

INGELICHT

Informatiemagazine van de Militaire Inlichtingen- en Veiligheidsdienst
voor de I&V-keten
juni 2010 - Nr 2

NI DA

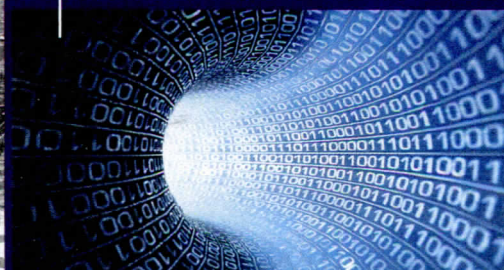


CSI in Afghanistan

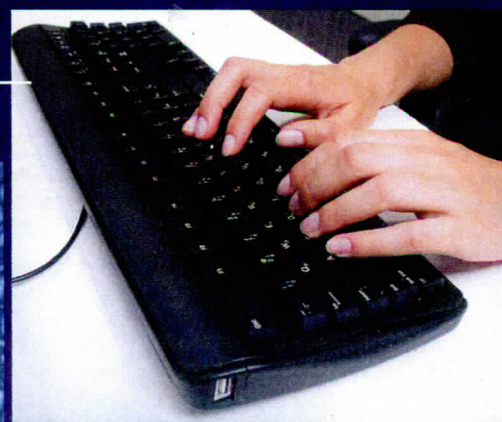


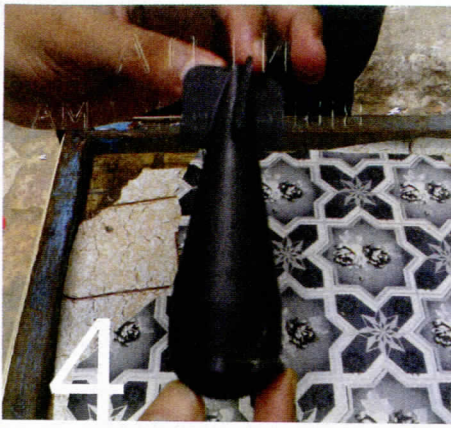
ZEE VAN GEHEIMEN

CRYPTOGRAFIE



VEILIGHEIDSZAKEN

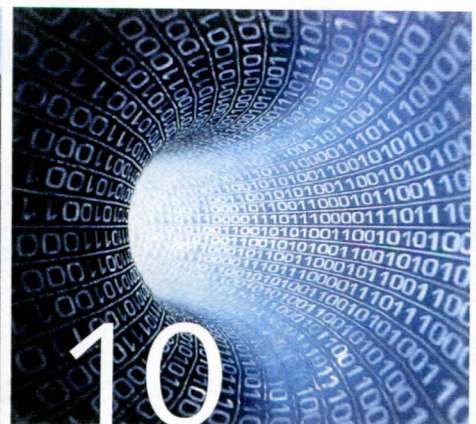




4 Numb3rs & Crime Scene Investigation in Afghanistan



8 Tegenstellingen in Haiti



10 de MIVD-crypto-analist: 'Van ons zul je nooit horen dat wij een programma hebben gekraakt'

13 Voel jij je veilig?

14 Aeolus: het nieuwe werken

18 Zee van geheimen

PERSONEELSKATERN



21



23



21 Bureau Veiligheidszaken doet veel meer dan je denkt.

23 't Is koers!

25 MIVD besteedt meer aandacht aan piraterij

26 Humor houdt je op de been

27 MIVD neemt deel aan de CPC-loop op zondag

28 Reusers kolom: Phishing

INGELICHT, INFORMATIEBLAD VAN DE MILITAIRE INLICHTINGEN- EN VEILIGHEIDSDIENST VOOR DE INLICHTINGEN- EN VEILIGHEIDSKETEN

Eindredactie: D.L. de Miranda Redactie: Bureau Communicatie Redactieadres: MIVD/Bureau Communicatie, Postbus 20701, 2500 ES Den Haag

E-mailadres: mivd@mindef.nl Telefoon: 070-441 90 40 Fotografie: Ministerie van Defensie, Audiovisuele dienst Defensie

Vormgeving: vijfkeerblauw.nl Druk: DeltaHage Oplage: 1.500 exemplaren

De redactie behoudt zich het recht om bijdragen - waaronder ingezonden brieven - niet, gedeeltelijk of gewijzigd te plaatsen. Aan de inhoud van dit blad kunnen geen rechten worden ontleend.

VOOR GEBRUIK VAN TEKSTEN EN FOTO'S UIT DIT BLAD DIEN T U TOESTEMMING TE VRAGEN AAN DE REDACTIE.

Turbulentie; Riemen vast

U kent het wel: "Dames en Heren neemt u plaats in uw stoelen en *fasten your seatbelts*. Dan moet je even wachten en dan begint het vliegtuig te bokken en te stampen of.....er gebeurt niets. In beide gevallen eindigt het met een PING en gaat het *fasten your seatbelts*-lichtje weer uit. Vervolgens gaat alles zijn gangetje en lijkt het alsof er niets is gebeurd.

Op dit moment hebben we bij de MIVD de stoelriemen even vast en probeert de MIVD-leiding om de turbulentie heen te vliegen. Waar omheen eigenlijk? Om het rapport Davids zijn we redelijk heen gevlogen en uiteindelijk zal het de positie van de MIVD als organisatie met vooruitziend vermogen verstevigen. De brede heroverwegingen, bedoeld om de regering keuzes te laten maken ten aanzien van de voorgenomen miljardenbezuinigingen, leiden niet direct tot desastreuze gevolgen voor de MIVD. Doordat we de handen ineen hebben geslagen met de AIVD lijkt deze turbulentie mee te vallen. Een gevallen regering op het voor de MIVD zwaarste dossier Afghanistan, kan vergaande consequenties hebben. In de eerste plaats is de vraag wat Nederland nu gaat doen in Afghanistan. De nieuwe regering zal antwoord moeten geven op het openstaande verzoek van de NAVO. Alle opties staan naar mijn mening open en omdat de MIVD vooruit moet kijken, betekent dit qua werkdruk voorlopig geen verlichting, maar juist een verzwaaring rond de te maken keuze voor de nieuwe regering.

Verkiezingsstrijd

In de tweede plaats is de verkiezingsstrijd losgebarsten en de daaronder liggende partijprogramma's laten ons soms de wenkbrauwen fronsen. Het CDA wil blijkbaar bureau HALT, de reclassering en de AIVD en de MIVD samenvoegen. Mevrouw Verdonks TON wil een ministerie van Veiligheid. Wat dat voor consequenties voor de inlichtingendiensten zal hebben is onduidelijk. Bij de uiteindelijke coalitievorming zal blijken wat er van die programma's overeind blijft. Om deze turbulentie kunnen we niet heen, daar zullen we dus dwars dóórheen moeten.

Bij Defensie hebben we financiële problemen met als gevolg dat er algemene maatregelen van bestuur zijn getroffen voor heel Defensie en dus ook voor de MIVD. Dat komt bij ons nogal hard aan, gezien de relatief eenzijdige grote investeringen in ICT en alles wat daarmee samenhangt. Er wordt door de plaatsver-



vangend directeur, hoofd stafafdeling Beleid en hoofd stafafdeling Control hard aan gewerkt om de schade zo beperkt mogelijk te houden. Ook door deze turbulentie moeten we dus heen.

Actie-reactie

De negatieve publiciteit lijkt weer even achter ons, maar dit kan zo maar weer de kop opsteken. Onze organisatie is immers nadrukkelijk aanwezig op alle terreinen van ons werkgebied. En actie leidt tot reactie (positief en negatief); we zullen hier dus aan moeten wennen. Deze turbulentie valt dus zeker niet te vermijden. De relatie met partnerdiensten is beter dan ooit tevoren. We zijn uitgenodigd om aan diverse fora van internationale grote diensten deel te nemen. Met de AIVD hebben we inmiddels een tweede, gezamenlijk en tevens laatste team operationeel. De gezamenlijke unit Contraproliferatie heeft in de eerste week van april de kranten gehaald als gevolg van een eclatant succes! Om deze turbulentie willen we niet heen. Kortom de riemen moeten nog even vast, maar de zon schijnt boven de wolken, de lente begint zich te ontvouwen, de vakantie komt langzaam in zicht en het wachten is op de PING het wachten is op de PING en het doven van de lampjes 'riemen vast'!

Pieter Cobelens, Generaal-majoor

p.s. De dame en de heren die de Beach 2 Border fietstocht hebben geregeld, heel veel dank voor een fantastische dag. Het verslag vindt u op pagina 23.

Numb3rs & Crime Scene Investigation in Afghanistan

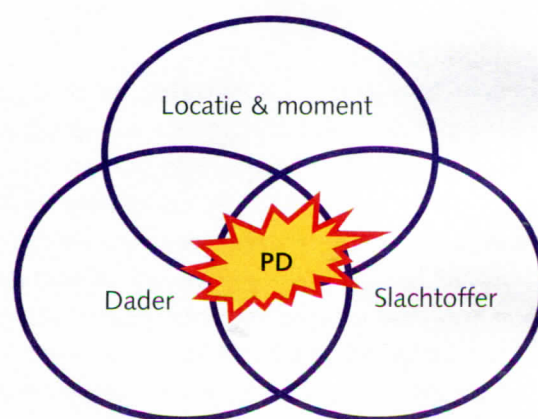
Met een ernstig gezicht stapt Grissom onder het afzetlint door en betreedt de Plaats Delict om onderzoek te doen naar de toedracht van de moord. Hij maakt foto's, neemt monsters, gaat op zoek naar vingerafdrukken en verdachte voorwerpen die iets over het gebeurde kunnen prijsgeven. Even later komt professor Charlie Eppes het PD bekijken. Eppes is een wiskundige die de FBI helpt om numerieke logica in schijnbaar niet gerelateerde misdaden te ontrafelen. Zomaar een scène uit de veelbekeken series Crime Scene Investigation en Numb3rs. Voor de Geographic Profiler is het realiteit: CSI in Afghanistan. "Het Nederlandse personeel waarmee ik gewerkt heb, heeft een bijzonder goede kennis en kunde op het gebied van Geographic Profiling", zegt prof. dr. Kim Rossmo, als research professor verbonden aan het Department of Criminal Justice van Texas State University in de VS.

Hoe vind je de persoon die verantwoordelijk is voor het plaatsen van een IED? Dat is - kort door de bocht - de vraag waar de *Geographic Profilers* in Afghanistan zich mee bezig houden. Net als de onderzoekers uit CSI gaan zij op de Plaats Delict op zoek naar gegevens, die worden gecombineerd met tal van andere informatie. Met als resultaat dat doorgaans vrij nauwkeurig kan worden aangegeven wat de verblijfplaats van de dader is. Dit gebeurt in het kader van *Geo Referenced Intelligence Fusion* of 'GRIF', een nieuwe defensie-inlichtingendisipline die in 2009 door de Directeur MIVD, generaal-majoor Cobelens werd geïmplementeerd om onder andere de bestrijding van bermbommen te verbeteren.

Drie ruimtelijke omgevingen

Bij Geographic Profiling wordt ondermeer een wiskundig algoritme gebruikt om een zogenaamd ankerpunt te vinden. Dat punt, de plaatst waar iemand de meeste tijd doorbrengt (dus woont, werkt of recreëert), fungeert vaak als vertrekpunt voor criminele activiteiten. Dit vertrekpunt is te vinden uit berekening met als 'input' de ligging van de verschillende

Plaatsen Delict (of incident locaties). Deze PD's dienen echter wel aan elkaar *gelinked* te zijn. Dat wil zeggen: de delicten dienen door één en dezelfde persoon te zijn gepleegd. Een Plaats Delict kan worden beschouwd als de (toevallige) samenkomst van een dader en slachtoffer(s) op een zekere locatie en moment. (zie onderstaand figuur).



Locaties en momenten kunnen door de dader zowel toevallig als weloverwogen zijn gekozen.



Indien er meerdere slachtoffers zijn, en ook PD's, is er sprake van een serie. Specifiek voor *Geographic Profiling* (of: geruimtelijke gedragswetenschap) is dat deze onderzoeksmethodologie een combinatie is van inzichten uit de ruimtelijke gedragswetenschappen, ruimtelijke inlichtingenanalyse, ruimtelijke criminologie en gedragsgeografie. Daarbij heeft het een sterke wiskundige basis. "Ruimtelijke aspecten kunnen het best beschreven worden als de omgeving waarin iemand zich bevindt en beweegt, kortom: waarin men zich ruimtelijk gedraagt. Zo'n omgeving wordt ook wel een *activity space* genoemd.

