SPIONAGE IN HET HART VAN EUROPA?

Kristof Clerix,
jounalist MO*

MO* PAPER
nummer 37 – november 2009
www.mo.be

MO*PAPER

MO*papers is een serie analyses die uitgegeven wordt door Wereldmediahuis vzw. Elke paper brengt fundamentele informatie over een tendens die de globaliserende wereld bepaalt. MO*papers worden toegankelijk en diepgaand uitgewerkt.

MO*papers worden niet in gedrukte vorm verspreid. Ze zijn gratis downloadbaar op www.mo.be. Bij het verschijnen van een nieuwe paper wordt een korte aankondiging gestuurd naar iedereen die zijn of haar e-mailadres bezorgt aan mopaper@mo.be (onderwerp: alert)

Kristof Clerix is journalist bij het maandblad MO*. Hij publiceerde in 2006 het boek Vrij spel, over buitenlandse inlichtingendiensten in België. Dat boek werd intussen ook in het Frans uitgegeven.

De tekst van deze MO*paper is ook verschenen als bijdrage in Geheime diensten, The Spy Who Loved Me, Kristof Clerix, Francis Desterbeck, Herman Matthijs, Fons Schoovaerts en Daniel Stevens, ISBN 978 90 4860 478 4, www.diekeure.be.

Informatie: mopaper@mo.be of MO*paper, Vlasfabriekstraat 11, 1060 Brussel

Suggesties: emiel.vervliet@mo.be

Wereldmediahuis is ook uitgever van het maandblad MO* en van de mondiale nieuwssite www.mo.be (i.s.m. het nieuwsagentschap IPS-Vlaanderen).

[inleiding]

'Brussel is een centrum waarin alle inlichtingendiensten geïnteresseerd zijn', zegt Alain Winants, administrateur-generaal van de Belgische Staatsveiligheid. 'Na New York en Genève is Brussel de derde stad met het grootste aantal diplomaten. Nergens anders vind je een concentratie van NAVO én Europese Unie én andere internationale instellingen. Het is evident dat Brussel alleen al daardoor een zekere aandacht genereert van buitenlandse geheime diensten.'[1]

In deze bijdrage beschrijven we de activiteiten die inlichtingendiensten uit alle hoeken van de wereld in Brussel ontplooien. Dat doen we aan de hand van spionagecases uit het afgelopen decennium: de Solana-case, de Justus Lipsius-case, de Simm-case, de Swift-case, de Batasuna-case en de ICT-case.

[1] Interview met Alain Winants op 16 juli 2009.

§ 1 De Solana-case

I. Spionage, een permanent fenomeen

'Zonder het te weten ben ik gedurende maanden bespioneerd door een niet-Europees land', vertrouwde Javier Solana op 9 juni 2009, na een lange conferentiedag in Madrid, aan enkele Spaanse journalisten toe.[1] In detail treden deed de secretaris-generaal van de Europese Raad liever niet. Spionage-affaires worden doorgaans niet aan de grote klok gehangen.

'Gezien zijn functie is het normaal Javier Solana bespioneerd wordt en de interesse weerhoudt van geheime diensten van niet-Europese landen', reageert Alexandro Legein, sinds 2000 hoofd van de veiligheidsdienst van de Europese Raad.[2] 'Is de problematiek gelimiteerd tot Solana alleen? Uiteraard niet. Alle personen die zich met materie zoals buitenlands beleid bezighouden zijn een potentieel doelwit, evenals hun assistenten. Geheime diensten ontplooien een heel panoplie aan mogelijkheden tegen hen. Zowel human intelligence als signals intelligence wordt ingezet – zowel menselijke bronnen als technologie.' In de affaire waar Solana naar verwees, ging het om signals intelligence: zijn elektronische communicatie werd onderschept. Legein: 'De aanval kon teruggetraced worden naar servers in Zuid-Oost Azië.' Volgens Legein staan Solana en co regelmatig bloot aan elektronische aanvallen van buitenaf: 'Het is een permanent fenomeen.'

[1] Solana revela que ha sido victima del espionagje cibernético de una potencia, El Pais, Miguel Gonzalez, 10.06.2009.
[2] Gebaseerd op interviews met Alexandro Legein op 18 januari 2005, 20 januari 2006 en 24 juli 2009.

II. Toenemend belang van Europese instellingen

Op zijn website – enkel toegankelijk voor de werknemers van de Europese Raad – publiceert Legein richtlijnen met veiligheidsadvies. 'Op die manier maken we onze ambtenaren bewust van de risico's. Spionage komt niet alleen voor in romans van John le Carré of Tom Clancy. In het verleden is duidelijk geworden dat ook werknemers van de Europese instellingen het doelwit kunnen zijn van inlichtingenwerk.[3] Geheime diensten zijn het er over eens dat een gewoon gesprek met werknemers een van de beste methodes is om informatie in te zamelen of dubbelchecken.'

Het secretariaat van de Europese Raad, gehuisvest in het Justus Lipsiusgebouw in Brussel, beschikt over geclassificeerde informatiesystemen die niet aan het internet gelinkt zijn en bijgevolg niet van daaruit gepenetreerd kunnen worden. Daarnaast is er een netwerk dat wél gelinkt is aan het wereldwijde web. Legein: 'Daar staat geen geclassificeerde informatie op, maar wel informatie waarmee een goede intelligence-analist een duidelijk beeld kan vormen van ontwikkelingen binnen de Europese Unie. Europese ambtenaren beseffen niet altijd wat de waarde is van de informatie waarmee zij werken. Ook stukjes van de puzzel kunnen analisten verder helpen. Daarom krijgt elke nieuwe ambtenaar bij de Europese Raad een algemene briefing waarin ook op de risico's van spionage wordt gewezen.'

Het risico op spionage is recht evenredig met het belang van de Europese instellingen in de wereld. En dat neemt steeds maar toe. Legein: 'De voorbije jaren heeft de EU zich steeds meer verantwoordelijkheden aangemeten op het gebied van veiligheidsbeleid en buitenlandpolitiek. Landen die geïnteresseerd zijn in die ontwikkelingen van de Europese Unie zullen hier automatisch inlichtingenactiviteiten ontplooien.' Concreet: sinds 2003 is de Europese Unie in het kader van het Veiligheids- en Defensiebeleid buiten haar eigen grenzen actief. Op een paar jaar tijd lanceerde de EU militaire operaties in Macedonië, Congo, Bosnië-Herzegovina, Darfur, Tsjaad en voor de kusten van Somalië. Brussel riep het Europees Defensieagentschap in het leven, stoomde snel inzetbare gevechtseenheden klaar – de zogenaamde battle groups – en zette zelfs een eigen, klein operationeel hoofdkwartier op. Op civiel vlak ontplooide de EU onder meer missies in Irak, Afghanistan, Georgië en Guinee-Bissau. Legein: 'Doordat de EU verregaand betrokken is bij crisisbeheeroperaties in het voormalige Joegoslavië, waaronder operatie Althea in de Balkan, zijn wij de facto onderhevig aan intens inlichtingenwerk van staten die geïnteresseerd zijn in de positie van de EU met betrekking tot de Balkan en de ontwikkelingen in die regio. Dat is iets wat interesse opwekt, en niet alleen bij grote landen als Rusland. De Serviërs zijn bijvoorbeeld heel geïntersseerd in wat Europa onderneemt in Kosovo. Iedereen die zich op politiek vlak bezighoudt met ontwikkelingen in de wereld, en die in de achtertuin van anderen actief wordt – zoals wij in de Balkan en Afrika doen – komt in het vizier van inlichtingendiensten die de belangen van hun land willen beschermen in die regio. Dat is bijna een axioma. De EU is aanwezig in Congo en Soedan, waar ook China strategische belangen heeft – met name tactische grondstoffen. Als je in Afrika werkt, kom je automatisch in het vizier van andere inlichtingendiensten.'

[3] Een voorbeeld: op 1 maart 2003 maakte de Franse krant Libération bekend dat de Brit Desmond Perkins, binnen de Europese Commissie bevoegd voor het versleutelen van communicatie, de cryptagesystemen had laten controleren door het Amerikaanse National Security Agency, waar een van zijn ouders werkte.

