Observant 65

30 juni 2014

Inhoudsopgave Observant nummer 65

Mocht je een interessant artikel hebben over je confrontatie met politie en justitie, een nieuwe wetgeving, onderzoek of scriptie mail het dan ons, info@burojansen.nl.

Externe publicaties zie de website
05 Dangerous Partnership & Contracting Insecurity
14 Grensgevangenen

Hier is de nieuwe Observant van Buro Jansen & Janssen. Om de twee maanden lukt nog niet, maar is nog steeds het streven. In dit nummer aandacht voor G4S, het grootste beveiligingsbedrijf van de wereld. Het motto van het bedrijf is ‘Securing your world’, maar is dat wel zo en hoe kritisch gaan de media en de overheid met het bedrijf om? Daarnaast Facebook (FB) als inlichtingendienst en als profiling center. Opnieuw benaderingen, een nieuwe website, een recensie, een oud boek en nog veel meer. Wilt u dat Jansen & Janssen de komende jaren onderzoek blijft doen naar politie, justitie en inlichtingendiensten, steun ons dan.

Wordt donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening N56INGB00006039 04 (ING 603904 BIC: INGBNL2A) ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam. Res Publica is de stichting van Jansen & Janssen.

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

G4S: Media, privatisering en burger- en mensenrechten

Heel langzaam sluipt de privatisering de beveiligingswereld in. Veiligheid lijkt te worden geïnterpreteerd als een allesomvattend concept. Beveiligingsfirma G4S draagt dit totale concept van veiligheid uit en dringt zo door tot in de haarvaten van de samenleving.

In enkele landen om ons heen verloopt het proces van beveiligingsontwikkeling nog wat sneller, maar over de gehele linie is duidelijk dat privatisering de veiligheid langzaam overneemt. Niet alleen vinden er controles op vliegvelden, in gevangenissen, politiecellen en winkels plaats, ook neemt de beveiliging van ambulances, reguliere opvang voor vluchtelingen, logistieke diensten en zelfs rond subsidieverlening toe.

G4S, de grootste beveiligingsfirma ter wereld, levert veiligheidsexperts aan de media, bewakers voor politiecellen in Nederland, ambulancepersoneel in het Verenigd Koninkrijk, complete gevangenissen in de VS, betaalt boeren uit in het kader van het Wereld Voedselprogramma van de Verenigde Naties en nog een veelheid aan diensten. Deze multinational is de op twee na grootste werkgever in de wereld. Het bedrijf groeit razendsnel door een eindeloze rij overnames, zowel op het gebied van de particuliere beveiliging als private militaire dienstverleners.

Bij ons eerdere onderzoek naar de relatie tussen Nederland en Israël in het kader van de beveiligingsindustrie, kwam G4S al bovendrijven (*Security Industry: links between Israel and the Netherlands? July 2011*). Hiervoor werden stukken opgevraagd over de relatie tussen de overheid en G4S. Bij de publicatie lag de nadruk vooral op de betrokkenheid van G4S bij de Israëlische bezetting van Palestina. Voortbordurend op dit rapport zal in deze *Observant*, en in een van de volgende, een serie artikelen verschijnen. Daarnaast hebben we een nieuwe reeks informatieverzoeken aan diverse overheidsorganen gestuurd.

Nu alvast de eerste drie artikelen over G4S. Het eerste belicht de relatie tussen de media en een beveiligingsexpert van het beveiligingsbedrijf, Glenn Schoen. Deze aparte relatie komt terug in het rapport *Dangerous Partnership, Private Military & Security Companies and the UN* dat in juni 2012 verscheen en waarvan in 2014 een update is gemaakt.

Op zowel *Security Industry* als *Dangerous Partnership* heeft G4S gereageerd. De reacties zijn opgenomen in de bijlagen van

de rapporten. *Dangerous Partnership* gaat over de relatie tussen de Verenigde Naties (VN) en private militaire en beveiligingsbedrijven, de verschillende rollen die deze bedrijven vervullen, van adviseur tot de eigenlijke bewaker, en natuurlijk ook de burger- en mensenrechten standaarden van die bedrijven. G4S en dochterondernemingen als Armorgroup komen regelmatig ter sprake in het rapport.

Wat het rapport en de update van waarde maakt, zijn niet alleen de beschrijving van de mensenrechtenschendingen en hoe de VN daar mee omgaat. Het rapport probeert ook de vraag te stellen wat het inhuren van bedrijven met een discutabele reputatie betekent voor de politieke geloofwaardigheid van een orgaan als de VN en wat het inhuren zegt over haar eigen legitimiteit. Hoewel er niet een eenduidig antwoord op volgt, is de vraag stellen al een belangrijk startpunt.

De VN heeft het over de noodzaak voor het inhuren, de kostenbesparingen en andere futiele argumenten die niet ingaan op de basisvragen ten aanzien van het aanzien dat de Verenigde Naties geniet, de reputatie van de ingehuurde bedrijven en andere fundamentele politiek/maatschappelijke vragen. De schrijfster van het rapport gebruikt het woord *bunkerization*, waarbij de VN niet meer vragen stelt over haar eigen rol maar zich achter een muur van veiligheidsmaatregelen terugtrekt.

De noodzaak van het inhuren, resoneert weer door in het artikel over de media en G4S. Daarin zegt Glenn Schoen dat "we in een gevaarlijke wereld leven". De VN huurt G4S in om haar te beschermen tegen 'de gevaarlijke wereld'. Vraag is echter waar het probleem ligt: bij de wereld of bij de ingehuurde bedrijven en de houding van de VN? *Dangerous Partnership* is zeker geen rapport over G4S, maar plaatst het bedrijf wel in een bepaalde context.

Tot slot in deze *Observant* een analyse van de documenten die zijn verkregen middels informatieverzoeken over de relatie tussen G4S en de overheid. Voor een van de komende nummers van de *Observant* wordt gewerkt aan stukken over G4S en de olie-, gas- en mijnindustrie, een lijst van incidenten waarbij G4S of haar dochterondernemingen betrokken waren, nieuwe inzage-documenten en de controle op de particuliere beveiligingssector in Nederland en daarbuiten.

Dangerous Partnerschip

Uit het rapport *Dangerous Partnerschip, Private Military &*

***Security Companies and the UN*:**

'The United Nations is increasingly hiring Private Military and Security Companies (PMSCs) for a wide array of security services. The UN's leadership says these services are needed to protect the organization's staff and worldwide operations from growing threats and unprecedented dangers.'

But many reports from governments, NGOs and the media have shown how PMSCs have committed serious human rights abuses, killed or injured innocent civilians, engaged in financial malfeasance and committed many other breaches of the law. Given the track record of these companies, serious questions arise as to whether PMSCs are appropriate UN partners for the complex task of creating a secure, just and lawful world. Opacity around the UN's use of PMSCs has so far prevented a healthy debate.'

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

Group 4 Securicor (G4S) is the world's largest security company in terms of revenues and has operations in more than 120 countries across six continents, according to the company website. With over 625,000 employees globally, it is the second largest private sector employer in the world, second to Wal-Mart.212 Several mergers helped G4S to obtain this position. In 2002, the Danish security firm Group 4 Falck A/S, as it was called back then, bought the American company Wackenhut, owner of several prisons in the US.213 In February 2004, Group 4 merged with the British company Securicor.

G4S offers a wide range of secure solutions and business processes, including secure facilities management, security consultancy, event security, secure transport services, security systems and security services to governments. The Group provides services to public, private and corporate customers.

In Israel, the Group's subsidiary is called G4S Israel (Hashmira Group). G4S Israel is the country's leading provider of security solutions and comprehensive security. The Group provides advanced security services, security systems and technology-rich protection, identification and control systems and patrol call center services. [… In 2010] G4S holds a 90.5% stake, while Igal Shermister, the Group's Chairman and grandson of the founder, holds 9.5% of shares.

G4S has been under fire for its presence in the Occupied Palestinian Territories (OPT) for about ten years now. In 2002, the security firm pulled guards out of the West Bank after investigations revealed how armed patrols work with Israeli settlers to intimidate, harass and control Palestinians.

Not much seems to have changed since. In November 2010, the journalistic watchdog DanWatch in Denmark published a report on G4S involvement in the OPT. According to their documentation, Hashmira has provided security services to three supermarkets in the settlements of Ramat Shlomo and Modi'in Illit. Additionally, another G4S subsidiary, called Moked 99, provides security services in several settlements.

On its webpage this company states it has so-called 'action zones' in the settlements of Har Adar, Maale Adumim and the settlement areas in East Jerusalem.

Bloomberg Businessweek lists Moked 99 as a Hashmira subsidiary. It is described as a patrol and monitoring operation, which provides design and installation services for intrusion/burglar alarms, fire detection systems, and closed-circuit television systems, also offering security services for hotels with building control, energy savings control, and low-voltage systems.

Also in November 2010, the Danish Berlingske Tidende revealed that G4S sold Israel torture instruments. This is from PressTV, a Danish publication reporting in English:

'The firm, named G4S, sells the devices to the detention facilities in the occupied West Bank, which provide the necessary means for torture of the Palestinian prisoners, Berlingske Tidende reported on Nov. 23. […] According to the Palestinian Ministry of Detainees, nearly 200 Palestinian inmates have so far died in Israeli confinement, either due to medical negligence or under torture.'

In a letter dated 21 December 2010, G4S responded to the allegations concerning its activities in the occupied territories and its involvement with illegal settlements. The company confirmed it had never pulled out of the occupied territories entirely. The letter does not clarify the extent of G4S involvement in the occupation at present.

'In 2002 we announced that we were withdrawing from several contracts providing security officers to residential settlements in the West Bank. Since then we have not

performed such work, nor bid for any such contracts. However, we continue to serve major commercial customers, for instance supermarket chains, whose operations include the West Bank. Under these contracts we will provide security officers to protect the premises of these commercial clients who serve the general public. The number of such officers deployed in the West Bank is generally less than 20 and currently stands at eight. Other G4S staff may also periodically travel through the West Bank in the course of their work.'

G4S does not address the alleged involvement in providing devices used for torture; the letter only refers to providing 'security equipment, including X-ray machines and body scanners, with associated maintenance services, to the Israeli police, prison service and Ministry of Defence. We do not control, nor are we necessarily aware, where this equipment is deployed as it may be moved around the country.'

As a result of the allegations about involvement in the occupied territories the City Council of Copenhagen decided to examine the possibility of cancelling its cooperation with Group 4 Securicor.

In the Netherlands, G4S is one of the two largest private security companies - turnover was 337.5 million Euros in 2008, (its rival Trigion made just a little less: 323 million Euros223). G4S offers a variety of services closely related to the activities of police and justice ('justitie' in Dutch), and other authorities. The company is most known to the public for surveillance and airport security. It also offers ATM management and transport of money and valuable articles. Less known services of G4S are, amongst others, organizing the detention of suspects in police custody, and providing guards for prison and refugee detention centres.

Accordingly, a quick-scan of the lists of contracts provided by the Dutch police regions and Ministries showed a lot of links with G4S. For the Regional Police Haaglanden, the company provides reception and security services. For Gelderland Midden, it provides training and safety solutions; for Hollands Midden, alarm and burglar installation and maintenance; while Limburg Zuid contracted G4S for key server services and alarm handling. Furthermore, the company provides surveillance and security services for the regions Utrecht, Friesland and Gooi en Vechtstreek. According to the list obtained from the VtsPN (a police body set up to coordinate cooperation within the Dutch police and as such responsible for supra-regional contracting) G4S obtained a national contract for the care of detainees in police cells

and another one for providing security services. The Ministry of Foreign Affairs hired the company to provide the security for Dutch official residences in Turkey, Denmark, Morocco and Poland.

One option to put pressure on G4S would be to join forces with trades unions, as the reputation of the company is reportedly bad on labour rights as well. Human Rights Watch recently conducted an investigation in the United States into the rights of employees to associate or to protest. HRW concluded that: 'G4S's attempt to deny rights of association and bargaining to 'sergeants' at the Florida Power and Light facility not only violated US law but also ran afoul of clear ILO norms.'

Indeed, in March 2009, The American Prospect (set up to pursue new policies and new possibilities for social justice) flagged up the problems unions have in organizing American workers. As an example to illustrate how unions increasingly find themselves having to organize the world, it used the example of the Service Employees International Union (SEIU) putting in global leverage to win the right to organize Wackenhut security guards.

'It began the campaign in 2002, but three years later, Wackenhut, a historically anti-union company of 35,000 U.S.-based security guards, became part of the immense British conglomerate G4S […]. The only way to organize Wackenhut in the U.S., SEIU determined, was to organize G4S globally. SEIU launched an ambitious campaign with its international affiliates, which included efforts to keep Wackenhut from receiving the security contract for the 2012 London Olympics; lawsuits in British, Indian, Indonesian, and Panamanian courts; and strikes by G4S employees across Africa. Awash in a global sea of troubles, on Dec. 16, 2008, G4S signed a groundbreaking agreement with the global network of unions, agreeing to obey national labour laws in each of the 115 countries where the company has a presence and honor a neutrality pledge during most unionization campaigns.'

G4S has a business ethics policy which was updated in December 2010, just after the Danish publications. It starts with a section on human rights, which seems to offer opportunities for holding the company to account:

'G4S supports the principles of the United Nations Universal Declaration of Human Rights and we are committed to upholding these principles in our policies, procedures and practices. Respect for human rights is and will remain integral to our

operations.

We will endeavour to work with business partners who conduct their business in a way that is compatible with our policies of respect for human rights and ethical conduct. We will work with customers to ensure that contractual requirements do not infringe human rights.

We will take measures to ensure that the work of our employees does not compromise internationally accepted human rights conventions, whilst recognising and respecting the diversity in local cultures across the different countries in which we operate." with customers to ensure that contractual requirements do not infringe human rights.

We will take measures to ensure that the work of our employees does not compromise internationally accepted human rights conventions, whilst recognising and respecting the diversity in local cultures across the different countries in which we operate.'

Observant 65, 30 juni 2014
Buro Jansen & Janssen 2014

Security Industry: links between Israel and the Netherlands? July 2011
http://www.burojansen.nl/paginas/pdf/SecurityIndustrylinksIsraeltheNetherlands.pdf

Dangerous Partnership, Private Military & Security Companies and the UN
http://www.globalpolicy.org/multimedia/podcast/51757-dangerous-partnership-private-military-and-security-companies-and-the-un-july-10-2012.html

Contracting Insecurity - Private military and security companies and the future of the United Nations
http://www.globalpolicy.org/images/pdfs/GPFEurope/PMSC 2014 Contracting Insecurity web.pdf

Media smullen van G4S 'terreurexpert'

Hij duikt de afgelopen jaren geregeld op in de media als 'onafhankelijk' expert op het gebied van terreur, Glenn Schoen. Hij verkondigt doemscenario's die de overheid dienen aan te sporen het pakket aan veiligheidsmaatregelen verder op te schroeven. Schoen echter is werkzaam voor de private beveiligingsfirma G4S, in wezen verkoopt hij zijn product.

Glenn Schoen is een graag geziene gast in de wereld van de media. Van het tv-programma *Dit is de dag* van Tijs van de Brink, BNR nieuwsradio, Pauw en Witteman, Met het Oog op Morgen tot aan Hubert Smeets van *NRC Handelsblad*: ze maken allemaal dolgraag gebruik van de diensten van Schoen. Hij wordt onder andere omschreven als 'terrorisme deskundige/expert', 'terreurdeskundige/expert', 'Al Qaida deskundige/expert', 'veiligheidsdeskundige/expert', 'veiligheidsanalist' en 'beveiligingsdeskundige'.

Waaraan hij al deze titels te danken heeft, is niet altijd even duidelijk. Schoen heeft geen indrukwekkende publicatielijst op zijn naam staan. Wie een boek van hem probeert te vinden, raakt teleurgesteld. Ook artikelen van zijn hand in de media zijn moeilijk te vinden. Zelfs op de website van G4S, het beveiligingsbedrijf waar hij voor werkt, bevat geen publicaties onder de naam van Schoen.

Hans Beerekamp schrijft in een van zijn tv-recensies in *NRC Handelsblad* (11-02-14) dat Glenn Schoen een 'praktijkman' is, 'in de hoogtij van wat toen steevast werd aangeduid als 'moslimterrorisme' werd nog wel eens een praktijkman (Glenn Schoen was de bekendste) voor de camera gehaald.' Volgens Beerekamp willen 'we (de media red.) tegenwoordig toch liever een wetenschapper.' Wie echter de mediastatus van Schoen bekijkt, constateert dat hij nog steeds een graag geziene gast is op radio en tv, maar ook in de geschreven media.

In de *NRC* wordt hij zelfs twee dagen eerder dan de angehaalde tv-recensie van Beerekamp door journalist en 'Ruslandkenner' Hubert Smeets geciteerd in relatie tot de veiligheid van de Olympische Winterspelen in het Russische Sotsji: "Neem van mij aan dat de Russen voor een goede package zorgen: politieauto's, motorrijders, busjes", zo weet Schoen te melden.

Dokter Clavan

Er is sprake van een aantal opvallende zaken die aan het

optreden van Schoen in de media ten grondslag liggen, maar ook de manier waarop de media met de man omgaan, baart enig opzien. De wijze waarop Schoen bijvoorbeeld zijn mening verkondigt, getuigt van een hoog 'dokter Clavan' gehalte. Misschien niet geheel vergelijkbaar met het niveau van het gesprek tussen interviewer Hobbema (acteur Wim de Bie) en dokter Clavan (Kees van Kooten) tijdens een tv-uitzending van *Keek op de Week* (12-11-89), maar veel recente opmerkingen van Schoen echoën het typetje van Van Kooten na:

Hobbema: "Dokter Clavan, het gaat allemaal ongelooflijk snel hè?"
Clavan: "Meneer Hobéma, het gaat eh, ongelooflijk snel."
Hobbema: "In een week tijd treedt de regering af, er komt een nieuw Politbureau, een vervroegde Partijconferentie... het is toch niet gering, hè, wat daar gebeurt?"
Clavan: "Als u nagaat dat in één week tijd de regering aftreedt, dat er een nieuw Politbureau wordt benoemd, dat er een vervroegde Partijconferentie wordt uitgeschreven... Dat is niet gering hoor, wat daar gebeurt."
Hobbema: "En dan de Muur, die eigenlijk geen functie meer heeft..."
Clavan: "De Muur heeft eigenlijk geen functie meer."

Taalhistoricus Ewoud Sanders schreef in zijn boek *Jemig de pemig!* (2000, etymologiebank.nl) dat de personage van dokter Clavan voortkwam uit het feit dat de ontwikkelingen (in Oost Europa red.) zo snel gingen en zo onduidelijk waren dat de gemiddelde leek die z'n krant had gelezen en naar CNN had gekeken, er evenveel zinnigs over kon opmerken als een wetenschapper die er jaren voor had doorgeleerd. Het was alom koffiedik kijken, speculeren en zinnen vullen zonder veel te zeggen.' Schoen is dan wel geen wetenschapper, hoewel hij soms MA (Master of Science) achter zijn naam laat zetten, maar gebruikt veel van de technieken van dr. Clavan.

In het artikel van Smeets over Sotsji, hoewel geen tv/radio, lijkt de conversatie van Hobbema en Clavan te worden gespiegeld. Smeets schrijft: 'De politie krijgt ondersteuning van 23.000 mannen en vrouwen van het paramilitaire Ministerie voor Noodtoestanden.' Smeets gaat verder over de draconische maatregelen die de Russen hebben afgekondigd. Dan volgt een vraag aan Glenn Schoen over de beveiliging van de Nederlandse hoogwaardigheid beklederS in Sotsji. Het antwoord van Schoen is dan zoals boven weergegeven: "Neem van mij aan dat de Russen voor een goede package zorgen: politieauto's, motorrijders, busjes."

Op 17 maart 2014 wordt Schoen uitgenodigd door BNR

Nieuwsradio voor een item over de verdwenen Boeing 777 van Malaysia Airlines (MH370) vanwege de lading en of het vliegtuig gekaapt zou kunnen zijn. De interviewer: "Want die theorie van die kaping is een hele serieuze aan het worden?" Schoen antwoordt: "Ja, dat is een hele serieuze aan het worden. Als we kijken naar hoe het toestel is gevlogen, wat er nodig moest zijn om het te veranderen. Welke route die initieel heeft gekozen? Het moment van de vlucht waarop het is gekozen?"

De Nuclear Security Summit van 24 en 25 maart in Den Haag vormde een van de hoogtepunten voor Schoen. Veel journalisten vonden hun weg naar onze 'terrorisme-expert'. Journalisten van onder andere het *Dagblad van het Noorden*, diverse edities van het *Algemeen Dagblad*, *het Parool*, *De Nieuws BV* van de VARA en het NOS Journaal raadpleegden hem. In *het Parool* (22-03-14) wordt Schoen geciteerd: 'Volgens Schoen draait het allemaal om het afdekken van voorspelbare en voorstelbare risico's. "De groepen moeten van elkaar gescheiden blijven; je wilt niet dat een Amerikaanse delegatielid wordt aangereden door een bakfiets."'

'Gevaarlijke wereld'

De gemeenplaatsen die Schoen keer op keer herhaalt, lijken voor de media aantrekkelijk. Hij spreekt heldere en duidelijke taal. Er is echter ook iets anders waarom de man een graag geziene gast is. Hij vertegenwoordigt een groot deel van de journalistieke wereld die geen kritiek heeft op politie, justitie en inlichtingendiensten. Woorden als repressieve tolerantie, repressie, doorgeslagen veiligheidscultuur, gewelddadig politie-optreden en overmatige inbreuk op de burger- en mensenrechten wensen veel media niet langer in hun programma's horen. Het gevaar van nu vormt bij de media het islamitisch terrorisme, de zelf ontbrandende burger, de eenzame waxinelicht-gooier en andere randverschijnselen van deze samenleving.

Schoen sluit naadloos aan bij deze ideologie van de veiligheidsstaat. In het *Financieele Dagblad* (20-08-13) wordt hij geciteerd: "Als een van de kernactiviteiten houdt Al Qaida zich al tien jaar bezig met het kijken naar treinen als doelwit." Voorbeelden hiervan zijn de aanslagen op treinen in Madrid in 2004 en op de Londense metro in 2005. "Dergelijke aanvallen zijn moeilijk te voorkomen. Het spoor is onderdeel van onze kritische infrastructuur, het is kwetsbaar, een aanslag werkt ontregelend. En helaas heeft een aantal incidenten laten zien dat je veel slachtoffers kunt krijgen", aldus de veiligheidsexpert. Het artikel is geschreven naar

aanleiding van een artikel in het blad *Bild* waarin beweerd wordt dat 'veiligheidsdiensten gewaarschuwd hebben voor mogelijke aanslagen op zowel treinmaterieel als spoorinfrastructuur.'

Veel van wat Schoen zegt is een open deur: "Een aanslag werkt ontregelend, je krijgt veel slachtoffers". Het ontbreekt de man aan kritische analyse: "Dergelijke aanvallen zijn moeilijk te voorkomen." Analyses van de aanslagen in Madrid en Londen, en de betrokkenheid en het falen van politie en inlichtingendiensten daarbij, zijn niet besteed aan Glenn Schoen.

"We leven in een gevaarlijke wereld", zegt hij aan het eind van een tv-uitzending van *Dit is de dag* met Tijs van den Brink (02-12-13). Het item gaat over het benaderen ven studenten die protesteerden tegen het bezuinigingsbeleid van de regering door de AIVD. Natuurlijk vindt Schoen het goed dat de dienst alles doet om de veiligheid van Nederland te waarborgen. Van den Brink is het helemaal met Schoen eens en stelt geen enkele kritische vraag aan de 'terreurdeskundige'. Ook vraagt de interviewer niet naar het bedrijf waar Schoen voor werkt. De EO heeft Schoen in de Rolodex staan, want hij treedt er geregeld op bij 'veiligheidsvraagstukken'.