Ieder mens heeft namelijk een *activity space* en bepaalde dagelijkse routines", zegt een *Geographic Profiler* van de MIVD. "Op basis hiervan kun je veel te weten komen over iemands gewoontes en gedragingen. Dat klinkt al snel *creepy*. Mensen willen niet voorspelbaar zijn. Maar ga maar na: je hebt een woonplaats en vandaar uit ga je naar je werk. Op de route doe je misschien boodschappen. Je pint geld. Je drinkt een biertje. Dan heb je al snel een profiel van waar de dader het

merendeel van zijn dag uithangt."

Een andere eigenschap van mensen en ook van criminelen is dat ze doorgaans gemakzuchtig zijn ingesteld. Vaak winkelt men bij voorkeur in de eigen vertrouwde woonomgeving of kiest men een locatie waar zonder al te veel moeite een misdaad is te plegen. De omgeving moet echter ook 'meewerken'. Zo kan de omgeving mogelijkheden bieden, of iemand juist belemmeren in het plegen van een misdrijf of aanslag. Een open vlakte, maakt het moeilijk een misdaad te plegen, terwijl bijvoorbeeld dichte begroeiing langs een route juist verdachte zaken kunnen maskeren. Daarbij komt ook dat elke dader een bepaalde zone heeft waar hij zich het meest op zijn gemak voelt om een misdaad te plegen, stelt de GP'er van de MIVD. "Ver genoeg van huis om niet herkend te worden, maar wel dichtbij genoeg om de omgeving goed te kennen. Dat is de comfortzone."

Als laatste is er de cirkel rond het slachtoffer. "De dader en het slachtoffer moeten elkaar op enig moment hebben ontmoet. Daarom moeten we ook het omgevingsgebied van het slachtoffer bepalen." Daar waar de drie cirkels elkaar overlappen kan door middel van

het Geoprofiling Algoritme, een wiskundige formule, het ankerpunt nauwkeurig worden berekend. De Geographic Profiler van Defensie legt een waargebeurde "oefen" casus van het KLPD uit welke in de opleiding werd behandeld. Tijdens de training (zie kader) zijn alle zestien PD's van een serie zedenmisdrijven bezocht. Het eerste deel van de PD's lag in een landelijk gebied, terwijl het andere deel zich in stedelijk gebied bevond. De PD's werden in chronologische volgorde bezocht om bepaalde ontwikkelingen op het gebied van gedrag en werkwijze van de dader te kunnen onderkennen. Op de PD werd gelet op zaken als bereikbaarheid, vluchtmogelijkheden, zichtbaarheid vanaf de weg. Van te voren was, aan de hand van de oorspronkelijke processen verbaal, van elke zaak een kort verslag van de gebeurtenissen in de engelse taal opgesteld, zodat Kim Rossmo zich een goed beeld kon vormen en daarmee in staat was de trainees te instrueren. De gehele inspectie nam behoorlijk wat tijd in beslag omdat de PD's nogal ver uit elkaar lagen. Ook in de tijd gezien lagen de delicten ver uit elkaar. Tussen de landelijke- en stedelijke serie zat een tijdspanne van zo'n tien jaar. Toch waren alle zaken aan één en dezelfde dader toe te wijzen. De dader werd eind jaren '80 gepakt en veroordeeld. Als onderdeel van de opleiding werd een berekening gemaakt van het ankerpunt van de dader. De studenten konden tot op de wijk nauwkeurig aangeven waar de dader daadwerkelijk opgepakt kon worden.

Netwerkanalyse

Dit lijkt nog steeds erg veel op *Crime Scene Investigation*. Wat heeft dat met Defensie te maken? "IED's zijn een van de grootste bedreigingen waar de **coalitie-forces** in Irak en Afghanistan mee te maken hebben", zegt prof. Dr. Kim Rossmo, auteur van het boek *Geographic Profiling*. "En het is de verwachting dat het in komende conflicten een probleem blijft. Voertuigen beter bepantseren heeft niet gewerkt, omdat de tegenstanders simpelweg grotere bommen maakten. Daarom is het noodzakelijk geworden om het IED-netwerk te verstoren. De hoofdlocaties van het distributienetwerk vaststellen is een essentieel onderdeel van deze strategie. Geographic Profile kan hierbij zeer goed werken." De Geographic Profiler van de MIVD/Defensie geeft een fictief voorbeeld. "Er zijn ver-

schillende IED's gevonden. Na analyse blijkt dat ze aan elkaar gelinked kunnen worden. Nu willen we natuurlijk weten waar we de dader kunnen vinden. De IED's liggen overal verspreid door de regio, maar wel allemaal langs wegen. Het middelpunt van de IED's is een kale rotspunt. De dader woont in dit geval dus niet in het midden. Dus moet het ankerpunt op een andere manier berekend worden. Door het ruimtelijk gedrag te analyseren en te combineren met mogelijkheden en beperkingen in het terrein, wordt een ruimtelijk gedragsprofiel samengesteld. Vervolgens wordt dit gedragsprofiel gecombineerd met het Geoprofiling Algoritme, een wiskundige formule waarmee het meest waarschijnlijke ankerpunt uitgerekend kan worden." In dit geval lag het ankerpunt helemaal niet in het midden van de incidenten, maar meer aan de rand en viel het precies samen met een klein dorpje dat bekend stond als 'pro-taliban'. "Het blijft fascinerend", zegt de GP'er enthousiast: "De omgeving bestaat voor negentig procent uit kale vlakke met vijf kleine nederzettingen. Daarvan is één nederzetting vijandig en het profiel valt precies samen met juist dat dorpje."

Onconventionele vijand

Hoewel ontwikkeld voor de politie, heeft deze onderzoeksmethode zich volgens de Geographic Profiler, in Afghanistan en Irak bewezen. "Het is een goed hulpmiddel tegen een onconventionele vijand waar de coalitietroepen in Afghanistan en Irak mee te maken hebben. In Kandahar deden we onderzoek waaruit bleek dat het gedrag van mensen onbewust routinematig en dus voorspelbaar is. En daar maken wij gebruik van. In Afghanistan moeten we een complex netwerk blootleggen. Dat netwerk strekt zich uit van een component van de IED die in het buitenland is gemaakt met behulp van cyberspace trainingfaciliteiten tot degene die de IED daadwerkelijk plaatst. We hebben te maken met verborgen moordwapens die geplaatst zijn door onzichtbare vijanden, die van de juiste goederen worden voorzien door een geheim netwerk. Door de achtergelaten aanwijzingen op een Plaatst Delict te analyseren, kunnen we de onzichtbare vijand lokaliseren, identificeren en hun werkzaamheden verstoren."



Van 9 t/m 18 maart heeft op het DIVI een opleiding *Geoprofiling for Military Applications* plaatsgevonden. De opleiding was georganiseerd door de MIVD en werd gegeven door prof. dr. Kim Rossmo, research professor verbonden aan het Department of Criminal Justice van Texas State University in de VS, mede oprichter van het *Environmental Criminology Research Inc.* in Canada. Hij staat tevens aan het hoofd van het 'Center for Geospatial Intelligence and Investigation (GII)' van Texas State University.

Deelnemers waren analisten van MIVD, Korps Landelijke Politiediensten, DIVI en 103 ISTAR bataljon en Afdeling Joint Special Operations van DOPS.

Rossmo kijkt tevreden terug op deze opleiding. Het Nederlandse personeel waarmee ik gewerkt heb, heeft een bijzonder goede kennis en kunde op het gebied van Geographic Profiling. Door buiten het kader te denken, boeken ze vooruitgang in de methodologie en vinden ze nieuwe counter-insurgency toepassingen voor Geographic Profiling."

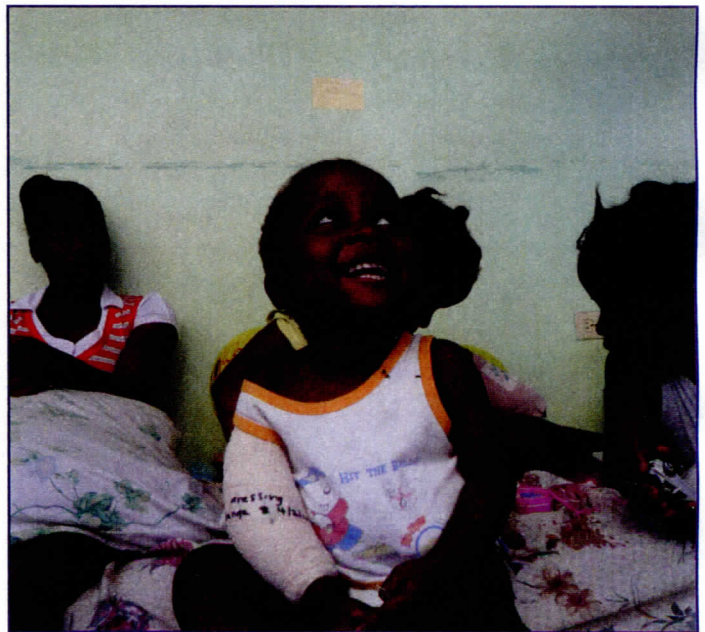
Tegenstellingen in Haïti

Hoe verwoestend de aardbeving voor Haïti is geweest, hoeveel doden en gewonden er ook zijn gevallen: al snel vindt het 'gewone' leven weer doorgang. MIVD'er adjudant Hans Poldervaart, één van de aanwezige MIVD'ers, was vlak na de aardbeving een maand in Haïti. Zijn verhaal in woord en beeld. "Wat je aantreft is chaos en puinhoop, maar je ziet ook al snel weer de verkoopstalletjes op straat verschijnen. De tegenstellingen zijn enorm."

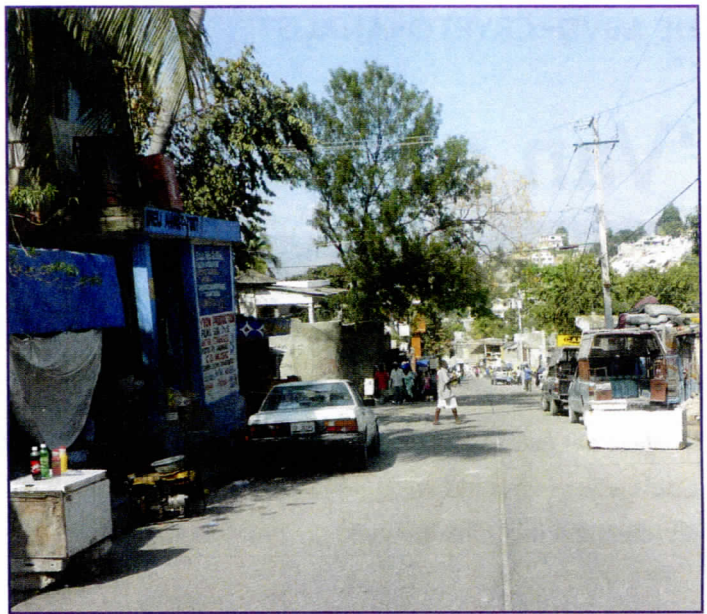
"Grote graafmachines ruimen met grof geweld puin. Blokken beton, ijzer, huisraad, maar ook ledematen worden opgepakt en afgevoerd. Op een andere plek een stuk verderop zijn forensische teams in de weer om de puinhoop stukje voor stukje af te graven. Zij proberen zo voorzichtig mogelijk te werk te gaan, om uiteindelijk eventueel onder het puin bedolven lijken te kunnen identificeren."



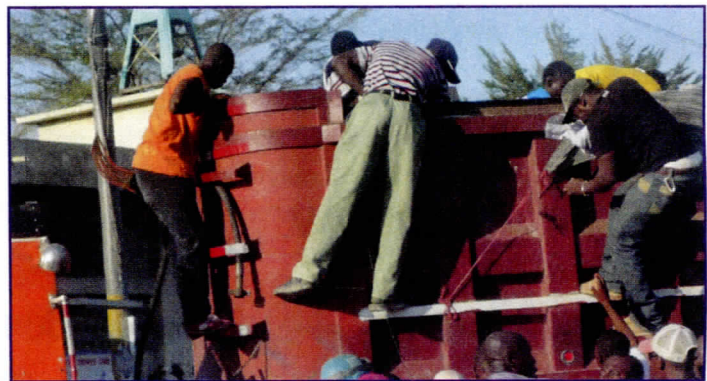
Dood – nieuw leven. De grootst mogelijke tegenstelling. In het ziekenhuis in Port-au-Prince worden niet alleen aardbevingsgerelateerde gewonden geholpen. Ook de 'gewone' patiënten komen binnen. "Het ene moment amputeert de chirurg een been. Een paar uur later komt er iemand binnen met een acute blindedarmontsteking of helpt de chirurg met een keizersnee een baby ter wereld." En terwijl Hans dagelijks wordt geconfronteerd met de verwoestende gevolgen van de aardbeving, wordt hij opa. "Ik kreeg bericht toen de bevalling was begonnen – we hadden gelukkig goede communicatiemogelijkheden. Toen mijn kleindochter Naomi was geboren, heb ik het in de Opsroom aan de Amerikanen (USSOUTHCOM) waar we dagelijks een briefing hadden verteld. Die gingen meteen staan en applaudisseerden en feliciteerden me. Geweldig!"



