Niet Transparante Wetenschap en Overheid

Buro Jansen & Janssen

Observant #71, februari 2018

Inhoudsopgave Observant #71 / februari 2018

Niet Transparante Wetenschap en Overheid

De treurige stand van de integriteit en openheid van de Nederlandse wetenschappelijke wereld is vervat in een zeer bijzonder advies van het LOWI (Landelijk Orgaan Wetenschappelijke Integriteit). Over het LOWI is veel meer te zeggen, maar zoals altijd doet Buro Jansen & Janssen eerst uitgebreid onderzoek en presenteert dan de feiten, en in het kader een klacht van Buro Jansen & Janssen wordt daarom alleen op het advies ingegaan niet op het orgaan LOWI zelf. De teneur van het verhaal toont grote gelijkenis met een tool die de Nederlandse overheid naar alle waarschijnlijkheid gebruikt, Kailax. Het is een soort zwarte doos met een heel andere achterkant, in het geval van Kailax de Israëlische inlichtingendiensten, erg transparant is daarmee de rechtstaat niet, iets dat ook over de integriteit van de wetenschap gezegd kan worden. Blijkbaar is men blij om gegevens achter te houden en daarmee twijfelachtig onderzoek te blijven steunen, slecht voor de wetenschap, maar ook slecht voor de rechtstaat. Hetzelfde is terug te zien in twee benaderingsverhalen. Druk uitoefenen op burgers, die hun vrienden en bekenden moeten verlinken. Welke rechtsorde van deze intimidatie door de inlichtingendienst beter wordt, is niet duidelijk. En de data die daarmee wordt verzameld zit bij de inlichtingendiensten in het archief. Is dit ook data over kiezers die op bepaalde partijen hebben gestemd? Erg democratisch is die verzameling niet. De rechtsorde is niet gebaat bij een dienst die meekijkt terwijl u uw stem uitbrengt op democratische politieke partijen.

Hoogste orgaan Wetenschappelijke Integriteit (LOWI): Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren. (samenvatting) is een samenvatting van het langere artikel over de klacht van Buro Jansen & Janssen bij het LOWI naar aanleiding van een procedure bij de Universiteit van Leiden.

Hoogste orgaan Wetenschappelijke Integriteit (LOWI): Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren. (uitgebreid) vertelt het verhaal over een advies die het LOWI (Landelijk Orgaan Wetenschappelijke Integriteit) heeft uitgebracht in de klacht van Buro Jansen & Janssen over het rapport van de Universiteit van Leiden van 2014 'Etnisch profileren in Den Haag. Een verkennend onderzoek naar opvattingen en beslissingen op straat'.

Volgens het LOWI is “het niet expliciet vermelden van afspraken met de politie Haaglanden en van het lidmaatschap van professor Van der Leun van de Adviesraad van de politie Haaglanden niet heel transparant te noemen.” In haar eindconclusie oordeelt het LOWI echter dat er geen sprake van een schending van de wetenschappelijke integriteit. Het LOWI advies heeft dan ook geen verdere consequenties voor onderzoeksleider Van der Leun.

Kailax technical details describes the technical details of a tool called Kailax. Buro Jansen has previously written about Kailax in the article ‘Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence’. This piece focuses on some of the technical details of the Unlocker and a few mysteries that still need solving. All of this information is coming from the HackingTeam leak that happened in 2014.

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence is an English translation of an article which was published in the beginning of 2017 and deals with the Kailax Unlocker which is exemplary of the secrecy and lack of transparency surrounding the trade in digital weapons. The Unlocker is a tool with which a burglar can gain entrance to any Windows computer, without the owner becoming aware.

There is hardly any information about the Unlocker and its manufacturer Kailax in the public domain. The website www.kailax.com only contains the address details of the company (an address in Singapore), but no additional information. From public sources, we can only gather that the Berlin based company 2beuropa serves as an intermediary for Kailax.

When the Dutch secret service came knocking on my door *is* the account of how the Dutch secret service (AIVD) approached Jurre van Bergen in 2013, and how he understands the events that took place. He was a student until summer 2013, and after OHM2013 was hired at an internet service provider. He also did some technical consulting and digital security trainings for Publeaks during that time. This is all prior to my involvement in Tails.

It is important to tell the whole story, the run up to the approach, the approach itself, how and when it happened, and discuss the aftermath. This is not an isolated incident but rather a pattern of harassment of hackers and other communities. With the new Dutch security services law coming up now, the services will gain additional measures and more power, he thinks this story is more relevant than ever.

Interesse AIVD voor Marokkaanse solidariteitsnetwerken vertelt het verhaal van 'Daan' die vanwege zijn betrokkenheid bij netwerken die in Nederland protestacties organiseren uit steun voor onderdrukte Marokkanen in het land van herkomst. 'Daan' werd divere keren door de AIVD benaderd. Op een manier die door hem als intimiderend werd ervaren.

Bulk gegevens verzamelen is van alle tijden, hield de BVD in de jaren tachtig mensen die op de Centrum Partij stemden in de gaten?, beschrijft informatie uit BVD-documenten waaruit blijkt dat de geheime dienst in de vorige eeuw zeer uitvoerig de extreem-rechtse partij CP in de gaten hield. Hier was sprake van analoge bulkinterceptie waarbij ook niet aan de partij gelieerde personen het doelwit waren.

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

Hoogste orgaan Wetenschappelijke Integriteit: Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren.

Het LOWI (Landelijk Orgaan Wetenschappelijke Integriteit) heeft advies uitgebracht in de klacht van Buro Jansen & Janssen over het rapport van de Universiteit van Leiden van 2014 'Etnisch profileren in Den Haag. Een verkennend onderzoek naar opvattingen en beslissingen op straat'.

Volgens het LOWI is "het niet expliciet vermelden van afspraken met de politie Haaglanden en van het lidmaatschap van professor Van der Leun van de Adviesraad van de politie Haaglanden niet heel transparant te noemen." In haar eindconclusie oordeelt het LOWI echter dat er geen sprake van een schending van de wetenschappelijke integriteit. Het LOWI advies heeft dan ook geen verdere consequenties voor onderzoeksleider Van der Leun.

Buro Jansen & Janssen diende een klacht in bij het LOWI, omdat het de totstandkoming van het Leidse rapport in strijd acht met de beginselen van eerlijkheid en zorgvuldigheid, controleerbaarheid, onpartijdigheid en onafhankelijkheid, zoals vastgelegd in de Gedragscode Wetenschapsbeoefening. Het LOWI is een onafhankelijk adviesorgaan dat de besturen van de bij het LOWI aangesloten instellingen adviseert over mogelijke schendingen van wetenschappelijke integriteit.

Het onderzoek van de Universiteit van Leiden en het optreden van professor Van der Leun zijn weinig transparant. De Universiteit van Leiden heeft het bestaan van de twee scripties die ten grondslag leggen aan het Leidse rapport altijd verzwegen, weigert deze openbaar te maken en wekt hiermee de indruk iets te verbergen te hebben. In het LOWI advies wordt het gebrek aan transparantie

deels onderkend, maar het LOWI kan de indruk niet wegnemen dat er inderdaad iets te verbergen valt.

Notulen

Het LOWI advies is om meerdere redenen opmerkelijk. Volgens de notulen van de korpsdirectie Haaglanden (door Buro Jansen & Janssen van de politie Haaglanden verkregen via een WOB verzoek) maakten de universiteit en de politie voorafgaande aan het onderzoek afspraken om een afbreukrisico te voorkomen wanneer het onderzoek zou wijzen op de mogelijke discriminatie door de Haagse politie.

Het LOWI beoordeelt de afspraken tussen de Universiteit van Leiden en de politie Haaglanden echter als 'gebruikelijke en niet afwijkende afspraken'. Het LOWI lijkt zich vooral te baseren op de verklaringen van onderzoeksleider Van der Leun, volgens wie er afspraken zijn gemaakt over onder meer de zorgvuldigheid van formuleren en anonimisering van individuele politieagenten. Wanneer er alleen gebruikelijke en niet afwijkende afspraken zijn gemaakt, valt echter moeilijk in te zien waarom het niet vermelden hiervan in het rapport door het LOWI als niet heel transparant wordt beoordeeld.

Het LOWI maakt in haar advies niet duidelijk of het de in de notulen vermeldde afspraak als 'gebruikelijk en niet afwijkend' beoordeelt, of dat men aanleiding heeft om te twijfelen aan de juistheid van de notulen.

Belangenverstrengeling

Het LOWI beoordeelt het niet vermelden in het rapport van het lidmaatschap van professor Van der Leun van de Adviescommissie Politie Haaglanden als "niet heel transparant", maar niet als een schending van de wetenschappelijke integriteit. Het LOWI beschouwt het lidmaatschap namelijk als "te weinig substantieel of concreet is om te veronderstellen dat Belanghebbende een persoonlijk belang zou hebben bij (de uitkomsten van) het onderzoek." Dit is opmerkelijk, aangezien het adviseurschap van wetenschappelijk onderzoekers volgens artikel 5.3 van de Gedragscode Wetenschapsbeoefening vermeldt dient te worden in publicaties.

Het LOWI maakt in haar advies echter niet duidelijk of het lidmaatschap van de Adviesraad beoordeelt als een adviseurschap zoals bedoeld in artikel 5.3 van de Gedragscode.

Het LOWI stelt in haar advies: "in redelijkheid kan niet worden gezegd dat de schijn van belangenverstrengeling is gewekt". Uit via de WOB openbaar gemaakte documenten blijkt echter dat professor Van der Leun in juli 2013 het initiatief nam voor nauwere samenwerking met de politie Haaglanden door middel van het opstellen van een convenant, hetgeen in januari 2014 leidde tot de ondertekening van een Verklaring tot intentie van samenwerking. In het Leidse rapport wordt dit niet vermeld, hoewel mogelijke schijn van belangenverstrengeling volgens de Gedragscode altijd dient te worden vermeden dan vermeld in publicaties. Volgens het LOWI is er echter te weinig aanleiding om te twijfelen aan de onafhankelijkheid van Van der Leun.

Scripties

Uit via de WOB openbaar gemaakte documenten blijk dat het Leidse rapport is gebaseerd op veldwerk dat twee masterstudenten criminologie in 2012 ten behoeve hun scripties uitvoerden. Toen het Ministerie van Veiligheid en Justitie en het Haagse gemeentebestuur eind 2013 de Tweede Kamer en de Haagse Gemeenteraad een onderzoek naar etnisch profileren toezegden, waren de scripties al afgerond en de conclusies van de scripties dus al bekend. De Universiteit van Leiden heeft nooit melding gemaakt van de scripties weigert om de scripties openbaar te maken en heeft de Tweede Kamer en de Haagse gemeenteraad herhaaldelijk onjuist en onvolledig geïnformeerd.

Het LOWI beoordeelt deze gang van zaken niet als problematisch en stelt: "De wijze waarop de scripties en het rapport in onderlinge samenhang tot stand zijn gekomen, is niet heel uitzonderlijk". Volgens het LOWI was er "vanuit wetenschappelijke integriteit ook geen noodzaak om in het rapport expliciet melding te maken van de scripties."

Het is opmerkelijk dat het LOWI in haar advies de overeenkomsten tussen het rapport en de scripties niet concreet benoemt. Volgens LOWI is het een "onjuiste aanname dat scripties en rapport

grotendeels overeenkomen", maar zijn "er inderdaad ook wel overeenkomsten". Volgens het LOWI bevat het rapport andere onderzoeksvragen en nieuwe analyses, maar de onderzoeksvragen en conclusies van de scripties worden in het advies niet benoemd. Hiermee blijft onduidelijk welke onderzoeksvragen en analyses in het rapport nieuw zijn, en welke ook in de scripties voorkomen.

Het LOWI had op eenvoudige wijze meer duidelijkheid kunnen geven over de overeenkomsten en verschillen tussen het rapport en de scripties door ten minste de onderzoeksvragen en conclusies van de scripties in haar advies te benoemen, maar heeft dit nagelaten. Dit klemt daar enkele door de politie Haaglanden via de WOB openbaar gemaakte documenten indiceren dat de onderzoeksvragen en conclusies van het rapport en de scripties substantieel overeenkomen.

Hoogste orgaan Wetenschappelijke Integriteit: Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren.(samenvatting)(pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Hoogste orgaan Wetenschappelijke Integriteit (LOWI): Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren. (uitgebreid)

Het LOWI-advies 2017 nr. 9

Samenvatting van LOWI-advies 2017, nr. 9

Reactie op het verweerschrift van de Universiteit van Leiden van 10 april 2017

bezwaar besluit College van Bestuur Universiteit Leiden met betrekking tot formele klacht/melding rapport 'Etnisch profileren in Den Haag? Een verkennend onderzoek naar beslissingen en opvattingen op straat' van de Universiteit Leiden

Universiteit mag data geheim houden

Antwoorden Burgemeester en Minister scheppen meer onduidelijkheid over etnisch profileren onderzoek Leiden

Wetenschappers in dienst van de overheid (kort)

Wetenschappers in dienst van de overheid

Professoren als spreekbuis van de politie (kort)

Professoren als spreekbuis van de politie

In vogelvlucht, Wetenschappelijk onderzoek naar politiediscriminatie

Naar inhoudsopgave Observant #71

Hoogste orgaan Wetenschappelijke Integriteit: Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren.

Het LOWI (Landelijk Orgaan Wetenschappelijke Integriteit) heeft advies uitgebracht in de klacht van Buro Jansen & Janssen over het rapport van de Universiteit van Leiden van 2014 'Etnisch profileren in Den Haag. Een verkennend onderzoek naar opvattingen en beslissingen op straat'.

Volgens het LOWI is "het niet expliciet vermelden van afspraken met de politie Haaglanden en van het lidmaatschap van professor Van der Leun van de Adviesraad van de politie Haaglanden niet heel transparant te noemen." In haar eindconclusie oordeelt het LOWI echter dat er geen sprake van een schending van de wetenschappelijke integriteit. Het LOWI advies heeft dan ook geen verdere consequenties voor onderzoeksleider professor Joanne van der Leun.

