

Matthias Dobbelaere

1. INLEIDING EN BEGRIPSOMSCHRIJVING

Is surfen op andermans internet strafbaar? De allereerste rechtszaak over dit brandend actueel thema werd onlangs in België behandeld.

De officiële aanklacht van het openbaar ministerie luidt “externe hacking”. Belangrijk is het verschil tussen ‘externe’ en ‘interne’ hacking. Externe hacking houdt in *het ongeoorloofd toegang verwerven tot een informaticasysteem of zich daarin handhaven*.¹ Interne hacking komt voor wanneer *hij die met bedrieglijk opzet of met het oogmerk om te schaden zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt..*² Cruciaal zijn de verschillen tussen beide figuren. Daar waar het materieel element bij ‘externe hacking’ ligt in het ongeoorloofd toegang verkrijgen, ligt het materieel element bij ‘interne hacking’ in het overschrijden van de bevoegdheid. Naast het materiële, is ook het moreel element van uitermate groot belang. Bij ‘externe hacking’ spreken we over een algemeen opzet, bij ‘interne hacking’ over het bedrieglijk en/of met opzet (oogmerk) om te schaden.

In casu gaat het om surfen op andermans internet, door het gebruik van een laptop met een Wi-Fi (Wireless-Fidelity) ontvanger. De eigenaar van deze laptop, een 22-jarige Pool, ging stevast met zijn wagen in een welbepaalde straat draadloos internet gaan aftappen van een onbeveiligd netwerk. De man palmde het internet van zijn “slachtoffers” zo in, dat zijzelf niet meer in staat waren om op internet te surfen (dit door de datalimieten). Een voorbijganger vond het verdacht dat de man steeds in dezelfde straat met zijn laptop op zijn schoot zat te surfen en alarmeerde de politie.³

De man is door het parket van Dendermonde aangeklaagd voor externe hacking, en dit omdat de draadloze connectie weliswaar illegaal is, maar anderzijds geen werkelijke schade heeft toegebracht (bv. diefstal van gegevens, het onmogelijk maken van toegang tot het systeem, het onklaar maken van essentiële bestanden, enz.).

Een kritische bedenking dringt zich op. Is men als eigenaar niet verantwoordelijk voor het beveiligen van de draadloze internetverbinding? Anders gezegd, indien men er, al dan niet bewust, voor kiest zijn netwerk *niet* te beveiligen, stelt men dit netwerk dan niet open voor gedeeld gebruik? De wetgever heeft de beveiliging niet opgenomen als voorwaarde in de strafbaarstelling, maar kon zij acht jaar geleden reeds weten welke de implicaties zouden zijn van onbeveiligde draadloze netwerken?

¹ Art. 550bis, §1 Sw.

² Art. 550bis, §2 Sw.

³ De Standaard, “Jongenman kraakt internet buur”, 8 april 2008, <http://www.standaard.be> en Het Belang van Limburg, “Op andermans internet surfen kan jaar cel kosten”, 4 oktober 2008, <http://www.hbvl.be>

Matthias Dobbelaere

2. RELEVANT PROCEDUREEL KADER

a. Strafrechtelijke basis: *nullum crimen sine lege*.

De strafrechtelijke basis voor de hoger besproken 'externe hacking' ligt in art. 550bis, §1 Sw., ingevoerd door art. 6 van de Wet inzake informaticacriminaliteit van 28 november 2000. Art. 550bis Sw. richt zich specifiek tot het wederrechtelijk toegang verkrijgen tot een systeem of een deel ervan waartoe men niet gerechtigd is.

b. Strafmaat.