"Iedereen lijkt te denken: alles voor mezelf en niets voor mijn naaste", zegt Hans nog steeds verbaasd. "Delen is er niet bij. Zelfs de mensen die het goed hebben, houden alles voor zichzelf. De een rijdt in een glanzende Hummer, de ander zit in een auto waarvan de onderdelen met draadjes bij elkaar worden gehouden. Er lopen mensen verdwaasd en zonder kleding over straat, terwijl er zoveel goederen, en ook kleding, het land in worden gedragen." Tegelijkertijd vindt er ook veel fraude plaats, vertelt Hans. "Er stond dagelijks een vrouw in de rij om een baal rijst te halen. Uiteindelijk bleek dat ze thuis al elf balen rijst had liggen en het dus eigenlijk niet nodig had. Fraude met voedselbonnen is erg gemakkelijk. Er was ook voor de aardbeving al een slechte registratie, dus als iemand zegt dat zijn gezin uit acht personen bestaat, is het moeilijk te controleren of dat ook echt zo is."



"De bevolking heeft ongelooflijk veel veerkracht. Al heel snel zag je weer verkoopstalletjes op straat verschijnen, waar van alles en nog wat werd verkocht. Gebraden kip, mobiele telefoons, noem maar op."



"In de *Meals Ready to Eat* zaten ook snoepjes", vertelt Hans. Die verzamelen de mannen om uit te delen aan kinderen. "Dat zijn mooie momenten. Als we een kind op straat zagen, dan wenkten we die om het een snoepje te kunnen geven. Dan begonnen die koppies te glimmen en zwaaiden ze ons na. Op een ander moment kwamen de kinderen vragend om dollars, water en drinken op ons af, terwijl ze ook met een mobiele telefoon rond lopen."



Op 10 maart was Hans één van de genodigden voor een ontvangst op paleis Huis ten Bosch. Koningin Beatrix en prins Willem-Alexander ontvingen de Nederlandse hulpverleners die zich hebben ingezet bij de aardbevingsramp in Haïti. De ontvangst op Huis ten Bosch was een blijk van waardering van de koningin en de prins voor de inspanningen van de hulpverleners, meldt de Rijksvoorlichtingsdienst. Hans vond het een geweldige ervaring. "Eén voor één werden we binnengeroepen, voorgesteld en handen geschud. Toen iedereen binnen was, begaven ze zich onder de mensen om hier en daar praatjes aan te knopen."

'Van ons zul je nooit horen dat wij een programma hebben gekraakt'

Wat doet een MIVD-crypto-analist eigenlijk? Eén van hen werd geïnterviewd voor het wiskundeblad 'Pythagoras'. Ingelicht heeft dit interview met dank bewerkt en overgenomen.

Veel jongens van een jaar of tien raken gefascineerd door geheime boodschappen en codes. Had jij dat ook al in je jeugd?

Het gekke is dat ik heel weinig affiniteit had met geheimschriften maken. Wel heb ik ontzettend veel puzzels uit puzzelboekjes gemaakt. Af en toe zat daar ook een geheimschrift tussen dat moest worden opgelost. Ik had daar niet specifiek een verbintenis mee in de trant: 'Dit wordt mijn toekomst'.

Komt cryptografie voor in de studie wiskunde?

Toen ik wiskunde studeerde in Leiden was cryptografie nog geen apart vak. Wel werden bepaalde onderdelen van cryptografie genoemd in andere vakken. RSA (genoemd naar de ontwikkelaars Rivest, Shamir en Adleman) is een versleutelmethode gebaseerd op het product van twee zeer grote priemgetallen. Dit werd behandeld bij getaltheorie. Nadat ik promoveerde in de getaltheorie werd cryptografie als een apart vak geïntroduceerd in Leiden.

Hoe kwam je op het idee voor de MIVD te gaan werken?

Na mijn promotie heb ik twee jaar gewerkt bij het CWI (Centrum voor Wiskunde en Informatica) bij de werkgroep Cryptologie. Ik organiseerde daar eenmaal per maand de *Workinggroup Cryptography* voor cryptologen uit geheel Nederland. Hieraan werd ook deelgenomen door medewerkers van het

TIVC (een onderdeel van de MARID, de MARine Inlichtingen Dienst, die later opging in de MIVD). Hier leerde ik al diverse toekomstige collega's kennen. De MIVD plaatst net als enig ander bedrijf vacatures. Ik heb dus ook gesolliciteerd.

Wat houdt je baan in?

De MIVD vergaart inlichtingen- en veiligheidsinformatie voor Defensie en andere behoeftezoekers. De MIVD mag daar niet elke methode voor gebruiken, want we zijn gebonden aan de WIV (Wet op de Inlichtingen- en Veiligheidsdiensten). Zomaar een beetje James Bond spelen is er dus niet bij. Mijn afdeling verwerkt uit de ether gehaalde signalen tot informatie. Ik doe onderzoek naar methodes om gecodeerde berichten te kraken. Wij spreken trouwens over 'vercijferde' berichten. Voor het uitvoeren van de daadwerkelijke ontcijferingen is een andere sectie verantwoordelijk, die de door mij gevonden methode toepast. Het gebruik van de zo verkregen informatie is aan strenge wettelijke regels gebonden.

Kun je iets zeggen over wat voor informatie dat is, waar het vandaan komt, en hoe dat in de loop der tijd veranderd is?

Ik vrees dat ik daarover niet zo gek veel kan vertellen. Het onderdeel waar ik begon, stamt uit de tijd dat de KNIL in Indonesië vocht tegen de Japanners. Geheimschriften van de Japanners werden daar gekraakt. Later kwam de dienst naar Nederland en werd de dienst ingezet om alle mogelijke codes te kraken. Zoals ik al eerder beschreef, mogen we de codes nog steeds kraken, maar mogen we de informatie die we zodoende op het spoor komen niet zonder meer gebruiken.

Er worden nog steeds geheimschriften ontwikkeld



Zomaar een beetje James Bond spelen is er niet bij

Is veel van het werk zo langzamerhand geautomatiseerd, of is het nog steeds telkens een kwestie van slim puzzels kraken?

Zoals de meeste onderzoekers geldt ook bij ons 1% inspiratie en 99% transpiratie. Het wezenlijke denkwerk, waarbij je met pen en papier aan het werk bent is slechts een klein deel van de werkzaamheden. Voor de rest is het veel programmeren. Het is nog een hele klus om die computers efficiënt aan te sturen en in te zetten.

Wat voor computers zijn dat?

Helaas is dat een staatsgeheim.

Noemt u eens een voorbeeld van een geslaagde klus op cryptografisch gebied.

Dat moet dan van heel lang geleden zijn, anders valt het onder de geheimhoudingsplicht. Ik neem altijd het voorbeeld van een persconferentie van een rechtechteteam. Zij hadden een stel boeven gevangen dankzij een gebruikt vercijferprogramma van deze boeven. De rechtechte had dit vercijferprogramma gekraakt. Op de persconferentie hingen er twee schilderijtjes.

In één schilderijtje was de vercijferde tekst te zien, in het andere de ontcijfering. Met naam en toenaam werd het programma genoemd. Uiteraard heeft

sindsdien geen boef meer dat programma gebruikt. Dat is nu precies wat wij proberen te vermijden. Van de MIVD zul je nooit horen dat zij een zus of zo programma hebben gekraakt, want daarmee zouden we onszelf in de toekomst in de vingers kunnen snijden. Dat betekent dat de MIVD nooit in het nieuws komt.

Worden er nog steeds nieuwe geheimschriften ontwikkeld? Of zijn de bestaande geheimschriften eigenlijk wel goed genoeg?

Er worden nog steeds geheimschriften ontwikkeld. Eigenlijk moet je de vraag stellen wat een geheimschrift is. In de praktijk kun je onderscheid maken tussen een vercijferalgoritme en de toepassingen in de praktijk. Deze toepassingen zijn zeer uiteenlopend, bijvoorbeeld heel simpel vercijfering van tekst (het klassieke geheimschrift), e-mail, bestanden, harde schijven, maar ook communicatie tussen twee personen of instellingen (denk bijvoorbeeld aan GSM-verkeer, of de veilige internet-verbinding

tussen een computergebruiker en een bank), financiële interactie (chipknip, pinpas, de OV-chipkaart, rekeningrijden), elektronische verkiezingen, digitale handtekening, etc. Het aantal toepassingen is de afgelopen jaren gigantisch toegenomen. Het aantal vercijferalgoritmen neemt eveneens toe, maar niet zo dramatisch. Als antwoord op de vraag: "Zijn de geheimschriften inmiddels niet goed genoeg" zeg ik: "Kijk maar op internet". Als medewerker van de MIVD mag ik daar geen antwoord op geven. Op internet zul je zien dat nieuwe vercijferalgoritmen worden ontwikkeld, omdat er behoefte is aan een vercijferalgoritme waarop geen patenten berusten (dat is goedkoop), of die sneller zijn dan de al bestaande, of die tegen een bepaald soort aanval bestand zijn.

Kun je een concreet voorbeeld geven van wiskunde die je nodig hebt bij je werk?

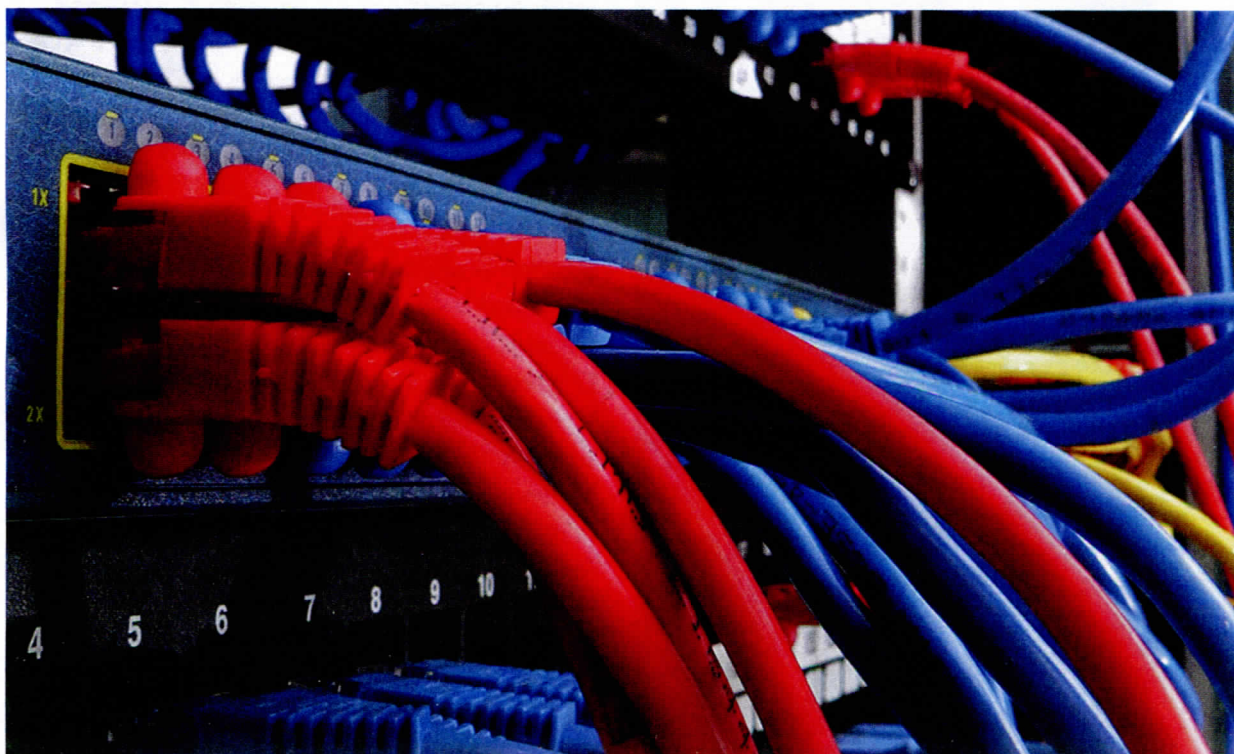
Ik moet me helaas beperken tot algemene termen. Ik denk dat voor onze sectie statistiek het belangrijkste onderdeel van de wiskunde is dat wordt gebruikt. Ik kan hier nog wel vertellen over een curieuze, onopgeloste zaak die we twee jaar geleden kregen van het Nederlands Instituut voor Militaire Historie (NIMH). Zij legden ons een telegram uit gedateerd 1913 in Albanië. Wellicht was het geheimschrift gerelateerd aan de moord op luitenant-kolonel Thomson, het eerste slachtoffer dat te betreuren was bij een vredesmissie, die in Albanië. In 1913 bestonden nog geen codeermachines of computers. Vercijfering werd in die tijd met

de hand uitgevoerd, dus heel ingewikkeld kan die niet zijn. Maar ondanks al onze inspanningen zijn we er niet uitgekomen. Er zijn veel onzekerheden: is het oorspronkelijke bericht wel in het Nederlands? Misschien was het een Albanees, Italiaans of Turks bericht. Is het bericht inderdaad gerelateerd aan de moord op Thomson? We weten het niet. Het NIMH kon evenmin aanvullende informatie verschaffen.