Uiteraard is ook de economische dimensie van de Europese Unie een belangrijk gegeven voor geheime diensten. 'Onderhandelingen over economische dossiers kunnen een belangrijke invloed hebben op de werkgelegenheid en het economisch welzijn van bepaalde regio's', zegt Legein. 'Voor inlichtingendiensten is het interessant om op voorhand de onderhandelingspositie van de EU te kennen. Neem nu visserijverdragen. Als je weet hoeveel potentiële jobs en investeringen daarmee verbonden zijn, begrijp je dat er tijdens onderhandelingen met grote visserijnaties zoals sommige Noord Afrikaanse ook interesse is van geheime diensten. Nationale interesses moeten verdedigd worden, en dat gebeurt ondermeer via inlichtingenwerk. Maar je moet het niet dramatiseren. Intelligence is een normaal fenomeen en je moet je daar doodgewoon tegen wapenen.'

Intelligence slaat overigens niet enkel op spionage. Legein: 'Ook beïnvloeding bestaat nog steeds. Net als tijdens de Koude Oorlog, toen je agents of influence had, proberen derde staten vandaag de gang van zaken te beïnvloeden.' Op 22 september 2008 stelde het Duitse Europarlementslid Daniel Cohn-Bendit een parlementaire vraag over de Ier Declan Ganley, multimiljonair en stichter en voorzitter van de pan-Europese partij Libertas. Tijdens het Iers referendum over het Verdrag van Lissabon in 2008 had Ganley een stevige neen-campagne gevoerd. Cohn-Bendit verwees in zijn parlementaire vraag naar artikels in de Ierse pers 'die aantoonden dat er mogelijk een link is tussen zij die de neen-campagne in Ierland financierden, het Pentagon en de CIA'.[4] Is Ganley een agent of influence voor de Verenigde Staten? Zelf ontkende hij die beschuldigingen eerder al met klem. 'Wat is het volgende? Dat ik voor de Marsmannetjes werk?' reageerde Ganley laconiek.[5]

III. Opgepast: knappe stagiaire met lange benen

In februari 2009 pakte de Frankfurter Allgemeine Zeitung uit met een interne nota van de Directie Veiligheid van de Europese Commissie.[6] 'Nieuwe gevallen tonen dat het spionage-gevaar dag na dag toeneemt', schreef diensthoofd Stephen Hutchins in die nota aan ambtenaren die zich bezig houden met human resources. Hutchins waarschuwde onder meer voor inlichtingenwerk door journalisten en lobbyisten.

De nota kreeg heel wat weerklank in de Europese pers, zeker nadat Commissie-woordvoerster Valerie Rampi er in een persbriefing nog een schepje bovenop deed: 'We wijzen niet alleen journalisten met de vinger. Het zou net zo goed kunnen gaan om de knappe stagiaire met lange benen en blonde haren.'[7] Koren op de molen van de pers. 'European officials warned of interns trading sex for secrets' kopte een grote Europese krant.[8] Hutchins nota mag dan al tot hilariteit hebben geleid, de man had natuurlijk een punt. Spionnen creëren covers waarmee ze zo onvallend mogelijk zo dicht mogelijk bij

[4] www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20080922+ITEM-017+DOC+XML+V0//EN
[5] Why impossible is nothing for the mysterious Mr No, The Sunday Times, 8 juni 2008.
[6] Der EU sind Reporter verdächtig, Michael Stabenow, Frankfurter Allgemeine Zeitung, 11 februari 2009.
[7] European Commission fears 'increasing' espionage, Philippa Runner, EU Observer, 11 februari 2009.
[8] European officials warned of 'interns trading sex for secrets, Bruno Waterfield, Telegraph.co.uk, 11 februari 2009.

hun doelwit kunnen geraken. Klassieke covers zijn journalistiek, diplomatie en lobbywerk. En uitgerekend aan die covers is er in Brussel geen gebrek.

A. Journalisten

De job van journalist en spion is vrijwel identiek: je specialiseert je in een vakgebied, legt contacten, bouwt een netwerk uit, wint informatie in en verwerkt die. Correspondenten die werken voor een persagentschap dat in handen is van een buitenlandse overheid krijgen al snel het verwijt dat ze spionnen zijn. Soms terecht, soms niet. Feit is dat een aantal journalisten die in de Europese instellingen geaccrediteerd zijn meer doen dan enkel krantenartikels schrijven.

'Tussen 1500 en 2000 journalisten komen naar de Europese toppen', zegt Legein. 'Brussel heeft het grootste perskorps van de wereld, groter dan dat van de VN in New York. Er zijn daarbij heel wat journalisten die twee man en een paardenkop vertegenwoordigen. Maar ze hebben wel een perskaart, accrediteren zich bij de Europese Commissie. Vermits ik geen kijk heb op het onderzoek door onze collega's van de Commissie op de legitimiteit van dat soort journalisten, kan ik geen risico nemen Vandaar dat we een extra screening doen van alle journalisten die de Raad bijwonen. De pers is voor mij een noodzaak, een bondgenoot. Maar ik kan me niet voorstellen dat ik een uitgever van een website die door vier man wordt gelezen als een bona-fide journalist beschouw. Ik beschouw zo iemand als een potentieel gevaar voor de goede orde op een topbijeenkomst van Europese staatsleiders . Dit is ten andere duidelijk gebleken toen mijn diensten een extreem nationalistische Russische "journalist" – waarover wij inlichtingen hadden ontvangen – weerden op een EU-Rusland top. Diezelfde kerel bekogelde in Praag, op een bijeenkomst van de NATO, de toenmalige Secretaris Generaal Lord Robertson met tomaten op het einde van een persconferentie.'

B. Lobbyisten

Naar schatting 15.000 tot 20.000 lobbyisten lopen de deuren plat van europarlementsleden en Europees commissarissen om hen te verleiden met viergangendiners, voetbaltickets, design citruspersen en voorgekauwde informatie.[9] Vooral bij de Commissie, die belangrijke beslissingen neemt over de vrijmaking van de interne markt en de normering van producten, wordt flink wat gelobbyd. Maar volgens de Staatsveiligheid zijn niet alle lobbyisten even onschuldig als ze zich voordoen: 'Een aantal buitenlandse inlichtingendiensten lobbyen bij het Europees Parlement. Parlementsleden zijn een prachtig doelwit voor inlichtingendiensten om de agenda van hun overheid aan op te dringen. Misschien moeten zij daarover beter gesensibiliseerd worden. Zien parlementsleden wel dat achter lobbyactiviteiten de agenda van nationale overheden kan schuilgaan en niet enkel van bonafide vzw's? Er is zeker een link tussen lobbyisten en geheime diensten. Ik ga geen namen van landen noemen. Maar denk gewoon aan welke landen geïnteresseerd kunnen zijn in de verschillende werkgroepen binnen het Europees Parlement en de Commissie, van Azië over Kosovo tot Congo. Zodra een standpunt moet worden ingenomen, beginnen landen te lobbyen. Neem nu de lijst met terroristische organisaties die de EU opstelt. Als daarover beslissingen genomen moeten worden, zullen buitenlandse inlichtingendiensten gaan lobbyen.'[10]

[9] Lobbyisten in Brussel: makelaars in macht, Sara Frederix, MO*, april 2003.
[10] Interview met een medewerker van de Staatsveiligheid die anoniem wenst te blijven.

C. Diplomaten

Ook diplomatie is een klassieke cover voor inlichtingenwerk. Het diplomatiek statuut biedt immers een aantal voordelen. Zo kan een diplomaat niet strafrechterlijk vervolgd worden in de ontvangststaat, ook niet voor spionage. Wanneer een diplomaat toch over de schreef gaat, kan hij in het ergste geval persona non grata verklaard worden. Een ander voordeel is dat een diplomaat vaak makkelijk deuren kunnen openen. Figuurlijk maar ook letterlijk. In het Europees parlement krijgen diplomaten van niet-EU-lidstaten een pasje dat toegang geeft tot het volledige Europees parlement. 'En als je toegang hebt tot het parlement,' zegt een bron uit de Belgische intelligencewereld[11], 'dan heb je ook toegang tot de parlementsleden en hun assistenten, die in verschillende comités werken rond thema's als energie, defensie, veiligheid en buitenlandse betrekkingen.'

