# 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)