Criminologie 2.0: over de worsteling met cybercrime

Wytske van der Wagen[a]
Patrick Van Calster[b]

[a] Promovenda Criminologie, Faculteit Rechtsgeleerdheid, Rijksuniversiteit Groningen, (Corresp.: w.van.der.wagen@rug.nl).
[b] Hoogleraar criminologie, Faculteit Rechtsgeleerdheid, Rijksuniversiteit Groningen (Corresp.: p.j.v.van.calster@rug.nl).

Cyberspace, of de virtuele wereld van het Internet, heeft de fysieke wereld die we bewonen flink uitgebreid, versneld en veranderd. Mensen brengen tegenwoordig in toenemende mate hun tijd door in cyberspace. Zij gaan er winkelen, bankieren, zoeken er informatie en onderhouden er (virtuele) vriendschappen. Het netwerk-technologische karakter van het Internet heeft afstanden doen verdwijnen en heeft het mogelijk gemaakt om ieder moment van de dag met een ieder waar ook ter wereld in contact te staan. Ook het bedrijfsleven en de overheid zijn voortdurend 'online' en plukken de vruchten van de vele mogelijkheden die Informatie- en communicatietechnologie (ICT) te bieden heeft. Er zit echter ook een schaduwzijde aan de voortschrijdende digitalisering en de prominente rol die cyberspace in het dagelijks leven van mensen speelt. Zo werd Nederland opgeschrikt door de DigiNotar-affaire die liet zien dat onze computersystemen zeer kwetsbaar zijn. De zaak Robert M. en de via Facebook beraamde moord op een tiener begin dit jaar lieten zien dat het Internet ook als *facilitator* kan fungeren. Cyberspace lijkt al lang niet meer uitsluitend een plek te zijn waar mensen veilig kunnen communiceren met anderen, kunnen experimenteren met hun identiteit en het leven kunnen leiden dat ze willen, zoals de utopisten ooit propageerden. Zij wordt tegelijkertijd beschouwd als een plek voor 'emotion dumping' (Hayward, 2012: 18) zoals scheldpartijen, bedreigingen, pesterijen, stalking en discriminatie/seksisme of als 'fantasy space' waar o.m. pedofielen gehoor kunnen geven aan hun fantasieën en lusten (Wilson & Jones, 2008).

Criminaliteit in cyberspace wordt doorgaans aangeduid met de term 'cybercrime'[1] en is een fenomeen dat zich lastig laat definiëren en classificeren. Voorbeelden van definities zijn: "Any crime that is facilitated or committed using a computer, network, or hardware device" (Gordon & Ford, 2006: 14) of "Criminal or harmfull activities that involve the acquisistion or manipulation of information for gain" (Wall, 2007: 10). In de literatuur wordt vaak een onderscheid gemaakt tussen cybercrime in 'ruime zin': traditionele delicten die door middel van ICT worden gepleegd (bv. cyberstalking, fraude en oplichting) en cybercrime in 'enge zin': de meer technologisch gefocuste vormen van cybercrime waarbij ICT zowel doelwit als instrument is (bijv. spamming, virusverspreiding, hacking). De financiële schade als gevolg van cybercrime loopt naar schatting in de miljarden (TNO, 2012). Verwacht wordt dat cybercrime en de daarmee gepaarde schade in de toekomst nog flink zal toenemen. Volgens Stol et al (2012) is de politie hier niet tegen opgewassen en ziet zij zich geconfronteerd met een fenomeen waar zij qua capaciteit en kennis onvoldoende voor uitgerust is. De criminologie zou wellicht in de kennislacune kunnen voorzien, maar is nog maar zeer recentelijk aan haar verkenningstocht in cyberspace begonnen.

Een terugkerend thema in zowel de internationale als de Nederlandse criminologische literatuur is de vraag of het bij cybercrime aan haar verkenningstocht in cyberspace begonnen.