Hoe vervelend is het om nooit over uw werk te kunnen praten?

Geheimhouding kan frustrerend zijn, zoals blijkt uit het volgende voorbeeld. Whitfield Diffie en Martin Hellman publiceerden in 1976 een heel bijzonder algoritme, waarbij twee partijen die alleen via een onveilig kanaal kunnen communiceren, het toch eens kunnen worden over een geheime sleutel om hun berichten mee te coderen. Zij zijn daar beroemd mee geworden. Pas in 1997 werd bekend dat James H. Ellis, Clifford Cocks, en Malcolm Williamson van de Engelse Militaire Inlichtingendienst (GCHQ) al tien jaar eerder een vergelijkbaar vercijferingsalgoritme ontdekt hadden. GCHQ achtte het echter niet verstandig de resultaten van hun werknemers bekend te maken.

Dit artikel is een bewerkte versie van een artikel van Arnout Jaspers dat in februari 2010 verscheen in het wiskundetijdschrift Pythagoras. Dit tijdschrift stelt zich ten doel havo- en vwo-leerlingen kennis te laten maken met de leuke en uitdagende kanten van wiskunde.



Voel jij je veilig?

Onlangs was ik met enkele collega's op de Beveiligingslanddag 2010 in het Marine Evenementencomplex te Amsterdam. Deze dag wordt jaarlijks georganiseerd en de Beveiligingsautoriteit neemt dan de gelegenheid om alle beveiligingsfunctionarissen in de veiligheidsketen binnen Defensie bij te praten over de laatste stand van zaken. De nieuwe campagne rond de 6 Gouden Beveiligingsregels bijvoorbeeld.

Door: Veiligheidsofficier, Bureau Veiligheidszaken

De Beveiligingsautoriteit (BA) is de hoogste autoriteit op dit vakgebied en valt direct onder de secretaris-generaal (SG) op het departement van Defensie. De BA maakt het beleid maar controleert dit ook zelf op de uitvoering. Ook voor onze dienst dus de leidende instantie. Niet alleen de BA en zijn staf waren aanwezig om zichzelf te presenteren, maar hij had ook enkele andere belangrijke spelers in de keten uitgenodigd om de nodige toelichting te geven op ontwikkelingen. Zo was de Commandant Defensie Inlichtingen en Veiligheidsinstituut aanwezig - voor ingewijden een oude bekende van onze dienst - en was de sectie Elektronische Veiligheidsonderzoeken van onze dienst present met een interessant verhaal over de laatste technieken met betrekking tot deze veiligheidsonderzoeken. En *last but not least* was er aandacht voor de toezichtbezoeken. Veel aandacht dus voor opleidingsaspecten, techniek en de fysieke aspecten van beveiliging.

Oranje foldertjes

Op mijn stoel in de zaal vond ik een aantal kleine oranje Z-cards. Op deze kleine foldertjes staat de essentie van het beveiligingsbeleid verwoord. Zes basisprincipes maken voor iedereen duidelijk waar beveiliging om draait, namelijk zelf verantwoordelijkheid nemen voor veiligheid door het juiste te doen en hierbij een voorbeeld te zijn voor collega's, ondergeschikten en meerderen. De regels zijn er dan ook niet slechts voor de organisatie, maar ten bate van onze eigen veiligheid. Daar doen wij dus allemaal ons voordeel mee.

De 6 Gouden Beveiligingsregels:

1. Spreek elkaar aan op gedrag.
2. Laat geen vreemden toe in onze gebouwen en systemen.
3. Lek geen informatie. Bewust of onbewust.
4. Weet met wie je zaken doet.
5. Voorkom misbruik en diefstal
6. Meld overtredingen en verdachte omstandigheden.

De oranje foldertjes van de BA waarin de 6 Gouden Beveiligingsregels staan, worden op dit moment verspreid binnen Defensie. Zonder elke regel hier uitvoerig te behandelen springen regel 1 en 6 er voor mij uit, omdat dit een betrokken actieve houding verwacht van iedere Defensiemedewerker afzonderlijk. Doe de dingen bewust en ga er niet van uit dat een ander het opknapt. Dit spreekt mij aan. Verder is regel 4 een doordener. Ben ik dan verantwoordelijk voor het vaststellen van de identiteit van een andere partij, ook als de communicatie plaatsvindt via de telefoon of per internet? Het antwoord is volmondig 'JA'. De gevaren van het ongewild lekken van informatie via een telefoongesprek, een e-mail of via een internetsite, denk aan Hyves, LinkedIn, Twitter etc, worden nog steeds onderschat.

Niet vrijblijvend

Genoeg advies, die krijgt u voldoende aangereikt. Als u het goede *doet*, dan gaat het goed met onze organisatie. De regels zijn trouwens niet vrijblijvend. Doet u niet het goede, dan zijn er mogelijk rechtspositionele gevolgen of tuchtrechtelijke sancties. Daar willen we liever niet aan denken. Het devies is dan ook: voorkomen is beter dan genezen, zeker als het om onze veiligheid gaat.

Aeolus: het nieuwe werken

Aeolus gaat deze zomer live! Daarmee treedt het langverwachte systeem in werking. "Maar", benadrukt Hoofd Bureau Personele Veiligheid, "aan het eind van het jaar komt het hele proces pas echt goed op stoom. Dan pas kunnen we echt resultaat verwachten."

We zaten echt te springen om een nieuw systeem", geeft hoofd Bureau Personele Veiligheid (BPV) aan. "Een systeem van deze eeuw, met een proces dat niet op papier, maar digitaal verloopt. Daardoor zal de samenwerking met andere bureaus en organisaties vele malen efficiënter gaan en is er ook meer tijd voor informatieverwerking en analyse."

De twee hoofddoelen van het nieuwe systeem Aeolus zijn dan ook: meer diepgang in de veiligheidsonderzoeken en een hogere capaciteit, waardoor meer onderzoeken in dezelfde tijd, danwel sneller uitgevoerd kunnen worden.

"Het gedigitaliseerde proces komt de workflow ten goede", zegt hoofd Afdeling Contra-Inlichtingen en Veiligheid (ACIV). Dit betekent een upgrade in kwaliteit. We weten nu over de hele lijn van het proces veiligheidsonderzoeken beter wat er gebeurd. Er kunnen bijvoorbeeld geen dossiers zoekraken, we worden door het systeem op tijd gewaarschuwd wanneer de termijn van een onderzoek wordt overschreden. Op die manier kunnen we ook eerder ingrijpen als de doorlooptijd wordt overschreden."

Per jaar worden er gemiddeld 30.000 veiligheidsonderzoeken aangevraagd. Een van de manco's van de 'oude manier van werken' was dat er nooit goed zicht was in welke tijd van het jaar een piek was. Hoofd ACIV: "Anticiperen op grote werkbelasting was daardoor niet mogelijk. Nu het proces geautomatiseerd is, kunnen we beter monitoren. Daardoor zijn we in staat te zien welke trends er gedurende een jaar zijn, wanneer er een piekbelasting is."

Achterstand

De invoering van Aeolus maakt deel uit van een heel pakket aan maatregelen om de bedrijfsvoering binnen ACIV te verbeteren. Voor BPV betekent dit dat naast het nieuwe systeem, het bureau het komende half jaar een personele uitbreiding krijgt. Ook heeft het personeel een hogere opleiding gehad en zijn de werkprocessen verbeterd. In samenwerking met het Defensie Inlichtingen- en Veiligheidsinstituut komt er een nieuw opleidingsplan voor analisten en veldonderzoekers. H-ACIV: "Zo willen we meer kwaliteit bereiken. Het gaat om het totale pakket." Had dit niet veel eerder gemoeten, problemen met de doorlooptijd van de onderzoeken spelen al langer? "Het probleem heeft eindelijk de juiste aandacht gekregen", antwoordt H-ACIV. Het probleem lag veel dieper dan we aanvankelijk dachten. En toen dat eenmaal boven water was,

moest er nog een oplossing worden gerealiseerd. Daar gaat tijd overheen. Vooral als je bedenkt dat het werk ook gewoon doorging. De implementatie van het nieuwe systeem, het opleiden van

Straks is alle ellende een gepasseerd station

het personeel, dat kwam er allemaal bij. Als straks de processen goed zijn ingeregeld en de kinderziekten uit het systeem zijn gehaald, is alle ellende een gepasseerd station." "Ook de medewerkers ervaren een druk omdat de achterstand groot is", reageert H-BPV. Alle defensieonderdelen zijn klant van ons. Die wil je tevreden houden door de doorlooptijd van het onderzoek zo kort mogelijk te houden, maar je wilt ook de onderzoeken zorgvuldig uitvoeren. Dat kunnen we binnenkort realiseren. Maar we moeten ook reëel zijn: we kunnen de komende tijd nog veel kinderziekten in het systeem verwachten en het proces moet nog goed ingeregeld worden. Daarnaast zijn we qua bezetting nog niet op volledige sterkte. Het systeem heeft veel potentie, maar we zitten nu nog in de beginfase."

De invoering van een dergelijk systeem heeft heel wat voeten in aarde, zegt ook de projectleider van de implementatie van het systeem. "Zoiets kan niet in een keer helemaal goed zijn. Daar is het systeem te omvangrijk voor. Daarom zullen er het komende

half jaar steeds weer nieuwe versies worden ingevoerd. We moeten dus niet verwachten dat de doorlooptijd van de veiligheidsonderzoeken ineens flink verkort. Er gaat nog even overheen voor het resultaat echt zichtbaar wordt."

Veiligheidsonderzoek

Een veiligheidsonderzoek komt in hoge mate overeen met het inlichtingenproces, legt H-BPV uit. "Hier gaat het om onderzoek naar een persoon en zijn omgeving. Ook hier is de cyclus: verwerven, verwerken, analyseren en rapporteren aan de orde. Er worden informatiebronnen binnen en buiten de overheid gebruikt. De veldorganisaties zijn experts op het gebied van het houden van interviews.

In het onderzoek wordt op een aantal criteria gelet. Er wordt gekeken of iemand integer, onafhankelijk, loyaal en eerlijk is. Er zijn een aantal indicatoren die er op kunnen wijzen dat iemand kwetsbaar is of een risico vormt voor de nationale veiligheid. Leugenachtig of heimelijk gedrag bijvoorbeeld. Hierdoor kan iemand gevoelig zijn voor chantage en niet-integer gedrag van anderen. Zware financiële problemen kunnen ook iemand kwetsbaar maken voor chantage of omkoping. Een verslaving kan iemand afhankelijk maken, waardoor iemand onvoldoende in staat is een vertrouwensfunctie betrouwbaar te vervullen. Bovendien bestaat door het gebruik van verboden middelen zoals drugs, verbinding met het criminele milieu. Een andere indicator is het deelnemen of het verlenen van steun aan activiteiten die de nationale veiligheid kunnen schaden. Dat kan zijn op het gebied van terrorisme, gewelddadig activisme, extremisme, spionage, proliferatie van massavernietigingswapens en georganiseerde misdaad. Ook wordt er gekeken naar justitiële antecedenten. Hieruit kan blijken of iemand problemen heeft met eerlijkheid, onafhankelijkheid, loyaliteit en integriteit.

Risico op terreuraanslagen in Europa hoog

Het risico op terreuraanslagen in Europa blijft onverminderd hoog. "Ook al was Europa al een tijdje geen doelwit van aanslagen, betekent dat niet dat er geen dreiging meer is", zei de Europese antiterreurcoördinator Gilles de Kerchove tegen het Duitse persbureau DPA.

Organisaties als al-Qaeda zijn volgens hem nog heel actief, ook al is het aantal aanslagen en pogingen tot aanslag verminderd. De laatste grote aanslagen waren in 2004 in Madrid (191 doden) en in 2005 in Londen (56 doden). De Belg De Kerchove volgde in 2007 Gijs de Vries op, die de baan van Europees antiterreurcoördinator als eerste vervulde. Duitsland, Groot-Brittannië en Spanje zijn volgens hem de landen met het hoogste risico. Maar de dreiging verschuift steeds naar landen waar autoriteiten streng optreden tegen islamieten.