Dubbele tong

Niet alleen de media zijn van hem gecharmeerd, ook in de semi-academische wereld van inlichtingen- en veiligheidsstudies is Glenn Schoen veelvuldig te vinden. Assistent Professor Giliam de Valk, docent aan de UvA, geeft samen met Schoen les aan de European Security Academy. Hun module is 'Direction' genaamd: 'Voorafgaand aan het diner wordt een praktisch verband gelegd via global threats.' De module behandelt onder andere de dreigingsmatrix en informatiepositie. Over Schoen staat geschreven dat hij 'G4S Risk Advisory' is en blijkbaar kennis heeft over 'global threats' en informatieposities van overheden en bedrijven.

Enkele jaren geleden heeft Professor Dr. Rob de Wijk van The Hague Centre for Strategic Studies Schoen uitgenodigd voor de derde internationale masterclass over *'International Emergency Management and specifically Consequence Management: try to prepare for the unthinkable disaster!'* Schoen sprak tijdens dit evenement in december 2011 over de bedreigingen van de moderne samenleving. Een jaar eerder waren de heren al gezamenlijk naar buiten getreden met het verhaal dat er sinds 11 september 2001 "zeker vijftig omvangrijke terroristische aanslagen van moslimextremisten in Europa voorkomen" (AD, 25-

09-10). Schoen stapte in 2010 over van Ernst & Young naar G4S. Ook Edwin Bakker, hoogleraar Terrorisme aan de Universiteit Leiden, kent Glenn Schoen al jaren en deelt vaak zijn mening over veiligheid en terrorisme in de media.

Hans Beerekamp schrijft in zijn tv-rubriek van 11 februari 2014 dat Schoen zo vaak optreedt omdat 'de meeste mensen die er echt iets vanaf weten er niet over mogen praten.' Volgens de NRC-journalist zouden mensen van de inlichtingen- en veiligheidsdiensten de mensen zijn 'die er echt iets vanaf weten.' Wie de kritische literatuur over het veiligheidsbeleid volgt, zal concluderen dat geheime diensten het meestal niet echt zo goed lijken te weten. De mogelijke val van de Muur ontging de CIA in het geheel, evenals de aanslagen van 11 september 2001. Ook de AIVD en haar voorloper de BVD hadden veel zaken niet door, zoals de moorden op Pim Fortuyn en Theo van Gogh.

Het gaat dus niet om de expertise van Schoen, maar om zijn mening die werd gevormd door zijn 'professionele' carrière. En daar doet zich iets geks voor. Wie in de krantenbank zoekt op de naam Glenn Schoen komt de expert of deskundige Schoen vaak tegen. Dat de man deskundige is, wordt overal vermeld, maar slechts in een derde van de artikelen over Schoen in *Lexis Nexis* van de afgelopen jaren wordt tevens de naam vermeld van het bedrijf waarvoor hij heeft gewerkt. Ook op radio en tv wordt vaak niet vermeld dat Schoen werkzaam is voor de beveiligingsindustrie.

Is dat dan zo belangrijk? Als Schoen zegt dat 'we in een gevaarlijke wereld leven', 'treinen gevaar lopen' en 'elke massa is doelwit' (*Parool*, 11-07-05), moet de mediaconsument weten dat hier iemand spreekt die zijn boterham verdient met beveiligen. Het aandikken van het gevaar kan, indirect, extra inkomsten voor het bedrijf waar Schoen voor werkt opleveren.

Inlichtingen- en beveiligingsadviezen in de commerciële wereld, maar ook in de publieke sector hebben zowel te maken met omzet als met politieke kleur. Glenn Schoen werkt al sinds 1988 in dienst van de commerciële inlichtingenwereld. Eerst onder de vleugels van Noel Koch, een *hard-liner* die diende onder president Nixon en Reagan, en sinds 2006 als beveiligingsanalist voor Ernst & Young en G4S. Het feit dat hij voor G4S, het grootste beveiligingsbedrijf van de wereld, werkzaam is, maar ook nog eens een groot deel van zijn professionele carrière bij bedrijven van een conservatief uit de rangen van Nixon, zegt iets over zijn mening omtrent beveiliging en hoe de wereld in elkaar zit.

Private inlichtingenwereld

Schoen kan dus in principe over alles meepraten. Of het nu gaat over Sotjsi, verdwijntips voor Holleeder, benaderen van studenten door de geheime dienst, Osama Bin Laden, een verdwenen Boeing, beveiliging rond de Olympische Spelen of de NSS; hij heeft een antwoord paraat. Hij werkt al vele jaren in de wereld van het op commerciële basis verzamelen van inlichtingen en adviezen geven over beveiliging. Een lucratieve wereld, zoals hij zelf ooit eens als veiligheidsadviseur van Ernst & Young duidelijk maakte. "Wereldwijd gaat er 53 miljard om in de beveiligingsindustrie", zegt Glenn Schoen, terrorisme-expert van Ernst & Young. "Meer dan in de film- en de muziekindustrie bij elkaar."(*Vrij Nederland,* 10-02-07)

Schoen begon zijn analytische carrière in 1988 bij International Security Management Inc. (ISM Inc.), een bedrijf uit het Amerikaanse Maryland. ISM Inc. is een zogenoemd beveiligings-adviesbedrijf. Het verdient zijn geld met het verkopen van reis- en veiligheidsadviezen aan bedrijven en vakantiegangers. De meeste van die adviezen bestaan uit het opnieuw verpakken van overheidsinformatie, maar ook uit het bijhouden van berichtgeving door de internationale media.

In 1998 legde Schoen uit dat het beter is om het Midden-Oosten te vermijden. *'Certain Islamic countries pose the biggest threat, security consultants like Schoen say, especially Iraq, Jordan, Yemen*', tekent de *Seattle Times News Services* (15-02-98) op uit de mond van Schoen. Schoen's informatie is echter grotendeels afkomstig van overheidsorganen en uit de media. '*The State Department has issued an alert urging American travelers to be aware of government warnings and travel advisory updates stemming from anxieties in the Persian Gulf*', wordt enkele regels eerder aan de opmerking van Schoen vermeld.

In het algemeen volgen private inlichtingenbedrijven de overheidsinformatie op de voet en 'verkopen' die door aan bedrijven en individuen. Een woordvoerder van het State Department legt Schoen bijna de woorden in de mond, al gebruikt die dan niet de namen van specifieke landen: '"*While at this time we know of no specific threats to U.S. citizens or interests overseas in relation to the present situation in Iraq, we cannot discount the possibility of random acts of anti-American violence", a spokesman said.*'

De baas van International Security Management Inc. is Noel

Koch die in 1986 ook de president wordt van een ander commercieel inlichtingenbedrijf, Transecur inc. Dit bedrijf wordt omschreven als een 'web-based' beveiligings-/adviesbedrijf dat inlichtingen over mogelijke gevaren verschaft aan bedrijven, overheden en rijke families. Koch werkte in de jaren '80 onder president Reagan als assistent van de minister van Defensie en als directeur speciale planningen van het Amerikaanse ministerie van Defensie. Daarvoor was hij tevens speciaal assistent van president Nixon. Hij leidde het eerste onderzoek naar de aanslagen op de Amerikaanse ambassade in Beiroet in 1983. Koch is duidelijk een hardliner en warm pleitbezorger van de private beveiligingswereld. Schoen heeft vanaf eind jaren '80 voor hem gewerkt.

Eind jaren '90 verkaste Schoen van International Security Management Inc. naar Transecur inc. waar Koch ook de baas van is. In 2004 opent Transecur een Europees kantoor in Den Haag. Koch benoemt Schoen tot directeur analytische diensten. *Business Wire* (01-06-04) omschrijft Schoen als een expert op het terrein van '*European and Middle Eastern sub-conflicts, and special interest activism*'.

Dat Schoen een goede leerling van Koch is geweest, blijkt uit een presentatie tijdens een conferentie in Polen, oktober 2012. Onder de titel 'Terrorism in Europe: Perspectives on 2013-2014' vertelt Schoen over hoe "*the terrorist threat from various quarters - leftwing, rightwing, Jihadist, separatist, activist - is evolving.*" Links, rechts, activist, of separatist, het zijn allemaal jihadi en gevaarlijk, zo is de 'overtuiging' van Schoen.

Media-carrière

In 2005 verlaat Schoen, na 18 jaar werkzaam voor Noel Koch te zijn geweest en na een jaar als Europese directeur van Transecur, zijn post en treedt in dienst van Ernst & Young als veiligheidsadviseur. In dat jaar begint ook zijn Nederlandse media-carrière. In Amerika had hij ook al een status als mediadeskundige opgebouwd, maar de Amerikaanse Nederlander moet in Holland natuurlijk een nieuwe status zien op te bouwen.

Dit gaat hem goed af, mede dankzij de hoogleraren Rob de Wijk en Edwin Bakker. In 2010 beweren de Wijk en Schoen beiden dat de inlichtingendiensten vijftig aanslagen hadden weten te voorkomen sinds 2001. Veel bewijs hadden ze er niet voor, maar de twee 'terreurdeskundigen' uit zowel de publieke als de private sector kregen veel aandacht in de media. In 2010

stapt Schoen over naar G4S om daar de post '*risk advisory*' in te vullen. Op de website van G4S is te lezen dat 'Security en Safety Risk Management een groeiende noodzaak' zijn.

Glenn Schoen werkt ondertussen bijna vier jaar als veiligheidsadviseur bij het grootste beveiligingsbedrijf ter wereld. G4S is daarnaast de een na grootste werkgever op aarde met meer dan 600.000 werknemers en biedt oplossingen voor zo'n beetje alles, waarbij het niet altijd alleen om veiligheid draait.

G4S verzorgt de beveiliging op vliegvelden, voor de Olympische Spelen, regeringsgebouwen, havens, allerlei instituties van de Verenigde Naties, niet gouvernementele organisaties, banken en andere commerciële bedrijven, mijnen, olievelden en installaties, kerncentrales. Maar het bedrijf is ook actief bij het geldtransport, in het gevangeniswezen, politiewerk, ambulancewerk, vluchtelingengevangenis en uitzettingen, huisarrest toezicht. G4S is op vele plaatsen doorgedrongen in de haarvaten van de samenleving. Een allround bedrijf, net als Schoen die van alle markten thuis is en overal kan aanschuiven.

Bij al die mediaoptredens werd Schoen sinds 2010 nooit iets over zijn eigen bedrijf gevraagd. Tijdens de elfde European Security Conference & Exhibition in april 2012 hield hij een lezing over 'Olympic Terrorism Concerns - Past & Present'. Niemand in de zaal zal hem lastige vragen hebben gesteld over het aanstaande debacle dat G4S in de zomer van dat jaar ontketende. Het bedrijf bleek niet in staat om genoeg beveiligers te rekruteren en voor een deugdelijk veiligheidsplan te zorgen. Het Britse leger moest uiteindelijk uitrukken om de Olympische Spelen in Londen door te kunnen laten gaan.

Iedere burger kan bedenken dat een van de eerste vereisten voor het voorkomen van aanslagen een goede beveiliging is. Daar hoef je geen deskundige of expert voor te zijn. Schoen is nooit over het disfunctioneren van G4S bij de Olympische Spelen in Londen ondervraagd. Ook rond het WK voetbal in Zuid-Afrika (2010) en de Olympische Winterspelen (2014) is Schoen over terreurdreigingen in de media verschenen.

Schandalen

Na het fiasco rond de gebrekkige beveiliging rond de Olympische Spelen van 2012 in Londen stapelden de schandalen rond G4S zich op. De schandalen speelden zich vooral af in Engeland, maar dit is deels bedrog aangezien de Britse media

veel publiceren over het bedrijf en haar medewerkers. Het gaat dan om uiteenlopende zaken, zoals het oplichten van de overheid bij een programma voor het controleren van mensen onder huisarrest. G4S heeft de overheid rekeningen gestuurd van mensen die allang geen huisarrest meer hadden, of die overleden waren.

De dood van een invalide man die werd vervoerd door een ambulance van G4S, het uitzetten van een zwangere vrouw die op het punt stond te bevallen, de dood van een vluchteling door toedoen van G4S-bewakers die de man voorafgaande ook nog racistisch zouden hebben bejegend, de slechte staat van de opvang voor asielzoekers waarbij de lokale overheid moest ingrijpen, zijn slechts enkele andere voorbeelden van de vele schandalen rond het bedrijf.

In het buitenland is het niet veel beter gesteld. G4S stuurde slecht getrainde labiele bewakers naar Irak die elkaar doodschoten en verwondden. In de VS konden mensen zomaar het terrein van een uraniumverrijkingsfabriek, beveiligd door G4S, oplopen. In Israël werkte G4S mee aan de afsluiting van de bezette gebieden, de West Bank en de Gaza-strook. Ook verzorgde het bedrijf de beveiliging van gevangenissen waar Palestijnse politiek gevangenen en kinderen worden opgesloten.

In Australië stierven vluchtelingen en gevangenen in de slecht geprivatiseerde gevangenissen van G4S, terwijl in Zuid-Afrika gevangenen werden gemarteld middels elektroshocks en plat spuiten. De meeste media schreven een nieuwsbericht over de martelingen en noemden G4S. In *De Groene Amsterdammer* beschrijft freelance-journalist Ruth Hopkins het onderzoek naar de behandeling van de gevangenen door G4S. Enkele media besteedden er iets meer aandacht aan, maar Glenn C. Schoen is in het openbaar nooit naar de situatie in de gevangenissen in Zuid-Afrika gevraagd.

Kritiekloze media

Begin dit jaar stonden de kranten vol van een personeelsstaking bij G4S wegens dreigende ontslagen. Dit als gevolg van de bezuinigingen en sluitingen van gevangenissen door het ministerie van Veiligheid en Justitie. Door middel van bezettingen, demonstraties en picket-lines probeerden de werknemers de directie van G4S op andere gedachten te brengen. De media-aandacht voor werknemers die worden ontslagen staat in schril contrast met de aandacht die de vele burger- en mensenrechtenschendingen door G4S krijgt.

Schoen's regelmatige mediaoptredens blijven ondertussen gewoon doorgaan. Op 8 maart 2014 treedt hij op als veiligheidsdeskundige in het NOS radioprogramma Met het Oog op Morgen, zonder de vermelding dat hij voor G4S werkt. Hij wordt gevraagd naar de mogelijkheid van een terroristische aanslag op vlucht MH370 van Malaysia Airlines. Op 11 april 2014 zit hij in de uitzending van WNL Opiniemakers van de publieke omroep over het feit dat er geen particuliere beveiligers worden toegelaten op Nederlandse koopvaardijschepen.

Tussendoor verschijnt er een interview met hem op de G4S website. Schoen geeft daarin aan dat "G4S zowel in een adviesrol als een operationele rol betrokken was bij de NSS. Als kleine schakel in een enorme operatie, heb ik persoonlijk invulling mogen geven aan de adviseursrol." Naast zijn eigen 'bescheiden' rol, noemt Schoen ook de rol van het gehele bedrijf waar hij voor werkt. "Naast de massale inzet van politie en defensie, droegen ook veel beveiligers uit de private sector een steentje bij op het gebied van *security* en *safety*. G4S leverde ongeveer 1.100 extra diensten tijdens de NSS", wordt uit de mond van Schoen opgetekend.

Natuurlijk wordt Schoen niet gevraagd waarom G4S eigenlijk niet de gehele beveiliging heeft mogen uitvoeren. Het Olympisch debacle zal G4S zo snel mogelijk willen vergeten. Over wat er dan met de adviezen van Schoen is gebeurd, wil de tekstschrijver van de website van G4S ook al niet weten, maar het artikel is dan ook bedoeld als promotie van de beveiligingsbranche en specifiek G4S.

Toch is er niet zoveel verschil tussen het optreden van Glenn C. Schoen op de website van G4S en zijn optreden in de Nederlandse media. Waarom de beveiliger met alle egards wordt ontvangen, lijkt minder met zijn expertise te maken te hebben dan met zijn onkritische houding ten aanzien van de veiligheidsstaat. Als beveiliger is het logisch om de wereld als het inferno van Dante te omschrijven, hoe gevaarlijker, hoe meer business. Voor de journalistiek lijkt in principe hetzelfde uitgangspunt te gelden. Geweld en ellende verkopen nu eenmaal beter dan het verhaal dat de meerderheid van de Nederlanders elke dag zonder problemen zal doorkomen.

Toch verwacht je van de journalistiek wel enige mate van feitenonderzoek, en op z'n minst dat de achtergrond van de 'deskundige' of 'expert' expliciet wordt vermeld. Het weglaten van de naam van het bedrijf waar Schoen voor werkt, geeft eigenlijk aan dat de media niet geïnteresseerd is in de werkelijke feiten ten aanzien van de veiligheid, maar graag

een mening wil horen die overeenkomt met die van de journalist. Bij de berichtgeving over het veiligheidsbeleid in Nederland of elders wordt bijna nooit voor een kritische insteek gekozen. Het optreden van Schoen in de media is daar dan ook een schoolvoorbeeld van.

Observant 65, 30 juni 2014

The United Nations and G4S: Challenges in the contracting of private military security companies for international peacekeeping and humanitarian support

Two reports authored by Lou Pingeot and published by the Global Policy Forum and the Rosa Luxemburg Stiftung – New York Office present the alarming trend of the United Nations (UN) contracting private military security companies (PMSCs) to provide a broad range of security and non-security services connected to peacekeeping and humanitarian missions as well as other UN operations. This article briefly reviews some of the findings of Pingeot's reports and the concerns raised regarding the relationships between the UN and PMSCs, particularly in light of the companies' track record of malfeasance and human rights abuses.

Pingeot's reports identified ten major PMSCs and of dozens smaller and local companies in the industry that have been contracted by the UN. This article focuses on G4S and its contracts with UN agencies, summarizing the UN contracts with the G4S family and presenting some examples of the company's misconduct. The responses of G4S to Pingeot's reports are also presented.

The fundamental concerns with the UN's use of PMSCs are described, along with the UN's response to the initial report, as presented by Pingeot in the follow-up report. The article ends with questions raised by this issue, in particular how to address the trend towards the "securitization" of peacekeeping and humanitarian efforts and how to hold private multinational corporations in the military and security industry accountable for their actions.

Key reports: *Dangerous Partnership* and *Contracting Insecurity*

In 2012, the Global Policy Forum and the Rosa Luxemburg Stiftung – New York Office published *Dangerous Partnership: Private military security companies and the UN*, exposing the growing reliance of United Nations (UN) on private military and security companies (PMSCs) for the provision of a broad range of services – from armed security of UN

facilities to transport and logistics support, from landmine clearing to identifying voting sites for elections (Pingeot 2012). Author Lou Pingeot presents the companies' negative track record on human rights, financial scandals, and other illegal and unethical practices, and questions whether PMSCs are appropriate partners for the UN.

Lack of transparency on UN contracting raises questions about accountability

The *Dangerous Partnership* report raises several concerns, among them the lack of transparency at the UN regarding contracting with PMSCs. The author uncovered **USD 44 million in security services contracting by the UN in 2009** and **USD 76 million in 2010**. A follow-up report by the same author documented **USD 113.8 million in UN expenditures for "security services" in 2011** and **USD 124.3 million in 2012** for a combination of UN contracts regarding "Security and Safety Services and Public Order" and "Security, Safety, Law Enforcement Equipment, including Demining and [Personal Protective Equipment]" (Pingeot 2014, p6).

These figures are incomplete, as not all UN agencies fully reported their expenditures in contracts with PMSCs. In the initial report, Pingeot analyzed data provided by the UN which listed the World Food Program (WFP) and UNICEF as having no private security service contracts, even though both agencies spend "substantial amounts" on private security. (Pingeot 2012, p46) The WFP is a UN agency dedicated to providing food supplies during emergencies, including armed conflicts, natural disasters, and crop failures. The WFP also provides emergency support to farmers and other impoverished communities engaged in food production. The WFP often contracts with PMSCs for security and logistics support in providing emergency relief to remote areas around the world.

Additionally, the figures provided by the UN do not include indirect contracting of PMSCs for UN-related activities. The WFP, for example, outsources food distribution operations to non-governmental organizations (NGOs) or local contractors that have the capacity and local contacts to provide emergency responses. These groups may in turn hire a PMSC to provide security for their WFP-funded

activities. NGOs like CARE – among several others – have reported using professional security firms to ensure the safety of convoys transporting food to areas in desperate need of humanitarian relief (International Alert, p26). This type of sub-contracting of PMSCs through a third party is not captured within the UN's reporting, even though these activities are paid for by the UN and the overall project is perceived as a UN project.

Another form of indirect PMSC contracting described by Pingeot takes place when member states hire PMSCs to conduct UN-related activities on their behalf. This includes allegations that PMSCs Aegis and Control Risks Group were contracted by the US and the UK to protect UN officials in Iraq, and instances of US contracting of PMSCs to provide police personnel for UN peacekeeping missions (Pingeot 2012, p26). These services are also excluded from the UN's reporting since they are not UN contracts.

The lack of comprehensive information available on the UN's contracts with PMSCs points to a culture of secrecy and lack of accountability that enables, and in fact encourages, the use of disreputable companies. Pingeot reports that the UN often issues no-bid contracts to PMSCs, which "allow for exceptional profits and maximum secrecy" (Pingeot 2012, p12). Prior to Pingeot's first report, the UN had never conducted a policy review of the impact of its use of PMSCs, nor had member states debated the issue. Despite the lack of standards and monitoring, UN contracting with PMSCs continues to grow, as evidenced by the figures cited above. Pingeot assesses the UN's justifications for using PMSCs – cost-effectiveness, immediate availability, and the need for a 'last resort' option – and finds that they are weak arguments and that the supposed benefits do not stand up to scrutiny.

The rise of the private military security industry and its misconduct

Pingeot's *Dangerous Partnership* report provides a background on the emergence of PMSCs as an industry with roots in mercenary groups that appeared in European colonies after World War II as well as the private detective and security business that originated in the

United States in the 1850s. After reviewing the concerns about PMSCs that have been expressed by public critics and governments, the report outlines the different types of services that PMSCs provide to the UN with examples of contracts and the questions that these contracts raise. Referring to mobile or convoy security provided by PMSCs, Pingeot states that "[m]any of the best-known scandals of security companies have arisen in this activity, when guards have been known to open fire on civilians wrongly suspected of evil intentions. In the past, the UN has contracted with notorious firms Lifeguard and DSL for such services" (Pingeot 2012, p25). Defence System Limited (DSL) became ArmorGroup in 1997, which in turn was acquired by G4S in 2008.

Among the concerns is the ubiquitous nature of PMSCs. The companies are often hired to work in the same geographic area on behalf of different clients – multiple agencies within the UN as well as NGOs and governments, providing different types of services. This creates confusion for local residents who do not differentiate among contracts and simply see the same people, sometimes carrying guns other times not, conducting a very broad variety of tasks. One example of this situation is described by Pingeot in relation to ArmorGroup in the Herat Province of Afghanistan. The United Nations Office for Project Services (UNOPS) – a UN agency that provides operational support for peacebuilding, humanitarian and development projects – contracted ArmorGroup to conduct mine clearance in the area at the same time that the company was sub-contracted to provide security for the US government's Shindand airbase in the same province.