Voorgeschiedenis

Het onderzoek van de Universiteit van Leiden staat al enige jaren ter discussie. In de Tweede Kamer en in de Haagse gemeenteraad werd eind 2013 gevraagd om een wetenschappelijk onderzoek naar het plaatsvinden van etnisch profileren, onder meer naar aanleiding van aanhoudende berichtgeving over politiediscriminatie in de Haagse Schilderswijk. Hierop zegden de Minister van Veiligheid en Justitie en het Haags gemeentebestuur eind 2013 een onderzoek door de Universiteit van Leiden toe, onder leiding van professor Joanne van der Leun van het Instituut voor Strafrecht & Criminologie van de Faculteit der Rechtsgeleerdheid van de Universiteit van Leiden.

De Universiteit van Leiden publiceerde in 2014 het onderzoek 'Etnisch profileren in Den Haag. Een verkennend onderzoek naar beslissingen en opvattingen op straat'. Hierin werd onder meer geconcludeerd dat er geen aanwijzingen zijn voor het structureel plaatsvinden van etnisch profileren. De kwaliteit van het Leidse rapport riep vragen op, onder meer bij een toelichting onder wetenschappers in de Haagse gemeenteraad in juni 2014.

Buro Jansen & Janssen verzocht in 2015 door middel van een beroep op de Wet Openbaarheid Bestuur bij het Ministerie van Veiligheid en Justitie, de politie Haaglanden, het Openbaar Ministerie, en de Universiteit van Leiden om openbaarmaking van de twee scripties, het onderliggende onderzoeksmateriaal en andere documenten rond de totstandkoming van het onderzoek. Het Ministerie en de politie Haaglanden maakten hierop enige stukken (met name interne e-mails en notities) openbaar, maar niet de twee scripties. De Universiteit maakte het bij de politie Haaglanden in 2011 ingediende onderzoeksvoorstel openbaar en weigert om de twee scripties en het onderliggende onderzoeksmateriaal openbaar te maken.

Uit de via WOB openbaar gemaakte documenten blijkt dat de Universiteit van Leiden de politie Haaglanden in 2011 benaderde met een onderzoeksvoorstel voor twee masterstudenten criminologie. Afgesproken werd dat de scripties in eerste instantie bedoeld waren voor intern gebruik door de politie Haaglanden. Voorafgaande aan het onderzoek maakten de universiteit en de politie afspraken om een afbreukrisico te voorkomen wanneer het onderzoek zou wijzen op de mogelijke discriminatie door de Haagse politie. De twee studenten verrichtten hun veldwerk in 2012 en rondden hun scripties in augustus 2013 af. Toen de Minister van Veiligheid en Justitie en het Haags gemeentebestuur eind 2013 een onderzoek naar etnisch profileren toezegden, waren de conclusies van de scripties dus al bekend. De Universiteit van Leiden heeft het bestaan van de scripties niet in het rapport vermeld. Ook heeft professor Van der Leun de scripties niet genoemd bij diverse publieke optredens, en hiermee de Tweede Kamer en de Haagse gemeenteraad dus onjuist en onvolledig geïnformeerd.

Buro Jansen & Janssen publiceerde in mei 2016 haar bevindingen in ‘Wetenschappers in dienst van de overheid. Het onderzoek van de Universiteit van Leiden naar etnisch profileren: een reconstructie’. https://respubca.home.xs4all.nl/pdf/wetenschappersindienstvandeoverheidobservant68bjjapril2016.pdf

Dit leidde tot Kamervragen en vragen in de Haagse gemeenteraad, maar niet tot meer duidelijkheid over de totstandkoming van het onderzoek, de gemaakte afspraken tussen de Universiteit van Leiden

en de politie Haaglanden, en de overeenkomsten tussen het rapport en de scripties.
Buro Jansen & Janssen diende in 2016 een klacht in bij de Commissie Wetenschappelijke Integriteit van de Universiteit van Leiden, wegens schending van de wetenschappelijke integriteit, omdat het Leidse rapport in strijd acht met de beginselen van eerlijkheid en zorgvuldigheid, controleerbaarheid, onpartijdigheid en onafhankelijkheid, zoals vastgelegd in de Gedragscode Wetenschapsbeoefening. Deze klacht werd in december 2016 afgewezen.

Vervolgens werd in januari 2017 een klacht ingediend bij het LOWI (Landelijk Orgaan Wetenschappelijke Integriteit). Het LOWI is een onafhankelijk adviesorgaan dat de besturen van de bij het LOWI aangesloten instellingen adviseert over mogelijke schendingen van wetenschappelijke integriteit. Het LOWI neemt uitsluitend een verzoek in behandeling nadat de instelling waar de schending zou hebben plaatsgevonden, een (voorlopig) besluit heeft genomen. Het LOWI bracht advies uit middels Advies (2017/9, gedateerd 29 juni 2017, gepubliceerd in september 2017)
https://www.lowi.nl/nl/bestanden/LOWIadvies2017nr.9.pdf

In december 2017 verzocht Buro Jansen & Janssen het CWI en het LOWI om een verduidelijking van het advies, omdat sommige passages in het advies niet eenduidig te interpreteren zijn. Het CWI heeft in het geheel niet gereageerd op dit verzoek. Het LOWI reageerde wel, maar gaf aan de vragen niet te beantwoorden. "Hoewel er begrip is voor de behoefte van het Buro aan een nadere toelichting, zal het LOWI die dan ook niet geven.", aldus het LOWI in antwoord op Buro Jansen & Janssen.

Afspraken

In de notulen van het Overleg Korpsdirectie van de Haagse politie van 27 december 2011 (via de WOB openbaar gemaakt door de politie Haaglanden) staat vermeld: "Afbreukrisico kan zijn dat het de aandacht kan vestigen op (mogelijke) discriminatie door de politie. Dit risico is met prof. Van der Leun besproken. Zij begrijpt de onwenselijkheid hiervan en heeft aangegeven dat zij dit punt

expliciet zal bespreken met de studenten en dat ze hierop zal letten bij de tussentijdse besprekingen van de (concept)scripties."

In het LOWI advies wordt onderkend dat de Universiteit van Leiden en de Politie Haaglanden voorafgaand aan het onderzoek afspraken hebben gemaakt, maar het betreft volgens het LOWI "gebruikelijke en niet afwijkende afspraken". Het LOWI baseert zich hierbij op verklaringen van professor Van der Leun. "Belanghebbende heeft aan de CWI (Commissie Wetenschappelijke Integriteit van de Universiteit van Leiden) toegelicht welke soort afspraken zijn gemaakt. Het gaat om de scope van het onderzoek (het LOWI begrijpt: …), de onderzoeksvragen, de vertrouwelijkheid, het anonimiseren, de zorgvuldigheid van formuleren en de gelegenheid om het conceptrapport te controleren op feitelijke onjuistheden", aldus het LOWI advies.

Het LOWI overweegt ten aanzien van de afspraken: "Het zijn afspraken die in beginsel geen afbreuk doen aan de integriteit van het onderzoek of Belanghebbende". Het LOWI stelt echter ook dat het "mede vanwege de gevoeligheid van het onderwerp, gelukkiger geweest wanneer in het rapport expliciet melding was gemaakt van deze afspraken". Het LOWI vervolgt: "Maar het achterwege blijven daarvan kan niet leiden tot het oordeel dat Belanghebbende de wetenschappelijke integriteit heeft geschonden. Redengevend is dat het gaat om gebruikelijke en niet afwijkende afspraken." Het LOWI concludeert: "Het bestaan van afspraken die strijdig zouden kunnen zijn met de regels van wetenschappelijke integriteit, is niet aannemelijk gemaakt en de afspraken waarvan wel gebleken is dat ze zijn gemaakt, leveren geen strijd op met die regels." (…) "Het niet expliciet vermelden van gemaakte afspraken (...) is niet heel transparant te noemen, maar onvoldoende voor het oordeel dat Belanghebbende de wetenschappelijke integriteit heeft geschonden".

Het advies is opmerkelijk. Wanneer er alleen 'gebruikelijke en niet afwijkende afspraken' zijn gemaakt, valt moeilijk in te zien waarom het niet vermelden hiervan in het rapport door het LOWI als niet heel transparant wordt beoordeeld. Afspraken over bijvoorbeeld zorgvuldigheid van formuleren en anonimisering van individuele politieagenten zijn immers gebruikelijke en vanzelfsprekende wetenschappelijke afspraken, die geen aparte vermelding in wetenschappelijke publicaties lijken te behoeven.

Het is onduidelijk in hoeverre het LOWI de inhoud van de notulen van de korpsdirectie in haar advies heeft betrokken. Het advies geeft namelijk een onvolledige weergave van de WOB documenten (i.c. de notulen van de Korpsdirectie Politie Haaglanden) en stelt: "uit de WOB stukken (…) blijkt alleen dat er bij X(politie Haaglanden) ten aanzien van de scripties enige zorg was over een mogelijk afbreukrisico. Daarover zou zijn gesproken met Belanghebbende(professor Van der Leun). Uit deze stukken kan echter niet worden opgemaakt dat Belanghebbende daadwerkelijk afspraken heeft gemaakt over de uitkomsten en conclusies van de scripties danwel het onderzoek "

De weergave in het LOWI advies is om meerdere redenen onvolledig. Volgens het LOWI bestond er
bij de politie Haaglanden enige zorg over een mogelijk afbreukrisico, maar volgens de notulen bestond deze zorg echter ook bij professor Van der Leun. De notulen vermelden immers dat zij "de onwenselijkheid hiervan begrijpt" - hiermee wordt verwezen naar het afbreukrisico wanneer het onderzoek de aandacht vestigt op (mogelijke) discriminatie door de politie.

Daarnaast stelt het LOWI dat er "zou er zijn gesproken" door de politie en de universiteit. Met deze formulering wordt het plaatsvinden van een dergelijk gesprek in twijfel getrokken. De notulen zijn op dit punt echter eenduidig en vermelden dat er is gesproken.

Tenslotte stelt het LOWI dat "uit deze stukken echter niet kan worden opgemaakt dat Belanghebbende daadwerkelijk afspraken heeft gemaakt over de uitkomsten en conclusies van de scripties danwel het onderzoek ". Hiermee gaat het advies dus voorbij aan het feit dat de notulen een concrete afspraak vermelden, namelijk dat Van der Leun het afbreukrisico van het onderzoek (dat het de aandacht kan vestigen op mogelijke discriminatie door de politie) expliciet zal bespreken met de studenten en hierop zal letten bij de besprekingen van het (concept) scripties.

Het LOWI citeert dus onvolledig uit de notulen. Ook enkele andere passages in het advies, waarin wordt verwezen naar de notulen, wekken bevreemding. Zo stelt het LOWI dat "Verzoeker heeft ook

ten aanzien van de scripties gesteld dat er ongeoorloofde afspraken zijn gemaakt met X (politie Haaglanden), maar ook van die afspraken is niet gebleken" en "Verzoeker heeft geen stukken overlegd waaruit het feitelijk bestaan van dergelijke afspraken is gebleken".

Bovenstaande passages vallen moeilijk te duiden. Buro Jansen & Janssen heeft stukken overlegd die gewag maken van het bestaan van afspraken over een afbreukrisico van het onderzoek. De in de notulen van de politie Haaglanden vermeldde afspraken zijn evident van invloed op de inhoud van de scripties: Van der Leun zal het afbreukrisico expliciet bespreken met de studenten, en hierop letten bij de tussentijdse besprekingen van de scripties. De precieze impact van het 'expliciet bespreken' en 'hierop letten' op de inhoud en conclusies van het onderzoek kan moeilijk beoordeeld worden. Het lijkt echter evident dat een transparant onderzoek naar het plaatsvinden van etnisch profileren bemoeilijkt wordt door vooraf af te spreken dat het onwenselijk is wanneer het onderzoek zal wijzen op discriminatie. Het is niet bekend in hoeverre deze afspraak tot aanpassingen van de scripties heeft geleid, welke onderzoeksresultaten en bevindingen mogelijk niet, of in aangepaste vorm, in de scripties en later in het Leidse rapport zijn opgenomen. De reden hiervoor is echter op de eerste plaats het gebrek aan transparantie van de Universiteit van Leiden, die zelf nooit gewag heeft gemaakt van de afspraken en de scripties. De universiteit weigert om de twee scripties openbaar te maken, waardoor het onmogelijk is om de inhoud van het rapport en de twee scripties met elkaar te vergelijken.

Buro Jansen & Janssen heeft het LOWI om een verduidelijking van haar advies verzocht en gevraagd of het de in de notulen vermeldde afspraak beoordeelt als een 'gebruikelijke niet afwijkende afspraak', of als 'een ongeoorloofde afspraak'. Het LOWI heeft niet geantwoord.

Mogelijk beoordeelt het LOWI de notulen van de korpsdirectie niet als een getrouwe weergave van de gesprekken tussen de Universiteit van Leiden en de politie Haaglanden, maar het advies bevat geen overwegingen hieromtrent. Buro Jansen & Janssen heeft het LOWI gevraagd of het aanleiding heeft om te veronderstellen dat de notulen geen getrouwe weergave vormen van de gevoerde

gesprekken, en welke overwegingen het in deze heeft. Het LOWI heeft niet geantwoord.

De onduidelijkheid in het LOWI advies over de inhoud van de gemaakte afspraken klemt te meer, daar bij het onderzoek betrokken partijen verschillende verklaringen hebben afgelegd over de vraag of er voorafgaand aan het onderzoek is gesproken over een mogelijk afbreukrisico van het onderzoek. Van der Leun ontkende in een artikel met NRC Handelsblad van 30 april 2016 dat ze met de politie Haaglanden heeft gesproken over een afbreukrisico. In het artikel wordt haar reactie gevraagd ten aanzien van het gebruik van het woord afbreukrisico: "Ze ontkent dat ze met de politie heeft gesproken over een mogelijk 'afbreukrisico'. In de gesprekken met de politie heb ik dat woord nooit gehoord, zegt ze. De hoogleraar vermoedt dat de politie haar in interne correspondentie woorden in de mond heeft gelegd die zij nooit heeft uitgesproken," aldus het NRC artikel.

De verklaringen van der Leun staan dus haaks op de notulen van de korpsdirectie, en verschillen tevens met de verklaringen van toenmalig Minister van Veiligheid en Justitie Van der Steur. Hij verklaarde in 2016 dat de Universiteit van Leiden en de Politie Haaglanden wel degelijk gesproken hebben over mogelijke afbreukrisico's van het onderzoek. Van der Steur antwoordde op Kamervragen: "In de afweging om medewerking te verlenen zijn door de politieleiding en de Universiteit van Leiden ook mogelijke afbreukrisico's besproken." Van der Steur gaf echter een andere betekenis aan de term afbreukrisico dan de notulen van de korpsdirectie: "Die (afspraken) zien op het feit dat individuele politieambtenaren zich open en kwetsbaar op zouden stellen door medewerking te verlenen aan het onderzoek." (Antwoord Minister Van der Steur 24 mei 2016 op Kamervragen Marcouch).