Nederland

Nederland en Groot-Brittannië hebben volgens hem hun alarmniveau verlaagd. "Men kan niet altijd op het hoogste niveau blijven, omdat dat te veel kost en de alertheid van de burgers aantast", stelt De Kerchove. Volgens De Kerchove moeten de EU-landen in de strijd tegen terrorisme de ontwikkelingslanden bij de hand nemen. "Dat betekent: ontwikkelingspolitiek in de vorm van preventie tegen radicalisering".

Bangladesh

Bijvoorbeeld in Bangladesh zijn veel jonge mannen zonder enig toekomstperspectief. "Hun enige opleiding bestaat eruit om de koran in het Arabisch uit het hoofd te leren. Dat geeft hen later geen baan." De wereldwijde recessie verergert de situatie. "De EU-landen verlagen hun uitgaven voor hulpprogramma's. Ze zouden juist meer moeten helpen", vindt de antiterreurcoördinator.

(Bron: ANP)

Arrestaties na informatie AIVD over export aan Iran

Op basis van informatie van de Unit Contraproliferatie, een samenwerkingsverband van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), heeft het OM dinsdag invallen gedaan bij een bedrijf dat de exportregels heeft overtreden. Dit heeft de AIVD bekendgemaakt.

De FIOD heeft op elf plekken doorzoekingen verricht en vier verdachten aangehouden. Het onderzoek van de FIOD richt zich op een bedrijf dat zaken doet met Iran en zogeheten 'dual use' goederen verhandelt. Dat zijn goederen voor tweërlei gebruik die onder andere voor de ontwikkeling en productie van massavernietigingswapens gebruikt kunnen worden. Het OM zegt aanwijzingen te hebben dat het bedrijf de goederen zonder toestemming aan Iran heeft geleverd.

(Bron: Blik op Nieuws)

Spionagerisico's in kaart gebracht

De Kwetsbaarheidsanalyse Spionage, uitgevoerd door de AIVD en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), is op voorstel van demissionair minister Hirsch Ballin van BZK naar de Tweede Kamer gestuurd.

Dat er in Nederland wordt gespioneerd is al langer bekend. In de analyse heeft de AIVD nu samen met geselecteerde bedrijven, overheden en wetenschappelijke instellingen in kaart gebracht welke informatie voor buitenlandse inlichtingendiensten interessant is en hoe die het beste kan worden beschermd. Het rapport stelt bedrijven, instellingen en overheden in staat om maatregelen te nemen die hen, en dus Nederland, op lange termijn moeten beschermen tegen de risico's van spionage.

Uit de analyse blijkt dat bepaalde ontwikkelingen de kwetsbaarheid voor spionage onbedoeld hebben vergroot. Een ongewenst gevolg van de door Nederland gewenste kennismigratie kan zijn dat buitenlandse inlichtingendiensten zich als onderzoeker of als student voordoen. Een ander voorbeeld is dat het uitbesteden van systeem- en serverbeheer ertoe kan leiden dat kwetsbare informatie onbedoeld over de grens wordt opgeslagen (op computers in het buitenland), waardoor buitenlandse inlichtingendiensten er gemakkelijker bij kunnen.

(Bron: Ministerraad, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Inlichtingendiensten plaatsten ruim duizend taps

De inlichtingendiensten hebben vorig jaar ruim 1100 taps geplaatst. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) zette er 1078 uit, de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) 53, meldt het ministerie van Binnenlandse Zaken in een brief aan de Tweede Kamer. De cijfers werden vrijgegeven, nadat de Tweede Kamer in februari instemde met een motie van onder meer de SP. Hiermee werd het kabinet opgedragen openbaar te maken hoe vaak in Nederland telefoons werden afgetapt door de inlichtingendiensten.

Het kabinet maakte alleen bekend welke telefoontjes door het Korps Landelijke Politiediensten worden afgeluisterd. Zij doen dat voor alle politiekorpsen, de bijzondere opsporingsdiensten, zoals de fiscale opsporingsdiensten en de Algemene Inspectiedienst, en de koninklijke marechaussee. Het aantal personen bij wie de inlichtingendiensten vorig jaar de ruim 1100 taps plaatsten, ligt volgens de minister lager, omdat personen meerdere telefoonnummers in gebruik kunnen hebben of van telefoonnummer wisselen. De taps van de inlichtingendiensten zijn slechts een fractie van de duizenden taps die jaarlijks in Nederland worden ingezet voor opsporingsdoeleinden.

(Bron: NOVUM)

Pakistan wil atoomspion Khan onderzoeken

De Pakistaanse regering heeft een rechtbank in Islamabad om toestemming gevraagd om onderzoek te doen naar de atoomgeleerde Abdul Qadeer Khan. Dat heeft een regeringsfunctionaris maandag laten weten. Het juridisch verzoek komt enkele dagen voor het begin van overleg tussen Pakistan en de Verenigde Staten. Het Aziatische land wil een nucleaire deal met de VS sluiten.

Khan bekende in 2004 dat hij nucleaire geheimen had verkocht aan Iran, Noord-Korea en Libië. Daardoor viel hij in ongenade bij de regering, die deze kwestie nu verder wil onderzoeken. Veel Pakistani zien Khan als held, omdat hij het land de kernbom heeft gegeven.

Khan werkte in het verleden bij ultracentrifugefabriek Urenco in Almelo. Daar zou hij technologie voor het verrijken van uranium hebben gestolen, zodat hij in Pakistan een kernbom kon ontwikkelen. In 1983 veroordeelde een rechtbank in Nederland hem wegens nucleaire spionage, maar het gerechtshof sprak hem in hoger beroep vrij wegens een vormfout.

(Bron: ANP)

Akkoord over nucleaire veiligheid

De deelnemers aan de internationale top over nucleaire veiligheid in Washington hebben dinsdag een reeks afspraken met elkaar gemaakt om de risico's van bijvoorbeeld atoomterrorisme te bestrijden.

De Amerikaanse president Barack Obama zei na afloop van de top dat "de wereld veiliger zal zijn" in de toekomst, "dankzij de stappen die we hebben gezet". Regeringsleiders van de 47 deelnemende landen hebben onder meer afgesproken dat er binnen vier jaar een einde moet komen aan de onduidelijkheid over waar bepaalde nucleaire materialen zich bevinden. Deze materialen, die levensgevaarlijk kunnen zijn als ze in handen vallen van terroristen, moeten in 2014 op een aantal strengbeveiligde locaties liggen opgeslagen. Obama denkt dat de extra inspanningen een bedrag van circa 10 miljard dollar (ruim 7,3 miljard euro) aan investeringen vergt van de internationale gemeenschap.

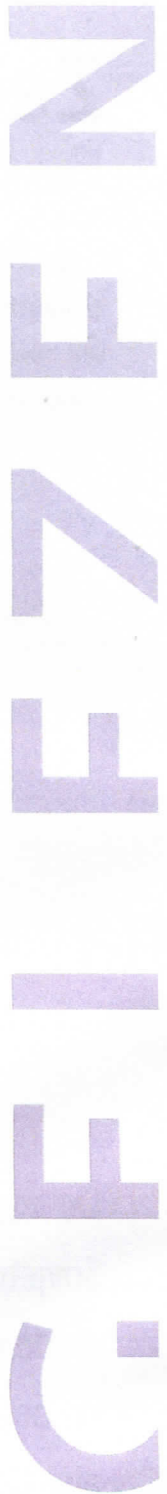
Illegale handel

Ook willen de landen meer gaan samenwerken bij het bestrijden van illegale handel in nucleair materiaal. Het Internationaal Atoomagentschap (IAEA), de atoomwaakhond van de Verenigde Naties, blijft het belangrijkste orgaan wat betreft de controle op zaken die te maken hebben met kernenergie en atoomwapens.

Tegelijkertijd benadrukken de ondertekenaars van de verklaring dat de veiligheidsmaatregelen niet mogen leiden tot het inperken van het recht van landen om nucleaire programma's op te zetten voor de ontwikkeling van bijvoorbeeld kernenergiecentrales.

De Amerikaanse president Barack Obama waarschuwde er op de tweede en laatste dag van de top voor dat het een "catastrofe voor de wereld" zou zijn als terroristen erin zouden slagen een atoomwapen te bemachtigen.(...)

(Bron: AFP)



Zee van geheimen

Geheimen van de zee. Duikers zullen meteen aan onontdekte koraalriffen denken. En inlichtingenmensen? Wies Platje schreef een boek inlichtingenoperaties tijdens de Koude Oorlog door zowel de NAVO-landen als de Sovjet-Unie.

De Atalanta-missie is succesvol. Nederland is zichtbaar in de golf van Aden en Somalische wateren en levert daarbij bijdragen aan de bescherming van de voedseltransporten van het World Food Programme. Tijdens de Koude Oorlog was de maritieme missie veel minder zichtbaarder. Maar misschien wel veel spectaculairder. "De confrontatie op zee was in sommige perioden bij tijd en wijle grimmig en dreigend, en de uitgevoerde inlichtingenoperaties waren niet zelden spectaculair", schrijft Platje in zijn boek. "Er is een aantal punten in de Koude Oorlog geweest dat het er echt om spande. Een voorbeeld daarvan is de achtervolging door de Amerikaanse marine tijdens de Cubaanse crisis van een Sovjetonderzeeboot. Er was reëel gevaar dat de gestreste jonge commandant een verkeerde keuze zou maken en zijn nucleaire wapen zou lanceren."

De voornaamste taak van de Sovjetmarine bestond aan het einde van de Koude Oorlog uit de bescherming van de nucleaire slagkracht door strategische onderzeeboten

Nucleaire slagkracht
Platje beschrijft in zijn boek de meer dan veertig jaar durende confrontatie tussen de zeestrijdkrachten van de NAVO en de Sovjetvloot. Hij beschrijft de manier waarop wederzijds werd geprobeerd strategische, operationele en

technische informatie over de zeestrijdkrachten van de tegenstander te vergaren.

De Sovjetmarine ontwikkelde zich gedurende de Koude Oorlog van een marine waarmee op beperkte schaal kustverdedigingsoperaties konden worden uitgevoerd tot een zeemacht die in staat was tot het ontplooiën van een militaire presentie op alle wereldzeeën. De Sovjetvloot kende aan het einde van de Koude oorlog echter weinig gehei-

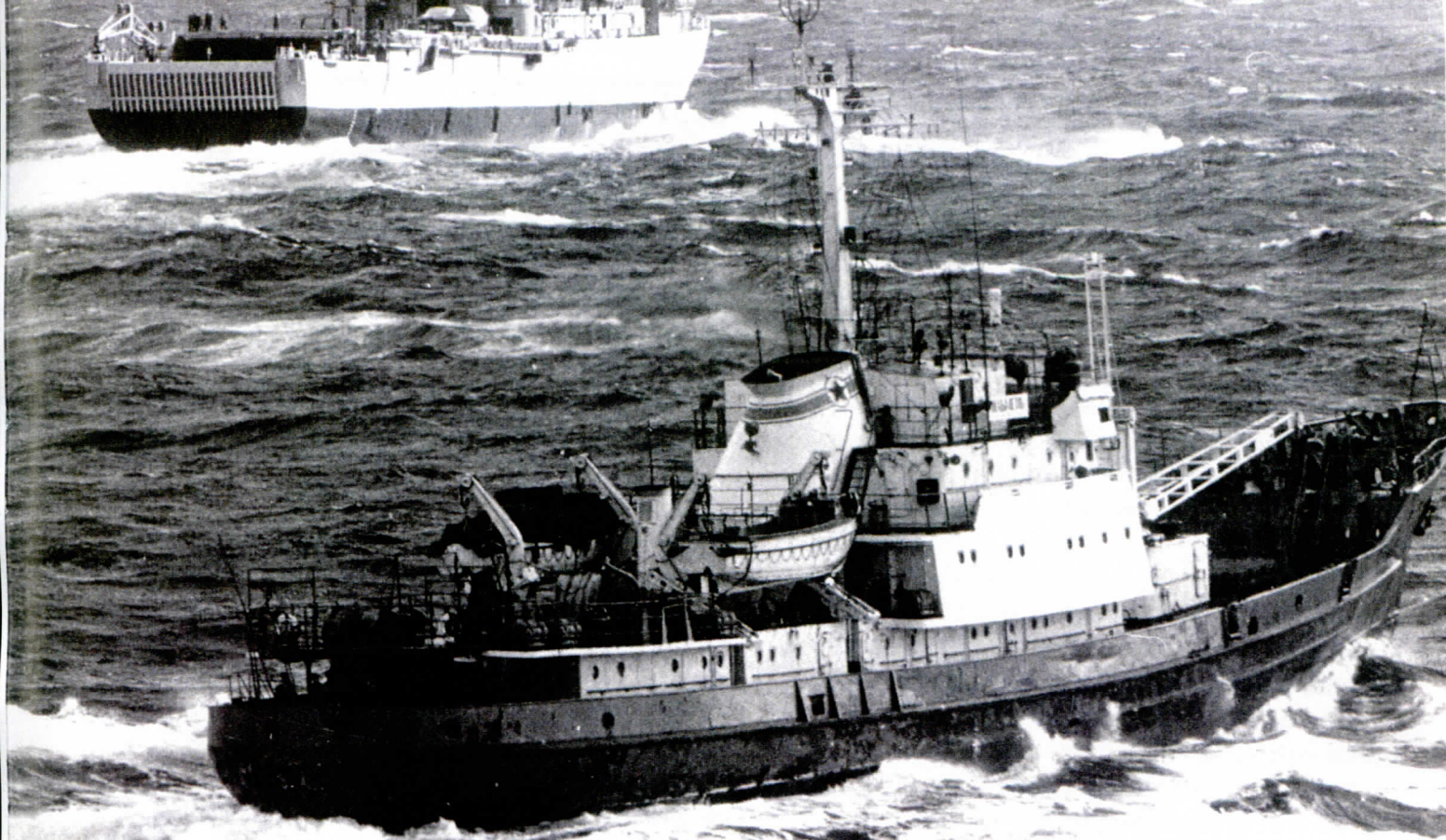
men voor de westerse inlichtingendiensten. "Operaties met oppervlakteschepen, onderzeeboten en vliegtuigen werden, zoals gezegd, nauwlettend gevolgd door NAVO-eenheden, en vooral door succesvolle onderscheppingen van de verbindingen van de Sovjetmarine werd een goed inzicht verkregen in de staat van operationele gereedheid en logistieke ondersteuning."