This particular situation had an additional complication when it was alleged that ArmorGroup had hired Afghan warlords to conduct its activities in Herat. The US Senate Committee on Armed Services investigated the allegations and released a report in September 2010 revealing that ArmorGroup had hired Afghan warlords to staff these contracts, including the provision of armed security guards to protect the UN-contracted demining operations. There were rival warlords involved, one killed the other, the dead warlord was replaced by his brother, and the arrangement continued. Despite the allegations and the US

Senate Committee report, and even though, as Pingeot states, "[t]hese events occurred while ArmorGroup was under a UN contract, ... there is no indication that the UN has conducted a thorough review of this case, that it has established strict rules on contractors' subcontracting and staffing practices, or that it has decided to suspend the company from its vendors' list following this incident. As of mid-2011 ArmorGroup was 'not on any [UN] blacklist'" (Pingeot 2012, p30).

UN reliance on PMSCs has implications for the institution's approach to fulfilling its mission

In light of the information uncovered, the *Dangerous Partnership* report questions the effectiveness of the UN's use of PMSCs for peace and security efforts. Specifically, Pingeot asks: **"Can [PMSCs] work for the UN to promote democracy, legality and human respect when they so evidently foster secrecy, impunity and a contemptuous warrior ethos?"** (Pingeot 2012, p8) The report highlights the alarming reality of the UN's use of disreputable companies: **"In the absence of guidelines and clear responsibility for security outsourcing, the UN has hired companies well-known for their misconduct, violence and financial irregularities – and hired them repeatedly.** These include DynCorp International, infamous for its role in a prostitution scandal involving the UN in Bosnia in the 1990s and, more recently, its participation in the US government's 'rendition' program; G4S, the industry leader known for its violent methods against detainees and deported asylum seekers; ArmorGroup, a G4S subsidiary singled out in a US Senate report for its ties to Afghan warlords; and Saracen Uganda, an offshoot of notorious mercenary firm Executive Outcomes with links to illegal natural resources exploitation in the Democratic Republic of Congo" (Pingeot 2012, p7).

More broadly, the report questions how the involvement of PMSCs shifts the framing of the UN's approach to peace and security. On this point, the report argues that PMSCs have helped to create a market for themselves by promoting stronger security measures within the UN, and that this has coincided with the establishment of increasingly 'robust' peacekeeping missions, 'integrated missions', and a

hardened security approach that privileges bunkerization. The report concludes that "[b]y using these companies to provide risk assessment, security training and guarding in critical conflict zones, the UN is effectively allowing PMSCs to define its security strategy and even its broader posture and reputation" (Pingeot 2012, p8).

Although the questions raised in *Dangerous Partnership* merit political considerations by the UN, the 2014 follow-up report documents the institution's growing reliance on PMSCs that is accompanied by bureaucratic measures to improve tracking of contracts . *Contracting Insecurity: Private military and security companies and the future of the United Nations* (Pingeot 2014) provides an update on the debate and argues that the problems created by the privatization of security cannot be solved by voluntary mechanisms and other 'soft' regulatory approaches. At the heart of the issue is the UN's ability to promote its peacekeeping mandate with the involvement of contractors that promote militarization and securitization.

G4S is among the companies contracted by the UN

One of the "disreputable" UN contractors is London-based Group 4 Securicor (commonly known as G4S), the world's third-largest private-sector employer whose *Securing Your World* motto is pursued by over 618,000 staff in over 120 countries. According to its website, the company specializes in "outsourced business processes and facilities in sectors where security and safety risks are considered a strategic threat." Their "provision of security products, services and solutions" includes – among several areas of work – government contracts for border security, "[f]rom ensuring travellers have a safe and pleasant experience in ports and airports around the world to secure detention and escorting of people who are not lawfully entitled to remain in a country."

G4S was created through the merging of British company Securicor and Danish Group 4 Falck, and has built up its operations through acquiring and merging with other companies around the world. For example, G4S acquired Global Solutions Limited (GSL) in 2008, a company that at the time had 9,000 staff in the UK, Australia, and South

Africa. Among other services, GSL held contracts with the Australian government for the transport of prisoners in the country. G4S also owns several military and security companies that often function under their original names, such as Wackenhut, the second largest security services company in the United States, which was acquired by Group 4 Falck in 2002. In 2008, G4S acquired RONCO Consulting, which specializes in landmine clearance and ArmorGroup, "a leading provider of defensive and protective services to national governments and international peace and security agencies." ArmorGroup was created in 1997 when US-based Armor Holdings acquired UK-based Defence System Limited (DSL).

The G4S family also includes local branches with a national presence that allows the company to compete for national gosvernment contracts. For example, the company recently announced on the G4S Kenya website that "G4S Kenya will be cementing its position as the leading provider of security solutions with a contract award from the Ministry of energy, to secure the Lake Turkana Wind Power Project; this will be the single largest wind power project to be constructed in Africa, and the largest private sector investment in the history of Kenya."

G4S: A disreputable company

G4S has been criticized for its mismanagement of government contracts linked to several incidents of abuse, violence, and deaths of people in the custody of G4S employees. In the 2012 *Dangerous Partnership* report, Pingeot states that "[o]ne of G4S' troubling business areas is the detention and management of illegal immigrants in Europe, the US, and Australia. In the UK, G4S was contracted by the government to deport refused asylum seekers back to their country of origin. The company's practices came under scrutiny following the death of an Angolan national during such a removal. A report by Amnesty International UK examining cases of abuse by G4S found widespread use of excessive force by the company during enforced removals. A G4S whistleblower described the company's practice as 'playing Russian roulette with detainees' lives.' G4S was finally removed from the contract. Its practices have also come under legal review in Australia, where the company provides prisoner

transport services" (Pingeot 2012, p30). The latter refers to the death of Mr. Ward, an aboriginal elder, when he was being transported by GSL officers in a custodial vehicle in Western Australia.

The 2014 *Contracting Insecurity* report updates and summarizes some of the incidents that has put G4S in the disreputable category, and which should raise alarm among UN officials who are hiring the company:

> "In the summer of 2012, G4S received unwanted attention when it proved incapable of fulfilling the terms of its contract to secure the Olympics in London. Originally tasked with providing more than 10,000 personnel for the Olympics, the firm admitted that it could provide fewer than 6,000, with less than a month remaining before the Games. The British Government had to mobilize military personnel to fill the gap.
>
> "G4S had previously been in the spotlight following the death of Angolan deportee Jimmy Mubenga, who suffocated while being restrained by three G4S guards on a flight from Heathrow to Angola. An inquest into Mubenga's death condemned the systematic use of excessive force during removals and found evidence of 'pervasive racism' among G4S personnel tasked with removing detainees.
>
> "G4S contracts to run prisons in several countries have also come under scrutiny in recent months. In early 2013, a South African government report found that G4S was illegally holding inmates in isolation for up to three years and failing to provide them with life-saving medication, charges that the company denied. In October, after a string of violent riots and stabbings and strikes by prison officers at a maximum security prison run by G4S, South African authorities announced they would take over the management of the facility [Mangaung Correctional Centre]. The government declared that 'the contractor [had] lost effective control of the facility.' G4S has also come under scrutiny for its management of prison facilities in the UK [including Oakwood prison], where the Inspectorate of Prisons found that the company was failing to provide

> basic health care and sanitation to prisoners. In 2012, a British high court judge found that the unlawful use of force and restraint techniques against children had been widespread in child prisons and 'secure training centers' operated by G4S and Serco between 1998 and 2008. G4S also manages security systems at the controversial Ofer Prison in the Occupied Palestinian Territories" (Pingeot 2014, p7).

In addition to the examples cited in Pingeot's reports, other G4S-related scandals include a riot involving local residents attacking asylum seekers being held in Papua New Guinea (PNG) in February 2014, which resulted in the death one asylum seeker and several people seriously injured (*The Guardian,* 24 February 2014). In 2013, the Australian government enacted a policy of sending refugees who were attempting to enter the country by boat to an immigration detention facility on PNG's Manus Island for processing prior to resettlement in PNG. The detention center in PNG has been the site of many incidents – including inhumane treatment of refugees and clashes among the security forces, prompting a report by Amnesty International in December 2013 and the creation of a special coverage page on *The Guardian* that as of June 2014 had 184 news items. Expressions of concern about the conditions in the Australian-run detention centers in PNG were made by the UN High Commissioner for Refugees (UNHCR) in November 2013, and reports of the volatile situation that could lead to violence began appearing in late November 2013.

After the February 2014 riot, a G4S guard who worked at the detention center testified that his colleagues allowed local residents on Manus Island to enter the compound and that he witnessed them violently attack the asylum seekers, aided by local guards. "The police fired warning shots and that scared the clients [asylum seekers] and they went into their rooms, so that's when the G4S went in. And when the G4S get into the camp, they belt, they fight with the clients [asylum seekers] and belt them very badly and some are wounded, blood run over their face," the witness told Australia's ABC News program (ABC News Australia, 24 February 2014). The UNHCR conducted an investigation of the incident and criticized Australia's regional processing policy for asylum seekers, affirming that Australia is

legally responsible for ensuring the safety of asylum seekers at Manus Island (*The Sydney Morning Herald,* 8 May 2014).

The UNHCR investigated another incident involving G4S, this time in relation to the beating of handcuffed Iraqi asylum seekers by G4S security officers under contract with the UK Border Agency during a charter flight back to Baghdad. In June 2010, *The Guardian* reported that as many as 25 men who were deported from the UK to Iraq were held in detention at Baghdad airport after Iraqi officials were alleged to have boarded the airplane to "...help security staff employed by the UK Border Agency (UKBA) punch and drag reluctant failed asylum seekers off the plane." (*The Guardian,* 18 June 2010) A UNHCR spokesperson was quoted in the news article confirming that UNHCR lawyers had interviewed deportees: "The men claim they were beaten while being forced on to the plane. We met six of the men and saw fresh bruises that indicate mistreatment."

UN contracts with G4S

Despite the high-profile scandals and scrutiny, the UN continues to do business with G4S and its affiliated companies, including ArmorGroup, RONCO, and Wackenhut. Armed security of UN compounds, security of refugee camps, security for transport convoys and transport logistics, risk assessments and security training for UN agency staff, landmine clearing and coordination of WPF-provided emergency benefits for farmers during crop failures are some examples of G4S services.

For G4S, the contracts with the UN and other humanitarian organizations are good for public relations and for supporting their corporate social responsibility claims. The G4S-Kenya website states that the company "secures and supports the operation of key NGOs in Kenya including the UN, UNHCR, Unicef, among others. ... G4S Kenya also works with other likeminded NGOs like Red Cross society to promote disaster management preparedness and responds to emergency situations as they arise." From the G4S-Madagascar website, we also learn that the company provided security training to 100 people involved with the UN in 2010 and 11 UNICEF staff in 2011.

The *Dangerous Partnership* report states that UNOPS paid G4S subsidiary ArmorGroup USD 15 million in 2008 for its services, including mine clearance activities in Afghanistan. In 2010, UNOPS paid G4S Risk Management more than USD 14 million for 'mine action' and related activities. The Haiti peacekeeping mission (MINUSTAH) contracted G4s to provide armed security guards at its Santo Domingo office, and received services from DSL (and later ArmorGroup) for transporting personnel, troops and humanitarian supplies into and within the county.

As reported by Pingeot, **in 2012 alone, G4S had more than sixty contracts with the UN for guards, 'security services', 'office security', security systems, consulting, mine action, cleaning, and other services.** This includes contracts with the International Atomic Energy Agency (IAEA) in Austria and Pakistan, the UN Development Program (UNDP) in Chile, India, Iraq and Somalia, and UNHCR in Kenya and the Democratic Republic of Congo (DRC).

Additional 2012 contracts indentified through the WFP include the hiring of G4S to coordinate the disbursement of cash assistance to farmers in Lesotho as part of an emergency assistance in response to crop failure in the country. During that same year, the WFP also hired G4S guards to provide security in a refugee camp in Lebanon, to protect Save the Children staff as they distributed food aid to Syrian refugees at the camp. The WFP has also hired G4S-owned RONCO on multiple occasions to clear landmines in the South Sudan.

G4S responds to Pingeot's reports

G4S is pro-active in responding to allegations that it has been involved in human rights violations and other misconduct. The company regularly issues statements to distance itself from incidents that cast it in a negative light, opening with statements such as: "G4S is the world's leading provider of secure outsourcing solutions. We are committed to fulfilling our responsibilities on the issue of human rights in all of our companies operating around the world." The letters continue with a short

description of G4S' corporate social responsibility (CSR) initiatives, such as the company's leadership in the development of an International Code of Conduct for Private Security Providers, and then they proceed to give nominal responses to the specific allegations of misconduct to which the company is responding, without addressing the main issue – its role in perpetuating violence and violating human rights. The company's responses to Pingeot's reports can be found in the Business and Human Rights Resource Center website.

The company's response to the 2012 *Dangerous Partnership* report limited itself to addressing the death of Jimmy Mubenga at the hands of G4S employees during his deportation from the UK to Angola in October 2010, the January 2008 death of Mr. Ward in Western Australia whilst being transported by escorting officers of GSL Custodial Service (subsequently acquired by G4S) from Laverton to Kalgoorlie, and the 2010 allegations that ArmorGroup had hired Afghan warlords. Regarding Mr. Mubenga, G4S states that the death was tragic and that the custody officers involved transferred to the new service provider (since G4S no longer provides escort services for the UK). Regarding Mr. Ward, G4S states that this incident took place prior to G4S acquiring GSL and that the company had ceased operating the contract with the State of Western Australia in June 2011. Furthermore, G4S has "publicly apologized to Mr. Ward's family and community for Mr. Ward's tragic death on several occasions." G4S also addresses "the unfounded assertion of the US Senate Armed Services Committee that ArmorGroup, now G4S Risk Management, turned to Afghan 'warlords' to serve as manpower providers during the duration of the UN contract. This was simply not true." According to the US Senate Committee, its inquiry "uncovered evidence of private security contractors funneling U.S. taxpayers dollars to Afghan warlords and strongmen linked to murder, kidnapping, bribery as well as Taliban and other anti-Coalition activities" (Senate Committee on Armed Services, p.i) In a section titled "U.S. and UN Funded Contracts Benefit Afghan Warlords," the Committee documented how ArmorGroup hired two known warlords to provide manpower to guard the US Air Force airbase construction project, one of whom was later transferred to service the UN contract. Although the Senate

Committee gathered testimony about the links between the guards hired by ArmorGroup and the Taliban, as well as information that the company was aware of the warlords' actions, G4S claims in its letter of response that the Senate Committee's findings are "not supported by evidence and did not exist."

The five-page response by G4S to the *Contracting Insecurity* report reads much like the 2012 response. After citing its CSR record, G4S takes on "specific issues mentioned in the February 2014 report by Lou Pingeot:" the "regrettable" failure to provide a complete, contracted security workforce for the London Games (which had led the UK government to bring in the military to provide security for the 2012 Olympics); the "tragic" death of Jimmy Mubenga, noting that the Crown Prosecution Service found no basis on which to bring criminal charges against G4S in this case; the situation at Mangaung Correctional Centre (MCC) in South Africa, noting that during the time it has been operated by G4S, "the MCC has come to be regarded as a benchmark in correctional services in South Africa, receiving numerous national and international awards"; the poor management of the Oakwood prison in the UK, at which the company has "taken steps to make improvements"; the use of restraint against young people at UK Secure Training Centers, stating that "[t]he issue referred to in [Pingeot's] report was a result of a conflict in the interpretation of the authority's rules and primary legislation"; and the company's operations in Israel and the West Bank, which the company concluded that it did not violate any national or international law.

The attitude of G4S that "stuff happens" as part of their "care and justice" work, which covers police and prison contracts, is exemplified in a *Financial Times* article titled "G4S: the inside story." In response to a question by an analyst at a investor meeting, "chief executive [Ashley Almanza] added: 'we do difficult things sometimes in difficult places... It's the nature of the business that we can... hit the ball out of the park for 364 days of the year and on the last day of the year something goes wrong.' His response hints at an uncomfortable truth. When uniformed staff – however tightly supervised – are placating violent prisoners, tackling pirates or even

fingerprinting drunks, the situation will occasionally get out of hand. Sometimes people will be hurt or could even die" (*Financial Times*, 14 November 2013).

The UN's response

The 2014 *Contracting Insecurity* report provides an update on the relationships between PMSCs and the UN and examines the institution's response to the 2012 report. The update indicates that the trend towards outsourcing security continues and that the UN's responses have been limited to addressing the concerns about tracking and oversight of contracts with PMSCs. "The UN's use of private military and security companies (PMSCs) is not a technical issue – it is a deeply political one. Since the publication of 'Dangerous Partnership'... , the UN has taken steps to improve the selection and oversight of these companies and to make its practices more transparent. While positive, these efforts have tended to focus on technical issues, such as the selection process and the definition of which services PMSCs can perform. There has been little reflection on the reasons behind the need for more security, the influence of PMSCs on UN security policies, or their potential impact on the perception of the organization by local populations" (Pingeot 2014, p5).

In late 2012, the UN Department of Safety and Security finalized a set of guidelines on the use of armed private security companies. The guidelines seek to standardize the use of PMSCs across UN agencies and provide an initial step towards transparency and accountability in the contracting of PMSCs. Pingeot states that these guidelines are severely limited as they rely primarily on companies self-reporting and there is insufficient monitoring and oversight of PMSCs with regards to training and screening of employees as well as to the companies' institutional practices and approach. "The guidelines also raise concerns that some controversial services – such as the use of armed private security for convoy protection – may become normalized" (Pingeot 2014, p10).

Another step taken by the UN was a first-ever report by the Secretary General on the use of armed private security

presented to the General Assembly in October 2012. The report explains the conditions under which PMSCs are contracted – primarily as a 'last resort' when internal options in the UN and among member states are exhausted – and describes the institution's new guidelines on armed private security. Pingeot points out that Secretary General's report "was slim on facts and numbers. It did not name any of the companies used by the UN and did not address the rise in private security contracts" (Pingeot 2014, p9).

A later report of the Advisory Committee on Administrative and Budgetary Questions (ACABQ) provided further details on contracting with PMSCs. The ACABQ report was incomplete and at times contradictory, thereby exposing the lack of oversight within the UN regarding contracts. As exemplified by Pingeot, the ACABQ report states that it has "only one contract with a large multinational armed private security company" – IDG Security in Afghanistan, and later lists contracts with other companies, including the multinational G4S and its local branches in Cameroon, Haiti, and Kosovo (Pingeot 2014, p9). The ACABQ only reported on political and peacekeeping missions and excluded contracts with other UN agencies, which hold important contracts with PMSCs. In addition to the inconsistencies and inaccuracies of the ACABQ report, the fact that this issue was taken up by an budgetary oversight body indicates the technical nature of the UN's approach, rather than the political response required by Pingeot's findings.

The UN reports led to the issues regarding UN contracting with PMSCs to be raised in the UN General Assembly committee that oversees administrative and budgetary matters. The debate in the committee in turn resulted in a set of recommendations from the committee to the General Assembly in early 2013. Pingeot summarizes that the "resolution is by far the clearest mandate that the UN has received from member states on the issue of PMSCs. It underlined the potential risks involved in the use of armed private security and demanded more transparency and accountability from the Secretariat" (Pingeot 2014, p10).

Overall, the UN response to the concerns raised regarding contracting with PMSCs is judged by Pingeot as insufficient in the political realm of the UN's ability to fulfill its mission and the role of PMSCs shaping the UN's approach to peacekeeping and security. "The use of PMSCs has important ramifications for the activities, mandate, and legitimacy of the UN. Ultimately, the question behind the UN's use of PMSCs is what the organization is today and what it might become" (Pingeot 2014, p5).

Unsettling conclusions

The lack of accurate information from the UN about the extent of its contracts with PMSCs is a significant obstacle for understanding the full scope of the situation. If the UN does not systematically track its contracts with PMSCs, how can they ensure that violations are not taking place in the institution's name?

Despite the incomplete picture, it is clear that the UN's reliance on PMSCs is compromising the institution's ability to fulfill its mission and that it is further entrenching the securitization of peacekeeping and humanitarian efforts. Additionally, three questions are surfaced:

- How can UN agencies that are tasked with guaranteeing human rights and investigating perpetrators of human rights violations simultaneously hire those perpetrators?
- Where does corporate social responsibility fit into this debate?
- As more public services and functions become privatized, this is resulting the privatization of human rights violations. How can we hold PMSCs accountable for their role in human rights violations?

How can UN agencies that are tasked with guaranteeing human rights and investigating perpetrators of human rights violations simultaneously hire those perpetrators?

G4S has been involved in high-profile incidents of ill-treatment of refugees, both during deportations and transfers and during the guarding of detention or

processing centers. The UNHCR is an important contracting body of PMSCs within the UN system, hiring G4S to guard refugee camps in several countries, among other services. At the same time, the UNHCR has been responsible for investigating incidents of human rights violations against refugees in Iraq and PNG, where G4S has been implicated. Despite its awareness of these situations, the UNHCR continues to hire G4S to provide security in refugee camps. At best, this is a sign of lack of coordination and communication within the agency that can lead to serious consequences. At worst, the UNHCR does not find it important that G4S has been involved these and other incidents, and is therefore complicit in the misconduct.

Where does corporate social responsibility fit into this debate?

G4S is an active promoter of corporate social responsibility (CSR) and proudly states that it is an active member of the Global Compact since February 2011. The Global Compact was launched by the United Nations in 2000 as a tool to promote 'responsible corporate citizenship'. It is open for any corporation to join as long as the sign on to its principles of human rights, labor, environment, and anti-corruption, and as long as they report annually on their CSR efforts. This voluntary mechanism lacks an enforceable legal framework – meaning that corporations cannot be held liable for human rights violations or other practices that go against the principles. While Global Compact members may be sanctioned if they fail to report, no company has ever been expelled for their practices that violate human rights (Friends of the Earth International 2012).

The Global Compact rewards members with privileged access to the UN and its agencies and at the same time it provides cover for the UN regarding its use of disreputable companies, since Global Compact members – such as G4S – should be legitimate partners for the UN. UN contracts are not the most profitable but they go a long way in building a positive profile of the companies, thereby feeding into the CSR smokescreen of PMSCs.

Using a similar model as the Global Compact, the UN's response to concerns about PMSCs was to focus on data management of its contracts and set up systems of monitoring of PMSCs based on self-reporting by the companies. As long as the technicalities of reporting are met, the companies get the stamp of approval. This approach ignores the institutional problems with relying on PMSCs as well as the fundamental issues regarding the PMSCs' influence over the UN's approach to peacekeeping and humanitarian missions.

As more public services and functions become privatized, this is resulting the privatization of human rights violations. How can we hold PMSCs accountable for their role in human rights violations?

As policing, security, and other public functions are increasingly privatized, it is to be expected that the human rights violations that were committed by state agents will now be committed by private contractors on behalf of the state. The profit-motive for PMSCs leads to poor working conditions among their employees – as evidenced by multiple reports of strikes of G4S guards at prisons and refugee camps, which in turn creates additional situations of stress and violence (see, for example, Corpwatch G4S corporate profile). Regarding mismanagement and incidents of abuse, the G4S CEO was quoted earlier as saying, "it is the nature of the business." When public entities are involved in human rights violations, they can be held accountable through the use of laws and multilateral treaties including the Universal Declaration on Human Rights. When private multinational entities are the perpetrators, how are they held accountable? The international legal frameworks need to be updated in order to respond to the trend of global privatization and hold multinational corporations accountable for rights-violations in all contexts (see, for example, Friends of the Earth International 2014).