Van uitermate belang voor de strafmaat is de vraag of er sprake is van bedrieglijk opzet. Dit aangezien de maximumstraf zonder het bedrieglijk opzet een gevangenisstraf van maximum 1 jaar kan opleveren, terwijl het aanwezig zijn van bedrieglijk opzet deze maximumstraf tot 2 jaar kan doen oplopen.⁴ Het is m.i. belangrijk het begrip 'bedrieglijk opzet' juist te kaderen inzake het "WiFi-liften". Het zou immers tot foute conclusies leiden indien men in deze het begrip 'opzet' al te letterlijk neemt aangezien men (quasi) steeds bewust connectie maakt met een netwerk. Men moet eerder kijken naar het al dan niet optreden van economische schade. Het bedrieglijk opzet moet hier dan ook worden begrepen als het toebrengen van economische schade door bv. de diefstal van gegevens terwijl men gebruik maakt van de draadloze internetverbinding. Indien men zich beperkt tot het legaal surfen kan er geen sprake zijn van een bedrieglijk opzet, en is de maximumstraf dan ook beperkt tot 1 jaar.

c. Kort: recidive en de poging.

Recidive werd in art. 550bis, §8 Sw. uitdrukkelijk behandeld. Het regime inzake herhaling is vrij streng. Indien een misdrijf uit art. 550bis, §1 - §7 begaan wordt binnen de 5 jaar na een eerdere veroordeling, worden de straffen verdubbeld.

Art. 550bis, §4 Sw. stelt de strafmaat van de poging gelijk aan die van het voltooide misdrijf. De wetgever wou hiermee aangeven dat de poging op zich ernstig wordt genomen en dat zij bovendien een onmiddellijk gevaar voor het systeem betekent. Bv. de dader plaatst een virus op het systeem van het slachtoffer. Dit virus is geprogrammeerd om a) wachtwoorden te stelen en b) de antivirus software uit te schakelen. Enkel b slaagt. Er is geen sprake van een voltooid misdrijf. Niettemin is het systeem door verlies van beveiliging ernstig in gevaar.

⁴ Art. 550bis, §1 Sw.

Matthias Dobbelaere

3. STRAFBAARHEID WIFI-LIFTEN

Uitgaande van de veronderstelling dat elke onrechtmatige verbinding met andermans draadloos netwerk een strafbaar feit zou uitmaken leidt dit tot zeer verre gaande gevolgen. Een hotelgast die zijn laptop openklapt en via (bijvoorbeeld) het Windows 'Netwerk Center' automatisch verbinding maakt met een onbeveiligd draadloos netwerk zou zich schuldig maken aan 'externe hacking', terwijl deze in de overtuiging kan zijn verbinding te hebben gemaakt met het netwerk van het hotel. Hetzelfde zou gelden voor de persoon die met de laptop eenmalig, en al dan niet bewust, verbinding maakt met een onbeveiligd netwerk om snel iets op te zoeken of de e-mails te bekijken.

Maken alle gevallen van WiFi-liften een strafbaar feit uit? Of is er nood aan criteria waaraan de rechter de concrete zaak kan toetsen? Indien men de eerste hypothese zou volgen kan men ontelbare situaties voorzien waarin een onoplettend persoon zich schuldig zou maken aan externe hacking. Dat laatste kan niet de bedoeling van de wetgever zijn en zou enkel zorgen voor grote rechtsonzekerheid, zowel bij eindgebruikers als bij politionele en gerechtelijke diensten.

De criteria die men kan vooropstellen zijn de volgende. Allereerst kan men kijken naar de **frequentie** van de inbreuk. Het kan immers niet de bedoeling zijn een eenmalige inbreuk – die zich beperkt tot het louter (legaal) surfen – te sanctioneren. Een tweede criterium die men kan aanwenden is die van het **bandbreedte-verbruik** van de gemaakte verbinding. Het is namelijk niet uitgesloten dat een persoon slechts eenmalig verbinding maakt met een welbepaald onbeveiligd draadloos netwerk en tegelijkertijd binnen een aantal uren de bandbreedte van het slachtoffer grotendeels opsloort (bv. door het downloaden van films). Een derde en laatste criterium die men vervolgens kan hanteren is die van de **onrechtmatigheid** van het surfgedrag. Terwijl bovenstaande criteria eerder eenvoudig en technisch vast te stellen zijn, gaat dit derde criterium in op de eigenlijke inhoud van de verbinding. Het hoeft geen nader betoog dat surfen naar een e-mail account wezenlijk verschilt van het surfgedrag van iemand die op zoek is naar kinderporno, illegale wapens of terreurwebsites. Het spreekt voor zich dat ook wanneer iemand niet wordt gevat door bovenstaande criteria strafbaar blijft wanneer hij eerst een beveiliging moet doorbreken vooraleer hij in staat is om verbinding te maken met het draadloos netwerk. Deze criteria hoeven bovendien niet cumulatief vervuld te worden, voldoen aan één van de criteria is voldoende om strafbaar te kunnen worden gesteld.

Bovenstaande criteria sluiten in elk geval de onoplettende computergebruiker uit, evenals de persoon die, al dan niet wetens willens, verbinding maakt met een onbeveiligd draadloos netwerk, maar zich daarin beperkt tot een eenmalige en kortstondige connectie met legaal surfgedrag. Toegepast op de concrete casus betekent dit dat een veroordeling gewenst is. Immers, het eerste criterium (*frequentie*) is van toepassing (herhaalde connecties), evenals de opsloping van bandbreedte waardoor het slachtoffer in casu niet in staat was om nog normaal te surfen. Het derde criterium is in deze zaak niet van toepassing.

Matthias Dobbelaere

4. ONTBREKEN VAN BEVEILIGING: CIJFERS & GEVAREN

Volgens een onderzoek van BIPT (Belgisch Instituut voor postdiensten en telecommunicatie) beschikt ruim 30% van de Belgische computergebruikers over een draadloos netwerk. In maar liefst 48% van de gevallen laat men na de draadloze internetconnectie te beveiligen.⁵ Onderzoek in Nederland door Dimension Data⁶ bracht aan het licht dat slechts 54% van de draadloze privénetwerken goed (met WPA of WPA2) is beveiligd. 28% gebruikt de zwakkere (en eenvoudig te kraken) WEP-encryptie en iets minder dan een vijfde is zelfs helemaal niet beveiligd. Voornaamste oorzaak van de niet-beveiliging is de onwetendheid van de eigenaar. Ook de technische onkunde kan een grote rol spelen. Echter mag niet alleen met de vinger worden gewezen naar de eindconsument. Aanbieders van draadloze netwerk-routers zouden verplicht moeten worden om een gebruiksvriendelijke 'wizard' (een programma dat stap voor stap de instellingen overloopt) uit te werken en daarin de klemtoon te leggen op de noodzaak van beveiliging. Een andere mogelijkheid is dat de aanbieder standaard de beveiliging incorporeert in het eindproduct en de gebruiker dan eenvoudigweg de nodige uitleg krijgt hoe deze beveiliging toe te passen.

Een draadloze netwerkverbinding onbeveiligd laten kan nochtans zware gevolgen hebben voor de eigenaar ervan. Een persoon die verbinding maakt met een onbeveiligd draadloos netwerk en vervolgens op zoek gaat naar kinderporno, illegale wapens, terreurorganisaties, etc. doet dit met de identificatie (IP-adres) van de draadloze netwerkverbinding. Politie-diensten die dergelijk surfgedrag op het spoor komen verdenken dan bijgevolg de (onschuldige) eigenaar. In dergelijk geval is het bewijs van onschuld zeer moeilijk te leveren en de gevolgen voor de eigenaar niet te overzien. Hetzelfde geldt voor diegene die via peer-to-peer programma's of nieuwsgroepen grote hoeveelheden auteursrechtelijk beschermd werk binnenhaalt. Wederom zal de verdenking op de eigenaar rusten. Er is ontegenzeggelijk nood aan meer ruchtbaarheid en sensibilisering dringt zich dan ook op.

5. DE UITSPRAAK

Op 14 november 2008 wordt bekend gemaakt dat de jongeman schuldig is verklaard aan surfen op andermans netwerk.⁷ De strafrechter heeft echter de gunst van opschorting van straf toegekend aan de beschuldigde. Het lijkt er dus op dat de Belgische strafrechter in dit precedent een belangrijk signaal wou uitdragen, evenwel blijft een gefundeerde motivering uit. Het is nochtans van uitermate groot belang voor de rechtszekerheid dat er duidelijke en gemotiveerde criteria gehanteerd worden, die later consistent kunnen worden toegepast.

⁵ BIPT, "Een draadloos netwerk beveiligen", http://www.bipt.be/nl/520/ShowContent/2885/Draadloze_netwerken/Een_draadloos_netwerk_beveiligen.aspx.

⁶ Dimension Data, "Draadloze netwerken slecht beveiligd", 23 juni 2008, http://www.dimensiondata.com/NR/rdonlyres/0586CF39-2C12-4077-9CD6-4D59280F7FE4/9668/Draadloze_privenetwerken_slecht_beveiligd1.pdf.

⁷ De Standaard, "Jongeman schuldig aan surfen op andermans netwerk", 14 november 2008.

Matthias Dobbelaere

6. HET DATACENTER-VONNIS

Recentelijk werd een soortgelijke zaak in Nederland behandeld door de Amsterdamse rechtbank.

Een groep verdachten had in een studentenflat een klein datacenter aangesloten op de aanwezige internetverbinding, welk verborgen werd gehouden door tijdelijk verwijderde plafondplaten. De eigenaar ontdekte dit ruim een half jaar na het plaatsen en de groep werd beticht van diefstal van dataverkeer, capaciteit van bandbreedte en uiteraard het aftappen van internet. De uitspraak is min of meer opvallend te noemen. De meervoudige strafkamer van de Amsterdamse rechtbank oordeelde dat *“door ongeoorloofd gebruik te maken van bandbreedte de rechthebbende immers niet noodzakelijk de feitelijke macht verliest”*.⁸ De rechtbank wees er ook op dat bovenstaande genoemde zaken geen ‘goederen’ zijn zoals in het artikel 310 van het Wetboek van Strafrecht staat aangegeven, waardoor van diefstal geen sprake is.

De gevolgen van deze rechtspraak zijn legio. Men kan hier een vrijgeleide in zien om in Nederland naar eigen goeddunken gebruik te maken van onbeveiligde netwerken. Bovendien mag men de datalimiet bij dit gebruik volledig onwerkbaar maken (door excessief veel te downloaden) zonder dat dit als ‘diefstal’ kan worden aanzien. Een positief gevolg is dat eigenaars van een onbeveiligde verbinding sneller geneigd zullen zijn deze toch te beveiligen. Gezien de heimelijke installatie van een datacenter (dat uiteraard met kwaad opzet werd geïnstalleerd) dringt een matiging of een correctie van dit vonnis zich niettemin op. Indien men deze zaak ook op de reeds geformuleerde criteria (zie *supra*) toepast, dan merken we dat ook in deze zaak een veroordeling gewenst zou zijn (toepassing *frequentie* en *bandbreedte-verbruik* criteria).

7. BESLUIT

Met de opkomst van de zgn. ‘mini-laptops’ zal het onrechtmatig verbinding maken met een draadloos netwerk alleen maar toenemen. Het belang van de uitspraak mag echter niet overschat worden. Er werd weliswaar besloten tot een veroordeling maar een effectieve straf evenals een gedegen motivering bleven uit. Niettemin zal dit vonnis ongetwijfeld gevolgen hebben voor de politionele en juridische kijk op dit fenomeen. Afsluitend kan gewezen worden op een belangrijk discussiepunt. Draagt de eigenaar een verantwoordelijkheid in het beveiligen van het netwerk? De wetgever heeft in de Wet inzake Informaticacriminaliteit niet in een dergelijke verantwoordelijkheid voorzien. Anderzijds kon men acht jaar geleden onmogelijk de problematiek van WiFi-liften voorspellen. De toekomst zal moeten verduidelijken of, hetzij door een wijziging in de wetgeving, hetzij door innoverende rechtspraak, er al dan niet rekening zal gehouden worden met de rol en de aansprakelijkheid van de eigenaar.

⁸ Rechtbank Amsterdam (meervoudige strafkamer), 11 september 2008, <http://www.boek9.nl>.