Een terugkerend thema in zowel de internationale als de Nederlandse criminologische literatuur is de vraag of het bij cybercrime om 'oude wijn in nieuwe zakken' gaat of dat het een heel nieuw fenomeen betreft (Yar, 2005; Jewkes & Yar, 2010; McGuire, 2008; Leukfeldt et al, 2011). Deze vraag is niet alleen relevant in het kader van de theoreti-

1 Daarnaast bestaan er diverse andere begrippen zoals internet crime (Jewkes & Yar, 2010; Jaishankar, 2011), computer crime (Casey, 2011), hypercrime (McGuire, 2008), high tech crime' (Van der Hulst & Neve, 2008), technology-enabled crime (McQuade, 2006; Choo, 2008). De term 'cybercrime' heeft net als 'cyberspace, een 'onwetenschappelijk' en enigszins 'fictief' maar wordt tot op de dag van vandaag het meest gehanteerd (Wall, 2007: 2008).

sche duiding van het fenomeen, maar ook voor de manier waarop cybercrime aanpakt zou kunnen worden. Een aantal vragen maken duidelijk dat het vaststellen van de nieuwheid van cybercrime niet eenvoudig is: Wat zijn de criteria om een fenomeen als 'oud' dan wel 'nieuw' te betitelen? Is cybercrime überhaupt los te beschouwen van traditionele criminaliteit? En kan cyberspace als criminogene ruimte wel afgebakend worden van de fysieke ruimte? In deze bijdrage willen we hiermee een bescheiden begin maken. In het eerste deel van deze bijdrage wordt cybercrime afgezet tegen traditionele criminaliteit, zodat een helder beeld ontstaat van de oud/nieuw problematiek. Hierbij komen de volgende drie thema's aan bod: Het Internet versus eerdere technologische transformaties, lokaal versus globaal en fysiek versus virtueel. Het tweede deel omvat een reflectieve discussie over de oud/nieuwe kwestie waarbij tevens gepleit wordt voor een criminologische update aangaande de duiding van cybercrime.

Het Internet versus eerdere technologische transformaties

Het Internet heeft veel radicalere implicaties gehad dan haar voorgangers (zoals de telefoon en de telegraaf) omdat zij de verschillende communicatietechnologieën heeft samengebracht. Dit proces van *convergence* heeft geresulteerd in een toename van interfunctionaliteit, processen van voortdurende (technologische) updates/innovatie en steeds meer nieuwe technologieën om individuen met elkaar te kunnen verbinden (Wall, 2007). Het kan niet anders dan dat de netwerk-technologische aard van het internet zowel technologische als sociale implicaties heeft gehad voor de aard van het delict, daderschap en slachtofferschap.

Volgens Wall (2007; 2008) kunnen er drie (opeenvolgende) generaties van cybercrimes worden onderscheiden. De eerste generatie betreft criminaliteit waarbij de computer gebruikt wordt om traditionele criminaliteit mee te plegen. Deze vorm van cybercrime is in wezen 'oud'; ze vindt plaats middels nieuwe technologieën. De tweede generatie betreft hybriden waarin traditionele vormen van criminaliteit een globalere dimensie hebben gekregen. Zij is 'oud' als het gaat om de activiteit, maar 'nieuw' als het gaat om de instrumenten en de schaal waarop het plaatsvindt. De derde generatie verwijst naar de 'true' cybercrimes die volledig gegenereerd worden door netwerktechnologie, zij hebben een gedistribueerd en geautomatiseerd karakter (zijn dus minder afhankelijk van *social engineering*, het via bedrog loskrijgen van persoonlijke gegevens), zijn niet gebonden aan tijd en plaats en zouden compleet verdwijnen als het internet ophoudt te bestaan. Zij zijn uitsluitend het product van door het internet gegenereerde mogelijkheden. Er zijn niet alleen technologische implicaties voor de delicten, maar ook voor het daderschap. Hoewel er net als bij traditionele criminaliteit verschillende motieven kunnen zijn voor het plegen van cybercriminaliteit, zoals geld, woede, wraak, status, sadisme, lust, macht, avontuur (Rogers, 2006; Van der Hulst & Neeve, 2008; Leukfeldt et al, 2011) wekt het weinig verbazing dat we bij de 'true cybercrimes' in zekere zin met een ander type dader te maken hebben. Volgens Hilton en Irons (2006) zijn de activiteiten voor de meerderheid van deze daders eerder een 'spel' of intellectuele uitdaging dan het doelbewust overtreden van de wet. Volgens journalist Mischa Glenny (2011), die onderzoek deed naar cardingwebsites en de actoren die daarbij betrokken zijn, is een deel van de hackers eerder geïnteresseerd in prestige en roem, dan in geld.[2]