"De inschatting van de NAVO van de maritieme strategie van de Sovjet-Unie was dat, bij een conflict met het Westen de Sovjetvloot zou uitvaren om de trans-Atlantische zeeverbindingen te verstoren, die waren namelijk voor de NAVO van levensbelang. Deze visie moest in de jaren tachtig voor een groot deel worden bijgesteld. De voornaamste taak van de Sovjetmarine bestond aan het einde van de Koude Oorlog uit de bescherming van de nucleaire slagkracht door strategische onderzeeboten die permanent patrouilleerden in de noordelijke gebieden van de Atlantische Oceaan en de Stille Oceaan. De eerdere visie was op basis van spectaculaire inlichtingenoperaties van de Amerikaanse Onderzeedienst bijgesteld. Hierbij werden onder meer communicatiekabels in de Zee van Ochhotsk en de Barentszee afgetapt.

Met het groeien van de marine, kreeg de Sovjet-Unie meer behoefte aan inlichtingen over westerse zeestrijdkrachten. Centraal hierbij stond het verkrijgen van een tijdige waarschuwing voor een aanval door de NAVO.

Rakettencrisis

De Koude Oorlog was overzichtelijker en rustiger dan de complexe missie in Afghanistan", zegt Platje. "De methodiek van het inlichtingenwerk is wel dezelfde: het in kaart brengen van somalische piratennesten of talibannetwerken. De dreiging - nucleaire vernietiging - echter was toen veel groter. In 1962 was de Cubaanse rakettencrisis op zijn top. Deze confrontatie tussen Cuba en de



Sovjet-Unie enerzijds en Amerika anderzijds, joeg de wereld schrik aan. Platje wist de hand te leggen op zeer geheime rapporten die in 2007 door het Amerikaanse National Security Archive werden vrijgegeven. Dit gaf informatie over de opmars van de Sovjeteenheden naar Cuba. Vier onderzeeboten zijn bewapend met torpedo's met een nucleaire kop. Platje: "Het was een dubbeltje op zijn kant, of een van deze onderzeeboten had een torpedo met kernkop afgevuurd. De Amerikanen deden pogingen om de onderzeeboten aan de oppervlakte te dwingen. Dit was echter een groot risico. De bemanning had het namelijk erg zwaar, uitgeput door wekenlang verblijf onder water onder moeilijke omstandigheden en bezorgdheid over het feit dat de Amerikaanse oefendieptebommen gevaarlijke explosieven zouden zijn. Twee commandanten hebben op het punt gestaan deze torpedo's te lanceren." In het boek beschrijft Platje het voorval waarbij de commandant in een woedeaanval opdracht geeft de nucleaire torpedo oorlogsgereed te maken en hoe de waarnemend brigade-commandant dit uiteindelijk heeft voorkomen. "De commandanten hadden vaak geen verbinding met Moskou en wisten niet wat de politieke en militaire situatie om hen heen was. De beslissing een torpedo te lanceren, heeft afgehangen van het persoonlijke oordeel van de commandant. Dit is het gevaarlijkste moment in de Koude Oorlog geweest."

Fotomateriaal verloren gegaan

Dit boek laat helaas niet alle kanten zien, zegt Platje. "Dat komt deels door de geheime informatie die helaas eerder wordt vernietigd dan dat de rubricering vervalt, waardoor je met hiaten in het verhaal blijft. Deels komt het doordat ik geen contacten heb met voormalige marineofficieren of inlichtingenmensen in Rusland. Dat is allemaal nog te gesloten. Er is dus nog veel te vertellen, al is dit boek wel uniek in Nederland. Ondanks deze hindernissen, heeft Platje een zeer omvangrijk boek geschreven. Hij heeft er zes jaar aan gewerkt en heeft zijn informatie breed gezocht. "Ik kreeg vaak royaal toegang. De MIVD heeft me ook goed geholpen. Ik heb een inzage verzoek in het kader van de Wet op de Inlichtingen- en Veiligheidsdiensten ingediend. Ik heb wel gemerkt dat veel materiaal, waaronder foto's, verloren is gegaan." Hij heeft ook onderzoek gedaan bij de NAVO. "Het stuk dat ik wilde inzien, was echter nog steeds geclassificeerd. Om een stuk te declassificeren, moeten alle NAVO-lidstaten instemmen. Dat is een procedure van tien jaar. Dat heb ik dus maar opgegeven."

Het was een dubbeltje op zijn kant, of een van deze onderzeeboten had een torpedo met kernkop afgevuurd.

Wodka on the Rocks

Zijn zoektocht naar informatie heeft interessant materiaal opgeleverd. Een enkele keer kwam hij erachter dat een zaak die op een bepaalde manier algemeen bekend was, toch anders in elkaar stak. Hij verwijst naar het verhaal dat bekend staat als 'Whiskey on the Rocks'. "Een Zweedse gepensioneerde kapitein ter zee vertelde mij over het onderzoek waarover hij de leiding had gehad, naar het stranden van een Sovjet-onderzeeboot op de bodem van Zweeds kustwater. Dit incident trok wereldwijd aandacht. Naar aanleiding hiervan bestond immers het risico op een militaire confrontatie tussen beide landen. "Deze onderzeeboot van de Whiskey-klasse zat in 1981 bij het krieken van de dag muurvast op de Zweedse zeebodem. De Zweedse regering stelde een commissie in om uit te zoeken of het om een uniek incident ging, of dat het een bewijs was dat de Sovjetmarine illegale onderwateroperaties uitvoerde. De Onderzeeboot Defensie Commissie stelt dat de Sovjetmarine systematisch de Zweedse territoriale wateren heeft geschonden met 'onderzeese vaartuigen'. Maar hiermee is de rust niet teruggekeerd. Diverse onderzoeken volgden. In 1995 wordt er een nieuwe commissie ingesteld met de opdracht de vermeende onderwaterschendingen te analyseren. Deze commissie concludeert ook dat er opzet in het spel was. "De Zweedse kapitein ter zee die de leiding had over het onderzoek in 1981 en die de bemanning heeft verhoord, is ervan overtuigd dat het allemaal niets met een inlichtingenoperatie van doen had. De Sovjetmarine beriep zich op technische mankementen, terwijl alle instrumenten van de onderzeeboot goed werkten toen ze na de stranding door de Zweden werden onderzocht. Een combinatie van gebrekkig vakmanschap, stress en een teveel aan alcohol en vermoeidheid zijn de oorzaak van de stranding. "Het hele incident is niet meer dan een Wodka on the rocks".

Contra-inlichtingen

De verdienste van de marine-inlichtingen toentertijd was het in kaart brengen van de Sovjetmarine en koopvaardijvloot. Nederland had een goede positie doordat Sovjetschepen onze havens aandedden. "In de jaren zeventig bevonden zich per dag gemiddeld vier tot zeshonderd Sovjetzeelieden in de Nederlandse havens. Zij wer-

den op grote schaal door de geheime diensten van de Sovjet-Unie gebruikt voor inlichtingenactiviteiten. Maar ook wij verkregen hierdoor veel informatie in het kader van contra-inlichtingen. Zo werd bijvoorbeeld door de Nederlandse inlichtingendienst geconstateerd dat twee bemanningsleden van het Sovjetvrachtschip Kolomna systematisch de omgeving van de Nieuwe Waterweg bij Rotterdam fotografeerden, en dat een opvarende van ditzelfde schip regelmatig grote hoeveelheden zeekaarten kocht van gebieden rond IJsland, de oost- en westkust van Groenland en de kustgebieden rond Cyprus.

Waakzaam oog

Het boek eindigt met het verval van de Sovjetvloot. Aan het einde van de Koude Oorlog tekenden de VS en de Sovjet-Unie overeenkomsten voor vergaande strategische en conventionele wapenreducties. Het aantal strategische onderzeeboten en maritieme nucleaire wapens werd teruggebracht. In 1989 beschikte de Sovjetmarine over 196 operationele nucleaire onderzeeboten. In 2003 waren dit er waarschijnlijk nog 80. Prof. Dr. B.G.J. de Graaff schrijft in de inleiding van het boek dat het boek niet alleen historisch inzicht biedt in het maritieme inlichtingenduel van de Koude Oorlog, 'maar ook een kijk verschaft op de belangen van een land dat moeite heeft zich neer te leggen bij zijn (tijdelijk) verminderde internationale status en daarom nog steeds een zeker inlichtingenbelang heeft, al zal het lang duren voordat dat weer dezelfde importantie zal hebben als in de hier beschreven periode.'

Platje betoogt dat een scherp en waakzaam oog op de zee een noodzakelijkheid is voor de Nederlandse krijgsmacht. "Rusland lijkt vastbesloten te zijn om haar plaats in de machtsverhoudingen van de wereld te accentueren. Of dit streven in de toekomst een bedreiging voor het Westen gaat vormen, is van veel factoren afhankelijk. Maar ook zeegaand terrorisme, piraterij en andere vormen van misdaad op zee, schurkenstaten en een lastig in kaart te brengen verspreiding van massavernietigingswapens vormen een reële bedreiging voor onze samenleving en onze kwetsbare maritieme levensaders. De dreiging van doelgerichte antiwesterse aanslagen en acties zijn beangstigende aspecten van de wereld waarin wij nu leven. De klassieke behoefte aan inlichtingen over de positie en intenties van de tegenstander blijft daarom een scherp en waakzaam oog op de zee rondom ons vereisen."

Integraal beveiligingsplan, clean desk-rondes: Bureau Veiligheidszaken doet veel meer dan je denkt.

Met een ferm 'goedemorgen' fietst Theo langs de bewaking de Frederikkazerne op. Hij loopt het MIVD-gebouw in. Bij de ingang van het gebouw stuit hij op de tourniquet. Een beveiligingsmaatregel bij uitstek? Zonder pasje en bijbehorende pincode natuurlijk geen toegang tot het gebouw. En zonder de juiste instellingen die er door de frontoffice van bureau Veiligheidszaken (BVZ) aan zijn gekoppeld, ook geen toegang tot de afdeling.

Clean desk-ronde

Als Theo op zijn kantoor komt, vindt hij daar een groen briefje: er is een clean desk-ronde geweest en op zijn kantoor was alles in orde. De waardebergmiddelen waren op de juiste manier afgesloten, er lagen geen gerubriceerde papieren of elektronische informatiedragers op zijn bureau. Als hij achter zijn computer gaat zitten, typt hij drie keer zijn wachtwoord verkeerd in. Zijn pas wordt direct geblokkeerd. "Op naar de frontoffice om mijn pas te laten deblokkeren", mompelt Theo als hij zijn kamer verlaat en de deur op slot draait.

