tries to recruit you, talk to your friends about it, to fellow hackspace users, community members, acquaintances, family and other people or even better, publish your story.

Buro Jansen & Janssen

I'm a citizen of The Netherlands with a MSc at TU Delft. I run several Tor-exit nodes for research purposes and got a recent visit from the Dutch intelligence service. The agents were a male-female couple that visited me at a gym facility where I was having a drink and was expected thought to be alone.

This is what happened: They approached me and identified themselves with a badge of the Ministry of Internal Affairs and said they were working for the AIVD (Dutch secret service). They asked me to hear them out. I was in a state of shock and thought I had committed a crime but they immediately started to talk about on my studies. They made it clear they've read my thesis on IT security and showered me with compliments before they were firing a round of job offers at me. To summarize:

+ they're building out a unit called JSCU (Joint Sigint Cyber Unit) and approaching IT students (it seems they're already monitoring young students in the last years of college) and need somebody in their generation but yet somewhat older to direct the younger ones, "because they need oversight and only not DDoS sites without a directing team leader that is qualified in their own field."

+ they asked me if I was interested in traveling for a couple of years and for example work in Germany at a technology company while visiting the Chaos Computer Club's hacker spaces to see what's going on and report back to them. All my expenditures would be covered.

Here I should 'have realized they were trying to recruit me to spy in Germany but I was still in shock because I never thought secret agents would have an interest in me. I continued to listen as they continued offering different possibilities, probably hoping I would be interested in one of them.

+ They also mentioned that occasionally there are hacker parties in Italy, Austria, Spain, and other countries, and they said I could see that as paid holidays. They were very honest about the fact that they were looking for foreign talent but mostly interested in keeping tabs on Dutch IT-professionals and hackers abroad. They emphasized on monitoring Dutch people abroad at least 3 times.

+ They knew about my Tor-exit nodes, at least the woman did. The man didn't seem he had much technical knowledge. She was younger too, I think 25-30 years old, while he could have been her father. She asked how I paid for the Tor-nodes and I told her I run them in the cloud which is cost-effective. She asked what I think about expanding Tor-exit nodes in The Netherlands with all costs paid and no worries for any abuse complaints? I was startled and said: "I'm not sure if that's legal."

This is where I should have left my drink and walked away but they were clinging on to me and kept talking fast as if they knew I was about leave. The man told me: "you are not obliged to do anything, just to hear us out. If you work with us there are benefits, for example if we ask you to crash a system in a public place and you would be arrested for that, we make sure you don't get arrested and nobody will know about it, not even the police".

+ The man took over from the girl saying that if I'm not interested in managing students at their facility, maybe I should travel to one of the hacking conferences to think things over, without directly infiltrating hackerspaces. He said they were mostly interested in building a community of techies around the developers of Tor and

Tails and that it would be an international effort. This was an option that wouldn't require me to work with the Dutch secret service AIVD officially but voluntarily and I could state the expenses and determine my own salary. He said: "this is a possibility too, if you're not asking 5.000 euros a month but we cover travels too."

At this point they stopped talking and looked at me. I said I didn't know what to do, and that I was curious about how they found me. Why me? Now the compliments on my thesis resumed. They didn't reveal who led them to my thesis. I told them I was shocked and felt uneasy about the whole deal and wanted to leave.

Now the vibe changed and the girl tried once more: you really miss out working for us, nobody knows what we're doing and you can have access to new types of technology, we know you're interested in technology, aren't you? I will give you my number so you can think about it. While she was writing down her mobile number I said: I am not interested, period, I will go now and please don't bother me again. I think this was a big mistake because the old man who showered me with compliments suddenly said: "look, we know about your Tor-exit nodes, if you run them with us you will be able to make a living out of it, but if you don't and something illegal happens, we can't help you if the police visits your home and seizes your equipment."

I replied : "I'm not doing anything illegal." But he didn't care about what I said, he continued: "we recommend that you not speak to anybody about this because it's punishable by Article 60 of the law and it's too bad you've chosen this route."

He said: "We go." They stood up and she said: "You're really a smart guy, if you change your mind, give us a call. But thanks for hearing us out, that was really nice of you to just hear what we had to say." The old man didn't say anything and stretched out his hand to say goodbye.