De netwerk-technologische aard van het internet heeft ook implicaties voor de sociale processen tussen (criminele) actoren (Wall, 2007). Op het internet kunnen daders immers gemakkelijker dan in de fysieke wereld (anoniem) met elkaar communiceren. Zo kunnen zij in zogenaamde virtuele netwerken, fora of Virtual Private Networks (VPN), ideeën, informatie en vaardigheden met elkaar uitwisselen. Zij komen op deze wijze in contact met personen die een aanvullend specialisme hebben of waarmee ze handel kunnen drijven in gegevens, apparaten of (kwaadaardige) software. Volgens Glenny (2011) speelt vertrouwen ten opzichte van traditionele criminaliteit een veel grotere rol bij het plegen van cybercriminaliteit omdat actoren meestal niet 'face to face' met elkaar in contact staan, onder pseudoniemen opereren, hun identi-

2 Volgens Leukfeldt et al (2010) zijn de 'true cybercrimes' niet alleen voorbehouden aan technologisch onderlegde personen. In toenemende mate komt deze vorm van criminaliteit ook in het bereik van gewone burgers (zie ook Leukfeld et al, 2011).

teit kunnen manipuleren en de sporen voor elkaar ook eenvoudig kunnen uitwissen. In dat opzicht zijn de sociale interacties tussen daders inderdaad anders dan bij traditionele criminaliteit. Echter, een ander aspect van de sociale interactie laat zien dat er ook wel degelijk overeenkomsten zijn met traditionele (georganiseerde) criminaliteit. Zo worden criminele fora gestructureerd via hiërarchische gezagsverhoudingen. Om de reputatie of het aanzien kenbaar te maken wordt bijvoorbeeld gebruik gemaakt van termen als 'Godfather,' en worden de belangrijkste actoren/leiders aangeduid als 'the Family' (Glenny, 2011). Kortom, ook in de 'true cybercrimes' kom je 'oude' aspecten tegen.

Lokaal versus globaal

Het Internet heeft naast sociale en technologische uitbreiding ook voor verdere globalisering van (cyber)criminaliteit gezorgd. Ten eerste heeft cybercrime ten opzichte van traditionele criminaliteit een zeer groot bereik zonder dat er veel geïnvesteerd hoeft te worden. Er kunnen meerdere delicten tegelijk worden gepleegd omdat voor veel criminele activiteiten dezelfde technieken worden gebruikt (Van der Hulst & Neeve, 2008). Technologie maakt het tegelijkertijd mogelijk dat slechts één dader of een (kleine) dadergroep veel (potentiele) slachtoffers tegelijk kan bereiken. Er worden weliswaar relatief veel slachtoffers gemaakt, maar er is weinig individueel leed per persoon (Knoops, 2011). Het globale karakter van cybercrime wordt nog verder gefaciliteerd door het feit dat cybercriminelen geautomatiseerde processen in gang kunnen zetten. Middels 'malware' kunnen zij zonder menselijke handeling wereldwijd een grote hoeveelheid computers infecteren (Wall, 2007). De schade die wordt aangericht is echter niet altijd te voorspellen of in te schatten. Ten tweede is cybercrime een fenomeen waarbij tijd en plaats niet of nauwelijks een belemmerende rol spelen. Een dader kan zich fysiek bevinden in land A, via een server in land B opereren en zijn slachtoffers in land C, D en E benaderen, bijvoorbeeld in landen waar bepaalde handelingen niet strafbaar zijn gesteld. In tegenstelling tot traditionele criminaliteit is cybercrime bovendien voortdurend en met grote snelheid aan het transformeren. Zo worden er constant nieuwe technieken en instrumenten ontwikkeld om blokkades voor de opsporing op te werpen. Anonimiteit, het gebruik van programma's zoals Onion routing, het versleutelen van gegevens (encryptie) en het gebruik van zogenaamde fast-flux netwerken die bestand zijn tegen (content) filtering (zie Lovet, 2009; Wall, 2007) maken dat cybercriminelen lastig getraceerd kunnen worden. De pakkans bij cybercrime is dan ook veel kleiner dan bij traditionele criminaliteit (zie voor een overzicht van de opsporingsproblemen o.a. Stol et al. 2012: 26).