Pingeot's reports raise critical questions about the direction that the UN is taking regarding peace and security, and the influence of PMSCs. Many NGOs in the humanitarian sector also contract with PMSCs for security of their offices and of their field operations at refugee

camps and elsewhere. Providing security services to humanitarian operations has become a niche market for PMSCs; G4S-owned ArmorGroup has counted several NGOs among their clients, including International Rescue Committee, CARE and Caritas. (International Alert, p16) This turn towards securitization has led to the normalization of violence and conflict, creating a context in which the UN and other organizations are cornered into making choices that effectively counter their efforts at humanitarian relief and peace.

Observant 65, 30 juni 2014
Buro Jansen & Janssen 2014

References

Pingeot, Lou, Dangerous Partnership: Private Military & Security Companies and the UN, Global Policy Forum and Rosa Luxemburg Stiftung – New York Office (2012). http://www.globalpolicy.org/images/pdfs/GPF_Dangerous_Partnership_Full_report.pdf

Pingeot, Lou, Contracting Insecurity, Global Policy Forum and Rosa Luxemburg Stiftung – New York Office (2014). http://www.globalpolicy.org/images/pdfs/GPFEurope/PMSC_2014_Contracting_Insecurity_web.pdf

Koenraad Van Brabant, Tony Vaux, Chris Seiple, Gregg Nakano, Humanitarian action and private security companies: Opening the debate, International Alert (2001) https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCIQFjAA&url=http%3A%2F%2Fpatronusanalytical.com%2Fpage11%2Fpage12%2Fassets%2FHUMANACT.pdf&ei=tF6hU9WrCaTpywP06YKYAQ&usg=AFQjCNG-juF-BzaZ6kLxWbdQk0bnCFLKKw&sig2=darhFtXVzrep04EI_adSkA&bvm=bv.69137298,d.bGQ

G4S website: http://www.g4s.com
G4S Kenya website: http://www.g4s.co.ke/en-KE/
G4S Madagascar website: http://www.g4s.mg/en-MG/

Sourcewatch profile of ArmorGroup International PLC: http://www.sourcewatch.org/index.php/ArmorGroup_International_PLC

Farrell, Paul, Manus guards let residents into centre as extra manpower, says G4S witness, The Guardian, 24 February 2014. http://www.theguardian.com/world/2014/feb/25/manus-guards-let-residents-into-centre-as-extra-manpower-says-g4s-witness

Amnesty International, The truth about Manus Island, 11 December 2013 http://www.amnesty.org.au/refugees/comments/33587/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+AIACampaigns+Amnesty+International+Australia+Campaigns

The Guardian special coverage page on Manus Island: http://www.theguardian.com/world/manus-island

ABC News Australia website: http://www.abc.net.au/7.30/content/2013/s3951437.htm

Whyte, Sarah, UNHCR slams Australia over violence at Manus Island asylum seeker camp, The Sydney Morning Herald, 24 May 2014 http://www.smh.com.au/federal-politics/political-news/unhcr-slams-australia-over-violence-at-manus-island-asylum-seeker-camp-20140508-zr6wb.html

Bowcott, Owen and Jones, Sam, Iraqi asylum seekers claim they were beaten on flight to Baghdad, The Guardian, 18 June 2010. http://www.theguardian.com/uk/2010/jun/18/iraq-asylum-seekers-beaten-deported

Business & Human Rights Resource Center website, G4S responses to the two Pingeot reports: http://www.business-humanrights.org/Search/SearchResults?SearchableText=G4S+response+Pingeot&x=0&y=0

Senate Committee on Armed Services , "Inquiry into the Role and Oversight of Private Security Contractors in Afghanistan," US, Septem¬ber 28, 2010

http://info.publicintelligence.net/SASC-PSC-Report.pdf

Hill, Andrew and Plimmer, Gill, G4s: The inside story, The Financial Times, 14 November 2013. http://www.ft.com/intl/cms/s/2/a6b46fc0-4cc0-11e3-958f-00144feabdc0.html#axzz34z0qO1AB

Reclaim the UN from corporate capture, Friends of the Earth International, 2012. http://www.foei.org/resources/publications/publications-by-subject/economic-justice-resisting-neoliberalism-publications/reclaim-the-un-from-corporate-capture/

Corpwatch profile on G4S: http://www.corporatewatch.org/company-profiles/g4s-staff

Groups call for UN treaty to tackle corporate human rights violations, Friends of the Earth International, 7 May 2014. http://www.foei.org/news/groups-call-for-un-treaty-to-tackle-corporate-human-rights-violations/

Overheidstaken G4S in strijd met duurzaamheidsbeleid

Beveiligingsbedrijf G4S raakt internationaal geregeld in opspraak, onder meer vanwege wangedrag van haar personeel. Verbindt de Nederlandse overheid, dat G4S heeft omarmd, hier geen consequenties aan? Buro J&J dook in de samenwerkingscontracten, met onthutsend resultaat.

In *Duurzaam afwimpelen* (28 maart 2012) analyseerde Buro Jansen & Janssen het duurzaamheidsbeleid van de Nederlandse overheid. Bij dit beleid gaat het vooral over ketenpartners, eigen verantwoordelijkheid van de bedrijven en het 'maatschappelijk middenveld als kwaliteitsbewaker'.

Aan de hand van schoonmakers en de elektronica-industrie werd beschreven dat de controle op milieu-, sociale- en andere aspecten van een product of dienst erg de wensen overlaat. Bezuinigingen op het maatschappelijk middenveld, gebrekkige controle en ondoorzichtige uitbesteding van opdrachten maken een duurzaamheidslabel zinloos. In het artikel over Chiquita van 23 juli 2013 wordt dit nog eens onderschreven.

Bijkomend probleem van het duurzaamheidsvraagstuk is dat de overheid als consument slechts moeizaam openheid geeft over de producten en diensten die zij afneemt. In het kader van het onderzoek naar beveiligingsreus G4S stelt Buro jansen & Janssen de vraag in hoeverre de overheid bij het uitbesteden van beveiligingstaken haar eigen duurzaamheidsnormen hanteert.

Informatieverzoeken

In de lente van 2011 vroegen wij daartoe bij de toen nog bestaande politieregio's om alle correspondentie, contacten en contracten met G4S Plc (Group 4 Securicor, Group 4 Falck) en enkele andere bedrijven beschikbaar te stellen. Dit informatieverzoek was een vervolg op het verzoek van juli 2010 over de contacten met bedrijven op het gebied van ICT, communicatie, dataverzameling en beheer, toegangscontrole, zichtsystemen, alarm, wapensystemen, beschermende oplossingen voor personeel, voertuigen en gebouwen, voertuigen, training en detachering.

De resultaten van dit verzoek druppelden in 2011 en begin 2012 binnen. Op dit moment is een vervolgverzoek ingediend over de contacten van de overheid met G4S. Het beveiligingsbedrijf kwam begin dit jaar in het nieuws door stakingen van werknemers. Ruim honderd beveiligers legden het

werk neer omdat zij een beter sociaal plan eisten voor de G4S werknemers die gedurende het lopende jaar zullen worden ontslagen.

G4S verliest tevens haar beveiligingspositie bij detentiecentra door bezuinigingen op het gevangeniswezen. In dezelfde periode overleed een vluchteling en raakten diverse anderen gewond in een opvangkamp gerund door G4S op Papua New Guinea (PNG). In totaal verschenen er vier korte nieuwsartikelen over het schandaal in de Nederlandse media.

Het contrast kan niet groter zijn en het roept de vraag op in hoeverre het gedrag van het bedrijf elders van invloed is op het aantal opdrachten dat het krijgt. Vindt er een afweging plaats over het gedrag van het bedrijf in Nederland en de rest van de wereld? Bestaat er zoiets als een VOG (Verklaring Omtrent het Gedrag) voor bedrijven?

In 2011 riep werkgeverscertificeerder CRF Institute G4S uit als *Top Employer* van Nederland, terwijl in dat jaar *The Guardian* onder de titel *Staff on deportation flights played 'Russian roulette' with lives* klokkenluiders aan het woord kwamen omtrent het gedrag van G4S-werknemers rond uitzettingen van vluchtelingen in het Verenigd Koninkrijk. In 2012 deelde hetzelfde CRF institute G4S in bij de Top Employers terwijl het bedrijf voor een totale chaos rond de beveiliging van de Olympische Spelen in Londen zorgde. Het leger moest worden in gezet omdat G4S haar afspraken niet nakwam.

Vraag is echter of deze praktijken van het beveiligingsbedrijf in het buitenland de Nederlandse vestiging zijn aan te rekenen. Een VOG voor individuen is duidelijk. Bepaalde misstappen zullen je carrière in de toekomst ernstig belemmeren. Hoe zit dat met G4S? Draait het bij de overheid enkel om het functioneren van G4S in Nederland en raakt het bedrijf haar contracten niet kwijt zodra haar werknemers zich in het buitenland misdragen? Hoe vult de Nederlandse overheid haar eigen sociale verantwoordelijkheid in?

Politie in de zak

In 2011 meldt politieregio Fryslân (nu eenheid Noord Nederland) dat zij met G4S 'een objectbeveiligingsovereenkomst, d.d. 12 juli 2007' heeft. Ook politieregio Drenthe (nu tevens eenheid Noord Nederland) 'beschikt ook over een contract met G4S betreffende beveiliging van het Politie Opleidings- en Trainingscentrum

(POTC), te Zuidlaren.'

Naast deze objectbeveiliging, bij Drenthe een contract dat 'telkenmale stilzwijgend wordt verlengd', heeft het bedrijf voor beide korpsen toegang tot een mini-competitie voor een openbare 'Europese Aanbesteding Beveiligingsdiensten (publicatienummer 2010/S 73-108997)'. Deze aanbesteding is nationaal georganiseerd en naast G4S doen ook Securitas Beveiliging BV en Trigion Beveiliging BV mee. Bij andere regio's vond eenzelfde competitie plaats. Ook politie Limburg-Zuid had een overeenkomst objectbeveiliging met G4S dat op 31 december 2010 afliep.

Hoewel het om oude contracten gaat die de politie met G4S had afgesloten, vallen er een aantal zaken op. De overeenkomsten zijn op briefpapier van G4S opgesteld en de algemene voorwaarden zijn van toepassing op de overeenkomst. Het lijkt wel of het de omgekeerde wereld is. G4S dicteert wat de politie moet doen.

Bij de aanbesteding van de beveiligingsdiensten lijkt de politie iets meer de macht over het contract naar zich toegetrokken te hebben. Bij de oude contracten, grofweg periode 2006 tot en met 2010/2011, bepaalt G4S de mate van controle. 'Op (onregelmatige) tijden zal de surveillant uw pand op de stille tijden (avond, nacht en weekeinde) controleren op eventuele gevaren of verstoringen van uw bedrijfsproces', bij controlerondes uit overeenkomst alarmcentrale juli 2007.

Het minimale aantal controles wordt niet vermeld, evenmin de aanrijtijd van het bedrijf. Ook als het bedrijf op bepaalde momenten geen controle uitoefent is zij niet aansprakelijk. 'Voor schade van Opdrachtgever die het gevolg is van een dergelijke verhindering (vertraagd, onderbroken of overgeslagen controle) is Group 4 Securicor niet aansprakelijk', wordt vermeld in de algemene voorwaarden.

Het bedrijf is echter ook niet aansprakelijk voor het disfunctioneren van haar medewerkers. Overeenkomst Objectbeveiliging, 19 december 2006: 'Indien een beveiliger niet blijkt te voldoen aan de overeengekomen eisen en binnen redelijke termijn ook niet aan die eisen zal kunnen voldoen, dan wel zijn werkzaamheden structureel niet naar behoren verricht, zal Group 4 Securicor op schriftelijk verzoek van Opdrachtgever en na overleg met Opdrachtgever de betreffende beveiliger vervangen.' De politie moet dus zelf aangeven dat de werknemer van G4S niet voldoet.

De algemene voorwaarden van G4S uit 2006 schetsen verder een beeld van een bedrijf dat probeert onder allerlei kosten uit te komen. 'Onder overmacht wordt in deze Algemene Voorwaarden verstaan alle omstandigheden die niet aan Group 4 Securicor kunnen worden toegerekend, […] Hieronder worden in ieder geval begrepen daden van terrorisme, werkstakingen binnen de onderneming van Group 4 Securicor, stakingen elders, voor zover Group 4 Securicor daardoor in haar dienstverlening wordt beperkt, het niet voldoen door leveranciers van Group 4 Securicor aan hun verplichtingen, alsmede extreme weers- en verkeersomstandigheden.'

In 2008 vermeldt de Algemene Rijksvoorwaarden voor het verstrekken van Opdrachten tot het verrichten van Diensten 2008 (ARVODI-2008) van het ministerie van Algemene Zaken dat stakingen en slechte leveranciers niet tot overmacht gerekend kunnen worden. Ook neemt het bedrijf geen verantwoordelijkheid voor de gedragingen van het personeel dat zij uitleent (2.12.2 Werkzaamheden onder toezicht en leiding van Opdrachtgever).

De politie op de huid

G4S heeft in de samenwerkingscontracten met politie en justitie de afgelopen jaren moeten inbinden op het terrein van overmacht. Het verloop van de staking van het G4S-personeel begin 2014 laat zien dat de beveiligingsfirma er alles aan gelegen is een staking slechts van korte duur te laten zijn. Het bedrijf probeerde na twee dagen de staking te breken. Nadat dit op woensdag 12 februari 2014 mislukte, zetten de stakers de hakken in het zand waardoor de werkonderbreking bijna twee weken duurde.

Op andere terreinen heeft het bedrijf echter de afgelopen jaren zich meer en meer in het politieapparaat gewerkt. Op 13 september 2012 tekende G4S met politie Amsterdam-Amstelland een convenant waarin onder meer intensieve communicatie en structurele informatie-uitwisseling is vastgelegd. Dit is geen eenrichtingsverkeer naar de politie, maar een duidelijke wederkerigheid.

Op de website politie.nl zegt de directeur van G4S: "We werken al veel langer samen door informatie uit te wisselen over bijvoorbeeld verdachte personen, kentekens van voertuigen of andere vormen van informatie. Met deze ondertekening formaliseren we onze samenwerking en weten we wat we van elkaar kunnen verwachten. We moeten niet alleen afhankelijk zijn van de informele contacten die er zijn."

Het beveiligingsbedrijf bouwt zo langzaam maar zeker haar eigen database op. In de algemene voorwaarden van de overeenkomsten van G4S met de korpsen Friesland, Drenthe en Limburg-Zuid wordt onder het subkopje 'gegevensverwerking en geheimhouding' vermeld dat 'Group 4 Securicor het recht heeft om alle gegevens afkomstig van Opdrachtgever, alsmede alle signalen van de Installatie te registreren en op te slaan in een (digitale) databank.' Het is onduidelijk of die gegevens worden vernietigd na afloop van het contract, maar wie bedenkt dat het bedrijf ook een landelijk meldkamer bezit, beseft dat het graag allerlei politietaken wil overnemen.

In de offerte alarmcentrale voor politie Hollands-Midden schrijft het bedrijf: 'De G4S Alarmcentrale is een van de meest geavanceerde alarmcentrales in Nederland. […] Op de G4S Alarmcentrale zijn meer dan 60.000 beveiligingssystemen van bedrijven en particulieren aangesloten die dagelijks duizenden meldingen genereren.'

Hoe zijn hierbij de basale burgerrechten geregeld zoals vastgelegd in nationale en internationale verdragen? In de overeenkomsten met de politie, maar ook in de eigen voorwaarden, is niets terug te vinden over privacyreglementen, klachtenprocedures, omgangsvormen, verantwoordelijkheden ten aanzien van slachtoffers van het bedrijf, inspectie, controle, toezicht en andere fundamentele rechtsstatelijke maatregelen. Misschien zijn deze wel vastgelegd in wet en regelgeving, maar je zou verwachten dat bij het uitbesteden van vitale taken van de rechtsstaat deze expliciet worden genoemd.

G4S leidt de politie

Aan de andere kant staat de politie ook niet bekend om haar eigen controle-, toezicht-, inspectie- en klachtenprocedures, maar uiteindelijk is de staat aansprakelijk. Bij de publiek-private samenwerking is onduidelijk wie aansprakelijk is. In de overeenkomsten die niet volgens de Rijksvoorwaarden werden afgesloten, probeerde G4S onder elke aansprakelijkheid uit te komen.

In de ARVODI-2008 (Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten) is geformuleerd dat de opdrachtgever, tenzij bewezen, niet aansprakelijk is, maar biedt de tekst tevens genoeg handvatten voor een langdurige juridische strijd. Dit heeft alles te maken met het feit dat ARVODI-2008 over diensten gaat en politiewerk nu eenmaal niet simpel weg te schrijven is als dienst, het is en blijft mensenwerk.

Politie Hollands-Midden heeft op 1 januari 2010 een 'overeenkomst alarmcentrale' getekend met G4S. Het is waarschijnlijkheid een vervolg contract. Want op 22 april 2010 wordt er een abonnement alarmcentrale overeengekomen. 'Ons Emergency & Care Center (ECG) functioneert als communicatiecentrum bij calamiteiten, voor hulpdiensten maar ook voor uw bedrijf. Het is als enige particuliere alarmcentrale in Nederland aangesloten op het nationaal noodnet en beschikt over de expertise en apparatuur om elk rampenteam in enkele minuten te activeren', schrijft het bedrijf in april 2010.

Voor de politie lijkt G4S de ideale partner, maar wie de voorwaarden goed leest valt opnieuw op hoe leidend het bedrijf is. De Rijksvoorwaarden lijken niet te zijn toegepast bij deze overeenkomst. 'Bij een geschil waarbij de door de Group 4 Securicor Alarmcentrale geregistreerde gegevens in het geding zijn, is de registratie van de Group 4 Securicor Alarmcentrale doorslaggevend', vermeldt de overeenkomst van 1 januari 2010.

De politie zal bij een geschil dus moeten inbinden en ook bij de werkinstructies van 11 januari 2008 over de alarmcentrale is het bedrijf leidend: 'De servicemedewerker zal handelen conform de algemene werkinstructies van Group 4 Securicor en de object gebonden werkinstructies, waarin de taken van de servicemedewerker nader zijn uitgewerkt. De object gebonden werkinstructies worden zoveel mogelijk in nauw overleg met Opdrachtgever opgesteld.'

Politie getraind door G4S

Het bedrijf claimt veel ervaring te hebben. Wereldwijd is het, met meer dan 600.000 werknemers, een grote speler op de markt van de veiligheidsindustrie. Dat is tien keer zoveel als het aantal Nederlandse politiefunctionarissen van rond de 60.000. Die macht, gekoppeld aan een lage vraagprijs (G4S staat niet bekend om haar hoge lonen) maakt het bedrijf tot een invloedrijke speler die zelfs de training van functionarissen naar zich toe weet te trekken.

Je zou verwachten dat op het terrein van opleiding en bijscholing de overheid het initiatief heeft, maar ook daar heeft de veiligheidsgigant voeten aan de grond. Politie Gelderland-Midden sloot op 27 april 2010 een 'diensthulpverleningsovereenkomst' met het bedrijf voor training op het gebied van bedrijfshulpverlening en brandveiligheid, kort omschreven als veiligheidsopleiding. In

de overeenkomst wordt expliciet vermeld dat G4S 'haar expertise op bovengenoemd gebied, ten behoeve van Politie Gelderland-Midden wil in zetten.' Het korps erkent daarmee dat het bedrijf 'meer' kennis zou hebben ten aanzien van veiligheid, op zich opmerkelijk.

Dat het bedrijf opnieuw in staat is om goede voorwaarden af te dwingen in het twee jaar durende contract, blijkt uit 'artikel 3 duur en beëindiging van de dienstverleningsovereenkomst'. Als de politie niet tevreden is, volgen er eerst nog twee evaluaties in een periode van drie maanden om G4S in de gelegenheid te stellen trainingsverbeteringen aan te brengen. Indien die evaluaties in de ogen van de politie niet voldoende zijn, is er nog een opzegtermijn van drie maanden. G4S kan zo haar contract nog zes maanden verlengen, ook als de opdrachtgever niet tevreden is.

Waardetransport

Naast deze trainingen verzorgde G4S het waardetransport en de verwerking van die waarden voor politie Gelderland-Midden, maar verloor de mini-competitie voor de beveiligingsdiensten. Securitas won deze competitie door een beter implementatieplan in te dienen, het scoorde tien punten hoger dan G4S.

Dit plan van G4S voor Gelderland-Midden uit 2011 is niet vrijgegeven door die regio. Bij Friesland, Groningen en Drenthe was er nog geen competitie geweest, maar al wel een implementatieplan. Het internationale bedrijf weet zichzelf flink te verkopen. Zo beweert het dat 'G4S een landelijk dekkende surveillancedienst heeft en het 24 uur per dag, zeven dagen per week alarmmeldingen opvolgt. Met een wagenpark van 128 surveillancewagens is G4S de meest efficiënte beveiligingsorganisatie in Nederland op het gebied van mobiele surveillance en kan daardoor snelle aanrijdtijden garanderen.'

De alarmcentrale/meldkamer komt ter sprake en ook toekomstige ontwikkelingen: 'Door in de toekomst gebruik te maken van camerasurveillance, kan bovendien worden aangestuurd op basis van onregelmatigheden in het dagelijks patroon.' Hoe dit echter wettelijk ingekaderd is, is onduidelijk. Het lijkt erop dat het bedrijf voorloopt op de camerasurveillance die de politie misschien zal gaan invoeren.

Het is onduidelijk waar het puntenverschil met Securitas inzit, maar hoewel G4S een landelijke dekking heeft, blijft

zij vaag over wat nu de precieze aanrijtijden zijn. Zij registreert die weliswaar, maar of dat vijftien minuten of een uur is, daar wordt in het implementatieplan niets over vermeld terwijl het bedrijf wel 'begrijpt dat het voor de deelnemer van groot belang is dat een snelle alarmopvolging na een melding volgt.'

Hoewel G4S bij Gelderland-Midden achter het net viste, schrijft het bedrijf dat zij een 'uitgebreide ervaring met het implementeren en leveren van diensten aan politiekorpsen' heeft. 'Binnen de raamovereenkomst leveren wij onder andere aan de korpsen Haaglanden, Limburg Zuid en Brabant-Noord (7 maart 2011).'

Bij deze korpsen had zich ook Utrecht zich aangesloten. Politiekorps Twente heeft, net als Amsterdam, een convenant af gesloten met de beveiligingsbranche, waaronder G4S. 'Tweerichtingsverkeer, welteverstaan. De Meldkamer zal foto's van verdachte huizen, auto's en personen voortaan doorsturen naar beveiligers die sneller ter plaatse kunnen zijn dan agenten', schrijft het *NRC Handelsblad* van 9 december 2011.

Korpschef Sitalsing is laaiend enthousiast over de uitwisseling van informatie met onder andere G4S. Het bedrijf zelf geeft bij monde van Director Business Development van G4S Secure Solutions. Jeroen van der Poel, toe dat het "lobbyt voor meer taken in het publieke domein." Van der Poel denkt hierbij ook aan het gevangeniswezen. Hij spreekt in de NRC van "volledige outsourcing van gevangenissen." Ofwel: een gevangenis die onder beheer staat van een bedrijf.

Misstanden

In het artikel wordt door de NRC-journalist met geen woord gerept over de misstanden in gevangenissen die G4S beheert in onder andere de VS en Groot-Brittannië. Hier zit ook het probleem van de aanbesteding. Ten eerste is er sprake van steeds meer schaalvergroting waardoor grote spelers op het terrein van de beveiliging eerder aan de bak zullen komen dan kleinere bedrijven. Grote spelers die dus ook veel meer macht hebben en kunnen lobbyen.

Vraag is dan waarom deze grote spelers niet worden afgerekend op hun gedrag elders. Het zou kunnen dat het gedrag van het bedrijf in Nederland goed te noemen is, hoewel ook dat moeilijk is na te gaan. In het NRC-artikel merkt Sitalsing op dat de politie niet weet of iedere beveiliger een blanco strafblad heeft. "Dat kan ik u wel voor de politie garanderen." Dat is echter maar een deel van het probleem.

Uiteindelijk gaat het er om wie verantwoordelijk is zodra er iets mis gaat. En of misstanden überhaupt worden geregistreerd, onderzocht en hoe dan. Binnen het huidige duurzaamheidsbeleid dat de overheid hanteert kun je ook nog de vraag stellen of je wel wilt samenwerken met een bedrijf dat van incident naar incident rolt. De vraag is wat dat doet met je eigen imago.

Dat G4S ook in Nederland over enige tijd gevangenissen zal gaan leiden, is niet ondenkbaar. Hoewel op dit moment de beveiligers van het bedrijf ontslagen worden bij de DJI (Dienst Justitiële Instellingen) heeft G4S al eerder 'arrestanten-verzorgers' geleverd aan korps Limburg-Zuid. Dit was al enige tijd gaande en op 8 november 2010 tekende het bedrijf een nieuwe overeenkomst met politie Limburg-Zuid.

Het bedrijf nam hierin wederom de leiding, haar werkinstructies zijn leidend naast de 'object gebonden' instructies en de arrestanten-verzorgers 'staan onder leiding van een groepsleider van G4S', vermeldt de overeenkomst. Als een verzorger zich misdraagt, niet functioneert, moet dit door de Opdrachtgever schriftelijk gemeld worden (overeenkomst februari 2007). De kosten voor de vervanging zijn niet automatisch voor G4S, terwijl die wel de selectie, training en een milieu- en antecedentenonderzoek moet garanderen.

In al deze overeenkomsten klinkt de macht van het bedrijf door. Zowel Amsterdam als Twente geven die macht ook uit handen en de vraag is natuurlijk waar het een keer misgaat. Op 12 april 2012 vond er een overval plaats op het gelddepot van G4S in Nieuwegein. Het *Algemeen Dagblad* tekende op dat 'de politie de stellige overtuiging heeft dat de overvallers hulp van binnenuit hebben gekregen.'

Nu is diefstal van waarden waar geen slachtoffers bij vallen minder erg dan missers bij arrestanten-verzorging, zoals in het buitenland regelmatig voorvalt. Dat doet de rechtsstaat in zijn geheel geen goed. De gretigheid van Sitalsing (Twente) en Aalbersberg (Amsterdam-Amstelland) om met G4S in zee te gaan duiden dan ook op een beperkt zicht op het functioneren van het bedrijf en een brevet van onvermogen voor de politie.

Menselijke factoren

Alarmcentrale, mobiele surveillance, objectbeveiliging, veiligheidstraining, arrestantenbewaking, waardetransport, informatie-uitwisseling... de politie werkt op allerlei

terreinen samen met G4S. De politie is consument, maar een bijzonder soort consument. Zij valt onder de verantwoordelijkheid van de minister van Veiligheid en Justitie en die moet zich op zijn beurt verantwoorden aan de Tweede Kamer. Vandaar dat de Rijksvoorwaarden ARVODI 2008 een passage over het contact met de Tweede Kamer bevat: 'Indien Opdrachtgever besluit over de resultaten van de geleverde Diensten en de daarmee gemoeide kosten de Tweede Kamer te informeren is de toestemming, bedoeld in het vierde lid, evenmin nodig' (Lid 11.5). De politie kan gewoon rapporteren zonder G4S daarvan op de hoogte te stellen.

Ook artikel 19 lijkt duidelijk: 'De partij die toerekenbaar tekortschiet in de nakoming van haar verplichtingen, is tegenover de andere partij aansprakelijk voor de door de andere partij geleden dan wel te lijden schade (lid 3).' En 'de opdrachtnemer vrijwaart Opdrachtgever tegen eventuele aanspraken van derden op vergoeding van schade als gevolg van het tekortschieten als bedoeld in het derde lid (lid 5).' 'Tekortschieten in het nakomen van de verplichtingen' is bij ICT-drama's bij de politie nog voorstelbaar, het zijn niet-menselijke grootheden. Maar bij beveiliging en bewaking gaat het om menselijke factoren. Binnen die overheidssectoren zal deze formulering voer voor juristen zijn.

Dit is ook het geval bij de 'overeenkomst objectbeveiliging' van korps Utrecht van 11 augustus 2008. Alleen voor het inwerken is een passage opgenomen over het niet functioneren van werknemers van G4S, en dan gaat het vooral over de kosten. 'Alleen in de navolgende gevallen komen de kosten van het inwerken voor rekening van Group 4 Securicor: […] ziekte […] verlof […] vervanging vanwege een gedraging van de beveiliger die kan worden aangemerkt als een dringende reden voor ontslag.'

Het is onduidelijk of G4S zich constant verantwoordelijk voelt voor het gedrag van haar personeel tijdens de objectbeveiliging in de regio Utrecht. De overeenkomst vermeldt namelijk dat als een werknemer 'zijn werkzaamheden structureel niet naar behoren verricht, zal Group 4 Securicor op schriftelijk verzoek van Opdrachtgever en na overleg met Opdrachtgever de betreffende beveiliger vervangen.' G4S draait op voor de kosten van de vervanging, het bedrijf zal dus zijn werknemers in het zadel proberen te houden.

Wie de schandalen bekijkt, kan zich voorstellen dat er gemakkelijk slachtoffers kunnen vallen. Het politieapparaat is niet het meest transparante bestuursorgaan. Snel melden aan de verantwoordelijke minister zit er niet in. Aan de

andere kant zal G4S ook niet heel snel misdragingen van zijn werknemers melden. Dit kost geld, vandaar de drempels. De politie huurt ook geen los personeel in, maar een volledige eenheid die onder zijn eigen 'G4S commandant' functioneert.

In het eerder aangehaalde artikel in *NRC Handelsblad* (09-12-11) komt ook Jan Willem van der Pol van de Politiebond aan het woord. Hij beweert dat particuliere beveiligers burgers zijn, maar dat is zeker bij G4S niet het geval. Misschien slaat het wel op hun bevoegdheden, maar het zijn werknemers van een gigantisch beursgenoteerd bedrijf, niet te vergelijken met Henk en Ingrid van om de hoek.

Bijkomend probleem is ook dat het bedrijf allerlei petten op heeft. Glenn Schoen, beveiligingsexpert van G4S, roept dat we in een hele gevaarlijke wereld leven. Directeur Jeroen van der Poel lobbyt voor private gevangenissen. Weer een andere manager regelt de arrestanten-verzorging of de informatie-uitwisseling en opslag met verschillende politiekorpsen, de training, melding, surveillance, en ga zo maar door. Waar is echter sprake van inspectie, controle en toezicht op het eigen functioneren?

Aansprakelijkheid

Politie Haaglanden heeft G4S in 2002 een grote opdracht voor receptie- en beveiligingsdiensten gegund. Het lijkt erop dat het bedrijf sindsdien niet meer weg te denken is bij dat korps. Dat G4S de opdracht heeft gekregen, zal misschien te maken hebben gehad met de grootte van de aanbesteding. 'Gezien de omvang van de opdracht receptie- en beveiligingsdiensten worden aan Kandidaat minimale omzeteisen gesteld. […] De omzet eis voor deze aanbesteding bedraagt gemiddeld over de boekjaren 2003, 2004 en 2005 tenminste € 2.000.000,- (twee miljoen euro) op jaarbasis', is te lezen in de aanvraag tot offerte.

De aanvraag is duidelijk over kwaliteit, kwaliteitstoetsen, audits, klantevaluaties en over het eigendomsrecht van de verzamelde data. Geen tweerichtingsverkeer in het laatste geval, de data is afkomstig van de politie Haaglanden. 'Het project wordt uitgevoerd in opdracht van de opdrachtgever en de eigendomsrechten van de door de Kandidaat gerealiseerde producten berusten derhalve bij de opdrachtgever. Onder deze eigendomsrechten vallen alle producten, documentatie, verzamelde data, rapportages en ontwikkelde werkwijze, die de Kandidaat in het kader van deze opdracht produceert of in de toekomst met betrekking tot dit project zal produceren' (offerte aanvraag december 2006).

In tegenstelling tot de Rijksvoorwaarden 2008 wordt in de algemene Inkoopvoorwaarden politieregio Haaglanden van 2005 vermeld dat 'Inspectie door of namens Opdrachtgever kan plaatsvinden zowel tijdens het verrichten van de Werkzaamheden/diensten als daarna, in welk laatste geval de inspectie tevens is gericht op beoordeling van het resultaat. Leverancier zal zonder kosten voor Opdrachtgever alle medewerking verlenen on informatie verschaffen om de inspectie mogelijk te maken.' Ook is er sprake van een begeleidingscommissie of stuurgroep terwijl dit bij andere overeenkomsten niet het geval is. Net als bij andere opdrachten is er geen regeling rond overmacht en voor aansprakelijkheid getroffen.

Op papier lijkt korps Haaglanden het beveiligingsbedrijf streng aan de regels te houden. G4S moet zijn medewerkers die voor Haaglanden werkzaam zijn voldoende scholing bieden hetgeen in het jaarplan dient te worden opgenomen. Nadat bleek dat G4S in vragen over de offerte de responstijd van haar mobiele surveillanten probeerde op te rekken, reageerde Haaglanden resoluut: de politie bepaalt hoe de responstijd gemeten wordt.

Aangaande de aansprakelijkheid antwoordde de regiopolitie Haaglanden in 2007 duidelijk 'nee'. G4S heeft duidelijk moeite met die aansprakelijkheid. 'Ten aanzien van uw Algemene voorwaarden en artikel 1-e-8 zijn wij verplicht, ten opzichte van onze moedermaatschappij, afspraken te maken over de mate van aansprakelijkheid. Zijn nadere afspraken ten aanzien van een limitering van aansprakelijkheid bespreekbaar?', vraagt G4S.

Het beveiligingsbedrijf legt hiermee de vinger op de zere plek. 'Echter zijn wij ons ook bewust van de grote menselijke factor in onze dienstverlening en hetgeen in een uitzonderlijk geval kan leiden tot een aanrekenbare fout die ons bedrijf schadeplichtig maakt', schrijft G4S bij vraag 49 aan Haaglanden.

Het vreemde is dat die uitzonderlijke gevallen niet zo uitzonderlijk lijken. De Chief Executive Officer van G4S (CEO Ashley Almanza) wordt in de *Financial Times* van 14 november 2013 geciteerd: *'It's the nature of the business that we can... hit the ball out of the park for 364 days of the year and on the last day of the year something goes wrong.'* Deze opmerking kun je op twee manieren interpreteren. Een positieve interpretatie is dat het bedrijf er alles aan doet om zijn werk naar behoren uit te voeren, maar dat het soms

mis kan gaan. Ashley Almanza beweert dit echter niet, hij zegt eigenlijk dat het bij de 'nature of the business' hoort, het kan niet worden voorkomen.

Vandaar dat de Nederlandse tak probeert de aansprakelijkheid anders te regelen. Het punt is echter dat op die ene dag dat het volgens G4S fout kan gaan, het goed fout gaat. Dan vallen er dodelijke slachtoffers, is er chaos bij de rekrutering, worden mensen gemarteld, wordt er gefraudeerd, de lijst is eindeloos.

Heeft G4S geen strafblad?

Begin deze eeuw formuleerde het politiekorps Haaglanden in het kader van het inhuren van een beveiligingsbedrijf kwaliteitseisen, stelde evaluaties verplicht en hielp een begeleidingscommissie in het leven. Logisch in het geval van politiewerk dat wordt uitbesteed en waarbij de menselijke factor een rol van betekenis speelt. G4S moest een juridische eigen verklaring afgeven die eigenlijk vooral belasting- en handelsregistergegevens omvatte.

Medewerkers van G4S moesten wel een 'verklaring volledige medewerking antecedentenonderzoek' (bijlage F) ondertekenen. 'De politie heeft een cruciale rol bij de opsporing van strafbare feiten en de handhaving van de openbare orde. Mede gelet op deze verantwoordelijkheid, zullen medewerkers die werkzaamheden voor of bij de politie verrichten, een integere status moeten hebben.' De G4S-medewerkers moeten van onbesproken gedrag zijn en worden gescreend op 'antecedenten openbare orde, laakbaar gedrag en criminele contacten.'

Let wel, dit geldt enkel voor de medewerkers van G4S, niet voor het bedrijf zelf. Nu gaat het er in dit geval niet om of het bedrijf wel of niet de gunning van Haagse politie krijgt. Uiteindelijk gaat het erom in hoeverre de overheid zelf haar eigen duurzaamheidsmantra serieus neemt. Alle stukken over G4S die tot nu toe door de politiekorpsen openbaar zijn gemaakt bevatten geen enkele verwijzing naar mogelijk laakbaar gedrag van de firma, het moederbedrijf of één van haar dochters.

Dat alleen al is opmerkelijk, want niet alleen de politie ook andere bestuursorganen maken gebruik van de diensten van G4S. Zo huurde het ministerie van Buitenlandse Zaken het bedrijf in voor de beveiliging van de Nederlandse residenties in Griekenland, Turkije, Denemarken, Marokko en Polen. Nederland en vooral Den Haag willen zich profileren als een land en stad van vrede en recht. Misschien past G4S daar wel bij, dat

is ter beoordeling van de verantwoordelijke bestuursorganen in het kader van een duurzame aanbestedingsprocedure. Minimaal één vraag over de internationale incidenten van het bedrijf zou echter op zijn plaats zijn geweest. Die leiden terug tot ver in de jaren '90 en zijn dus niet nieuw te noemen.

Observant 65, 30 juni 2014

Met de billen bloot op Facebook

Er wordt alom voor gewaarschuwd: je sociale leven kan redelijk eenvoudig in kaart worden gebracht zodra je actief een Facebook-pagina onderhoudt. Buro J&J brengt het resultaat visueel in kaart.

Metadata zijn sporen die je na laat gedurende je communicatie via internet en telefoon. Dit zijn vooral individuele sporen, sporen over jezelf en het directe contact dat je onderhoudt met mensen. Natuurlijk kan naar aanleiding van die sporen een beeld geschetst worden van je sociale leefwereld, maar daarvoor moet je iemands data wel eerst voor langere tijd opslaan.

Individuele data is harde data over waar, hoe laat en met wie je hebt gesproken waarmee je als verdachte, getuige of onbekende kunt worden gelabeld door opsporingsdiensten. Je bent in de buurt geweest, je hebt met iemand gebeld of *gewhatsappt*, je reageert niet op een sms-bombardement, alles in het kader van de opsporing.

Metadataverzameling

Voor directe vervolging zijn die data van belang, voor inlichtingendiensten minder. Zij zullen ongetwijfeld veel data verzamelen (*'At a meeting with his British counterparts in 2008, Keith Alexander, then head of the National Security Agency, reportedly asked, "Why can't we collect all the signals, all the time?"', the Washington Post* 13 mei 2014), maar dat ligt in de aard van inlichtingendiensten. Die data heeft ook pas inlichtingenwaarde op het moment dat je iemands digitale stappen langer volgt. Voor het voorkomen van aanslagen zijn die data meestal zinloos. Zij geven misschien wel patronen aan, maar hebben geen voorspellende waarde voor mogelijke acties.

Op 20 december 2013 opent NBC news met: *'NSA program stopped no terror attacks, says White House panel member' The Guardian* (14-01-14) onderstreept deze claim met de stelling dat volgens de *Senate judiciary committee* het verzamelen van bulk telefoondata een beperkte rol heeft gespeeld in het voorkomen van terrorisme.

The Guardian baseert haar stelling op een onderzoek door de New America Foundation die tot de conclusie kwam dat de NSA geen enkele aanslag heeft weten te voorkomen. De aanslag op de marathon van Boston van 15 april 2013 onderschrijven die

conclusie. Meerdere diensten (FBI, CIA en NSA) hielden de verdachten in de gaten, maar zij konden hun aanslagen toch uitvoeren.

Nederland laat hetzelfde beeld zien. De inlichtingendiensten hebben de moord op Fortuyn en Van Gogh niet weten te voorkomen. Van de Hofstadgroep, waar Mohammed Bouyeri toe behoorde, was reeds bekend dat de meeste leden benaderd waren door de AIVD. Tevens was bekend dat zij bijeen kwamen in het huis van Bouyeri en dat het adresboek van hem door de Amsterdamse politie was gekopieerd voor de inlichtingendienst. De dienst heeft aangegeven dat zij webfora kunnen hacken, daarnaast heeft de dienst naar alle waarschijnlijkheid telefoontaps en internettaps op de Hofstadgroep leden geplaatst. Theo van Gogh is ondanks die dataverzameling vermoord (zie *Onder Druk*, Buro Jansen & Janssen).

Open boek

Voor inlichtingendiensten is het voorkomen van aanslag echter niet het belangrijkste. Zij willen de 'subversieven', de 'tegencultuur' in kaart brengen. Specifieke informatie kan dan belangrijk zijn om op een groep in te kunnen zoomen, maar die data (metadata) is slechts deels interessant.

Je kunt bijvoorbeeld vastleggen dat Margriet en Barbara (de twee vrouwen in dit verhaal) veel met elkaar communiceren, bijvoorbeeld elke dag om 16.00 uur gedurende twee minuten. Margriet bevindt zich ten oosten van het centrum van Amsterdam, Barbara ten westen. Een locatie is er ook voor beide vrouwen. Laurence (de man in dit verhaal) communiceert slechts zelden met beide vrouwen, met Barbara op bepaalde momenten. Groepsgesprekken hebben de drie nooit.

Eigenlijk ben je nu al het zicht op de '*bigger picture*' kwijt, omdat je direct inzoomt op het individu. Je verliest zo het helikopterperspectief, je staat niet meer boven de persoon, maar eigenlijk direct naast hem. Voor opsporingsdiensten is dit van belang voor het traceren van verdachten van misdrijven, je legt iemands leven in retrospectief vast. Voor inlichtingendiensten is deze data eigenlijk zinloos, je bent altijd te laat, zoals de moord op Van Gogh laat zien.

Dat tegenwoordig iedereen een spoor van data trekt, is sinds de onthullingen van Edward Snowden op de achtergrond geraakt. De overheid heeft een grote verzamelwoede en dat is de 'schuldige' in de discussie. Dit is al vele jaren bekend,

maar veel mensen leken en lijken zich daar niets van aan te trekken. De discussie over de massa aan data die mensen zelf op het internet storten door eigen communicatie, is op de achtergrond geraakt.

Communicatie over mijn aanwezigheid in de Albert Heijn gebeurt zowel verhuld (metadata) als open (twitter, instagram). Het lijkt erbij te horen dat bij een actie, bijvoorbeeld het omtrekken van stellingkasten in de AH tegen de macht van de supermarkten, je niet alleen je metadata meesleept (zonder bellen al je locatie prijsgeven), maar ook nog eens met diezelfde telefoon twittert (hashtag #valAHaan) en fotografeert.

Dat de overheid die data verzamelt is dan eigenlijk bijzaak geworden. Veel mensen delen hun gehele leven elke seconde van de dag, niet alleen via metadata ook door 'echte' data. Het op straat gooien van persoonlijke data is ook zichtbaar bij Facebook. Wij hebben drie mensen (Margriet, Barbara en Laurence) die buitenparlementair politiek actief zijn, gevraagd of wij hun Facebook-data mochten analyseren. Die analyse hebben we vervolgens in een grafisch beeld omgezet.

Wie is wie

Stel, je bent vagelijk bevriend met Margriet. Je hebt nooit haar vrienden ontmoet en wordt uitgenodigd voor haar dertigste verjaardag. Margriet geeft een knalfuif en al haar familie, vrienden en bekenden komen langs. Zelfs incidentele vrienden van uitgaansgelegenheden zijn van de partij.

Zodra je van de grote zaal waar de party plaatsvindt een foto zou maken, krijg je grofweg een schets van de Facebook-pagina van Margriet. Haar familie zoekt elkaar op, mensen van de ngo waar zij actief voor is doen hetzelfde, krakers delen de laatste nieuwtjes uit, de deelnemers aan haar dansgroepen begroeten elkaar, en anderen hokken in groepjes. Door de gehele ruimte zwerven enkele eenlingen die niet echt mensen kennen.

In de loop van de avond vormt de dansvloer het middelpunt van het feest, ook daar is sprake van groepsvorming. Het eerste moment van de avond, dat bekenden elkaar opzoeken, zie je terug in de afbeelding op de Facebook-pagina van Margriet. Nu niet alleen op haar dertigste verjaardagsdag, maar dagelijks.

In het algemeen valt op dat de meeste mensen met hun volledige naam (voor- en achternaam) zich op Facebook presenteren. Ook ngo´s, actiegroepen, bands, kraakpanden en

alternatieve uitgaansgelegenheden vermelden een volledig profiel op sociale media. Daardoor wordt vrij snel duidelijk waar iemand sympathie voor heeft, waar hij of zij uitgaat, welke kraakpanden de persoon kent en welke acties door iemand worden ondersteund.

Opvallend is dat al die acties en ngo's ook bij elkaar horen. Er zitten geen vreemde zaken bij, zoals bijvoorbeeld bedrijven als Coca Cola, Monsanto of Shell. De drie activisten tonen hun politieke opvatting door middel van hun Facebook-pagina duidelijk. Natuurlijk zijn Margriet, Barbara en Laurence bekenden van Jansen & Janssen, maar zelfs bij onbekende activisten zal het eenvoudig zijn om de politieke kleur, vrienden, familie, werk en je sociale netwerk op te tekenen.

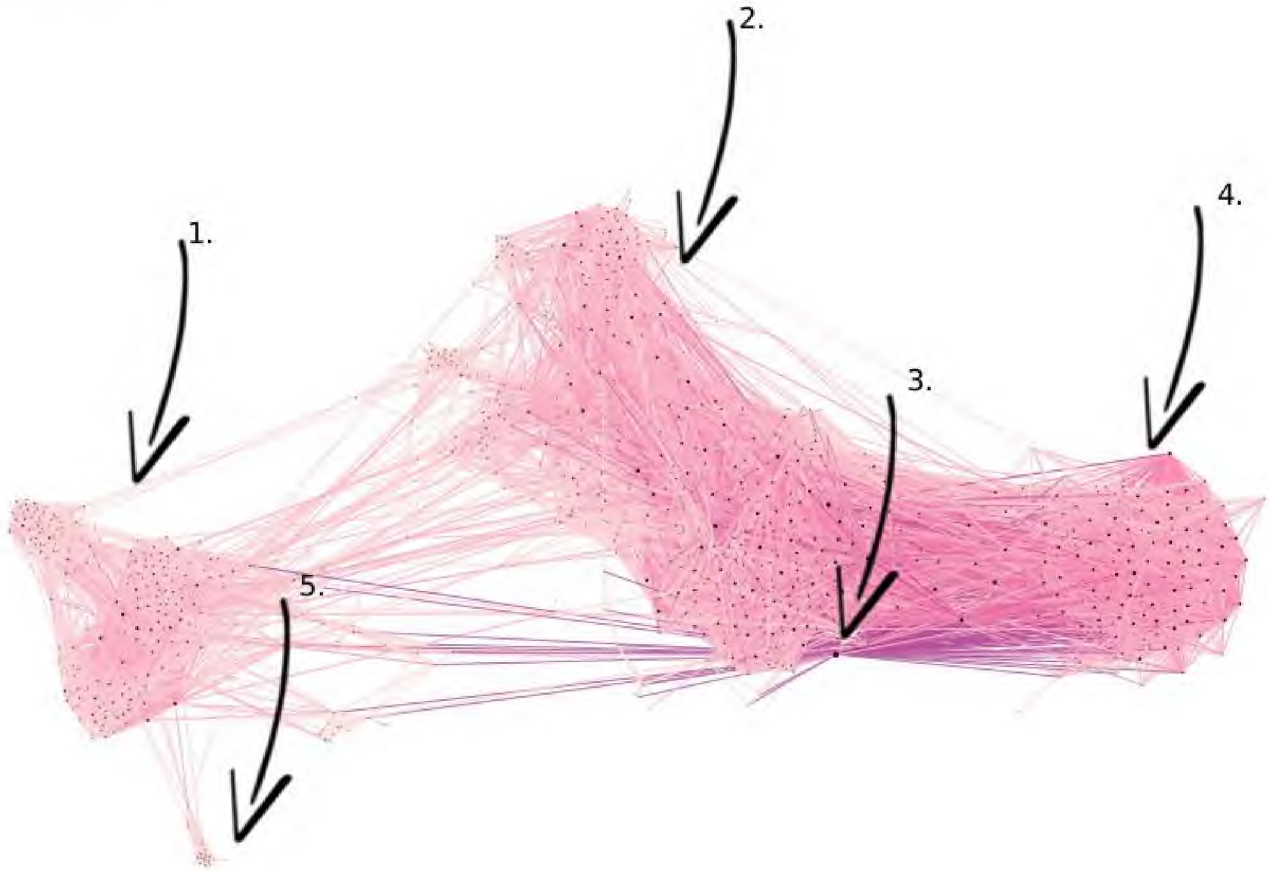
Een kraaksymbool op Facebook bijvoorbeeld is iets totaal anders dan een kraaksymbool op een T-shirt dat je vandaag draagt. Dat T-shirt draag je waarschijnlijk anoniem, zonder naambordje of rug-burgerservicenummer. Via je Facebook-pagina is dat T-shirt gekoppeld aan je naam, je sociale netwerk, je leefwereld. Dat is niet anoniem, het gaat zelfs verder dan je persoonlijke identificatie.

Niet perfect

Natuurlijk is het beeld niet perfect en moet er rekening worden gehouden met allerlei ongerijmdheden, maar de grafische representatie van de drie mensen schept een beeld van hun leven. Bij het zien van het beeld viel het Margriet op dat haar "sociale netwerk heel goed zichtbaar is". Dat het beeld niet perfect is viel haar ook op: "Grappig dat er ook een muziekband en een persoon tussen zitten die inmiddels amper nog actief zijn." Het beeld is niet perfect en daarom worden hier enkele kanttekeningen bij de interpretaties geplaatst.

Veel communiceren, veel 'liken' of veel 'likes' krijgen op Facebook betekent niet alles. In de beelden hebben de verschillende personen en groepen een andere kleuren. Donker rood is een teken van grote activiteit, maar in deze analyse wordt daar niet dieper op ingegaan. Veel activiteit valt bij een oppervlakkige analyse niet goed te definiëren. Wel maakt het beeld duidelijk dat met verfijnde oplossingen de mate van activiteit en welke activiteit nader kan worden ingekleurd. Automatisch moet bij de analyse van de beelden voorzichtig worden omgesprongen met conclusies over leiderschap en hiërarchie.

Ook zegt de communicatie op Facebook niet alles. Mensen die op internet zeer actief zijn, zijn misschien in werkelijkheid erg verlegen. Mensen met een grote mond en die stoer doen op internet, vervullen niet per se een belangrijke rol binnen een groep en/of sociaal netwerk. Tevens is niet iedereen aanwezig op Facebook. Er zijn nog steeds mensen die geen Facebook-pagina hebben, die zijn dus niet zichtbaar in het netwerk. Zelfs met deze kanttekeningen moet Laurence ook toegeven dat zijn leven redelijk goed in beeld wordt gebracht.



Facebook-beeld van Barbara
Pijl 1 oude vriendengroep en contacten via derden, geen sterke banden
Pijl 2 collega's en ngo's gerelateerd aan het werk van Barbara
Pijl 3 sterke relatie met Barbara, springt eruit in het netwerk, is haar vriend Evert
Pijl 4 collega's en uitgaansgelegenheden gerelateerd aan Evert vriend van Barbara
Pijl 5 oude vriendengroep en contacten via familie zwerm, geen sterke banden
Tussen pijl 1 en 5 Familie zwerm
Tussen pijl 2 en 4 individuen, kraakpanden en alternatieve uitgaansgelegenheden.

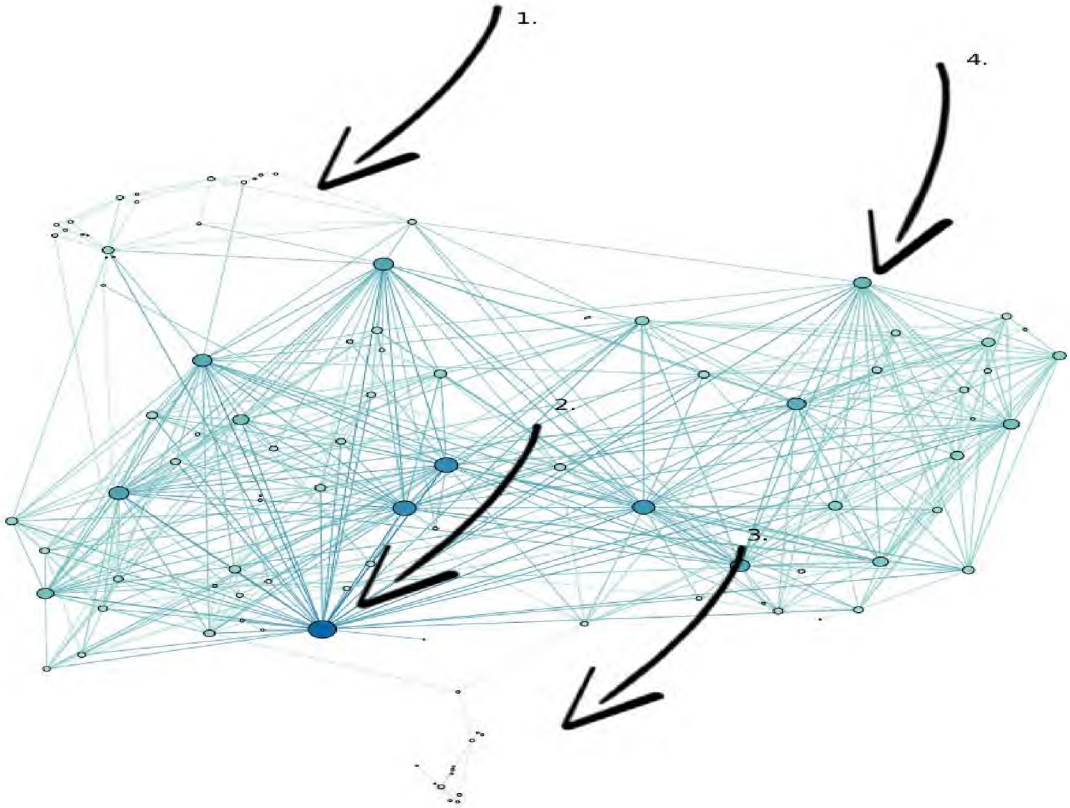
Familie zwerm

Het Facebook beeld van Margriet bestaat uit een grote zwerm (pijl 1 van haar beeld), een klein wolkje onder (pijl 3), twee wolken bij elkaar (pijl 4) en enkele losse individuen bovenaan. Het beeld van Barbara laat links een kleine wolk zien met een plukje daaronder (pijl 1 en 5) en rechts een grote zwerm in een boog van boven naar beneden (pijl 2, 3 en 4). Laurence laat een grote wolk in het midden zien (pijl 2 en 4) en twee plukjes boven (pijl 1) en beneden (pijl 3).

Bij alle drie de beelden springen de plukjes familie er uit. Margriet heeft een klein wolkje familie (pijl 3) die ver onder haar 'eigen' wolk hangt. Barbara heeft een grote wolk links van de centrale zwerm. Dat is haar familie en waarschijnlijk oude vrienden in het land waar zij vandaan komt. Laurence heeft een klein wolkje onder de hoofdwolk, waar zijn familie en enkele oude vrienden zich hebben verenigd.

Alle drie de activisten hebben 'afstand' tot hun familie. Bij Barbara heeft het met fysieke afstand te maken, bij Laurence en Margriet kan het iets zeggen over de mate van gehechtheid. Bij Barbara is nog opvallen dat naast de 'familie' zwerm (tussen pijl 1 en pijl 5) er nog twee kleine wolkjes (pijl 1 en 5) verder van de centrale wolk afstaat. De verklaring van deze wolk: een groep vrienden of bekenden in het land waar Barbara vandaan komt. Pijl 1 laat een klein netwerk zien dat verbonden is met enkele wolken bij de centrale zwerm. Het is niet direct verbonden met de centrale persoon (pijl 3) in de grote wolk. Waarschijnlijk is dit een groep uit het verleden waar om verschillende redenen minder relaties mee onderhouden zijn.

Hoe zijn die specifieke familie-zwermen te onderscheiden van elkaar? Eigenlijk vrij simpel. De activisten staan op Facebook met hun achternaam. In de 'familie' wolken komt die naam veel voor. Natuurlijk is het een aanname, maar bij navraag blijkt Margriet aan te geven dat "rechtsonder de familie zit". Ook Laurence zegt dat pijl 3 een "opvallend los netwerkje is. Dit is een netwerk van oude vrienden en familie. Ik heb daar weinig contact mee en dat lijkt zelfs uit het Facebook-beeld te halen", geeft Laurence aan. In ieder geval is de familie zwerm niet opgenomen in de centrale wolk van alle drie de activisten.



Facebook-beeld van Laurence
Pijl 1: wolkje vrienden of collega's die betrokken zijn bij een ngo's
Pijl 2: activisten zwerm rond kraakpand in Amsterdam (groepen, individuen, kraakpanden etc.)
Pijl 3: Familie zwerm en wat oude vrienden
Pijl 4: activisten zwerm rond groep in Den Haag (groepen, individuen, kraakpanden etc.)

Activisten zwerm

De activisten zwerm bestaat bij alle drie uit een verzameling groepen, kraakpanden, alternatieve uitgaansgelegenheden en personen. Bij Margriet bestaat die wolk (pijl 1) uit verschillende delen. Links boven bevindt zich een groep mensen, muziekbands en groepen rond enkele uitgaansgelegenheden en kraakpanden zoals de OCCii aan de Amstelveenseweg in Amsterdam West en het kraakpand de Valreep in Amsterdam Oost.

Links onder in de centrale wolk komt het woord anarchisme regelmatig terug, zoals Anarchistische Groep Friesland en Anarchistisch Kollektief Utrecht. Deze groepen en mensen 'hangen' rond bij Doorbraak, een linkse basisorganisatie. Rechts onder bevinden zich individuen in de zwerm die actief zijn voor verschillende ngo's. Gezien het werk van Margriet is het logisch dat zij verbinding met deze groep mensen

heeft. Slechts enkele groepen komen er in voor, het zijn vooral personen.

Tot slot rechtsboven is een groep mensen en enkele bands gegroepeerd die tussen de alternatieve uitgaansgelegenheden en kraakpand (links boven) en de twee wolken rechts van de activisten zwerm staan. Rechtsboven vormt een soort brug naar twee dansgroepen die rechts van de centrale wolk staan.

De activistenzwerm van Laurence (pijl 2 en 4) is even scherp in te delen in aparte delen. Rechtsonder een specifiek groepje krakers/activisten die dezelfde hobby's erop nahouden. Rechtsboven een groep mensen en organisaties georganiseerd rond het Autonoom Centrum Den Haag (pijl 4). Linksonder is weer het kraakpand de Valreep in Amsterdam Oost present, net als bij Margriet. Het is opvallend hoe de Valreep (pijl 2) bij Laurence als een soort spin vele connecties maakt met mensen en groepen.

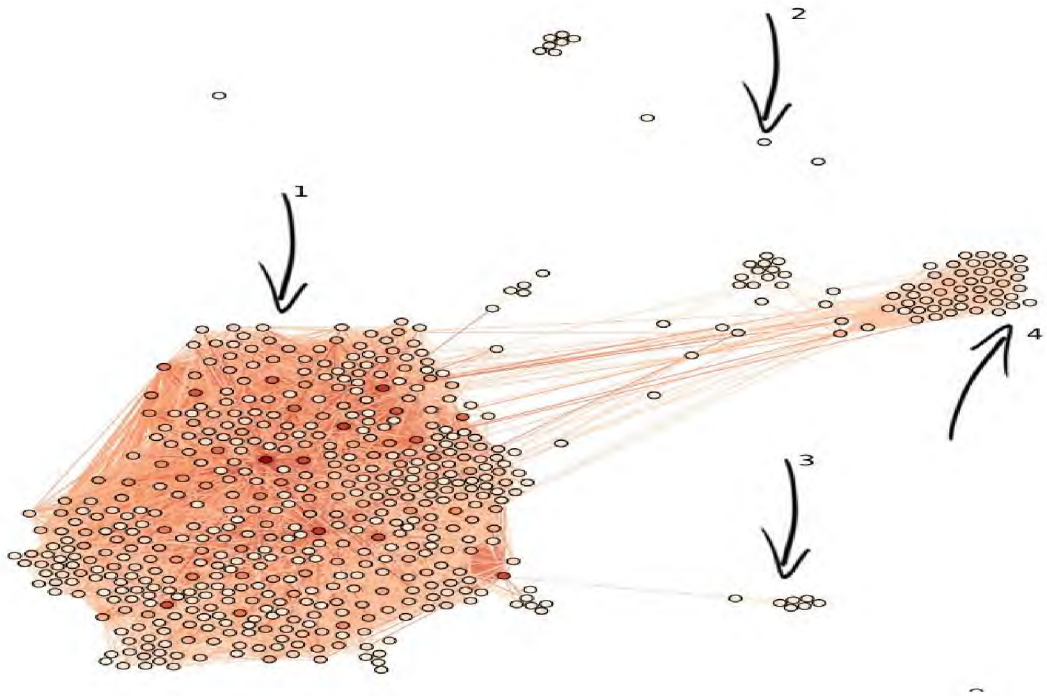
Hier omheen hangen wat activisten en krakers uit Amsterdam. De centrale as in de activistische zwerm van Laurence wordt gevormd tussen de Valreep in Amsterdam en het Autonoom Centrum in Den Haag. Linksboven zijn een paar personen aanwezig die de link vormen tussen de Amsterdamse kraakscene en het wolkje dat links boven de activistenzwerm van Laurence zweeft. Dit kleine wolkje dat los is geweekt van de centrale wolk zijn mensen die betrokken zijn bij een ngo.

De as 'de Valreep - Autonoom Centrum' in de activistenzwerm van Laurence is niet direct zichtbaar bij Margriet. Daar spelen eerder enkele individuen een centrale rol in de 'grote wolk'. Margriet: "in de grote wolk (pijl 1) springen er een aantal erg uit die blijkbaar zeer actief zijn op Facebook zoals Albert en Astrid." Deze twee mensen waren vroeger actief (jaren '90 en begin '0), maar spelen nu geen belangrijke rol meer binnen de activisten scene. Niet alleen groepen kunnen dus een verbindende factor spelen, maar ook individuen zoals de zwermen rond Albert en Astrid laten zien. Zij houden de wolk van Margriet bij elkaar.

Bij Barbara is iets vergelijkbaars aan de hand. De onderkant van de grote wolk (pijl 2, 3 en 4) wordt bij elkaar gehouden door één persoon (pijl 3). Dat is iemand waarmee Barbara veel connecties heeft, haar vriend Evert. Zelfs zonder kennis over de relatie tussen Barbara en Evert valt in ieder geval zijn zeer actieve positie binnen haar netwerk op. Het is duidelijk dat Evert heel dicht bij Barbara staat. Dit kan ook worden geconcludeerd uit het feit dat Evert veel contacten heeft met de familie zwerm (tussen pijl 1 en 5).

Rechts van Evert wordt het laagste deel van de wolk (pijl 4) ingenomen door collega´s en groepen rond de uitgaansgelegenheid waar hij werkt. In het midden zijn vooral de alternatieve uitgaansgelegenheden en kraakpanden vertegenwoordigd (rond pijl 3). Halverwege de top is er een lichte breuk zichtbaar in de wolk. De top lijkt daardoor een beetje los te staan van het deel er onder (pijl 2).

Die top wordt ingenomen door collega´s van de werkplek van Barbara, een ngo die enkele contacten onderhoudt met de activistische scene. Vanuit die top zijn er enkele individuen die tegen de grote wolk aanhangen in twee kleine plukken verdeeld en die ook contact onderhouden met de 'overkant', de familie en oude vrienden zwerm. Dat zijn mensen die connecties hebben met het land waar Barbara vandaan komt, iets dat is op te maken uit de namen van de verschillende mensen.



Facebook-beeld van Margriet

Pijl 1: activisten zwerm met groepen, individuen, kraakpanden en alternatieve uitgaansgelegenheden.
Pijl 2: Losse individuen, merendeel oud klasgenoten van de middelbare school
Pijl 3: Familie zwerm
Pijl 4: Vertier wolk: een grote (waar de pijl naar wijst) en kleine dansgroep (links van de grote wolk)

Vertier wolk

Bij Margriet is het opvallend dat zij twee aparte wolken ter rechterzijde van de activisten zwerm heeft (pijl 4 en iets naast pijl 4). Centraal in die twee wolken staan de namen van een dansgroep. De individuen daaromheen zullen naar alle waarschijnlijkheid leden zijn of sympathisanten, zoals bij de activisten zwerm. Barbara en Laurence geven niet zo heel duidelijk hun hobby's prijs, maar het kan ook betekenen dat zij activiteiten doen met mensen die geen gebruik maken van Facebook of niet zichtbaar zijn in een duidelijk clubverband.

In principe is er natuurlijk sprake van diverse opties ten aanzien van het wel of niet zichtbaar zijn van groepen. Toch is dat niet helemaal waar, want de clusters rond werk, connecties rond een ngo, rond een kraakpand of een uitgaansgelegenheid, zijn wél heel duidelijk. Een logischer verklaring is dat de activiteit meer is ingebed in de bestaande structuur, waardoor er geen losse groep is. Dit is zo als een activiteit niet in een officieel club- of groepsverband, zoals de twee dansgroepen van Barbara, plaatsvindt. Bij Margriet lijkt dit te kloppen, ook ten aanzien van haar oude klasgenoten uit het verleden. "Het groepje helemaal bovenin zijn oud-klasgenoten van mijn middelbare school met enkele geïsoleerde contacten", analyseert Margriet haar eigen Facebook-beeld.

Barbara laat eigenlijk twee wolken zien. Een familie- en vriendenzwerm met daarnaast twee aparte wolken oud-vrienden of bekenden waar nu minder contact mee wordt onderhouden. Deze wolk staat los van haar leven in Nederland, maar is vergelijkbaar met de danswolken van Margriet, gescheiden werelden met enkele connecties. Bij de wolk met het werk van Barbara boven en het werk van Evert beneden wordt het centrum ingenomen door uitgaan, persoonlijke contacten en wat activisme en kraakpanden. Een duidelijke aparte groep sport, cultuur of natuur heeft Barbara niet binnen haar netwerk. Barbara en Margriet zijn wel weer in dat centrum aan elkaar gekoppeld. Margriet en Barbara komen terug in het netwerk van Laurence.

Sociaal netwerk vastleggen

Na het zien van zijn Facebook-beeld vraagt Laurence zich af hoeveel hij gaat veranderen aan zijn gedrag op Facebook. "Het geeft een duidelijk inzicht in mijn sociale leven", constateert hij. Hij merkt daarbij op dat een analyse van de gegevens van Facebook duidelijk maakt waar de zwakke schakels in zijn leven zich bevinden. "Dat is best *scarry*, vreemd om

dat op deze manier te ontdekken", voegt hij eraan toe.

Ook Margriet is verbaasd over hoe scherp haar sociale leven door Facebook in kaart wordt gebracht. "Als je weet in welke thema´s die zwermen of wolken geïnteresseerd zijn, heb je een schat aan informatie. Door een combinatie te maken van individuen en groepen wordt dat snel duidelijk. Je weet echter niet alleen welke thema's centraal staan, ook is zichtbaar hoe bepaalde informatie kan worden verspreid binnen die specifieke netwerken. Je weet namelijk wie actief is, een centrale rol speelt, veel connecties heeft, ga zo maar door. En dan hoeft het niet alleen om commerciële boodschappen te gaan", laat zij weten.

Facebook legt iemands sociale leven vast, maar doet dat echter niet alleen. Mensen leveren het internetbedrijf hun persoonlijke data. Die informatie is misschien onschuldig als je naar de elementen kijkt, maar wie de data in context plaatst kan een foto maken van de bezoekers van de dertigste verjaardag van Margriet. Die foto weerspiegelt haar sociale leven, niet alleen op die dag. Het plaatst mensen in groepen, kleurt politieke ideeën in en geeft inzicht in verhoudingen.

Wie van alle groepen en personen van de Facebook-pagina van Margriet (hetzelfde geldt voor Barbara en Laurence) een grafisch beeld maakt, kan een nog specifiekere sociale geschiedenis van haar optekenen. Jeugd, school, universiteit, arbeidsverleden, vrije tijd, activisme en politieke voorkeuren kunnen deels worden ingevuld. Misschien niet perfect, maar Facebook bezit zoveel data dat die perfectie in de loop der jaren naar alle waarschijnlijkheid zal toenemen.

Vraag is natuurlijk of je je hele sociale leven op straat wilt leggen, of dat je daar zelf controle over wilt hebben en/of houden. Dat is een persoonlijke keuze die niets met privacydiscussies te maken heeft. 'Wat deel je met een bedrijf en daarbij indirect met de wereld?', is de primaire vraag die je jezelf moet stellen.

Maikel van Leeuwen

Observant 65, 30 juni 2014

Facebook beelden, beelden van je Facebook pagina of een social graph

De bijgevoegde beelden zijn een visualisatie van de Facebook-pagina's van Margriet, Barbara en Laurence. De verbindingen in het netwerk, de lijnen tussen de rondjes worden ook wel 'edges' genoemd. In het Nederlands vertaald zou dit randen of richels betekenen. Eigenlijk zegt dit al iets over de voorzichtigheid die in acht genomen moet worden bij interpretaties. Randen en richels zijn geen diepe verbindingen. Een verbinding kan een 'like' zijn of een opmerking.

Een node, een rondje in de beelden, is een persoon en/of organisatie binnen het netwerk. Nodes en edges vormen tezamen een social graph, een Facebook beeld. De grote van een node bepaald de 'populariteit' in het netwerk. Met allerlei berekeningen kan bepaald worden hoe populair een node is. De populariteit wordt bepaald door het aantal likes, maar ook door de mate van activiteit door het versturen van berichten of het krijgen van berichten.

NSA program stopped no terror attacks says white house panel
http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588

Is the NSA´s data snooping actually effective
http://theweek.com/article/index/254401/is-the-nsas-data-snooping-actually-effective

NSA review panel senate phone data terrorism
http://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism

Review finds NSA metadatacollection hasn´t stopped an attack
http://america.aljazeera.com/articles/2014/1/13/review-finds-nsametadatacollectionhasntstoppedanattack.html

Facebook, het ultieme inlichtingenbedrijf

Je kan Facebook vergelijken met de *people's secret service*. Want hoe je het wendt of keert, uiteindelijk zijn het de internetgebruikers die vrijwillig hun persoonlijke leven prijsgeven aan het commerciële bedrijfsleven en de overheid.

In het voorafgaande artikel 'Met de billen bloot op Facebook', over Facebook *profiling*, gaat het vooral over netwerken waarin mensen zich bevinden. *Profiling* bestaat echter niet alleen uit netwerkanalyse, maar ook uit identificatie-analyse. Wie de profielen van Margriet, Barbara en Laurens bekijkt, krijgt niet alleen de beschikking over veel informatie met betrekking tot familie, vrienden, kennissen, heden en verleden, maar ook voorkeuren.

Facebook fungeert als een soort inlichtingendienst. Het verzamelt informatie die mensen zelf aanleveren. Het lijkt anders dan het persoonsdossier van de inlichtingendienst die bestaat uit krantenartikelen, mediaoptredens, twitterberichten, Facebook postings, vergadernotulen, observatieverslagen en telefoon-/internettaps.

Verzamelwoede

Wie echter inzoomt op de Facebook-data constateert dat het commerciële internetbedrijf dezelfde data beheert die inlichtingendiensten proberen te verzamelen. Informatie die betrekking heeft op persoonlijke voorkeuren, relaties, contacten en netwerken. Het verschil met inlichtingendiensten is dat Facebook niets hoeft te doen voor die dataverzameling. Zij stelt een gratis dienst ter beschikking. Gratis betekent in dit geval natuurlijk niet voor niets. Daarbij gaat het bij Facebook allang niet meer om de advertenties die je moet tolereren.

Het Facebook-beeld van de drie aan ons visualisatie-/analyseproject deelnemende activisten geeft een aantal zaken weer, waar inlichtingendiensten ook constant naar op zoeken zijn. Wie zijn je vrienden (op Facebook), bij welke actiegroepen en politieke partijen ben je aangesloten en voor welke demonstraties en acties heb je sympathie. *Likes* spelen daarbij natuurlijk een rol, maar het gaat ook om de interactie en de berichten die gekoppeld zijn aan die politieke voorkeuren.

Met de *subscribe* knop kan Facebook waarde koppelen aan verschillende persoonlijke relaties die je hebt. De relaties en voorkeuren leggen je sociale leven bloot. Naar welke

muziek luister je graag, welke boeken lees je en hoe (e-book of papier), favoriete tv-series, de sport die je beoefent, de games die je speelt als je je even verveelt.

Dit is geen persoonlijke informatie die Facebook aan mensen ontfutselt. Het is geen inlichtingendienst die je bibliotheekgegevens opvraagt om te weten welk boek je hebt geleend. Mensen leveren Facebook al hun data aan, vrijwillig zonder dwang. Hooguit kun je spreken van groepsdruk, druk van het argument 'iedereen gebruikt het'.

De kennis van het bedrijf over je sociale leven strekt zich uit van je voornaam, achternaam, geboortedatum en leeftijd tot aan je afkomst, je gezicht (scan), zeg maar je GBA (Gemeentelijke Basis Administratie) gegevens. Maar Facebook beschikt ook over gegevens betreffende je basisschool, middelbare school en hoger onderwijs (DUO Dienst Uitvoering Onderwijs gegevens), tot aan je seksuele oriëntatie (GGD gegevens in verband met inentingen en tests op HIV en andere seksueel overdraagbare ziekten), je huidige en voormalig werkgevers (UWV en DWI gegevens), partner en ex-partners (GBA gegevens), creditcard gegevens (banken/ en creditcard bedrijven), fysieke locatie (telefoonmaatschappijen en internetproviders). Gegevens die overheidsdiensten bij allerlei instanties moeten opvragen.

Duistere achterkant

Mensen delen veel en Facebook vraagt ook regelmatig om je profiel volledig in te vullen. Inlichtingendiensten kloppen bij al die instanties aan, of proberen direct en constant toegang tot deze data te verkrijgen. Aan de achterkant weet je eigenlijk niet wat Facebook met die data doet. Advertenties koppelen aan je profiel is de meest opvallende, maar die achterkant blijft duister.

Met de onthullingen van Edward Snowden over datastofzuiger de National Security Agency (NSA), is duidelijk geworden dat multinationals zoals Facebook, maar ook Google, Microsoft en Apple hun achterdeur voor de inlichtingendienst(en) open zetten. Het Amerikaanse blad *Mother Jones* kopte in december 2013: '*Where Does Facebook Stop and the NSA Begin?*'

Toch is deze weergave niet helemaal correct. Het lijkt eerder op de omgekeerde wereld. 'Waar stoppen de inlichtingendiensten en gaat het bedrijf Facebook verder?' Dit zit niet in de interacties tussen je vrienden op Facebook of met groepen; Facebook wil veel meer van je weten en of je nu ingelogd bent of niet, het bedrijf zorgt ervoor dat ze op

de hoogte is van wat er in je leven gebeurt.

Eind oktober 2013 vertelde analist Ken Rudin van Facebook dat het bedrijf testen uitvoert om cursorbewegingen van individuele burgers op Facebook vast te leggen en te analyseren. Het gaat hierbij om het vastleggen van bewegingen met de muis naar locaties op het scherm om vervolgens daaruit af te kunnen leiden wat de interesse is van de afzonderlijke gebruikers.

De analist beweerde dat dit van doen heeft met het plaatsen van advertenties, maar uiteindelijk heeft het te maken met het profileren van de gebruikers. Zo kan Facebook namelijk ook zien of de persoon tijdens het gebruik van het sociale medium naar zijn telefoon of computerscherm kijkt, hoe lang, wanneer en wat. Allemaal nog wel gerelateerd aan de website van het bedrijf, maar met aanvullende functies als de sport applicatie pedometer kan Facebook vastleggen hoe lang, waar en wanneer je hebt hardgelopen of gewandeld.

Het duurt niet lang meer voordat het bedrijf je algehele conditie heeft doorgrond als aanvullende applicaties over bloeddruk en hartslag beschikbaar worden gesteld. Zo ontwikkelt Google een slimme contactlens voor diabetes patiënten en investeert zij in bedrijven die zicht bezig houden met diabetes. Allemaal gratis natuurlijk. Of is het niet gratis?

Rijkdom aan informatie

Facebook wil graag toegang tot de microfoon van je computer, headset of telefoon en dringt daarmee door tot in je huiskamer waar je, misschien zonder Facebook, naar muziek luistert die de private inlichtingendienst dan kan horen en toevoegen aan het profiel van jou. Hoe iemand zich voelt komt zo binnen bereik van het bedrijf. Want zelfs als je een andere naam, adres, geboortedatum en andere zaken opgeeft, volgt het bedrijf je. Het legt het apparaat vast waarmee je op Facebook bent ingelogd, met bijbehorend ip-adres, maar ook je locatie, tijdzone, datum en tijdstip.

Ook al vermijdt je te *liken,* het private bedrijf volgt je stappen langs de *'events'* en *'checkins'*, de websites die je bezoekt zodra je geobserveerd wordt door Facebook. Zo kan het bedrijf kennis nemen van jouw favoriete café's, restaurants, gerechten en recepten. Het inlichtingenbedrijf legt vast welke mensen je regelmatig bezoekt, op welke locaties je fotografeert en filmt, met wie je chat en welke groepen je in de gaten houdt.

Foto's en films die worden toegevoegd aan Facebook bevatten een rijke verzameling aan extra gegevens, zoals met welk apparaat ze zijn gemaakt, sluitertijd en diafragma, locatie, auteur, tijd etc. En van de chats en berichten bewaart Facebook ook de uitgewiste stukken tekst. Je wilt een vriend schrijven dat hij een 'eikel' is, maar wist dat vervolgens uit omdat je je vriendschap ermee niet op het spel wilt zetten. Je stuurt deze vriend een berichtje dat je geen tijd hebt dit weekend. Facebook weet zo meer over jouw relatie met die vriend, dan die vriend zelf.

Bij dit alles moet worden aangetekend dat je ingelogd moet zijn op 'jouw' Facebook-pagina en dat je bepaalde applicaties hebt geïnstalleerd en aan hebt staan, zoals GPS voor je plaatsbepaling en de pedometer voor je hardloop *tracking*. Met de gezichtsherkenning kunnen mensen die onzichtbaar willen zijn door Facebook uit de duisternis worden getrokken. Niet door het bedrijf zelf, maar door haar medewerkers, de gebruikers van Facebook. Wie gaat er echter zo bewust mee om? En vooral: wie staat er bij stil dat jouw identiteit altijd gekoppeld is aan die van anderen?

In die zin is Facebook de ultieme inlichtingendienst. Het bedrijf is de *people's secret service*, wat zoveel inhoudt dat de individuele gebruikers het werk als medewerkers van de geheime dienst vervullen voor henzelf en voor anderen. De Stasi zou haar vingers erbij aflikken, vandaar dat inlichtingendiensten als de NSA graag toegang hebben tot de achterkant van Facebook, het bedrijf zal de vergaarde informatie ook zonder blikken of blozen vrijgeven.

Steun overheid van belang

Het vrijgeven van vergaarde persoonlijke informatie aan inlichtingendiensten heeft met verschillende aspecten te maken. Ten eerste zijn grote internationaal opererende bedrijven afhankelijker van hun 'nationale regering' dan ze zelf zullen toegeven. Zo onderhoudt Shell innige relaties met zowel de Nederlandse als de Britse regering om haar operaties in het buitenland veilig te stellen. Als er ergens iets misgaat wordt zowel het diplomatieke als het militaire apparaat van het 'thuisland' gemobiliseerd.

Amerikaanse bedrijven als Facebook en Google zullen dat ook doen. Als Gmail (Google) wordt gehackt zal het bedrijf de Amerikaanse overheid over haar schouder laten meekijken, maar diezelfde overheid zal langs diplomatieke, en zo nodig langs militaire (in dit geval waarschijnlijk cyber-militaire) weg,

het bedrijf ondersteunen. Dat is natuurlijk niet vreemd, Google is een groot bedrijf en van belang voor de Amerikaanse economie en hegemonie.

Hetzelfde geldt voor Facebook waarvan diverse accounts begin 2013 werden gehackt. De Amerikaanse overheid zal vaak worden gevraagd om 'officieel' te reageren om in veel gevallen de Chinezen terecht te wijzen. Die steun van de Amerikaanse overheid is echter ook niet gratis. Zij zal druk op de bedrijven uitoefenen om de achterdeur voor inlichtingendiensten als de NSA, maar ook de FBI, open te houden. Je kunt bijna spreken van public private partnership waarbij multinationals vaak niet voor de overheidsdiensten hoeven te betalen.

Daarnaast proberen overheden een zo fijnmazig netwerk te creëren van diplomatieke posten en ambassades om hun land in het buitenland te promoten. Die posten hebben ook een andere functie. De onthullingen van Snowden hebben onderstreept dat de Amerikanen en bevriende naties als Canada, Australië, Groot-Brittannië en Nieuw Zeeland die diplomatieke posten gebruiken om in de gehele wereld de mogelijkheid te hebben om af te luisteren.

Werknemers van internationale bedrijven die wereldwijd opereren, zullen regelmatig gevraagd worden bij te dragen aan de inlichtingenoperatie van die overheid. Zij zitten vaak op andere plaatsen dan de diplomaten die vaak onder een vergrootglas in het buitenland opereren. Landen proberen dus hun zicht op het buitenland, de concurrenten en de vijanden zo scherp mogelijk te krijgen. Hoe meer diplomatieke posten en meewerkende bedrijven hoe scherper het beeld. Facebook probeert eigenlijk hetzelfde te doen met de data die zij van haar gebruikers verzamelt en analyseert. Hoe meer data, hoe scherper de analyses en hoe meer zicht op de verbanden en de interacties, hoe helderder het beeld.

In de loop der jaren heeft Facebook het aantal pixels (punten) van de foto van de profielen vergroot. Uiteindelijk werkt zij aan een haarscherp beeld van het profiel van haar gebruikers. Facebook realiseert dit zelf ook. Op 12 november 2013 diende het bedrijf een patent aanvraag in, de '*178th patent application for a consumer profiling technique the company calls inferring household income for users of a social networking system*' (Facebook Future Plans for Data Collection Beyond All Imagination, 4 december 2013).

Deze aanvraag omschrijft de hoeveelheid en diversiteit van de data. Facebook heeft sinds oktober 2013 1,189,000,000 actieve

gebruikers in de gehele wereld. Die data gebruikt het bedrijf nu al voor sociaal wetenschappelijk onderzoek door het Data Science Team van het bedrijf. Dit team doet niet alleen onderzoek naar de data, maar gebruikt de gebruikers ook als onderzoeksmateriaal, zoals het onderzoek van Eytan Bakshy die de toegang tot materiaal van 250 miljoen gebruikers manipuleerde. De gebruikers als proefpersonen in de ideale wereld van Facebook.

Gewoon een bedrijf

Uiteindelijk is Facebook natuurlijk geen gratis dienst. In eerste instantie zal het vooral proberen geld te verdienen door de verkoop van gebruikersprofielen ten bate van gerichte advertenties. De volgende stap heeft het bedrijf al gezet door de voorwaarden die ze stelt voor het aanmaken van een Facebook-pagina. Foto's en films zijn in principe niet meer je eigendom. Het bedrijf kan die foto's rechtenvrij gebruiken. Dit geldt natuurlijk ook voor Instagram. Andere bedrijven als Twitter (Twitpic's) doen hetzelfde.

Wat geldt voor foto's en films geldt natuurlijk ook voor teksten en andere content die je aan je pagina toevoegt. Voor deze zeer positieve voorwaarden is het bedrijf natuurlijk ook afhankelijk van de Amerikaanse overheid. Mocht wetgeving plotseling veranderen en gebruikers geld van Facebook eisen, zou dat voor het bedrijf een ramp zijn.

Afgaande op de totale omvang van de gebruikers, bijna evenveel als China inwoners heeft, en data die het bedrijf heeft verzameld en beheert, zou je bijna vergeten dat het gewoon een bedrijf is met 6.818 werknemers, een raad van bestuur en aandeelhouders die uiteindelijk graag hun inleg en winst terug willen zien.

De raad van bestuur geeft inzicht op welke plek Facebook in de markt staat. De verschillende leden zijn uit allerlei windstreken gerekruteerd. Natuurlijk Google Inc., Microsoft Corp. en haar dochter Skype, eBay Inc. en andere technologiebedrijven, maar ook entertainment bedrijven als Netflix en Walt Disney Co. Alsmede enkele banken, zoals Morgan Stanley & Co. LLC en Credit Suisse, maar ook The World Bank Group.

Contacten met de politiek zijn ook van belang, dat vindt plaats via oud-leden van de White House Chief of Staff of de US Department of The Treasury. En tot slot natuurlijk de ouderwetse consumentenmarkt zoals General Motors Corp. en Starbucks. Met een klein aantal leden van de raad van bestuur

dekt Facebook haar contacten in verleden en heden af. Uiteindelijk is en blijft het gewoon een bedrijf, misschien wel een private inlichtingendienst, maar zonder winst zullen op een gegeven moment de aandeelhouders weglopen en valt het om.

Alternatieven?

Wat er met de vergaarde persoonlijke data gebeurt zodra het bedrijf failliet gaat, is onduidelijk. De overname van Whatsapp door Facebook liet zien dat gebruikers zich plots beducht waren voor hun persoonlijke informatie en op zoek gingen naar 'alternatieven'.

Aan de bestaande alternatieven kleven eigenlijk dezelfde bezwaren als aan Facebook. Google Hangouts maakt onderdeel uit van een andere multinational, net als Imessenger. Bij Telegram werd geroepen dat het een Russische app is, maar waarom dat slechter is dan een Amerikaanse Whatsapp, los van de technische mankementen, blijft onduidelijk.

Uiteindelijk gaat het niet meer om een discussie over privacy, burgerrechten en/of bigdata. Facebook verzamelt namelijk niet zelf de data, zij verkrijgt het van haar gebruikers/agenten en die staan de persoonsgebonden informatie geheel vrijwillig af. Los van groepsdruk is er geen sprake van drang en dwang.

De Facebook inlichtingendienst stelt indirect solidariteit en de minderheid centraal. Hoe solidair zijn wij met mensen die misschien wel op de foto willen maar niet *getagd* wllen worden. Die wel iets schrijven maar niet *geliked* willen worden. Die wel op de foto willen maar zich niet op Facebook geplaatst willen zien. Het debat rond Facebook gaat ook over pluriformiteit versus uniformiteit. Over allemaal hetzelfde, Facebook, of iedereen iets anders.

Observant 65, 30 juni 2014

Facebook registreert in meer of mindere mate het volgende van jou:

Je cursor bewegingen, geo-locatie, meta-data van foto's en films (type, sluitertijd, geo-locatie indien gps aanstaat, auteur), biometrische gegevens (scan van het gezicht, matched zeer goed), chat gegevens en tekst die je zelfs niet verstuurd hebt, *likes*, vrienden, politieke kleur, seksuele oriëntatie, school, afkomst, ip-adressen van ingelogd zijn, wanneer je op je scherm van de smart device kijkt, welke *smart devices* waarmee je op Facebook bent, wanneer je achter de computer zit, hoelang je achter de computer zit, leeftijd, voormalige werkgevers en huidige, partner, familie, vrienden, ex-vriendinnen, muziek, boeken, films, series, games, sport, interacties tussen alle vrienden groepen, welke websites je bezoekt als je ingelogd bent, welke content je bekijkt op Facebook zelf, andere biometrische gegevens (zoals stappen, algehele conditie met sport applicaties).

What Facebook knows
www.technologyreview.com/featuredstory/428150/what-Facebook-knows/

Facebook's Future Plans for Data Collection Beyond All Imagination
www.alternet.org/civil-liberties/how-Facebooks-applications-patents-give-away-its-designs-profiting-our-behavior

How Facebook Uses Your Data to Target Ads, Even Offline
lifehacker.com/5994380/how-Facebook-uses-your-data-to-target-ads-even-offline

What Facebook Collects and Shares
www.mysecurecyberspace.com/articles/features/what-facebook-collects-and-shares.html

Report: Facebook Is Collecting Data on Your Cursor Movements
mashable.com/2013/10/30/Facebook-data-cursor-movements/

Your Facebook Data File: Everything You Never Wanted Anyone to Know
searchenginewatch.com/article/2114059/Your-Facebook-Data-File-Everything-You-Never-Wanted-Anyone-to-Know

Who Owns Photos and Videos Posted on Facebook, Instagram or Twitter?
www.nyccounsel.com/business-blogs-websites/who-owns-photos-and-videos-posted-on-Facebook-or-twitter/

Where Does Facebook Stop and the NSA Begin?
webcache.googleusercontent.com/search?q=cache:aUXOidL3e-gJ:www.motherjones.com/media/2013/10/facebook-personal-data-online-privacy-social-norm+&cd=1&hl=nl&ct=clnk&gl=nl&client=opera

Facebook Tests Software to Track Your Cursor on Screen
http://blogs.wsj.com/cio/2013/10/30/Facebook-considers-vast-increase-in-data-collection/

Google zoekt met je mee...

Een hoteltje boeken op internet, reuze eenvoudig. Maar besef wel dat je met Google een spoor aan informatie achterlaat waar het bedrijfsleven en inlichtingendiensten wel oren naar hebben.

Pieter Bindt en Gea Wind willen hun relatie bezegelen met een weekendje weg in Nederland. Ze twijfelen lang over de bestemming, maar besluiten toch naar Limburg te gaan. Ergens in Valkenburg moet toch wel een stiekem hotelletje te vinden zijn. Voor het zoeken op internet maken ze gebruik van Google, al beseffen ze dat dit sporen nalaat. Dus maken ze tijdelijke nep-mailadressen aan.

Bindt, werkzaam voor de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), weet uit ervaring dat Ronald Plasterk ooit een email heeft aangemaakt onder de naam ronaldplasterk@gmail.com. Pieter Bindt krijg gevoelige informatie over de ministers meteen door van zijn medewerkers. Hij mag Plasterk niet echt, een omhoog gevallen professor, zo noemt hij hem binnen de muren van de MIVD.

Hij besluit voor het vinden van een hotelletje dan ook het mailadres ronaldhaplasterk@gmail.com aan te maken. Mochten er bepaalde diensten achter komen dat zich allerlei buitenechtelijke relaties binnen de wereld van de geheime diensten in Den Haag afspelen, dan moeten ze eerst maar eens uitzoeken dat ronaldhaplasterk@gmail.com niet aan de minister toebehoort.

Ook Gea Wind maakt zich zorgen over haar sporen op internet. Ze heeft een vreselijke hekel aan Jeanine Hennis Plasschaert, minister van Defensie. Ze verdenkt de baas van haar minnaar ervan dat zij een oogje op Pieter heeft. Haar jongens van de Team High Tech Crime (THTC) houden Plasschaert scherp in de gaten, helemaal sinds ze een mailadres bij riseup heeft aangemaakt (jeanine-hennis-plasschaert@riseup.org).

Riseup is volgens de THTC een bijenkorf voor linkse activisten en Jeanine was in het Europees Parlement een groot voorstander van privacy. Een en een is twee, zo heeft het team van THTC (Team High Tech Crime) bedacht. Gea Wind weet ook dat Plasschaert door Pieter met fluwelen handschoenen wordt aangepakt, hij vindt haar te leuk. Zij wil Jeanine een hak zetten en maakt het mailadres jeanine-hennis-plasschaert@gmail.com aan.

Gea en Pieter weten namelijk dat Google al hun zoektermen bewaart en tevens de data van gebruikte mailadressen scant. Google zegt dat het voor advertentiedoeleinden is, maar onze tortelduifjes weten uit eigen ervaring dat advertenties slechts een van de redenen vormt. Ook de Amerikaanse geheime dienst NSA en andere diensten willen graag meekijken en voor wat centen doet Google daar graag aan mee.

Zodra Pieter is ingelogd met zijn nieuwe ronaldhaplasterk@gmail.com mailadres en ook nog eens van Google gebruik maakt, is alles aan elkaar gekoppeld. Gea zou aanvankelijk de boeking doen, maar besluit niet te reserveren en ook geen aanbetaling over te maken. Ze zoekt met Google zonder in te loggen met het door haar aangemaakte jeanine-hennis-plasschaert@gmail.com mailadres. Internetgebruik laat digitale sporen achter en zoeken met Google zeker.

Bij hun laatste ontmoeting hebben Pieter en Gea enkele zoektermen afgesproken. 'Hotel Limburg', 'hotel Valkenburg' en enkele andere termen waren bij hen opgekomen en ze zouden kijken of er een discrete plek te vinden zou zijn. Zoeken met Google laat echter allerlei sporen achter. Niet alleen de zoektermen, maar ook de resultaten. Die kunnen voor Pieter en Gea verschillen, afhankelijk van hun zoekgeschiedenis.

Pieter komt regelmatig in Limburg. Hij bezoekt dan de NAVO-basis Geilenkirchen net over de grens voor overleg met de VS. Jeanine gaat soms mee. Het zijn vaak lange dagen en Pieter wil dan het liefst overnachten in de buurt, dat scheelt reistijd en is hij wakker genoeg om erop toe te zien wat de Amerikanen er doorheen proberen te drukken. Hij heeft zo zijn vaste logeeradressen, gevonden met Google, maar wil niet dat Gea met hem daar naartoe gaat. Andere zaken zouden dan misschien wel aan het licht komen.

Zijn zoektocht op internet naar een nieuw hotel wordt echter gestuurd door die historie. Hij beseft dat Google al veel over hem weet, maar wil zijn reizen naar Geilenkirchen en zijn uitje met Gea graag gescheiden houden. Pieter probeert dus door gebruikmaking van verschillende zoektermen andere hotelletjes te vinden dan die hij gewoonlijk bezoekt. Dit laat echter veel sporen na. Gea is voorzichtiger, zij zoekt een keer met enkele zoektermen. Hoe minder spoor hoe beter.

Als Gea zoekt op 'hotel Valkenburg' krijgt ze heel veel resultaten. Het is verleidelijk om al die websites af te struinen. Soms is er sprake van een aanbieding en dan weer ‘hotel aan de Geul’. Gea beseft dat als zij die websites aanklikt, Google dat ook weet. Uiteindelijk heeft het bedrijf

dan een overzicht van alle websites die Gea bezocht heeft, naast de lijst met resultaten die het bedrijf al vergaard heeft. Google kan dus een lijstje van mogelijke hotels samenstellen waar Gea een weekend met Pieter zal doorbrengen. Dat wil Gea zien te voorkomen en noteert enkele namen van hotels die ze tussen de resultaten aantreft.

Pieter maakt zich niet zo druk om Google. Niet alleen omdat Google op schoot zit bij de inlichtingendiensten, maar ook omdat hij Plasterk een hak wil zetten. Daarnaast is Gea misschien wel zijn minnares, maar geheim agenten en politie liggen altijd gevoelig. Hij klikt alle pagina´s van hotels in en rond Valkenburg aan om zoveel mogelijk sporen achter te laten. Wie weet komen de gegevens van Google op straat te liggen en gaat een journalist zoeken naar Plasterk in Limburg.

Observant 65, 30 juni 2014

Noot: voor de totstandkoming van dit artikel is niet gekeken naar de gegevens die Google kan verzamelen over ip-adres, locatie, het apparaat waarmee je zoekt en dergelijke. Ook Gmail is niet betrokken bij de totstandkoming van dit artikel. Je kunt je voorstellen dat zodra je ingelogd bent op Google, waardoor je bij je Google Hangout, Gmail, Google + en andere diensten van het bedrijf terecht kunt, dat de private onderneming een veelvoud aan informatie verzamelt.

AIVD benadert IT'er om hackers-informatie

Zomer vorig jaar benaderde de AIVD een IT'er met het verzoek om tegen vergoeding als informant te gaan werken op het gebied van hackers. De IT'er weigerde en doet zijn relaas omtrent zijn ontmoeting van de AIVD'er.

Op maandag 3 juni 2013, een mooie zomerdag, verliet ik het schoolgebouw waar ik werkzaam ben als IT'er. Terwijl ik naar de parkeerplaats liep, zag ik op mijn gsm dat ik een bericht had gemist afkomstig van een voor mij onbekend nummer. Ik belde terug maar kreeg geen gehoor. Enkele minuten later werd ik gebeld door de persoon met hetzelfde nummer en ik nam op. Er klonk een man met een Haags accent aan de andere kant van de lijn die mij gevonden had via internet. Voor het gemak noem ik hem 'Pieter'.

Het gesprek verliep normaal, Pieter wilde een afspraak met mij maken om het te hebben over "webbeveiliging en dat soort dingen...". Prima dacht ik, dat is juist mijn ding. We spraken enkele dagen later af in een koffiebar in mijn woonplaats. Intussen bereidde ik me voor op het gesprek. Uiteraard heb ik enkele websites ontworpen en gebouwd, maar weinig ervaring met legale penetratietesten. Vandaar dat ik een 'collega', genaamd Edwin, om hulp vroeg. Achteraf gezien was dit allemaal verspilde moeite.

Tevens zocht ik op internet op wie de man uit Den Haag nu eigenlijk was die ik zou gaan ontmoeten. Tot mijn verbazing was er eigenlijk niets opmerkelijks over hem te vinden. Op de dag van de afspraak arriveerde ik bij de koffiebar maar was tien minuten te vroeg. Ik bleef netjes in mijn auto wachten en enkele minuten later zag ik een oude man die stond te telefoneren. Op dat moment ging mijn telefoon over, het was Pieter. Ik ben naar de man toegelopen, hebben elkaar de hand geschud en namen plaats buiten op het terras.

Mijn eerste vraag aan Pieter was natuurlijk wie hij dan wel niet was. "Waar denk je dat ik van ben?", vroeg hij mij. Op dat moment kreeg ik een vervelend onderbuikgevoel. Daarop zei ik dat ik geen idee had voor welk bedrijf hij werkzaam zou moeten zijn. "Ik ben van de AIVD", antwoordde hij. Pieter maakte vervolgens zijn tas open waaruit hij zijn id-pasjes tevoorschijn haalde: eentje van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en een AIVD-toegangspas, althans, zo meen ik gezien te hebben.

Daar zat ik dan, tegenover een medewerker van de AIVD. Voor

mij was dit een verrassing. Ik probeerde het gesprek te vervolgen door hem te vragen waarom hij mij wilde spreken en uiteraard waarover. Het eerste wat in mijn op kwam was de zaak omtrent hacker Sven Olaf Kamphuis, die kort daarvoor gearresteerd was in Spanje voor 'de grootste aanval in de geschiedenis van het internet', en wel op spambestrijder Spamhaus. Pieter wilde het hebben over mijn visie op de DDoS-aanvallen van vitale systemen (DigiD/banken) destijds. Ik heb Pieter verteld hoe ik daarover dacht, dat het wellicht een afleidingsmanoeuvre zou kunnen zijn geweest voor een hack of iets dergelijks. Hier hebben we een hele tijd over zitten praten.

Pieter deed alsof hij maar weinig verstand had van het hele internetgebeuren. Hij merkte op een boek te hebben gelezen over computerbegrippen zodat hij alles een beetje kon volgen. Uiteraard is dit natuurlijk wel opmerkelijk, want waarom zou de AIVD iemand sturen die totaal niets van computers af weet? Waarom zou de AIVD uitgerekend Pieter langs sturen om met mij, een IT'er, te praten? Na nog een aantal keer aan Pieter te hebben gevraagd waarom hij bij mij terecht gekomen was, zei hij dat hij had gezien dat ik het op Twitter vaak op had genomen voor Sven Olaf Kamphuis. Sven, die inmiddels uitgeleverd was aan Nederland. Interessant.

Ik heb Pieter daarop uitgelegd dat Sven naar mijn weten niets met de DDoS-aanvallen te maken zou hebben gehad. Dat deze Spamhaus-aanvallen een actie van een paar gekke Russen, Chinezen en mensen uit Engeland zouden moeten zijn geweest en dat Sven hier niks aan kon doen. Zover ik wist had Stophaus, een groep mensen gericht tegen Spamhaus, via een illegale manier hun 'probleem' met Spamhaus op hebben willen lossen door DDoS aanvallen uit te voeren. Klaarblijkelijk heb ik met deze mensen gechat, mensen die inmiddels veelal van het internet verdwenen zijn.

Pieter heeft mij dus (deels?) benaderd vanwege mijn connectie met deze mensen en door mijn connectie met Sven. Tijdens zijn verhoor kreeg Sven van de rechercheurs, in dienst van Team High Tech Crime en Fox-IT, de vraag voorgelegd of hij 'Goo' kende, het IT-bedrijf waar ik voor werk. Verder natuurlijk totaal irrelevant omdat ik niets te maken heb gehad met de DDOS-aanvallen. Maar wat moest ik hier dan wél van denken? Geen idee. Ik heb Pieter meerdere malen doorverwezen naar personen als Ronald Prins of ex-boefje Rickey Gevers, die ook veel over cybercrime afweten. Dat beweren ze althans (knipoog), maar helaas, Pieter wilde iemand hebben die in zijn ogen toch wat meer over het wereldje zou weten. Het wereldje van kwaadwillende hackers.

Het gesprek verliep na enige tijd nogal moeizaam omdat ik verder niet veel wist te vertellen. Hierop stuurde Pieter het gesprek richting het einde en wilde graag nog een vervolgafspraak maken om mijn visie over wat andere onderwerpen aan te horen. Dit eventueel tegen betaling. Volgens Pieter was tijd immers geld en heeft de AIVD daar "een budget voor." Ik zei dat ik er nog over na zou denken, omdat ik op dat moment nogal verbaasd was vanwege het feit dat de AIVD mij als een soort informant zag.

Een week later heb ik de AIVD opgebeld om te checken of er wel een Pieter werkzaam is. Dit was het geval en ik werd doorverbonden. Telefonisch heb ik hem kenbaar gemaakt dat ik geen behoefte heb om informantje te gaan zitten spelen en dat ze toch echt beter bij de echte cybercrime-deskundigen zoals Ronald Prins- en Rickey Gevers aan kunnen kloppen voor de nodige informatie/visie op bepaalde (cruciale) zaken.

Er verstreek vervolgens een maand waarna ik toch weer werd gebeld door Pieter. Hij probeerde mij opnieuw over te halen, maar ik bedankte nogmaals. Wellicht had ik dan nog wel interesse in een gesprek over de vraag waarom ik geen informant wilde zijn? Nou, nee. Heb Pieter zijn aanbod vriendelijk afgeslagen. Hierop wenste de AIVD'er mij veel succes in de toekomst en zei op een vervelende toon dat we elkaar wellicht nog wel eens een keer tegen zouden komen. Nou Pieter, ik wens jou ook veel succes toe.

Goo

Observant 65, 30 juni 2014
Buro Jansen & Janssen 2014

Pieter is Hans Turksma van Binnenlandse Zaken of de AIVD

Van bemiddelaar tot doelwit AIVD

Doe je iets positiefs voor de samenleving, is de beloning aandacht van de inlichtingendienst. Een kraker benaderen die de overheid al eens eerder geholpen heeft, voelt aan als een trap na.

Dit overkwam 'Kees' die in Bilthoven bemiddelde tussen enkele krakers en de overheid. Tot zover niets aan de hand. De politie die in de gemeente De Bilt normaal gesproken zich coöperatief opstelt, was nu in rep en roer in verband met het aanwezige asbest in het voormalige hotel Heidepark dat die ochtend was gekraakt. Politie en brandweer kwamen op 21 april 2014 langs en het leek allemaal uit te lopen op een ontruimingsshow.

Een van de brandweermannen ter plaatse herkende Kees die in de buurt woont. De brandweerman vroeg of hij soms wilde bemiddelen. Het ging er niet om dat de krakers die binnen zaten gearresteerd werden, maar de brandweer wilde dat zij het pand verlieten en hun kleren lieten reinigen in verband met het aanwezige asbest. Hulpverleners wilden de krakers in eerste instantie zelfs geen hand geven in verband met mogelijke besmetting.

Kees kreeg de garantie dat de krakers niet zouden worden gearresteerd en dit werd bevestigd door een vrouwelijke hulpofficier die aanwezig was. Alles verliep zoals afgesproken, de overheidsdiensten hielden zich aan de afspraken en de zaak leek geregeld. Aan het einde van de dag vertrokken de krakers vrijwillig en van verspreiding van asbest was geen sprake. Kees ging naar huis en dacht dat daarmee de kous af was.

Helaas voor hem, want hij was nu plots opgevallen als een benaderbare persoon. Drie dagen later werd hij gebeld door 'Marcel van de Griend' van de RID Midden Nederland, telefoonnummer 0619627546. Marcel wilde in het geniep afspreken, zoals een echte geheim agent. Hij had het idee dat de Regionale Inlichtingendienst (RID) en Kees iets voor elkaar konden betekenen.

Kees vroeg Van de Griend waar hij dan aan dacht. Welnu, volgens hem konden de RID en Kees elkaar helpen "met betrekking tot kraken, ontruimingen en interessante panden." Op de vraag wat Kees dan zelf met het contact met de RID opschoot, kon Van de Griend niet echt antwoord geven. Het voordeel dat Kees aan het contact zou overhouden, was er eigenlijk niet.

Waarom Kees werd benaderd is niet duidelijk. De actie bij Hotel Heidepark kwam wel in het nieuws via RTV Utrecht in de vorm van een bericht op de website plus enkele foto's. De naam van Kees komt echter niet voor in het artikel. Het kan zijn dat de brandweerman of de vrouwelijke hulpofficier dit in hun verslagen hebben opgenomen, maar ook dat is niet duidelijk. Het mobiele nummer van Kees heeft Van de Griend waarschijnlijk uit de politierapportages van de wijkagent.

Kees had de betreffende wijkagent na de benadering gebeld om te checken of hij Van de Griend had ingelicht over hem. De wijkagent gaf aan dat hij wel rapportages had geschreven over bezoeken aan het pand waar Kees woont, met zijn naam en telefoonnummer als contactpersoon. "Wellicht hebben ze in het systeem naar 'kraken' gezocht en dan komen die rapportages ook naar voren", vertelde de wijkagent aan Kees. Hij had zelf niet de RID op Kees afgestuurd, want daarmee zou hij "zijn eigen ruiten ingooien", voegde hij eraan toe.

Het verhaal van de wijkagent kan kloppen aangezien het contact tussen Kees en hem goed is. De inlichtingendienst op iemand afsturen is natuurlijk niet positief, want daarmee probeer je iemand zijn collega-krakers te verlinken. Het moet namelijk allemaal in het "geniep", zoals Marcel van de Griend aan de telefoon aangaf. Een beetje netjes met burgers omgaan, komt in het vocabulaire van inlichtingendiensten niet voor. Kees heeft enkele dagen na het telefoontje van Marcel van de Griend gebeld met de mededeling dat hij van verder contact afzag.

Observant 65, 30 juni 2014

Het is onduidelijk of de naam Marcel van de Griend de echte naam van de RID'er is, Kees is een fictieve naam.

Boekrecensie: The Way of the Knife

Na de Koude Oorlog heeft de Amerikaanse geheime dienst CIA zich weer toegelegd op het uitvoeren van doodseskaders. In '*The Way of the Knife*' wordt uit de doeken gedaan hoe de CIA wereldwijd oorlog voert.

In het boek '*The way of the knife*' loopt Mark Mazzetti, correspondent voor *The New York Times*, zeer vlot door de recente geschiedenis van de CIA en doet dat soms zo snel dat een pagina een aantal keer herlezen moet worden. Hij laat zien welke impact 9/11 heeft gehad en nog steeds heeft op het functioneren van de CIA. Het opmerkelijkste van het boek is dat het een menselijk en soms aandoenlijke ruzies laat zien binnen deze geheime (blijkbaar niet zo'n goed geoliede) wereld.

De politieke beslissingen of interpretaties van wetten die in het geheim worden genomen, komen pas echt tot leven wanneer voorbeelden worden opgevoerd. Op een zorgwekkende manier wordt omschreven dat Amerika in oorlog is met bepaalde 'terroristen', en niet enkel met landen. Hetgeen Amerika naar eigen interpretatie carte blanche geeft om elk willekeurig land ter wereld binnen te vallen wanneer zij dat nodig acht.

License to Kill

Een voorbeeld hiervan zijn de militaire drone-missies in Jemen en Pakistan. Dat zijn landen die officieel niet in oorlog zijn met Amerika. Hoewel deze missies, waarbij onbemande vliegtuigen doelwitten bombarderen, publiek geheim zijn, worden deze niet erkend of ontkend door Amerika.

Mazetti legt de vinger op de zere plek door aan te geven dat de CIA intern bijna gespleten raakte vanwege deze '*Licenses to Kill*'. De oudgedienden waren nog niet de lessen vergeten van de Koude Oorlog. Lessen over mislukte terreur-aanvallen en politieke moorden zorgden destijds voor zeer pijnlijke PR-aangelegenheden en diplomatieke trauma's. In totaal heeft dit decreet van niet-moorden ongeveer 25 jaar bestaan.

Nu, onder het toezicht van Bush en Obama, lopen de lijsten van te ter dood veroordeelde personen van in beginsel 52 op naar tienduizenden. De gehele modus operandi van 'niet-moorden' naar het opzetten van doodseskaders, wordt scherp in beeld gebracht door Mazetti. De twijfels, de mensen die uit zichzelf ontslag namen omdat zij het niet langer meer konden aanzien, de alfamannetjes die '*flies on their eyes*' (van de

'terroristen') willen zien, tot en met cowboy George Bush die het allemaal wel zag zitten.

Wie denkt dat Obama schone handen heeft, komt van een koude kermis thuis: De inzet van drones, het algehele afluisternet van de NSA, de inzet van JSOC (Joint Special Operations Command); het werd allemaal onder zijn regering uitgebouwd. En de belofte om Guantanamo Bay te sluiten? Daar zitten nog steeds 149 gedetineerden zonder uitzicht.

Blijvend trauma

Wie kent niet de beelden van Guatanamo Bay? Mensen die in het beginsel op de hitlists stonden, werden gearresteerd, gedrogeerd en via blacksites naar kamp X-RAY gebracht. Een gevangenis die leek op een uit de kluiten gewassen hondenkennel. Al met al gaf dit een PR-probleem. De beelden werden uitgezonden over de gehele wereld en tot op vandaag is er nog discussie over de resterende 149 mensen die daar gedwongen verblijven.

Drones kunnen makkelijk moeilijke gebieden penetreren om een bevolking te bespieden of om 'gericht' een aanval uit te voeren. Een bijkomend voordeel is dat het ver weg gebeurt van kritische ogen. Mazetti legt uit hoe euforisch de sfeer was in het Witte Huis toen de eerste drone-aanval in Jemen werd uitgevoerd. Het boek gaat verder over de diplomatieke uitdagingen om het drone-programma in Pakistan door te kunnen zetten door eerst met drone-aanvallen een klusje voor Pakistan te klaren. Zo wordt duidelijk dat de CIA stap voor stap weer een doodseskader van Amerika maakt.

Soms legt de auteur op vermakelijke toon uit hoe 'onsexy' de CIA de drones aanvankelijk maar vonden. Het niveau van de eerste drones was ongeveer van het kaliber *Breaking Bad*: Een camper bij de grens van Pakistan om deze drones aan te sturen, met een vertraging van vijf seconden tussen aansturing tot daadwerkelijk activeren van de drone. Hierbij speelde de bandbreedte parten, omdat de satellieten te druk bezig waren met het streamen van belangrijke sportevenementen. Zo werkt het komisch genoeg voor het grootste en meest geavanceerde technoleger ter wereld.

Mazetti's verhaalt verder over een jaloers leger dat haar eigen doodseskader heeft bestaande uit 4.000 leden, genaamd JSOC (Joint Special Operations Command). Een gebundelde vuist van alle speciale legereenheden, zoals Navy Seals en Delta Force. Met haar eigen speciale inlichtingendienst die zeer nauw en soms overlappend samenwerkt met de NSA. Dit maakt

JSOC op dit moment het grootste doodseskader dat in meer dan 115 landen opereert, en wie weet nog wel meer. Met een ongekende hoeveelheid aan '*intelligence*'.

Oorlog by Proxy

Een oude vos verliest nimmer zijn streken. Een beproefde methode van de CIA is om een oppositiepartij meer gewicht te geven door het leveren van informatie, wapens of simpel geld aan de partij waarmee zij sympathiseert. Mazetti legt vrij scherp uit hoe oorlogen, zoals in Somalië, in het voordeel van Amerika worden beslecht. Dit alles zonder dat Amerika zelf voeten aan de grond zet, of alleen haar '*birds*' laat deelnemen aan de oorlog.

'*The Way of the Knife*' is verplichte kost om inzicht te krijgen in de werkwijze van de CIA en JSOC in naam van het 'land van de vrijheid'. De onthullingen van Snowden kunnen we spiegelen aan de informatie uit dit boek. Bijvoorbeeld over de meta-data die Nederland vermoedelijk afstaat aan de Amerikanen. Meta-data is data over data, zoals wie met wie heeft gebeld, wanneer en waar.

Buro Jansen en Jansen zal deze zomer hier uitvoerig over publiceren op haar website en in nieuwsbrieven. Omdat mensen aangevallen kunnen worden door drones op basis van profielen die met behulp van deze meta-data zijn opgesteld. Wat Plasterk er van ook van probeert te maken. De NSA ontving deze meta-data en op basis hiervan zijn mensen gebombardeerd door drones.

Bij lezing van het boek bekroop mij soms het gevoel dat Mazetti voorstander is van de CIA in oude vorm, van voor de '*license to kill*' periode. Los van wellicht het romantische beeld dat Mazetti ophoudt van die tijd, geeft het boek goed weer hoe de CIA momenteel op wereldwijd niveau oorlog voert. In ruim 300 bladzijdes wordt beschreven hoe a-symetrische oorlogen in deze tijd worden uitgevochten en belicht Mazetti de meest sinistere kanten hier van.

Maikel van Leeuwen

Observant 65, 30 juni 2014

The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth. By Mark Mazzetti Penguin Press, US ISBN 1594204802, 400pp. http://markmazzetti.net/

migratie-beleid.nl

De website migratie-beleid.nl is een nieuw initiatief van Buro Jansen & Janssen. Hierop zullen zoveel mogelijk aan migratie gerelateerde overheidsdocumenten die óf door de overheid zelf openbaar zijn gemaakt óf via de Wet Openbaarheid van Bestuur (WOB) óf de Wet Inlichtingen en Veiligheidsdiensten zijn verkregen, worden gepubliceerd.

De website is een virtuele kritische onderzoeksgroep naar migratie in Nederland en Europa. In eerste instantie zal het vooral over Nederland gaan, maar uiteindelijk zal ook het migratiebeleid in de gehele Europese Unie onder de loep worden genomen. Naast overheidsdocumenten zullen analyses, publicaties en onderzoek op de website worden gepubliceerd.

Uitgangspunt van dat onderzoek is niet alleen om aan te geven wat er nu gebeurt op het gebied van het migratiebeleid, maar tevens om parallellen te trekken met het beleid in de afgelopen decennia. Je kan zelf een bijdrage leveren aan kritisch onderzoek naar het migratiebeleid door documenten te Wobben, onderbouwde analyses te schrijven, archieven in te scannen en openbaar te maken.

Jansen & Janssen wil op deze manier een bijdrage leveren aan de discussie over het migratiebeleid in Nederland en Europa. Voor de website wordt data verzameld en geanalyseerd over onderwerpen als het Kinderpardon, de krakende vluchtelingen in Amsterdam, het zogenoemde 'etnisch profileren' door de politie, de hongerstakingen van vluchtelingen in gevangenissen en andere incidenten en gebeurtenissen. Dit ten bate voor kritische mensen die zich het lot van de vluchtende mens aantrekken.

De website borduurt voort op de rijke geschiedenis van onderzoek naar het migratiebeleid door het Autonoom Centrum uit Amsterdam. Een deel van de publicaties van die organisatie zullen op migratie-beleid.nl worden opgenomen. Een ander deel van de documenten zijn reeds op andere plekken bij Buro Jansen & Janssen te vinden. Het leek ons echter zinvol om alle aan migratie gerelateerde stukken bij elkaar te brengen op een website die de overheidsbemoeienis met vluchtelingen kritisch in beeld brengt.

U kunt bijdragen door documenten te openbaren, wobben, wiven, analyseren, duiden, in historisch perspectief te plaatsen of op een andere wijze inhoudelijk, moreel of financieel het werk van Jansen & Janssen te steunen.

Observant 65, 30 juni 2014
Buro Jansen & Janssen 2014

Donateurs gezocht

Sympathie voor het werk van Buro Jansen & Janssen? Wordt dan nu donateur.

Wordt donateur of vraag familie, vrienden en bekenden donateur te worden. Bankrekening NL56 INGB 0000 6039 04 (ING 603904 BIC: INGBNL2A) ten name van Stichting Res Publica, Postbus 11556, 1001 GN Amsterdam. Res Publica is de stichting van Jansen & Janssen.

Buro Jansen & Janssen 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.