Staat van Inlichtingen

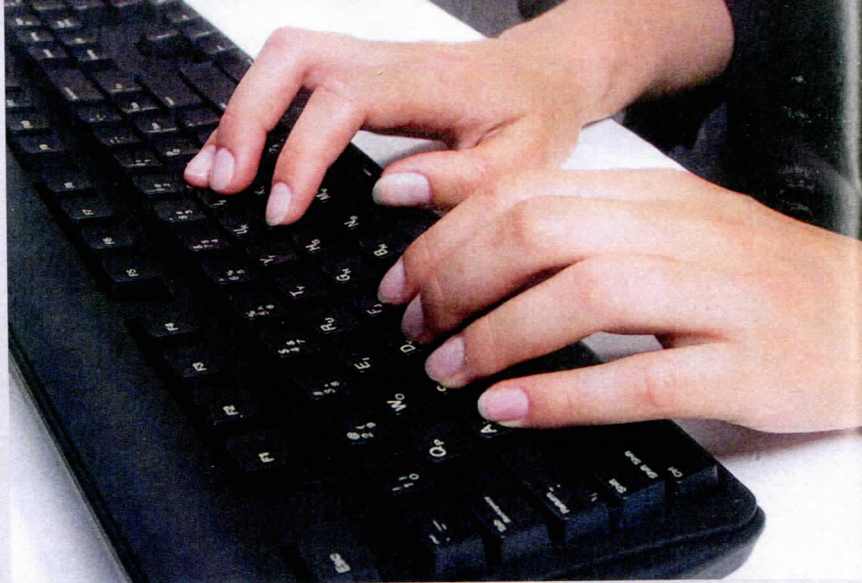
Eenmaal achter zijn computer leest hij een nieuwsflits over een nieuwe Order van Blijvende Aard over de Request for Visit. Dat herinnert hem eraan dat hij nog een Request for Visit bij BVZ moet indienen. Tegelijkertijd valt zijn blik op zijn postvak: daarin ligt een Staat van Inlichtingen van een nieuwe medewerker. Die moet hij ook niet vergeten bij BVZ in te leveren. BVZ is namelijk de administratieve tussenpersoon tussen hem en ACIV waar het veiligheidsonderzoek wordt gestart.

Integraal beveiligingsplan

Halverwege de dag heeft hij een afspraak op een andere MIVD-locatie. Ook voor deze locatie heeft BVZ een integraal beveiligingsplan gemaakt. Die moeten elk jaar weer tegen het licht worden gehouden om te kijken of de beveiliging nog up-to-date is.



In een integraal beveiligingsplan worden organisatorische en bouwkundige maatregelen beschreven. De organisatorische maatregelen hebben betrekking op procedures omtrent de toegang tot locaties en hoe om te gaan met informatie. In de bouwkundige maatregelen is opgenomen van welke kwaliteit de sloten, ramen en deuren moeten zijn. Er wordt bijvoorbeeld besloten of de ramen slagvast moeten zijn, of er een trilsensor aan bevestigd moet worden en een infraroodsensor om te zien of iemand zich ongeautoriseerd toegang heeft verschaft. BVZ gaat er vanuit dat iemand met de juiste middelen binnen kan komen. Doordat de beveiliging in schillen is opgebouwd, is een inbreker niet zomaar bij de waardevolle informatie waarnaar hij misschien op zoek is. In het beveiligingsplan is daarom ook de interventietijd berekend. Een goede mix van bouwkundige en organisatorische maatregelen kan veel ellende voorkomen. Daarnaast is het menselijk handelen een zwakke schakel als het gaat om beveiliging. Als de medewerkers zich niet voldoende aan de regels houden, kan er alsnog een veiligheidsincident plaatsvinden. Daarom doet BVZ veel aan veiligheidsbewustzijn bij de medewerkers.



BVZ verleent ook autorisaties voor het verstrekken van gegevensdragers als usb-sticks en externe harde schijven. Bureau ICT verstrekt deze middelen, maar niet zonder toestemming van BVZ. BVZ kijkt of het noodzakelijk is dat iemand van een dergelijk middel gebruikmaakt en ook of het wel veilig is. Soms komt BVZ met onverwachte alternatieven. Elke vorm van losse gegevensdragers kunnen namelijk een veiligheidsrisico zijn. BVZ heeft als taak de informatie op een dergelijk middel te beschermen en daarom is het gebruik van een dergelijk medium gebonden aan richtlijnen.

Bezoekers

Weer terug in zijn eigen gebouw meldt hij bij de portier alvast bezoekers voor morgen aan. Buitenlandse gastbezoeken verlopen vaak via Bureau Externe Relaties. BVZ assisteert wanneer het wenselijk is dat er niet veel tijd verloren gaat bij de uitgifte van de pasjes. "Er komt hooggeplaatst bezoek en die kunnen we niet lang laten wachten", zegt Theo tegen de portier.

Codes wijzigen

Weer terug op zijn plek stapt er iemand van BVZ binnen die de codes van de waardekasten komt wijzigen. Dit moet elk half jaar gebeuren en nu is het weer tijd. Theo zucht: "Vanochtend nadat mijn computer was geblokkeerd, heb ik een nieuw wachtwoord voor mijn computer gekozen en nu ook nog een nieuwe code voor mijn kast? Dat is wel erg veel op een dag om te onthouden." Even overweegt hij om een briefje onder zijn toetsenbord te leggen met het wachtwoord, maar dan herinnert hij zich een column van BZV in Ingelicht waarin – heel terecht – ten eerste wordt afgeraden dit te doen.

Vervoer gerubriceerde informatie

Aan het eind van de dag besluit hij wat werk mee naar huis te nemen. Daarvoor moet hij wel de juiste toestemming hebben. "Stel je voor dat er morgenochtend een controle is en ik de regels overtreed omdat ik de spullen niet op de juiste manier vervoer." Weer betreft Theo zich op een verkeerde gedachte. "Stel je voor dat mijn tas wordt gestolen of dat ik die laat liggen en er gerubriceerde documenten in verkeerde handen vallen. Daarom moet ik bij BVZ navragen hoe ik de spullen moet meenemen en verpakken."

Niet veel later stapt hij in de lift. "Einde werkdag, morgen weer een nieuwe."

BVZ doet nog veel meer. Te veel om allemaal in dit artikel op te noemen. Kijk op intranet/afdelingen/SAO/BVZ.

Even overweegt hij om een briefje onder zijn toetsenbord te leggen met het wachtwoord...

't Is koers!



Regelmatig komen er bij de directie klachten binnen dat de afstand tussen Eibergen en Den Haag te groot is. Deze klacht vormde de directe aanleiding om per fiets op onderzoek te gaan.

Vergeet de start van de Giro d'Italia in Amsterdam, vergeet de *Grand Départ* van de Tour in Rotterdam. De enige koers die er dit jaar echt toe deed, begon in Den Haag en eindigde in Eibergen; de Beach-2-Borderfietsstocht.

Met D-MIVD als kopman werd op 28 mei 2010 door de uiterst gemotiveerde en goedgetrainde wielerploeg van de MIVD de afstand tussen beach en border overbrugd. Deze 195 kilometer, die later 'per ongeluk' 215 bleek te zijn, werd in één dag afgelegd.

De Koers

Bij het krieken van de dag vertrok de ploeg vanaf de Frederikkazerne. Via de oneindige vlakke van het Groene Hart baande het peloton zich een weg richting Loosdrechtse en Maarsseveense Plassen alwaar de *équipe* zich te goed deed aan koffie en appeltaart. Daarna vertrok het team richting het middelgebergte van de Utrechtse Heuvelrug. Door het lichte briesje in de rug en de ochtendzon op het gezicht werd het bikkelgehalte tot een minimum beperkt. De verzuurde benen werden bij de ravitaillering in Amersfoort enige rust gegund en de cavalerie deelde enthousiast LuPa's uit. Voordat de besneeuwde toppen van het Veluwemassief opdoemden, met enkele cols van *hors catégorie* als scherprechter, probeerden enkelen de koers hard te maken (en hun carrière ten gronde te richten). Deze uitbraakpoging werd na vermanende woorden van

de kopman geneutraliseerd zodat de laatste toppen van de Veluwe bergetappe in gesloten formatie genomen werden. Vervolgens werd afgedaald richting IJsselvallei alwaar er, vanwege het parse karakter van de Dienst, een maritieme component aan de koers was toegevoegd; het pontje van Brummen naar Bronckhorst. Als reactie hierop operden enkele luchtmachters de rest van de afstand per C-17 af te leggen. Vanwege beperkte landingsmogelijkheden in de omgeving van Eibergen moest dit toch uit het hoofd worden gezet.

Na Bronckhorst baande het peloton zich een weg door het zacht glooiende Achterhoekse land. En toen, eindelijk, na 215 kilometer, doemde het bordje 'Bundesrepublik Deutschland' op. Voor het eerst in de Nederlandse geschiedenis werd de Duitse grens met grote blijdschap overschreden. Het glas werd geheven en de laatste drie kilometer naar kamp Holterhoek werden met grote opluchting afgelegd.

De Bikkeltrofee

In kamp Holterhoek werd de ploeg opgewacht door de mensen die de 'Hel van Eibergen' gefietst hadden en door de motorrijders. Bij aankomst deed iedereen zich te goed aan een BBQ en bier. In spanning werd afgewacht wie dit jaar de bikkeltrofee in ontvangst kon nemen. De winnaar van vorig jaar, Ad, besloot Karin tot de bikkel van 2010 te huldigen. Karin, van harte!



En volgend jaar? In de Eibergse wandelgangen wordt gefluisterd over Eibergen – Burum. Maar voor hetzelfde geld knallen ze volgend jaar in een dag naar Wiesbaden. Het blijven doorzetters, die bikkels.

De Motorkoers

De bikkels waren al enkele uren vertrokken toen de motoren de straat op gingen. De tour was zo uitgezet dat de motorrijders de bikkels zoveel mogelijk zouden ontmoeten. Een mechanische hobby heeft van nature het nadeel dat er wat kapot kan gaan en na ongeveer 30km moesten we een van onze gemotoriseerde tweewielers achterlaten. Jammer, maar er is altijd wel een plekje achterop en zo ging het verder naar 't Kikkertje' in Oud Maarsseveen. Doordat de weergoden gezorgd hadden voor wind uit het westen ging het de fietsers letterlijk en figuurlijk voor de wind en waren zij ruim voor de geplande tijd daar. De motorrijders arriveerden pas toen de wielploeg alweer op weg was naar Amersfoort. Na een snelle en heerlijke koffie met gebak ging het door naar de lunch in Amersfoort; dit keer samen met de bikkels. Daarna verder via de prachtige natuur van de Veluwe, richting het oosten. Na de Veluwe ging het via een pontje over de IJssel naar het historische stadje Bronckhorst. Midden in het stadje staat de Herberg 'de Gouden Leeuw' waar het ideaal toeven was, wachtend op de fietsers. Na de nodige 'brandstof' en het maken van een groepsfoto ging het richting Eibergen, via schilderachtige taferelen van het Achterhoekse- en Twentse landschap. Intussen was er een aantal ontmoetingen geweest met de nog steeds fris ogende bikkels. In de buurt van Eibergen nam de lokale matador Ton het over en loodste ons via prachtige weggetjes naar kamp Holterhoek. Om ongeveer 18.30uur hebben we onder luid applaus de bikkels binnengehaald...Chapeau, want 215km ongemotoriseerd afleggen, is niet mis. De avond liet ook niets te wensen over, met een perfecte BBQ en een drankje. Op zaterdag hebben we met een aantal motorrijders nog een tour gemaakt via de Achterhoek, Duitsland en het land van Maas, Rijn en Waal. In de loop van de middag ging "ieder zijns weegs".

Dialogoog

In onze nieuwsbrief, die onlangs is uitgekomen, heeft u kunnen lezen dat wij een advies hebben uitgebracht over de reorganisatie van de afdeling Contra-Inlichtingen en Veiligheid. We vinden het niet alleen belangrijk dat deze afdeling een kwantitatieve en kwalitatieve impuls krijgt, maar ook dat het reorganisatieproces transparant verloopt en dat de belangen van het betrokken personeel optimaal behartigd worden. De directie heeft ons bedankt voor dat advies en eens te meer onderstreept dat zij groot belang hecht aan medezeggenschap. Daardoor wordt het wederzijdse begrip vergroot, het draagvlak voor voorgenomen maatregelen verbreed en de kans op misverstanden gereduceerd.

Er zijn nog vele andere onderwerpen waarover wij als MC een dergelijke constructieve dialoog willen aangaan of voortzetten. Om er een paar te noemen: de ARBO-omstandigheden in de verschillende vestigingen van de MIVD, de positie van de MIVD in de Bestuursstaf, de toekomst van het Van Alkemade-complex en de evaluatie van de reorganisatie van de overige delen van de dienst. Stuk voor stuk onderwerpen die de werk- en leefomstandigheden van alle medewerkers van de MIVD direct kunnen beïnvloeden en onze aandacht meer dan waard zijn.

Het valt ons echter steeds moeilijker om dergelijke onderwerpen de aandacht te geven die zij verdienen. De MC wordt steeds kleiner door natuurlijk verloop, maar ook door opleidingen en uitzendingen. Daarom doe ik andermaal een beroep op u, onze achterban. Wij willen graag een MC blijven die van alle markten thuis is en een geloofwaardige vertegenwoordiging vormt van het personeel van de dienst. Wilt u de MC met raad en daad terzijde staan, dan bent u van harte welkom. De contactgegevens vindt u op intranet (Afdelingen/MC-site).