I got home and I can't describe how I feel but I had a very bad night. Because I'm an ethical hacker I am sharing this story with you. It's for publication as I strongly believe they won't be knocking on my door again when it's published.

By the way their names were Rob de Vries and Fatma (no last name given) but these are probably fakes. The number wasn't a mobile number but the real public number of the which she memorized.

[Original '*this message is intended for publication, with the IT hacking community in mind*]

Dutch secret service tries to recruit Tor-admin (pdf)

AIVD benadert Tor-beheerder (pdf Dutch translation)

Naar inhoudsopgave Observant #69

AIVD benadert Tor-beheerder

Recentelijk kreeg een Nederlander met een MSc (Master of Science) aan de TU Delft en beheerder van enkele Tor-exit nodes bezoek van twee AIVD'ers. Ze wilden de man rekruteren als informant of infiltrant die ook de buitenlandse hackersgemeenschap zou gaan bespioneren. De benaderde doet zijn verhaal.

Onderstaand oorspronkelijk Engelstalige verhaal heeft Buro Jansen & Janssen anoniem van een persoon ontvangen. Wij hebben uitgezocht of de betreffende persoon bestaat en hem ook getraceerd. Hij wilde geen verdere vragen beantwoorden en wenst anoniem te blijven. Wij respecteren dit. Wij publiceren dit verhaal omdat het belangrijk is dat de hackersgemeenschap in Nederland, maar ook daarbuiten, kennis neemt van deze benadering.

Verhalen over benaderingen zijn complex. Het betreft hier een contact tussen een dienst en een burger waarvan de overheid nooit zal zeggen dat het daadwerkelijk plaats gevonden heeft, noch dat er informatie over naar buiten wordt gebracht. De gevolgen van benaderingen kunnen ernstig zijn, zo leert ons de ruim 35 jaar ervaring die Buro Jansen & Janssen met inlichtingendiensten en benaderingen heeft opgedaan.

Mensen die benaderd worden zijn uitverkozen, meestal omdat ze beïnvloedbaar, kwetsbaar en instabiel zijn. Dit kan te maken hebben met iemands persoonlijkheid of door gebeurtenissen in het leven van een persoon waardoor die op dat moment kwetsbaar, instabiel en beïnvloedbaar is. Inlichtingendiensten misbruiken deze zwakheden, overvallen mensen, laten zien dat ze veel weten en bedreigen hen daarmee.

De agenten 'Rob de Vries' en 'Fatma' bedreigden in onderhavige geval de benaderde persoon voor het naar buiten brengen van dit verhaal. Dit dreigement is nergens op gebaseerd. Mocht je benaderd zijn, meldt het dan zeker aan je

vrienden, mede hackspace gebruikers, kennissen en anderen. Of nog beter, publiceer je verhaal.

Buro Jansen & Janssen

Ik ben een Nederlander met een MSc (Master of Science) aan de TU Delft (Technische Universiteit van Delft). Run een aantal Tor-exit nodes [Tor is een server netwerk om anoniem te kunnen browsen, red.] voor onderzoeksdoeleinden en kreeg recent bezoek van de Nederlandse inlichtingendienst. Een mannelijke en een vrouwelijke agent benaderden mij op de sportschool die ik frequent bezoek en dacht dat ik daar in alle rust iets kon drinken. Het volgende overkwam mij.

De agenten identificeerden zich met een badge van het Ministerie van Binnenlandse Zaken en zeiden dat ze voor de AIVD werkten, de Algemene Inlichtingen en Veiligheidsdienst. Ze wilden me graag spreken. Ze hadden mij niet eerst gebeld en hun bezoek aangekondigd. Ik voelde me nogal overrompeld, dacht dat ik in de problemen zat en misschien verdacht werd van het plegen van strafbare feiten.

Ze vroegen echter in eerste instantie naar mijn studie. Ze hadden mijn scriptie over IT-beveiliging gelezen en complimenteerden me uitvoerig. Vervolgens leek het of ze mij allerlei functies bij de AIVD aanboden, zowel bij de dienst zelf op kantoor dan wel als informant/infiltrant. De geheim agenten vertelden mij dat de AIVD een eenheid aan het opzetten is met de naam JSCU (Joint Sigint Cyber Unit). Ze benaderen daarvoor IT-studenten.

Mijn benadering maakte duidelijk dat ze studenten in het laatste jaar van hun studie al langer in de gaten houden. Ze zijn ook op zoek naar mensen die iets ouder zijn, maar wel verbonden aan de gemeenschap/generatie van nu. Deze kan teamleider worden die onderdeel uitmaakt van de gemeenschap, maar tevens richting weet te geven aan de IT-studenten zodat het niet alleen om DDOS-sites draait. Ik was een van de kandidaten die ze voor ogen hadden.

Vervolgens vroegen ze mij of ik geïnteresseerd was om voor een aantal jaren te gaan reizen en bijvoorbeeld te werken voor een

technologiebedrijf in Duitsland. Het idee was dat ik in Duitsland dan Hackspaces van de Chaos Computer Club zou gaan bezoeken om te kijken wat daar gebeurde. Ik moest wel over die bezoeken rapporteren aan de AIVD. Alle onkosten zouden worden betaald door de inlichtingendienst.

Rekrutering

Op dat moment van het gesprek had ik me moeten realiseren dat ze mij probeerden te rekruteren. Ze wilden dat ik voor ze ging werken als informant of infiltrant in Duitsland. Ik voelde me echter overvallen, zonder aankondiging hadden ze mij aangesproken in de sportschool. Ik had er nooit bij stilgestaan dat de inlichtingendienst interesse in mij zou kunnen hebben. Ik ben niet weggelopen of heb het gesprek afgebroken, bleef zitten en luisterde verder naar hun verdere verhaal.

Ze bleven mij allerlei voorstellen doen. Misschien hoopte ik dat ze me iets zouden aanbieden dat de moeite waard is. Ik weet het niet, maar kapte ze in ieder geval niet af, realiseerde misschien ook niet echt wat er gebeurde. De opsomming van de ongekende mogelijkheden die de inlichtingendienst mij kon bieden, vervolgde. De agenten vertelden dat er hackersfeesten worden georganiseerd in Italië, Oostenrijk, Spanje en andere landen en dat ik die mag zien als betaalde vakanties.

Ze maakten duidelijk waarin ze geïnteresseerd zijn. Ze zoeken buitenlands hackerstalent, maar willen vooral zicht houden op de Nederlandse IT-professionals. Ze benadrukten op verschillende momenten dat ze vooral interesse hadden in Nederlanders hackers actief in het buitenland en benoemden dat minstens drie keer. De vrouwelijke AIVD'er bleek goed op de hoogte, terwijl de man over niet al teveel technische bagage leek te beschikken. Ik schat de vrouw tussen de 25 en 30 jaar, haar collega had haar vader kunnen zijn.

Ze wisten dat ik Tor-exit nodes draai. De vrouw vroeg waar ik het geld daarvoor vandaan haal. Ik vertelde haar dat ze in de *Cloud* draaien zodat het niet te veel hoeft te kosten. Blijkbaar hadden ze daar nog niet naar gekeken. De agente wilde van me weten wat ik er van zou vinden het aantal Tor-exit nodes in Nederland uit te breiden. De kosten zouden worden gedekt en ik hoefde me geen zorgen te maken over klachten of

misbruik. Ik schrok, was erg verbaasd en zei dat ik er niet echt zeker van was of zoiets wel legaal is.

Controle volledig kwijt

Op dat moment had ik het gesprek écht moeten beëindigen, maar het voelde alsof ik dat niet zomaar kon doen. Ze waren zo aardig, ze wisten wat ik deed, wisten waar ik naartoe ging, waar ik was, het voelde als een val. Ze waren ook erg vasthoudend, verhullend, sussend en veranderden snel van onderwerp of praatten door alsof ze wisten dat ik weg wilde.

De man pakte de draad op en ging een stapje verder: ,,Je bent nergens toe verplicht, luister gewoon naar wat wij je te bieden hebben, te vertellen hebben.'' Het klonk zo redelijk allemaal, maar dat was het zeker niet. ,,Als je voor ons werkt zijn er allerlei voordelen'', zei hij, om eraan toe te voegen dat ik strafbare feiten kon plegen zonder verdere gevolgen. ,,We kunnen je bijvoorbeeld vragen om een systeem in een publieke ruimte plat te leggen. Wij zorgen er dan wel voor dat je niet wordt gearresteerd en dat niemand er achter komt, zelfs de politie niet.” Eigenlijk was ik te verbijsterd om iets te doen. Zij hadden volledig de controle over mij, dat voelde eng.

De mannelijke agent leek gaandeweg de leiding over het gesprek over te nemen. Als ik niet geïnteresseerd was om teamleider te worden van een groep studenten bij een eenheid van de AIVD kon ik ook eerst naar een hackersconferentie gaan zodat ik de tijd had na te kunnen denken over het aanbod. Ik hoefde van hem niet meteen bij een hackspace te infiltreren, kon er ook gewoon eerst over nadenken.

Hij zei dat de AIVD vooral geïnteresseerd was in de ontwikkelaars van Tor en Tails. De agenten doelden hiermee natuurlijk op het werven van informanten of infiltranten, maar hij omschreef het omslachtig. De inlichtingendienst is geïnteresseerd in het opbouwen van een gemeenschap bestaande uit technische mensen rond ontwikkelaars van Tor en Tails. Volgens de AIVD'ers maakte dit onderdeel uit van een internationale operatie.

Zelf zou ik niet gedwongen worden om voor de AIVD te werken. Het kon allemaal op vrijwillige basis en de onkosten kon ik in rekening brengen bij de dienst en mocht zelfs mijn eigen salaris bepalen. Om zijn woorden kracht bij te zetten zei hij nogmaals dat dat laatste mogelijk was, zodra

ik maar niet meer dan 5.000 euro per maand zou vragen. Alsof vijfduizend zeker niet genoeg was, voegde hij er nog aan toe dat dan ook de reiskosten worden vergoed.

De sfeer sloeg om

Dat was het moment dat de AIVD'ers stopten met praten. Ze keken we verwachtingsvol aan, was ik om? Maar ik was de schok te boven en klaar met ze. Antwoordde dat ik niet geïnteresseerd was maar wilde wel graag weten hoe ze bij mij terecht waren gekomen, waarom juist ik? Opnieuw begonnen ze mijn scriptie de hemel in te prijzen waarmee het gesprek opnieuw leek te beginnen. Ze wilden niet aangeven wie de persoon was die de AIVD op mijn scriptie had gewezen.

Eindelijk kon ik ze zeggen dat ik geschrokken was door hun benadering, dat ik me erg ongemakkelijk voelde door hun overvaltactiek en alles dat zij mij hadden voorgesteld. Ik wilde weg. De sfeer sloeg plotseling om. De vrouwelijke agent probeerde het nog een keer: ,,Je gaat echt iets missen als je niet voor ons werkt. Niemand weet wat we doen, jij wel. En je krijgt toegang en de mogelijkheid om te werken met allerlei nieuwe technologieën. Wij weten dat jij geïnteresseerd bent in technologie, of niet soms? Ik zal je mijn nummer geven zodat je kan nadenken over ons aanbod."

Terwijl ze het nummer van haar mobiel aan het opschrijven was, maakte ik opnieuw duidelijk dat ik niet geïnteresseerd was. ,,Ik heb geen interesse, punt uit. Ik ga nu en val me niet meer lastig." Misschien hadden ze niet verwacht dat ik hen zou afwijzen, of was die laatste opmerking tegen het zere been.

De mannelijke agent veranderde plotsklaps van toon. Hij had me misschien complimenten gegeven over mijn scriptie en kennis, maar dat was nu voorbij. ,,Kijk, wij weten dat je Tor-exit nodes draait. Als je dat doet terwijl je voor de AIVD werkt, kun je er van gaan leven. Als je echter niet voor de inlichtingendienst werkt en er vindt iets illegaals plaats dan helpen wij je niet zodra de politie bij je binnenvalt en je apparatuur in beslag neemt.

,,Ik doe niets illegaals", antwoordde ik slechts. Hij was echter niet langer geïnteresseerd in wat ik te zeggen had. ,,Wij raden je aan met niemand over dit gesprek te spreken, want het is een overtreding van artikel 60

van de wet en het is heel jammer dat je niet met ons gaat samenwerken. We gaan.” Ze stonden op maar de vrouw probeerde het nog een keer: ,,Je bent echt een slimme jongen, als je van gedachten verandert, geef ons dan een seintje, maar bedankt voor het gesprek, het was aardig van je om te luisteren naar wat wij te zeggen hadden.”

Ik kan niet omschrijven hoe ik me voelde, die nacht kon ik de slaap niet vatten. Ik ben een ethische hacker en wil daarom dit verhaal met jullie delen. Nog één ding. De twee AIVD'ers gaven zich uit voor 'Rob de Vries' en 'Fatma' (zij heeft geen achternaam gegeven), maar ik ga er vanuit de namen vals zijn. Ze hebben me geen mobiel nummer gegeven, maar het openbare nummer van de AIVD.

[Vertaling van ‘*this message is intended for publication, with the IT hacking community in mind*]

Dutch secret service tries to recruit Tor-admin

Dutch secret service tries to recruit Tor-admin (pdf)

AIVD benadert Tor-beheerder (pdf)

Naar inhoudsopgave Observant #69

Vernieuwde website J&J en Contrast Network

Het heeft even geduurd, maar nu is 'ie er dan: de vernieuwde website van Buro Jansen & Janssen. Uitgangspunt bij het bouwen van deze site was de integratie van alle archiefstukken van de afgelopen dertig jaar. Bij de vorige vernieuwing, tien jaar geleden, was ons dat nog niet gelukt. Zo stond het oude html-archief nog los van het nieuwe content-management systeem dat er ook nog eens al snel verouderd uitzag.

Nu gaat het bij J&J niet om hoe het eruit ziet, maar om de inhoud. De website was echter ook onhandig in onderhoud en de veiligheid van de site niet goed geregeld. Nu bewaart J&J geen gevoelige data op haar website. De adressen van de mailinglijst worden elders bewaard, dus is er geen direct gevaar voor bezoekers, maar in een wereld waarbij constant de veiligheid van websites en databases in gevaar is, leek het ons van belang een nieuwe site te bouwen.

Nog niet alles is klaar, maar omdat nu veel artikelen weer normaal te vinden zijn, hebben we besloten online te gaan. Naast het feit dat al het oude html-werk van twee websites uit de jaren '90 opgenomen is in de database, zijn alle oude links ook nog eens bewaard gebleven en eveneens opgenomen in de nieuwe database. Dit moet voorkomen dat bestaande connecties met andere websites verloren gaan.

Tevens is ervoor gekozen de andere websites van J&J, zoals justitie en veiligheid, nieuwsblog, openbaarheid en het nationaal veiligheidsarchief, een prominentere plek te geven in de nieuwe opzet. De bouw van de huidige portal heeft ook opgeleverd dat er zicht is op allerlei zaken die nog ontbreken binnen de digitale infrastructuur van J&J. Het gaat hierbij om toekomstige thema-sites over inlichtingendiensten, Europa en migratie waar in de komende tijd aan zal worden gewerkt.

Wees gerust, J&J gaat niet overstag in de zin van toevoeging van advertenties, sociale media, nietszeggende korte berichten en andere zogenaamde moderne media ontwikkelingen. Bij J&J ging, gaat en zal het blijven gaan over inhoud, toegankelijkheid, veiligheid en anonimiteit voor onze bezoekers. Natuurlijk hebben we geld nodig, maar dat moet geen een leidend argument worden voor goed en gedegen onderzoek.

Contrast Network, voor een fair internet

De bouw van de nieuwe website valt samen met opbouw van een digitale infrastructuur. Buro Jansen & Janssen participeert in een nieuw initiatief, genaamd stichting Contrast, contrast.network. Contrast wil bouwen aan een fair internet door kwalitatief goed georganiseerde digitale ruimte beschikbaar te stellen aan groepen en individuen die daarin zelf participeren en de structuren onderhouden.

Dit houdt zoveel in dat er gestreefd wordt naar een veilige internetstructuur, met encryptie, eigen e-mail voorzieningen, eigen cloud voorzieningen, het zelf hosten van websites en andere diensten. Ook voorlichting aan andere internetgebruikers behoort tot de taak van Contrast en zelfs het opleiden van mensen om die structuren op te zetten en te onderhouden. Het is ambitieus, maar in een wereld die verder digitaliseert en multinationals de markt beheersen, is het opbouwen van eigen structuren van groot belang voor het behoudt van de eigen identiteit en zelfstandigheid.

Om dit te stimuleren wordt er een netwerk-helpdesk opgezet waarmee gebruikers elkaar kunnen ondersteunen. Om de eigen digitale infrastructuur te complementeren wordt gewerkt aan een serie cursussen waarmee mensen getraind worden in het opzetten en beheren van web- en mailservers, veiligheid/firewall, afslaan van aanvallen, virtualisatie etc. Doel is politiek en techniek aan elkaar te koppelen, en tevens mensen op te leiden voor het ondersteunen van projecten.

Dit alles combineert Contrast met onderzoek naar de activiteiten van overheidsspelers zoals politie, justitie, inlichtingendiensten en haar private partners zoals bedrijven en stichtingen op het internet. Doel van dit onderzoek is het verkrijgen van meer inzicht in onder andere het witwassen van informatie afkomstig van politie, justitie en inlichtingendiensten, het zogenoemde onschuld-adagium, de toetsing van maatregelen, de rechtsbescherming etc. Het onderzoek valt grofweg uiteen in de volgende onderwerpen: surveillance, huiszoeking en ontruiming.

Surveillance

Surveillance op het internet, denk aan #twicident bij Twitter, Facebook surveillance en andere sociale media, naast het reguliere aftappen. Huiszoeking op het internet (bezoek en kopiëren van gegevens van burgers op privépagina's en gebiedsverboden op het internet, zwarte lijsten, etc.) Ontruiming, huisuitzetting op het internet, notice and takedown en andere acties, zoals inbeslagname van domeinen, servers etc. Meer in het algemeen onderzoek dat verricht wordt door de overheid en particuliere sector naar in beslag genomen servers of draaiende machines op het internet. De publiek–private samenwerking en bestuursrechtelijk en strafrechtelijk optreden op het internet. Maar ook samenwerking tussen justitie en universiteiten zal onderwerp van onderzoek zijn.

Dit alles met als doel om een fair internet te bevorderen, waar de publieke ruimte ook daadwerkelijk van iedereen is en ruimte wordt geboden aan diversiteit. Niet alleen technologische internetgiganten beheersen de digitale wereld, ook de overheid en haar partners patrouilleren steeds frequenter op dit terrein en eigenen zich het recht toe om te bepalen wat wel en niet mag op het internet, meestal zonder onafhankelijke toetsing. Contrast wil daar een tegenwicht aanbieden, hoe klein dat ook is.

Contrast behoudt zich het recht om mensen en organisaties, dan wel hun berichten, te weigeren die seksistisch, racistisch, fascistisch of anderzijds discriminerend van aard zijn. Contrast neemt haar verantwoordelijkheid, maar vraagt van haar gebruikers ook tijd en energie te investeren in de eigen veiligheid op het internet. Een infrastructuur of netwerk en fair internet bouw je namelijk niet alleen op. Contrast vraagt van de mensen die deelnemen aan het alternatieve netwerk ook zelf te investeren in de infrastructuur en het netwerk zodat we elkaar verstevigen.

Functioneert Contrast anders dan vergelijkbare initiatieven met dezelfde insteek? Contrast pretendeert van niet, het netwerk is niet-commercieel maar is niet gratis. Met het initiatief wordt een poging gedaan mensen aan te sporen om bewuster gebruik te maken van het internet, zowel voor zichzelf als voor anderen. Zodra de gebruikers tegen problemen aanlopen, kunnen ze gebruik maken van de helpdesk voor vragen en/of feedback. Zo leren de 'techneuten' waar de knelpunten liggen en helpen zij de deelnemers een stukje verder op weg. Voorbeelden hiervan zijn versleuteld e-mailen, beveiligd chatten en gegevens delen.

Alleen gezamenlijk kunnen deelnemers en techneuten het Contrast-netwerk verstevigen. En iedereen kan leren bewuster om te gaan met moderne communicatiemiddelen.

Vernieuwde website J&J en Contrast Network (pdf)

Naar inhoudsopgave Observant #69

Stay Secure Online 2016

Een gids voor Britse politie functionarissen over hoe zij hun veiligheid op het internet kunnen verbeteren met informatie over privacy instellingen voor sociale media, het veilig surfen op het internet en het gebruik van smartphones en tablets.

Zij schrijven zelf:

"We live in the age of the digital, with information readily accessible to all who seek to find it, including those who we wish to keep it safe from. With every tweet, like or share, our digital footprint grows. It is our responsibility, as individuals, to keep our data safe.

This book provides tips and guidance on protecting your online data across a range of social media platforms, browsers and devices. This guide has been written with sharing in mind so please feel free to share it with family and friends, as in some cases it is they who may be putting information about you online when you would rather they did not."

National Police Chiefs' Council (Verenigd Koninkrijk)

Stay Secure Online 2016

Naar inhoudsopgave Observant #69

Sympathie voor het werk van Buro Jansen & Janssen?

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.

Wordt donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening 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).

Voor Buro Jansen & Janssen betekent dit:

- Een ANBI hoeft geen successierecht of schenkingsrecht te betalen over erfenissen en schenkingen die de ANBI ontvangt in het kader van het algemeen belang.

- Uitkeringen die een ANBI doet in het algemene belang zijn vrijgesteld voor het recht van schenking.

Al 30 jaar diepgravend, kritisch en doortastend burgerrechten onderzoek. Buro Jansen & Janssen, gewoon inhoud

2.3.6 Afscherming

Lessen in veiligheid

openbaar!

Amsterdam, 27 april 2014

Aan Ministerie van Veiligheid en Justitie
Minister
Den Haag

Onderwerp: bezwaar informatieverzoek ideologische misdaad

Geachte

We leven in een tijdperk waarin de overheid intensieve aandacht heeft voor alle data en de zelfredzaamheid van burgers. Burgers zijn zowel verdachte van een mogelijke misstap in de wereld van Big Data, als potentiële werknemers van de BV

De pijlers van deze welzijnsstaat worden getroffen door privatisering, bezuinigingen, schandalen, disfunctioneren en van instanties en het ontspoorde toezicht. . Wij moeten meewerken om de bezuinigingen op allerlei fundamentele voorzieningen mogelijk te maken. Tegelijkertijd wordt geprobeerd die voorzieningen om te vormen tot winstgevende bedrijven.

Als bewoners van Nederland moeten participeren, zal de staat haar informatie en zeggenschap moeten delen. Openbaarheid, medezeggenschap in beleid en transparantie zijn dan logische zaken. Voor een goede controle op de democratische besluitvorming en overheidshandelen is openbaarheid van essentieel belang.

rapport met de titel "Criminaliteitsbeeld Analyse Ideologische Misdaad" geschreven door Het kapitalisme wordt door de Nederlandse politie niet gezien als ideologie.

Zonder deze openbaarheid is controle door de burger niet uitvoerbaar. De transparantie in het huidige Nederland faalt. Burgers mogen hun buren verzorgen, maar niet toezichthouder van de overheid zijn en kunnen het beleid niet mede vormgeven. Na privatisering van een voorziening staat de burger helemaal met lege handen. Buro vecht al dertig jaar voor een meer transparante overheid die rekenschap aflegt niet alleen binnen de politieke arena, maar vooral direct aan haar burgers. Dit doet zij vooral op het terrein van he veiligheidsbeleid, maar meer en meer ook op andere beleidsterreinen. Openbaarheid als uitgangspunt voor een interactieve samenleving, pas dan kan echte participatie plaats vinden.

Buro
Amsterdam
www.burojansen.nl
www.openbaarheid.nl
www.hetnationaalveiligheidsarchief.nl