Overeenkomsten tussen de scripties en het rapport

Uit de via de WOB openbaar gemaakte documenten blijkt dat de twee scripties in augustus 2013 waren afgerond. Toen het Ministerie van Veiligheid en Justitie en het Haags gemeentebestuur eind 2013 een onderzoek naar etnisch profileren toezegden, waren de

conclusies van de scripties dus al bekend. De Universiteit van Leiden heeft het bestaan van de twee scripties nooit vermeld.

Het LOWI beoordeelt deze gang van zaken in niet als bezwaarlijk. Het advies stelt: "De wijze waarop de scripties en het rapport in onderlinge samenhang tot stand zijn gekomen, is niet heel uitzonderlijk. Dat de scripties niet openbaar zijn is een terechte keuze en levert geen strijd op met de wetenschappelijke integriteit. Er was vanuit wetenschappelijke integriteit ook geen noodzaak om in het rapport expliciet melding te maken van de scripties." Volgens het LOWI is er ook geen sprake van plagiaat, omdat het rapport andere onderzoeksvragen beantwoordt dan de scripties en additionele informatie bevat, de studenten in het rapport als co auteur worden genoemd, er geen verplichting is om in rapport duidelijk te maken welke delen afkomstig zijn uit scripties, en het rapport de eerste openbare presentatie van de data was.

Omdat de Universiteit van Leiden weigert om de twee scripties openbaar te maken is het onmogelijk om de inhoud van het rapport en de scripties met elkaar te vergelijken. Het LOWI heeft - volgens haar advies - de twee scripties ingezien. Volgens het LOWI is het "een onjuiste aanname dat de onderzoeksvragen en de bevindingen in de scripties en het rapport grotendeels overeenkomen", maar "er zijn inderdaad ook wel overeenkomsten tussen de scripties en het rapport". Het LOWI vervolgt: "Gebleken is dat, kort samengevat, (de data uit) de scripties de basis vormen voor dit rapport, waarin echter andere onderzoeksvragen zijn gesteld en waarin nieuwe analyses zijn weergegeven".

Het LOWI gaat in haar advies dus niet concreet in op de overeenkomsten en verschillen tussen het rapport en de scripties. Volgens het LOWI bevat het rapport andere onderzoeksvragen en nieuwe analyses, maar hiermee blijft onduidelijk welke onderzoeksvragen en analyses nieuw zijn, en welke ook al in de scripties voorkomen. Buro Jansen & Janssen heeft het LOWI om een verduidelijking verzocht en gevraagd of geen van de vier onderzoeksvragen in het rapport in de scripties behandeld worden, of dat sommige onderzoeksvragen in de scripties overeenkomen met die in het rapport en het rapport daarnaast andere onderzoeksvragen bevat? Het LOWI heeft geen antwoord gegeven.

Het LOWI advies is opmerkelijk, aangezien de politie Haaglanden in 2016 via de WOB enkele documenten openbaar heeft gemaakt die indiceren dat het rapport en de scripties substantieel overeenkomen. Het betreft met name de documenten Uitkomst Onderzoek (van eind 2013) en Factsheet Onderzoek (van augustus 2013). Deze documenten bevatten (volgens de politie Haaglanden in haar toelichting bij de beantwoording van het WOB verzoek van Buro Jansen & Janssen) een samenvatting van de opzet en conclusies van de scripties. De documenten duiden er sterk op dat ten minste twee van de vier onderzoeksvragen uit het rapport ook in de scripties behandeld worden.

Het Leidse rapport bevat vier onderzoeksvragen, die op pagina 8 van het rapport genoemd worden:
1 In hoeverre kunnen beslissingen van agenten om in concrete situaties te handelen worden gerechtvaardigd in die situatie en welke rol spelen etniciteit en/of huidskleur daarbinnen?
2 Welke opvattingen hebben politieagenten over het plaatsvinden van etnisch profileren.
3 Welke ervaringen hebben jongvolwassenen met de politie
4 Welke opvattingen hebben jongvolwassenen over etnisch profileren.

Uit het document Uitkomst Onderzoek blijkt dat onderzoeksvraag 2 en 4 ook behandeld worden in één van de scripties. De titel van deze scriptie luidt namelijk: 'Vertrouwen in de politie en opvattingen over etnisch profileren: Een kwantitatieve en kwalitatieve studie naar het vertrouwen van jongvolwassenen in de politie en de opvattingen over etnisch profileren bij jongvolwassenen en politieambtenaren'. Het document Uitkomst onderzoek indiceert ook anderszins dat de onderzoeksvragen 2 en 4 behandeld worden in de scripties. Het document stelt: "Ruim een derde van de jongvolwassenen rapporteert een persoonlijke ervaring met etnisch profileren." Het rapport stelt op pagina 36 iets vergelijkbaars: "Aan jongvolwassenen is gevraagd of zij zelf ooit het gevoel hebben gehad dat zij alleen vanwege hun etnische achtergrond werden gestopt. Hierop antwoordden 81 van de 205 jongvolwassenen dat zij dit ooit ervaren hebben.

Ook een interne nota van het Ministerie van Veiligheid en Justitie van 12 november 2013 (via de WOB openbaar gemaakt) indiceert

dat de onderzoeksvragen van het rapport en de scripties substantieel overeenkomen. Ambtenaren schrijven hierin: "De universiteit Leiden heeft het veldonderzoek reeds afgerond. Hierdoor is geen invloed meer mogelijk op de onderzoeksopdracht."

Het LOWI gaat in haar advies niet inhoudelijk in op bovengenoemde WOB documenten. Wel is het opmerkelijk dat in paragraaf 3.2 van het advies (in de samenvatting van het verweerschrift van het College van Bestuur van de Universiteit van Leiden) wordt gesteld dat "de onderzoeksvraag van het rapport geheel anders is dan die van de scripties". Deze passage valt moeilijk te duiden, aangezien het rapport vier onderzoeksvragen bevat. Buro Jansen & Janssen heeft het LOWI om een verduidelijking verzocht en gevraagd op welke van de vier onderzoeksvragen in paragraaf 3.2 van het advies wordt gedoeld. Het LOWI heeft geen antwoord gegeven.

Hoewel het LOWI (summier) ingaat op de onderzoeksvragen van het rapport en de scripties, wordt in het advies in het geheel niet ingegaan op de conclusies van het rapport en de scripties, en de overeenkomsten en verschillen hiertussen. Dit is opmerkelijk, omdat via de WOB openbaar gemaakte documenten indiceren dat de conclusies substantieel overeenkomen.

Een conclusie van het Leidse rapport is dat er geen aanwijzingen zijn voor het structureel plaatsvinden van etnisch profileren. De via de WOB door de politie Haaglanden openbaar gemaakte documenten bevatten vergelijkbare noties. Zo stelt de Factsheet Onderzoek: "Dat etnisch profileren door de politie, ook in Den Haag, wel eens voorkomt, wordt van politiezijde niet ontkend. Op basis van de ervaringen tot dusverre wijst volgens de onderzoekers echter niets erop dat etnisch profileren een structureel probleem is." De Notitie Onderzoek naar etnisch profileren in eenheid Den Haag stelt: "Dat etnisch profileren door de politie, ook in Den Haag, wel eens voorkomt is bekend. Op basis van de ervaringen tot nu toe wijst ook volgens de onderzoekers er tot dusverre echter niets op, dat het een structureel probleem is. Ook het onderzoek dat in Den Haag plaatsvindt, wijst daar niet op. De conclusie dat het wel een structureel probleem zou zijn, komt volledig voor de rekening van Amnesty." Het LOWI gaat in haar advies echter niet inhoudelijk in op bovengenoemde WOB documenten.

Het LOWI benoemt de overeenkomsten en verschillen tussen het rapport en de scripties dus niet concreet. Omdat de Universiteit van Leiden weigert om de scripties openbaar te maken, kunnen de inhoud van het rapport en de scripties niet met elkaar vergeleken worden. Het LOWI had op eenvoudige wijze meer duidelijkheid kunnen verschaffen over de overeenkomsten tussen het rapport en de scripties door de onderzoeksvragen en conclusies van de scripties in haar advies expliciet te benoemen. Het LOWI heeft dit echter nagelaten.

Buro Jansen & Janssen heeft het LOWI gevraagd naar haar overwegingen om de onderzoeksvragen en conclusies van de scripties in het advies niet te benoemen. Het LOWI heeft geen antwoord gegeven.

Openbaar maken van de scripties

De Universiteit van Leiden weigert om de twee scripties openbaar te maken. Het LOWI beoordeelt dit in haar advies als terecht. "Dat de scripties niet openbaar zijn is een terechte keuze en levert geen strijd op met de wetenschappelijke integriteit", aldus het advies. Het LOWI overweegt hiertoe dat "de data uit interviews niet waren verkregen als anonimiteit niet was gegarandeerd, dat de beloofde anonimiteit borgen een verantwoordelijkheid van de onderzoekers is(…) en in dit geval kan dat alleen door de scripties niet openbaar te maken".

Buro Jansen & Janssen pleit voor openbaar making van de scripties. Etnisch profileren is een maatschappelijk gevoelig thema dat transparant onderzoek behoeft. Openbaar making van de scripties past hierbij.

Het LOWI onderkent in haar advies dat etnisch profileren een maatschappelijk gevoelig thema is, en onderkent tevens dat er een maatschappelijk belang bestaat bij het openbaar maken van de scripties. Het LOWI beschouwt dit maatschappelijk belang echter als minder zwaarwegend dan het belang van anonimisering van individuele politieagente die in het kader van het onderzoek zijn geïnterviewd of geobserveerd. Het advies stelt: "Omdat anonimiteit niet kan worden kon worden gegarandeerd, is het ethisch verantwoord en in het belang van X (de politie Haaglanden) en

onderzoeksgroep om de scripties niet openbaar te laten zijn. Dit weegt zwaarder dan het belang van Verzoeker of algemeen van het publiek om de data zelf te kunnen controleren."

De redenering van het LOWI is opmerkelijk. Bij het openbaar maken van documenten via de WOB is het immers gebruikelijk dat onderdelen van documenten zwart en/of onleesbaar worden gemaakt wanneer het bijvoorbeeld gaat om persoonsgegevens of wanneer de anonimisering van individuen anderzijds in het geding is. Het valt moeilijk in te zien waarom deze handelwijze niet gehanteerd zou kunnen worden bij het openbaar maken van de twee scripties.

Lidmaatschap Adviesraad

Professor Van der Leun maakte tijdens het onderzoek deel uit van de Adviesraad van de Politie Haaglanden. Dit wordt in het Leidse rapport niet vermeld.

Volgens het LOWI leidt het lidmaatschap van de Adviesraad niet tot belangenverstrengeling. Als reden hiervoor noemt het LOWI dat "X (de politie Haaglanden) niet de opdrachtgever was van het rapport of de scripties" en dat "de betrokkenheid van Belanghebbende bij X (politie Haaglanden) in een adviescommissie te weinig substantieel of concreet is om te veronderstellen dat Belanghebbende een persoonlijk belang zou hebben bij (de uitkomsten van) het onderzoek". Het LOWI merkt hierbij op dat Van der Leun's lidmaatschap van de adviesraad wel vermeld stond op haar persoonlijke pagina op de website van de Universiteit van Leiden. Wel overweegt het LOWI: "Wel was het, mede vanwege de gevoeligheid van het onderwerp, gelukkiger geweest wanneer in het rapport melding was gemaakt van met name het lidmaatschap van de adviescommissie". Het LOWI concludeert: "In redelijkheid kan niet worden gezegd dat de schijn van belangenverstrengeling is gewekt. Het niet expliciet vermelden van het lidmaatschap van de adviescommissie is niet heel transparant te noemen, maar onvoldoende voor het oordeel dat Belanghebbende de wetenschappelijke integriteit heeft geschonden."

De redenering van het LOWI is opmerkelijk. Volgens het LOWI leidt het lidmaatschap van de adviesraad niet tot belangenverstrengeling. Het valt in dat geval echter moeilijk in te zien waarom het niet vermelden van het lidmaatschap in het rapport als niet gelukkig en niet heel transparant wordt beoordeeld. Wanneer er geen sprake is van belangenverstrengeling, hoeft dit volgens de Gedragscode Wetenschapsbeoefening immers ook niet vermeld te worden.

Het oordeel van het LOWI valt bovendien moeilijk te rijmen met Artikel 5.3 van de Gedragscode Wetenschapsbeoefening, waarin expliciet wordt gerefereerd aan het adviseurschap van wetenschappelijk onderzoekers: "Altijd wordt duidelijk gemaakt wat de verhouding is tussen opdrachtgever en onderzoeker, bijvoorbeeld wanneer adviseurschappen of andere verbindingen bestaan. Mogelijke schijn van belangenverstrengeling wordt altijd vermeden danwel vermeld". Het LOWI stelt dat het lidmaatschap van de adviesraad van de politie Haaglanden niet leidt tot belangenverstrengeling, maar maakt niet duidelijk of het lidmaatschap wordt beoordeeld als een adviseurschap zoals bedoeld in artikel 5.3.

Buro Jansen & Janssen heeft bij het LOWI om verduidelijking verzocht en gevraagd of het lidmaatschap van de Adviesraad in wordt beoordeeld als een adviseurschap zoals bedoeld in artikel 5.3. Het LOWI heeft niet geantwoord.

Convenant

Volgens het LOWI advies kan "in redelijkheid niet worden gezegd dat de schijn van belangenverstrengeling is gewekt". Deze redenering is, behalve vanwege het lidmaatschap van de Adviesraad, ook om een andere reden opmerkelijk.

In 2013 nam professor van der Leun namelijk het initiatief om tot een nauwere samenwerking tussen de Universiteit van Leiden en de politie Haaglanden door middel van het opstellen van een convenant. Dit blijkt uit documenten die de politie Haaglanden eind 2016 naar aanleiding van een WOB verzoek van Buro Jansen & Janssen openbaar heeft gemaakt. Van der Leun nam dit initiatief in de tweede helft van 2013 - dezelfde periode waarin het Ministerie

van Veiligheid en Justitie en Haags gemeentebestuur een onderzoek naar etnisch profileren toezegden. In het Leidse rapport wordt dit convenant niet vermeld.