Bijgaande cartoon illustreert hoe belangrijk een constructieve dialoog is. Namens alle leden van de MC wens ik u alvast een prettige zomervakantie periode toe.



MIVD besteedt meer aandacht aan piraterij

De toegenomen piraterij voor de kust van Jemen, Kenia en Somalië heeft verhoogde aandacht gekregen van de Militaire Inlichtingen- en Veiligheidsdienst, blijkt uit het jaarverslag dat demissionair minister van Defensie Eimert van Middelkoop naar de Tweede Kamer heeft verstuurd.

Inmiddels staat piraterij hoog op de internationale agenda. Mede door de Nederlandse bijdrage aan de NAVO-missie Allied Protector en de EU-missie Atalanta is de bescherming van koopvaardij schepen in de Golf van Aden verbeterd. De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft Allied Protector en Atalanta succesvol ondersteund in 2009, en zal dat ook doen in 2010.

Voor het expeditionaire optreden van de krijgsmacht is het van belang, dat wanneer het politieke besluit is genomen aan een missie deel te nemen, de MIVD al een informatiepositie heeft in het missiegebied. De MIVD is dan in staat snel voort te bouwen op het bestaande, wereldwijde netwerk van informanten en onderschepte telecommunicatie, de zogeheten Human Intelligence en Signals Intelligence. Hierdoor kan de dienst de krijgsmacht voorzien van relevante en benodigde inlichtingen.

Afghanistan

Evenals voorgaande jaren heeft de MIVD zich vooral gericht op het ondersteunen van de krijgsmacht en civiele autoriteiten bij het uitvoeren van de operatie in de Afghaanse provincie Uruzgan. Daartoe werden dreiging-, (contra)inlichtingen- en veiligheidsanalyses opgesteld voor de defensieleiding, de commandant Task Force Uruzgan en het civiele deel van de missie. De dreiging- en inlichtingenanalyses geven de commandant TFU inzicht in de strategische en tactische posities en intenties van de tegenstander, op basis waarvan de commandant maatregelen kan treffen. Veiligheidsanalyses geven een prognose van de veiligheidssituatie in het inzetgebied. Mede op basis van deze analyses kan de commandant (veiligheids)maatregelen treffen. Analyses van bestuurlijke en tribale structuren ondersteunen de medewerkers bij het civiele opbouwwerk in de Afghaanse provincie.

Cyber Warfare

De MIVD heeft in 2009 meer aandacht geschonken aan het fenomeen Cyber Warfare. Er is een begin gemaakt met het opbouwen van een normbeeld door middel van het monitoren en het vastleggen van mogelijke indicatoren. Hiertoe is samengewerkt met verschillende partijen binnen en buiten het ministerie van Defensie. De MIVD levert een bijdrage aan het tegengaan van cyberaanvallen, met haar expertise op het gebied van het ontsleutelen van informatie verkregen uit satellietinterceptie.

Geospatial Intelligence

Geospatial Intelligence zijn inlichtingen uit georuimtelijke informatie, gecombineerd met beeldmateriaal. Wanneer dit wordt samengebracht en geanalyseerd met andere in een geografische context geplaatste inlichtingen, gaat het over Geospatial Referenced Intelligence Fusion (GRIF). Dit is een revolutionaire ontwikkeling in de inlichtingenvoorziening aan de operationele gebruikers. Van complexe situaties worden namelijk vierdimensionale visualisaties gemaakt. Dit maakt het militaire besluitvormers op zowel strategisch, operationeel als tactisch niveau mogelijk om naar plaats en tijd gecorreleerde inlichtingen te gebruiken bij het nemen van beslissingen. In 2009 heeft de MIVD meer aandacht besteed aan de verdere ontwikkeling van Geospatial Intelligence.

Humor houdt je op de been: GV Café in Den Helder

Lang samenwerken op een schip, maanden doorbrengen op een compound, of samen een kantoor delen: als militair kom je in zeer verschillende situaties terecht. Humor is onmisbaar om iets wat onoplosbaar is te relativeren.

Daarover ging het in het GV Café van 12 april in Den Helder. Het GV Café is een maandelijkse avond op de Nieuwe Haven in Den Helder, georganiseerd door Diensten Geestelijke Verzorging in Den Helder. Spreker daarvoor was Henk Boomstra. Tijdens zijn carrière als marineman heeft hij een tekentalent ontwikkeld en een fijn gevoel voor humor. Zo maakte hij aan boord al karikaturen van

bemanningsleden en wist hij de lotgevallen van een schip en haar bemanning na afloop van een lange reis vaak humoristisch vast te leggen in een grote overzichtstekening.

Waar draait het in humor om? Om herkenning, hield Boomstra zijn gehoor voor. Er zijn talloze situaties waarin mensen zich herkennen, en als mensen iets herkennen, worden ze enthousiast. Boomstra liet de bezoekers ook zelf tekenen, want "iedereen kan tekenen!" Als je een situatie in een tekening wilt vastleggen en je zoekt de herkenning en de lach; laat dan de kijker nadenken. Dus kies een moment vóór of ná het moment suprême.



Generaal-majoor Cobelens neemt boek in ontvangst

Op 3 mei nam de directeur MIVD het boek Zee van Geheimen in ontvangst van Wies Platje, oud-inlichtingenofficier. In dit boek beschrijft de auteur hoe zowel de landen van de NAVO als de Sovjet-Unie informatie over elkaar verzamelden. In het begin van de Koude Oorlog ging dit vooral door het uitsturen van westerse onderzeeboten en vliegtuigen die waren uitgerust met elektronische interceptieapparatuur.

Deze eenheden voerden operaties uit, soms ook over de grenzen van de Sovjet-Unie. In het boek wordt ook aandacht geschonken aan de inzet van menselijke bronnen, inlichtingsatellieten en het af luisteren van vijandelijke radioverbindingen. De Nederlandse Marine Inlichtingendienst speelde bij het in kaart brengen van deze activiteiten binnen de NAVO een belangrijke rol.

Co de Rood

Henk Slijkhuis



MIVD neemt deel aan de CPC-loop op zondag



14 maart 2010

Op zondag 14 maart 2010 is in Den Haag de 36^{ste} editie van de City-Pier-City (CPC) Loop gehouden. Het hardloopparcours voert door Den Haag / Scheveningen en is sinds een aantal jaren een stadsparcours geworden. De CPC is de grootste en gezelligste stratenloop van Nederland. De start en finish waren dit jaar bij het Malieveld.

Door: Henk Bretveld, DP&O/BS/burOpl

Dit jaar was noodgedwongen, in verband met diverse opbrekingen in Den Haag en Scheveningen, een nieuw parcours uitgezet.

De weersverwachtingen waren voor een dergelijk evenement niet ideaal, maar tijdens het lopen viel het alleszins mee. Een beetje wind, gelukkig droog en met een zonnetje. Daardoor stond er veel publiek langs de kant, klonk er op vele plaatsen muziek uit luidsprekers of livemuziek, waardoor het lopen een stuk eenvoudiger leek. Dit jaar was er een record aantal van ruim 27000 deelnemers.



Drie MIVD-teams

MIVD-medewerkers werden net als in eerdere jaren in de gelegenheid gesteld om aan deze sportieve *happening* mee te doen in de vorm van Business teams. De gezamenlijke MIVD-ers deden mee aan de 10 km en de halve marathon (21,1 km).

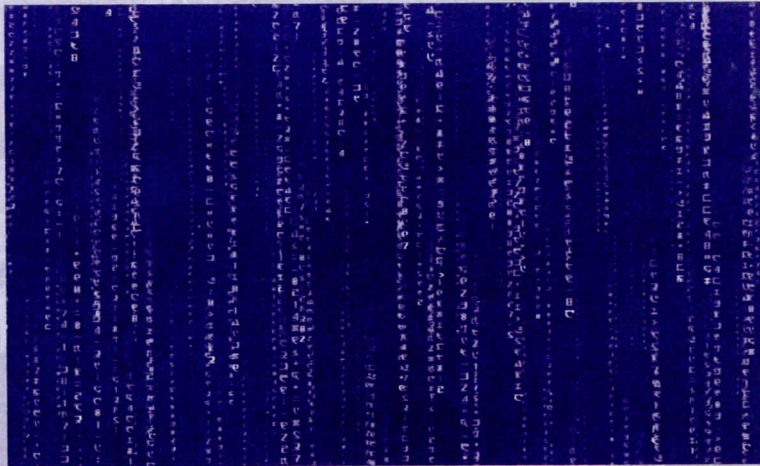
Er namen drie MIVD teams deel aan het CPC-Business-programma. Een Business team bestaat uit acht personen. In totaal deden zeven lopers mee aan de 10 km en twaalf lopers aan de 21 km. Bij de 21,1 km deden twee vrouwelijke collega-lopers mee; de overige deelnemers waren mannen. Van de deelnemers waren er zeven militair en twaalf burgers.

Er is door de MIVD een goed sportief resultaat neergezet. De snelste loper op de halve marathon was Erik. Hij kwam speciaal voor dit evenement uit Eibergen en liep de 21,1 km in 1.33.54. De snelste tijd op de 10 km werd gezet door Peter (AS).

Ook volgend jaar staat er al weer een CPC-loop gepland en wel op zondag 13 maart 2011. Het is te hopen dat ook dan een aantal lopers namens de MIVD wil en kan deelnemen. Het trainen daarvoor kan nu al beginnen!

Phishing

Phishing is de wellustige kunst van het ontlokken van privégegevens van argeloze mensen. Gegevens zoals creditcardnummers, bankaccountgegevens, logon ID's, wachtwoorden, etc. Ook wordt de techniek toegepast om stiekem virussen of Trojans op uw PC te installeren. De meeste van de *phishing* pogingen zijn dermate onbeholpen dat je wel erg onoplettend moet zijn om erin te trappen. Toch schijnt dat nog dikwijls te gebeuren.



Volgens een rapport van Trusteer Inc.¹ heeft 45 procent van bankklanten die naar een *Phishing* site werden omgeleid geen enkel probleem in het geven van persoonlijke data zoals wachtwoorden, creditcardnummers e.d. Ongeveer een half procent van de mensen trapt in de val, hetgeen tot tien miljoen dollar verlies oplevert. Nu lijkt een half procent niet veel, maar afgezet tegen de stortvloed van *phishing* mails die worden verzonden, kan dat aantal aanzienlijk zijn. Bedenk dat het er tegenwoordig niet om gaat in één keer vijftig miljoen te stelen, maar om vijftig miljoen keer één euro.

Leuke truc

Onderzoek aan de Harvard Universiteit laat ook interessante feiten zien: negentig procent van de proefpersonen heeft grote moeite onderscheid te maken tussen échte e-mail en *Phishing* e-mail. Bijna een kwart kijkt nooit naar de adresbalk, statusbalk of andere veiligheidsaanwijzingen van de browser. Ook bleek dat veel proefpersonen moeite hebben om URL's te begrijpen. Enkele voorbeelden (overigens, nu ik dit schrijf is uw aandacht gevestigd op de voorbeelden die ik geef, zodat die nogal simpel lijken. In het 'echt' zou u waarschijnlijk niet langer dan een fractie van een seconde naar de URL kijken):

1. <http://www-ebay-com.secure.org> Veel proefpersonen meenden dat dit de URL van eBay was.

<Http://National.VWesternBank.com>, in plaats van National.WesternBank.com. Afhankelijk van het lettertype van uw browser is het

verschil tussen de VV en W bijna niet te zien. Leuke truc, net zoals het vervangen van de letter "l" door iets wat er sterk op lijkt, zoals de letter "1", het getal "1", of de verticale balk "l".

CNN alerts

De leukste *Phishing*-poging kreeg ik onlangs binnen. Als hoofd van bureau Open Source Intelligence krijg ik nogal wat automatische *alerts* van grote persbureaus per e-mail binnen. Daarbij zat ook een alert van CNN over een gebeurtenis, met zoals het hoort de titel van het bericht, inhoud en een link waarop men kon klikken indien de alerts niet meer gewenst waren. Dat had ik bijna gedaan tot ik mij realiseerde dat ik helemaal geen alerts bij CNN had lopen.

Lotto gewonnen?

Natuurlijk beschik ik ook over de nodige mails waarin wordt aangekondigd dat ik weer eens een paar miljoen rijker ben geworden door hetzij een lotto (gemaaild vanuit het Verenigd Koninkrijk, terwijl de mail headers een afzender uit Spanje laten zien?), hetzij een aardige prins uit het buitenland. Dat lijkt trouwens ook het échte gevaar van *phishing* te zijn: stel je voor dat één van de lotto mails écht is?

¹ <http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf>