door volgend jaar in deze rubriek te relateren wat er ondertussen is gerealiseerd.
Samenvattend kunnen we besluiten dat de aanbevelingen van het Comité P open deuren intrappen. Geen enkele aanbeveling is voor onderzoekers in moordzaken nieuw. Integendeel werden de meeste al herhaaldelijk aan het beleid gesignaleerd zonder resultaat. Naar aanleiding van het onderzoek door het Comité P zullen waarschijnlijk de onderzoekers van Leuven zich moeten verantwoorden. Zoals bijna altijd als er bij de politie een onderzoek misloopt zullen de laagsten in rang het geweten hebben. De grootste tekortkomingen zitten echter in sommige politiestructuren die afstralen op de individuele onderzoeker. We geloven best dat het enkele jaren duurt vooraleer structurele veranderingen op het terrein voelbaar zijn, maar toch geen 11 jaar na de politiehervorming. Er wordt weinig of niets gedaan aan de inertie die al jaren bij sommige diensten heerst. Het is aangewezen dat het Comité P een onderzoek opent waarom haar – terechte – aanbevelingen, die in politiemiddens al jaren gekend zijn, niet gerealiseerd werden. Pas dan zal men kunnen vaststellen of de fouten in het Leuvens onderzoek individuele fouten zijn.

Marc Bockstaele*

Naar een nationale Nederlandse politie

De Nederlandse minister van Veiligheid en Justitie heeft een wetsvoorstel nieuwe politiewet voorbereid tot invoering van "nationale politie in één korps". In de Tweede Kamer werd het op 12 januari duidelijk dat een parlementaire meerderheid kan gevonden worden voor deze hervorming. Hierdoor zou het aantal regionale korpsen herleid worden tot 10 en onder de koepel komen van één nationale politie. De korpsbeheerder , de politiechefs, de burgemeesters en het openbaar ministerie moesten zich tegen eind januari 2011 ten overstaan van de minister uitspreken over zijn voorstel.
Het ziet er dus naar uit dat er in 2012 een nationale politie komt in Nederland. Deze belangrijke stap is ook noodzakelijk om beter het hoofd te kunnen bieden aan gewelddadige verstoringen van de openbare orde en rampen, om de grote moeilijkheden in de technische infrastructuur van het politiewezen te kunnen overwinnen en om de verspilling van mensen en middelen aan overbodige bureaucratie te stoppen. Er loopt nu wel een discussie over het feit hoe de beoogde nationale politie beter kan ingebed worden in de gemeenten. Wel houdt de burgemeester het gezag over de ordehandhaving en hulpverlening en hij moet zich hierbij verantwoorden tegenover de gemeenteraad en deze raad moet nauw betrokken worden bij het opstellen van de beleidsplannen.

Willy Bruggeman*

Oude wijn in nieuwe zakken? De aard van cybercrime en de implicaties voor de opsporingspraktijk

1. Inleiding

Sinds medio jaren 90 van de vorige eeuw is internet voor het grote publiek toegankelijk. Het is verweven geraakt met ons dagelijks leven en niet meer weg te denken. Een recente studie toont aan dat 88% van de Vlamingen tussen 18 en 30 jaar en 81% van de Vlamingen tussen 31 en 45 jaar internet gebruikt (Moreas, 2007). Het laatste onderzoek van OIVO (Onderzoeks- en informatiecentrum van de verbruikersorganisaties) toont aan dat 92% van de Belgische jongeren tussen 10 en 17 jaar op het internet surft. (Hendrickx & Vercammen, 2010). Internet wordt voor verschillende doeleinden gebruikt, van het communiceren met mensen over de hele wereld middels e-mail of Skype tot het boeken van vakanties, het doen van betalingen en het bijhouden van contacten via sociale netwerksites. Ook criminelen maken gebruik van de mogelijkheden van internet, in hun geval voor het plegen van hun misdrijven. Dat is niet nieuw. Al sinds internet voor het brede publiek toegankelijk is, wijzen wetenschappers hierop (Duncan, 1997; Van Eecke, 1997; Boerstra, 1997; Grabosky en Smith, 1998; Stol e.a., 1999). Lange tijd lijken deze vormen van criminaliteit echter geen prioriteit te hebben gehad van politie en justitie.

* Gepubliceerd in eigen naam
Marc Bockstaele is licentiaat in de criminologie, hoofdcommissaris bij de federale gerechtelijke politie Gent.

* Willy Bruggeman is Professor Benelux Universitair Centrum, voorzitter Federale Politieraad.

Pas dit laatste decennia geeft de overheid prioriteit aan de bestrijding van cybercrime. Met de Belgische wet op de informatiecriminaliteit werd in 2000 in België een hele reeks vormen van cybercriminaliteit strafbaar gesteld. De wetgever wilde een aantal concrete stappen nemen om de actoren van justitie de adequate juridische instrumenten aan te reiken om de criminaliteit in cyberspace te bestrijden. De wet beoogde de strafrechtelijke beteugeling van informaticacriminaliteit. Dit begrip is dubbelzinnig en dekt zowel criminele aanvallen tegen computers en netwerken, zoals computerinbraak en de verspreiding van computervirussen, als allerlei oude soorten van misdrijven waarbij nu van computers of netwerken gebruik kan worden gemaakt. Voorts heeft het Europese Cybercrime verdrag er voor gezorgd dat de Belgische wetgeving verder werd aangepast. Met de nieuwe wet van 2003 inzake e-handel werd beslist dat men elektronische post (e-mail, maar ook b.v. SMS, MMS) voor reclamedoeleinden enkel met voorafgaande toestemming mag sturen. Op deze manier probeerde de wetgever het gebruik van spam te beperken (De Pauw, 2010a). Verder werd het verspreiden van kinderpornografie (art. 383bis Sw.) en uitingen die aanzetten tot discriminatie, racisme of vreemdelingenhaat (wet van 30 juli 1981) strafbaar gesteld (art, 1° en 3° antidiscriminatiewet 23 februari 2003) (De Pauw, 2010a).
Naast veranderingen in wetgeving worden ook speciale politieteams opgericht die zich bezig houden met de bestrijding van cybercriminelen (zie onder 2). Om criminaliteit effectief te kunnen bestrijden is kennis vereist over aard en omvang van de criminaliteit. Dat is ook één van de uitgangpunten van de informatiegestuurde politie (IGP). In deze benadering is het uitvoeren van wetenschappelijk onderzoek naar bepaalde criminaliteitsvormen een eerste stap in criminaliteitsbestrijding (Van Panhuis, 2008). Doordat er nog weinig empirisch onderzoek is gedaan naar de aard en de omvang van cybercrime, kan geconcludeerd worden dat het huidige opsporingsbeleid geen solide fundament heeft. In dit artikel beschrijven we de organisatie van de bestrijding van cybercrime in België. Daarnaast presenteren we de belangrijkste conclusies van recent empirisch onderzoek naar cybercrime in Nederlandse politiedossiers (Leukfeldt e.a, 2010). We besluiten dit artikel met de beschrijving van de implicaties die de onderzoeksresultaten hebben voor de Belgische politie.

2. De organisatie van de bestrijding van cybercrime in België

In 1992 zagen de Computer Crime Units (kortweg CCU) van de Gerechtelijke Politie het levenslicht. Drie jaar later, in 1995, voorzag ook de toenmalige Rijkswacht in de oprichting van een gespecialiseerde eenheid: het Team voor Bijstand en Opsporingen in Geautomatiseerde Omgevingen (kortweg BOGO-team). De reorganisatie van de politiediensten op federaal niveau bracht met zich mee dat het BOGO-team van de Rijkswacht en de National Computer Crime Unit van de Gerechtelijke Politie samensmolten tot de Federal Computer Crime Unit (Beirens, 1998). Naast deze FCCU werden ook Regionale Computer Crime Units opgericht. De FCCU moet er samen met de regionale CCU's voor zorgen dat politiediensten op een doeltreffende en snelle wijze bijgestaan worden in dossiers die verband houden met ICT-criminaliteit. De Federal Crime & Computer Unit (FCCU) is op dit moment de belangrijkste actor in de bestrijding van cybercrime in België. De federale politie heeft sinds de politiehervorming van 2001 geïnvesteerd in de oprichting en de uitbreiding van de gespecialiseerde diensten, de Federal Computer Crime Unit (FCCU) en de Regional Computer Crime Units (RCCU). Deze diensten bevinden zich op centraal niveau binnen de directie Economische en financiële criminaliteit (DJF) voor wat de FCCU betreft; en op arrondissementeel niveau voor wat de RCCU's betreft. Deze laatste zijn georganiseerd in 25 van de 27 gerechtelijke arrondissementen. In totaal zijn er op dit ogenblik 173 personen werkzaam binnen de CCU's, 33 binnen de FCCU en 140 binnen de RCCU's (Beirens, 2010).
De hoofdtaak van FCCU en RCCU ligt in het forensisch onderzoek op informatica gebruikt in alle vormen van criminaliteit en hulp bij opsporingen op internet (identificatie en lokalisatie van targets) in steun van lokale politie en alle FGP's en centrale opsporingsdiensten. Daarnaast bestaat hun opdacht uit de strijd tegen informaticacriminaliteit (hacking, spionage, sabotage) (Beirens, 2010).
Tot slot kunnen burgers en internetgebruikers via de website www.e-cops.be, uiteenlopende vormen van internetcriminaliteit melden (De Pauw, 2010b). De FCCU bestudeert de klacht en zal hem ofwel

doorspelen naar bevoegde instanties, ofwel zelf een onderzoek starten. Indien men zelf het slachtoffer werd van bepaalde feiten die zich afspeelden op internet, kan men contact opnemen met de regionale eenheid of zal de FCCU doorverwijzen naar de lokale politie om een klacht in te dienen (De Pauw, 2010b, Beirens, 2010). Vaak treden hier echter problemen op, aangezien de lokale eenheden niet over de know-how beschikken om met deze zaken aan te pakken (vgl. Toutenhoofd e.a., 2009).

3. Methodologische verantwoording

De resultaten die we hierna presenteren zijn afkomstig uit een empirisch onderzoek dat het lectoraat Cybersafety van NHL Hogeschool en Politieacademie uitvoerde in opdacht van het Nederlandse Korps Landelijke Politiediensten (KLPD). Doel ervan was het bieden van inzicht in de voor de politie meest relevante verschijningsvormen van cybercrime. Onderzoeksvragen waren: (1) wat is de aard van cybercrime, (2) wat zijn de daderkenmerken, (3) wat is de omvang van cybercrime en (4) wat is de maatschappelijke impact.

Er is (inter)nationaal gezien niet één algemeen geaccepteerde definitie van cybercrime in omloop (Sey e.a., 2008; Van de Hulst en Neve, 2008; PAC, 2008). Wij hanteren cybercrime als overkoepelend begrip voor alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict. Daarbij onderscheiden we twee subcategorieën. Voor delicten waarbij ICT zowel instrument als doelwit is, hanteren we de term 'cybercrime in enge zin'. Voorbeelden zijn hacken en de verspreiding van virussen. In de tweede subcategorie, 'cybercrime in ruime zin', vallen delicten waarbij ICT van wezenlijk belang is voor de uitvoering, maar waarbij ICT geen doelwit is. Voorbeelden hiervan zijn het plegen van fraude via internet en de verspreiding van kinderpornografie. Niet iedere verschijningsvorm van cybercrime kon in het onderzoek worden meegenomen, daarvoor is de lijst met cybercrimes te lang (bijvoorbeeld Domenie e.a., 2009; Van der Hulst en Neve, 2008). We richtten ons op de voor de politie meest relevante cybercrimes. Dat zijn cybercrimes die als belangrijke maatschappelijke problemen gezien kunnen worden en/of voor politie en justitie hoge prioriteit genieten. Dit is gedaan op basis van literatuuronderzoek en beleidsanalyse. We komen dan tot de volgende vijf vormen: hacken, e-fraude, cyberafpersen, verspreiding van kinderpornografie en haatzaaien. Identiteitsmisbruik (of -diefstal, zoals het vaak in de literatuur beschreven wordt) heeft ook prioriteit. Daarom hebben we bij alle andere cybercrime steeds gekeken of er sprake was van identiteitsmisbruik.