Hoewel het Internet het mogelijk maakt om globaal te opereren, betekent het niet dat cybercrime intrinsiek een globaal fenomeen is. Het is belangrijk om voor ogen te houden dat cybercrime ook in een meer 'lokale context' kan plaatsvinden. Volgens Leukfeldt, Domenie en Stol (2011) zijn daders en slachtoffers vaak, net als bij traditionele criminaliteit, juist bekenden van elkaar zoals exgeliefden, vrienden, klasgenoten en zakenpartners. Ook stellen Leukfeldt, De Pauw, Domenie en Stol (2011) op basis van een dossierstudie, dat er, als het gaat om de structuur of 'schaal' van de criminaliteit, overeenkomsten zijn tussen traditionele criminaliteit en cybercrime. Er is in beide gevallen sprake van een meerderheid aan 'kleine' delicten of veelvoorkomende criminaliteit waar individuele daders bij betrokken zijn en in mindere mate is er sprake van georganiseerde misdaad. 'Oud' en 'nieuw' zijn dus wederom beide vertegenwoordigd.

Fysiek versus virtueel

In tegenstelling tot de meeste vormen van traditionele criminaliteit staan bij veel vormen van cybercrime niet zozeer fysieke of stoffelijke voorwerpen centraal, maar juist digitale gegevens en de toegang daartoe. Immers, de creditcard zelf wordt niet gestolen, maar wel de creditcardgegevens of de identiteit van mensen. Bovendien is het tegenwoordig mogelijk om 'virtuele diefstal' te plegen, denk maar aan de Runescape zaak, waarin het wegnemen van een virtueel masker en amulet gekwalificeerd werd als diefstal. Diefstal van (persoonlijke) gegevens wordt vergemakkelijkt door het feit dat mensen een groot deel van de dag online zijn, hun computers slecht beveiligen en veel persoonlijke gegevens op het Internet plaatsen (Furnell, 2010). De keerzijde van de voortdurende digitale aanwezigheid is dat *social engineering* gemakkelijker wordt gemaakt omdat criminele

actoren veel achtergrondinformatie over mensen kunnen verzamelen en daardoor eenvoudiger te weten kunnen komen welke wachtwoorden ze gebruiken (Miller in Hayward, 2012).

Naast de informatisering of digitalisering van goederen is er bij cybercrime in tegenstelling tot traditionele criminaliteit sprake van betrokkenheid van 'virtuele mensen,' actoren die in zekere zin niet menselijk of 'levend' zijn. Het meest prominente voorbeeld hiervan is virtuele kinderporno. Hierbij gaat het om kinderpornografisch materiaal dat wordt geproduceerd middels computersimulatie en waarbij geen gebruik is gemaakt van 'echte' kinderen. Dit is strafbaar gesteld omdat er 'echte' schade in de fysieke wereld kan uit voortvloeien. Een ander voorbeeld van virtueel slachtofferschap is cyberverkrachting, waarbij het virtuele self wordt geschonden (Williams in Brown, 2005: 232-233). Deze voorbeelden laten niet alleen zien dat we in toenemende mate te maken hebben met een versmelting tussen mens en technologie, maar ook dat virtuele of gesimuleerde activiteiten 'echte' consequenties kunnen hebben.

Discussie

Er zijn verschillende visies mogelijk ten aanzien van de vraag of cybercrime een vorm van criminaliteit is die fundamenteel nieuw is of dat zij een technologische voortzetting is van traditionele criminaliteit. Aangezien het fenomeen een zeer groot veld bestrijkt van delicten en criminaliteitsvormen is het erg ongenuanceerd om hier een eenzijdige uitspraak over te doen. Virtueel slachtofferschap, het op grote schaal geautomatiseerd kunnen plegen van delicten en het feit dat daders en slachtoffers op 'zero' afstand van elkaar bestaan zijn toch wel als voorbeelden te beschouwen die voor 'nieuw' pleiten. Het feit dat sommige delicten ten opzichte het traditionele delict slechts verschillen als het gaat om de gebruikte instrumenten ondersteunt daarentegen de 'oude wijn in nieuwe zakken' visie. De oud/nieuwheidskwestie wordt echter alleen nog maar lastiger omdat veel vormen van traditionele criminaliteit in toenemende mate een 'cyberdimensie' krijgen (Leukfeldt et al, 2011) bv omdat daders met elkaar via het internet in contact komen of hun slachtoffer via deze weg selecteren. Traditionele criminaliteit beweegt zich net als cybercrime in een complexere sociale (en digitale) realiteit. De vraag is dan: waar ligt de grens tussen traditionele criminaliteit en cybercrime en tussen 'oud' en 'nieuw' dan nog? En, zoals Thoman (2006: 390) stelt: "Will the 'new' have any meaning in a world that is updated by the microsecond everytime there is fresh activity in the system? Where smart objects know what we want before we have thought of it ourselves?" Wij zouden willen betogen dat de oud/nieuwheidskwestie illustreert dat de criminologie het probleem van cybercrime niet zozeer moet trachten te begrijpen door vast te blijven houden aan een dualistisch denkkader. Fysieke en virtuele realiteiten los van elkaar beschouwen, beperkt haar om de complexiteit van een techno-sociaal fenomeen als cybercrime te begrijpen (Brown, 2006). Cyberspace wordt dan ook al snel neergezet als een aparte ruimte, waarin iemand zich bevindt (zie McGuire, 2008: 6) en die los van de offline wereld bestaat. Cyberspace raakt echter, zoals reeds naar voren kwam, steeds meer met de fysieke ruimte vervlochten.[3] Cybercrime activiteiten kunnen dan meer als een 'proces' worden beschouwd: "as phenomena in constant dialogue and transformation with other phenomena/technologies" (Hayward, 2012: 16) en als fenomenen waarbij het 'oude' en het 'nieuwe' voortdurend door elkaar heen lopen en 'nieuwe' mogelijkheden genereren. Op soortgelijke wijze zou de criminologie, met het oog op de steeds verdergaande virtualisering, moeten afstappen van dualismen zoals mens en object. Het onderscheid tussen mens en object, natuur en cultuur is niet meer te maken in de huidige tijd (Brown, 2006) en heeft in wezen ook nooit bestaan (Latour, 1993).

Het feit dat de criminologie vooral 'oude' concepten toepast op een fenomeen dat op een aantal fronten tegelijkertijd ook fundamenteel 'nieuw'

3 Het is desalniettemin, ook in de criminologische context, niet noodzakelijk om af te stappen van het woord 'cyberspace' als 'ruimte,' omdat het wel degelijk mogelijk is om ruimtelijke eigenschappen toe te kennen aan cyberspace (die in de fysieke wereld niet gelden). Door woorden als 'cyberspace' te gebruiken doelt men volgens Yar (2005) niet noodzakelijkerwijs op twee aparte ontologische werelden zoals McGuire (2008) stelt. Belangrijk is om voor ogen te houden dat je de twee werelden los kunt benoemen, maar niet los van elkaar kunt beschouwen.

of 'anders' is, is een ander punt van aandacht. Veel concepten die centraal staan in de verklarende schema's van de meeste criminologische theorieën zoals (fysieke) locaties, activiteiten en doelwitten verliezen aan betekenis in de hedendaagse sociale werkelijkheid. Theorieën zoals de Routine Activity Theory (RAT) blijven erg populair voor het begrijpen van cybercrime en het slachtofferschap daarbij (Holt & Bossler, 2009; Pratt et al, 2010) ondanks het feit dat het perspectief grove tekortkomingen heeft in onze gedigitaliseerde wereld. Immers, in cyberspace zijn geen tijd- en afstandsbarrières, aspecten die slechts beperkt door de RAT zijn te ondervangen (Yar, 2005; Campbell, 2011). Om met de complexiteit van cybercrime om te gaan zou de criminologie juist bereid moeten zijn nieuwe theoretische concepten te ontwikkelen. Zo stelt Brown (2006) dat Latours 'Actor Network Theory' (ANT) een zinvolle bijdrage kan leveren aan het begrijpen van hedendaagse criminologische fenomenen, omdat in dit perspectief de interactie centraal staat tussen menselijke en niet-menselijke relaties. Als het gaat om de duiding van de ruimtelijke aspecten van criminaliteit en cyberspace zou ANT eveneens kunnen worden toegepast (zie Baloch & Cusack, 2009). Ook kan in dit kader gedacht worden aan de Non-Representational Theory (NRT) een cultureel geografische benadering die aandacht besteedt aan complexe, 'experiential' en affectieve en inter-materiële aspecten van ruimte. NRT wil niet zozeer laten zien hoe gedrag of emoties in de ruimte ontstaat, maar juist hoe zij de ruimte vormen (Hayward, 2012).

Kortom, volgens ons zou de criminologie bij haar verkenningstocht in cyberspace een hybride bril moeten opzetten. We moeten ons echter ook niet volledig van het 'oude' distantiëren omdat dan het gevaar van een technologisch fetisjisme of een cyberpunk-criminologie op de loer ligt. Een verrijking of beter gezegd, een update van de criminologie waarbij bruikbare hybride concepten worden ontwikkeld is volgens ons een stap in de goede richting om de criminologische fenomenen van deze tijd beter te begrijpen.

Referenties

Baloch, F.K. en Cusack, B. (2009). Re-visualizing Cyberspace: Using Quasi Objects for Spatial Definitions, 20th Australasian Conference on Information Systems, 2-4 Dec, Melbourne

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. Theoretical criminology, 10(2), p. 223 – 244

Campbell, E. (2011). Landscapes of performance: stalking as choreography. Environment and Planning D: Society and Space, 29, p. 1 – 18

Casey, E. (2011). Digital evidence and computer crime: forensic science, computers and the internet. Waltham: Elsevier Inc.

Choo, K, -K. R. (2008). Organized crime groups in cyberspace: a typology, Trends in Organized Crime, 11, p. 270- 295

Furnell, S.M. (2010). Online identity: giving it all away? Information security technical support, 14(2), p. 42-46

Glenny, M. (2011). Dark Market: Cybercriminelen, Cyberpolitie en onze veiligheid in een digitale wereld. Amsterdam: Anthos Uitgevers

Gordon, S. en Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2, p. 13-20

Hayward, K.J. (2012). Five spaces of cultural criminology. British journal of criminology, 52 (3), p. 441-462

Hilton, K. en Irons, A. (2006). A "Criminal Personas" approach to criminal activity. Crime Prevention and Community Safety; an international Journal, 8, p. 248 – 259

Holt, J.T. en Bossler, A.M.: Examining the applicability of Lifestyle- routine activities theory for cybercrime victimisation. Deviant Behaviour, 30, 1–25 (2009)

Hulst, R.C. van der en Neve, R.J.M. (2008). High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie. Boom Juridische Uitgevers: Wetenschappelijk Onderzoek- en Documentatiecentrum

Jaishankar, K. (2011). Cyber Criminology. Exploring Internet Crimes and Criminal Behaviour. Boca Raton: Taylor & Francis Group

Jewkes, Y. & Yar, M. (2010). Handbook of internet crime. United Kingdom: Willan Publishing.

Knoops, B-J. (2011). The Internet and its opportunities for cybercrime. Tilburg Law School Legal Studies Research Paper Series, 9, p. 734 – 754

Latour, B. (1993). We have never been modern. Cambridge: Harvard University Press

Leukfeldt, E.R. en Stol, W.Ph. (2012). De rol van internet bij fraudedelicten; internetfraudeurs en klassieke fraudeurs vergeleken, Justitiële Verkenningen, 38(1), p. 108-120
Leukfeldt, E.R., M.M.L. Domenie en W.Ph. Stol (2011) Cybercrime is van het volk. Onderzoeksconsequenties voor de beleidsvorming. Secondant. 25 (1) 42-45
Leukfeldt, E.R., Pauw, E. de, Domenie, M.M.L. en Stol, W.Ph. (2011) Oude wijn in nieuwe zakken? De aard van cybercrime en de implicaties voor de opsporingspraktijk. Panopticon, 32 (2), p. 70-74
Lovet, G. (2009). Fighting cybercrime: technical, juridical and ethical challenges. Virus Bulletin Conference, Geneve. Geraadpleegd op 5 maart 2012 via < http://208.91.114.28/sites/default/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf
McQuade, S. (2006). Technology-enabled crime, policing and security, Journal of Technology Studies, 31(1), p. 32 – 42
McGuire, M. (2008). From Hyperspace to Hypercrime. Technologies and the new geometries of deviance and control. Papers from the British Criminology Conference, 8, p. 3 – 17
Pratt, T.C, Holtfreter, K. & Reisig, M.D. (2010). The Routine Online Activity and Internet Fraud Activity: Extending the Generality of the Routine Activity Theory. Journal of Research in Crime and Delinquency, 47, p. 267-296
Rogers, M.K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, 3(2), p. 97-102
Stol, W., Leukfeldt, E. en Klap, H. (2012). Cybercrime en politie; een schets van de Nederlandse situatie anno 2012, Justitiële Verkenningen, 38(1), p. 25-39
Thomas, S. (2006). The end of cyberspace and other surprises. Convergence: The International Journal of Research into New Media Technologies
TNO, 2012, Kosten cybercrime grotendeels voor bedrijfsleven. Geraadpleegd op 15 mei 2012 via: http://www.tno.nl/content.cfm?context=thema&content=prop_nieuwsbericht&laag1=897&laag2=920&laag3=115&item_id=2012-04-10%2011:37:10.0&Taal=1
Wall, D.S (2007). Cybercrime. The Transformation of Crime in the Information Age. Malden: Polity Press
Wall, D.S. (2008). Cybercrime and the culture of fear, Information, Communication & Society, 11(6), p. 861-884
Wilson, D & Jones, T (2008). 'In My Own World': A Case Study of a Paedophile's Thinking and Doing and His Use of the Internet. The Howard Journal, 47(2), p. 107 – 120
Yar, M. (2005). The Novelty of Cybercrime. European Journal of Criminology, 2(2), p. 407 – 427

Maatschappelijke dienstverlening / social work (1)

Criminalisering in de vreemdelingenwetgeving. Schijnhuwelijken als casus

Jan De Lien[a]

[a] Advocaat, Balie Antwerpen (Corresp.: jan.delien@progresslaw.net).

1. Inleiding

Van 1800 tot 1914 heeft Europa zijn migraties vooral als emigraties ervaren. Tussen 1920 en 1940 (in het geval van het Verenigd Koninkrijk en Frankrijk) en tot 1960 (voor landen als Duitsland en België) waren er wel immigraties op gang gekomen maar die bleven grotendeels binnen Europa. Het is eigenlijk pas vanaf 1960 via de arbeidsmigratie uit de Maghreb- landen en Turkije, dat Europa voor het eerst met de niet-Europese migrant in contact is gekomen. Dit wil zeggen dat ruim drie vierde van de Belgische migratiegeschiedenis niet als een inwijking van van vreemdelingen ervaren wordt. Immigratie is dus eigenlijk een zeer recent fenomeen.

De arbeidsmigratie werd in 1974 stopgezet. Dit was een gevolg van de oliecrisis, die geleid heeft tot een algemene economische recessie. In de meeste West-Europese landen werden in die periode gelijklopende restricties ingevoerd. De immigratiestop betekende echter geenszins het einde van de migratie. Er vond een verschuiving plaats, waarin een deel van de arbeidsmigratie in de tweede helft van de jaren 70 werd vervangen door "volgmigratie" (gezinshereniging en huwelijksmigratie).

In de jaren 80 werd de "asielmigratie" belangrijker. Dit had zichtbare en voelbare gevolgen op vlak