België telt maar liefst 279 diplomatieke missies. Zowat 5.000 buitenlandse diplomaten zijn geaccrediteerd in België. Maar dat is nog niet alles. De Protocoldienst van Buitenlandse Zaken beheert 60.000 dossiers van buitenlanders met een diplomatiek of aanverwant statuut, gezinsleden inbegrepen. Het gaat om hoge ambtenaren maar ook om chauffeurs of poetspersoneel verbonden aan ambassades. Ze genieten allemaal een bepaalde vorm van diplomatieke onschendbaarheid. Volgens Buitenlandse Zaken is Brussel door de aanwezigheid van die 60.000 diplomaten en internationale ambtenaren de eerste diplomatieke hoofdstad ter wereld.[12]

Hoeveel personen van de 60.000 buitenlandse diplomaten en internationale ambtenaren in België op de payroll staan van geheime diensten kan niemand zeggen. Ook de Protocoldienst van Buitenlandse Zaken niet, nochtans het belangrijkste aanspreekpunt voor die 60.000. 'We weten welke functie de diplomaten officieel bekleden. Maar wat ze effectief doen? Dat is koffiedik kijken', klinkt het bij Buitenlandse Zaken.[13] 'Van alle landen die zichzelf als grootmacht bestempelen en die een rol willen spelen op wereldvlak kan je er van uitgaan dat zij op ambassades over inlichtingenagenten beschikken.'

Je zou verwachten dat Buitenlandse Zaken systematisch de achtergrond screent van alle nieuwe diplomaten die in België toekomen, om op die manier een zicht te hebben op de spionnen die onder diplomatieke cover opereren. Maar dat gebeurt niet. Alleen nieuwe ambassadeurs moeten een goedkeuringsprocedure doorlopen en vervolgens een geloofsbrief voorleggen. Hun naam en CV wordt doorgespeeld voor ze naar België komen. Vervolgens kan de Staatsveiligheid nagaan of ze gekend staan als spion. Ook diplomaten uit landen met een visumplicht voor België kunnen op verzoek van de Dienst Vreemdelingenzaken door de Staatsveiligheid gescreend worden. Zo een screening betekent dat de Staatsveiligheid nagaat of de naam van de diplomaat 'gekend' is.

Een medewerker van de Staatsveiligheid[14] vertelt hoe zijn dienst probeert een zicht te krijgen op de aanwezigheid van spionnen op diplomatieke vertegenwoordigingen: 'Inlichtingenagenten van bevriende landen zijn officieel vertegenwoordigd op de ambassades. Die namen kennen we. Bij niet-bevriende landen gaat het er niet zo

[11] Interview met een bron uit de Belgische intelligencewereld, 2009.
[12] Interview met bronnen bij Buitenlandse Zaken op 19 december 2005; de cijfers zijn geüpdated in 2009.
[13] Interview met bronnen bij Buitenlandse Zaken op 19 december 2005.
[14] Interview met een medewerker van de Staatsveiligheid die anoniem wenst te blijven, 2006.

openlijk aan toe en is het een uitdaging om hen te detecteren. Dat is niet gemakkelijk. Als bijvoorbeeld een jonge diplomaat uit China toekomt en je kent zijn parcours niet, begin dan maar eens uit te zoeken of hij werkt voor een inlichtingendienst. Hoe performanter de geheime dienst, hoe beter ze hun agenten zullen camoufleren. Daarom vragen we in die gevallen aan buitenlandse zusterdiensten of de diplomaten bij hen gekend zijn.'

Dat Brussel zoveel diplomaten huisvest maakt de stad trouwens op zich al een doelwit voor inlichtingenwerk. 'Brussel is vanuit intelligence-standpunt belangrijk door de concentratie aan diplomatie', zegt Tim Weiner, auteur van Een spoor van vernieling. De geschiedenis van de CIA.[15] 'Vergeet niet dat liaison ook penetratie betekent. Dat is altijd al zo geweest, en zal altijd zo zijn. Je zegt goedendag met je ene hand, en steelt tegelijkertijd met je andere.' Weiner onderscheidt twee vormen van diplomatie. 'Enerzijds heb je open overeenkomsten, die op een transparante manier worden bereikt. Die moet je niet bespioneren. Maar daarnaast zijn er nog de geheime deals. En sommige daarvan worden ook in Brussel gesloten.'

§ 2 De Justus Lipsius-case

'De telefoon doet het niet. Er zit wat ruis op. Kunnen jullie eens nagaan wat het probleem is?' [16] Een banale telefoonstoring in de grote vergaderzaal van het Justus Lipsiusgebouw leidde op 28 februari 2003 tot de ontdekking van een van de grootste spionage-zaken na de Koude Oorlog. In de mastedont van marmer en glas die in 1995 was ingehuldigd, vonden medewerkers van Alexandro Legein vijf zwarte dozen vol spionage-apparatuur. Spionage, het moest er ooit van komen. In 2000 was een vertrouwelijk EU-rapport over de veiligheid van het Justus Lipsiusgebouw uitgelekt in de pers. 'Raadsgebouw zo lek als een zeef', kopten de kranten toen.[17]

De vijf zwarte dozen waren identiek op één detail na. Enkel aan de doos die het eerst was ontdekt, zat een kabeltje dat buiten de muur zichtbaar was. De andere dozen waren met het blote oog volledig onzichtbaar. Vakwerk. De zwarte dozen konden vanop afstand geactiveerd worden en waren verbonden met de delegatieruimtes van Frankrijk, Italië, Duitsland, het Verenigd Koninkrijk, Spanje en Oostenrijk.[18] Aangezien ze perfect ingemetseld waren in de muren van Justus Lipsius, is de kans groot dat ze al tijdens of vlak na de bouw van de betonnen constructie waren aangebracht.

Tijdens de ontmanteling van de dozen stond Legein verbaasd: ze bevatten digitale technologie die zelfs bij de ontdekking – zoveel jaren na de plaatsing – nog geavanceerd was. Slechts een handvol inlichtingendiensten in de wereld kunnen zo een gesofistikeerd systeem in elkaar knutselen. 'Ik heb altijd bewondering voor vakmanschap en dit was vakmanschap', aldus Legein. 'Het was een prachtig georganiseerde operatie die we niet zouden hebben ontdekt als ze geen stommiteiten hadden begaan. De clue van het verhaal zit in de vergaderzaal waar op 28 februari 2003

[15] Interview met CIA-kenner Tim Weiner, Kristof Clerix, MO.be, 25 september 2007.
[16] Gebaseerd op interviews met Alex Legein op 18 januari 2005 en 20 januari 2006.
[17] Bolwerk Europese Unie blijkt zo lek als een zeef, Marc Peeperkorn, Gazet van Antwerpen, 17 februari 2000.
[18] Vijf zwarte dozen maar zes landen? Eén zwarte doos was verbonden met twee verschillende delegatieruimtes.

een storing op de telefoonlijn is vastgesteld. Net daarvoor was officieel aangekondigd dat in die zaal de Lentetop zou plaatsvinden. De staats- en regeringleiders en hun ministers van Buitenlandse Zaken van de – toen nog vijftien – EU-lidstaten zouden de kwestie-Irak bespreken.' Legein legt uit waarom aan slechts één van de vijf zwarte dozen een kabeltje zat dat buiten de betonmuren zichtbaar was. 'Aanvankelijk waren de zwarte dozen enkel verbonden met de delegatieruimtes van zes lidstaten. Maar nadat bekend was gemaakt dat de Lentetop in die bepaalde zaal zou plaatsvinden, heeft iemand één zwarte doos opnieuw afgesteld. Het afluistersysteem in die ene doos werd verbonden met de telefoonlijn in de bewuste vergaderzaal van de Lentetop. Met als zichtbaar resultaat dat ene kabeltje. Ik denk dat de aanpassing zo amateuristisch is uitgevoerd omdat de dader heel snel heeft moeten werken.'

Blijkbaar was de afluisterapparatuur gemanipuleerd en waarschijnlijk ook geplaatst door de inlichtingendienst van een land met grote belangen in Irak. De inlichtingendienst had het risico genomen om een perfect lopende afluisteroperatie op het spel te zetten, enkel en alleen om de standpunten van de EU-lidstaten over de kwestie-Irak te kennen. In de media werd druk gespeculeerd over de mogelijke daders. De Verenigde Staten, Israël en Rusland werden herhaaldelijk genoemd.

Het federaal parket opende in mei 2003 een onderzoek naar het afluisterschandaal in het Raadsgebouw. Midden 2006 liet voormalig federaal procureur Daniel Bernard weten dat het federaal parket het onderzoek nog datzelfde jaar hoopte af te ronden.[19] Daar kwam niets van in huis: meer dan 6,5 jaar na de ontdekking van de afluisterapparatuur loopt het onderzoek nog steeds.[20]

Volgens welingelichte bronnen is er intussen een sterk vermoeden over de daders, maar zouden de speurders op het terrein de instructie hebben gekregen niet verder te zoeken. 'Er spelen politieke belangen van het hoogste niveau mee. De remedie zou wel eens erger kunnen zijn dan de kwaal.'[21] Toch zijn er in maart 2009 nog huiszoekingen gebeurd in het kader van het onderzoek. Parketwoordvoerster Lieve Pellens: 'Er zijn ook drie personen personen ondervraagd, zowel van Belgische als Israëlische nationaliteit. Dat heeft niets opgeleverd. Dit maar om te zeggen dat er nog steeds onderzoeksdaden worden verricht. Het onderzoek loopt nog steeds.'[22]

Dat een persoon van Israëlische nationaliteit ondervraagd is, werpt de vraag op of er een link is met het van oorsprong Israëlische bedrijf Comverse. De besprekingen van de Europese Raad werden destijds immers voor de vertalers opgenomen met de inmiddels ontmantelde technologie van Comverse. Het bedrijf is geen onbekende in het wereldje van intelligence en werd reeds geciteerd in verschillende spionageschandalen. Federaal parket: 'Geen commentaar.'[23] Er zit dus niets anders op dan het verdere verloop van het onderzoek af te wachten. Of mogelijk kan het Comité I wel opheldering brengen. Het opende in 2006 een toezichtsonderzoek naar de wijze waarop de Belgische inlichtingendiensten in het Justus Lipsius-dossier zijn geïntervenieerd, en kreeg in het najaar van 2008 inzage in het gerechtelijk dossier.[24]

[19] Telefonisch interview met federaal procureur Daniel Bernard op 14 juli 2006.
[20] Telefonisch interview met Leen Nuyts, woordvoerster van het Federaal parket, op 13 augustus 2009.
[21] Spionage bij Europese Raad blijft raadsel, Kristof Clerix, MO*, februari 2008.
[22] Telefonisch interview met Lieve Pellens, woordvoerster van het Federaal Parket, op 3 juli 2009.
[23] Telefonisch interview met Leen Nuyts, woordvoerster van het Federaal parket, op 13 augustus 2009.
[24] Activiteitenverslag 2008, Vast Comité I, Intersentia 2009, p. 78.

§ 3 De Simm-case

A. Herman Simm, spion voor Rusland[25]

Op 21 september 2008 werd in Estland Herman Simm (61) gearresteerd op verdenking van spionage. Simm was niet de eerste de beste: hij was eerst hoofd van de Estse politie, werkte daarna op het Estse ministerie van Defensie als Hoofd Beveiliging en stond vervolgens een tijdlang aan het hoofd van de Estse National Security Authority, de instantie bevoegd voor het beveiligen van informatie. In die positie had Simm toegang tot alle top secret NAVO-documenten die tussen de lidstaten van het westers bondgenootschap werden uitgewisseld. 'Maar er is meer', zeggen goedgeïnformeerde bronnen binnen de veiligheidsdiensten van de Europese instellingen.[26] 'Simm had niet enkel toegang tot geheime NAVO-documenten maar ook tot "EU classified information (EUCI)". Een paar keer per jaar nam Simm in Brussel deel aan vergaderingen van de Commission Security Policy Advisory Group en het Council Security Committee, twee adviesclubs in verband met informatiebeveiliging.' Simm was ook verantwoordelijk voor het toekennen van veiligheidsmachtigingen aan Estse ambtenaren, waaronder medewerkers van het Estse leger en inlichtingen- en veiligheidsdiensten.

Het was alweer een hele tijd geleden dat er nog een geval van spionage binnen de NAVO publiek werd gemaakt. De laatste grote case dateert van 1998, toen de Franse inlichtingenofficier Pierre Bunel door de Franse geheime diensten werd opgepakt op verdeking van spionage. Bunel had in Brussel geheime NAVO-informatie doorgespeeld aan de Servische diplomaat Jovan Milanovic, een agent van de Servische militaire inlichtingendienst ODOJ.

Volgens The Baltic Times werd Simm in 1995 tijdens een vakantie in Tunesië gerekruteerd door Valery Zentsov, een officier van de Russische geheime dienst SVR. Simm zou niet voor het geld hebben toegehapt, maar werd gepaaid met de belofte dat hij de titel van kolonel terugkreeg die hij tijdens de Sovjet-periode was kwijtgespeeld. Vervolgens werd Simm "gerund" door Sergei Yakovlev, een Russische illegal die opereerde onder Portugese valse identiteit in Madrid. Gedurende twaalf jaar speelde hij honderden pagina's geclassificeerde informatie door aan de Russen. Helemaal interessant werd het voor Moskou toen Estland in 2004 lid werd van de NAVO en de Europese Unie.

De zaak-Simm kwam aan het licht nadat Yakovlev een ambtenaar van een andere NAVO-lidstaat tevergeefs had geprobeerd te recruteren. Plots gingen in Tallinn en Brussel alle alarmbellen af. 'Wanneer zo'n zaak aan het licht komt, moeten er verschillende stappen gezet worden', zei Alain Winants, administrateur-generaal van de Belgische Staatsveiligheid, in de nasleep van de affaire. 'Eerst een damage assessment en vervolgens moet men daaruit conclusies trekken: waar is het verkeerd

[25] Gebaseerd op: I Spy: Estonian official accused of KGB connections, Russia Today, 17 november 2008; Estonian Spy Scandal Shakes Nato and EU, Holger Stark, Spiegel Online, 17 november 2008; Fog in the Baltic, The Economist, 8 november 2008; Estonia Spy Case Rattles Nerves at NATO, Ellen Barry, The New York Times, 25 december 2008; Simm gets 12 years for treason, The Baltic Times, 26 februari 2009; Simm stripped of honours, The Baltic Times, 13 maart 2009; International praise for Simm's case, The Baltic Times, 2 maart 2009.

[26] Interview met bronnen binnen de veiligheidsdiensten van de Europese instellingen die anoniem wensen te blijven, 2009.

gelopen, waar moet de beveiliging worden opgetrokken en hoe kunnen dit soort incidenten in de toekomst worden vermeden?'[27] Het onderzoek werd geleid door het Nato Office of Security. Uiteindelijk werd Simm eind februari 2009 in Estland voor verraad veroordeeld tot een boete van 1,2 miljoen euro én een gevangenisstraf van twaalf jaar en zes maanden. De Orde van de Witte Ster-decoratie, die hij eerder had ontvangen voor bewezen diensten, werd hem door de Estse president Toomas Hendrick ontnomen.

B. 'Russische spionage exponentieel toegenomen'

Twee maanden na de veroordeling van Simm trok de NAVO in Brussel de accreditatie in van twee Russische diplomaten op beschuldiging van spionage: Viktor Koetsjakov, hoofd van de dienst politiek van de Russische missie bij de NAVO, en attaché Vassili Tsjizjov, zoon van de Russische ambassadeur bij de Europese Unie. [28] Dmitri Rogozin, de ambassadeur van Rusland bij de NAVO, noemde de maatregel een provocatie en zei dat de twee diplomaten in kwestie niets te maken hadden met spionage. Hij noemde de beschuldigingen 'uitgevonden' en 'onverantwoord'.

Volgens Alain Winants was de maatregel géén vergelding voor de Simm-case. 'De accreditatie van de twee Russen is ingetrokken omdat er aanwijzingen waren dat zij zich bezighielden met het verzamelen van inlichtingen, gericht tegen de NAVO. Het is de NAVO die de beslissing heeft genomen. Tengevolge van het zetelakkoord dat België heeft met de NAVO, trok België de accreditatie in en vroeg het de personen om zich te laten terugtrekken. Het was dus geen persona non grata-verklaring.'[29]

Volgens Winanats hanteren de Russische inlichtingendiensten anno 2009 'zeer agressieve methodes' en is de NAVO daarbij een van hun hoofddoelen: 'Ik denk dat men met een gerust gemoed kan zeggen – en dat wordt door alle westerse diensten in globo vastgesteld – dat de activiteit van de Russische diensten in het buitenland exponentieel is toegenomen. Dat zij blijk geeft van een zekere agressiviteit, zelfbewustheid. Dat er tamelijk veel agenten van Russische diensten actief zijn. En dat men in de meeste landen vaststelt dat het niveau van de aanwezigheid en de aard van de activiteiten eigenlijk bijna opnieuw, zoniet helemaal, hetzelfde zijn als tijdens de Koude Oorlog.' Hoe vaak worden inlichtingenactiviteiten door Russische spionnen waargenomen? Winants: 'Ik ga niet zeggen dagdagelijks, want inlichtingenwerk is niet iets punctueels. Het gaat om zaken die lopen in de tijd: wanneer men iemand wenst te manipuleren, dan regel je dat niet tussen maandag en vrijdag. Het is een werk van lange adem.'

Alexandro Legein bevestigt de trend die Winants signaleert: 'Ook bij de Europese Raad stellen we een verhoogde interesse vast van de Russische inlichtingendiensten, vooral in activiteiten op het gebied van crisis management (zowel militair als civiel), non-proliferatie en de energieproblematiek. Energie is de grootste bron van inkomsten voor de Russische Fedederatie. Het spreekt voor zich dat zij die bron van inkomsten met alle middelen van de staat zullen proberen te garanderen. Dat is in de huidige

[27] Interview met Alain Winants, chef Staatsveiligheid, Kristof Clerix, MO.be, 4 december 2008.
[28] Gebaseerd op: Nato Expels Two Russians Accused of Spying, Clifford J. Levy, The New York Times, 1 mei 2009; Nato expels Russian diplomats from HQ in spy row, Luke Harding, Guardian.co.uk, 30 april 2009.
[29] De quotes van Alain Winants in de volgende alinea's zijn gebaseerd op: Russische spionage-activiteit is exponentieel toegenomen, Kristof Clerix, MO.be, 4 december 2008; interview met Alain Winants op 16 juli 2009.

economische crisis nog belangrijker dan vroeger. Het spreekt voor zich dat de Russische inlichtingendiensten er aandacht aan besteden, en dat de EU als grote klant van de Russische energiesector een potentieel doelwit van hun activiteiten is.' Winants: 'De Russen proberen te achterhalen wat de positie van Europa als geheel is op de toekomst van de energieproblematiek. Verder zullen de Russische inlichtingendiensten trachten tweedracht te zaaien in Europa als het gaat om een gemeenschappelijke visie op de energieproblematiek.'

Volgens goedgeïnformeerde bronnen is Rusland bij de Europese Commissie onder meer geïnteresseerd in Galileo, Europese energie-politiek, IT-regelgeving en buitenlands beleid:[30] 'Gezien zijn militaire mogelijkheden zijn de Russen zeker geïnteresseerd in Galileo, het Europese civiele globale satellietnavigatiesysteem dat momenteel in ontwikkeling is. Ook IT is een doelwit. Met name het Enisa-agentschap in Kreta, dat de Europese regelgeving in verband met IT uitvoert, is daarin belangrijk. En natuurlijk de buitenlandse politiek van Europa. Vergeet niet dat de ambassades van de EU worden gerund door de Commissie. De Russen zijn zeer professioneel. Ze verkennen constant heel breed de mogelijkheden: waar kunnen we een ingang vinden?'

C. De hoogste informatiedichtheid ter wereld

Brussel huisvest niet alleen de Europese Raad, de Europese Commissie, het Europees Parlement en het hoofdkwartier van de NAVO. Ook multinationals, internationale vakbondskoepels, de Wereld Douaneorganisatie met 162 lidorganisaties en de Europees-Economische Ruimte hebben hun hoofdzetel in ons land. Verder opereren ook Eurocontrol, de Europese organisatie voor de veiligheid van de luchtvaart, en de West Europese Unie, de eerste Europese instelling die bevoegd was voor defensiebeleid, vanuit België. Volgens socioloog Eric Korijn van de Vrij Universiteit Brussel huisvest de hoofdstad maar liefst 2500 internationale agentschappen, meer dan 2000 internationale ondernemingen en 150 internationale advocatenbureaus.[31] Door de aanwezigheid van al die internationale organisaties behoort Brussel samen met New York en Genève tot de steden met de hoogste informatiedichtheid ter wereld. Ook al die ondernemingen en organisaties kunnen het doelwit worden van spionage. Dat werd duidelijk in de Swift- en de Batasuna-case.

[30] Interview met bronnen binnen de veiligheidsdiensten van de Europese instellingen, die anoniem wensen te blijven, 2009.

[31] Staten-Generaal van Brussel. Brussel, internationale stad, E. Corijn ea, Brussels Studies, synthesenota nr. 13, 24 februari 2009. (p. 2)

§ 4 De Swift-case[32]

Tot groot ongenoegen van het Witte Huis onthulden drie Amerikaanse kranten op 23 juni 2006 een geheim CIA-programma in de strijd tegen terrorisme. Het voorpaginanieuws van The New York Times, de Los Angeles Times en The Wall Street Journal sloeg in als een bom, niet in het minst in België. 'Op basis van een geheim programma van de regering-Bush, dat een paar weken na de terreuraanslagen van 9/11 is opgesteld, hebben contraterrorisme-functionarissen toegang gekregen tot financiële bestanden van een enorme internationale databank', opende The New York Times. 'Volgens regerinsfunctionarissen is het programma beperkt tot het opsporen van transacties van mensen die verdacht worden van banden met Al Qaeda. Dat gebeurt door databestanden te inspecteren afkomstig van het zenuwcentrum van de wereldwijde bankindustrie, een Belgisch coöperatief dat elke dag zowat zes biljoen dollar rondstuurt tussen banken, makelarijen, beurzen en andere instellingen.' Het Belgisch bedrijf in kwestie was Swift (Society of Worldwide Interbank Financial Telecommunication). Vanuit Terhulpen nabij Brussel verzorgt Swift dagelijks het versturen van 10 miljoen beveiligde berichten tussen 8.300 financiële instellingen in meer dan 208 landen.

Onder toezicht van het Amerikaanse ministerie van Financiën hebben de CIA, de FBI en andere agentschappen tienduizenden financiële transacties onderzocht. Heet hangijzer: in tegenstelling tot de normale gang van zaken gebeurde de CIA-inzage in de Swift-databank niet op basis van een gerechtelijk bevelschrift maar op basis van een administratief bevel. Met andere woorden: heel het geheime programma was volledig onttrokken aan gerechtelijke controle.

Na het uitlekken van de Swift-gate kwamen toenmalig premier Guy Verhofstadt en minister van Justitie Laurette Onkelinx uit de lucht vallen. Beiden ontkenden formeel dat ze op de hoogte waren van het geheime Amerikaanse programma. 'Ons land is solidair in de strijd tegen het terrorisme en verleent zijn volle medewerking op bilateraal en multilateraal vlak', reageerde Verhofstadt. 'Ik neem aan dat dit is gebeurd met volledig respect van de fundamentele vrijheden en binnen de bestaande wettelijke beperkingen. Het kan evenwel niet dat dit zou gebeuren zonder respect voor de fundamentele vrijheden en de waarborgen van de rechtstaat. Ik heb onze diensten de opdracht gegeven de zaak te onderzoeken.' Waren wél op de hoogte van het geheime Terrorist Financing Tracking Program: de Nationale Bank van België (NBB) en minister van Financiën Didier Reynders. In februari 2002 al had Swift de Britse, Amerikaanse en Europese centrale banken én de NBB ingelicht over het geheime en controversiële CIA-programma. De NBB is immers belast met extern toezicht op Swift. Toch heeft de NBB de Belgische overheid nooit formeel op de hoogte gebracht. De bank beriep zich daarvoor op haar beroepsgeheim. De noodzakelijke voorwaarden om dat beroepsgeheim op te heffen waren volgens de NBB niet aanwezig. Senator Hugo Vandenberghe: 'De NBB vergeet dat het beroepsgeheim er is om de privacy te beschermen, niet om de schenders van de privacy te beschermen.' Vreemd genoeg bleek het beroepsgeheim niet meer dwingend toen de NBB in april 2006 via informele weg minister van Financiën Didier Reynders inlichtte over het CIA-programma.

[32] Overgenomen uit: Vrij Spel, Buitenlandse geheime diensten in België, Kristof Clerix, Manteau 2006; nawoord bij de Franstalige editie, Les Services Secrets Etrangers en Belgique. En toute impunité?, Kristof Clerix, Editions Racine 2008.

Het onderzoek naar de Swift-gate dat de regering in eerste instantie had laten uitvoeren door de NBB, de Cel voor Financiële Informatieverwerking en de Staatsveiligheid bracht weinig nieuwe elementen aan het licht. Opvallendste conclusie: de Staatsveiligheid, bevoegd voor de bescherming van de Belgische economie en de controle op buitenlandse geheime diensten, wist van niets. Het zegt veel over de verhouding tussen de Belgische inlichtingendienst en zijn Amerikaanse grote broer.

De Europese Commissie liet weten dat er geen Europese wetgeving bestaat over de datatransfer waar Swift bij betrokken is, en noemde de kwestie een 'nationale zaak'. Lees: het was aan België om uit te zoeken of alle wetten werden nageleefd. Het Europees Parlement eiste een hoorzitting over de Swift-affaire. Intussen kregen het Comité-I en het ministerieel college voor Inlichtingen en Veiligheid de opdracht om de zaak verder te onderzoeken.

Uiteindelijk werd op vraag van België een tweeledige oplossing uitgewerkt door de Europese Unie. Enerzijds kwamen er unilaterale Amerikaanse garanties met betrekking tot de gegevensbescherming, die door de EU werden erkend als 'adequate bescherming' volgens de Europese wet. De Europese Commissie stelde ook een rechter aan – de Franse antiterrorismespecialist Jean-Louis Bruguière – om jaarlijks de gegevensuitwisseling te evalueren. Anderzijds moest Swift zich in regel stellen met de Belgische privacywetgeving. In dat kader trad het bedrijf toe tot Safe Harbour, een internationaal erkende gedragscode voor gegevensbeheer. Swift stelde ook een overeenkomst op met de aangesloten banken. Die moeten voortaan in hun algemene voorwaarden aan cliënten meedelen dat specifieke gegevens doorgespeeld kunnen worden aan de VS. Opmerkelijk is wel dat de gegevensuitwisseling intussen gewoon is blijven doorgaan, ook voor de EU deze tweeledige oplossing had uitgedokterd.

Het Federaal parket sloot in december 2006 het strafdossier tegen Swift. Het vond onvoldoende elementen in het rapport van de Belgische privacycommissie om het bedrijf te vervolgen. Nochtans had de Europese Commissie kort daarvoor geoordeeld dat Swift de privacywet wel had overtreden.

§ 5 De Batasuna-case

'De televisie hapert. Last van interferenties. Kunnen jullie eens nagaan wat het probleem is?' [33] Na maanden van storingen op het Spaanse kanaal TVE was Gorka Elejabarrieta Diaz het beu. Hij belde de Brusselse kabelmaatschappij Brutele en vroeg een technicus langs te sturen. Gorka kwam in 2002 naar België als assistent van het Baskische Europarlementslid Koldo Gorrostiaga. Samen betrokken ze een ruim appartement boven een Marokkaanse winkel in de Elsense Steenweg, een drukke winkelstraat in hartje Brussel. Ook nadat Gorrostiaga in 2004 niet herkozen raakte – de Baskische politieke partij Batasuna was intussen in Spanje buiten de wet gesteld en belandde op de lijst van terroristische organisaties van de EU – bleef Gorka als lobbyist voor Batasuna in het appartement wonen.

De Brutele-technicus kon de storingen niet thuisbrengen, zoiets had hij in zijn hele carrière nog nooit meegemaakt. Mogelijk zorgde een ander toestel voor interferenties. Uiteindelijk trok Gorka dan maar zelf op onderzoek. In de hoek van de living – die dienst doet als kantoor van Batasuna – vond hij op 23 januari 2007 achter een plint een verborgen gesofisticeerd toestel. Er stond een serienummer op: 139S2V5.1. Het bleek om afluisterapparatuur te gaan, verbonden met een elektriciteitskabel in de muur. Meteen wist Gorka nu zeker wat hij al jaren vermoedde. Gorka: 'Vanaf het begin dat ik in België vertoefde, had ik het gevoel dat ik bespioneerd werd. Soms had ik de indruk dat iemand mij op straat achtervolgde. Op andere momenten merkte ik dat mijn gsm en telefoon werden afgetapt, en mijn e-mails gescreend. Wanneer ik bijvoorbeeld voor Batasuna naar het buitenland ging om politici te ontmoeten, gebeurde het wel eens dat die politici door Spaanse diplomaten werden aangesproken over de nakende ontmoetingen. Hoe wisten ze van mijn geplande trips? Dat kon alleen via spionage.'

Na de vondst van de afluisterapparatuur belegde Gorka thuis een persconferentie. 'Dit apparaat, en de manier waarop het geplaatst werd, vertonen frappante gelijkenissen met afluisterapparatuur die ontdekt werd in het hoofdkantoor van Batasuna in het Franse Bayonne', klonk het. 'Het apparaat heeft de mogelijkheid om, na vanop afstand geactiveerd te zijn, een audiosignaal uit te zenden van alles wat in de vergaderruimte gezegd werd. Het apparaat kan niet functioneren zonder een gesloten ontvangstruimte.'

Het nieuws sloeg in als een bom. 'Het zal de eerste en laatste keer niet zijn dat inlichtingendiensten buiten het wettelijk kader in België of in andere landen opereren', aldus Brice De Ruyver, veiligheidsadviseur van toenmalig premier Verhofstadt, in De Morgen. 'De densiteit aan internationale instellingen in België genereert een densiteit in het verzamelen van inlichtingen.' Het federaal parket meldde niets af te weten van een onderzoek naar Batasuna – bijgevolg kon de afluisterapparatuur niet door de Federale Politie geplaatst zijn. En de Staatsveiligheid mag sowieso niemand afluisteren.

De Batasuna-case leidde op 27 februari 2007 in de Kamer tot een interessante zitting van de Commissie voor de Justitie. 'Men kan niet zeggen dat de Staatsveiligheid momenteel uitgerust is om op een efficiënte manier het hoofd te bieden aan elk type van dreiging, inclusief de spionageactiviteiten ten voordele van buitenlandse entiteiten die op ons grondgebied kunnen plaatsvinden', reageerde toenmalig justitieminister

[33] Gebaseerd op: nawoord bij de Franstalige editie, Les Services Secrets Etrangers en Belgique. En toute impunité?, Kristof Clerix, Editions Racine 2008.

Onkelinx op interpellaties van kamerleden. 'Ik durf zelfs zeggen dat vandaag de dag de Staatsveiligheid in grote mate afhankelijk is van de buitenlandse inlichtingendiensten die doen wat hij niet kan. Deze situatie is onduldbaar geworden en in strijd met onze rechtstaat.' Voor het eerst gaf een Belgische minister van Justitie met zoveel woorden de problematiek van spionage door buitenlandse inlichtingendiensten toe.

Gorka vond achter een andere plint in zijn living nog een tweede afluisterapparaat. 'Ik denk dat de Spaanse geheime dienst hier achter zit', zegt Gorka', al heb ik er geen bewijzen voor. Wie anders zou geïnteresseerd zijn in onze vergaderingen hier in het appartement? Op het moment van de ontdekking van de apparatuur zaten we trouwens midden in een vredesproces. De ontwikkeling van een vredesproces in Baskenland is nauw verbonden met de steun van de EU en haar instellingen. Het is dan ook cruciaal dat de hoofdstad van Europa daarbij een ruimte voor dialoog kan blijven, voor de uitwisseling van politieke ideeën, voor het respect voor de wet, de democratie en de burgerlijke en politieke rechten.'

Gorka diende klacht in bij de lokale politie van Elsene. Het Brussels parket opende een onderzoek en het federaal parket nam het dossier op 13 juli 2007 over. Het onderzoek loopt nog steeds.[34] 'Een deskundige van de Koninklijke Militaire School heeft de spionage-apparatuur intussen onderzocht. De producent is een Deense firma die levert aan overheidsinstellingen', viel te vernemen uit welgeïnformeerde bronnen.[35] Benieuwd wat de crosscheck van het serienummer met de Deense firma oplevert. 'Ook is de reikwijdte van het apparaat onderzocht. Het reikte in ieder geval niet tot bij de Spaanse ambassade, die op een steenworp van het appartement van Gorka ligt.' Opvallend in het onderzoeksdossier is een proces-verbaal van de politie, dat verwijst naar het bezoek van een medewerker van de Staatsveiligheid in het gezelschap van twee niet-geïdentificeerde mannen, die de spionage-apparatuur kwamen bekijken.

Over de uitkomst van het onderzoek toont Gorka zich niet echt hoopvol. 'Mijn indruk is dat België de zaak ernstig onderzoekt. Maar ik denk niet dat er ooit iemand op het beklaagdenbankje zal verschijnen. Dit soort affaires wordt tussen staten onderling opgelost.'

[34] Telefonisch interview met Leen Nuyts, woordvoerster van het Federaal parket, op 13 augustus 2009.
[35] Interview met welgeïnformeerde bronnen die anoniem wensen te blijven, 2009.

§ 6 De ICT-case

A. Chinese cyberaanval[36]

Naast hoofdzetel van een pak internationale instellingen en bedrijven is Brussel in de eerste plaats natuurlijk de hoofdstad van België. En ook Belgische overheidsinstanties worden wel eens het slachtoffer van spionage.[37] Op 30 april 2008 maakte toenmalig minister van Justitie Jo Vandeurzen bekend dat de Staatsveiligheid 'informatie had over pogingen tot een elektronische aanval tegen e-mailadressen van de federale overheid.' Vandeurzen: 'Vooralsnog kan niet worden bewezen dat de Chinese autoriteiten bij de aanvallen betrokken zijn. De context wijst echter wel in de richting van China.' Volgens Vandeurzen stelt het land 'bijzonder veel belang in België, omdat wij een belangrijke rol vervullen in Afrika en zowel de belangrijkste EU-instellen als de NAVO huisvesten.' De minister liet ook weten dat technische informatie over de aanvallen nog vrij beperkt en fragmentair beschikbaar was. 'Momenteel kunnen we niet met zekerheid stellen of de aanvallen hun doelwit hebben bereikt. De informaticadienst van de Staatsveiligheid werkt samen met de informaticadiensten en de veiligheidsofficieren van de getroffen Federale Overheidsdienst aan een forensisch onderzoek naar de elektronische aanvallen.'

'We hebben inderdaad een aantal elektronische aanvallen tegen overheidsdiensten onderzocht', zegt Alain Winants. 'Ze waren zeer goed gecibleerd, duidelijk gericht tegen bepaalde personen in bepaalde overheidsdiensten die zich met bepaalde dossiers bezighielden. Het gaat onder meer om dossiers die betrekking hebben op Europese aangelegenheden en op de energieproblematiek.' De Staatsveiligheid stelde vast dat de aanvallen gebeurden volgens een systeem van social networking. Winants: 'Personen kregen berichten die ze uit hoofde van hun functie normaalgezien moesten openen. Zodra ze dat deden, werd er schade aangericht.' Volgens Winants zijn er geen harde bewijzen dat de aanvallen afkomstig waren van China, 'maar er zijn toch zeer duidelijke aanwijzingen dat het vanuit die richting werd aangestuurd.'

Professioneel aangestuurde cyberaanvallen zijn zeer moeilijk te traceren. Op een recente spionage-conferentie in het Europees Parlement gaf Shai Blitzblau van het Israëlisch-Italiaanse bedrijf voor informatiebeveiliging Maglan Europe uitleg over hoe zulke IT-aanvallen verlopen. 'Stel dat ik wil penetreren in Volvo in Zweden', aldus Blitzblau.[38] 'Als ik dat zou doen vanuit mijn kantoor in Italië, kan ik snel opgespoord worden. Om dat te voorkomen zal ik eerst in een systeem in Azië binnendringen, een kleuterschool bijvoorbeeld. Vandaaruit zal ik proberen een systeem in Zuid-Afrika te penetreren, misschien de mailserver van een kerk. De mogelijkheid om mij te traceren wordt op die manier bijna zero. Vanuit Zuid-Afrika gaat het achtereenvolgens naar Israël, Iran en Zweden. Vaak gebruiken hackers ook politieke kennis. Zie je Iran al naar

[36] Gebaseerd op: nawoord bij de Franstalige editie, Les Services Secrets Etrangers en Belgique. En toute impunité?, Kristof Clerix, Editions Racine 2008 ; interview met Alain Winants op 16 juli 2009.

[37] Een voorbeeld van meer dan twintig jaar geleden: in 1988 waren computerfanaten Bart Halewyck en Luc Pancoucke binnengedrongen in het Bistel-systeem, het Belgian Information System By Telephone. Dat stond enkel ter beschikking van ministers, staatssekretarissen, kabinetsleden en hooggeplaatste ambtenaren. De correctionele rechtbank veroordeelde beide heren tot een voorwaardelijke gevangenisstraf. Bron: Zware straffen voor Bistel-Krakers, De Tijd, 9 november 1990.

[38] Shai Blitzblau van Maglan Europe op de conferentie "EU Exposed - from Network Intelligence to Industrial Espionage", georganiseerd door MEP Mario Mauro, Europees parlement, 30 maart 2009.

Israël bellen: iemand is vanuit jouw land bij ons binnengedrongen? No way. Dat gebeurt niet.'

De Staatsveiligheid is niet uitgerust om zelfstandig dat soort aanvallen te onderzoeken of de bron ervan te traceren. Winants: 'Het gaat om een forensisch onderzoek op pc's, dat zeer tijdrovend, arbeidsintensief en kostelijk is. Het onderzoek naar de ICT-aanvallen op de computers van een Belgische overheidsdienst hebben we dan ook in samenwerking gedaan met de militaire inlichtingendienst ADIV.' Nochtans is dat in principe niet de taak van de ADIV. 'Landsverdediging is niet belast met de bescherming van de nationale kritieke infrastructuur tegen hackers', antwoordde minister van Defensie Pieter De Crem op een parlementaire vraag over de Chinese cyberaanvallen.[39]

Na het bekendmaken van de affaire liet Vandeurzen weten dat Justitie plannen heeft om een speciale overheidsdienst op te richten die spionage- en hackerspogingen tegen de overheid moet helpen verijdelen. Op basis van het witboek 'Voor een nationaal informatieveiligheidsbeleid', door het Ministerieel comité voor Inlichtingen en Veiligheid goedgekeurd, werkte de Federale Overheidsdienst Informatie- en Communicatietechnologie (Fedict) een concreet voorstel uit. Dat voorziet in de eerste plaats in de oprichting van een nationaal Computer Security Incident Response Team, een 'reactiecentrum voor informatica-incidenten dat de evolutie van de risico's opvolgt, de maatschappij informeert over de nodige maatregelen en eventuele crisissen kan beheren'[40]. Verder moet volgens het voorstel prioriteit worden gegeven aan de bescherming van kritieke informatie-infrastructuren, vooral in de energie- en transportsector. Ten slotte zou binnen ieder federaal departement een adviseur worden aangesteld om de informatieveiligheid te coördineren.

Het voorstel van Fedict werd in oktober 2008 door de interkabinettenwerkgroep goedgekeurd. Voor 2009 voorziet de overheid een budget van bijna twee miljoen euro om het verder uit te werken. Het is aan Vincent Van Quickenborne, minister voor Ondernemen en Vereenvoudigen, om concrete initiatieven te nemen. Alain Winants: 'Het is de bedoeling dat er op vrij korte termijn een organisme zou komen dat zich kan inlaten met het bestrijden van ICT-aanvallen komende van buitenaf. Men is ermee bezig maar het is een zeer, zeer moeilijk onderwerp. Niet alleen in termen van kosten. We moeten ook zien op welke manier, wanneer en hoe het best gereageerd wordt.' To be continued.

B. Ghostnet

Op 29 maart publiceerden onderzoekers van de University of Toronto een lijvig rapport over Chinese cyberspionage. In Tracking Ghostnet: investigating a Cyber Espionage Network[41] legden ze bloot dat een gigantisch elektronisch spionagenetwerk meer dan duizend computers van officiële instanties wereldwijd had geïnfiltreerd. De onderzoekers waren in het voorjaar van 2008 ingehuurd door de diensten van de dalai lama, de Tibetaanse leider in ballingschap, om hun computers te onderzoeken op

[39] Vraag van Denis Ducarme aan de minister van Landsverdediging over "de Chinese cyberaanvallen op het federaal computernetwerk en de betrokkenheid van het departement Landsverdediging bij een antihackingstrategie", beknopt verslag, commissie voor landsverdediging, 14 mei 2008.

[40] Vraag van senator Yves Buysse aan de vice-eersteminister en minsiter van Justitie en Institutionele Hervormingen, ingediend op 9 oktober 2008 en beantwoord op 4 december 2008.

[41] Tracking Ghostnet: investigating a Cyber Espionage Network, Information Warfare Monitor March 29, 2009, www.tracking-ghost.net

malafide software. Zo stootten ze op het wereldomspannende elektronische spionagenetwerk, dat onder meer vanuit drie Chinese GhostNet-computers aanvallen lanceerde. De onderzoekers waarschuwen er wel voor dat het voorbarig zou zijn om te besluiten dat de Chinese overheid achter de spionage zit.

Ook in België bleek het e-mailverkeer van het dalai lama-bureau geïnfiltreerd. 'We zijn niet verrast', reageerde Tashi Wangdi van het Brusselse Tibetbureau – de vertegenwoordiger van de Dalai Lama in Europa – in De Morgen.[42] 'We hadden al een tijdje het gevoel dat onze mails door onbevoegden werden gelezen. Gelukkig zijn die vermoedens nu bewezen.'

Op de lijst van getroffen doelwitten prijkten onder meer ook de ambassades van India en Malta in Brussel. Die laatste leidde eerder al tot wenkbrauwgefrons in het Europese intelligencewereldje. De locatie van de Maltese ambassade in de Rue Archimede is zeer strategisch, want ze ligt op amper een paar meter van het gebouw van de Europese Commissie. Groot was dan ook de verbazing bij de veiligheidsdiensten van de Europese instellingen toen bleek dat China in 2007 voor meer dan 200.000 euro aan meubels en kantoormateriaal schonk aan de Maltese ambassade 'om 35 jaar vriendschap te vieren tussen de twee landen'. De goederen werden rechtstreeks geïmporteerd uit China.[43] De veiligheidsdiensten drongen bij de Maltese geheime dienst aan op een grondige sweep van het dertien verdiepingen tellende gebouw. Die zakte af naar Brussel maar vond er geen spionage-apparatuur. Toch blijven volgens goedgeïnformeerde bronnen verschillende inlichtingendiensten van grote EU-lidstaten de Maltese ambassade nauwkeurig in de gaten houden.

Alain Winants wijst erop dat de Chinese inlichtingendiensten in België zeer actief zijn. 'Het gaat misschien niet om dezelfde klassieke activiteit van inlichtingendiensten. Maar we hebben hier wel een vrij grote aanwezigheid van Chinese journalisten en studenten. U hebt ook mensen die in grote firma's werkzaam zijn en nadien terugkeren naar China. China is ook bijzonder geïnteresseerd in het standpunt van Europa inzake energie en dergelijke zaken meer. En het wetenschappelijk en economisch potentieel is natuurlijk een domein waarin de Chinezen bijzonder geïnteresseerd zijn. Ik denk dat wij in de toekomst rekening moeten houden met een nog grotere toename van de aandacht van de Chinezen voor verschillende zaken in de Europese politiek.'[44]

§ 7 Besluit

Brussel is een magneet voor buitenlandse geheime diensten. Dat blijkt duidelijk uit bovenstaande voorbeelden – geen oude spionageverhalen maar cases van de voorbije jaren. Brussel huisvest tal van interessante doelwitten voor inlichtingenwerk en biedt bovendien ook de ideale covers voor spionnen. De vraag is hoe de Belgische overheid best omgaat met die realiteit.

[42] Doelwit van hackings waren kantoren van dalai lama, ook in België, Ayfer Erkul, De Morgen, 30 maart 2009.
[43] RCC sees China Red, Karl Schembri, Malta Today, 25 februari 2007.
[44] Russische spionageactiviteit is exponentieel toegenomen, Kristof Clerix, MO.be, 4 december 2008.

Het Comité I heeft herhaaldelijk de noodzaak onderstreept om de problematiek van spionage aan te pakken. 'De controle op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied is as such niet opgenomen als wettelijke taak voor de Staatsveiligheid of de ADIV', schrijft het Comité I in zijn Activiteitenverslag 2006. 'Het Comité I is van oordeel dat deze bevoegdheid expliciet in de wet zou moeten worden ingeschreven. De Belgische inlichtingendiensten zijn immers het best geplaatst om de activiteiten van (ook bevriende) zusterdiensten te herkennen en te beoordelen.' Het comité vindt zelfs dat dat een van de basisopdrachten van de Staatsveiligheid en de ADIV moet worden. In zijn Activiteitenverslag 2007 herhaalt het Comité I die aanbeveling: 'Het Ministerieel Comité voor inlichtingen en veiligheid moet dringend de samenwerking met de buitenlandse inlichtingendiensten reglementeren. Het ontbreken van een dergelijke reglementering brengt de Belgische inlichtingendiensten vaak in een penibele situatie. Op dat vlak moet een evenwicht worden gevonden tussen een noodzakelijke en effectieve samenwerking met bevriende landen en de vrijwaring van de rechten en vrijheden.' En in het Activiteitenverslag 2008 klinkt nogmaals: 'De controle op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied moet as such in de wet worden opgenomen als taak voor de Staatsveiligheid en de ADIV.' Hopelijk is de boodschap intussen aangekomen.

En dan is er nog iets. Buitenlandse geheime diensten weten heus wel dat de Belgische Staatsveiligheid geen telefoons mag afluisteren, e-mails mag onderscheppen of andere bijzondere inlichtingenmethodes (BIM) mag toepassen. Decennialang heeft de Staatsveiligheid als het ware met pijl en boog tegen buitenlandse spionnen moeten strijden. Daarin moet de BIM-wet verandering brengen. Midden juli keurde de Senaat het wetsvoorstel alvast goed, de bal ligt nu[45] in het kamp van de kamerleden.

Twee belangrijke opmerkingen daarbij. Ten eerste zal de Staatsveiligheid een pak extra werkingsmiddelen moeten krijgen om de bijzondere inlichtingenmethodes ook daadwerkelijk te kunnen toepassen. Daarover moet een ernstig debat gevoerd worden. Ten tweede: om de balans tussen vrijheid en veiligheid te garanderen, zal doorgedreven controle op de toepassing van de BIM-wet cruciaal zijn. Ook daarvoor moeten voldoende middelen voorzien worden. Bovendien moet de politieke wereld zorgen voor meer transparantie. Waar blijft het jaarverslag van de Staatsveiligheid dat al zolang beloofd wordt? En de brochure waarin het Belgische publiek gesensibiliseerd wordt over de risico's van spionage door buitenlandse geheime diensten? Alleen wanneer de controle en transparantie groot genoeg zijn, kunnen de bijzondere inlichtingenmethoden op een duurzame manier hun dienst bewijzen. Want aan BIM-schandalen heeft de Staatsveiligheid al helemaal geen boodschap.

'Ik weet niet of buitenlandse geheime diensten onze eerste target zullen zijn', zegt Alain Winants.[46] 'Maar de BIM-wetgeving zal ons binnen het kader van onze bevoegdheden toch op bepaalde vlakken duidelijke informatie geven. Ik denk dat dan ook het imago van onze dienst moet worden bijgesteld. Vanaf dat ogenblik treden we als inlichtingendienst eindelijk de 21ste eeuw binnen.'

[45] Deze bijdrage is ingestuurd op 18 augustus 2009.
[46] Interview met Alain Winants op 16 juli 2009.