De belangrijkste onderzoeksmethode is een analyse over 665 politiedossiers. Op basis van sleutelwoorden selecteerden we aselect dossiers uit de registratiesystemen van de Nederlandse politie. We selecteerden 175 hackendossiers, 314 e-fraudedossiers, 13 cyberafpersingdossiers, 159 kinderpornodossiers en 40 haatzaaidossiers. Omdat cybercrime grensoverschrijdend is, veronderstellen we dat de bevindingen uit het Nederlandse onderzoek ook geldig zijn voor België.

4. Onderzoeksresultaten: de aard van cybercrime

De belangrijkste conclusie van het onderzoek is dat cybercrime niet alleen gepleegd wordt door (georganiseerde) high-tech criminelen uit verre landen. Bij aanvang van dit onderzoek zagen we dit beeld wel op basis van literatuur, de media en beleidsdocumenten. Dit beeld verdient echter te worden genuanceerd. Uit de dossiers blijkt juist dat er veel 'kleine delicten' gepleegd worden door min of meer alledaagse verdachten die individueel opereren. Dat wil natuurlijk niet zeggen dat er geen georganiseerde cybercriminele groeperingen actief zijn. Aangiften tegen dergelijke groepen zijn we in de dossierstudie echter bijna niet tegengekomen. Het beeld dat uit de dossierstudie komt is dat cybercrime dezelfde structuur heeft als klassieke (offline) criminaliteit. Ook bij de klassieke criminaliteit is er immers sprake van een grote groep daders die relatief kleine delicten (zoals diefstallen en inbraken) plegen op min of meer individuele basis en is er sprake van een aantal groeperingen dat zich bezighoudt met internationaal georganiseerde criminaliteit. Georganiseerde groepen hebben niet het monopolie op cybercrime. Cybercrime is van iedereen. De gemiddelde cybercrimineel in de Nederlandse politiedossiers is geen onderdeel van een georganiseerde bende whizzkids die extreem gecompliceerde dingen met een computer uithalen. Net als bij gewone criminaliteit zijn de meeste verdachten mannen onder de 45 jaar, en net als bij gewone

criminaliteit zijn er ook vrouwelijke verdachten en verdachten uit andere leeftijdscategorieën.
Bij e-fraude, de meest voorkomende cybercrime in de politiedossiers, moet men niet allereerst denken aan internationaal opererende bendes en technische hoogstandjes. De daders uit onze dossiers werken veelal alleen en putten uit een beperkt reservoir aan criminele technieken. Ze plaatsen een advertentie op een verkoopsite of maken een website die het slachtoffer ertoe moet brengen te betalen voor een goed of dienst die vervolgens niet wordt geleverd.
Dat het plegen van e-fraude, kinderpornodelicten en haatzaaien 'van het volk' is, is wellicht beter voor te stellen dan dat hacken dat is. In de literatuur wordt immers beweerd dat verdachten van hacken (net als e-fraudeurs) in hoge mate technisch onderlegd zijn (bv. Rogers, 2000; Van der Hulst en Neve, 2007). Maar blijkens ons onderzoek is het eens aan whizzkids voorbehouden hacken gedemocratiseerd, dat wil zeggen binnen het bereik van velen gekomen. Dat hacken alledaagser is geworden, heeft vermoedelijk (ook) te maken met de mate waarin mensen in onze samenleving gebruikmaken van en vertrouwd zijn geraakt met de virtuele wereld. Steeds meer mensen presenteren zichzelf op internet. Voor jonge mensen, opgegroeid met cyberspace, is het rommelen met andermans account of profiel niet per se een technisch hoogstandje, maar gewoon een manier om een ander te grazen te nemen. Ze weten hoe dat moet en maken van die kennis ook daadwerkelijk gebruik.

5. Implicaties voor politiebeleid in België

Cybercrime is dus van het volk. Dat komt er in de praktijk op neer dat cybercrime niet alleen wordt gepleegd door georganiseerde groeperingen uit het buitenland en dat de bestrijding van cybercrime dan ook *niet alleen* het domein moet zijn van specialistische teams (zoals nu overwegend het geval is). Kennis en kunde op het gebied van cybercrime moeten korpsbreed aanwezig zijn: iedere agent moet in ieder geval beschikken over enige basiskennis inzake cybercrime. Politiemensen krijgen niet alleen met op zichzelf staande cybercrimes te maken. Er is een groeiende kans dat agenten ook in klassieke zaken te maken krijgen met een cybercrime-aspect, denk bijvoorbeeld aan iemand die gestalkt wordt en waarvan het e-mailaccount wordt gekraakt.
Nieuwe generaties, die opgroeien in een tijdperk waarin de computer en internet niet meer zijn weg te denken, zullen steeds vaker te maken krijgen met cybercrime en met klassieke delicten zoals bedreiging, smaad en laster, waaraan een cybercrimeaspect zit. Dientengevolge krijgt de politie in de volle breedte van de organisatie vaker te maken met cybercrime: bijvoorbeeld bij sociale problemen voor de gebiedsagent, bij aangiften voor de intake, bij verhoor door de tactische recherche en bij het formuleren van beleid door de korpsleiding. Op dit moment heeft slechts een klein deel van de politiemedewerkers de benodigde basiskennis over cybercrime, terwijl het een groot deel van de politiemedewerkers raakt. Cybercrimezaken zijn echter juist vaak relatief kleine simpele zaken. Die komen niet bij de FCCU of RCCU terecht, waar de meeste kennis op het gebied van cybercrime is, en hebben daardoor een valse start. Het is de vraag of en hoe deze zaken worden opgepakt door de politieteams op lokaal niveau. De politieorganisatie zal zich moeten aanpassen. Het stimuleren van de aanwezigheid van de politie op het internet is hierin een eerste stap. Niet enkel de e-cops dienen zich online te bevinden, ook de lokale politie kan zich hierin profileren.
Een tweede belangrijke implicatie uit het genoemde onderzoek is dat hacken en e-fraude het alledaagse werkaanbod van de politie internationaliseren. Bijna een kwart van de hackenverdachten en bijna 15 procent van de e-fraudeverdachten opereert vanuit het buitenland. Door het mondiale karakter van internet is het voor verdachten makkelijk om over de grenzen slachtoffers te maken. Cybercrime, en hier dus vooral hacken en e-fraude, is een probleem dat lang niet altijd bij de landsgrenzen ophoud. Het werkaanbod van de politie internationaliseert.
Internationaal opererende daders zijn niet nieuw. Echter, van oudsher waren internationaal opererende daders in de regel onderdeel van een georganiseerde dadergroep (denk bijvoorbeeld aan drugs- en mensensmokkel). Internationaal opererende daders kwamen bij de politie dan terecht bij specialistische teams, namelijk teams die zich bezighielden met zware en georganiseerde criminaliteit. Bij cybercrime zijn het nu ook kleinere

criminelen die internationaal opereren. Ook het meer alledaagse werkaanbod van de politie wordt op deze wijze geïnternationaliseerd. Dat gaat dan politieonderdelen aan die tot voor kort misschien niet met internationaal opererende verdachten te maken kregen. Ook hier moet de politieorganisatie zich op instellen, wil ze niet achter de feiten aan (blijven) lopen.

Rutger Leukfeldt, Evelien de Pauw, Miranda Domenie en Wouter Stol *

Literatuur

Beirens, L. (1998) 'Op zoek naar criminele bits, digitaal rechercheren', *Politeia*, , afl. 8, 9-12.

Beirens, L. (2010) De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace. *Orde van de dag*, Kluwer, 49, 51-68. Boerstra, E. (1997) Rechercheren in cyberspace. *Algemeen Politieblad*, *146* (21), 8-9.

De Pauw, E. (2010a) Casestudy: de aanpak van overlast en criminaliteit in cyberspace. In: *Cahier Integrale Veiligheid, Europa en integrale Veiligheid*, Politeia, 139 -149.

De Pauw, E. (2010b) Sociale controle in online gemeenschappen. Een taak van de overheid of volstaat zelfregulering? *Orde van de Dag*, Kluwer, 49, 5-15.

Domenie, M.M.L., Leukfeldt, E.R., & Stol, W.Ph. (2009). *Werkaanbod cybercrime bij de politie. Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercrime*. Leeuwarden: Noordelijke Hogeschool Leeuwarden.

Duncan, M. (1997) Making Inroads Against Crime on the Internet. *RCMP Gazette*, *59* (10), 4-11.

Eecke, P. van (1997) *Criminaliteit in cyberspace: misdrijven, hun opsporing en vervolging op de informatiesnelweg*. Gent: Mys en Breesch.

Grabosky, N.P. & Smith, R.G. (1998). *Crime in the digital age*. Transaction Publishers: New Brunswick NJ.

Hendrickx, S.& Vercammen, M. (2010). Internetgebruik bij jongeren. Onderzoeksrapport OIVO, januari 2010 (www.oivo.crioc.org/files.nl/4689.nl.pdf)

Hulst, van der R.C. & Neve, R.J.M. (2008) *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders*. Den Haag: WODC.

Jewkes, Y. and M. Yar (2008) Policing cybercrime: emerging trends and future challenges. In: Handbook of policing. Second Edition.

Leukfeldt, E.R., M.M.L. Domenie en W.Ph. Stol (2010) Verkenning Cybercrime in Nederland 2009. Den Haag: Boom Juridische Uitgevers.

Moreas, M. (2007) Digitale kloof in Vlaanderen, SVR-rapport, Studiedienst van de Vlaamse gemeenschap, Brussel.

PAC (2008) *Programmaplan. Programma Aanpak Cybercrime*. De Bilt: interne notitie.

Panhuis, P. van (2008). Informatiegestuurde politie en criminaliteitsanalyse. In W.Ph. Stol & A.Ph. van Wijk (red.), *Inleiding Criminaliteit en Opsporing*. Den Haag: Boom Juridische uitgevers.

Rogers, M. (2000). *A New Hacker Taxonomy* (revised version). Manitoba: University of Manitoba, Department of Psychology.

Sey, A., Zinn, P., Oss, J. van & Schuurbiers, M. (2008) *Visiedocument 2007-2010 Team High Tech Crime. Dienst Nationale Recherche/Korps Landelijke Politiediensten*.

Stol, W.Ph., R.J. van Treeck and A.E.B.M. van der Ven (1999). *Criminaliteit in cyberspace – een praktijkonderzoek naar aard, ernst en aanpak in Nederland*. Den Haag: Elsevier.

Toutenhoofd-Visser, M.H., Veenstra, S., Domenie, M.M.L., Leukfeldt, E.R. & W.Ph. Stol (2009) *Politie en Cybercrime. Intake en Eerste Opvolging. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie*. Leeuwarden: NHL.

* Rutger Leukfeldt en Miranda Domenie zijn als onderzoeker verbonden aan het Lectoraat Cybersafety van NHL Hogeschool en Politieacademie. Evelien de Pauw is als docent en onderzoeker verbonden aan het Expertisecentrum Maatschappelijke Veiligheid, KATHO. Wouter Stol is lector van het lectoraat Cybersafety van NHL Hogeschool en Politieacademie, en bijzonder hoogleraar politiestudies aan de Open Universiteit Nederland.