De WOB documenten bevatten onder meer email correspondentie tussen de Universiteit van Leiden en de politie Haaglanden. Op 2 juli 2013 mailt Van der Leun aan van Mussert: ”Ik zit natuurlijk in de adviesraad, maar ook verschillende collega’s werken samen met de eenheid Den Haag voor onderzoek en onderwijs. Zou het geen plan zijn de samenwerking meer te formaliseren?”´ Zij bepleit “een soort algemeen convenant dat we samenwerken dat we vervolgens in de praktijk nader specificeren”. “Ik zie het vooral als een soort intentieverklaring dat we samenwerken”, aldus Van der Leun.

Op 13 augustus 2013 verstuurt Van der Leun een eerste concept versie van het convenant aan de politie Haaglanden. In de hierop volgende maanden wordt deze verder ontwikkeld, hetgeen resulteert in het document ‘Verklaring van intentie tot samenwerking door Politie Den Haag en het Instituut voor Strafrecht & Criminologie van de Faculteit der Rechtsgeleerdheid, Universiteit Leiden’ van januari 2014’. Blijkens de WOB documenten wordt dit document diezelfde maand ondertekend door de universiteit en de politie Haaglanden.

Het Leidse rapport maakt geen melding van de Verklaring van intentie tot samenwerking. Volgens de Gedragscode Wetenschapsbeoefening artikel 5.3 dient mogelijke belangenverstrengeling echter altijd te worden vermeden danwel vermeld in publicaties. Het LOWI stelt in haar advies over het document echter dat “die te weinig aanleiding vormt voor twijfel aan de onafhankelijkheid van betrokkene. In de intentieverklaring hebben X en Y vastgelegd dat zij bereid zijn om verschillende vormen van samenwerking te ontwikkelen, maar dat diskwalificeert Belanghebbende niet als onderzoeker op het terrein van de werkzaamheden van X.”

Het LOWI oordeelt dat de schijn van belangenverstrengeling niet gewekt is. Dit is opmerkelijk. Zo bevat de Verklaring van intentie tot samenwerking onder meer de bepaling dat de politie Den Haag zich bij behoefte aan extern onderzoek op gebied van criminologie en

strafrecht zich in eerste instantie tot het Criminologisch Instituut van de Universiteit van Leiden zal wenden.

Gebrek aan transparantie duurt voort

Etnisch profileren is een maatschappelijk gevoelig thema dat onafhankelijk en transparant wetenschappelijk onderzoek behoeft. Het LOWI beoordeelt het niet vermelden van de gemaakte afspraken tussen de politie Haaglanden en de Universiteit van Leiden en het lidmaatschap van de Adviescommissie politie Haaglanden in het rapport als niet heel transparant.

Dit is op zich opmerkelijk. Het LOWI is hiermee kritischer dan de CWI (Commissie Wetenschappelijke Integriteit) van de Universiteit van Leiden. In het besluit van de CWI van december 2016 wordt geen enkele kritische kanttekening geplaatst bij het onderzoek, ook niet over het niet vermelden in het rapport van de afspraken en het lidmaatschap van de adviesraad.

Het LOWI advies lijkt echter geen verdere consequenties te hebben voor onderzoeksleider professor van der Leun en de andere bij het onderzoek betrokken wetenschappers. Het LOWI kan het bestuur van aangesloten wetenschappelijke instellingen adviseren om hun voorlopige besluit over een klacht te wijzigen. Volgens haar jaarverslag zijn LOWI adviezen niet bindend maar ook niet vrijblijvend, en dient een College van Bestuur van een bij het LOWI aangesloten instelling in ieder geval te motiveren wanneer het een LOWI advies niet opvolgt. In dit geval is dit echter niet aan de orde. Het LOWI beoordeelt het optreden van Van der Leun weliswaar op twee punten als niet transparant, maar verbindt hier geen verdere consequenties aan en komt er niet op terug in de eindconclusies van haar advies. Het LOWI adviseert het College van Bestuur van de Universiteit van Leiden “om het besluit (van het CWI) ongewijzigd over te nemen als definitief besluit”.

De totstandkoming van het Leidse onderzoek wordt gekenmerkt door een gebrek aan transparantie. De Universiteit van Leiden heeft het bestaan van de scripties en de gemaakte afspraken altijd verzwegen en weigert de twee scripties openbaar te maken,

waardoor het onmogelijk is om de inhoud van het rapport en de twee scripties met elkaar te vergelijken.

Hoewel het LOWI het optreden van de Universiteit van Leiden op twee punten als niet transparant beoordeelt, is het LOWI advies zelf op meerdere punten echter ook weinig transparant. Het LOWI maakt niet duidelijk of het lidmaatschap van Van der Leun van de Adviescommissie Politie Haaglanden beoordeelt als een adviseurschap, zoals bedoeld in artikel 5.3 van de Gedragscode Wetenschapsbeoefening. Tevens maakt het LOWI niet duidelijk of het de in de notulen van de korpsdirectie vermeldde afspraak over het voorkomen van een afbreukrisico van het onderzoek als een gebruikelijke en niet afwijkende afspraak beoordeelt. Het advies wekt de suggestie dat het LOWI de notulen niet als een getrouwe weerspiegeling van de gesprekken tussen de politie en de universiteit beschouwt, maar het LOWI maakt haar mogelijke overwegingen in deze niet expliciet.

Wellicht wreekt zich hier het feit dat het LOWI geen eigen onderzoek heeft gedaan. Het LOWI gaat volgens haar advies "in beginsel uit van de juistheid van het onderzoek van de CWI (Commissie Wetenschappelijke Integriteit) van de Universiteit van Leiden" dat volgens het LOWI aan de zorgvuldigheidseisen voldoet. Het CWI baseert zich op de verklaringen van slechts een van de bij de afspraak betrokken partijen, namelijk professor Van der Leun. Het LOWI heeft verder geen eigen onderzoek gedaan naar de juistheid van de notulen, en bijvoorbeeld niet zelf de politie Haaglanden of de twee betrokken masterstudenten criminologie gehoord.

Het LOWI advies is met name niet transparant in haar beoordeling van de verschillen en overeenkomsten tussen het rapport en de twee scripties. Het LOWI had hierin op eenvoudige wijze meer inzicht kunnen geven door in het advies tenminste de onderzoeksvragen en conclusies van de scripties concreet te benoemen. Hiermee zouden het rapport en de scripties nog enigszins met elkaar vergeleken kunnen worden, zolang de scripties door de Universiteit van Leiden niet openbaar gemaakt worden. Het LOWI heeft dit nagelaten. Een reden valt moeilijk te bedenken.

Dit is zorgelijk. De Universiteit van Leiden heeft het bestaan van de scripties altijd verzwegen en weigert dit openbaar te maken. Dat we

überhaupt weten van de scripties komt door documenten die via de Wet Openbaarheid Bestuur door met name de politie Haaglanden openbaar zijn gemaakt. De Universiteit van Leiden wekt al enige jaren de indruk iets te willen verbergen. Het LOWI advies kan de indruk niet wegnemen dat er inderdaad iets te verbergen valt.

Hoogste orgaan Wetenschappelijke Integriteit: Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren.(pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Hoogste orgaan Wetenschappelijke Integriteit (LOWI): Universiteit van Leiden niet transparant bij onderzoek naar etnisch profileren. (samenvatting)

Het LOWI-advies 2017 nr. 9

Samenvatting van LOWI-advies 2017, nr. 9

Reactie op het verweerschrift van de Universiteit van Leiden van 10 april 2017

bezwaar besluit College van Bestuur Universiteit Leiden met betrekking tot formele klacht/melding rapport 'Etnisch profileren in Den Haag? Een verkennend onderzoek naar beslissingen en opvattingen op straat' van de Universiteit Leiden

Universiteit mag data geheim houden

Antwoorden Burgemeester en Minister scheppen meer onduidelijkheid over etnisch profileren onderzoek Leiden

Wetenschappers in dienst van de overheid (kort)

Wetenschappers in dienst van de overheid

Professoren als spreekbuis van de politie (kort)

Professoren als spreekbuis van de politie

In vogelvlucht, Wetenschappelijk onderzoek naar politiediscriminatie

Naar inhoudsopgave Observant #71

Kailax technical details

Buro Jansen has previously written about Kailax in the article 'Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence'. This piece focuses on some of the technical details of the Unlocker and a few mysteries that still need solving. All of this information is coming from the HackingTeam leak that happened in 2014.

Unlocking locked Windows computers

Kailax has two solutions at their disposal. The Unlocker and the add-on U-Cap. Let's focus on the Unlocker tool first.

Kailax's Unlocker is a hardware device that can be attached with a USB to the victim's Windows computer to bypass the Windows lock screen.

Envision that you leave the house to visit friends, you shut down your computer and imagine that no one can mess with it. They simply don't have the password. Most IT-security people think different about it and the surveillance industrial complex has a lot of solutions to get around some of the security features that you might have enabled.

A malicious actor doesn't need your password in order to unlock the computer and plant spyware or worse, get control of an administrator account.

The same applies when the computer is powered off. It seems that full disk encryption is a possible solution to prevent unwanted entry into your computer.

However, most solutions present only partial disk encryption. This is due to having 2 separate locations on your hard drive, a boot partition and the encrypted data partition. The boot partition is an unencrypted partition and therefor vulnerable to tampering.

Most commercial operating systems and software running on them, do not have an option available to mitigate the partial encryption problem.

However, if you would run a free and/or open source system, you can achieve full disk encryption.

The Unlocker works on all x86 and x64 versions of the following operating systems:

* Windows Vista

* Windows 7

* Windows 8

* Windows 8.1

* Windows Server 2008

* Windows Server 2008 R2

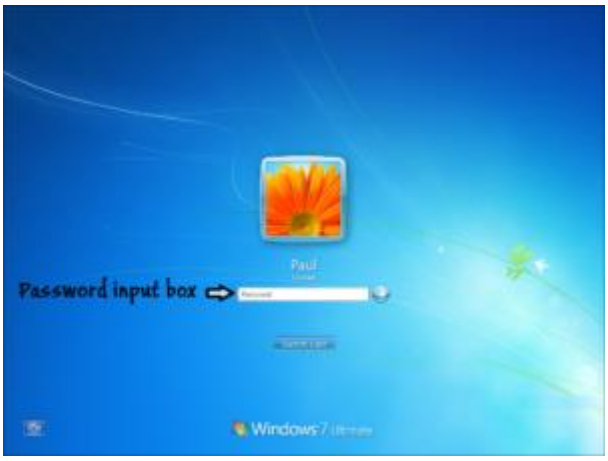
* Windows Server 2012

Server Core (no GUI) versions of Windows Server are not supported.

Note:

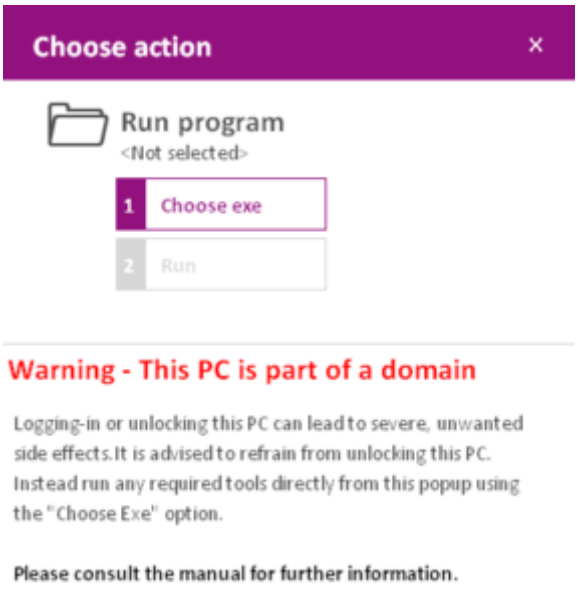
As you can see, Windows 10 support is missing from this list. At the time of the leak, Windows 10 hadn't been released. At the time of writing we're unsure if Windows 10 is supported by either the Unlocker or U-cap.

After the Unlocker is attached to the victim's computer, a new screen appears in purple, it will ask you to either launch an executable or bypass the lockscreen.



If you alt-tab you will see that the purple screen disappears and allows you to click on the password input text box. If you now put in a single letter and click enter, the PC will be unlocked and Windows will switch to the user desktop. The same attack will work for any other users that may exist on the same computer.

As Kailax indicates in their user manual: "You can use the Unlocker to bypass the Windows password and use the PC like a regular user. This option should be used with extreme care if stealth is required, and it is the user's responsibility to put the PC back in the same state as before the unlocking once done. Before bypassing the password, check if there's a warning at the bottom of the purple popup screen stating that the PC is part of a Domain."



However, if absolutely necessary, as Kailax indicates, it still might be possible to bypass the password, even if the PC is part of a Domain. An extract of their user's manual follows below:

The recommended and stealthiest method to use the Unlocker is through the "Run program" option. If bypassing the password is absolutely necessary, read the following carefully:

* Bypassing passwords on PCs that are part of a domain will only work if Cached Credentials are enabled in the Group Policy of the Domain Controller.

* Bypassing passwords on PCs that are part of a domain will cause a brief network disconnection. As a result, any existing VPN connections will likely disconnect.

* Trying to bypass the password on a domain PC when it is locked (as opposed to when a user has yet to log-on) will work, but will set the user's cached password to the password entered during the bypass. It will therefore be impossible to log-on or unlock the PC in the future with the *correct* password if the Domain Controller is unavailable. This password re-set will last until the correct password is used to unlock or logon AND the Domain Controller is available through either LAN/WAN or a VPN.

This means that in most real-world scenarios, bypassing the password on a PC that is part of a domain AND is connected to the domain through a VPN will lock the legitimate user out of their PC until they connect to the organization’s LAN/WAN.

* Trying to bypass the password on a domain PC with a user that is not currently logged on may work, but is likely to cause the PC account to be locked on the domain, so that only the Domain Administrator can release the account and make the PC usable again.

* Some typical enterprise client side software, for example Outlook, SharePoint client, Lync and others may behave unexpectedly, and in particular require re-authentication.

The Unlocker comes with an mute device that can be inserted in the audio out jack. This is to make the attack be silent, since when an USB device is (dis)connected it makes a sound. Or mute it when the keyboard allows you to.

In addition, Kailax' Unlocker comes with an included a USB flash drive. You can use the drive to store forensics software and other tools you may wish to use on target PCs, and/or save downloaded data onto it.

It should also be noted that the Unlocker works, even if the Autorun option is disabled in Windows.

U-Cap

U-Cap is an add-on for the Unlocker tool that enables the use of a so-called payload to deliver spyware to the victim’s computer or execute a payload with SYSTEM privileges, which is the equivalent of having full administrator control on the computer. A working Unlocker with version 1.3 is required to be able to use the U-cap device.

From the U-Cap user manual:

Step A

- Check the state of the target PC:

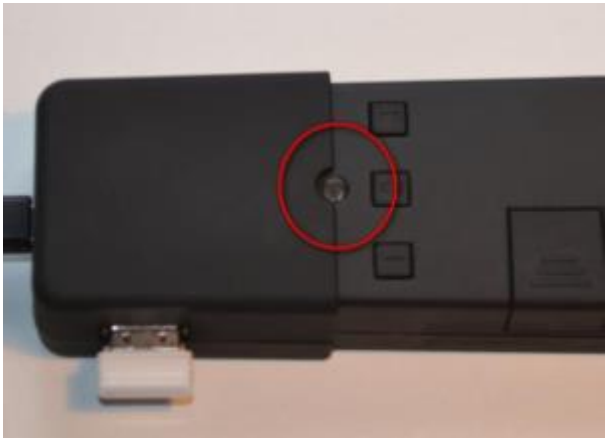
* If the PC is powered off - start the PC (power on), and wait for the logon screen to appear. Once the logon screen appears, wait an additional two minutes for background services to complete loading, then continue to Step B.

* If the PC is powered on but not locked, you can use the U-Cap to execute your payload with SYSTEM privileges. To do so, start by locking the PC (via the windows menu or by hitting windows key + L) and then continue to Step B. **Note** however that after a successful execution the PC will remain locked.

* If the PC is locked - continue to step B.

Step B

Connect the U-Cap unit to the Unlocker unit until semicircular indentation on U-Cap engulfs the LED indicator on the Unlocker unit.



Step C

Plug in the pre-formatted and payload loaded Flash drive into unit USB plug

Step D

Plug in the Micro USB connector of the Unlocker USB cable to U-Cap's Micro USB socket.

Step E

Plug in the other side of the USB cable into any free USB port on the target PC. If possible, use a USB2 port and not USB3 (blue) port.

Step F

Follow the steps as detailed in the table below – these are the same steps as running Unlocker, except for the last stage.

How do they do it?

Unfortunately, how they manage to pull off those attacks are not clear at the time of writing. Kailax is very protective of their intellectual property and no details can be found in the documents

that are leaked or through the discussions they had via e-mail. We're not sure if this is because of a so-called Zero Day or a Windows feature they're abusing.

Please refer to the Kailax FAQ.pdf for additional minor technical details.

To be complete it should be noted that there are off-the-shelf commercial devices like FinFireWire

(https://wikileaks.org/spyfiles4/documents/Release-Notes-FinFireWire-3.5.=pdf)

and open source frameworks like Inception that can target operating systems like MacOS, Windows and Linux using 'direct memory access' or short DMA. Some examples of those ports are Thunderbolt, Firewire, PCI(e), Cardbus or Expresscard. DMA allows data transfer at a very high rate between devices like camera's or storage devices, but it could also be exploited by an attacker to retrieve parts of the memory of a running computer where sensitive information might be stored.

Many experts agree however that, if you leave your computer unguarded and an attacker has a window of opportunity, the device should be considered compromised.

If you have any information or samples to share, please e-mail the author: drwhax [@] riseup [dot] net

Jurre van Bergen

Kailax technical details (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence (pdf)

Providence and the Dutch National Police Supply chain liability via a former police officer (English translation of article from Observant #69)

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 #71

Kailax / Nir (Max) Levy
The magic hand of Israeli intelligence

The Kailax *Unlocker* is exemplary of the secrecy and lack of transparency surrounding the trade in digital weapons. The *Unlocker* is a tool with which a burglar can gain entrance to any Windows computer, without the owner becoming aware.

There is hardly any information about the *Unlocker* and its manufacturer Kailax in the public domain. The website www.kailax.com only contains the address details of the company (an address in Singapore), but no additional information. From public sources, we can only gather that the Berlin based company 2beuropa serves as an intermediary for Kailax.

It wasn't until the publication of the Wikileaks documents about Hacking Team in 2015 that we gained any insight into the existence of the Kailax *Unlocker* and the trade in this tool. The Kailax *Unlocker*, sometimes also referred to as *Unlocker/U-cap* appears to be a desirable digital tool. According to its manufacturer, who calls himself either Max or Nir Levy in his emails, Kailax distributes the *Unlocker* to seventy countries.

There is no way to check whether this claim is true. What does become apparent from the Wikileaks files is that Italian computer company Hacking Team has expressed an interest in adding it to their selection of products. In order to do so they approach British company Providence, which appears to present itself as an intermediary offering the *Unlocker*.

The Kailax *Unlocker* is emblematic of the secrecy and the lack of transparency surrounding the trade in digital weapons. The provenance of digital weapons is often unclear, which begs the question whether governments and intelligence services have any idea about the products they're buying and the companies with which they do business. The interference of intermediaries like Providence only adds to the lack of transparency and security.

Buro Jansen & Janssen executed a digital search into the provenance of the *Unlocker*, which led to Israel. The Kailax *Unlocker* appears to be Israeli in origin, and there are former members of Israeli intelligence involved.

Hacking Team and Kailax

From the Wikileaks documents published in 2015 we can see that the Italian company Hacking Team started showing an interest in the Kailax *Unlocker* at the beginning of 2015. With the *Unlocker,* any burglar can gain entry into a Windows computer and log on without the owner becoming aware. This concerns Windows Vista/7/8/8.1 Server 2008/Server 2012- 32/64 bit.

Hacking Team uses a similar technique with its Tactical Network Injector (TNI) for Firewire. In a 'Statement of Work' Nir Levy (Max) of the manufacturing company Kailax writes that the 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.*' According to Kailax it leaves little to no trace on the computer of the victim.

The Italians consider the *Unlocker* to be an asset to their digital burglary toolkit. They might be able to develop the tool themselves, but without a prototype this seems to be beyond the capabilities of the Italians. Hacking Team tried to acquire the tool at first via Kailax's offices in Singapore, but to no avail, the request is left unanswered.

On January, 23rd, 2015 Walter Furlan asks in an internal email to some employees of Hacking Team whether they are familiar with the Kailax *Unlocker*. A Swiss client of the Italians, the Kantonspolizei Zürich, has bought the *Unlocker* from 2beuropa. Another client, the Raggruppamento Operativo Speciale (ROS, Special Operations Group) of the Italian military police, also acquired the *Unlocker* from 2beuropa.

Following this, Giancarlo Russo of Hacking Team contacts Rami Zoltak of 2beuropa. This Berlin-based company operates as intermediary for Kailax. However, Zoltak responds that 2beuropa only deals with governments: '*We are working only with governmental offices, we are unfortunately unable to assist.*'

The Italians, however, are persistent. Russo bluffs that an 'LEA client' (Law Enforcement Agency) has expressed an interest in the *Unlocker*.

Eventually, Max, who first signs as Kailax Sales, responds. He says that Hacking Team's client can only acquire a USB *Unlocker* from Kailax' offical dealer, though he doesn't mention who this dealer is supposed to be.

Russo tries to convince Max one more time, but Kailax keeps refusing. Little by little they do reveal more information about the tool: '*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.*' According to Max the *Unlocker* has been sold to over seventy countries.

Max gives Hacking Team one option: they may install the *Unlocker* on their systems, which provides unlimited use of the tool. He asks Russo to guarantee that no one else is provided access to Kailax's IP-address: '*you also have to convince and assure us that no one else but you will have access to our IP.'* In this instance Max signs as Nir Levy (Max).

The Italian and Max exchange emails for a while, but they don't seem to get much further. Max keeps him at arm's length: '*We are both manufacturer suppliers of technology we are in essence competitors*', he writes. '*As you must know we are in same niche market that is usually based on trust*.'

Max does offer an intermediate solution. Hacking Team may operate as a sort of subcontractor, who can only sell the black box to customers: '*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.*'

The Italians aren't comfortable with this option and they decide to approach some of their clients to get them to acquire the Kailax *Unlocker* for Hacking Team. Russo approaches the Swiss police, the Kantonspolizei Zurich.

The Swiss don't respond, so the Italians try their Italian client, the Raggruppamento Operativo Speciale (ROS, Special Operations Group) of the Italian military police. Hacking Team asks the ROS to order two *Unlockers*, but the military police don't seem to be all that keen to be used by Hacking Team.

Providence enters the picture

At the beginning of March 2015 contact between Hacking Team and Kailax breaks down. Then the Italians approach the British company Providence. Both companies are familiar with one another, and have tried to forge a co-operation in Australia and Ecuador, whereby Providence proposed to act as intermediary for products of Hacking Team.

Providence claims to have their own tool, the *'Windows Unlocker'* and '*U-Cap*' in their product range. This caters to a similar need as the Kailax *Unlocker*. Sometimes the Kailax *Unlocker* is also referred to as the *Unlocker/U-Cap*. On March 18th, 2015, Providence gives a presentation at the ISS World MEA in Dubai titled 'Tactical Bypass of IT Security', which members of Hacking Team attend.

A week later Giancarlo Russo of Hacking Team writes to Steve Minto of Providence stating that the Italians are interested in discussing a business relationship. Russo mails on April 8th, 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*.'

That same day Peter Stolwerk responds that they would be very interested to develop business relations with Hacking Team regarding the *'Windows Unlocker and U-Cap* (the special add-on for the *Unlocker*)'. At this stage Providence does not yet let on that they haven't developed the *Unlocker* themselves.

Stolwerk travels to Milan to give a presentation, but this doesn’t go smoothly. The Italians notice that the *Unlocker* leaves traces: '*Regarding the product I would like to have a feedback regarding the behavior we experienced during the demo (pop-ups on unlocked PC)*.'

Russo writes a report of the meeting and sends this to Stolwerk. It seems that in their meeting Russo and Stolwerk have discussed '*Partnership on Training programs for HT Clients. Social Engineering and how to get increasing benefit from HT technologies in real case operations.*'

From this report it becomes clear that Hacking Team wants to offer Providence a deal. It will accept Providence as some kind of distributor, in exchange for the 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.*'

As intermediary for Hacking Team, Providence can sell their products and train their clients to get the most out of the cyber weapons: '*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)*.' Providence may also offer their clients Hacking Team's software products: '*Providence would play more the role of an agent/consultant, rather than a distributor*'.

Concerning the '*Unlocker + U-cap*' it appears that the Italians would rather bypass Providence altogether and obtain all options to add the product to their assortment. '*Regarding the cooperation we feel that the first, easiest and fastest, way to cooperate is to include the USB Unlocker into our portfolio*', Russo informs Stolwerk.

During the meeting in Milan, however, it slowly becomes apparent that Providence has no say in the matter of the USB *Unlocker*. Stolwerk keeps referring to the manufacturer, which he only mentions by name once: 'Max'. Russo of Hacking Team writes immediately after the meeting in Milan, in which Max apparently has been mentioned: '*I expect you and Max to elaborate more on which cooperation options you consider viable*'. Stolwerk responds after talking to Max: '*Agreed, I spoke to Max and he is positive that we will together find a solution on this.*'
Hacking Team has already been in direct contact with Max at the beginning of 2015 about the possible acquisition of the *Unlocker*.

However, it isn't clear from the Wikileaks documents whether the Italians are aware of this or whether they have informed Providence of this fact.

Acquisition of new clients

Hacking Team is invited to the offices of Providence in Hereford, UK, in May 2015 to discuss further co-operation. The English company seems keen and asks Hacking Team, amongst other things, if it would be prepared to give their defensive cyber war training to 20 people from the Middle East. It looks like Providence still does not really understand what it is the Italians actually do. A subsequent phone conversation is needed to point out to the English that Hacking Team only sells digital weapons.

Besides seeking to acquire the 'U-cap + *Unlocker'*, the Italians also appear to be interested in acquiring new clients via Providence: '*We should go to Hereford and take advantage to visit them and also perform a demo for their sales team*', writes Vinci of Hacking Team.

Vinci also suggests organising a meeting with the British Ministry of Defence: '*There is a big MOD field camp in Hereford. We can try to organize a meeting with MOD (Ministry of Defence)*'. Hacking Team hopes Providence will prove useful with regards to the British MOD. There are, however, also other potential intermediaries, like Bob Quick of BlueLight Global Solutions. Apart from the MOD, there are also other potential clients they are interested in, like the National Crime Agency and BAE Systems, a large military weapons manufacturer.

Providence's offer of courses and trainings does not really interest the Italians. Vinci mails: '*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.*'

The Italians continue to be rather evasive and Providence appears to have a long way to go to be accepted as intermediary: '*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.*'

The Italians are proposing that if Providence wants to be considered as an intermediary for Hacking Team they will first have to deliver some easy clients. If Providence wants to pursue any clients themselves, they first need to run the details past Hacking Team, who will decide whether the English may proceed or not. They know from experience that some clients are already being served by another intermediary. This was the case in Ecuador where Providence suggested a company with which Hacking Team was already doing business via another intermediary (Robotec).

Deal or no deal

On May 8th, 2015, the relation between Max and Providence finally becomes clear. Stolwerk: '*The manufacturer 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.*'

Apparently, Providence have managed to persuade Max. According to Stolwerk, Providence is the distributor of the *Unlocker* for a large part of the world. He doesn't specify for which of the seventy countries that Max alleges the Kailax USB stick is distributed to, Providence acts as an intermediary. The other parts are being serviced by local distributors like 2beuropa.

Kailax is prepared to make a special version of the *Unlocker/U-cap* combination, especially for Hacking Team. Its development will be at the cost of the Italians. It seems nothing stands in the way of a successful meeting in Hereford. The Italians will be presenting their jewel in the crown - the Galileo RCS (Remote Control System) - and would like to see the full range of the English, '*in particular the training and workshop around cyber, covert entry, installation, surveillance, getting close to the targets, etc*.'

During the following months, the communication between Hacking Team and Providence mostly concerns the *Unlocker*. The Italians claim to have a customer for the Kailax USB stick and want to know how they can satisfy them. Giancarlo Russo of Hacking Team claims it concerns an Italian crime department and that Max is already familiar with it.

Stolwerk is eager to hold onto the Italians as possible partners and writes that there is some interest from The Netherlands in the products of Hacking team: '*I will speak to the guys here as I have some good news about the Netherlands for your products.*'

And still, the Italians do not seem completely convinced by the credentials of Providence. At the end of May 2015 a Hacking Team employee, who has studied the presentations of the English, writes: '*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*.' It appears that Providence started compiling their trainings at the beginning of 2015, so they only recently came into being and their email addresses are wrong.

Providence and Hacking Team are close to an agreement. The Italians are even invited to an exclusive gathering of Providence on August 26th, 2015. On the Hereford premises some workshops and a little barbecue have been organised. Apart from Hacking Team, Tac Up (a Providence outfit), Claresys Covert Video Surveillance (part of the British Ministry of Defence), and another twenty companies are invited, among them Cobham, Eomax, Sentinor. All 'friends' of Providence.

From the Wikileaks files it isn't clear whether Hacking Team finally added the *Unlocker* to their selection. In July 2015 Hacking Team is hit by a hack and internal documents about the company are published by Wikileaks. The company is also plagued by criticism over their distribution of arms to repressive regimes and it loses its export licence to trade outside the European Union.

Kailax - Mhyli

The correspondence between Hacking Team and Providence provides a revealing insight into the world of intermediaries in digital weapons. The Kailax *Unlocker* is exemplary of the mystery and lack of transparency surrounding the trade in digital weapons. The provenance of digital weapons is often shady, which raises the question if governments and security services are fully aware of what kind of products they're buying and from what kind of companies. The interference of an intermediary like Providence only adds to the opaqueness.

There is hardly any public information available about the company called Kailax. They do have a website (www.kailax.com), according to which the company is registered under the name of Kailax in Singapore: Kailax PTE LTD op 129 Lower Delta Rd. #09-03 CendexCenter. On the website are two sentences: 'We provide solutions in the cyber security domain' and 'For details please contact us at info@kailax.com'. Apart from that, it contains no information about products, expertise, revenue, investors, clients, etc.

Kailax itself has never been present at any of the different trade fairs for digital weapons or ISS World. It handles its sales through the company 2beuropa. This company is run by Rami Zoltak and is registered in Berlin on the MittenwalderStrasse. Zoltak comes from the world of real estate and trades in all kinds of products, among which digital weapons from Kailax.

On the website of 2beuropa it says that the company deals in 'taktischen Überwachung beste High-End-Hardware- und Softwareprodukte.' This concerns surveillance, tactical surveillance and high end hardware and software products. These products also encompass VIP security cases, drugs tests, smelly sprays as a public order measure, containers for the transport of explosives. On the website of 2beuropa it mentions Kailax as partner ever since the new version went online in 2014.

However, the website does not show what kind of products Kailax offers. What does stand out is that Rami Zoltak exclusively offers Israeli products. All of its partners are Israeli companies that are linked to the IDF, the Israeli army. 2beuropa indicates on their website that their partners include: Towersec, Karil International, Touch&Know, iDenta, Septier, ITP Novex, Memtex, Prosecs, ODF Optronics, ODI-X and Pro4tech. It also mentions Kailax among them, so it is reasonable to assume Kailax is an Israeli company.

Max – Nir Levy - Mhyli

The person corresponding on behalf of Kailax is Max. He also uses the name Nir Levy in his correspondence with Hacking Team, but it is unclear whether this is his real name. The Kailax website contains no further information about Max and/or Nir Levy. From the Wikileaks files it appears that Max/Nir Levy is the most important person within Kailax.

Buro Jansen & Janssen has tried to obtain more information about Max/Nir Levy. It appears to be the same person. He uses the email address max@kailax.com

There are a number of domain names linked to this email address, these are: s-mic.com, k-mic.info, *Unlocker*-u.com and toplucktrading.com. Few of these sites are functional, with exception of the *Unlocker*-u.com, which refers to kailax.com. Toplucktrading doesn't hold office in Singapore, but in Hong Kong, at this address: Unit 1203 12F CEO Tower, Admin Street: 77 Wing Hong St Cheung Sha Wan, Kowloon.

A digital search for Max and Nir Levy does not provide much information. The transcript of domain names in Nir Levy's name does however provide an interesting pallet. There seem to be multiple Nir Levy's: most of whom are Israeli, with one or two residing in the US. Regarding the above-mentioned domain names, like *Unlocker*-u.com, Nir Levy is mentioned as part of Kailax, with the email address of max@kailax.com. However, there are other domain names in the name of Nir Levy, that are linked to a former employee of the Israeli secret service.

Domain names

Of all the Nir Levy's who have registered domain names, there are only two that use the name Max. This concerns a Nir Levy with the email address max@mknowledge.com and a Nir Levy with the address max@mhyli.com

Both Maxes appear to apply to the same Nir Levy, who gives his address as: 7 shamir, hodhasharon in Israel, phone number +972.97480608. These details are also linked to the following websites: mknowledge-demo.com and mknowledge.com (linked to the email address max@mknowledge.com) and mknowledge.info, smthid.com and mhyli.com (linked to the email address max@mhyli.com).

Max from Kailax and Max from ‘mknowledge’ and ‘mhyli’ seem to one and the same. No other Nir Levy's that use the name Max can be found. Furthermore, the websites are equally inaccessible as those of Kailax.

On the website of Mhyli there's a short but remarkable presentation by Max, where he explains that he's also director of Pro4tech, a manufacturer of tactical surveillance video solutions (Pro4tech is also

connected to 2beuropa, which also operates as intermediary for Kailax). Max also writes on the Mhyli website that he is CEO of EDM, a company that deals in automation of internet information gathering. According to the 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*.'

The reason why Nir Levy (Max) is so evasive about his background, has to do with his career before he entered the world of business. Max worked for the Israeli secret service for 25 years. The Mhyli website reveals: *'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.'*

This is truly astonishing. On Kailax' website there is no trace of background information on Max or Nir, but on the Mhyli website he seems to be much more forthcoming about his background: *'He also completed various managerial technical and command courses in the Prime Minister's Office, including the Senior Commander course.*'

His colleague at Mhyli, Daniel Kario, also appears to have a past with the Israeli army. According to the website he has worked as *'group leader in a leading technological unit of IDF'* (Israeli Defence Forces).

It's impossible to determine whether Kailax is an independent company and is solely run by Nir Levy. The Kailax website does not provide any information whatsoever, nor does it provide any insight whether Nir Levy and Daniel Kario are qualified IT-developers who designed the tool themselves.

That Kailax' Max and Mhyli's Max are one and the same makes complete sense if you consider the mystery surrounding Kailax. Who would want to buy a digital weapon from a former employee of Israeli Intelligence? In some countries there would be a certain amount of reluctance to do business with Kailax if it were to become known that the company is Israeli, and even more if their contacts involved the Israeli intelligence services.

Clueless about origin *Unlocker*

During research into the relations of The Netherlands with the Israeli security industry, Buro Jansen & Janssen concluded in 2011 that the Israeli are doing everything they can to get a foothold in The Netherlands and Europe. They use their war in the occupied territories as evidence-based advertising for their products. At the same time they are trying to obscure their ties to Israel by using proxy foreign companies that handle the trade with certain countries.

The company called Kailax fits this profile. It's quite likely that Kailax delivers to similar countries/clients as Hacking Team and Gamma Group/Finfisher, either through Providence or another intermediary. It's very doubtful whether the buyers of the Kailax *Unlocker* are aware of the background of the company, its employees, investors and clients.

This question is also relevant regarding The Netherlands. In answer to a Freedom of Information (FOI) request by Buro Jansen & Janssen, the Dutch National Police declared that they have purchased 39 products or services from Providence. The police, however, refuses to specify which items they bought from them. It is not unthinkable that they purchased the Kailax *Unlocker.*

Providence is a relative newcomer to the security market. The British company offers trainings, accommodation and equipment. For trainings the Dutch police can make use of their own trainers and training centres. Most equipment the police buys from regular suppliers like Cellebrite, Nice-Systems and other companies, which leaves the question whether Providence has anything better to offer.

In answer to the FOI request, the National Police claims that it would harm their crime detection abilities to reveal any more information about Providence. This claim can hardly be applied to the regular selection of

Providence's offer of trainings and equipment, because they don't serve crime detection purposes. The argument could make sense if it concerns digital weapons.

In the rejection of the request, the National Police does explicitly state that it made the purchase from Providence on an individual basis: '*This means that they have been acquired if and when the concerning department needed a specific tool for police and/or detection activities'*. This doesn't appear to apply in any way to the trainings and equipment in Providence's selection, but it does apply to the Kailax *Unlocker*.

With the Kailax *Unlocker* computers can be unlocked using an internet connection. Max / Nir Levy indicates in the correspondence with Hacking Team that he offers them a black box that obscures the technique and the IP address of the server of the *Unlocker*. '*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.*'

If the Dutch police does make use of the Kailax *Unlocker*, The Netherlands just might have brought in a second Israeli black box. One that is even more obfuscated than the wiretapping switchboards of Nice Systems that were acquired earlier. The Minister for Security and Justice referred to the previous switchboards in a February 2016 statement, saying that more clarity was needed about the functioning of the equipment. 'With the many telephone taps the police executes, the supplier of the tapping equipment is closely involved. But essential information about the taps has not been shared by the same supplier'. 'There is no guarantee that the police has a full overview of all interferences on the tapping system' (NOS, February 12th, 2016).

Kailax / Nir (Max) Levy; The magic hand of Israeli intelligence (pdf)

Kailax technical details (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Providence and the Dutch National Police Supply chain liability via a former police officer (English translation of article from Observant #69)

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 #71

When the Dutch secret service came knocking on my door

This is the account of how the Dutch secret service (AIVD) approached me in 2013, and how I understand the events that took place. I was a student until summer 2013, and after OHM2013 was hired at an internet service provider. I also did some technical consulting and digital security trainings for Publeaks during that time. This is all prior to my involvement in Tails.

It is important to tell the whole story, the run up to the approach, the approach itself, how and when it happened, and discuss the aftermath. This is not an isolated incident but rather a pattern of harassment of hackers and other communities. With the new Dutch security services law coming up now, the services will gain additional measures and more power, I think this story is more relevant than ever.

Being surveilled?

It's 2013, the year of the Snowden leaks, the arrests and trials of some people associated with Lulzsec, and OHM2013 - the Dutch hacker camp that takes place every four years.

OHM2013 was not without its controversy. The primary sponsor was Fox-IT, an IT-security company that is deeply involved with the Dutch government and has helped catch teenagers doing some DDoS attacks. Fox-IT is also rumored to have had contracts with the Mubarak regime in Egypt.

Due to this fact, some of us decided to organize NoisySquare, to put the resistance back in OHM. We had our own tipi tent organized as an additional track in the OHM2013 program. Lectures, workshops, panel discussions and our meeting circles were hosted in this tipi.

A couple of months before OHM2013 would start, my aunt received a phone call from somebody who claimed to be my friend and was looking for my mobile number. However, I never gave any of my friends my aunt's phone number. My aunt was alarmed, she asked who she was speaking to,

and made it clear that she found this a rather strange conversation. The person on the phone didn't really identify himself, and my aunt hung up.

For a while I thought one of my friends was trying to prank me and my aunt, and I soon forgot about the incident.

When I was in Germany in May of that year, I went to an event that was about Chelsea Manning and Collateral Murder (Wikileaks released video footage of a US Apache helicopter attacking and killing Reuters journalist Namir Noor-Eldeen, driver Saeed Chmagh, and several others in a public square in Eastern Baghdad), me and my then partner left the event and found that our mobile batteries were losing charge even though we were not using the phone. The situation with the battery normalized after I returned to the Netherlands.

Later in the year, I had the same experience with my phone while attempting to help with the build-up of OHM2013. My phone battery was draining quite quickly, even though I wasn't using it. I asked whether other people had the same issue and was told that the GSM towers were probably overloaded, even though nobody else was having any of these issues.

This is where it starts getting a little weird, I assumed it must have been an IMSI-catcher but I couldn't back up this claim with actual evidence. But the same insane battery drain happened while the phone wasn't being used much. During OHM2013, I lost my phone. I only got it back after OHM2013 when somebody returned it to the lost and found box and a friend managed to bring it back to me.

When I got the phone back, I saw someone had been trying to call me from a number I did not recognize. I later learned it belonged to an AIVD agent, as he left his mobile phone number with my father.

Hans Turksma, AIVD

Just before OHM2013 took place, I had dropped out of my university studies and on top of that I was a bit of an emotional mess after a romantic

break-up. I have a feeling that the intelligence service pried on this mental state of mine.

On a Monday afternoon 2 weeks after the OHM2013 event, a stranger approached my parents' home. He rings the doorbell, no reply, he tries a few more times, nobody is home, my parents are walking the dogs. He continues to wait in front of the house for some time and leaves soon after.

He comes back the following day, now there are people home. My stepmother opens the door, the man identifies himself as Hans Turksma, from the 'Ministry of Interior' and explains he's looking for me. My stepmother explains that I'm not home and invites him in. But he doesn't want to come in and they continue talking at the door. My stepmother calls to my father to explain that there is someone looking for me.

My father asks whether he works for the AIVD and after asking the question several times, Hans Turksma acknowledges that he works for the AIVD and that he would like to speak to me. My dad asks why Turksma is interested in speaking to me, he's surely not here to offer his son a job. Turksma makes it clear he isn't there to offer a job but rather to "see how the image of the AIVD can be improved among the hacker community". How Turksma would like to do this remains unclear. My dad explains to Turksma that he never wants to see him again near his house or near his son, and to stop the harassment. Turksma indeed, never came back.

While Turksma was at my parents' house, I was having a meeting at a provider to run our first Dutch Tor exit nodes. After I went to the library to check some e-mails, my dad calls, "Hey Jurre, don't freak out, but there was someone from the AIVD at the door looking for you."

My heart skips a beat. My head has too many questions. I hang up and remove the battery from my mobile phone. At this point I stopped using mobile phones for a while.

At the time I was freelancing and people expect to call me and that I will pick up the phone during the day. Imagine trying to explain that you just had an AIVD agent at the door looking for you. The faces are priceless.

Uninvited guest

Some weeks later at the end of August, we were having a Publeaks meeting at an outdoor cafe in Amsterdam Noord. It's early and the terrace is abandoned, we sit down and shortly after, a man who looked like he was in his fifties sits down next to us, orders a coffee, pays immediately in cash and watches us the entire time listening in on our conversation. As soon as we talk more informally, he gets up and leaves on his bike.

After a while, all these little coincidences become a pattern. I was told I was being paranoid and might be delusional. Some people even expect the AIVD to roam around the hacker world to look for the "bad guys" and would be disappointed if they didn't.

Unfortunately, there is a big downside for the people who've been asked to inform on their peers and friends. It's not exactly a nice feeling. And, you're left with questions: Am I being followed? Will I get charged with some bullshit charge? You start being more careful in how you communicate with people. How do I explain this to any future or current partners? These interactions make you change a little bit as a person.

At a later point in time, it became clear to me that more people have been approached and asked to become informants. I have not been explicitly asked to become an informant, but from what I understand by talking with Buro Jansen & Janssen is that this is probably the real reason for approaching me.

I never called the mobile phone number that was left by Hans Turksma. I never spoke to them, nor did I ever agree to inform.

Time and time again we see people being approached and manipulated in different communities. Some of them are not even politically active, nor are they activists, some just want to throw a party with some of their hacker friends. These are the same people who organize events or started

hackerspaces. We aren't those bad guys they think we are, we haven't been accused of a crime and yet we are still being harassed.

Another approach - Sabu?

In 2017 I learned that another approach had taken place. The security services approached a Tor exit node operator and Msc student of the TU-Delft. It became clear that the security services would like to infiltrate hackerspaces, hacker events throughout Europe, and especially the Chaos Computer Club and free software projects like Tor and Tails. It looks like this is an international effort.

They offered the Delft student a get-out-of-jail card if he gets caught hacking for assignments from the security services. I'm no law expert, but that sounds like it could be slightly illegal, even under the new law.

Now, you might wonder: Where have I heard of something similar to this? It smells a lot like the Sabu case, the hacker turned informant who hacked and snitched on several hackers, notably the Lulzsec hackers and Sigurdur “Siggi” Thordarson from Wikileaks, who also turned out to be an FBI informant. Both cases proved to be quite a success for the American government. Perhaps there is now an international effort to ruin more people’s lives.

All of this is giving me the creeps. It's not exactly good for your mental health to know, <if true> that someone is really trying to get you. You don't know the purpose nor how they will do it. Will they employ honey traps? Do they want to put backdoors in the software? Even though they promised the Dutch parliament not to place backdoors in the software? If a foreign agency succeeds in whatever technique they might employ and share it with the Dutch agency, will the Dutch "whitewash" the access that way?

I've became very distrustful over the years of people and especially of the government and how they try to rip communities apart. I think the approach totally freaked me out and changed me a little bit and not exactly for the better.

Why not sit down with them

Some people have asked why I didn't sit down with them to tell them what I think about all of this. Some will say, this might help to catch some potential bad guys so what's the fuss?

I disagree because you might be approached, you politely decline, and they never return, right? Well, some people are being harassed for long time, where the AIVD will try to persuade you to become an informant with a slew of manipulative tricks; they don't take no for an answer in most cases. They will offer all kinds of rewards but in the end they will always drop you after they used you. They got what they needed and you are no longer interesting.

And there is something else. The people who they pick often have no perspective, they are in debt and easy to manipulate for the service. If they want out of the informant role, they are pressured by the service who will threaten to snitch on them to family and friends. So much for democracy and oversight …

My answer is clear: I don't talk with people who are selected to work for the service and educated to perform manipulative tricks on their targets. There is a power imbalance between us - they can lie, I can't lie. They suffer from not being able to self-reflect. Should I trust some black box organization on their "blue eyes"? Or on the service's track record, since its inception, of harassment of anything or anyone that's slightly critical of the democracy?

With the stories so far, the next couple of years will be quite interesting for the tech community. We'll see more attempts of the services trying to recruit informants, giving them direct access to databases or networks. Let's hope they never try to recruit people who work for the NCSC in the Netherlands and try to force them to inform on the community.

If you really want to protect democracy and you care about the rule of law, say no to becoming an informant. To those working at the security services: leak more documents or at the very least, ask for a self-reflection course.

Ways forward

First of all, it's ok to say NO. It’s legal to refuse to collaborate. If you're unsure about what they might ask of you, contact a lawyer, contact the CTIVD to submit a complaint, or contact Buro Jansen & Janssen.

If you're based in the United States of America, I encourage you to read the following text: https://crimethinc.com/2017/05/17/if-the-fbi-approaches-you-to-become-an-informant-an-faq-what-you-need-to-know.

Some of this, I think, comes down to consent. The security services might try to continue to lure you into their web, even though a one-time firm "no" should be enough to back them off. Unfortunately, when it comes to recruitment of informants, you might have to say no multiple times.

And that's really bad, especially if you haven't done anything wrong, or illegal, and your own government is trying to persuade you to do possibly illegal things to fulfill their needs to conduct cyberwar or destroy communities.

However, I'd like to propose some ways to create a more resilient and emphatic community.

1) I'm open to creating a group of people who have been approached, and see what we can do as a group of people, for example, submitting a complaint to the CTIVD.

2) We can create a “Frequently Asked Questions” document, like the one from Crimethinc, according to our local laws in the countries we're based in. What can they ask for? Can you decline? What could this mean? What to do when you are approached and they're giving you a hard time?

3) Empathy, if somebody has been an informant and has been (hopefully) naive and wants out, we should help them get out and perhaps rejoin the community at a later stage through restorative justice processes.

4) Don't accuse your peers of being feds, agents or informants without credible evidence that proves your case. Don't destroy someone else's life. Investigate rumors thoroughly and if sure present facts in a decent manner.

5) Write down your story when it happens, while the information is still fresh in your head. This can help in the future when you hear of similar stories and it can aid in understanding the aim of the operation in question.

In short: (from Crimethinc)

- Non-cooperation is the best way to protect our communities and movements against state repression.

- If they are approaching you about informing, they probably have a weak case if they have a case at all.

- You do not have to cooperate. You have the right to remain silent.

- Contact a lawyer as soon as possible.

Jurre van Bergen // email: drwhax@riseup.net

My KeyID: 0x9586d84b70dcae8c
My fingerprint: EBDD 1240 CBC8 91C2 6C48 75D0 9586 D84B 70DC AE8C

[When the Dutch secret service came knocking on my door (pdf)]

[Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)]

Naar inhoudsopgave Observant #71

Interesse AIVD voor Marokkaanse solidariteitsnetwerken

Vanwege zijn betrokkenheid bij netwerken die in Nederland protestacties organiseren uit steun voor onderdrukte Marokkanen in het land van herkomst, werd 'Daan' diverse keren door de AIVD benaderd. Op een manier die door hem als intimiderend werd ervaren.

Net als in andere landen in de regio raakten begin 2011 burgers in Marokko in de ban van wat de Arabische lente wordt genoemd. Sinds de eerste grote demonstratie op 20 februari 2011 in Rabat gingen regelmatig een paar duizend mensen de straat op. Deze '20 februari-beweging' streefde naar vrijheid en rechtvaardigheid. Ook in Nederland werden destijds hier en daar demonstraties georganiseerd uit solidariteit met de beweging in Marokko. Daan was erbij.

'Daan' is een maatschappelijk betrokken man van Marokkaanse afkomst en woonachtig in Nederland. Hij geeft een stem aan mensen die moeilijk gehoord worden en neemt deel aan manifestaties en demonstraties tegen onrecht. De politieke ontwikkelingen in Marokko volgt hij nauwgezet. Er gebeurt daar van alles wat het oog niet mag zien en het oor niet mag horen. De AIVD heeft hem inmiddels diverse keren benaderd voor het verschaffen van informatie. Daan begrijpt niet waarom.

benadering om 20 februari-beweging

Het was midden in de zomer van 2011 dat Daan gebeld werd op zijn werk. De vrouw aan de lijn noemde zichzelf Najat. Ze kende zijn voor- en achternaam en zei dat ze bij de politie werkzaam was. Ze wilde met hem praten: “Het gaat niet over jou, er is niets ernstigs.” Daan herinnert zich dat het geen open vraag was. Hij moest direct zijn werk verlaten en zich begeven naar een café aan de overkant van de straat.

Daar trof hij twee personen aan, Najat en een man zonder naam. Najat legde hem nu uit dat ze van de inlichtingendienst waren. De anonieme man stelde zich niet voor en zat er bij als een soort van bodyguard; hij was voor Daan de belichaming van de intimidatiemethode van de AIVD. Daan voelde zich zeer ongemakkelijk. Najat vertelde dat hij als de “extra oren en ogen” van de inlichtingendienst moest gaan fungeren. Daan

kende de Marokkaanse gemeenschap goed en kon informatie verschaffen die voor de geheime dienst van belang was.

Wat het nut van deze inlichtingen was, bleef tijdens het veertig minuten durende gesprek mistig. Het ging namelijk niet over mensen die van terrorisme werden verdacht of andere criminele activiteiten. Waarover het dan wel ging, wilde Najat niet duidelijk benoemen.

Het ging volgens Najat over wat zich op dat moment in Nederland afspeelde. Daan zou in de gaten moeten houden wie wat en waar organiseerde en welke netwerken er werden gevormd. Gezien de netwerken waarin Daan zich in die periode begaf, kon het niet anders zijn dan dat ze doelde op de Nederlandse tak van de 20 februari-beweging. Daan weigerde beleefd maar kordaat zijn medewerking.

benadering om Rif protesten

Begin januari van dit jaar bevond Daan zich met griep thuis toen ‘s middags rond een uur of drie werd aangebeld. Er stonden twee onbekende personen voor de deur, een man en een vrouw. De vrouw groette Daan amicaal, alsof ze oude bekenden waren, wat de verwarring slechts groter maakte. Daan antwoordde gemeten met “hoi”. “Ik ben Tonnie”, zei de vrouw, terwijl ze haar portemonnee pakte en het pasje met foto en blauwe kroontje liet zien. “Ik ben van de AIVD”, vervolgde ze.

De man sprak hem niet aan, herkenning alom. “We willen graag met je praten”, klonk het gedecideerd. Daan vroeg waarover, maar daar kwam geen antwoord op. Enkel wanneer hij hen binnen zou laten of een afspraak met ze zou maken voor een gesprek, zouden ze het onderwerp benoemen en toelichten. Daan vroeg herhaaldelijk naar de aanleiding van hun bezoek. Uiteindelijk gaf Tonnie toe dat het geen persoonlijke benadering was, maar dat ze met hem wilden praten over een aantal ontwikkelingen die gaande zijn.

Daan zag overeenkomsten met het gesprek met Najat en haar anonieme kompaan in de zomer van 2011. Daan is thans wederom bekend met de Nederlandse tak van de volksbeweging in het Rif-gebied in het noorden van Marokko die (opnieuw) oproept tot vrijheid en rechtvaardigheid. In Marokko is momenteel een grootschalige onderdrukking gaande van deze beweging, waarvan meer dan 400 mensen zijn gearresteerd en

verdacht worden van oproepen tot een verboden demonstratie.

Daan werd boos over de onbeschofte en intimiderende AIVD-benadering. “Als de overheid informatie wil van mensen uit de Marokkaanse gemeenschap, kunnen ze gewoon een brief sturen met een uitnodiging waar iemand rustig in zijn eigen tijd op kan reageren. Dit hebben jullie een paar jaar geleden ook gedaan en is helemaal niet nodig. Zo ga je niet met burgers om.”

“Hoe komen jullie eigenlijk aan mijn adres en waarom staan jullie zo dwingend bij mij op de stoep?”, wilde hij weten. Tonnie antwoordde dat ze Daan’s gegevens uit de BRP (Basisregistratie Personen) afkomstig zijn en beaamde dat ze wist van de eerdere benadering: “Daarvan zijn we op de hoogte.” De man achter haar stond er zwijgend en met een zelfde gelaatsuitdrukking bij, als een soort van robot. Daan schudde zijn hoofd: “Ik wil hier niets mee te maken hebben, ik vind dit onbeschoft.”

Tonnie bleef herhalen dat ze met Daan wilde praten en benadrukte de vertrouwelijkheid van het gesprek. Ze wilden het discreet houden. Er was niets wat Daan kon uitbrengen om tot ze door te dringen. Wat moest hij doen? De deur dicht gooien, schreeuwen, ze weg duwen? Waartoe waren deze AIVD'ers in staat? Daan voelde zich onveilig. Uiteindelijk gaf Tonnie haar visitekaartje met mobiel nummer en eindigde het gesprek met de woorden: “We bellen je wel een keer.” Het klonk als een waarschuwing waarna ze vertrokken.

Onder druk

Op zijn smartphone zag Daan dat hij eerder die dag gebeld was door hetzelfde nummer als op het visitekaartje. Ze hadden zijn 06-nummer klaarblijkelijk al in bezit. Plots herinnerde Daan zich dat een collega op zijn werk hem verteld had dat er iemand voor hem langs gekomen was, terwijl er geen afspraken vast stonden. Na een telefonisch onderhoud met zijn collega werd het duidelijk dat het dezelfde persoon betrof als die bij hem zojuist voor de deur had gestaan.

Tonnie was al op zijn werk langs geweest om informatie te vergaren. Daan werd misselijk van wat hij ervoer als bedreiging en mishandeling. Een paar weken later, halverwege januari, belde Tonnie inderdaad op, maar Daan nam niet op. Hetzelfde herhaalde zich eind januari. Tonnie belde opnieuw op. Later die dag werd er bij hem thuis aangebeld. Daan

liep naar het raam om te kijken wie er voor de deur stond maar zag niemand. Vertwijfeld deed hij de deur open en zag verderop Tonnie en haar partner de straat oversteken en in een auto stappen.

Die avond nam Daan contact op met Buro Jansen & Janssen. Daan wil niet met de AIVD praten, maar heeft het gevoel geen keus te hebben. Ze blijven aandringen, duwen en poken en zijn erg naargeestig. In 2011 had Daan ook al contact opgenomen met Buro Jansen & Janssen maar wilde destijds niets doen met zijn verhaal. Hij had Najat en haar AIVD tijdens dat gesprek afgepoeierd en vond het wel goed zo. Maar ditmaal voelt het anders.

Daan is woedend over de intimidatiepraktijken van de AIVD. “Wat hebben zij tegen mensen die gebruik maken van hun recht en betrokken zijn bij negatieve kwesties die zich in de wereld afspelen? Het gaat hier om mijn vrijheid van meningsuiting en vrijheid om mensen te ondersteunen die zich bewegen in een repressief regime zoals dat van Marokko. Mag dat niet in Nederland?”, vraagt hij zich af. “Mag je niet maatschappelijk betrokken zijn en boos zijn over wat er gebeurt in het land van herkomst?”

Daan, een gefingeerde voornaam, wenst anoniem te blijven en wil ook niet dat zijn woonplaats bekend wordt om eventuele repercussies te vermijden, zowel hier als in Marokko. Buro Jansen & Janssen is in het bezit van opnames, het telefoonnummer dat door de AIVD aan Daan is gegeven en de gegevens van de auto die Tonnie en haar collega gebruikten.

Interesse AIVD voor Marokkaanse solidariteitsnetwerken (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

Naar inhoudsopgave Observant #71

Bulk gegevens verzamelen is van alle tijden

Hield de BVD in de jaren tachtig mensen die op de Centrum Partij stemden in de gaten?

Uit BVD-documenten blijkt dat de geheime dienst in de vorige eeuw zeer uitvoerig de extreem-rechtse partij CP in de gaten hield. Hier was sprake van analoge bulkinterceptie waarbij ook niet aan de partij gelieerde personen het doelwit waren.

Op 21 maart vinden de gemeenteraadsverkiezingen plaats, maar ook het raadgevend referendum over de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV 2017). Deze wet regelt het wettelijk kader van de inlichtingendiensten AIVD/MIVD. Tegenstanders omschrijven de nieuwe opsporingsmaatregel als de Sleepwet, een verwijzing naar de bulkinterceptie van het dataverkeer die mogelijk wordt gemaakt middels invoering van de WIV 2017.

Met bulkinterceptie wordt digitale data van elke burger verzameld, verdacht of niet. De overheid stelt dat ze in eerste instantie data van iedereen verzamelt, maar dat er vervolgens een schifting plaatsvindt. In de WIV 2017 wordt bulkinterceptie om die reden OOG-interceptie genoemd, wat staat voor Onderzoeks Opdracht Gerichte interceptie. Met de benaming OOG-interceptie willen de diensten aangeven dat zij weliswaar de data van iedereen verzamelen, maar die niet allemaal bewaren en bestuderen.

Voorbeelden hiervan blijven abstract. Wordt alle data van elke inwoner van de Haagse Schilderswijk verzameld, of van mensen die communiceren met Rusland of Jemen, lid zijn van politieke partijen als Denk en Forum voor de Democratie? De WIV 2017 is vorig jaar door het parlement aangenomen en staat in de startblokken, maar eerst wordt de uitslag van het referendum afgewacht. Er is dus nog geen sprake van dagelijkse praktijk, of toch wel?

Communisten in het vizier

Tijdens de Koude Oorlog werden leden en sympathisanten van de Communistische Partij Nederland (CPN) in de gaten gehouden. De Binnenlandse Veiligheidsdienst (BVD), voorloper van de AIVD,

verzamelde lijsten van mensen die betrokken waren bij die partij of organisaties van communistische signatuur. Abonneeregistraties van partijkrant *De Waarheid* werden bemachtigd, ledenlijsten van lokale afdelingen van de CPN en andere registers. Kortom, van personen die op de een of andere manier er openlijk voor uitkwamen dat zij sympathiseerden met de CPN.

Deze mensen wilden natuurlijk niet door de BVD bespioneerd worden, maar hun lidmaatschap of abonnement toonde een zekere mate van betrokkenheid, interesse en affiniteit met de communisten. Dit wil niet zeggen dat de aandacht van de inlichtingendiensten geoorloofd was, want de CPN en verschillende maatschappelijke organisaties waren legale organen die onderdeel uitmaakten van de Nederlandse samenleving.

In het verleden, maar ook thans met de WIV 2017, konden de inlichtingendiensten individuen en organisaties in de gaten houden die een gevaar vormden voor de democratische rechtsorde. Na de Tweede Wereldoorlog werd het communisme als een gevaar gezien en dus hadden de CPN en gelieerde organisaties de bijzondere aandacht van de BVD. Vandaar dat de inlichtingendienst alle aan het communisme gelieerde personen in het vizier hield.

In dat opzicht verandert er niets met de nieuwe wet. Maar met bulkinterceptie wordt echter breder gekeken door de AIVD. Natuurlijk wordt geprobeerd alle data van leden of sympathisanten van bijvoorbeeld een netwerk van Syriëgangers te verzamelen. Bulkinterceptie is dan ook bedoeld om daadwerkelijk alle data van bepaalde personen te verzamelen, met name over zaken die misschien niet zijn onderschept middels het aftappen van individuen en organisaties.

Bulkinterceptie omvat echter niet alleen verdachten, maar ook volstrekt onbekenden die misschien alleen maar langs het huis van de verdachte lopen. AIVD-directeur Bertholee: “Stel dat het huis aan de overkant van de straat verdacht is. Dan zie ik mensen door de straat lopen. Ik kan er niks aan doen, maar ik zie ze. Zowel in m’n hoofd als in het observatierapport komen ze niet meer voor: ik mik ze er onmiddellijk uit.” [NRC, 04-02-18]

Centrum Partij bespioneerd

Worden passanten die langs een verdacht object lopen daadwerkelijk uit het observatierapport verwijderd? De BVD hield in de jaren '80 van de vorige eeuw de extreem-rechtse Centrum Partij (CP), en naderhand de extreem-rechtse CD en CP86, in de gaten. Via openbaarheidsverzoeken heeft Buro Jansen & Janssen verschillende documenten in handen gekregen van het omvangrijke dossier van de CP dat in het bezit is van de inlichtingendiensten.

Naast krantenartikelen, flyers, posters en partijblaadjes bevinden zich tussen de documenten allerlei stukken die duiden op een grote inlichtingenoperatie binnen de politieke partij. Verslagen van zowel publieke als besloten partijbijeenkomsten, notulen van vergaderingen en zelfs brieven. De CP werd zeer nauwlettend in de gaten gehouden omdat de partij een gevaar zou vormen voor de democratisch rechtsorde.

Het bespioneren van een politieke partij als de CP roept, net zoals het bespioneren van de CPN in de jaren '50 – '80, vragen op over de rechtmatigheid daarvan en in hoeverre er sprake kan zijn van het vormen van een bedreiging van de rechtsorde door een politieke partij.

Er is echter meer aan de hand. In het kader van de analoge bulkverzameling door de BVD bij haar onderzoek naar de CP heeft de dienst ook gekeken naar de kiezers op die partij. Zoals tijdens de raadsverkiezingen van 16 mei 1984 in de Rotterdamse deelgemeenten Prins Alexander, IJsselmonde en Charlois.

Tussen de documenten bevinden zich overzichten van de 'voorlopige uitslag deelgemeenteraadsverkiezingen deelgemeente Prins Alexander' per stemlokaal (stembureau). De BVD wist op die manier bijvoorbeeld dat 16 mensen bij stemlokaal 216 op het Varnasingel 201 op de CP hadden gestemd. In hoeverre er in het BVD-dossier van de CP meer documenten van kiezers, zoals bijvoorbeeld individuele stembiljetten, zitten, is niet duidelijk. De archieven zijn zeer beperkt openbaar.

Kiezers zijn misschien wel sympathisanten van een partij, maar niet noodzakelijk daarbij betrokken. Eens in de zoveel jaar stemmen ze op de CP, maar hun relatie hoeft niet verder dan dat te reiken. Ze zijn te vergelijken met de door Bertholee in de *NRC* aangeduide mensen die op straat langs een observatiepost lopen, maar blijkbaar zijn hun stemgegevens niet ‘weg gemikt’. Die zitten ruim dertig jaar later nog

steeds in het dossier.

De beperkte kennis over het CP-dossier van de BVD en de hoeveelheid verzamelde data die daarin is opgenomen en niet zomaar te herleiden valt uit interne notulen en brieven, roept de vraag op of burgers in 1984 ook hun stem in vrijheid en anonimiteit konden uitbrengen. Welke rol speelde de inlichtingendienst binnen de CP, hoeveel kennis had zij van niet-leden en betrokkenen, maar ook van hun kiezers? Welke invloed heeft de operatie van de BVD gehad op het functioneren van de CP? Vormde de CP een bedreiging van de rechtsorde of was het de BVD?

Bulkinterceptie omvat meer dan je denkt

In de tijd van Big Data en Open Data wordt het steeds gebruikelijker dat gegevens van stembureaus openbaar worden gemaakt zodat voor iedereen inzichtelijk wordt hoe de stemming in een buurt is verlopen. Zo zijn de definitieve verkiezingsuitslagen van de Rotterdamse gemeenteraadsverkiezingen van 2010 op internet terug te vinden.

Die ene stem op de Nederlandse Moslim Partij (NMP) bij stembureau 5, Springerstraat 340, is voor iedereen duidelijk. Ook pamfletten, sociale media gegevens en krantenartikelen over deze partij zijn op internet te raadplegen. De NMP-kiezer is misschien wel gelokaliseerd als zijnde woonachtig in de omgeving van stembureau 5 in Rotterdam, maar de persoon in kwestie heeft in vrijheid en anonimiteit zijn stem op het biljet doen laten gelden.

Uiteraard is bij bulkinterceptie ook de willekeurige voorbijganger doelwit van de inlichtingendiensten. Daar hoeven de diensten in principe geen bulkinterceptie voor in te zetten. De willekeurige voorbijganger die op internet een *like* uitdeelt, een positieve of negatieve reactie levert, zijn stem geeft aan de partij, zijn wel degelijk het doelwit van bulkinterceptie. De analoge bulkverzameling van de BVD met betrekking tot de Centrum Partij in Rotterdam maakt dat duidelijk.

Bulk gegevens verzamelen is van alle tijden (pdf)

Gehele Observant #71 Niet Transparante Overheid en Wetenschap (pdf)

BVD documenten deelgemeenteraadsverkiezingen 1984

Naar inhoudsopgave Observant #71

Maak het werk van Buro Jansen & Janssen mogelijk, word donateur

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

Word donateur of vraag familie, vrienden en bekenden donateur te worden. 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

Voorkom Vernietiging

Buro Jansen & Janssen heeft via via te horen gekregen dat de inlichtingendiensten niet blij zijn met de website https://voorkomvernietiging.nl. Wij willen daarom nu alvast iedereen bedanken voor hun steun zowel moreel als financieel en voor het indienen van allerlei inzageverzoeken. Blijkbaar heeft onze oproep een bescheiden effect en willen we dit graag voortzetten en uitbreiden. Vraag daarom anderen, vrienden, familie, kennissen ook verzoeken in te dienen of verspreid de oproep verder. Natuurlijk kunnen wij indien gewenst steun verlenen.

Buro Jansen & Janssen wil voorkomen dat de immense archieven van de Nederlandse inlichtingendiensten waaronder de BVD en diverse militaire inlichtingendiensten) worden vernietigd. Wij roepen mensen daarom op om zoveel mogelijk dossiers op te vragen in het belang van onze veiligheid, democratische controle op de diensten, burgerrechten en kennis over de betrokkenheid van de inlichtingendiensten bij allerlei sociaal maatschappelijke, culturele en politieke en andere gebeurtenissen in binnen- en buitenland.

De bevoegdheden van opsporingsdiensten en inlichtingendiensten zijn de afgelopen dertig jaar gestaag uitgebreid. De diensten beweren steeds dat dat in het belang is van onze veiligheid. De politiek gaat graag mee in die stelling en voorziet de diensten van de gevraagde bevoegdheden. Zo ook recentelijk.

De Tweede Kamer ging akkoord met het ongericht aftappen van het internet door de inlichtingendiensten. Het is te vergelijken met de grootschalige stofzuiger van de Amerikaanse inlichtingendienst, de NSA, die door Edward Snowden openbaar is gemaakt. De Nederlandse stofzuiger is natuurlijk van een kleiner kaliber.

Nu wordt er altijd geroepen dat de uitbreiding van die bevoegdheden en dus ook het aftappen van het internet door inlichtingendiensten in dit geval van belang is voor onze veiligheid. Rusland staat digitaal

voor de deur, terroristen zouden op het internet plannen beramen en andere voorbeelden worden aangehaald. Of je nu wel of niet die argumentatie van de diensten en de politiek steunt, is het natuurlijk van belang om te weten wat voor werk diensten in het verleden hebben uitgevoerd, wat de mislukkingen waren, de successen, de schendingen van grondrechten en de redenen van dat werk.

Die successen, mislukkingen en andere zaken zitten in de archieven van de inlichtingendiensten. Grote delen van deze archieven worden naar de brandstapel gebracht, wij weten niet wat, want dat is ook geheim. De Tweede Kamer die de bevoegdheden goedkeurde, keurde ook de vernietiging goed, dus van de politiek moeten we het niet hebben als wij willen weten wat de inlichtingendiensten in de Koude Oorlog en daarna voor werk hebben uitgevoerd en wat het resultaat daarvan was. Een groot deel van de archieven van de Inlichtingendienst Buitenland (IDB) zijn ook zonder slag of stoot van de politiek vernietigd.

Om te voorkomen dat de archieven vernietigd worden, roepen wij iedereen op om dossiers op te vragen om zo het archief veilig te stellen voor de toekomst. Wij publiceren een lijst wat u kunt opvragen, de adressen van de diensten, voorbeeldbrieven, zijn bereid indien gewenst de brieven op te stellen met onderwerpen naar keuze, willen ze fysiek versturen, zijn bereid bezwaar, beroep en hoger beroep te begeleiden, maar hebben uw handtekening en adres nodig. Procedures zijn lang, meestal jaren, wij hebben het geduld, wij rekenen op uw steun.

Kennis over het verleden is van essentieel belang voor kennis over het handelen in het heden en de activiteiten in de toekomst.

Buro Jansen & Janssen, maart, 2017

Naar inhoudsopgave Observant #71

ONDERMIJNER